Data Breach® TODAY
Prevention. Response. Notification.

http://www.databreachtoday.com/

Anti-Malware , ATM Fraud , Fraud

Malware Warning: Banks, Customers, ATMs Under Fire

Beware Cash-Out Attacks, Banking Trojans Via Malvertising and POS Memory-Scraping Malware

Mathew J. Schwartz (euroinfosec) • September 25, 2015 1 Comment

Security experts warn about a trio of malware threats that are designed to steal cash, online banking credentials as well as payment-card data from point-of-sale devices.

See Also: Cloud-based Privileged Identity Management for the Modern Enterprise

The new warnings center on three types of unrelated malicious code. For starters, malware has been spotted in the wild that is being used to drain cash from ATMs in Mexico, although security researchers warn that it could go global. The Shifu banking Trojan, meanwhile, has moved beyond Japan and is now being used to target customers of four U.K. banks. Finally, the notorious Neutrino crimeware has gotten an upgrade, allowing it to scrape POS device memory and steal payment-card data.

Cash-Out Attacks: GreenDispenser Malware

The newly spotted ATM cash-out malware has been dubbed "GreenDispenser," by cybersecurity firm Proofpoint, which says that while it has only seen the malware used to "cash out" ATMs in Mexico, the malicious code could soon spread to other countries (see *Authorities Detain Suspects in ATM Cash-Out*).

"GreenDispenser provides an attacker [with] the ability to walk up to an infected ATM and drain its cash vault," Proofpoint security researcher Thoufique Haq says in a blog post. "When installed, GreenDispenser may display an 'out of service' message on the ATM, but attackers who enter the correct PIN codes can then drain the ATM's cash vault and erase GreenDispenser using a deep-delete process, leaving little if any trace of how the ATM was robbed." A deep delete in this case means that the malware not only deletes itself, but also employs Microsoft's sdelete to make it much more difficult for any malware-related bits and bytes to be recovered via later digital forensic analysis.

The malware resembles the PadPin - a.k.a. Tyupkin - ATM malware that first surfaced in March 2014, and which could be used to make an ATM dispense all of its money, in what's known as a "jackpotting" or cash-out attack, Proofpoint says, adding that it believes that installing the malware requires physical access to an ATM (see *Easy Access Fuels ATM Attacks*).

Like PadPin, GreenDispenser is designed to interact with a set of standard programming interfaces, or APIs, that are built into most ATM host computers and components, known as XFS - which stands for "extensions for financial services" (see *Hacking ATMs: No Malware Required*).

But this new generation of ATM malware includes a number of tricks designed to disguise the presence of the malware, as well as prevent unauthorized thieves from using it to drain ATMs. For starters, any ATM that gets infected with GreenDispenser displays an "out of order message." Proofpoint says it has recovered samples of the malware that display a message either in grammatically challenged English - "We regret this ATM is temporary out of service" - or else in Spanish: *Temporalmente fuera de servicio*.

Based on Proofpoint's GreenDispenser teardown, it found that the malware was coded to only run if the year was 2015, and the month was earlier than September, thus suggesting that this might have been a test run, or else designed to avoid detection. To cash out the ATM, meanwhile, an attacker must enter a preset PIN, scan a QR code displayed on screen, and then enter a second PIN, after which they can instruct the ATM to dispense all of its money, or tell the malware to delete itself.

"We suspect that the attacker has an application that can run on a mobile phone with functionality to scan the barcode and derive the second PIN - a two-factor authentication of sorts," Proofpoint says. "This feature ensures that only an authorized individual has the ability to perform the heist."

Malvertising Attacks Now Serve Shifu Banking Trojan

The banking malware known as Shifu - after the Japanese word for thief - has returned, and is no longer just targeting Japanese banks. In a Sept. 25 blog post, the French researcher who maintains the Malware Don't Need Coffee blog, who goes by the name Kafeine, warns that in recent days, the malware has been spotted targeting four U.K. banks: Bank of Scotland, Halifax, Lloyds Bank and TSB. To date, it's not clear how many banking customers' systems may have been infected with the malware.

