On April 22, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco products.

Correction: Last week I stated in paragraph 7 of the CCTV article there is one camera installed for every 4.1 people in China and In the U.S. there is one camera for every 4.6 people. This figures should be the other way around, 4.6 for China and 4.1 for the US.

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

24 April 2020

In The News This Week

Apple iPhone at risk of hacking through email app

A flaw in Apple's mobile operating system may have left millions of iPhone and iPad users vulnerable to hackers. Research published by ZecOps, a mobile security firm, said a bug in the Mail app made devices susceptible to sophisticated attacks. The firm said it had "high confidence" the bug has been used to exploited at least six high-profile victims. An Apple spokesperson told Reuters a fix would be included in upcoming software updates. ZecOps reported the bug to Apple in March. The tech giant had not previously known about the issue. To exploit this flaw, hackers would send a seemingly blank message to an iPhone or iPad users Mail account - the email app on iOS devices. When the email was opened it would crash the app forcing the user to reboot. During the reboot, hackers would be able to access information on the device. What makes this attack different from other hacks is users do not need to download any external software or visit a website that contains malicious software (malware). Typically hacks require some action on the part of the victim - those steps make possible to trace the origin of the attack.
Read the full story here: BBC News

DForce hacker returns $25m in 'stolen' crypto-currencies

A mystery hacker allegedly stole $25m (£20m) in crypto-currencies - and then returned the funds two days later. Records show that funds in a variety of crypto currencies were withdrawn from the DForce platform based in China. A sum of $10m was taken in Ethereum, for example, while a further $10m was taken in digital coins tied to the US dollar and $4m in other coins. Roughly the same amount has now been returned - although in a different mix of crypto-currencies. DForce is an online service that allows users to make crypto-currency transactions with one another. "The hackers have attempted to contact us and we intend to enter into discussions with them," wrote DForce founder Mindao Yang in a blog shortly after the attack happened, on Sunday."
Read the full story here: BBC News

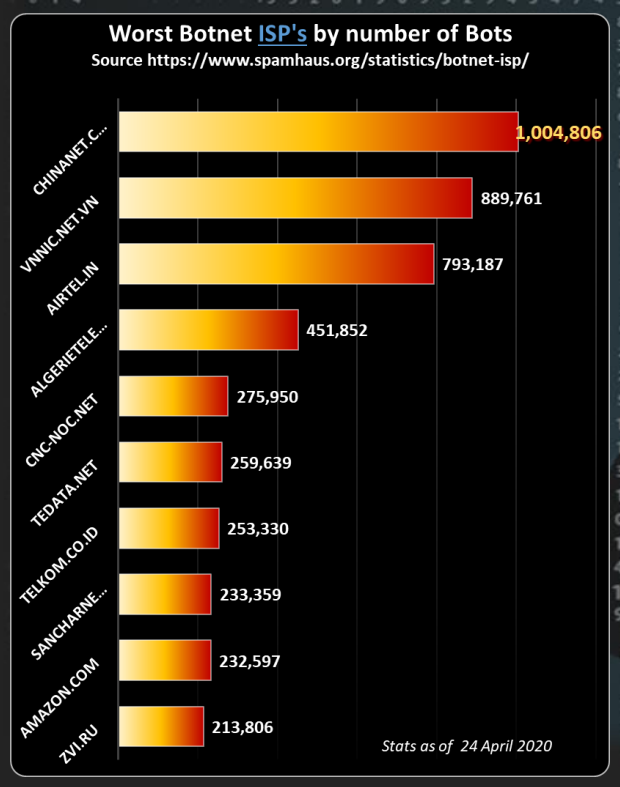
WHO confirms credentials leak included staff working on COVID-19 response

The World Health Organization (WHO) said the recent leak of 450 active WHO email addresses and passwords along with credentials of thousands working on the response to the coronavirus pandemic didn't put the organization's systems at risk. Explaining that its systems were largely spared because "the data was not recent," WHO said in a release that "the attack did impact an older extranet system, used by current and retired staff as well as partners." Credentials from WHO, the CDC and Gates Foundation recently started making their way onto the likes of 4chan, Pastebin and Twitter, with the latter taking steps to remove them earlier this week"
Read the full story here: SC Magazine

News snippets from the past - Computers & crime

Teen is charged with Internet fraud – May 1995

The following news snippet was found in The Free Lance-Star, Fredericksburg, Virginia, May 3, 1995
Salt Lake City (AP) – A 15-year-old boy has been charged in a bogus Internet merchandising scheme that authorities say brought him at least $10,000. He opened right up to us. He said 'Here take my computer. Every time I get on it, I get into trouble," Jeff Robinson, and investigator for the Utah County prosecutor, said Tuesday. County and state officials arrested the youth Monday. His name was not made public because of his age. The youth received at least $10,000 from up to 15 people around the country who responded to his Internet ads for low-cost computer-related items such as memory chips, authorities said. Buyers received nothing, or accepted delivery of C.O.D packages containing worthless materials. Read the full story and more here: GoogleArchives



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

Email spoofing – how easy is it?

