FORENSIC REPORT

Incident Response to May 29, 2018 Intrusion at Acme Sandwich Company

EXECUTIVE SUMMARY

A forensic analysis of 3 systems owned by the Acme Sandwich Company was conducted by J.M. Bhavan, H.N. Man & V.B. Shun Security Consultants At-Large. The results showed that Acme's Supersecret sandwich recipe was stolen on May 29, 2018 by an unidentified attacker. The attacker was able to gain access to the intellectual property because the network did not have adequate firewall or intrusion prevention system, and a system on the network did not have the most up-to-date Windows security updates. Configuring firewalls, installing intrusion detection systems and anti-virus software, as well as strengthening passwords and encryption standards could prevent future intrusions like this incident from occurring.

Background:

On May 29, Acme Sandwich Company (Acme) requested the services of J.M. Bhavan, H.N. Man & V.B. Shun Security Consultants At-Large in response to a potential network intrusion that may have occurred and threatened the company's super-secret sandwich recipe. Acme provided three forensic images of machines on their network, packet captures and snapshots of the volatile memory of each machine.

A forensic analysis was conducted, which focused on the three machines and network traffic to and from those machines. The router which connected the machines to the internet was beyond the scope of this forensic investigation; however, Acme made their staff readily available to answer incident related enquiries.

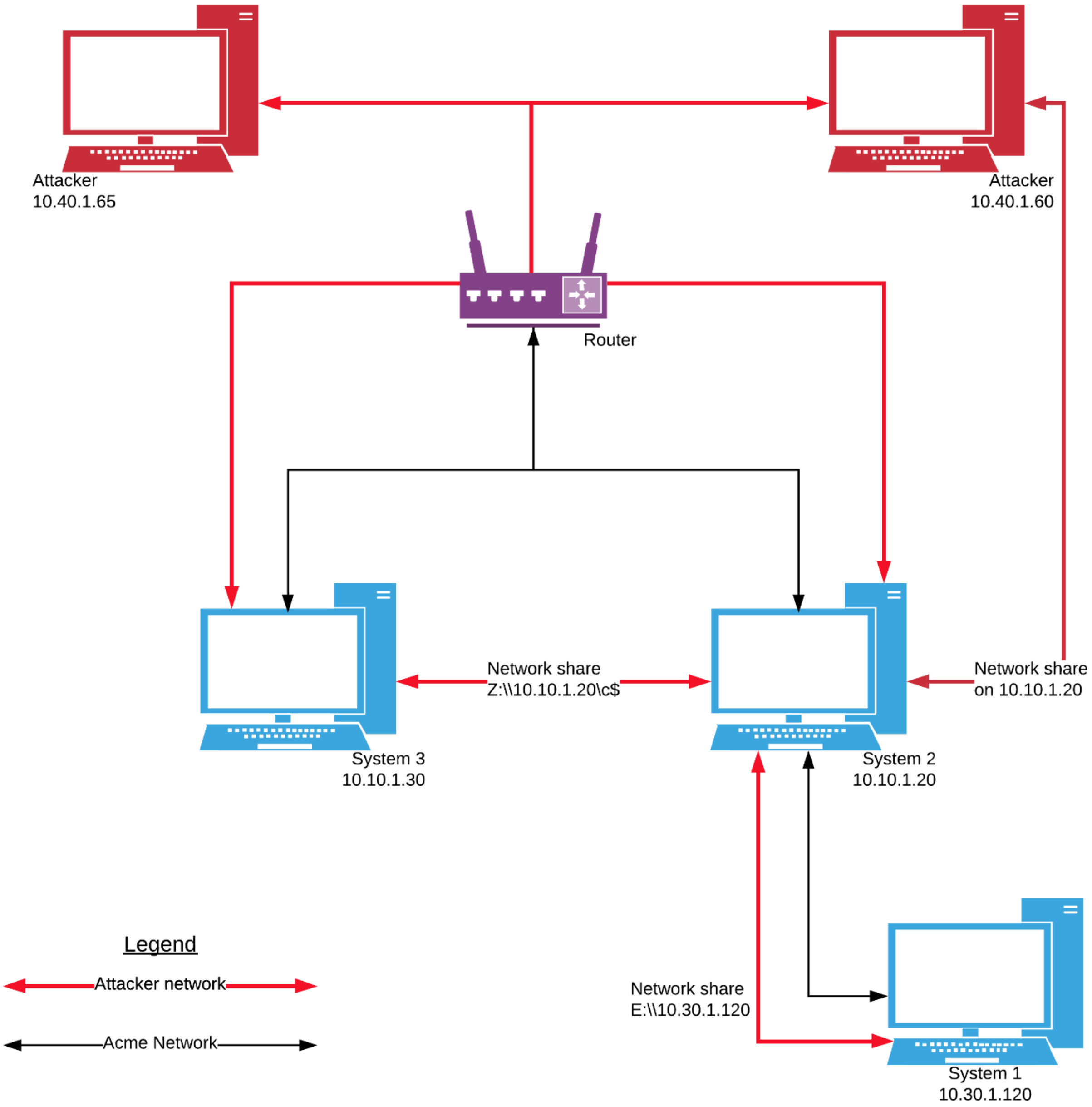
J.M. Bhavan & Associates objectives were to determine if the super-secret sandwich recipe had indeed been stolen, develop a timeline for the attack, illustrate a network topology of the attack surface and provide recommendations to prevent future intrusions.

