Appendix 2

OSINT Investigation Appendix 2

CMIT-450-81: Senior Seminar Project

Instructor Michael Atwood

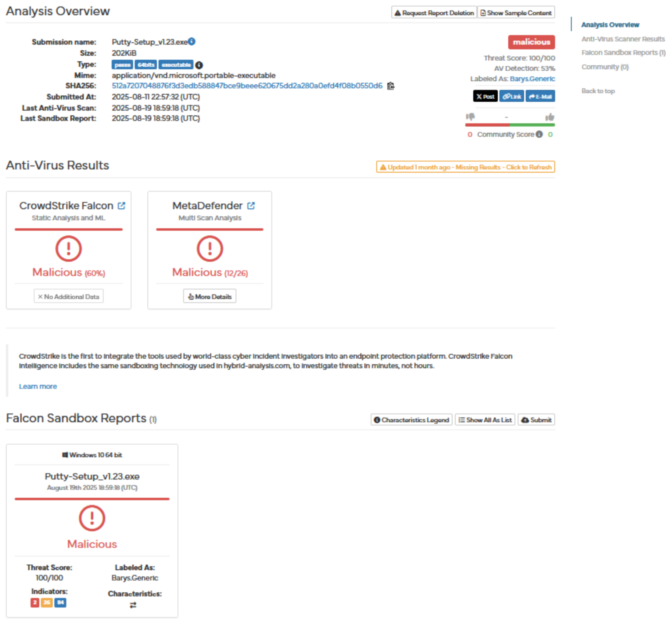
Kyle Hathaway

11.2.2025

Contents

Appendix 2

Confirmed Malicious Domain #1 Evidence



Analysis Overview

Submission name: Putty-Setup_v1.23.exe
Size: 202KiB
Type: peexe 64bits executable
Mime: application/vnd.microsoft.portable-executable
SHA256: 512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6
Submitted At: 2025-08-11 22:57:32 (UTC)
Last Anti-Virus Scan: 2025-08-19 18:59:18 (UTC)
Last Sandbox Report: 2025-08-19 18:59:18 (UTC)

malicious
Threat Score: 100/100
AV Detection: 53%
Labeled As: Barys.Generic

0 Community Score 0

Anti-Virus Results

Updated 1 month ago - Missing Results - Click to Refresh

CrowdStrike Falcon
Static Analysis and ML
Malicious (60%)
× No Additional Data

MetaDefender
Multi Scan Analysis
Malicious (12/26)
More Details

CrowdStrike is the first to integrate the tools used by world-class cyber incident investigators into an endpoint protection platform. CrowdStrike Falcon intelligence includes the same sandboxing technology used in hybrid-analysis.com, to investigate threats in minutes, not hours.

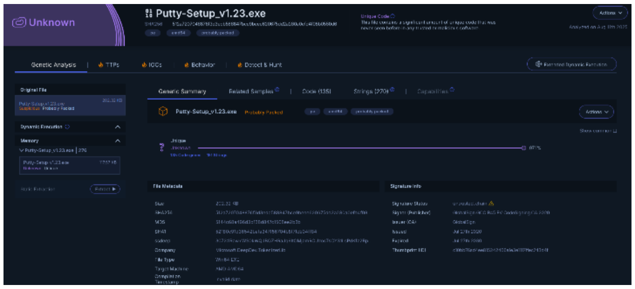
Learn more

Falcon Sandbox Reports (1)

Windows 10 64 bit
Putty-Setup_v1.23.exe
August 19th 2025 18:59:18 (UTC)
Malicious
Threat Score: 100/100
Labeled As: Barys.Generic
Indicators: 2 26 84
Characteristics: ⇄

Figure 1: Hybrid-analysis report on domain #1.

(Free Automated Malware Analysis Service - Powered by Falcon Sandbox, n.d.)



Unknown
Putty-Setup_v1.23.exe
Unique Code

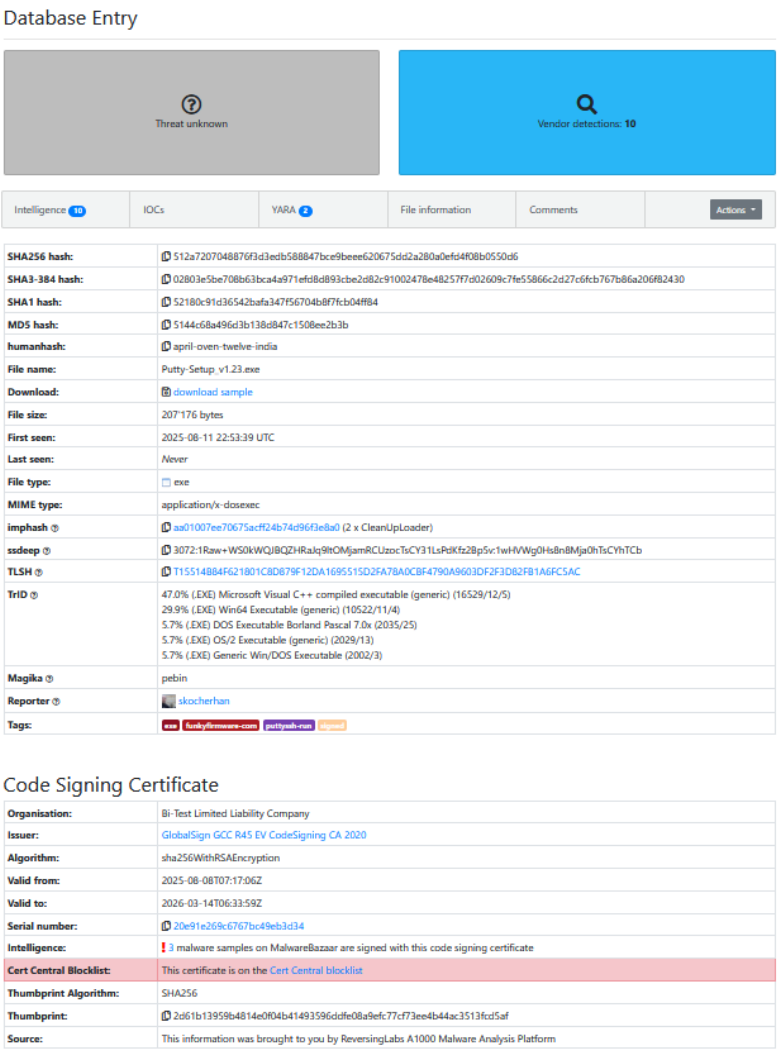
File Metadata
Size
SHA256
MD5
SHA1
ssdeep
Company
File Type
Target Machine
Compilation Timestamp

Signature Info
Signature Status
Signer (Publisher)
Issuer (CA) GlobalSign
Issued
Expired
Thumbprint (ID)

Figure 2: Intezer report on domain # 1.

