Hunting pack use case: RedLeaves malware

community.rsa.com/community/products/netwitness/blog/2017/05/03/hunting-pack-use-case-redleaves-malware

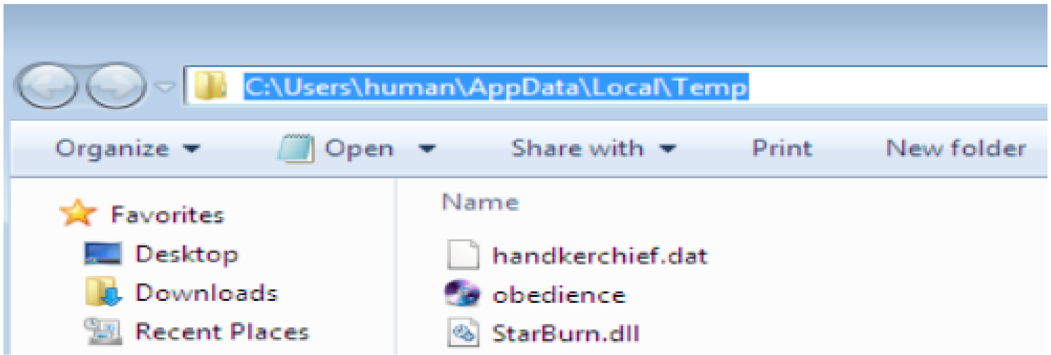
May 3, 2017

On April 27, 2017 The United States Computer Emergency Readiness Team (US-CERT) released an alert TA17-117A [1] with information on an emerging sophisticated campaign. The campaign has been active since at least May 2016 and targets organization in several sectors, including Information Technology, Energy, Healthcare and Public Health, Communications and Critical Manufacturing. The threat actors have deployed multiple malware families and variants in their campaign including PlugX and RedLeaves.

This threat advisory discusses the host and network behavior of RedLeaves malware. In addition, it shows how to leverage the Hunting pack to detect RedLeaves network activity using RSA NetWitness Logs and Packets.

A typical infection scenario starts with a dropper dropping a legitimate application (EXE), a malicious DLL, and an encoded DATA file in the user %TMP% folder [2].

The screenshot below shows the files dropped by a RedLeaves sample on a victim machine [3]:



