OSINT Investigation Log v0.02

CMIT-450-81: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

10.16.2025

Research Question

How do malware campaigns use malicious advertising to spread malware through fake download sites?

Confirmed Malicious Domain #1

Basic Information

Domain: puttyssh.run
URL: http://puttyssh.run/files/Putty-Setup_v1.23.exe
Status: Confirmed Malicious
Source: https://urlscan.io/result/0198a075-44f2-70bc-95c1-e0b3346508ff/
VirusITotal Detections: 50/72 vendors
Date First Seen: 2025-08-12T22.44.56Z
Date Last Seen:
IP Address: 104.21.16.48

Malicious Activity

Downloads: Putty-Setup_ v1.23exe
File Hash:512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6

Additional Reports

https://tria.ge/s?q=sha256%3A512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6
https://analyze.intezer.com/files/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6
https://bazaar.abuse.ch/sample/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6
https://www.virustotal.com/gui/file/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6/detection
https://hybrid-analysis.com/sample/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6

Verdicts

Triage: 8/10 (Execution, Persistence)
Intezer: Suspicious, Probably Packed
MalwareBazaar: 10 Vendor Detections
Hybrid-Analysis: 100/100 Malicious

Behavior Highlights

Blocklisted process makes network requests.
Contacts 194.213.18.89.
Loads dropped DLL.
Scheduled Task/Job
Suspicious behavior: EnumeratesProcesses.
Suspicious use of WriteProcessMemory.
User Task Scheduler COM API.

512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6 | *Triage*. (n.d.). https://tria.ge/250812-d6zftsdn31/behavioral1

Evidence

See OSINT Investigation Appendix 2, Figures 1-6.

Confirmed Malicious Domain #2

Basic Information

Domain: winscp.download
URL: https://winscp.download/WinSCP-6.5.1.exe
Status: Confirmed Malicious
Source: https://urlscan.io/result/01983f91-91b4-744c-a361-95227e7b0683/
Date First Seen: 2025-07-25
Date Last Seen:
IP Address: 188.114.97.3

Malicious Activity

Downloads: WinSCP-6.5.1.exe
File Hash: a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab

Additional Reports

https://tria.ge/250711-lyd4xstvfx
https://urlhaus.abuse.ch/url/3612733/
https://hybrid-analysis.com/sample/a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab

Verdicts

Triage: 7/10
Hybrid-Analysis: Suspicious

Behavior Highlights

Reads WinSCP keys stored on the system
Checks computer location settings.
Component object model hijacking.

Checks installed software on the system.
Drops file in the Program Files directory.
Executes dropped DLL.
Enumerates physical storage devices.
System Language Discovery.
Modifies registry class.
Script User-Agent.
Suspicious behavior: EnumertesProcesses.
Suspicious behavior: FindShellTrayWindow.
Suspicious behavior: WriteProcessMemory.
a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab | *Triage*. (n.d.).
https://tria.ge/250711-lyd4xstvfx/behavioral1

Evidence

See OSINT Investigation Appendix 2, Figures 7-10.

Confirmed Malicious Domain #3

Basic Information

Domain: anydesk.com
URL: https://anydesk.com/en/downloads/thank-you?dv=win_exe
Status: Confirmed Malicious
Source: https://urlscan.io/result/019a30fb-b864-757a-9433-ac0e9b157179/
Date First Seen: 2025-10-29
Date Last Seen:
IP Address: 18.245.60.125

Malicious Activity

Downloads: Anydesk.exe
File Hash: c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6

Additional Reports

https://hybrid-analysis.com/sample/c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6
https://tria.ge/251028-egk3kstrfz

Verdicts

Triage: 8/10
Hybrid-Analysis: Malicious 100/100

Behavior Highlights

Reads terminal service-related keys.
Found a string that may be used as part of an injection method.
Writes data to a remote process.
Found a reference to a WMI query string known to be used for VM detection.

Marks file for deletion.
May check for the presence of a forensics or monitoring tool.
Possibly tries to evade analysis by sleeping many times.
Possibly tries to implement anti-virtualization techniques using MAX address detection.
Tries to hide tracks of having downloaded a file from the internet.
Tries to sleep for a long time, more than two minutes.
Queries kernel debugger information
Contacts 2 domains and 5 hosts.
Free Automated Malware Analysis Service - powered by Falcon Sandbox. (n.d.). https://hybrid-analysis.com/sample/c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6

Evidence

See OSINT Investigation Appendix 2, Figures 11-13.