(Malicious File 5144c68a496d3b138d847c1508ee2b3b - Intezer, n.d.)

Appendix 2



Database Entry

SHA256 hash:	512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6
SHA3-384 hash:	02803e5be708b63bca4a971efd8d893cbe2d82c91002478e48257f7d02609c7fe55866c2d27c6fcb767b86a206f82430
SHA1 hash:	52180c91d36542bafa347f56704b8f7fcb04ff84
MD5 hash:	5144c68a496d3b138d847c1508ee2b3b
humanhash:	april-oven-twelve-india
File name:	Putty-Setup_v1.23.exe
Download:	download sample
File size:	207'176 bytes
First seen:	2025-08-11 22:53:39 UTC
Last seen:	*Never*
File type:	exe
MIME type:	application/x-dosexec
imphash	aa01007ee70675acff24b74d96f3e8a0 (2 x CleanUpLoader)
ssdeep	3072:1Raw+WS0kWQJBQZHRaJq9ltOMjamRCUzocTsCY31LsPdKfz2Bp5v:1wHVWg0Hs8n8Mja0hTsCYhTCb
TLSH	T15514B84F621801C8D879F12DA169551SD2FA78A0CBF4790A9603DF2F3D82FB1A6FC5AC
TrID	47.0% (.EXE) Microsoft Visual C++ compiled executable (generic) (16529/12/5) 29.9% (.EXE) Win64 Executable (generic) (10522/11/4) 5.7% (.EXE) DOS Executable Borland Pascal 7.0x (2035/25) 5.7% (.EXE) OS/2 Executable (generic) (2029/13) 5.7% (.EXE) Generic Win/DOS Executable (2002/3)
Magika	pebin
Reporter	skocherhan
Tags:	exe funkyfirmware-com puttyssh-run signed

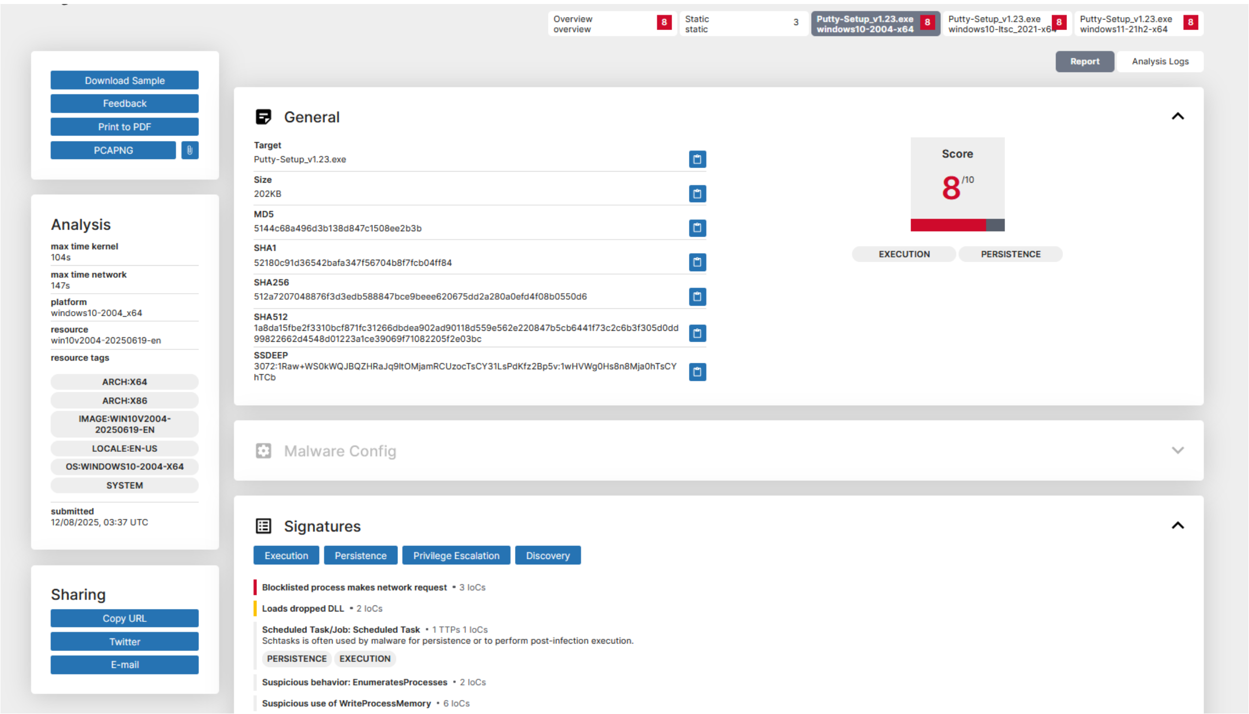
Code Signing Certificate

Organisation:	Bi-Test Limited Liability Company
Issuer:	GlobalSign GCC R45 EV CodeSigning CA 2020
Algorithm:	sha256WithRSAEncryption
Valid from:	2025-08-08T07:17:06Z
Valid to:	2026-03-14T06:33:59Z
Serial number:	20e91e269c6767bc49eb3d34
Intelligence:	! 3 malware samples on MalwareBazaar are signed with this code signing certificate
Cert Central Blocklist:	This certificate is on the Cert Central blocklist
Thumbprint Algorithm:	SHA256
Thumbprint:	2d61b13959b4814e0f04b41493596ddfe08a9efc77cf73ee4b44ac3513fcd5af
Source:	This information was brought to you by ReversingLabs A1000 Malware Analysis Platform

Figure 3: Malwarebazaar report on domain #1.

(MalwareBazaar - Putty-Setup_v1.23.exe, n.d.)

