CYBER SECURITY NEWS
Vol. 6 | Issue 1
January 2021

Page 2 | Page 3 | Page 4 | Challenge | Closing

Welcome to the TXDPS Cyber Security Newsletter!

Happy New Year! May 2021 bring you lots of joy and good cheer!

By now, you've probably heard of the SolarWinds breach that's making its way through current-event headlines. If you haven't, the long story short is a sophisticated hacker group gained access to computer systems belonging to multiple US government departments (the US Treasury and Justice Department, to name a few) and other high-profile companies such as Microsoft and Cisco.

They did this by compromising the infrastructure of SolarWinds, an Austin-based company that sells network monitoring software. Once this group hacked SolarWinds, they used that access to insert malicious code into trusted software updates of their "Orion" product. These updates were then made available to customers as legitimate software updates. Once these updates were applied, the malicious actors gained access to customer network environments.

So who exactly is SolarWinds?

SolarWinds is a popular software company that primarily deals in systems management tools used by IT professionals. They serve over 300,000 customers, including the US Federal government, state and local governments, US Fortune 500 companies, and other customers worldwide.

In fact, they are arguably the most widely used Network Management System (NMS) software vendor. To borrow a quote from a cyber security company, SANS, "SolarWinds is to NMS as Kleenex is to tissues."

Since SolarWinds provides services to a wide range of customers across multiple sectors, the full extent of this breach is still unfolding as remediation and investigations continue.

For a more technical dive into this attack and for some insight on lessons learned , you can read this article: https://www.darkreading.com/omdia/solarwinds-hack-lessons-learned-finding-the-next-supply-chain-attack/a/d-id/1339871

Cyber Risk Management

Remember that pesky Data Classification we talked about in November? (Feel free to reference November's newsletter if your answer is "no"; my feelings are only a little hurt.)

As consumers and handlers of DPS data, the data classification concept is important for us to know because we also need to make sure that others who come in contact with the data are aware of its classification.

This is done through "media marking" which is this month's cyber risk control focus. Media marking is the labeling of data with the appropriate classification. For example, clearly marking whether the information is public, sensitive, confidential or regulated to ensure users of the data can easily identify the classification of data they are handling. Media will be handled differently depending on the classification level of the data.

Media can be digital (disks and drives) or non-digital (paper and microfilm), and refers to physical items where information can be stored. With media marking, we're specifically concerned about physical items that can be easily removed from a secure area such as printed reports, USB flash drives*, CDs, hard drives, etc.

Think about the reports you print out or email regularly. Are those clearly marked when the information is sensitive or confidential? What if you burn information onto a CD or save it on a flash drive? How is that physical item labeled to ensure it's handled and stored properly?

If we don't correctly mark the media we handle, we run the risk of unintentionally disclosing sensitive or confidential data. Mislabeled, unlabeled, or mishandled media can result in an accidental DPS data breach which could have been avoided with more care and attention given to data classification and media marking.

If you are unsure of the data classification for specific data, and therefore unsure how to properly mark that data, you'll want to check with your Division leadership. As always, the Cyber Security Risk Management team is here to help with these discussions and can provide guidance in this area so don't hesitate to reach out with questions or concerns.

*Note on USB drives – users should only be using DPS-approved USB drives, and these should remain physically secure and never be plugged into non-DPS machines.

Credential Harvesting

Credential harvesting, also known as password harvesting, is the process of gathering valid usernames, passwords, private emails, and email addresses through breaches. Though this can be done through various malicious methods, phishing is the most common scheme.

We've seen these types of phishing emails here at DPS so it's important to be aware of what these look like. There's no easier way for a hacker to steal your password than to just ask you for it.

Here's how it typically happens:

1. **The hacker sends a phishing email.**

   As we've discussed, fear and intrigue are often used as a distracting motivator, and the topic is something that we can relate to. Expect to see logos and important titles. There may also be a deadline in the message, since we're more apt to act without thinking if we're rushed.

2. **You're encouraged to click on a link and perform a task.**

   As mentioned above, you're encouraged to act quickly in order to resolve some sort of issue. Honestly, this would be a good place to stop and reread the email and assess its validity. Need help? Send it over to SPAM@dps.texas.gov, and we'll take a look at it for you.

3. **The link takes you to a web page.**

   Much like the phishing email, the web page will look legitimate. The truth is, however, that one of the first steps a hacker has to take to set up these elaborate phishing schemes is to make a replica of a real website to draw you in even further. Unfortunately, behind what looks like a legitimate site, lurks a malicious website, and the hacker's server which captures any information you type into the password fields.

4. **You're tricked into entering your email address and password.**

   You'll likely see a short message and be encouraged to sign-in using your email address and password.

