On April 25, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco, Drupal, 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

03 May 2019

In The News This Week

President Trump signs executive order to improve cybersecurity workforce.

On Thursday, 2 May 2019, President Donald Trump signed an executive order aimed at improving the cybersecurity workforce within the federal government. Senior administration officials said during a call with reporters that the order will create a rotational program for cybersecurity staffers within the federal government to let them work at different agencies and pick up new skills. And they said that other measures in the order, like creating a "President's Cup Cybersecurity Competition" for cybersecurity, will ultimately improve the quality of cybersecurity staffers in both the government and in the private sector. Studies have pointed to a significant gap within the cybersecurity workforce, with there being far fewer qualified professionals than there are jobs in the field. Among other measures, the order establishes a rotational program for federal workers. Workers at the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) will be able to swap out with similar staff at other federal agencies. That program is in line with one that would be created by a bill recently passed in the Senate. The order also implements measures meant to assist federal agencies in retraining employees who are interested in joining the cybersecurity field. And it requires that an existing set of guidelines for the education of cybersecurity workers be used in the training of federal cyber staffers. Trump said in a statement that cybersecurity jobs "represent an incredible economic opportunity for America's workers — and my Administration is working to ensure they have the skills they need to seize it." "These actions will enable more Americans to secure well-paying jobs that grow our Nation's wealth and increase our security," he said. Read the full article by JACQUELINE THOMSEN here: The Hill **Read the complete Executive order here:** Whitehouse

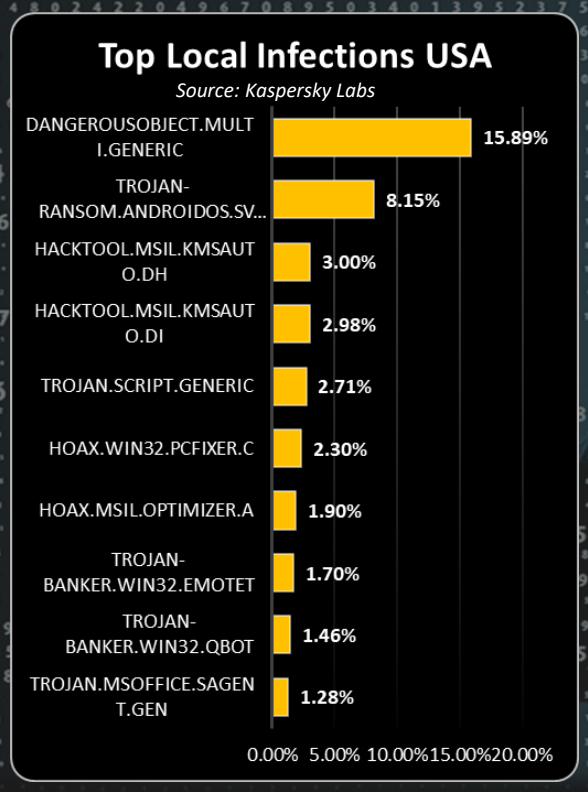
Peer-to-Peer Vulnerability Exposes Millions of IoT Devices Including Remote Access Cameras -

A flaw in the software used to remotely access cameras and monitoring devices could allow hackers to easily take control of millions of pieces of the IoT. Software intended to help homeowners be more secure may deliver their security devices into the hands of hackers. That's the conclusion of research conducted into a variety of IoT devices. In a blog post, researcher Paul Marrapese describes the flaw in the peer-to-peer (P2P) functionality of software named iLnkP2P, software developed by Shenzhen Yunni Technology, a Chinese vendor of security cameras, webcams, and other internet-of-things (IoT) monitoring devices. The software is intended to allow device owners to view footage and monitor activity from their smart devices on the Internet. However, Marrapese found that the software requires no authentication and no encryption. While the software was developed by Shenzhen Yunni Technology, scores of different vendors and product lines use the application. According to Marrapese, the vulnerability exists because of the "heartbeat" that many P2P apps use to establish communications with their control servers. This heartbeat will establish a link with the server, bypassing most firewall restrictions on links initiated from outside the local network to a device on the inside. If an attacker can enumerate the device (guess the correct UID) based on a known alphabetic prefix and six-digit number, it can use that to establish a direct connection to the device and then own the device for any number of malicious purposes. *(The ease with which the enumeration can be performed on these devices is described in CVE-2019-11219)*
Adam Meyers, vice president of intelligence at CrowdStrike, said: "Given the aggressive use by the government of the People's Republic of China of facial recognition and AI to aid in law enforcement and against political dissidents, anyone using low cost IOT devices communicating back to China should be cautious about how and where they implement this technology. "Read the complete Executive order here
Read the full story by Curtis Franklin Jr. here: DARKReading Article

