THE PACKET

SPRING

JANUARY 2021

IN THIS ISSUE

ART BY @TIMA-MIROSHNICHENKO

THE UNIVERSITY OF ARIZONA

LETTER FROM THE EDITOR

A MESSAGE FROM PROFESSOR MICHAEL GALDE

--- BEGIN MESSAGE ---

Welcome to the **<u>JANUARY</u>** issue of **"The PACKET"** produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde, and as you can see, I have made a few changes to the look and feel of this digital product. The look may be different, but the mission is the same. This will serve as a learning tool for current, previous and future students and will inform you of what is going on in the world of cyber security. With this new year we leave behind 2020 and forge ahead to 2021 and in this new year it will be another year of hostile cyber threats and a constant change to our digital world. Me and the other professors at the University of Arizona will try and prepare you for everything that you will encounter but it is likely you will find something none of us have ever encountered before. To combat this, we will arm you with the tools and knowledge to identify, analyze and finally mitigate the threat. 2020 showed us a world where a vast majority of the population worked from home. This experiment will likely continue for a portion of 2021 and the digital consequences for industries and organization who failed to prepare will be forced to make changes as they struggle to adapt. Each student will be a part of that adaption technique and it will be up to you to guide, and in many ways, lead the digital future. Welcome to the year 2021, may it bring you great joy.

--- END MESSAGE ---

HACKS OF THE MONTH

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

MICROSOFT IDENTIFIES ADROZEK MALWARE FAMILY

Microsoft Identified malware that injects ads into the browser. This is not a new technique but what is new; however, is that this infects multiple browsers. This malware also maintains persistence and exfiltrates website credentials causing even more additional harm to infected users. The Adrozek malware is installed on devices through drive-by download. Attackers relied heavily on polymorphism, which allows attackers to churn huge volumes of samples as well as to evade detection.

RANSOMWARE INCIDENT “IMMATERIAL” TO COMPANY

Total System Services Inc. (TSYS) is the third-largest third-party payment processor for financial institutions in North America, and a major processor in Europe. On December 8, the cybercriminal gang responsible for deploying the Conti “Ryuk” ransomware strain and published more than 10 gigabytes of data that it claimed to have removed from TSYS’s networks. the company says the malware did not jeopardize card data, and that the incident was limited to administrative areas of its business.

HACKS OF THE MONTH

REVIEWING THE LAST 30 DAYS OF REPORTED HACKS

ACCOUNT HIJACKING SITE OGUSERS HACKED… AGAIN

The OGUsers forum and database which is used to sell compromised accounts has been itself compromised. The hack was acknowledged by the forum's current administrator, who assured members that their passwords were protected with a password obfuscation technology that was extremely difficult to crack. The hackers have told users that their profiles and private messages could be removed from an impending database leak by paying between $50 and $100. The hacker was apparently a banned member.

iPHONE ZERO-CLICK WI-FI EXPLOIT FIXED

A memory corruption bug in the iOS kernel gave attackers remote access to the entire device over Wi-Fi with no user interaction was fixed after an iOS update. It worked by exploiting a buffer overflow bug in a driver for AWDL, an Apple mesh networking protocol that makes things like Airdrop work. The researcher said they have no evidence the vulnerability was ever exploited in the wild, although he noted that at least one exploit seller was aware of the critical bug in May.

DEPARTMENT OF DEFENSE

CYBER SCHOLARSHIP

INFORMATIONAL MEETING

VIEW THE INFO MEETING AND LEARN HOW YOU CAN APPLY FOR THE PROGRAM BY VISITING HERE!

- Full cost of tuition and ALL fees provided for 2020-2021 academic year.
- A $25,000 (undergraduate) or $30,000 (graduate) stipend for room and board.
- Covering the cost of all required books (up to $1,250 a year).
- A laptop (up to $1,500).

BASIC REQUIREMENTS

- Minimum cumulative GPA of 3.2 (undergraduate) or 3.5 (graduate).
- Must be entering junior or senior year or a graduate program in Fall 2020.
- Must be a U.S. Citizen.
- Agree to work for the DoD as a civilian for one year for each year of scholarship received.

FACEBOOK SAYS HACKERS BACKED BY VIETNAM'S GOVERNMENT ARE LINKED TO IT FIRM

Facebook said it has linked an advanced hacking group widely believed to be sponsored by the government of Vietnam to what's purported to be a legitimate IT company in that country. The group goes under the monikers APT32 and OceanLotus. Facebook identified Vietnamese IT firm CyberOne Group as being linked to OceanLotus. The group lists an address in Ho Chi Minh city.

The naming of CyberOne Group isn't the first-time researchers have publicly linked a government-backed hacking group to real-world organizations. In 2013, researchers from Mandiant, now a part of security firm FireEye, identified a 12-story office tower in Shanghai, China, as the nerve center for Comment Crew, a hacking group that was responsible for hacks on more than 140 organizations over the previous seven years. The building was the headquarters for the People's Liberation Army Unit 61398. And in 2018, FireEye said that potentially life-threatening malware that tampered with the safety mechanisms of an industrial facility in the Middle East was developed at a research lab in Russia.

LASER-BASED HACKING FROM AFAR GOES BEYOND AMAZON ALEXA

Academic researchers broadened their research to show how light can be used to manipulate a wide range of digital assistants, including Amazon Echo 3 and sensing systems found in medical devices, autonomous vehicles, industrial systems and even space systems. The researchers also delved into how the ecosystem of devices connected to voice-activated assistants such as smart-locks, home switches and even cars also fail under common security vulnerabilities that can make these attacks even more dangerous. The paper shows how using a digital assistant as the gateway can allow attackers to take control of other devices in the home. The PhD researcher Sara Rampazzi presented her and her teams' research at Blackhat Europe 2020.

