

FOLLOW THE MONEY:

DISSECTING THE OPERATIONS
OF THE CYBER CRIME GROUP FIN6

SS					
	Primary Account No. (19 digits max.)	Name (26 alphanumeric characters max.)	Expiration Date (YY/MM) Service Code	No. of Characters 4 3	No. of Characters

CONTENTS

Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6	3
FIN6	4
Gaining Access - Indiscriminate or Intentional?	5
FIN6 - Getting the Job Done	6
Underground Card Shops - Following the Money	9
Conclusion	11



FOLLOW THE MONEY:

DISSECTING THE OPERATIONS OF THE CYBER CRIME GROUP FIN6

Reports on payment card intrusions and theft are often fragmentary. The focus is on various pieces of the attack and less about capturing the end-to-end cycle of compromise, data theft, illicit sale and use. The full scope of attacker activity traditionally occurs beyond the view of any one group of investigators. Incident response teams may have visibility into the technical aspects of the breach itself, while cyber crime researchers monitor the movement and sale of stolen data in the criminal underground.

FireEye Threat Intelligence and iSIGHT Partners recently combined our research to illuminate the activities of one particular threat group: FIN6. This combined insight has provided unique and extensive visibility into FIN6's operations, from initial intrusion to the methods used to navigate the victims' networks to the sale of the stolen payment card data in an underground marketplace. In this report, we describe FIN6's activities and tactics, techniques and procedures (TTPs), and provide a glimpse into the criminal ecosystem that supports the "payoff" for their operations.


FIN6

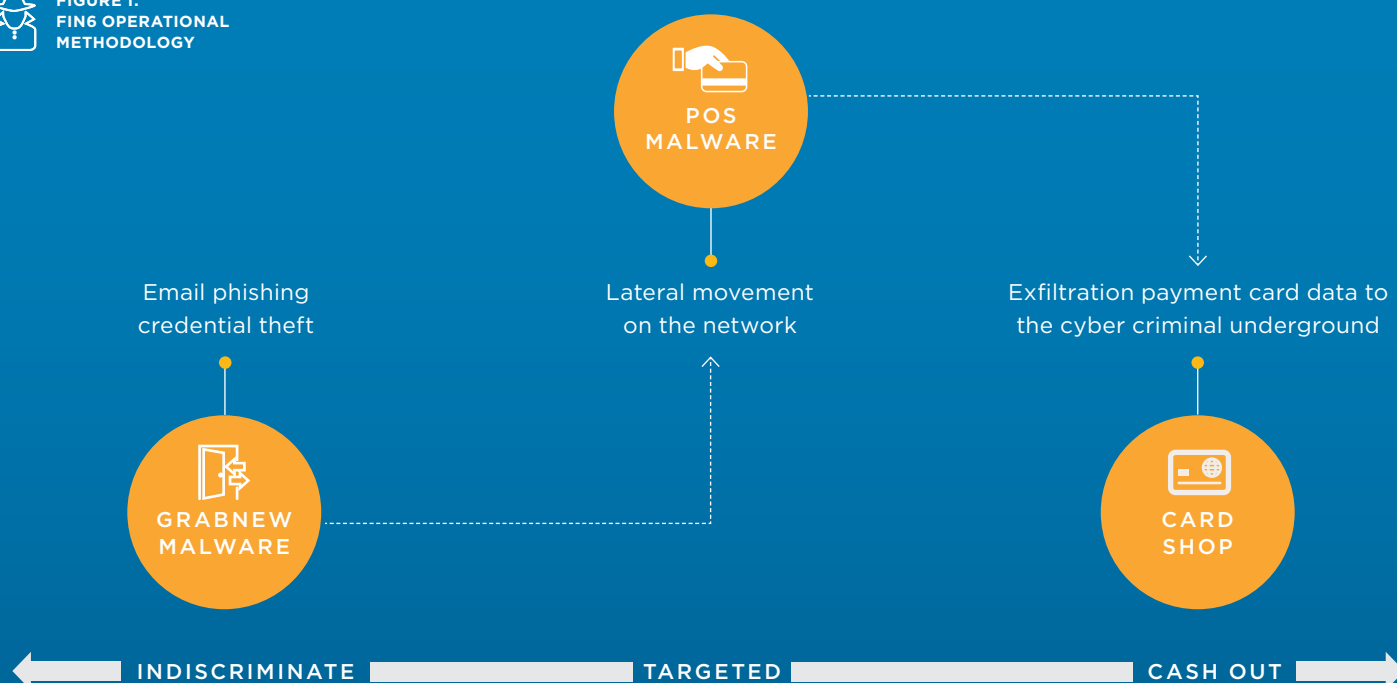
FIN6 is a cyber criminal group intent on stealing payment card data for monetization. In 2015, FireEye Threat Intelligence supported several Mandiant Consulting investigations in the hospitality and retail sectors where FIN6 actors had aggressively targeted and compromised point-of-sale (POS) systems, making off with millions of payment card numbers. Through iSIGHT, we learned that the payment card numbers stolen by FIN6 were sold on a “card shop” — an underground criminal marketplace used to sell or exchange payment card data. Figure 1 illustrates what we believe to be FIN6’s typical operational methodology.