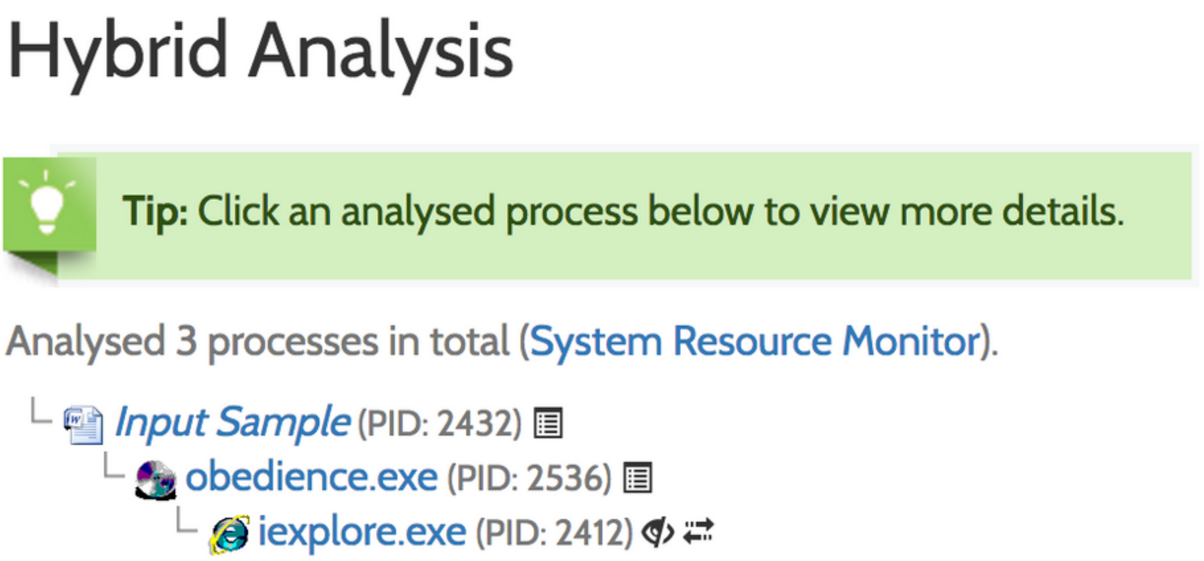
C:\Users\human\AppData\Local\Temp

Name

handkerchief.dat
obedience
StarBurn.dll

Filename	SHA256
obedience.exe	aba4df64717462c61801d737c9fa20a7fada61539eaef50954331d31f7306d27
StarBurn.dll	adb72a24429441f743bd2b1a9c0116ae9a1e7b217e047849d70ca1e9054dbdb6
handkerchief.dat	773b176b3a68c3d21fae907af8fba7908b55726bd591c5335c8c0bc9de179b76

It then starts the application. Taking advantage of DLL preloading, the EXE file loads the malicious DLL, which reads, decodes, and then executes the DATA file. It then creates a new process and injects itself into it. Below is a snapshot of the process tree after running the same sample on hybrid-analysis.com [4]:



Hybrid Analysis

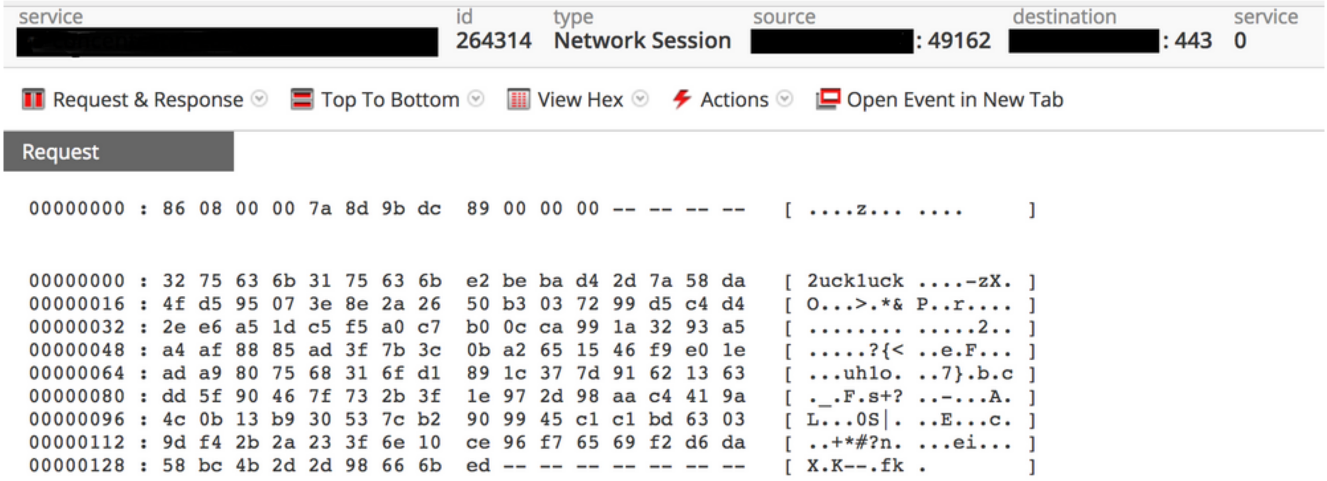
Tip: Click an analysed process below to view more details.

Analysed 3 processes in total (System Resource Monitor).

- *Input Sample* (PID: 2432)
  - obedience.exe (PID: 2536)
    - iexplore.exe (PID: 2412)

To ensure that one instance of the malware is running on an infected system, the malware creates a mutant. In this case, it is vv11287GD. To gain persistency on the system, the malware creates a link in the Startup folder pointing to the legitimate application dropped in the %TEMP% folder.

