-

Situational Intelligence Report

February 2019

FIN6 Cybercrime Group Expands Threat to eCommerce Merchants

Summary

FIN6 is a financially motivated threat actor group in operation since at least 2015. The group has compromised multiple point-of-sale (POS) environments using the TRINITY POS (aka FrameworkPOS) malware. In September 2017, forensic investigations of several undisclosed entities revealed evidence that FIN6 actors changed to target card-not-present (CNP) data when they could not deploy their malware in the POS environment. Evidence shows that FIN6 injected malicious code into the merchants' eCommerce environment, placing skimming malware on the victims' checkout pages. **Based on Visa Payment Fraud Disruption's (PFD) analysis of eCommerce compromises throughout 2018, FIN6's focus on the CNP environment has only amplified, suggesting that the cybercrime group has fully incorporated targeting CNP environments into their criminal methodology.**

The majority of eCommerce compromises reported in 2018 involved direct targeting of vulnerabilities within the eCommerce website itself. As one of the more sophisticated groups targeting eCommerce merchants, FIN6 brings their POS compromise approach to the emerging threat landscape of CNP breaches. FIN6 targets companies, using phishing emails in an attempt to infect the targeted victim's network. The actors then move through the network to identify POS and eCommerce environments. PFD assesses that the increased focus of a sophisticated cybercrime group, such as FIN6, on eCommerce environments is a broader representation of the overall cybercriminal focus on the CNP space.

Recent Activities

At the end of 2018, Visa Payment Intelligence analysts discovered that FIN6 actors targeted multiple high value eCommerce merchants with malicious documents that contained links to a malicious server that allowed the execution of PowerShell scripts, granting the attackers direct access to the merchants' networks. The PowerShell scripts were only present in memory, and did not download additional files to the user's machine, making it difficult for the victim to detect. The FIN6 actors were able to utilize this access to move through the merchant's networks to access the eCommerce environment, and specifically the payment servers. A full investigation of these compromises show that the FIN6 actors specifically targeted the eCommerce networks and did not exploit them opportunistically.

