|  |
| --- |
|  |
| **Cyber Protection Team 175 Threat Emulation Plan: APT 82** |
| **OPERATION GRUNGY PAINT III** |
| **03 OCT 2019** |
|  |
| **1.0.0** |



**Table of Contents**

[Threat Emulation Plan: APT 82 2](#__RefHeading___Toc1189_1794271398)

[1 APT 82 Overview 2](#__RefHeading___Toc1170_1794271398)

[1.1 MITRE ATT&CK Group ID: 2](#__RefHeading___Toc3891_1794271398)

[1.2 Aliases: 2](#__RefHeading___Toc3893_1794271398)

[1.3 Operations: 2](#__RefHeading___Toc3895_1794271398)

[1.4 Target Industries: 3](#__RefHeading___Toc3897_1794271398)

[1.5 Objectives: 3](#__RefHeading___Toc3899_1794271398)

[1.6 Background: 3](#__RefHeading___Toc3901_1794271398)

[1.7 APT 82 Tools and Techniques 3](#__RefHeading___Toc1172_1794271398)

[1.8 APT 82 Tool Functionality 7](#__RefHeading___Toc1174_1794271398)

[2 Emulation Phases 9](#__RefHeading___Toc1176_1794271398)

[2.1 Most likely: 9](#__RefHeading___Toc3903_1794271398)

[2.2 Recommendation: 9](#__RefHeading___Toc3905_1794271398)

[2.3 Indicators of compromise 9](#__RefHeading___Toc3907_1794271398)

[2.3.1 IOC 1 9](#__RefHeading___Toc3909_1794271398)

[*2.3.2 IOC 2* 10](#__RefHeading___Toc3911_1794271398)

[*2.3.3 IOC 3* 11](#__RefHeading___Toc3913_1794271398)

[*2.3.4 IOC 4* 12](#__RefHeading___Toc3915_1794271398)

[2.4 Attribution 13](#__RefHeading___Toc3917_1794271398)

[2.5 Phase 1 - RECON 13](#__RefHeading___Toc1178_1794271398)

[2.6 Phase 2 - SCANNING 13](#__RefHeading___Toc1180_1794271398)

[2.7 Phase 3 - EXPLOITATION 13](#__RefHeading___Toc1182_1794271398)

[3 Bibliography 14](#__RefHeading___Toc1184_1794271398)

[4 Appendix 16](#__RefHeading___Toc1186_1794271398)

# Threat Emulation Plan: APT 82



# APT 82 Overview

*This section provides an overview of the threat, including any assumptions made during the development of the TEP. Provides a brief narrative of how the adversary conducts operations. Cites sources of information where applicable.*

## 1.1 MITRE ATT&CK Group ID:

APT 82

## 1.2 Aliases:

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

## 1.3 Operations:

APT 82 operates from a post cold war Warsaw Pact nation which operates on a deeply nationalistic and xenophobic platform. APT 82 seeks to destabilize democracy in neighboring states and other similar geopolitical targets in order to advance their propaganda and world views. They have been known to:

* Gain access to networks through deployments of remote server based C2 clients (e.g. CHOST, other C2 malware) by means of drive-by or phishing vectors
* Enumerate access and conduct privilege escalation on the victim networks utilizing process injection and lateral movement techniques
* Leverage Base64 encoded commands and command and control (C2) encrypted communications on Active Directory controller
* Compress proprietary data (e.g. WinRar, 7zip) and exfiltrate to a external location using very small packets over port 80

## 1.4 Target Industries:

Government entities, agencies, and infrastructure to disrupt the democratic process

## **1.5 Objectives:**

Targeting of these entities is intended to make the public lose faith in the current elected government and destabilize trade relations with capitalistic trade partners to eventually replace the current regime via either kinetic coup or conventional legal means (new election) or a combination of methodologies.

