PunkeyPOS Malware

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 variant of a point of sale malware (POS) that has been affecting around 200 terminals throughout the United States. This malware is known as PunkeyPOS and can steal credit card data.

About PunkeyPOS Malware

PunkeyPOS isn't new and was discovered last year in April of 2015, and its name is based on the 80s sitcom Punky Brewster. This malware belongs to the NewPOSthings family of malware due to the similarity in its functionality. This new variant was discovered by accident from Panda Security's PandaLabs unit. The PunkeyPOS malware can drop a keylogger to record keystrokes and is encrypted using AES, and then sends that data to the command and control server, to read the memory of the processes running on the system the malware uses RAMscraper.
This malware doesn't discriminate when it comes to Windows operating system; it works on them all. This POS malware is installed in the POS terminal and steals some personal identifiable information from bank cards, including account numbers and other sensitive information.
The unique thing about the malware is that it has the capability to differentiate between card data and irrelevant information not about a card. The card data that is useful is taken from process memory and is then encrypted and stored on a remote web server as stated by Panda Security. The encryption of the information allows hiding from network monitoring tools. The information collected is later sold to thieves to clone for fraudulent use.
According to PandaLabs most employees are tricked into installing the malware via social engineering, but this is not the only tactic that can be used to download this malware.

Conclusion and Mitigation

POS malware continues to be a threat and is always evolving. That's why it is important to have some safeguards in place to combats threats like these. The best practice against POS malware is to make sure that systems are always up to date.
Make sure that a defense-in-depth approach is taken to mitigate the risk and other monitoring tools. Since social engineering is one the ways to infect a system, make sure all personnel are aware of these threats to help combat the risk of infection.

References

http://www.infosecuritymagazine.com/news/punkeyposmalwaresetssightson/
https://www.trustwave.com/Resources/SpiderLabsBlog/NewPOSMalwareEmergesPunkey/?page=1&year=0&month=0

http://www.pandasecurity.com/mediacenter/malware/punkeypos/
http://www.infosecuritymagazine.com/news/punkeyposvariantslurpingdataus/

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