Operations and Intelligence Report

Metrobank

April 2017

BEST IN CLASS – INFORMATION SECURITY

INTELLIGENCE AND OPERATIONS

Table of Contents

1. About This Report

The purpose of this document is to report on the "state" of security for your organization. It must be noted that GLESEC bases its information analysis on the systems under contract. The information generated by these systems is then aggregated, correlated and analyzed. The more complete the set of systems under contract the more accurate and complete the results will be. The report is organized to provide an executive summary with recommendations (as necessary or applicable) followed by more detailed information.

We at GLESEC believe information security is a holistic and dynamic process. This process requires on-going research and follow up. Holistic since no single "device" can provide the security necessary for an organization. Technology alone cannot provide the security necessary, but people that understand the operations and information generated by the security devices are a key to proper security. The process is dynamic since due to the nature of Internet security given the constant discovery of new security vulnerabilities and exploits, the proliferation of hacking tools that make it easier for script-kiddies with minimal knowledge to cause damage. The increase in malware, phishing, insider threats, espionage, organized crime, intellectual property theft, and hacktivism are the very cause of information security exposure and are most commonly driven by financial gain.

2. Confidentiality

GLESEC considers the confidentiality of client's information as a trade-secret. The information in this context is classified as:

a) Client name and contact information
b) System architecture, configuration, access methods and access control
c) Security content

All the above information is kept secure to the extent in which GLESEC secures its own confidential information.

3. Scope of This Report

GLESEC Contracted Services

MSS: Managed Security Service (full outsourcing)

Service	Manufacturer	Model	Service Expiration
MSS-APS	Radware	DefensePro 516 ODS2-S1	06/01/2017
MSS-APFW	Radware	AppWall ODS1XL	06/01/2017
MSS-VME			06/01/2017

4. Executive Summary

This report corresponds to the period from April 1, 2017 to April 30, 2017.

This month we see an increase of **3**% in attack activity from prior month and approximately a **19**% drop in **critical** attacks over the prior month. Most of the attacks are short in duration (less than a minute), this month there are only a few attacks of more than one hour.

Most are targeting multiple ports followed by port **80**, port **4500** and port **5060** attacks. Which is consistent with the previous month.
Approximately **12**% of the attacks this month are coming from GLESEC's tracked "known threat sources" which is a significant decrease over the previous month.

Most of the attacks this month are from the **United States, Panama, Germany, Columbia, United Kingdom, China, Russian Federation, Netherlands, Ukraine, and France**
The US continues to account for the bulk of the attacks on your site, originating approx. 65% of total attacks this month.

The bulk of the attacks, **38**%, are **Scanning** attacks, which are specifically designed to probe the perimeter and map the network infrastructure to collect data to plan more detailed attacks. The DefensePro is able to recognize and block this type of attack effectively.

This month we blocked a number of critical attacks that are Behavioral-DOS based and that target the perimeter and web-server vulnerabilities that have exist in your environment for some time and have been identified in several previous reports.

While this shows the effectiveness of the protection provided by our countermeasures, we believe that potential actors may see these vulnerabilities and try to exploit them and while we are stopping the attacks we recommend that you adopt a more proactive security posture by reducing these vulnerabilities.

There are 7 out of 23 vulnerable hosts. The vulnerabilities in April are **7** critical, **5** high, **44** medium vulnerabilities and **10** low to a total of **66** total.

The categories for vulnerabilities this month is:
General vulnerabilities are the most prevalent vulnerability category with **33** detected vulnerabilities followed by Web Servers with **11**, then both Misc and CGI abuses with **8** each, Service Detection with **3**, and Windows with **3** for the report period.
The DefensePro and Appwall both have operated properly with **100.00%** up time and good performance.

Risk Value

To provide a way to quantify the risk of a Company, GLESEC introduces a definition for a metric value to capture the exposure risk that allows evaluating the vulnerabilities and also the record of change over time. This procedure to qualify can be used to evaluate the ROI in the security measures we have implemented.

It is important to mention that this metric considers a median value for the vulnerabilities classified as ¨high¨, ¨medium¨ and ¨low¨, given them a value of 100% 50% and 10% to each, so the factor of the total number of system that are vulnerable.

This takes into consideration all of the vulnerabilities, but is important to point out that these values (100, 50 and 10) are arbitrary chosen by us, so this measure can in time change as we understand more of the risk involved. We can use this metric to evaluate the progress in time and to compare one over the other using a common amount set.

Total IP's Scanned	IP's Vulnerable
23	7

Risk Distribution				
Critical	High	Medium	Low	Total
7	5	44	10	66

Risk Value	0.2
Vulnerabilities Weighted Sum	0.67

According to the metrics:

RV= 0.2

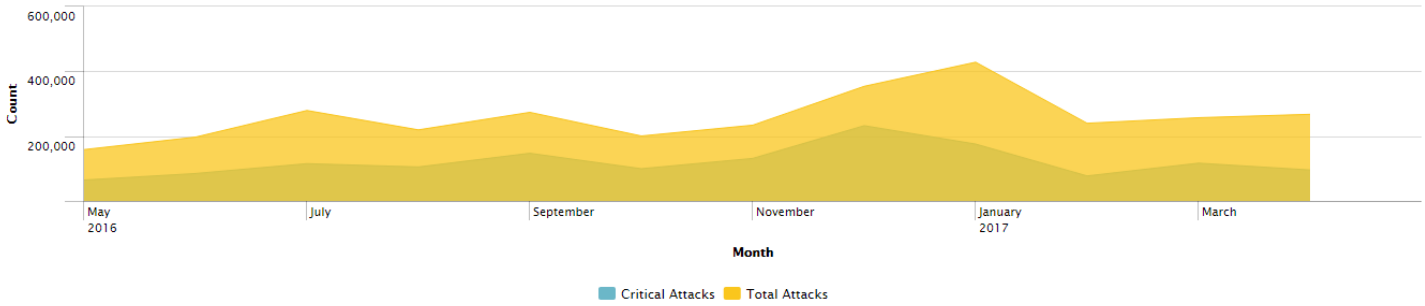
The following values are to clarify RV:
RV=1 Points to every IP address in the infrastructure that are susceptible to attacks
RV=0 Points to no IP address in the infrastructure aret susceptible to attacks
RV=0.1 Point to 1/10 IP address in the infrastructure that are susceptible to attacks

Attack Summary

Based on the information gathered from the DefensePro and AppWall during this period **267,343** attacks on Metrobank, **95,553** of which were considered critical were all stopped by the Radware devices.

Metrobank receives an average of **251,594** total attacks and **116,869** critical attacks on a monthly basis which equates to an average of **9,094** total daily attacks and **4,224** critical daily attacks. As the graph illustrates total attack levels in relation to the previous report period totaled **257,049** total attacks and critical attacks in compared with a last period's total of **116,595**.

This statistical graph provides the count of critical and total attacks blocked per month calculated on a rolling 12 month period (Last 12 months)

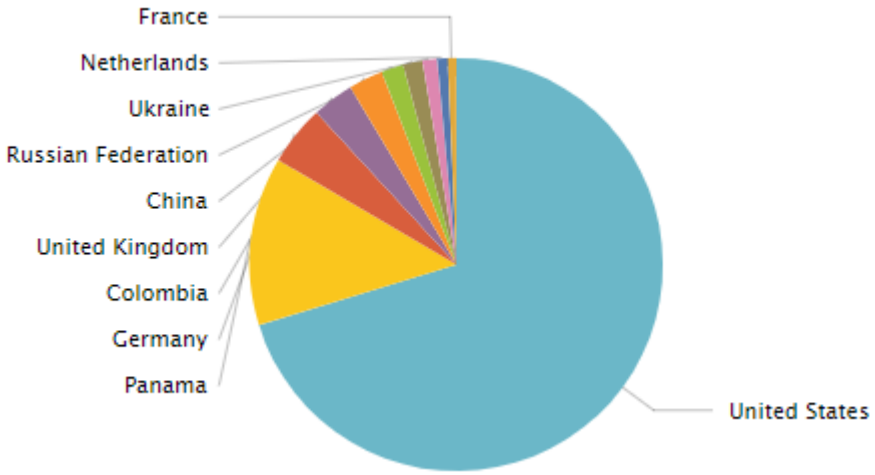


Comparison of previous month with month actual.

Description	March	April
Total Attack	**257,049**	**267,343**
Critical Attacks	**116,595**	**95,553**
Monthly attack average	**262,930**	**251,594**
Daily Attack Average	**9,226**	**9,094**
Monthly Critical attack average	**119,359**	**116,869**
Daily Critical Attack Average	**4,188**	**4,224**

Geography

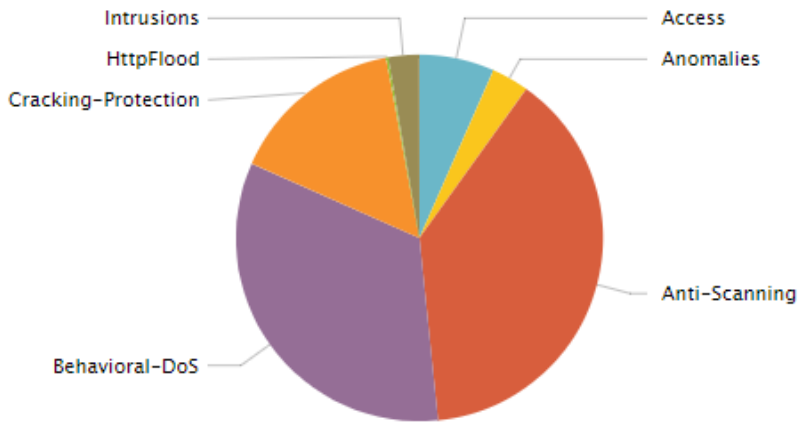
The vast majority of attacks on Metrobank originated geographically from the following Top 10 countries: **United States, Panama, Germany, Columbia, United Kingdom, China, Russian Federation, Netherlands, Ukraine,** and **France** listed in order of frequency. The attacks that we observed are happening to companies all around the world. Geographic borders offer little or no protection against cyber-attacks, in fact just the opposite is true offering more opportunity for anyone to carry out an attack.



*Please view the Maps and **Graph: Top 10 Attacking Countries Blocked**, **Graph: Top 10 Attacking Countries Blocked by Attack Type**, **Graph: Top 10 Attacking Countries Blocked by Protocol** available in the Security Intelligence section of the report.

Category Distribution

Category distribution for this report period is illustrated and detailed below.



Scanning accounted for 38.50 % of attacks during this report period

Network-wide Anti-Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modelling, commonplace after the information gathering phase of a targeted or planned attack.

Intrusions accounted for 2.71 % of attacks during this report period

These include vulnerability-based threats such as: Worms and Botnets; Trojan horses and the creation of backdoors; Vendor-specific exploitation vulnerabilities in products e.g., Microsoft, Oracle; Exploitation of vulnerabilities in applications such as web, mail, VoIP, DNS, SQL; Spyware, Phishing, anonymizes.

Packet Anomalies accounted for 3.27% of attacks during this report period

This anomalous traffic is usually caused by attacks or evasion tactics directed at the network devices such as firewalls in order to bypass their functions which if allowed to pass could permit scanning of the internal network or overloading the central processing unit of the device rendering it unusable and effectively causing a network bottleneck or DoS condition. They are also used as a method to collapse the underlying network infrastructure with packet crafting tools used by threat agents to interrupt services or distract security teams with volumetric attacks while more targeted attacks are directed at important assets to allow for data exfiltration. Packet Anomalies can also be caused by applications that do not adhere to RFC standards.

Access accounted for 6.62% of attacks during this report period

Access category relates directly to blacklists configured by GLESEC on the DefensePro for known threat sources.

Denial of Service accounted for 0% of attacks during this report period

Denial of service (DoS) usually refers to an attack that attempts to make a computer resource unavailable to its intended users by flooding a network or server with requests and data. Depending on the nature of your enterprise, this can effectively disable your organization.

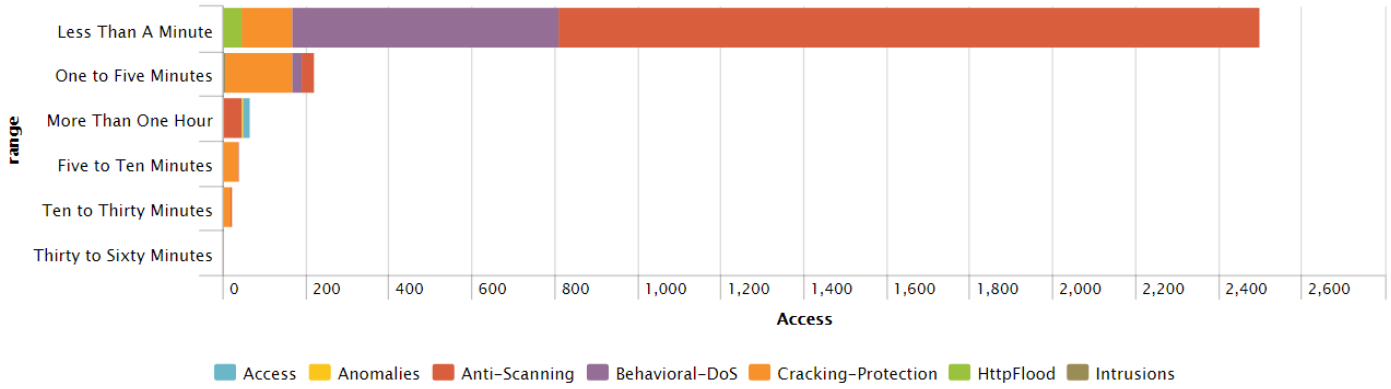
Behavioral-DoS accounted for 33.25% of attacks during this report period

The B-DoS system protects against Network Flood Attacks, which cause a great deal of irrelevant traffic to fill available network bandwidth, denying the use of network resources to legitimate users.

Network Flood protection types include: SYN Flood, TCP Flood, UDP Flood, ICMP Flood, IGMP Flood

Duration

Attack duration for specific categories for this report period is illustrated below.



Bandwidth

Behavioral-DoS dropped **50.94** Gbps, Access protection dropped **621.04** Mbps, Intrusion protection dropped **55.31** Mbps of total traffic, **32.45** Mbps dropped by Packet Anomaly protection rules, Anti-Scanning protection dropped **1.55** Gbps. A total of **50.94** Gbps of malicious traffic was discarded this period.

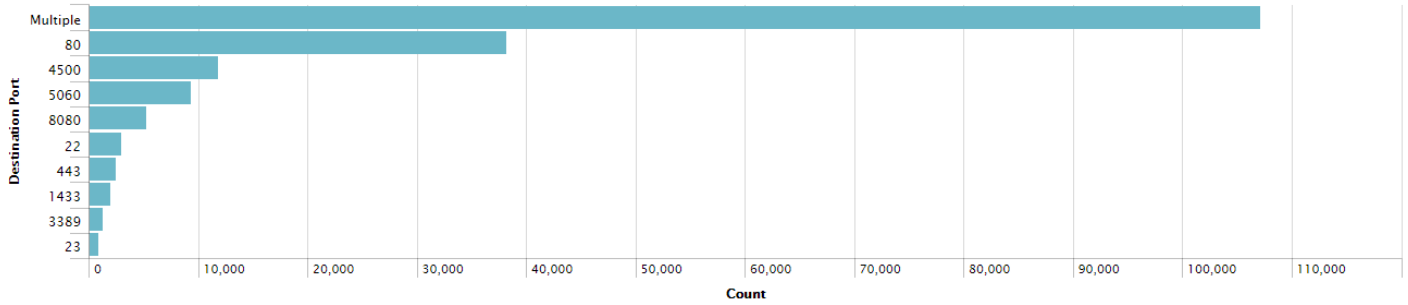
Category	Gbps	Mbps
Behavioral-DoS	50.94	52166.15
Anti-Scanning	1.55	1585.76
Access	0.61	621.04
Cracking-Protection	0.07	75.38
Intrusions	0.05	55.31
Anomalies	0.03	32.45
HttpFlood	0.01	5.31
Total Bandwidth in Gbps/Mbps	53.26	54541.40

*Please view the , **Graph: Bandwidth by Blocked Threat Category by Hour of Day** and and **Bandwidth** available in the Security Intelligence section of the report.

Port Activity

The advanced intrusion detection and prevention capabilities offered by the DefensePro IPS NBA, DoS and Reputation Service provides maximum protection for network elements, hosts and applications. It is composed of different application-level protection features to prevent intrusion attempts such as worms, Trojan horses and single-bullet attacks, facilitating complete and high-speed cleansing of all malicious intrusions.

The DefensePro assisted in preventing attacks directed at network and server level which were directed at well-known port numbers: **80** (http), **4500** (sip), **5060** (ipsec-nat-t), **8080** (http-alt), **22** (ms-sql), **443** (https), **1433** (ssh), **3389** (rdp), **23** (telnet) in order of frequency for this report period.

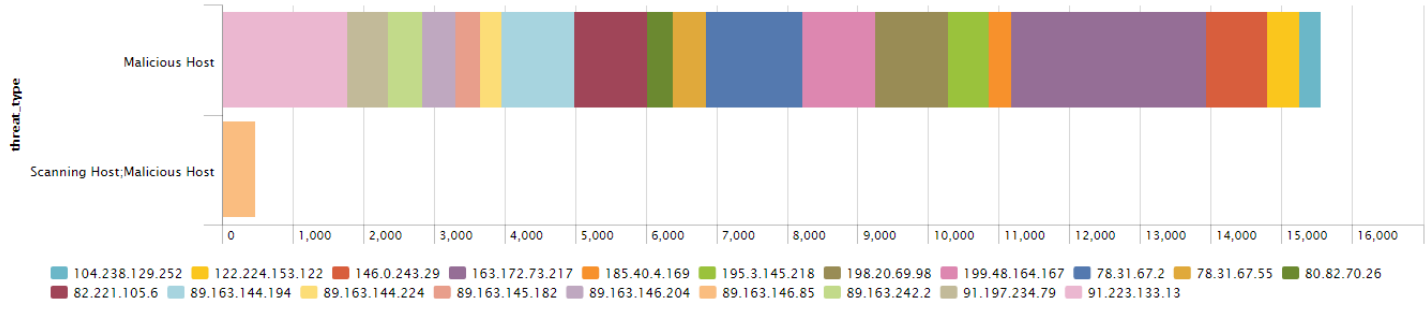


Port number information utilized is based on IANA Service Name and Transport Protocol Port Number Registryand additional outside sources are used to illustrate the relationship to commonly exploited attacks vectors.

*Please view the **Port Information**, and and available in the Security Intelligence section of the report.

Known Threat Sources by Threat Type

Of the attacks on Metrobank, **34,329** are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro attack logs and outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.



Vulnerability Summary

The following network ranges for Metrobank was scanned for vulnerabilities.
190.34.183.0/24

A total of **23** hosts were scanned of which were found to be vulnerable.

Vulnerabilities were detected for the following host IPs:

Host	Critical	High	Medium	Low	Total
190.34.183.153	5	4	13	1	23
190.34.183.149	0	0	9	2	11
190.34.183.152	2	0	6	1	9
190.34.183.132	0	0	6	1	7
190.34.183.139	0	0	4	2	6
190.34.183.129	0	1	1	2	4
190.34.183.154	0	0	3	1	4
190.34.183.131	0	0	1	0	1
190.34.183.144	0	0	1	0	1

Vulnerability –Current Month and Previous Month

A comparison of persistent vulnerabilities of the current month and previous month.

host-ip	Previous Month	Current Month
190.34.183.129	4	4
190.34.183.131	1	1
190.34.183.132	6	7
190.34.183.139	6	6
190.34.183.144	2	1
190.34.183.149	9	11
190.34.183.152		9
190.34.183.153		23
190.34.183.154	3	4

Please view **Recommendations** for more details.

Risk Distribution

Category distribution for this report period is illustrated and detailed below.

Based on the information gathered from the GLESEC MSS-VME a total of **66 Vulnerabilities** were found which consisted of **12 Critical/High Risk Vulnerabilities** during this period, **44 Medium Risk Vulnerabilities** and **10 Low Risk Vulnerabilities.**

Name	Critical	High	Medium	Low	Total
Metrobank	7	5	44	10	66

Critical / High risk vulnerabilities accounted for 6% of the discoveries during this report period

High are defined as being in one or more of the following categories: Backdoors, full Read/Write access to files, remote Command Execution, Potential Trojan Horses, or critical Information Disclosure (e.g. passwords).

Medium risk vulnerabilities accounted for 71% of the discoveries during this report period

Medium describes vulnerabilities that either expose sensitive data, directory browsing and traversal, disclosure of security controls, facilitate unauthorized use of services or denial of service to an attacker.

Low risk vulnerabilities accounted for 23% of the discoveries during this report period

Low describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social-engineering or similar attacks.

Vulnerability Categories

Most frequent type of vulnerabilities.

1	Preliminary Analysis	9	Firewalls	17	Network Devices
2	SMB/NetBIOS	10	SSH Servers	18	Malformed Packets
3	Simple Network Services	11	Mail Servers	19	Proxy Servers
4	Policy Checks	12	SQL Servers	20	Wireless AP
5	Web Servers	13	FTP Servers	21	Webmail Servers
6	RPC Services	14	Server Side Scripts	22	NFS Services
7	Backdoors	15	SNMP Services	23	Printers
8	Encryption and Authentication	16	DNS Servers		

The list below indicate your vulnerability most frequent:

General vulnerabilities are the most prevalent vulnerability category with **33** detected vulnerabilities followed by Web Servers with **11**, then both Misc and CGI abuses with **8** each, Service Detection with **3**, and Windows with **3** for the report period.

Category	Critical	High	Medium	Low	Total
General	0	1	28	4	33
Web Servers	1	2	7	1	11
CGI abuses	4	2	2	0	8
Misc.	0	0	3	5	8
Service detection	0	0	3	0	3
Windows	2	0	1	0	3

General vulnerabilities accounted for 65% of the discoveries during this report period

A set of checks that gather information about the remote system such as operating system and service identification, network connectivity, and more.

Service Detection vulnerabilities accounted for 6% of the discoveries during this report period

Security checks that allow Nessus to detect a wide variety of services on a remote host.

Misc. vulnerabilities accounted for 16% of the discoveries during this report period

Plugins that test for a wide variety of software including client-side and server issues.

Windows vulnerabilities accounted for 6% of the discoveries during this report period

Checks for software installed on Microsoft Windows systems including Adobe Reader, Adobe Flash, Antivirus software, web browsers, iTunes, and much more

Web Server vulnerabilities accounted for 6% of the discoveries during this report period

Various high-profile hacking attacks have proven that web security remains the most critical issue to any business that conducts its operations online. Web servers are one of the most targeted public faces of an organization, because of the sensitive data they usually host. Securing a web server is as important as securing the website or web application itself and the network around it. If you have a secure web application and an insecure web server, or vice versa, it still puts your business at a huge risk. Your company's security is as strong as its weakest point.

5. Recommendations

GLESEC recommends for Metrobank to address the following vulnerabilities assigned a Critical Risk by the MSS-VME .

