

Threat Emulation Plan: APT 10

Developed by: CW3 James Honeycutt

(from CPT 169)

Threat Emulation Plan: APT 10

# APT 10 Overview

APT10 or menuPass has been known to hide in plain sight using common tools built into the system to steal secrets. They have also been known to use valid accounts when moving from an on-premises location to a MSP, managed service provider. With the assumption of compromise, the CPT will conduct pilfering, lateral movement and simulated data exfiltration operations. Operations will be conducted using common built-in operating system tools and tools to simulate APT10’s custom tools.

**ATT&CK Group ID:** Group/G0045

**Aliases:** Stone Panda, APT10, Red Apollo, CVNX, HOGFISH

**Operations:** No known named operations.

**Target Industries:** Health care, Defense, Aerospace, Government Sectors, and Japanese University

**Objectives:** Steal intellectual property.

**Background:** The threat actor is believed to be based in China. The actor traditionally targets international targets, including the US. There operate in three main phases:

Phase 1 – Initial setup of C2, defense evasion techniques, and initial compromise

This phase will be simulated. No actual breaching operations will be conducted.

Phase 2 – Discovery, privilege escalation, lateral movement, persistence, and execution

This is the phase the operation will be focused on.

Phase 3 – Collection, data staging, and exfiltration

This phase will be partially simulated. No data will be moved out of the protected enclave. Data will be exfiltrated to a secure share within the enclave for emulation purposes.

## APT 3 Tools

This chart represents the tools that the threat actor has been known to use.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Software Type** | **Availability** | **Notes** |
| ADFind | Active Directory cmdline tool | Windows Native Tool |  |
| Certutil | Certificate cmdline tool | Windows Native Tool |  |
| ChChes | First Stage C2 tool | Custom | Can be emulated |
| Cmd | Windows cmdline interpreter | Windows Native Tool |  |
| Esentutil | Database cmdline tool | Windows Native Tool |  |
| EvilGrab | Recon Malware | Custom | Can be emulated |
| Impacket | Python module to construct network protocols | Open Source |  |
| Mimikatz | Credential Dumper | Open Source |  |
| Net | Windows utility to control local users, local groups, services and network connections | Windows Native |  |
| Ping | Network troubleshooting tool | Windows Native |  |
| PlugX | Remote Access Tool |  | Can be simulated |
| PoisonIvy | Remote access Tool |  | Can be simulated |
| PowerSploit | Offensive PowerShell Module Framework | Open source |  |
| PsExec | Sysinternal tool for remote administration | Microsoft Sysinternals Download |  |
| Pwdump | Credential Dumper | Open Source |  |
| QuasaRAT | Remote Access Tool | Open Source |  |
| RedLeaves | Remote Access Tool |  | Code overlaps with PlugX |
| SNUGRIDE | Initial Backdoor | Custom |  |
| UPPERCUT | Persistent Backdoor | Custom | Can be simulated |
|  |  |  |  |