INDUSTRIAL, FACTORY AND MEDICAL GEAR REMAIN LARGELY UNPATCHED WHEN IT COMES TO THE URGENT/11 AND CDPWN GROUPS OF VULNERABILITIES.

According to researchers at Armis, a whopping 97 percent of the OT devices impacted by URGENT/11 have not been patched, despite fixes being delivered in 2019. And 80 percent of those devices affected by CDPwn remain unpatched. URGENT/11 is a collection of 11 different bugs that can affect any connected device leveraging Wind River's VxWorks. VxWorks is a real-time operating system (RTOS) that third-party hardware manufacturers have embedded in more than 2 billion devices across industrial, medical and enterprise environments. Most concerningly, URGENT/11 includes six remote code-execution (RCE) vulnerabilities that could give an attacker full control over a targeted device, via unauthenticated network packets. CDPwn encompasses five critical vulnerabilities discovered in February in the Cisco Discovery Protocol (CDP), the info-sharing layer that maps all Cisco equipment on a network. The bugs can allow attackers with an existing foothold in the network to break through network-segmentation efforts and remotely take over millions of devices.

K-12 CYBERATTACKS DRAMATICALLY ON THE RISE

In an alert from the FBI and the Cybersecurity and Infrastructure Security Agency (CISA), officials said that data from the Multi-State Information Sharing and Analysis Center (MS-ISAC) shows that 57 percent of ransomware incidents reported to the MS-ISAC involved K-12 schools, "Unfortunately, K-12 education institutions are continuously bombarded with ransomware attacks, as cybercriminals are aware, they are easy targets because of limited funding and resources". Cyber-actors will attack ports 445 (SMB) and 3389 (RDP) to gain network access, they then move laterally throughout a network (often using SMB), escalate privileges, access and exfiltrate sensitive information, harvest credentials or deploy a wide variety of malware.

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

SPRING SCHEDULE 2021

CAT #	COURSE	Books
CYBV 301	FUNDAMENTALS OF CYBERSECURITY	Book
CYBV 310	INTRO SECURITY PROGRAMMING I	Book
CYBV 311	INTRO SECURITY PROGRAMMING II	Book
CYBV 312	INTRODUCTION TO SECURITY SCRIPTING	Book
CYBV 326	INTRO METHODS OF NETWORKING ANALYSIS	Book
CYBV 329	CYBER ETHICS	Book
CYBV 354	PRINCIPLES OPEN-SOURCE INTEL	Book
CYBV 385	INTRO TO CYBER OPERATIONS	Book
CYBV 381	INCIDENT RESPONSE TO DIGITAL FORENSICS	Book
CYBV 382	NETWORK FORENSICS	Book
CYBV 388	CYBER INSTIGATIONS AND FORENSICS	Book 1, Book 2
CYBV 400	ACTIVE CYBER DEFENSE	Book 1, Book 2
CYBV 435	CYBER THREAT INTELLIGENCE	Book 1, Book 2, Book 3
CYBV 436	COUNTER CYBER THREAT INTEL	Book

SIGN UP FOR CLASSES SOON AND CHECK OUT WHAT EACH CLASS REQUIRES FOR BOOKS

CAT #	COURSE	Books
CYBV 437	DECEPTION & COUNTER-DECEPTION	Book
CYBV 440	DIGITAL ESPIONAGE	Book 1, Book 2
CYBV 441	CYBER WAR, TERROR AND CRIME	Book 1, Book 2
CYBV 450	INFORMATION WARFARE	Book 1
CYBV 454	MALWARE THREATS & ANALYSIS	Book
CYBV 471	ASSEMBLY LANG PROG FOR SEC PROF	Book
CYBV 473	VIOLENT PYTHON	Book 1, Book 2
CYBV 474	ADVANCED ANALYTICS FOR SEC OPS	Book 1, Book 2
CYBV 480	CYBER WARFARE	Book 1, Book 2
CYBV 481	SOC ENG ATTACK & DEFENSE	Book 1, Book 2

SPRING SCHEDULE 2021

BEFORE YOU KNOW WHERE YOU GO YOU NEED TO KNOW WHERE YOU CAME FROM

CYBER SECURITY HISTORY

OPERATION AURORA FIRST PUBLICLY DISCLOSED BY GOOGLE

Operation Aurora was a series of cyber attacks conducted by advanced persistent threats such as the Elder wood Group based in Beijing, China, with ties to the People's Liberation Army, the attacks began in mid-2009 and continued through December 2009. According to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at high tech, security and defense contractor companies. Technical evidence including IP addresses, domain names, malware signatures, and other factors, show China groups behind this attack series.

JANUARY 12, 2010

DATA ENCRYPTION STANDARD (DES) PUBLISHED AS FEDERAL STANDARD (FIPS PUB 46)

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of digital data. The origins of DES date to 1972, when a National Bureau of Standards study of US government computer security identified a need for a government-wide standard for encrypting unclassified, sensitive information. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography. DES is now considered insecure due to the relatively short 56-bit key size. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. This cipher has been superseded by the Advanced Encryption Standard (AES). DES has been withdrawn as a standard by the National Institute of Standards and Technology.

JANUARY 15, 1977

BRAIN BOOT SECTOR VIRUS IS RELEASED

Brain is the industry standard name for a computer virus that was released in its first form on January 19, 1986 and is the first computer virus for MS-DOS. Brain affects the IBM PC by replacing the boot sector of a floppy disk with a copy of the virus. The real boot sector is moved to another sector and marked as bad. Infected disks usually have five kilobytes of bad sectors. The disk label is usually changed to ©Brain, and the following text can be seen in infected boot sectors:

Welcome to the Dungeon (c) 1986 Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!

