On March 28, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Mozilla, and WordPress products. This alert level still remains.
On April 16, 2019 an advisory were released for Oracle Quarterly Critical Patches

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
19 April 2019

In The News This Week

Ecuador Claims It's Been Hit With 40 Million Cyberattacks Since Giving Up Julian Assange -

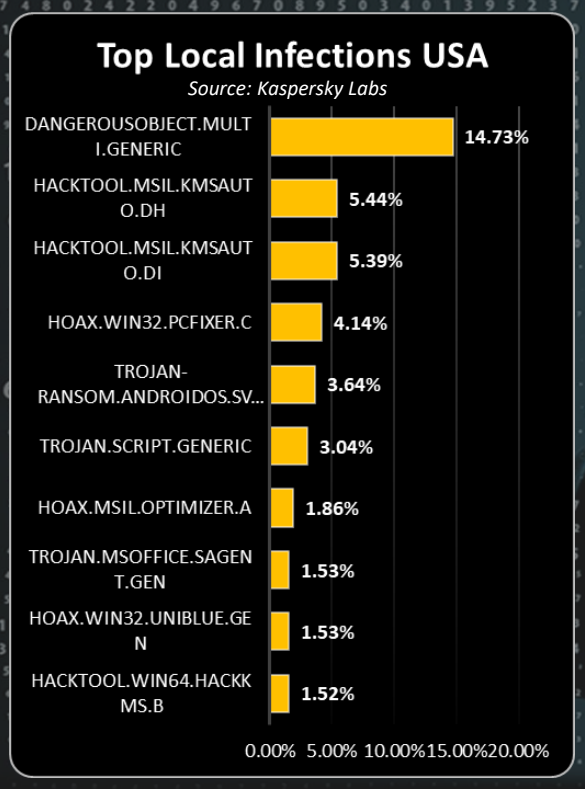
Ecuadorian officials claim the country has suffered some 40 million cyber attacks since it allowed UK police to forcibly remove Wikileaks founder Julian Assange from their embassy in London, according to Agence France-Presse. According to AFP, the 40 million number comes courtesy of Ecuador's deputy minister for information and communication technologies, Patricio Real, who said the attacks began shortly after the arrest on April 11. Patricio Real said the attacks, which began on Thursday, had "principally come from the United States, Brazil, Holland, Germany, Romania, France, Austria and the United Kingdom," as well as from the South American country itself. Javier Jara, undersecretary of the electronic government department of the telecommunications ministry, said the country had suffered "volumetric attacks" that blocked access to the internet following "threats from those groups linked to Julian Assange."
Volumetric attacks are a type of distributed denial of service attack, in which attackers flood servers with requests in an attempt to overload them and prevent access by legitimate users; the 40 million number should be understood not as the number of independently coordinated attacks, but the cumulative number of automated attempts to disrupt targeted systems. Sites for the foreign ministry, central bank, President Lenin Moreno's office, tax authorities, and myriad other government websites were targeted, AFP wrote.
No institutions reported successful attempts to steal or destroy data, the news agency added.
Read the full story by Tom McKay here: GIZMODO

As Cyber Security controls get tighter crooks resort back to middle-of-the-night physical means to steal cash.

Over the past month, criminal gangs have been using diggers to break building walls and steal ATMs across Northern Ireland. Nine such incidents have happened in the recent past. Reports from Irish news sites say crooks steal nearby digging equipment, which they use to knock down building walls, scoop the ATMs in the diggers' cups, and then place it in the back of a truck or van that had its roof cut off. The gangs involved in these attacks flee the scenes in their trucks and vans, leaving the digger behind. Attacks, some of which have been recorded on CCTV cameras, last no more than a few minutes, giving crooks enough time to escape before police arrive on the scene. See the videos and read the full story here: ZDNetArticle

Cyber-security firm Verint hit by ransomware

In an extreme case of irony, ransomware hits cyber-security firm - The Israel offices of US cyber-security firm Verint have been hit by ransomware, according to a screenshot taken by a Verint employee that started circulating online on Wednesday. "There is currently a critical issue affecting the on premise Email and Green zone VDI [Virtual Desktop Infrastructure] services," read a warning message that was displayed earlier today on Verint employees' computers. "If you get a ransomware pop up, please turn off your machine immediately and notify The IT Help Desk. IT is working to contain and address the issue, including working with external resources. "We are working to have this addressed as soon as possible and will provide updates as appropriate," the internal warning message read. Multiple sources have told ZDNet the incident is real, and that FireEye's Mandiant incident response team is on-premise to help with recovery efforts. Verint confirmed the incident to Israeli news sites The Marker, Calcalist, and Globes. "The company's defense system identified the attack immediately after it began," a Verint spokesperson said, "and carried out the activity required to thwart it." Read the full Story here: ZDNetArticle (2)



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

Cybersecurity Ventures Reports:
The number of connected devices on the Internet will exceed
50 billion
by 2020 according to Cisco

How does Cyber Honeypots work?