Description

MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.

Note that this plugin sends a client Certificate TLS handshake message followed by a CertificateVerify message. Some Windows hosts will close the connection upon receiving a client certificate for which it did not ask for with a CertificateRequest message. In this case, the plugin cannot proceed to detect the vulnerability as the CertificateVerify message cannot be sent.

Systems Affected

443 / tcp / www 190.34.183.152

Solution

Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.

Description

MS15-034: Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553) (uncredentialed check)

The version of Windows running on the remote host is affected by a vulnerability in the HTTP protocol stack (HTTP.sys) due to improperly parsing crafted HTTP requests. A remote attacker can exploit this to execute arbitrary code with System privileges.

Systems Affected

443 / tcp / www 190.34.183.152

Solution

Microsoft has released a set of patches for Windows 7, 2008 R2, 8, 8.1, 2012, and 2012 R2

Description

OpenSSL 1.0.2 < 1.0.2i Multiple Vulnerabilities (SWEET32)

According to its banner, the remote host is running a version of OpenSSL 1.0.2 prior to 1.0.2i. It is, therefore, affected by the following vulnerabilities :

- Multiple integer overflow conditions exist in s3_srvr.c, ssl_sess.c, and t1_lib.c due to improper use of pointer arithmetic for heap-buffer boundary checks. An unauthenticated, remote attacker can exploit this to cause a denial of service. (CVE-2016-2177)

- An information disclosure vulnerability exists in the dsa_sign_setup() function in dsa_ossl.c due to a failure to properly ensure the use of constant-time operations.
An unauthenticated, remote attacker can exploit this, via a timing side-channel attack, to disclose DSA key information. (CVE-2016-2178)

- A denial of service vulnerability exists in the DTLS implementation due to a failure to properly restrict the lifetime of queue entries associated with unused out-of-order messages. An unauthenticated, remote attacker can exploit this, by maintaining multiple crafted DTLS sessions simultaneously, to exhaust memory.
(CVE-2016-2179)

- An out-of-bounds read error exists in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation. An unauthenticated, remote attacker can exploit this, via a crafted time-stamp file that is mishandled by the 'openssl ts' command, to cause denial of service or to disclose sensitive information.
(CVE-2016-2180)

- A denial of service vulnerability exists in the Anti-Replay feature in the DTLS implementation due to improper handling of epoch sequence numbers in records.

An unauthenticated, remote attacker can exploit this, via spoofed DTLS records, to cause legitimate packets to be dropped. (CVE-2016-2181)

- An overflow condition exists in the BN_bn2dec() function in bn_print.c due to improper validation of user-supplied input when handling BIGNUM values. An unauthenticated, remote attacker can exploit this to crash the process. (CVE-2016-2182)

- A vulnerability exists, known as SWEET32, in the 3DES and Blowfish algorithms due to the use of weak 64-bit block ciphers by default. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.
(CVE-2016-2183)

- A flaw exists in the tls_decrypt_ticket() function in t1_lib.c due to improper handling of ticket HMAC digests. An unauthenticated, remote attacker can exploit this, via a ticket that is too short, to crash the process, resulting in a denial of service.
(CVE-2016-6302)

- An integer overflow condition exists in the MDC2_Update() function in mdc2dgst.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or possibly the execution of arbitrary code.
(CVE-2016-6303)

- A flaw exists in the ssl_parse_clienthello_tlsext() function in t1_lib.c due to improper handling of overly large OCSP Status Request extensions from clients. An unauthenticated, remote attacker can exploit this, via large OCSP Status Request extensions, to exhaust memory resources, resulting in a denial of service condition.
(CVE-2016-6304)

- An out-of-bounds read error exists in the certificate parser that allows an unauthenticated, remote attacker to cause a denial of service via crafted certificate operations. (CVE-2016-6306)

- A flaw exists in the GOST ciphersuites due to the use of long-term keys to establish an encrypted connection. A man-in-the-middle attacker can exploit this, via a Key Compromise Impersonation (KCI) attack, to impersonate the server. (VulnDB 144759)

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to OpenSSL version 1.0.2i or later.

Note that the GOST ciphersuites vulnerability (VulnDB 144759) is not yet fixed by the vendor in an official release; however, a patch for the issue has been committed to the OpenSSL github repository.

Description

PHP 5.6.x < 5.6.26 Multiple Vulnerabilities

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.26. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in ext/standard/var_unserializer.re when destroying deserialized objects due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this, via a deserialize call that references a partially constructed object, to corrupt memory, resulting in a denial of service condition. (CVE-2016-7411)

- An heap buffer overflow condition exists in the php_mysqlnd_rowp_read_text_protocol_aux() function within file ext/mysqlnd/mysqlnd_wireprotocol.c due to a failure to verify that a BIT field has the UNSIGNED_FLAG flag. An unauthenticated, remote attacker can exploit this, via specially crafted field metadata, to cause a denial of service condition. (CVE-2016-7412)

- A use-after-free error exists in the wddx_stack_destroy() function within file ext/wddx/wddx.c when deserializing recordset elements.
An unauthenticated, remote attacker can exploit this, via a specially crafted wddxPacket XML document, to cause a denial of service condition. (CVE-2016-7413)

- An out-of-bounds access error exists in the phar_parse_zipfile() function within file ext/phar/zip.c due to a failure to ensure that the uncompressed_filesize field is large enough. An unauthenticated, remote attacker can exploit this, via a specially crafted archive, to cause a denial of service condition. (CVE-2016-7414)

- A stack-based buffer overflow condition exists in the ICU4C library, specifically within file common/locid.cpp in the the msgfmt_format_message() function, due to a failure to properly restrict the locale length provided to the Locale class. An unauthenticated, remote attacker can exploit this, via a long first argument to a MessageFormatter::formatMessage() function call, to cause a denial of service condition. (CVE-2016-7416)

- A flaw exists in the spl_array_get_dimension_ptr_ptr() function within file ext/spl/spl_array.c due to a failure to properly validate the return value and data type when deserializing SplArray. An unauthenticated, remote attacker can exploit this, via specially crafted serialized data, to cause a denial of service condition.
(CVE-2016-7417)

- An out-of-bounds read error exists in the php_wddx_push_element() function within file ext/wddx/wddx.c when handling an incorrect boolean element, which leads to mishandling the wddx_deserialize() call. An unauthenticated, remote attacker can exploit this, via a specially crafted wddxPacket XML document, to cause a denial of service condition. (CVE-2016-7418)

- An out-of-bounds access error exists in the phar_parse_tarfile() function within file ext/phar/tar.c when handling the verification of signatures. An unauthenticated, remote attacker can exploit this to cause an unspecified impact. (VulnDB 144264)

- An integer overflow condition exists in the fgetcsv() function when handling CSV field lengths due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code. (VulnDB 144270)

- An integer overflow condition exists in the wordwrap() function within file ext/standard/string.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code.
(VulnDB 144271)

- An integer overflow condition exists in the fgets() function within file ext/standard/file.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in a denial of service condition or the execution of arbitrary code. (VulnDB 144273)

- An integer overflow condition exists in the xml_utf8_encode() function within file ext/xml/xml.c due to improper validation of certain input. An unauthenticated, remote attacker can exploit this to cause an unspecified impact. (VulnDB 144275)

- A flaw exists in the exif_process_IFD_in_TIFF() function within file ext/exif/exif.c when handling uninitialized thumbnail data. An unauthenticated, remote attacker can exploit this to disclose memory contents.
(VulnDB 144287)

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to PHP version 5.6.26 or later.

Description

PHP 5.6.x < 5.6.27 Multiple Vulnerabilities

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.27. It is, therefore, affected by multiple vulnerabilities :

- A NULL pointer dereference flaw exists in the SimpleXMLElement::asXML() function within file ext/simplexml/simplexml.c. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 145598)

- A heap-based buffer overflow condition exists in the php_ereg_replace() function within file ext/ereg/ereg.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (VulnDB 145599)

- A flaw exists in the openssl_random_pseudo_bytes() function within file ext/openssl/openssl.c when handling strings larger than 2GB. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 145600)

- A flaw exists in the openssl_encrypt() function within file ext/openssl/openssl.c when handling strings larger than 2GB. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.
(VulnDB 145601)

- An integer overflow condition exists in the imap_8bit() function within file ext/imap/php_imap.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (VulnDB 145602)

- A flaw exists in the _bc_new_num_ex() function within file ext/bcmath/libbcmath/src/init.c when handling values passed via the 'scale' parameter. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 145603)

- A flaw exists in the php_resolve_path() function within file main/fopen_wrappers.c when handling negative size values passed via the 'filename' parameter. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 145604)

- A flaw exists in the dom_document_save_html() function within file ext/dom/document.c due to missing NULL checks. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.
(VulnDB 145605)

- A use-after-free error exists in the unserialize() function that allows an unauthenticated, remote attacker to dereference already freed memory, resulting in the execution of arbitrary code. (VulnDB 145606)

- An integer overflow condition exists in the mb_encode_*() functions in file ext/mbstring/mbstring.c due to improper validation of the length of encoded data. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (VulnDB 145607)

- A NULL pointer dereference flaw exists in the CachingIterator() function within file ext/spl/spl_iterators.c when handling string conversions. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 145608)

- An integer overflow condition exists in the number_format() function within file ext/standard/math.c when handling 'decimals' and 'dec_point' parameters that have values that are equal or close to 0x7fffffff. An unauthenticated, remote attacker can exploit this to cause a heap buffer overflow, resulting in a denial of service condition or the execution of arbitrary code.
(VulnDB 145609)

- A stack-based overflow condition exists in the ResourceBundle::create and ResourceBundle::getLocales methods and their respective functions within file ext/intl/resourcebundle/resourcebundle_class.c due to improper validation of input passed via the 'bundlename' parameter. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution or arbitrary code. (VulnDB 145610)

- An integer overflow condition exists in the php_pcre_replace_impl() function within file ext/pcre/php_pcre.c due to improper validation of user-supplied input. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code. (VulnDB 145611)

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to PHP version 5.6.27 or later.

Description

PHP 5.6.x < 5.6.28 Multiple Vulnerabilities

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.28. It is, therefore, affected by multiple vulnerabilities :

- A flaw exists in the parse_url() function due to returning the incorrect host. An unauthenticated, remote attacker can exploit this to have a multiple impacts depending on how the function is implemented, which can include bypassing authentication or conducting open redirection and server-side request forgery attacks.
(VulnDB 145227)

- An integer overflow condition exists in the
_php_imap_mail() function in file ext/imap/php_imap.c when handling overly long strings. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in a denial of service condition or the execution of arbitrary code.
(VulnDB 146957)

- A flaw exists in the bzcompress() function when handling overly long strings. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.
(VulnDB 146975)

- An integer overflow condition exists in the gdImageAALine() function within file ext/gd/libgd/gd.c due to improper validation of line limit values. An unauthenticated, remote attacker can exploit this to cause an out-of-bounds memory read or write, resulting in a denial of service condition, the disclosure of memory contents, or the execution of arbitrary code.
(VulnDB 147321)

Note that this software is reportedly affected by other vulnerabilities as well that have not been fixed yet in version 5.6.28.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to PHP version 5.6.28 or later.

Description

PHP 5.6.x < 5.6.29 Multiple Vulnerabilities

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.29. It is, therefore, affected by multiple vulnerabilities :

- A memory corruption issue exists in the php_wddx_push_element() function in ext/wddx/wddx.c that is triggered when decoding empty boolean elements. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the execution of arbitrary code. (CVE-2016-9935)

- A flaw exists in the in the openssl_pbkdf2() function in ext/openssl/openssl.c that is triggered when handling overly large key length parameters. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 148478)

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to PHP version 5.6.29 or later.

GLESEC recommends for Metrobank to address the following vulnerabilities assigned a High Risk by the GLESEC MSS-VME .

Description

Apache 2.4.x < 2.4.25 Multiple Vulnerabilities (httpoxy)

According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.25. It is, therefore, affected by the following vulnerabilities :

- A flaw exists in the mod_session_crypto module due to encryption for data and cookies using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default). An unauthenticated, remote attacker can exploit this, via a padding oracle attack, to decrypt information without knowledge of the encryption key, resulting in the disclosure of potentially sensitive information. (CVE-2016-0736)

- A denial of service vulnerability exists in the mod_auth_digest module during client entry allocation.
An unauthenticated, remote attacker can exploit this, via specially crafted input, to exhaust shared memory resources, resulting in a server crash. (CVE-2016-2161)

- The Apache HTTP Server is affected by a man-in-the-middle vulnerability known as 'httpoxy' due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated.
(CVE-2016-5387)

- A denial of service vulnerability exists in the mod_http2 module due to improper handling of the LimitRequestFields directive. An unauthenticated, remote attacker can exploit this, via specially crafted CONTINUATION frames in an HTTP/2 request, to inject unlimited request headers into the server, resulting in the exhaustion of memory resources. (CVE-2016-8740)

- A flaw exists due to improper handling of whitespace patterns in user-agent headers. An unauthenticated, remote attacker can exploit this, via a specially crafted user-agent header, to cause the program to incorrectly process sequences of requests, resulting in interpreting responses incorrectly, polluting the cache, or disclosing the content from one request to a second downstream user-agent. (CVE-2016-8743)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to Apache version 2.4.25 or later.

Note that the 'httpoxy' vulnerability can be mitigated by applying the workarounds or patches as referenced in the vendor advisory asf-httpoxy-response.txt. Furthermore, to mitigate the other vulnerabilities, ensure that the affected modules (mod_session_crypto, mod_auth_digest, and mod_http2) are not in use.

Description

OpenSSL 1.0.2 < 1.0.2k Multiple Vulnerabilities

According to its banner, the version of OpenSSL running on the remote host is 1.0.2 prior to 1.0.2k. It is, therefore, affected by multiple vulnerabilities :

- A carry propagation error exists in the Broadwell-specific Montgomery multiplication procedure when handling input lengths divisible by but longer than 256 bits. This can result in transient authentication and key negotiation failures or reproducible erroneous outcomes of public-key operations with specially crafted input. A man-in-the-middle attacker can possibly exploit this issue to compromise ECDH key negotiations that utilize Brainpool P-512 curves. (CVE-2016-7055)

- An out-of-bounds read error exists when handling packets using the CHACHA20/POLY1305 or RC4-MD5 ciphers. An unauthenticated, remote attacker can exploit this, via specially crafted truncated packets, to cause a denial of service condition. (CVE-2017-3731)

- A carry propagating error exists in the x86_64 Montgomery squaring implementation that may cause the BN_mod_exp() function to produce incorrect results. An unauthenticated, remote attacker with sufficient resources can exploit this to obtain sensitive information regarding private keys. Note that this issue is very similar to CVE-2015-3193. Moreover, the attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. For example, this can occur by default in OpenSSL DHE based SSL/TLS cipher suites. (CVE-2017-3732)

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Upgrade to OpenSSL version 1.0.2k or later.

Description

PHP 5.6.x < 5.6.25 Multiple Vulnerabilities

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.25. It is, therefore, affected by multiple vulnerabilities :

- An unspecified flaw exists in the object_common2() function in var_unserializer.c that occurs when handling objects during deserializaiton. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (VulnDB 143096)

- An integer overflow condition exists in the php_snmp_parse_oid() function in snmp.c. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow, resulting in the execution of arbitrary code. (VulnDB 143100)

- An integer truncation flaw exists in the select_colors() function in gd_topal.c that is triggered when handling the number of colors. An unauthenticated, remote attacker can exploit to cause a heap-based buffer overflow, resulting in the execution of arbitrary code.
(VulnDB 143101)

- An overflow condition exists in the sql_regcase() function in ereg.c due to improper handling of overly long strings. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code. (VulnDB 143102)

- A NULL pointer dereference flaw exists in the php_wddx_pop_element() function in wddx.c that is triggered during the handling of Base64 binary values.
An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 143103)

- An unspecified NULL pointer dereference flaw exists in the php_wddx_pop_element() function in wddx.c. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 143104)

- An integer overflow condition exists in the php_base64_encode() function in base64.c that occurs when handling overly long strings. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (VulnDB 143105)

- A NULL pointer dereference flaw exists in the php_wddx_deserialize_ex() function in wddx.c that occurs during the handling of invalid XML content. An unauthenticated, remote attacker can exploit this to cause a denial of service condition. (VulnDB 143106)

- An integer overflow condition exists in the php_quot_print_encode() function in quot_print.c that occurs when handling overly long strings. An unauthenticated, remote attacker can exploit this to cause a heap-based buffer overflow condition, resulting in the execution of arbitrary code. (VulnDB 143107)

- A use-after-free error exists in the unserialize() function in var.c. An unauthenticated, remote attacker can exploit this to dereference already freed memory, resulting in the execution of arbitrary code.
(VulnDB 143108)

- A flaw exists in the php_ftp_fopen_connect() function in ftp_fopen_wrapper.c that allows a man-in-the-middle attacker to silently downgrade to regular FTP even if a secure method has been requested. (VulnDB 143109)

- A flaw exists in the php_wddx_process_data() function in wddx.c that occurs when deserializing invalid dateTime values. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.
(VulnDB 143110)

- A flaw exists in the exif_process_IFD_in_TIFF() function in exif.c that occurs when handling TIFF image content.
An unauthenticated, remote attacker can exploit this to disclose memory contents. (VulnDB 143111)

- An integer overflow condition exists in the php_url_encode() function in url.c that occurs when handling overly long strings. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code. (VulnDB 143112)

- An integer overflow condition exists in the php_uuencode() function in uuencode.c. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code. (VulnDB 143113)

- An integer overflow condition exists in the bzdecompress() function in bz2.c. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code.
(VulnDB 143114)

- An indexing flaw exists in the imagegammacorrect() function in gd.c that occurs when handling negative gamma values. An unauthenticated, remote attacker can exploit this to write a NULL to an arbitrary memory location, resulting in a denial of service condition or the execution of arbitrary code. (VulnDB 143116)

- An integer overflow condition exists in the curl_escape() function in interface.c that occurs when handling overly long escaped strings. An unauthenticated, remote attacker can exploit this to corrupt memory, resulting in the execution of arbitrary code. (VulnDB 143117)

- An unspecified flaw exists in session.c that occurs when handling session names. An unauthenticated, remote attacker can exploit this to inject arbitrary data into sessions. (VulnDB 143118)

Systems Affected

443 / tcp / www 190.34.183.153

Solution
Upgrade to PHP version 5.6.25 or later.

Description
PHP 5.6.x < 5.6.30 Multiple DoS

According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.30. It is, therefore, affected by the following vulnerabilities :

- A floating pointer exception flaw exists in the exif_convert_any_to_int() function in exif.c that is triggered when handling TIFF and JPEG image tags. An unauthenticated, remote attacker can exploit this to cause a crash, resulting in a denial of service condition. (CVE-2016-10158)

- An integer overflow condition exists in the phar_parse_pharfile() function in phar.c due to improper validation when handling phar archives. An unauthenticated, remote attacker can exploit this to cause a crash, resulting in a denial of service condition. (CVE-2016-10159)

- An off-by-one overflow condition exists in the phar_parse_pharfile() function in phar.c due to improper parsing of phar archives. An unauthenticated, remote attacker can exploit this to cause a crash, resulting in a denial of service condition. (CVE-2016-10160)

- An out-of-bounds read error exists in the finish_nested_data() function in var_unserializer.c due to improper validation of unserialized data. An unauthenticated, remote attacker can exploit this to cause a crash, resulting in a denial of service condition or the disclosure of memory contents.
(CVE-2016-10161)

- An out-of-bounds read error exists in the phar_parse_pharfile() function in phar.c due to improper parsing of phar archives. An unauthenticated, remote attacker can exploit this to cause a crash, resulting in a denial of service condition. (VulnDB 149621)

- A denial of service vulnerability exists in the bundled GD Graphics Library (LibGD) in the gdImageCreateFromGd2Ctx() function in gd_gd2.c due to improper validation of images. An unauthenticated, remote attacker can exploit this, via a specially crafted image, to crash the process. (VulnDB 150576)

Systems Affected
443 / tcp / www 190.34.183.153

Solution
Upgrade to PHP version 5.6.30 or later.

Description
Small SSH RSA Key

The remote SSH daemon has a small key size, which is insecure. Given current technology, it should be 768 bits at a minimum.

Systems Affected

22 / tcp / ssh 190.34.183.129

Solution

Generate a new, larger key for the service.

GLESEC recommends for Metrobank to address the following vulnerabilities assigned a Medium Risk by the GLESEC MSS-VME .

Description

SSL 64-bit Block Size Cipher Suites Supported (SWEET32)

The remote host supports the use of a block cipher with 64-bit blocks in one or more cipher suites. It is, therefore, affected by a vulnerability, known as SWEET32, due to the use of weak 64-bit block ciphers. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session.

Proof-of-concepts have shown that attackers can recover authentication cookies from an HTTPS session in as little as 30 hours.

Note that the ability to send a large number of requests over the same TLS connection between the client and server is an important requirement for carrying out this attack. If the number of requests allowed for a single connection were limited, this would mitigate the vulnerability. However, Nessus has not checked for such a mitigation.

Systems Affected

25 / tcp / smtp	190.34.183.149
443 / tcp / www	190.34.183.132, 190.34.183.139, 190.34.183.149, 190.34.183.152, 190.34.183.153, 190.34.183.154

Solution

Reconfigure the affected application, if possible, to avoid use of all 64-bit block ciphers. Alternatively, place limitations on the number of requests that are allowed to be processed over the same TLS connection to mitigate this vulnerability.

Description

SSL Medium Strength Cipher Suites Supported

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Systems Affected

25 / tcp / smtp	190.34.183.149
443 / tcp / www	190.34.183.149, 190.34.183.152, 190.34.183.132, 190.34.183.139, 190.34.183.154, 190.34.183.153

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Description

SSL Certificate Cannot Be Trusted

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Systems Affected

25 / tcp / smtp	190.34.183.149
443 / tcp / www	190.34.183.154, 190.34.183.132, 190.34.183.153

Solution
Purchase or generate a proper certificate for this service.

Description
SSL Version 2 and 3 Protocol Detection

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC'S definition of 'strong cryptography'.

Systems Affected
25 / tcp / smtp 190.34.183.149
443 / tcp / www 190.34.183.149, 190.34.183.139, 190.34.183.152

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.1 (with approved cipher suites) or higher instead.

Description
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Systems Affected

25 / tcp / smtp	190.34.183.149
443 / tcp / www	190.34.183.149, 190.34.183.132, 190.34.183.152

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Description

Microsoft Exchange Client Access Server Information Disclosure

The Microsoft Exchange Client Access Server (CAS) is affected by an information disclosure vulnerability. A remote, unauthenticated attacker can exploit this vulnerability to learn the server's internal IP address.

Systems Affected

443 / tcp / www	190.34.183.149

Solution

There is no known fix at this time.

Description

SMB Signing Disabled

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Systems Affected

445 / tcp / cifs	190.34.183.144

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Description

SSH Protocol Version 1 Session Key Retrieval

The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol.

