

Threat Emulation Plan: APT 28

Developed by: CW3 James Honeycutt

(from omicron persei 8)

Threat Emulation Plan: APT 28

# APT 3 Overview

This plan lists the threat actors’ tactics, techniques, and procedures. The information was gathered from open source intel location. The sources will be attached in ‘Appendix A - Sources’. The scope of this plan covers actions after the initial breach and compromise of the system. This action will be simulated by the trusted sources and Information Assurance team requesting this operation.

**ATT&CK Group ID:** Group/G0007

**Aliases:** APT28, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

**Operations:** Hillary Clinton campaign, World anti-doping Agency, Organization for the Prohibition of Chemical Weapons

**Target Industries:**

**Objectives:** Exfiltration of documents. They have been known to target printers and file shares.

**Background:** Threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165.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 28 Tools

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Software Type** | **Availability** | **Notes** |
| ADVSTORESHELL | Spying Backdoor | Custom | Can be emulated |
| Cannon | Remote Access Tool | Custom | Can be emulated |
| Certutil | Command line utility | Windows native | Can be used |
| CHOPSTICK | Backdoor | Custom |  |
| CORESHELL | Downloader | Custom | Can be emulated |
| DealersChoice | HTTP C2 | Custom | Can be emulated |
| Downdelph | UAC Bypass | Custom |  |
| Drovorub | Toolset | Custom | Linux Tool set |
| Forfiles | Command line utility | Custom | Can be emulated on Windows |
| Fysbis | Linux Backdoor | Custom | Linux Tool |
| HIDEDRV | Exploit Kit | Custom | Out of scope |
| JHUHUGIT |  |  |  |
| Koadic |  |  |  |
| Komplex |  |  |  |
| LoJax |  |  |  |
| Mimikatz | credential dumper | Open Source |  |
| OLDBAIT |  |  |  |
| RESPONDER | LLMNR, NBT-NS and MDNS poisoning | open source |  |
| USBSTEALER |  |  |  |
| Winexe |  |  |  |
| X-Agent for Android |  |  | Out of Scope |
| XAgentOSX |  |  | Out of Scope |
| XTunnel |  |  |  |
| Zebrocy |  |  |  |

## APT 28 Tool Functionality

This chart represents the tool and our associated emulation methods.

|  |  |  |
| --- | --- | --- |
| **Name** | **Windows Built-in** | **Metasploit** |
|  | Tasklist/ftp/net/tree/dir/cmd.exe /Rundll32.exe/netstat/taskkill/del/  ipconfig | Ps/download/execute/reflective  \_dll\_inject/enum\_ad\_computers  /tcpnetstat/ls/kill/upload |
|  | Type/del/copy/tasklist/taskkill/sc/  Regedit/netstat/net/shutdown/  Cmd.exe/sqlcmd | Execute/ps/kill/reg/tcpnetstat/  Migrate/shell/run metsvc/mssql\_sql/Keyscan |
|  | Ipconfig/whoami/net/workstation/  Systeminfo/ver/set/reg query/ping  / | Ipconfig/sysinfo/reg/enum\_shares  /netenum/enum\_domain\_tokens/  Smb\_enumusers/domain\_list\_gen |
|  |  |  |
| Mimikatz |  |  |
|  |  |  |
|  | Net/copy/xcopy/explorer.exe | Shell/copy |
|  |  |  |
|  |  |  |
|  |  |  |
|  | N/A |  |

# Emulation Phases

APT3 performs recon on target boxes once initial compromise has been done. They gauge the value of the target account and decide on whether to continue or try again. Once operations continue, they drop multiple backdoors on the target. Each has unique, independent C2 profiles, to provide redundancy. They continue this activity for the first few hops. Main targets for them to go after are print servers and file servers. Once they have the information they want, it is packaged up and password protected before exfiltration.

## Phase 1- Initial Compromise

During this phase phishing emails are composed and sent out. They also set up webpages and domains for C2 operations. This phase of the operation will be simulated. Access will be granted by Professor Farnsworth. 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

APT3 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 by Professor Farnsworth. 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