10 Basic Types of Hackers

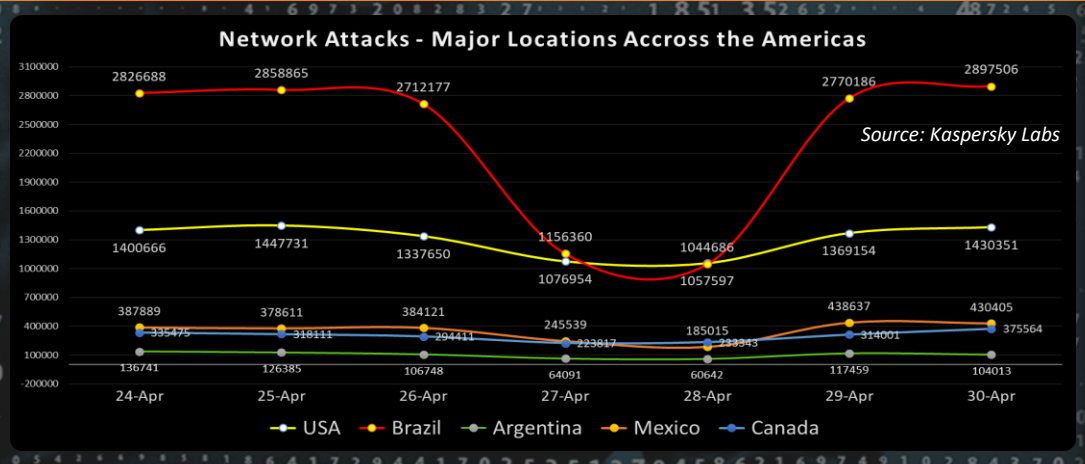
Hackers, and the malware they build and use, have grown up in the last couple of decades. When computers were big putty-coloured boxes, hackers were just learning to walk, and their pranks were juvenile. As computers have evolved into an economy of their own, hackers, too, have evolved out of those wide-eyed nerds into an audacious army of criminals. Computers are no longer novel. And hackers are no longer messing around. Gone are the social misfits entertaining themselves with a bit of all-night geek hijinks, energy drinks and junk food. Today's hackers are skilled professionals with serious jobs. The hacker profiles fall roughly into these **ten basic types**. (1) The Bank Robber - Once there were bank robbers who rode horses and pointed guns as they stole money from banks, travellers, merchants, etc. Today's financial hackers ride into town on ransomware and use fake invoices, dating scams, fake checks, denial-of-service attacks, and any other scam or hack that will help them steal money from individuals, companies, banks, etc. (2) The Nation State - Today, most sophisticated nations have thousands, if not more, of skilled hackers on their payroll. Their job? Sneak behind enemy lines at other nations' military and industrial networks to map assets and install malicious back doors. That way, when hostilities happen, the cyberwarfare machine will be ready. Nation state hacking happens all the time, mostly unnoticed. (3) The Corporate Spy - For many hackers, a day in the office involves stealing corporate intellectual property, either to resell for personal profit or to further the objectives of others. A common type of corporate espionage is to steal secret patents, future business plans, financial data, contracts, etc. Anything that gives competitors a leg up on the hacked organization is fair game. (4) The Rogue Programmer - You might consider your teenager's gaming habit nothing more than an obstacle to good grades. For millions of people, though, gaming is a serious business. It has spawned an industry that's worth billions of dollars. Gamers spend thousands on cutting-edge, high-performance hardware. They spend hundreds, if not thousands, of hours annually playing games. Is it any surprise, then, that the gaming industry has its own specialized hackers? They steal their competitors' credit caches, cause anti-competitive denial of service attacks, and even alert police to expose competing hackers. (5) The Resource Vampire - Harnessing other's people's computing power is a trick hackers used since computers first started landing on the desks of the masses. In the early days, hackers used other people's hard drives to store large files such as videos. And, for years, SETI enlisted volunteers to install a screen saver that harnessed the CPU power of the many to help search for alien life. But the biggest reason hackers steal computer resources today is to "mine" cryptocurrencies. Cryptominers spread malware—either by directly exploiting browser visitors or by infecting the web sites they visit, which then exploit their visitors, to harness computers and resources, including electricity and cooling, to mine cryptocurrencies for them. Mining malware is one of the fastest growing classes of malware. (6) The Hacktivist - Hacktivists use hacking to make a political statement or promote social change. They either want to steal