Appendix 1

OSINT Investigation Appendix 1

CMIT-450-81: Senior Seminar Project

Instructor Michael Atwood

Kyle Hathaway

10.8.2025

Contents

Confirmed Malicious Domain #1 Evidence 2

Confirmed Malicious Domain #2 Evidence 3

Confirmed Malicious Domain #3 Evidence 4

Confirmed Malicious Domain #4 Evidence 6

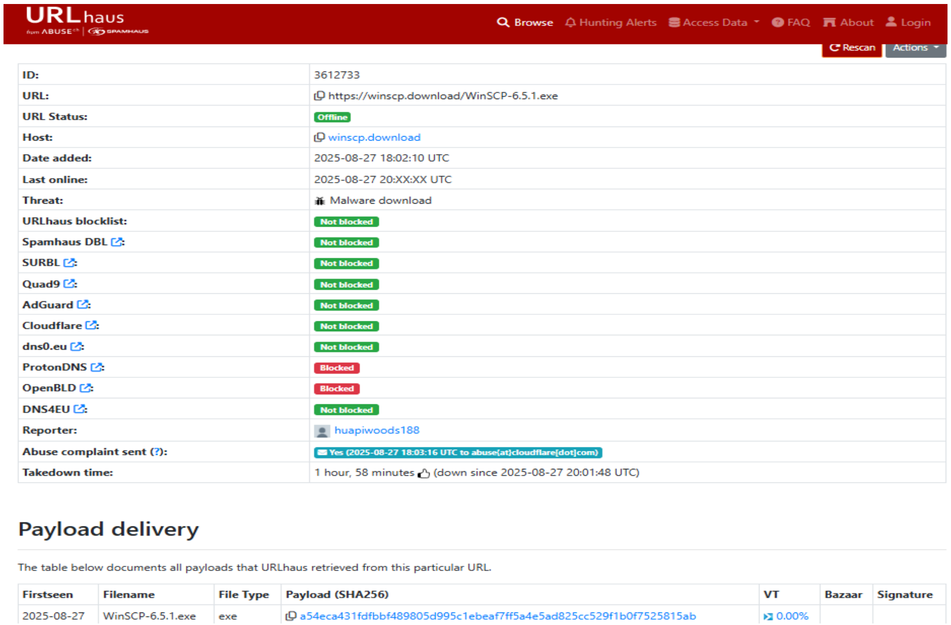
Confirmed Malicious Domain #5 Evidence 8

Confirmed Malicious Domain # 6 Evidence........ 10

Figure 1: URLhaus report on domain #1. 2
Figure 2: VirusTotal report on domain # 1......... 2
Figure 3: URLhaus report on Domain #2. 3
Figure 4: Virustotal report on domain #2. 3
Figure 5: URLhaus report on domain #3. 4
Figure 6: VirusTotal report on domain #3. 5
Figure 7: URLhaus report on domain #4. 6
Figure 8: VirusTotal report on domain #4. 7
Figure 9: URLhaus report on domain #5. 8
Figure 10: VirusTotal report on domain #5. 9
Figure 11: URlhaus report on domain #6. 10
Figure 12: VirusTotal report on domain #6. 11

Appendix 1

Confirmed Malicious Domain #1 Evidence



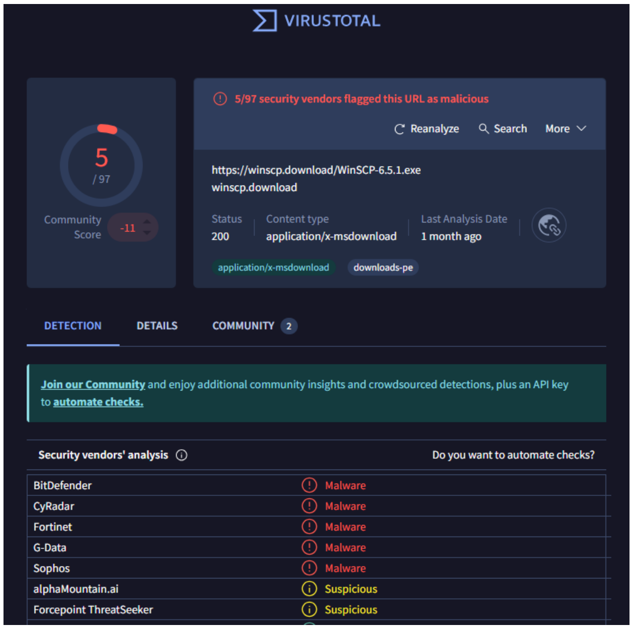
ID:	3612733
URL:	https://winscp.download/WinSCP-6.5.1.exe
URL Status:	Offline
Host:	winscp.download
Date added:	2025-08-27 18:02:10 UTC
Last online:	2025-08-27 20:XX:XX UTC
Threat:	Malware download
URLhaus blocklist:	Not blocked
Spamhaus DBL:	Not blocked
SURBL:	Not blocked
Quad9:	Not blocked
AdGuard:	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 1: URLhaus report on domain #1.



5/97 security vendors flagged this URL as malicious

https://winscp.download/WinSCP-6.5.1.exe
winscp.download

Status	Content type	Last Analysis Date
200	application/x-msdownload	1 month ago

application/x-msdownload downloads-pe

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

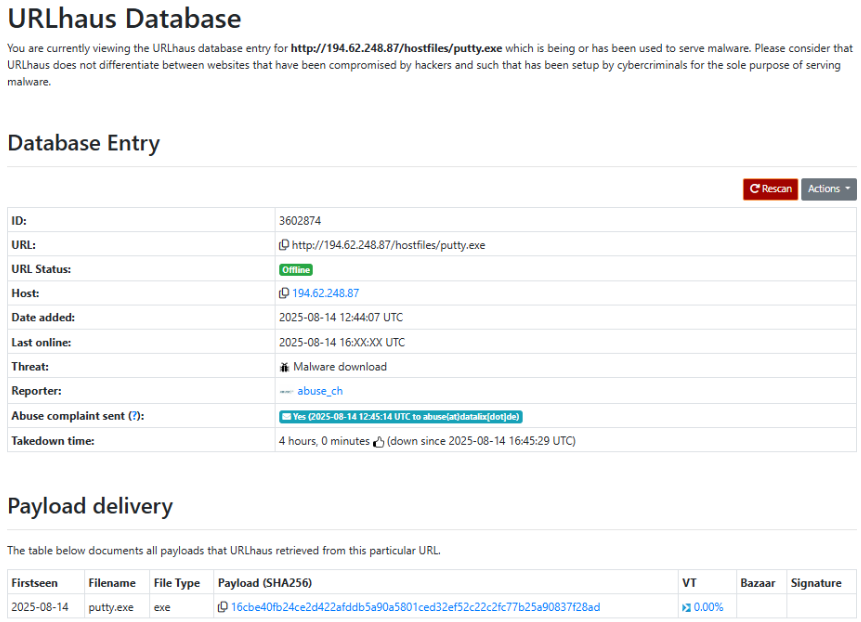
Security vendors' analysis — Do you want to automate checks?

