NETOP®
Remote Control
Secure Remote Management and Support

Netop

Protecting Your Point-Of-Sales System from Remote Malware Attacks

A Multi-tier, "Defense in Depth" Strategy for Securing Point of Sale Systems from Remote Access Attacks

Retailers are continuously being threatened by an array of malware aimed directly at point-of-sale (PoS) systems. This white paper includes an example of a threat that was designed to steal payment card data from retailers and provides techniques that retailers and POS suppliers can use to protect themselves and their customers from attacks conducted through remote access software.

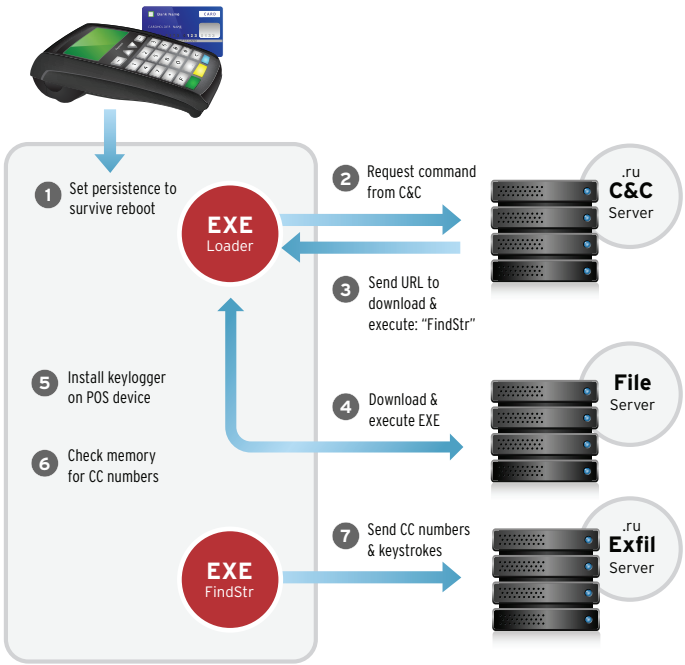
A Malware Progression

In March 2015, the Cisco Security Solutions team[1] identified a new Trojan program they called PoSeidon that skims credit card information from point-of-sale systems. This whitepaper explains how PoSeidon works, and provides techniques that retailers and POS suppliers can use to protect themselves and their customers from this threat, and from other, similar attacks conducted through remote access software.

WHAT IS POSEIDON?

PoSeidon is the name given to a new Trojan program that targets point-of-sale terminals, stealing consumer payment card data for use by criminals. Lucian Constantine of IDG New Service[2] described the malware this way:

> The CSS researchers have identified three malware components that are likely associated with PoSeidon: a keylogger, a loader and a memory scraper that also has keylogging functionality.
>
> The keylogger is designed to steal credentials for the LogMeIn remote access application. It deletes encrypted LogMeIn passwords and profiles that are stored in the system registry in order to force users to type them again, at which point it will capture them.
>
> The CSS researchers believe this keylogger is potentially used to steal remote access credentials that are needed to compromise point-of-sale systems and install PoSeidon. Past studies have showed that PoS terminals are typically compromised through stolen or brute-forced remote access credentials, as many of them are configured for remote technical support.
>
> Once the PoSeidon attackers get access to a PoS terminal, they install a component known as a loader. This component creates the registry keys needed to maintain the infection's persistence across system reboots and downloads another file called FindStr from a hard-coded list of command-and-control (C&C) servers.
>
> As its name implies, FindStr is used to find strings that match payment card numbers in the memory of running processes. The Trojan then verifies that the captured strings are actually credit card numbers by using an algorithm known as the Luhn formula, and uploads them to one of several command-and-control servers along with other data captured through its key logging functionality.



"...the attackers may have stolen LogMeIn credentials in order to remotely access the POS device (and perhaps many others with the same account) and install the POS malware."

