MTR170446
MITRE TECHNICAL REPORT

MITRE

APT3 Adversary Emulation Plan

Dept. No.: J83L
Project No.: 0717MM09-AA

Annapolis Junction, MD

Authors: Christopher A. Korban
Douglas P. Miller
Adam Pennington
Cody B. Thomas

September 2017

Abstract

To advance the practice of security testing through adversary emulation, we present this emulation plan to be used by a team looking to emulate the APT3 threat group. It includes their commonly known behavior through the tactics, techniques, and procedures that have been documented in publicly available reporting. To ground the plan in a common taxonomy, it is based on the MITRE ATT&CK model. The scope covers the adversary lifecycle, from initial network compromise through exfiltration. It discusses tools, methods, style, tradecraft, and end-goals. To fill intel gaps, best-estimates based on experience in threat intelligence and adversary emulation are provided.

Acknowledgments

We would like to acknowledge the people that contributed to the content, review, and format of this document. This includes: Frank Duff, Katie Nickels, and Blake Strom.

Table of Contents

1 Overview 1-1
2 APT3 Overview 2-1
2.1 APT3 Tools 2-2
2.2 APT3 Tool Functionality 2-4
2.2.1 Pirpi Functions 2-4
2.2.2 PlugX Functions 2-6
2.2.3 OSInfo Functions 2-7
2.2.4 Pwdump Functions 2-9
2.2.5 Mimikatz Functions 2-9
2.2.6 RemoteCMD Functions 2-9
2.2.7 Dsquery Functions 2-9
2.2.8 LaZagne Functions 2-10
2.2.9 ScanBox Functions 2-10
3 Emulation Phases 3-10
3.1 Phase 1 – Initial Compromise 3-11
3.1.1 Implant Command and Control 3-11
3.1.2 Defense Evasion 3-11
3.1.3 Initial Access 3-11
3.1.3.1 Case 1 – Spear Phishing with Browser Exploit [2] 3-11
3.1.3.2 Spear Phishing with Malicious RAR Attachment [3] 3-12
3.1.3.3 Spear Phishing with Malicious RAR Attachment [21] 3-12
3.1.3.4 Spear Phishing with Malicious RAR Attachment [21] 3-13
3.1.3.5 Flash Exploit with Malware Concealed Within GIF [12] 3-13
3.1.3.6 Victim Profiling [14] 3-13
3.2 Phase 2 - Network Propagation 3-13
3.2.1 Machine Operations 3-14
3.2.1.1 Discovery 3-14
3.2.1.2 Local Privilege Escalation 3-15
3.2.1.3 Persistence 3-16
3.2.1.4 Credential Access 3-16
3.2.2 Lateral Movement 3-17
Remote Copy and Execution 3-17
3.3 Phase 3 - Exfiltration 3-17
4 Bibliography 1

List of Figures

Figure 1 APT3's Three Phases of Action 2-2
Figure 2 APT3 Phase 2 Flow Chart 3-14
Figure 3 APT3 Discovery ATT&CK Techniques 3-15
Figure 4 APT3 Privilege Escalation ATT&CK Techniques 3-15
Figure 5 APT3 Persistence ATT&CK Techniques 3-16
Figure 6 APT3 Credential Access ATT&CK Techniques 3-16
Figure 7 APT3 Lateral Movement and Execution ATT&CK Techniques 3-17
Figure 8 APT3 Exfiltration ATT&CK Techniques 3-17

List of Tables

Table 1 APT3 Tool Usage 2-3
Table 2 Pirpi Functions and Emulation 2-4
Table 3 PlugX Functions and Emulation 2-6
Table 4 OSInfo Functionality and Emulation 2-7
Table 5 Pwdump Functions and Emulation 2-9
Table 6 Mimikatz Functions and Emulation 2-9
Table 7 RemoteCMD Functions and Emulation 2-9
Table 8 Dsquery Function and Emulation 2-9
Table 9 LaZagne Functions and Emulation 2-10
Table 10 ScanBox Functions and Emulation 2-10

1 Overview

In an effort to advance the practice of security testing through adversary emulation and adversarial engineering, we present this emulation plan to be used by an adversary emulation team looking to emulate the threat group commonly known as APT3. The plan includes the group's commonly known behavior through the tactics, techniques, and procedures (TTPs) that have been documented in publicly available threat reporting. To ground the plan in a common taxonomy, it is based on the MITRE ATT&CK model[1]. The scope of this emulation plan covers the adversary lifecycle, beginning with initial network compromise and ending with exfiltration. It discusses tools, methods, style, tradecraft, and end state objectives. Historically, information about attackers' on-target actions and goals have been difficult to obtain and APT3 reporting is no exception; however, the document bases instructions off publicly accessible sources whenever possible, focusing on sources that could be cross-referenced to some degree. To fill the intel gaps, the authors relied on their experience in threat intelligence and adversary emulation for best-estimates.

Threat reporting sources vary widely, and correlation of activity to a threat group is not straightforward, and as such the authors have worked to ensure reputable sources are referenced. While many threat intelligence sources work to provide information that is as accurate as possible to the community, there is still an inherent risk that third-party threat reporting may provide inaccurate information.

Note: Within this document, italicized text represents notes. These notes represent comments that are not supported by evidence but represent the author's opinion. For example, they discuss concessions that have been made to make the emulation instructions practical or to indicate where inconsistent or nonexistent reporting has required gaps to be filled in with best-guess estimates of adversary behavior.

References are indicated in-line with bracketed numbers [#] and listed at the end of this document.

2 APT3 Overview

ATT&CK Group ID: Group/G0022

Aliases: APT3, Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-0110

Operations: Clandestine Wolf, Clandestine Fox [1], Operation Double Tap [2]

Target Industries: Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, Transportation [1]

Adversary Objectives: Reporting indicates APT3 actors are interested in exfiltration of documents [3]. They have been known to target printers and file shares [3]. They also target intellectual property, often industrial in nature. [4].