Appendix 2



General

Target
Putty-Setup_v1.23.exe

Size
202KB

MD5
5144c68a496d3b138d847c1508ee2b3b

SHA1
52180c91d36542bafa347f56704b8f7fcb04ff84

SHA256
512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6

SHA512
1a8da15fbe2f3310bcf871fc31266dbdea902ad90118d559e562e220847b5cb6441f73c2c6b3f305d0dd99822662d4548d01223a1ce39069f71082205f2e03bc

SSDEEP
3072:1Raw+WS0kWQJBQZHRaJq9ltOMjamRCUzocTsCY31LsPdKfz2Bp5v:1wHVWg0Hs8n8Mja0hTsCYhTCb

Score
8/10

EXECUTION PERSISTENCE

Analysis

max time kernel
104s

max time network
147s

platform
windows10-2004_x64

resource
win10v2004-20250619-en

resource tags
ARCH:X64
ARCH:X86
IMAGE:WIN10V2004-20250619-EN
LOCALE:EN-US
OS:WINDOWS10-2004-X64
SYSTEM

submitted
12/08/2025, 03:37 UTC

Sharing

Malware Config

Signatures

Blocklisted process makes network request • 3 IoCs

Loads dropped DLL • 2 IoCs

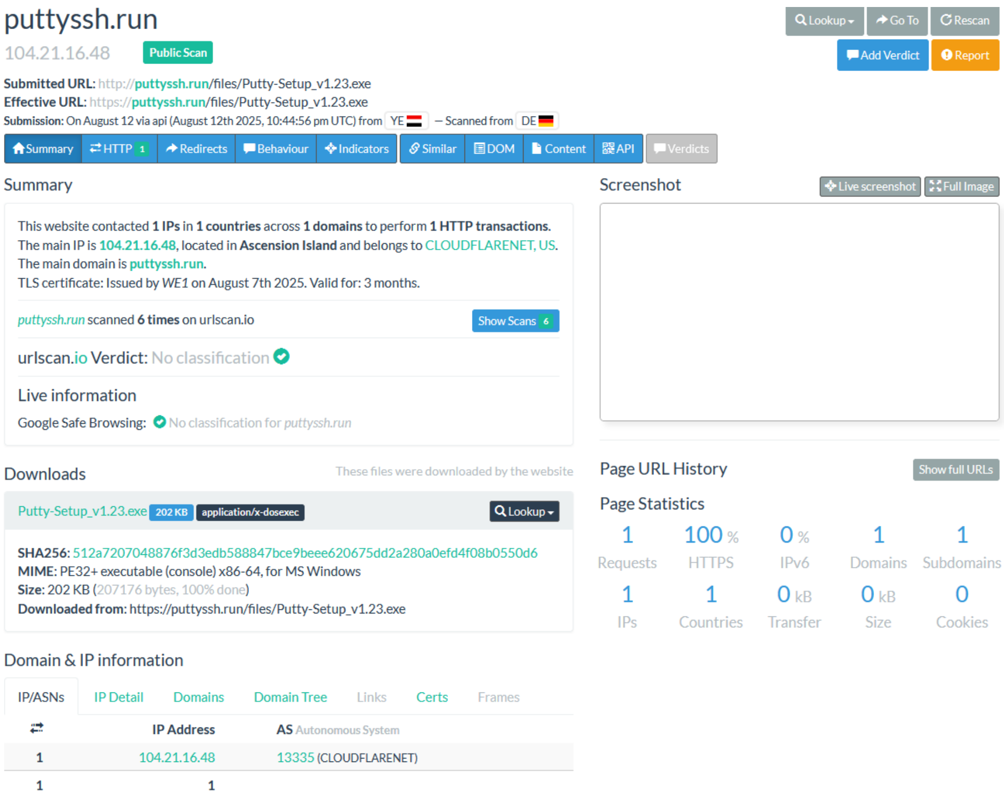
Scheduled Task/Job: Scheduled Task • 1 TTPs 1 IoCs
Schtasks is often used by malware for persistence or to perform post-infection execution.
PERSISTENCE EXECUTION

Suspicious behavior: EnumeratesProcesses • 2 IoCs

Suspicious use of WriteProcessMemory • 6 IoCs

Figure 4: Triage report on domain #1.

(512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6 | Triage, n.d.)



puttyssh.run
104.21.16.48

Submitted URL: http://puttyssh.run/files/Putty-Setup_v1.23.exe
Effective URL: https://puttyssh.run/files/Putty-Setup_v1.23.exe
Submission: On August 12 via api (August 12th 2025, 10:44:56 pm UTC) from YE — Scanned from DE

Summary

This website contacted **1 IPs** in **1 countries** across **1 domains** to perform **1 HTTP transactions.**
The main IP is **104.21.16.48**, located in **Ascension Island** and belongs to CLOUDFLARENET, US.
The main domain is **puttyssh.run**.
TLS certificate: Issued by *WE1* on August 7th 2025. Valid for: 3 months.

puttyssh.run scanned **6 times** on urlscan.io

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *puttyssh.run*

Screenshot

Page URL History

Page Statistics

1	100 %	0 %	1	1
Requests	HTTPS	IPv6	Domains	Subdomains
1	1	0 kB	0 kB	0
IPs	Countries	Transfer	Size	Cookies

Downloads

These files were downloaded by the website

Putty-Setup_v1.23.exe 202 KB application/x-dosexec

SHA256: 512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6
MIME: PE32+ executable (console) x86-64, for MS Windows
Size: 202 KB (207176 bytes, 100% done)
Downloaded from: https://puttyssh.run/files/Putty-Setup_v1.23.exe