These protocols are not completely cryptographically safe so they should not be used.

Systems Affected

22 / tcp / ssh 190.34.183.149

Solution

Disable compatibility with version 1 of the protocol.

Description

SSL Certificate Signed Using Weak Hashing Algorithm

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.

Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.

Systems Affected

443 / tcp / www 190.34.183.132, 190.34.183.153

Solution

Contact the Certificate Authority to have the certificate reissued.

Description

SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

Systems Affected

25 / tcp / smtp	190.34.183.149
443 / tcp / www	190.34.183.149, 190.34.183.152

Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

Description

SSL Self-Signed Certificate

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Systems Affected

443 / tcp / www	190.34.183.132, 190.34.183.153

Solution

Purchase or generate a proper certificate for this service.

Description

SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (BEAST)

A vulnerability exists in SSL 3.0 and TLS 1.0 that could allow information disclosure if an attacker intercepts encrypted traffic served from an affected system.

TLS 1.1, TLS 1.2, and all cipher suites that do not use CBC mode are not affected.

This plugin tries to establish an SSL/TLS remote connection using an affected SSL version and cipher suite and then solicits return data.
If returned application data is not fragmented with an empty or one-byte record, it is likely vulnerable.

OpenSSL uses empty fragments as a countermeasure unless the 'SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS' option is specified when OpenSSL is initialized.

Microsoft implemented one-byte fragments as a countermeasure, and the setting can be controlled via the registry key HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\SendExtraRecord.

Therefore, if multiple applications use the same SSL/TLS implementation, some may be vulnerable while others may not be, depending on whether or not a countermeasure has been enabled.

Note that this plugin detects the vulnerability in the SSLv3/TLSv1 protocol implemented in the server. It does not detect the BEAST attack where it exploits the vulnerability at HTTPS client-side (i.e., Internet browser). The detection at server-side does not necessarily mean your server is vulnerable to the BEAST attack, because the attack exploits the vulnerability at the client-side, and both SSL/TLS clients and servers can independently employ the split record countermeasure.

Systems Affected

25 / tcp / smtp	190.34.183.149
443 / tcp / www	190.34.183.149, 190.34.183.132, 190.34.183.152

Solution

Configure SSL/TLS servers to only use TLS 1.1 or TLS 1.2 if supported.
Configure SSL/TLS servers to only support cipher suites that do not use block ciphers. Apply patches if available.

Note that additional configuration may be required after the installation of the MS12-006 security update in order to enable the split-record countermeasure. See Microsoft KB2643584 for details.

Description

Web Application Potentially Vulnerable to Clickjacking

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

Systems Affected

80 / tcp / www 190.34.183.131
443 / tcp / www 190.34.183.153

Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

Description

Apache mod_info /server-info Information Disclosure

It is possible to obtain an overview of the remote Apache web server's configuration by requesting the URL '/server-info'. This overview includes information such as installed modules, their configuration, and assorted run-time settings.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

If required, update Apache's configuration file(s) to either disable mod_info or ensure that access is limited to valid users / hosts.

Description

Apache mod_status /server-status Information Disclosure

It is possible to obtain an overview of the remote Apache web server's activity and performance by requesting the URL '/server-status'. This overview includes information such as current hosts and requests being processed, the number of workers idle and service requests, and CPU utilization.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

If required, update Apache's configuration file(s) to either disable mod_status or ensure that access is limited to valid users / hosts.

Description

Browsable Web Directories

Multiple Nessus plugins identified directories on the web server that are browsable.

https://190.34.183.153/dashboard/docs/
https://190.34.183.153/dashboard/docs/images/
https://190.34.183.153/dashboard/docs/images/access-phpmyadmin-remotely/
https://190.34.183.153/dashboard/docs/images/activate-use-xdebug/
https://190.34.183.153/dashboard/docs/images/backup-restore-mysql/
https://190.34.183.153/dashboard/docs/images/configure-vhosts/
https://190.34.183.153/dashboard/docs/images/configure-wildcard-subdomains/
https://190.34.183.153/dashboard/docs/images/create-framework-project-zf1/
https://190.34.183.153/dashboard/docs/images/create-framework-project-zf2/
https://190.34.183.153/dashboard/docs/images/deploy-git-app/
https://190.34.183.153/dashboard/docs/images/install-wordpress/
https://190.34.183.153/dashboard/docs/images/reset-mysql-password/
https://190.34.183.153/dashboard/docs/images/send-mail/
https://190.34.183.153/dashboard/docs/images/transfer-files-ftp/
https://190.34.183.153/dashboard/docs/images/troubleshoot-apache/
https://190.34.183.153/dashboard/docs/images/use-different-php-version/
https://190.34.183.153/dashboard/docs/images/use-php-fcgi/
https://190.34.183.153/dashboard/docs/images/use-sqlite/

https://190.34.183.153/dashboard/images/
https://190.34.183.153/dashboard/images/addons/
https://190.34.183.153/dashboard/images/blog/
https://190.34.183.153/dashboard/images/flags/
https://190.34.183.153/dashboard/images/screenshots/
https://190.34.183.153/dashboard/images/stamps/
https://190.34.183.153/dashboard/images/team/
https://190.34.183.153/dashboard/stylesheets/
https://190.34.183.153/img/
https://190.34.183.153/xampp/

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Make sure that browsable directories do not leak confidential informative or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

Description

HTTP TRACE / TRACK Methods Allowed

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Disable these methods. Refer to the plugin output for more information.

Description

PHP expose_php Information Disclosure

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

Description

Web Server info.php / phpinfo.php Detection

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo()' for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including :

- The username of the user who installed PHP and if they are a SUDO user.
- The IP address of the host.
- The version of the operating system.
- The web server version.
- The root directory of the web server.
- Configuration information about the remote PHP installation.

Systems Affected

443 / tcp / www 190.34.183.153

Solution

Remove the affected file(s).

GLESEC recommends for Metrobank to address the following vulnerabilities assigned a Low Risk by the GLESEC MSS-VME .

Description

SSL RC4 Cipher Suites Supported (Bar Mitzvah)

The remote host supports the use of RC4 in one or more cipher suites.
The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

Systems Affected

443 / tcp / www 190.34.183.149, 190.34.183.139

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Description

SSH Server CBC Mode Ciphers Enabled

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext.

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions.

Systems Affected

22 / tcp / ssh 190.34.183.129

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Description

SSH Weak MAC Algorithms Enabled

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Systems Affected

22 / tcp / ssh 190.34.183.129

Solution

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Description

SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

Systems Affected

443 / tcp / www 190.34.183.132

Solution

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

Description

SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

Systems Affected

443 / tcp / www 190.34.183.139

Solution

Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

Description

Web Server HTTP Header Internal IP Disclosure

This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server.

There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection.

Systems Affected

443 / tcp / www 190.34.183.149

Solution

None

GLESEC recommends “Implementing the First Five Quick Wins” based on the Twenty Critical Security Controls for Effective Cyber Defense, Version 4.1 that were formulated as a joint effort from the NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities. These are readily available from GLESEC which has provided the following link:
The Critical Controls represent the biggest bang for the buck to protect your organization against real security threats. Within Critical Controls 2-4 are five “quick wins.” These are subcontrols that have the most immediate impact on preventing the advanced targeted attacks that have penetrated existing controls and compromised critical systems at thousands of organizations.

The five quick wins are:

a) Application white listing (in CSC2)
b) Using common, secure configurations (in CSC3)
c) Patch application software within 48 hours (in CSC4)
d) Patch systems software within 48 hours (CSC4)
e) Reduce the number of users with administrative privileges (in CSC3 and CSC12)

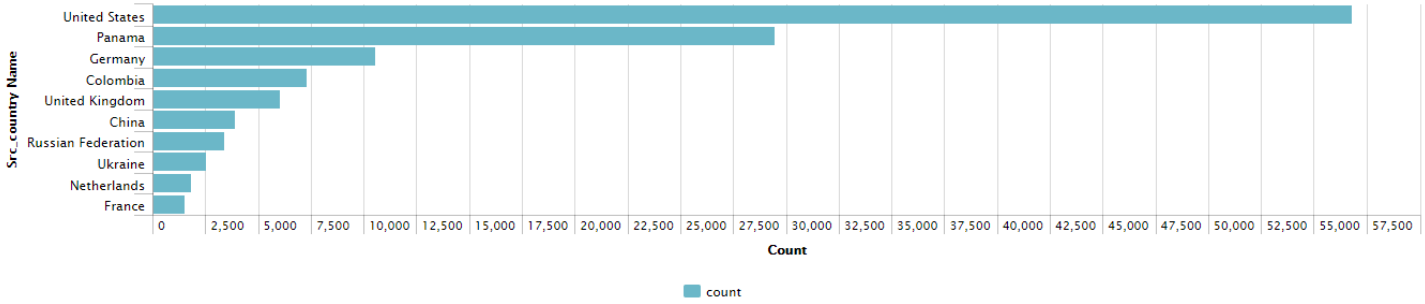
6. Security Intelligence

The purpose of this section is to highlight intelligence gathered from the devices under contract as well as outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

The vast majority of attacks on Metrobank originated geographically from the following Top 10 countries: **United States, Panama, Germany, United Kingdom, China, Netherlands, Russina Federation, France, Indonesia,** and **Ukraine** listed in order of frequency. The attacks that we observed are happening to companies all around the world. Some results do not include location information that allows map plotting.

Graph: Top 10 Attacking Countries Blocked - DefensePro

This report provides the count of total attacks blocked by country



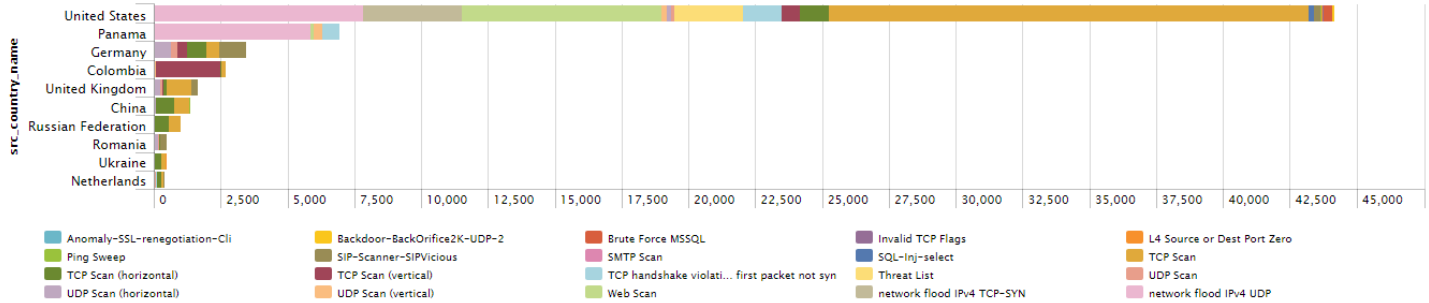
Graph: Top 10 Attacking Countries Blocked - AppWall

This report provides the count of total attacks blocked by country

For this period there are not sufficient AppWall results to generate information

Graph: Top 10 Attacking Countries Blocked by Attack Type - DefensePro

This report provides the count of total attacks types blocked by country

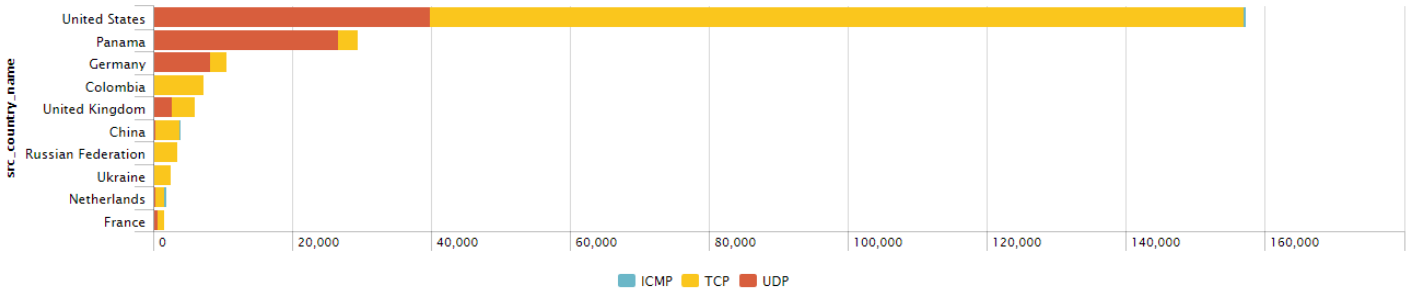


Graph: Top 10 Attacking Countries Blocked by Attack Type – AppWall

For this period there are not sufficient AppWall results to generate information

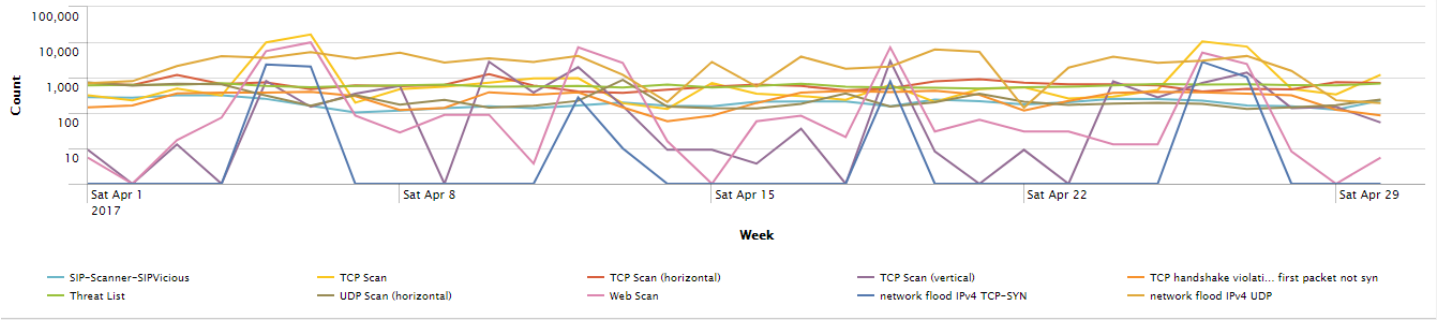
Graph: Top 10 Attacking Countries Blocked by Protocol

This report provides the count of attack protocols blocked by country



Graph: Attacks Types Blocked by Week - DefensePro

This report provides the count of attacks blocked by week



Graph: Attacks Types Blocked by Week - AppWall

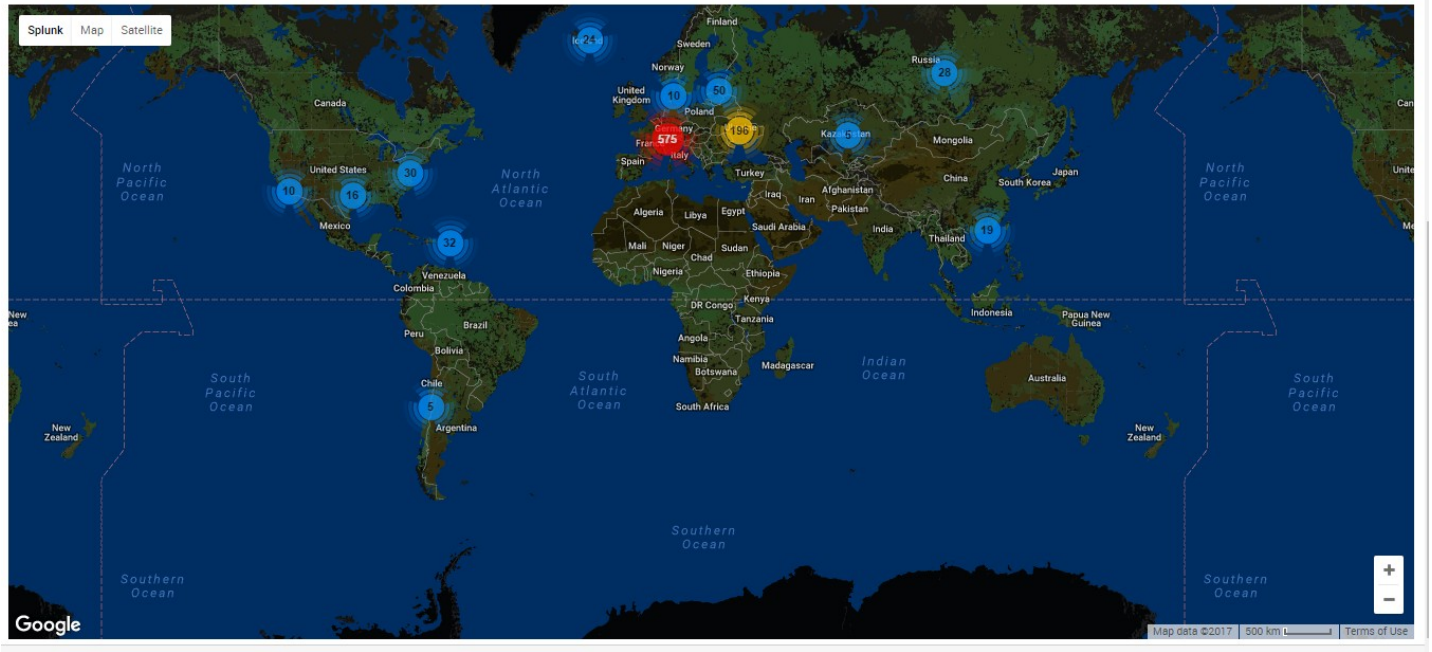
This report provides the count of attacks blocked by week

For this period there are not sufficient AppWall results to generate information

Known Threat Source Information

Of the attacks on Metrobank, **34,329** are from known threat sources that have been compiled and correlated with attack source IPs gathered from the DefensePro attack logs and outside sources such honeypots, known malicious sources, vulnerability databases, relationships with CERT and CSIRT teams that GLESEC possesses, together with various other threat feeds.

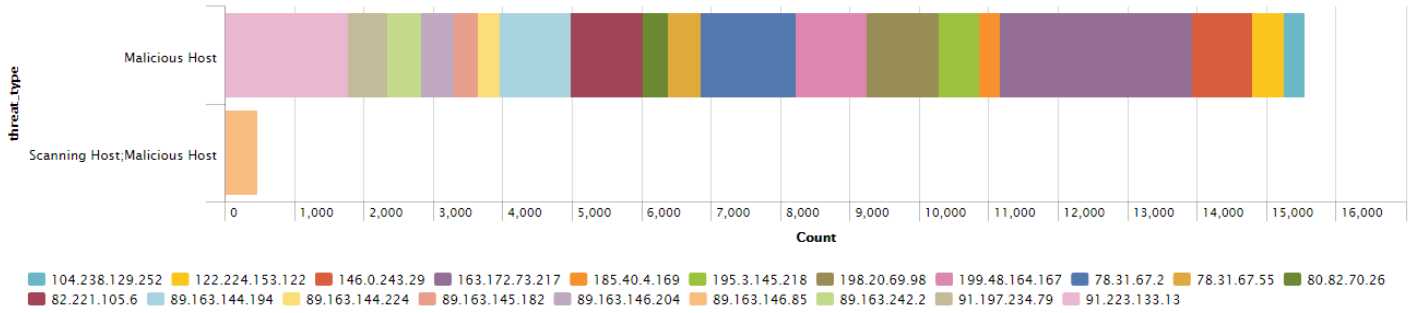
The **73,705** attacks on Metrobank from the DNS Blacklist were obtained by correlating values from the Project Honey Pot Database. Some results do not include location information that allows map plotting.



Map of geographic distribution of **73,705** attacks on Metrobank from known threat sources obtained by correlating values from AlienVault Labs; Emerging Threats; Zeus, Spyeye, and Palevo Tracker. Some results do not include location information that allows map plotting.

Graph: Known Threat Sources by Threat Type - DefensePro

This report provides the Top 20 known threat sources by IP and their respective infringing threat type.



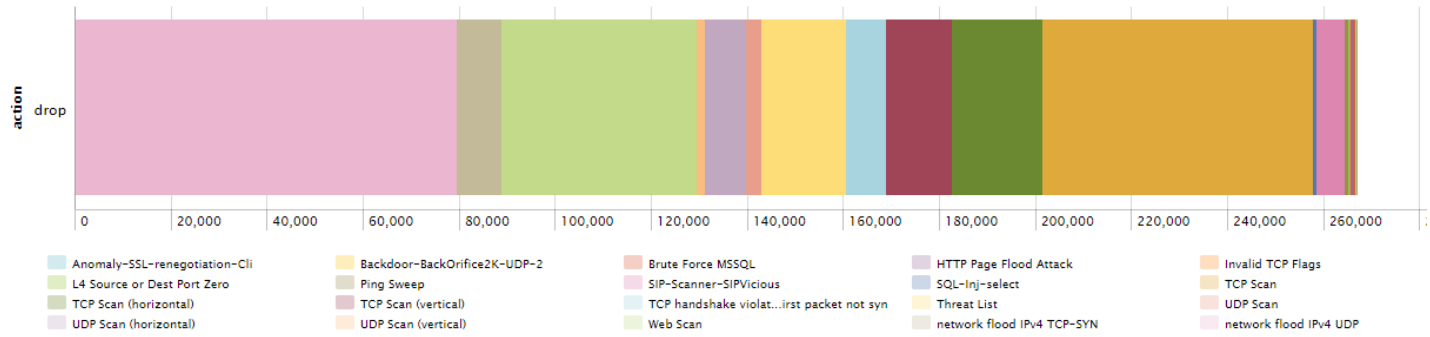
Graph: Known Threat Sources by Threat Type – AppWall

This report provides the Top 20 known threat sources by IP and their respective infringing threat type.

For this period there are not sufficient AppWall results to generate information

Graph: Attacks Denied

This report provides the count of total denied attacks along with network security rule.



Port Information

Port Information: Port **80** (http), Port **1443** (ms-sql), Port **8080** (https-alt), Port **3306** (mysql)

Commonly scanned in order to attack web servers. SQL injection is currently the most common form of web site attack in that web forms are very common, often they are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available online. This kind of exploit is easy enough to accomplish that even inexperienced hackers can accomplish mischief. However, in the hands of the very skilled hacker, a web code weakness can reveal root level access of web servers and from there attacks on other networked servers can be accomplished. Structured Query Language (SQL) is the nearly universal language of databases that allows the storage, manipulation, and retrieval of data. Databases that use SQL include MS SQL Server, MySQL, Oracle, PostgreSQL, MongoDB, Access and Filemaker Pro and these databases are equally subject to SQL injection attack.

Web based forms must allow some access to your database to allow entry of data and a response, so this kind of attack bypasses firewalls and endpoint defenses. Any web form, even a simple logon form or search box, might provide access to your data by means of SQL injection if coded incorrectly.

