Satana Ransomware

This is a security alert for all TruShield clients, the financial services industry, and the community as a whole. We have learned of a new ransomware named Satana. This ransomware goes on the boot record and prevents the computer from starting.

About Satana Ransomware

Satana is a new ransomware that is a mix between Petya and Mischa ransomware. The name Satana means “devil” in Italian. Like most ransomware, Satana encrypts files on a computer. It is a relatively new ransomware and, according to Malwarebytes, it is a “malware-in-development” and will most likely evolve due to the fact that the current version contains a lot of bugs. This ransomware is similar to Petya in the way that the “dropper (packed in an FUD/crypter) writes to the beginning of the infected disk and the second mode encrypts the files one by one” as stated by Malwarebytes Labs. It uses both the methods at the same time to sabotage a user’s computer. Satana changes the MBR and encrypts it and the files that are encrypted are renamed as <email_address>_<original_name>. The encryption algorithm may be a block cipher or custom XOR based.

How does it work?

Once the ransomware is running, it will disappear, and it will hide under a different name in the %TEMP% folder. Depending on the account used for in installing Satana, it will always prompt the user to download the malicious file until they click yes. Once the action starts, the malicious code will be written to the beginning of disk. Malwarebytes Labs stated that this ransomware “announces everything that it does,” which is indicative of early stages of development.

After it installs and runs its malicious code, Satana then waits until the computer is rebooted to let the user know that they are infected. It won’t start; it will just show Satana’s ransom note. Then it will show a screen with the ransom note, like most ransomware. To communicate Satana uses a C&C address to send information about the user. The use of the C&C is not always necessary for encryption as it can encrypt offline, but the issue that arises from this is the fact that the key is lost. Some users who do decide to pay might not get “their files back if they (or the C&C) went offline when encryption happened” as stated by Malwarebytes Labs.

Satana’s Targets

The MBR is the first part targeted, then the following file extensions are targeted:

.bak	.doc	.jpg

.jpe	.txt	.tex
.dbf	.db	.xls
.cry	.xml	.vsd
.pdf	.csv	.bmp
.tif	.1cd	.tax
.gif	.gbr	.png
.mdb	.mdf	.sdf
.dwg	.dxf	.dgn
.stl	.gho	.v2i
.3ds	.ma	.ppt
.acc	.vpd	.odt
.ods	.rar	.zip
.7z	.cpp	.pas
.asm	Shadow backups	

Conclusion

This ransomware is a work in progress and, as mentioned above, seems to be employing the tactics of other ransomware. Satana is likely only going to improve, as the developers work on fixing the bugs that exist and getting some features working, such as the bitcoin wallet.

References

https://blog.malwarebytes.com/threat-analysis/2016/06/satana-ransomware/
http://news.softpedia.com/news/satana-ransomware-encrypts-your-boot-record-and-prevents-your-pc-from-starting-505933.shtml
http://www.securityweek.com/satana-ransomware-encrypts-mbr-and-user-files

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