[1] https://attack.mitre.org

Background: APT3 is a China-based threat group. APT3 has traditionally targeted a myriad of US and international targets; however, reporting dated September 2016 indicates the group shifted focus around March 2016 to target Hong Kong organizations [3].

APT3's process can be broken up into three main phases as shown below:

1. Initial Setup of command and control (C2), defense evasion techniques, and getting initial compromise
2. Discovery, privilege escalation, lateral movement, persistence, and execution
3. Collection, data staging, and exfiltration

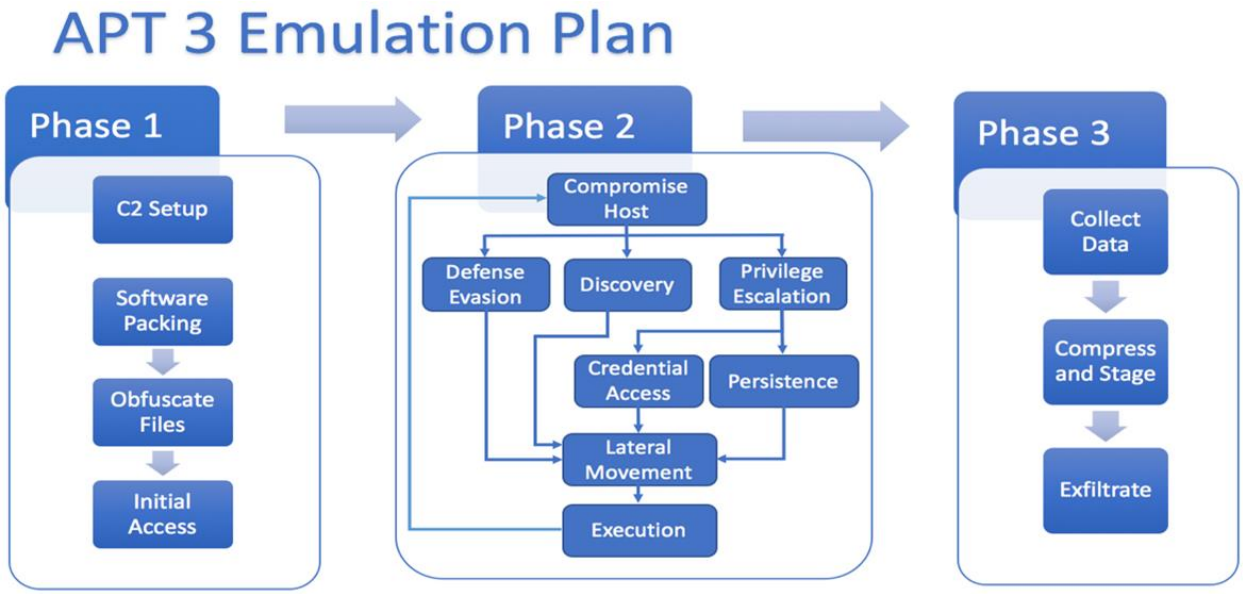

Figure 1 APT3's Three Phases of Action

These phases are broken up into more detail in the following sections. The next section is about the tools that APT3 uses for their operations, how to emulate them, and what ATT&CK tactics and techniques they correspond to. Command-line examples, as well as descriptions of what the tools do, are included in the accompanying "APT3 Adversary Emulation Field Manual" for reference.

2.1 APT3 Tools

APT3 uses a combination of custom and openly available tools. Because custom adversary tools can have hidden functionality, be difficult to tailor to new environments, or utilize server-side controllers which may be unavailable, recommendations are made for replacements that can accurately perform similar activity. Adversary emulators and defenders should be aware that replacement tools will typically leave different footprints than adversary tools, specifically different file hashes, command line arguments, Antivirus detection, API calls, and network signatures. There are lots of ways to accomplish the same objectives with built-in Windows tools, but the focus for APT3 tends to be on more simplistic tools rather than more advanced Windows utilities like WMIC, WinRM, and PowerShell. The following table describes how to emulate the tools as well as detailing which ATT&CK Tactics are represented by them.

Table 1 APT3 Tool Usage

Name	Software Type	Availability	Emulation Notes	ATT&CK Tactic
Pirpi, SHOTPUT, Backdoor.APT.CookieCutter	RAT	Custom	*Standard Windows Binary based post-compromise toolkits such as MetaSploit (free)* [5] *or Cobalt Strike (paid)* [6]	*Defense Evasion, Credential Access, Discovery,*
PlugX [7] [8]	RAT	Custom, but seen across multiple groups		
OSInfo [3]	Information Discovery	Custom	*Several Windows commands can be used to gather similar information (net use, systeminfo, set), also PowerShell scripts* [9]	*Discovery*
Customized pwdump [3]	Windows Password Dumper	Unmodified version openly available	*Standard version of pwdump or mimikatz*	*Credential Access*
Customized Mimikatz	Windows Password Dumper	Unmodified version openly available	*Standard version of mimikatz* [10]	*Credential Access*
Keylogger [3]	Keylogger	Custom	*Numerous publicly available keyloggers*	*Collection, Credential Access*
RemoteCMD [3]	Remote Execution	Custom	*Operates similarly to PsExec* [11]	*Execution, Lateral Movement*
Dsquery	Information Discovery	Openly Available, default on Windows Server	*A copy of Dsquery can be brought onto a system if it doesn't have it by default.*	*Discovery*
ChromePass [3]	Browser Password Dumper	Openly Available	*ChromePass* [12] *is a publicly available program from NirSoft*	*Credential Access, Collection*

Lazagne [3]	Application Password Dumper	Openly Available	*Lazagne* [13] *source code is freely available on Github*	*Credential Access*
ScanBox [3]	ExploitKit/ Host Profiler, and JavaScript Keylogger	Custom	*Used just before initial exploit, effectively out of scope since pre - initial network compromise.*	*N/A (Case could be made for "Collection" for Keylogger part however)*

2.2 APT3 Tool Functionality

APT3's custom tools provide a breadth of functionality. This section aims to break down these custom tools from the table above a bit further into their specific functions and show how they relate to ATT&CK, Windows utilities, and toolkits that are open source and commercially available.