## 1.6 Background:

APT 82 is a threat group that has been attributed to Polandia's Main Intelligence Directorate of the Polandia General Staff by a July 2018 U.S. Department of Justice indictment. This group reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. APT 82 has been active since at least 2004. They have been known to:

## 1.7 APT 82 **Tools and Techniques**

*APT 82 employs these tools and techniques:*

|  |  |
| --- | --- |
| **Techniques Used** | **Use** |
| Buy domain name | APT82 registered domains imitating NATO and OSCE security websites and Caucasus information resources. |
| Obtain/re-use payloads | APT82 reused the SOURFACE downloader as the payload of a lure document. |
| Access Token Manipulation | APT82 has used CVE-2015-1701 to access the SYSTEM token and copy it into the current process as part of privilege escalation. |
| Automated Collection | APT82 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. |
| Bootkit | APT82 has deployed a bootkit along with Downdelph to ensure its persistence on the victim. The bootkit shares code with some variants of BlackEnergy. |
| Command-Line Interface | APT82 uses cmd.exe to execute commands and custom backdoors. |
| Communication Through Removable Media | APT82 uses a tool that captures information from air-gapped computers via an infected USB and transfers it to network-connected computer when the USB is inserted. |
| Component Object Model Hijacking | APT82 has used COM hijacking for persistence by replacing the legitimate MMDeviceEnumerator object with a payload. |
| Connection Proxy | APT82 used other victims as proxies to relay command traffic, for instance using a compromised Georgian military email server as a hop point to NATO victims. The group has also used a tool that acts as a proxy to allow C2 even if the victim is behind a router. APT82 has also used a machine to relay and obscure communications between CHOPSTICK and their server. |
| Credential Dumping | APT82 regularly deploys both publicly available and custom password retrieval tools on victims. |
| Custom Cryptographic Protocol | APT82 installed a Delphi backdoor that used a custom algorithm for C2 communications. |
| Data Compressed | APT82 used a publicly available tool to gather and compress multiple documents on the DCCC and DNC networks. |
| Data from Information Repositories | APT82 has collected information from Microsoft SharePoint services within target networks. |
| Data from Local System | APT82 has retrieved internal documents from machines inside victim environments, including by using Forfiles to stage documents before. |
| Data from Removable Media | An APT82 backdoor may collect the entire contents of an inserted USB device. |
| Data Obfuscation | APT82 added "junk data" to each encoded string, preventing trivial decoding without knowledge of the junk removal algorithm. Each implant was given a "junk length" value when created, tracked by the controller software to allow seamless communication but prevent analysis of the command protocol on the wire. |
| Data Staged | APT82 has stored captured credential information in a file named pi.log. |
| Deobfuscate/Decode Files or Information | An APT82 macro uses the command certutil -decode to decode contents of a .txt file storing the base64 encoded payload. |
| Dynamic Data Exchange | APT82 has delivered JHUHUGIT and Koadic by executing PowerShell commands through DDE in Word documents. |
| Email Collection | APT82 has collected emails from victim Microsoft Exchange servers. |
| Exploitation for Client Execution | APT82 has exploited Microsoft Office vulnerability CVE-2017-0262 for execution. |
| Exploitation for Defense Evasion | APT82 has used CVE-2015-42 to bypass security features. |
| Exploitation for Privilege Escalation | APT82 has exploited CVE-2014-4076, CVE-2015-237, CVE-2015-1701, CVE-2017-0263 to escalate privileges. |
| Exploitation of Remote Services | APT82 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement. |
