On August 2, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in Wind River and Google 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

09 August 2019

In The News This Week

AT&T employees took bribes to plant malware on the company's network.

DOJ charges Pakistani man with bribing AT&T employees more than $1 million to install malware on the company's network, unlock more than 2 million devices.

AT&T employees took bribes to unlock millions of smartphones, and to install malware and unauthorized hardware on the company's network, the Department of Justice said yesterday. These details come from a DOJ case opened against Muhammad Fahd, a 34-year-old man from Pakistan, and his co-conspirator, Ghulam Jiwani, believed to be deceased. The DOJ charged the two with paying more than $1 million in bribes to several AT&T employees at the company's Mobility Customer Care call center in Bothell, Washington.

OPERATING SINCE 2012 - The bribery scheme lasted from at least April 2012 until September 2017. Initially, the two Pakistani men bribed AT&T employees to unlock expensive iPhones, so they could be used outside AT&T's network. The two recruited AT&T employees by approaching them in private via telephone or Facebook messages. Employees who agreed, received lists of IMEI phone codes which they had to unlock for sums of money. Employees would then receive bribes in their bank accounts, in shell companies they created, or as cash, from the two Pakistani men. This initial stage of the scheme lasted for about a year, until April 2013, when several employees left or were fired by AT&T.

THE MALWARE STAGE - That's when Fahd changed tactics and bribed AT&T employees to install malware on AT&T's network at the Bothell call center. Between April and October 2013, this initial malware collected data on how AT&T infrastructure worked. According to court documents unsealed yesterday (6 Aug 2019), this malware appears to be a keylogger, having the ability "to gather confidential and proprietary information regarding the structure and functioning of AT&T's internal protected computers and applications. The DOJ said Fahd and his co-conspirator then created a second malware strain that leveraged the information acquired through the first. This second malware used AT&T employee credentials to perform automated actions on AT&T's internal application to unlock phone's at Fahd's behest, without needing to interact with AT&T employees every time.

In November 2014, as Fahd began having problems controlling this malware, the DOJ said he also bribed AT&T employees to install rogue wireless access points inside AT&T's Bothell call center. These devices helped Fahd with gaining access to AT&T internal apps and network, and continue the rogue phone unlocking scheme.

ONE AT&T EMPLOYEE MADE $428,500 - The DOJ claims Fahd and Jiwani paid more than $1 million in bribes to AT&T employees, and successfully unlocked more than two million devices, most of which were expensive iPhones. One AT&T employee received more than $428,500 in bribes over a five-year period, investigators said.

The DOJ said the two operated three companies named Endless Trading FZE, Endless Connections Inc., and iDevelopment. These companies were a front business for SwiftUnlocks, a website that let users unlock iPhones from their carrier network. Fahd was arrested in Hong Kong in February 2018, and extradited to the US on August 2, last week.
Read the full story by Catalin Cimpanu here: ZDNet Article

"Warshipping" – The modern-day Trojan horse.

Hackers can ship their attacking devices in parcels directly to your mail room!

STOP WAIT A MINUTE MR POSTMAN, you're delivering cybersecurity exploits directly to a target's mailroom so cyber crims don't need to break into networks over the web.

So says IBM X-Force Red security researchers, which have shed light on the so-called 'warshipping' hacking technique that involves shipping low-powered and disposable computers to targets. This enables close-proximity attacks to be performed remotely anywhere in the world from anywhere in the world.

"All a malicious actor needs to do is hide a tiny device (similar to the size of a small cell phone) in a package and ship it off to their victim to gain access to their network. In fact, they could ship multiple devices to their target location thanks to low build cost," explained Charles Henderson, head of IBM's offensive operations arm.
"The device, a 3G-enabled, remotely controlled system, can be tucked into the bottom of a packaging box or stuffed in a child's teddy bear (a device no bigger than the palm of your hand) and delivered right into the hands or desk of an intended victim." – *(remember my article on Raspberry PI's a few weeks back)*