2.2.1 Pirpi Functions

Table 2 Pirpi Functions and Emulation

Pirpi Function	Windows Built-in	Cobalt Strike/Beacon	Metasploit/Meterpreter	ATT&CK Technique
List processes	tasklist	ps, shell qprocess *	ps	T1057 - Process Discovery
Download file	ftp	download [filename]	Download [filename]	T1041 - Exfiltration over Command and Control Channel
Execute file	cmd.exe /c file.exe	shell [filename] shell cmd.exe /c [filename]	Execute –f [filename] [–i] [-H]	T1059 - Command-Line Interface
Load/execute DLL (from disk)	Rundll32.exe [filename.dll], entry	shell rundll32 [filename.dll], entry	post/windows/manage/ reflective_dll_inject	T1085 - Rundll32
Load/execute DLL (from memory)			post/windows/manage/ reflective_dll_inject	

List servers in domain	net group “Domain Computers” /domain	shell net group “Domain Computers” /domain	post/windows/gather/ enum_ad_computers	T1018 - Remote System Discovery
List TCP connections	Netstat -ano	shell netstat -ano	post/windows/gather/ tcpnetstat	T1049 - System Network Connections Discovery
List connected users	Net session	shell net session	post/windows/gather/ enum_logged_on_users	T1049 - System Network Connections Discovery
List domain controllers	Net group “Domain Controllers” /domain, Nltest /dclist	shell net group “Domain Controllers” /domain, shell nltest /dclist, net dclist		T1049 - Remote System Discovery
List directories	Dir, tree	shell dir	ls	T1083 - File and Directory Discovery
Terminate Process	Taskkill	shell taskkill /pid [pid]	kill [pid]	
Delete file	Del [filename]	shell del [filename]	execute –f cmd.exe “del [filename]”	T1107 - File Deletion
Sleep		sleep [time in seconds]		
Get Network Adapter Info	Ipconfig /all, netsh config	shell ipconfig /all	execute –f cmd.exe “ipconfig /all”	T1016 - System Network Configuration Discovery
Upload file	ftp	upload [filename]	upload [filename] [destination]	T1105 - Remote File Copy

2.2.2 PlugX Functions

Table 3 PlugX Functions and Emulation

Note: The PlugX table differs from the other tables in that each row refers to a module, not function, of PlugX. Modules within PlugX leverage other PlugX modules to perform functions, for example, the Disk module allows other modules to use any of the functions it provides on the disk, such as execute, create new files, copy, delete, etc..

PlugX Modules [8]	Windows Built-in	Cobalt Strike/Beacon	Metasploit/ Meterpreter	ATT&CK Technique
Disk	.\[file], type [file], del, copy	shell [file/type/del/copy], upload	execute -f cmd.exe "shell [file/type/del/copy]", upload	T1059 – Command-Line Interface, T1083 – File and Directory Discovery
Process	Tasklist, taskkill	ps, shell taskkill /pid [pid]	ps, Kill [pid]	T1057 – Process Discovery
Service	sc [query/start/stop/ config/create/ delete]	shell sc [query/start/stop/ config/create/ delete]	execute –f cmd.exe "sc [query/start/stop/config/create/delete]"	T1050 – New Service, T1031 – Modify Existing Service, T1035 – Service Execution
Regedit	regedit	shell regedit	reg	T102 – Query Registry, T1112 – Modify Registry
Netstat	netstat	shell netstat	post/windows/gather/tcpnetstat	T1049 – System Network Connections Discovery
Nethood	net view [/domain]	shell net view [/domain]	execute -f cmd.exe "net view [/domain]"	T1018 – Remote System Discovery
Option	shutdown [/l,/r,/t]	shell shutdown [/l,/r/t]	execute -f cmd.exe "shutdown [/l,/r,/t]"	N/A

PortMap	Details still N/A.	Details still N/A.	Details still N/A.	Details still N/A.
Screen	PrintScreen key if GUI available	screenshot PID [x64]	migrate PID | use espia | screengrab	T1113 – Screen Capture
Shell	cmd.exe /c [command]	shell [command]	shell or "execute -f cmd.exe -c -I"	T1059 – Command-Line Interface
Telnet	pkgmgr /iu:"TelnetServer"*	shell pkgmgr /iu:"TelnetServer"	run metsvc	T1050 – New Service, T1108 Redundant Access
SQL	Osql**	shell osql	auxiliary/admin/mssql/mssql_sql	N/A
Keylog	N/A	keylogger [pid] [x86|x64]	Keyscan_start, keyscan_dump	T1056 – Input Capture

*Note: pkgmgr has been archived and may not be on newer Windows systems.

**Note: osql is usually found on Windows Server systems and will be replaced with sqlcmd instead.

2.2.3 OSInfo Functions

Table 4 OSInfo Functionality and Emulation

OSInfo Function	Windows Built-in	Cobalt Strike/Beacon	Metasploit/Meterpreter	ATT&CK Technique
Domain	Ipconfig, whoami, net config workstation	Shell ipconfig	ipconfig	T1016 - System Network Configuration Discovery
Osinfo	systeminfo, ver, set	systemprofiler	Sysinfo, get_env.rb, run winenum	T1082 - System Information Discovery
Tsinfo	Reg query	Shell reg query	Reg (built into meterpreter, not windows reg)	T1012 - Query Registry
Netuseinfo	net use	Shell net use	Enum_shares.rb	T1049 - System Network Connections Discovery

