Kaspersky®
Embedded Systems
Security

Point of Threat or Point of Sale: Threats Targeting PoS Terminals

The world is only now becoming aware of the volume of threats targeting the very specialized computer data systems that are PoS (Point of Sale) terminals. An electronic kiosk or ticket vending machine may not superficially resemble an office workstation or home laptop, but these PoS terminals are just as vulnerable to cyberattack as any other intelligent processor-based machine. And, in some ways, they are under even greater threat.

The year 2014 saw a major incident that affected millions of US residents: cybercriminals gained access to confidential data concerning over 70 million customers of a large retail chain, and more than 40 million bank cards. Investigations showed that neither the payment processing system nor the company's servers had been compromised. The theft was conducted via infected cash registers and PoS terminals. Malware, installed by cybercriminals onto these devices, intercepted payment data which was openly stored in the RAM of the terminals.

The incident demonstrates that cybercriminals don't just closely follow trends in the evolution of payment handling though processing technologies and devices, but also continuously develop specialized malware designed to exploit these new developments and steal valuable financial data.

It would be unfair to imply that the problem of malware for PoS terminals wasn't addressed prior to these high-profile retail network hacking incidents. But up to this point, even though PoS malware had been employed regularly to attack enterprises since at least 2010, PoS cyberattacks had not caught the attention of the public and mass. In 2010, the discovery of Trojan-Spy.Win32.POS (a.k.a. CardStealer), which searched for payment card data on infected workstations and sent any information found to the cybercriminals' server, became worldwide news. Since then, not a year has passed without anti-malware experts discovering new variations of malware designed to steal payment data from PoS terminals.

These days, PoS terminal infection has gone way beyond 'pinpoint' attacks. With PoS technologies, cybercriminals have gained a new springboard for implementing threats, providing greater potential access to other people's money than ever before.

- 2010 — Trojan-Spy.Win32.POS (CardStealer)
- 2011 — Backdoor.Win32.Desty (Dexter)
- 2012 — Trojan-Spy.Win32.Vskim (vSkimmer)
- 2013 — BlackPOS (modified CardStealer)
- 2013 — Trojan.Win32.Fsysn (Chewbacca)
- 2014 — Backdoor.Win32.Backoff (Backoff)
- 2015 — LogPOS, Punkey, POSeydon, FindPOS

Figure #2: Some of the commands received by Dexter from its command server

General-purpose Operating Systems vs. Specific-purpose Malware

The nefarious activities of cybercriminals are made easier by the fact that PoS devices are essentially ordinary computers that can be (and, in the case of small businesses, often are used) for 'general-purpose' work, like surfing the internet and checking emails. These activities can potentially allow cybercriminals remote access to the devices.

A malicious program detected in 2012 and given the name Dexter was designed to steal bank card details by attacking PoS terminals running under operating systems utilizing Windows programs. The malware injected its code into the iexplore.exe system process, read the contents of RAM and searched for payment data sufficient to create a fake plastic card, i.e. cardholder name, expiration date and card number (including issuer code), card class and type, account number, etc. It then uploaded the accumulated information to a remote server controlled by the cybercriminals.

During its lifetime, Dexter compromised hundreds of PoS systems in well-known retail, hotel and restaurant chains, as well as in private parking facilities. It's a safe bet that most of the PoS systems affected ran under Windows XP.

Another example is the infamous threat known as Backoff, a PoS Trojan designed to steal payment card information from payment terminals. Like Dexter, this malware read the PoS terminal's RAM, searching for payment card data. In addition, some Backoff versions included a keystroke interception component (keylogger), presumably to cater for cases where the infected computer was a workstation (with the user entering stealable information through a keyboard) rather than a PoS terminal.

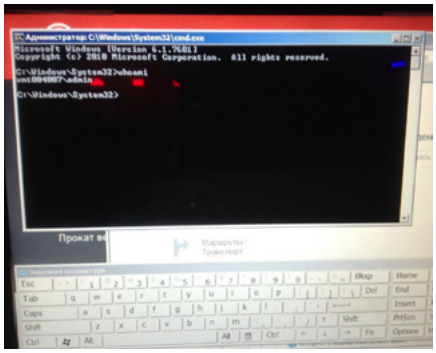


Figure #3: Example of parking meter app exploitation

Points of Sale in Non-trade Related Environments

Today, PoS devices aren't just found in retail chains, supermarkets and hotels. On every street there are terminals used to pay for parking, or user-friendly 'kiosks' for charging your mobile device. Airports and railway terminals currently feature a variety of ticket machines and information kiosks, and cinemas now offer terminals for automated seat reservation and ticket purchase. In clinics and public offices, there are electronic queue machines. Nowadays, even public toilets may be equipped with payment terminals.

