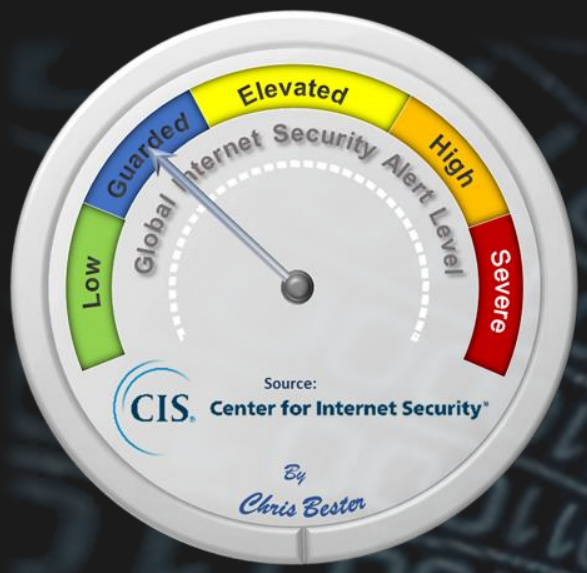


On March 28, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple, Mozilla, and WordPress products. This level still remains. On April 2, 2019 an advisory were released for Multiple Vulnerabilities in Google Android OS that Could Allow for Remote Code Execution

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

05 April 2019

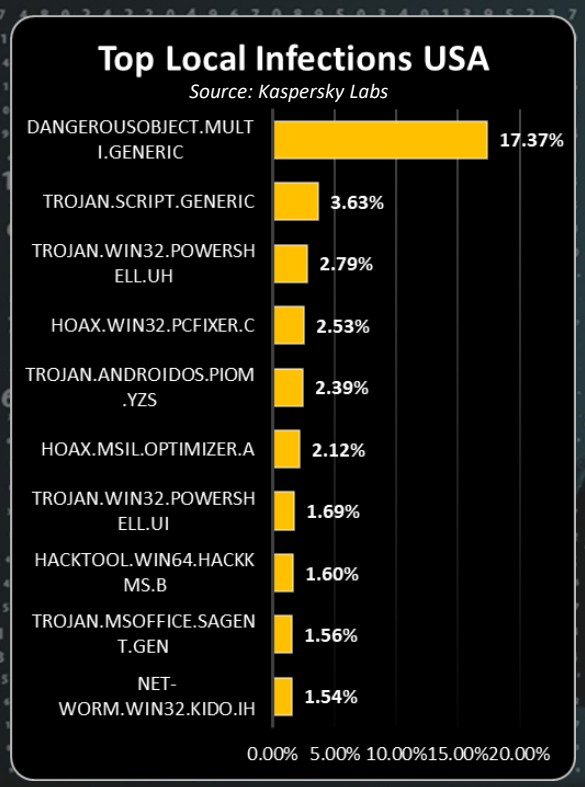
In The News This Week

Third Parties in Spotlight as More Facebook Data Leaks

Two third-party services left Facebook user data exposed online -- in one case, 540 million records of user comments -- highlighting the ease with which third-party developers can access data and the risk of lax security. A Mexican media company's unprotected Amazon S3 container exposed more than 540 million records of Facebook users' comments and interests. Also, a defunct integrated Facebook app, At the Pool, left sensitive information of more than 22,000 users exposed, said cloud-security firm UpGuard on April 3.
The data, found by the company's storage-scanning service, had explicitly been saved in two separate Amazon Simple Storage Service (S3) buckets, allowing public downloading, according to a blog post. The larger data set, left online by Mexican media firm Cultura Colectiva, consisted of 146GB of comments and whether other users liked or responded to those posts, says Chris Vickery, director of cyber-risk research at UpGuard. "In this concentrated mass, 540 million records, this is the same type of data that companies like Cambridge Analytica, or anyone else in the marketing [or] psychographic field, can exploit to develop … profiles and really learn how to control a population," he says. "In the aggregate, it is scary." Third-party developers and corporate users of Facebook's information have become a large security and public-relations problem for the company. In 2018, a Facebook insider revealed that Cambridge Analytica and its parent company, the SCL Group, had collected data on millions of Americans as a prelude to profiling them and targeting advertising to influence the 2016 presidential election. Soon after, the company revealed that most of its users likely had had their profiles scraped by third-party developers. Multiple lawsuits have since been filed against Facebook.
-- Adapted from an article by Peter Lemos – read the full story here: https://www.darkreading.com/

