



MONTHLY OPERATIONS & INTELLIGENCE REPORT

TECHNICAL REPORT

Institute of Electrical and Electronics Engineers

March 2018

Tel: +1 609-651-4246

Tel: +507-836-5355

Info@glesec.com

www.glesec.com

CONFIDENTIAL

Table of Contents

Table of Contents.....	2
About This Report	3
Confidentiality	3
Managed Vulnerability Service	4
Vulnerabilities found in the Institute of Electricals and Electronics Engineers by severity	6
Managed Breach Attack Simulation Service	16
Summary.....	16
Mail Attack Summary	17
Mail Attack Mitigation Summary	20
Mail Risk Analysis per Type	21
Recommendations	28
Appendix A	30

CONFIDENTIAL



About This Report

This is a for the MSS-BAS service.

Confidentiality

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

- Client name and contact information
- System architecture, configuration, access methods and access control
- Security content

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

CONFIDENTIAL



Managed Vulnerability Service (MSS-VM)

The Managed Vulnerability Service (MSS-VM) enables organizations to minimize the risk of vulnerabilities by quickly discovering weaknesses, measuring the potential risk and exposure, reporting, providing remediation information necessary to mitigate those risks on an on-going basis and facilitating reporting and compliance with regulations and best practices.

In the address range given by the Institute of Electrical and Electronics Engineers, we have found a total of 23 hosts, of which 12 are vulnerable. These vulnerabilities are divided in the following severities as shown in the following table. Additionally you can notice the Risk Value score of your organization according to our metrics.

Total IP's Scanned		IP's Vulnerable		
23		12		
Risk Distribution				
Critical	High	Medium	Low	Total
18	22	28	0	68

According to the metrics:

RV= 0.372122762

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

All the vulnerabilities found in your organization belong to the following categories:

Category	Critical	High	Medium	Low	Total
Web Servers	11	0	17	1	29
CGI abuses	9	11	2	0	22
General	0	0	17	0	17
FTP	0	1	5	0	6
Misc.	0	0	1	5	6

- Web Servers
- CGI Abuses
- General
- FTP
- Misc

Additional details about these vulnerabilities are presented in the Vulnerabilities

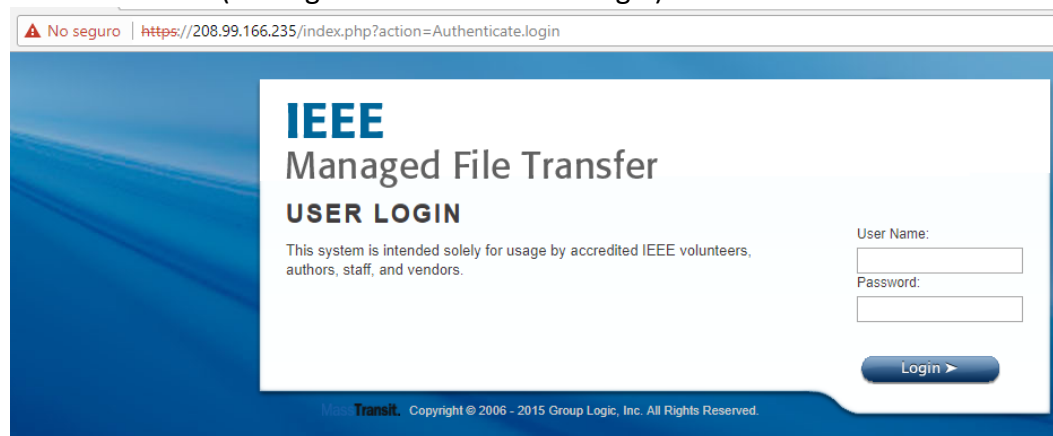
CONFIDENTIAL



found in the Institute of Electricals and Electronics Engineers by severity section of the MSS-VM on page 6.

Our analysts consider that for your organization these are the top 5 most vulnerable hosts:

200.99.166.235 (Managed File Transfer user login)

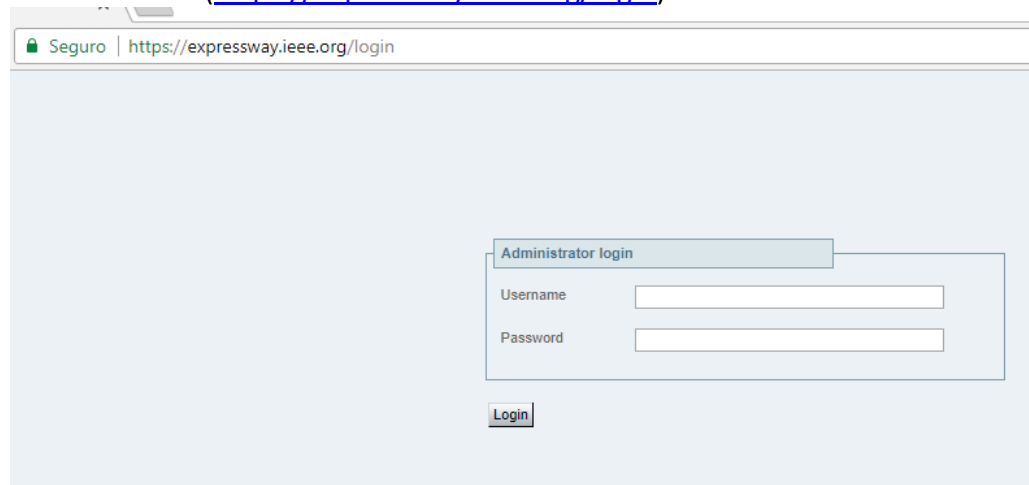


140.98.196.80 (ftp4.computer.org this page presents certificate errors and answers through HTTP)

140.98.202.40

140.98.200.215 (masstransit.ieee.org, redirects to the Managed File Transfer user login)

140.98.200.22 (<https://expressway.ieee.org/login>)



If the mentioned IP must be accessible from the internet, it is necessary to improve the existing security measures. The ip address 200.99.165.235 has PHP versions that

CONFIDENTIAL

are no longer supported. The ip address 140.98.200.22 presents an administrative login page, we consider that this webpage should not be reached from the internet and we recommend removing the external access from this page.

Vulnerabilities found in the Institute of Electricals and Electronics Engineers by severity

The following section will describe in detail each vulnerability found according to their severity.

Critical Risk Level Vulnerabilities

All the vulnerabilities in this level require a PHP update and are categorized as CGI abuses.

Microsoft IIS 6.0 Unsupported Version Detection

Description

According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of Microsoft IIS that is currently supported.

Affected Systems

Port	Hosts
80 / tcp/www	140.98.194.52, 140.98.194.53, 140.98.194.55, 140.98.194.56, 140.98.194.59, 140.98.194.61, 140.98.194.62, 140.98.194.63, 140.98.194.64, 140.98.194.160, 140.98.194.161

Microsoft Windows Server 2003 Unsupported Installation Detection

Description

The remote host is running Microsoft Windows Server 2003

Solution

CONFIDENTIAL



Upgrade to a version of Windows that is currently supported.

