They've asked us to do some analysis. I'd like you to determine what happened: Was the traffic malicious? If so, where did it originate and what was the result? Was the aide's computer infected with malware? If so, what kind? These questions are only starting points. You'll come up with additional questions (and answers, I hope) during your analysis. Like last time, your analysis should be complete and systematic. I'm looking forward to seeing your report.

Look for the initial point of contact (in a browser interaction, it is known as the landing page)—and then watch for other details about exactly what transpired as the attack unfolded

Each Snort alert was triggered by a single packet. Find the packets that triggered each of the Snort alerts. Hint: look for common features in both the Snort alerts and the network packets. If you can find a single feature that uniquely maps Snort alerts back to packets, you'll have the packets that triggered the alerts.

Now it's time to start building our analysis.The answers to these questions belong in your technical section.

Confirm the date and time of the compromise.

If you have determined that an Exploit Kit (EK) was involved, answer the following questions for your technical appendix:

Identify the IP address(es) and host(s) that generated the EK traffic.
IP: 108.178.15.187, 173.194.39.31
Host:

What website did the user visit

Which EK do you suspect? Why?
Nuclear EK - I suspect the Nuclear Exploit Kit was used as the Snort alert file lists this name directly.

What vulnerability or vulnerabilities were exploited in the attack?
Outdated Flash Player

Some of these questions will be easy to answer. Others require more work. Don't expect to zip through this in a single sitting.

Construct a timeline of the most important events in the attack, explaining what happened at each point in time. Make your timeline concise and easy to read. Each timeline entry should contain (1) a packet number, and (2) a brief (no more than one or two lines) description of the event in plain English. You may use EK terminology, URLs', and host names in your event descriptions, but no other technical terms or technical content.

Your timeline of the most important events in the attack.
A technical section containing all your notes, useful screenshots, and observations about the PCAP
A list of your questions, working hypotheses, and confirmed facts substantiated by the PCAP
A list of refevant references that were useful to you during your investigation

You may organize (2), (3), and (4) any way you like, but your timeline must follow our timeline specifications.

Here are the key packets to focus on:

~~The packet where the laptop first accessed the compromised wolfgangssteakhouse[.]co[.]kr website.~~
~~Any packets where the laptop was redirected through gates leading to the EK landing page.~~
~~The packet where the laptop first accessed the EK landing page.~~
~~Any packets where the EK sent exploits to the laptop.~~
~~Any packets where the EK sent payloads to the laptop.~~

Active Hypotheses:

User logged on and made several queries in what seemed to be an attempt to search for a Microsoft documentation site. User was maliciously redirected (via a Cushioning Attack) to an EK landing site (wolfgangsteakhouse) where malware payload(s) were delivered.

Timeline:

Packet #1148 (23:33:39.356557): Barto-PC first accesses compromised website '*wolfgangssteakhouse.co.kr'*

Packet #1837 (23:33:44.978479): Barto-PC is redirected from (*wolfgangssteakhouse.co.kr*) to gate (bnureb0up683ppcbgt1fz9g.isbul.info)

Packet #2104 (23:33:45.849418): Barto-PC (from bnureb0up683ppcbgt1fz9g.isbul.info) is sent to (http://zz1lb82z00y16gdow25fcxm.ilaclama.us/watch.php?fuhgi=MTIyMDU5ODkwNjhkMTQ5ODNkNDI2YWEzNWJjYjNjNTJ)

Packet #2521 (23:33:48.225258): Barto-PC redirected (from zz1lb82z00y16gdow25fcxm.ilaclama.us) to EK landing page (http://f9wb0396aobdotyzddcwdtf.ilaclama.us/VQlXBEpVSwQ.html)

Packet #2561 (23:33:49.033657): Barto-PC accesses EK landing page (/VQlXBEpVSwQ.html)

Packet #2617 (23:33:54.669953): Nuclear EK sends an SWF exploit to Barto-PC; SWF denotes an Adobe Flash File format that the EK is attempting to exploit

Packet #2634 (23:33:56.058965): Nuclear EK sends SilverLight exploit to Barto-PC SilverLight denotes a framework application that is now available as a plug-in which the EK is attempting to exploit