BitDefender	Malware
CyRadar	Malware
Fortinet	Malware
G-Data	Malware
Sophos	Malware
alphaMountain.ai	Suspicious
Forcepoint ThreatSeeker	Suspicious

Figure 2: VirusTotal report on domain # 1.

Appendix 1

Confirmed Malicious Domain #2 Evidence



URLhaus Database

You are currently viewing the URLhaus database entry for **http://194.62.248.87/hostfiles/putty.exe** which is being or has been used to serve malware. Please consider that URLhaus does not differentiate between websites that have been compromised by hackers and such that has been setup by cybercriminals for the sole purpose of serving malware.

Database Entry

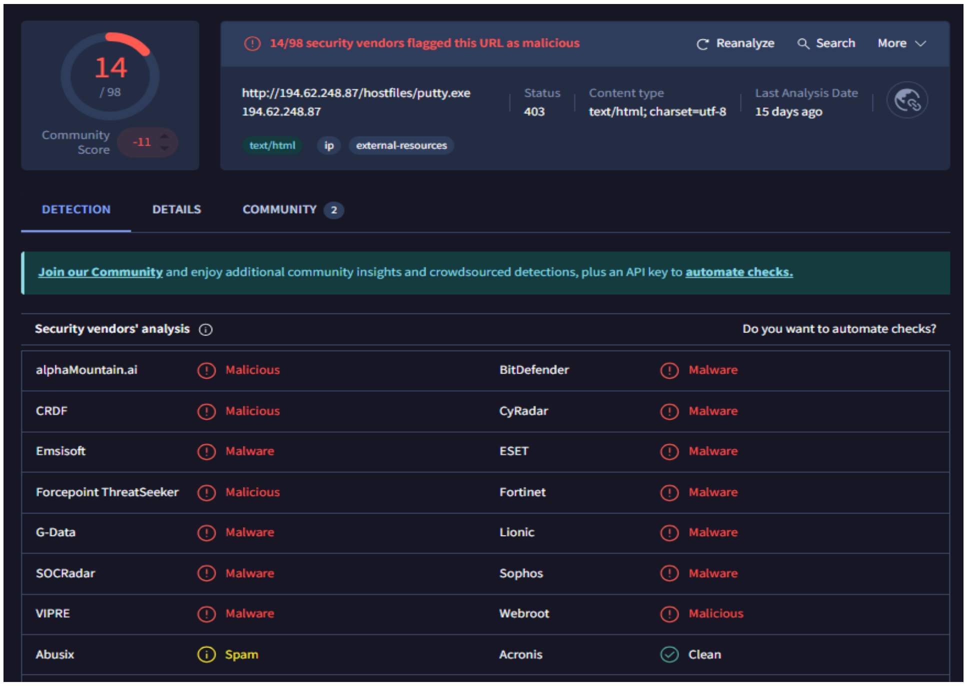
ID:	3602874
URL:	http://194.62.248.87/hostfiles/putty.exe
URL Status:	Offline
Host:	194.62.248.87
Date added:	2025-08-14 12:44:07 UTC
Last online:	2025-08-14 16:XX:XX UTC
Threat:	Malware download
Reporter:	abuse_ch
Abuse complaint sent (?):	Yes (2025-08-14 12:45:14 UTC to abuse[at]datalix[dot]de)
Takedown time:	4 hours, 0 minutes (down since 2025-08-14 16:45:29 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
2025-08-14	putty.exe	exe	16cbe40fb24ce2d422afddb5a90a5801ced32ef52c22c2fc77b25a90837f28ad	0.00%		

Figure 3: URLhaus report on Domain #2.



14/98 security vendors flagged this URL as malicious

http://194.62.248.87/hostfiles/putty.exe
194.62.248.87

Status
403

Content type
text/html; charset=utf-8

Last Analysis Date
15 days ago

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

Security vendors' analysis

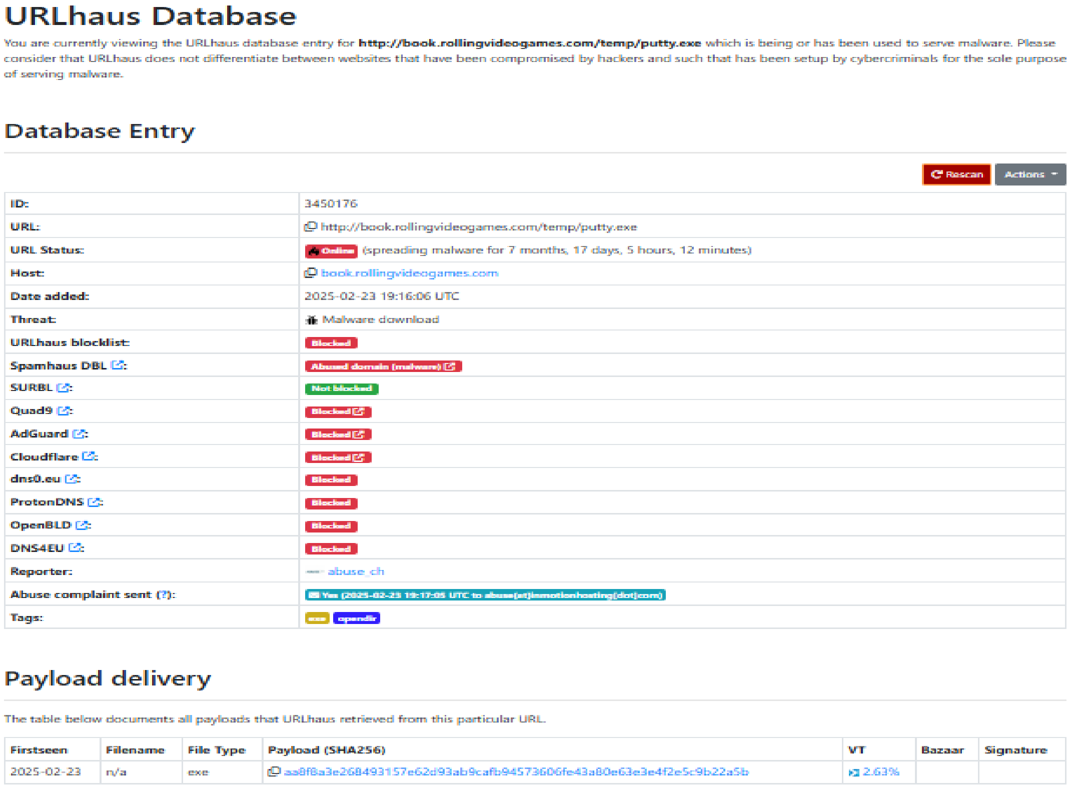
Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CRDF	Malicious	CyRadar	Malware
Emsisoft	Malware	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Data	Malware	Lionic	Malware
SOCRadar	Malware	Sophos	Malware
VIPRE	Malware	Webroot	Malicious
Abusix	Spam	Acronis	✓ Clean