Note: Support for this operating system by Microsoft ended July 14th, 2015. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

Affected Systems

Port	Hosts
n/a	140.98.194.52 140.98.194.53, 140.98.194.55, 140.98.194.56, 140.98.194.59, 140.98.194.61, 140.98.194.62, 140.98.194.63, 140.98.194.64, 140.98.194.160, 140.98.194.161

PHP 5.5.x < 5.5.24 Multiple Vulnerabilities

Description

According to its banner, the version of PHP 5.5.x running on the remote web server is prior to 5.5.24. It is, therefore, affected by multiple vulnerabilities:

1. An unspecified use-after-free error exists in the `_zend_shared_memdup()` function within file `ext/opcache/zend_shared_alloc.c` that allows an unauthenticated, remote attacker to have an unspecified impact.
2. A NULL pointer dereference flaw exists in the `build_tablename()` function within file `pgsql.c` in the PostgreSQL extension due to a failure to validate token extraction for table names. An authenticated, remote attacker can exploit this, via a crafted name, to cause a denial of service condition.
3. An out-of-bounds read error exists in the Phar component due to improper validation of user-supplied input when handling phar parsing during `unserialize()` function calls. An unauthenticated, remote attacker can exploit this to cause a denial of service condition or the disclosure of memory contents.
4. A memory corruption issue exists in the `phar_parse_metadata()` function in file `ext/phar/phar.c` due to improper validation of user-supplied input when parsing a specially crafted TAR archive. An unauthenticated, remote attacker can exploit this to cause a denial of



service condition or the execution of arbitrary code.

5. Multiple stack-based buffer overflow conditions exist in the `phar_set_inode()` function in file `phar_internal.h` when handling archive files, such as tar, zip, or phar files. An unauthenticated, remote attacker can exploit these to cause a denial of service condition or the execution of arbitrary code.

6. A flaw exists in the Apache2handler SAPI component when handling pipelined HTTP requests that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code.

7. A flaw exists in multiple functions due to a failure to check for NULL byte (`%00`) sequences in a path when processing or reading a file. An unauthenticated, remote attacker can exploit this, via specially crafted input to an application calling those functions, to bypass intended restrictions and disclose potentially sensitive information.

8. A type confusion error exists in multiple functions within file `ext/soap/soap.c` that is triggered when calling `unserialize()`. An unauthenticated, remote attacker can exploit this to disclose memory contents, cause a denial of service condition, or execute arbitrary code.

9. Multiple type confusion errors exist within files `ext/soap/php_encoding.c`, `ext/soap/php_http.c`, and `ext/soap/soap.c` that allow an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code.

10. A type confusion error exists in the `__PHP_Incomplete_Class()` function within file `ext/standard/incomplete_class.c` that allows an unauthenticated, remote attacker to cause a denial of service condition or the execution of arbitrary code.

11. A type confusion error exists in the `exception::getTraceAsString()` function within file `Zend/zend_exceptions.c` that allows a remote attacker to execute arbitrary code.



12. A denial of service vulnerability exists due to a flaw in the bundled libmagic library, specifically in the `mget()` function within file `softmagic.c`. The function fails to maintain a certain pointer relationship. An unauthenticated, remote attacker can exploit this, via a crafted string, to crash the application.

13. A denial of service vulnerability exists due to a flaw in the bundled libmagic library, specifically in the `mcopy()` function within file `softmagic.c`. The function fails to properly handle an offset that exceeds 'bytecnt'. An unauthenticated, remote attacker can exploit this, via a crafted string, to crash the application.

14. A flaw exists in the `ZEND_VM_HELPER_EX()` function within file `/Zend/zend_vm_def.h` when handling a `__get()` function call. An unauthenticated, remote attacker can exploit this to cause a denial of service condition.

45. A type confusion error exists in the `php_stream_url_wrap_http_ex()` function within file `ext/standard/http_fopen_wrapper.c` that allows an unauthenticated, remote attacker to execute arbitrary code.

16. A use-after-free error exists in the `php_curl()` function within file `ext/curl/interface.c` that allows an unauthenticated, remote attacker to execute arbitrary code.

Solution

Upgrade to PHP version 5.5.x.or later.

Output

Version source : X-Powered-By: PHP/5.5.16

Installed version : 5.5.16

Fixed version : 5.5.24

Affected Systems

443 / tcp / www 208.99.166.235

All the vulnerabilities in this level require a PHP update and are categorized as CGI

CONFIDENTIAL



abuses.

High Risk Level Vulnerability

All the vulnerabilities in this level require a PHP update and are categorized as CGI abuses and some of them are also affecting FTP servers. These vulnerabilities are affecting the same system as the critical vulnerabilities; refer to that section for details on the affected system.

FTP Privileged Port Bounce Scan

Description

It is possible to force the remote FTP server to connect to third parties using the PORT command.

The problem allows intruders to use your network resources to scan other hosts, making them think the attack comes from your network.

Solution

See the CERT advisory in the references for solutions and workarounds.

Affected Systems

Port	Hosts
21 and 990/ tcp / ftp	140.98.196.80

Medium Risk Level Vulnerability

All the vulnerabilities in this level require a PHP update and are categorized as CGI abuses; there are also weaknesses in SSL cipher suite and in the FTP server.

HTTP TRACE / TRACK Methods Allowed

Description

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.

Solution

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

Affected Systems

Port	Hosts
------	-------

CONFIDENTIAL



80 / tcp / http_proxy 140.98.202.41, 140.98.194.3, 140.98.194.119,
140.98.202.53, 140.98.202.41, 140.98.193.157, 140.98.202.89, 140.98.202.49

SSL Medium Strength Cipher Suites Supported

Description

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.

Solution

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

Affected Systems

Port	Hosts
443 / tcp / http_proxy	140.98.194.156, 140.98.196.190, 140.98.200.35, 140.98.200.36, 140.98.200.85, 140.98.200.181, 208.99.166.235
21 / tcp	140.98.194.110
5061 / tcp / sip	140.98.200.22

F5 BIG-IP Cookie Remote Information Disclosure

Description

The remote host seems to be an F5 BIG-IP load balancer. The load balancer encodes the IP address of the real web server by which it acts on behalf of a cookie. In addition, the information after 'BIGipServer' is configured by the user and can be the logical name of the device. These values may disclose confidential information, such as internal IP addresses and names.

Affected Systems

443 / tcp / www 140.98.202.89, 140.98.202.45, 140.98.202.117, 140.98.202.48
140.98.202.102, 140.98.202.116
80 / tcp / www 140.98.202.40 140.98.202.53

SSL Certificate Signed Using Weak Hashing Algorithm

Description

CONFIDENTIAL



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.

