PWNED Transcripts – Season 2 – Episode 4 – TTPs for COVID-19 Threats

This is Pwned the weekly podcast for cybersecurity professionals. We answer your cybersecurity questions and share stories from the trenches about how security professionals' engineers and CISOs are protecting their organizations. Pwned as always is brought to you by NuHarbor Security, your end to end provider of security services and security solutions if you're looking for complete cyber security protection for your business and a security partner that actually gives a BEEP visit us at www.nuharborsecurity.com

This is Justin Fimlaid and I am your host of Pwned. Today we are talking about TTP s and COVID. Now, TTP stands for tactics, techniques and procedures. So, you can think of this as the fingerprint of a specific attacker or certain signature that exists that would identify said attacker. Security researchers and security analysts use TTP to identify nefarious actors within an Event Stream. So TTP is really just a fancy way to describe the actions and activities that a potential nefarious actor would be using or is conducting in order to carry out an attack. So, a case in point, or an example might be if you have an Iranian hacktivist group, they would have certain TTP that are indicative of a certain type of attack or a specific threat actor who's carrying out the attack. security analysts will use these TTP across a large data set or series of events to try to identify which event is being carried out by which actor which subsequently could indicate remediation activities that could occur to prevent the attack from proliferating further. So with the recent pandemic and everything that's been going on, you would imagine that there are many threat actors within the marketplace today or within our industry today that are trying to capitalize on the COVID-19 or Coronavirus news or activity in order to conduct either hacking attempts or try to scam organizations out of money.

As of February, of this year, the number of COVID 19 related domain creations is averaging between 500 and 700 new domains a day to carry out these types of attacks. And so basically what this means is that any URL that might contain a combination of COVID 19, COVID, COVID news, Corona virus, Corona virus help or any derivation of something like that is being registered as a new domain and attackers are using these to gain trust of users who might be honestly looking for news or information related to the pandemic. Now within our security operations center today at NuHarbor, we track a whole host of TTP. related to the COVID virus, or the COVID-19 pandemic and the corona virus, the number of TTP s that are currently in the marketplace today is so numerous to go through all of them here is going to be too many. So what we'll do is we'll include the TTP within the show notes so that if you're listening to this, you can go back to our show notes and collect the TTP either for your own self edification, or if you're running a security operation center or MSSP, you can pull in this information and hopefully it helps out your operations as well. Some of the more common TTP or some of the more nefarious ones I'll point out here So the first one I would highlight, there's been a large number of phishing emails primarily targeting Italian email addresses containing malicious Microsoft documents with embedded VBA macros that are being used to drop a trick bot exploit. Trick bot is a banking Trojan that can be used to steal victim's confidential information and drop additional malware. What we've been seeing from these emails is that the email subject line in most cases has a fixed subject line that actually has Italian text which I'll include in the show notes because I'm just gonna butcher the name here trying to re pronounce everything. But additionally, with this email, the intent to create credibility within the email is being authored by popular and well-known doctors who work in Italy but are employed by the WHO. Another common campaign that we We've been seeing his emails using the FedEx trademark in phishing attacks claiming to provide victims with information on global FedEx operations while the COVID-19 outbreak continues. These emails often will contain PDF files that are listed as customer advisories. And when the customer opens that PDF files, the victim becomes infected with the Loki bot malware. The next one I would choose to highlight here is also being used as a lure and what researchers suspect is a Mustang panda campaign. You're not familiar with some of these names within the security, security vertical. We do have creative names for our threat actors. But Mustang panda is suspected Chinese government linked threat actor group the fishing lure used in this campaign was actually a .rar file purportedly containing statements from being Vietnamese Prime Minister regarding Cova 19. The .rar file contains a dot link file that when open, the victim executes an executable via command line to run the malicious scripts contained within the link file. When the malicious script executes, a Word document with Vietnamese text will be displayed to the victims and ultimately, a DLL side loading technique is used to download and execute a malicious a malicious payload that creates a command and control server from that user's laptop, therefore effectively giving that threat actor continuous access to that user's PC. Once that threat actor has access to a user's PC, there's numerous types of attacks that could occur directly to that user either compromising files on that PC potentially compromising further credit Have that user also that PC could then become part of a larger bot network that would be controlled by that threat actor group to carry out other indifferent attacks on other users. The other TTP that I will include in the show notes comes from the North Korean Baby Shark malware.

Maybe my favorite because Baby shark is my daughter's favorite song. This malware claims to contain information on South Korea's response to the COVID 19 virus. That TTP includes malicious Microsoft Word documents that will drop malware on the user's machine when it's open. Today within the security industry, we've been seeing that the corona virus pandemic is being capitalized on by threat actors and is being weaponized as a way to spread spyware and various Types of malware by all kinds of nation state actors from North Korea to Iran to various Russian threat actors. And the breadth of attacks span everything from email phishing attacks, to crafting nefarious URLs and capitalizing on internet and news watering holes for victims looking for information on the Cova or Corona virus. So at this point, looking forward in the outlook for these types of attacks in these TTP in my opinion will be relatively short lived, but we can expect to see them for the next few months and especially for as long as the pandemic continues to go on. And news of treatment starts to come forward about potential cures for this virus. So if you are an organization trying to figure out how to protect your company, In your users from these types of attacks, there's a few things that you can be doing on your side and there's some actions that you can be taking to mitigate the risk. The first thing that you can be doing as an organization is to be educating your users to be vigilant and be on the lookout and somewhat skeptical of COVID 19 or coronavirus news. The other thing that can be done for those organizations that leverage outsource security operations centers, or MSSP. Ask your security operations center or your MSSP what they're doing to capture t TTP in order to protect your organization. And then lastly, if you operate your own security operations center, look to this episode show notes to capture some of the T TTP that you can import into your own security operation center. So if you are an organization or user at an organization, who finds themselves in a situation where you think You might have been compromised by one of these attacks, whether it's a phishing attack or you have known command and control coming off of your network, if you do not have the expertise in house to correctly investigate and quarantine these types of attacks, it's important that you reach out to a trusted security partner for help in order to mitigate the most amount of risk to your organization. And if you're looking for a trusted security partner with the expertise to help you out NuHarbor security can and will be your trusted security partner to guide you through the investigation and remediation of these types of events. Please visit us at www.nuharborsecurity.com. This was Justin Finland and I'm here host of Pwned. Thank you for listening. Next week we'll be touching on artificial intelligence and whether it's helping our security industry or it's just marketing fluff