Figure 4: Virustotal report on domain #2.

Appendix 1

Confirmed Malicious Domain #3 Evidence



URLhaus Database

You are currently viewing the URLhaus database entry for **http://book.rollingvideogames.com/temp/putty.exe** which is being or has been used to serve malware. Please consider that URLhaus does not differentiate between websites that have been compromised by hackers and such that has been setup by cybercriminals for the sole purpose of serving malware.

Database Entry

ID:	3450176
URL:	http://book.rollingvideogames.com/temp/putty.exe
URL Status:	Online (spreading malware for 7 months, 17 days, 5 hours, 12 minutes)
Host:	book.rollingvideogames.com
Date added:	2025-02-23 19:16:06 UTC
Threat:	Malware download
URLhaus blocklist:	Blocked
Spamhaus DBL:	Abused domain (malware)
SURBL:	Not blocked
Quad9:	Blocked
AdGuard:	Blocked
Cloudflare:	Blocked
dns0.eu:	Blocked
ProtonDNS:	Blocked
OpenBLD:	Blocked
DNS4EU:	Blocked
Reporter:	abuse_ch
Abuse complaint sent (?):	Yes (2025-02-23 19:17:05 UTC to abuse(at)inmotionhosting(dot)com)
Tags:	exe opendir

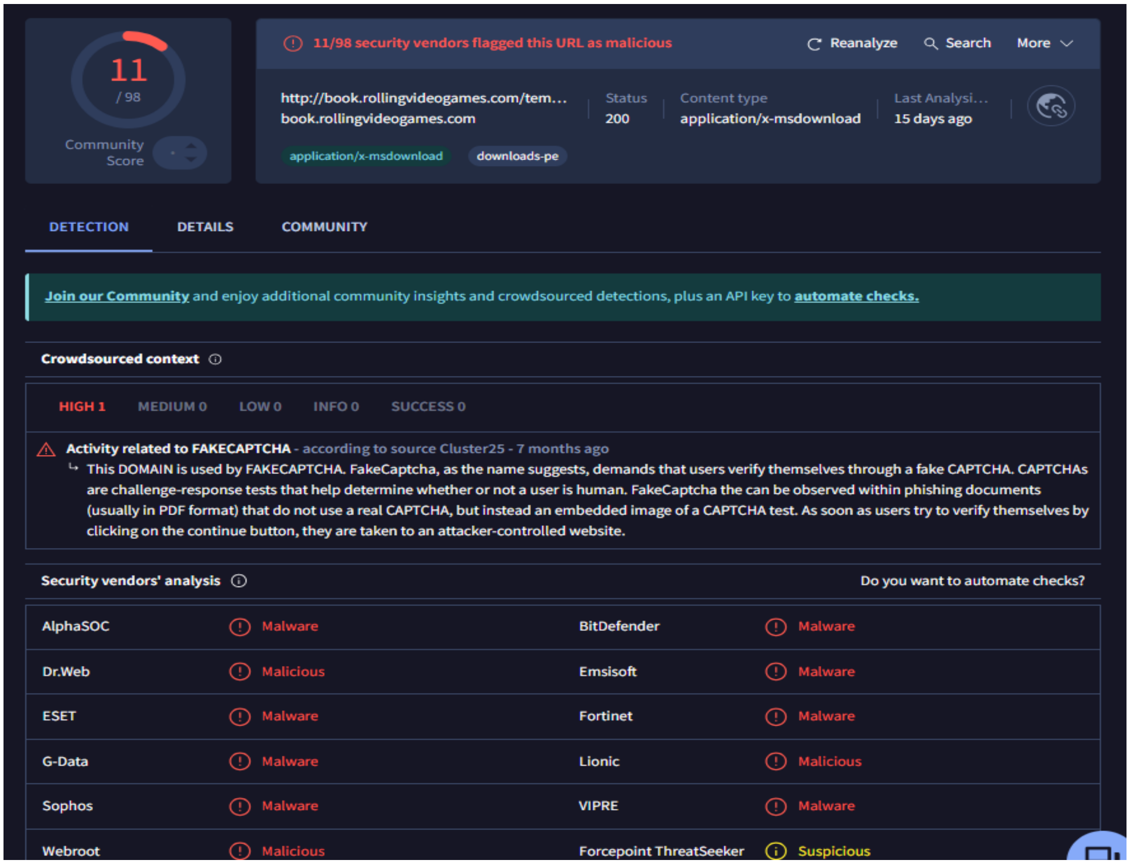
Payload delivery

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

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2025-02-23	n/a	exe	aa8f8a3e268493157e62d93ab9cafb94573606fe43a80e63e3e4f2e5c9b22a5b	2.63%		

Figure 5: URLhaus report on domain #3.

Appendix 1



11/98 security vendors flagged this URL as malicious

http://book.rollingvideogames.com/tem… book.rollingvideogames.com	Status 200	Content type application/x-msdownload	Last Analysi… 15 days ago

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

Crowdsourced context

Activity related to FAKECAPTCHA - according to source Cluster25 - 7 months ago

↳ This DOMAIN is used by FAKECAPTCHA. FakeCaptcha, as the name suggests, demands that users verify themselves through a fake CAPTCHA. CAPTCHAs are challenge-response tests that help determine whether or not a user is human. FakeCaptcha the can be observed within phishing documents (usually in PDF format) that do not use a real CAPTCHA, but instead an embedded image of a CAPTCHA test. As soon as users try to verify themselves by clicking on the continue button, they are taken to an attacker-controlled website.