FIREEYE INTELLIGENCE TRACKS

targeted Financial threats (known as “FIN” groups) capable of using a wide range of tools and tactics during their computer network intrusions. These groups employ a high level of planning, organization and task management to accomplish their goals. The threat actors generally target a particular demographic or type of organization, and their goal is financial gain from the data they steal. They may profit through direct sale of stolen data (such as payment cards or personally identifiable information), unauthorized transfer of funds (such as with stolen bank account or bank routing credentials); or insider trading (based on the theft of non-public business information).

 **FIGURE 1:**
FIN6 OPERATIONAL
METHODOLOGY





GRABNEW, ALSO KNOWN AS NEVERQUEST AND VAWTRAK, emerged around 2013 and since then has been consistently and indiscriminately spread through massive spam campaigns. We typically differentiate between threat actors who indiscriminately distribute malware and threat actors who use malware selectively. GRABNEW itself is a credential-stealing backdoor with form-grabbing capabilities and the ability to inject code into specific web pages to, for example, mimic a valid login prompt for a financial institution to facilitate banking fraud. In some cases, the presence of GRABNEW malware has overlapped with the spread of POS malware such as PoSeidon, a variant of the Backoff POS malware.

GAINING ACCESS


INDISCRIMINATE OR INTENTIONAL?

It's not entirely clear how FIN6 initially compromises victims. In Mandiant's investigations, FIN6 already possessed valid credentials to each victim network and used those credentials to initiate further intrusion activity.¹ In one case, GRABNEW malware was found on a victim computer that FIN6 later used in its operations. We suspect that the computer was originally compromised with GRABNEW by a separate threat actor, who used GRABNEW to capture valid user credentials. FIN6 may have obtained those credentials (through purchase or trade) and used them for its operations.

FIN6's use of GRABNEW, or credentials collected by GRABNEW, is not altogether surprising and possibly points to a cyber crime support ecosystem that opens doors to threat actors capable of lateral movement and more damaging activities. Previously, we observed another FIN group — FIN2 — leverage several existing Citadel compromises to deploy their custom tools and expand within a network to compromise payment card systems. Likewise, Proofpoint recently observed GRABNEW variants leading to downloads of POS malware known as AbaddonPOS.

¹ When investigating an intrusion, it may be challenging to determine the initial method of compromise — the means through which a threat group first gained access to a victim network. While in some cases evidence may point to a spear-phishing attack or exploit execution, in other cases little to no forensic evidence of the original compromise remains.

After locating POS systems within the target's environment, FIN6 deployed POS malware that we call TRINITY.



FIN6

GETTING THE JOB DONE

All threat groups generally follow a broad operational framework known as the Attack Lifecycle. While the phases of the Attack Lifecycle — from initial compromise to privilege escalation to maintaining presence and completing the mission — are remarkably consistent, the specific TTPs used vary widely based on a group's skills, motivations and ultimate goals.