Threat Group Employs Amazon-Style Fulfillment Model to Distribute Malware

The operators of the Necurs botnet are using a collection of US-based servers to send out banking Trojans, ransomware, and other malware on behalf of other cybercriminals.
A threat group with possible connections to the operators of the notorious Necurs botnet has employed what security vendor Bromium this week described as an Amazon-style fulfillment model to host and distribute malware on behalf of other cybercriminals. The group is using a collection of more than one dozen US-based servers to help attackers distribute a variety of ransomware, banking Trojans, and other malware to targets located mostly within the country. The IP addresses of the hosting servers belong to a single autonomous system — or range of IP addresses — registered with a so-called "bulletproof" hosting company in the US. Eleven of the servers hosting malware are located in a single data center in Nevada belonging to the company. Typically, malware hosting servers are located in jurisdictions known to be uncooperative with law enforcement. The fact that this particular group is operating from within the US using a highly consolidated set of servers is significant, says a malware researcher at Bromium, who did not wish to be identified.
"One benefit of the infrastructure being in the US is that the connections to download the malware are more likely to succeed inside organizations that block traffic to and from countries outside of their typical profile of network traffic." Bromium has been tracking the group's operation for close to a year and says it has observed the US-based servers being used to host at least five families of banking Trojans, two ransomware families, and three information stealers. The malware includes the Dridex banking Trojan, GandCrab ransomware, and the Neutrino exploit kit. Evidence suggests that a single group is hosting the malware and also distributing it via mass phishing campaigns on behalf of other threat actors. The use of the same servers to host multiple malware families, for instance, suggests that a single entity is behind the operation, Bromium said.
Read the full article by Jai Vijayan here: https://www.darkreading.com/



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

Cybersecurity Ventures Reports:
The world will need to cyber protect **300 billion** passwords globally by 2020.

Dealing with Cybercrime

Cybercrime - What do we need to know and what do we need to do?

Know your enemy

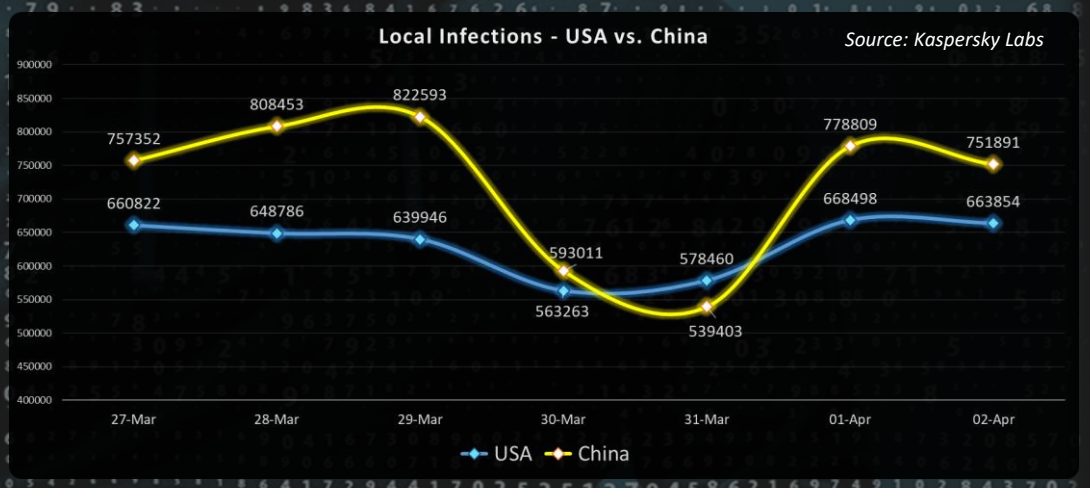
The scary part the multi-faceted nature of modern cybercrime is that there is no single technological countermeasure. According to the Federation of Small Businesses (FSB), there are four types of cybercrime that are the most common.