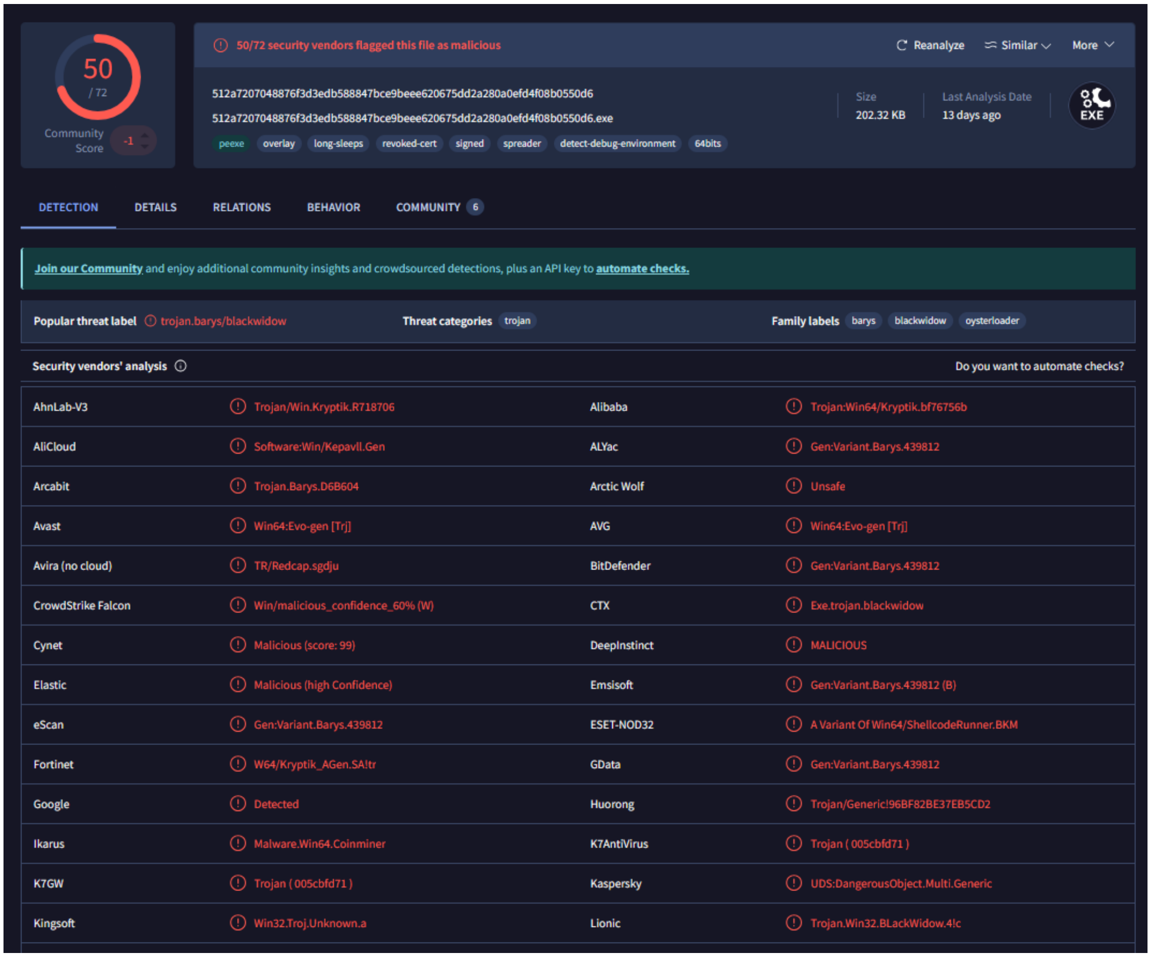
Domain & IP information

⇄	IP Address	AS Autonomous System
1	104.21.16.48	13335 (CLOUDFLARENET)
1	1	

Figure 5: URLscan report on domain #1.

Appendix 2

(Urlscan.Io, n.d.)



50/72 security vendors flagged this file as malicious

512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6

512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6.exe

peexe overlay long-sleeps revoked-cert signed spreader detect-debug-environment 64bits

Size 202.32 KB

Last Analysis Date 13 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.barys/blackwidow

Threat categories trojan

Family labels barys blackwidow oysterloader

Security vendors' analysis

Do you want to automate checks?

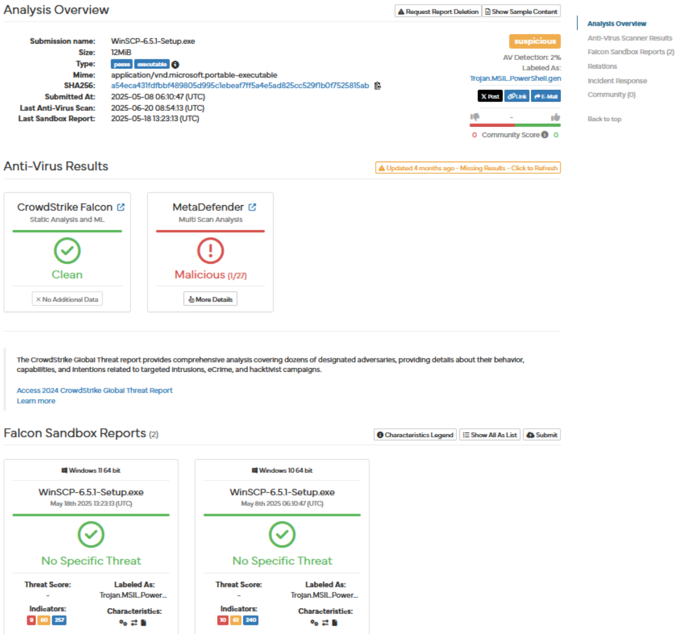
AhnLab-V3	Trojan/Win.Kryptik.R718706	Alibaba	Trojan:Win64/Kryptik.bf76756b
AliCloud	Software:Win/Kepavll.Gen	ALYac	Gen:Variant.Barys.439812
Arcabit	Trojan.Barys.D6B604	Arctic Wolf	Unsafe
Avast	Win64:Evo-gen [Trj]	AVG	Win64:Evo-gen [Trj]
Avira (no cloud)	TR/Redcap.sgdju	BitDefender	Gen:Variant.Barys.439812
CrowdStrike Falcon	Win/malicious_confidence_60% (W)	CTX	Exe.trojan.blackwidow
Cynet	Malicious (score: 99)	DeepInstinct	MALICIOUS
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Barys.439812 (B)
eScan	Gen:Variant.Barys.439812	ESET-NOD32	A Variant Of Win64/ShellcodeRunner.BKM
Fortinet	W64/Kryptik_AGen.SA!tr	GData	Gen:Variant.Barys.439812
Google	Detected	Huorong	Trojan/Generic!96BF82BE37EB5CD2
Ikarus	Malware.Win64.Coinminer	K7AntiVirus	Trojan (005cbfd71)
K7GW	Trojan (005cbfd71)	Kaspersky	UDS:DangerousObject.Multi.Generic
Kingsoft	Win32.Troj.Unknown.a	Lionic	Trojan.Win32.BLackWidow.4!c

Figure 6: Virustotal scan on domain #1.

(VirusTotal - File - 512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6, n.d.)

Appendix 2

Confirmed Malicious Domain #2 Evidence



Analysis Overview

Submission name: WinSCP-6.5.1-Setup.exe
Size: 12MiB
Type: peexe executable
Mime: application/vnd.microsoft.portable-executable
SHA256: a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab
Submitted At: 2025-05-08 06:10:47 (UTC)
Last Anti-Virus Scan: 2025-06-20 08:54:13 (UTC)
Last Sandbox Report: 2025-05-18 13:23:13 (UTC)

suspicious
AV Detection: 2%
Labeled As:
Trojan.MSIL.PowerShell.gen

0 Community Score 0

Anti-Virus Results

Updated 4 months ago - Missing Results - Click to Refresh

CrowdStrike Falcon
Static Analysis and ML
Clean

MetaDefender
Multi Scan Analysis
Malicious (1/27)

The CrowdStrike Global Threat report provides comprehensive analysis covering dozens of designated adversaries, providing details about their behavior, capabilities, and intentions related to targeted intrusions, eCrime, and hacktivist campaigns.

