On March 28, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Mozilla, and WordPress 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

29 March 2019

In The News This Week

Microsoft Takes Down 99 Hacker-Controlled Websites

A judge granted Microsoft the injunction allowing them to disrupt a network of sites operated by an Iranian-linked group of hackers.
Microsoft said it has taken down 99 websites belonging to an Iranian state-linked hacking group it calls "Phosphorus," aka APT35, Charming Kitten, and Ajax Security Team.
According to court documents unsealed this week, Microsoft received a court order allowing them to take control of websites the hacking group had used to execute phishing attacks with fake Microsoft security warnings.

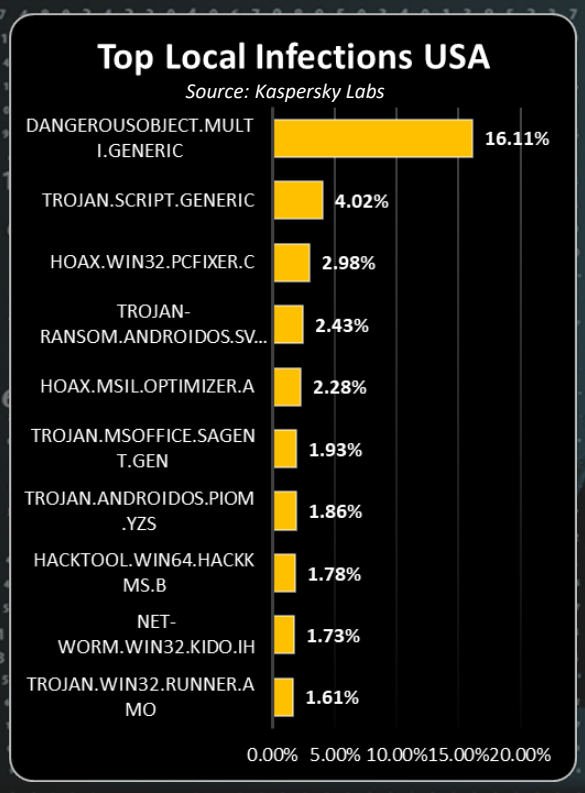
In a blog post on the takedown, Microsoft's Tom Burt, corporate vice president, customer security & trust, wrote that the company had worked with other companies, including Yahoo and a number of domain registrars to build the case that was taken before the judge to obtain the injunction.
Microsoft had been tracking Phosphorus since 2013 and had seen the group launch attacks around the world, though its more recent activity seemed to target businesses, government agencies, and "those involved in advocacy and reporting on issues related to the Middle East."

The Iranian hacking group last December was spotted by researchers at Cerfta attempting to hack email accounts of US Treasury members, defenders, detractors, Arab atomic scientists, Iranian civil society figures, DC think-tank employees, and enforcers of the US-Iran nuclear deal.

Phil Reitinger, president and CEO of the Global Cyber Alliance, says Microsoft's use of legal power to disrupt the group is a best-case scenario. "Using what amounts to civil judicial remedies where you can get the evidence to back it up strikes me as a best practice for disrupting a group that's harming you. Can mistakes be made? Sure, but for the sophisticated players that can support this, it is the most certain and defensible way to proceed," he says.

Monique Becenti, channel and product specialist at SiteLock, says Phosphorus' operation presents a cautionary tale for other businesses. "This is the second time Microsoft has had a run-in with nation-state cybercriminals and it goes to show that even one of the biggest and most sophisticated technology companies in the world can't prevent these types of attacks," she says.
That opinion was echoed by Terence Jackson, CISO at Thycotic. "Bad actors often know websites are often the weakest link and have infiltrated this time and time again."

Microsoft, meanwhile, has dealt with this type of site impersonation in the past. In his blog post, Burt wrote, "We have used this approach 15 times to take control of 91 fake websites associated with Strontium."
Ultimately, Reitinger hopes that other organizations will see this action as effective and use it as a model, rather than relying on other, extra-legal tactics.
"I think it's worth highlighting the difference between this and the kind of activity referred to as 'hack-back.' I'm not in favor of hack back because it's people taking the law into their own hands," he says. "Using civil remedies - such as a temporary restraining order to take control of malicious sites - is a powerful tool that can be used to prevent or mitigate cyberattacks."
Adapted from and article by Curtis Franklin Jr. here: https://www.darkreading.com/



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

Cybersecurity Ventures Reports:
Global ransomware damage costs are predicted to hit **$20** billion in 2021, up from $11.5 billion in 2019, $5 billion in 2017, and just $325 million in 2015

Interesting Facts

CRYPTOJACKING & SIM-SWAPPING

Cryptojacking is illegally mining cryptocurrencies, and it's gaining ground on ransomware as a favourite revenue stream for cybercriminals. The problem is so severe that Google announced it would ban all extensions that involved cryptocurrency mining from its Chrome browser. SIM swapping is on the rise and poses a major threat to cryptocurrency account holders.

