trushield

New Trojan – Panda Banker

This is a security alert for all TruShield clients, the financial services industry, and the community as a whole. We have learned about a new banking Trojan that utilizes some Zeus code to do its damage. This new Trojan is called Panda Banker.

About Panda

Panda Banker is a banking Trojan discovered in February by Fox-IT InTELL. Proofpoint researchers further analyzed this Trojan and they named it Panda Banker. The Trojan borrows the code of the Zeus Banking Trojan. The malware is delivered via a spear-phishing email with a malicious attachment and the use of different exploit kits. Panda Banker was at first spotted targeting people working in mass media and manufacturing organizations, and a remote server was used to download the banker Trojan for this particular campaign, as stated on the SecurityWeek website. Then later when targeting the financial industry, the loader Godzilla was used to download Panda Banker. The three different exploit kits the Proofpoint researchers observed delivering Panda Banker are Neutrino, Nuclear, and Angler. Australia and the United Kingdom are the two countries that this Trojan is a targeting, based on the geo-filtering that was observed by Proofpoint researchers.

After the Trojan is downloaded, it reaches out to the command and control server to send and receive information. Some of the information that it sends includes the following: "system uptime, the process in which the malware is running, the current user name, a unique id for the infection, the botnet name, the botnet version, OS version information, latency, local time, computer name, the name of antivirus software installed, installed anti-spyware, and the installed firewall" as stated on Proofpoint's website. The rest of process includes a response with more information on modules and configuration commands for the malware. The researchers at Proofpoint were able to pinpoint the similarities between this malware and Zeus, namely the mutexes, files, folders and registry keys it creates. A unique method of Panda Banker "involves the use of numerous IP addresses associated with a single malicious domain known as Fast Flux DNS" and this makes it harder to combat this malware as stated by Proofpoint researchers.

Conclusion

Banking Trojans are known for their popularity in stealing millions from victims, and this particular Trojan is no different; it steals banking credential to perform the malicious act of stealing money, and it uses some of Zeus code to its duty. It does have multiple ways to go about stealing the information that it needs.

Protecting against Banking Trojans

To protect against banking Trojans like Panda Banker do not open emails from unknown senders, make sure that systems are and remain up to date with the latest patches, and employ other methods of detecting malware signatures and preventing them.

Indicators of Compromise

SHA256
1cccc844fcdb255f833a9ef36c2d3c690557b828ed5d0a45d068aeb2af1faac7
0fd5413365f474b99f4a49560e20c5e97418d09a2f53e5e7436b88e3f5c16668
a395357a9012b0a4087e0878e7d642877d3b856de53c71cb9805f806dc958264
Fa867ddf9f3116da75b62a1bf8007410ac0d3adf7a92e7f3d2effeef982ad73d
bdc912caf9b9e078bc7bd331deacae9c460c8e8893442048b9474790c52e1ab9
6dc0bd77e51eb9af143c749539bd638020d557083479bcd4c4b9639fe61eb0f8
8d381ee21b6cbc7d3ae0e503ab7b05235eb31594d2810e67093c5e9a51437992

Domains
secpressnetwork[.]com
alwaysonline[.]pw
denoted-chioces[.]com

References

http://www.securityweek.com/new-panda-banker-trojan-borrows-code-zeus

https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market

TruShield Security Solutions

TruShield is a leading provider of Managed Security Services across the globe. We are dedicated to helping companies achieve success by making sure they are properly prepared against the current and emerging threats in today's digital world. Our service offerings include: Continuous, 24/7/365 Monitoring, Penetration Testing and Vulnerability Assessments, Audit and Compliance, and many other Managed Services such as Managed Firewalls and Hosted Log Management. We also offer Security Awareness Training and Management Consulting services.

Contact us today to find out how we can help you protect your organization and safeguard your information.

Contact Information:

Email: support@trushieldinc.com
Web: www.trushieldinc.com
Phone: (877)-583-2841

Follow us on:

Twitter: @TruShield
LinkedIn: https://www.linkedin.com/company/trushield-security-solutions
Facebook: https://www.facebook.com/trushieldinc