Update to Shade Ransomware

This is a security alert for all TruShield clients and the community as a whole. We have learned of a new update to Shade Ransomware. The update allows for the ransomware to search for the precise file extension and execute upon finding it, and it also downloads additional malware to the system.

About Shade Ransomware

Shade Ransomware is an encryption ransomware and like most ransomware it encrypts a victim's computer files based on an extension list that has to be matched, and then asks for payment or a ransom to decrypt it. This ransomware affects Russia, Ukraine and Germany. It surfaced in late 2014 to early 2015. At the time it was one of the most widespread encryptors in Russia. It's being detected as "Trojan-Ransom.Win32.Shade, Trojan.Encoder.858, Ransom:Win32/Troldesh".
Shade ransomware is delivered via spam and infection occurs when the file in the attachment is clicked to open. Another method of delivery is through the use of exploit kits and that happens when a user visits a website that has been compromised. Next, that the malicious code on that website is then used to exploit vulnerabilities within the user's browser where the malware is downloaded. In this instance no executable runs and the user is aware of what is going on in the background.

Once the system is infected with the Trojan, it gets a public RSA-3072 key by communication to its C&C server, and this same key is used to encrypt the files. Once it finishes its encryption and demands a ransom, the malware "starts an infinite loop in which it requests a list from the C&C server containing the URLs of additional malware. It then downloads that malware and installs it in the system." as stated by Securelist researchers.
The following malware are downloaded:

- Trojan.Win32.CMSBrute (a more detailed description is provided below).
- Trojan.Win32.Muref
- Trojan.Win32.Kovter
- Trojan-Downloader.Win32.Zemot

The extension that it adds to the files after it encrypts it are .xtbl, and .ytbl. This Trojan is used to bruteforcing website passwords. The new update to this malware "looks for strings associated with banking softwares and, if it does find it, it executes a file from a URL in its configuration" as stated on Securityweek's news website. It also downloads additional malware to the victim's system and the code associated with doing this is known as Teamspy. This bot spies on its victim to determine the amount of cash that it should ask for as ransom.

Indicators of Compromise

MD5
Dfcd797a1ffdab6dbedafe190d0992ad
21723762c841b2377e06472dd9691da2
Bb159b6fe30e3c914feac5d4e1b85a61
543d1620ce976cb13fec190ccc1bc83a

File Names
doc_dlea podpisi.com
doc_dlea podpisi.rar
documenti_589965465_documenti.com
documenti_589965465_documenti.rar
documenti_589965465_doc.scr
doc_dlea podpisi.rar
неподтвержден 308853.scr
documenti dlea podpisi 05.08.2015.scr.exe
akt sverki za 17082015.scr

Mitigation

- Back up all of your files using an external memory device or a Cloud-based backup method.
- Use a strong security program that is fully up-to-date to intercept any threatening components.
- Avoid visiting websites considered unsafe, such as pornographic websites or websites with pirated content.
- Use a reliable anti-spam filter to ensure that spam emails with threatening file attachments never make it to your inbox.

Conclusion

Ransomware seems to become more rampant and advanced. New and old ones are being updated to try out new techniques, and this will probably become the trend of the future. This is why it is important to raise awareness about new ones that are discovered or old ones that are updated because it will help in deterring them and also prevent infections from taking place. This is not the end of this ransomware, and there will be more variants and modes of operation for the Shade Ransomware and they will only become more intelligent in the way that it ask for ransoms.

References

http://www.enigmasoftware.com/shaderansomware-removal/
http://www.securityweek.com/shade-ransomware-updated-backdoor-capabilities
https://support.kaspersky.com/viruses/common/10952#block0
https://securelist.com/blog/research/75645/shade-not-by-encryption-alone/

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