In August, IBM reported that it first saw Shifu being used for in-the-wild attacks, beginning at least in April. But Kafeine says that after cross-referencing his findings on Sept. 24 with security researchers at Fox-IT and Dell SecureWorks, they found that collectively they had been tracking Shifu since September 2014. "We were using a 'non public' name to talk about it," Kafeine reports.

In the United Kingdom, Shifu is being spread via malvertising attacks, Kafeine says. To date, it's not clear if these attacks are part of a campaign that has successfully served malicious advertising via multiple popular sites, including dating sites Plenty of Fish and Match.com (see *Match.com Suspends UK Ads After Malware Attacks*).

In those U.K. malvertising attacks, systems were first infected with a crimeware toolkit called Angler Exploit Kit, which is designed to exploit known vulnerabilities (see *Why Malvertising Attacks Won't Stop*). In many of the prior U.K. attacks, Angler then installed Bedep ad-fraud malware as well as CryptoWall ransomware, which can encrypt systems and then demand a ransom to unlock them (see *FBI Alert: $18 Million in Ransomware Losses*).

Angler EK
Shifu call Home
Gain a Degree in Art & Design
Online Courses accredited by the University of Hertfordshire
FIND OUT MORE

Kafeine
@kafeine

Follow

Shifu <3 Great Britain
malware.dontneedcoffee.com/2015/09/shifu-…

4:06 AM - 25 Sep 2015

25 ★ 19

The Shifu malvertising attack campaign is quite similar, reports Kafeine, except that after U.K.-based systems get infected with Angler and Bedep, the attack doesn't go down the ad-fraud path. Instead, Shifu malware gets installed - as well as an Apache Web server - and then begins ransacking infected systems for anything of potential value to attackers, from online banking credentials, to cryptocurrency wallets, to point-of-sale configuration information, for example if it successfully infects a POS device.

Neutrino Malware Targets POS Devices

Meanwhile, upgraded Neutrino - a.k.a. Kasidet - crimeware toolkit malware is also now targeting POS devices, report researchers RonJay Caragay and Michael Marcos at information security firm Trend Micro. Previously, the crimeware toolkit - which competes with Angler - was known in part for its ability to facilitate distributed denial of service attacks.

In a Sept. 24 blog post, Trend Micro says that new research has found that Neutrino version 2.9, which debuted in March, included for the first time the ability to steal credit card details - by "scraping" the RAM of infected devices, via a feature referred to as "ccsearch." But in July, it says, a cracked edition of version 3.6 of Neutrino - which had previously only been available via cybercrime markets, for a price - was leaked onto underground forums, meaning it is now available for free.

Trend Micro - which is headquartered in Japan - reports that based on data gathered from its users' antivirus software, the greatest number of recent Neutrino infections have been seen in Japan, followed by the United Kingdom, Taiwan, France and the United States. It warns that it saw a 1,288 percent spike in related malware detections between May and June, even before the malware became available for free in July.

Neutrino, the security firm says, is designed to infect Windows systems via removable drives and network folders, and gives attackers the ability to use capture keystrokes and screenshots from infected systems, copy clipboard data, launch a remote shell, launch DDoS attacks, as well as steal data from POS device memory (see *New Alerts About POS Malware Risks*).

"Upgrading old malware to include POS RAM-scraping capabilities is a new technique in the threat landscape, but it's not surprising, given how lucrative stolen payment card data is," Trend Micro says. Furthermore, the release of the cracked, free version of Neutrino continues to lower the barriers to entry for payment-card-seeking criminals. "Scoring this tool is basically finding a valuable tool in a bargain bin and ending up not having to even pay for it," Trend Micro says.

About the Author

Mathew J. Schwartz

Executive Editor, DataBreachToday & Europe

Schwartz is an award-winning journalist with two decades of experience in magazines, newspapers and electronic media. He has covered the information security and privacy sector throughout his career. Before joining Information Security Media Group in 2014, where he now serves as the Executive Editor, DataBreachToday and for European news coverage, Schwartz was the information security beat reporter for InformationWeek and a frequent contributor to DarkReading, amongst other publications. He lives in Scotland.