MONTHLY OPERATIONS & INTELLIGENCE REPORT

TECHNICAL REPORT

Institute of Electrical and Electronics Engineers

April 2018

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

Info@glesec.com
www.glesec.com

Table of Contents

About This Report

This report is a companion to the Monthly Operations & Intelligence Executive Report. The purpose of this document is to provide Technical and Tactical level information, detail and recommendations to the extent that can be summarized. GLESEC processes significant amount of data and not all can be presented in a detail report format. For more information you can review the dashboards of the GMP or if necessary contact us at the GLESEC Operation Centers (GOC).

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.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

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 4 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				4
Risk Distribution				
Critical	**High**	**Medium**	**Low**	**Total**
0	0	4	0	4

According to the metrics:

RV= 0.086956522

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

In general, Institute of Electrical and Electronics Engineers vulnerabilities in this period have been medium; It was discovered that 4 of the 23 hosts analyzed have at least one problem of vulnerability, 4 at medium risk, .the vulnerabilities found this month by name are: Return Of Bleichenbacher's Oracle Threat (ROBOT) Information disclosure (208.99.166.235, 208.99.166.247,208.99.166.251),followedSSL Certificate Cannot Be Trusted (https://208.99.166.251/).

The port considered most vulnerable for this period were 443(HTTPS), this is due to the fact that many vulnerabilities were found that are related to them and are classified at a medium severity level.

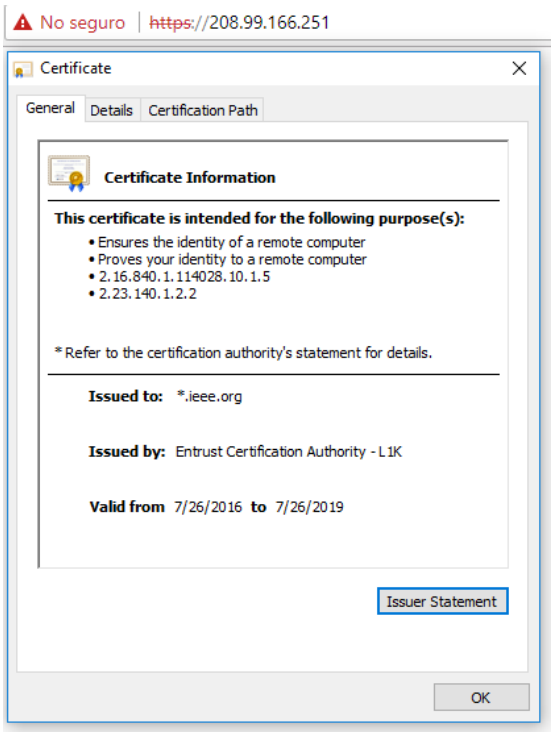
GLESEC www.glesec.com
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

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

Category	Critical	High	Medium	Low	Total
General			4		4

A vulnerability found by our MSS-VME service, called Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure (in which a malicious user can gain information about the handshake method used during a communication with a client and could allow the malicious user to impersonate the server or decrypt communications that should be encrypted).

The SSL certificates that cannot be trusted. In this particular cases, since the tests were done using the IP address of the hosts, the name that comes in the certificate do not match with the IP.



The ip 208.99.166.247 and 208.99.166.247 presents both the ROBOT vulnerability and the SSL certificate error, however further investigations on this IP 208.99.166.247, redirected to the following webpage https://webservices.ieee.org/bms/services_update.html .

Medium Risk Level Vulnerability

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

Description
The remote host is affected by 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.

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.

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

Affected Systems
443 / tcp / www 208.99.166.247208.99.166.251
443 / tcp 208.99.166.249

Output

```
The test sent a crafted RSA ciphertext and then sent a TLS Finished message with incorrect
padding.
The following differences in behaviour were seen by Nessus :
  - As a baseline with correct formatting : server sent TLS alert 40, server sent TLS alert 40,
server sent TCP FIN
  - With incorrect leading bytes          : server sent TLS alert 40, server sent TCP FIN
  - With the 0x00 byte in incorrect place : server sent TLS alert 40, server sent TLS alert 40,
server sent TCP FIN
  - With the 0x00 byte missing            : server sent TLS alert 40, server sent TCP FIN
  - With an incorrect version number      : server sent TLS alert 40, server sent TLS alert 40,
server sent TCP FIN
```