embarrassing information from a victim company, cause operational issues for the company, or wreak any havoc that will cost the victim company money or bring attention to the hacktivist's cause. The Anonymous collective is one famous hacktivist group who identified and exposed multiple child porn sites and also named names of their members. Many otherwise well-meaning, law-abiding people get caught up with hacktivist goals and crimes, though, and end up getting arrested. Despite their well-meaning intentions, they can be prosecuted for the same crimes as hackers with less noble motives. (7) The Botnet Masters - Many malware coders create bots, which they send out into the world to infect as many computers as they can. The goal is to form large botnet armies that will do their evil bidding. Once they have turned your computer into their minion, it sits waiting for instruction from its master. These instructions usually come from command-and-control (C&C) servers. The botnet can be used directly by the botnet creator but more often that master rents it out to whoever wants to pay. A famous example is the Mirai bot, which attacks routers, cameras and other IoT devices. (8) The Adware Spammer - These days you're lucky if your company is only compromised by a spam malware program or your browser is only hijacked by an adware program that is looking to sell you something. Adware works by redirecting your browser to a site you did not intend to go to. Perhaps you were searching for "cats" and the adware program sent you instead to "camping gear." Many legitimate companies are surprised to learn that their own online marketing campaigns are using spam and adware. Spam and adware might not seem like a huge threat, but it can be a symptom of a serious system leak. These tools find their way through unpatched software, social engineering, and other means. (9) The Sport Hacker - Most hackers these days are working with a financial goal in mind, a boss with malicious motives, or a political goal. But there does remain a class of hacker who is in it for the thrill. They may want to demonstrate, to themselves and perhaps an online community, what they can do. There aren't as many of these as there once were because hacking, whatever the motive, breaks laws and prosecution is a real possibility. Today's sport hacker is often most interested in hardware hacking. The appearance of general purpose hardware hacking kits, with chips, circuits, and jump wires (like Raspberry Pi kits), have steadily increased the public's interest in hacking hardware as a sport. There are even hardware hacking web sites created for kids. (10) The Accidental Hacker - Lastly, some hackers are more like tourists than serious miscreants. Perhaps they have some technical ability but never intentionally set out to hack anything. Then one day they come across a web site with a glaring coding error. Fascinated by the puzzle it presents, they begin to play at hacking in. To their own surprise, they discover it was as easy as it looked. History is full of people who happened upon, for example, a web site that used easily guessable numbers in the URL to identify customers.

Adapted from a slideshow by Roger A. Grimes which you can find here: CSO



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

Cybersecurity Ventures Predict:
The global smartphone install base will grow to
6 billion
devices over the next 4 years



AUTHOR: CHRIS BESTER