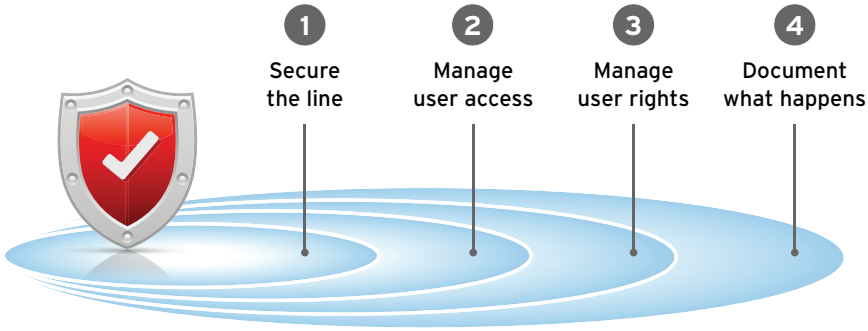
SAGIE DULCE, SECURITY RESEARCHER AT IMPERVA[3]

HOW CAN YOU DEFEND YOURSELF?

Defending against malware like PoSeidon is difficult. There is no silver-bullet to protect your network against the variety of tools, exploits and attacks criminals will throw against you. As a result, Netop recommends a defense-in-depth strategy for security. Because Point of Sale attacks often target remote access tools, it is vital your remote access and control strategies include multiple overlapping layers of defense and protection.

Netop has been supplying the retail industry with unparalleled security for remote access and remote control for nearly 30 years. With 24% of the world's top 100 retailers and 42% of the world's top banks using Netop Remote Control, you can trust our security has been tested and verified.

Netop's approach to security focuses on four overlapping strategies:



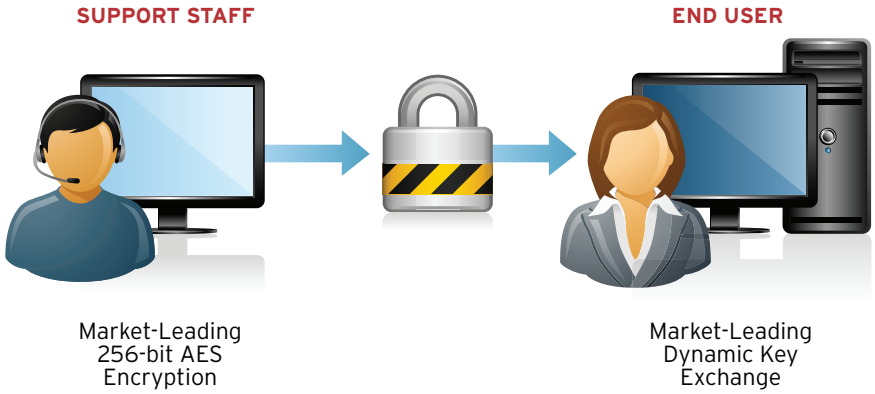
Spartan Stores strengthened their security and achieved a 30% increase in efficiency when they switched to Netop Remote Control

Spartan Stores

SECURE THE LINE

Secure remote access relies on strong encryption to ensure the confidentiality, integrity and authenticity of data being transmitted. Encryption is like a three legged stool. One weak leg and the stool collapses. Many remote access vendors provide high levels of encryption, but provide weak key exchange and message authentication, creating a dangerous risk of collapsing their encryption. Netop's approach to encryption is comprehensive:

- Data confidentiality is ensured with up to 256-bit AES (Advanced Encryption Standard)
- Data integrity is ensured with upt to 256-bit SHA HMAC (Secure Hash Standard or Keyed-Hash Message Authentication Codes)
- Data authenticity is ensured with a combination of 2048-bit Diffie Hellman key exchange and the 256-bit AES and 512-bit SHA

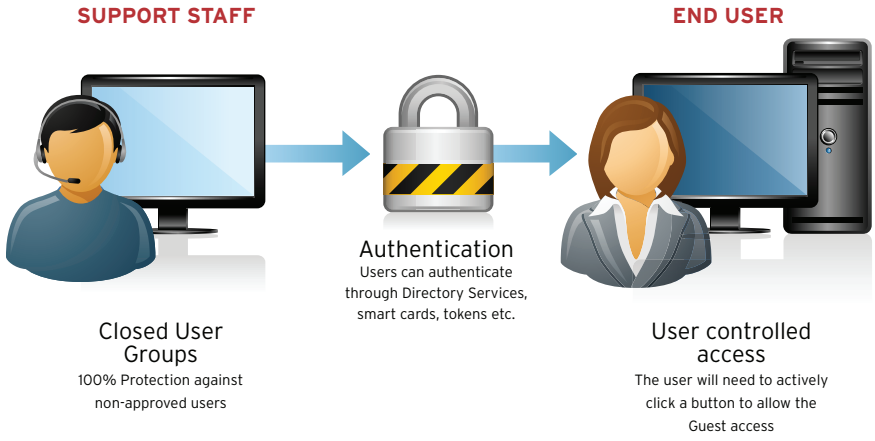


The Liquor Control Board of Ontario, one of Canada's largest retailers meets security standards with a remote support solution from Netop that provides centrally managed security, authentication and authorization for point of sale systems.