Output

The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

| -Subject : C=US/ST= /L= /O=IEEE/OU= /CN= /E=
| -Signature Algorithm : SHA-1 With RSA Encryption
| -Valid From : Jun 03 15:54:10 2017 GMT
| -Valid To : Jun 03 15:54:10 2018 GMT

Affected Systems

21 / tcp 140.98.194.110

Output

The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

| -Subject : C=US/ST=New
Jersey/L=Piscataway/O=IEEE/OU=IT/CN=xploreqa.ieee.org
| -Signature Algorithm : SHA-1 With RSA Encryption
| -Valid From : Jun 10 20:27:41 2009 GMT
| -Valid To : Jun 08 20:27:41 2019 GMT

Affected Systems

443 / tcp 140.98.202.16

Output

The following certificates were part of the certificate chain sent by the remote host, but contain hashes that are considered to be weak.

| -Subject : C=US/ST=New
Jersey/L=Piscataway/O=IEEE/OU=IT/CN=xploreuat.ieee.org
| -Signature Algorithm : SHA-1 With RSA Encryption
| -Valid From : Jan 12 19:18:58 2010 GMT
| -Valid To : Jan 10 19:18:58 2020 GMT

Affected Systems

443 / tcp / http_proxy140.98.202.40

Solution

Contact the Certificate Authority to have the certificate reissued.

Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure**Description**

The remote host is affected by an information disclosure vulnerability. The SSL/TLS service supports RSA key exchanges, and incorrectly leaks whether or not the RSA key exchange sent by a client was correctly formatted. This information can allow an attacker to decrypt previous SSL/TLS sessions or impersonate the server.

Solution

Upgrade to a patched version of the software. Alternatively, disable RSA key exchanges.

Affected Systems

443 / tcp / www 208.99.166.247, 208.99.166.235

Note that this plugin does not attempt to recover an RSA ciphertext, however it sends a number of correct and malformed RSA ciphertexts as part of an SSL handshake and observes how the server responds. This plugin attempts to discover the vulnerability in multiple ways, by not completing the handshake and by completing it incorrectly, as well as using a variety of cipher suites. Only the first method that finds the service to be vulnerable is reported.

Serv-U < 14.0.2.0 FTP Server SSL Renegotiation DoS**Description**

According to its banner, the installed version of Serv-U is earlier than 14.0.2.0 and is, therefore, potentially affected by a denial of service vulnerability. A remote attacker could cause denial of service conditions by continually sending SSL renegotiation requests to the application.

Solution

Upgrade to Serv-U version 14.0.2.0 or later.



Affected Systems

990 and 21 / tcp / ftp 140.98.196.80

Serv-U FTP Server < 15.0.0.0 Multiple Security Vulnerabilities**Description**

According to its banner, the installed version of Serv-U is a version prior to version 15.0.0.0. It is, therefore, potentially affected by multiple vulnerabilities:

1. An unspecified error exists related to SSL that can be exploited to cause a denial of service.
2. An unspecified error exists when using the 'Require Fully Qualified Membership' LDAP login settings.

Solution

Upgrade to Serv-U version 15.0.0.0 or later.

Affected Systems

990 and 21 / tcp / ftp 140.98.196.80

Apache Server ETag Header Information Disclosure**Description**

The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files.

Solution

Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information.

Affected Systems

443 / tcp / www 140.98.202.49

SSH Weak Algorithms Supported**Description**

CONFIDENTIAL



GLESEC has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution

Consult product documentation to remove the weak ciphers.

Affected Systems

21 / tcp / ssh 140.98.200.215

Low Risk Level Vulnerability

The vulnerabilities in this category are weaknesses in SSH servers.

SSH Server CBC Mode Ciphers Enabled**Description**

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.

Solution

Consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption.

Affected Systems

21 / tcp / ssh 140.98.200.215, 140.98.196.80, 140.98.200.22

Web Server Load Balancer Detection**Description**

The remote web server seems to be running in conjunction with several others behind a load balancer. Knowing that there are multiple systems behind a service could be useful to an attacker as the underlying hosts may be running different operating systems, patchlevels, etc.

Solution

Update the web configuration to hide information disclosure.

Affected Systems

443 / tcp / www 140.98.193.235



Managed Breach Attack Simulation Service (MSS-BAS)

The Managed Breach Attack Simulation Service (MSS-BAS) is a collection of advanced pre-exploitation, post-exploitation and awareness testing services. The testing is on real targets based on simulated attacks; therefore these provide conclusive (no false positive) results. The different attack vectors test the organization's configurations, countermeasures, implementations and ability to respond in a continuous fashion producing valuable intelligence and recommendations.

Summary

The MSS-BAS e-mail Vector enables organizations to know different metrics that are used to measure and know your e-mail security position: an "e-mail Security Exposure Level", a "Risk Score" and types and severity of the malware that you are exposed to, via the e-mail attack vector.

The e-mail Security Exposure Level can be "Low", "Medium" and "High" and it is based in the "Risk Score" which is a percentage. The Risk Score is a Key Parameter Indicator, KPI, and it is used as an indicator of an increase/decrease from report to report, of how is the "overall" security in your organization. In this case related to the e-mail attack vector

The Risk Score is calculated based on different parameters like the number of e-mails containing malicious software that are able to penetrate your security and other factors that are taken into consideration based on the type of malware and the "risk" for that malware. For instance for Ransomware, the Risk is calculated evaluating also parameters like number of "double clicks" needed to open the malicious file sent to the organization and the impact for your organization, of this type of malware if it is able to penetrate your security. The "Risk" for each malware is also classified as High Probability, Medium Probability and Low Probability depending in the type and probability of occurrence. For instance, Ransomware has a very high impact to the organization, but there is Low, Medium y High probability Ransomware, depending of the probability of occurrence.

The "**e-mail Security Exposure Level**" for your company this month was classified as "Low" based on the "Risk Score" of 22%. The "**web gateway Security Exposure**



Level” (Browser) for your company this month was classified as “High” based on the “Risk Score” of 40%.

In the **email simulation** 69% of the different file types, holding a malicious payload within, were able to penetrate your security measures (see “Top 10 Penetrated File Types). This is something that should be of concern to the organization because this means that, as right now, you do not have a proper set of security measures in place that are blocking or dropping any e-mails, containing the type of malware that we used in this simulation.

In the **Browser simulation** 99% of the different file types, holding a malicious payload within, were able to penetrate your security measures (see “Top 10 Penetrated File Types). This is a situation of high relevance to the organization because this means that, as right now, the current Secure Web Gateway, has no measures or rules that detect and drop or filter the payloads and URL used in this simulation.

A very important detail that can be observed in the Assessment Result (see below in the Mail Risk Analysis per Type Section) is that the highest percentage penetration for the **email vector** this month comes from exploits at 31%. These exploits are present in outdated versions of Microsoft Office and present in Windows itself. This Medium risk factor indicates that your organization is very vulnerable via e-mail to these types of attacks. Exploits vector can be mitigated by keeping all the software up to date with the latest hotfixes. After these threats enter the network they can be executed in many different ways causing high impact to the organization.

In the Assessment Result (see below in the Mail Risk Analysis per Type Section) is that the highest percentage penetration for the **Browser vector** this month comes from exploits at 100%, it is also worth mentioning that there are two additional high penetration rate simulations, Files (98%) and Policy (56%).

Mail Attack Summary

Within the set of threats that can penetrate via email, exists a high percentage of penetration in critical threats mainly Exploits, followed by Ransomware. For our analysts the Risk Score for your organization is of level Medium. It has to be clear that only the e-mail vector was used for this proof of concept, but the proof of concept for this vector is based on real threats (you can see the description in



Appendix A). All vectors, in a continuous cycle have to be considered to give an idea of the security state of all you infrastructure.