| File and Directory Discovery | APT82 has used Forfiles to locate PDF, Excel, and Word documents during. The group also searched a compromised DCCC computer for specific terms. |
| File Deletion | APT82 has intentionally deleted computer files to cover their tracks, including with use of the program CCleaner. |
| Hidden Files and Directories | APT82 has saved files with hidden file attributes. |
| Indicator Removal on Host | APT82 has cleared event logs, including by using the commands wevtutil cl System and wevtutil cl Security. |
| Input Capture | APT82 has used tools to perform keylogging. |
| Logon Scripts | An APT82 loader Trojan adds the Registry key HKCU\Environment\UserInitMprLogonScript to establish persistence. |
| Network Sniffing | APT82 deployed the open source tool Responder to conduct NetBIOS Name Service poisoning, which captured usernames and hashed passwords that allowed access to legitimate credentials. |
| Obfuscated Files or Information | APT82 encrypted a .dll payload using RTL and a custom encryption algorithm. APT82 has also obfuscated payloads with base64, XOR, and RC4. |
| Office Application Startup | APT82 has used the Office Test persistence mechanism within Microsoft Office by adding the Registry key HKCU\Software\Microsoft\Office test\Special\Perf to execute code. 2 |
| Pass the Hash | APT82 has used pass the hash for lateral movement. |
| Peripheral Device Discovery | APT82 uses a module to receive a notification every time a USB mass storage device is inserted into a victim. |
| PowerShell | APT82 downloads and executes PowerShell scripts. |
| Process Discovery | An APT82 loader Trojan will enumerate the victim's processes searching for explorer.exe if its current process does not have necessary permissions. |
| Remote File Copy | APT82 has downloaded additional files, including by using a first-stage downloader to contact the C2 server to obtain the second-stage implant. |
| Replication Through Removable Media | APT82 uses a tool to infect connected USB devices and transmit itself to air-gapped computers when the infected USB device is inserted. |
| Rootkit | APT82 has used a UEFI (Unified Extensible Firmware Interface) rootkit known as LoJax. |
| Rundll32 | APT82 executed CHOPSTICK by using rundll32 commands such as rundll32.exe “C:\Windows\twain\_64.dll”. APT82 also executed a .dll for a first stage dropper using rundll32.exe. An APT82 loader Trojan saved a batch script that uses rundll32 to execute a DLL payload. |
| Screen Capture | APT82 has used tools to take screenshots from victims. |
| Scripting | An APT82 loader Trojan uses a batch script to run its payload. The group has also used macros to execute payloads. |
| Spearphishing Attachment | APT82 sent spearphishing emails containing malicious Microsoft Office attachments. |
| Spearphishing Link | APT82 sent spearphishing emails which used a URL-shortener service to masquerade as a legitimate service and to redirect targets to credential harvesting sites. |
| Standard Application Layer Protocol | APT82 used SMTP as a communication channel in various implants, initially using self-registered Google Mail accounts and later compromised email servers of its victims. Later implants such as CHOPSTICK use a blend of HTTP and other legitimate channels, depending on module configuration. |
| Template Injection | APT82 used weaponized Microsoft Word documents abusing the remote template function to retrieve a malicious macro. |
| Timestomp | APT82 has performed timestomping on victim files. |
| Trusted Relationship | Once APT82 gained access to the DCCC network, the group then proceeded to use that access to compromise the DNC network. |
| User Execution | APT82 attempted to get users to click on Microsoft Office attachments containing malicious macro scripts. |
| Valid Accounts | APT82 has used legitimate credentials to maintain access to a victim network and exfiltrate data. The group also used credentials stolen through a spearphishing email to login to the DCCC network. |

