09/08/2020

U.S. agencies must implement vulnerability-disclosure policies by March 2021, according to a new CISA mandate

URL: https://threatpost.com/u-s-agencies-vulnerability-disclosure-policies-march-2021/158913/

Article Published: 09/02/2020

Summary

This article overviews a new mandate from "the Cybersecurity and Infrastructure Security Agency (CISA)" regarding "vulnerability-disclosure policies (VDPs)". The CISA mandate requires government organizations to "publish policies with detailed descriptions of which systems are in scope" for white-hat vulnerability checkers. This change will make it easier for government agencies to receive information on vulnerabilities from white hat hackers, and make the scope in which those hackers can operate more clearly defined.

Reflection

Knowing how government operates, I am sorry to say that I'm not surprised that it took them this long to start requiring these VDPs for government agencies. The fact that government agencies have essentially ignored the vast resource of white-hat hackers at their disposal until now speaks to how far behind/slow to implement new changes the government is. I am, however, glad that CISA is getting government agencies to utilize hackers to help secure their systems through vulnerability reports, and I'm eager to see how this will affect security changes in government systems in the future. Also, as a side note, I'm curious whether or not this mandate will open the eyes of government officials to methods used by private companies to find bugs in their own systems (federal bug bounties anyone?).

09/11/2020

Cybercriminals are Targeting Gaming Industry Worldwide

URL: https://cyware.com/news/cybercriminals-are-targeting-gaming-industry-worldwide-fd14db5b

Article Published: 09/11/2020

Summary

Due to the increase in overall revenue in the gaming industry, the increase in threats from hackers has been growing exponentially. As is the same with other industries, hackers go after anything sellable including but not limited to: user info, payment info, virtual items, escalated game access, etc. The most recent major attack was "a malicious JavaScript library disguised as "Fall Guys: Ultimate Knockout" game API" which stole the files from the user.

Reflection

I play video games a lot if I'm being honest. The industry has had quite a few bad cases of hacking and I myself have had IPs from random assorted nations try to gain access to my accounts. The main factor that has kept my accounts from being successfully broken into has been a two-factor login system, which usually involves some form of text message code after entering the correct password to login to my accounts. The reason that I know that foreign IPs were the ones responsible for attempting to access my account was due to receiving text message codes without me trying to login and when I checked my account afterward the service my account is through flagged the failed login attempts and gave a worldly location for the IPs whereabouts.

Anyway, I digress, I never realized the true financial scope of hacks on the gaming industry and I believe this will change the way I think of the gaming industry in the future (mostly for job prospects).

09/16/2020

GitHub's move away from Passwords: A Sign of Things to Come?

URL: https://hackaday.com/2020/09/15/githubs-move-away-from-passwords-a-sign-of-things-to-come/?web_view=true

Article Published: 09/15/2020

Summary

GitHub services are moving away from username password authentication. All of their services aside from their Enterprise Servers will be affected. This change was announced back in November 2019 and is now being slowly implemented with a deadline for complete implementation by November 13th, 2019. There are listed ways to help prepare for the change to other authentication methods.

Reflection

While I am a relatively new GitHub user, I find this very interesting as it will affect how I manage my school portfolio. This step away from username password authentication kind of comes out of left field for someone like me who hasn't really kept up with direct changes in GitHub, but it is interesting to think of alternatives especially considering I'm currently working on password cracking for lab04 and realizing how potentially vulnerable the current system is. I'm interested to see how this move may affect other services I use and whether or not it will be a more secure and effective system for authentication.

09/20/2020

Living-off-the-Land Attacks Surge, Attackers Focus on Abusing Legitimate Tools and Services

URL: https://cyware.com/news/living-off-the-land-attacks-surge-attackers-focus-on-abusing-legitimate-tools-and-services-1101a1fb

Article Published: 09/20/2020

Summary

In this article they look at last years tracked cyber-attacks and tactics involved in cyber-attacks. Recently there has been an uptick in attacks that use legit tools and services to break into enterprise networks. Kaspersky Lab has gathered data that shows that 30% of attacks in 2019 used legit tools in a malicious manner. With hackers using legitimate tools, in malicious manners or not, it makes it much more difficult to spot security threats.

