Overview

The 2021 Codebreaker Challenge consists of a series of tasks that are worth a varying amount of points based upon their difficulty. Schools will be ranked according to the total number of points accumulated by their students. Solutions may be submitted at any time for the duration of the Challenge.

While not required, we recommend that you solve tasks in order, since they flow with the storyline. Later tasks may rely on artifacts / inputs from earlier tasks.

Each task in this year's challenge will require a range of skills. We need you to call upon all of your technical expertise, your intuition, and your common sense.

Good luck. We hope you enjoy the challenge!

Background

DISCLAIMER - The following is a FICTITIOUS story meant for providing realistic context for the Codebreaker Challenge and is not tied in any way to actual events.

The Internet is home to many different cyber actors. To better prepare for and defend against these actors, NSA routinely investigates foreign cyber actors and their activities. During one such investigation, a new IP address was identified to be part of an unknown actor's infrastructure. NSA believes it is a listening post (https://wiki.cbc.cybersecurity.nmt.edu/doku.php?id=listeningpost) (LP).

Note: All IP addresses have been anonymized.

Task 0 - (Community of Practice, Discord Server) Points: 1

As a participant in the Codebreaker Challenge, you are invited to join New Mexico Tech’s Codebreaker Challenge Community of Practice!

We're piloting this community to provide Codebreaker Challenge participants and people interested in cybersecurity a place to talk about Codebreaker, cybersecurity, and other related topics. You should have received an invitation link to the Community Discord server in your confirmation email.

(https://nsa-codebreaker.org/sidecar)

To complete this task, join the Discord server. Once there, type `!task0` in the chat. Follow the prompts, and paste the answer the bot gives you below.

Note: You must provide the bot with the email you used to register for the Challenge.

Task Completed at Sat, 11 Sep 2021 01:59:23 GMT:

Welcome! Feel free to ask questions and discuss general tips and strategy with the community!

Task 1 - (Network Forensics, Command Line) Points: 25

The NSA Cybersecurity Collaboration Center has a mission to prevent and eradicate threats to the US Defense Industrial Base (DIB). Based on information sharing agreements with several DIB companies, we need to determine if any of those companies are communicating with the actor's infrastructure.

You have been provided a capture of data en route to the listening post as well as a list of DIB company IP ranges. Identify any IPs associated with the DIB that have communicated with the LP.

Downloads:

- Network traffic heading to the LP (capture.pcap) (/files/task1/capture.pcap?1631325573)
- DIB IP address ranges (ip_ranges.txt) (/files/task1/ip_ranges.txt?1631325573)

Enter the IP addresses associated with the DIB that have communicated with the LP, one per line

Submit

Task 2 - (Log Analysis) Points: 50

NSA notified FBI, which notified the potentially-compromised DIB Companies. The companies reported the compromise to the Defense Cyber Crime Center (DC3). One of them, Online Operations and Production Services (OOPS) requested FBI assistance. At the request of the FBI, we've agreed to partner with them in order to continue the investigation and understand the compromise.

OOPS is a cloud containerization provider that acts as a one-stop shop for hosting and launching all sorts of containers -- rkt, Docker, Hyper-V, and more. They have provided us with logs from their network (https://nsa-codebreaker.org/sidecar)

proxy and domain controller that coincide with the time that their traffic to the cyber actor's listening post was captured.

Identify the logon ID of the user session that communicated with the malicious LP (i.e.: on the machine that sent the beacon *and* active at the time the beacon was sent).

Downloads:

- Subnet associated with OOPS (oops_subnet.txt) (/files/task2/oops_subnet.txt?1631325573)
- Network proxy logs from Bluecoat server (proxy.log) (/files/task2/proxy.log?1631325573)
- Login data from domain controller (logins.json) (/files/task2/logins.json?1631325573)

Enter the logon ID of the user session that communicated with the malicious LP

Submit

Task 3 - (Email Analysis) Points: 150

With the provided information, OOPS was quickly able to identify the employee associated with the account. During the incident response interview, the user mentioned that they would have been checking email around the time that the communication occurred. They don't remember anything particularly weird from earlier, but it was a few weeks back, so they're not sure. OOPS has provided a subset of the user's inbox from the day of the communication.

Identify the message ID of the malicious email and the targeted server.

Downloads:

- User's emails (emails.zip) (/files/task3/emails.zip?1631325573)

Enter the message ID of the malicious email (format: <111111111111.22222.33333333333333333333@aaa.bbb>)

Enter the domain name of the server that the malicious payload sends a POST request to

Submit

Task 4 - (PowerShell, Registry Analysis) Points: 150

A number of OOPS employees fell victim to the same attack, and we need to figure out what's been compromised! Examine the malware more closely to understand what it's doing. Then, use these artifacts to determine which account on the OOPS network has been compromised.

Downloads:

- OOPS forensic artifacts (artifacts.zip) (/files/task4/artifacts.zip?1631325573)

Enter the name of the machine the attackers can now access

Enter the username the attackers can use to access that machine

Submit

Task 5 - (Docker Analysis) Points: 300

A forensic analysis of the server you identified reveals suspicious logons shortly after the malicious emails were sent. Looks like the actor moved deeper into OOPS' network. Yikes.