- Cryptojacking was one of the fastest growing cybersecurity threats in 2018, with 25 percent of all businesses already falling victim to it.
- A report from the Cyber Threat Alliance (CTA) indicates a massive 459 percent increase in the rate of cryptojacking, through which hackers hijack computer processing power to mine cryptocurrencies such as bitcoin and Monero.
- Cryptojacking participants can use more sophisticated means to evade detection — and according to one study only around 50 percent of malicious attacks are detected.
- On average, most cryptojackers don't earn much. 1 out of every 500 of the top million Alexa-ranked sites hosts cryptojacking code. The ten most profitable cryptomining sites identified generate between $119 to $340 per day, according to academics at Braunschweig University of Technology in Germany. It remains to be seen how many cryptojackers will revert to ransomware, and data theft and resale on the Dark Web for higher pay-outs.
- SIM swapping attacks have stolen tens-of-millions of dollars' worth of cryptocurrency. The compromise involves tricking a mobile carrier employee into rerouting a subscriber's phone number to a hacker's SIM card. This enables the perpetrator to intercept the victim's messages — including 2FA codes — which helps locate the private keys used to access a cryptocurrency account. The first hacker convicted of SIM swapping was sentenced to 10 years in prison.

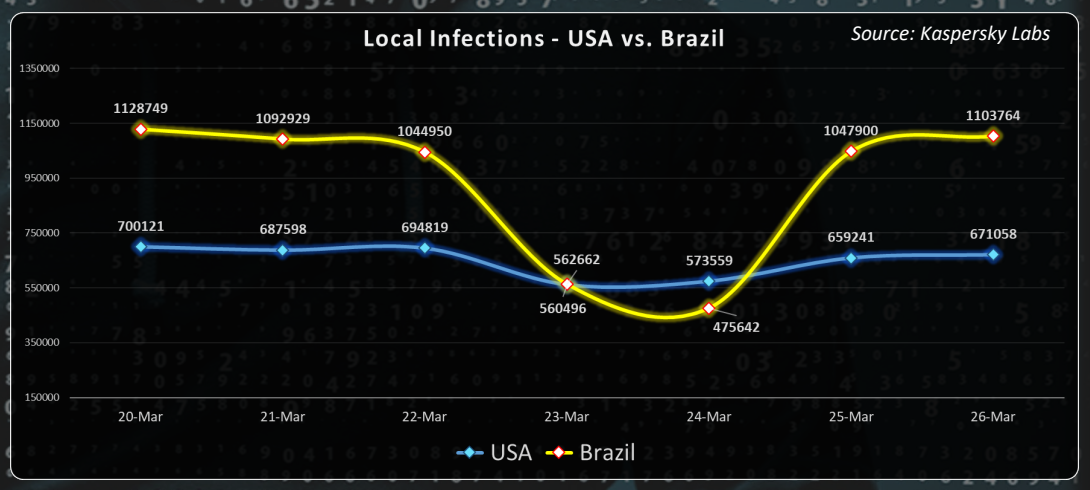
RANSOMWARE

Ransomware damage costs are predicted to be **57X more in 2021 than they were in 2015.** This makes ransomware the fastest growing type of cybercrime. The U.S. Department of Justice (DOJ) has described ransomware as a new business model for cybercrime, and a global phenomenon.

- Global ransomware damage costs are predicted to hit $20 billion in 2021, up from $11.5 billion in 2019, $5 billion in 2017, and just $325 million in 2015, according to Cybersecurity Ventures.
- Ransomware attacks saw a 350 percent increase in 2018, according to one estimate. Cybersecurity Ventures expects that businesses will fall victim to a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019, and every 40 seconds in 2016.
- Global spending on security awareness training for employees — one of the fastest growing categories in the cybersecurity industry — is predicted to reach $10 billion by 2027, up from around $1 billion in 2014. Much of this training is centred on combating phishing scams and ransomware attacks.
- It's widely reported that more than 90 percent of successful hacks and data breaches stem from phishing scams, emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn't. Training users how to detect and react to these threats is a critical ransomware deterrent.
- The No More Ransom online portal is now available in 35 different languages and carries 59 free decryption tools, covering some 91 ransomware families. So far, the tools provided on No More Ransom have managed to decrypt the infected computers of over 72,000 victims worldwide.by 2021. And by 2022, 1 trillion networked sensors will be embedded in the world around us, with up to 45 trillion in 20 years.

Read the full report here: https://cybersecurityventures.com/cybersecurity-almanac-2019/

The world's digital content is expected to grow to 96 zettabytes by 2020 (Now just how much is a Zettabyte? - One Zettabyte is approximately equal to a thousand Exabytes, a billion Terabytes, or a Trillion Gigabytes!!



Author: Chris Bester