MANAGED BREACH ATTACK SIMULATION
MSS-BAS Test – eMail Vector

Inspira Health Network

Technical Report

December 2017

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

Info@glesec.com
www.glesec.com

Table of Contents

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

About This Report

This is a technical report 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.

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

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 "Medium" based on the "Risk Score" of 48%.
In this simulation 62% of the different file types, holding a malicious payload within, were able to penetrate your security measures. 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.

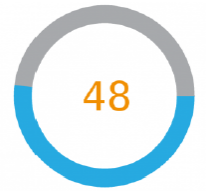
A very important detail that can be observed in the Assessment Result (see below in the Mail Risk Analysis per Type Section) is that the penetration of files containing malicious Exploits was of 100% and Ransomware was of 58%. After these threats enter the network they can be executed in many different ways causing high impact to the organization.

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

Mail Attack Summary

Within the set of threats that can penetrate via email, exists a high percentage of penetration in critical threats mainly Ransomware, Exploits, followed by Dummy. For our analysts the Risk Score for your organization is of Medium level. 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. December 2017
E-mail Security Exposure Level: Medium
Risk Score



Simulation Summary 24/44

Risk Level	*Sent*	*Penetrated*
High	15	3
Medium	8	7
Low	21	14

MSS-BAS e-mail vector Risk Summary Matrix

E.g: Vulnerable to a Medium Probability Ransomware like WannaCry	**21%**	**13%**	*Impact* →	E.g.: Vulnerable to a High Probability Ransomware like WannaCry
E.g.: Vulnerable to a Low Probability Payload like Meterpreter Shell	**58%**	**8%**		E.g.: Vulnerable to a High Probability Payload like Meterpreter Shell

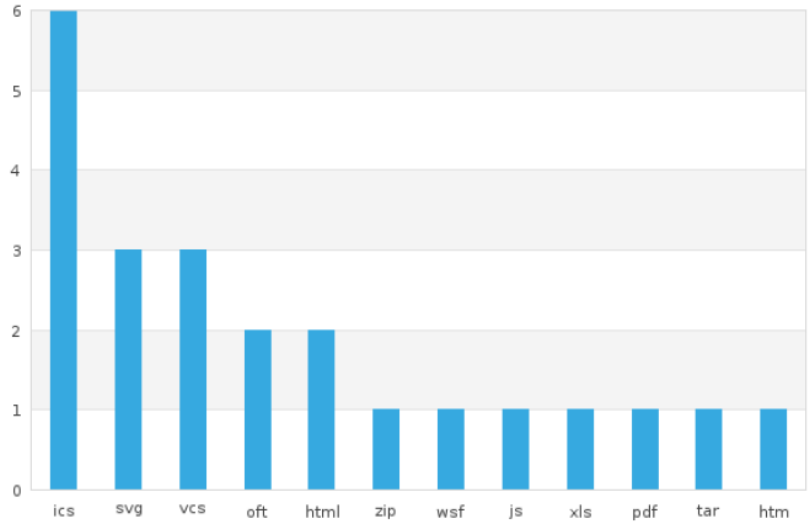
Probability →

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.

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 25% of the flaws
For svg files it will solve 13% of the flaws
For vcs files it will solve 13% of the flaws
For oft files it will solve 8% of the flaws
For html files it will solve 8% of the flaws
For zip files it will solve 4% of the flaws
For wsf files it will solve 4% of the flaws
For js files it will solve 4% of the flaws

For xls files it will solve 4% of the flaws
For pdf files it will solve 4% of the flaws
For tar files it will solve 4% of the flaws

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

Mail Risk Analysis per Type

Assessment Result

33%
Worm
Software using Common techniques in order to spread itself inside a Windows based network.

58%
Ransomware
Software encrypting user files and denies access until ransom is paid

0%
Malware
Malware, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

56%
Dummy
Dummy category is code execution proof of concept without actual damage to the system.

100%
Exploit
Known and signed exploits of commonly used software that leads to code execution because of vulnerabilities discovered.

50%
Payload
Common attacks delivered to clients like: Data extraction attacks or Stagers downloading the real malware.

