Charles Dulin
Krieger
IA473 Final
April 15th, 2025

IA473 Final

Executive Summary

At a local auto shop the owner was unable to login to his account that is affiliated with his position at the auto shop. The owner suspects he has been hacked and wants a forensic investigation. The network at the auto shop has just been setup and the contractors who built the network did not do any patching or hardening or anything else to prevent unauthorized access.This investigation will be used to determine what happened to the system. The results and finding show that suspicious malicious activity and hacking attempts were made on this network, with some being successful. The auto shop owner was locked out of his account and there are counts of privilege escalation techniques being done on the network.

Initial Evidence Processed

- I found e8220.dscd.akamaiedge.net inside of the DNS query of the pcap file networking_00007_20190306080000.pcap. The MD5 checksum of this pcap file is 4550d111ac94c2cd653491f7adccb8d4. e8220.dscd.akamaiedge.net could be linked to some spyware, this was found in 2019 by hybrid analysis sandbox. This e8220.dscd.akamaiedge.net posts files to a webserver and imports suspicious modules, sends traffic on a typical HTTP port but without HTTP header, uses a user agent but no browsers were launched. These are characteristics of spyware. The PEFile also has an unusual section name, meaning this could be linked to malware, an unusual section name means that this could be malware that is packed. Packed malware refers to malware that is compressed or encrypted making the malware harder to analyze and detect. This network packet is also some pcap file packets away from the biggest pcap files. The malware it is linked to is called Mnemosyne.sys.e8220.dscd.akamaiedge.net had a count of 6. Also in the file.mime_type I see 'application/ocsp-responseapplication/ocsp-response' which is a digitally signed message that confirms the revocation of specific certificates.
- I see e8220.dscd.akamaiedge.net again in networking_00008_20190306090000.pcap. MD5 checksum for networking_00008_20190306090000.pcap is 5d35914a4ed688e8f8c91c268c0fc5ba.
- I see an invalid server certification in the pcap file of networking_00011_20190306001200.pcap.

- Inside of networking_00017_20190306180000.pcap I see ET JA3 Hash - [Abuse.ch] Possible Adware. Security Onion is detecting possible adware inside of this pcap file. It comes from unknown traffic and the severity is low.
    - I also see 2.1.168.192.in-addr.arpa, 74.20.76.164.in-addr.arpa, 34.116.85.3.in-addr.arpa. All of these are used for reverse DNS lookup, which is also used for information gathering in hacking.
    - I also see 4 invalid server certificates inside of this pcap file.
- Inside of the networking_00019_20190306200000.pcap pcap file i see ET INFO RDP - Response To External Host, which is also linked to a ransomware, it is linked to the nokoyawa ransomware which the attackers were HTML smugglers.
    - I also see ET REMOTE_ACCESS MS Remote Desktop Administrator Login Request. This is used to remotely access the administrator role remotely on the desktop of a computer.
    - Inside the packet I see prod.normandy.prod.cloudops.mozgcp.net, which is flagged by Hybrid Analysis as found with malicious artifacts seen of a contacted host and in context of an input URL.
- Inside of the networking_00026_20190307030000.pcap I see multiple instances of attacks. I see ET WEB_SPECIFIC_APPS Apache Tomcat Possible CVE-2017-12617 JSP Upload Bypass Attempt, which is a web application attack attempt. I also see ET WEB_SERVER WebShell Generic - ASP File Uploaded, this was flagged as a trojan from Security Onion. I also see ET WEB_SERVER Possible SQL Injection (exec) in HTTP Request Body which is an Attempted Administrator Privilege Gain attack. I also see ET WEB_SERVER Observed FxCodeShell Web Shell Password which is flagged as another trojan that came through on the network.
    - I see 1 count for the web application attack and multiple counts for the other suspicious activity.
    - The source IPs i see associated with these attacks and suspicious activity are 116.226.70.132, 192.168.1.100, 162.125.34.6,
    - The destination IPs I see that are associated with this are 192.168.1.2 & 192.168.1.100.
    - Ports used are 50346, 443, 50322, 50315 & 56171.
-

Tools Used

- Security Onion - A free and open source Linux distribution designed for network security monitoring, log management and threat hunting. It also acts as an intrusion detection system and enterprise security monitoring. It also simplifies deployment and management of network security monitoring infrastructure. Enabling organizations to detect, analyze and respond to security threats.