443 / tcp 208.99.166.235

Output

```
The test sent a crafted RSA ciphertext and then waited, without sending a TLS Finished message.
The following differences in behaviour were seen by Nessus :
  - As a baseline with correct formatting : server waited
  - With incorrect leading bytes          : server sent TLS alert 40, server sent TCP FIN
  - With the 0x00 byte in incorrect place : server sent TLS alert 40, server sent TCP FIN
  - With the 0x00 byte missing            : server sent TLS alert 40, server sent TCP FIN
  - With an incorrect version number      : server sent TLS alert 40, server sent TCP FIN
```

SSL Medium Strength Cipher Suites Supported

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption.
Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network

Solution

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

Affected Systems

443 / tcp 208.99.166.235208.99.166.249

Output

```
Here is the list of medium strength SSL ciphers supported by the remote server :

  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    EDH-RSA-DES-CBC3-SHA         Kx=DH          Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    ECDHE-RSA-DES-CBC3-SHA       Kx=ECDH        Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1
    DES-CBC3-SHA                 Kx=RSA         Au=RSA      Enc=3DES-CBC(168)        Mac=SHA1

The fields above are :

  {OpenSSL ciphername}
  Kx={key exchange}
  Au={authentication}
  Enc={symmetric encryption method}
  Mac={message authentication code}
  {export flag}
```

SSL Certificate Signed Using Weak Hashing Algorithm

Description

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

an attacker to masquerade as the affected service.

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

Solution
Contact the Certificate Authority to have the certificate reissued.

