|  |
| --- |
|  |
| **Cyber Protection Team 175 Threat Emulation Plan: APT 92** |
| **OPERATION GRUNGY PAINT III** |
| **03 OCT 2019** |
|  |
| **1.0.0** |



**Table of Contents**

[Threat Emulation Plan: APT92 | Komitet Cyber Bureau (KCB) 2](#__RefHeading___Toc1431_3799018206)

[1 APT92 Overview 2](#__RefHeading___Toc1433_3799018206)

[1.1 APT92 Tools and Techniques 3](#__RefHeading___Toc1435_3799018206)

[1.2 APT92 Tool Functionality 5](#__RefHeading___Toc1437_3799018206)

[2 Emulation Phases 7](#__RefHeading___Toc1439_3799018206)

[2.1 Phase 1 - RECON 7](#__RefHeading___Toc1441_3799018206)

[2.2 Phase 2 - SCANNING 7](#__RefHeading___Toc1443_3799018206)

[2.3 Phase 3 - EXPLOITATION 8](#__RefHeading___Toc1445_3799018206)

[3 Bibliography 8](#__RefHeading___Toc1447_3799018206)

[4 Appendix 8](#__RefHeading___Toc1449_3799018206)

# Threat Emulation Plan: APT92 | Komitet Cyber Bureau (KCB)



# APT92 Overview

*In 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.*

**MITRE ATT&CK Group ID: APT92**

**Aliases:** YTTRIUM, The Dukes, Cozy Bear, CozyDuke, APT29, Komitet Cyber Burea (KCB)

**Operations:** APT92 aka Komitet Cyber Bureau (KCB) is an organic APT82n government cyber agency with a cadre of aging coldwar era agents; their expertise resides almost entirely in penetrating now outdated European government systems. They have been known to:

* Gain access to networks through deployments of remote server based C2 clients (e.g. SeaDaddy implant developed in Python, X-Agent malware with remote command execution, file transmission and keylogging capabilities) by means of drive-by or phishing vectors.
* Enumerate access and conduct privilege escalation on the victim networks sophisticated power shell techniques.
* Leverage another Powershell backdoor with persistence accomplished via Windows Management Instrumentation (WMI) system.
* Engaging in a number of anti-forensic analysis measures to evade detection, such as periodic event log clearing (via wevtutil cl System and wevtutil cl Security commands) and resetting timestamps of files.
* Exfiltrating sensitive data via compressed and encoded packets over port 80 or port 53 for the purposes of political scandal or coercion.

**Target Industries:** Government entities, agencies, and infrastructure to disrupt the democratic process

**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.

**Background:**

APT92 is threat group that has been attributed to the Polandian government and has operated since at least 2008. This group reportedly compromised the US Democratic National Committee starting in the summer of 2015.

## APT92 **Tools and Techniques**

*APT92 employs these tools and techniques:*

|  |  |
| --- | --- |
| **Techniques Used** | **Use** |
| Accessibility Features | APT92 used sticky-keys to obtain unauthenticated, privileged console access. |
| Bypass User Account Control | APT92 has bypassed UAC. |
| Commonly Used Port | APT92 has used Port Number 443 for C2. |
| Domain Fronting | APT92 has used the meek domain fronting plugin for Tor to hide the destination of C2 traffic. |
| Exploitation for Client Execution | APT92 has used multiple software exploits for common client software, like Microsoft Word and Adobe Reader, to gain code execution as part of. |
| File Deletion | APT92 used SDelete to remove artifacts from victims. |
| Indicator Removal on Host | APT92 used SDelete to remove artifacts from victims. |
| Multi-hop Proxy | A backdoor used by APT92 created a Tor hidden service to forward traffic from the Tor client to local ports 3389 (RDP), 139 (Netbios), and 445 (SMB) enabling full remote access from outside the network. |
| Obfuscated Files or Information | APT92 uses PowerShell to use Base64 for obfuscation. |
| Pass the Ticket | APT92 used Kerberos ticket attacks for lateral movement. |
| PowerShell | APT92 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke. APT92 also used PowerShell scripts to evade defenses. |
| Registry Run Keys / Startup Folder | APT92 added Registry Run keys to establish persistence. |
| Rundll32 | APT92 has used rundll32.exe for execution. |
| Scheduled Task | APT92 used named and hijacked scheduled tasks to establish persistence. |
| Scripting | APT92 has used encoded PowerShell scripts uploaded to CozyCar installations to download and install SeaDuke, as well as to evade defenses. |
| Shortcut Modification | APT92 drops a Windows shortcut file for execution. |
| Software Packing | APT92 used UPX to pack files. |
| Spearphishing Attachment | APT92 has used spearphishing emails with an attachment to deliver files with exploits to initial victims. |
| Spearphishing Link | APT92 has used spearphishing with a link to trick victims into clicking on a link to a zip file containing malicious files. |
| Standard Non-Application Layer Protocol | APT92 uses TCP for C2 communications. |
| User Execution | APT92 has used various forms of spearphishing attempting to get a user to open links or attachments, including, but not limited to, malicious Microsoft Word documents, .pdf, and .lnk files. |
| Windows Management Instrumentation | APT92 used WMI to steal credentials and execute backdoors at a future time. |
| Windows Management Instrumentation Event Subscription | APT92 has used WMI event filters to establish persistence. |