OWASP Top 10 for 2013 lists A1-Injection as the greatest threat and defines this category as:

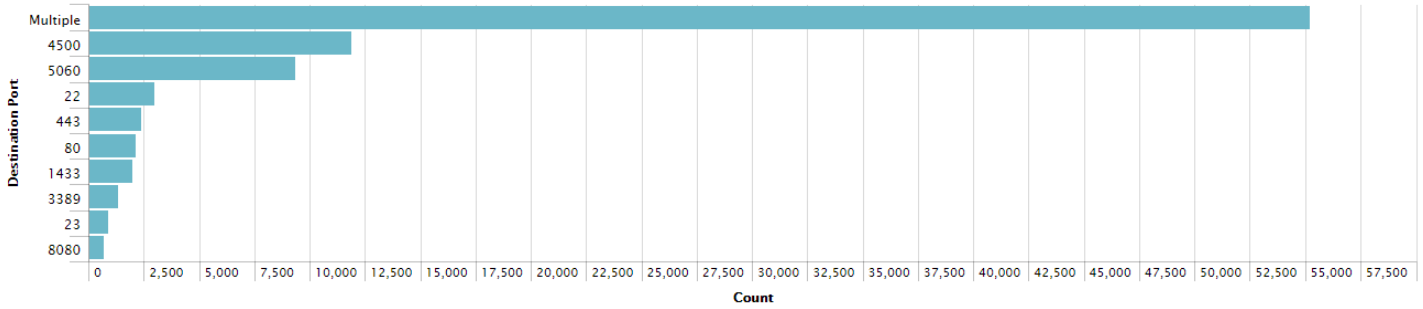
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration

operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Graph: Attacks Blocked by Destination Port - DefensePro

This report provides information on the total number of attacks blocked that were attempted on which port and for how many times.



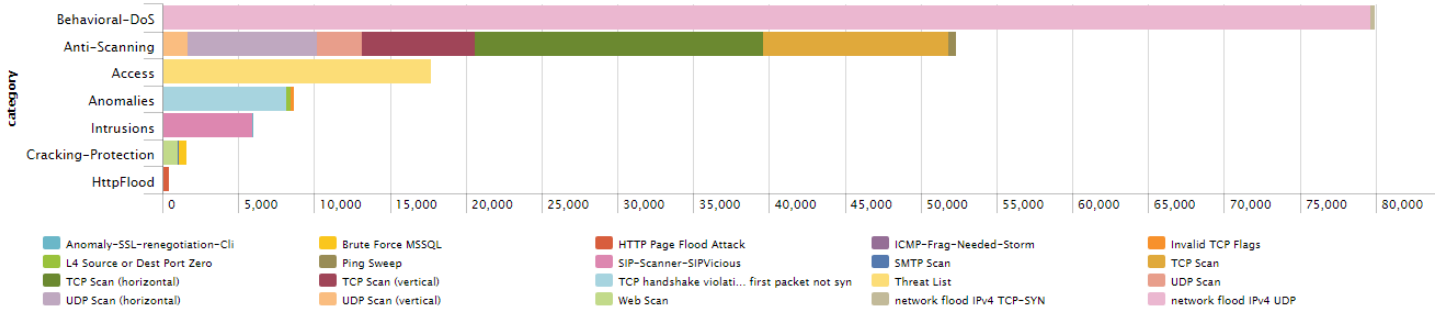
Graph: Attacks Blocked by Destination Port - AppWall

This report provides information on the total number of attacks blocked that were attempted on which port and for how many times.

For this period there are not sufficient AppWall results to generate information

Graph: Attacks Blocked By Threat Category - DefensePro

This report lists the attacks blocked per Attack Category, listing the attack name.



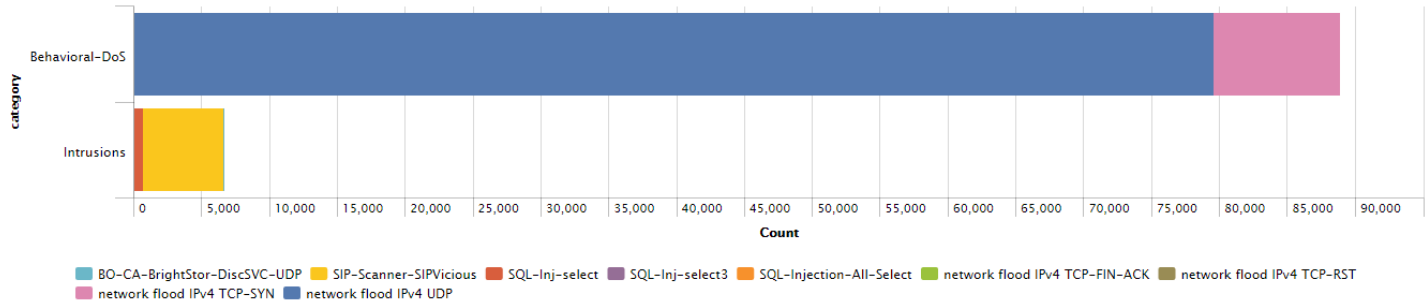
Graph: Attacks Blocked By Threat Category - AppWall

This report lists the attacks blocked per Attack Category, listing the attack name.

For this period there are not sufficient AppWall results to generate information

Graph: Critical Attacks Blocked - DefensePro

This report provides Critical Attacks information, attack name, network security rule along with the number of times the attack was launched.



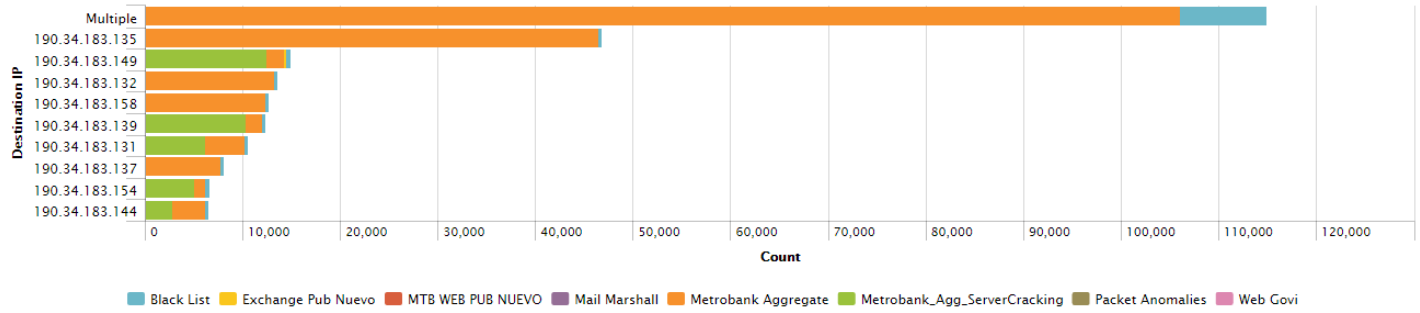
Graph: Critical Attacks Blocked - AppWall

This report provides Critical Attacks information, attack name, network security rule along with the number of times the attack was launched.

For this period there are not sufficient AppWall results to generate information

Graph: Top Attacked Destinations Blocked - DefensePro

This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.



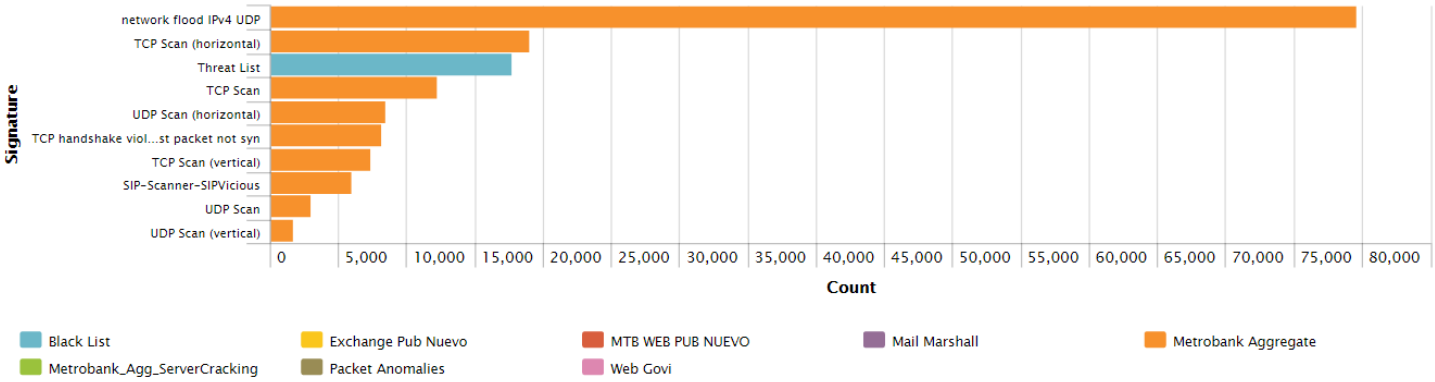
Graph: Top Attacked Destinations Blocked - AppWall

This report provides information on the system IPs, which were the destination of the attacks for most number of times along with the network security rule.

For this period there are not sufficient AppWall results to generate information

Graph: Top Attacks Blocked - DefensePro

This report provides information on the Top Attacks Blocked, the attack name, network security rule and the total number of attacks blocked with this combination.



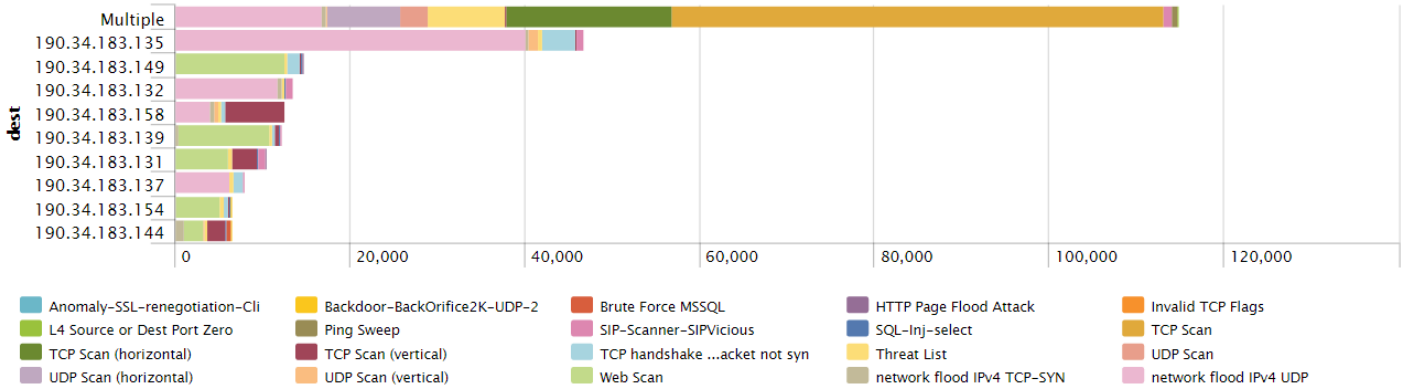
Graph: Top Attacks Blocked - AppWall

This report provides information on the Top Attacks Blocked, the attack name, network security rule and the total number of attacks blocked with this combination.

For this period there are not sufficient AppWall results to generate information

Graph: Top Attacks Blocked by Destination

This report provides information on the top attacks targeted at destinations that were blocked on the DP IPs. In this report the destination on which the attack was targeted, attack name, and count are shown.



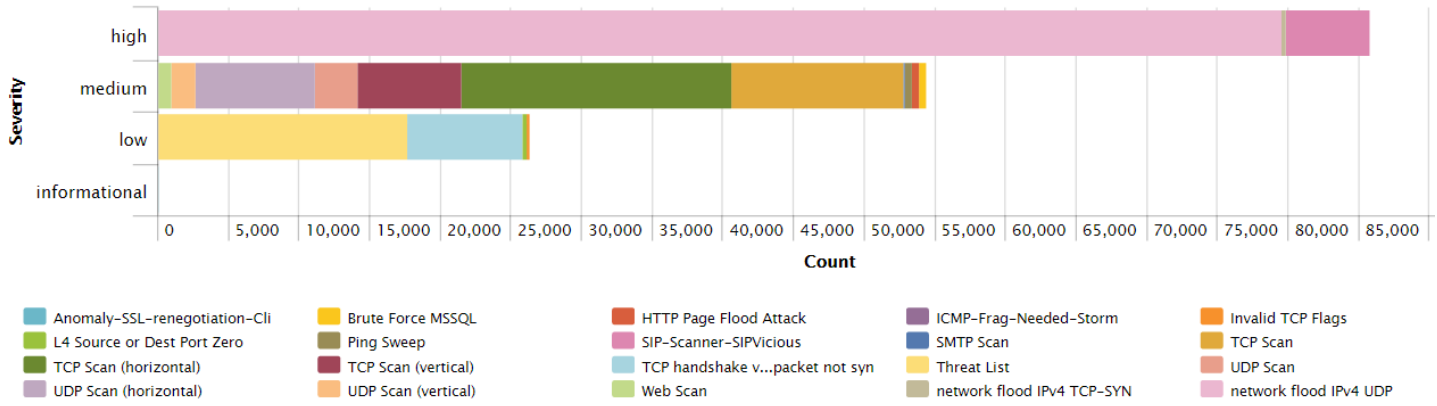
Graph: Top Attacks Blocked by Destination

This report provides information on the top attacks targeted at destinations that were blocked on the AFW IPs. In this report the destination on which the attack was targeted, attack name, and count are shown.

For this period there are not sufficient AppWall results to generate information

Graph: Top Attacks Blocked By Risk - DefensePro

This report provides information on the attacks, which were blocked on DP IPs based on their risk. In this report the risk of the attack and attack name are shown.



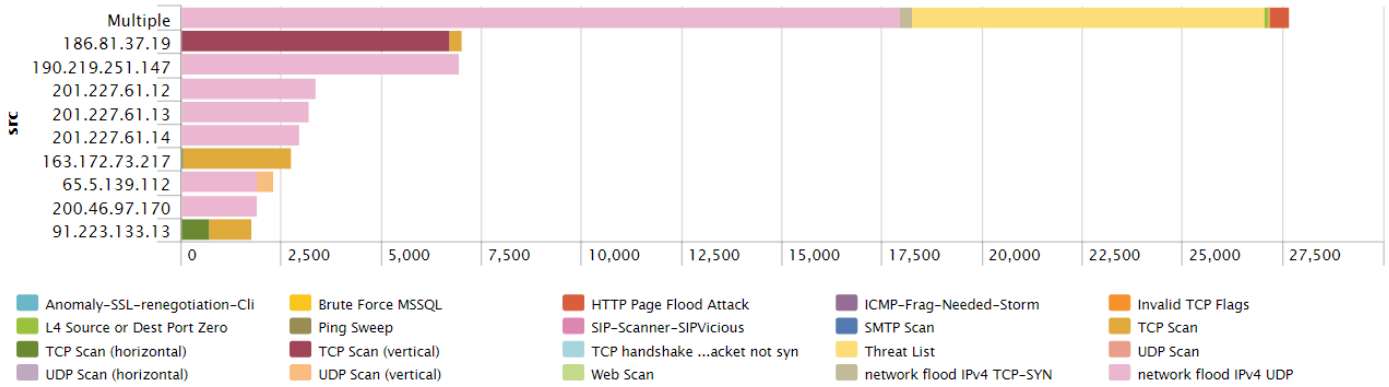
Graph: Top Attacks Blocked By Risk - AppWall

This report provides information on the attacks, which were blocked on AFW IPs based on their risk. In this report the risk of the attack and attack name are shown.

For this period there are not sufficient AppWall results to generate information

Graph: Top Attacks Blocked by Source - DefensePro

This report provides information on the top attacks blocked, categorized by attacks for each source that was the source of attacks along with the attack name and the number of attacks that triggered with this combination.



Graph: Top Attacks Blocked by Source - AppWall

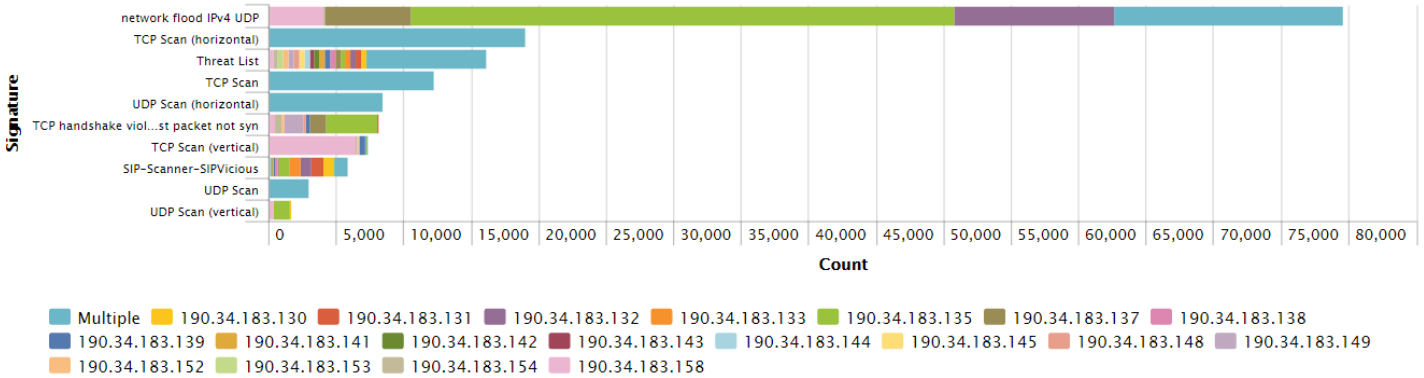
This report provides information on the top attacks blocked, categorized by attacks for each source that was the source of attacks along with the attack name and the number of attacks that triggered with this combination.

For this period there are not sufficient AppWall results to generate information

See Appendix 1 – Critical Attack Sources (WHOIS Information)

Graph: Top Destinations by Attacks Blocked - DefensePro

This report provides information on the attacks attempted for the most number of times on the destination protected system IPs.



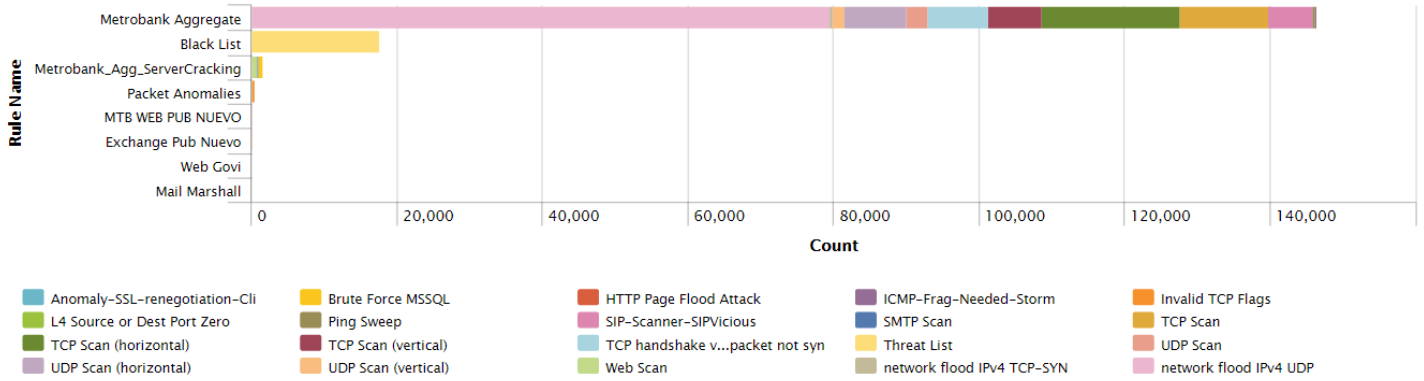
Graph: Top Destinations by Attacks Blocked - AppWall

This report provides information on the attacks attempted for the most number of times on the destination protected system IPs.

For this period there are not sufficient AppWall results to generate information

Graph: Attacks Blocked by Network Security Rule - DefensePro

This report lists the attacks per network security rule, listing the attack name.



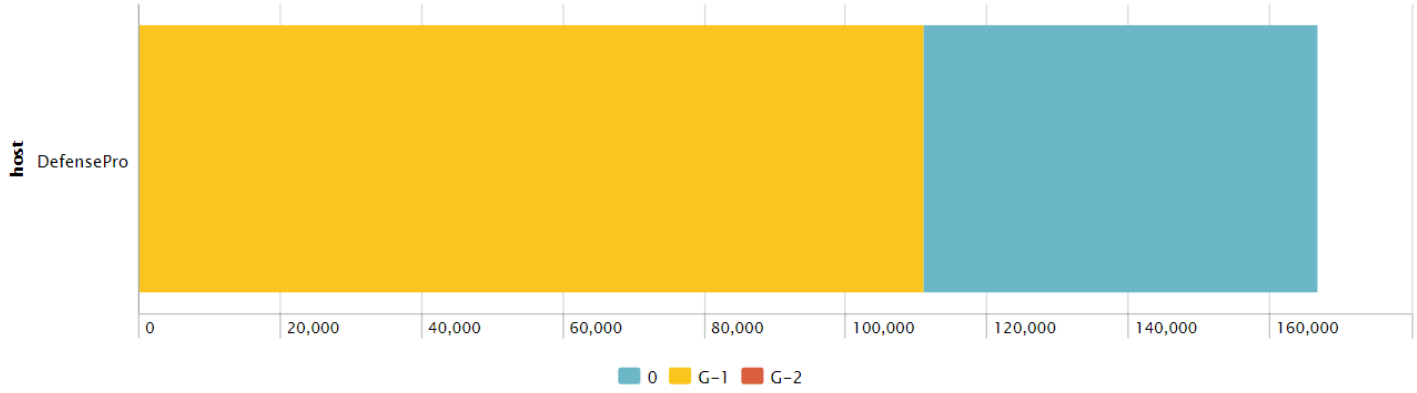
Graph: Attacks Blocked by Network Security Rule - AppWall

This report lists the attacks per network security rule, listing the attack name.

For this period there are not sufficient AppWall results to generate information

Graph: Attacks Blocked by Physical Port (per single IPS device)

This report lists the attacks per physical port.



Graph: Top Page Requests Blocked by Source - AppWall

This report provides information on the top page requests that were blocked, categorized by attacks for each source that was the source of attacks along with the attack name and the number of attacks that triggered with this combination.

