On January 16, 2019, the Cyber Threat Alert Level was evaluated and is elevated to Blue (Guarded) due to vulnerabilities in PHP and Oracle Products. (No change in status this week)

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

25 January 2019

In The News This Week

Identity fraud in the UK at 'epidemic' levels, experts warn. (Sources confirmed similar trends in the US and rest of the world)

Internet crimes rise while the number of frauds being attempted on bank accounts and credit or debit cards falls. The number of cases of identity fraud being committed in the UK has reached "epidemic" levels, experts have warned, as new figures reveal a surge in crimes. A total of 89,201 cases were registered in the UK between January and June – more than 500 every day and a rise of 5 % on the same period a year earlier. The number of crimes being reported is now at record levels as criminals exploit new technology to steal victims' identities. Figures show 83 % of identity fraud cases now take place online. The new data, released by fraud prevention body Cifas, prompted experts to warn that criminals are "relentlessly" targeting individuals and businesses. Cifas chief executive, Simon Dukes, said: "We have seen identity fraud attempts increase year on year, now reaching epidemic levels. "These frauds are taking place almost exclusively online. The vast amounts of personal data that is available either online or through data breaches is only making it easier for the fraudster. "Criminals are relentlessly targeting consumers and businesses and we must all be alert to the threat and do more to protect personal information. "For smaller and medium-sized businesses in particular, they must focus on educating staff on good cyber security behaviours and raise awareness of the social engineering techniques employed by fraudsters. "Relying solely on new fraud prevention technology is not enough." Criminals use their victims' identities to apply for loans, insurance, phone contracts and a range of products online. Some stolen identities are sold to others via the dark web. Internet crimes have risen while the number of frauds being attempted on bank accounts and plastic cards has fallen. Victims often do not realise they have been targeted until noticing a payment on a bank statement or receiving a letter from a company they have never dealt with. Those aged between 31 and 50 are most likely to fall victim to scams, with this age group making up almost half of all identity fraud cases. Criminals use a variety of methods to take someone's identity, including stealing their post, hacking their computer or email accounts and using data available on social media. Others use "phishing" emails and phone calls in which they pretend to be from a trusted authority such as a bank or the police in an attempt to trick unsuspecting victims into handing over personal information. . (Read the full story by Benjamin Kentish here: www.independent.co.uk)

Chinese Hacker Publishes PoC for Remote iOS 12 Jailbreak On iPhone X and earlier models.

Some concerning news for iPhone users. A Chinese cybersecurity researcher has today revealed technical details of critical vulnerabilities in Apple Safari web browser and iOS that could allow a remote attacker to jailbreak and compromise victims' iPhoneX running iOS 12.1.2 and before versions. To do so, all an attacker needs to do is trick iPhoneX users into opening a specially crafted web page using Safari browser, that's it. However, finding flaws and creating a working exploit to carry out such attacks is not as easy as it may sound for every iOS hacker. Discovered by security researcher Qixun Zhao of Qihoo 360's Vulcan Team, the exploit takes advantage of two security vulnerabilities that were first demonstrated at TianfuCup hacking contest held in November last year and then was later responsibly reported to the Apple security team. Zhao today released some details of and a proof-of-concept video demonstration for his exploit, which he dubbed "Chaos," after Apple just yesterday released iOS version 12.1.3 to patch the issues. So make sure you update your phone! (Read the full story by Wang Wei here: https://thehackernews.com/)

Hoaxes and Fake News in Social Media?

How do you know if you are being taken for a ride? —"In today's world, nobody can tell for sure that the information they receive is 100 percent accurate and reliable," says Janey Lee, Ph.D., assistant professor of journalism at Lehigh University in Bethlehem, PA. "Even experts have a hard time weeding out fake accounts and automatic messages." You could read and spread inaccuracies from either side of the partisan divide, even if your information comes from political leaders. Last month President Trump falsely claimed that his State of the Union address drew the biggest audience ever. And U.S. Senator Bernie Sanders incorrectly told NBC's Meet the Press that 40 percent of guns sold in the U.S. don't involve a background check. Fake news divides people, and bots can make those divisions worse. Bots are a form of artificial intelligence that can mimic human behaviour. They can retweet a story or push a link, aiming to polarize people. Many are linked to Russia. "What the Russian bots are trying to do is sow discord and make us fight," says Randall Minas Jr., assistant professor and head of the Information Technology Management Association at the Shidler College of Business at the University of Hawaii. Bots pick up on keywords or hashtags in controversial topics and use computer algorithms to create and spread extreme views that emotionally arouse people. "Those messages can create a perception of serious political polarization and huge divisions in society," says Lee.

Networks of bots can spread messages quickly, fooling social media platforms and creating the perception that a topic is trending, when in fact it's just being posted and retweeted by computers. People then believe that these trending topics reflect what most people think. If they see contrasting opinions trending, they believe that there is a huge division in public opinion. "Bots don't create trends, they amplify them. That's what we saw in Florida when David Hogg became a trending topic on multiple platforms. Bots were pushing that," says Sam Huxley, practice chair of risk and business strategy, for the communications firm LEVICK. He's referring to the claims that "crisis actors," not actual students, were playing the roles of the teenagers who survived the Parkland school shootings.

