



# NJCCIC

NJ CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL

## Incident: New Jersey Business Infected with Point-of-Sale Malware

October 28, 2015

TLP: WHITE | *On October 13, 2015 a New Jersey business discovered an infection of a point-of-sale (PoS) malware variant, detected by antivirus software as lanst.exe, one of many variants commonly known as Dexter.* It remains definitively unclear how an employee's laptop was initially exposed to the malware, though the NJCCIC assesses it was likely via a spear-phishing or drive-by download tactic. In this instance, the malware exploited the business' lack of two-factor authentication and 'flat' network—meaning there was no segregation between various components—as well as outdated computer systems and weak security policies. There is currently no evidence that any business or customer data was exfiltrated from the network.

### Summary

During routine maintenance, a system administrator observed that a Windows security event log had been deleted by a known user account. It was determined that prior to the incident, an authorized system administrator logged on to a user's laptop with administrator privileges to troubleshoot an issue that was preventing the user from printing. This particular laptop, used for marketing purposes, was potentially compromised with malware, though the initial infection vector remains unknown. Once the system administrator logged in with privileges, the threat actor was able to infiltrate the network by using the administrator's legitimate credentials and install the Dexter malware onto a server within the internal network. Once executed, the Dexter malware, inclusive of the lanst.exe file, scanned and mapped the network architecture and identified key components. The malware then compiled network topography, encrypted user passwords, and customer transaction data into individual folders in preparation for exfiltration.

Last week, researchers from cybersecurity firm FireEye revealed a cybercrime group known as FIN5 that used similar tactics to steal 150,000 credit card numbers from a casino in 2014. This group used a Tornhull backdoor and virtual private network (VPN) client, Flipside, to maintain persistence on the infected network, even after mitigation steps were taken. Again, in this case, two-factor authentication was the effective remediation.

### Indicators

Known indicators of compromise (IoC) from this incident include:

- Deleted or modified Windows event logs
- Corrupted pfs.exe (print file server) on local computers as well as server locations
- Excessive or off-hours remote logon sessions from trusted users

### Mitigation

- Implement [two-factor authentication](#) on all enterprise applications that require user credentials and provide access to sensitive information, including email, cloud solutions, and remote access tools.
- Isolate compromised computers from the network to rectify potential or confirmed infections.
- When responding to incidents, ensure IT staff uses accounts with limited administrator privileges.
- Ensure updates and security patches are deployed to all computer systems, devices, software, web-browsers, and plugins as soon as possible.

Traffic Light Protocol: **WHITE** information may be distributed without restriction.

- 
- Conduct a comprehensive audit to identify all devices that comprise the network, and remove unsupported or outdated devices.
  - Implement the principle of least privilege when creating or modifying a user account.
  - Limit VPN access to essential personnel only.
  - Download and install an uncorrupted copy of the pfs.exe file. Ensure that the downloaded executable is not compromised by checking the hashcode against a known good copy of the file.
  - ‘Subnet’ or segregate components of the network to restrict the ability of attackers to move laterally once one system is compromised.
  - Establish strong password complexity and length requirements, ideally ten characters consisting of using upper and lowercase letters, numbers, and special characters.
  - Implement periodic, mandatory password resets that prevent the use of old passwords.
  - Conduct regular cybersecurity education and awareness trainings with all employees on topics such as spear-phishing, social engineering, safe-browsing, and information security policies.
  - For a comprehensive list of mitigation strategies and details on current PoS malware variants, refer to the NJCCIC’s relevant analysis: [Point-of-Sale Malware Continued Threat to Businesses and Consumers](#).

## Dexter Overview

Dexter was first discovered in December 2012 by Seculert and remains one of the most prevalent variants of PoS malware, infecting machines via phishing emails, drive-by downloads, or by exploiting default system access credentials. Dexter targets vulnerabilities in Windows XP, Windows 7, and Windows Server 2003 operating systems. After infecting the target PoS system, Dexter parses memory dumps for PoS processes that contain Track 1 and Track 2 card data. It simultaneously monitors changes in the system and maintains persistence by injecting itself into the Windows Explorer executable file and preventing session termination. It then communicates with a command-and-control (C2) server over HTTP (port 80) to transmit the card data back to the hacker. Variants of Dexter include ‘Stardust’, ‘Millenium’, and ‘Revelation’.

## Dexter References

- For more information on Dexter PoS malware, please refer to the following open-source resources:
- Security Intelligence: [Protecting POS System From Dexter and Other Advanced Malware](#).
- Casino News: [FIN5 Hacking crew hits Jackpot, Steals 150,000 Credit Cards from Casino](#).
- Trustwave: [The Dexter Malware: Getting Your Hands Dirty](#).
- Volatility Labs: [Unpacking Dexter POS "Memory Dump Parsing" Malware](#).
- Fortinet: [How Dexter Steals Credit Card Information](#).

## Additional PoS Resources

- United States Secret Service, the Financial Services Information Sharing Analysis Center (FS-ISAC), and the Retail Cyber Intelligence Sharing Center (R-CISC): [Protecting Merchant Point of Sale Systems during the Holiday Season](#).
- US-CERT: [Malware Targeting Point of Sale System](#).

## Contact Information

To report an incident, or if your organization would like to learn more about the NJCCIC, contact a Cyber Liaison Officer at [NJCCIC@cyber.nj.gov](mailto:NJCCIC@cyber.nj.gov) or by calling 1-866-4- SAFE-NJ.