ShareInfo	net share, net view	Shell net share	Enum_shares.rb, auxiliary/scanner/smb/ smb_enumshares	T1135 - Network Share Discovery
Connect Test	ping	Shell ping	Netenum.rb	T1018 - Remote System Discovery
Local Group User Info	net user, net localgroup	Net localgroup, shell net user	Post/windows/gather/ enum_domain_tokens, auxiliary/scanner/smb/ smb_enumusers	T1087 - Account Discovery, T1069 - Permission Groups Discovery
Global Group User Info	net user, net group	Net group, shell net user	Domain_list_gen.rb, post/windows/gather enum_domain_group_users, auxiliary/scanner/smb/ smb_enumusers	T1087 - Account Discovery, T1069 - Permission Groups Discovery
Group Administrators	net localgroup, net group	Net localgroup, net group	Domain_list_gen.rb, post/windows/gather enum_domain_group_users, auxiliary/scanner/smb/ smb_enumusers	T1087 - Account Discovery, T1069 - Permission Groups Discovery
Group Power Users	net localgroup, net group	Net localgroup, net group	Domain_list_gen.rb, post/windows/gather enum_domain_group_users, auxiliary/scanner/smb/ smb_enumusers	T1087 - Account Discovery, T1069 - Permission Groups Discovery
Group Domain Admins	net localgroup, net group	Net localgroup, net group	Domain_list_gen.rb, post/windows/gather enum_domain_group_users, auxiliary/scanner/smb/ smb_enumusers	T1087 - Account Discovery, T1069 - Permission Groups Discovery

2.2.4 Pwdump Functions

Table 5 Pwdump Functions and Emulation

pwdump Function	Cobalt Strike/Beacon	Metasploit/Meterpreter	ATT&CK Technique
Dump creds from SAM	Mimikatz !lsadump:sam	Run hashdump, hashdump	T1003 - Credential Dumping
Inject into LSASS	Logonpasswords, hashdump, mimikatz	Mimikatz's wdigest	T1003 -Credential Dumping

2.2.5 Mimikatz Functions

Table 6 Mimikatz Functions and Emulation

Mimikatz Function	Cobalt Strike/Beacon	Metasploit/Meterpreter	ATT&CK Technique
Dump creds from SAM	Mimikatz !lsadump:sam	Run hashdump, hashdump	T1003 - Credential Dumping
Inject into LSASS	Logonpasswords, hashdump, mimikatz	Mimikatz's wdigest	T1003 -Credential Dumping

2.2.6 RemoteCMD Functions

Table 7 RemoteCMD Functions and Emulation

RemoteCMD Function	Windows Built-in	Other Tools	ATT&CK Technique
SMB Copy	net use, copy, xcopy, explorer.exe	PsExec	T1105 - Remote File Copy
Remote Service	sc	PsExec	T1021 - Remote Services
Remote Schtasks	schtasks, at		T1053 - Scheduled Task

2.2.7 Dsquery Functions

Table 8 Dsquery Function and Emulation

Dsquery Function	Cobalt Strike/Beacon	Metasploit/Meterpreter	ATT&CK Technique
Account and Permission Groups Discovery	shell Dsquery*	shell / dsquery	T1087 – Account Discovery, T1069 – Permission Groups Discovery

* Note : Dsquery is found on Windows Server systems and may not be on all machines by default.

2.2.8 LaZagne Functions

Table 9 LaZagne Functions and Emulation

LaZagne Function	Cobalt Strike/Beacon	Metasploit/Meterpreter	ATT&CK Technique
Gather credentials from browsers, IM software, databases, memory, and other software		Post/windows/gather/credentials/credential_collector, Post/multi/gather/firefox_creds	T1081 - Credentials in Files, T1003 – Credential Dumping

2.2.9 ScanBox Functions

Table 10 ScanBox Functions and Emulation

ScanBox Function	Function Notes	Emulation Notes
ExploitKit-style recon and profiling	Software, browser plugins, flash, SharePoint, Adobe PDF reader, Chrome security plugins, Java, Internal IP address	N/A since this is used before initial compromise.
Keylogger	Written in JavaScript, only logs what's typed while on the page that loads the keylogger JS.	N/A since this is used before initial compromise.

3 Emulation Phases

APT3 disseminates spam-like phishing campaigns with various payload delivery methods [1]. Once on a machine, the actors collect information about the victim such as connected users [14] and analyze it for its value, trying to determine where they landed and what access they have. Admin access is an obvious main target due to the increased access it will likely provide. The actors then drop multiple backdoors, usually 2-4 on the initial system and 5+ versions within the first few hops, with independent C2 profiles for redundancy [Redundant Access – T1108]. Next they then dump as many credentials as possible, and quickly continue spreading throughout the network. They specifically go after file servers and print servers [1] [3]. Once they're moved to all the machines they think have value, they collect all the documents they want, package them up and password protect them, and exfiltrate them out of the organization [15]. In some cases, however, they've been known to persist within a network for very lengthy periods without ever exfiltrating data.

The sections below show how APT3 acts through their entire lifecycle. Phase 1 documents what happens during initial compromise, phase 2 highlights techniques used during network propagation, and phase 3 documents one way they have been known to perform exfiltration.

3.1 Phase 1 – Initial Compromise

The goal of the Initial Compromise phase is to achieve successful code execution and control of a system within the target environment.

APT3 primarily conducts initial compromise using spear phishing, delivering implants through both malicious attachments and malicious links. They have used new 0-days on multiple browsers [15]. They have targeted existing 0-days in Internet Explorer [2], Windows [2], and Flash [14]. They have also been known to compromise weakly secured legitimate websites to which users are directed through spear phishing emails [16].