Risk conditions based in test MSS-BAS e-mail vector. March 2018

E-mail Security Exposure Level: Medium

Risk Score



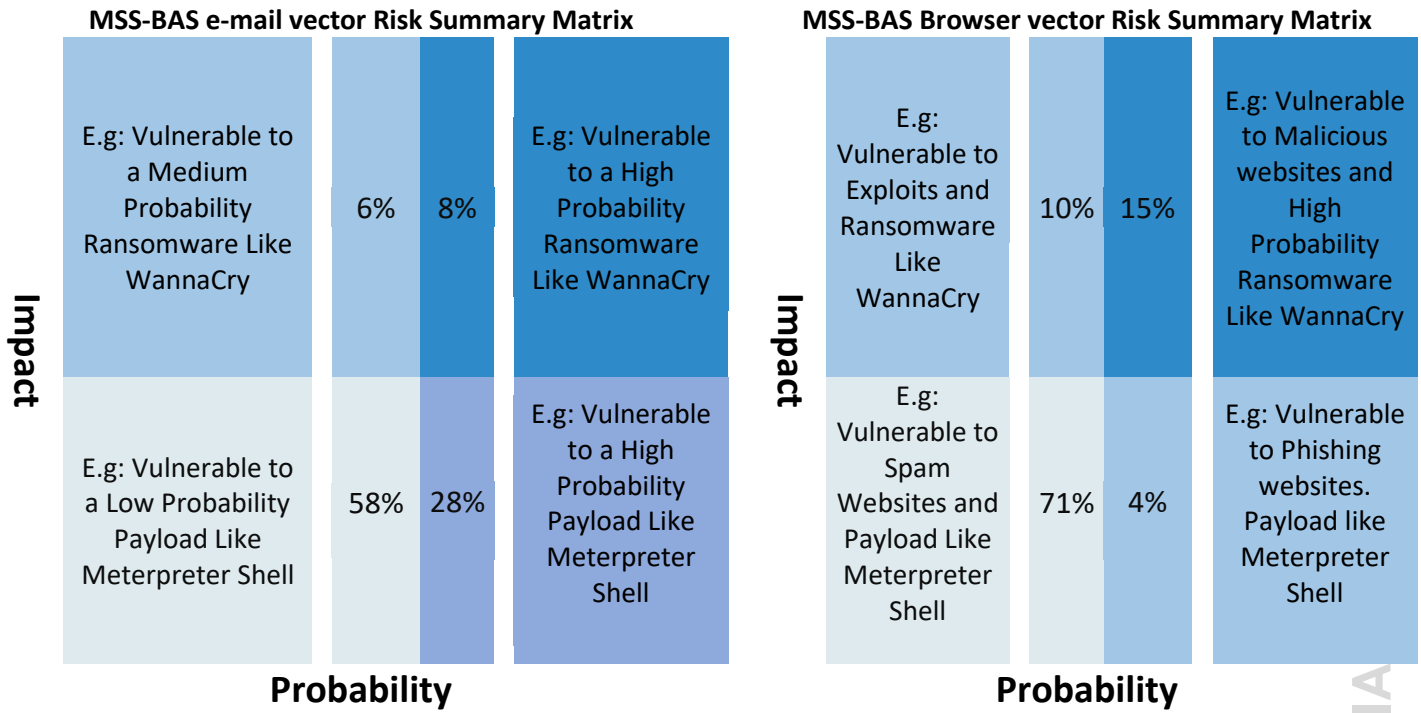
Email Simulation Summary: 1139/4127

Browser Simulation Summary: 3332/4970

<u>Risk Level</u>	<u>Sent</u>	<u>Penetrated</u>	<u>Risk Level</u>	<u>Sent</u>	<u>Penetrated</u>
High	550	57	High	1014	505
Medium	1222	230	Medium	474	466
Low	2375	401	Low	3482	2361

CONFIDENTIAL





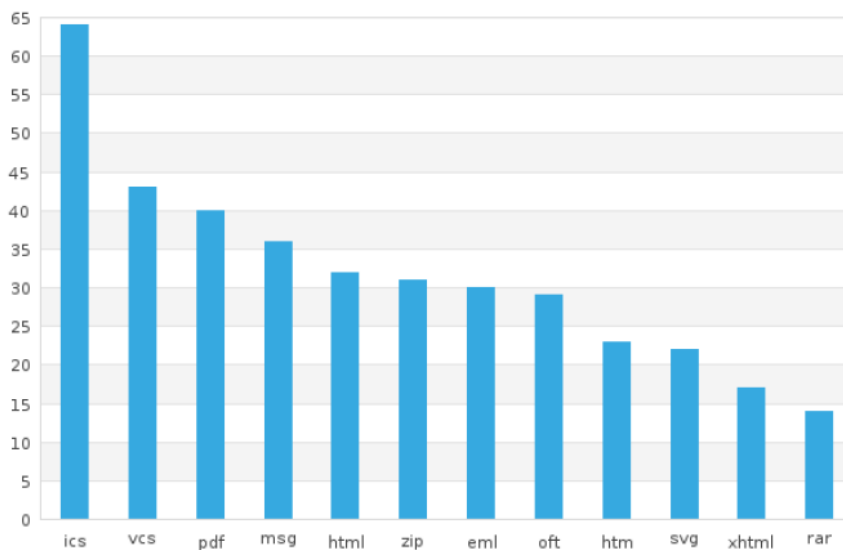
In Appendix A you can find a description on each malware used for the simulation, the similarity to the real ones, the attack vectors and mitigation techniques for each one.

CONFIDENTIAL

Mail Attack Mitigation Summary

Below is the 10 Top of Files Types that were able to penetrate your security with malware.

Top 10 Penetrated file types



Mail Relay, Content disarm and reconstruction or sandbox solutions:

For ics files it will solve 11% of the flaws

For pdf files it will solve 8% of the flaws

For vcs files it will solve 7% of the flaws

For msg files it will solve 7% of the flaws

For eml files it will solve 6% of the flaws

For zip files it will solve 6% of the flaws

For oft files it will solve 5% of the flaws

For html files it will solve 5% of the flaws

For svg files it will solve 4% of the flaws

For htm files it will solve 4% of the flaws

For xhtml files it will solve 3% of the flaws

Refer to the appendix A to find more details in mitigation techniques for each file type.

CONFIDENTIAL

Mail Risk Analysis per Type

Assessment Result for Email Simulation:

23%**Dummy**

Dummy category is code execution proof of concept without actual damage to the system.

31%**Exploit**

Known and signed exploits of commonly used software that leads to code execution because of vulnerabilities discovered.

28%**Payload**

Common attacks delivered to clients like: Data extraction attacks or Stagers downloading the real malware.

17%**Links**

A malicious website is a site that attempts to install malware onto your device.

11%**Worm**

Software using Common techniques in order to spread itself inside a Windows based network.

17%**Ransomware**

Software encrypting user files and denies access until ransom is paid.

10%**Malware**

Malware, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

Assessment Result for Web Gateway Simulation:

17%**Ransomware**

Software encrypting user files and denies access until ransom is paid.

5%**Phishing**

The activity of defrauding an online account holder of financial information by posing as a legitimate company.