For this period there are not sufficient AppWall results to generate information

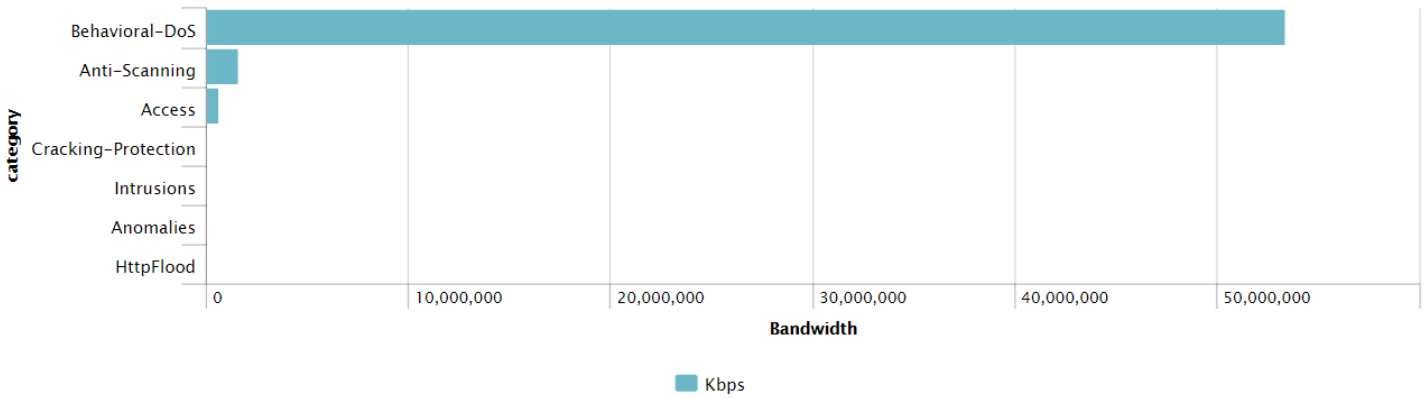
Bandwidth Information

Behavioral-DoS dropped **50.94** Gbps, Access protection dropped **621.04** Mbps**,** Intrusion protection dropped **55.31** Mbps of total traffic, **32.45** Mbps dropped by Packet Anomaly protection rules, Anti-Scanning protection dropped **1.55** Gbps**.** A total of **50.94** Gbps of malicious traffic was discarded this period.

Category	Gbps	Mbps
Behavioral-DoS	50.94	52166.15
Anti-Scanning	1.55	1585.76
Access	0.61	621.04
Cracking-Protection	0.07	75.38
Intrusions	0.05	55.31
Anomalies	0.03	32.45
HttpFlood	0.01	5.31
Total Bandwidth in Gbps/Mbps	53.26	54541.40

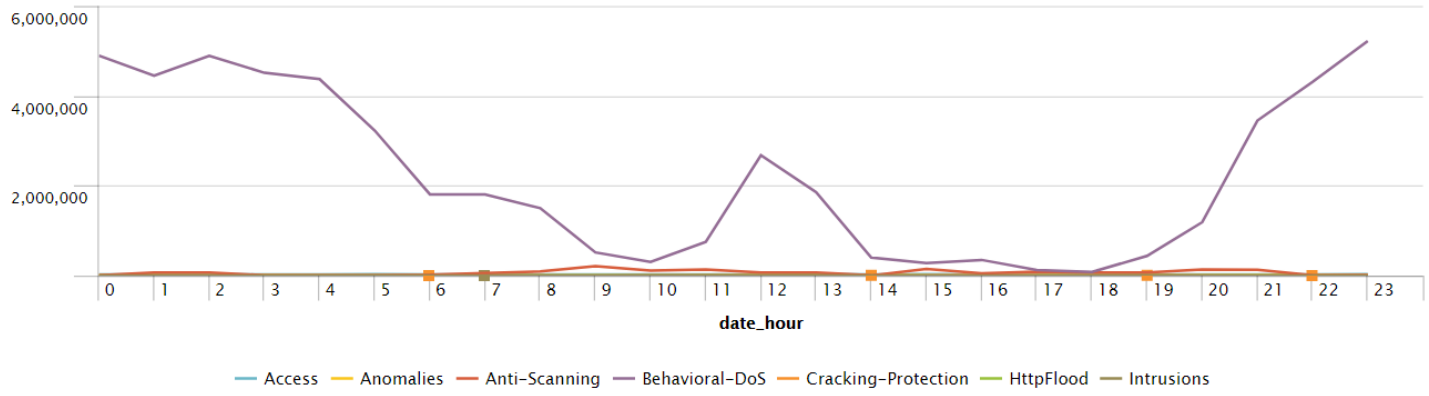
Graph: Attack Categories Blocked by Bandwidth

This report shows the attack categories based on the BW of the attacks sharing the same category including Kbps.



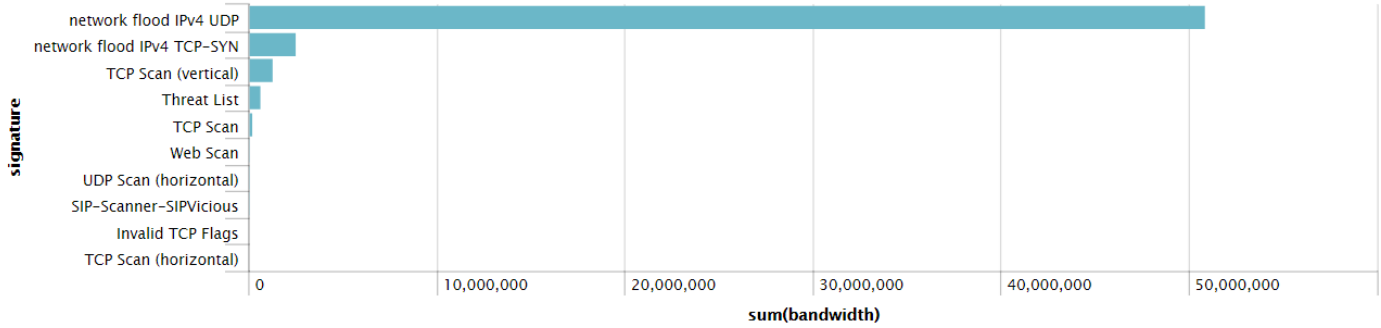
Graph: Bandwidth by Blocked Threat Category by Hour of Day

This report shows the most bandwidth consuming threat categories based on the bandwidth of the attacks sharing the same threat category for each hour of day.



Graph: Top Attacks Blocked by Bandwidth

This report shows the most bandwidth consuming attacks based on the BW of the attack including Kbits.



Scanning Information

Map of geographic distribution of **121,927** attacks on Metrobank from scanning sources. Some results do not include location information that allows map plotting.

Network-wide Anti Scanning protections dropped enumeration attempts which otherwise thwart any effort for threat modeling, commonplace after the information gathering phase of a targeted or planned attack.

We have included some of the most important ports scanned this period which tend to be exploited frequently by attackers. **Port Information:** Port **80** (http), Port **443** (http-alt)

Commonly scanned in order to attack web servers. SQL injection is currently the most common form of web site attack in that web forms are very common, often they are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available online. This kind of exploit is easy enough to accomplish that even inexperienced hackers can accomplish mischief. However, in the hands of the very skilled hacker, a web code weakness can reveal root level access of web servers and from there attacks on other networked servers can be accomplished. Structured Query Language (SQL) is the nearly universal language of databases that allows the storage, manipulation, and retrieval of data. Databases that use SQL include MS SQL Server, MySQL, Oracle, PostgreSQL, MongoDB, Access and Filemaker Pro and these databases are equally subject to SQL injection attack.

Web based forms must allow some access to your database to allow entry of data and a response, so this kind of attack bypasses firewalls and endpoint defenses. Any web form, even

a simple logon form or search box, might provide access to your data by means of SQL injection if coded incorrectly.

Port Information: Port **1433** (ms-sql-s), **3306** (mysql)
OWASP Top 10 for 2013 lists A1-Injection as the greatest threat and defines this category as: Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

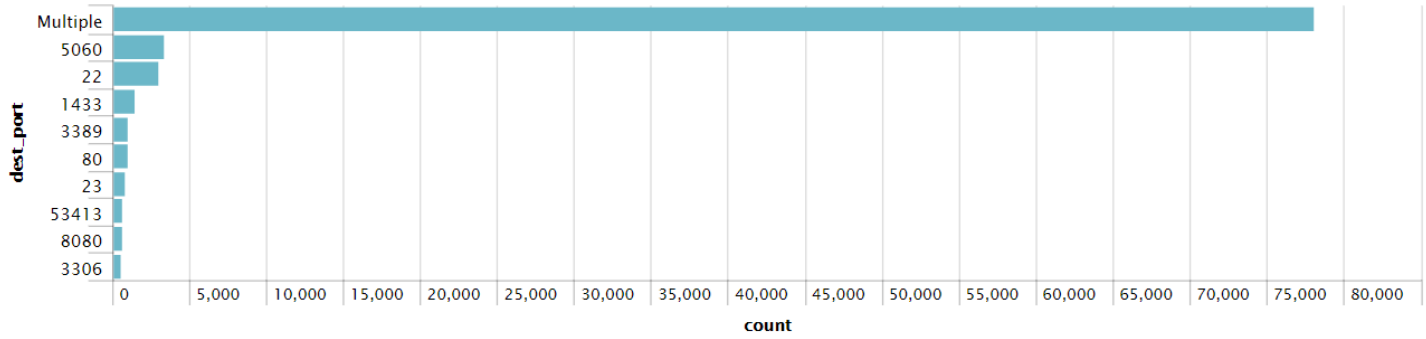
A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Port Information: Port **23** (telnet), **22** (ssh)
This port is commonly bruteforced for default administrative accounts which usually provide access to network and communications equipment.

Port Information: Port **5060** (sip)
The default gateway commonly associated with the SIP (Session Initiation Protocol) is the system port 5060. This communication portal supports the signaling protocol which is widely deployed for setting up (including tearing down) of sessions involving multimedia communication like video calls, voice calls and even VoIP (Voice over Internet Protocol). Threat actors commonly seek out these servers to comandeer the service in order to make free calls to countries of their choice or use them to carry out phone scams.

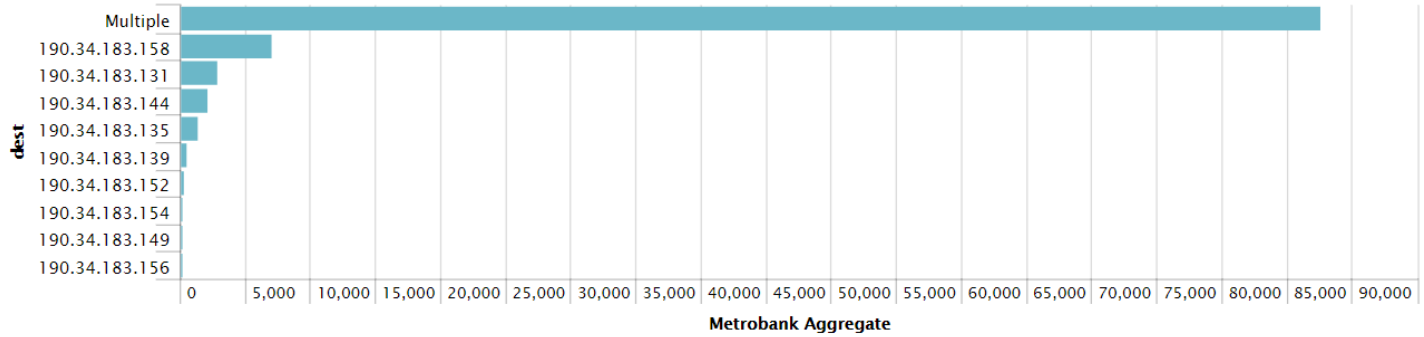
Graph: Top Probed Applications Blocked

This report shows historical view of the Top probed L4 ports.



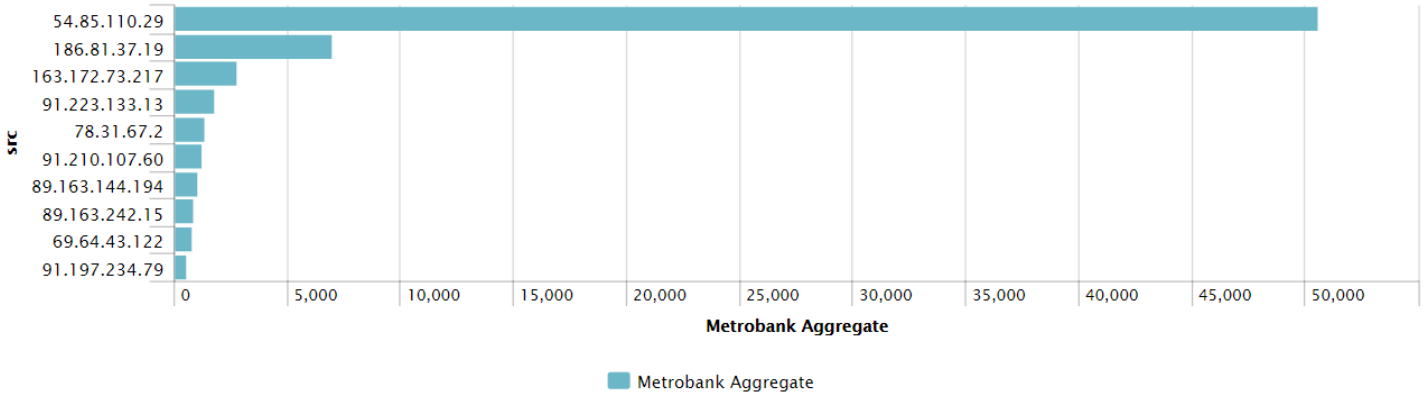
Graph: Top Probed IP Addresses Blocked

This report shows historical view of the Top probed IP addresses that were being scanned along with the network security rule.



Graph: Top Scanners Blocked (Source IP Addressed)

This report shows historical view of the Top source IP addresses that have scanned the network by network scanning activities along with the network security rule.



See Appendix 2 – Top Scanners Blocked (Source IP Addressed)

Vulnerability Management

It is important to establish a vulnerability management program as part of the information security strategy because soon after new vulnerabilities are discovered and reported by security researchers or vendors, attackers engineer exploit code and then launch that code against targets of interest. Any significant delays in finding or fixing software with dangerous vulnerabilities provides ample opportunity for persistent attackers to break through, gaining control over the vulnerable machines and getting access to the sensitive data they contain. Organizations that do not scan for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their systems compromised.

The GLESEC MSS'VME Management System platform performs a security mapping of your organization network, runs tests on everything the speaks IP, and accurately evaluates the presence of vulnerabilities.

Many of the vulnerabilities will provide CVE data. CVE (Common
Vulnerabilities and Exposures) is a list of information security exposures and vulnerabilities sponsored by US-CERT and maintained by the MITRE Corporation. The CVE mission is to provide standard names for all publicly known security exposures as well as standard definitions for security terms. The CVE can be searched online at

Vulnerability Score

The score of a vulnerability is determined by its risk factor; High, Medium or Low, as well as its value in the Common Vulnerability Scoring System (CVSS). The CVSS "base score" represents the innate risk characteristic of each vulnerability. CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize and coordinate a joint response to security vulnerabilities by communicating the base, temporal and environmental properties of each vulnerability. In addition to numeric scores, the CVSS provides severity rankings of High, Medium, and Low but these qualitative rankings are simply mapped from the numeric CVSS scores.
Vulnerabilities are labelled as:

a) Low risk if they have a CVSS base score of 0.0 – 3.9
b) Medium risk if they have a CVSS base score of 4.0 – 6.9
c) High risk if they have a CVSS base score of 7.0 – 10.0

Vulnerabilities in the report are classified into 3 risk categories: high, medium or low.
High Risk
Describes vulnerabilities that can allow an attacker to gain elevated privileges, remote command execution, full read/write access, or critical information disclosure (e.g. passwords, hashes) on a vulnerable machine and should be addressed as top priority.

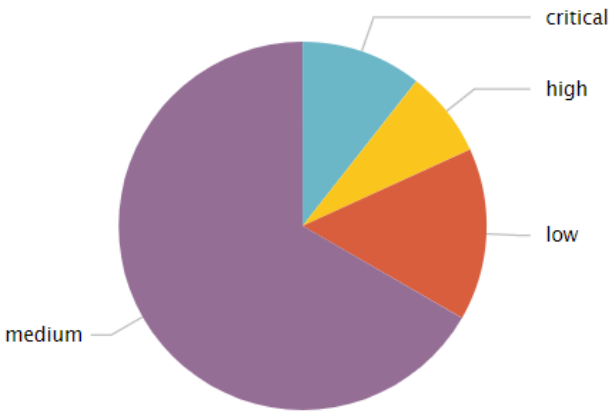
Medium Risk
Describes vulnerabilities that either expose sensitive data, directory browsing and traversal, disclosure of security controls, facilitate unauthorized use of services or denial of service to an attacker.

Low Risk
Describes vulnerabilities that allow preliminary or sensitive information gathering for an attacker or pose risks that are not entirely security related but maybe used in social-engineering or similar attacks.

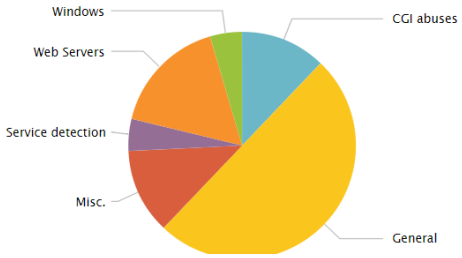
Vulnerability Information

We can observe that Intrusions (known attack signatures), HTTP Flood and Web Scanning attempts are targeting Web Servers and are being dropped by the DefensePro. We cannot be 100% sure but there is a high probability that this type of attack is occurring and if the DefensePro was not in place, the attack might have been successfully carried out. The same is true for Mail servers which are frequently being scanned (Web Scanning).

Graph: Risk Distribution
This report depicts the risk distribution of vulnerabilities discovered this report period

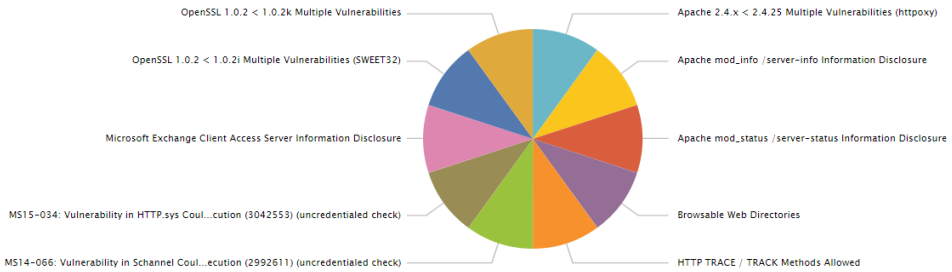


Graph: Most Frequent Vulnerability Category
This report depicts the most frequent vulnerabilities by category discovered this report period



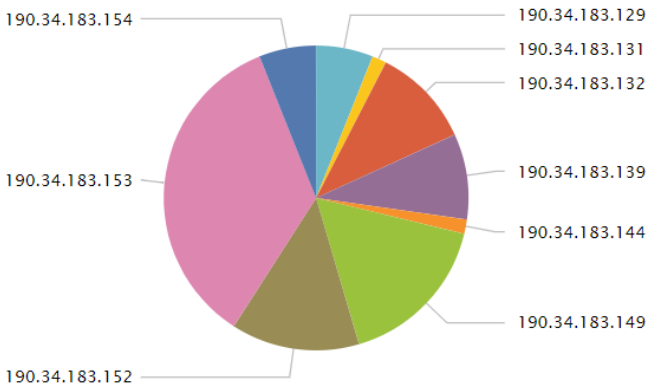
Graph: Most Frequent Vulnerability Name

This report depicts the most frequent vulnerabilities discovered this report period



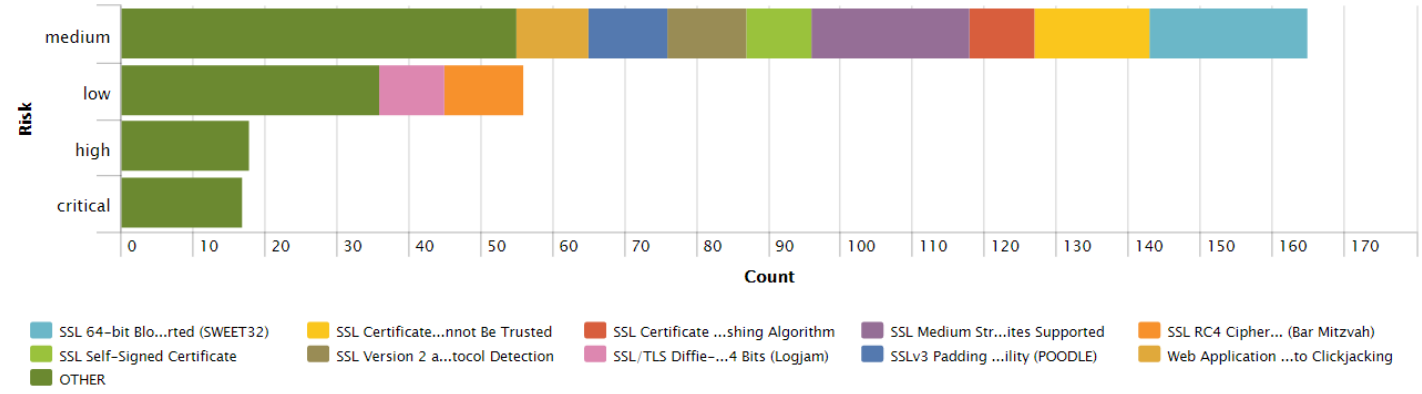
Graph: Most Vulnerable Host

This report depicts the most vulnerable hosts discovered this report period



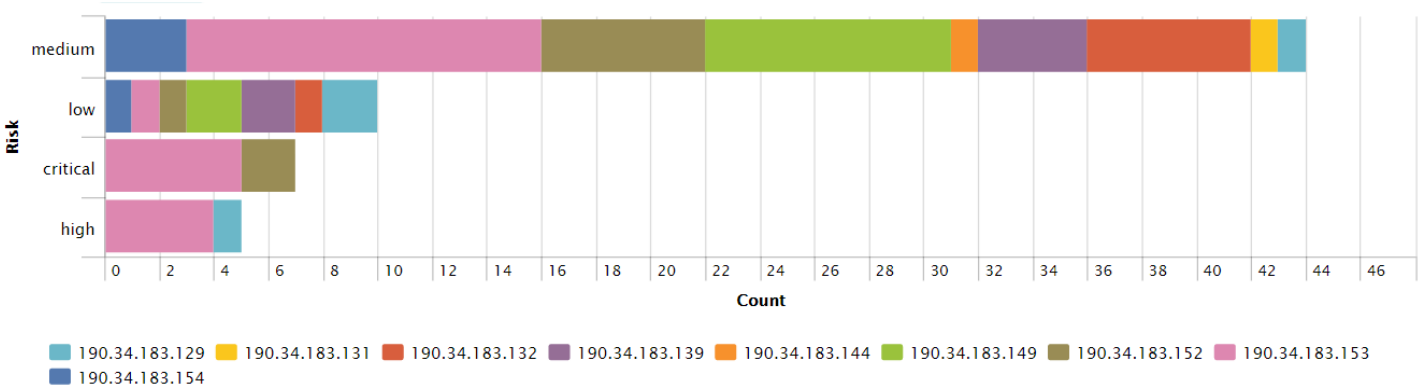
Graph: Vulnerability Risk by Vulnerability Name

This report illustrates the vulnerability risk and count by vulnerability name discovered this report period