The following tools were used to process and analyze the data:

- Autopsy was used to process the forensic images
- Volatility plug-ins were used to review the volatile memory.
- Wireshark and Network Miner were used to review the packets of data transferred between machines and enumerate the attackers.
- FTK Imager was used to look at the file systems and mount the images on the analysts' machines.
- Sysinternals Suite was used to review Windows Registry and identify the persistence mechanisms established by the attacker(s).
- Plaso log2timeline was used to verify the timeline built from artifacts with Windows event logs

What follows is a forensic report containing the results of the analysis.

Acme Network Topology:



Event timeline:

0128	29 MAY	Port scanning begins against System 3 from 10.40.1.65
0131	29 MAY	Attacker established connection to System 3
0134	29 MAY	Persistence mechanism established on System 3
0137	29 MAY	attackTools folder created on System 3 and nc.exe uploaded
0143	29 MAY	Attacker discovers System 2 on network
0205	29 MAY	Network share created between System 3 and System 2
0220	29 MAY	Nc.exe positioned onto System 2
0223	29 MAY	Batfile.bat executed and Netcat session started on System 2
0239	29 MAY	Attacker discovers 10.30.1.0/24 subnet
0320	29 MAY	NMAP folder created on System 2
0334	29 MAY	Port scanning begins against System 1 from System 2
0335	29 MAY	Network share created between System 2 and System 1
0336	29 MAY	Attacker logs on to network share as ringo
0337	29 MAY	Super-Secret Sandwich recipe is stolen using \`type\` command

Narrative of Event:

The first evidence that Attacker 1 (10.40.1.65) began port scanning System 3 (10.10.1.30) was at 01:28:46 on 29 MAY. The attacker began with port 22 and scanned hundreds of ports over a duration of approximately 3 minutes[1].

At 01:31:18, Attacker 1 used a connection over port 445 to establish a session on port 1038 of System 3 which can be seen in the Syn, Syn-Ack, Ack, sequence of packets no. 426-428[2] and 560-562[3], respectively. Indeed, the System 3 memory contains evidence of a TCP connection on port 1038 with Attacker 1 on port 18815 which is identical to the packet capture[4] [5]. Network miner artifacts infer that Attacker 1 used a Linux operating system and the Metasploit Framework to exploit System 3[6] [7].

The attacker established a persistence mechanism at 01:34:06 by either installing or writing a Visual Basic script file titled GgkRkJQLd.vbs and modifying the HKLM registry to run it[8]. 49 seconds later the attacker created a directory titled attackTools. Next, s/he uploaded an executable file titled, nc.exe (Netcat) into attackTools. This occurred at 01:37:23 [9] (Netcat is an application that allows an attacker to operate a system remotely).

[1] Artifact No.1: View packet No. 10 of the System 3 Packet capture

[2] Artifact No.2: View packet No. 426-428 of the System 3 Packet capture

[3] Artifact No. 3: View packet No. 560-562 of the System 3 Packet capture

[4] Artifact No. 4: Run Volatility.exe plug-in: connscan, input file:memory_system3.raw, profile=WinXPSP2x86

[5] Artifact No. 5: Run Volatility.exe plug-in: connections, input file:memory_system3.raw, profile=WinXPSP2x86

[6] Artifact No. 6: Use Network Miner to view System 2 pcap, the NTLM Username under 10.40.1.65 Host details is "Metasploit"

[7] Artifact No.7: Use Network Miner to view System 3 pcap, the OS under 10.40.1.65 is listed as "Other"

[8] Artifact No. 8: Use Plaso log2timeline to view windows event logs for System 3 at 01:34:06. See the Creation Time for GgkRkJQLd.vbs and the modification to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

[9] Artifact No. 9: In Autopsy, use keyword search "nc.exe" against system3.E01 shows attackTools/nc.exe was created at 01:37:23

The attacker became aware of System 2 by 01:43:11. Packet number 1660 of system3.pcap shows s/he typed “ping 10.10.1.20” into the reverse shell at this time[10].

By 02:05:00 the attacker had created a shared file between System 3 and System 2. and moved nc.exe from System 3 onto System 2. Then, at 02:20:12, the attacker moved nc.exe again. This time into WINDOWS\system32 folder on System 2[11].