3.1.1 Implant Command and Control

APT3 implants issue command and control (C2) traffic as HTTP GET requests that beacon at set intervals [14]. The HTTP Cookie field contains information for the C2 server, which responds with a webpage that contains the command encoded within a specific HTML tag [15]. APT3 implants have also been known to use custom binary protocols [2]. Pirpi.2014 and Pirpi.2015 both contain several kinds of sleep and anti-sandbox strategies that cause the RAT to pause between executions [15]. Some of the Pirpi instances have been known to also use SSL for their communications and even include public/private keys within the binaries [17]. This level of C2 customization can be achieved with Cobalt Strike's malleable C2 profiles, as seen in the accompanying Malleable C2 profile modeled on [14].

3.1.2 Defense Evasion

Many of APT3's open source tools are customized or modified to prevent detection. Additionally, APT3's malware uses a series of anti-disassembly techniques [3], including requiring certain command line parameters to run [17]. These are defense evasion techniques that APT3 sets up before getting initial access to the target environment.

It is recommended to use anti-antivirus (AV) capabilities to prevent AV detection of commonly available tools. If Sandboxing is a problem, possibly encrypt tools to bypass sandboxing. An example of this would be Veil-Evasion [18] *or Artifact Kit* [19]. *ATTACK techniques:* T1027 – Obfuscated Files or Information, T1045 – Software Packing, T1066 – Indicator Removal from Tools.

3.1.3 Initial Access

For Initial Compromise, both web server drive-by and malicious attachments are within APT3's tradecraft. The Social Engineering Toolkit (free) [20] *and Cobalt Strike (paid)* [6] *have features that support these methods.*

3.1.3.1 Case 1 – Spear Phishing with Browser Exploit [2]

In late November 2014 an APT3 campaign used a spear phishing email (see Appendix A) containing a link to a malicious site. The site contained JavaScript that triggered CVE-2014-6332 (an Internet Explorer exploit [21]) which launched a VBscript and PowerShell based payload. The PowerShell script in turn downloaded and ran a stager which dropped two files, "doc.exe"

and “test.exe”. “doc.exe” attempts to trigger CVE-2014-4113 (a Windows Kernel exploit [22]) and run “test.exe” with the resultant elevated privileges. “test.exe” runs two commands:

```
cmd.exe /C whoami

schtasks /create /tn "mysc" /tr C:\Users\Public\test.exe /sc ONLOGON /ru "System"
```

The first command is used to check that the process is running as SYSTEM. The second establishes persistence via Schtasks.

In addition, the implant connected to a command and control server over port 1913 using the SOCKS5 protocol. This dropper supports writing to or executing files at the following locations:

```
C:\Users\[Username]\AppData\Local\Temp\notepad1.exe

C:\Users\[Username]\AppData\Local\Temp\notepad.exe

C:\Users\[Username]\AppData\Local\Temp\notepad2.exe

C:\Users\[Username]\AppData\Local\Temp\newnotepad.exe
```

In addition, the software supports exfiltrating the file written at the following location [T1074 – Data Staged]:

```
C:\Users\[Username]\AppData\Local\Temp\note.txt
```

In October 2014, a downloader like “test.exe” was observed to download Pirpi.

3.1.3.2 Spear Phishing with Malicious RAR Attachment [3]

In attacks dating late 2015 to early 2016 APT3 has been known to use a zip archive containing a Windows shortcut file with an Internet Explorer logo. Clicking on this link led to a download of APT3’s Pirpi RAT.

3.1.3.3 Spear Phishing with Malicious RAR Attachment [7]

In attacks reported in June 2014, APT3 actors sent a RAR archive as an email attachment. It contained a resume and program purported to be written by the job candidate. The program, ttcalc.exe, contained a legitimate version of TTCalc but also dropped Pirpi to:

```
%USERPROFILE%/Application Data/mt.dat
```

And a bat file that was saved at [T1064 – Scripting]:

```
%USERPROFILE%/Start Menu/Programs/Startup/vc.bat
```

The bat file contained the following script:

```
@echo off

cmd.exe /C start rundll32.exe "C:\Documents and Settings\admin\Application
Data\mt.dat" UpdvaMt
```

The bat file will be triggered when the user logged in and would have caused Pirpi to start with rundll32 [T1085 – Rundll32].

3.1.3.4 Spear Phishing with Malicious RAR Attachment [7]

Reported in June 2014, APT3 actors sent an encrypted self-extracting RAR attachment. The RAR contained a trojanized setup program which attempts to drop and run ttcalcBAK.exe another self-extracting RAR which drops a DLL version of the PlugX RAT at:

```
%ALLUSERSPROFILE%\chrome_frame_helper
```

The RAT is loaded via DLL side-loading with a valid version of Chrome [T1073 – DLL Side-Loading].

3.1.3.5 Flash Exploit with Malware Concealed Within GIF [14]

Reported in 2015, two different APT3 campaigns targeted Flash exploits, CVE-2014-1776 and CVE-2015-3113. In both cases the Flash exploit loaded the payload (the Pirpi RAT) from specially crafted GIF images.

3.1.3.6 Victim Profiling [16]

Reported in July 2015, APT3 used spear phising to direct targets to a compromised site. This site had ScanBox installed which was used to profile the victims and in some cases, deliver exploits to selected victims.

3.2 Phase 2 - Network Propagation

The goal of the Network Propagation phase is to identify and move to desired systems within the target environment with the intention of discovering credentials and documents for exfiltration.

Publicly reported direct observation of APT3's Network Propagation techniques is almost non-existent. One report that discusses general characteristics of APT3 is [23]*, but it is uncertain what data sources were used to compile the listed TTPs. Aside from that report we draw conclusions of how APT3 operates based on the capabilities of Pirpi and other tools that they are reported to use. There are some persistence techniques that they have used during Initial Compromise that can be applied to Network Propagation. Despite this, there are significant gaps in the public knowledge of APT3's tradecraft. Where necessary we fill in details with best guesses or recommendations.*

The process within this phase can be described with the below diagram. Each step within this phase is broken out by ATT&CK tactic and the corresponding APT3 specific techniques documented in reports. A command-line reference for emulating the specific ATT&CK techniques with built-in Windows utilities, Cobalt Strike, and Metasploit can be found in the accompanying "APT3 Adversary Emulation Field Manual".