Reflection

In class we have looked at direct methods of hacking with Linux and tracked an attack through FTP on legit software. After reading the article, I am surprised at the number of hacks that involved legitimate software. I've always heard of and been warned about legit software being used in attacks, but I never would have guessed it was anywhere near as common as 30%. Knowing that so many attacks involve legit software definitely opens my eyes to how difficult it can be to detect attacks while they're still in progress and gives me a new appreciation for the IT security field. What disturbs me most is that with legit software being involved you would have an incredibly difficult time decerning an attack from normal traffic.

09/24/2020

Cisco: How Real is a Passwordless Future?

URL: https://www.infosecurity-magazine.com/news/cisco-passwordless-future/

Article Published: 09/23/2020

Summary

In this article, the author summarizes and quotes a speech given by CISO J. Wolfgang Goerlich at a Cisco webinar as well as interviews with other CISOs in attendance. Goerlich believes that logging in without a password is in the near future. Goerlich and other CISOs believe that with the enhancement of secondary tokens it is possible to see to a password-less login system using a username and a form of secondary authentication. They believe it is primarily possible due to having "more secure enclaves on phones than before, and more trusted processing on laptops."

Reflection

This is the second article I've found regarding this topic, and seeing it again being raised by even more credible sources only gives more reason to believe this is a very possible future outcome. I find it very interesting, however, that the CISOs had no highlighted technical ways of achieving the second form of authentication. All the CISOs were very vague on how they could see it being implemented in the future.

Personally, I think this is a very interesting possibility and worthy of looking into and keeping an eye on in the future. It very well could revolutionize the way we authenticate and make systems strong or could have the exact opposite effect. Only time will tell whether this is a true possibility or a pipe dream.

09/24/2020

CISA: Detections of LokiBot Info-Stealer Are Soaring

URL: https://www.infosecurity-magazine.com/news/cisa-detections-lokibot/

Article Published: 09/23/2020

Summary

CISA has detected an uptick in use of the LokiBot trojan malware. The article covers the history of LokiBot, what it's used for, when it was first found, etc. The author also interviewed Gurucul CEO, Saryu Nayyar who believes that the trojan malware has been actively modified to beat out the developed corporate protections.

Reflection

The notion that hackers are actively adapting viruses to outgrow a corporations efforts to render it ineffective isn't necessarily new, but this is the first instance I've personally noticed. To think that somewhere on the darkweb there is a group of hackers doing legit development to try and make a virus like LokiBot more effective sounds almost like a conspiracy theory. The only problem with it being a conspiracy theory is the question of how else it would be improving at the rate that it is.

10/01/2020

One in Three Not Worried About Cybersecurity Despite Rise in Threats

URL: https://www.infosecurity-magazine.com/news/one-three-worried-cybersecurity/

Article Published: 09/30/2020

Summary

About a third of the United Kingdoms populace are not concerned with cybersecurity. According to a study by ESET around half don't believe they've been hacked, and the article goes on to say that approximately a quarter of the participants admit that they don't know how to tell when they've been hacked. The article goes on to say that the HMRC are investigating the UK's hackers exploiting the current COVID-19 pandemic.

Reflection

Firstly, I'd like to preface this by saying that I didn't even realize that most people (not in the IT field) don't think about technology the way I do until around about my junior year in college. That said, I am shocked that so many people (even if they are in the UK) don't really think about cybersecurity. I feel like there is such a rise hacking in the world that it is just crazy to me that such a large portion of a population doesn't even really know anything about it. Worse yet, with the frequency of attacks ramping up it seems very odd that more people aren't even concerned that they could fall victim to them.

10/03/2020

US Treasury: Paying Ransomware Gangs Could Violate Regulations

URL: https://www.infosecurity-magazine.com/news/fines-for-paying-ransomware-gangs/

Article Published: 10/02/2020

Summary

This article is an overview of an OFAC (Office of Foreign Assets Control) advisory which cautioned ransomware victims to avoid paying ransomware attackers their ransom due to the possibility that those they are paying may be on a sanction list. They go on to stress the hazardous nature of paying a ransom to these attackers because it will only encourage them and those like them to continue.