5. **The hacker retrieves your password from his server.**

   The fake webpage might be a clone of something legitimate, but the back end of it is set to send information right to the hacker. Often, you're redirected to a legit website after submitting your credentials to further distract you from the hack. You go on with your day, unaware you just handed over your username and password.

6. **The hacker exploits your harvested credentials.**

   Once they have them, cybercriminals can use your harvested credentials in a number of ways including gaining access to anything from personal bank records to employer files, and using your email address to trick your family and friends and coworkers into surrendering important company data, banking access or private information. Your credentials can also be sold on the dark web for others to use at will.

As with any phishy email, be wary of links and attachments, especially when asked to perform an action. And never provide usernames, passwords, or personal information to any unsolicited request. Don't make it that easy for hackers!

In the News

Hey Alexa, Who Am I Messaging?

(Elizabeth Montalbano | December 23, 2020)

Research shows that microphones on digital assistants are sensitive enough to record what someone is typing on a smartphone to steal PINs and other sensitive info.

The potential for digital-home assistants like Amazon Alexa to infringe on user privacy by making and saving voice recordings of them is already widely known. Now researchers have discovered that the devices also may be able to "hear" and record what people are typing on nearby smartphones, even amid background noise.

The microphones on digital assistants are sensitive enough that they can record the taps people make on a mobile device when sitting up to a foot and a half away, according to a team of researchers from the University of Cambridge. The researchers constructed an attack in which they used this capability to identify PINs and text typed into a smartphone.

"Given just 10 guesses, five-digit PINs can be found up to 15 percent of the time, and text can be reconstructed with 50 percent accuracy," the team - Almos Zarandy, Ilia Shumailov and Ross Anderson—wrote in a paper published online, "Hey Alex, What Did I Just Type" [PDF].

The same group of researchers already had discovered ways that various forms of technology can potentially violate user privacy by engaging in what they call "acoustic snooping." Last year, they published research on how a smartphone app has the ability record the sound from its microphones and figure out from that what someone has typed, giving it the potential to steal PINs and passwords.

The new research also builds on previous research that found that voice assistants could record the typing of keys on a computer to determine someone's input, Anderson wrote in a blog post.

"We knew that voice assistants could do acoustic snooping on nearby physical keyboards, but everyone had assumed that virtual keyboards were so quiet as to be invulnerable," he wrote.

It turns out that they are not, researchers found. Because modern voice assistants like Alexa have two to seven microphones, they can do directional localization, just as human ears do but with even greater sensitivity, the researchers discovered.

"We assess the risk and show that a lot more work is needed to understand the privacy implications of the always-on microphones that are increasingly infesting our work spaces and our homes," they wrote.

Full Story: https://threatpost.com/hey-alexa-who-messaging/

A Few More Cyber News Stories:

Hackers Amp Up COVID-19 IP Theft Attacks
https://threatpost.com/hackers-amp-up-covid-19-ip-theft-attacks

A Google Docs Bug Could Have Allowed Hackers See Your Private Documents
https://thehackernews.com/2020/12/a-google-docs-bug-could-have-allowed.html

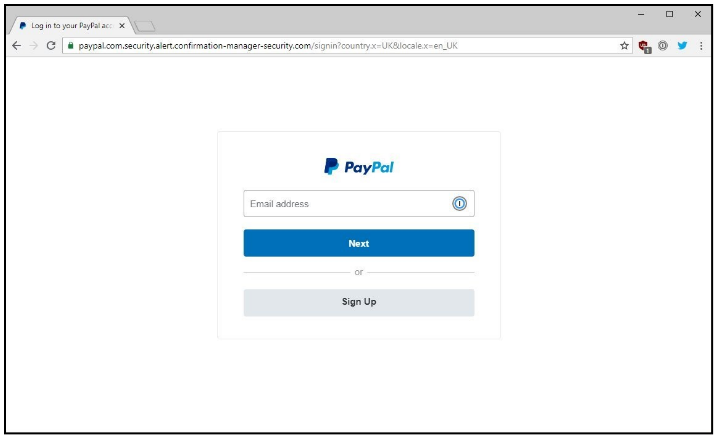
Hackers phish 615,000 login credentials by using Facebook ads
https://www.hackread.com/hackers-phish-login-credentials-with-facebook-ads

CYBER CHALLENGE

Spot the Fake Website

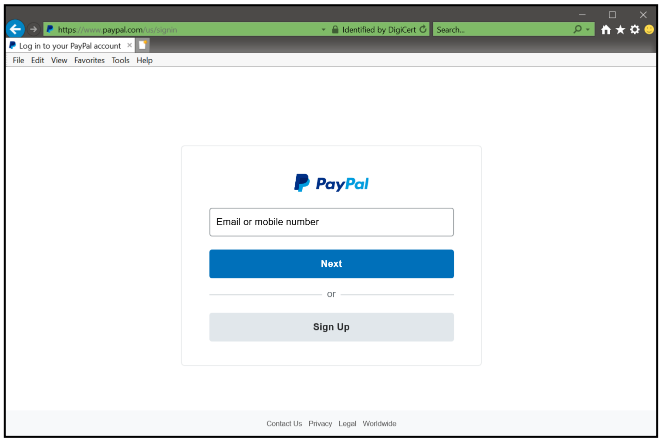
This Month's Challenge

For this month's challenge, I'd like to get back to some real-world practice. Fake logon pages were mentioned a few times in this newsletter. So let's practice identifying fake websites. Look these over (may have to zoom in), and let me know which of these isn't a legit website but a malicious clone. Maybe all of them are fake...



