On June 19, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in Mozilla Thunderbird and Firefox 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

28 June 2019

In The News This Week

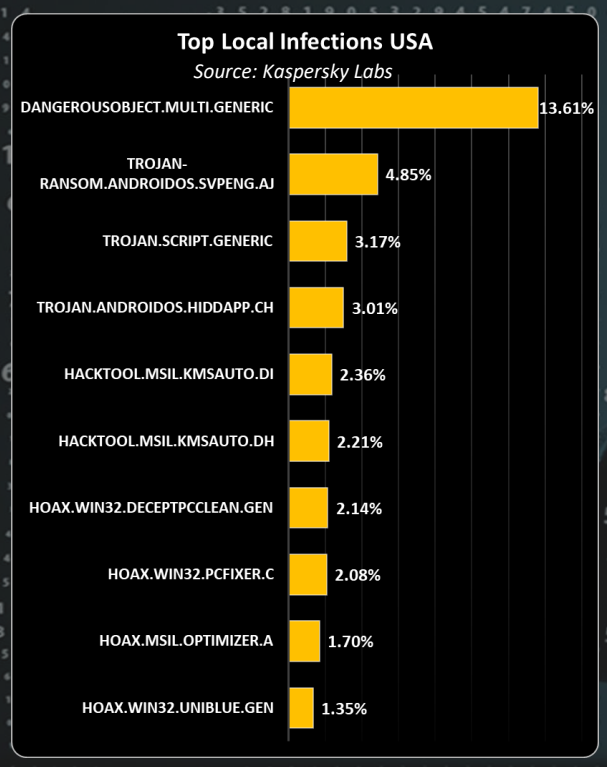
Raspberry Pi hack puts NASA in security jam.

It was revealed this week that a low-cost, barebones computer that can fit in your palm left NASA open to a cyberattack, according to a recent audit report by the space agency. In April 2018, NASA's Jet Propulsion Laboratory discovered that a hacker was able to gain access to one of its "major mission systems" by targeting an unauthorized Raspberry Pi computer that was attached to the JPL network. The Raspberry Pi hack went undetected for 10 months, according to the NASA Office of Inspector General, and the perpetrator stole 500 MB of data from 23 files. Two of those files contained information on the transfer of restricted military and space technology related to the Mars Curiosity Rover mission, according to the June audit report. The JPL is dedicated to robotic spacecraft construction. While the intruder has evaded authorities, the audit report highlights that other devices were also attached to the network without NASA's knowledge. But none of the other devices have been marked as a security risk or an "advanced persistent threat," a term usually meant for nation-state hacking groups. Because of the hack, NASA stopped some of its agencies from using a core gateway due to fear that the hacker could harm currently active spacecraft." You can find the Nasa Audit report here NASA-OIG-REP and the story here: c|net Article

Hackers broke into 10 telecoms companies to steal customers' phone records.

Researchers at Cybereason say a nation-state-backed intelligence operation has compromised at least 10 global telco companies - to such an extent the attackers run a "de facto shadow IT department". A nation-state-backed hacking operation of Chinese origin has been targeting global telecommunications providers for a number of years, with cyber attackers gaining access to call data records, the geolocation of users and other information about hundreds of millions of people. The campaign is thought to have impacted at least ten telecommunications operators around the world and has been uncovered by security researchers at Cybereason after they began investigating suspicious activity on a customer's network last year. "Someone was actually active in the network, going from computer to computer stealing credentials and siphoning out what can only be described as an insane amount of data – hundreds of gigabytes of data. Amit Serper of Cybereason said "The hacking campaign – dubbed Operation Soft Cell – had compromised the IT infrastructure of the investigated target to such an extent that it could be described as the "de facto shadow IT department of the company". The attackers had even set up their own VPN and at least ten different accounts with administrator privileges, providing access to vast swathes of data and potentially the ability to shut off the network. Affected targets have been identified in Europe, Africa, the Middle East and Asia, and it's believed the campaign has been active since at least 2017 – if not before. However, despite having the networks of telecommunications providers around the globe in their hands, the attackers appear to be focused on gaining access to information about specific individuals who researchers describe as high-value targets. About 20 likely targets have been identified since Cybereason first began the investigation. That information syphoned off was metadata related to who they're calling, the time and duration of calls, along with information about who they're texting and when. The metadata also provides attackers with the ability to track the user, because their geolocation is revealed by the cellular towers they connect to during the day. "This is basically attacking without hacking – they're attacking the telcos for strategic assets. It's an access operation: they want to gain access to a never-ending fountain of intelligence and data. And they can do it all without touching the victim's phone," Serper he said.