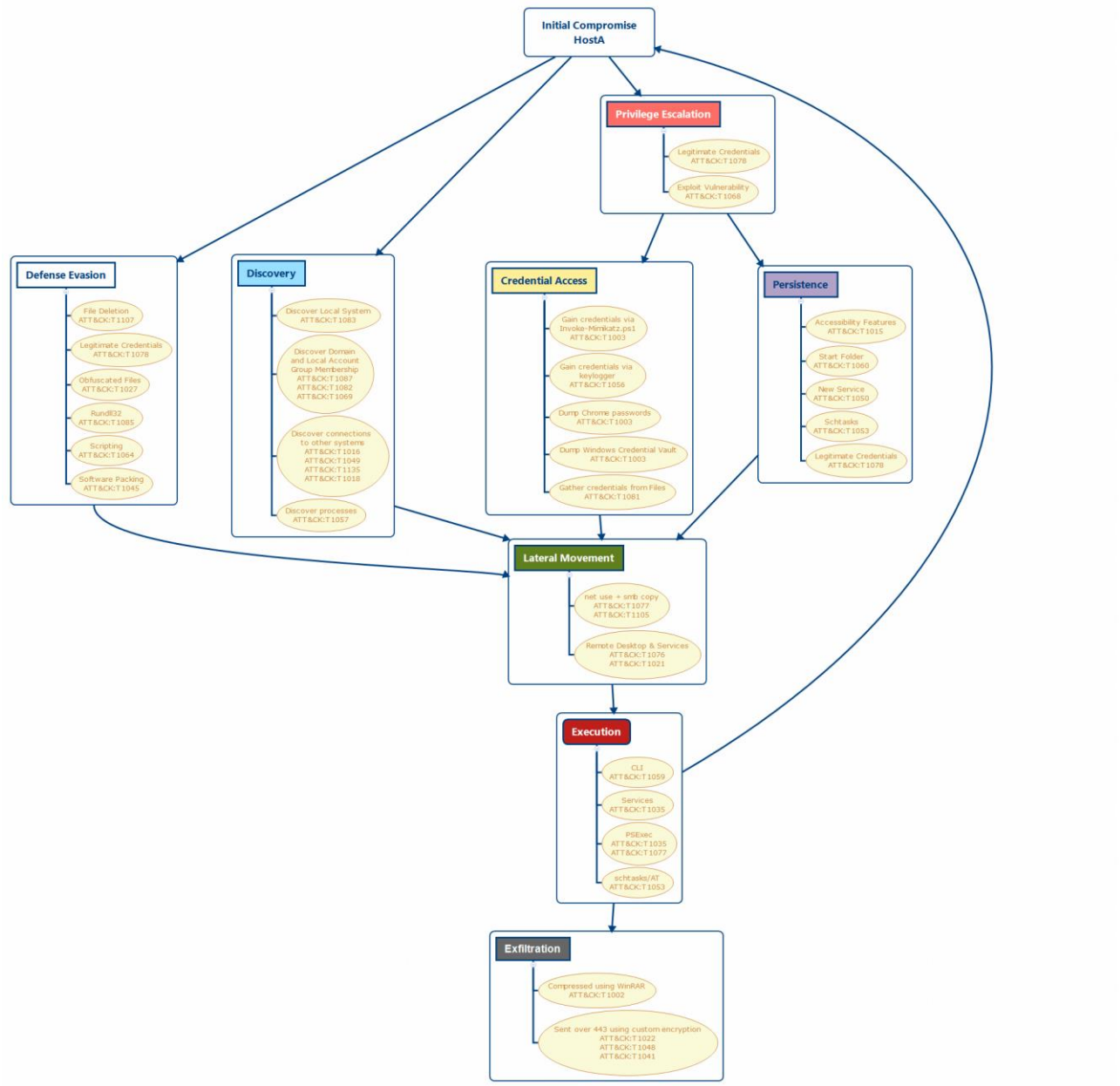

Figure 2 APT3 Phase 2 Flow Chart

3.2.1 Host Operations

3.2.1.1 Discovery

APT3 can perform discovery with its OSInfo tool and by running built-in Windows utilities on the command-line using cmd.exe. Based on the commands available in APT3's toolset, there is a lot of time spent enumerating domain groups with elevated permissions like "Domain Admins", "Enterprise Admins", and "Power Users" [T1069 - Permission Groups Discovery]. There's also a heavy emphasis on enumerating users in these special groups with the "net user" command [T1087 – Account Discovery].

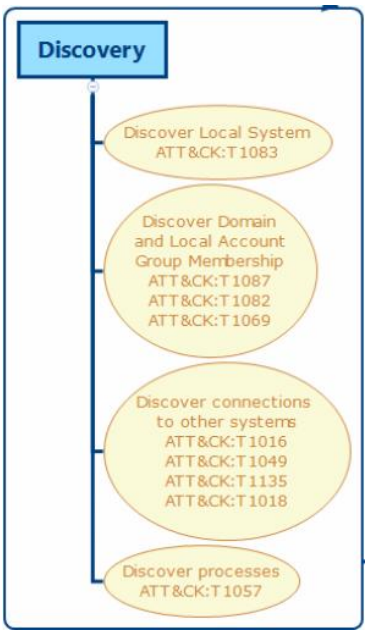

Figure 3 APT3 Discovery ATT&CK Techniques

*When doing discovery, certain actions are very closely intertwined (as shown grouped together in the above diagram). Querying the domain for the "Domain Admins" group [*T1069 – Permission Groups Discovery*] returns the users that are members of that group, which then involves looking up those users to see if they're part of any other interesting groups [*T1087 – Account Discovery*]. This process can repeat for a while as all interesting users and groups are* enumerated. *Similarly, querying systems for their configuration [T1016 – System Network Configuration Discovery] and their current network connections [*T1049 – System Network Connections Discovery*] are heavily integrated.*

3.2.1.2 Local Privilege Escalation

Credential dumping and persistence may require local privilege escalation if the attacker does not have control of a high integrity process; however, the only reporting available on local privilege escalation methods used by APT3 is CVE-2014-4113 [2]. It is possible that their strong reliance on credential access (detailed later) allows them to use credentials with increasing levels of access in place of other local privilege escalation mechanisms. Their perceived focus during this phase, however, is on finding credentials that allow direct admin permissions. In this case, control falls through to credential access or persistence.