## 1.8 APT 82 Tool Functionality

|  |  |
| --- | --- |
| **Tool** | **Techniques** |
| ADVSTORESHELL | Command-Line Interface, Commonly Used Port, Component Object Model Hijacking, Data Compressed, Data Encoding, Data Encrypted, Data Staged, Execution through API, Exfiltration Over Command and Control Channel, File and Directory Discovery, File Deletion, Input Capture, Modify Registry, Obfuscated Files or Information, Peripheral Device Discovery, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Rundll32, Scheduled Transfer, Standard Application Layer Protocol, Standard Cryptographic Protocol, System Information Discovery |
| Cannon | Exfiltration Over Command and Control Channel, File and Directory Discovery, Process Discovery, Remote File Copy, Screen Capture, Standard Application Layer Protocol, System Information Discovery, System Owner/User Discovery, System Time Discovery, Uncommonly Used Port, Winlogon Helper DLL |
| certutil | Deobfuscate/Decode Files or Information, Install Root Certificate, Remote File Copy |
| CHOPSTICK | Command-Line Interface, Communication Through Removable Media, Connection Proxy, Domain Generation Algorithms, Fallback Channels, File and Directory Discovery, Input Capture, Modify Registry, Query Registry, Remote File Copy, Replication Through Removable Media, Screen Capture, Security Software Discovery, Standard Application Layer Protocol, Standard Cryptographic Protocol, Virtualization/Sandbox Evasion |
| CORESHELL | Binary Padding, Custom Cryptographic Protocol, Data Encoding, Obfuscated Files or Information, Registry Run Keys / Startup Folder, Remote File Copy, Rundll32, Standard Application Layer Protocol, System Information Discovery |
| DealersChoice | Exploitation for Client Execution, Scripting, Standard Application Layer Protocol |
| Forfiles | Data from Local System, File and Directory Discovery, Indirect Command Execution |
| HIDEDRV | Process Injection, Rootkit |
| JHUHUGIT | Clipboard Data, Component Object Model Hijacking, Data Encoding, Exploitation for Privilege Escalation, Fallback Channels, File Deletion, Logon Scripts, New Service, Obfuscated Files or Information, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Rundll32, Scheduled Task, Screen Capture, Scripting, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery |
| Koadic | Bypass User Account Control, Clipboard Data, Command-Line Interface, Credential Dumping, Data from Local System, Mshta, Network Service Scanning, Network Share Discovery, Process Injection, Regsvr32, Remote Desktop Protocol, Remote File Copy, Rundll32, Scripting, Service Execution, Standard Cryptographic Protocol, System Network Configuration Discovery, System Owner/User Discovery, Windows Management Instrumentation |
| Komplex | Custom Cryptographic Protocol, File Deletion, Hidden Files and Directories, Launch Agent, Process Discovery, Standard Application Layer Protocol, System Owner/User Discovery |
| LoJax | Modify Registry, NTFS File Attributes, Registry Run Keys / Startup Folder, Rootkit, System Firmware |
| Mimikatz | Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection |
| OLDBAIT | Credential Dumping, Masquerading, Obfuscated Files or Information, Standard Application Layer Protocol |
| Responder | LLMNR/NBT-NS Poisoning and Relay, Network Sniffing |
| USBStealer | Automated Collection, Automated Exfiltration, Communication Through Removable Media, Data from Removable Media, Data Staged, Exfiltration Over Physical Medium, File and Directory Discovery, File Deletion, Masquerading, Obfuscated Files or Information, Peripheral Device Discovery, Registry Run Keys / Startup Folder, Replication Through Removable Media, Timestomp |
| Winexe | Service Execution |
| X-Agent for Android | Location Tracking, Repackaged Application |
| XAgentOSX | Execution through API, File and Directory Discovery, File Deletion, Input Capture, Peripheral Device Discovery, Process Discovery, Screen Capture, Standard Application Layer Protocol, System Information Discovery, System Owner/User Discovery |
| XTunnel | Binary Padding, Command-Line Interface, Connection Proxy, Credentials in Files, Fallback Channels, Network Service Scanning, Obfuscated Files or Information, Remote File Copy, Standard Cryptographic Protocol |
| Zebrocy | Automated Collection, Command-Line Interface, Custom Command and Control Protocol, Data Encoding, Data Encrypted, Data Staged, Deobfuscate/Decode Files or Information, Exfiltration Over Command and Control Channel, File and Directory Discovery, File Deletion, Hooking, Logon Scripts, Network Share Discovery, Peripheral Device Discovery, Process Discovery, Query Registry, Registry Run Keys / Startup Folder, Remote File Copy, Screen Capture, Software Packing, Standard Application Layer Protocol, Standard Cryptographic Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Time Discovery, Uncommonly Used Port, Windows Management Instrumentation |