Packet #2658 (23:33:57.418697): Nuclear EK delivers Payload to Barto-PC

Packet #2798 (23:34:01.876444): Nuclear EK delivers second Payload to Barto-PC

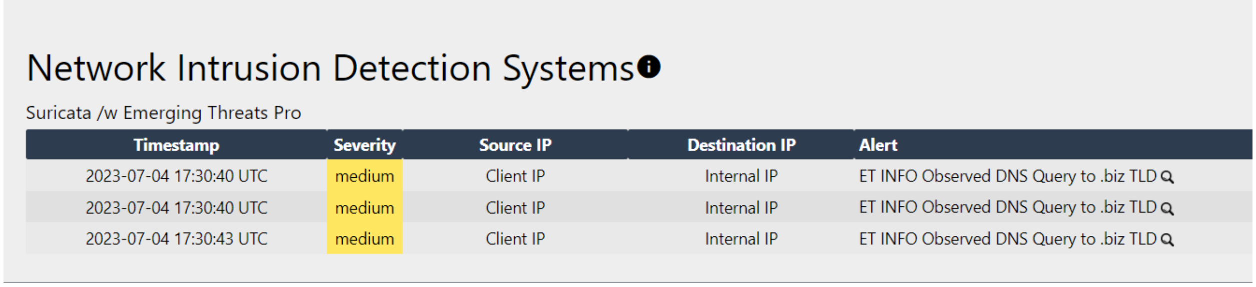
Unverified Facts:

IP(s) that generated EK traffic:
108.178.15.187, 173.194.39.3, 173.194.39.31 (?)
Host(s): wolfgangssteakhouse.co.kr

Verified Facts:
Laptop IP: **192.168.137.81**
Laptop Host name: **Barto-PC**
Laptop MAC address: **5c:f9:dd:6a:bd:22**
PCAP Duration: **609.514826 seconds (~10 minutes)**

EK landing page ‘http://f9wb0396aobdotyzddcwdtf.ilaclama.us/VQIXBEpVSwQ.html’

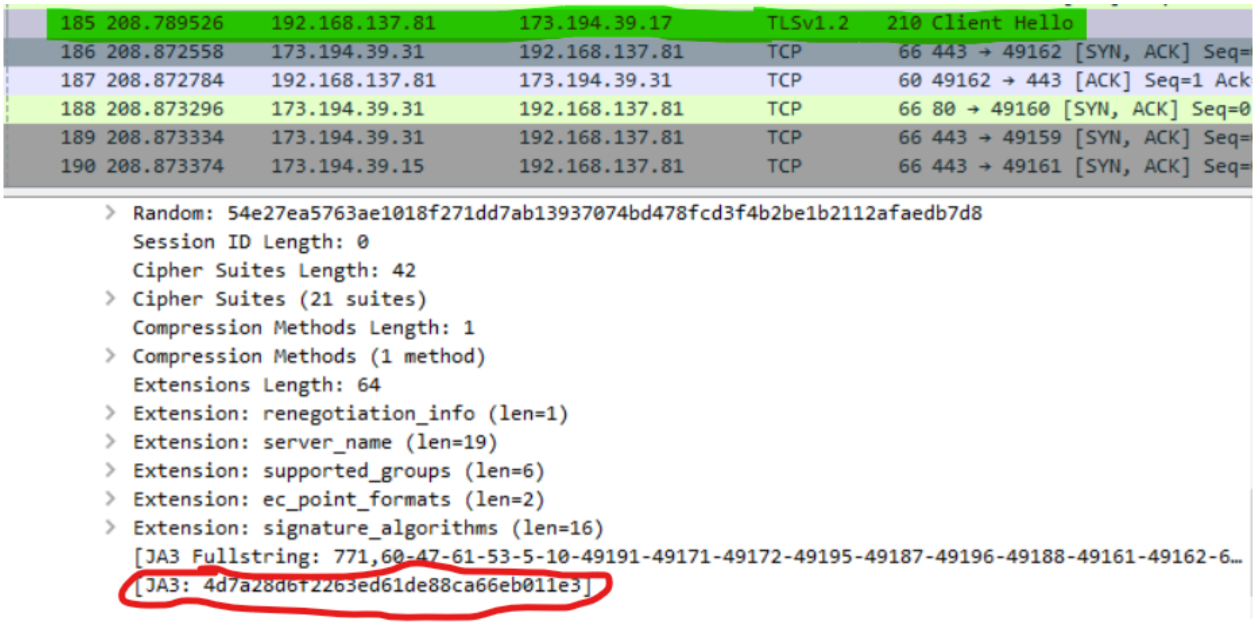
The ‘wolfgangssteakhouse.co.kr’ host alerted to a medium severity (security risk) threat when ran through urlquery.net - screenshot below.