JANUARY 19, 1986

IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

1/3

ABUSING APPLICATION LAYER GATEWAYS NAT SLIPSTREAMING

NAT SLIPSTREAMING allows a malicious user to remotely access any TCP/UDP service used by a victim machine. After abusing the victim's NAT/firewall following the victim visiting a website. For reference, your router maps what your internal IP is and keeps a record when you connect to an external service. So, when you communicate with a website outside of your network, your router knows where to send the data.

You generally do not want to have your computer connected directly to the internet, so this is where NAT or Network Address Translation comes into place. Take CYBV 326 for more information about this and many other network protocols. Anyhow, the process of SLIPSTREAMING makes use of an abuse of the application layer protocol “Session Initiation Protocol” or SIP. SIP is used for many things, but I am more familiar with it as a VoIP protocol. If you work at an organization with VoIP phones you are going to more likely find SIP network messages.

SIP is a text-based protocol, just like HTTP you can view the contents within Wireshark and see how the message is formatted. VoIP traditionally works better peer-to-peer, so there is a REGISTER option that allows a malicious user to punch a hole into your firewall. This exploit will utilize a fake SIP registration process on an external server to gain access to the internal network.

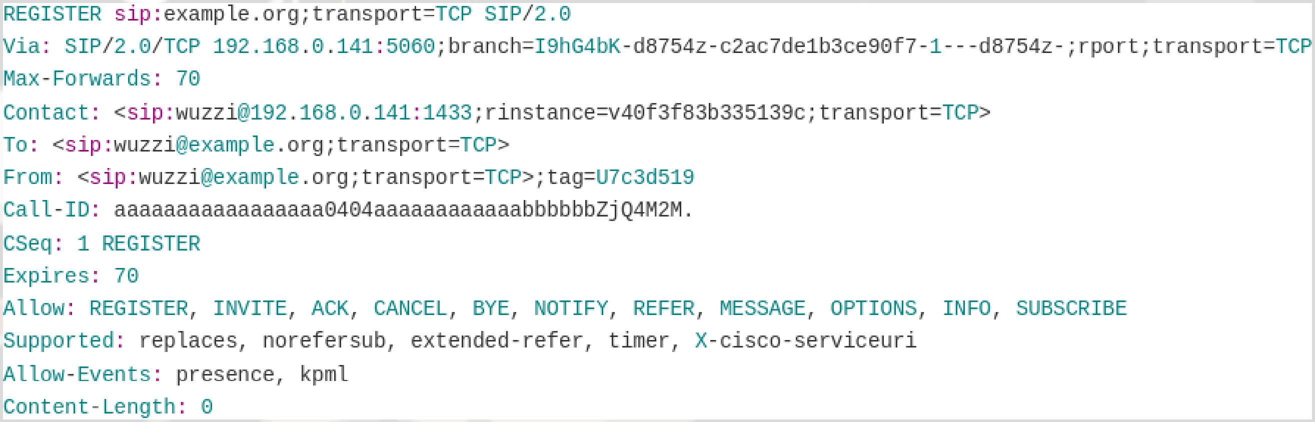
CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. THIS SERIES IS INTENDED FOR ACADEMIC PURPOSES ONLY AND IS MEANT TO PROVIDE EDUCATION TO CYBER SECURITY PROFESSIONALS... IF YOU WANT TO DO THIS STUFF FOR REAL, DO GOOD IN SCHOOL AND GET A JOB THAT PAYS YOU TO DO IT - LEGALLY!!

2/3

ABUSING APPLICATION LAYER GATEWAYS NAT SLIPSTREAMING

The first thing we are going to do is set up a SIP server on an external connection. For this concept to work it needs to be outside of your internal network. We also do not need a full SIP server as we will not be utilizing legitimate data so all we need is something small that can do the registration communication.

The GitHub repo located here allows us to do just that within a python environment. This can be set up in any environment that allows python to run and for you to run a server. So, for this example we could use a Digital Ocean VPS to run this and point our malicious connection to this location. After the fake SIP server is up and running outside your network, you can try to punch a hole in your firewall. This is done by sending the REGISTER request to the server. This can be done in two ways, the first way is using a PowerShell script if you have Windows and the second is a bash script you can run on Linux, MacOS or some Windows variants if you have the proper tools installed. The first script can be found here, and you would save this locally as a ps1 file so that PowerShell knows to open it. The bash script is located here, and you would save this as a .sh file. MacOS needs an additional change and the instructions are included in this file. When you run one of these your machine then crafts a SIP REGISTER packet as shown below.



```
REGISTER sip:example.org;transport=TCP SIP/2.0
Via: SIP/2.0/TCP 192.168.0.141:5060;branch=I9hG4bK-d8754z-c2ac7de1b3ce90f7-1---d8754z-;rport;transport=TCP
Max-Forwards: 70
Contact: <sip:wuzzi@192.168.0.141:1433;rinstance=v40f3f83b335139c;transport=TCP>
To: <sip:wuzzi@example.org;transport=TCP>
From: <sip:wuzzi@example.org;transport=TCP>;tag=U7c3d519
Call-ID: aaaaaaaaaaaaaaaaaa0404aaaaaaaaaaaaabbbbbbZjQ4M2M.
CSeq: 1 REGISTER
Expires: 70
Allow: REGISTER, INVITE, ACK, CANCEL, BYE, NOTIFY, REFER, MESSAGE, OPTIONS, INFO, SUBSCRIBE
Supported: replaces, norefersub, extended-refer, timer, X-cisco-serviceuri
Allow-Events: presence, kpml
Content-Length: 0
```