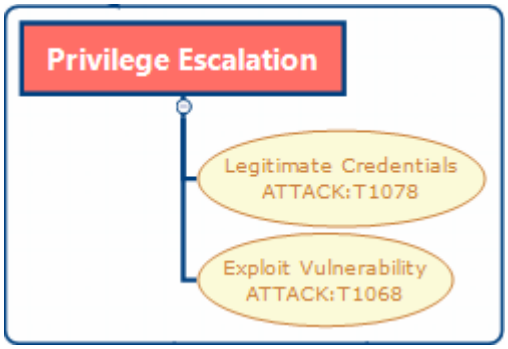

Figure 4 APT3 Privilege Escalation ATT&CK Techniques

During an engagement, adversary emulators may find it necessary to perform local privilege escalation due to time constraints. Most common frameworks (including Metasploit and Cobalt Strike) contain some methods for privilege escalation. Also, UACBypass [24] *and PowerUp* [9] *are common and freely available tools that may be used to perform Privilege Escalation.*

3.2.1.3 Persistence

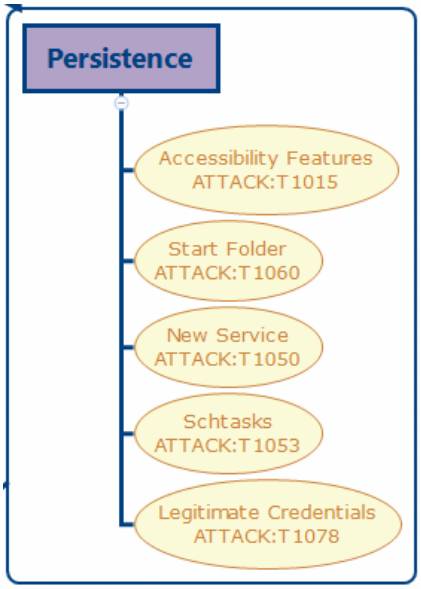

Figure 5 APT3 Persistence ATT&CK Techniques

APT3 has used multiple methods for persistence: creating a service [23] (T1050 - New Service), creating a scheduled task [2] (T1053 - Scheduled Task), and also by placing scripts in the Startup Folder [7] [T1060 - Registry Run Keys/Start Folder].

APT3 has replaced the Sticky Keys binary (`C:\Windows\System32\sethc.exe`) with cmd.exe [T1015 - Accessibility Features] and enabled Remote Desktop Protocol (RDP) if it is not already enabled [T1076 – Remote Desktop Protocol]. This specific Persistence technique has an added benefit of allowing an operator to open a command prompt when connected over RDP without having to provide valid credentials [23].

APT3 has been known to create or enable accounts, for example "support_388945a0", and add them to the local admin group [23] [T1136 – Create Account]. Presumably this is done for easier future access.

Recommendation: On new hosts, establish persistence by creating a service or schtasks. On systems where RDP capabilities are desired, it might also be useful to enable sticky keys and RDP.

3.2.1.4 Credential Access

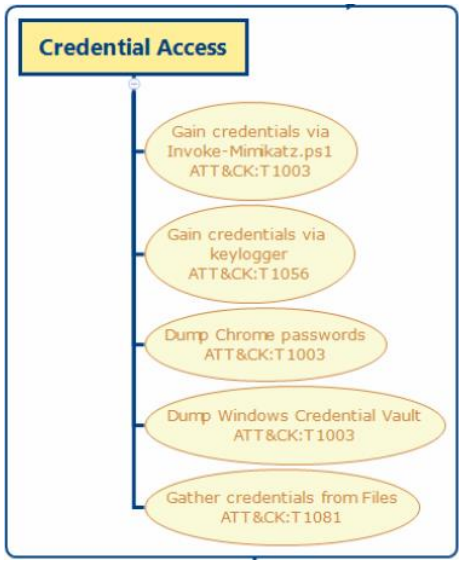

Figure 6 APT3 Credential Access ATT&CK Techniques

APT3 uses many forms of credential access. They used customized versions of pwdump, and later a custom compiled version of mimikatz, to search for cached Windows credentials [T1003 - Credential Dumping] as well as ChromePass and Lazagne [(T1081 - Credentials in Files], to search though browser and other credential caches. Their pwdump tool injects itself into lsass.exe and is executed by running the GetHash export of the lsremora.dll [3] Mimikatz is used to dump plaintext credentials by injecting into lsass.exe. [T1003 - Credential Dumping].

They also install a keylogger, which can be used to discover credentials and remote systems [T1056 - Input Capture]. This keylogger installs itself as a service and records keystrokes in encrypted files such as thumbcache_96.dbx [T1027 – Obfuscated Files or Information] [3].

