|  |
| --- |
|  |
| **Cyber Protection Team 175 Threat Emulation Plan: Skript-Kit-Eaze** |
| **OPERATION GRUNGY PAINT III** |
| **03 OCT 2019** |
|  |
| **1.0.0** |



Table of Contents

[Threat Emulation Plan: Skript-Kit-Eaze 2](#__RefHeading___Toc1431_3799018206)

[1 Skript-Kit-Eaze Overview 2](#__RefHeading___Toc1433_3799018206)

[1.1 Skript-Kit-Eaze Tools and Techniques 3](#__RefHeading___Toc1435_3799018206)

[1.2 Skript-Kit-Eaze Tool Functionality 6](#__RefHeading___Toc1437_3799018206)

[2 Emulation Phases 9](#__RefHeading___Toc1439_3799018206)

[2.1 Phase 1 - RECON 9](#__RefHeading___Toc1441_3799018206)

[2.2 Phase 2 - SCANNING 9](#__RefHeading___Toc1443_3799018206)

[2.3 Phase 3 - EXPLOITATION 9](#__RefHeading___Toc1445_3799018206)

[3 Bibliography 9](#__RefHeading___Toc1447_3799018206)

[4 Appendix 10](#__RefHeading___Toc1449_3799018206)

# Threat Emulation Plan: Skript-Kit-Eaze



# Skript-Kit-Eaze 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: Skript-Kit-Eaze**

**Aliases:** Waterbug, WhiteBear, VENOMOUS BEAR, Snake, Krypton, Script Kitties, MoronChan, Script Kiddies, Skript-Kit-Eaze

**Operations:** Skript-Kit-Eaze is the designation for individuals who are not aligned with any known threat actors. They have their own individual views and work independently or in small groups.

**Target Industries:** Government entities, agencies, and contractors as well as critical infrastructure in addition to private enterprise or private individuals who they feel do not conform to their individual world view.

**Objectives:** Social disruption, social awareness, social justice, personal vengeance, general malfeasance.

**Background:** Skript-Kit-Eaze are a blend of loosely affiliated or completely unaffiliated individuals from nearly every continent. Communication can be by any channel including Roman ciphers in classified ads and mailed paper letters. Turla has infected victims in over 45 countries, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies since 2004. Heightened activity was seen in mid-2015. Turla is known for conducting watering hole and spear phishing campaigns and leveraging in-house tools and malware..