Read the full story here: ZDNet Article



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

According to ComputerWeekly
The InfoSec Market is expected to grow 8.7% in 2019 to
$124bn

Raspberry Pi in the news – What is it?

As the humble Raspberry Pi Single Board Computer is in the news this week as a hacking device, many of you, who are not familiar with these little critters, are probably wandering what the heck it is. Well, as the name Single Board Computer or SBC suggest, it is a complete "little" computer built on a single circuit board, with microprocessor(s), memory, input/output (I/O) ports and other features required of a fully functional computer. It is highly popular in the robotics fraternity since most of the popular brands are just about the size of a credit card and you can program it to do almost anything and control things like little servo motors, sensors, cameras and even other computers, and its cheap, anything from about $20 upward. There are many available but some of the more popular brands are; Arduino, Raspberry Pi, Beagleboard etc., some more sophisticated than others. About a year and a half ago I bought my 12 year old son (then 10) an Arduino starter kit as he got bored with the Lego robotics class he attended and since then he build numerous little contraptions to "scare" his dad and so on. An ex colleague of mine is building 3D printers using an Arduino to control it and another colleague built an automatic fish feeder, just as an example of some of the things people get up to with these little things.

Now lets look more into the Raspberry Pi the NASA hackers used. The little Raspberry Pi is one of the first SBC's that came out and the latest models sports a quad-core 64Bit 1.4Ghz processer, 1 GB RAM, build in Bluetooth, Wi-Fi and a Gigabit Network Interface and many more features that makes it a powerful tool in the skilled hacker's arsenal. Storage is via a Micro SD card which is now available in 512GB!, and it can run various Linux or Windows OS systems.

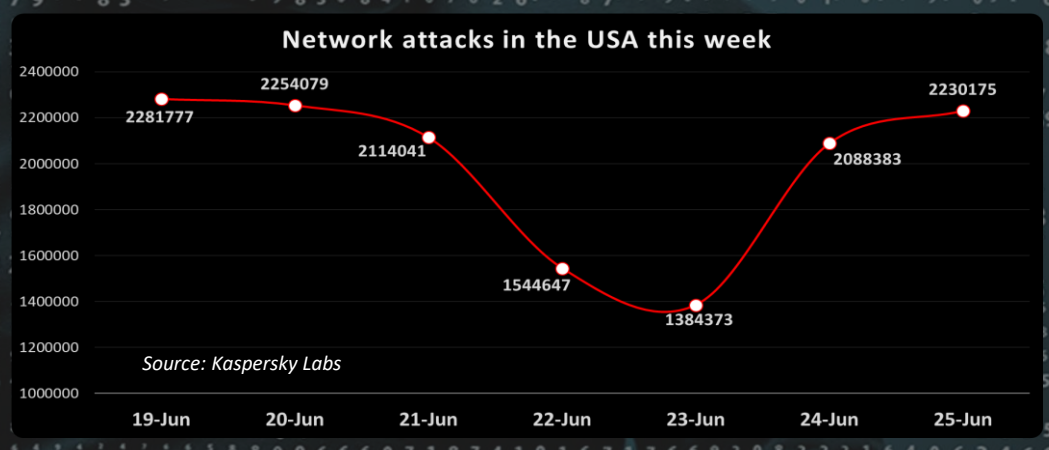
How did the hacker do it? It is speculated that he or she probably connected the Raspberry to the network with a standard Ethernet connection (behind the firewall on the internal network) onto it's network interface and then made use of It's Wi-Fi capabilities to gain access. The NASA audit report does not reveal details of exactly how it was done but it was left "hanging" there for over 10 months before it was discovered. The hacker had to have physical access to the computer room and facilities which begs the question of how did he or she get it through all the rigorous security checks and scans? Well it is so small that you could probably carry it in your briefcase in one of those small lead-lined film canister bags (for those of us who are old enough to remember them), and go through undetected as the X-ray scanner will only show it as a small solid object.

The possibilities of these little SBC's are endless and there are literally gazillions of programs available for download on the internet. So you don't even have to write the programs yourself, you can just download someone else's code and then just tweak it for your own purposes. Many of the IoT gadgets out there started their live out as an Arduino or Raspberry Pi project.

Now for us as cyber security practitioners, the versatility of these little things are scary, what will the crooks come up with next, and how will we stop them from breaking into our systems? But on the other hand, we can also jump on the bandwagon and use SBC's for our own security projects. You can build your own firewall, network alert system or video scanning system etc. As endless the possibilities are for the crooks, so are the possibilities for protecting yourself.

Check out how to build your own security box running Kali Linux on a Raspberry Pi: Pi Projects

Below are examples of the more popular Raspberry Pi and Arduino SBC's



Author: Chris Bester
chris.bester@yahoo.com