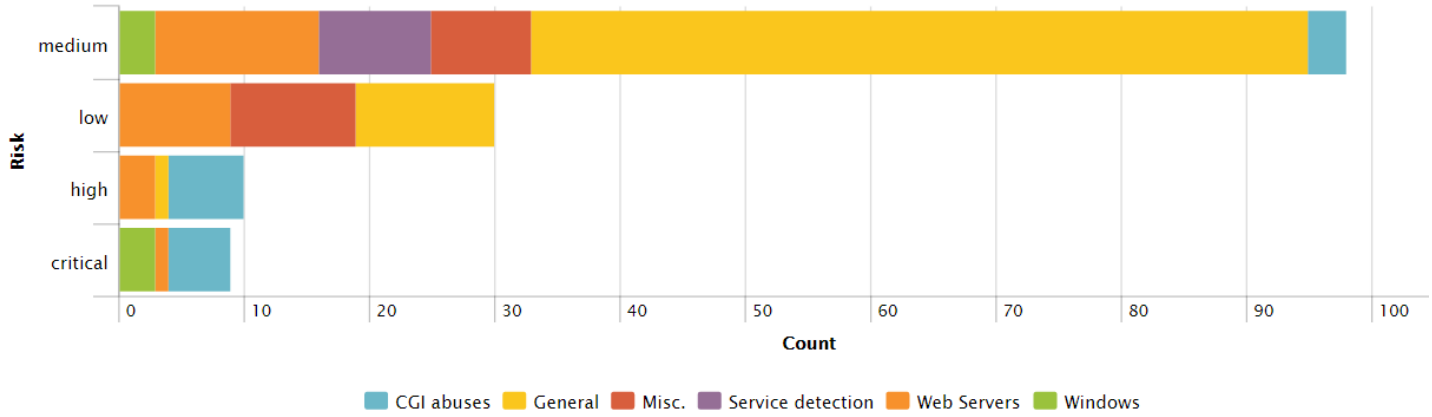
Graph: Vulnerability Risk by Host

This report illustrates the vulnerability risk and count by category discovered this report period



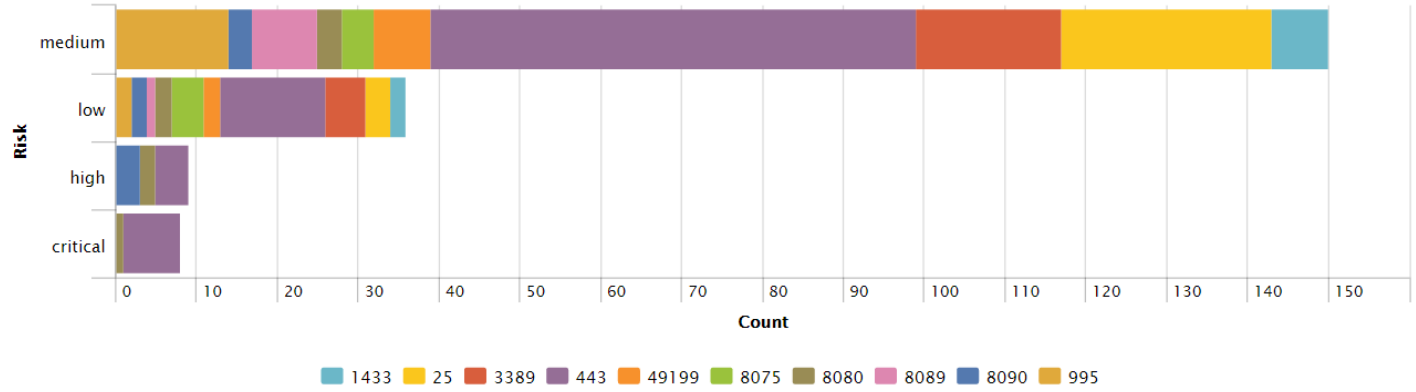
Graph: Vulnerability Risk by Category

This report illustrates the vulnerability risk and count by category discovered this report period



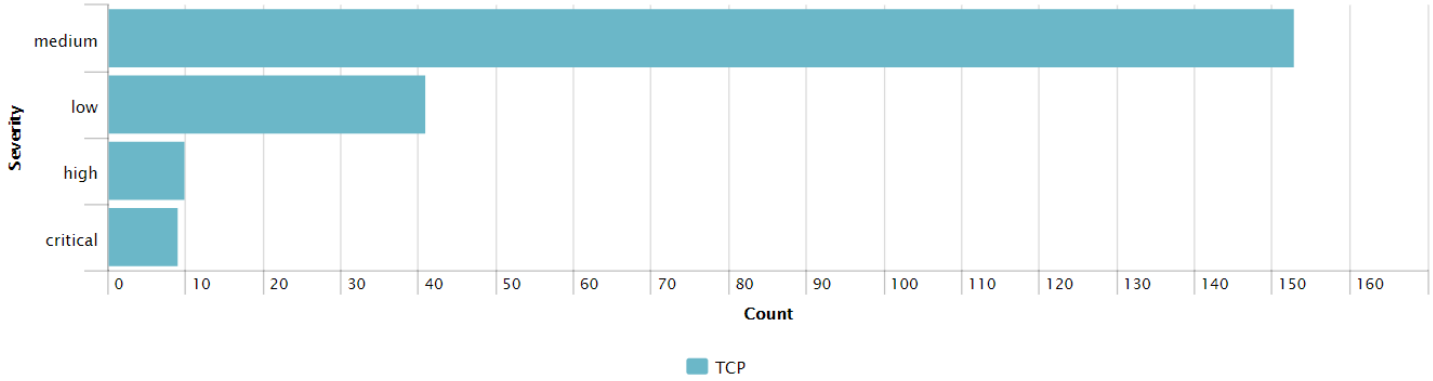
Graph: Vulnerability Risk by Port

This report illustrates the vulnerability risk and count by port discovered this report period



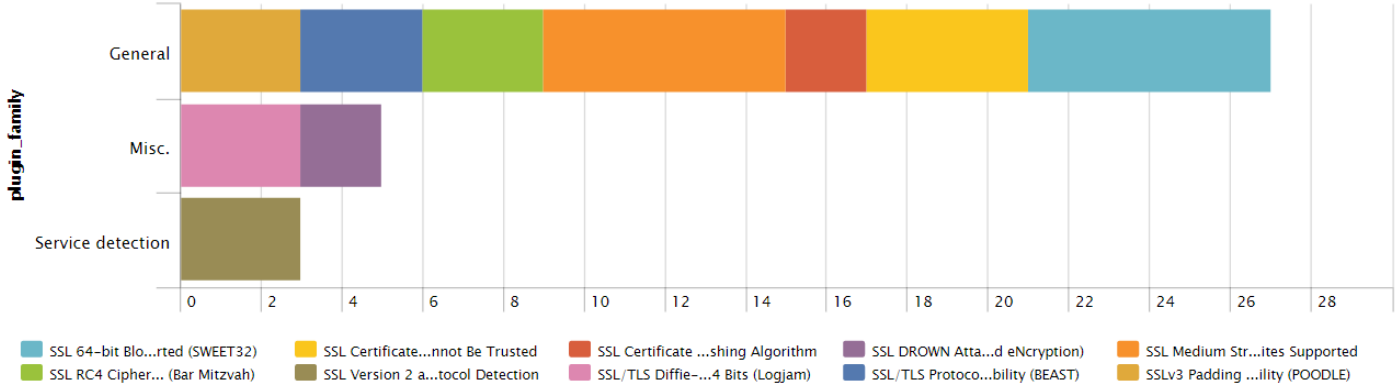
Graph: Vulnerability Risk by Protocol

This report illustrates the vulnerability risk and count by protocol discovered this report period



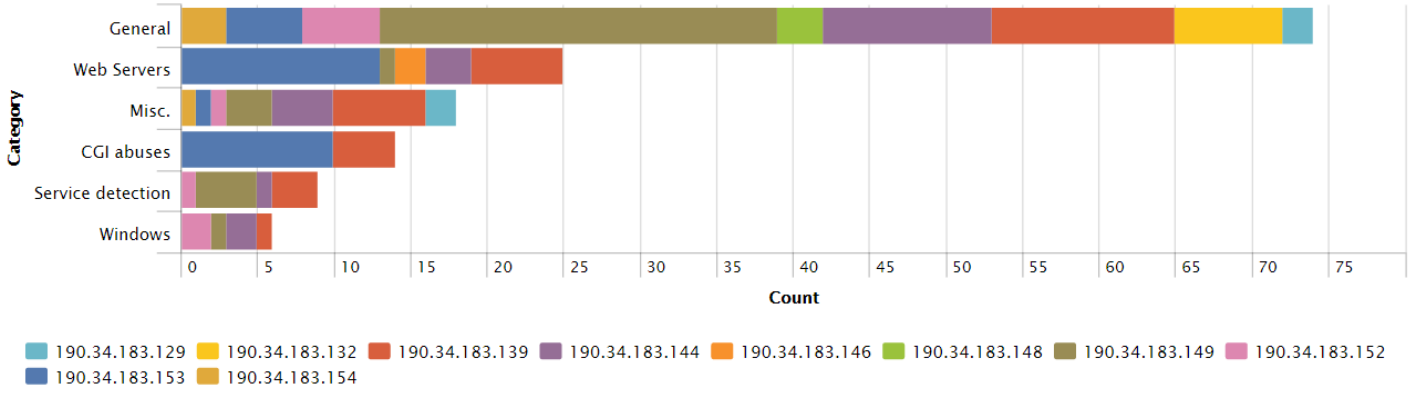
Graph: Vulnerability Category by Vulnerability Name

This report illustrates the vulnerability category and count by vulnerability name discovered this report period



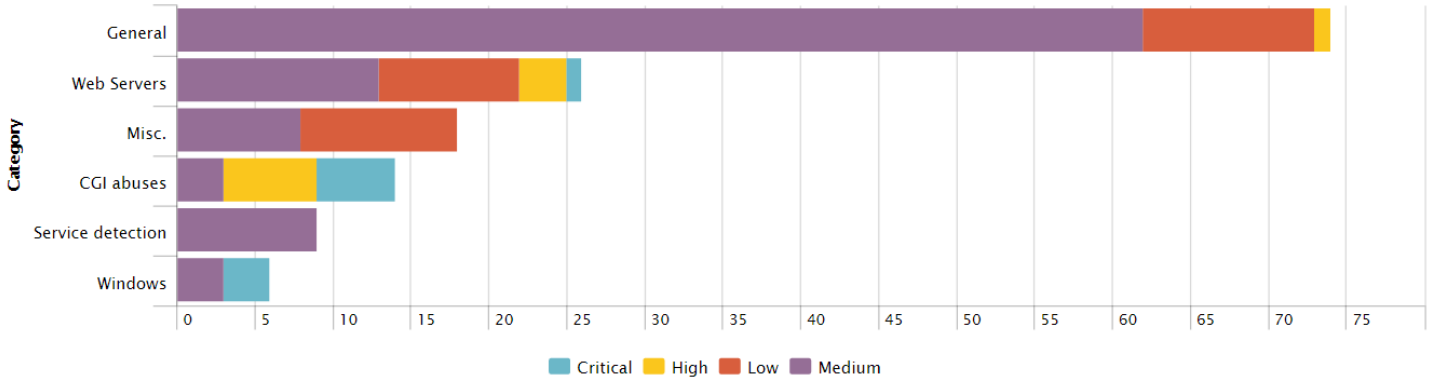
Graph: Vulnerability Category by Host

This report illustrates the vulnerability category and count by host discovered this report period



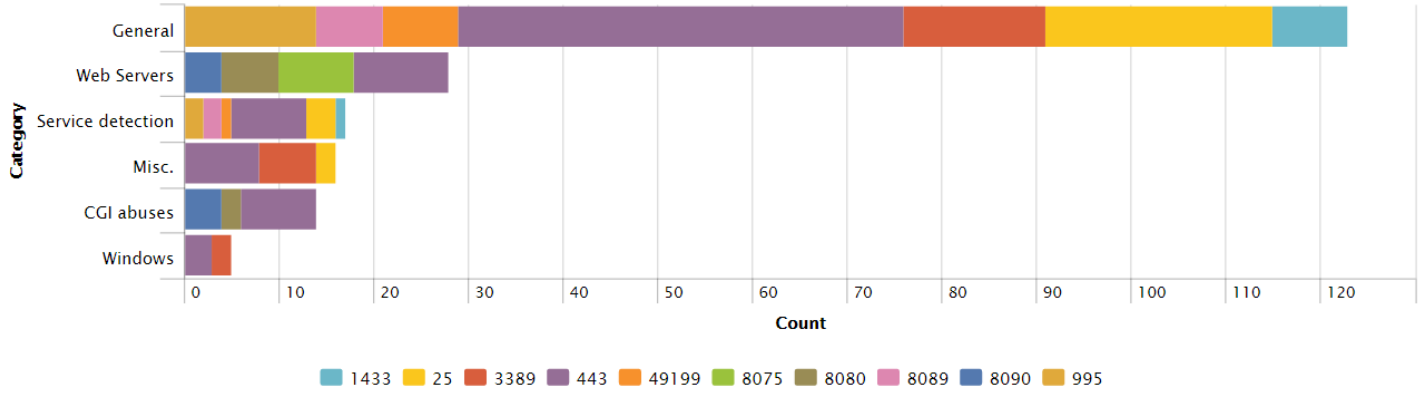
Graph: Vulnerability Category by Risk

This report illustrates the vulnerability category and count by risk discovered this report period



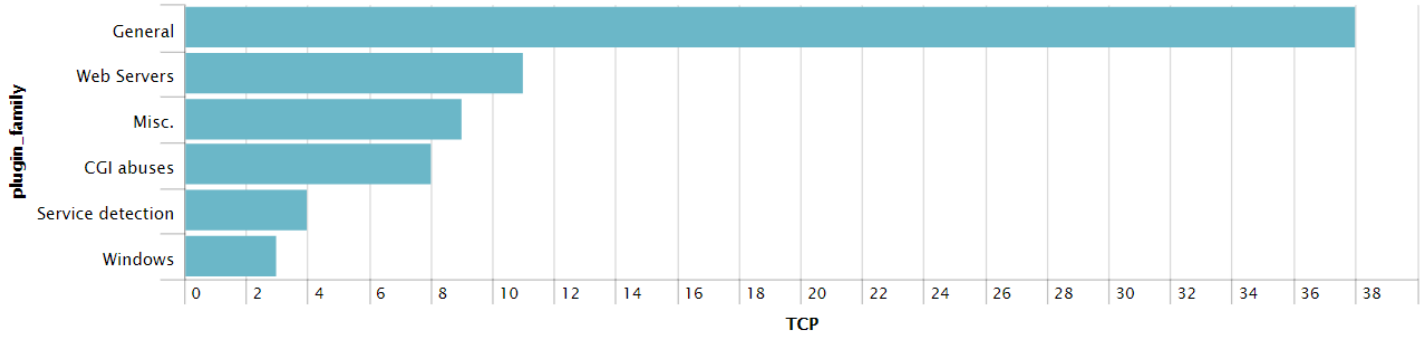
Graph: Vulnerability Category by Port

This report illustrates the vulnerability category and count by port discovered this report period



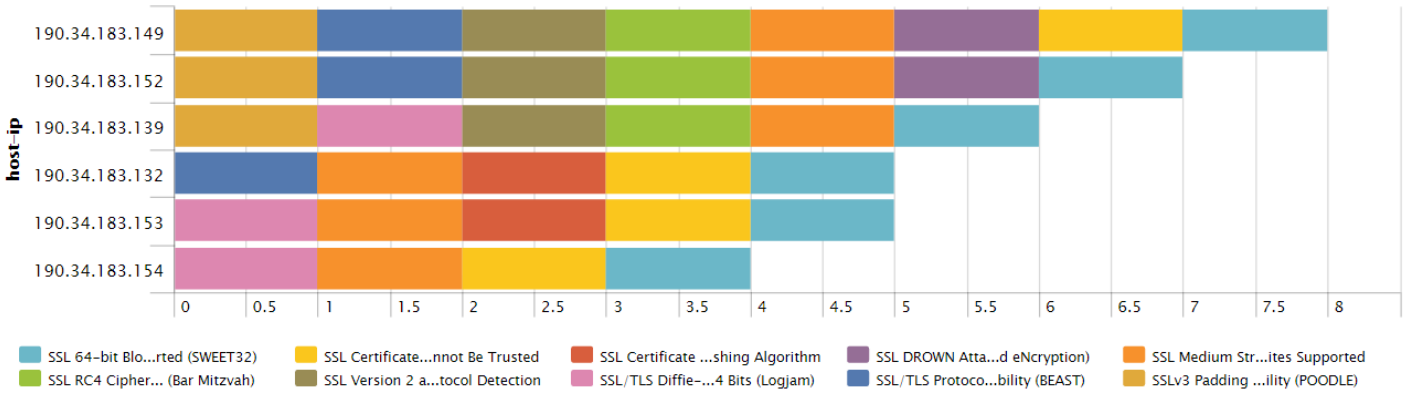
Graph: Vulnerability Category by Protocol

This report illustrates the vulnerability category and count by protocol discovered this report period



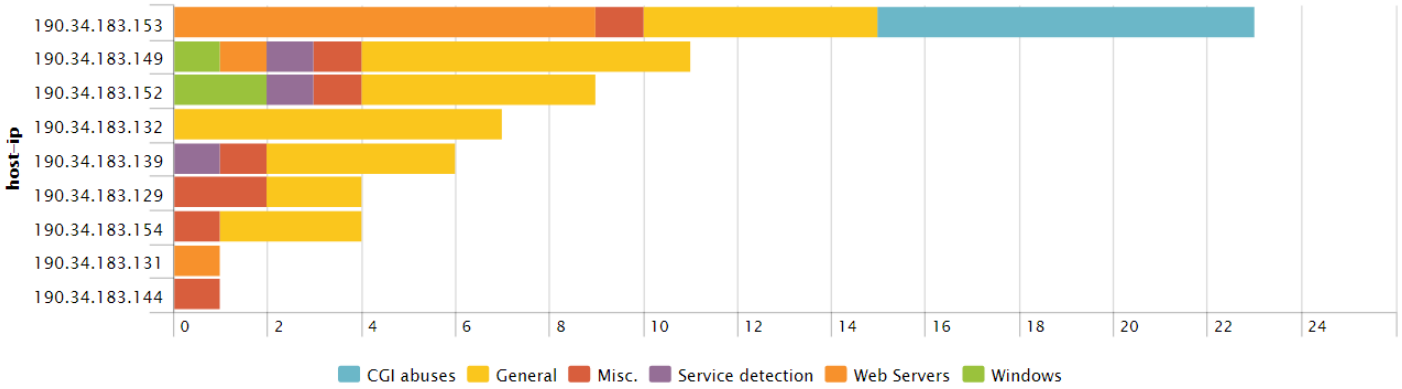
Graph: Host by Vulnerability Name

This report illustrates the vulnerability name and count by hosts discovered this report period



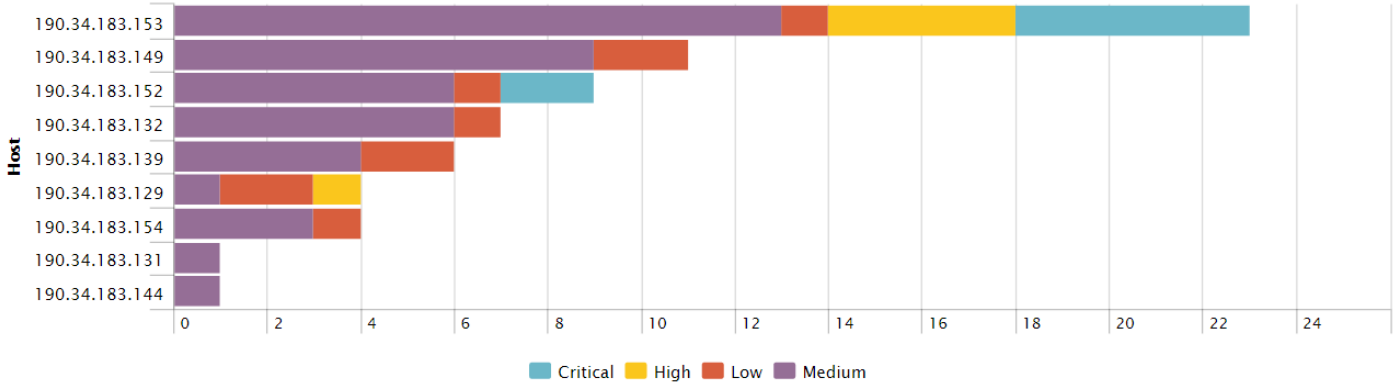
Graph: Host by Vulnerability Category

This report illustrates the vulnerability category and count by hosts discovered this report period



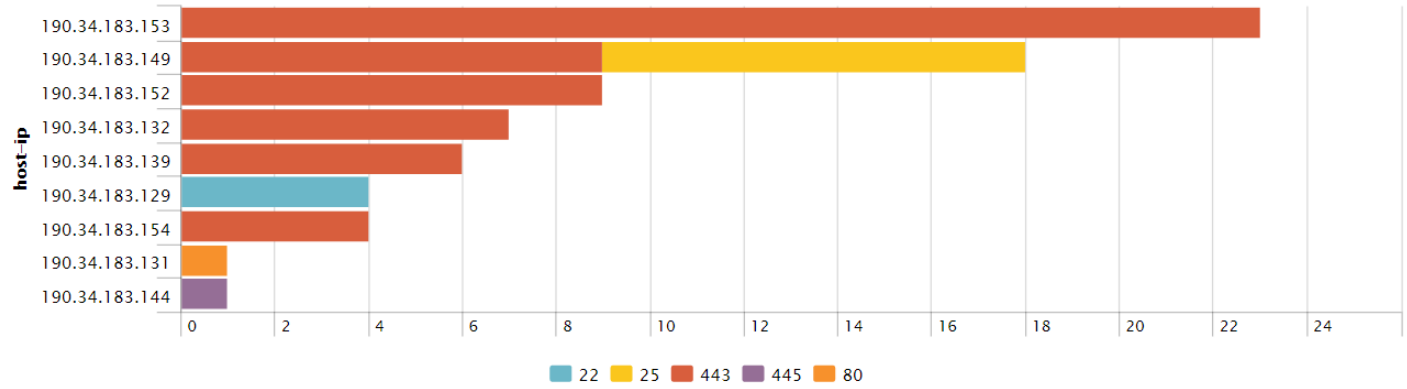
Graph: Host by Vulnerability Risk

This report illustrates the vulnerability risk and count by hosts discovered this report period



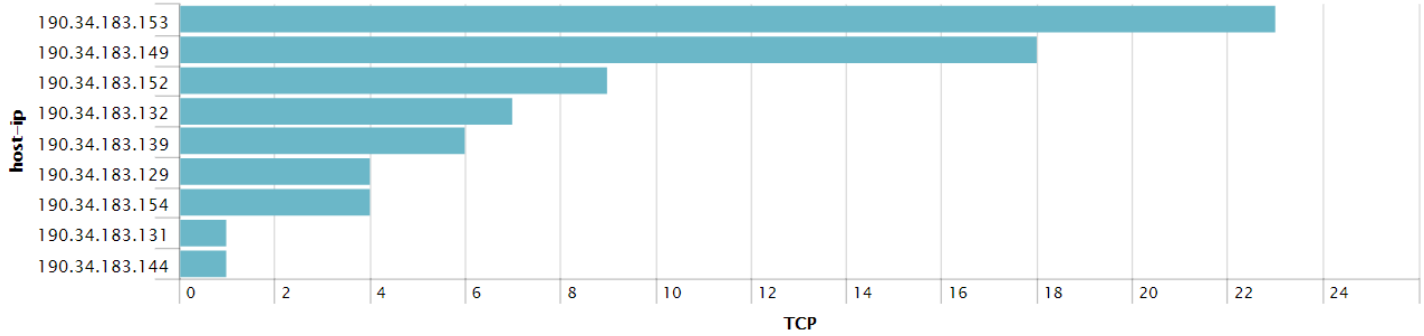
Graph: Host by Port

This report illustrates the port and count by hosts discovered this report period



Graph: Host by Protocol

This report illustrates the protocol and count by hosts discovered this report period



7. Security Operations

The purpose of this section is to highlight the activities performed by GLESEC's Global Operations Center (GOC) including: monitoring availability and performance of equipment under contract, Change Management and Incident Response activities.

a) Monitoring System Availability

Metrobank DefensePro Availability:

The DefensePro was considered up and available 100**%** during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	30d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	30d 0h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	30d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Metrobank AppWall Availability:

The AppWall was considered up and available 100**%** during this report period.

