On April 29, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Autodesk, Google, and Adobe products.

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

01 May 2020 – Workers day edition

In The News This Week

Shade (Troldesh) ransomware shuts down and releases decryption keys

The Shade ransomware gang have published more than 750,000 decryption keys on GitHub. The operators of the Shade (Troldesh) ransomware have shut down over the weekend and, as a sign of goodwill, have released more than 750,000 decryption keys that past victims can now use to decrypt their files. Security researchers from Kaspersky Lab have confirmed the validity of the leaked keys and are now working on creating a free decryption tool. In a short message posted in a GitHub repository, the Shade team explained what led to their decision. "We are the team which created a trojan-encryptor mostly known as Shade, Troldesh or Encoder.858. In fact, we stopped its distribution in the end of 2019. Now we made a decision to put the last point in this story and to publish all the decryption keys we have (over 750 thousands at all). We are also publishing our decryption soft; we also hope that, having the keys, antivirus companies will issue their own more user-friendly decryption tools. All other data related to our activity (including the source codes of the trojan) was irrevocably destroyed. We apologize to all the victims of the trojan and hope that the keys we published will help them to recover their data."
While the Shade gang explained why they released the decryption keys, they did not explain why they shut down. Several theories have started to form among ransomware experts, yet none are based on actual tangible threat intelligence. Read the full story by Catalin Cimpanu here: ZDNet Article 1

Hackers Hijack Microsoft Teams Accounts Using a Single Weaponized GIF Image

Microsoft has patched a subdomain takeover vulnerability in Microsoft Teams that affects every user who uses the Teams desktop or web browser version. Microsoft Teams is a leading communication and collaboration platform that combines workplace features such as chat, video meetings, file storage, collaboration on files, and integration with applications. Researchers from CyberArk discovered a worm-like vulnerability that lets hackers use a malicious GIF file to scrape user data and to take over the entire roster of Teams accounts. The vulnerability resides in how the application programming interfaces (APIs) used to validate the communication between the client and the server. Read the full story here: GBHackers

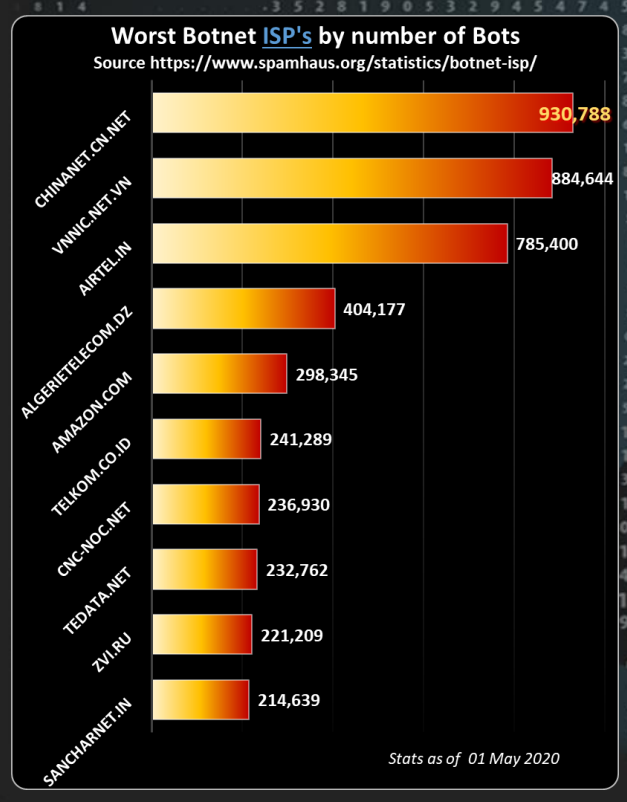
New Android Malware Targets PayPal, CapitalOne App Users

An Android mobile malware has been uncovered that steals payment data from users of popular financial apps like PayPal, Barclays, CapitalOne and more. The infostealer, called EventBot, has targeted users of more than 200 different banking, money-transfer services and general cryptocurrency wallet apps. First identified in March 2020, EventBot is still in early development – but researchers warn that it's rapidly evolving with new versions being released every few days. "EventBot is particularly interesting because it is in such early stages," said experts from Cybereason, in a Thursday analysis. "This brand-new malware has real potential to become the next big mobile malware, as it is under constant iterative improvements, abuses a critical operating system feature, and targets financial applications." Read the article by Lindsey O'Donnell here: ThreatPost

News snippets from the past - Computers & crime

'Virus' sends computers down across the country – November 1988

The following news snippet was found in the Beaver County Times , November 4 1988 - SAN JOSE. Calif. – An electronic "virus" set loose in a network of research computers swept across the nation Thursday, forcing computers to shut down at major universities and defences agencies from Silicon Valley to Harvard Square. The virus, which experts were calling the most widespread assault ever on the nation's computers used electronic messaging systems to "mail" itself from one computer to another and then replicated itself repeatedly in its unwilling hosts. Read the story here: GoogleArchives



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

The anatomy of a Phishing Attack?

Phishing comes in many forms and the general user hear the words "beware of phishing attacks" much too often from the communications or cyber security departments but do they really know what it is and how it works? I believe that we as security practitioners quite often warn our users of a specific threat but we fail to tell them what it really is and how it works. Below is an adapted and shortened version of an article written by Josh Fruhlinger of CSO that gives a layman's perspective on Phishing.

What is phishing? How this cyber attack works and how to prevent it

Phishing is a method of trying to gather personal information using deceptive e-mails and websites. Here's what you need to know about this venerable, but increasingly sophisticated, form of cyber-attack.