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

High Risk

Here are the findings with High risk that penetrated your organization:
Ransomware with 3 Payloads in high risk

Medium Risk

Here are the findings with Medium risk that penetrated your organization:
Ransomware with 4 Payloads in Medium risk
Exploit with 2 Payloads in Medium risk
Worm with 1 Payloads in Medium risk

Summary by type/risk (see graph below)

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

2 Payload sent and 1 penetrated your organization:
1 of the files are in Low risk

3 Worm sent and 1 penetrated your organization:
1 of the files are in Medium risk

24 Ransomware sent and 14 penetrated your organization:
7 of the files are in Low risk
4 of the files are in Medium risk
3 of the files are in High risk

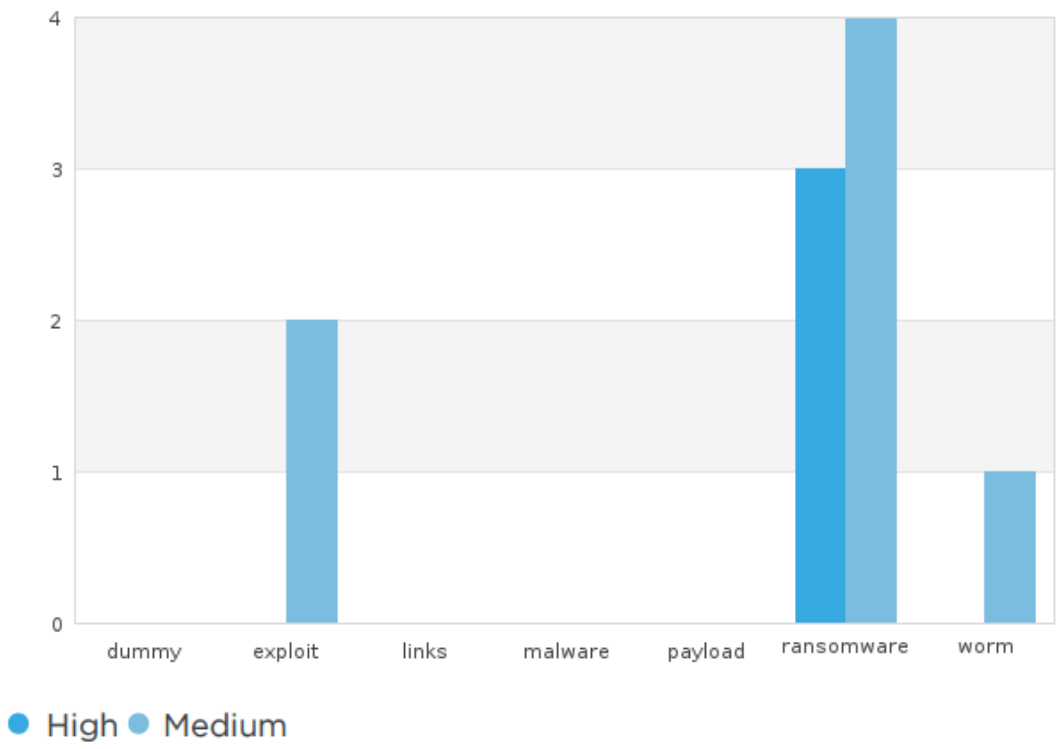
3 Malware sent and 0 penetrated your organization

9 Dummy sent and 5 penetrated your organization:
5 of the files are in Low Risk

3 Exploit sent and 3 penetrated your organization:
1 of the files are in Low risk
2 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

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



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

Successful High level simulated attacks

The 3 High risk files were able to penetrate the perimeter were Ramsonware. This specific type of ransomware was categorized as a high risk, because the amount 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 3 different file types:

- 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.
- VSC: This type of file is well known to be used as McAfee VirusScan configuration files. Nevertheless, it is possible that other applications use them as well.
- 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.

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 above.

Successful Medium level simulated attacks

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

- Ransomware: 4 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:
  - SVG-ZIP
  - HTM-ZIP
  - HTML-ZIP
  - JS-WSF

This ransomware has the same impact to your Organization if executed, but

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

it is little less accessible. Please refer to the recommendations section, items number 2 and 3.

- Exploit: 2 files targeting two different vulnerabilities, first one affects Adobe Acrobat Professional version 8.1.3 and lower by creating a specially crafted pdf that a contains malformed util.printf() entry, allowing an attacker to execute arbitrary code. The other one aims to instigate a stack overflow attack MSCOMCTL.OCX, this attack targets Microsoft Office 2007 and 2010. Please refer to the recommendations section, item number 1.

- Worms: 1 file that is run automatically by the Office Macro scans ports and infects other computers in the network.

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

Successful Low level simulated attacks

14 out of 21 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.

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

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. It's been detected that many of e-mail containing malicious files that use exploits were able to penetrate the network. Old versions of software are vulnerable to many known exploits, malicious code can be hidden within files that should be allowed because they are of regular usage, and bypass many security measures. 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. 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.