Paid actors stirring up trouble in a time of crisis can seem almost unbelievable, but our brains have powerful instincts toward resolving conflict, explains Minas. Here's how our brains do it. Say you're in favour of AR-15 rifles and you find out that the AR-15 was used to kill 17 people in Florida. You are faced with an internal conflict, or what experts call cognitive dissonance. You feel good about the AR-15, but bad about the kids. So, when you hear the fake news that those kids were just paid crisis actors, you feel better. You see that news repeated in your social media feeds, and you believe it must be true. You can discount the severity of the Florida school shooting and continue to feel good about the AR-15. Your conflict is resolved.

Minas worries about the threat created by fake news and bots. "Hacking into minds, which is essentially what's happening, is difficult to prove," he says. "When you have 320 million people disagreeing on what truth is, that can do much more damage to society than hacking into the State department."

HOW CAN YOU SPOT THE FAKES? Start by assuming that not all the news in your feed is true. Then: Question the source. If a story comes from a newspaper, IS it from a reputable site? The Denver Guardian, cited often in 2016, never existed and listed an empty car park as its address.

- Look for confirmation. If you don't see a story across mainstream media, there's probably a good reason why. "Mainstream media is motivated by getting an audience." Huxley says.
- Check the facts with third-party sites like:
  - www.Snopes.com,
  - www.politifact.com, www.factcheck.org,
  - www.hoax-slayer.com,
  - https://ispa.org.za/spam/419-scams/

  Admittedly, though, fact checking has its limits. By the time a claim is researched and proven false, it may have already reached millions of accounts.
- Call out fake news you see in your network — but do it privately. "What polarizes people further is calling them out publicly. Then people get defensive because it makes them look stupid or gullible for posting it in the first place." Huxley says.

Adapted from an article by Stephanie Thurrott at NBCNews: **https://www.nbcnews.com/**

TOP local Infections registered for last week in the USA

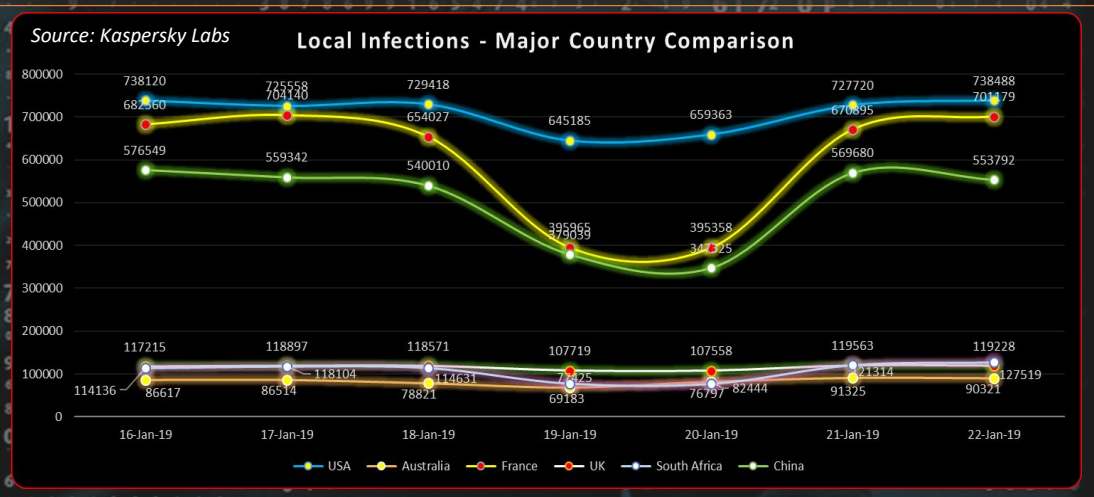
#	KNOWN AS	(%)
1	DangerousObject.Multi.Generic	27.39%
2	Trojan.Script.Generic	6.19%
3	Trojan-Ransom.AndroidOS.Svpeng.ah	5.33%
4	Hoax.MSIL.Optimizer.a	2.95%
5	Trojan.PDF.Alien.gen	2.68%
6	Trojan-Downloader.MSOffice.SLoad.gen	2.16%
7	Trojan.PDF.Badur.b	1.79%
8	Hoax.Win32.PCRepair.gen	1.48%
9	Hoax.Win32.Uniblue.gen	1.48%
10	HackTool.Win64.HackKMS.b	1.38%

Source: Kaspersky Labs

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

According to Cyren Security the top targeted brands by professional Phishing outfits in 2018 were:

Microsoft Office – 25.4%
Yahoo – 17.2%
PayPal – 17.1%
Dropbox – 9.8%
Apple – 5.0%
Gmail – 3.9%
AOL – 3.8%
Bank of America – 3.7%
Excel – 2.8%.



Author: Chris Bester