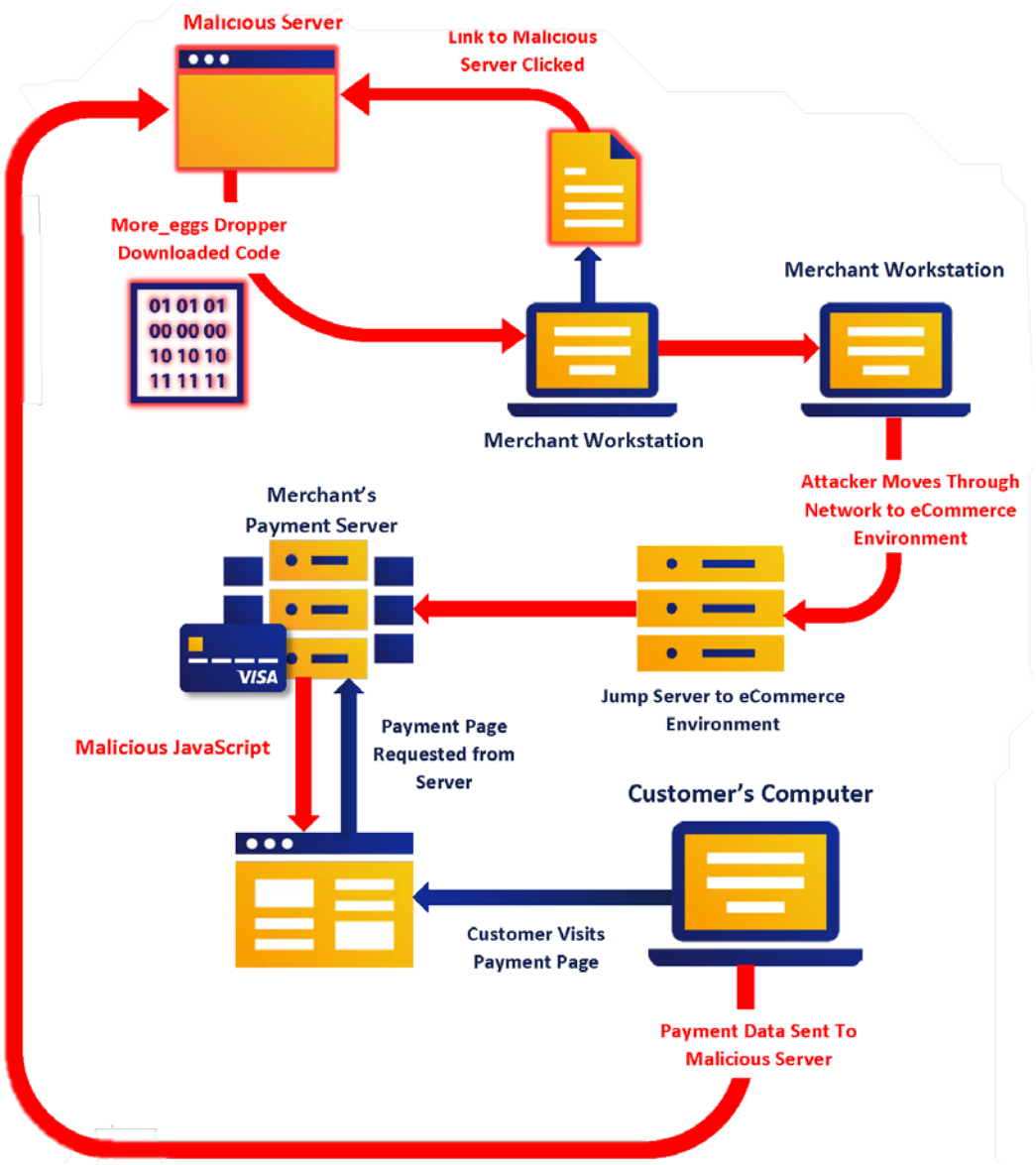

Figure 1 - FIN6 eCommerce Attack Flow

Tactics, Techniques, and Procedures (TTPs)

Initial Compromise

FIN6 employs a multitude of tactics within the initial phase of their operations. In the most recent compromises attributed to FIN6, forensic investigators identified the use of malicious documents to infect victims with malware known as *More_Eggs (aka Terra Loader)* that is used to launch malicious scripts on the infected machine.

Maintain Access

FIN6 establishes a foothold within a victim's environment by leveraging various payloads, such as components of the Metasploit Framework (e.g., Meterpreter, *JSPSPY* and *CmdSQL*), or through a

specialized version of the *AMMYY* remote administration tool (RAT) known as *FlawedAmmyy*. In the most recent cases, attackers then establish persistent access to the victim's network using Meterpreter related code, allowing the attackers to maintain a remote connection to the infected system.

Internal Reconnaissance

FIN6 uses legitimate publicly available tools to map the internal network and conduct reconnaissance. During the reconnaissance phase, the actors gather information on systems running SQL Database Server instances and dump schemas for multiple databases and SQL user accounts. The actors also target network credentials using a malware family known as *Stealer One* (see below in the section *Technical Analysis and Indicators of Compromise*). Additionally, FIN6 employs legitimate administrative tools, such as:

- Microsoft's built-in SQL querying tool (osql.exe)
- Query Express (a free, portable graphical SQL client)
- AdFind (a free command-line tool for querying Active Directory)
- ProcDump (a Microsoft SysInternals command-line utility used to perform analysis of running processes).

Escalate Privileges

Once FIN6's accesses are established with preferred backdoors, they use additional public utilities, such as Windows *Credentials Editor* and Metasploit-related tools, for privilege escalation and credential harvesting.

Move Laterally/Maintain Presence

Capitalizing on data acquired via internal reconnaissance, FIN6 relies on credentials stolen from various systems (e.g. usernames and password hashes) for lateral movement. Investigations show that FIN6 relies on PowerShell scripts and Meterpreter based shells to maintain access to and move laterally through the network (see below in the section *Technical Analysis and Indicators of Compromise*).

Technical Analysis and Indicators of Compromise (IOCs)

Malicious Files – *Stealer One*

Stealer One is a credential stealer, first observed by industry forensic investigators in March 2017. The malware targets a variety of applications, including email clients, web browsers, FTP clients, and other file transfer utilities.

Observed File Name:	46602.txt
SHA256:	4b914bc94c453d88ee82545ff6184491e8b100b6d9a3d0316a2b656187e4fb6a
DNS Request(s):	static.akamaitechnologies[.]kz (185.180.198[.]110)
HTTP Request(s):	hxxps://static.akamaitechnologies[.]kz/sonemone/version.php
Notes:	Stealer One (aka SONE or InfoStealer) Malware

Observed File Name:	8632.txt
SHA256:	59cbd46db5f28536872bf7f7dd86da0a5ef1e147ff2418c37fc037ab9ed5e34c
Authenticode Signature Block	**Signature verification**: **Signed file, verified signature** **Signing date**: 03/05/2018 **Signers:** 223647473 (MJO TM LTD) **Certificate SHA-1 Thumbprint**: E1E086A9B6C1614470A94A515AEA1D372E1640A9 **Certificate Serial Number**: 56 E1 98 80 2B 37 C7 09 54 81 67 2B 7B 58 21 F4
DNS Request(s):	static.akamaitechnologies[.]kz (185.180.198[.]110)
HTTP Request(s):	hxxps://static.akamaitechnologies[.]kz/sonemone/version.php
Notes:	Stealer One (aka SONE or InfoStealer) Malware

VirusTotal Intelligence (VTI)

Visa discovered seven other files on VirusTotal which are signed with the same "223647473 (MJO TM LTD)" certificate, suggesting these files are controlled by the same cybercrime group.