0%**C&C**

Command and control servers (C&C servers) are computers that issue commands to members of a botnet.

98%**Files**

Downloadable Malicious Files such as: Exploits, Malwares, Ransomwares, Payloads, Worms.

100%**Exploits**

An exploit kit is a software kit designed to run on web servers, with the purpose of identifying software vulnerabilities.

56%**Policy**

Using categories for URL filtering is the quickest and easiest way to block access to productivity-sapping or harmful websites and avoid potential HR issues.

CONFIDENTIAL



High Risk

Here are the findings with high risk that penetrated your organization:

Malware with 33 Payloads in high risk.

Ransomware with 15 Payloads in high risk.

Worm with 9 Payloads in high risk.

505 of the files used in the web gateway vector that penetrated successfully are of high risk.

Medium Risk

Here are the findings with medium risk that penetrated your organization:

Links with 127 Payloads in Medium risk.

Payload with 34 Payloads in Medium risk.

Exploit with 30 Payloads in Medium risk.

Malware with 18 Payloads in Medium risk.

Ransomware with 13 Payloads in Medium risk

Worm with 8 Payloads in Medium risk.

453 of the files used in the web gateway vector that penetrated successfully are of medium risk.

Summary by type/risk (see graph below)

759 Links sent and 127 penetrated your organization:

127 of the links are in Medium Risk

464 Payload sent and 130 penetrated your organization

33 of the files are in Low Risk

8 of the files are in Medium Risk

9 of the files are in High Risk

465 Worm sent and 50 penetrated your organization:

33 of the files are in Low Risk

8 of the files are in Medium Risk

9 of the files are in High Risk

474 Ransomware sent and 80 penetrated your organization:

52 of the files are in Low Risk

13 of the files are in Medium Risk

15 of the files are in High Risk

CONFIDENTIAL



1270 Malware sent and 125 penetrated your organization:

74 of the files are in Low Risk

18 of the files are in Medium Risk

33 of the files are in High Risk

580 Dummy sent and 137 penetrated your organization:

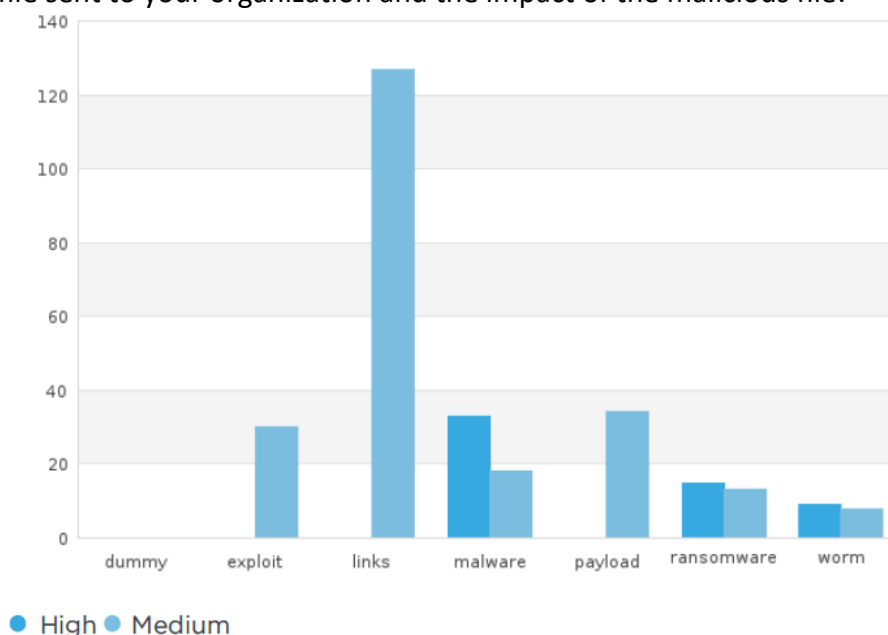
134 of the files are in Low Risk

135 Exploit sent and 42 penetrated your organization:

12 of the files are in Low Risk

30 of the files are in Medium Risk

Risk: the risk level is evaluated by the number of click needed to open the malicious file sent to your organization and the impact of the malicious file.



Successful High level simulated attacks

15 out of 57 High risk files able to penetrate the perimeter were Ransomware. This specific type of ransomware was categorized as a high risk, because the number of clicks required to execute it are considerably low.

Malicious code can be hidden within different other file types so that it is not recognized and stopped by regular security countermeasures. The malicious

CONFIDENTIAL

Ransomware was hidden within 21 different file types:

- HTM: An HTM file is an HTML web page used by web browsers. It contains markup code that is stored in a plain text format and is used to display and format text and images in a web browser.
- JSE: Script written in JScript, a programming language used for Windows and Microsoft Internet Explorer scripting; contains source code in a format similar to JavaScript.
- ACCDB: An ACCDB file is a database created with Microsoft Access 2007 or later. It typically contains data organized into tables and fields.
- MDB: An MDB file is a database file created by Microsoft Access. It contains the database structure (tables and fields) and database entries (table rows).
- ICS: this extension refers to calendar application files, most common apps that use this type of files are: Microsoft Outlook, IBM Lotus Notes, Apple Calendar, Yahoo! Calendar, among others.
- XLS: An XLS file is a spreadsheet file created by Microsoft Excel. An XLS spreadsheet may contain one or more worksheets, which store and display data in a table format.
- XLM: Contains macros used for automating processes in Microsoft Excel.
- DOTM: A DOTM file is a document template created by Microsoft Word. It contains the default layout, settings, and macros for a document.
- PDF: A PDF file is a multi-platform document created PDF application. The PDF format is commonly used for saving documents and publications in a standard format that can be viewed on multiple platforms.
- XLAM: File used by Microsoft Excel, contains a macro-enabled add-in, which provides extra functionality and tools that may execute macros.
- XLSM: An XLSM file is a macro-enabled spreadsheet created by Microsoft Excel. It contains worksheets of cells arranged by rows and columns as well as embedded macros programmed in the VBA language.
- VCS: Contains information about an event or appointment, saved in the vCalendar format; includes the event date and time and other information about the event.
- XLK: Backup file created by Microsoft Excel; contains a backup copy of an .XLS file.
- XLT: An XLT file is a template created by Microsoft Excel. It contains default formatting and data for a spreadsheet and is used as a basis for creating new .XLS files.
- HTML: This is the standard web page file type on the internet. The content of

this type of files is accessible through any web browser.

- XLTM: Template file created by Microsoft Excel, contains default settings and layout properties for a macro-enabled spreadsheet; used to create a new macro-Enabled workbook .XLSM file.
 - 7z: A 7Z file is a compressed archive created with Igor Pavlov's 7-Zip file compression utility.
 - EML: An EML file is an email message saved by Microsoft Outlook or other e-mail programs. It may also contain an e-mail attachment, which is a file sent with the message.
 - XLL: A special type of file similar to the DLL libraries but exclusively used by Excel.
 - SVG: An SVG file is a graphics file that uses a two-dimensional vector graphic format. It describes images using a text format that is based on XML.
 - EXE: An EXE file contains an executable program for Windows. Also, is one of the most common extensions for hiding malware.
-
- Malware: 33 files that await remote commands from a command and control server.
 - Worms: 9 files disguised as Office Macros that attempt to spread through the network to infect other computers.