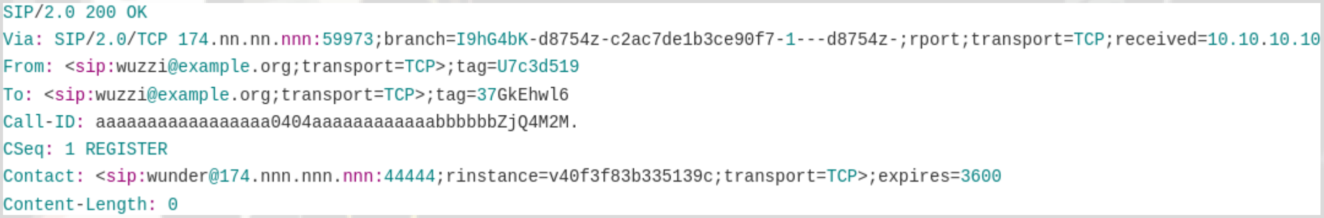
IN ORDER TO LEARN HOW TO DEFEND YOU MUST UNDERSTAND HOW TO ATTACK

HACKING POC

3/3

ABUSING APPLICATION LAYER GATEWAYS NAT SLIPSTREAMING

When you are crafting this message, you need to make a few changes for everything to work correctly. You need to identify the port for the remote SIP server and identify the port you want to expose on the internal network. Now when the script is run it is addressed and sent to the external network but once it reaches the internal network's router, the router will change the requesting IP address to the internal network's public IP address. The router has recognized that an internal machine is attempting to request a SIP transmission and any response will be forwarded to the internal machine. This will also require the internal router to have ALG SIP enabled which is likely if the target already utilizes a SIP server for VOIP activity. Now your external SIP server will send a response message which will be addressed to the public IP address and will open the requested port which in this case will be port 1433. You have now just punched a hole into the internal network and for about 2 minutes you will have access to the internal machine. A malicious actor can do a lot of damage in only 2 minutes and at this point you have what you need. Access to an internal machine while bypassing firewall protections.



```
SIP/2.0 200 OK
Via: SIP/2.0/TCP 174.nn.nn.nnn:59973;branch=I9hG4bK-d8754z-c2ac7de1b3ce90f7-1---d8754z-;rport;transport=TCP;received=10.10.10.10
From: <sip:wuzzi@example.org;transport=TCP>;tag=U7c3d519
To: <sip:wuzzi@example.org;transport=TCP>;tag=37GkEhwl6
Call-ID: aaaaaaaaaaaaaaaaa0404aaaaaaaaaaaabbbbbbZjQ4M2M.
CSeq: 1 REGISTER
Contact: <sip:wunder@174.nnn.nnn.nnn:44444;rinstance=v40f3f83b335139c;transport=TCP>;expires=3600
Content-Length: 0
```

Now you could simply block ALG SIP on your router and not have to deal with this, but many organizations rely on VOIP communications and may not have this as an option. Therefore, knowing which machines should be able to make this connection would need to be whitelisted to ensure only trusted devices can communicate this way which should not be a production machine.

SOMETIMES YOU JUST NEED SOMEONE TO POINT YOU IN THE RIGHT DIRECTION

Nmap is a tool I feel like I have used in every engagement I have been a part of. Nmap has the power to give you a "mapping" of what is on the network currently and tell you with some accuracy what OS is in use and what services may be running. Or at least all the open ports that will respond. Now Nmap has been around for a while and was even one of the commands in the Matrix Reloaded movie when Carrie-Anne Moss shuts down the power grid.

So, for a little background of what this tool can do, when you run it you can discover what hosts are on the network, discover what ports respond on each of those hosts. Use fingerprinting tools to get an idea of what version services are running and what Operating system is in use on each system and finally it allows you to script events out using its internal tools or with Lua. So, when we run Nmap we need to identify a target. This can be an IP address like 192.168.1.1 or a range of IP address like 192.168.1.0/24 which will scan all IP's in that subnet.

COMMAND	RESULT
nmap 192.168.1.1	Scan a single IP
nmap www.google.com	Scan a single host
nmap 192.168.1.1-20	Scan a range of IPs
nmap 192.168.1.0/24	Scan a subnet
nmap -iL list-of-ips.txt	Scan targets from a text file

When you run these commands, you will run a default scan, which will scan 1000 TCP ports and do a simple host discovery.

SOMETIMES YOU JUST NEED SOMEONE TO POINT YOU IN THE RIGHT DIRECTION

TIPS & TRICKS OF THE TRADE

Now we can also tell Nmap to look at only some ports to narrow down what we are looking for or to make the search even quicker for us.

COMMAND	RESULT
nmap -p 22 192.168.1.1	Scan a single Port (ex. 22)
nmap -p 1-100 192.168.1.1	Scan a range of ports
nmap -F 192.168.1.1	Scan 100 most common ports
nmap -p- 192.168.1.1	Scan all 65535 ports

We can also adjust this to scan ports using some additional modifiers

COMMAND	RESULT
nmap -sT 192.168.1.1	Scan using TCP connect
nmap -sS 192.168.1.1	Scan using TCP SYN scan
nmap -sU -p 123,161,162 192.168.1.1	Scan UDP ports
nmap -Pn -F 192.168.1.1	Scan selected ports - ignore discovery

And finally, we can also do some light fingerprinting and identify the host OS and services using the following.

COMMAND	RESULT
nmap -A 192.168.1.1	Detect OS and Services
nmap -sV 192.168.1.1	Standard service detection
nmap -sV --version-intensity 5 192.168.1.1	More aggressive Service Detection
nmap -sV --version-intensity 0 192.168.1.1	Lighter banner grabbing detection

GET UP AND RUNNING TODAY TO START SOMETHING NEW

QUICK PROJECT

1/4

SELF HOSTED RESOURCE PLANNING - GROCY

Resource management is a skill you learn over many years and this can be applied to many different jobs that you may apply to in the future. This project will have you set up your own web server that will track your internal kitchen inventory. Host the website locally in your house and put an old tablet on the fridge and track every item down to what ever level you wish.