The malware starts beaconing to its C2 server using raw TCP over port 443 as follows:



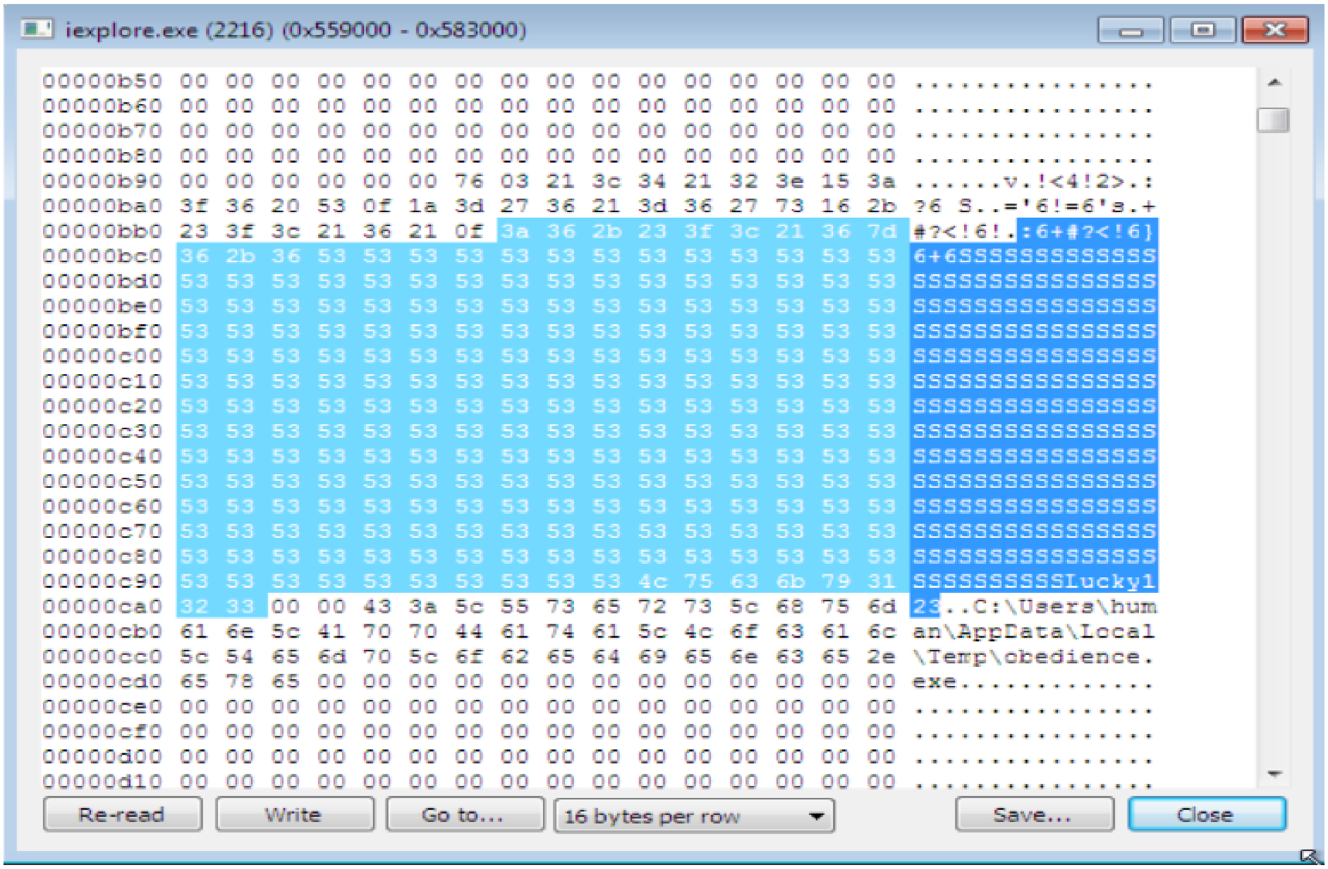
service	id	type	source	destination	service
[redacted]	264314	Network Session	[redacted]: 49162	[redacted]: 443	0