Reflection

Let me preface by saying this is exactly why I don't really like a vast majority of government oversight. This is a prime example of a "damned if you damned if you don't" scenario. From the perspective of the victim of ransomware, if you don't pay you risk your data being irretrievable and, potentially even worse, having that information leaked, whereas if you do pay, not only are you potentially out millions of dollars, potentially not going to get your data back, and losing your stable public image, but you are also potentially incurring legal action brought against you by your own government for – knowingly or not – being part of a transaction with members who are on a sanction list.

While I do understand OFAC's position on this issue and the potential hazard with allowing millions of dollars to go to nefarious elements the world over, adding a penalty to the victim and not the perpetrator is completely detrimental to the situation. OFAC is essentially taking a bad situation and making it worse.

10/07/2020

Ransomware threat surge, Ryuk attacks 20 orgs per week

URL: https://www.bleepingcomputer.com/news/security/ransomware-threat-surge-ryuk-attacks-about-20-orgs-per-week/?&web_view=true

Article Published: 10/06/2020

Summary

This article shows us data form Check Point and IBM Security X-Force. They noticed a dramatic uptick in ransomware attacks on the healthcare industry in the last half of 2020. This uptick hasn't just been observed in the US either, with countries like Russia, India and Sri Lanka also having noticeable upticks as well. In particular they note that ransomware threats were particularly high in June of 2020.

Reflection

Upon reflection, it seems obvious that ransomware groups would start targeting healthcare companies more heavily since COVID-19 was announced. The ransomware groups have shown a notable ability to target industries that are doing particularly well for themselves and have a high motivation to keep their systems up and running (a.k.a. would be willing to spend more to get their data back). The massive uptick particularly in June seems rather odd especially considering the lull in the months afterward in ransomware activity. It is definitely something to keep an eye on in the future for the potential of exponential growth of these attacks.

10/08/2020

Canada Bombarded with COVID-19-Themed Cyber-attacks

URL: https://www.infosecurity-magazine.com/news/canada-bombarded-with-covid19/?&web_view=true

Article Published: 10/06/2020

Summary

The Canadian Internet Registration Authority (CIRA) released a "2020 Cybersecurity Report". In the report over 25% of Canadian IT workers believe their organizations have been hit by COVID-19-themed cyber-attacks. Organizations are also reportedly less likely to report a breach as well as being more likely to have a breach. Resources at the surveyed organizations are also projected to have less overall growth potentially leading to even worse detection and prevention relative to the growth in cyberattack threats.

Reflection

I know that I've looked at articles regarding other countries reports on cybersecurity, but I still find it incredibly interesting to read about other countries metrics on cyberthreats and security. The overall takeaway from the article has lead me to believe that Canadian corporations and organizations are not only becoming less likely to report attacks, but also are putting less resources into preventing attacks. This information leads me to think that either they don't understand the danger or are becoming complacent in their defense against cyberthreats overall. Perhaps they need better (American) IT guys to help them out? Please hire me.

10/15/2020

BazarLoader used to deploy Ryuk ransomware on high-value targets

URL: https://www.bleepingcomputer.com/news/security/bazarloader-used-to-deploy-ryuk-ransomware-on-high-value-targets/?&web_view=true

Article Published: 10/12/2020

Summary

TrickBot gang operators have begun using a newer and stealthier trojan on high value targets called BazarLoader. The article goes further to give examples of how the new BazarLoader/BazarBackdoor can be used in attacks and goes even further to show actual examples of the phishing emails used for initially delivering the trojan.

Reflection

This is the first article that I have found that has shown actual real-life examples. They even go so far as to show a general layout/visualized representation of how it infects your systems in a step by step process. In our class we haven't really touched on ransomware in particular, although we have looked at different phishing methods and implementations. I must say that being able to actually see real life examples of how it could be implemented kind of brings what we've been doing so far into a bigger picture and makes me realize that we're only a few steps away from being on the same (if basic) level as some hacker groups.

