Carbanak and FIN7 Attack Techniques

trendmicro.com/en_us/research/21/d/carbanak-and-fin7-attack-techniques.html

April 20, 2021

APT & Targeted Attacks

What happens in Carbanak and FIN7 attacks? Here are some techniques used by these financially motivated threat groups that target banks, retail stores, and other establishments.

By: Trend Micro April 20, 2021 Read time: (words)

Constant monitoring of threat groups is one of the ways that security researchers and law enforcement agencies are able defend systems against cybercrime. Among these cybercriminals are financially motivated threat groups Carbanak and FIN7. Although both names have at times been used to refer to the same group, organizations such as MITRE identifies them as two separate entities that wield the Carbanak backdoor in their attacks. However, the groups use not just the Carbanak backdoor but also other types of malware such as Pillowmint, a point-of-sale malware, and Tirion, which is said to be geared to replace Carbanak.

MITRE also identifies different main targets for each group: While Carbanak focuses on banking institutions, FIN7 targets food, hospitality, and retail establishments.

This week, the results of this year's round of the MITRE Engenuity ATT&CK Evaluations were released, which focused on Carbanak+FIN7. We also separately discussed how Trend Micro solutions deal with these threats.

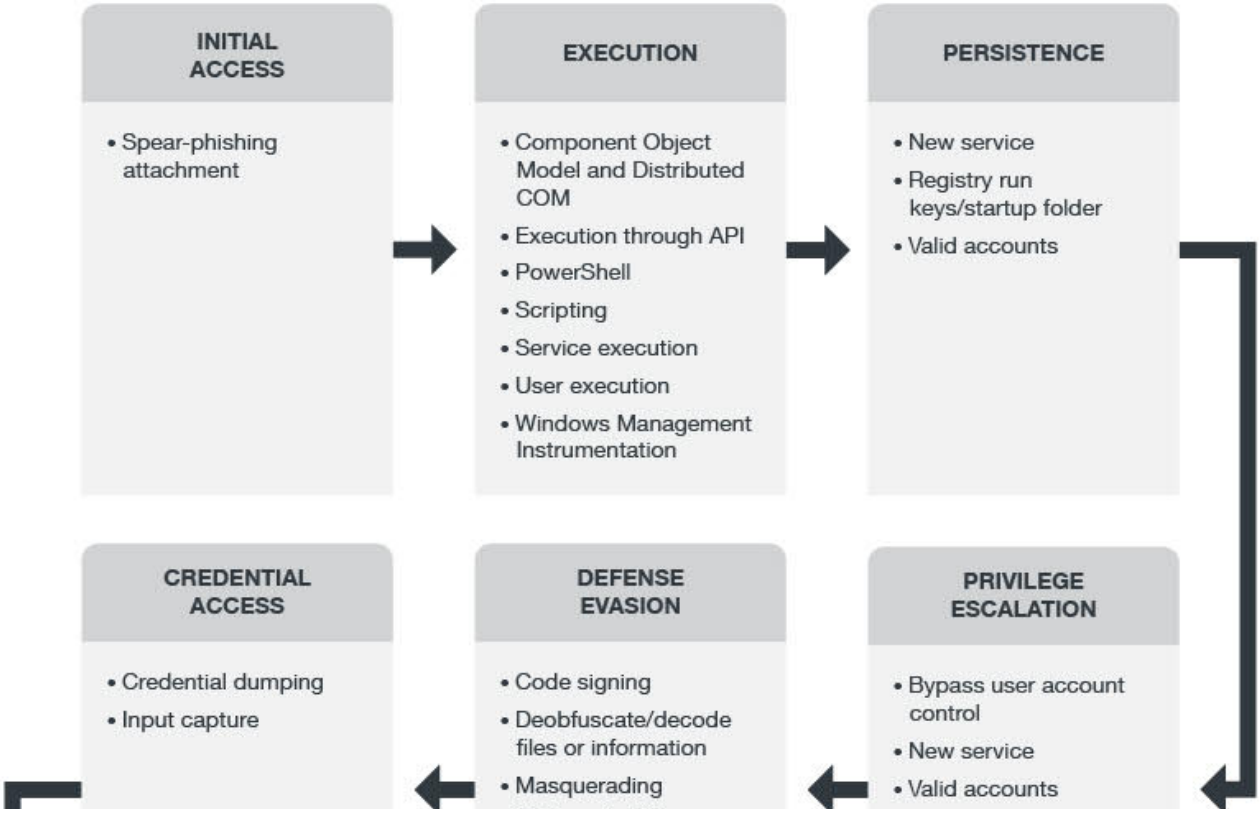
For more background on what happens in attacks launched by Carbanak and FIN7, we pieced together information from our studies of these groups as well as information from ATT&CK tactics and techniques (a total of 65 techniques across 11 tactics) identified by MITRE to be related to these threat groups.