Affected Systems
443 / tcp 208.99.166.249
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=WA/L=Seattle/O=MyCompany/OU=IT/CN=localhost.localdomain/E=root@localhost.localdomain
|-Signature Algorithm : SHA-1 With RSA Encryption
|-Valid From          : Sep 11 02:44:12 2014 GMT
|-Valid To            : Sep 08 02:44:12 2024 GMT
```

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 expose 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 23%.

In the **email simulation** 55 of the different file types, holding a malicious-payload within, were able to penetrate your security measures (See "Files detected as ALLOWED"). 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.

A very important detail that can be observed in the Summary is that the highest percentage penetration for the **email vector** this month comes from exploits at 29%. 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.

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. April 2018
E-mail Security Exposure Level: Low
Risk Score: 23

Least Vulnerable To:

worm

*i.e: Deprosy worm, Stuxnet.

Most Vulnerable To:

exploit

*i.e: adobe, office, browsers exploits.

Email Simulation Summary: 756/4190

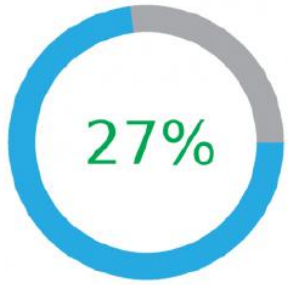
Risk Level	*Sent*	*Penetrated*
High	550	58
Medium	1222	304
Low	2375	394

Infected Simulated File types

The following charts show the infected simulated files by filetype, with the percentage of successful infiltrations.

Known Exploits

An exploit takes advantage of a bug or vulnerability in a software such as: Adobe, Word etc...



Executable Files

An executable file is a file that is used to perform various functions or operations on a computer that can be malicious.

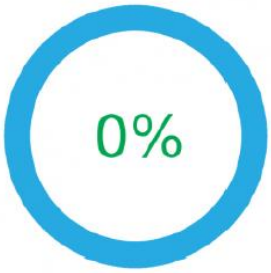
GLESEC
USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355

Office Files

Such as: Word, Excel, Power-point that may potentially contain malicious code execution.

Encrypted Files

Such as: Zip, Rar, 7z that may potentially contain malicious code execution and cannot be detected as



Files types detected as ALLOWED

.mcl	.one	.rtf	.pub	.csv	.mp3	.7z	.tar	.cab	.gz	.lha	.arj	.rar	.ods
.lzh	.dot	.accdb	.mdb	.pot	.pps	.ppt	.ppa	.dotm	.xlw	.xll	.xlsb	.xml	.xlsm
.xltm	.xlm	.xlk	.xlam	.xla	.slk	.pptx	.htm	.xls	.pptm	.eml	.ppsm	.potm	.doc
.svg	.oft	.wav	.xhtml	.xlsx	.vcs	.zip	.docx	.xsl	.pdf	.msg	.ics	.html	

The chart above illustrates the file types that were used on the simulated attack and were able to access the network.

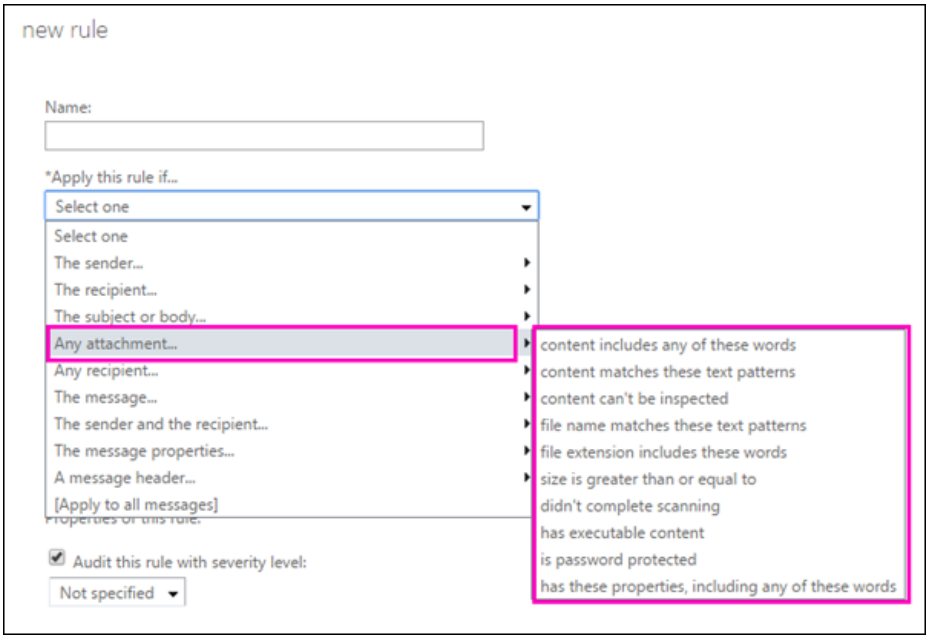
Remediation for the most popular mail servers

If any of the file extensions shown, is not part of the allowed file types in your organization, it would be recommended to create a rule in the antispam filters and/or the email server. Based on the results and the information provided, there are some adjustment that can be done on the most popular mail servers (Exchange, Postfix and Sendmail) to reduce the number of file types that can penetrate the network.

The following recommendations are valid for on-premise email servers. Hosted email

servers configurations must be done by provider.

Microsoft Exchange, comes with several options to analyze mail with attachments that arrives to the Exchange Server, these rules can be created in Exchange Admin Center (EAC).



Microsoft Exchange can analyze various common file types and verifies if the file extension matches with the content of the attachments. Microsoft has a list of all the supported file types in the following link.
https://technet.microsoft.com/en-us/library/jj919236(v=exchg.150).aspx

Other common mail server solutions are Postfix and Sendmail. Sendmail comes integrated with some measures of anti-spam features, based in rules, in version 8 and later but not with anti-malware. Postfix also comes integrated with anti-spam filters but not with antimalware scanners/filters as Exchange. Both platforms can be integrated with software that fulfill those roles, common examples are *Spamassassin* and *ClamAV*. Integration of the software depends on the OS that is running the mail server.

The integration of SpamAssassin and ClamAV into Postfix vary depending on the Linux distro.

For ClamAV in Ubuntu:

1. Open a terminal

2. Write the following command: sudo apt-get install clamav clamav-freshclam clamsmtp.

3. Accept the installation of any dependency requested.
After the installation is complete, the daemon will be already running and there are some additional configurations that must be done.

- Change the ports defined in /etc/clamsmtpf.conf to the ports used by Postfix.
- In postfix, add the following lines to the /etc/main.cf:

content_filter = scan:127.0.0.1:10025
receive_override_options = no_address_mappings

In the /etc/postfix/master.cf file add the following lines at the end of the file:

AV scan filter (used by content_filter)
scan unix - - n - 16 smtp
smtp_send_xforward_command=yes
# For injecting mail back into postfix from the filter
127.0.0.1:10026 inet n - n - 16 smtpd

- content_filter=
- receive_override_options=no_unknown_recipient_checks,no_header_body_checks
- smtpd_helo_restrictions=
- smtpd_client_restrictions=
- smtpd_sender_restrictions=
- smtpd_recipient_restrictions=permit_mynetworks,reject
- mynetworks_style=host
- smtpd_authorized_xforward_hosts=127.0.0.0/8

To configure automatic updates:

- Open a terminal, write the command sudo crontab -e
- Add the following line 00 1 * * * /usr/bin/freshclam –quiet. (Adjust the hour to an hour that is adequate to the needs of the organization).

For SpamAssassin in Ubuntu:

- Open a terminal, execute apt-get install spamassassin spamc

- Create a user for Spamassasin with adduser spamd --disabled-login
- In Postfix you have to define the content filter to use, this can be done in /etc/postfix/master.cf adding the following lines:

```
smtp      inet  n       -       -       -       -       smtpd
 content_filter=spamassassin
spamassassin unix -     n       n       -       -       pipe
 user=spamd argv=/usr/bin/spamc -f -e
/usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

For this change to take effect, Postfix has to be restarted with:

```
systemctl restart postfix.service
systemctl enable spamassassin.service
systemctl start spamassassin.service
```

Additional configurations regarding Spam filters can be requested to GLESEC Personnel.

