On August 29, 2019, the Cyber Threat Alert Level was evaluated and is being raised to Blue (Guarded) due to vulnerabilities in Google and Apple 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.

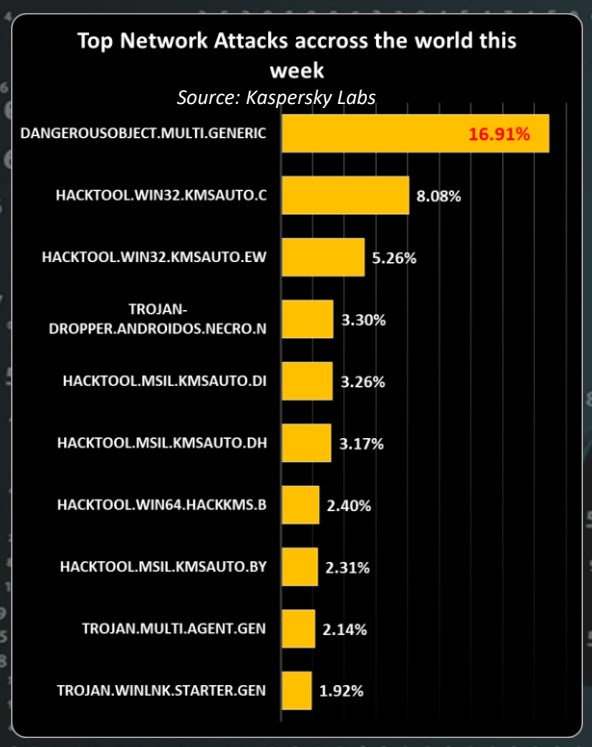
WEEKLY IT SECURITY BULLETIN

06 September 2019

In The News This Week

Hackers could steal a Tesla Model S by cloning its key fob – again! - Just shy of a year ago, researchers revealed a serious flaw in the security of Tesla's vehicles. With little more than some standard radio equipment, they were able to defeat the encryption on a Model S's keyless entry system to wirelessly clone the sedan's key fob in seconds, unlocking a car and driving it away without ever touching the owner's key. In response, Tesla created a new version of its key fob that patched the underlying flaw. But now, those same researchers say they've found yet another vulnerability—one that affects even the new key fobs. In a talk at the Cryptographic Hardware and Embedded Systems conference in Atlanta last week, researcher Lennert Wouters of Belgian university KU Leuven revealed that his team has again found a technique capable of breaking the Model S key fob's encryption. That would allow them to again clone the keys and stealthily steal the car. Tesla has acknowledged the possibility of thieves exploiting the technique, but the good news for Tesla owners is that this vulnerability can be fixed by an over-air software update, which owners should expect soon. Read the story here: Wired Article

French police hijack a botnet and remotely killed roughly 850,000 malware infections -
In a rare feat, French police have hijacked and neutralized a massive cryptocurrency mining botnet controlling close to a million infected computers. The notorious Retadup malware infects computers and starts mining cryptocurrency by sapping power from a computer's processor. Although the malware was used to generate money, the malware operators easily could have run other malicious code, like spyware or ransomware. The malware also has wormable properties, allowing it to spread from computer to computer. According to a blog post announcing the bust, security firm Avast confirmed the operation was successful. The security firm got involved after it discovered a design flaw in the malware's command and control server. That flaw, if properly exploited, would have "allowed us to remove the malware from its victims' computers" without pushing any code to victims' computers, the researchers said. The exploit would have dismantled the operation, but the researchers lacked the legal authority to push ahead. Because most of the malware's infrastructure was located in France and Avast then contacted French police. After receiving the go-ahead from prosecutors in July, the police went ahead with the operation to take control of the server and disinfect affected computers. The French police called the botnet "one of the largest networks" of hijacked computers in the world.
The operation worked by secretly obtaining a snapshot of the malware's command and control server with cooperation from its web host. The researchers said they had to work carefully as to not be noticed by the malware operators, fearing the malware operators could retaliate. "But if they realized that we were about to take down Retadup in its entirety, they might've pushed ransomware to hundreds of thousands of computers while trying to milk their malware for some last profits." With a copy of the malicious command and control server in hand, the researchers built their own replica, which disinfected victim computers instead of causing infections. "[The police] replaced the malicious [command and control] server with a prepared disinfection server that made connected instances of Retadup self-destruct," said Avast in a blog post. "In the very first second of its activity, several thousand bots connected to it in order to fetch commands from the server. The disinfection server responded to them and disinfected them, abusing the protocol design flaw." In doing so, the company was able to stop the malware from operating and remove the malicious code to over 850,000 infected computers. Jean-Dominique Nollet, head of the French police's cyber unit, said the malware operators generated several million euros worth of cryptocurrency.
Remotely shutting down a malware botnet is a rare achievement — but difficult to carry out.
Read the full story here: TechCrunch



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

What Is A Botnet & How Does It Work?