This project I will admit is a little overkill for most people, but I also see it as a fun project. You will learn how to set up your own web service and then how to secure that service. You can then download the mobile app and control the entire ecosystem. You will not need to rely on any 3rd party service like Google or Amazon and will have your own learning experience. And in the end, you get an overly geeky tool to track everything in your kitchen.

The first thing we are going to do is install a operating system. In this example we will use Debian 10.7 and you can choose which version you want but I am just going to use the minimal install method.

Next, we run the following commands:

```
Sudo apt-get update && Sudo apt-get full-upgrade –y
```

This will install any updates and the –y will auto allow this command to take place. This may take a while so sit back and relax for a few and get a cup of coffee.

Now that our system is up to date, we are going to install a few packages for use to use.

```
Sudo apt install -y nginx sqlite3 php-fpm php-sqlite3 php-gd unzip
```

This is going to install nginx which we will use to host our web instance, sqlite3 which will be our database for all our yummy food items, php and its dependencies which will handle the logic and finally unzip so that we can decompress our file.

2/4

SELF HOSTED RESOURCE PLANNING - GROCY

Next, we will get our copy of Grocy. We will pull the latest stable version from the GitHub repo.

```
wget https://releases.grocy.info/latest
```

Now this may take a little time but once this is done, we can unzip the file in our web directory.

```
Sudo unzip latest -d /var/www/html
```

Next, we will change ownership information for the files.

```
Sudo chown -R www-data:www-data /var/www
```

Now we just need to change a few settings within Grocy to enable the service to work correctly. We will be using the default settings so just do the following command.

```
Sudo cp /var/www/html/config-dist.php /var/www/html/data/config.php
```

This is going to move the default configuration over to the active configuration settings. You can go into this and change settings if you wish.

Now we are going to set up the webserver and will configure it for many of our items to work and link correctly. First, we will create and edit a file Nginx will use for php files. We will type the following command:

```
Sudo nano /etc/nginx/conf.d/fastcgi_params
```

This will first create a new file called fastchi_params and we will then copy the following into this file:

```
include fastcgi_params;
fastcgi_split_path_info ^(.+?\.php)(|/.*)$;
fastcgi_pass unix:/var/run/php/php7.3-fpm.sock;
```

Now exit out by using Ctrl-X and hit Y to save changes. Next, we will need to tell Nginx about our new web service so we will change directories to add our Grocy service.

```
Cd /etc/nginx/sites-available
```

Now we will take the default configuration and make a new file name grocy.

```
Sudo cp default grocy
```

This copies the file default into a new file named grocy.

3/4 SELF HOSTED RESOURCE PLANNING - GROCY

Now we will link this file to the sites-enabled directory. Nginx uses this to keep track of what to show and how.

```
Sudo ln –s /etc/nginx/sites-available/grocy /etc/nginx/sites-enabled/grocy
```

And now we will remove the default configuration

```
Sudo rm default
```

Now we can edit our configuration file by typing

```
Sudo nano grocy
```

We will type the following

```
server {
      listen 80;
      listen [::]:80;
      root /var/www/html/grocy/public;
      index index.html index.htm index.nginx-debian.html index.php;
      server_name _;
      location / {
            try_files $uri /index.php;
        }
      location ~ \.php$ {
            include snippets/fastcgi-php.conf;
            fastcgi_pass unix:/run/php/php7.3-fpm.sock;
        }
}
```

We will then close this file by hitting CTRL-X and typing Y to save changes.

Now I am using PHP version 7.3 and you would want to check your version by typing

```
Php –version
```

Now we also want to check that Nginx is reading the configuration file correctly so we will run the following command.

```
sudo nginx –t
```

You should get a readout saying that the syntax is ok, and the test was successful.

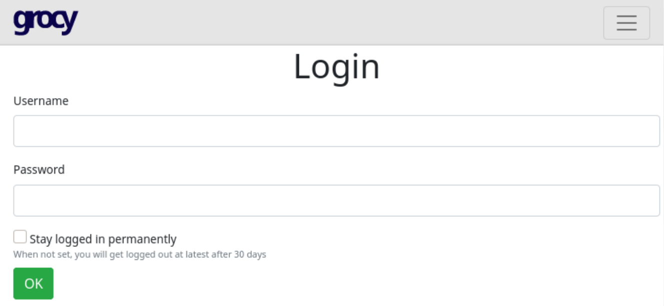
4/4

SELF HOSTED RESOURCE PLANNING - GROCY

Once we get a good read, we can now restart the Nginx service by typing the following command.

```
systemctl restart nginx.service
```

Now go to the IP address of your web server and you should now have the login screen for grocy!