Security vendors' analysis

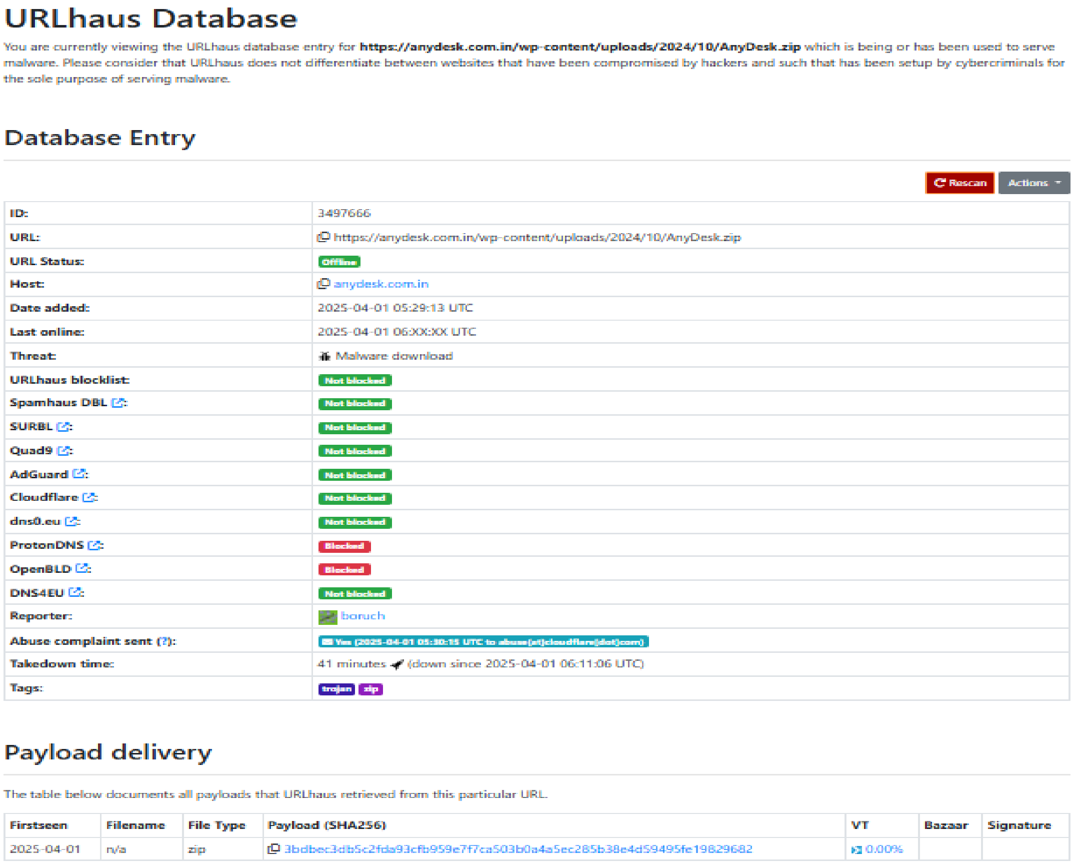
Do you want to automate checks?

AlphaSOC	Malware	BitDefender	Malware
Dr.Web	Malicious	Emsisoft	Malware
ESET	Malware	Fortinet	Malware
G-Data	Malware	Lionic	Malicious
Sophos	Malware	VIPRE	Malware
Webroot	Malicious	Forcepoint ThreatSeeker	Suspicious

Figure 6: VirusTotal report on domain #3.

Appendix 1

Confirmed Malicious Domain #4 Evidence



URLhaus Database

You are currently viewing the URLhaus database entry for **https://anydesk.com.in/wp-content/uploads/2024/10/AnyDesk.zip** which is being or has been used to serve malware. Please consider that URLhaus does not differentiate between websites that have been compromised by hackers and such that has been setup by cybercriminals for the sole purpose of serving malware.

Database Entry

ID:	3497666
URL:	https://anydesk.com.in/wp-content/uploads/2024/10/AnyDesk.zip
URL Status:	Offline
Host:	anydesk.com.in
Date added:	2025-04-01 05:29:13 UTC
Last online:	2025-04-01 06: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:	boruch
Abuse complaint sent (?):	✉ Yes (2025-04-01 05:30:15 UTC to abuse(at)cloudflare(dot)com)
Takedown time:	41 minutes (down since 2025-04-01 06:11:06 UTC)
Tags:	trojan zip

