SECURITYWEEK NETWORK:

- Information Security News
- Infosec Island
- Suits and Spooks

Security Experts:

WRITE FOR US

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

- Subscribe (Free)
- Security White Papers
- ICS Cyber Security Conference
- Contact Us

- Malware & Threats
  - Vulnerabilities
  - Email Security
  - Virus & Malware
  - White Papers
  - Desktop Security
- Cybercrime
  - Cyberwarfare
  - Fraud & Identity Theft
  - Phishing
  - Malware
  - Tracking & Law Enforcement
  - Whitepapers
- Mobile & Wireless
  - Mobile Security
  - Wireless Security
- Risk & Compliance
  - Risk Management
  - Compliance
  - Privacy
  - Whitepapers
- Security Architecture
  - Cloud Security
  - Identity & Access
  - Data Protection
  - White Papers
  - Network Security
  - Application Security
- Management & Strategy

New PoS Trojan Steals Card Data, Intercepts Browser Requests

By SecurityWeek News on September 18, 2015

Researchers from anti-virus firm Dr.Web have discovered new malware designed to infect point-of-sale (PoS) terminals and capable of intercepting GET and POST requests sent from Web browsers on infected machines.

Dubbed **Trojan.MWZLesson**, the Trojan can modify the registry branch in charge with autorun on the infected PoS terminals, while also being able to check the device's RAM for credit card information, the security firm said.

All of the acquired bankcard data along with intercepted communication, including GET and POST requests, is sent to the command and control server. However, the malware is also capable of executing a series of commands, which makes it even more dangerous.

Dr.Web explains in a blog post that the commands supported by the Trojan include CMD (forward the command to the interpreter - cmd.exe), UPDATE, FIND (search for documents using a mask), DDoS (mount an HTTP Flood attack), and rate (set a time interval for communication with the command and control server).

Additionally, Trojan.MWZLesson supports a LOADER command, which allows it to download and run a file (dll—using the regsrv tool, vbs—using the wscript tool, exe—run directly), and communicates with the server over the HTTP protocol. Packages sent by the malware are not encrypted, but the server ignores any package that does not include a special cookie parameter.

According to Dr.Web researchers, the Trojan borrows code from previously discovered Dexter malware that targets PoS terminals, while its architecture looks similar to that of Neutrino, though it is rather a downsized version of the latter.

The Trojan can also steal data from the Microsoft Mail application, as well as FTP login credentials, the experts said.

POS terminals are often targeted by cybercriminals. Over the past year, many different malware types have been found targeting Point-of-Sale systems, including PoSeidon, Spark, Poslogr, and POSCLOUD, to name a few. MalumPOS, is another recently discovered PoS threat found targeting Oracle Micros PoS Systems, while NitlovePOS malware was discovered by FireEye spreading through an email spam campaign.

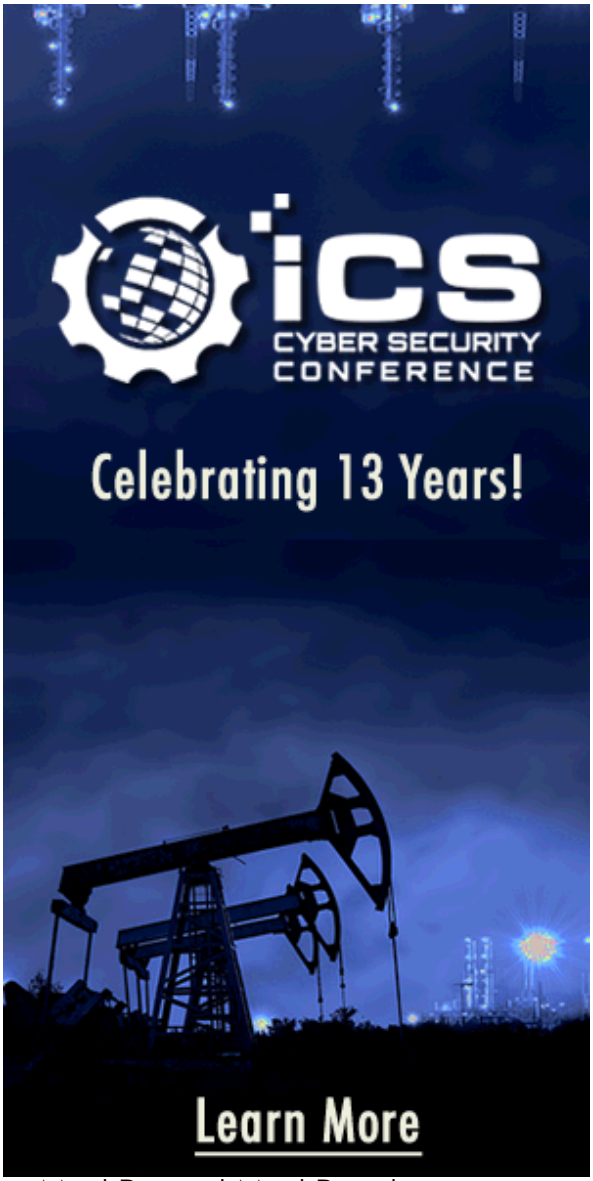
Other PoS malware familes include vSkimmer, Dexter, Backoff, LusyPOS and Dump Memory Grabber.

In its annual Global Threat Intel Report, security firm CrowdStrike noted that criminals have been increasingly turning to ready-to-use PoS malware kits in the cyber-underground. According to Adam Meyers, vice president of intelligence at CrowdStrike, the price of these kits varied depending on their complexity, with some going for tens of dollars and others costing in the hundreds or thousands.

Previous Columns by SecurityWeek News:

New PoS Trojan Steals Card Data, Intercepts Browser Requests
G DATA Launches Security Messaging App for Android
Apple Patches Vulnerabilities in iOS, OS X, iTunes, Xcode
IT Teams Question Security of App Containers: Survey
iOS 9 Resolves Hijacking via AirDrop Vulnerability

Tags:
Desktop Security NEWS & INDUSTRY Malware Cybercrime



Most Recent Most Read

- New PoS Trojan Steals Card Data, Intercepts Browser Requests
- Event Preview: Suits and Spooks at the Wingtip Club - San Francisco
- Critical Flaw in Bugzilla Could Expose Zero-Day Bugs
- Dutch Nab Hackers Setting Ransoms to Unlock Computers
- G DATA Launches Security Messaging App for Android
- Apple Patches Vulnerabilities in iOS, OS X, iTunes, Xcode
- IT Teams Question Security of App Containers: Survey
- Cultivate a Talent Pipeline While Bridging the Cybersecurity Resource Gap
- Russian Hackers Target Industrial Control Systems: US Intel Chief
- U.S. Defense Contractors Targeted by Chinese Threat Group

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security
Application Security
Smart Device Security

Security Community

- IT Security Newsletters
- IT Security White Papers
- Suits and Spooks
- ICS Cyber Security Conference
- CISO Forum
- InfosecIsland.Com

Stay Intouch

- Twitter
- Facebook
- LinkedIn Group
- Cyber Weapon Discussion Group
- RSS Feed
- Submit Tip
- Security Intelligence Group

About SecurityWeek

- Team
- Advertising
- Events
- Writing Opportunities
- Feedback
- Contact Us