Operations and Intelligence

Institute of Electrical and Electronics Engineers

December 2017

BEST IN CLASS – INFORMATION - SECURITY

INTELLIGENCE AND OPERATIONS

Table of Contents

1. About This Report

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

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

2. Confidentiality

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

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

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

3. Scope of This Report

GLESEC Contracted Services

MSS: Managed Security Service (full outsourcing)

Service	Service Expiration
MSS-BAS (Managed Breach Attack Simulation)	12/30/18

4. *EXECUTIVE SUMMARY*

Mail Attack Summary

MSS-BAS Mail Vector enables organization to challenge this main attack vector. The number of targeted attacks has dramatically increased in recent years. Poor configuration or implementation of security products might lead to the false assumption that you are safe. This assessment allows you to test those assumptions, prove yourself wrong and improve your email posture with every use. Security products might lead to a false assumption that you are safe.

64% of the attacks were successful to penetrate the network. Out of these many types of malware and Ransomware are able to penetrate. This is should be of concern to the organization.

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

	High	Medium
Malware	73	73
Ransomware	35	35
Worm	17	30
Dummy	1	0
Exploit	0	31
Payload	0	60
Links	0	0

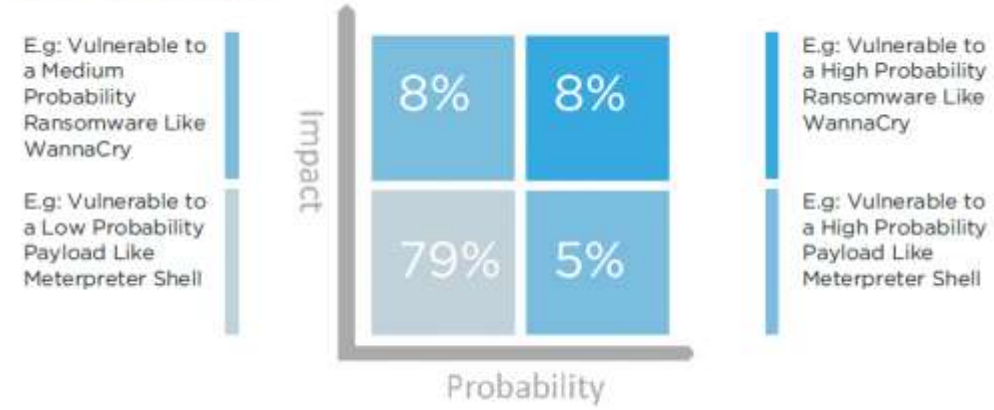
5. *E-Mail Security Exposure*

Simulation Summary

Risk Level	Sent	Penetrated
High	551	126
Medium	1118	229
Low	2353	1320

Total Assessment: 1675 / 4022

Risk Summary Matrix



6. *Assessment Result*

7. *Executive Action Items*

8. 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 test/simulation/service/ showed that various attacks can compromise your local network.

1. Short term recommendations:
   Mail Relay, Content disarm and reconstruction or sandbox solutions:
   For ics files it will solve 14% of the flaws
   For vcs files it will solve 13% of the flaws
   For svg files it will solve 7% of the flaws
   For pdf files it will solve 6% of the flaws
   For html files it will solve 6% of the flaws
   For oft files it will solve 6% of the flaws
   For eml files it will solve 6% of the flaws
   For msg files it will solve 6% of the flaws
   For htm files it will solve 5% of the flaws
   For zip files it will solve 5% of the flaws
   For xhtml files it will solve 3% of the flaws

2. Due to the fact that a penetration could have already compromised the internal systems it is recommended to conduct a forensic evaluation of your local network and/or critical systems. Contact your GLESEC representative for assistance with the more effective ways to handle this.

3. It is also important to take a pro-active approach to avoid infection by deployment of technology or contracting a service that can identify an attack without signatures and mitigate this before it causes harm to the organization. Contact your GLESEC representative for assistance with this.

9. Appendix 1 – Glossary of Terms

Links

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

Payload

The payload is the part of malware such as worms or viruses which performs the malicious action; deleting data, sending spam or encrypting data. In addition to the payload, such malware also typically has overhead code aimed at simply spreading itself, or avoiding detection. Payload can be A small software that downloads the more advanced Payload from the remote C&C.

Worm

Malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth.

Ransomware

Ransomware is computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransompayment to decrypt it or not publish it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, and display a message requesting payment to unlock it. More advanced malware encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Malware

Malware, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. The fragment may be machine code that infects some existing application, utility, or system program, or even the code used to boot a computer system. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. Malwares are often referenced to Trojans, C&C, credential Theft Software.

Dummy

The dummy files are Windows MessageBox, code execution proof of concept. Malicious files are coded very often (thousands a day) and therefore relying on Signatures to block malicious files is outdated. Dummy files can prove the code execution is possible and share the same aspect of new unsigned malicious files.

Exploit

An exploit is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur on computers. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation, or a denial-ofser

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

Panamá
Central America HQ
Prime Time
Address. La Rotonda Costa del Este
Panamá City, Panamá
Tel. +507.836.5355

Argentina
South América HQ
+54.11.5917.6120

Brasil
+55.11.3711.5699

Chile
+56.2938.1496

Perú
+51.1708.7197

México
+52.55.5018.1164