

Prolific Cybercrime Gang Favors Legit Login Credentials

DR darkreading.com/analytics/prolific-cybercrime-gang-favors-legit-login-credentials/d/d-id/1322645

Kelly Jackson Higgins

October 13, 2015



[Analytics](#)

4 MIN READ

ARTICLE

FireEye researchers shed more light on infamous cybercriminals associated with RawPOS malware. and christen it 'FIN5.'

October 14, 2015

FIREEYE CYBER DEFENSE SUMMIT -- Washington, D.C. -- No 0days. No spearphishing, either: The cybercriminal group tied to numerous payment card breaches [including Goodwill](#) and best known by its so-called "RawPOS" malware employed legitimate user credentials to access its targets' networks.

Researchers at FireEye here today shared their recent findings on this prolific and long-running cybercrime gang that has been the subject of multiple [Visa security alerts](#) to merchants. The RawPOS memory scraper malware has been infecting the lodging industry in epidemic proportions over the past year, and is considered one of the first memory scrapers to target point-of-sale systems.

FireEye has dubbed the cybercrime gang FIN5. "One of the most unique things about FIN5 is that in every intrusion we responded to where FIN5 has been active, legitimate access was identified. They had valid user credentials to remotely log into the network," said Barry Vengerik, principal threat analyst at FireEye. "No sexy zero-days, no remote exploits -- not even spearphishing. They had credentials from somewhere."

FIN5, which earlier this year was profiled by researchers at Trend Micro and has been in action since at least 2008, uses real credentials from the victim organization's virtual private network, Remote Desktop Protocol, Citrix, or VNC. Vengerik says the attackers got those credentials via third parties associated with the victims' POS systems.

"Most of the maintenance and administration of POS systems are done by a third party -- the maintenance, patching, troubleshooting" is done remotely via those credentials, he said.

"FIN5 maintained access to two or more payment processor networks primarily for the goal of logging into and accessing their customers' environments," he said. "It's a textbook case of a lateral compromise between companies based on trust."

FireEye last year investigated a massive breach at a casino hotel with 1,200 endpoints that suffered losses to more than 150,000 payment cards. Vengerik declined to name the hotel.

The casino attackers used a stolen VPN account to gain access, said Emmanuel Jean-Georges, senior consultant with FireEye's Mandiant.

FIN5 uses a tool called GET2 Penetrator, a brute force scanning tool that looks for remote login and hard-coded credentials, as well as a free tool called EssentialNet that scans the victim's network to give the attackers "the lay of the land," Vengerik said.

RawPOS pulls information from a POS system's memory. The malware includes several components, FireEye found: Duebrew, which ensures the malware remains on the infected Windows machine, even when it gets rebooted; Fiendcry, a memory scraper that grabs the payment card data; Driftwood, which encodes the stolen payment card information to hide it from analysis tools.

Another unusual feature of FIN5's operation is that the malware code is "well-commented," Vengerik said. "That's incredibly rare in malware, the author taking time to comment on the code and to show what section of code is doing what," he said. It's like a secure development lifecycle approach, he noted.

The release notes for the Driftwood code are written in an older Russian language character set, the researchers showed.

Why would the malware author actively comment on the code? "It points to a possible ecosystem -- for advertising or support" of the malware as a product, Vengerik told *Dark Reading*.

FireEye says the attackers first target the Active Directory to get to the card data, and use tools such as Windows Credentials Editor in their quest for legit credentials. They also created several custom tools for covering their tracks and cleaning up any traces of the malware, as well as proxy tools for accessing segregated network segments.

"They also encoded hard kill-times into most of their malware for a hard end date" of the attack, he said.

Trend Micro earlier this year noted how RawPOS was able to evolve to target various types of POS software. "Aside from being multi-component, RawPOS is notable for its support for multiple PoS software. Since business establishments would have different PoS software, attackers have modified RawPOS' code to support multiple PoS software over time," Trend Micro researchers wrote in [a blog post in late April](#).

Meanwhile, FireEye today also announced that it has partnered with Visa Inc. to power a new threat intelligence service for merchants and card issuers. The so-called Visa Threat Intelligence service is the first product under a newly forged partnership between Visa and FireEye.

"We want to offer faster, actionable intelligence to our constituents," said Mark Nelson, senior vice president of risk products at Visa.

Vulnerabilities/ThreatsThreat Intelligence

Keep up with the latest cybersecurity threats, newly-discovered vulnerabilities, data breach information, and emerging trends. Delivered daily or weekly right to your email inbox.

[Subscribe](#)