Log in to your PayPal acc

paypal.com.security.alert.confirmation-manager-security.com/signin?country.x=UK&locale.x=en_UK



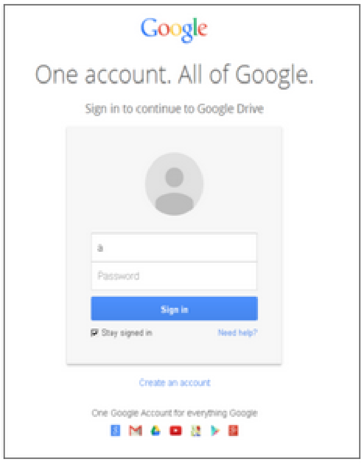
https://www.paypal.com/us/signin

Identified by DigiCert

Search...

Log in to your PayPal account

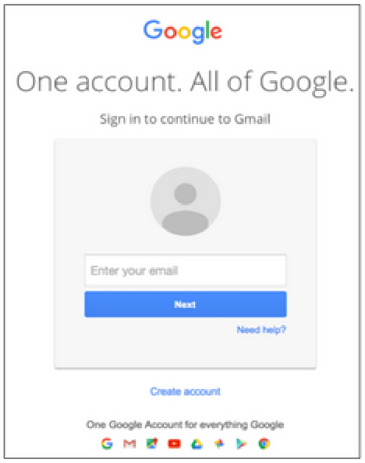
File Edit View Favorites Tools Help
PayPal
Email or mobile number
Next
or
Sign Up
Contact Us Privacy Legal Worldwide



Google

One account. All of Google.

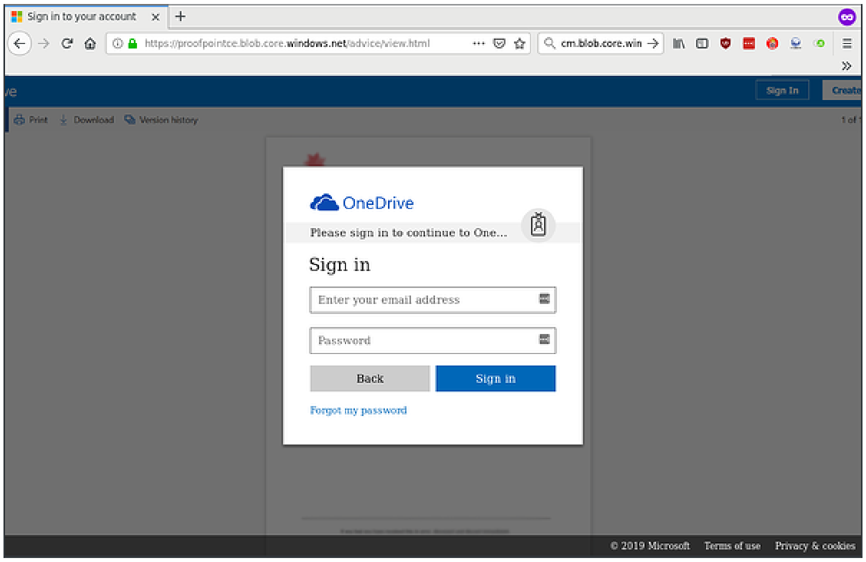
Sign in to continue to Google Drive



Google

One account. All of Google.

Sign in to continue to Gmail



Sign in to your account

https://proofpointce.blob.core.windows.net/advice/view.html

cm.blob.core.win

</Closing Comments>

As we close this month's newsletter, we'd like to give a quick shout out to those of you who took the time to take a guess with the last cyber challenge! We fully appreciate you taking a few minutes out of your day to engage with us! Please keep doing so; and get others to join you!

A big THANK YOU to all who emailed us!

I want to share this tongue-in-cheek video I saw during a Cyber Awareness summit recently. I hope you get a giggle out of it. I know this is how it must feel sometimes because this is how it feels for me sometimes, as well. Enjoy! (Clicking this picture should take you to YouTube.)

PLEASE STAND BY FOR A CYBER PARODY BROADCAST

I'm looking forward to this new year! Let's stay safe in 2021. And, as always, thank you for your cyber vigilance!

- Eric Posadas