To a point, this knowledge almost make me want to follow the rabbit a bit, but I know that should I do that I'll end up finding how deep the rabbit hole goes pretty darn quickly and I might not like what I see at the end. Paranoia prevailing, I won't be touching this with a ten yard pole, but I will definitely be looking out for counters to this method in the future.

10/16/2020

With database hacks on the rise, how can companies protect themselves?

URL: https://www.helpnetsecurity.com/2020/10/14/securing-exposed-databases/?web_view=true

Article Published: 10/14/2020

Summary

Unsecured and misconfigured databases are the subject of this article in particular. It goes on to mention that with the increased speed in searching the internet for unsecure databases it is more likely that an attack will occur to those databases. Sometimes attackers copy, replace, delete, or even ransom these open databases before the owners realize they are exposed. Prevention of database unintentionally ending up unsecured is basically boiled down to if you don't know what you are doing you should hire someone who does.

Reflection

I think it is downright bizarre that database admins fairly commonly misconfigure their databases. I didn't really think that things like this happened all that commonly in the professional world and it kind of make me feel more secure in my knowledge and use of databases that I haven't unintentionally done this myself in my previous database courses. In the article they even mention that databases like MongoDB and MariaDB are pretty susceptible to becoming unsecured, and my group and I in IT440 used both of these systems for our distributed database projects (although we ultimately went with MongoDB for our final presentation).

10/21/2020

Remember insider threat? Old news now. Focus on malware detection, says EU infosec agency

URL:
https://www.theregister.com/2020/10/20/enisa_annual_report_cybersecurity/?&web_view=true

Article Published: 10/20/2020

Summary

The EU Agency for Cybersecurity (ENISA) believes that future cyberthreat focus will not be on "personalized" attack vectors like phishing and social engineering but will rather be focused on system-based attack vectors like malware. They go on to make several warnings about threat actors figuring out how to properly implement AI in their attacks. Additionally, they mention that there is an increase in nation-states using the internet as a "war domain" essentially waging cyber warfare with each other in increase frequency.

Reflection

Knowing that this report was released yesterday makes me think that ENISA is a little behind the curve with their warning about system-focused attacks increasing in the future. As evidenced by the previous articles I've looked at there has already been a noticeable uptick in malware-based attacks and, what seems to be, a less of an increase in person-based attacks (social engineering and phishing). Granted, I don't know the availability and the quality of the data that I have previous read, but I would imagine that it held a fair bit of truth if they are just now parroting the same thing that was derived from the data.

10/21/2020

Fooling self-driving cars by displaying virtual objects

URL: https://securityaffairs.co/wordpress/109697/hacking/self-driving-cars-hacking.html?web_view=true

Article Published: 10/19/2020

Summary

Researchers at Ben-Gurion University of the Negev have been studying potential virtual interference with self-driving cars. They tested using projectors as well as digital screens to display road signs and "depthless" 3d objects such as people or roadblocks. Additionally, they have also tested the systems with flashes of those objects to see how they would react.

Reflection

Ever since I got my license at 16 I've always dreamt of having a self-driving car. With researchers having confirmed my fear of virtual interference with self-driving cars sensors, I have to say we have a long way to go before I will be assured enough in the safety of these car systems to keep me from dying a terrible death because some cyber actor decided to throw a virtual person in front of my car and cause a 20 car pileup on the highway. We've got a long way to go and I really hope I get to see a working version in the future.

10/27/2020

Insider Threats: How Menacing are They

URL: https://cyware.com/news/insider-threats-how-menacing-are-they-9bf34783

Article Published: 10/26/2020

Summary

Insider threats are real. Companies oftentimes disregard insiders as any real threat, but they can still become disastrous. With Phishing become more and more prominent, the ability of attackers to get employee credentials is still a real threat to any business. Of course, there is also the ever present possibility that a disgruntled current or former employee may use their knowledge of a businesses systems to help attackers as a form of payback.