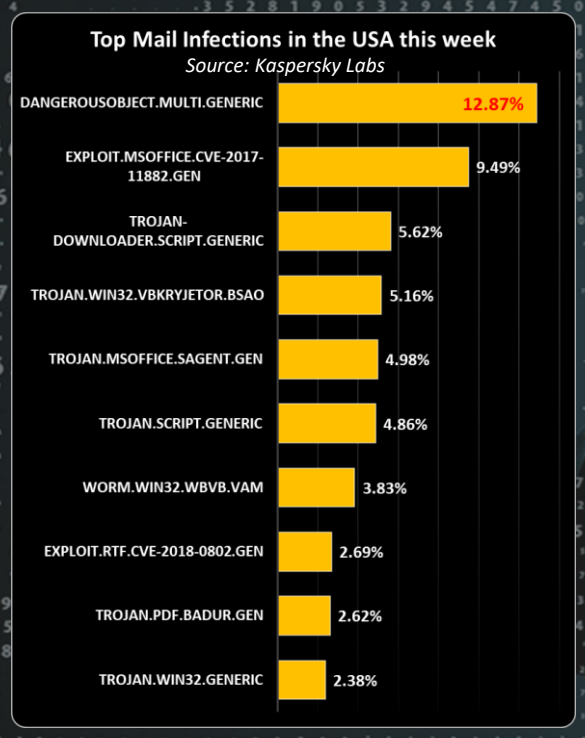
The researchers created a proof-of-concept device, which used a small 3G modem, cost some $100 to build and once set up periodically scanned for nearby networks allowing for the parcel the device is being shipped in to be tracked.
"Once we see that a warship has arrived at the target destination's front door, mailroom or loading dock, we are able to remotely control the system and run tools to either passively, or actively, attack the target's wireless access," said Henderson.

After a network has been compromised, the so-called warship then seeks out data that it could then grab and send back to a more powerful system, so it could be hacked later.

"As an example, we listened for a handshake, a packet signalling that a device established a network connection. One of the warship devices transmitted the captured hash to our servers, which we then utilised on the backend to crack the pre-shared key, essentially the user's wireless password, and gain Wi-Fi access," said Henderson.
He also noted that the warship could also be used to create a rogue wireless network to coax a victim into joining it and thereby opening themselves up to further attacks.
The technique might seem like something out of Mr Robot, but apparently, it presents a potentially lucrative opportunity to criminals given how many packages are shipped worldwide and how many of us get things delivered to our offices, especially in the holiday sales seasons.

Henderson warned that a secure package policy and avoiding bringing in packages into sensitive parts of a business can help stop such attacks, as can ensuring a Wi-Fi network uses strong WPA2 security.

The general advice is to be very careful what packages you accept and if it is addressed to someone in the organisation, confirm and verify the contents with them.
Adapted from an article by Roland Moore-Colyer which you can find here: The Inquirer



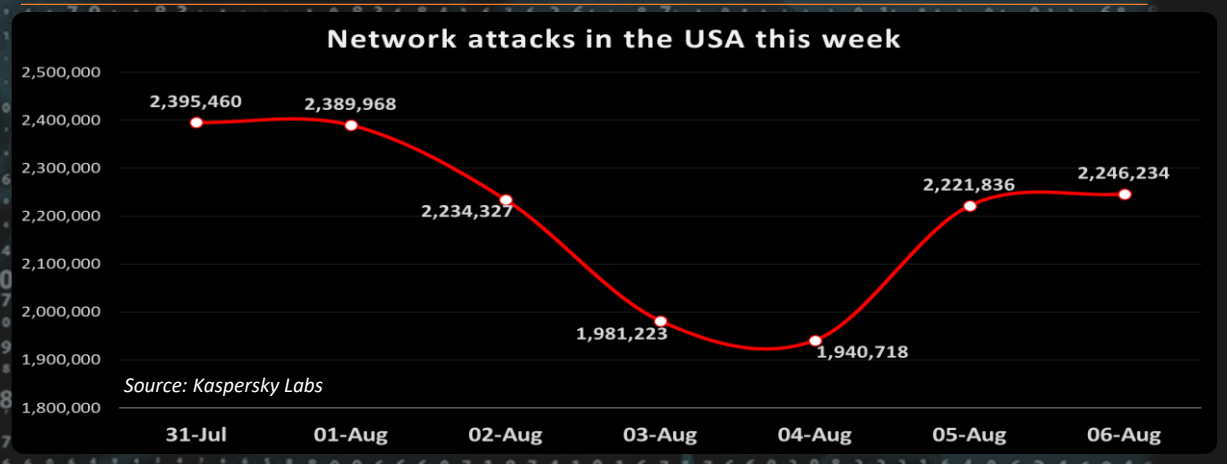
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

According to a 2019 statement released by Global Market Insights: The value of the Cyber Security Market is anticipated to reach **$300 billion** by 2024

Who are talking about me on the internet or social media?

Set up a Google Alert to see who mentions your name (or other stuff)

Google-Alert



AUTHOR: CHRIS BESTER
chris.bester@yahoo.com