# Emulation Phases

## 2.1 Most likely:

*Spear phishing email or drive-by website with malicious weaponized payload (executive file, macro, link, etc.).*

## 2.2 Recommendation:

*Review/Search Download histories and Browser Histories.*

## 2.3 Indicators of compromise

### 2.3.1 IOC 1

*20191001:1103* – User: Andres.E.Caller visited a malicious website and caused a ‘Drive-By-Download’ of malicious file named ‘CHOST.exe’ on to workstation host 10.0.3.2

IR team manually found CHOST.exe on host

Support team scanned remaining boxes with Gh0stHunt framework, and found CHOST.exe on 10.0.3.24

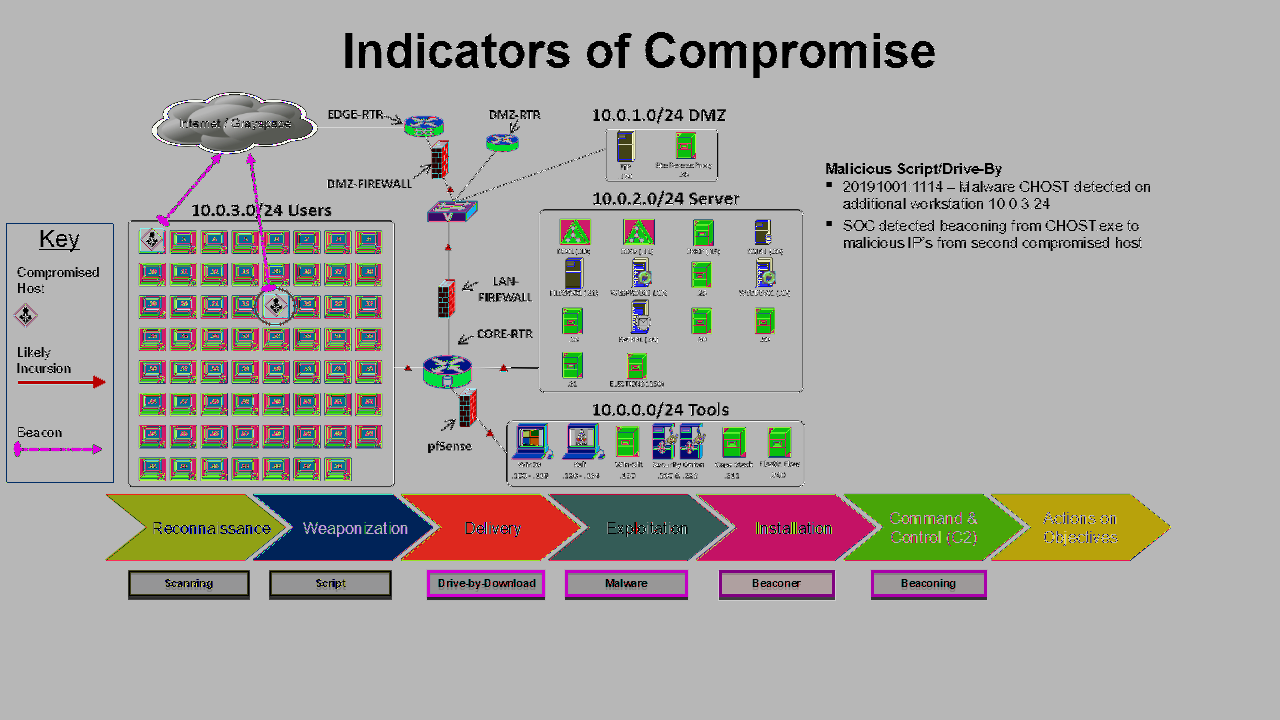
SOC detected beaconing from CHOST.exe to malicious IP’s which led to attribution.