Host State Breakdowns:

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	30d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	30d 0h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	30d 0h 0m 0s	100.000%	100.000%

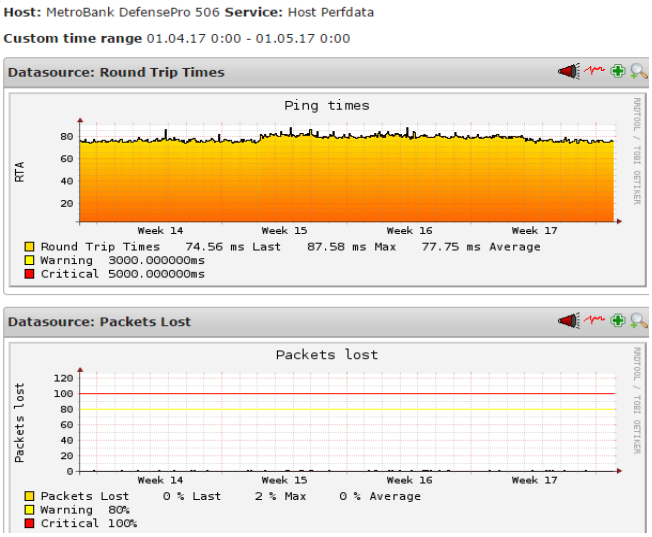
State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	100.000% (100.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

b) Monitoring system performance

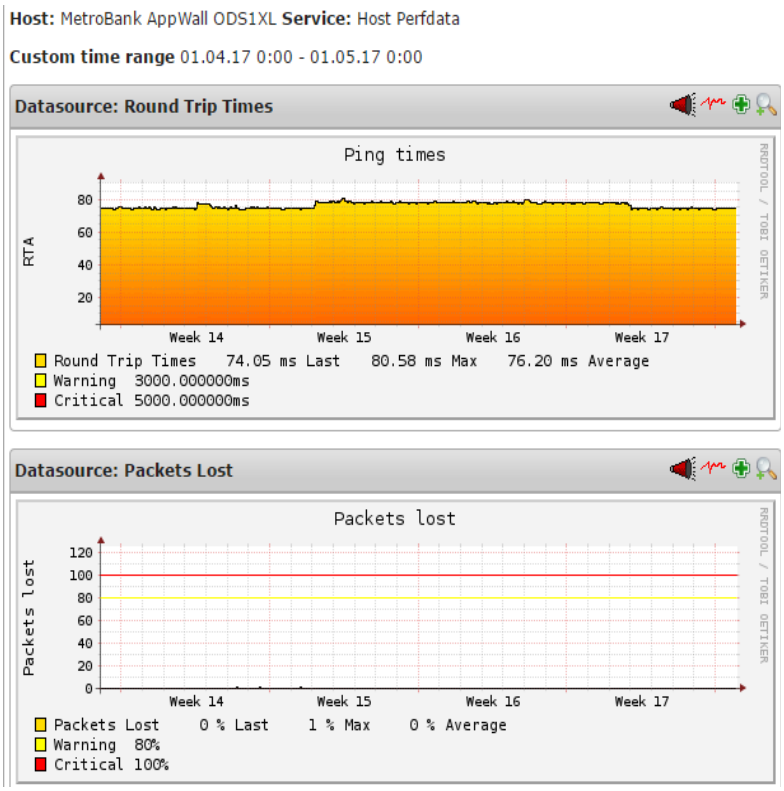
Metrobank DefensePro Host Performance

Round trip ping times averaged 77.75 ms from the GLESEC GOC to Metrobank with 0% average packet loss.



Metrobank AppWall Host Performance

Round trip ping times averaged 76.20 ms from the GLESEC GOC to Metrobank with 0% average packet loss.



c) Change Management Activities

The GOC has been working with Metrobank Staff to tune the AppWall. Work continues into May

d) Incident Response Activities

No incident Response activity during the month of April 2017

9. Appendix 2 – Top Scanners Blocked (WHOIS Information)

This section provides additional WHOIS detail for the Graph: Top Scanners Blocked (Source IP Addressed)

NetRange: 65.5.139.96 - 65.5.139.127
CIDR: 65.5.139.96/27
OriginAS:
NetName: BLS-65-5-139-96-27-1007264407
NetHandle: NET-65-5-139-96-1
Parent: NET-65-0-0-0-1
NetType: Reassigned
RegDate: 2010-07-26
Updated: 2010-07-26
Ref: http://whois.arin.net/rest/net/NET-65-5-139-96-1

CustName: Datapro
Address: 770 Ponce De Leon
City: Coral Gables
StateProv: FL
PostalCode: 33131
Country: US
RegDate: 2010-07-26
Updated: 2011-03-19
Ref:
OrgAbuseHandle: ABUSE81-ARIN
OrgAbuseName: Abuse Group
OrgAbusePhone: +1-919-319-8265
OrgAbuseEmail:
OrgAbuseRef:
OrgTechHandle: IPOPE3-ARIN
OrgTechName: IP Operations
OrgTechPhone: +1-888-510-5545
OrgTechEmail:
OrgTechRef:
RAbuseHandle: ABUSE81-ARIN
RAbuseName: Abuse Group
RAbusePhone: +1-919-319-8265
RAbuseEmail:
RAbuseRef:

RTechHandle: IPOPE3-ARIN
RTechName: IP Operations
RTechPhone: +1-888-510-5545
RTechEmail:
RTechRef:

inetnum: 200.46.160/20
status: allocated
aut-num: N/A
owner: Cable Onda
ownerid: PA-CAON1-LACNIC
responsible: Climaco Manuel Paz
address: Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address: 55-0593 - Panama - PA
country: PA
phone: +507 390 3485 []
owner-c: CAO
tech-c: CAO
abuse-c: CAO
inetrev: 200.46.174/23
nserver: NS.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 19981221
changed: 20140826

nic-hdl: CAO
person: Cable Onda Panama
e-mail:
address: Edificio Cable Onda, Pueblo Nuevo, 0, 0
address: 0831-0059 - Panama - PA
country: PA
phone: +507 3907616 []

created: 20021009
changed: 20071107

inetnum: 200.46.160/20
status: allocated
aut-num: N/A
owner: Cable Onda
ownerid: PA-CAON1-LACNIC
responsible: Climaco Manuel Paz
address: Ave. 12 de Octubre, Pueblo Nuevo, Edif. Cable Onda, 0593,
address: 55-0593 - Panama - PA
country: PA
phone: +507 390 3485 []
owner-c: CAO
tech-c: CAO
abuse-c: CAO
inetrev: 200.46.174/23
nserver: NS.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.PSINETPA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 19981221
changed: 20140826

nic-hdl: CAO
person: Cable Onda Panama
e-mail:
address: Edificio Cable Onda, Pueblo Nuevo, 0, 0
address: 0831-0059 - Panama - PA
country: PA
phone: +507 3907616 []
created: 20021009
changed: 20071107

NetRange: 23.24.0.0 - 23.25.255.255

CIDR: 23.24.0.0/15
NetName: CBC-ALLOC-4
NetHandle: NET-23-24-0-0-1
Parent: NET23 (NET-23-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Comcast Business Communications, LLC (CBCI)
RegDate: 2012-01-13
Updated: 2012-02-23
Ref: http://whois.arin.net/rest/net/NET-23-24-0-0-1

OrgName: Comcast Business Communications, LLC
OrgId: CBCI
Address: 1800 Bishops Gate Blvd.
City: Mount Laurel
StateProv: NJ
PostalCode: 08054-4628
Country: US
RegDate: 2001-12-21
Updated: 2011-01-06
Ref: http://whois.arin.net/rest/org/CBCI

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName: Network Abuse and Policy Observance
OrgAbusePhone: +1-888-565-4329
OrgAbuseEmail:
OrgAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

OrgTechHandle: IC161-ARIN
OrgTechName: Comcast Cable Communications Inc
OrgTechPhone: +1-856-317-7200
OrgTechEmail:
OrgTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

RTechHandle: IC161-ARIN
RTechName: Comcast Cable Communications Inc
RTechPhone: +1-856-317-7200
RTechEmail:
RTechRef: http://whois.arin.net/rest/poc/IC161-ARIN

RAbuseHandle: NAPO-ARIN
RAbuseName: Network Abuse and Policy Observance
RAbusePhone: +1-888-565-4329
RAbuseEmail:
RAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

NetRange: 23.24.160.0 - 23.24.191.255
CIDR: 23.24.160.0/19
NetName: CBC-MIAMI-25
NetHandle: NET-23-24-160-0-1
Parent: CBC-ALLOC-4 (NET-23-24-0-0-1)
NetType: Reallocated
OriginAS:
Organization: Comcast Business Communications, LLC (CBCI)
RegDate: 2012-02-24
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-23-24-160-0-1

OrgName: Comcast Business Communications, LLC
OrgId: CBCI
Address: 1800 Bishops Gate Blvd.
City: Mount Laurel
StateProv: NJ
PostalCode: 08054-4628
Country: US
RegDate: 2001-12-21
Updated: 2011-01-06
Ref: http://whois.arin.net/rest/org/CBCI

OrgAbuseHandle: NAPO-ARIN
OrgAbuseName: Network Abuse and Policy Observance
OrgAbusePhone: +1-888-565-4329
OrgAbuseEmail:
OrgAbuseRef: http://whois.arin.net/rest/poc/NAPO-ARIN

OrgTechHandle: IC161-ARIN
OrgTechName: Comcast Cable Communications Inc
OrgTechPhone: +1-856-317-7200

OrgTechEmail:
OrgTechRef:

inetnum: 190.34/15
status: allocated
aut-num: N/A
owner: Cable & Wireless Panama
ownerid: PA-CWPA-LACNIC
responsible: Cable and Wireless Panama
address: 0834-00659, Panama, 9A,
address: 083400659 - Panama - -
country: PA
phone: +507 2696181 []
owner-c: CAP3
tech-c: CAP3
abuse-c: CAP3
inetrev: 190.34/15
nserver: NS.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 20061122
changed: 20061122

nic-hdl: CAP3
person: Russell Bean
e-mail:
address: Apartado 659, PA,
address: 9A - Panama -
country: PA
phone: +507 882 2200 [22]
created: 20030416
changed: 20130509

inetnum: 190.33/16
status: allocated
aut-num: N/A
owner: Cable & Wireless Panama
ownerid: PA-CWPA-LACNIC
responsible: Cable and Wireless Panama
address: 0834-00659, Panama, 9A,
address: 083400659 - Panama - -
country: PA
phone: +507 2696181 []
owner-c: CAP3
tech-c: CAP3
abuse-c: CAP3
inetrev: 190.33/16
nserver: NS.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
nserver: NS2.CWPANAMA.NET
nsstat: 20141109 AA
nslastaa: 20141109
created: 20060815
changed: 20060815

nic-hdl: CAP3
person: Russell Bean
e-mail:
address: Apartado 659, PA,
address: 9A - Panama -
country: PA
phone: +507 882 2200 [22]
created: 20030416
changed: 20130509

inetnum: 200.46.226.208/28
status: reallocated
owner: STARUN, S.A.

ownerid: PA-STSA1-LACNIC
responsible: NET2NET IP Admin
address: Colon, 1, 1
address: 11111 - Colon -
country: PA
phone: +507 3008888 []
owner-c: NEA3
tech-c: NEA3
abuse-c: NEA3
created: 20050504
changed: 20050504
inetnum-up: 200.46.224/19

nic-hdl: NEA3
person: Net2Net Admin
e-mail:
address: Plaza Bal Harbour Paitilla, 1,
address: 55-0779 - Panama - PA
country: PA
phone: +507 206-3000 [ATM]
created: 20030414
changed: 20091028

NetRange: 22.0.0.0 - 22.255.255.255
CIDR: 22.0.0.0/8
NetName: DNIC-SNET-022
NetHandle: NET-22-0-0-0-1
Parent: ()
NetType: Direct Allocation
OriginAS:
Organization: DoD Network Information Center (DNIC)
RegDate: 1989-06-26
Updated: 2009-04-15
Ref: http://whois.arin.net/rest/net/NET-22-0-0-0-1

OrgName: DoD Network Information Center
OrgId: DNIC

Address: 3990 E. Broad Street
City: Columbus
StateProv: OH
PostalCode: 43218
Country: US
RegDate:
Updated: 2011-08-17
Ref: http://whois.arin.net/rest/org/DNIC

OrgTechHandle: REGIS10-ARIN
OrgTechName: Registration
OrgTechPhone: +1-800-365-3642
OrgTechEmail: disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef: http://whois.arin.net/rest/poc/REGIS10-ARIN

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName: Network DoD
OrgTechPhone: +1-614-692-6337
OrgTechEmail: disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef: http://whois.arin.net/rest/poc/MIL-HSTMST-ARIN

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName: Registration
OrgAbusePhone: +1-800-365-3642
OrgAbuseEmail: disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgAbuseRef:

inetnum: 203.178.0.0 - 203.183.255.255
netname: JPNIC-NET-JP
descr: Japan Network Information Center
country: JP
admin-c: JNIC1-AP
tech-c: JNIC1-AP
remarks: JPNIC Allocation Block
remarks: Authoritative information regarding assignments and
remarks: allocations made from within this block can also be
remarks: queried at whois.nic.ad.jp. To obtain an English

remarks: output query whois -h whois.nic.ad.jp x.x.x.x/e
mnt-by: MAINT-JPNIC
changed: 19991208
status: ALLOCATED PORTABLE
source: APNIC

role: Japan Network Information Center
address: Urbannet-Kanda Bldg 4F
address: 3-6-2 Uchi-Kanda
address: Chiyoda-ku, Tokyo 101-0047,Japan
country: JP
phone: +81-3-5297-2311
fax-no: +81-3-5297-2312
e-mail:
admin-c: JI13-AP
tech-c: JE53-AP
nic-hdl: JNIC1-AP
mnt-by: MAINT-JPNIC
changed: 20041222
changed: 20050324
changed: 20051027
changed: 20120828
source: APNIC

inetnum: 203.178.148.16 - 203.178.148.23
netname: ISI-JP
descr: University of Southern California, Information Sciences Institute
country: JP
admin-c: JH3937JP
tech-c: YP221JP
remarks: This information has been partially mirrored by APNIC from
remarks: JPNIC. To obtain more specific information, please use the
remarks: JPNIC WHOIS Gateway at
remarks: http://www.nic.ad.jp/en/db/whois/en-gateway.html or
remarks: whois.nic.ad.jp for WHOIS client. (The WHOIS client
remarks: defaults to Japanese output, use the /e switch for English
remarks: output)
changed: 20110810
changed: 20110823

source: JPNIC

inetnum: 190.62/16
status: allocated
aut-num: AS22833
abuse-c: RAC3
owner: CTE S.A. de C.V.
ownerid: SV-CSCV-LACNIC
responsible: CLARO INTERNET
address: Colonia Roma, Calle El Progreso, Complejo Telecom, A,
address: 4175 - San Salvador - SS
country: SV
phone: +503 22503836 []
owner-c: EAB4
tech-c: EAB4
abuse-c: EAB4
created: 20110121
changed: 20120523

nic-hdl: EAB4
person: Alexander Peña
e-mail:
address: xxxx, ,
address: 0000 - San Salvador -
country: SV
phone: +503 503 22505555 []
created: 20101103
changed: 20130809

nic-hdl: RAC3
person: Alberto Lemus
e-mail:
address: Colonia Roma Calle El Progreso Complejo Telecom, 4175,
address: 4175 - San Salvador - SS
country: SV
phone: +503 250 3836 []
created: 20040510
changed: 20060713

10. Appendix 3 – Glossary of Terms

Amplification Attack

An Amplification Attack is any attack where an attacker is able to use an amplification factor to multiply its power. Amplification attacks are "asymmetric", meaning that a relatively small number or low level of resources is required by an attacker to cause a significantly greater number or higher level of target resources to malfunction or fail. Examples of amplification attacks include Smurf Attacks (ICMP amplification), Fraggle Attacks (UDP amplification), and DNS Amplification.

Botnet

A botnet is a collection of compromised computers often referred to as "zombies" infected with malware that allows an attacker to control them. Botnet owners or "herders" are able to control the machines in their botnet by means of a covert channel such as IRC (Internet Relay Chat), issuing commands to perform malicious activities such as distributed denial-of-service (DDoS) attacks, the sending of spam mail, and information theft. As of 2006, the average size of any given botnet around the world was around 20,000 machines (as botnet owners attempted to scale down their networks to avoid detection), although some larger more advanced botnets such as BredoLab, Conficker, TDL-4, and Zeus have been estimated to contain millions of machines.

Computer Emergency Readiness Team Computer Emergency Response Team Computer Security Incident Response Team

Computer Emergency Response Team is a name given to expert groups that handle computer security incidents. Most groups append the abbreviation CERT or CSIRT to their designation where the latter stands for Computer Security Incident Response Team.

DDoS (Distributed Denial-of-Service) Attack

DDoS or Distributed Denial-of-Service attacks are a variant of Denial-of-Service DoS attacks where an attacker or a group of attackers employ multiple machines to carry out a DoS attack simultaneously, therefore increasing its effectiveness and strength. The "army" carrying out the attack is mostly often composed of innocent infected zombie computers manipulated as bots and being part of a botnet controlled by the attacker via a Command and Control Server. A botnet is powerful, well coordinated and could count millions of computers. It also insures the anonymity of the original attacker since the attack traffic originates from the bots' IPs rather than the attacker's. In some cases, mostly in ideological DDoS attacks, this "army" could also be composed of recruited hackers/hacktivits participating in large DDoS attack campaigns (Operation Blackout, Operation Payback etc.). DDoS attacks are hard to detect and block since the attack traffic is easily confused with legitimate traffic and difficult to trace.

There are many types of DDoS attacks targeting both the network and the application layers. They could be classified upon their impact on the targeted computing resources (saturating

bandwidth, consuming server's resources, exhausting an application) or upon the targeted resources as well:

- Attacks targeting Network Resources: UDP Floods, ICMP Floods, IGMP Floods.
- Attacks targeting Server Resources: the TCP/IP weaknesses –TCP SYN Floods, TCP RST attacks, TCP PSH+ACK attacks – but also Low and Slow attacks as Sockstress for example and SSL-based attacks, which detection is particularly challenging.
- Attacks targeting the Application Resources: HTTP Floods, DNS Floods and other Low and Slow attacks as Slow HTTP GET requests (Slowloris) and Slow HTTP POST requests (R-U-Dead-Yet).

A DDoS attack usually comprises more than three attack vectors thus increasing the attacker's chances to hit its target and escape basic DoS mitigation solutions.

DoS (Denial-of-Service) Attack

A Denial-of-Service DOS attack is an attack targeting the availability of web applications. Unlike other kinds of attacks, DoS attacks' primary goal is not to steal information but to slow or take down a web site. The attackers' motivations are diverse, ranging from simple fun, to financial gain and ideology (hacktivism). A DoS attack generates high or slow rate attack traffic exhausting computing resources of a target, therefore preventing legitimate users from accessing the website. DoS attacks affect enterprises from all sectors (e-gaming, Banking, Government etc.), all sizes (mid/big enterprises) and all locations. They target the network layer and up to the application layer, where attacks are more difficult to detect since they could easily get confused with legitimate traffic. There are several types of DoS attacks. A (non-distributed) DoS attack is when an attacker uses a single machine's resources to exhaust those of another machine, in order to prevent it from functioning normally. Large Web servers are usually robust enough to withstand a basic DoS attack from a single machine without suffering performance loss. A DoS attack famous variant is the DDoS or Distributed Denial of Service attack where the attack originates from multiple computers simultaneously, therefore causing the victim's resources exhaustion.

DNS Amplification Attack

DNS amplification attack is a sophisticated denial of service attack that takes advantage of DNS servers' behavior in order to amplify the attack. In order to launch a DNS amplification attack, the attacker performs two malicious tasks. First, the attacker spoofs the IP address of the DNS resolver and replaces it with the victim's IP address. This will cause all DNS replies from the DNS servers to be sent to the victim's servers. Second, the attacker finds an internet domain that is registered with many DNS records. During the attack, the attacker sends DNS queries that request the entire list of DNS records for that domain. This results in large replies from the DNS servers, usually so big that they need to be split over several packets. Using very few computers, the attacker sends a high rate of short DNS queries to the multiple DNS servers asking for the entire list of DNS records for the internet domain it chose earlier. The DNS servers look for the answer and provide it to the DNS resolver. However, because the

attacker spoofed the IP address of the DNS resolver and set it to be the IP address of the victim, all the DNS replies from the servers are sent to the victim. The attacker achieves an amplification effect because for each short DNS query it sends, the DNS servers reply with a larger response, sometimes up to 100 times larger. Therefore, if the attacker generates 3 Mbps of DNS queries, it is actually amplified to 300Mbps of attack traffic on the victim. The victim is bombed with a high rate of large DNS replies where each reply is split over several packets. This requires the victim to reassemble the packet, which is a resource consuming task, and to attend to all of the attack traffic. Soon enough, the victim's servers become so busy handling the attack traffic that they cannot service any other request from legitimate users and the attacker achieves a denial-of-service.

DNS Flood

A DNS Flood is an application-specific variant of a UDP flood. Since DNS servers use UDP traffic for name resolution, sending a massive number of DNS requests to a DNS server can consume its resources, resulting in a significantly slower response time for legitimate DNS requests.

