On March 7, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Adobe 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

15 March 2019

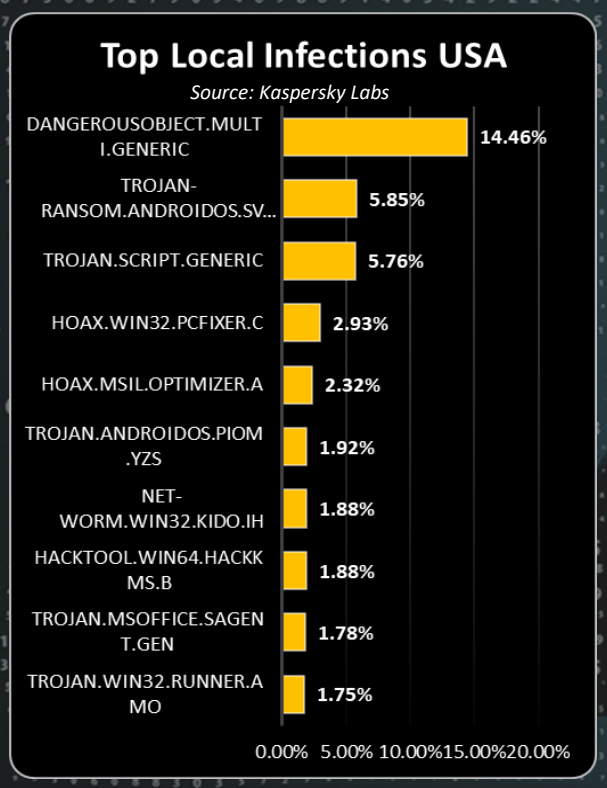
In The News This Week

19 Minutes to Escalation: Russian Hackers Move the Fastest

New data from CrowdStrike's incident investigations in 2018 uncover just how quickly nation-state hackers from Russia, North Korea, China, and Iran pivot from patient zero in a target organization. It takes Russian nation-state hackers just shy of 19 minutes to spread beyond their initial victims in an organization's network - yet another sign of how brazen Russia's nation-state hacking machine has become. CrowdStrike gleaned this attack-escalation rate from some 30,0000-plus cyberattack incidents it investigated in 2018. North Korea followed Russia at a distant second, at around two hours and 20 minutes, to move laterally; followed by China, around four hours; and Iran, at around five hours and nine minutes. "This validated what we've seen and believed - that the Russians were better [at lateral movement]," says Dmitri Alperovitch, co-founder and CTO of CrowdStrike. "We really weren't sure how much better," and their rapid escalation rate came as a bit of a surprise, he says. Cybercriminals overall are slowest at lateral movement, with an average of nine hours and 42 minutes to move from patient zero to another part of the victim organization. Russia's speedy infiltration of organizations versus other nation-states like China - which overall was the most active of all nation states in hacking in 2018 - reflects how Russia's cyber operations have evolved dramatically over the past few years. "One of the definitive characteristics of Russia is that it's willing to go fast and break things" without caring about getting identified or outed, notes John Bambenek, director of cybersecurity research at ThreatStop. "They behave in atypical ways for an intel agency [in cases]. They get a beachhead and keep moving."It's often easier to attribute attacks to Russian hacking teams because they move so quickly and are more likely to make mistakes that out or catch them in their tracks, he says. "Their mindset is to go fast and break things ... and they are still getting results," Bambenek says. Even if they are outed, they rarely face consequences given the lack of an extradition agreement between the US and Russia. –
Adapted from an article by Kelly Jackson Higgins: https://www.darkreading.com/

Ignorance or Don't Care? - Three in Five Politicians' Websites Don't Use HTTPS

Comparitech assessed the websites of more than 7,500 politicians in 37 countries and found 60.8% did not use valid SSL certificates. Security and politics have become so intertwined since the 2016 presidential election that research group Comparitech decided it was time to look into the security of politicians' websites. What they found is alarming: Three in five politicians' websites lack basic HTTPS security, according to their new study. HTTPS provides a way to ensure site visitors that they are communicating with the correct party, says Paul Bischoff, the tech journalist, privacy advocate, and VPN expert, who posted a blog about the study for Comparitech. "It's really easy for fraudsters to set up a phishing site and collect money," Bischoff says. "There needs to be a push for the politicians to lead by example and make their sites more secure."
In all, Comparitech assessed the websites of more than 7,500 politicians in 37 countries. It found 60.8% did not use valid SSL certificates, meaning visitors' connections to those sites are not private or secure — not great when they collect forms and donations and ask people to sign up for e-newsletters, Bischoff says.
There were some surprises in the study, too. Among them: Tech-savvy countries such as South Korea and India did not fare well. In South Korea, 92.3% of politicians' websites were insecure, while in India the number was 83.9%. While the United States fared well, with only 26.2% of websites insecure, that's "a pretty high number given how security-conscious people are in the United States," Bischoff says. -
Adapted from an article by Steve Zurier: https://www.darkreading.com/



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

Cybersecurity Ventures predicts that by 2021 more than **70%** of all cryptocurrency transactions annually will be for illegal activity, up from current estimates ranging anywhere from 20% (of the 5 major cryptocurrencies) to nearly 50% (of bitcoin)

Browsing Safely: Understanding Active Content and Cookies

What is active content?