### *2.3.2 IOC 2*

*Malicious Script/Drive-By*

*20191001:1114 – Malware CHOST detected on additional workstation 10.0.3.24*

*SOC detected beaconing from CHOST.exe to malicious IP’s from second compromised host*

**

### ***2.3.3 IOC 3***

***Boot Script***

20191002:1239 – DC02 found to be compromised via a scheduler exploit

20191002:1614 – DC01 anomalies revealed Kerberos likely compromised.

20191001:1730 – Finance workstation10.0.3.23 found to be compromised via a scheduler exploit

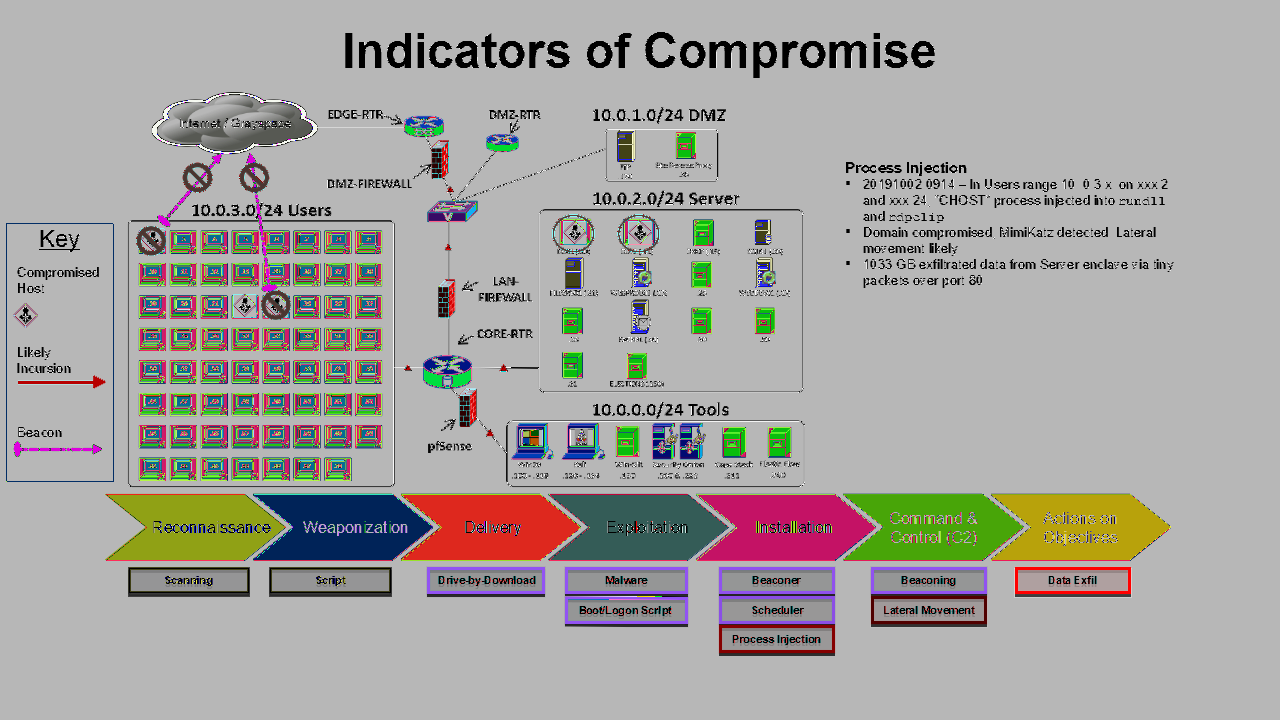
### ***2.3.4 IOC 4***

***Process Injection***

20191002:0914 – In Users range 10..0.3.x on xxx.2 and xxx.24, “CHOST” process injected into rundll and rdpclip

Domain compromised, MimiKatz detected. Lateral movement likely.

1033 GB exfiltrated data from Server enclave via tiny packets over port 80.

****

## 2.4 Attribution

**Attribution**

Threat actors believed to be using Cobalt Strike or similar tool.