## Skript-Kit-Eaze **Tools and Techniques**

*Skript-Kit-Eaze employs these tools and techniques:*

|  |  |
| --- | --- |
| **Techniques Used** | **Use** |
| Access Token Manipulation | Skript-Kit-Eaze RPC backdoors can impersonate or steal process tokens before executing commands. |
| Brute Force | Skript-Kit-Eaze may attempt to connect to systems within a victim's network using net use commands and a predefined list or collection of passwords. |
| Command-Line Interface | Skript-Kit-Eaze RPC backdoors have used cmd.exe to execute commands. |
| Connection Proxy | Skript-Kit-Eaze RPC backdoors have included local UPnP RPC proxies. |
| Credentials in Files | Skript-Kit-Eaze has gathered credentials from the Windows Credential Manager tool. |
| Data Encrypted | Skript-Kit-Eaze has encrypted files stolen from connected USB drives into a RAR file before exfiltration. |
| Data from Local System | Skript-Kit-Eaze RPC backdoors can upload files from victim machines. |
| Data from Removable Media | Skript-Kit-Eaze RPC backdoors can collect files from USB thumb drives. |
| Deobfuscate/Decode Files or Information | Skript-Kit-Eaze has used a custom decryption routine, which pulls key and salt values from other artifacts such as a WMI filter or PowerShell Profile, to decode encrypted PowerShell payloads. |
| Disabling Security Tools | Skript-Kit-Eaze has used a AMSI bypass, which patches the in-memory amsi.dll, in PowerShell scripts to bypass Windows antimalware products. |
| Execution through API | Skript-Kit-Eaze and its RPC backdoors have used APIs calls for various tasks related to subverting AMSI and accessing then executing commands through RPC and/or named pipes. |
| Exfiltration Over Alternative Protocol | Skript-Kit-Eaze has used WebDAV to upload stolen USB files to a cloud drive. |
| File and Directory Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover files in specific locations on the hard disk %TEMP% directory, the current user's desktop, and in the Program Files directory. Skript-Kit-Eaze RPC backdoors have also searched for files matching the lPH\*.dll pattern. |
| Indicator Removal from Tools | Based on comparison of Gazer versions, Skript-Kit-Eaze made an effort to obfuscate strings in the malware that could be used as IoCs, including the mutex name and named pipe. |
| Modify Registry | Skript-Kit-Eaze has used the Registry to store encrypted payloads. |
| Obfuscated Files or Information | Skript-Kit-Eaze has used encryption (including salted 3DES via PowerSploit's Out-EncryptedScript.ps1), random variable names, and base64 encoding to obfuscate PowerShell commands and payloads. |
| PowerShell | Skript-Kit-Eaze has used PowerShell to execute commands/scripts, in some cases via a custom executable or code from Empire's PSInject. Skript-Kit-Eaze has also used PowerShell scripts to load and execute malware in memory. |
| Process Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover running processes using the tasklist /v command. Skript-Kit-Eaze RPC backdoors have also enumerated processes associated with specific open ports or named pipes. |
| Process Injection | Skript-Kit-Eaze has used Metasploit to perform reflective DLL injection in order to escalate privileges. Skript-Kit-Eaze has also used PowerSploit's Invoke-ReflectivePEInjection.ps1 to reflectively load a PowerShell payload into a random process on the victim system. |
| Query Registry | Skript-Kit-Eaze surveys a system upon check-in to discover information in the Windows Registry with the reg query command. Skript-Kit-Eaze has also retrieved PowerShell payloads hidden in Registry keys as well as checking keys associated with null session named pipes . |
| Registry Run Keys / Startup Folder | A Skript-Kit-Eaze Javascript backdoor added a local\_update\_check value under the Registry key HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run to establish persistence. Additionally, a Skript-Kit-Eaze custom executable containing Metasploit shellcode is saved to the Startup folder to gain persistence. |
| Remote File Copy | Skript-Kit-Eaze has used shellcode to download Meterpreter after compromising a victim. Skript-Kit-Eaze RPC backdoors can also download files onto victim machines. |
| Remote System Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover remote systems on a local network using the net view and net view /DOMAIN commands. |
| Scripting | Skript-Kit-Eaze has used PowerShell and VBS scripts throughout its operations. |
| Spearphishing Attachment | Skript-Kit-Eaze has used spearphishing emails to deliver BrainTest as a malicious attachment. |
| Spearphishing Link | Skript-Kit-Eaze attempted to trick targets into clicking on a link featuring a seemingly legitimate domain from Adobe.com to download their malware and gain initial access. |
| Standard Application Layer Protocol | Skript-Kit-Eaze has used HTTP and HTTPS for C2 communications. |
| System Information Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover operating system configuration details using the systeminfo and set commands. |
| System Network Configuration Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover network configuration details using the arp -a, nbtstat -n, nbtscan, and net config commands. Skript-Kit-Eaze RPC backdoors have also retrieved registered RPC interface information from process memory. |
| System Network Connections Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover active local network connections using the netstat -an, net use, net file, and net session commands. Skript-Kit-Eaze RPC backdoors have also enumerated the IPv4 TCP connection table via the GetTcpTable2 API call. |
| System Service Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover running services and associated processes using the tasklist /svc command. |
| System Time Discovery | Skript-Kit-Eaze surveys a system upon check-in to discover the system time by using the net time command. |
| User Execution | Skript-Kit-Eaze has used spearphishing via a link to get users to download and run their malware. |
| Web Service | A Skript-Kit-Eaze JavaScript backdoor has used Google Apps Script as its C2 server. |
| Windows Admin Shares | Skript-Kit-Eaze used net use commands to connect to lateral systems within a network. |
| Windows Management Instrumentation Event Subscription | Skript-Kit-Eaze has used WMI event filters and consumers to establish persistence. |
| Winlogon Helper DLL | Skript-Kit-Eaze established persistence by adding a Shell value under the Registry key HKCU\Software\Microsoft\Windows NT\CurrentVersionWinlogon. |