The server in question maintains OOPS' Docker image registry, which is populated with images created by OOPS clients. The images are all still there (phew!), but one of them has a recent modification date: an image created by the Prevention of Adversarial Network Intrusions Conglomerate (PANIC).

Due to the nature of PANIC's work, they have a close partnership with the FBI. They've also long been a target of both government and corporate espionage, and they invest heavily in security measures to prevent access to their proprietary information and source code.

The FBI, having previously worked with PANIC, have taken the lead in contacting them. The FBI notified PANIC of the potential compromise and reminded them to make a report to DC3. During conversations with PANIC, the FBI learned that the image in question is part of their nightly build and test pipeline. PANIC reported that nightly build and regression tests had been taking longer than usual, but they assumed it was due to resourcing constraints on OOPS' end. PANIC consented to OOPS providing FBI with a copy of the Docker image in question.

Analyze the provided Docker image and identify the actor's techniques.

Downloads:

- PANIC Nightly Build + Test Docker Image (image.tar) (/files/task5/image.tar?1631325573)

(https://nsa-codebreaker.org/sidecar)

Enter the email of the PANIC employee who maintains the image

Enter the URL of the repository cloned when this image runs

Enter the full path to the malicious file present in the image

Submit

Task 6 - (Reverse Engineering) Points: 500

Now that we've found a malicious artifact, the next step is to understand what it's doing. Identify some characteristics of the communications between the malicious artifact and the LP.

Enter the IP of the LP that the malicious artifact sends data to

Enter the public key of the LP (hex encoded)

Enter the version number reported by the malware

Submit

Solo Challenges Below

Solo challenges must be solved without any guidance, assistance, or help from others. In addition, you should not help others on solo challenges during the competition.

We hope you enjoy the most difficult portions of Codebreaker 2021. Good luck!

Task 7 - (Protocol Analysis) *Solo Challenge* Points: 500

(https://nsa-codebreaker.org/sidecar)

With the information provided, PANIC worked with OOPS to revert their Docker image to a build prior to the compromise. Both companies are implementing additional checks to prevent a similar attack in the future.

Meanwhile, NSA's Cybersecurity Collaboration Center is working with DC3 to put together a Cybersecurity Advisory (CSA) for the rest of the DIB. DC3 has requested additional details about the techniques, tools, and targets of the cyber actor.

To get a better understanding of the techniques being used, we need to be able to connect to the listening post. Using the knowledge and material from previous tasks, analyze the protocol clients use to communicate with the LP. Our analysts believe the protocol includes an initial crypt negotiation followed by a series of client-generated requests, which the LP responds to. Provide the plaintext a client would send to initialize a new session with the provided UUID.

Downloads:

- Victim ID to use in initialization message (victim_id) (/files/task7/victim_id?1631325573)

Provide a hex dump of the plaintext packet (not frame) contents a client would send to initialize a session with the provided UUID

Submit

Task 8 - (Cryptanalysis) *Solo Challenge* — Points: 3000

Knowing the contents we'd send to initialize a new session is good progress. The next step is to uncover additional details about the protocol.

We suspect the Docker malware was specifically tailored to PANIC's image and written exclusively to steal their source code. Given that, it seems likely that the malware only contains a subset of the communications protocol supported by the LP. Our network capture does appear to have communications from other malware variants. If we could decrypt those communications, then we could analyze the underlying plaintext to recover additional details about the protocol.

As a reminder, our analysts believe the protocol includes an initial crypt negotiation followed by a series of client-generated requests, which the LP responds to.

Decrypt the other sessions captured in the PCAP. Provide the UUIDs of each of the clients associated with the DIB that registered with the LP.

Provide the UUIDs of each of the clients associated with the DIB that registered with the LP, one per line

(https://nsa-codebreaker.org/sidecar)

Submit

Infra - (Infrastructure) Points: 0

Now that we know how to connect to the listening post, we're ready to interact with it.

This is serious. We need to be stealthy, so that we don't tip off the actor that we're on to them.

Click the button below when you're ready to connect. That'll spin up some stuff to let you connect in a stealthy way. The stuff goes away three hours or so, so work quickly. We can always connect again later, but there's a bit of a cooling off period, to avoid suspicion on their end.

No submissions are allowed: You must complete all of the following tasks first:

- Task 1
- Task 2
- Task 3
- Task 4
- Task 5
- Task 6
- Task 7
- Task 8

Submit

Task 9 - (Protocol Analysis, Software Development) *Solo Challenge* Points: 3500

Now that we're able to register, let's send some commands! Use the knowledge and material from previous tasks to identify other clients that have registered with the LP.

Enter the other UUIDs that have registered with the LP, one per line

Submit

(https://nsa-codebreaker.org/sidecar)

Task 10 - (Protocol Analysis, Software Development, Exploit Development) *Solo Challenge*

Points: 5000

NSA worked with FBI to notify all of the identified victims, who in turn notified DC3. Nicely done.

The final task is to uncover additional information about the actor's infrastructure.

Gain access to the LP. Provide the IP and port that the `psuser` account has transmitted data to. What lies behind the listening post?

Enter the next IP in the actor's infrastructure chain

Enter the port the LP connects to on that IP

Submit