Unfortunately, not all these devices are sufficiently protected against cybercrime. In the summer of 2014, Kaspersky Lab experts discovered flaws in the configuration software of bicycle-parking terminals that made it possible to access the device's memory, resulting in the ability to compromise user data (including payment data).

An application running under a Windows operating system enabled the bike-parking station user to register and see the location of other parking stations, as well as bars, cafés and other objects. This information is displayed using a Google widget built into the product. While the user can't minimize the full-screen application or leave its window, the application has a configuration flaw which makes it possible to compromise the device: there are links – 'Report an Error', 'Confidentiality' and 'Terms of Use' – which launch the Internet Explorer browser when tapped by the user.

The possibilities opened up by such configuration flaws allow for exploitation by cybercriminals. For example, attackers can extract the administrator password openly stored in the memory. They can also obtain access to the bike-parking meter app's stored memory. It may be possible to extract users' personal data from the stored data dump, including full names, email addresses and phone numbers – a database of verified addresses and phone numbers is always particularly valuable on the cybercrime 'black market.' An attacker can also install a keystroke logger, intercepting all data entered on the keyboard and sending it to a remote server, or even implement an attack scenario resulting in the collection of still more data by cybercriminals, achieved by including additional data entry fields.

Global Expertise in Kaspersky Lab Technologies

The results of independent tests regularly confirm the effectiveness of Kaspersky Lab products. In 2016, the company ranked first among security solution developers based on the TOP 3 metric. According to the results of 78 different tests and reviews carried out by respected testing organizations worldwide, Kaspersky Lab solutions were ranked among the top three in 90% of all results, and took the number one position 55 times. These tests verify that Kaspersky Lab leads the industry when it comes to the quality of protection we provide.