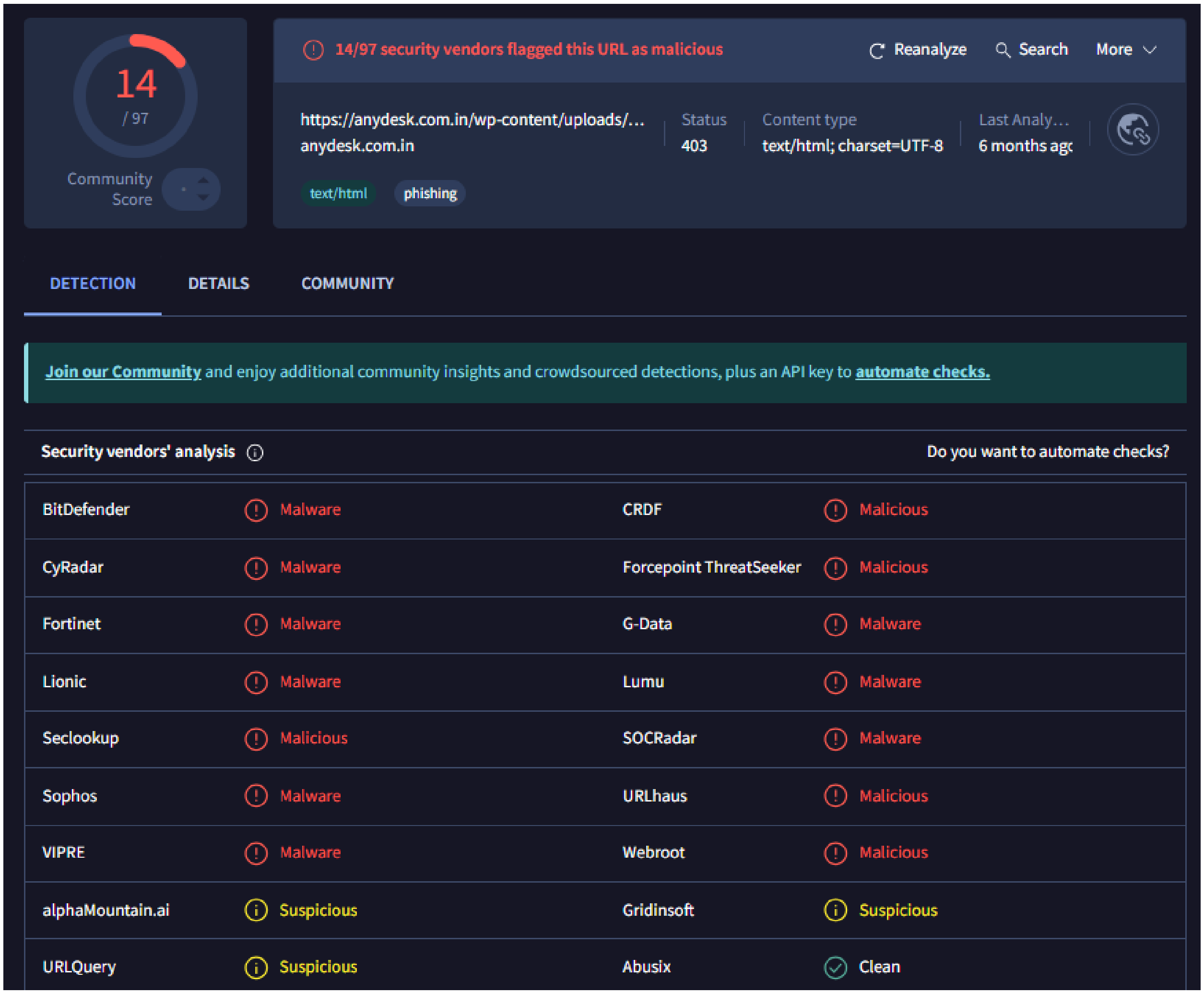
Payload delivery

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

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2025-04-01	n/a	zip	3bdbec3db5c2fda93cfb959e7f7ca503b0a4a5ec285b38e4d59495fe19829682	0.00%		

Figure 7: URLhaus report on domain #4.

Appendix 1



14/97 security vendors flagged this URL as malicious

https://anydesk.com.in/wp-content/uploads/...
anydesk.com.in

Status 403

Content type text/html; charset=UTF-8

Last Analy... 6 months agc

text/html phishing

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

Security vendors' analysis

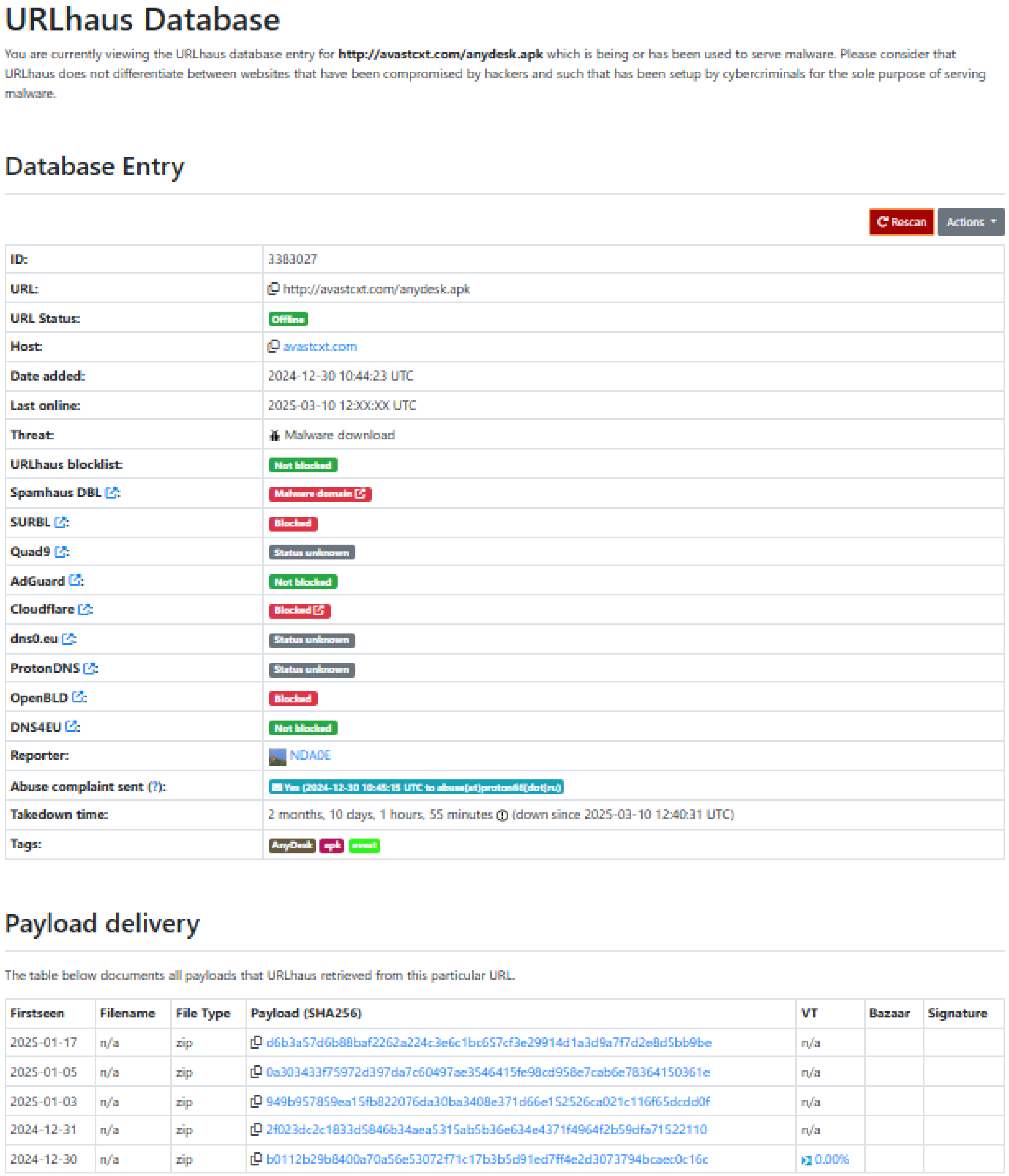
Do you want to automate checks?