It should be noted that the simulation performed was very limited in scope. We only performed one attack vector out of five (only email) and for this attack vector only 40 attacks out of several thousand. However, the findings are clear in that **certain actions should be conducted to strengthen the security of Inspira Health Network**. A more detailed POC can be implemented to execute all tests and provide

a detail report on the findings with corresponding recommendations. The test and/or the POC can provide evidence of the need for the ongoing **MSS-BAS** or Managed Breach Attack Simulation. This service includes weekly testing, indexing and correlation of the data, incident alerts and consolidated monthly Operations & Intelligence reporting. Based on the other services in operation with Inspira this "threat and testing" service provides valuable information to add to **RISK** and **VALIDATION**. Some other points mentioned in the report are supported by GLESEC's portfolio but are not included in the report.

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

Appendix A

Waveform Audio File Format Exploit Risk Level: Low

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

Adobe Util Print PDF Exploit Risk Level: Medium

Description
This file exploits a buffer overflow in Adobe Reader and Adobe Acrobat Professional < 8.1.3. By creating a specially crafted pdf that a contains malformed util.printf() entry, an attacker may be able to execute arbitrary code. 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.
- Block .ics with file size that is larger than 10k.

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

Cymulate Ransomware Risk Level: High

Description
Cymulate 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.

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

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

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

Cymulate Ransomware Risk Level: Medium

Description
Cymulate 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.

Dummy Payload Risk Level: Low

Description
Dummy Payload is a WinAPI MessageBox code execution proof of concept. 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.
• 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.

Cymulate Ransomware Risk Level: Medium

Description
Cymulate 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 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

• 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.

PowerBat Exploit Risk Level: Low

Description

Cisco Ironport, Symantec email security cloud, McAfee email gateway and Clearswift email gateways, all kind of work like AV, Uses signatures. So when using Object Linking and Embedding (OLE), OLE commonly consists of an embedded windows shortcut References PowerShell "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -exec bypass -c ... ", they appeared to detect "Powershell" as malicious, And by replacing "Powershell.exe"with"%allusersprofile:~3,1%%allusersprofile:~5,1%%windir:~3,1%% localappdata:~5,2%%windir:~9,1%he%localappdata:~-1%%localappdata:~- 1%", we

can call powershell without "Powershell.exe" and bypass email gateways. Final OLE: "%allusersprofile:~3,1%%allusersprofile:~5,1%%windir:~3,1%%localappdata:~5,2%% windir:~9,1%he%localappdata:~1%%localappdata:~- 1%-exec bypass -c ... "

Mitigation

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

Dummy Payload Risk Level: Low

Description

Dummy Payload is a WinAPI MessageBox code execution proof of concept. 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.
- 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.

Meterpreter Reverse HTTPS Risk Level: Low

Description

Meterpreter Reverse Https is a Metasploit stager downloading Metasploit's Meterpreter payload from a remote server.

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.

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

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

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

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

Cymulate Ransomware Risk Level: High

Description
Cymulate 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.

Cymulate Ransomware Risk Level: Medium

Description
Cymulate 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.

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

Cymulate Worm Risk Level: Medium

Description
Cymulate 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.

Cymulate Ransomware Risk Level: Low

Description
Cymulate 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.

Cymulate Ransomware Risk Level: High

Description
Cymulate 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.

Cymulate Ransomware Risk Level: Medium

Description
Cymulate 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.

PowerBat Exploit Risk Level: Low

Description
Cisco Ironport, Symantec email security cloud, McAfee email gateway and Clearswift email gateways, all kind of work like AV, Uses signatures. So when using Object Linking and Embedding (OLE), OLE commonly consists of an embedded windows shortcut References PowerShell "C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe -exec bypass -c... ", they appeared to detect "Powershell" as malicious, And by replacing "Powershell.exe"with"%allusersprofile:~3,1%%allusersprofile:~5,1%%windir:~3,1%% localappdata:~5,2%%windir:~9,1%he%localappdata:~-1%%localappdata:~- 1%", we can call powershell without "Powershell.exe" and bypass email gateways. Final OLE: "%allusersprofile:~3,1%%allusersprofile:~5,1%%windir:~3,1%%localappdata:~5,2%% windir:~9,1%he%localappdata:~-1%%localappdata:~- 1%-exec bypass -c ... "

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

Winrar Spoof Risk Level: Low

Description

This module abuses a filename spoofing vulnerability in WinRAR. The vulnerability exists when opening ZIP files. The file names showed in WinRAR when opening a ZIP file come
from the central directory, but the file names used to extract and open contents come from the Local File Header. This inconsistency allows to spoof file names when opening ZIP files with WinRAR, which can be abused to execute arbitrary code, as exploited in the wild in March 2014

Mitigation

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

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

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

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

Info@glesec.com
www.glesec.com