MANAGE USER ACCESS

Strong encryption is a crucial first step to securing data, but encryption alone is not sufficient to keep you safe. Managing user access is necessary to prevent unintended users from accessing your network and unencrypting the data with stolen credentials. Netop provides several options for managing user access that includes:

- Minimize Threat Vectors. Your network is being scanned continuously. Every public IP address, all your open ports, and any inbound firewall exceptions you've allowed are now threat vectors. Netop's WebConnect service provides Internet connectivity without open ports or inbound firewall exceptions. Within closed networks Netop can be configured to prevent devices from advertising connection details, preventing network browse requests and using specific IP address checks prior to making a connection. Using Netop's secure gateways, customers can provide a single secured access point into closed network segments without opening those devices to the Internet.
- Closed User Groups. Unique to Netop Remote Control, closed user groups provide protection against non-approved users by limiting communication to devices that have been pre-configured with a unique Closed User Group License. The Closed User Group is a highly effective mechanism for preventing outside parties from interacting with the systems in your network.
- Multi-Factor Authentication. Dual factor or multi factor authentication mitigates the threat of stolen or compromised passwords. Netop supports multi-factor authentication options including: RSA SecureID, Windows Azure, Radius servers, smart cards, tokens and others.
- User Controlled Access. For attended devices, Netop can be configured so that end-users must confirm and allow remote access before a remote session can be established. Even if user controlled access is not enforced, connection notifications can be configured to notify the local user upon, during, or after a session.

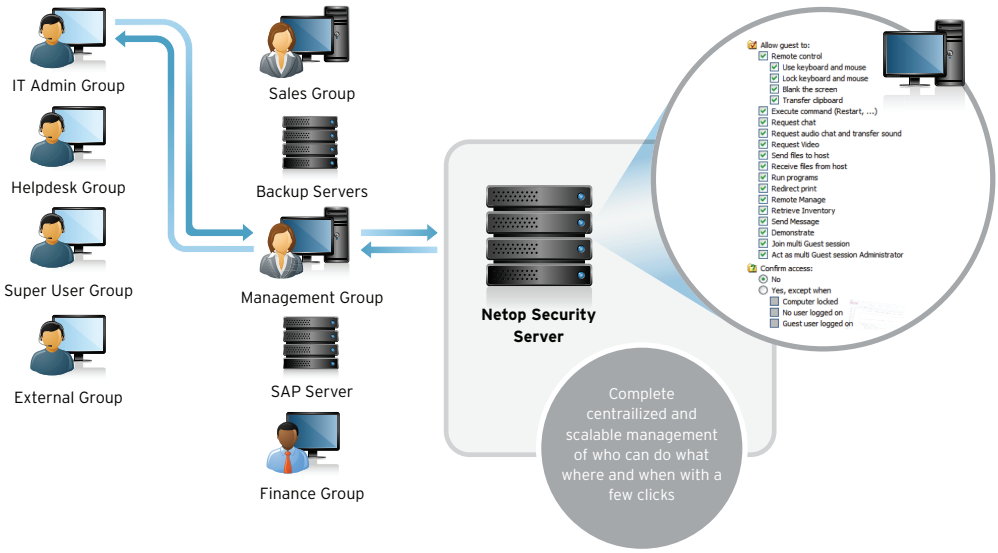


POS equipment vendor SIR Solutions turned to Netop for a cost-effective and secure way to support thousands of retail devices across hundreds of locations.

MANAGE USER RIGHTS

Securing remote access doesn't stop with encrypted traffic and authenticated users. Once a user has successfully accessed a networked device, managing their rights and permissions is the next step in maintaining your security.