grocy

Login

Username

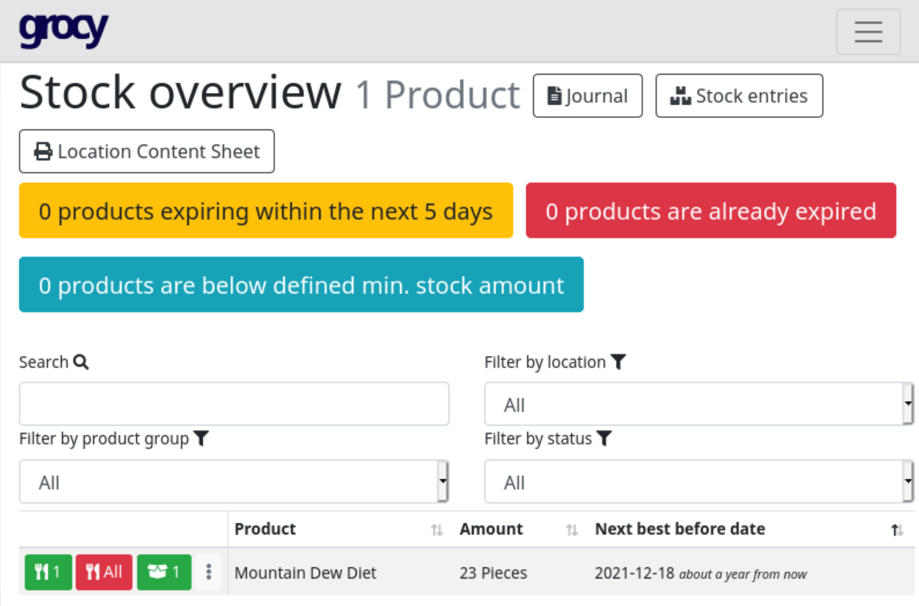
Password

□ Stay logged in permanently

When not set, you will get logged out at latest after 30 days

OK

Now the default login is admin for both the username and password. Now once you login you can select the upper right and select manage users to change the password to something more suited to your tastes. You can also create additional users to add and consume products. Now you can also generate an API key and if you download the android app you can link this app to your server and you now control the entire infrastructure. You now own the shopping app, and everything needed to run it your self. You learn resource management which Is a valuable life skill but also how to set up your own web server, how to enable an API key and so much more. Now go scan everything in your shelves and start tracking everything.



grocy

Stock overview 1 Product

0 products expiring within the next 5 days

0 products are already expired

0 products are below defined min. stock amount

Search

Filter by location: All

Filter by product group: All

Filter by status: All

	Product	Amount	Next best before date
1 All 1	Mountain Dew Diet	23 Pieces	2021-12-18 *about a year from now*

RISING STARS OF THE CYBER SECURITY COMMUNITY

STUDENT INTERVIEW

I have been talking to a former Cyber Operations student who is now working at the National Security Administration (NSA) and has agreed to answer a few questions. Because their position within the NSA they have asked me to refer to them as Agent Smith. Well, they said I can call them anything, so I chose Agent Smith because of the movie "The Matrix".

First off thank you Agent Smith for taking the time to answer my questions, first what did you want to be when you grew up as a child and what made you finally want to be in cybersecurity?

As a child, I knew I wanted to be involved with public service in one form or another. I would like to say this innate drive was derived from my family, as I have many relatives who work in the public service sector. The focal point of this desire took many forms as I matured, ranging from law enforcement to forensic investigations. However, I did not learn of Cyber Operations until my freshman year of college.

At that time, I was a Business major at a community college and had enrolled in an introduction to cyber course. By the end of the first lecture, I was fascinated by the opportunity to pursue a career in this ever-changing field. More importantly, I was thrilled that I could be involved in a field that allowed me the opportunity to positively impact the nation.

Concurrently, the Cyber Operations program at the University of Arizona was being established. After discussing the skillset acquired with the Cyber Operation's Program Director, I decided to switch majors and start down the path that led me to where I am today.

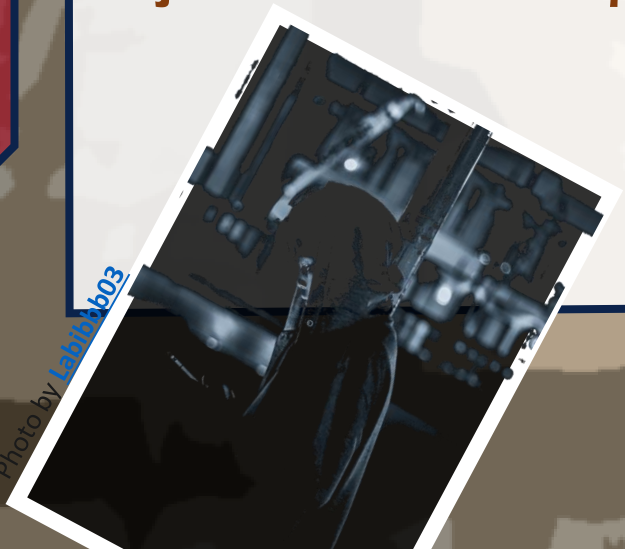


Photo by Labibbb03

Well Agent Smith If you could talk to yourself self-10-ish years ago what would you say?

If I could talk to myself from ten years ago, the advice I would give is to start exploring low-level programming (C and Assembly) and the critical role it has within the realm of Cyber Operations. Having a foundational knowledge of how low-level programming is integrated into every facet of Cyber Operations is invaluable. Although numerous other high-level languages might be easier to learn, low-level languages give insight into a computer's architecture via machine code instructions.

What topic in cybersecurity was your favorite vs. what could you do without?

The topic in cybersecurity that was my favorite in college were Python programming and malware analysis. Although I learned C, Assembly, and Python programming during my academic career, I most enjoyed Python. Specifically, its applications within Cyber Operations. This was emphasized in the Violent Python course, which introduced scripting methods to analyze network traffic, how to extract evidence from large files, and many other complex tasks that are relevant to a cyber professional.

Malware analysis is also one of my favorite topics in Cyber Operations. I have a strong knowledge of Assembly programming, so the logical leap to analyzing binary files was not vast. More so, I enjoy the "puzzle-solving" aspect of malware analysis.

In all honesty, there is not one aspect of Cyber Operations that I shy away from or do not enjoy. As such, I will answer the question through a different lens. Instead, if there is one topic of Cyber Operations that I would like to learn more about it is internet of things (IoT) security vulnerabilities. Because IoT devices are so ubiquitous, exploring this technology further is a subject matter I foresee myself investing more time into in the future.

Now that you have been working at the NSA, a dream for many students, do you have any advice for current students who may be looking for positions at the NSA or in federal service?

There is a lot of advice for current students seeking positions within the NSA or federal service. For the sake of brevity, I will provide two pieces of advice. First, apply for every summer internship you can with the agencies you are interested in working with. In my opinion, I believe internships can be the most effective way to learn about what an Agency does and to see if it would be a good fit for you.