Request

```
00000000 : 86 08 00 00 7a 8d 9b dc  89 00 00 00 -- -- -- --   [ ....z... ....      ]


00000000 : 32 75 63 6b 31 75 63 6b  e2 be ba d4 2d 7a 58 da   [ 2uck1uck ....-zX. ]
00000016 : 4f d5 95 07 3e 8e 2a 26  50 b3 03 72 99 d5 c4 d4   [ O...>.*& P..r.... ]
00000032 : 2e e6 a5 1d c5 f5 a0 c7  b0 0c ca 99 1a 32 93 a5   [ ........ .....2.. ]
00000048 : a4 af 88 85 ad 3f 7b 3c  0b a2 65 15 46 f9 e0 1e   [ .....?{< ..e.F... ]
00000064 : ad a9 80 75 68 31 6f d1  89 1c 37 7d 91 62 13 63   [ ...uh1o. ..7}.b.c ]
00000080 : dd 5f 90 46 7f 73 2b 3f  1e 97 2d 98 aa c4 41 9a   [ ._.F.s+? ..-...A. ]
00000096 : 4c 0b 13 b9 30 53 7c b2  90 99 45 c1 c1 bd 63 03   [ L...0S|. ..E...c. ]
00000112 : 9d f4 2b 2a 23 3f 6e 10  ce 96 f7 65 69 f2 d6 da   [ ..+*#?n. ...ei... ]
00000128 : 58 bc 4b 2d 2d 98 66 6b  ed -- -- -- -- -- -- --   [ X.K--.fk .        ]
```

As explained in the alert issued by US-CERT, the payload follows two 12-bytes fixed length headers. The first header comes in its own packet, the second header and the payload in a separate packet in the same TCP stream. The first four bytes of the second header (0x3275636b) represent the length of the encrypted and compressed payload (XOR encoded with the first four bytes of the RC4 key), the second four bytes of the second header (0x3175636b) represent the length of the decrypted and decompressed payload (XOR encoded with the first four bytes of the RC4 key).

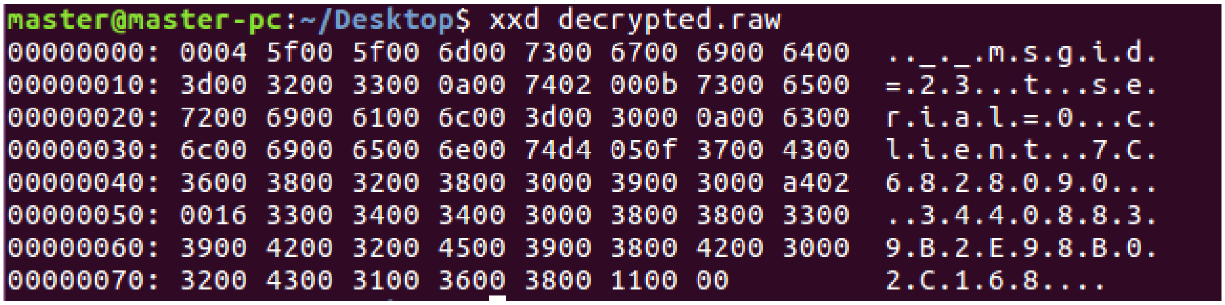
Analyzing the strings in the address space of the injected process; in this case iexplore.exe; suggests that the RC4 key is Lucky123 with null byte appended:



iexplore.exe (2216) (0x559000 - 0x583000)

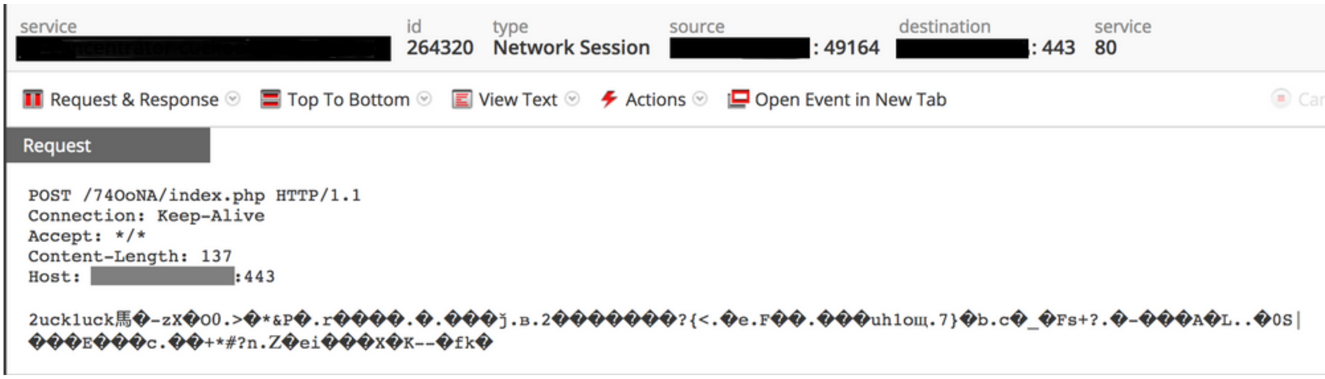
```
00000b50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000b60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000b70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000b80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000b90 00 00 00 00 00 00 76 03 21 3c 34 21 32 3e 15 3a ......v.!<4!2>.:
00000ba0 3f 36 20 53 0f 1a 3d 27 36 21 3d 36 27 73 16 2b ?6 S..='6!=6's.+
00000bb0 23 3f 3c 21 36 21 0f 3a 36 2b 23 3f 3c 21 36 7d #?<!6!.:6+#?<!6}
00000bc0 36 2b 36 53 53 53 53 53 53 53 53 53 53 53 53 53 6+6SSSSSSSSSSSSS
00000bd0 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000be0 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000bf0 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c00 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c10 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c20 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c30 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c40 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c50 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c60 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c70 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c80 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 53 SSSSSSSSSSSSSSSS
00000c90 53 53 53 53 53 53 53 53 53 53 4c 75 63 6b 79 31 SSSSSSSSSSLucky1
00000ca0 32 33 00 00 43 3a 5c 55 73 65 72 73 5c 68 75 6d 23..C:\Users\hum
00000cb0 61 6e 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c an\AppData\Local
00000cc0 5c 54 65 6d 70 5c 6f 62 65 64 69 65 6e 63 65 2e \Temp\obedience.
00000cd0 65 78 65 00 00 00 00 00 00 00 00 00 00 00 00 00 exe.............
00000ce0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000cf0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000d00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000d10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Here is the decrypted payload:



```
master@master-pc:~/Desktop$ xxd decrypted.raw
00000000: 0004 5f00 5f00 6d00 7300 6700 6900 6400  .._._.m.s.g.i.d.
00000010: 3d00 3200 3300 0a00 7402 000b 7300 6500  =.2.3...t...s.e.
00000020: 7200 6900 6100 6c00 3d00 3000 0a00 6300  r.i.a.l.=.0...c.
00000030: 6c00 6900 6500 6e00 74d4 050f 3700 4300  l.i.e.n.t...7.C.
00000040: 3600 3800 3200 3800 3000 3900 3000 a402  6.8.2.8.0.9.0...
00000050: 0016 3300 3400 3400 3000 3800 3800 3300  ..3.4.4.0.8.8.3.
00000060: 3900 4200 3200 4500 3900 3800 4200 3000  9.B.2.E.9.8.B.0.
00000070: 3200 4300 3100 3600 3800 1100 00         2.C.1.6.8....
```

The malware also sends the same payload along with the second header to the server as an HTTP POST request over port 443:



service	id	type	source	destination	service
[redacted]	264320	Network Session	[redacted]: 49164	[redacted]: 443	80

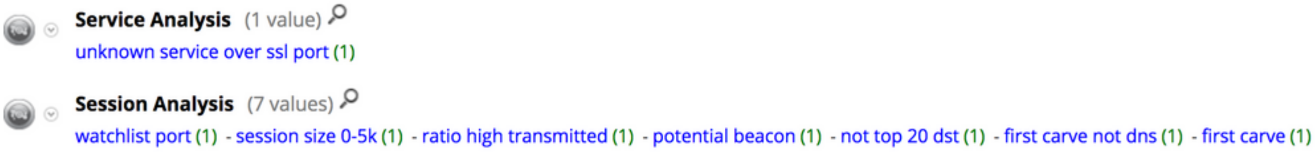
```
POST /74OoNA/index.php HTTP/1.1
Connection: Keep-Alive
Accept: */*
Content-Length: 137
Host: [redacted]:443

