TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

August 2021

This monthly publication provided courtesy of Adam Cambreleng, Inside Account Manager here at Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

FBI issues rare 'flash alert' about OnePercent

In what may be a first for the agency, the FBI has issued a "flash alert" related to a specific ransomware gang. Dubbed the OnePercent group, the FBI has warned that the threat actors are responsible for numerous attacks on U.S. companies dating back to 2020. The ransomware used in those attacks was the Cobalt Strike variant, specifically following the infection vector given by the IcedID banking Trojan. The OnePercent group has links to REvil (Sodinokibi) ransomware gang, and according to the FBI, uses this connection to leak stolen data, as REvil has web pages dedicated to such content.

The flash alert details multiple facts about OnePercent, most notably their modus operandi. They appear to follow a very specific attack method without much deviation. This can be found in the following excerpt from the alert:

Continued on next page...

'OnePercent Group actors encrypt the data and exfiltrate it from the victims' systems. The actors contact the victims via telephone and email, threatening to release the stolen data through The Onion Router (TOR) network and clearnet, unless a ransom is paid in virtual currency. OnePercent Group actors' extortion tactics always begin with a warning and progress from a partial leak of data to a full leak of all the victim's exfiltrated data'

Some in the information security community are slightly confused by the release of this flash alert. While reporting for Dark Reading, reporter Jai Vijayan quotes an interview with Alec Alvarado, the head of Digital Shadows' threat intelligence team. In it, Alvarado states that "It is certainly interesting to ponder why the FBI chose the OnePercent group to release a Flash about, as the group doesn't necessarily appear to sway significantly from known ransomware tactics." In an additional commentary, Alvarado surmises that either the OnePercent group is ramping up its activity, or the FBI believes that there has not been enough coverage of the group.

In any case, OnePercent is dangerous and effective, so anyone in IT should be aware of their methodology.

—*Derek Kortepeter, TechGenix*

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

vmware® PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-TECH (option 2)

Sales@TechHero.com

UC SAN DIEGO HEALTH SUFFERS DATA BREACH, PHISHING TO BLAME

According to recent disclosures from the UC San Diego Health System, the institution has experienced a significant data breach. UC San Diego Health is one of the top hospitals in the United States, serving as the primary health center for the MLB's San Diego Padres and other high-profile clients. The data breach was discussed in detail on a dedicated page on the institution's website entitled "Data Security FAQs." The explanation of the incident and how the organization responded is found in the following excerpt from this page:

"*When UC San Diego Health discovered the issue, we terminated the unauthorized access to these accounts and enhanced our security controls. UC San Diego Health reported the event to the FBI and is working with external cybersecurity experts to investigate the event and determine what happened, what data was impacted, and to whom the data belonged. This process of analyzing the data in the email accounts is ongoing. UC San Diego Health is moving as quickly as possible while taking the care and time to deliver accurate information about which data was impacted. At this time, we are aware that these email accounts contained personal information associated with a subset of our patient, student, and employee community. We estimate this review will be complete in September.*"

Continued on next page...

According to UCSDH, there are no known instances of this personal data being used by threat actors. Additionally, there is no current evidence suggesting that any other university systems were penetrated during the attack. As is the case with incidents like this, the fallout tends to not be known until many months after the fact. This is why UCSDH is giving anyone potentially affected by the breach credit monitoring and access to identity protection services. Anyone who had data in the university system between Dec. 2, 2020, and April 8, 2021 (the time period over which the breach occurred) should pay close attention to their accounts.

When reporting on the data breach, Bleeping Computer noted that the root cause of this incident was a phishing attack. The news organization was able to obtain this information via UC San Diego Health's Executive Director of Communications and Media Relations Jacqueline Carr. In a correspondence with Bleeping Computer, Carr disclosed this fact.

—*Derek Kortepeter for Techgenix*

Client Spotlight

BUILDING SOLUTIONS

Ally Building Solutions provides finish products, installation, and design studio services to new home production builders, custom builders and multi-family projects in Orlando, Jacksonville, Ocala and Tampa, FL.

SORRY, NOT SORRY: MICROSOFT SAYS YOU CAN'T BYPASS WINDOWS 11 REQUIREMENTS

Worried that your organization won't have the right hardware to run Windows 11? Microsoft hears your cries. But when it comes to the requirements needed to install Windows 11, they're not going to do anything about it.

Microsoft doubles-down on Windows 11 requirements

The company just put out an "Ask Microsoft Anything" video where Microsoft tech experts explain what you will need to run Windows 11 — although the requirements seem unnecessarily restrictive to many IT admins tasked with installing the operating system. With a beta version of Windows 11 out, many IT pros have been trying to fiddle around with the hardware requirements to get older machines to run the OS. One of the things Microsoft hammered home in the video is that this will not be possible with the final release of Windows 11.

'Hardware enforcement'

Windows 11 will automatically check your computer's requirements, and if it doesn't pass, it won't allow the download. Some IT pros have been able to tweak the registry's Group Policy to allow the beta to download even if their machines don't have the necessary requirements. But Microsoft senior program manager Aria Carley said in the video that this type of IT MacGyvering will not get around the "hardware enforcement" in the Windows 11 final version. "We're still going to block you from upgrading your device to an unsupported state since we really want to make sure that your devices stay supported and secure," Carley said.

Continued on next page...

'We know it sucks that some aren't going to be eligible for Windows 11. But the great thing to remember is the reason we're doing that is to keep to devices more productive, have a better experience, and better security than ever before so they can stay protected in this new workforce.'

— Aria Carley, Microsoft senior program manager

What about TPM?

A major topic continues to swirl around the Trusted Platform Module (TPM), specifically TPM 2.0. Having the TPM chip on your computer is a requirement to run Windows 11. The confusion stems because many older computers don't have TPM 2.0. Additionally, some that do have the TPM chip don't have it enabled. In either case, the computer will fail Microsoft's minimum requirements to install Windows 11.

—*Peter King for Techgenix*