Access 2024 CrowdStrike Global Threat Report
Learn more

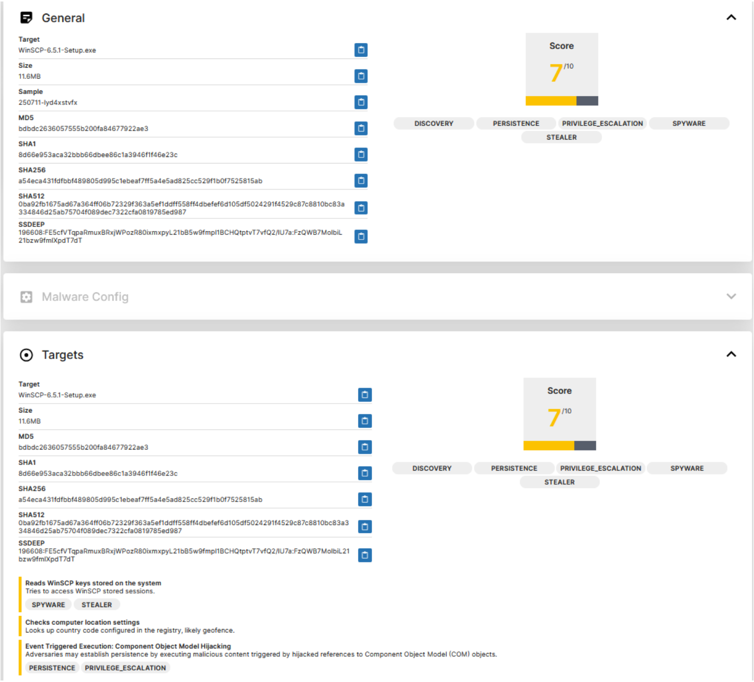
Falcon Sandbox Reports (2)

Windows 11 64 bit
WinSCP-6.5.1-Setup.exe
May 18th 2025 13:23:13 (UTC)
No Specific Threat
Threat Score: -
Labeled As: Trojan.MSIL.Power...
Indicators: 9 60 257
Characteristics:

Windows 10 64 bit
WinSCP-6.5.1-Setup.exe
May 8th 2025 06:10:47 (UTC)
No Specific Threat
Threat Score: -
Labeled As: Trojan.MSIL.Power...
Indicators: 10 61 240
Characteristics:

Figure 7: Hybrid-analysis report on Domain #2.

(Free Automated Malware Analysis Service - Powered by Falcon Sandbox, n.d.)



General

Target
WinSCP-6.5.1-Setup.exe
Size
11.6MB
Sample
250711-lyd4xstvfx
MD5
bdbdc2636057555b200fa84677922ae3
SHA1
8d66e953aca32bbb66dbee86c1a3946f1f46e23c
SHA256
a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab
SHA512
0ba92fb1675ad67a364ff06b72329f363a5ef1ddff558ff4dbefef6d105df5024291f4529c87c8810bc83a334846d25ab75704f089dec7322cfa0819785ed987
SSDEEP
196608:FE5cfVTqpaRmuxBRxjWPozR80ixmxpyL21bB5w9fmpl1BCHQtptvT7vfQ2/lU7a:FzQWB7MolbiL21bzw9fmlXpdT7dT

Score
7/10

DISCOVERY PERSISTENCE PRIVILEGE_ESCALATION SPYWARE STEALER

Malware Config

Targets

Target
WinSCP-6.5.1-Setup.exe
Size
11.6MB
MD5
bdbdc2636057555b200fa84677922ae3
SHA1
8d66e953aca32bbb66dbee86c1a3946f1f46e23c
SHA256
a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab
SHA512
0ba92fb1675ad67a364ff06b72329f363a5ef1ddff558ff4dbefef6d105df5024291f4529c87c8810bc83a334846d25ab75704f089dec7322cfa0819785ed987
SSDEEP
196608:FE5cfVTqpaRmuxBRxjWPozR80ixmxpyL21bB5w9fmpl1BCHQtptvT7vfQ2/lU7a:FzQWB7MolbiL21bzw9fmlXpdT7dT

Score
7/10

DISCOVERY PERSISTENCE PRIVILEGE_ESCALATION SPYWARE STEALER

Reads WinSCP keys stored on the system
Tries to access WinSCP stored sessions.
SPYWARE STEALER

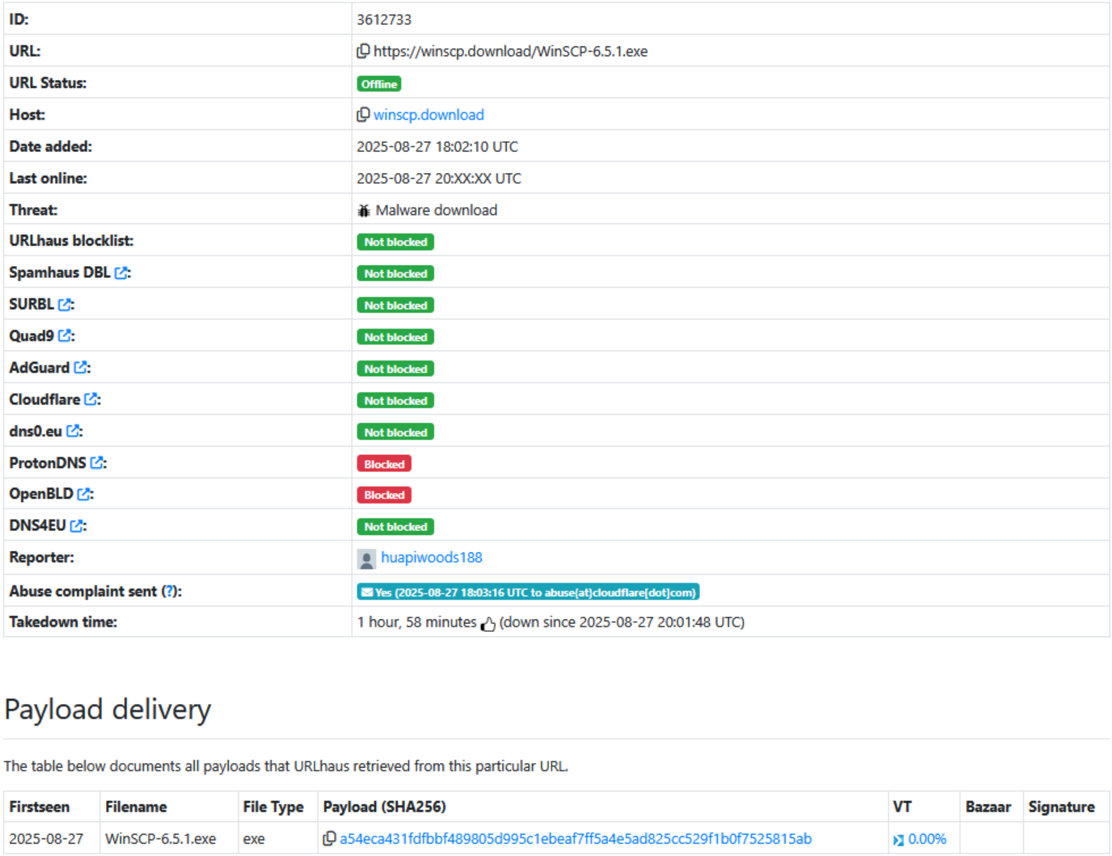
Checks computer location settings
Looks up country code configured in the registry, likely geofence.

