IMMEDIATE THREAT CYBER ASSESSMENTM

Institute of Electrical and Electronics Engineers

March 2018

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

Info@glesec.com
www.glesec.com

Table of Contents

Table of Contents 2
About This Report 3
Confidentiality 3
Immediate Theat Cyber Assessment 4
Recommendations 5

GLESEC
www.glesec.com
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

IMMEDIATE THREAT CYBER ASSESSMENT

Files containing any type of malware are a real and immediate threat to every organization. Our intelligence team continuously collects these types of immediate threats and tests your organization against these real world attacks as they emerge. This report includes the new public breaches and exploits that were found and can potentially be used by hackers. These types of files should be filtered or contained immediately as they are the hottest threats used by hackers and cybercrime organizations around the world.

MSS-BAS (e-mail vector)

GLESEC carried out, as part of the MSS-BAS service contracted by your organization, a simulation with the latest threats located in the DeepWeb to-date.

As a result of the 1 types of tests of this simulation we found that 1 was able to successfully penetrate your organization's defenses. This test is associated with extension (.slk), called Symbolic Link (SYLK) format created by Microsoft.

Simulation Summary

Risk Level	Sent	Penetrated
High	1	1
Medium	0	0
Low	0	0

Total Assessment: 1 / 1

DESCRIPTION

This attack was sent attached to an email as "WSCJan2018_PaymentRequest.slk". What is important is that it is considered as a direct exposure to the threat since this malicious file is not hidden within other file formats. These SLK files also support the ability to execute malicious commands. With these sort of attacks the user might receive a few warnings that should set off red flags before the infection begins. Unfortunately, most anti-virus engines do not catch these attacks.

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

RECOMMENDATION

The best thing one could do against this type of attack is not letting it through; since it may or not be a kind of Ransomware it's best to prevent it.

Preventive/remediation measures include:

1. Configure your email filters to eliminate all possible file extensions
2. Keep the antivirus updated, this can help and it is one of the best practices in cyber security. This is however a necessary **but not sufficient condition.** We recommend that your utilize other non-signature based forensic and remediation technologies, preferably of low false-positives. *Contact us at GLESEC for more information on this.*
3. Ensure that your applications and operating systems have been patched with the latest updates to minimize exploits to known vulnerabilities
4. Execute and maintain a periodically data backup schedule
5. Erase the malware in case a user downloads it. Be aware that malware applications create a number of additional files. All of these have to be eliminated. *Contact us at GLESEC for more information on this.*
6. Educate users to be watchful and avoid downloading software from unknown sources. *We recommend complementing this with the GLESEC MSS-BAS Phishing Vector.*
7. Make sure that windows request to enable macros is **always on** and not disabled.

Block known malicious files such as:

- Malicious Files:
  - **SHA-256: 5b5f4973ddac5ef61d69a12fc073dd1a2953215222d7b69c9b4110f7e274d0c7**
  - File name **WSCJan2018_PaymentRequest.slk**
  - File size 6.52 KB
  - Last analysis 2018-03-10 18:13:12 UTC
- Malicious File:
  - **SHA-256: b54574e09b961f9194bbbb5920beb4ccb68d3dfd3caea580cfef75371e35c343**
  - File name **AMSTREAM2.EXE**
  - File size 1.2 MB
  - Last analysis 2018-02-15 14:21:34 UTC

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