Network Intrusion Detection Systems

Suricata /w Emerging Threats Pro

Timestamp	Severity	Source IP	Destination IP	Alert
2023-07-04 17:30:40 UTC	medium	Client IP	Internal IP	ET INFO Observed DNS Query to .biz TLD
2023-07-04 17:30:40 UTC	medium	Client IP	Internal IP	ET INFO Observed DNS Query to .biz TLD
2023-07-04 17:30:43 UTC	medium	Client IP	Internal IP	ET INFO Observed DNS Query to .biz TLD

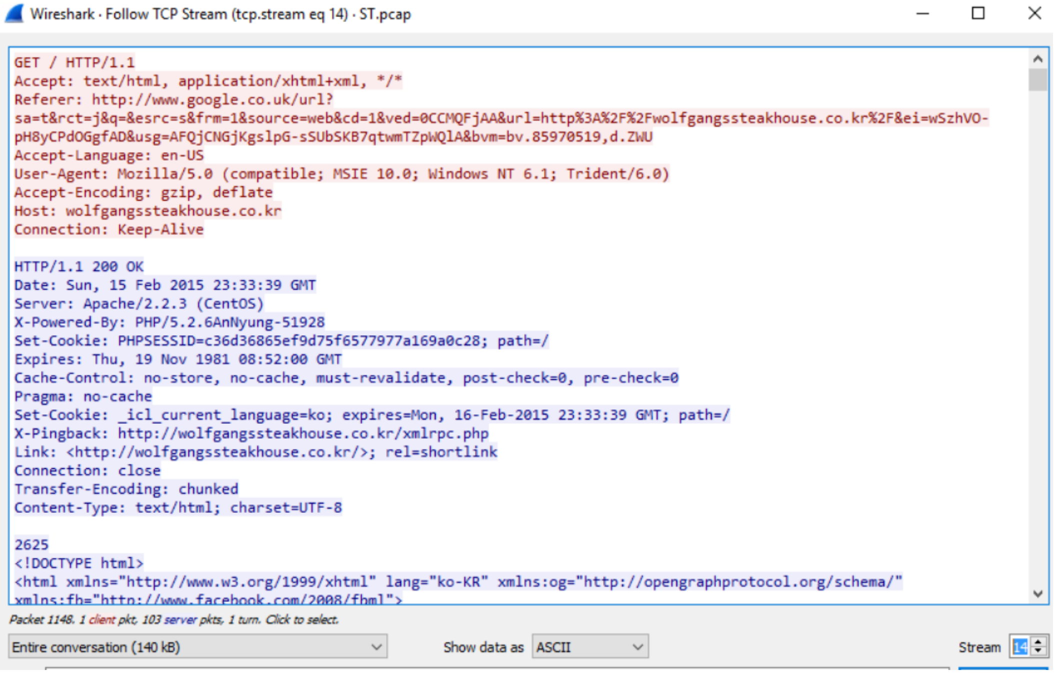


```
185 208.789526   192.168.137.81   173.194.39.17    TLSv1.2   210 Client Hello
186 208.872558   173.194.39.31    192.168.137.81   TCP        66 443 → 49162 [SYN, ACK] Seq=
187 208.872784   192.168.137.81   173.194.39.31    TCP        60 49162 → 443 [ACK] Seq=1 Ack
188 208.873296   173.194.39.31    192.168.137.81   TCP        66 80 → 49160 [SYN, ACK] Seq=0
189 208.873334   173.194.39.31    192.168.137.81   TCP        66 443 → 49159 [SYN, ACK] Seq=
190 208.873374   173.194.39.15    192.168.137.81   TCP        66 443 → 49161 [SYN, ACK] Seq=

    > Random: 54e27ea5763ae1018f271dd7ab13937074bd478fcd3f4b2be1b2112afaedb7d8
      Session ID Length: 0
      Cipher Suites Length: 42
    > Cipher Suites (21 suites)
      Compression Methods Length: 1
    > Compression Methods (1 method)
      Extensions Length: 64
    > Extension: renegotiation_info (len=1)
    > Extension: server_name (len=19)
    > Extension: supported_groups (len=6)
    > Extension: ec_point_formats (len=2)
    > Extension: signature_algorithms (len=16)
      [JA3 Fullstring: 771,60-47-61-53-5-10-49191-49171-49172-49195-49187-49196-49188-49161-49162-6…
      [JA3: 4d7a28d6f2263ed61de88ca66eb011e3]
```