What happens in Carbanak and FIN7 attacks?

In our analysis of a related past campaign, we observed that attackers enter the system through spear phishing. After gaining a foothold in the system, the dynamic data exchange (DDE) feature in Windows and legitimate cloud-based services will then be abused to deliver the malware or to establish command-and-control (C&C) communication.

After this, the Carbanak backdoor can then be used to log keystrokes and capture screenshots, steal and delete cookies, inject malicious code on sites, and monitor various traffic. For lateral movement, the malware abuses remote and system administration tools.

To be more specific in terms of ATT&CK® techniques, Carbanak and FIN7 share a notable number of similarities. However, some techniques are only used by one of them, as we discuss in the subsequent sections.



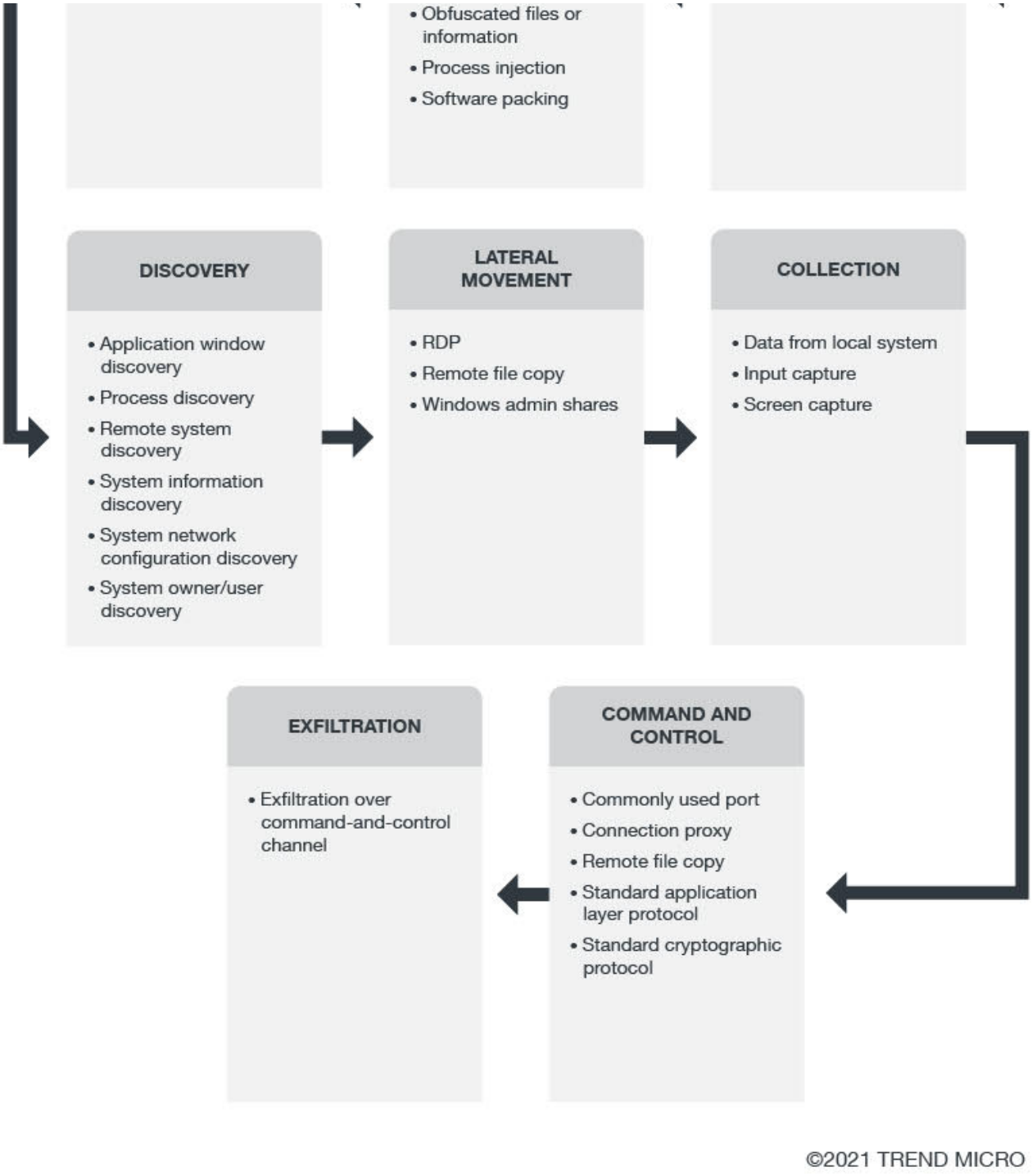


Figure 1. ATT&CK® tactics shared between Carbanak and FIN7

The following are the tactics and techniques that are employed by Carbanak and FIN7, as shared by MITRE.

