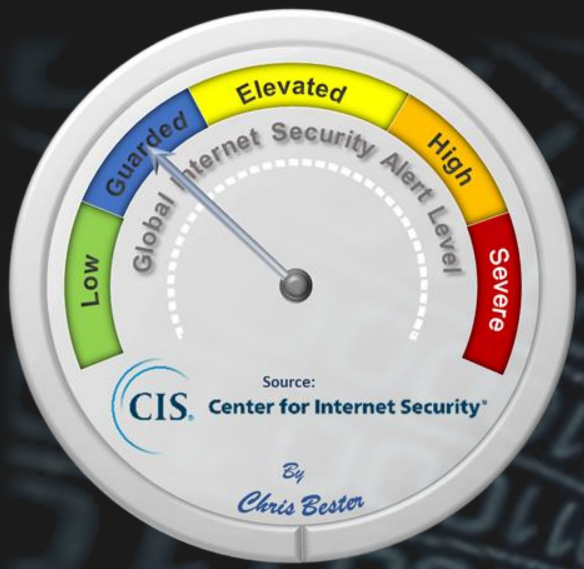

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

On April 10, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft and Adobe 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

26 April 2019

In The News This Week

The future of cybersecurity: Your body as a hacker-proof network - Could a 'body area network' be the key to keeping medical devices safe or transferring data between individuals?

What do insulin pumps, pacemakers, and MRI scanners have in common? If you said they're all medical devices that can help to save your life, you're right. If you guessed that they're all medical devices that can be hacked, you're sadly all too correct too. Increasing numbers of implantable medical devices are now gaining internet connectivity, giving doctors the ability to monitor patients health remotely, and even updates the devices to tweak a treatment plan. Unfortunately, that flexibility offers a way for hackers to hijack that hardware, and even potentially make changes to the way the devices work. While so far, no attacks have been successful, proof-of-concept attacks have been available for years. (And in the popular TV program MacGyver, the concept was highlighted when a guy's pacemaker was infected with a virus)

And while it might be tempting to hope that cybercriminals might see corrupting life-sustaining devices as a step too far, they haven't historically shown much of a conscience, cheerfully extorting money away from hospitals, for example, and putting patients at risk. In future, as connected medical devices not only monitor health condition but also dispense drugs and actively treat patients, keeping health hardware locked down is going to take on greater significance not only for tech companies, but for the individuals whose life might depend on them. But will it really be possible to keep personal health networks secure?

Traditionally, connected medical devices have used wireless to share data with healthcare systems. Using wireless, however, means signals from the devices can be read from tens of metres away -- and so potentially hacked. (The Department of Homeland Security recently gave a severity rating of 9.3 out of 10 to a flaw that allowed implantable defibrillators to be hacked from 20 feet away.) Researchers at Lafayette's Purdue University have come up with a new approach to protecting implantable medical devices. As that wireless connectivity is one major way medical devices could be open to attack, one way around the problem is to use the device-wearer themselves as a conduit, routing the signal through their body -- which dramatically cuts the distance over which any data can be read. The Purdue researchers aren't the first to come up with the idea of using the human body as the carrier for a network, but earlier versions of 'human body communication' still ended up radiating signal over a distance outside the body, leaving them theoretically open to attack. Adapted from an article by Jo Best that you can read here: ZDNet(1)

Facebook asked to clamp down on cops creating fake accounts. - Police officers are creating covert, fake accounts in order to spy on users during investigations.

Facebook has been urged to ramp up its efforts to prevent law enforcement from creating fake accounts in the name of surveillance. The Electronic Frontier Foundation (EFF) says that despite repeated warnings issued by Facebook which decree that law enforcement is required to use authentic identities on the social networking platform -- a rule also stipulated for the general public -- these demands are being ignored and the police are creating both fake and impersonator accounts en masse. Social networks and the sharing of information, both public and personal, can be used by law enforcement to circumvent legal requirements such as the issuance of warrants in investigations. While it is up to us how much information we share, our contacts may also post or share data, unwittingly, which can be used in law enforcement activities.

One of the most recent accounts of such schemes was exposed by The Guardian earlier this month. US law enforcement officers under the US Immigration and Customs Enforcement (ICE) umbrella were found to be

Read the full article by Charlie Osborne here: ZDNet(2)

What is Sandbox Security?

Last week we explored what Cyber Honeypots are and how it works. This week we will take a high level look at Cyber Sandboxing , what it means and the basics of how it works.

Sandbox Security Defined

In cybersecurity, a sandbox is an isolated environment on a network that mimics end-user operating environments. Sandboxes are used to safely execute suspicious code without risking harm to the host device or network.

Using a sandbox for advanced malware detection provides another layer of protection against new security threats—zero-day (previously unseen) malware and stealthy attacks, in particular. And what happens in the sandbox, stays in the sandbox—avoiding system failures and keeping software vulnerabilities from spreading.

Threats Sandbox Testing Protects Against

Sandbox environments provide a proactive layer of network security defense against new and Advanced Persistent Threats (APT). APTs are custom-developed, targeted attacks often aimed at compromising organizations and stealing data. They are designed to evade detection and often fly under the radar of more straightforward detection methods.

How Does Sandbox Technology Work?