Emotet Malware in TLS (?) JA3 = 4d7a28d6f2263ed61de88ca66eb011e3

TCP Stream 14 (below) - Shows the client/server | server/client traffic to the compromised site (wolfgangsteakhouse.co.kr)



```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://www.google.co.uk/url?
sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CCMQFjAA&url=http%3A%2F%2Fwolfgangssteakhouse.co.kr%2F&ei=wSzhVO-
pH8yCPdOGgfAD&usg=AFQjCNGjKgslpG-sSUbSKB7qtwmTZpWQlA&bvm=bv.85970519,d.ZWU
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; Trident/6.0)
Accept-Encoding: gzip, deflate
Host: wolfgangssteakhouse.co.kr
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sun, 15 Feb 2015 23:33:39 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.2.6AnNyung-51928
Set-Cookie: PHPSESSID=c36d36865ef9d75f6577977a169a0c28; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: _icl_current_language=ko; expires=Mon, 16-Feb-2015 23:33:39 GMT; path=/
X-Pingback: http://wolfgangssteakhouse.co.kr/xmlrpc.php
Link: <http://wolfgangssteakhouse.co.kr/>; rel=shortlink
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

2625
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" lang="ko-KR" xmlns:og="http://opengraphprotocol.org/schema/"
xmlns:fb="http://www.facebook.com/2008/fbml">
```

Packet 1148. 1 client pkt, 103 server pkts, 1 turn. Click to select.

Entire conversation (140 kB)

Show data as: ASCII

Stream: 14

References/Questions

What is LLMNR protocol: Link-Local Multicast Name Resolution; The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.

What is a '302 Cushioning Attack': The HTTP 302 cushioning attack is used by cybercriminals to take advantage of the 302 Found HTTP response status code to redirect the browser of the user to a new location, usually a malicious site.

https://www.malware-traffic-analysis.net/2014/12/10/index.html

https://www.zscaler.com/blogs/security-research/nuclear-exploit-kit-complete-infection-cycle

https://isc.sans.edu/diary/A+recent+decline+in+traffic+associated+with+Operation+Windigo/20065

https://www.malwarebytes.com/blog/threats/nuclear

https://www.zscaler.com/blogs/security-research/angler-exploit-kit-utilizing-302-cushioning-and-domain-shadowing

https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-280a

Task 3, Part 2:

An exe found on the infected computer:
9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d

Additional artifacts found in the infected computer’s browser cache:

- d9f266eb1dbd2bca408c837c3c4eaa39135417649ace63ba20d58c2df88ea19f
- c4b1c55a90877d0618c2dc8bad01b33f1d60f3613b3673bdb08465569bdb8236
- b4cb839573156364fc2a10a2d0a57cced697f076ce9fe4aa3604ada0b7a77523

~~Which of the suspicious files located by the forensics team contained an executable malware payload? Identify the malware by file hash and filename.~~
9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d
Filename: Win32 EXE

~~Based on the VirusTotal analysis reports, what malware or malware family was likely contained within that file?~~
Trojan/Win32.Glupteba

Returning to WireShark:

Open the TCP stream that contains the payload sent to the laptop.
Can you identify the XOR key used to obfuscate the payload and evade detection?