Event Triggered Execution: Component Object Model Hijacking
Adversaries may establish persistence by executing malicious content triggered by hijacked references to Component Object Model (COM) objects.
PERSISTENCE PRIVILEGE_ESCALATION

Figure 8: Triage report on domain #2.

(A54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab | Triage, n.d.)

Appendix 2



ID:	3612733
URL:	https://winscp.download/WinSCP-6.5.1.exe
URL Status:	Offline
Host:	winscp.download
Date added:	2025-08-27 18:02:10 UTC
Last online:	2025-08-27 20:XX:XX UTC
Threat:	Malware download
URLhaus blocklist:	Not blocked
Spamhaus DBL:	Not blocked
SURBL:	Not blocked
Quad9:	Not blocked
AdGuard:	Not blocked
Cloudflare:	Not blocked
dns0.eu:	Not blocked
ProtonDNS:	Blocked
OpenBLD:	Blocked
DNS4EU:	Not blocked
Reporter:	huapiwoods188
Abuse complaint sent (?):	Yes (2025-08-27 18:03:16 UTC to abuse{at}cloudflare[dot]com)
Takedown time:	1 hour, 58 minutes (down since 2025-08-27 20:01:48 UTC)

Payload delivery

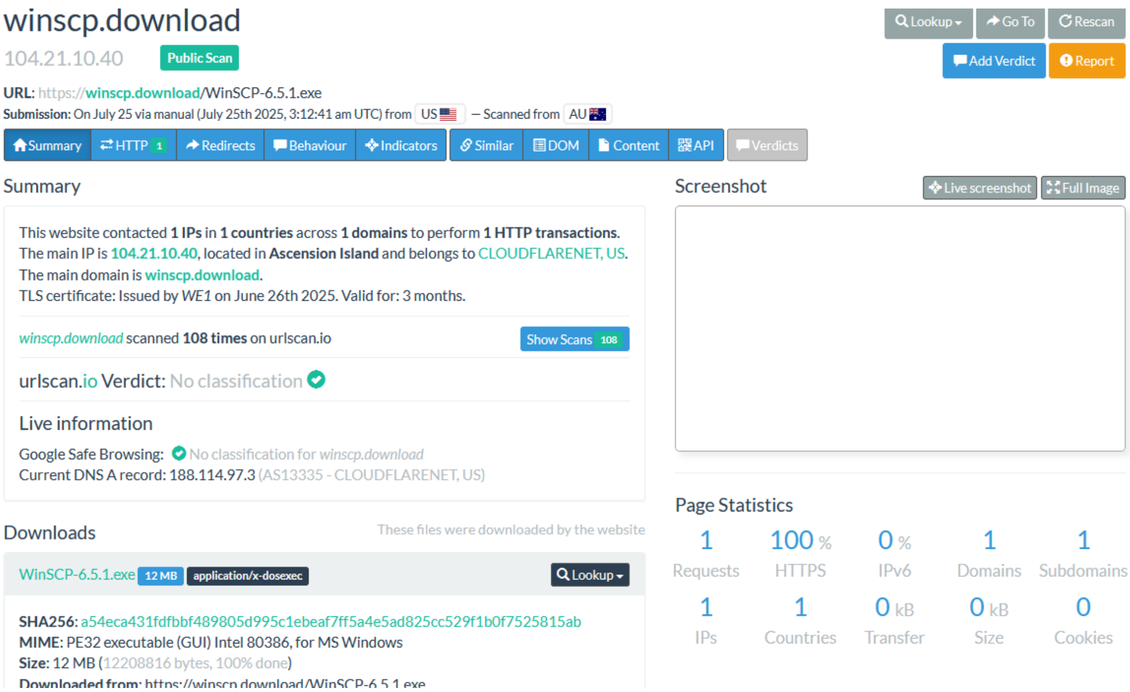
The table below documents all payloads that URLhaus retrieved from this particular URL.

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2025-08-27	WinSCP-6.5.1.exe	exe	a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab	0.00%		

Figure 9: URLhaus report on domain #2.

(URLhaus - Https://Winscp.Download/WinSCP-6.5.1.exe, n.d.)

Appendix 2



winscp.download

104.21.10.40 Public Scan

URL: https://winscp.download/WinSCP-6.5.1.exe
Submission: On July 25 via manual (July 25th 2025, 3:12:41 am UTC) from US — Scanned from AU

Summary

This website contacted **1 IPs** in **1 countries** across **1 domains** to perform **1 HTTP transactions.** The main IP is 104.21.10.40, located in **Ascension Island** and belongs to CLOUDFLARENET, US. The main domain is winscp.download.
TLS certificate: Issued by *WE1* on June 26th 2025. Valid for: 3 months.

winscp.download scanned **108 times** on urlscan.io

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ *No classification for winscp.download*
Current DNS A record: 188.114.97.3 (AS13335 - CLOUDFLARENET, US)

Screenshot

Page Statistics

1	100 %	0 %	1	1
Requests	HTTPS	IPv6	Domains	Subdomains
1	1	0 kB	0 kB	0
IPs	Countries	Transfer	Size	Cookies