In November 2018, I touched on this very topic but I decided to talk about it again as the number of spoofing emails skyrocketed since the beginning of the Corona pandemic. As we read last week, scammers are sending millions of hoax emails, masquerading as official Covid-19 communiqué and spoofing the World Health Organization (WHO) and local health authorities. And, since everyone is anxious to know what is happening around the world regarding the virus, 90% of the users fall for it. Nowadays, there are even better resources available and I found a comprehensive guide by Simon Hall from 'digital shadows' called SECURITY PRACTITIONER'S GUIDE TO EMAIL SPOOFING AND RISK REDUCTION that really go into the nitty gritties of spoofing. Below is an adapted and shortened version but if you want to go a bit deeper into the technical side of it, please go and read the full guide.

For as long as there have been electronic communications, or any communications for that matter, there have been people attempting to intercept or impersonate the sender and the message. Back in the Roman Empire that involved faking seals on the backs of letters. In the modern day, it's all about spoofing the "From" address in an email. Email spoofing has been around for a long time and it's still going strong, flooding inboxes and spam folders with the usual malicious documents or links to a landing page cloned from a legitimate service.
Spoofing an email is a relatively easy process: all it takes is for the attacker to create, compromise or find a Simple Mail Transfer Protocol (SMTP) server that allows the forger to send the spoofed emails.
In order to understand spoofing in more detail, we should first look at what an email in composed of.

ANATOMY OF AN EMAIL

You can think of an email in the same way you would an old-fashioned letter. Just as that letter would need to be addressed to a specific person and/or location, so too do emails.

		Email	Postal Letter - Formal
Envelope		MAIL FROM: sender@origin.xyz	To: recipient + address
		RCPT TO: recipient@domain.xyz	Return Address: sender + address
Content		To: Recipient	To: Recipient
		From: Sender	From: Author
		Subject: Document Title	Title: Document Title
		Date: Date of Writing	Date: Date of Writing
		Body: Message content, often text or HTML	Body: Letter content

As you can see, postal letters and emails have very similar structures, aside from, perhaps, the return addresses. When an email is sent from your email client of choice, the process is generally the same. You provide the To, From, Subject and Body, and the client application will then deal with the rest.

(1) A connection will be established to your email provider's SMTP (Simple Message Transfer Protocol) server. (2) The client will introduce itself with a simple hello (HELO/EHLO) along with the clients fully qualified domain name (FQDN). (3) While the HELO message can be pretty much anything, most mail servers will check that the FQDN exists and has Mail Exchange (MX) DNS records associated. If not, it may reject or affect the reputation of the mail sender address.
Sending the content is straightforward and achieved with three commands. The first two commands are part of the envelope detailing where the email needs to go.
(1) MAIL FROM: sender@origin.xyz, (2) RCPT TO: recipient@domain.xyz (3) DATA
The next commands detail any information to be populated inside the envelope (The letter), which will contain, To, From, Subject, Date, and other headers. The end of the DATA section is identified by a line containing a single period.

SPOOFING

For an email to be spoofed, it is as simple as changing the from email address on the envelope. As an example, if you were to replace the "MAIL FROM" value with a different sender email address, and populated the required commands and headers, you have yourself a spoofed message. The most common mail providers implement measures that allow the recipient to check where the MAIL FROM domain should originate from, such as SPF (Sender Policy Framework). Spoofing really is as simple as that. For example, the recent sextortion campaigns spoofed the recipient email addresses to convince the recipient that the sender has control over their email. They are also often used to perform Business Email Compromise or CEO fraud, by spoofing the email address of a colleague or executive level member of the organization.

FINDING A SERVER THAT ALLOWS ANYONE TO SEND AN EMAIL

If the forger is looking for mass-distribution, then Open Relay servers would be the likely choice. Simple misconfigurations of SMTP servers often leave them open to allow anyone to connect without authentication and to specify the "To" and "From" addresses, as well as the content and any other fields they want to populate.
By looking at Shodan we can identify more than 6,000,000 SMTP servers; while not all of these will allow Open Relay, the amount that do would surprise you. These can be pretty ephemeral too. Quite often you will find that a development or staging servers are deployed with default or weak SMTP service configurations leaving them open to abuse. Threat actors will often scan for these open relay services, validate them, and then share them publicly or trade them on forums. The attacker now has a large list of servers that they can send their spoofed emails through.

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