MD5 Hash	File Description
e1bf80ef5fb111b087b8c172a38c0b23	*More_Eggs (aka Terra Loader)* Malware (Bot Version - 3.0)
b4dcb80246769a6b291a4c7e98a380bd	*More_Eggs (aka Terra Loader)* Malware
e526722fdd276e56fdd932f3d0e72cbb	TeamViewer Component
cbf0d3faef2e51798ef838a238855bdf	TeamViewer Component
388e3854f7ceb64b0c931eeceab29295	TeamViewer Component
bdd2c72c1fcf7712cd66b98cf0f1cc18	Metasploit Shellcode Loader 94.130.52[.]230:443
4376a330323789c6cc1591bbe737ff7e	*Stealer One* (aka *SONE* or *InfoStealer*) Malware

Encoded PowerShell Commands

Visa analyzed a number of encoded PowerShell commands identified in recent FIN6 activity and determined the majority are related to Metasploit activity, including:

Metasploit Bind TCP Stager (different local ports were observed)
Metasploit Reverse TCP Stager – 46.4.113[.]237:443
Metasploit Reverse HTTPS Stager – 185.154.52[.]140:443

Network IOCs

Malicious C2 IPs
185.180.198[.]110:443
46.4.113[.]237:443
185.154.52[.]140:443
94.130.52[.]230:443
185.159.82[.]78:443

Malicious C2 Domains
static.akamaitechnologies[.]kz
contactlistsagregator[.]com
teamviewer[.]com
onlinemail[.]kz

Malicious HTTPS Activity
hxxps://static.akamaitechnologies[.]kz/sonemone/version.php
hxxps://contactlistsagregator[.]com/j2378745678674623/ajax.php
hxxps://onlinemail[.]kz/apison215/version.php

More_Eggs Network IOCs

In addition to the C2 information provided, which can change, below are some network IOCs that can be used to detect *More_Eggs* beaconing out of the network:

Connectivity Check
The malware checks network connectivity by sending an HTTP HEAD (GET in some new versions) request to the following legitimate URL:

- hxxp://www[.]w3[.]org/1999/XSL/Format

Sleep Function
The malware issues an HTTP GET request to the following Google public DNS IP, which takes a few seconds to complete, causing the program to pause its activity temporarily. This is used as a method to avoid detection, by delaying further exploitation:

- hxxp://8.8.8[.]8/<Random Path>
- **User-Agent**: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)

Recommendations & Additional Resources

Visa recommends clients take the following actions to mitigate against these threats:

- **Institute recurring checks in local networks for IOCs provided in this report.**
- **Verify the implementation of required security patches:** Payment Card Industry Data Security Standard (PCI DSS) requires that all system components and software are protected from known vulnerabilities by installing security patches. Visit the Payment Card Industry Security Standards Council (PCI SSC) website for more information.
- **Regularly scan and test eCommerce sites for vulnerabilities or malware.** Hire a trusted professional or service provider with a reputation of security to secure the eCommerce environment. Ask questions and require a report of what was done. Trust, but verify the steps taken by the company you hire.
- **Consider using a fully-hosted checkout solution** where customers enter their payment details on another webpage hosted by that checkout solution, separate from the merchant's site. This is the most secure way to protect the merchant and their customers from eCommerce skimming malware. Hosted checkout forms embedded inline on the merchant's checkout page, such as Visa Checkout, are another secure option.
- **Use a Payment Card Industry Data Security Standard (PCI DSS) validated third-party service provider** to store, process or transmit cardholder data. Criminals commonly target merchant websites that process payment data. When merchants use a validated and secure service provider, risk exposure for CNP fraud and compromise decreases. A list of validated, registered service providers is available on the Global Registry of Service Providers.
- **Comply consistently with industry security standards**, such as the Payment Card Industry Data Security Standard (PCI DSS), including the PCI Best Practices for Securing e-Commerce, January 2017.

- **Set up a Web Application Firewall** to block suspicious and malicious requests from reaching the website. There are options that are free, simple to use, and practical for small merchants.
- **Limit access to the administrative portal** and accounts to those who need them.
- **Require strong administrative passwords** (use a password manager for best results) and enable two-factor authentication.
- **Regularly ensure shopping cart, other services, and all software are upgraded or patched** to the latest versions to keep attackers out.
- **Monitor for suspicious activity**—create and regularly check logs and receive alerts if changes to the site are made.
- **Ensure staff are trained in security best practices** and follow the designated procedures**.**

If a merchant suspects a compromise, they should contact their acquiring bank immediately for guidance on next steps and to ensure compliance with all Visa investigation and compliance guidelines. For more information, refer to the What to Do If Compromised (WTDIC) guide.

Additional Resources

Visa eCommerce Malware Webinar

Visa Merchant Library

PCI Best Practices for Securing e-Commerce, January 2017

PCI How-to Guide for Incident Management

PCI Data Security Standard

Contact Information

For more information, please contact paymentintelligence@visa.com

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com
- Europe: Datacompromise@visa.com
- Latin America & Caribbean: LACFraudInvestigations@visa.com
- U.S. and Canada: USFraudControl@visa.com

Disclaimer:

This report is intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. Visa is not responsible for your use of the information contained in this report (including errors, omissions, or non-timeliness of any kind) or any assumptions or conclusions you may draw from it. Dissemination or redistribution of PFD products without express permission is strictly prohibited.