Downloads

These files were downloaded by the website

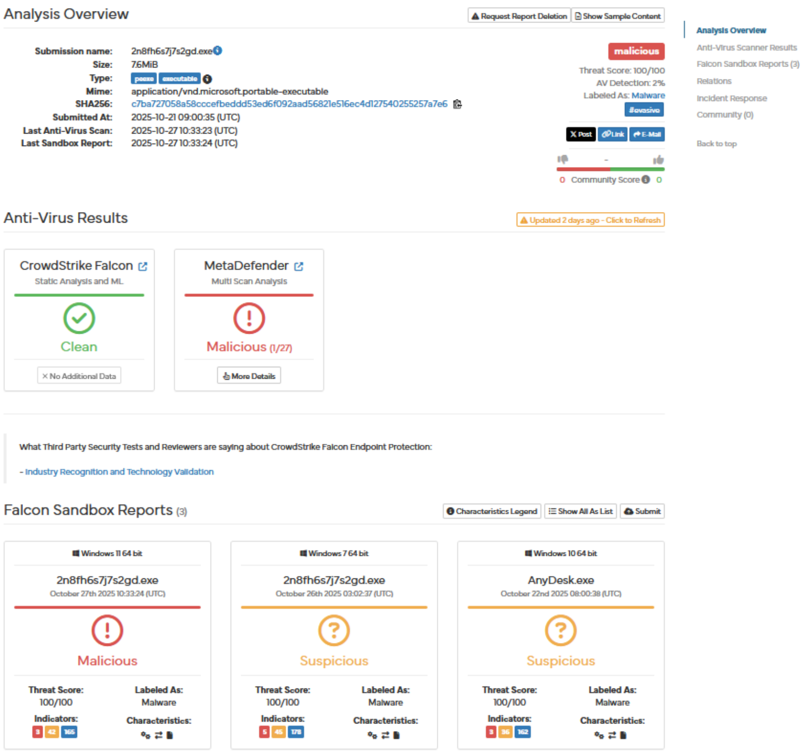
WinSCP-6.5.1.exe 12 MB application/x-dosexec

SHA256: a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab
MIME: PE32 executable (GUI) Intel 80386, for MS Windows
Size: 12 MB (12208816 bytes, 100% done)
Downloaded from: https://winscp.download/WinSCP-6.5.1.exe

Figure 10: URLscan report on domain #2.

(Urlscan.Io, n.d.)

Confirmed Malicious Domain #3 Evidence



Analysis Overview

Submission name: 2n8fh6s7j7s2gd.exe
Size: 7.6MiB
Type: peexe executable
Mime: application/vnd.microsoft.portable-executable
SHA256: c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6
Submitted At: 2025-10-21 09:00:35 (UTC)
Last Anti-Virus Scan: 2025-10-27 10:33:23 (UTC)
Last Sandbox Report: 2025-10-27 10:33:24 (UTC)

malicious
Threat Score: 100/100
AV Detection: 2%
Labeled As: Malware
#evasive

0 Community Score 0

Anti-Virus Results

CrowdStrike Falcon Static Analysis and ML	MetaDefender Multi Scan Analysis
Clean	Malicious (1/27)

What Third Party Security Tests and Reviewers are saying about CrowdStrike Falcon Endpoint Protection:

- Industry Recognition and Technology Validation

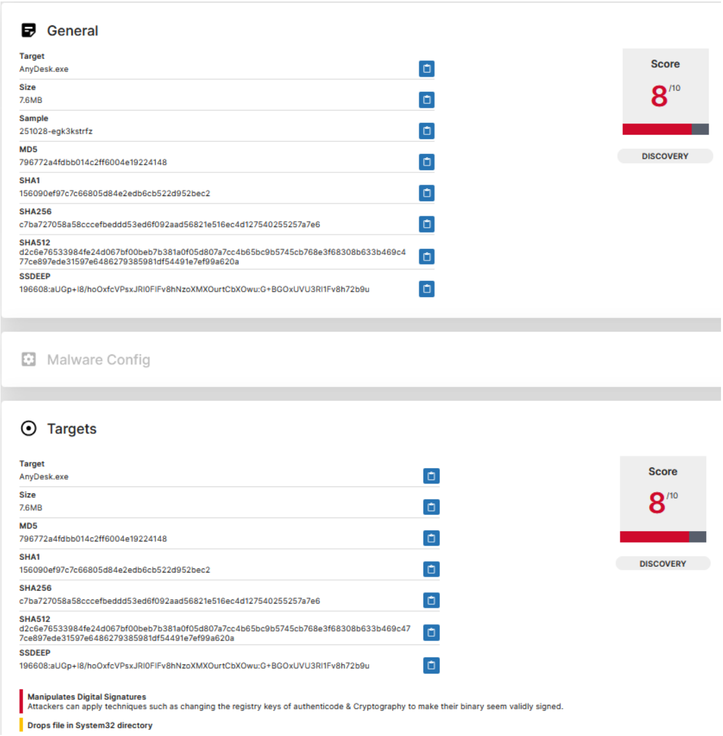
Falcon Sandbox Reports (3)

Windows 11 64 bit	Windows 7 64 bit	Windows 10 64 bit
2n8fh6s7j7s2gd.exe October 27th 2025 10:33:24 (UTC)	2n8fh6s7j7s2gd.exe October 26th 2025 03:02:37 (UTC)	AnyDesk.exe October 22nd 2025 08:00:38 (UTC)
Malicious	Suspicious	Suspicious
Threat Score: 100/100	Threat Score: 100/100	Threat Score: 100/100
Labeled As: Malware	Labeled As: Malware	Labeled As: Malware
Indicators: 3 42 165	Indicators: 5 45 178	Indicators: 3 36 162
Characteristics:	Characteristics:	Characteristics:

Figure 11: Hybrid-analysis report on domain #3.

Appendix 2

(Free Automated Malware Analysis Service - Powered by Falcon Sandbox, n.d.)



General

Target
AnyDesk.exe

Size
7.6MB

Sample
251028-egk3kstrfz

MD5
796772a4fdbb014c2ff6004e19224148

SHA1
156090ef97c7c66805d84e2edb6cb522d952bec2

SHA256
c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6

SHA512
d2c6e76533984fe24d067bf00beb7b381a0f05d807a7cc4b65bc9b5745cb768e3f68308b633b469c4
77ce897ede31597e6486279385981df54491e7ef99a620a

SSDEEP
196608:aUGp+I8/hoOxfcVPsxJRI0FIFv8hNzoXMXOurtCbXOwu:G+BGOxUVU3RI1Fv8h72b9u

Score
8 /10

DISCOVERY

Malware Config

Targets

Target
AnyDesk.exe

Size
7.6MB

MD5
796772a4fdbb014c2ff6004e19224148

SHA1
156090ef97c7c66805d84e2edb6cb522d952bec2

SHA256
c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6

SHA512
d2c6e76533984fe24d067bf00beb7b381a0f05d807a7cc4b65bc9b5745cb768e3f68308b633b469c47
7ce897ede31597e6486279385981df54491e7ef99a620a