After gaining access with valid credentials, we observed FIN6 leveraging components of the Metasploit Framework to establish their foothold. For example, in one case, FIN6 used a Metasploit PowerShell module to download and execute shellcode and to set up a local listener that would execute shellcode received over a specific port. Similarly, FIN6 used at least two downloaders called HARDTACK and SHIPBREAD (apparent variations on Metasploit payloads) to establish backdoor access to the compromised environment. Both of these tools are configured to connect to remote command

and control (CnC) servers and download and execute shellcode. FIN6 generally used either registry run keys or Windows scheduled tasks in order to establish persistence for these tools.

Once their accesses were established with preferred backdoors, FIN6 used additional public utilities such as Windows Credentials Editor for privilege escalation and credential harvesting. Additional privilege escalation tools exploited Microsoft Windows vulnerabilities in an attempt to compromise privileged account credentials on various hosts. The tools targeted CVE-2013-3660, CVE-2011-2005 and CVE-2010-4398, all of which could allow local users to access kernel-level privileges.² Continuing their use of Metasploit-related tools, FIN6 also used Metasploit's PsExec NTDSGRAB module to obtain a copy of the Active Directory database (ntds.dit). Access to this file would allow them to extract password hashes from the file and crack them offline.

² These vulnerabilities have all been patched by Microsoft; Windows systems with up-to-date software and security patches should not be exploitable.

In addition to collecting credentials, FIN6 used publicly available tools to map the internal network and conduct reconnaissance against Active Directory, Structured Query Language (SQL) servers and NetBIOS. In particular, during the reconnaissance phase they gathered information on systems running SQL instances, dumping schemas for multiple databases and SQL user accounts. Specific tools used by FIN6 included Microsoft's built-in SQL querying tool (osql.exe), Query Express (a free, portable graphical SQL client capable of connecting to Microsoft SQL and Oracle databases) and AdFind, a free command-line tool for querying Active Directory. Over the course of one day, for example, the group targeted more than 900 SQL servers to dump reconnaissance information to support further operations.

Capitalizing on the acquired reconnaissance data, FIN6 began lateral movement using credentials stolen from various systems on which they gathered usernames and password hashes. They likely cracked these hashes outside of the target's network before using multiple sets of domain admin credentials in combination with remote command execution tools such as PsExec and Remote Command Executor (RemCom) throughout the rest of the lateral movement phase.

To maintain presence and support interactive access in the environment, FIN6 leveraged the publicly available Plink command-line utility (part of the PuTTY SSH and Telnet suite) to create SSH tunnels to CnC servers under their control. As shown in Figure 2, they used these SSH tunnels to route Remote Desktop Protocol (RDP) traffic and allow for interactive RDP sessions with systems in the target network.

After locating POS systems within the target's environment, FIN6 deployed POS malware that we call TRINITY (also known as FrameworkPOS), with Scheduled Tasks being used for persistence. TRINITY runs

continuously and targets system processes not listed in its accompanying process blacklist, seeking data that matches payment card track data. Once the malware identifies track 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. In one particular case — and as an example of scale — FIN6 compromised and deployed TRINITY on around 2,000 systems, resulting in millions of exposed cards.