Additional countermeasures that minimize malware penetration

For file extensions that are part of the permitted list there are two approaches to take:

- A restrictive approach that could greatly reduce the malware penetrations in the mail vector is a Content Disarm and Reconstruction (CDR) solution to examine the mails before delivering it to their destination.
  This type of solution usually correctly identify the file type without relying on the file extension, deconstruct the file in several components to then remove any unneeded data and rebuild the file again without any loss in functionality and keeps the original final in quarantine, delivering the sanitized file to its destination.

- A less restrictive approach is the use of a software with the capability to detect and analyze the behaviors and actions taken by the files in a detailed fashion allowing to identify from which file or process the action was originated with timestamp, actions taken, directories affected then report the events, allowing further analysis to be done before taking action, but with the capability to take immediate action if necessary.

Successful High level simulated attacks

High risk files able to penetrate the perimeter were Worm, 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 Ransomware was hidden within different file types:

•HTM: An HTM file is an HTML web page used by web browsers. It contains markup code that is stored a plain text format and is used to display and format text and images in a web browser.
•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.

•Malware: files that await remote commands from a command and control server or try to obtain elevated privileges by disrupting the user activities with pop-ups.
•Worms: files disguised as Office Macros that attempt to spread through the network to infect other computers.

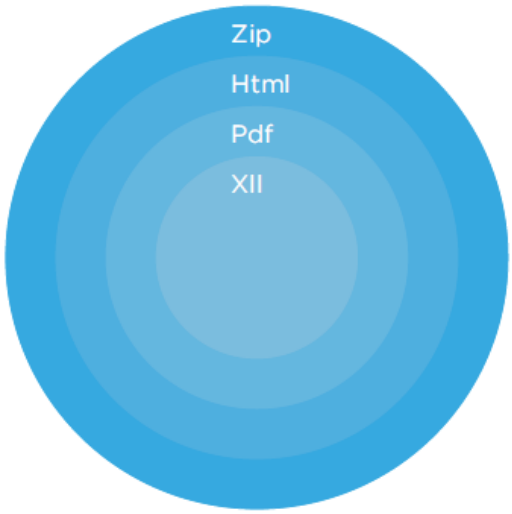
Even though all the other tested threats: Payload, Worms, Links, Malware, Exploits and Dummy were able to penetrate the perimeter, we consider Ransomware alone as the highest risk due to its probability of occurrence and possible negative impact.
Successful Low level simulated attacks

Comments

Malware that uses Office documents as infection method commonly use macro files to execute the payload. Another method that is becoming more common, as seen by the malware that exploits CVE-2017-0199, consists in making winword.exe, or any program of the Office suite, issue an HTTP request to a remote server to retrieve a file that contains the malware script; in this method the user is presented with a decoy document instead of a macro file to trick the end-user that is a legitimate document.

This method of leveraging documents to retrieve the payload itself instead of directly embedding in the document makes standard AV protection unable to detect anything malicious in the email attachment, until the payload is being downloaded in the victim's computer.

A graphical representation for this is showed below:



Web Gateway Attack Summary

Within the set of threats that can penetrate via Browser, exists a high percentage of penetration in critical threats mainly files, followed by policy. For our analysts the Risk Score for your organization is of level Low.

The "Web Gateway Security Exposure Level" (Browser) for your company this month was classified as "Low" based on the (Average) "Risk Score" of 21%. We noted a reduction in a 100% about exploit penetration, but an increment over 3% in Command&Control potential risk and 38% in website related organization policy.

File penetration is about 98%, indicating high value penetration events of files infected about broad types of malware and, then, incrementing infection's likelihood in IEEE premise.

In GLESEC, we encourage you to follow the next recommendations.