## Skript-Kit-Eaze Tool Functionality

|  |  |
| --- | --- |
| **Tool** | **Techniques** |
| Arp | System Network Configuration Discovery |
| Carbon | Account Discovery, Commonly Used Port, Data Staged, Deobfuscate/Decode Files or Information, Exfiltration Over Alternative Protocol, New Service, Obfuscated Files or Information, Process Discovery, Process Injection, Query Registry, Remote System Discovery, Scheduled Task, Standard Non-Application Layer Protocol, System Network Configuration Discovery, System Network Connections Discovery, System Time Discovery |
| certutil | Deobfuscate/Decode Files or Information, Install Root Certificate, Remote File Copy |
| ComRAT | Component Object Model Hijacking, Standard Application Layer Protocol |
| Empire | Access Token Manipulation, Accessibility Features, Account Discovery, Browser Bookmark Discovery, Bypass User Account Control, Clipboard Data, Command-Line Interface, Commonly Used Port, Create Account, Credential Dumping, Credentials in Files, Data Compressed, Distributed Component Object Model, DLL Search Order Hijacking, Domain Trust Discovery, Email Collection, Execution through API, Exfiltration Over Alternative Protocol, Exfiltration Over Command and Control Channel, Exploitation for Privilege Escalation, Exploitation of Remote Services, File and Directory Discovery, Group Policy Modification, Hooking, Input Capture, Kerberoasting, LLMNR/NBT-NS Poisoning and Relay, Modify Existing Service, Network Service Scanning, Network Share Discovery, Network Sniffing, Obfuscated Files or Information, Pass the Hash, Pass the Ticket, Path Interception, PowerShell, Private Keys, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Remote Services, Scheduled Task, Screen Capture, Scripting, Security Software Discovery, Security Support Provider, Service Execution, Shortcut Modification, SID-History Injection, Standard Application Layer Protocol, Standard Cryptographic Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, Timestomp, Trusted Developer Utilities, Video Capture, Web Service, Windows Management Instrumentation |
| Epic | Account Discovery, Code Signing, Data Compressed, Data Encrypted, Extra Window Memory Injection, File and Directory Discovery, File Deletion, Obfuscated Files or Information, Permission Groups Discovery, Process Discovery, Query Registry, Remote System Discovery, Security Software Discovery, Standard Application Layer Protocol, Standard Cryptographic Protocol, System Information Discovery, System Network Configuration Discovery, System Network Connections Discovery, System Owner/User Discovery, System Service Discovery, System Time Discovery |
| Gazer | Code Signing, Connection Proxy, Custom Cryptographic Protocol, File Deletion, NTFS File Attributes, Obfuscated Files or Information, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Scheduled Task, Screensaver, Shortcut Modification, Standard Application Layer Protocol, System Owner/User Discovery, Timestomp, Winlogon Helper DLL |
| Kazuar | Account Discovery, Application Window Discovery, Command-Line Interface, Data Destruction, Data Encoding, Data from Local System, Data Staged, Fallback Channels, File and Directory Discovery, File Deletion, New Service, Obfuscated Files or Information, Permission Groups Discovery, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, Remote File Copy, Scheduled Transfer, Screen Capture, Shortcut Modification, Standard Application Layer Protocol, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery, Video Capture, Web Service, Windows Management Instrumentation |
| LightNeuron | Automated Collection, Automated Exfiltration, Command-Line Interface, Data Encrypted, Data from Local System, Data Obfuscation, Data Staged, Deobfuscate/Decode Files or Information, Email Collection, Execution through API, Exfiltration Over Command and Control Channel, File Deletion, Masquerading, Obfuscated Files or Information, Remote File Copy, Scheduled Transfer, Standard Application Layer Protocol, Standard Cryptographic Protocol, System Information Discovery, System Network Configuration Discovery, Transmitted Data Manipulation |
| Mimikatz | Account Manipulation, Credential Dumping, Credentials in Files, DCShadow, Pass the Hash, Pass the Ticket, Private Keys, Security Support Provider, SID-History Injection |
| Mosquito | Command-Line Interface, Component Object Model Hijacking, Custom Cryptographic Protocol, Execution through API, File Deletion, Modify Registry, Obfuscated Files or Information, PowerShell, Process Discovery, Registry Run Keys / Startup Folder, Remote File Copy, Rundll32, Security Software Discovery, System Network Configuration Discovery, System Owner/User Discovery, Windows Management Instrumentation |
| nbtstat | System Network Configuration Discovery, System Network Connections Discovery |
| Net | Account Discovery, Create Account, Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery, Remote System Discovery, Service Execution, System Network Connections Discovery, System Service Discovery, System Time Discovery, Windows Admin Shares |
| netstat | System Network Connections Discovery |
| PowerStallion | Obfuscated Files or Information, PowerShell, Process Discovery, Scripting, Timestomp, Web Service |
| PsExec | Service Execution, Windows Admin Shares |
| Reg | Credentials in Registry, Modify Registry, Query Registry |
| Systeminfo | System Information Discovery |
| Tasklist | Process Discovery, Security Software Discovery, System Service Discovery |
| Uroburos | Rootkit, Software Packing |