BitDefender	Malware	CRDF	Malicious
CyRadar	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Lionic	Malware	Lumu	Malware
Seclookup	Malicious	SOCRadar	Malware
Sophos	Malware	URLhaus	Malicious
VIPRE	Malware	Webroot	Malicious
alphaMountain.ai	Suspicious	Gridinsoft	Suspicious
URLQuery	Suspicious	Abusix	Clean

Figure 8: VirusTotal report on domain #4.

Appendix 1

Confirmed Malicious Domain #5 Evidence



URLhaus Database

You are currently viewing the URLhaus database entry for **http://avastcxt.com/anydesk.apk** which is being or has been used to serve malware. Please consider that URLhaus does not differentiate between websites that have been compromised by hackers and such that has been setup by cybercriminals for the sole purpose of serving malware.

Database Entry

ID:	3383027
URL:	http://avastcxt.com/anydesk.apk
URL Status:	Offline
Host:	avastcxt.com
Date added:	2024-12-30 10:44:23 UTC
Last online:	2025-03-10 12:XX:XX UTC
Threat:	Malware download
URLhaus blocklist:	Not blocked
Spamhaus DBL:	Malware domain
SURBL:	Blocked
Quad9:	Status unknown
AdGuard:	Not blocked
Cloudflare:	Blocked
dns0.eu:	Status unknown
ProtonDNS:	Status unknown
OpenBLD:	Blocked
DNS4EU:	Not blocked
Reporter:	NDA0E
Abuse complaint sent (?):	Yes (2024-12-30 10:45:15 UTC to abuse(at)proton66(dot)ru)
Takedown time:	2 months, 10 days, 1 hours, 55 minutes (down since 2025-03-10 12:40:31 UTC)
Tags:	AnyDesk apk avast

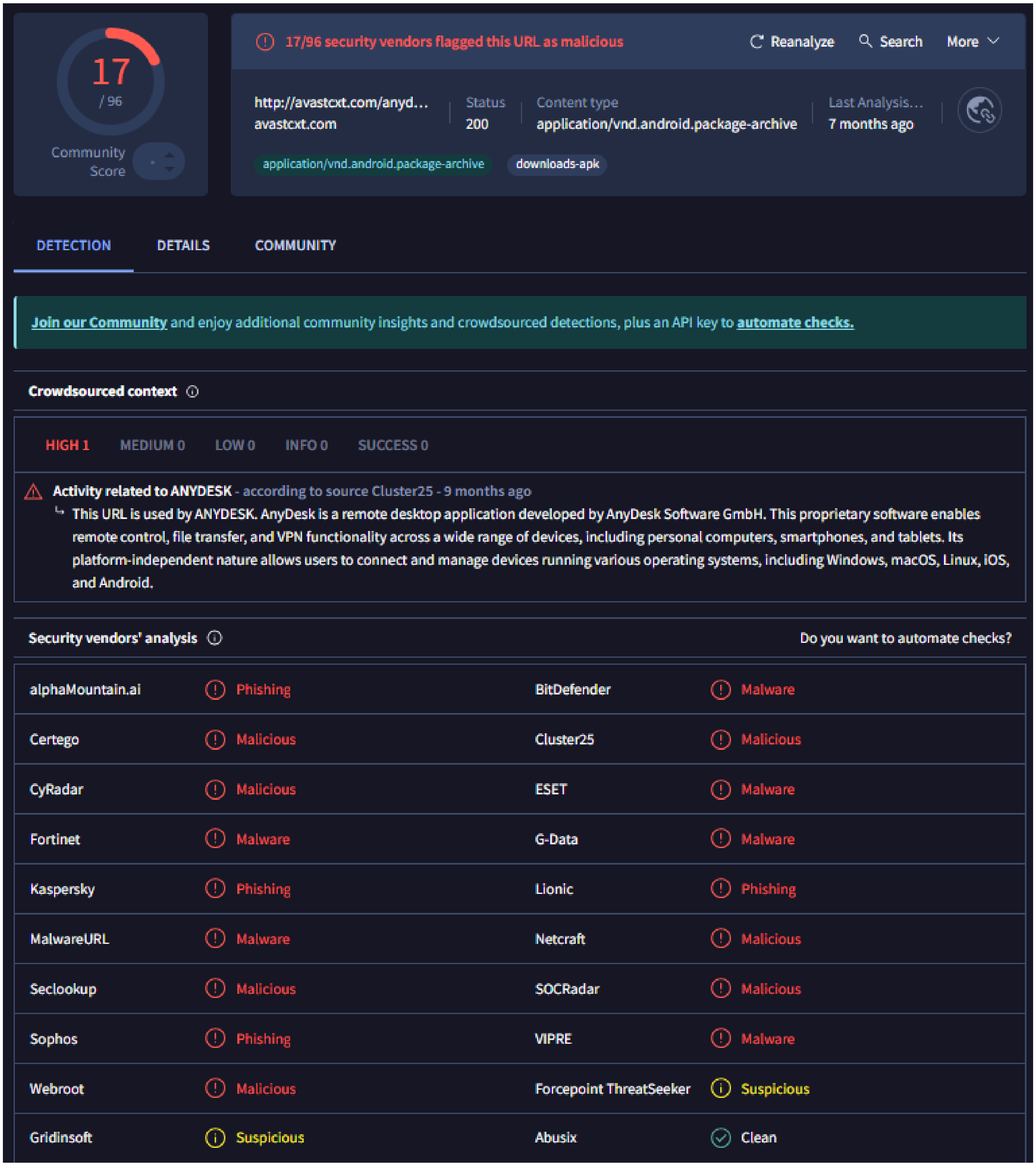
Payload delivery

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

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2025-01-17	n/a	zip	d6b3a57d6b88baf2262a224c3e6c1bc657cf3e29914d1a3d9a7f7d2e8d5bb9be	n/a		
2025-01-05	n/a	zip	0a303433f75972d397da7c60497ae3546415fe98cd958e7cab6e78364150361e	n/a		
2025-01-03	n/a	zip	949b957859ea15fb822076da30ba3408e371d66e152526ca021c116f65dcdd0f	n/a		
2024-12-31	n/a	zip	2f023dc2c1833d5846b34aea5315ab5b36e634e4371f4964f2b59dfa71522110	n/a		
2024-12-30	n/a	zip	b0112b29b8400a70a56e53072f71c17b3b5d91ed7ff4e2d3073794bcaec0c16c	0.00%		

Figure 9: URLhaus report on domain #5.