You can compose an email to Serper below. Your report should document the following:

Match all the hashes for these four new files to packets. One hash may be associated with more than one packet.

Include a copy of your final timeline from the previous report, and insert these four new entries into their correct positions within that larger timeline. Please put all your new insertions in a red type font so they pop.

Identify the XOR key used to obfuscate the payload, and the name of the payoad's malware family.

Finally, include a section with all supporting evidence and any external sources you used to reach your conclusions. If you have multiple hypotheses about the type of malware delivered in this attack, rank them.

XOR Key: KNcUKKaX

Timeline:

Packet #1148 (23:33:39.356557): Barto-PC first accesses compromised website (wolfgangssteakhouse.co.kr)

Packet #1837 (23:33:44.978479): Barto-PC is redirected from (wolfgangssteakhouse.co.kr) to gate (bnureb0up683ppcbgt1fz9g.isbul.info)

Packet #2104 (23:33:45.849418): Barto-PC (from bnureb0up683ppcbgt1fz9g.isbul.info) is sent to (http://zz1lb82z00y16gdow25fcxm.ilaclama.us/watch.php?fuhgi=MTIyMDU5ODkwNjhkMTQ5ODNkNDI2YWEzNWJjYjNjNTJ)

Packet #2521 (23:33:48.225258): Barto-PC redirected (from zz1lb82z00y16gdow25fcxm.ilaclama.us) to EK landing page (http://f9wb0396aobdotyzddcwdtf.ilaclama.us/VQlXBEpVSwQ.html)

Packet #2561 (23:33:49.033657): Barto-PC accesses EK landing page (VQlXBEpVSwQ.html)

^Hash for EK landing page: d9f266eb1dbd2bca408c837c3c4eaa39135417649ace63ba20d58c2df88ea19f

Packet #2617 (23:33:54.669953): Nuclear EK sends an SWF exploit to Barto-PC; SWF denotes an Adobe Flash File format that the EK is attempting to exploit

^Hash for EK Flash exploit: c4b1c55a90877d0618c2dc8bad01b33f1d60f3613b3673bdb08465569bdb8236

Packet #2634 (23:33:56.058965): Nuclear EK sends SilverLight exploit to Barto-PC; SilverLight is a Microsoft framework application that is now available as a plug-in, which the EK is attempting to exploit

^Hash for EK Silverlight exploit:
b4cb839573156364fc2a10a2d0a57cced697f076ce9fe4aa3604ada0b7a77523

Packet #2658 (23:33:57.418697): Nuclear EK delivers Payload to Barto-PC

^Hash for EK payload:
9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d

Packet #2798 (23:34:01.876444): Nuclear EK delivers second Payload to Barto-PC

Resources:

https://www.garykessler.net/library/file_sigs.html

https://isc.sans.edu/diary/Nuclear+EK+traffic+patterns+in+August+2015/20001

https://www.malware-traffic-analysis.net/2014/12/10/index.html

https://resources.infosecinstitute.com/topic/network-traffic-analysis-for-ir-content-deobfuscation/

https://www.malwarebytes.com/blog/detections/trojan-glupteba

https://unit42.paloaltonetworks.com/unit42-understanding-angler-exploit-kit-part-1-exploit-kit-fundamentals/

1 - My favorite part of Immediate Immersion was the assignment where we exploited the LFI vulnerability and cracked the webmaster’s hashed password - felt like a hacker! I really enjoyed the whole course, but I would say my least favorite part would be the first part of Task 3, mainly because I felt I struggled with this task the most.

2 - I would say I spent somewhere between 8-16 hours a week.

3 - Immediate Immersion definitely met my expectations as an introductory course; I thought it was going to be a little more difficult but definitely understand how hard it could be for those without any technical background (I have some experience with a degree from UT Austin in Management Information Systems).

4 - Immediate Immersion definitely increased my interest in cybersecurity/infosec; I was really unaware of how much could be done with Wireshark/those tools and have really never thought about the digital forensics/network analyst scene at all.

5 - Nothing comes to mind at the moment!