If you've ever had an ant problem in your home, it's likely that you've used ant traps. Ants are attracted to food high in carbohydrates, especially sugary stuff. Ant traps work because they contain bait that lures ants in. So, they might go for your ant trap rather than the cookie crumbs you dropped on the kitchen floor. When used properly, the trap allows you to kill ants before they infest your home.

Honeypots in computer networks use the same concept. Cyber-attacks travel through the internet to private computer networks constantly. What if you could put something in your network that will attract attacks, so you can catch them before they hit your important server and client machines?

How do you use the honeypot concept for your network? So, you want to set up something on your network that looks like an attractive computer to attack. Should you just install Windows 3.1 on a legacy machine, make sure its TCP/IP interface has basic functionality, and plug an Ethernet cable into it? No, that would be a terrible idea. Ideally, a honeypot should resemble a computer on your production network, but with weaker security. In the long run, it's probably better to make your honeypot a virtual machine. These are easier to maintain and are more scalable. You can tinker around with the virtual hardware specs more easily, and experiment with different amounts of memory and CPU cores. Plus, because virtualization sandboxes your honeypot OS from its host machine, allowing you to contain the effects of cyber-attacks more effectively. Did your virtual machine honeypot get infected with ransomware? Just delete it and its virtual disk from your VM client and make a new one!

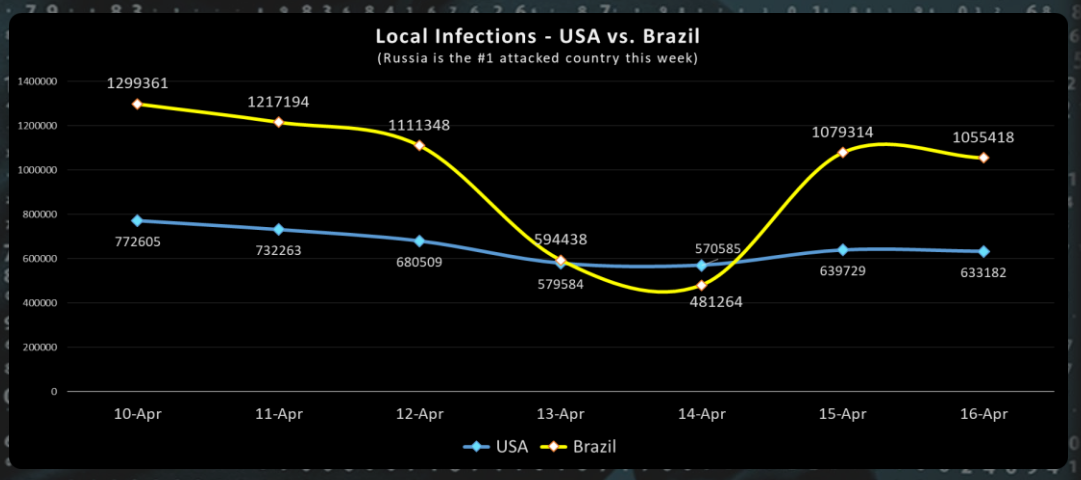
Install your honeypot on virtual machines from the same disc images you use to install operating systems in your production network. Configure them in much the same way, with the same drivers and applications. Just make the security a bit weaker than your information security policy requires. Make fake accounts that are local to your honeypot and create weak passwords. Be sure that your honeypot doesn't automatically install security patches and make the most recently installed patches a few months old. Configure its local firewall to have more open TCP/IP ports, and fewer filtered ports altogether. Leave more of the default OS and application settings. That way, if an attacker OS fingerprints your honeypot, they can try exploiting some vulnerabilities that have been known for a long time. Or not.

The basic principle of making your honeypot like your production machines, but less security hardened, should be maintained in most situations. But all the other details may be tweaked and modified according to your specific needs. Whatever configuration and set up is best may take some experimentation to determine. A good honeypot will allow you to understand what sort of cyber-attacks your production machines may face. Having a honeypot that teaches you about malicious network activity will likely take you some trial and error.

Your honeypot must also be set up so that it constantly generates logs on every applicable function. At the very least you should make sure that its OS system logging works and there should be constant logging on its built-in software firewall. If you use some sort of antivirus software in your honeypot, its logs are important as well. You can then run all those logs through a SIEM, just like all the other logs your network generates.

The next question is, where should you put your honeypots? Putting a honeypot outside of your DMZ and toward the internet is a popular option. That's an excellent location for watching external cyber-attacks on your network. You probably don't want to put a honeypot inside your DMZ, because attacks to your DMZ can have terrible consequences. You should also consider putting a honeypot on the other side of your DMZ, in a location that's accessible to users in your private network. As long as you make sure as few employees and contractors know about the internal honeypot as possible, it can be an effective way to catch and analyse internal as well as external attacks. Internal attacks are a big deal. According to IBM's 2016 Cyber Security Intelligence Survey, about 60% of cyber-attacks are done by insiders.

Adapted from an article by KIM CRAWLEY which you can find here: AlienVault



Author: Chris Bester