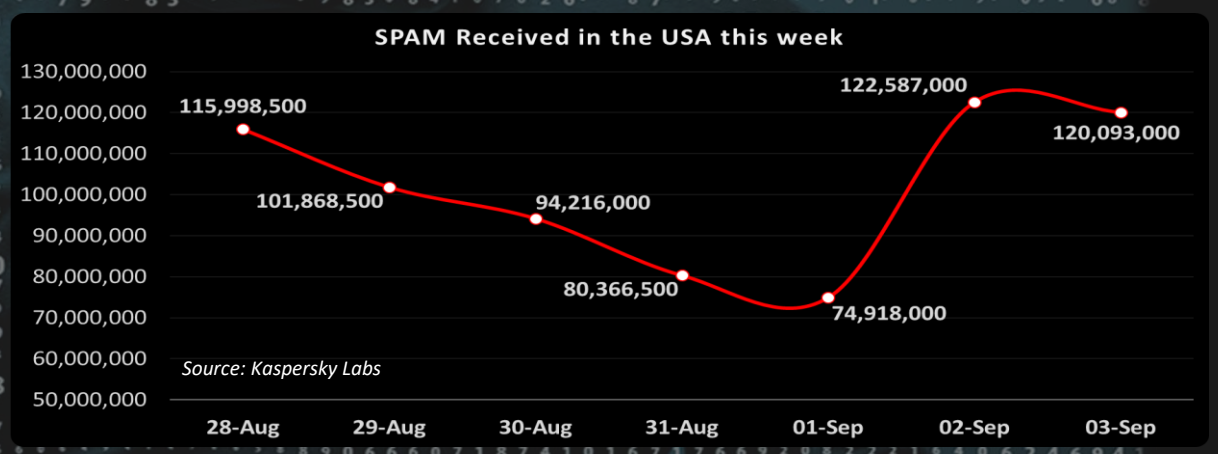
When thinking about a botnet, it's helpful to visualize it as an army of connected devices. The army comparison works here because botnets are a collection of individual devices working together as a single unit. It's a little more obvious if you break down the name: robot + network = botnet. It's literally a network of robots. These "armies" can be made up of PCs, mobile devices, servers and IoT devices. Basically any internet-connected or network-connected device can be infiltrated through malware or drive-by-downloads and brought into a botnet army. Your **home computer** or **IoT** devices could be part of a botnet without you knowing it.

Why Are Botnets a Concern? – In recent days, botnets have grown from one that largely existed only in the cybersecurity space to a more universal discourse. Botnets have been used to facilitate the spread of "fake news" sites that have proved capable of driving public opinion around the economy, government, elections and more. Botnets have shown that with this capability comes a great amount of power. One prominent example even comes from over a decade ago. Cybercriminals launched a DDoS attack in Estonia that sparked an international conflict that is still ongoing. And that is certainly not an isolated incident. As more information moves to the cloud, governments have become a popular target for cybercriminals as their networks hold valuable personal information that can be exploited. In the Estonia attack, this was definitely the case. In years prior, the nation was lauded for its use of the internet to improve government efficiency and give people easier access to services that previously crawled along in bureaucracy. Estonians could check their medical records, file taxes and even vote online. The general move toward digital information storage opens the door for risks. Governments are trying to mitigate these risks every day, and that includes the United States government. Even as recently as 2018, the U.S. Department of Homeland Security highlights botnets as a risk that warrants very serious attention. The department even released a report promoting action against botnets and other automated threats in January this year.
But it's just as true in the private sector. In fact, many speculate that to protect the digital ecosystem these two entities need to cooperate in fighting against botnet attacks. Gary Shapiro, president and CEO of the Consumer Technology Association said following the release of the US government report. "Perhaps collaboration can prevent more large-scale attacks to governments and businesses, but it is difficult to imagine an efficient security system to that end being implemented any time soon."
However, this is not the only reason botnets are used. It's not even the most common. Most attacks are on a much smaller scale.

So, What Are Botnets Typically Used For? - As you can imagine, they're used most commonly in malware attacks. It's one in a long list of examples of how good technology can be used for corrupt causes. What's more concerning however, is how easy they are to set up. Internet criminals generally has a very low barrier to cross for entry. All you really need is an internet connection, a small amount of cash, the know-how and about a half hour of free time to set up a botnet. But this section is not about how to build a botnet, it's about what they're used for.
Put simply, if your computer or mobile device is part of a botnet, that usually means it's been infected with some type of malware and a robot in the botnet army. It is one of a network of devices waiting for commands from whoever is controlling the botnet. Once a criminal has grown this network to a fair size, he or she might not always employ it for personal use. Some criminals rent out access to their botnet. Larger botnets can be used in distributed denial-of-service (DDoS) attacks. Smaller botnets can be used to circulate spam emails or to mine bitcoins. There are many more creative uses and many yet to be exposed, but for now, let's look at one of the most common uses, DDoS attacks.

Botnets for DDoS Attacks - DDoS attacks are some of the most easily accomplished cyber-attacks, and botnets almost seem tailormade to carry them out. The person controlling the botnet will command the bots to all access a designated website or IP at the same time. This flood of traffic overwhelms the site and can cause a website to slow down to an almost standstill or even shut down completely due to the massive influx of traffic from a botnet. In short, the goal of a DDoS attack is to cause disruption for a website or service.
For reference, the average botnet size is in the early 2000s was said to be around 20,000 computers, and that was before IoT devises could be infected by a botnet. This number can also vary greatly. In 2009, Conficker, one of the largest botnets ever, was estimated to have infected over 15 million computers. Imagine the firepower a botnet built of 15 million computers could have during a DDoS attack. If you want to check out a more recent large-scale DDoS attack, read the Pwnie Express post-mortem on the Mirai botnet. (Remember, we spoke about Mirai in our article last week)

The Internet of Things (IoT) and Botnets - As Mirai has shown, the Internet of Things opens up all kinds of doors for botnet armies to gain access to more power. As more connected devices enter the market, there are more opportunities for botnet attacks. Cheap connected devices like webcams, coffee makers, workout trackers and more have little or no security and it's easy for cyber criminals to gain access and bring them into the botnet army. Mirai was used in the Dyn DDoS attack in 2016 that took down notable websites like Twitter and Netflix with a botnet made of over 100,000 IoT devices.
Adapted from an article by Pwnie Express that you can find here: Pwnie Express



AUTHOR: CHRIS BESTER
chris.bester@yahoo.com