2uck1uck馬�-zX�O0.>�*&P�.r����.�.���ĵ.в.2��������?{<.�e.F��.���uh1oщ.7}�b.c�_�Fs+?.�-���A�L..�0S|
���E���c.��+*#?n.Z�ei���X�K--�fk�
```

A list of commands supported by RedLeaves can be found in the report released by the NCC Group Cyber Defence Operations team [5].

Detection using Hunting Pack

The Hunting pack is designed to allow you to quickly hunt for indicators of compromise or anomalous network activity by dissecting packet traffic within the NetWitness Suite and populating specific meta keys with natural language values for investigation. For more information on the hunting pack including how to deploy it in your environment, please refer to RSA documentation [6].

The screenshot below shows some of the meta keys registered by the hunting pack for the initial RedLeaves beaconing session. That is the one using a raw TCP connection over port 443:



Service Analysis (1 value)
unknown service over ssl port (1)

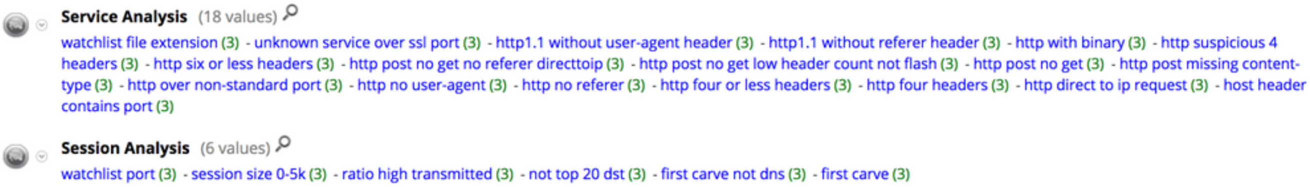
Session Analysis (7 values)
watchlist port (1) - session size 0-5k (1) - ratio high transmitted (1) - potential beacon (1) - not top 20 dst (1) - first carve not dns (1) - first carve (1)

The session was tagged with different meta values indicating suspicious traffic over SSL port. Here is a description of some of those values:

Meta Value	Description
session size 0-5k	A total session size, request + response payload, between 0KB and 5KB
ratio high transmitted	Between 75% and 100% of the session payload transmitted outbound
potential beacon	Session assumed to be programmatic, nefarious communications
not top 20 dst	org.dst is not one of the most common 20 destinations

Meta Value	Description
first carve	outbound traffic with two streams and payload > 0
first carve not dns	outbound traffic with two streams and payload > 0 and not service type 53

The screenshot below shows some of the meta keys registered by the hunting pack for the following RedLeaves beaconing sessions. Those are the ones that use HTTP POST requests over port 443:



Service Analysis (18 values)

watchlist file extension (3) - unknown service over ssl port (3) - http1.1 without user-agent header (3) - http1.1 without referer header (3) - http with binary (3) - http suspicious 4 headers (3) - http six or less headers (3) - http post no get no referer directtoip (3) - http post no get low header count not flash (3) - http post no get (3) - http post missing content-type (3) - http over non-standard port (3) - http no user-agent (3) - http no referer (3) - http four or less headers (3) - http four headers (3) - http direct to ip request (3) - host header contains port (3)

Session Analysis (6 values)

watchlist port (3) - session size 0-5k (3) - ratio high transmitted (3) - not top 20 dst (3) - first carve not dns (3) - first carve (3)

The sessions were tagged with different meta values indicating suspicious HTTP traffic over SSL port. Here is a description of some of those values:

Meta Value	Description
watchlist file extension	Any executable extension commonly used with malware like .exe, .php, .zip, etc
http with binary	HTTP with binary data in the body
http suspicious 4 headers	Sessions with only HTTP POST and four HTTP headers
host-header contains port	Host header directly declares a port such as 'www.example.com:80'
http post no get low header count not flash	An HTTP POST request with less than 6 Headers and the user-agent is not ‘shockwave flash’
http post no get no referrer directtoip	HTTP session with at least one POST request to an IP address, no GET requests, and no referer

While the network behavior explained earlier is not unique to RedLeaves malware, the hunting pack can help an analyst in identifying suspicious traffic in the environment without relying on any network signatures.

References:

1. https://www.us-cert.gov/ncas/alerts/TA17-117A
2. http://blog.jpcert.or.jp/2017/04/redleaves---malware-based-on-open-source-rat.html
3. https://www.virustotal.com/en/file/5262cb9791df50fafcb2fbd5f93226050b51efe400c2924eecba97b7ce437481/analysis/
4. https://www.hybrid-analysis.com/sample/5262cb9791df50fafcb2fbd5f93226050b51efe400c2924eecba97b7ce437481?environmentId=100
5. https://github.com/nccgroup/Cyber-Defence/blob/master/Technical%20Notes/Red%20Leaves/Source/Red%20Leaves%20technical%20note%20v1.0.md
6. https://community.rsa.com/docs/DOC-62341