Even though all the other tested threats: Payload, Worms, Links, Malware, Exploits and Dummy were able to penetrate the perimeter, we consider Ransomware alone as the highest risk due to its probability of occurrence and possible negative impact. Please refer to the recommendations number 2 and 3 below.

Successful Medium level simulated attacks

Email vector: 230 files within this severity indicator were able to penetrate the perimeter and they can be broken down into 3 different categories:

- Ransomware: 13 files were able to penetrate the perimeter at this level as well, what this means is that using different combinations for containing this malicious code were successful in entering the network. These types are considered medium risk because they require more clicks to be executed, as contained in more different types of files. The ones that were able to access

your network were:

- ICS-VCS-XLK
- XHTML-ICS-MDB
- LHA-PDF-ACCDB
- ARJ-PDF-ACCDB
- RAR-PDF-ACCDB
- ZIP-ICS-XLL
- GZ-PDF-ACCDB
- VCS-ICS-XLM
- LZH-PDF-ACCDB
- MSG-VCS-XLT
- CAB-PDF-ACCDB
- TAR-PDF-ACCDB
- 7z-EML-PDF-ACCDB

This ransomware has the same impact to your Organization if executed as a “High risk” ransomware, but it is little less accessible. Please refer to the recommendations section, items number 2 and 3.

- Exploit: 30 files targeting five different vulnerabilities. The first one aims to instigate a stack overflow attack MSCOMCTL.OCX, this attack targets Microsoft Office 2007 and 2010. The second vulnerability refers to a flaw in email gateways that allow an external agent to bypass them by inserting Object linking and embedding in a PowerShell environment. The third vulnerability used, makes uses of Microsoft Word macro to gain access to a power shell command line. The fourth vulnerability allow remote code execution in older Firefox versions (50.0.1 or lower). The fifth vulnerability uses an undocumented feature in Microsoft Word that allows malicious attackers to collect information about the OS and software versions remotely. Please refer to the recommendations section, item number 1.



- Worms: 8 files that are run automatically by the Office Macro scans ports and infects other computers in the network.
- Links: 127 payloads that redirect to webpages that host malware attempting to download it to the victim's computer.
- Payloads: 34 infected files that periodically take screenshots of the user's desktop and attempts to read input from the user.

The other types of attacks sent by this simulation were blocked by your Organization security countermeasures.

Successful Low level simulated attacks

411 out of 2357 low risk malicious codes were able to access your network. These types of files are considered of low risk because (a) they require many clicks to execute or (b) even if they were executed they don't cause a high impact. By securing the network against higher severity criteria mentioned before in this report, it is likely that the amount of low risk malware that penetrated is also reduced.

CONFIDENTIAL



Recommendations

Despite the growing investment in cyber security, sophisticated attackers still manage to bypass even the most advanced security systems, including next-generation, non-signature based security. The reason is that advanced threats are coded to look like legitimate behavior. Therefore, they are extremely difficult to identify using conventional systems and can proceed unimpeded within the target networks.

This simulation showed that various attacks may compromise your local network.

1. This month, some e-mails containing malicious files that use exploits for Microsoft Office Suite 2007 and 2010, WinRAR, Firefox 50.0.1, among others were allowed through, as was reported last month. Also, at the Gateway level a number of exploits that affect Adobe Flash Player, Internet Explorer and Firefox under Windows and Linux were able to bypass it. Old versions of software are vulnerable to many exploits which can be hidden within files that should be allowed because they are of regular usage. It is important to keep the software updated with the latest patches to prevent attackers from using these exploits, this process can be done manually or automated using an endpoint manager to check and enforce compliance policies.
2. Although there were some ransomware classified as “Medium Risk” or “Low Risk” their impact to the organization is the same as a “High Risk” Ransomware and should not be dismissed. The lower risk level comes from the fact that these ransomware are contained in several other file types and require a lot more “double-clicks” to actually open the malicious code.
3. This month, in the Web Gateway vector simulation detected a large number of URL that were able to bypass the Gateway; also, the majority of files sent in the simulation were able to penetrate the Gateway. If the issues at the Gateway are corrected, it is possible that this also lowers the risk level in the email vector.
4. Specific recommendations:
 - a. See Appendix A for details for each of the simulated attacks
 - b. Configure a Mail-Relay rule to block the penetration vector exterior file type.



- c. Anti-Virus definition update might be required.
- d. Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- e. Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

CONFIDENTIAL



Appendix A

From the total amount of samples sent, our analysts team classified 62 of the samples as High Risk level and are presented in the Appendix.

Email samples used:

Emails Command And Control Malware Risk Level: High

Description

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

UAC Nagger Trojan Malware Risk Level: High

Description

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.

CONFIDENTIAL



Emails Command And Control Malware Risk Level: High**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Credentials Nagger Trojan Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Credentials Nagger Trojan Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .html with file size that is larger than 10k.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: High**Description**

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High

CONFIDENTIAL



Description

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: High**Description**

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers,

Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .htm files larger than 10k
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are

able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .htm files larger than 10k

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

CONFIDENTIAL



- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.

Credentials Nagger Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High

CONFIDENTIAL



Description

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: High**Description**

worm is scanning ports and using the current user primary token to infect other

computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Emails Command And Control Malware Risk Level: High**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Emails Command And Control Malware Risk Level: High**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.

- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: High**Description**

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.



- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .htm files larger than 10k

Ransomware Risk Level: High**Description**

CONFIDENTIAL



ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High

Description

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .html files larger than 10k

UAC Nagger Trojan Malware Risk Level: High

Description

malware attacking the user interface and forcing him to click Yes when UAC Prompts

CONFIDENTIAL



for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.

Emails Command And Control Malware Risk Level: High

Description

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics files larger than 10k

Worm Risk Level: High

Description

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro

automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .html files larger than 10k

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

CONFIDENTIAL



Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .eml files larger than 10k

Credentials Nagger Trojan Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .eml files larger than 10k

Credentials Nagger Trojan Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented

- in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
 - Contact the Security Product Vendor in-order to solve the security flaw.
 - Configure Group Policy to block Office Macros from running.
 - Block .ics files larger than 10k

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .eml files larger than 10k

Worm Risk Level: High**Description**

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented

- in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
 - Contact the Security Product Vendor in-order to solve the security flaw.
 - Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs files larger than 10k

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: High**Description**

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Credentials Nagger Trojan Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.
- Block .html with file size that is larger than 10k.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Credentials Nagger Malware Risk Level: High**Description**

Cymulate malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan Malware Risk Level: High**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs files larger than 10k.

Credentials Nagger Trojan Malware Risk Level: High**Description**

malware attacking user and forcing him to enter username and password. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics files larger than 10k.

Ransomware Risk Level: High

CONFIDENTIAL



Description

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .eml files larger than 10k.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs files larger than 10k.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .htm files larger than 10k

Ransomware Risk Level: High

CONFIDENTIAL



Description

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics files larger than 10k

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: High

CONFIDENTIAL



Description

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: High**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics files larger than 10k.

Ransomware Risk Level: High**Description**

CONFIDENTIAL



ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .svg files larger than 10k.