Reflection

However major the threat of a direct attack is on a system, you should always consider the possibility of an inside man, I learned that as a kid playing strategy games on my computer. To think that all of that time playing strategy games is now applicable to real life brings me some comfort about how I spent my time as a kid. Honestly, if you had asked me before I read this article I would have probably told you that companies take inside threats seriously, but after having read the article I am astonished to think that companies seem to so easily disregard the potential destructive capability of someone with inside information. They may not be that common of a threat in the everyday operations of a business, but if utilized properly they could spell disaster. Never disregard a potential opponent because as soon as you do, you will get stabbed in the back.

10/29/2020

The lowly DDoS attack is still a viable threat for undermining elections

URL: https://www.cyberscoop.com/lowly-ddos-attack-still-viable-threat-undermining-elections/?web_view=true

Article Published: 10/27/2020

Summary

This article is about the overall vulnerability of election services. Things as simple as DDoS attacks and overwhelming traffic have contributed to election systems complications and the FBI and DHS believe they could potentially be perpetrated by foreign actors to disrupt the election cycle.

Reflection

With the election getting closer, I find myself more and more worried about the systems in use and how prepared they are against possible attacks. While I personally don't think anything as simple as DDoSing is going to truly disrupt the election, I am concerned about more complex threats. What really bothers me regarding this subject is the general acceptance by those I've talked too that the election very well could be disrupted or even tampered with and they don't really seem to care if the election ends up accurate or not unless I specifically bring up the implications. I know that I am more technology inclined than your average American, but I feel like normal people should at least understand the gravity and effect that disruption could have on a legal process like an election.

11/03/2020

TrickBot Rises From the Ashes

URL: https://cyware.com/news/trickbot-rises-from-the-ashes-d02b0e92

Article Published: 11/02/2020

Summary

The backend of TrickBot was disrupted earlier this month by Microsoft, ESET, Lumen's Black Lotus Labs, NTT Ltd., and others. Additionally, the Cyber Command division of the US Military carried out an attack to take control of TrickBot systems and were successful in hampering TrickBots ability to carry out attacks. As of mid-October, however, TrickBot updated their configuration file for their server and it seems TrickBot is up and running again.

Reflection

This is one heck of a story. I know from previous articles that I've read that TrickBot has been a major player in trojan attacks and to say that they have become somewhat well known is definitely the truth. That they have become so well known that they have even garnered the attention of the US military is kind of crazy to think about. Even crazier is that they were able to recover from the combined attack of the US military, Microsoft, Black Lotus Labs, and NTT relatively quickly (they weren't even down for a month). This just goes to show that cyberthreats will always be present and no matter how many you take down their will always be more to take its place.

11/04/2020

BEC attacks increase in most industries, invoice and payment fraud rise by 155%

URL: https://www.helpnetsecurity.com/2020/11/03/bec-attacks-increase-quarter-over-quarter/?web_view=true

Article Published: 11/03/2020

Summary

BEC (Business E-mail Compromise) attacks have continued to increase with the frequency in the energy/infrastructure industry jumping up 93%. BEC attacks across the board have been increasing in frequency in just about every industry. Invoice and payment fraud have also increased by a staggering 155% between Q2 and Q3. Additionally, email attacks have shifted to primarily target group mailboxes.

Reflection

Email attacks will probably never go away within my lifetime. That said, seeing such dramatic increases across the board is still very concerning to see. Thinking back to Lab 09 when we used the social engineering toolkit I feel like it is only going to get easier to carry out email attacks. This being my last semester in college, I have a feeling that I'm going to need to keep an eye on this specific attack vector when I go into the industry in the future.

11/10/2020

The Evil Game That Has Besieged the Gaming Industry

URL: https://cyware.com/news/the-evil-game-that-has-besieged-the-gaming-industry-c1fe5a30

Article Published: 11/10/2020

Summary

Capcom, a Japanese game developer, has been hit with a cyberattack effecting multiple systems. It is reported that the Ragnar Locker ransomware was used in the attack to steal 1TB of confidential data. Hacker groups have also claimed to have hacked into the source codes of gaming titles such as Watch Dogs: Legion and Albion.