Phishing definition

Phishing is a cyber-attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment. What really distinguishes phishing is the form the message takes: the attackers masquerade as a trusted entity of some kind, often a real or plausibly real person, or a company the victim might do business with. It's one of the oldest types of cyberattacks, dating back to the 1990s, and it's still one of the most widespread and pernicious, with phishing messages and techniques becoming increasingly sophisticated. "Phish" is pronounced just like it's spelled, which is to say like the word "fish" — the analogy is of an angler throwing a baited hook out there (the phishing email) and hoping you bite. The term arose in the mid-1990s among hackers aiming to trick AOL users into giving up their login information. The "ph" is part of a tradition of whimsical hacker spelling, and was probably influenced by the term "phreaking," short for "phone phreaking," an early form of hacking that involved playing sound tones into telephone handsets to get free phone calls.

Nearly a third of all breaches in the past year involved phishing, according to the Verizon Data Breach Investigations Report. For cyber-espionage attacks, that number jumps to 78%. The worst phishing news for 2019 is that its perpetrators are getting much, much better at it thanks to well-produced, off-the-shelf tools and templates.

What is a phishing kit?

The availability of phishing kits makes it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns. A phishing kit bundles phishing website resources and tools that need only be installed on a server. Once installed, all the attacker needs to do is send out emails to potential victims. Phishing kits as well as mailing lists are available on the dark web. A couple of sites, Phishtank and OpenPhish, keep crowd-sourced lists of known phishing kits. Some phishing kits allow attackers to spoof trusted brands, increasing the chances of someone clicking on a fraudulent link. Akamai's research provided in its Phishing--Baiting the Hook report found 62 kit variants for Microsoft, 14 for PayPal, seven for DHL, and 11 for Dropbox. The Duo Labs report, "Phish in a Barrel", includes an analysis of phishing kit reuse. Of the 3,200 phishing kits that Duo discovered, 900 (27%) were found on more than one host. That number might actually be higher, however. "Why don't we see a higher percentage of kit reuse? Perhaps because we were measuring based on the SHA1 hash of the kit contents. A single change to just one file in the kit would appear as two separate kits even when they are otherwise identical," said Jordan Wright, a senior R&D engineer at Duo and the report's author.

Anatomy of a Phishing Kit

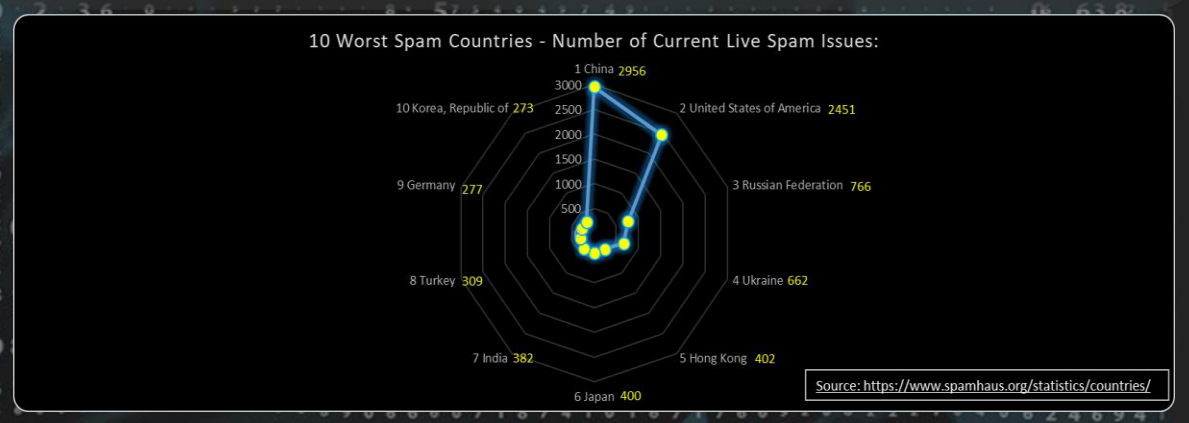
Before we dive into the results, it is important to talk a bit about how phishing kits work. Following is the basic structure of the phishing attack. (1) The legitimate website is cloned → (2) The login page is changed to point to a credential stealing script → (3) The modified files are bundled into a zip file to make a phishing kit → (4) The phishing kit is uploaded to the hacked website , files are unzipped. → (5) Emails are sent with links pointing to the new spoofed website.

Analysing phishing kits allows security teams to track who is using them. "One of the most useful things we can learn from analysing phishing kits is where credentials are being sent. By tracking email addresses found in phishing kits, we can correlate actors to specific campaigns and even specific kits," said Wright in the report. "It gets even better. Not only can we see where credentials are sent, but we also see where credentials claim to be sent from. Creators of phishing kits commonly use the 'From' header like a signing card, letting us find multiple kits created by the same author."

Types of phishing

If there's a common denominator among phishing attacks, it's the disguise. The attackers spoof their email address, so it looks like it's coming from someone else, set up fake websites that look like ones the victim trusts, and use foreign character sets to disguise URLs. That said, there are a variety of techniques that fall under the umbrella of phishing. There are a couple of different ways to break attacks down into categories. One is by the purpose of the phishing attempt. Generally, a phishing campaign tries to get the victim to do one of two things:

- Hand over sensitive information. - These messages aim to trick the user into revealing important data — often a username and password that the attacker can use to breach a system or account.
- Download malware. - Like a lot of spam, these types of phishing emails aim to get the victim to infect their own computer with malware.
- Spear phishing - When attackers try to craft a message to appeal to a specific individual, that's called spear phishing. (The image is of a fisherman aiming for one specific fish, rather than just casting a baited hook in the water to see who bites.)
- Whaling - Whale phishing, or whaling, is a form of spear phishing aimed at the very big fish — CEOs or other high-value targets.



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com