Note: Check the types of files in the section "Successful High level simulated attacks"

Whole Compiled Recommendations

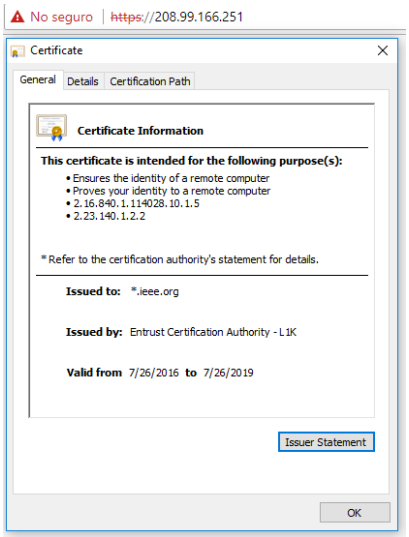
Despite the growing investment in cyber security, sophisticated attackers still manage to bypass even the most advanced security systems, including next-generation, non-signature based security. The reason is that advanced threats are coded to look like legitimate behavior. Therefore, they are extremely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

1. One of the recommendations for a vulnerability found by our MSS-VME service, called Return Of Bleichenbacher's Oracle Threat (ROBOT) Information Disclosure (in which a malicious user can gain information about the handshake method used during a communication with a client and could allow the malicious user to impersonate the server or decrypt communications that should be encrypted), GLESEC recommend to verify with your devices vendor if there is a patch available for the TLS implementation. In case there is no patch available, it is recommended to disable RSA key exchange and enable instead ECC (Elliptic Curve Diffie Hellman).

   The IPs 208.99.166.247 and 208.99.166.247 presents the ROBOT vulnerability.

   Another vulnerability found correspond to SSL certificates that cannot be trusted. In these particular cases, since the tests were done using the IP address of the hosts, the name that comes in the certificate do not match with the IP. This in itself does not represent a vulnerability. To remove the message, define the IP address of the hosts as Subject Alternative Name field in the certificate.

USA | PANAMA | ARGENTINA | MEXICO | COLOMBIA | PERU | CHILE | ECUADOR
Tel: +1 (609)-651-4246 / +(507)-836-5355



Further investigations on this IP 208.99.166.247 that also presented the SSL certificate error, redirected to the following webpage: https://webservices.ieee.org/bms/services_update.html

2. The service MSS-BAS used a group of sample files to simulate the attacks, most of this samples were contained in one or several file types, the following table illustrates which embedded file types were able to successfully infiltrate your network:

.mcl	.one	.rtf	.pub	.csv	.mp3	.7z	.tar	.cab	.gz	.lha	.arj	.rar	.ods
.lzh	.dot	.accdb	.mdb	.pot	.pps	.ppt	.ppa	.dotm	.xlw	.xll	.xlsb	.xml	.xlsm
.xltm	.xlm	.xlk	.xlam	.xla	.slk	.pptx	.htm	.xls	.pptm	.eml	.ppsm	.potm	.doc
.svg	.oft	.wav	.xhtml	.xlsx	.vcs	.zip	.docx	.xsl	.pdf	.msg	.ics	.html	

To detect malicious file that could be hidden within another file type solutions such as Sandbox/Content-Disarm & Reconstruct can be implemented. A Sandbox solution contains the suspicious file in an isolated environment and attempt to execute it in several ways behaving like an end-user, if the payload is triggered, the sandbox can use Content disarm, removing the malicious code embedded in the file and leaving the original file cleansed.

3. Recommendations of the Browser vector
    - Filter the web files (through web filtering)

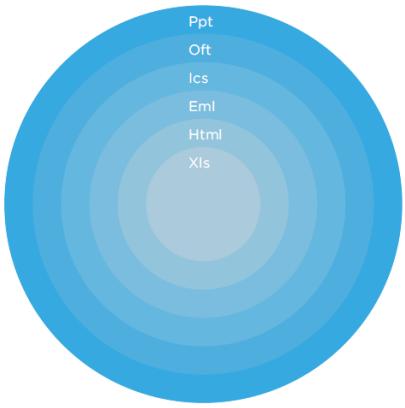
- Use disarm and reconstruction tools that reach the files embedded in the access and remove the dangerous codes from them.
- In some cases in the simulation test of the Browser vector, configure the filter to eliminate VCS files that contain the string **"ATTACH; ENCODING=BASE64; VALUE=BINARY; X-FILENAME="**
- Use docker to open "potentially dangerous" files

For example

The packaged file
PPT←OFT←ICS←EML←HTML←XLS, where "a ← b" means file "a" contain file "b" or file "b" is (inside) file "a".

The file is a power point that inside, has an openoffice file (OFT) which in turn has an ICS, and in turn, one mail (EML) and in turn a web page (HTML) and in turn, one of Excel (XLS), which contains the malicious code.

A graphical representation for this is showed below:



4. We have noticed a sharp decline in the number of hosts discovered, we recommend allowing access to our systems to provide the full view of the assets discovery results and vulnerability discovery.

Appendix A

There is extensive amount of more detail that can be provided upon request.

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

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

Info@glesec.com
www.glesec.com