Reflection

First, I'd just like to say that lately I haven't been a big fan of Ubisoft so I don't have any sympathy for the hack on Watch Dogs, that aside, I think it is INCREDIBLY ironic that a game about hackers hacking things got hacked and had some of its source code released to other hackers. If that isn't ironic I don't know what is.

Now, into the meat of the issue, I know from previous articles that the gaming industry has been a prime target for hackers and it saddens me to see that they've had such great success in hacking a major developer like Capcom. I've played with the thought of getting into the gaming industry and still have it open as a possibility in the future so to hear about such a major breach concerns me and my potential future. Now more than ever I realize the need for information security and the ability to preempt potential attacks no matter the industry I choose to get in to.

11/12/2020

Microsoft warns against SMS, voice calls for multi-factor authentication: Try something that can't be SIM swapped

URL: https://www.theregister.com/2020/11/11/microsoft_mfa_warning/?&web_view=true

Article Published: 11/11/2020

Summary

Microsoft encourages users to use multi-factor authentication, so long as it isn't over public telephone networks. Their reasoning against trusting SMS-based multi-factor authentication is that it is fundamentally insecure. SIM swapping in particular poses a massive threat to SMS-based authentication. Other attacks like SS7 interception are also extremely effective against SMS-based authentication.

Reflection

This honestly doesn't come as much of a surprise to me after doing the midterm theory for this class. Either Microsoft is just reiterating their stance on it, or they may even be behind the curve a little on possible future exploits. I'd like to think that our midterm theory was just ahead of the curve, but I'm not going to go out of my way to research the subject to find out who got there first. Whatever the case, I've taken steps to get away from SMS authentication myself and have advised my family to do the same, so with any luck these methods won't be effective against us.

10/16/2020

Egregor ransomware causes printers to spit out ransom notes

URL: https://www.databreaches.net/egregor-ransomware-causes-printers-to-spit-out-ransom-notes/?web_view=true

Article Published: 11/15/2020

Summary

A new attack using Egregor ransomware has now involved threat actors sending messages to compromised systems with a list of their demands and printing their message out on receipt printers in multiple stores in Argentina and Chile. The notes didn't start printing until the devices were beginning to be encrypted. This feature of Egregor could potentially lead to thousands of ransom notes printed out across the network.

Reflection

My first thought when reading this article was "They're either being way overly cocky, or they have so completely locked them out that they have a reason to be this cocky." To not only have your systems get hacked but also have the hackers themselves send you any number of written messages essentially laughing in your face is a whole new level of trolling that I did not expect from hackers trying to turn a profit. I know back in the 2000s the hacking group anonymous pulled the same kind of stunts without using ransomware by sending nothing but black pages to fax machines in order to run them dry on ink, but I haven't heard of an attack like that happening in at least the last 10 years.

I guess hackers never lose their sense of humor.

10/19/2020

Ransomware Attacks No More Restricted to Just Encryption

URL: https://cyware.com/news/ransomware-attacks-no-more-restricted-to-just-encryption-6e86c252

Article Published: 11/19/2020

Summary

Ransomware attacks in the past have relied upon encrypting data, but a new trend has emerged that is geared more toward data exfiltration rather than encryption. The reason for this shift is due to a newfound ability to encrypt and extort data after it is exfiltrated in order to get an even higher payday. The way some hackers have been leveraging the victims of ransomware into paying their ransom is by publicly advertising that they have the victims data.

Reflection

The evolution of ransomware tactics has always been fascinating to me ever since I first heard about them. Seeing this article talk about data exfiltration and extortion definitely piques my interest towards ransomware as a whole. Probably the thing that most interests me about it is the fact that some hacker groups are trying to leverage the victim into paying by essentially publicly ridiculing them. I'm just amazed that they can get away with it and not have those public declarations be traced back to them effectively. It is definitely something I will continue to keep an eye on even after I am finished with this class.