**Supporting Evidence for *Cobalt Strike***

Process injection in VDS.exe connecting to identical remote IPs as CHOST.exe pointing to C2 activity

LSASS injection indicates Pass the Hash and use of MimiKatz

Base64 Encoded string on DC01 indicates encoded use of Sysinternals PSEXEC and Powershell

## 2.5 Phase 1 - RECON

The attack starts with a drive by download of a malicious weaponized payload from a compromised website. This establishes a beachhead on a then compromised workstation from which C2 is established via a beacon. Once APT 82 has reliable C2, their objective becomes to establish additional beachheads to solidify persistence and perform actions on the objective.

## 2.6 Phase 2 - SCANNING

APT 82 registered domains imitating NATO and OSCE security websites and Caucasus information resources. It is assumed they will repeat this practice to compromise Polandia.

APT 82 reused the SOURFACE downloader as the payload of a lure document. This or a similar technique will likely be used to perform internal scans and network mapping once a host is compromised.

## 2.7 Phase 3 - EXPLOITATION

APT 82 has exploited Microsoft Office vulnerability CVE-2017-0262 for execution.

APT 82 has used CVE-2015-42 to bypass security features.

APT 82 has exploited CVE-2014-4076, CVE-2015-237, CVE-2015-1701, CVE-2017-0263 to escalate privileges.

APT 82 exploited a Windows SMB Remote Code Execution Vulnerability to conduct lateral movement.

Tools used may include DealersChoice and JHUHUGIT among others.

# Bibliography

Mueller, R. (2018, July 13). Indictment - United States of America vs. VIKTOR BORISOVICH NETYKSHO, et al. Retrieved September 13, 2018.

Gallagher, S. (2018, July 27). How they did it (and will likely try again): GRU hackers vs. US elections. Retrieved September 13, 2018.

Alperovitch, D.. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. Retrieved August 3, 2016.

FireEye. (2015). APT 82: A WINDOW INTO RUSSIA’S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015.

SecureWorks Counter Threat Unit Threat Intelligence. (2016, June 16). Threat Group-4127 Targets Hillary Clinton Presidential Campaign. Retrieved August 3, 2016.

FireEye iSIGHT Intelligence. (2017, January 11). APT 82: At the Center of the Storm. Retrieved January 11, 2017.

Department of Homeland Security and Federal Bureau of Investigation. (2016, December 29). GRIZZLY STEPPE – Russian Malicious Cyber Activity. Retrieved January 11, 2017.

Falcone, R. (2018, March 15). Sofacy Uses DealersChoice to Target European Government Agency. Retrieved June 4, 2018.

Lee, B., Falcone, R. (2018, June 06). Sofacy Group’s Parallel Attacks. Retrieved June 18, 2018.

Symantec Security Response. (2018, October 04). APT 82: New Espionage Operations Target Military and Government Organizations. Retrieved November 14, 2018.

ESET Research. (2019, May 22). A journey to Zebrocy land. Retrieved June 20, 2019.

Anthe, C. et al. (2015, October 19). Microsoft Security Intelligence Report Volume 19. Retrieved December 23, 2015.

Bitdefender. (2015, December). APT 82 Under the Scope. Retrieved February 23, 2017.

Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.

Accenture Security. (2018, November 29). SNAKEMACKEREL. Retrieved April 15, 2019.

Sherstobitoff, R., Rea, M. (2017, November 7). Threat Group APT 82 Slips Office Malware into Doc Citing NYC Terror Attack. Retrieved November 21, 2017.

Paganini, P. (2017, November 9). Russia-Linked APT 82 group observed using DDE attack to deliver malware. Retrieved November 21, 2017.

Mercer, W., et al. (2017, October 22). "Cyber Conflict" Decoy Document Used in Real Cyber Conflict. Retrieved November 2, 2018.

ESET. (2016, October). En Route with Sednit - Part 2: Observing the Comings and Goings. Retrieved November 21, 2016.