Sandbox testing proactively detects malware by executing, or detonating, code in a safe and isolated environment to observe that code's behaviour and output activity. Traditional security measures are reactive and based on signature detection—which works by looking for patterns identified in known instances of malware. Because that detects only previously identified threats, sandboxes add another important layer of security. Moreover, even if an initial security defense utilize artificial intelligence or machine learning (signature less detection), these defences are only as good as the models powering these solutions – there is still a need to complement these solution with an advanced malware detection.

Sandbox Security Implementations

There are several options for sandbox implementation that may be more or less appropriate depending on your organization's needs. Three varieties of sandbox implementation include:

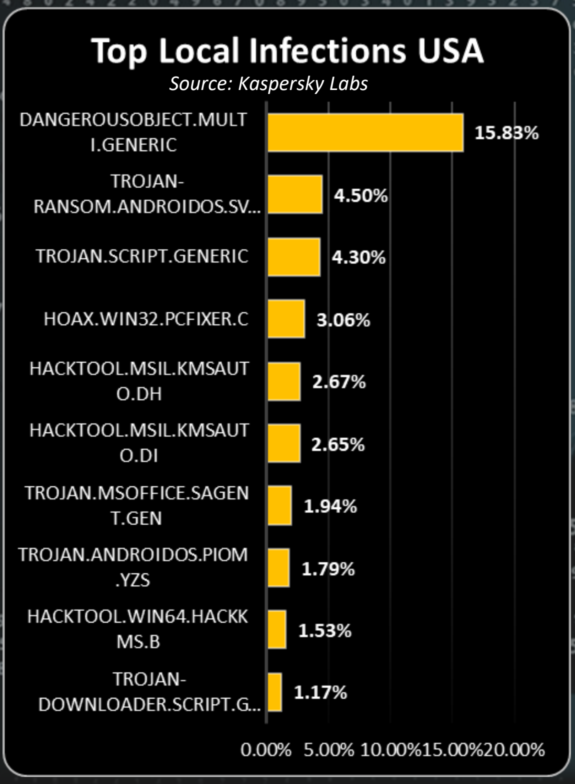
- ❖ Full System Emulation: The sandbox simulates the host machine's physical hardware, including CPU and memory, providing deep visibility into program behaviour and impact.
- ❖ Emulation of Operating Systems: The sandbox emulates the end user's operating system but not the machine hardware.
- ❖ Virtualization: This approach uses a virtual machine (VM) based sandbox to contain and examine suspicious programs.

Sandbox Evasion Techniques

On the other side of the coin, malware authors are constantly working to respond to the newest, most sophisticated threat detection. Some primary sandbox evasion techniques include.

- ❖ Detecting the Sandbox: Sandbox environments look slightly different than an end user's real system. If malware detects a sandbox, it can either terminate immediately or stall execution of harmful activities.
- ❖ Exploiting Sandbox Gaps and Weaknesses: As sophisticated as a particular sandbox might be, malware authors can often find and exploit its weak points. One example is using obscure file formats or large file sizes that the sandbox can't process. Or, if the sandbox's monitoring method is circumvented, the sandbox gains a "blind spot" where malicious code can be deployed.
- ❖ Incorporating Context-Aware Triggers: Context-aware malware works by exploiting weaknesses of the automated sandbox technology. For example, what are sometimes referred to as "logic bombs" can delay code detonation for a specified period of time or until triggers occur that typically only happen in an end user's system—like system reboots or keyboard and mouse interactions.

Adapted from an article by Forcepoint which you can find here: ForcePoint



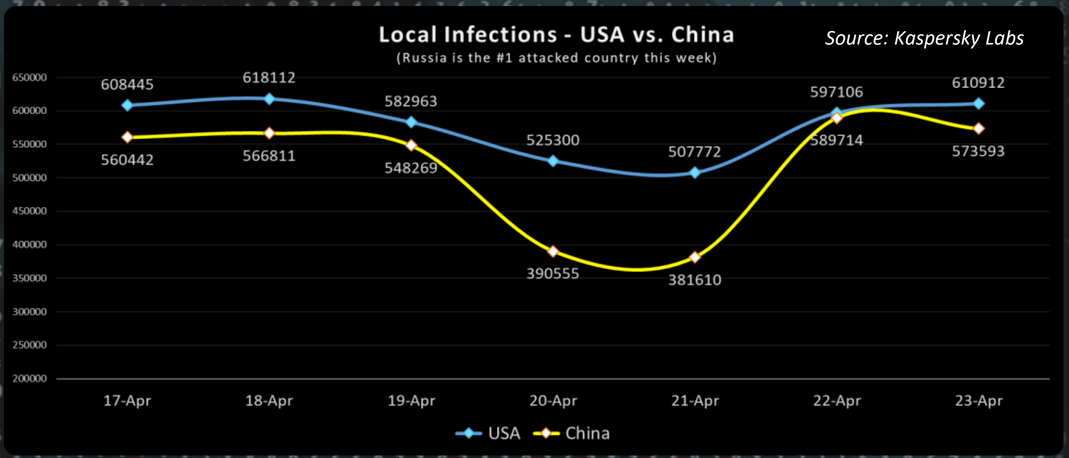
For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

Cybersecurity Ventures Predict:

There will be

3.5 million

unfilled cybersecurity jobs by 2021



AUTHOR: CHRIS BESTER