Next, PsExec was used to run badfile.bat - a script the attacker had written and placed on system 2. This occurred at 02:23:59 (PsExec is part of the SysInternals Suite that allows administrators to start processes and run executable files on a system from remote locations). The Badfile.bat script used Netcat to open a command prompt on port 56. Now the attacker could send commands to System 2[12] [13] [14]. At this point, the attacker began to operate the shell from a different ip address – 10.40.1.60 and established a network share with 10.10.1.20. Network Miner shows this ip address belonged to a Windows XP host[15]. Although this could mean the attack was coordinated amongst two different parties, it is more likely the attacker changed operating systems because it made the network pivot easier to accomplish.

The attacker typed ipconfig into the command line at 02:39:00 and discovered a separate network interface configured to another subnet with IP 10.30.1.20[16].

Nmap is a tool used to scan a network and identify the other computers that are on it. Starting at 03:20:29, the attacker used Nmap to find System 1, which contained the super-secret recipe[17] [18]. Server Message Block (SMB) traffic began at 03:35:10, indicating the attacker created a network share between System 1 and 2, and between 10.40.1.60 and System 2[19]. Shortly thereafter, at 03:36:35, the attacker logged on to the shared drive as ringo, indicating s/he had been able to obtain the passwords of both jon and ringo at some point prior. The passwords could have been obtained during the attack by accessing the NTLM user hashes from System 3 and decrypting them, or through a separate phishing attack. Regardless, the super-secret recipe for Acme was in an unencrypted text file on the desktop of user:

[10] Artifact No. 10: Use Wireshark to view system3.pcap packet no. 1660. Follow TCP stream.

[11] Artifact No. 11: Use Network Miner to view system3 pcap. Under the Files tab, see where nc.exe was added to \\10.10.1.20\C$ and then moved again to WINDOWS/system32.

[12] Artifact No. 12: Use Autopsy to do keyword search for “psexec” in system2.EO1. See that psexec called badfile.bat at 02:23:59.

[13] Artifact No. 13: Use Autopsy to do keyword search for “badfile.bat” in system2.EO1. See that badfile.bat contains script “c:\windows\system32\nc.exe -e cmd.exe -Lp 56”

[14] Artifact No. 14: Use Plaso log2timeline to view windows event logs for System 2 starting at 02:23:59. See that wsock.dll was called, followed by the nc.exe prefetch file.

[15] Artifact No. 15: Use Network Miner to view System 2 memory, the OS under 10.40.1.60 is listed by Ettercap as “Windows XP Pro”

[16] Artifact No. 16: Use Wireshark to view System 2 pcap. Type “frame contains “ipconfig” “ and see where attacker discovered subnet 10.30.1.0/24.

[17] Artifact No. 17: Use Autopsy to do keyword search for “nmap” in system1.EO1. Notice that nmap-6.00 Created Time is 03:20:29 UTC.

[18] Artifact No. 18: Use Wireshark to open System 1 pcap. Notice the port scanning of 10.30.1.120 that began with packet 4940 at 03:34:10.

[19] Artifact No. 19: Use Wireshark to open System 1 pcap. Notice a Syn, Syn-Ack, Ack TCP handshake occur between 10.30.1.20 and 10.30.1.120, starting at packet no. 7034. Followed by SMB traffic, indicating a network share was created between System 1 and 2.

ringo[20]. At 03:37:50 the attacker was able to navigate to the document and read it in the command line by typing, "type Supersecret Recipe.txt," at which point s/he exclaimed "GOT IT!"[21]

Areas of Improvement:

As part of the scope of contract, it was important to provide Acme corporation's lovable staff with recommended actions that can be taken to prevent future intrusions. What follows is a list of areas of improvement that would increase Acme's ability to keep their secret sandwich recipes safe in the future:

- Activate and configure a network firewall on the router.
- Disallow ICMP traffic on the router by default.
- Install and configure a Network-based intrusion prevent system (IPS), as well as host-based IPS.
- Install an Anti-virus on hosts within the network.
- Update the company's password policy to ensure compliance with stronger passwords that are in accordance with the National Institute of Standards and Technology (NIST).
- Use encryption to protect important files, such as super-secret recipes.
- Update existing Windows XP systems to the newest Service Pack and, where possible upgrade systems to the newest versions of operating systems.
- Destroy the persistence mechanism the attacker created on System 3 by using Task Manager to end the process responsible for running the GgkRkJQLd.vbs.

[20] Artifact No. 20: Use Autopsy or FTK imager to view "system 1.EO1\Documents and Settings\ringo\Desktop\SuperSecret Recipe.txt" in the image system1.EO1.

[21] Artifact No. 21: Use Wireshark to the follow TCP stream starting at packet 45262. See when the attacker accesses the shared drive using ringo's credentials and reads the secret recipe by typing the command, "type Supersecret Recipe.txt."