I would also add that students should be very intentional when applying/processing for any internship. I say this because many of the federal service internships are available nationally, so there could be thousands of applicants applying for a small number of seats. Therefore, students should treat the process as you would a job. This means filling out and submitting all paperwork promptly, consistently staying in contact with your recruiter, and be prepared for anything they might ask of you. Doing this will usually give you the best chance of being selected.

The second piece of advice I will provide is to apply early if you are interested in a job with a federal service agency. Comparatively to the application process for other positions within the Cyber Operations realm, there is one major component that can take a significant amount of time to complete – the security clearance. From my experience, most federal service agencies recommend students apply around a year before their graduation date. This is because of the in-depth nature of the security processing that takes place to determine employment eligibility. In other words, if you wait to apply for a job until right before you graduate, likely, you will not be eligible to start until a year or more later.

Would you like to offer any general advice to current students?

If I could offer general advice to current students, it would be to discover what you are passionate about in Cyber Operations and pursue it. This could range from malware analysis to cloud computing and anything in between. The takeaway here is that once you find what you enjoy, explore the career opportunities that exist around it. There is no shortage of job vacancies within the Cyber sector and pursuing your passion will only increase your chances of success.

More so, with the availability of the internet, a wealth of knowledge about the Cyber sector exists at your fingertips. Whether it be using online learning platforms like Udemy or honing your skillset on HackTheBox, it is important to take the time to find what you enjoy and start expanding the skillset that encompasses your interests.

Well Agent Smith it has been a pleasure and I would like to thank you for your time, your service and thank you for making us here at the University of Arizona Proud. Now if I can only talk you into getting me an awesome challenge coin that would be sweet!

Photo by Tima Miroshnichenko

JOBS & INTERNSHIPS

DATA SCIENTIST
FORT MEADE, MD

Data Scientists are hired into positions directly supporting a technical mission office or the Data Scientist Development Program (DSDP). The NSA/CSS Data Scientist Development Program is a three-year opportunity to build your data science talent, experience the breadth of data science at NSA through six- to nine-month assignments in a variety of diverse organizations, and collaborate with NSA's experts in the field of data science. You will have opportunities to attend technical conferences with experts from industry and academia. You will routinely discuss and share NSA's challenges and successes at weekly technical roundtables. We foster an environment where you will develop your data science skills, allowing you to quickly contribute to NSA's mission.

CYBER MITIGATIONS ENGINEER
FORT MEADE, MD

System Vulnerability Analysts identify vulnerabilities and attacks to the design and operation of a system (H/W, S/W, personnel, procedures, logistics, and physical security). They compare various system attack techniques and develop effective defensive mitigations. Additionally, System Vulnerability Analysts produce formal and informal reports, briefings, and perspectives of actual and potential attacks against the systems or missions being studied.

LEARN ABOUT CYBER SECURITY AND WORK IN CYBER SECURITY

JOBS & INTERNSHIPS

INFORMATION SECURITY FORT MEADE, MD

Information System Security professionals are hired into positions directly supporting a technical mission office or into the Cybersecurity Engineering Development Program.

The Cybersecurity Engineering Development Program is a 3-year program. To meet the Agency's evolving mission, NSA's core discipline of Information System Security and Cryptographic Engineering must remain strong and agile. Information System Security and Cryptographic Engineering integrates computer science, engineering and mathematics along with Information Assurance/Cybersecurity Analysis skills, so that the Agency can define the standards for high-assurance as the trusted authority for National Security System (NSS) communications.

COMPUTER NETWORK ANALYST FORT MEADE, MD

Computer Network Analysts are hired into positions directly supporting a technical mission office (either on the offensive or defensive side) or one of a few different development programs like the Intrusion Analyst Skill Development Program (IASDP) and the Cybersecurity Operations Development Program (CSODP) (formerly named the Information Assurance and Cyber Development Program (IACDP)). These development programs are 3 years in length and combine formal training and diverse work assignments that may cross both offensive and defensive missions.

UNIX SYSTEMS ADMINISTRATOR SIERRA VISTA, AZ

Intermediate UNIX Systems Administrator supporting the Web Development Team, Regional Cyber Center – CONUS (RCC-C) at Fort Huachuca, a 24×7 enterprise support organization.

- Daily monitoring and maintenance of Tomcat systems.
- Installing, configuring, and maintaining web and application servers
- Monitoring log files, performance issues, and the production environment for mission critical systems
- Participate in an on-call rotation for support and server maintenance issues
- Ensuring the security posture of the environment
- Secret clearance or ability to obtain interim Secret
- Requires HS + 4 years of similar experience, AA/AS + 2 or BA/BS +0.

FORENSIC ANALYST SCOTTSDALE, AZ

McKesson's Intern program provides you with an opportunity to experience in the healthcare industry, first-hand. By applying your education to a real-life working environment, you will receive a solid foundation of experience as a McKesson intern team. Within the McKesson ISRM Active Defense Intelligent Security Operations Center role (iSOC), the intern(s) will have an opportunity to participate in a structured program that will provide them the opportunity to experience how a global security organization orchestrates threat detection and response, computer forensics analysis, eDiscovery processing, incident response and command, cyber threat intelligence, security analytics, automation and orchestration, forensic analysis, as well as what it takes to build and operate a world-class intelligence security operations center (iSOC).