Exploit

An exploit is an implementation of a vulnerability meant to allow one to actually compromise a target. Exploits can be difficult to develop, as most modern vulnerabilities are much more complex than older ones due to the existence of advanced security measures and complicated constructs in modern hardware and software. Exploits based on previously unknown vulnerabilities, known as "Zero-Day" exploits are highly sought after by hackers and developers and manufacturers alike. By using a zero-day exploit, a hacker can guarantee that his or her attempt to break into a particular computer or device that possesses such vulnerability that the exploit is based on will succeed. Zero-day exploits are traded on both the black market and through legitimate middlemen between legitimate parties from anywhere between $5,000 to $250,000 depending on the effects of the exploit and which system they target. Where a PDF exploit might only fetch a few thousand dollars, a severe exploit targeting the latest version of Apple's mobile operating system, iOS, might fetch $100,000 or more.

Flood

"Flood" is the generic term for a denial-of-service (DoS) attack in which the attacker attempts to constantly send traffic (often high volume of traffic) to a target server in an attempt to prevent legitimate users from accessing it by consuming its resources. Types of floods include (but are not limited to): HTTP floods, ICMP floods, SYN floods, and UDP floods.

Hacker

The term "hacker" has been used to mean various things in the world of computing: one who is able to subvert computer security (regardless of intentions), one who is a member of the open-source software community and subculture, and one who attempts to push the limits of computer software and hardware through home modifications. In the world of computer

security, the term “hacker” is often portrayed as negative by mass media, despite the prevalence of “white hat hacking”, or ethical hacking for the purpose of discovering potential security flaws and reporting them to the proper individuals or organizations so that the flaws may be patched. Black hat hacking, on the other hand, is the breaking into computer systems without any intention of reporting discovered vulnerabilities, often with malicious or financial incentives. The hackers who fall somewhere on the spectrum between “white hats” and “black hats” are referred to as “grey hats”. Grey hat hackers will often perform mischievous activities with (usually non-malicious although at times questionably ethical) motivations. Additionally, grey hat hackers often choose not to report security flaws to the proper channels; rather, they report such information to the hacking community and the general public, enjoy watching the fallout as those with the security flaws scramble to fix them before they can be abused by black hat hackers. Within the open-source software and computer hobbyist communities, however, “hacker” usually has a less negative connotation. Within these cultures, hackers are often individuals regarded as intelligent and clever, and able to come up with creative solutions to existing problems that a software or hardware product developer may have not thought of or publicly released yet. These hackers often refer to “hackers” within the computer security world as “crackers” (as in safe-cracker) to emphasize their belief that calling such individuals “hackers” is incorrect. With the rise of hacker and “hacktivist" groups such as LulzSec (now LulzSec Reborn) and Anonymous, the mass media portrayal of the term “hacker” continues to lead the general public to believe “hacker” is synonymous with “cybercriminal”.

Hacktivist

“Hacktivist”, a portmanteau of “hack” and “activism”, was a term coined in 1996 by Omega, a member of the hacking coalition “Cult of the Dead Crow” (cDc). The term can be loosely defined as, “the ethically ambiguous use of computers and computer networks in order to affect the normal operation of other systems, motivated by a desire to protest or promote political ends.”Oftentimes these events take the form of web site defacements, denial-of-service attacks, information theft, web site parodies, virtual sit-ins, typo squatting, and virtual sabotage. The term has become popular among media outlets in recent years due to the rise of various politically motivated cyber attacks by groups such as Anonymous and LulzSec (now LulzSec Reborn) on governments and corporations across the world.

Honeypot

In computer security, a honeypot is a program or a server voluntarily made vulnerable in order to attract and lure hackers. The attackers who think they are targeting a real resource behave “normally”, using their attack techniques and tools against this lure site, which allow the defenders to observe and monitor their activities, analyze their attacking methods, learn and prepare the adequate defenses for the real resources. There are several kinds of honeypots, some used for research purposes only while others are actively acting as defenses for the real sites.

HTTP Flood

An HTTP flood is an attack method used by hackers to attack web servers and applications. It consists of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a target web server. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service condition (without necessarily requiring a high rate of network traffic). Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP flood attacks may be one of the most advanced non-vulnerability threats facing web servers today. It is very hard for network security devices to distinguish between legitimate HTTP traffic and malicious HTTP traffic, and if not handled correctly, it could cause a high number of false-positive detections. Rate-based detection engines are also not successful at detecting HTTP flood attacks, as the traffic volume of HTTP floods may be under detection thresholds. Because of this, it is necessary to use several parameters detection including rate-based and rate-invariant.

I2P

I2P is an anonymous overlay network - a network within a network. It is intended to protect communication from dragnet surveillance and monitoring by third parties such as ISPs.

ICMP Flood

Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood - the sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) - can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

Internet pipe saturation

These attacks are volumetric floods and often involve flooding the target with an overwhelming bandwidth. Common attacks utilize UDP as it is easily spoofed and difficult to mitigate downstream. Out of state, SYN floods and malformed packets are also often seen. While many attacks aim at saturating inbound bandwidth, it's not uncommon for attackers to identify and pull large files from websites, ftp shares, etc. in order to saturate outbound bandwidth as well.

IP Address

An IP address is an identifier for a device connected to a network using TCP/IP - a protocol that routes network traffic based on the IP address of its destination. IP addresses can either be 32-bit IPv4 addresses consisting of four base-10 numbers separated by periods representing eight digit binary (base-2) numbers called "octets" (i.e. 0.0.0.0 to 255.255.255.255), or 128-bit IPv6 addresses consisting of eight hexadecimal (base-16) numbers separated by colons representing sixteen digit binary (base-2) numbers (i.e. 0000:0000:0000:0000:0000:0000:0000:0000 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF where consecutive groups of four zeroes are replaced by a double colon). When the Internet first became popular, IPv4, with its 32-bit

addresses, offered 232, or roughly 4.3 x 109 unique addresses. As the number of Internet-connected devices began to grow significantly, people worried that the IPv4 protocol would not contain enough addresses to meet the growing demand for new unique addresses this is why IPv4 will eventually be replaced by IPv6 on a large scale (IPv6 already officially launched in August 2012), which contains 2128 or roughly 3.4 x 1038 unique addresses. The Dynamic Host Configuration Protocol (DHCP), which runs on special devices (usually routers) allows for the assigning of IP addresses within a local area network (LAN). DHCP assigns IP addresses on a temporary "lease" basis; once a device's IP address lease expires, a DHCP server will assign it a new (potentially different) one. IP addresses automatically assigned by a DHCP server are therefore referred to as "dynamic IP addresses", as a device with a DHCP-assigned IP address may eventually receive an IP different from its original one.

DHCP servers will not assign devices just any IP address in the maximum range of IPv4 addresses (0.0.0.0 to 255.255.255.255), as certain IP addresses are reserved for special purposes. Such addresses include:

- 0.0.0.0 – Represents the "default" network, i.e. any connection
  255.255.255.255 – Represents the broadcast address, or place to route messages to be sent to every device within a network
- 127.0.0.1 – Represents "localhost" or the "loopback address", allowing a device to refer to itself, regardless of what network it is connected to
- 169.254.X.X – Represents a "self-assigned IP address", which a device will assign itself if it is unable to receive an IP address from a DHCP server

Users' DHCP-assigned IP addresses on a LAN are not the same as their "external" or Internet IP address. This address will be the same for all users connected to a DHCP server, which itself receives an IP address from the Internet Service Provider (ISP) it is connected to. As IP addresses can be used as unique identifiers for users' machines (and subsequently the users themselves), knowledge of a malicious user's external Internet IP address can allow law enforcement officials to block, locate, and eventually arrest him or her. As a result, the more advanced attack tools and hackers will employ anonymization techniques - such as the use of proxy servers, VPNs, or a routing network like Tor or I2P - that can make it seem like they are using a different IP address other than their own, located somewhere else in the world. An attack tool called Low Orbit Ion Cannon (LOIC) became infamous for not hiding its users' IP addresses; this resulted in the arrest of various LOIC users around the world for their participation in distributed denial-of-service (DDoS) attacks.

IP Spoofing

IP Spoofing is the act of creating an IP packet with a forged source IP address for the purpose of hiding the true source IP address, usually for the purpose of launching special types of distributed denial-of-service (DDoS attacks). By forging the source IP address of a packet; the individual sending it can direct the target IP address' machine to send its reply packet somewhere other than the real IP address of the source machine. Those wishing to launch

DDoS attacks without large botnets can therefore send packets with random spoofed source IP addresses in order to both conceal their own identity and make the attack harder to block (as it looks like it is originating from many sources).

IRC (Internet Relay Chat)

IRC (Internet Relay Chat) is a protocol for real-time text messaging between internet-connected computers created in 1988. It is mainly used for group discussion in chat rooms called “channels” although it supports private messages between two users, data transfer, and various server-side and client-side commands. As of April 2011, the top 100 IRC networks served over 500,000 users at a time on hundreds of thousands of channels. IRC is a popular method used by botnet owners to send commands to the individual computers in their botnet. This is done either on a specific channel, on a public IRC network, or on a separate IRC server. The IRC server containing the channel(s) that are used to control bots is referred to as a “command and control” or C2 server.

ISP (Internet Service Provider)

An Internet Service Provider (ISP) is a company that provides internet access for its customers. ISPs are required by law in many countries to provide a certain level of monitoring capabilities to aid government law enforcement and intelligence agencies, and are often asked by such officials to intervene during cyber attacks by cutting off internet service to the offending machines.

itsoknoproblembro

The 'itsoknoproblembro' tool was designed and implemented as a general purpose PHP script injected into a victim’s machine allowing the attacker to upload and execute arbitrary Perl scripts on the target’s machine. The 'itsoknoproblembro' script injects an encrypted payload, in order to bypass IPS and Malware gateways into the website main file index.php, allowing the attacker to upload new Perl scripts at any time. Initial server infection is usually done by using the well known Remote File Inclusion (RFI) technique. By uploading Perl scripts that run different DOS flood vectors, the server might act as a Bot in a DDOS Botnet army. Although originally designed for general purpose, some variants of this tool found in the wild were customized to act as a proprietary DDOS tool, implementing the flood vector logics inside without the need to upload additional scripts.

Malware

“Malware”, short for “malicious software”, is any program designed to help a hacker negatively affect the normal operation of a computer. Most forms of malware - including viruses, worms, Trojan horses, spyware, adware, and rootkits - are intended to allow hackers to gain unauthorized access to a machine, without the knowledge of its owner, in order to perform criminal tasks including information theft and amassing botnets to perform distributed denial-of-service (DDoS) attacks. Computer users are often tricked into installing malware through social engineering techniques, or are unaware that a seemingly non-

malware infected program they have installed was infected, containing additional code designed to stealthily perform malicious tasks.

MSSP

An MSSP (Managed Security Service Provider) is an organization which provides "Security as a Service" (Sec-aaS) and may include elaborate operations such as SOCs and NOCs, or something as simple as a cloud-based key management service. Generally speaking, an MSSP is considered an outsourced operation of what was an internal security device or process management function.

Network scan

Scanning is typically an automated process that is used to discover devices such as pc, server and peripherals that exist on a network. Results can include details of the discovered devices, including IP addresses, device names, operating systems, running applications/services, open shares, usernames and groups. Scanning is often related to pre -attack or reconnaissance activities. There are two types of scanning: Horizontal Scan in which the scanner scans for the same port on multiple IPs, and Vertical Scan in which the scanner scans multiple ports on one IP.

Packet

A packet is a formatted unit of data used to transmit information piece by piece across a packet switched network. Packets usually contain three sections: a header, the payload, and a trailer (also called “footer”). A packet header contains information such as the length of the packet (if the network does not use a predetermined fixed packet size), synchronization bits to help the packet match up with the network, a packet number to differentiate each packet from the others, the protocol (i.e. type of information contained within the packet), and the source and destination IP addresses. The “payload” of a packet contains the actual information being transmitted. The trailer or “footer” usually contains a series of bits signaling to the receiving device that it has reached the end of the packet, as well as some type of error-checking information to ensure that the packet was not modified in transit.

Port Scan

A port scanner is a technical leverage to identify available technical services (ports) on a server or application and may include logic to evaluate whether or not those services are vulnerable to common exploits or configuration issues. This is done by sending predetermined traffic to the target and based on a response or lack of a response, the port scanner in use makes its own conclusions with regards to the functionality of the port being scanned.

Reflector/Reflective DoS attacks

Reflection Denial of Service attacks makes use of a potentially legitimate third party component to send the attack traffic to a victim, ultimately hiding the attackers’ own identity. The attackers send packets to the reflector servers with a source IP address set to their victim’s IP therefore indirectly overwhelming the victim with the response packets.

The reflector servers used for this purpose could be ordinary servers not obviously compromised, which makes this kind of attack particularly difficult to mitigate. A common example for this type of attack is Reflective DNS Response attack.

SIP Brute Force

SIP brute force is an adaptation of normal brute force attacks which attack SIP servers and attempt access to servers to make unauthorized outbound calls at another's expense.

SIP Client Call Flood

This is a flood technique focused on SIP application protocol which involves illegitimate call requests. The idea here is to flood the Session Boarder Control (SBC) and / or SIP / VOIP PBX with too many requests to handle and thus making the service unavailable.

SIP Malformed Attack

Application layer attack on the Session Initiation Protocol- SIP in use in VoIP services, targeted at causing denial of service to SIP servers. A SIP malformed attack consists of sending any kind of non-standard messages (malformed SIP Invite for ex) with an intentionally invalid input, therefore making the system unstable.

SIP Register flood

Application layer attack on the Session Initiation Protocol- SIP in use in VoIP services, targeted at causing denial of service to SIP servers. A SIP Register flood consists of sending a high volume of SIP REGISTER or INVITE packets to SIP servers (indifferently accepting endpoint requests as first step of an authentication process), therefore exhausting their bandwidth and resource

SIP Server Flood

Application layer attack on the Session Initiation Protocol- SIP (in use in VoIP services), targeted denial of service to SIP servers. Common attack vectors include SIP invite and register floods.

Scrubbing Center

A centralized data cleansing station where traffic is analyzed and malicious traffic (ddos, known vulnerabilities and exploits) is removed. Scrubbing centers are often used in large enterprises, such as ISP and Cloud providers, as they often prefer to off-ramp traffic to an out of path centralized data cleansing station. When under attack, the traffic is redirected (typically using DNS or BGP) to the scrubbing center where an attack mitigation system mitigates the attack traffic and passes clean traffic back to the network for delivery. The scrubbing center should be equipped to sustain high volumetric floods at the network and application layers, low and slow attacks, RFC Compliance checks, known vulnerabilities and zero day anomalies.

Social Engineering

Social Engineering (within the context of computer security) is the act of using psychological manipulation in order to gain access to sensitive information, computers, or computer networks. Many famous computer hackers (both white hat and black hat) have used social

engineering in combination with computer-related methods in order to gain information; reformed cyber criminal Kevin Mitnick admitted that it's much easier to trick a person into giving up sensitive passwords or information than it is to obtain the same material solely through the use of computers. One example of a social engineering technique is "pretexting", or engaging the target subject in a specific manner with some form of background information that makes it more likely that he or she will divulge sensitive information. Pretexting often involves extensive research, as the social engineer will need to prepare answers to identifying questions that he or she may be asked during the process of obtaining information. This newly obtained information can often be used in further pretexting attempts, especially in scenarios where the social engineer wishes to gain even greater access to his or her target.

SQL Injection

SQL injection is an attack targeting web applications taking advantage of poor application coding where the inputs are not sanitized therefore exposing application vulnerabilities. SQL injection is the most famous type of injection attacks which also count LDAP or XML injections. The idea behind a sql injection is to modify an application SQL (database language) query in order to access or modify unauthorized data or run malicious programs. Most web applications indeed rely on databases where the application data is stored and being accessed by SQL queries and modifications of these queries could mean taking control of the application. An attacker would for example be able to access the application database with administrator access, run remote commands on the server, drop or create objects in the database and more.

For instance, the sql query below, aiming at authenticating users, is common in web applications:

- myQuery= "SELECT * FROM userstable WHERE username = 'userinput1' and password ='userinput2';"
- Replacing userinput1 by: 'OR 1=1'); -- would result in granting the attacker access to the database without knowing the real username and password as the assertion "1=1" is always true and the rest of the query is being ignored by the comment character (- - in our case).
- Replacing the userinput1 by ' OR 1=1"); drop table users;-- would additionally drop the application users table.

SYN Flood

A SYN flood is a denial-of-service (DoS) attack that relies on abusing the standard way that a TCP connection is established. Typically, a client sends a SYN packet to an open port on a server asking for a TCP connection. The server then acknowledges the connection by sending SYN-ACK packet back to the client and populating the client's information in its Transmission Control Block (TCB) table. The client then responds to the server with an ACK packet establishing the connection. This process is commonly known as a "three-way handshake". A

SYN flood overwhelms a target machine by sending thousands of connection requests to it using spoofed IP addresses. This causes the target machine to attempt to open a connection for each malicious request and subsequently wait for an ACK packet that never arrives. A server under a SYN flood attack will continue to wait for a SYN-ACK packet for each connection request, as the delay could be normal and related to network congestion. However, because a SYN-ACK packet never arrives for any of the connection requests; the massive number of half-open connections quickly fills up the server's TCB table before it can time any connections out. This process continues for as long as the flood attack continues. Attackers will sometimes add legitimate information to their requests as well, such as sequence number or source port 0, as this increases a target server's CPU usage on top of causing network congestion, and could more effectively cause a denial-of-service condition.

TCP Flood

TCP SYN floods are one of the oldest yet still very popular Denial of Service (DoS) attacks. The most common attack involves sending numerous SYN packets to the victim. The attack in many cases will spoof the SRC IP meaning that the reply (SYN+ACK packet) will not come back to it. The intention of this attack is overwhelm the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall which also has to process and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP; this is perhaps the biggest strength of the attack.

Tor

Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.

UDP Flood

A UDP flood is a network flood and still one of the most common floods today. The attacker sends UDP packets, typically large ones, to single destination or to random ports. In most cases the attackers spoof the SRC IP which is easy to do since the UDP protocol is "connectionless" and does not have any type of handshake mechanism or session. The main intention of a UDP flood is to saturate the Internet pipe. Another impact of this attack is on the network and security elements on the way to the target server, and most typically the firewalls. Firewalls open a state for each UDP packet and will be overwhelmed by the UDP flood connections very fast.

Vulnerability

A vulnerability (in computer security) is any weakness in a computer system, network, software, or any device that allows one to circumvent security measures and perform actions not intended by its developers or manufacturers. Vulnerabilities range from minor to major, with the most significant allowing for privilege escalation (unauthorized administrator or root privileges) or code execution (the running of unsigned 3rd party software). New vulnerabilities can often be discovered by the process of "fuzzing", or purposely trying to break something by attempting to give it unreasonable input values. Once some kind of crash occurs and can be analyzed, one can discover the existence of a vulnerability that may have not been previously documented. Previously unknown vulnerabilities, known as "Zero-Day" vulnerabilities are highly sought after by hackers and developers and manufacturers alike. By using an exploit based on zero-day vulnerability, a hacker can guarantee that his or her attempt to break into a particular computer or device that possesses such vulnerability will succeed. Zero-day exploits are traded on both the black market and through legitimate middlemen between parties for anywhere from $5,000 to $250,000 depending on the effects of the exploit and which system they target. Where a PDF exploit might only fetch a few thousand dollars, a severe exploit targeting the latest version of Apple's mobile operating system, iOS, might fetch $100,000 or more.

Vulnerability Scanner

A vulnerability scanner is a type of computer program used to gather information on computers and systems on a network in order to find their weaknesses. By using a vulnerability scanner tool such as nmap or unicornscan, one can determine the number of clients attached to a particular network as well as various information regarding their addresses, ports, applications and services and potential exploits that can be used against them. Some scanners offer the ability to deploy payloads for the purpose of using a found exploit, and others simply display information on network topology. Types of vulnerability scanners include: port scanners, network enumerators, network vulnerability scanners, web application security scanners, database security scanners, ERP security scanners, and computer worms (which require scanning capabilities to spread within a network).

Wireshark

Wireshark is a free cross-platform open-source network traffic capture and analysis utility. It began as a project called "Ethereal" in the late 1990s, but its name was changed to "Wireshark" in 2006 due to trademark issues. The initial code was written by Gerald Combs, a computer science graduate of the University of Missouri-Kansas City, today the Wireshark website now lists over 600 contributors. The program is GUI-based and uses pcap to capture packets, although there is also a command-line version of Wireshark called TShark with the same functionality. Wireshark essentially "understands" the formats of various types of network packets, and is able to display the header and content information of captured packets in an easy-to-read format with various filtering options. Packets can be either captured directly with Wireshark, or captured with a separate utility and later viewed within

Wireshark. As a powerful (and free) network analysis tool, Wireshark has become an industry standard utility for network traffic analysis.

Zeus

Zeus is a well-known Trojan Horse that steals financial information from a user's browser using man-in-the-browser key logging and form grabbing. Additionally, Zeus installs a backdoor on the machines it infects, so these machines can become part of a botnet used for distributed denial-of-service (DDoS) attacks and other malicious activities. Zeus was first detected in 2007 when it was used to attack the United States Department of Transportation, however, it did not become significantly widespread until March 2009. Attacks involving the use of Zeus occurred throughout 2010, including an October 2010 attack by a large organized crime ring attempting to steal over $70M from individuals in the US with Zeus-infected computers. The FBI made over 90 arrests of suspected members in the US, and various others were arrested in the UK and Ukraine in connection with the attack. In May 2011 the source code of the version used then of Zeus (v2) was leaked, leading to various customized Zeus-based bots being created. Some of the more advanced custom bots based on the leaked code (such as Ice IX) attempted to fix many of the existing issues with Zeus rendering it even harder to detect. However, many security researchers have discovered that even the most well-known custom versions are extremely similar to the original leaked Zeus source code, and are therefore not significantly more innovative or dangerous.

Zero-Day/Zero-Minute Attack

A Zero-Day (or Zero-Minute) Attack is a type of attack that uses a previously unknown vulnerability. Because the attack is occurring before "Day 1" of the vulnerability being publicly known, it is said that the attack occurred on "Day 0" - hence the name. Zero-Day exploits are highly sought after - often bought and sold by private firms anywhere from $5,000 to $250,000, depending on what applications and operating systems they target - as they almost guarantee that an attacker is able to stealthily circumvent the security measures of his or her target. Private security firms aside, software vendors will also usually offer a monetary reward among other incentives to report zero-day vulnerabilities in their own software directly to them.

Zombie

A "zombie" or "bot" is a compromised computer under the control of an attacker who often controls many other compromised machines that together make up a botnet. The term "zombie" was coined to describe such an infected computer because the computer's owner is often not aware that his or her computer is being used for malicious activities.

References

http://security.radware.com/knowledge-center/DDoSPedia/

Your Global e-Security Partner

info@glesec.com

United States

Worldwide Corporate HQ
Address. 66 Witherspoon Street
Princeton, NJ 08542
Tel. 609.651.4246

Panama

Central America HQ
Address. Edificio Century Tower
El Dorado, 1th Floor D-12
Panama City, Panama
Tel. +507.836.5355

Argentina

South America HQ
+54.11.5917.6120

Brazil

+55.11.3711.5699

Chile

+56.2938.1496

Peru

+51.1708.7197

Mexico

+52.55.5018.1164