# Emulation Phases

***Most likely:*** *Social engineering attacks are common. “Mob mentality” techniques can be effective on social media. Skript-Kit-Eaze are notorious for hacking into unpatched systems with poor firewall rules and no anti-virus in Polandia.*

***Recommendation:*** *Review/Search Download histories and Browser Histories. Educate users on social engineering techniques. Harden and monitor vulnerable ICS/SCADA systems.*

## Phase 1 - RECON

The attack starts with a target reputation on social media, in chat rooms, and on blogs as well as on public social media channels about their intended target.

## Phase 2 - SCANNING

Skript-Kit-Eaze have initiated successful crowd sourced or cloud based DDOS attacks against individual targets using commonly available Hacking tools such as Low Orbit Ion Cannon and have successfully compromised social media accounts.

## Phase 3 - EXPLOITATION

Skript-Kit-Eaze rely on publically available hacking tools and scripts and use them or other commonly available hacking tools. The majority of attacks are not sophisticated.

# Bibliography

Kaspersky Lab's Global Research and Analysis Team. (2014, August 7). The Epic Turla Operation: Solving some of the mysteries of Snake/Uroburos. Retrieved December 11, 2014.

ESET. (2017, August). Gazing at Gazer: Turla’s new second stage backdoor. Retrieved September 14, 2017.

Meyers, A. (2018, March 12). Meet CrowdStrike’s Adversary of the Month for March: VENOMOUS BEAR. Retrieved May 16, 2018.

ESET, et al. (2018, January). Diplomats in Eastern Europe bitten by a Turla mosquito. Retrieved July 3, 2018.

Faou, M. and Dumont R.. (2019, May 29). A dive into Turla PowerShell usage. Retrieved June 14, 2019.

ESET Research. (2018, May 22). Turla Mosquito: A shift towards more generic tools. Retrieved July 3, 2018.

Symantec DeepSight Adversary Intelligence Team. (2019, June 20). Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments. Retrieved July 8, 2019.

Rapid7. (2013, November 26). meterpreter/source/extensions/priv/server/elevate/. Retrieved July 8, 2018.

ESET. (2017, March 30). Carbon Paper: Peering into Turla’s second stage backdoor. Retrieved November 7, 2018.

ESET. (2018, August). Turla Outlook Backdoor: Analysis of an unusual Turla backdoor. Retrieved March 11, 2019.

Levene, B, et al. (2017, May 03). Kazuar: Multiplatform Espionage Backdoor with API Access. Retrieved July 17, 2018.

Symantec. (2015, January 26). The Waterbug attack group. Retrieved April 10, 2015.

Faou, M. (2019, May). Turla LightNeuron: One email away from remote code execution. Retrieved June 24, 2019.

Kaspersky Lab's Global Research & Analysis Team. (2017, August 30). Introducing WhiteBear. Retrieved September 21, 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

**ICS/SCADA**

There are too many recommendations to make a comprehensive list here. The general recommendation is to implement all “best practices” recommendations from ICS-Cert in the following areas.

Creating Cyber Forensics Plans for Control Systems

Developing an Industrial Control Systems Cybersecurity Incident Response Plan

Good Practice Guide for Firewall Deployment on SCADA and Process Control Networks

Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies

Patch Management for Control Systems

Recommended Practice Case Study:  Cross-Site Scripting

Remote Access for Industrial Control Systems

Securing Control System Modems

Updating Antivirus in an Industrial Control System