- Phishing – web sites, phone calls and spam emails that appear legitimate, but are actually scams designed to acquire private data. Phishing accounts for **49%** of reported cybercrime across all sectors, according to the FSB. 'Spear phishing', where an email appears to be from a known person or organisation, accounts for 37%.
- Malware – malicious software installed inadvertently, usually by visiting a malware-infected (but otherwise genuine) website, or by opening an attachment from a phishing email. Malware can be used for anything from spying on keyboard input to infiltrating secure networks, and accounts for 29% of reported cybercrime.
- Denial of Service (DOS) – a mass orchestrated attack that floods a computer system (often a website) with countless requests for information, rendering it incapable of responding to real users. DOS attacks typically rely on 'botnets' – vast networks of hacked and remotely controlled computer systems – and make up 5% of attacks.
- Ransomware – a type of malware that locks users out of a computer system, often by encrypting its data, and threatens deletion until a ransom is paid. 4% of small businesses have reported ransomware attacks, according to the FSB, while other research reckons 54% of all British businesses have been targeted.

Preparation is everything

- Relying on common sense as a countermeasure for social engineering attacks isn't enough (remember 49% are phishing attacks), but staff training can make a huge difference. Identifying sophisticated phishing spam by sight may not be easy but knowing that legitimate organisations never ask for login details by email is more easily remembered.
- Staying up-to-date is essential - Sensible and well-implemented IT policies are also key and these needn't be complex. Simply upgrading to the latest version of a browser will block most web phishing attempts and a wide range of other web-based attacks.
- How the cloud can help - (a) Cloud backup services are the obvious answer here. Secure and redundant offsite storage is expensive, but cloud storage makes it much more affordable – and there's no backup hardware to maintain. With backups available instantly in any place, lost data can be restored quickly in the event of a serious attack and business resumed with minimal disruption. (b) The cloud is also an invaluable asset for other security measures. Cloud hosting makes web sites much more resilient to DOS attacks than self-hosted setups, for example, since providers can rapidly deploy additional hardware (and considerable expertise) to cope with even the most determined.
- If an attack happens - The complexities of cybercrime mean there can be no guaranteed defence, but a clear plan for limiting the damage caused should an attack succeed will make a big difference in the days that follow. Most important here is knowing when an attack has actually happened and that's not always easy. Unlike more traditional crime, cybercrime can leave few traces. Intrusion detection needs more than just up-to-date anti-malware software. Computer systems require constant monitoring to detect abnormal behaviour, but that obviously hinges on what constitutes 'normal' behaviour.
- Dealing with data breaches - Other steps depend on the type of attack. Where data theft is involved, locking down the affected systems to limit further damage should be a priority, as should identifying the target. The appropriate classification of sensitive data will also help. Just like a pre-prepared inventory of office equipment will help assess the loss following a break in, knowing the kind of data that's been stolen will help determine a suitable course of action. Affected parties also need to be notified about data breaches as soon as possible, along with relevant law enforcement agencies in line with local privacy laws and regulations. A public statement may also be necessary, but keep this simple and factual, and follow the advice of security experts and law enforcement, where appropriate.
- Most important of all, don't lose sight of the bigger picture – getting back to business as usual as quickly as possible.

Adapted from an British Telecom article found here:
https://business.bt.com/solutions/resources/the-facts-about-cybersecurity/#enemy/



Author: Chris Bester