Appendix 1



17 / 96

Community Score

17/96 security vendors flagged this URL as malicious

http://avastcxt.com/anyd...
avastcxt.com

Status: 200

Content type: application/vnd.android.package-archive

Last Analysis...: 7 months ago

application/vnd.android.package-archive downloads-apk

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

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

⚠ **Activity related to ANYDESK** - according to source Cluster25 - 9 months ago

↳ This URL is used by ANYDESK. AnyDesk is a remote desktop application developed by AnyDesk Software GmbH. This proprietary software enables remote control, file transfer, and VPN functionality across a wide range of devices, including personal computers, smartphones, and tablets. Its platform-independent nature allows users to connect and manage devices running various operating systems, including Windows, macOS, Linux, iOS, and Android.

Security vendors' analysis

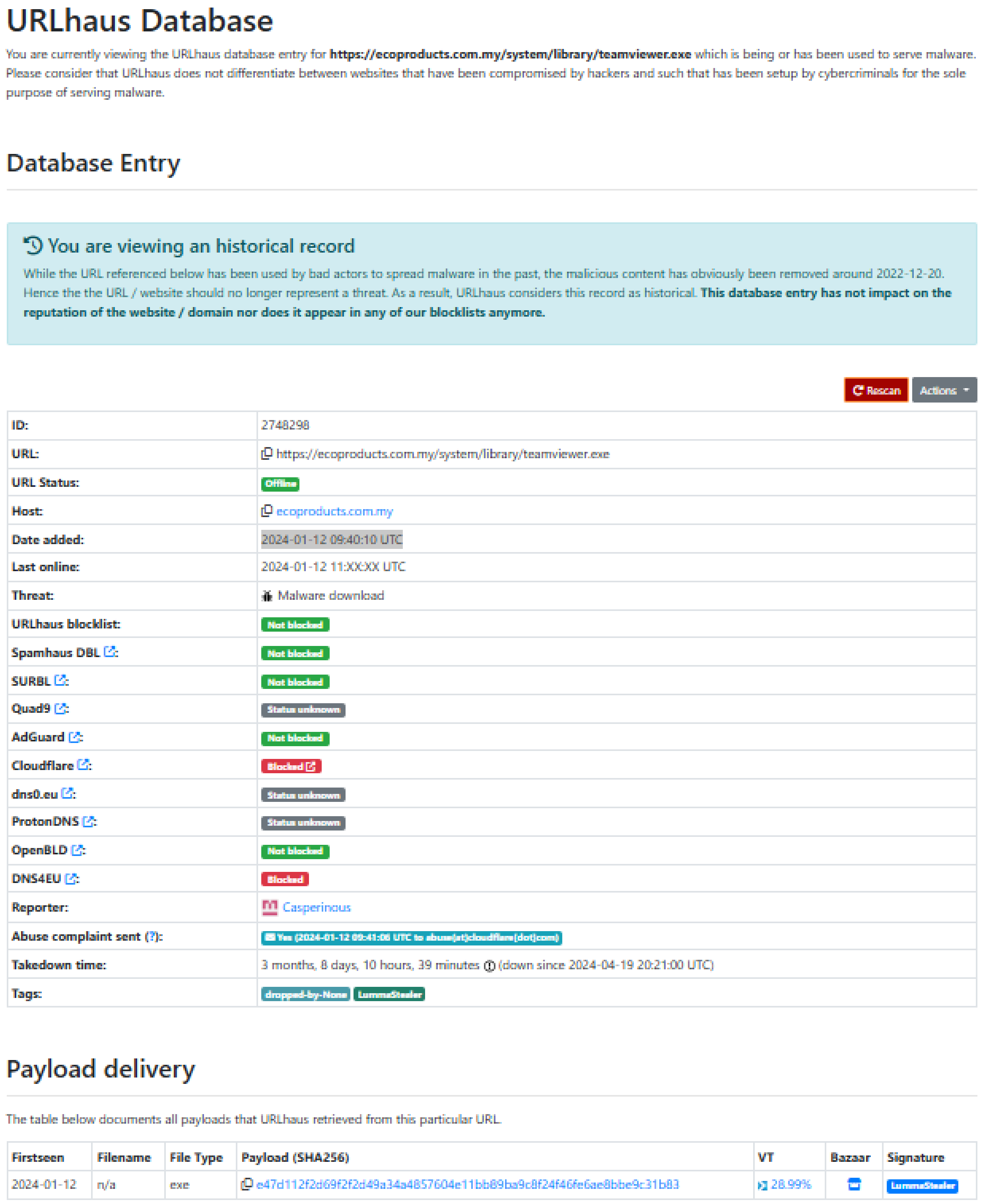
Do you want to automate checks?

alphaMountain.ai	ⓘ Phishing	BitDefender	ⓘ Malware
Certego	ⓘ Malicious	Cluster25	ⓘ Malicious
CyRadar	ⓘ Malicious	ESET	ⓘ Malware
Fortinet	ⓘ Malware	G-Data	ⓘ Malware
Kaspersky	ⓘ Phishing	Lionic	ⓘ Phishing
MalwareURL	ⓘ Malware	Netcraft	ⓘ Malicious
Seclookup	ⓘ Malicious	SOCRadar	ⓘ Malicious
Sophos	ⓘ Phishing	VIPRE	ⓘ Malware
Webroot	ⓘ Malicious	Forcepoint ThreatSeeker	ⓘ Suspicious
Gridinsoft	ⓘ Suspicious	Abusix	✓ Clean

Figure 10: VirusTotal report on domain #5.

Appendix 1

Confirmed Malicious Domain # 6 Evidence



URLhaus Database

You are currently viewing the URLhaus database entry for **https://ecoproducts.com.my/system/library/teamviewer.exe** which is being or has been used to serve malware. Please consider that URLhaus does not differentiate between websites that have been compromised by hackers and such that has been setup by cybercriminals for the sole purpose of serving malware.