Worm Risk Level: High

Description

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics files larger than 10k.

UAC Nagger Trojan Malware Risk Level: High

Description

CONFIDENTIAL



malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.

Ransomware Risk Level: High

Description

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs files larger than 10k.

Emails Command And Control Malware Risk Level: High

Description

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or

files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Here are presented the 15 exploit kits used to test the Web Gateway:

adobe_flash_domain_memory_uaf.swf Risk Level: High

Description: This module exploits a use-after-free vulnerability in Adobe Flash Player. The vulnerability occurs when the ByteArray assigned to the current ApplicationDomain is freed from an ActionScript worker, when forcing a reallocation by copying more contents than the original capacity, but Flash forgets to update the domainMemory pointer, leading to a use-after-free situation when the main worker references the domain Memory again. This module has been tested successfully on Windows 7 SP1 (32-bit), IE 8 and IE11 with Flash 17.0.0.134.

adobe_flash_casi32_int_overflow.swf Risk Level: High

Description: Integer overflow in Adobe Flash Player. The vulnerability occurs in the casi32 method, where an integer overflow occurs if a ByteArray of length 0 is setup as domainMemory for the current application domain. This module has been tested successfully on Windows 7 SP1 (32-bit), IE 8 to IE 11 and Flash 15.0.0.167.

adobe_flash_copy_pixels_to_byte_array.swf Risk Level: High

Description: This module exploits an integer overflow in Adobe Flash Player. The vulnerability occurs in the copyPixelsToByteArray method from the BitmapData object. The position field of the destination ByteArray can be used to cause an integer overflow and write contents out of the ByteArray buffer. This module has been tested successfully on: * Windows 7 SP1 (32-bit), IE 8 to IE 11 and Flash 14.0.0.176, 14.0.0.145, and 14.0.0.125. * Windows 7 SP1(32-bit), Firefox 38.0.5 and Adobe Flash 14.0.0.179. *Windows 8.1, Firefox 38.0.5 and Adobe Flash 14.0.0.179.

adobe_flash_hacking_team_uaf.swf Risk Level: High

Description: This module exploits a use-after-free vulnerability in Adobe Flash Player. The vulnerability occurs when the ByteArray assigned to the current ApplicationDomain is freed from an ActionScript worker, when forcing a reallocation by copying more contents than the original capacity, but Flash forgets to update the domainMemory pointer, leading to a use-after-free situation when the main worker references the domainMemory again. This module has been tested successfully on Windows 7 SP1 (32-bit), IE8 and IE11 with Flash 17.0.0.134.

adobe_flash_nellymoser_bof.swf Risk Level: High

Description: This module exploits a buffer overflow on Adobe Flash Player when handling nellymoser encoded audio inside a FLV video, as exploited in the wild on June 2015. This module has been tested successfully on: Windows 7 SP1 (32-bit), IE11 and Adobe Flash 18.0.0.160, Windows 7 SP1(32-bit), Firefox 38.0.5 and Adobe Flash 18.0.0.160, Windows 8.1, Firefox 38.0.5 and Adobe Flash 18.0.0.160, Linux Mint 'Rebecca' (32 bits), Firefox 33.0 and Adobe Flash 11.2.202.466, and Ubuntu 14.04.2 LTS, Firefox 35.01, and Adobe Flash 11.2.202.466. Note that this exploit is effective against both CVE-2015-3113 and the earlier CVE-2015-3043, since CVE-2015-3113 is effectively a regression to the same root cause as CVE-2015-3043.

adobe_flash_net_connection_confusion.swf Risk Level: High

Description: This module exploits a type confusion vulnerability in the NetConnection class on Adobe Flash Player. When using a correct memory layout this vulnerability allows to corrupt arbitrary memory. It can be used to overwrite dangerous objects, like vectors, and ultimately accomplish remote code execution. This module has been tested successfully on: * Windows 7 SP1 (32-bit), IE 8, IE11 and Adobe Flash 16.0.0.305. * Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 16.0.0.305. * Windows 8.1, Firefox 38.0.5 and Adobe Flash 16.0.0.305. * LinuxMint 'Rebecca' (32 bits), Firefox 33.0 and Adobe Flash 11.2.202.424. * Ubuntu 14.04.2 LTS, Firefox 33.0 and Adobe Flash 11.2.202.442.

adobe_flash_pixel_bender_bof.swf Risk Level: High

Description: This module exploits a buffer overflow vulnerability in Adobe Flash Player. The vulnerability occurs in the flash.Display.Shader class, when setting specially crafted data as its bytecode, as exploited in the wild in April 2014. This module has been tested successfully on the following operating systems and Flash

versions: Windows 7 SP1, IE 8 to IE 11 with Flash 13.0.0.182, Windows 7 SP1, Firefox 38.0.5, Flash 11.7.700.275 and Adobe Flash 13.0.0.182, Windows 8.1, Firefox 38.0.5 and Adobe Flash 13.0.0.182, Linux Mint 'Rebecca' (32 bit), Firefox 33.0 and Adobe Flash 11.2.202.350.

adobe_flash_shader_job_overflow.swf Risk Level: High

Description: This module exploits a buffer overflow vulnerability related to the ShaderJob workings on Adobe Flash Player. The vulnerability happens when trying to apply a Shader setting up the same Bitmap object as src and destination of the ShaderJob. Modifying the width' attribute of the ShaderJob after starting the job it's possible to create a buffer overflow condition where the size of the destination buffer and the length of the copy are controlled. This module has been tested successfully on: Windows 7 SP1(32-bit), IE11 and Adobe Flash 17.0.0.169, Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 17.0.0.169, Windows 8.1, Firefox 38.0.5 and Adobe Flash 17.0.0.169, and Linux Mint 'Rebecca' (32 bits), Firefox 33.0 and Adobe Flash 11.2.202.457.

adobe_flash_uncompress_zlib_uaf.swf Risk Level: High

Description: This module exploits a use after free vulnerability in Adobe Flash Player. The vulnerability occurs in the ByteArray::UncompressViaZlibVariant method, when trying to uncompress() a malformed byte stream. This module has been tested successfully on: * Windows 7 SP1 (32 bits), IE 8 to IE 11 and Flash 16.0.0.287, 16.0.0.257 and 16.0.0.235. * Windows 7 SP1 (32-bit), Firefox 38.0.5 and Adobe Flash 16.0.0.287. * Windows 8.1, Firefox 38.0.5 and Adobe Flash 16.0.0.305. * Linux Mint 'Rebecca' (32 bits), Firefox 33.0 and Flash 11.2.202.424.

adobe_flash_uncompress_zlib_uninitialized.swf Risk Level: High

Description: This module exploits an uninitialized memory vulnerability in Adobe Flash Player. The vulnerability occurs in the ByteArray::UncompressViaZlibVariant method, which fails to initialize allocated memory. When using a correct memory layout this vulnerability leads to a ByteArray object corruption, which can be abused to access and corrupt memory. This module has been tested successfully on Windows 7 SP1 (32-bit), IE 8 and IE11 with Flash 15.0.0.189.

