PoS Attacks Net Crooks 20 Million Stolen Bank Cards

By Tom Spring

Published: 2016-04-21 · Archived: 2026-04-05 18:03:40 UTC

A report released Thursday shines a bright light on point-of-sales system attack targeting hospitality and retail businesses that could have earned cyber crooks a $400 million payday.

In a storyline that rivals an episode of The Sopranos, researchers at FireEye documented the heist of bank card data from 20 million individuals that involved a complex web of crooks that may have netted hackers more than $100 million since 2014.

In conjunction with recently acquired Isight Partners, FireEye released a report Thursday that shines a bright light on point-of-sale system attacks targeting hospitality and retail businesses. The attacks, outlined in a report "Follow the Money," began in 2014 and are ongoing by a group FireEye is calling FIN6.

What is unique about the report is that FireEye's research goes beyond the technical, such as attack vectors and exploits used in PoS attacks. Instead, the report reveals the often undocumented way criminals work together to penetrate a network, install malware, plant shellcode, steal bank card data and sell it on the black market.

FireEye said, PoS systems are increasingly being targeted. That's because as more U.S. companies snuff out point of sale malware by deploying chip-and-PIN bankcard technology, attackers are rushing to exploit existing magnetic strip card systems still vulnerable to malware.

FIN6, FireEye said, is tied to more than 20 million stolen credit cards. In the course of its investigation, FireEye observed the cards showing up on an underground marketplace being sold for $21 a card – potentially delivering a $400 million payday.

Researchers say that FIN6 most likely initially worked with a group that offered malware as a service to essentially shop for PoS victims. Initial infections were of random computers via indiscriminate spam campaigns that included malicious Word macros.

FireEye identified Grabnew (also known as Vawtrek and Neverquest) as the primary malware planted on computers and used to capture credentials on infected systems. Those credentials, FireEye suspects, were then cross referenced with previously stolen data supplied by other third parties to help identify optimum PoS targets.

"FIN6's use of Grabnew, or credentials collected by Grabnew, is not altogether surprising and possibly points to a cybercrime support ecosystem that opens doors to threat actors capable of lateral movement and more damaging activities," wrote FireEye.

After gaining access to systems, FIN6 used a Metasploit PowerShell module to download and execute shellcode to set up a local listener that would execute shellcode received over a specific port, according the FireEye. FIN6 then used downloaders Hardtack and Shipbread to embolden its attack and establish backdoor access to compromised

environment. Both tools, according researchers, were configured to connect to remote command and control servers giving attackers remote control of compromised systems, according to FireEye.

After FIN6 cyber criminals have penetrated computers tied to PoS systems they deploy Trinity (aka FrameworkPOS) PoS malware to steal magnetic-stripe payment card data. FireEye was able to document FIN6 criminals' ability to amass 20 million bank card records from one incident. FireEye said the cards stolen, in that instance, were predominantly from U.S. victims.

Once Trinity identifies bank card data, "it copies and encodes it to a local file in a subdirectory of the c:\windows\ directory while attempting to conceal these files with .dll or .chm extensions," according to the report. In one particular case, researchers say, FIN6 compromised and deployed Trinity on 2,000 systems, resulting in millions of exposed cards.

So what does a crook do with millions hot credit card numbers that are losing value every hour after they have been stolen? Sell them on the black market. That's when FIN6 calls in the expertise of a digital fence that deals with laundering stolen credit card data.

"In reality, the shop would typically only make a fraction of this figure ($400 million), since not all the data would be sold (laundering stolen cards is typically much harder than stealing them), buyers want the newest data they can get (data that has been on the shop for a while loses its value), and the shop offers discounts based on various criteria. Still, a fraction of $400 million is a significant sum," according to FireEye's report.

The operators of the underground card shops, FireEye said, hung online shingles in geographies where law enforcement is ill equipped to track them down or within anonymous networks such as Tor.