SSDEEP
196608:aUGp+I8/hoOxfcVPsxJRI0FIFv8hNzoXMXOurtCbXOwu:G+BGOxUVU3RI1Fv8h72b9u

Score
8 /10

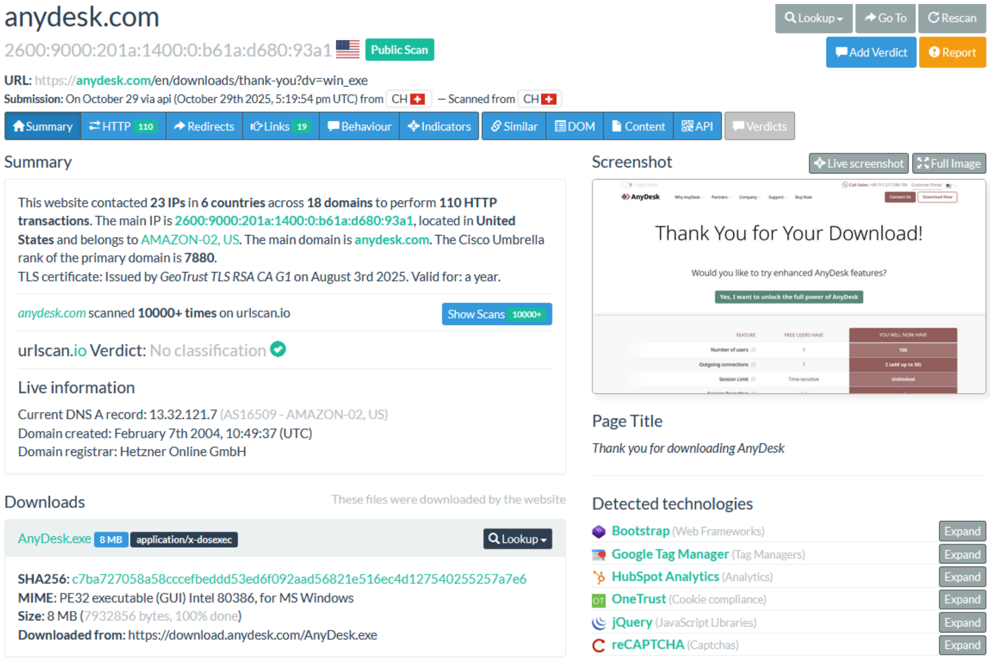
DISCOVERY

Manipulates Digital Signatures
Attackers can apply techniques such as changing the registry keys of authenticode & Cryptography to make their binary seem validly signed.

Drops file in System32 directory

Figure 12: Triage report on domain #3.

(C7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6 | Triage, n.d.)



anydesk.com

2600:9000:201a:1400:0:b61a:d680:93a1 Public Scan

URL: https://anydesk.com/en/downloads/thank-you?dv=win_exe
Submission: On October 29 via api (October 29th 2025, 5:19:54 pm UTC) from CH — Scanned from CH

Summary

This website contacted **23 IPs** in **6 countries** across **18 domains** to perform **110 HTTP transactions**. The main IP is **2600:9000:201a:1400:0:b61a:d680:93a1**, located in **United States** and belongs to AMAZON-02, US. The main domain is **anydesk.com**. The Cisco Umbrella rank of the primary domain is **7880**.
TLS certificate: Issued by *GeoTrust TLS RSA CA G1* on August 3rd 2025. Valid for: a year.

anydesk.com scanned **10000+ times** on urlscan.io

urlscan.io Verdict: No classification

Live information

Current DNS A record: 13.32.121.7 (AS16509 - AMAZON-02, US)
Domain created: February 7th 2004, 10:49:37 (UTC)
Domain registrar: Hetzner Online GmbH

Screenshot

Live screenshot
Full Image
AnyDesk
Thank You for Your Download!
Would you like to try enhanced AnyDesk features?
Yes, I want to unlock the full power of AnyDesk

Page Title

Thank you for downloading AnyDesk

Downloads

These files were downloaded by the website

AnyDesk.exe 8 MB application/x-dosexec

SHA256: c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6
MIME: PE32 executable (GUI) Intel 80386, for MS Windows
Size: 8 MB (7932856 bytes, 100% done)
Downloaded from: https://download.anydesk.com/AnyDesk.exe

Detected technologies

Bootstrap (Web Frameworks)	Expand
Google Tag Manager (Tag Managers)	Expand
HubSpot Analytics (Analytics)	Expand
OneTrust (Cookie compliance)	Expand
jQuery (JavaScript Libraries)	Expand
reCAPTCHA (Captchas)	Expand

Figure 13: URLscan report on domain #3.

(Urlscan.Io, n.d.)

Appendix 2

Sources

Urlscan.Io. (n.d.). *Puttyssh.run - urlscan.io*. https://urlscan.io/result/0198a075-44f2-70bc-95c1-e0b3346508ff/

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

Malicious file 5144c68a496d3b138d847c1508ee2b3b - Intezer. (n.d.). https://analyze.intezer.com/files/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6/genetic-analysis

MalwareBazaar - Putty-Setup_v1.23.exe. (n.d.). https://bazaar.abuse.ch/sample/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6

VirusTotal - File - 512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6. (n.d.). VirusTotal. https://www.virustotal.com/gui/file/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6/detection

Free Automated Malware Analysis Service - powered by Falcon Sandbox. (n.d.). https://hybrid-analysis.com/sample/512a7207048876f3d3edb588847bce9beee620675dd2a280a0efd4f08b0550d6

Urlscan.Io. (n.d.). *winscp.download - urlscan.io*. https://urlscan.io/result/01983f91-91b4-744c-a361-95227e7b0683/

a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab | Triage. (n.d.). https://tria.ge/250711-lyd4xstvfx

URLhaus - https://winscp.download/WinSCP-6.5.1.exe. (n.d.). https://urlhaus.abuse.ch/url/3612733/

Free Automated Malware Analysis Service - powered by Falcon Sandbox. (n.d.). https://hybrid-analysis.com/sample/a54eca431fdfbbf489805d995c1ebeaf7ff5a4e5ad825cc529f1b0f7525815ab

Appendix 2

Urlscan.Io. (n.d.). *Anydesk.com - urlscan.io*. https://urlscan.io/result/019a30fb-b864-757a-9433-ac0e9b157179/

Free Automated Malware Analysis Service - powered by Falcon Sandbox. (n.d.). https://hybrid-analysis.com/sample/c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6

c7ba727058a58cccefbeddd53ed6f092aad56821e516ec4d127540255257a7e6 | Triage. (n.d.). https://tria.ge/251028-egk3kstrfz