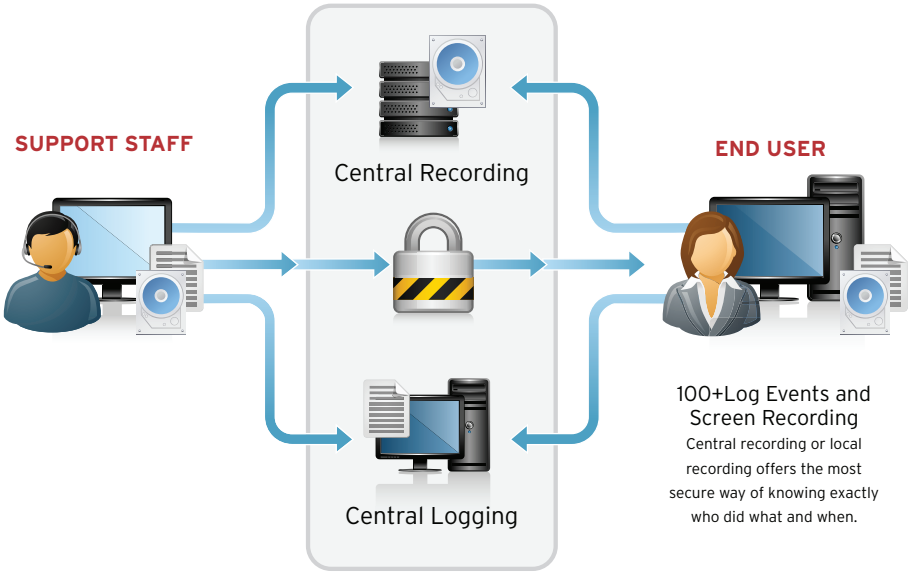
Netop provides a sophisticated system of role based access controls with centralized and scalable management of who can do what, where and when. Specific features including file transfer, remote keyboard and mouse control, monitoring, and system inventory can be turned on or off with the click of a button



Netop Remote Control offers cloud hosting or on premise options to meet your security needs.

DOCUMENT WHAT HAPPENS

The last line of defense against hackers and criminals is robust logging and activity histories. Having the ability to identify what happened, when it happened and who was involved is critical to mitigating ongoing attacks and cleaning up an attack that has been resolved. Netop Remote Control includes over 100 logable events and provides full screen recording if required. Logs and screen recordings can be stored locally or centrally. Systems can be configured to prevent connectivity if screen recording is unavailable or disabled.



CONCLUSION

Security matters. While no company can protect themselves against every form of attack, there are basic steps that retailers and system providers can take to safeguard customer data from PoSeidon and other forms of malware that attack point-of-sale systems through remote access software. Start by assessing the remote access solutions used at your company. Are you using general purpose remote access software, or a solution that is designed for PCI compliance and security like Netop Remote Control? Are you taking advantage of advanced security features like multi-factor authentication and closed user groups? If so, then you should be able to protect your company and your customers from PoSeidon. If not, talk to Netop about how to make your remote access system more secure.

ABOUT NETOP REMOTE CONTROL

Why do 24% of the world's top 100 retailers use Netop Remote Control? Because security matters. Netop is the most secure, trusted and scalable remote support software solution on the market today. We've been helping customers grow their enterprises with secure remote control and support for workstations, servers, embedded systems and mobile devices for 30 years.

REFERENCE LIST

1. Cisco Threat Research blog post by Talos Group dated March 20, 2015:
   http://blogs.cisco.com/security/talos/poseidon

2. PC World article dated March 23, 2015 by Lucian Constantine, IDG News Service:
   http://www.pcworld.com/article/2900552/new-malware-program-poseidon-targets-pointofsale-systems.html

3. IT Security Guru article dated March 23, 2015 by Dan Raywood:
   http://www.itsecurityguru.org/2015/03/23/poseidon-malware-poses-fresh-retail-threat

4. Netop Case Study: Spartan Stores Realizes 30% Efficiency Gain with Netop Remote Control
   http://www2.netop.com/spartancasestudy

5. Netop Case Study: POS Equipment Vendor Leverages Netop Remote Control to Support Thousands of Retail Devices Across Hundreds of Locations http://www2.netop.com/sir-solutions

6. Netop Case Study: Liquor Control Board of Ontario Securely Manages POS Systems with Netop
   http://www2.netop.com/LCBOCaseStudy