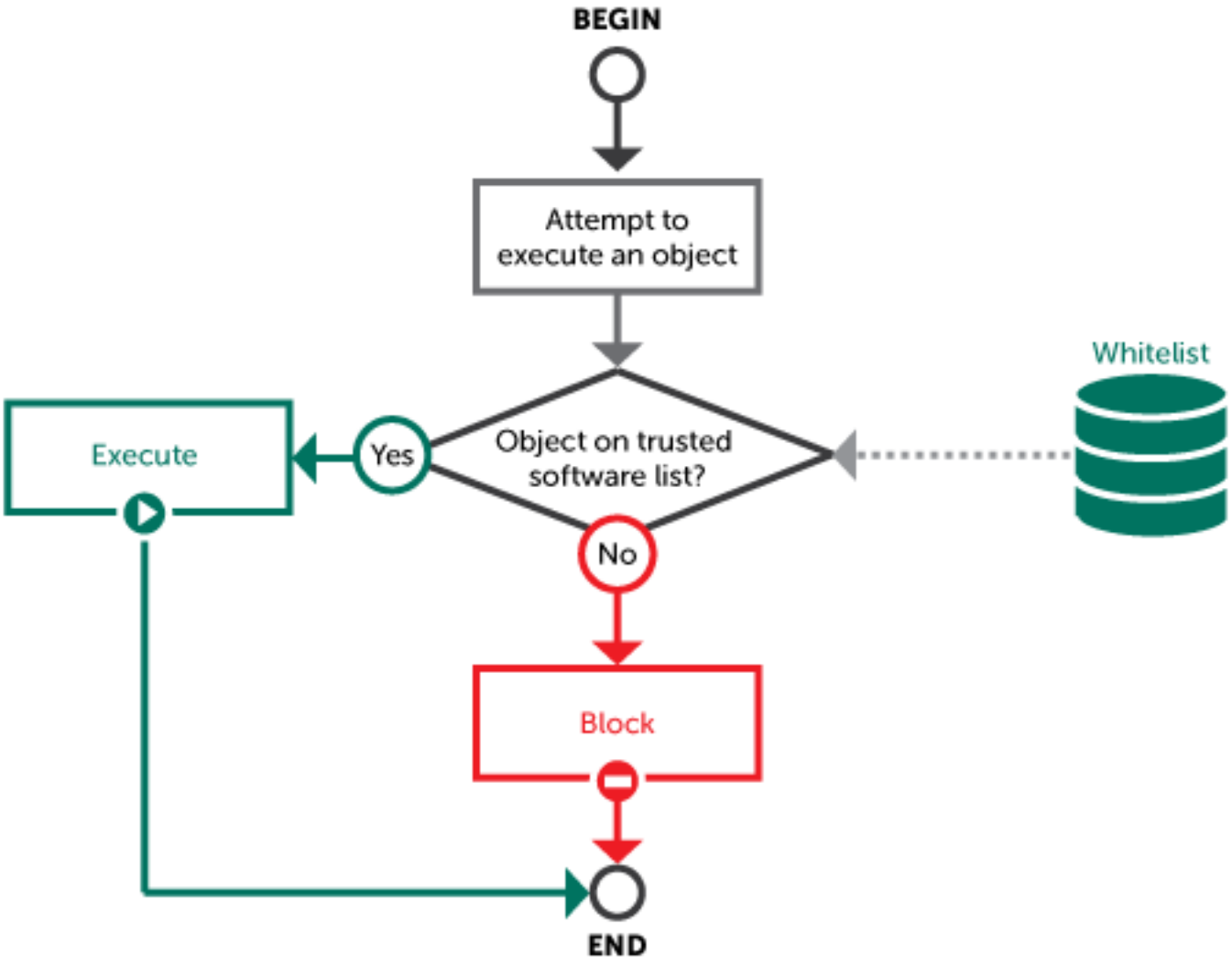
Point-of-sale Security

PoS device operating systems are very like workstation operating systems, and vulnerable to the same threats. So even if a terminal doesn't encounter a custom-designed Trojan, there's always the risk of infection from ordinary desktop OS malware – just as effective at putting the PoS device out of operation and causing financial damage. That's why Kaspersky Lab's security solution for embedded systems includes anti-malware technologies providing protection against all types of malicious programs, including those which, while not specifically targeting PoS devices, can make their way into the operating system and trigger a Denial of Service incident.

In the world of traditional workstations and servers, the https://securelist.com/analysis/publications/57882/computing-securely-the-trusted-environment-concept/ paradigm and the whitelisting technology behind it have long been widely used. Default Deny and whitelisting can ensure that only the software needed to perform business-related tasks is allowed to run on corporate computers.

Kaspersky Lab experts have developed Kaspersky Embedded Systems Security, a security solution for PoS and ATM systems, which has been designed specifically for this type of device and which includes Default Deny technologies to protect embedded operating systems from the threats targeting them. When the security solution is installed onto a terminal, the execution of all applications on that terminal follows this scenario:

- The operating system initiates the execution of an application, script or library.
- The product's security system verifies whether the application, script or library is trusted, using a whitelist of trusted applications and components.
- The operating system initiates the execution of an application, script or library.



About Kaspersky Lab

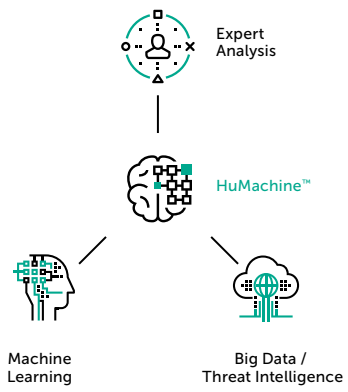
Kaspersky Lab is a global cybersecurity company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats.

Over 400 million users are protected by Kaspersky Lab technologies and we help 270,000 corporate clients protect what matters most to them.

Learn more at
http://www.kaspersky.com/enterprise

Default Deny technologies make it possible to create a PoS terminal OS environment that only permits the execution of software applications necessary to performing the terminal's limited range of tasks. As a result, any attempt by cybercriminals to execute arbitrary code in the running OS of a terminal protected by Default Deny technologies will be unsuccessful.

Financial organizations and businesses that operate PoS terminals should be more vigilant when protecting their devices, giving consideration not only to the security of hardware components but also to operating systems and the entirety of the overall networked IT infrastructure. To achieve this level of advanced protection, organizations can utilize both security tools that have long been in place on corporate networks, and dedicated solutions for embedded systems. In the unlikely event of a security breach, it's essential to provide a rapid response and to work in conjunction with law-enforcement agencies and security companies to track the source of the problem.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com