3.2.2 Lateral Movement

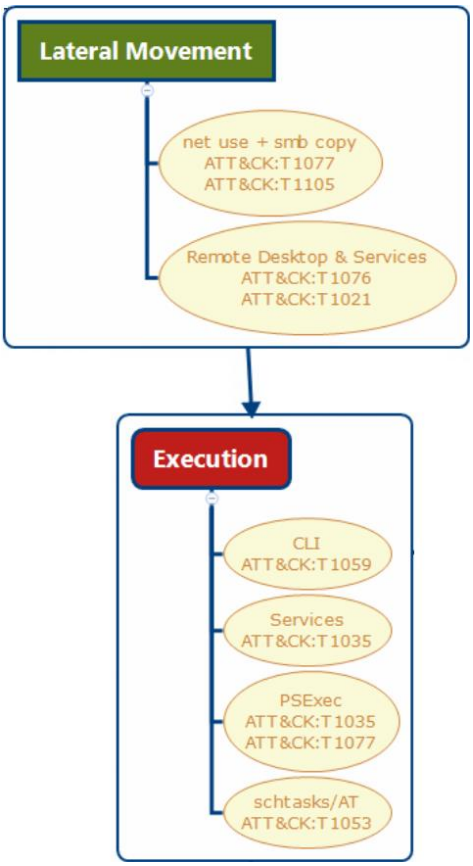

Figure 7 APT3 Lateral Movement and Execution ATT&CK Techniques

Though publicly reported information on how APT3 enumerates machines aside from related commands in APT3's tools, they've been known to use "net view" and dsquery to do so. This may be due to a lack of available information on how APT3 operates during an operation since most reports tend to be focused on forensic information. Pirpi has commands that list servers in the domain, list TCP connections and retrieve connected users (T1049 - Network Connections Discovery), and list Domain Controllers (T1018 - Remote System Discovery). Some of this information may be used to identify target hosts for lateral movement. In addition to built-in Windows utilities, there are some open source tools which collect similar information. APT3 will quickly spread to other machines as fast as possible, often checking for easy password reuse by trying to mount shares from other machines via "net use" [T1078 – Valid Accounts] [T1077 - Windows Admin Shares] [T1110 – Brute Force].

APT3 prioritizes file and printer servers.

Remote Copy and Execution

APT3 uses a custom tool called RemoteCMD that can run commands on a remote system. It's not clear what protocol(s) are being used, but RemoteCMD supports file operations (upload, download, delete and rename) service operations (creation, deletion, start and stop) and scheduled tasks (AT,schtasks). Presumably these are done over SMB (files), Remote Service (services) and Remote Schtasks (AT).

3.3 Phase 3 - Exfiltration

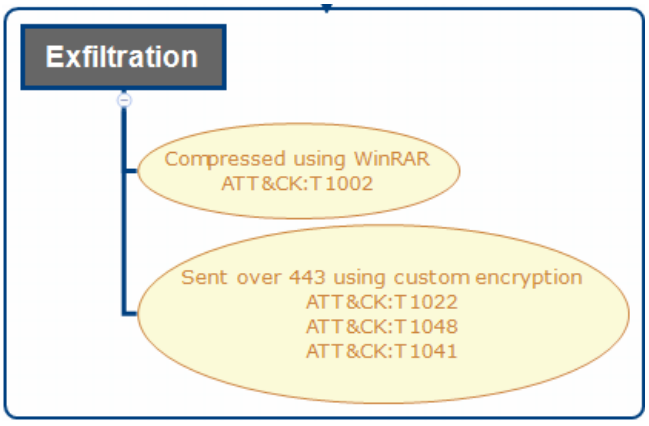

Figure 8 APT3 Exfiltration ATT&CK Techniques

It's likely that APT3 will compromise a network to a certain degree of satisfaction before starting to exfil, due to stealth concerns. Depending on the defensive setup, exfiltration could be much noisier and noticeable than attempting to hide in the noise with lay-of-the-land tools.

The only source we were able to find for APT3 exfiltration methods is from 2012. For exfiltration, they will identify Office documents on the computer [23] [T1005 - Data from Local System]. They then drop the command-line Chinese language version of WinRAR and use it to compress and encrypt the discovered documents [T1002 - Data

Compressed]. This archive will then be stored in the recycle bin [23], usually on a machine designated as a staging server, which they move the exfiltration through [T1074 - Data Staged]. Data is exfiltrated over port 443 which is typically HTTPS traffic, however they have used SSL encryption [17] and normal HTTP [23] [T1043 - Commonly Used Port] .

4 Bibliography

[1] [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html.

[2] [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/11/operation_doubletap.html.

[3] [Online]. Available: https://www.symantec.com/connect/blogs/buckeye-cyberespionage-group-shifts-gaze-us-hong-kong.

[4] [Online]. Available: https://threatpost.com/emergency-adobe-flash-patch-fixes-zero-day-under-attack/113434/.

[5] [Online]. Available: https://www.metasploit.com/.

[6] [Online]. Available: https://www.cobaltstrike.com/.

[7] [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/06/clandestine-fox-part-deux.html.

[8] [Online]. Available: https://www.lastline.com/labsblog/an-analysis-of-plugx-malware/.

[9] [Online]. Available: https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon.

[10] [Online]. Available: https://github.com/gentilkiwi/mimikatz.

[11] [Online]. Available: https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx.

[12] [Online]. Available: http://www.nirsoft.net/utils/chromepass.html.

[13] [Online]. Available: https://github.com/AlessandroZ/LaZagne.

[14] [Online]. Available: http://researchcenter.paloaltonetworks.com/2015/07/ups-observations-on-cve-2015-3113-prior-zero-days-and-the-pirpi-payload/.

[15] [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html.

[16] [Online]. Available: http://pwc.blogs.com/cyber_security_updates/2015/07/pirpi-scanbox.html.

[17] [Online]. Available: https://recon.cx/2017/montreal/resources/slides/RECON-MTL-2017-evolution_of_pirpi.pdf.

[18] [Online]. Available: https://github.com/Veil-Framework.

[19] [Online]. Available: https://www.cobaltstrike.com/help-artifact-kit.

[20] [Online]. Available: https://github.com/trustedsec/social-engineer-toolkit/.

[21] [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6332.

[22] [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-4113.

[23] [Online]. Available: http://carnal0wnage.attackresearch.com/2012/09/more-on-aptsim.html.

[24] [Online]. Available: https://github.com/hfiref0x/UACME.

This page intentionally left blank