Database Entry

You are viewing an historical record

While the URL referenced below has been used by bad actors to spread malware in the past, the malicious content has obviously been removed around 2022-12-20. Hence the the URL / website should no longer represent a threat. As a result, URLhaus considers this record as historical. **This database entry has not impact on the reputation of the website / domain nor does it appear in any of our blocklists anymore.**

ID:	2748298
URL:	https://ecoproducts.com.my/system/library/teamviewer.exe
URL Status:	Offline
Host:	ecoproducts.com.my
Date added:	2024-01-12 09:40:10 UTC
Last online:	2024-01-12 11:XX:XX UTC
Threat:	Malware download
URLhaus blocklist:	Not blocked
Spamhaus DBL:	Not blocked
SURBL:	Not blocked
Quad9:	Status unknown
AdGuard:	Not blocked
Cloudflare:	Blocked
dns0.eu:	Status unknown
ProtonDNS:	Status unknown
OpenBLD:	Not blocked
DNS4EU:	Blocked
Reporter:	Casperinous
Abuse complaint sent (?):	Yes (2024-01-12 09:41:06 UTC to abuse(at)cloudflare(dot)com)
Takedown time:	3 months, 8 days, 10 hours, 39 minutes (down since 2024-04-19 20:21:00 UTC)
Tags:	dropped-by-None LummaStealer

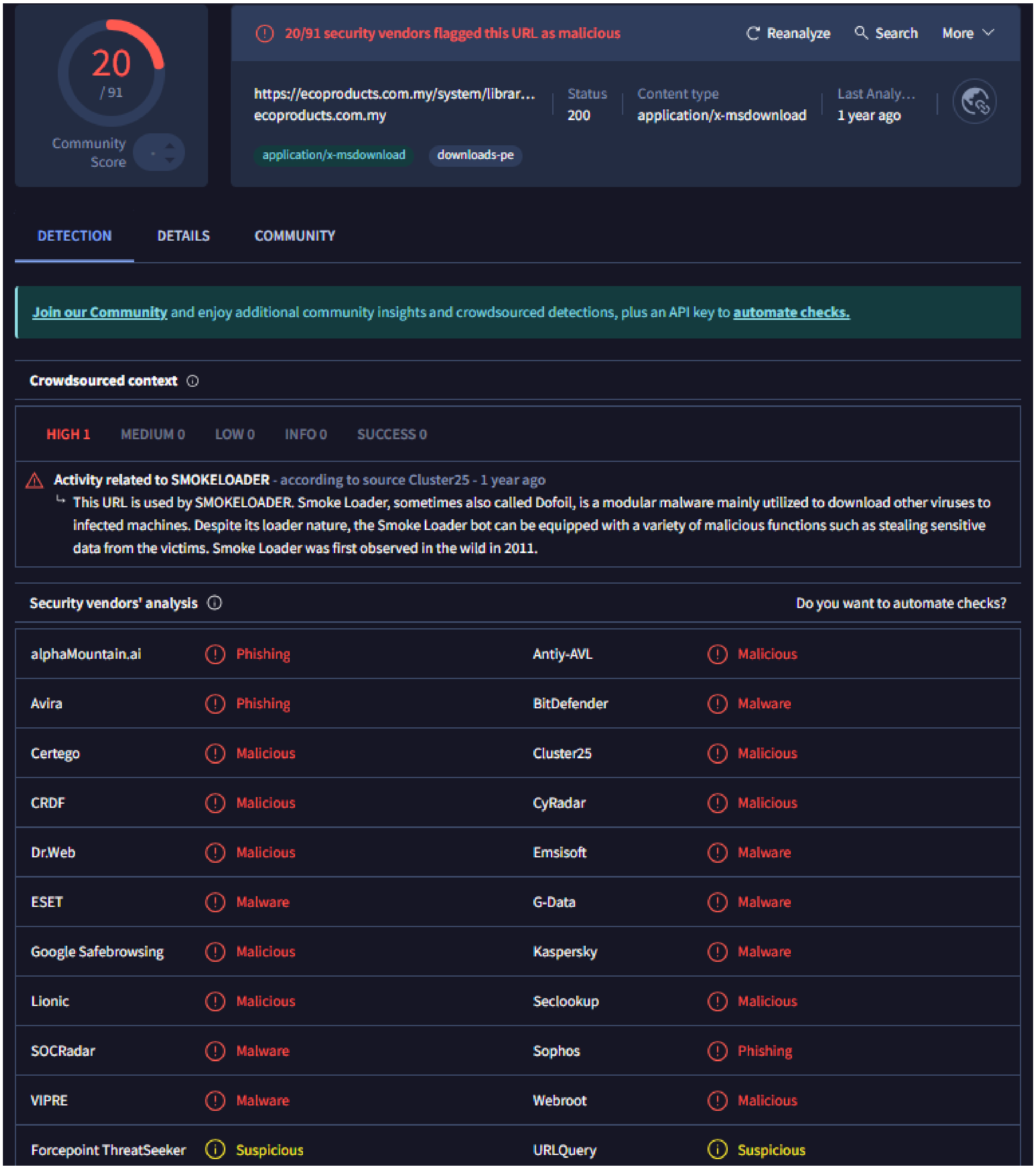
Payload delivery

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

Firstseen	Filename	File Type	Payload (SHA256)	VT	Bazaar	Signature
2024-01-12	n/a	exe	e47d112f2d69f2f2d49a34a4857604e11bb89ba9c8f24f46fe6ae8bbe9c31b83	28.99%		LummaStealer

Figure 11: URlhaus report on domain #6.

Appendix 1



20/91 security vendors flagged this URL as malicious

https://ecoproducts.com.my/system/librar...
ecoproducts.com.my

Status
200

Content type
application/x-msdownload

Last Analy...
1 year ago

application/x-msdownload downloads-pe

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

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to SMOKELOADER - according to source Cluster25 - 1 year ago

This URL is used by SMOKELOADER. Smoke Loader, sometimes also called Dofoil, is a modular malware mainly utilized to download other viruses to infected machines. Despite its loader nature, the Smoke Loader bot can be equipped with a variety of malicious functions such as stealing sensitive data from the victims. Smoke Loader was first observed in the wild in 2011.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Phishing	Antiy-AVL	Malicious
Avira	Phishing	BitDefender	Malware
Certego	Malicious	Cluster25	Malicious
CRDF	Malicious	CyRadar	Malicious
Dr.Web	Malicious	Emsisoft	Malware
ESET	Malware	G-Data	Malware
Google Safebrowsing	Malicious	Kaspersky	Malware
Lionic	Malicious	Seclookup	Malicious
SOCRadar	Malware	Sophos	Phishing
VIPRE	Malware	Webroot	Malicious
Forcepoint ThreatSeeker	Suspicious	URLQuery	Suspicious

Figure 12: VirusTotal report on domain #6.