1/3

SOLARWINDS / SUNBURST: AN ANALYSIS

So, while we are ending the year 2020, we have a very complex and involved cyber attack. This was a cyber-espionage attack effecting multiple victims by infecting a popular supply chain. The company originally targeted was the cybersecurity vendor SolarWinds. This is a notable event because it is a global incident effecting multiple victims through a supply chain which is historically rare, and this analysis will break down the events for you. Now at the time of this writing there is still a lot that needs to be figured out so this analysis may be a little out of date as more information is presented. So, first off, what makes SolarWinds such an important event was that this would be considered a supply chain attack which is usually a state sponsored activity and as stated before, supply chain attacks are rare. Now you may be aware of a NSM as a Network Security Monitor and SolarWinds produces a tool called the Orion NMS or Network Management System which is not the same thing. Network Management Systems are a good target for attackers because they likely have connections to all devices that the organization deploying this tool considers to be valuable. The tool once deployed monitors inbound and outbound communication and acts when a pre-described event takes place. SolarWinds is a software company that sells mostly system management tools used by IT professionals in many organizations. SolarWinds has many customers like the Department of Defense, Microsoft, Intel and FireEye. SolarWinds has a customer base of over 300,000 customers with many in the US federal government and 425 of the fortune 500 companies. SolarWinds also has many international customers so the impact of this attack is very large and still not completely understood yet as forensics is still taking place. Historic cyber attacks can generally be argued as being complex and in many ways, this is correct however this attack shows advanced sophistication that is not very commonly seen which is the main reason this attack is believed to be a nation-state level of attack. The WannaCry attack could be argued as being complex but compared to SolarWinds, this is a change in what an organization would usually protect against.

2/3 SOLARWINDS / SUNBURST: AN ANALYSIS

So, what is the timeline of events here? For starters, it is not known currently how SolarWinds was breached or when this took place, but the fist sign of infection came from a malicious software update that came from official SolarWinds infrastructure and was digitally signed correctly using the Symantec keys. This indicates that the attackers had access before this known infection.

The malicious SolarWinds update malware does not execute its payload unless the software has been deployed for at least 12 to 14 days. Waiting 12 to 14 days prevents detection in high security environments where pre-testing takes place as to avoid being detected before the malware can preform its function. Additionally, the malware will not deploy unless the machine is connected to a domain as to ensure that the malware will only execute within production environments. The malware is designed to ensure that it activates its payload only once placed into a production environment. So, what did this malicious malware even do? The malware can be broken into different function areas, the first being a backdoor into the infected system, one component nicknamed SUNBURST can transfer files, execute programs, profile and identify the system, preform a system reboot and disable system services. SUNBURST will store reconnaissance results within legitimate plugin configuration files allowing it to blend in with legitimate SolarWinds activity as to further avoid detection as information is collected or exfiltrated out of the network environment. The next component has been nicknamed TEARDROP and loads a custom version of Cobalt Strike BEACON into system memory. TEARDROP will run as a system service and reads its instructions from a fake JPG file. TEARDROP then checks the system to ensure that a registry entry exists indicating that it is in a correct environment before being executed and then unpacks the remaining malware using a rolling XOR algorithm. The malware authors then change the Command-and-Control infrastructure or C2 to match the victim's environment to evade detection so that all C2 communication appears to be legitimate internal communication.

3/3 SOLARWINDS / SUNBURST: AN ANALYSIS

The original infection date of SolarWinds, March 2020 is the earliest point of activity at the time of the writing. It is likely the malware authors had access to SolarWinds internal network before this point, however, there is no forensic timeline available as it is still being researched. The cybersecurity industry acted quickly to triage internal networks and many agencies are taking part in forensics. So, if you were an organization that was been hit by the SolarWinds incident what are you to do anyhow? Well malicious actors likely had full access to your network and internal infrastructure. While many companies were targeted and breached, the malicious actors could have deployed additional weapons that have not been reported. SUNBURST and DROPPER were more espionage tools that could have additionally been used to deploy other unknown malware variants. The very first report of this incident came from the cybersecurity firm FireEye on December 8, 2020 indicating that the company had an internal breach involving many internal cyber security tools the company developed inhouse for cybersecurity engagements. This was followed by the United States Treasury department on December 13, 2020 who reported a breach of many internal communications to include internal email services. This later became a flood of potential victims as forensics of the incident started to be shared and studied. It is likely that the full report of the SolarWinds event will take many months and maybe even years before we know the full story and timeline but already the incident has caused many organization to re-evaluate internal security and the role vendors play in that part. Due to the LIMITED cyber security workforce available, many organizations will continue to use vendors for network security monitoring. The need for more trained individuals in competent methods have never been so clear and the role of Cyber Security individuals like yourselves will always be evolving to protect against the evolving cyber security threats.

RYAN CHAPMAN AND HIS TEAM ARE LOOKING FOR VOLUNTEERS TO SUPPORT ARIZONA'S CACTUSCON.

VOLUNTEERS CAN RECEIVE TRAINING ON MODERATOR BOT CREATION, UNDERSTANDING THE BACKEND SYSTEMS, AND HOW THEY OPERATE WITHIN DISCORD.

POTENTIALLY THE MOST IMPORTANT ASPECT IS THE ABILITY TO NETWORK WITH CYBER PROFESSIONALS.

IF YOU ARE INTERESTED IN PARTICIPATING, PLEASE CONNECT TO THE CACTUSCON DISCORD SERVER. COMMUNICATE WITH RYAN OR THE ADMINS THAT YOU ARE THERE FROM THE UNIVERSITY OF ARIZONA TO VOLUNTEER.

```
>.  ---CONNECTION ESTABLISHED---
>.  HAVE A HAPPY NEW YEAR ……
>.  FROM EVERYONE AT THE UNIVERISTY OF ARIZONA
>.  ---END TRANSMISSION---
```

THANK YOU

CONTACT US

CIIO@EMAIL.ARIZONA.EDU

1140 N. Colombo Ave. | Sierra Vista, AZ 85635

Phone: 520-458-8278 ext 2155

http://cyber-operations.azcast.arizona.edu/

ART BY @Julia_Larson

THE UNIVERSITY OF ARIZONA