Results and Findings for Network evidence

- Inside of the earlier pcap files I see multiple instances of suspicious activity. In almost all of the pcap files I saw multiple instances of potential corporate policy violations and also many failed server certificate validations on each pcap file.
- Inside of the networking_00007_20190306080000.pcap file I saw e8220.dscd.akamaiedge.net, now e8220.dscd.akamaiedge.net is linked to a spyware found by a Hybrid Analysis box. The behavior that e8220.dscd.akamaiedge.net has of spyware is posting files to a webserver and importing suspicious modules, sending traffic on a typical HTTP port but without HTTP header and using a user agent but no browsers were launched. The PE sections also had unusual section names which happens when a malware is packed. Malware being packed means that the file is compressed and harder to analyze and debug.
    - This seems as if this is when the gathering information stage of the hacking cycle started for these malicious hackers.
    - The hash for networking_00007_20190306080000.pcap file is ‘4550d111ac94c2cd653491f7adccb8d4’.
- I saw multiple instances of e8220.dscd.akamaiedge.net, which could be linked to a spyware found in 2019, in most of the pcap files before the first attack attempts started.
    - Seems as if the auto shop was being targeted hours before the first attack attempt.
    - The attackers seemed to be gathering information on the auto shop to see if they were vulnerable to attacks.
- I see an invalid server certification in most of the pcap files.
    - This means that there was a problem with the SSL/TLS certificate used to secure a website or a server connection.
- I saw an instance of adware inside of the pcap file ‘networking_00017_20190306180000.pcap’.
    - The adware was flagged by Security Onion as ‘ET JA3 Hash - [Abuse.ch] Possible Adware.’ but the severity was low for this type of adware.
    - I also see instances of reverse DNS lookup. They were flagged by Security Onion as ‘2.1.168.192.in-addr.arpa, 74.20.76.164.in-addr.arpa, 34.116.85.3.in-addr.arpa.’
    - Reverse DNS lookup is used in the information gathering stage of the hacking cycle before they implement an attack.
- Inside of networking_00019_20190306200000.pcap pcap file I see ET INFO RDP - Response To External Host, which is also linked to ransomware.
    - It is linked to the nokoyawa ransomware which the attackers were HTML smugglers. This can be looked up.

    - I also see ET REMOTE_ACCESS MS Remote Desktop Administrator Login Request. This is used to remotely access the administrator role remotely on the desktop of a computer. This would most likely not be used by an auto shop.
    - The hash for networking_00019_20190306200000.pcap pcap file is ‘c9a279b545c8014a5dc46b95d3431e85’.

-
- Inside of the networking_00026_20190307030000.pcap file I see different attempted and some successful attacks on the network. I see the flag ET WEB_SPECIFIC_APPS Apache Tomcat Possible CVE-2017-12617 JSP Upload Bypass Attempt. This is an attempt at a web application attack.
    - I also see ET WEB_SERVER WebShell Generic - ASP File Uploaded. This was flagged by Security Onion as a trojan that was uploaded to the network.
    - I also sawa another trojan aws flagged by entering the network, I also see ET WEB_SERVER Observed FxCodeShell Web Shell Password was the flag for it.
    - I also saw the flag ET WEB_SERVER Possible SQL Injection (exec) in HTTP Request Body, this is an attempt at privilege escalation within the network.
    - This seems as if this was when the attack phase started for the hackers in this network.
    - I see 1 count for the web application attack and multiple counts for the other suspicious activity. This means that the web application attack was executed at least 1 time during the 26th hour after getting the network packets, and multiple execution of other forms of attacks like uploading a trojan horse (malicious executable files) and other forms of SQL injection to perform privilege escalation techniques.
    - The source IPs I see associated with these attacks and suspicious activity are 116.226.70.132, 192.168.1.100, 162.125.34.6. This means that these are the IPs that are the IP addresses that initiated the network request or communication during this hour on the network. Most likely one of these IPs is associated or is the hacker attacking the network of the auto shop.
    - The destination IPs I see that are associated with this are 192.168.1.2 & 192.168.1.100. This means that these are the IPs of the recipient of the network traffic, I suspect the auto shop's IP is 192.168.1.100 since the IP shows up in the destination and source IPs. And also the IP of the auto shop would most likely have to send and receive network traffic in order to be hacked.

  - Ports used are 50346, 443, 50322, 50315 & 56171. These were the ports used to send and receive information over the network during the hour of the privilege escalation attempt, the web application attack and the trojan uploads onto the network.
  - The hash for networking_00026_20190307030000.pcap file is ‘000d7357a6a54de989c1caecfce2b473’.
- I believe that the above results and findings show very strong evidence that a hacking attempt and a hack has occurred. It seems as if the attacks were well thought out and planned and took about 19 hours to implement after starting to gather information on the auto shop. I caught the gathering information phase in pcap file 7, which is hour 7 after grabbing the network traffic. And I also see when malicious attacks started, which was hour 26, pcap file 26, after grabbing the network traffic. I believe that the attackers could have had a successful attempt at privilege escalation and that could have locked the auto shop owner out of his account if any changes were made , after gaining access and successful attempts at privilege escalation.