## APT 3 Tool Functionality

This chart represents the tool and our associated emulation methods.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Windows Built-in** | **Metasploit** | **Python Modules** |
| ADFind | ADFind |  |  |
| Certutil | CertUtil |  |  |
| ChChes |  | Reverse\_tcp |  |
| Cmd | Builtin |  |  |
| Esentutil | Builtin |  |  |
| EvilGrab |  | Record\_mic/webcam\_snap/screengrab/  Keyscan\_start/keyscan\_dump |  |
| Impacket |  |  | smbclient.py  lookupsid.py  reg.py  rpcdump.py  samrdump.py  services.py  ifmap.py  opdump.py  getArch.py  netview.py |
| Mimikatz |  | Load/help/mimikatz\_command |  |
| Net | Builtin |  |  |
| Ping | Builtin |  |  |
| PlugX |  | Execute/ps/kill/reg/tcpnetstat/  Migrate/shell/run metsvc/mssql\_sql/Keyscan |  |
| PoisonIvy |  | Execute/ps/kill/reg/tcpnetstat/  Migrate/shell/run metsvc/mssql\_sql/Keyscan |  |
| PowerSploit | Invoke-DllInjection/ Invoke-Shellcode/  Get-GPPPassword/  Get-Keystrokes/  Get-TimedScreenshot/  Invoke-NinjaCopy |  |  |
| PsExec | PsExec.exe |  |  |
| Pwdump |  | Hashdump |  |
| QuasaRAT |  | Execute/ps/kill/reg/tcpnetstat/  Migrate/shell/run metsvc/mssql\_sql/Keyscan |  |
| RedLeaves |  | Execute/ps/kill/reg/tcpnetstat/  Migrate/shell/run metsvc/mssql\_sql/Keyscan |  |
| SNUGRIDE |  | Migrate process |  |
| UPPERCUT |  | Sysinfo/ps/kill (PID)/getuid/upload or download/pwd or lpwd/cd or lcd/cat/bglist/bgrun/Bgkill/background/edit/shell/migrate/idletime/screenshot/clearev/? or Help/exit / quit:/shutdown / reboot/use/channel |  |

# Emulation Phases

APT10 uses two avenues of initial compromise. The one that will not be emulated is compromise of the trust relationship. The CPT will assume initial compromise by way of spearphishing. After the initial spearphishing compromise, APT10 establishes persistence and C2 (command and control). Then they start pilfering and looking for intellectual property to steal

## Phase 1- Initial Compromise

During this phase phishing emails with compromised Microsoft Office documents are composed and sent out. They also set up webpages and domains for C2 operations. This phase of the operation will be simulated, however, the compromised Microsoft Office document will be used as an artifact to find. Access will be granted. The trusted insider will also be our contact for any mission related changes or problems that might arise.

## Phase 2 - Discovery and lateral movement

During this phase of the operation we will be enumerating the network and host systems in the enclave. The scope will be all systems in the enclave. Network infrastructure will be out of scope for this operation. User accounts, service accounts, and machine accounts will be targeted during this operation. As this is a training environment, every effort will be made to not bring the enclave down or conduct denial of service attacks.

### Discovery

Discovery operations will be conducted using the tools listed in chart 1-1. Based on the commands in the threat actors tool kits, a lot of time is spent enumerating the environment. Special interest is shown to members of elevated permission groups (i.e. Domain Admins, Administrators, etc.)

Appendix B has a list of specific command that will be run. The appendix is broken down into sections appropriately.

### Local Privilege Escalation

Credential dumping and persistence may require local privilege escalation. The threat actor relies on gaining high level accounts as its primary focus. This is also the objective of the operation. Privilege escalation exploits and methods will be used if high level account access can not be gained.

Appendix B has a list of specific command that will be run. The appendix is broken down into sections appropriately.

### Credential Access

APT10 has many tools available to gather credentials. The operation will emulate this action and perform multiple methods of credential gathering. Key loggers are used during this phase on the compromised systems to try to capture credentials.

Appendix B has a list of specific command that will be run. The appendix is broken down into sections appropriately.

### Lateral Movement

Information about the network and connected hosts will be gathered and processed to determine a good path to the print servers and file servers. Built-in Windows utilities as well as other methods will be used for this. The intent is to mimic the quick spread to other machines that the threat actor is known for. Using pass the hash and password reuse attacks is the primary tactic.

Appendix B has a list of specific command that will be run. The appendix is broken down into sections appropriately.

## -Exfiltration

During this phase identification of Microsoft Office documents is priority. WinRAR will be used to compress and encrypt the documents before exfil to the secure storage that is being provided. No data will leave the protected enclave during this phase.

Appendix B has a list of specific command that will be run. The appendix is broken down into sections appropriately.

# Bibliography

*\*\*\*\*\*\*SNIP\*\*\*\*\*\*\**

*Section cut for brevity*

# Appendix

Appendix A – Not attached

Appendix B – Commands and Methods used – Attached