OSINT Investigation Log

CMIT-450-81: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

10.8.2025

Contents

Research Question

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

Confirmed Malicious Domain #1

Basic Information

Domain: winscp.download
URL: https://winscp.download/WinSCP-6.5.1.exe
Status: Confirmed Malicious
Source: URLhaus
VirusITotal Detections: 5/97 vendors
Date First Seen: 2025-08-2718:02:10 UTC
Date Last Seen: 2025-08-27 20:XX:XX UTC
IP Address: 188.114.96.3

Malicious Activity

Downloads: WinSCP-6.5.1.exe

File Hash: a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab
Delivery Method: Fake Software Download

Evidence

See Figures 1 and 2 in Appendix 1.

Confirmed Malicious Domain # 2

Domain: 194.62.248.87
URL: http://194.62.248.87/hostfiles/putty.exe
Status: Confirmed Malicious
Source: URLhaus
VirusTotal Detections: 14/98 vendors
Date First Seen: 2025-08-14 12:44:07 UTC
Date Last Seen: 2025-08-14 16:XX:XX UTC
IP Address: 194.62.248.87

Malicious Activity

Downloads: putty.exe
File Hash: 16cbe40fb24ce2d422afddb5a90a5801ced32ef52c22c2fc77b25a90837f28ad
Delivery Method: Fake Software Download

Evidence

See figures 3 and 4 in Appendix 1.

Confirmed Malicious Domain # 3

Domain: book.rollingvideogames
URL: http://book.rollingvideogames.com/temp/putty.exe
Status: Confirmed Malicious
Source: URLhaus
VirusTotal Detections: 11/98 vendors
Date First Seen: 2025-02-23 19:16:06 UTC
Date Last Seen: Still Online
IP Address: 23.235.202.121

Malicious Activity

Downloads: None Listed
File Hash: aa8f8a3e268493157e62d93ab9cafb94573606fe43a80e63e3e4f2e5c9b22a5b
Delivery Method: Fake Software Download

Evidence

See figures 5 and 6 in Appendix 1.

Confirmed Malicious Domain # 4

Domain: anydesk.com.in
URL: https://anydesk.com.in/wp-content/uploads/2024/10/AnyDesk.zip
Status: Confirmed Malicious
Source: URLhaus
VirusTotal Detections: 14/98 vendors
Date First Seen: 2025-04-01 05:29:13 UTC
Date Last Seen: 2025-04-01 06:XX:XX UTC
IP Address: 104.21.22.96

Malicious Activity

Downloads: None Listed
File Hash: 3bdbec3db5c2fda93cfb959e7f7ca503b0a4a5ec285b38e4d59495fe19829682
Delivery Method: Fake Software Download

Evidence

See figures 7 and 8 in Appendix 1.

Confirmed Malicious Domain # 5

Domain: anydesk.com.in
URL: http://avastcxt.com/anydesk.apk
Status: Confirmed Malicious
Source: URLhaus
VirusTotal Detections: 17/98 vendors
Date First Seen: 2024-12-30 10:44:23 UTC
Date Last Seen: 2025-03-10 12:XX:XX UTC
IP Address: 193.143.1.14

Malicious Activity

Downloads: None Listed
File Hash:
d6b3a57d6b88baf2262a224c3e6c1bc657cf3e29914d1a3d9a7f7d2e8d5bb9be
0a303433f75972d397da7c60497ae3546415fe98cd958e7cab6e78364150361e
949b957859ea15fb822076da30ba3408e371d66e152526ca021c116f65dcdd0f
2f023dc2c1833d5846b34aea5315ab5b36e634e4371f4964f2b59dfa71522110
b0112b29b8400a70a56e53072f71c17b3b5d91ed7ff4e2d3073794bcaec0c16c
Delivery Method: Fake Software Download

Evidence

See figures 9 and 10 in Appendix 1.

Confirmed Malicious Domain # 6

Domain: ecoproducts.com.my
URL: https://ecoproducts.com.my/system/library/teamviewer.exe
Status: Confirmed Malicious
Source: URLhaus
VirusTotal Detections: 20/98 vendors
Date First Seen: 2024-01-12 09:40:10 UTC
Date Last Seen: 2024-01-12 09:40:10 UTC
IP Address: 172.67.139.199

Malicious Activity

Downloads: None Listed
File Hash: e47d112f2d69f2f2d49a34a4857604e11bb89ba9c8f24f46fe6ae8bbe9c31b83
Delivery Method: Fake Software Download

Evidence

See figures 11 and 12 in Appendix 1.

Sources

VirusTotal - Home. (n.d.). VirusTotal. https://www.virustotal.com/gui/home/upload

URLhaus - Malware URL exchange. (n.d.). https://urlhaus.abuse.ch/