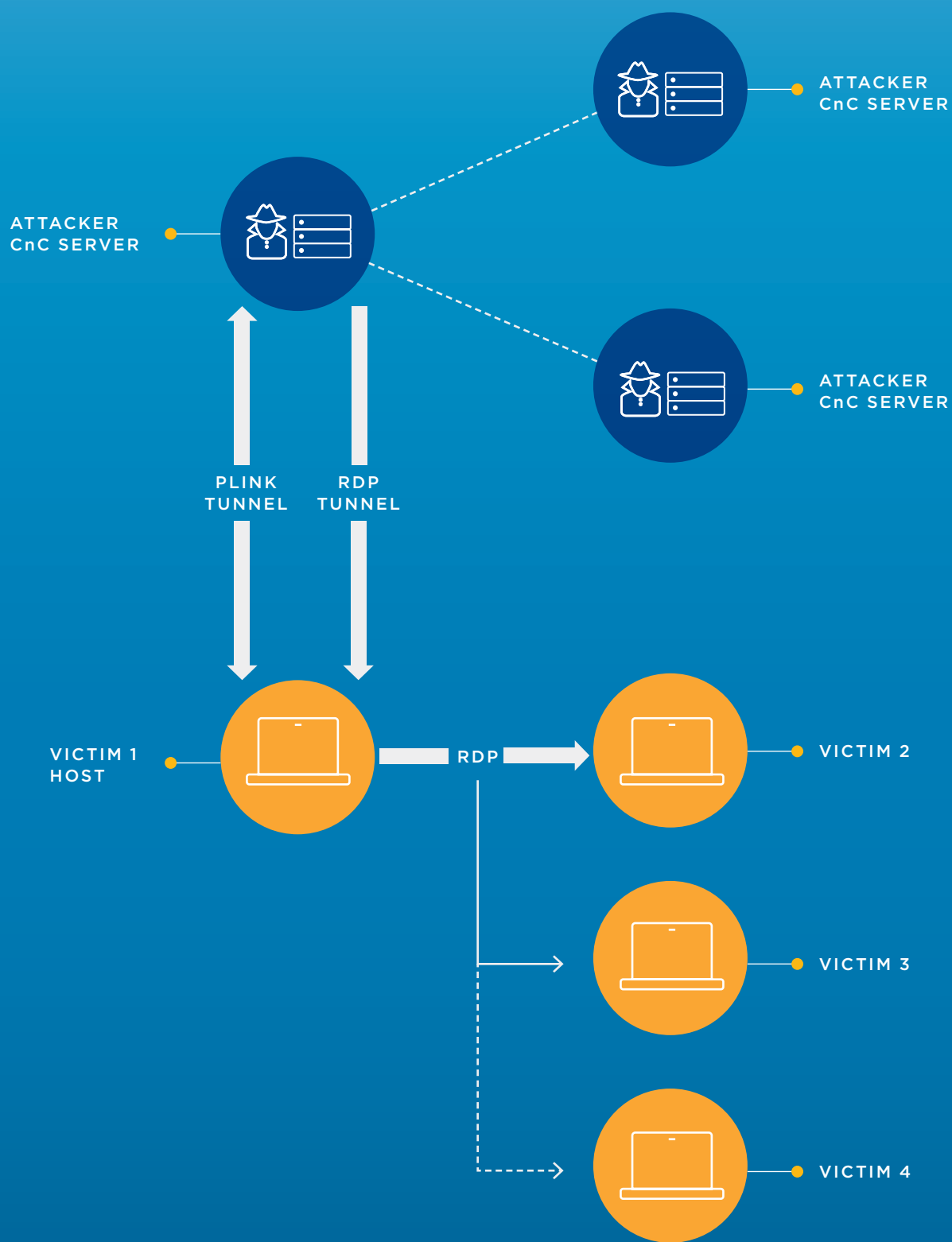


TRINITY IS POS MALWARE THAT ATTEMPTS TO LOCATE AND STEAL PAYMENT CARD DATA FROM MEMORY.

The malware first creates mutexes named m_number3 and MuTex-Check and exits if either already exists. The malware then continuously iterates over the current process listing and examines the memory space of each process. Processes with module names less than five characters are skipped, along with some specific process names that are unlikely to contain payment card information. TRINITY logs captured data to disk, typically to a file in %WINDIR%\temp or %WINDIR%\help. The malware encodes the data with a simple substitution cipher and single-byte XOR using the 0xAA key.

Finally, to move the stolen payment card data out of the environment, FIN6 used a script to systematically iterate through a list of compromised POS systems, copying the harvested track data files to a numbered "log" file before removing the original data files. They then compressed the log files into a ZIP archive and moved the archive through the environment to an intermediary system and then to a staging system. From the staging system, they then copied the stolen data to external CnC servers under their control using the FTP command line utility. In another case, FIN6 used an alternative extraction method to upload payment card data to a public file sharing service.