adobe_flash_worker_byte_array_uaf.swf Risk Level: High

Description: This module exploits a use-after-free vulnerability in Adobe Flash Player. The vulnerability occurs when the ByteArray assigned to the current ApplicationDomain is freed from an ActionScript worker, which can fill the memory

and notify the main thread to corrupt the new contents. This module has been tested successfully on Windows 7 SP1 (32-bit), IE 8 to IE 11 and Flash 16.0.0.296.

firefox_svg_plugin.swf Risk Level: High

Description: This exploit gains remote code execution on Firefox 17 and 17.0.1, provided the user has installed Flash. No memory corruption is used. First, a Flash object is cloned into the anonymous content of the SVG 'use' element in the (CVE-2013-0758). From there, the Flash object can navigate a child frame to a URL in the chrome:// scheme. Then a separate exploit (CVE-2013-0757) is used to bypass the security wrapper around the child frame's window reference and inject code into the chrome:// context. Once we have injection into the chrome execution context, we can write the payload to disk, chmod it (if posix), and then execute. Note: Flash is used here to trigger the exploit but any Firefox plugin with script access should be able to trigger it.

ms14_064_ole_code_execution.html Risk Level: High

Description: This module exploits the Windows OLE Automation array vulnerability, CVE-2014-6332. The vulnerability is known to affect Internet Explorer 3.0 until version 11 within Windows 95 up to Windows 10, and no patch for Windows XP. However, this exploit will only target Windows XP and Windows 7 box due to the Powershell limitation. Windows XP by defaults supports VBS, therefore it is used as the attack vector. On other newer Windows systems, the exploit will try using Powershell instead.

Out of all samples sent, our analysts team classified 68 worth mentioning Medium Risk samples and are presented in this Appendix.

Ransomware Risk Level: Medium**Description**

ransomware encrypts all files in the user Documents folder. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block



by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Ransomware Risk Level: Medium

Description

ransomware encrypts all files in the user Documents folder. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

MS Word Comctlbof Exploit Risk Level: Medium

Description

This file exploits a stack buffer overflow in MSCOMCTL.OCX. It uses a malicious RTF to embed the specially crafted MSComctlLib.ListViewCtrl.2 Control as exploited in the wild on April 2012. This module targets Office 2007 and Office 2010 targets. The DEP/ASLR bypass on Office 2010 is done with the Ikazuchi ROP chain proposed by Aabysssec. This chain uses "msgr3en.dll", which will load after office got load, so the malicious file must be loaded through "File / Open" to achieve exploitation. Shellcode: Dummy MessageBox.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Anti-Virus definition update might be required.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.

- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload Payload Risk Level: Medium**Description**

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Ransomware Risk Level: Medium**Description**

ransomware encrypts all files in the user Documents folder.

New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Worm Risk Level: Medium**Description**

worm is scanning ports and using the current user primary token to infect other

computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Worm Risk Level: Medium**Description**

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically runs the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware Risk Level: Medium**Description**

ransomware encrypts all files in the user Documents folder.
New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,EMails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

MS Word comctlbof Exploit: Medium**Description**

This file exploits a stack buffer overflow in MSCOMCTL.OCX. It uses a malicious RTF to embed the specially crafted MSComctlLib.ListViewCtrl.2 Control as exploited in the wild on April 2012. This module targets Office 2007 and Office 2010 targets. The DEP/ASLR bypass on Office 2010 is done with the Ikazuchi ROP chain proposed by Abysssec. This chain uses "msgr3en.dll", which will load after office got load, so the malicious file must be loaded through "File / Open" to achieve exploitation. Shellcode: Dummy MessageBox

Mitigation

CONFIDENTIAL



- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Anti-Virus definition update might be required.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Waveform Audio File Format: Medium

Description

This file exploits a buffer overflow in APDF WAV to MP3 v1.0.0. When the application is used to import a specially crafted m3u file, a buffer overflow occurs allowing arbitrary code execution. Shellcode: Dummy MessageBox

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Anti-Virus definition update might be required.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

- Block .ics with file size that is larger than 10k.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,EMails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,EMails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .vcs with file size that is larger than 10k.

Standard Payload: Medium

CONFIDENTIAL



Description

Payload is a malicious file retrieving computer Usernames, E-Mails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .vcs with file size that is larger than 10k.

Emails Command And Control: Medium**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

CONFIDENTIAL



Description

Payload is a malicious file retrieving computer Usernames,EMails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,EMails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Emails Command And Control: Medium**Description**

CONFIDENTIAL



Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or

Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Emails Command And Control: Medium**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan: Medium**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .eml with file size that is larger than 10k.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

CONFIDENTIAL



- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs with file size that is larger than 10k.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

CONFIDENTIAL



- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.



- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .vcs with file size that is larger than 10k.

Emails Command And Control: Medium**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types

and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Emails Command And Control: Medium**Description**

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file

hidden inside the penetration vector file types.

- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.

Emails Command And Control: Medium

Description

Cnc is a malware listening to general commands from a command and control server. Command Examples: Usernames, E-Mails, Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan: Medium

Description

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.

- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .eml with file size that is larger than 10k.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs with file size that is larger than 10k.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block

by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the

penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file

hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file

hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file

hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file

hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file

hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.

- Configure Group Policy to block Office Macros from running.
- Block .ics with file size that is larger than 10k.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics with file size that is larger than 10k.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames,Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the



penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics with file size that is larger than 10k.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types. Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics with file size that is larger than 10k.

Worm: Medium

Description

worm is scanning ports and using the current user primary token to infect other computers in the network. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.

CONFIDENTIAL



- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium**Description**

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.

- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

UAC Nagger Trojan: Medium

Description

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication.

When the user clicks Yes, he's elevated permissions token is stolen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Block .eml with file size that is larger than 10k.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block



by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics with file size that is larger than 10k.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.

- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .ics with file size that is larger than 10k.

UAC Nagger Trojan: Medium**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

UAC Nagger Trojan: Medium**Description**

malware attacking the user interface and forcing him to click Yes when UAC Prompts for authentication. When the user clicks Yes, he's elevated permissions token is stolen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.
The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file

type.

- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Standard Payload: Medium

Description

Payload is a malicious file retrieving computer Usernames, Emails and takes a Printscreen. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer.

The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.
- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.

Ransomware: Medium

Description

ransomware encrypts all files in the user Documents folder. New malicious files or files that were Packed by Packers, Crypters or Protectors are able to run on this computer. The Office Macro automatically running the malicious file.

Mitigation

- Configure a Mail-Relay rule to block the penetration vector exterior file type.
- Configure the sandbox to run and test the penetration vector file types and block by detecting malicious behavior of files hidden inside files as presented in the penetration vector.

REPORT FOR:

Institute of Electrical and Electronics Engineers

- Applying File Content disarm and reconstruction to remove the Code Execution file hidden inside the penetration vector file types.
- Contact the Security Product Vendor in-order to solve the security flaw.
- Configure Group Policy to block Office Macros from running.
- Block .vcs with file size that is larger than 10k.

CONFIDENTIAL





USA-ARGENTINA-PANAMA
México-Perú-Brasil- Chile

Tel: +1 609-651-4246
Tel: +507-836-5355

Info@glesec.com
www.glesec.com