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**](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**](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**](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/**](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/**](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.