FIGURE 2: NETWORK DIAGRAM SHOWING FIN6 PLINK SSH TUNNEL USED TO ROUTE RDP TRAFFIC TO VICTIM COMPUTERS





Our analysis of the data sold through this underground vendor indicates that FIN6's compromises are highly profitable to the actors involved, potentially resulting in extensive fraud losses.

UNDERGROUND CARD SHOPS

FOLLOWING THE MONEY

Using iSIGHT Partners' collected intelligence, we discovered that the stolen payment card data from these intrusions were sold in an underground card shop. This particular shop is advertised on multiple underground cyber crime forums and has offered diverse criminals access to millions of stolen payment cards on a regular basis. This closes the loop on the "lifecycle" of cyber criminal activity and exemplifies one of the final stages of cyber crime actors monetizing their stolen data.

We have identified stolen data from several of FIN6's victims being sold by this vendor as far back as 2014. This connection means that data

stolen by FIN6 has almost certainly ended up in the hands of fraud operators across the world, as they buy and exploit payment cards from the underground shop. In each case, the stolen data began appearing in the shop within six months of the FIN6 breach. While the amount of data sold through the shop varies by breach, in some cases more than 10 million cards associated with a specific FIN6-linked breach have been identified on the shop. After being posted, much of the stolen card data is quickly purchased for exploitation. Along with the data we have linked to FIN6, this underground shop has sold data from millions of other cards, which may be linked to breaches perpetrated by other threat actors.



UNDERGROUND COMMUNITIES DEALING IN STOLEN CARD DATA EXIST ACROSS THE world and are a major facilitator of money laundering operations. A large number of these communities take the form of illicit e-commerce sites called “card shops” or “dump shops” (criminals refer to stolen card-present transaction data as “dumps”). These shops allow their clientele to use a web-based platform to sort through data on thousands or millions of payment cards and purchase exactly the types they want based on their money laundering capabilities. These data are then added to the client’s cart for checkout, similar to a legitimate website. Subsequently, customers use the card information they have purchased for many different money laundering schemes, such as buying and reselling gift cards or electronics.

Our analysis of the data sold through this underground vendor indicates that FIN6’s compromises are highly profitable to the actors involved, potentially resulting in extensive fraud losses. For instance, in one FIN6-linked breach the vendor was advertising nearly 20 million cards. These cards were predominantly from the United States and selling for an average of \$21. So the total return for the shop — if all the data was sold at full price — could have been about \$400 million.

In reality, the shop would typically only make a fraction of this figure 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. In turn, cyber

criminals purchasing the data would expect to make more than they paid for the cards by conducting fraudulent transactions using those cards.

Not all of the data sold on this particular card shop has been tied to an identified compromise or specific cyber criminal group. Additionally, as is often the case with prominent cyber criminal vendors, it is not yet clear how the operators of the underground site are linked to the actors who steal the data the shop sells. The vendor has sold large amounts of card data with varied characteristics, so it is possible the shop operators maintain relationships with more than one data provider. FIN6 members could include some of the operators behind this shop; alternately, FIN6 could be selling stolen data to the operators of this site.

CONCLUSION

Good threat intelligence comes from a combination of factors. It requires visibility into the threat landscape, including both a broad view (the ability to identify activity across a range of countries, industries and organizations) and a deep view (the ability to gather detailed information about how threat actors operate). It also requires skilled analysts who are able to review, fuse and understand the available data.

In this case, the combined intelligence from FireEye, Mandiant and iSIGHT intelligence teams was able to not only identify malicious activity aimed at stealing payment card data, but also provide a detailed window into that activity from compromise through monetization of the stolen data.

The story of FIN6 shows how real-world threat actors operate, providing a glimpse not only into the technical details of the compromise, but also into the human factor as well; namely, the interactions between different criminals or criminal groups, and how it is not just data being bartered or sold in the underground, but also tools, credentials and access.

To download this or other
FireEye Threat Intelligence reports,
visit: www.fireeye.com/reports.html

FireEye, Inc.

1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

© 2016 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc.
All other brands, products, or service names are or may be trademarks
or service marks of their respective owners. SP.FIN6.EN-US.042016