Guarnieri, C. (2015, June 19). Digital Attack on German Parliament: Investigative Report on the Hack of the Left Party Infrastructure in Bundestag. Retrieved January 22, 2018.

Lee, B, et al. (2018, February 28). Sofacy Attacks Multiple Government Entities. Retrieved March 15, 2018.

ESET. (2016, October). En Route with Sednit - Part 1: Approaching the Target. Retrieved November 8, 2016.

Kaspersky Lab's Global Research & Analysis Team. (2018, February 20). A Slice of 2017 Sofacy Activity. Retrieved November 27, 2018.

Maccaglia, S. (2015, November 4). Evolving Threats: dissection of a CyberEspionage attack. Retrieved April 4, 2018.

Smith, L. and Read, B.. (2017, August 11). APT 82 Targets Hospitality Sector, Presents Threat to Travelers. Retrieved August 17, 2017.

ESET. (2016, October). En Route with Sednit - Part 3: A Mysterious Downloader. Retrieved November 21, 2016.

FireEye Labs. (2015, April 18). Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia’s APT 82 in Highly-Targeted Attack. Retrieved April 24, 2017.

Hacquebord, F.. (2017, April 25). Two Years of Pawn Storm: Examining an Increasingly Relevant Threat. Retrieved May 3, 2017.

ESET. (2018, September). LOJAX First UEFI rootkit found in the wild, courtesy of the Sednit group. Retrieved July 2, 2019.

Falcone, R., Lee, B. (2018, November 20). Sofacy Continues Global Attacks and Wheels Out New ‘Cannon’ Trojan. Retrieved November 26, 2018.

Microsoft. (2017, March 14). Microsoft Security Bulletin MS17-010 - Critical. Retrieved August 17, 2017.

Falcone, R. (2016, July 20). Technical Walkthrough: Office Test Persistence Method Used In Recent Sofacy Attacks. Retrieved July 3, 2017.

Lee, B., Falcone, R. (2018, December 12). Dear Joohn: The Sofacy Group’s Global Campaign. Retrieved April 19, 2019.

Kaspersky Lab's Global Research and Analysis Team. (2015, December 4). Sofacy APT hits high profile targets with updated toolset. Retrieved December 10, 2015.

Robert Falcone. (2017, February 14). XAgentOSX: Sofacy's Xagent macOS Tool. Retrieved July 12, 2017.

Dani Creus, Tyler Halfpop, Robert Falcone. (2016, September 26). Sofacy's 'Komplex' OS X Trojan. Retrieved July 8, 2017.

CrowdStrike Global Intelligence Team. (2016). Use of Fancy Bear Android Malware in Tracking of Ukrainian FIeld Artillery Units. Retrieved February 6, 2017.

# Appendix

**Hardening recommendations:**

**Network**

Implement Access control lists within routers/Firewalls:

Access control lists should be defined permitting only the required traffic

Reduce risk of unauthorized lateral movement

Deny externally established connections into Network

Harden Router/Firewall User Account Access

Restrict management access to a defined list of internal hosts, using only encrypted protocol such as SSH

**Workstations**

Disable administrator accounts on machines

Disable guest accounts

Remove miscellaneous accounts

Disable all unnecessary services

Enable host firewalls & ensure all system firewalls are turned on with standardized rules

Update workstations with latest patches

Microsoft patches

All other vendor patches

**Servers**

Create a backup of the database instance

Reassign the MSSQL to a non-standard port

Turn off SQL Server browser service

Turn off named pipes

Disable unnecessary services

Restrict access to the DB backup

Patch the system to the latest KB

**Active Directory**

Enable Windows Firewalls for domain client machines

Disable HTTP listeners and use WinRM over HTTPS

Deploy Sysmon to monitor AD domain controllers

Deny user write to unauthorized locations

Enforce strong password policy

Complex password required

Enforce Password expiration

Password age set to 60 days to lock inactive accounts