To increase functionality or add design embellishments, web sites often rely on scripts that execute programs within the web browser. This active content can be used to create "splash pages" or options like drop-down menus. Unfortunately, these scripts are often a way for attackers to download or execute malicious code on a user's computer. JavaScript - JavaScript is just one of many web scripts (other examples are VBScript, ECMAScript, and JScript) and is probably the most recognized. Used on almost every web site now, JavaScript and other scripts are popular because users expect the functionality and "look" that it provides, and it's easy to incorporate (many common software programs for building web sites have the capability to add JavaScript features with little effort or knowledge required of the user). However, because of these reasons, attackers can manipulate it to their own purposes. A popular type of attack that relies on JavaScript involves redirecting users from a legitimate web site to a malicious one that may download viruses or collect personal information.
Java and ActiveX controls - Different from JavaScript, Java and ActiveX controls are actual programs that reside on your computer or can be downloaded over the network into your browser. If executed by attackers, untrustworthy ActiveX controls may be able to do anything on your computer that you can do (such as running spyware and collecting personal information, connecting to other computers, and potentially doing other damage). Java applets usually run in a more restricted environment, but if that environment isn't secure, then malicious Java applets may create opportunities for attack as well. JavaScript and other forms of active content are not always dangerous, but they are common tools for attackers. You can prevent active content from running in most browsers but realize that the added security may limit functionality and break features of some sites you visit. Before clicking on a link to a web site that you are not familiar with or do not trust, take the precaution of disabling active content. These same risks may also apply to the email program you use. Many email clients use the same programs as web browsers to display HTML, so vulnerabilities that affect active content like JavaScript and ActiveX often apply to email. Viewing messages as plain text may resolve this problem.

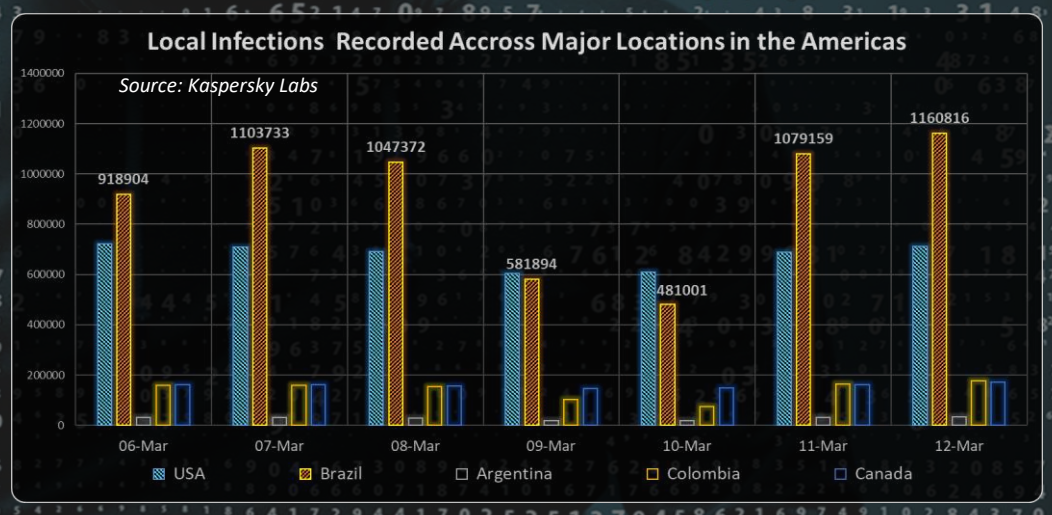
What are Cookies?

When you browse the Internet, information about your computer may be collected and stored. This information might be general information about your computer (such as IP address, the domain you used to connect (e.g., .edu, .com, .net), and the type of browser you used). It might also be more specific information about your browsing habits (such as the last time you visited a particular web site or your personal preferences for viewing that site).
Cookies can be saved for varying lengths of time:

- Session cookies - Session cookies store information only as long as you're using the browser; once you close the browser, the information is erased. The primary purpose of session cookies is to help with navigation, such as by indicating whether or not you've already visited a particular page and retaining information about your preferences once you've visited a page.
- Persistent cookies - Persistent cookies are stored on your computer so that your personal preferences can be retained. In most browsers, you can adjust the length of time that persistent cookies are stored. It is because of these cookies that your email address appears by default when you open your Yahoo! or Hotmail email account, or your personalized home page appears when you visit your favourite online merchant. If an attacker gains access to your computer, he or she may be able to gather personal information about you through these files.

To increase your level of security, consider adjusting your privacy and security settings to block or limit cookies in your web browser (see Evaluating Your Web Browser's Security Settings for more information). To make sure that other sites are not collecting personal information about you without your knowledge, choose to only allow cookies for the web site you are visiting; block or limit cookies from a third-party. If you are using a public computer, you should make sure that cookies are disabled to prevent other people from accessing or using your personal information.

You can read the full article by Mindi McDowell here: **https://www.us-cert.gov/ncas/tips/ST04-012/**



Author: Chris Bester