Initial Access

Both groups use spear-phishing campaigns with attachments that are embedded with exploits as an entry point to the target system.

Execution

Successfully entering the system leads to the next step: executing the attack. For code and behavior execution, both groups use a variety of techniques through native API, PowerShell, service execution, user execution, Windows Component Object Model (COM) and Distributed COM, and Windows Management Instrumentation (WMI).

Carbanak also abuses command-line interface and DDE client-server protocol.

On the other hand, FIN7 takes advantage of Mshta, a utility that can execute VBScript, and scheduled tasks to run malicious code on user systems.

Persistence

Once the malicious behavior is executed, the attackers will attempt to keep their presence in a system. To maintain persistence, the groups create new services. They also add programs to a startup folder that can be referenced with a registry run key. We detected a variant of the Carbanak malware that adds registry entries and keys as an autostart technique. Credentials of existing valid accounts were also abused.

In the case of FIN7, the use of application shimming databases (which can allow developers to apply fixes to applications without rewriting code) and hooking processes that allow the modification of program behaviors are some of the techniques that can be applied. The former has been utilized in a campaign involving the Pillowmint malware.

Privilege Escalation

Some functions that are needed for the attack require admin privileges. To elevate privileges, the groups bypass Windows User Account Control (UAC) mechanisms, new services, and valid accounts to elevate process privileges.

For the same purpose, on Linux systems, Carbanak attacks can use sudo, a program that permits users to execute the programs of a superuser.

FIN7 attacks can and inject code into processes and hijack the search order used to load DLL files.

Defense Evasion

After a series of malicious behavior, attackers need to remain stealthy and undetected by using security solutions that can remove threats out of the system. For defense evasion, both groups create or acquire tools for code signing the malware, or deobfuscate or decode files or information by using malware functions or utilities in the system. Both groups also employ masquerading to make features appear benign to security solutions, files or information obfuscation to make these files and information difficult to discover, software packing to conceal code, and process injection to evade process-based defense.

Carbanak also performs techniques for disabling security tools, deleting files that are left in malicious activity, and modifying registry to hide configuration information.

FIN7 utilizes guardrails to restrict execution and abused utilities that allow indirect command execution that can go past security restrictions. The group also evades virtualization and sandboxes and injects malicious code into hollowed processes to dodge process-based defenses.

Credential Access

Some portions of the system are protected by credentials. To steal these, both groups employed credential dumping and input capture. The former involves credentials that are usually in the form of hash or clear text, while the latter involves API or web portals.

Carbanak also performs brute force tactics or takes advantage of credentials that are saved in web browsers.

On the other hand, FIN7 performs hooking.

Discovery

For the discovery phase, the Carbanak and FIN7 campaigns gain more knowledge about the system by gathering listings of various information: open application windows, running processes, IP addresses and other network identifiers in remote systems, detailed hardware and system information, system network configuration and settings, and system owners and users.

Carbanak also collects information on accounts, files and directories, group permissions, and registries.

FIN7 gathers information on network shares.

The gathered information can aid in the next step: lateral movement.

Lateral Movement

The groups move through the network and identify key assets and data by logging in via RDP, copying files to upload adversary tools through remote file copy, and abusing Window admin shares.

In Carbanak attacks, the groups' attacks can involve logging into services that accept remote connections and using stolen password hashes through the "pass the hash" method.

Collection

After moving through the network and identifying assets to target, the next step would be to gather key data. At the collection phase, Carbanak and FIN7 campaigns harvest data from local system sources and through input and screen capture (as performed in a related campaign using the Tirion malware).

FIN7 attacks can stage collected data in a particular location in preparation for exfiltration.

Command and Control

In both Carbanak and FIN7 attacks, communication with users' compromised systems is done through bypassing firewalls or network detection systems via commonly used ports, using connection proxies to avoid direct connections to the threat group's infrastructure, employing the command-and-control channel to remotely copy files from an external system, blending in with existing network traffic by using standard application layer protocol, and taking advantage of standard cryptographic protocol to disguise command-and-control traffic.

Carbanak campaigns can also use legitimate programs and remote access software for command and control. They also employ standard non-application layer protocols for communication.

Exfiltration

In the final phase of the attack, the groups exfiltrate the stolen data into the normal communications channel via command-and-control channels.

For FIN7 attack routines, data can be compressed and/or encrypted before being exfiltrated.

ATT&CK® tactics and techniques for Linux were also shared by MITRE.

Continuous vigilance against threat groups is an important aspect of keeping up with — if not being one step ahead of — threats. Solutions such as Trend Micro Vision One™ provide visibility, correlated detection, and behavior monitoring across multiple layers: email, endpoints, servers, cloud workloads.