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)

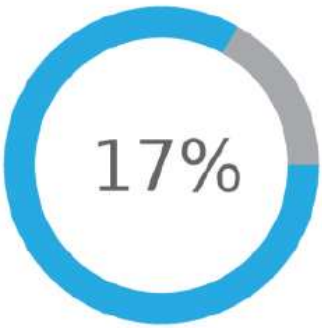
GLESEC carried out, as part of the MSS-BAS service contracted by your organization, a simulation with the latest threats located in the DeepWeb to-date.

As a result of the 12 types of tests of this simulation we found that 2 were able to successfully penetrate your organization's defences. These tests are associated with extensions (.mp3 & .png), called "ElTest Campaign".

Simulation Summary

Risk Level	Sent	Penetrated
High	5	0
Medium	3	2
Low	4	0

Total Assessment: 2 / 12



DESCRIPTION

ElTest Campaign, this new method uses 2 different actions that depend on the web browser the user is using, the web browsers affected are Internet Explorer and Google Chrome. **Google Chrome actions were successfully blocked by the browser.**

The actions related to Internet Explorer were successful (.mp3 & .png)

If the browser is Internet Explorer, the user is presented with pop-up window, alerting the user that the computer is infected with a very dangerous malware and they must call a phone number to solve the issue or all the sensible information in the computer would be compromised.

GLESEC 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:

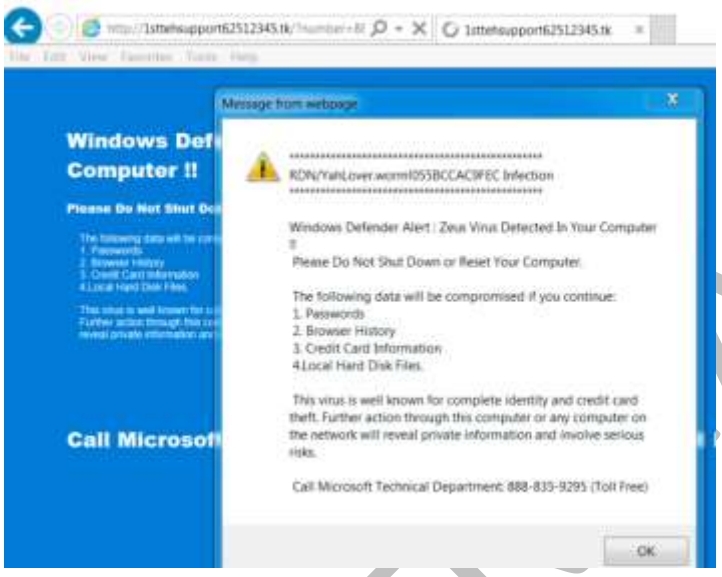
1. Configure your email filters to eliminate at all possible file extensions
2. Keep the antivirus updated, this can help and it is one of the best practices in cyber security. This is however a necessary **but not sufficient condition.** We recommend that your utilize other non-signature based forensic 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.*

Block known malicious sites such as:

- rustyhealyinsurance.com - GET /
- 212.1.208.53 port 80 - www.liceobelgrano.edu.ar - GET /o o.php
- 31.31.196.204 port 443 (HTTPS) - printscreens.info - GET /JSX/tespost.php?get=1&file=[various file names]

- .31.196.204 port 443 (HTTPS) - printscreens.info - GET /JSX/tespost.php
- DNS query for bmwfastcar1337.com - resolved to 94.242.198.167
- 94.242.198.167 port 1488 - 94.242.198.167 – POST
- http://94.242.198.167/fakeurl.htm
- Add anti-virus rules to block the following malicious files by the file hash, these hashes are related to the actions that use Chrome:
- SHA256 hash:
  - 3e65faf4b8917f5c610efe7a97b165664b62b180e71a5a567f7b07d749d3438d
  - File size: 420,072 bytes
  - File name:: Font_Chrome.exe
  - File description: malware downloader for NetSupport Manager RAT
- SHA256 hash:
  - 482632c47f6fab4a376e0d509c008960dafbadab13fdc591321971f18ffc1132
  - File size: 287,876 bytes
  - File location: C:\Users\[username]\AppData\Local\Temp\js.js
  - File description: JavaScript dropped by the malware downloader, used to download and install NetSupport Manager RAT
- SHA256 hash:
  - c9aef58c5a639778b2f83495d30a4a9466d79e70b2d089cffb9e1974d335b4ed
  - File size: 34,808 bytes
  - File location: C:\Users\[username]\AppData\Roaming\ALEX\client32.exe
  - File description: NetSupport Client Application, version 11.0.0.476 - not inherently malicious, if you don't mind RATs.

We attach an image showing a fake AV page that should not be executed:



References: http://www.malware-traffic-analysis.net/2017/12/26/index2.html

For any questions please do not hesitate to contact us.

Sincerely,

GLESEC OPERATIONS CENTER – GOC.