## APT92 Tool Functionality

|  |  |
| --- | --- |
| **Tool** | **Techniques** |
| CloudDuke | Remote File Copy, Standard Application Layer Protocol, Web Service |
| Cobalt Strike | Access Token Manipulation, BITS Jobs, Bypass User Account Control, Command-Line Interface, Commonly Used Port, Connection Proxy, Credential Dumping, Custom Command and Control Protocol, Data from Local System, Distributed Component Object Model, Execution through API, Exploitation for Privilege Escalation, Indicator Removal from Tools, Input Capture, Man in the Browser, Multiband Communication, Network Service Scanning, Network Share Discovery, New Service, Pass the Hash, PowerShell, Process Discovery, Process Hollowing, Process Injection, Remote Desktop Protocol, Remote Services, Remote System Discovery, Scheduled Transfer, Screen Capture, Scripting, Service Execution, Standard Application Layer Protocol, Timestomp, Valid Accounts, Windows Admin Shares, Windows Management Instrumentation, Windows Remote Management |
| CosmicDuke | Automated Exfiltration, Clipboard Data, Credential Dumping, Custom Cryptographic Protocol, Data from Local System, Data from Network Shared Drive, Data from Removable Media, Email Collection, Exfiltration Over Alternative Protocol, Exploitation for Privilege Escalation, File and Directory Discovery, Input Capture, New Service, Scheduled Task, Screen Capture, Standard Application Layer Protocol |
| CozyCar | Command-Line Interface, Credential Dumping, Masquerading, New Service, Obfuscated Files or Information, Registry Run Keys / Startup Folder, Rundll32, Scheduled Task, Security Software Discovery, Standard Application Layer Protocol, System Information Discovery, Virtualization/Sandbox Evasion, Web Service |
| GeminiDuke | Account Discovery, File and Directory Discovery, Process Discovery, Standard Application Layer Protocol, System Network Configuration Discovery, System Service Discovery |
| HAMMERTOSS | Custom Cryptographic Protocol, Data Obfuscation, Exfiltration Over Alternative Protocol, PowerShell, Standard Application Layer Protocol, Web Service |
| meek | Domain Fronting |
| Mimikatz | Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection |
| MiniDuke | Fallback Channels, Remote File Copy, Standard Application Layer Protocol, Web Service |
| OnionDuke | Credential Dumping, Standard Application Layer Protocol, Web Service |
| PinchDuke | Credential Dumping, Data from Local System, File and Directory Discovery, Standard Application Layer Protocol, System Information Discovery |
| POSHSPY | Data Transfer Size Limits, Domain Generation Algorithms, Obfuscated Files or Information, PowerShell, Remote File Copy, Standard Cryptographic Protocol, Timestomp, Windows Management Instrumentation Event Subscription |
| PowerDuke | Application Window Discovery, Command-Line Interface, Commonly Used Port, Data Destruction, File and Directory Discovery, File Deletion, NTFS File Attributes, Obfuscated Files or Information, Process Discovery, Registry Run Keys / Startup Folder, Remote File Copy, Rundll32, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, System Time Discovery |
| PsExec | Service Execution, Windows Admin Shares |
| SDelete | Code Signing, Data Destruction, File Deletion |
| SeaDuke | Command-Line Interface, Data Compressed, Data Encoding, Email Collection, File Deletion, Pass the Ticket, PowerShell, Registry Run Keys / Startup Folder, Remote File Copy, Scripting, Shortcut Modification, Software Packing, Standard Application Layer Protocol, Standard Cryptographic Protocol, Valid Accounts, Windows Management Instrumentation Event Subscription |
| Tor | Multi-hop Proxy, Multilayer Encryption |

# Emulation Phases

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

***Recommendation:*** *Review/Search Download histories and Browser Histories.*

**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

## 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 APT92 has reliable C2, their objective becomes to establish additional beachheads to solidify persistence and perform actions on the objective.

## Phase 2 - SCANNING

APT92 has gained access to networks via very sophisticated spear phishing campaigns, usually disguised as emails concerning political financial contributions, which trigger deployments of remote server based C2 clients such as SeaDaddy implant developed in Python, and X-Agent malware with remote command execution, file transmission, and keylogging capabilities.

## Phase 3 - EXPLOITATION

APT92 has used spearphishing emails with an attachment to deliver files with exploits to initial victims.

APT92 has used multiple software exploits for common client software, like Microsoft Word and Adobe Reader, to gain code execution.

Tools used may include Cobalt Strike and CosmicDuke among others.

# Bibliography

F-Secure Labs. (2015, September 17). The Dukes: 7 years of Russian cyberespionage. Retrieved December 10, 2015.

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

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

Dunwoody, M. and Carr, N.. (2016, September 27). No Easy Breach DerbyCon 2016. Retrieved October 4, 2016.

Symantec Security Response. (2015, July 13). “Forkmeiamfamous”: Seaduke, latest weapon in the Duke armory. Retrieved July 22, 2015.

Dunwoody, M. (2017, March 27). APT92 Domain Fronting With TOR. Retrieved March 27, 2017.

Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT92 Phishing Campaign. Retrieved November 27, 2018.

Adair, S.. (2016, November 9). PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs. Retrieved January 11, 2017.

Dunwoody, M.. (2017, April 3). Dissecting One of APT92’s Fileless WMI and PowerShell Backdoors (POSHSPY). Retrieved April 5, 2017.

Microsoft Defender Research Team. (2018, December 3). Analysis of cyberattack on U.S. think tanks, non-profits, public sector by unidentified attackers. Retrieved April 15, 2019.

# 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