On September 25, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google, 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

27 September 2019

In The News This Week

Smart TVs send user data to tech heavyweights including Facebook, Google, Netflix

University researchers say that smart TVs are leaking sensitive, private user information to companies including Google, Facebook, and Netflix. As reported by the Financial Times, smart television sets produced by popular vendors including Samsung, Apple, and LG, alongside content and app streaming devices such as Amazon's FireTV and Roku, are sending out information potentially without the knowledge or consent of users.

Academics from Northeastern University and Imperial College London examined 81 Internet of Things (IoT) devices in the US and UK, including TVs, smart home hubs, and appliances. In a paper titled, "Information Exposure From Consumer IoT Devices", the team said that 34,586 controlled experiments revealed a total of 71 out of 81 devices send information to destinations other than the device manufacturer; 56 percent of US devices and 83.8 percent of UK products will leak information abroad, and every device involved in the study exposes information via at least one plaintext flow. User and device behaviour, in 30 out of 81 cases, can be "reliably inferred" from eavesdropping whether or not information flows are encrypted. This may include our interactions with television sets and other household IoT products. Read the full article by Charlie Osborne here: ZDNet Article1

Metasploit Creator HD Moore's Latest Hack: IT Asset Discovery Without Admin Rights!

HD Moore, famed developer of the wildly popular Metasploit penetration testing tool, has built a network asset discovery tool that wasn't intended to be a pure security tool, but it addresses a glaring security problem.

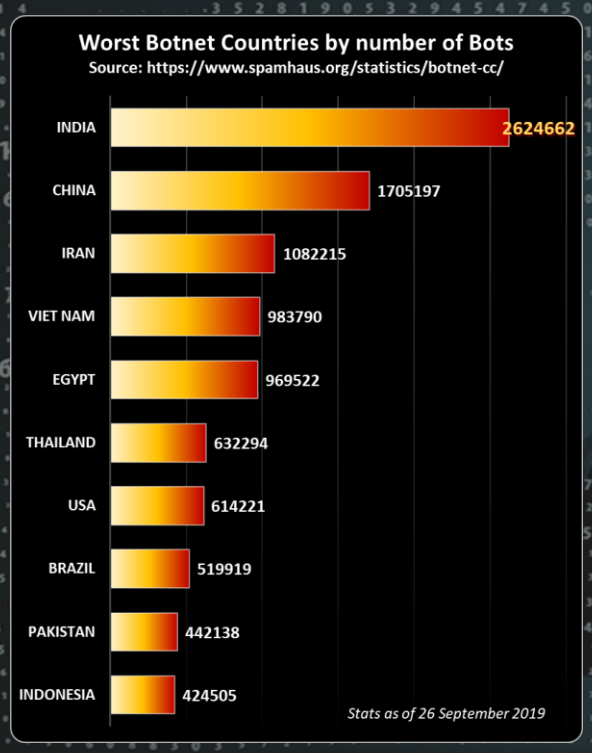
Moore's IT asset discovery tool. Rumble Network Discovery. aims to solve one of the most basic yet confounding problems organizations face and have faced for years: getting a true inventory of all of the devices and services running in their increasingly diverse and growing networks. Misconfigured systems. misconfigured network settings, and unknown unpatched devices sitting on the network are among the most common weak links that expose enterprises today to attacks and data breaches. It's a problem getting exacerbated now with the official — and sometimes unofficial — arrival of Internet of Things (IoT) devices on networks.

It's not that there aren't any IT asset discovery and security tools available today, but the underlying challenge remains that most of today's discovery tools require administrative access control of the network devices as well as visibility.

The goal of Rumble, he says, is to provide a discovery tool that doesn't require credentials to inventory the devices or monitor the ports. "You can just drop it into a network and find everything," Moore says. It sounds so simple and obvious — a true mapping and inventory of devices and their status on the network — but it's one of the biggest security holes for many organizations.

Moore had wanted to build the tool for IT people who may or may not have security experience or responsibilities, but most of his beta users have been IT people with security roles, security researchers, or IT managers.

Adapted from an articled published by DARKReading which you can find here: DARKReading



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

Gartner forecasts that more than **half a billion** wearable devices will be sold worldwide in 2021, up from roughly 310 million in 2017. Wearables includes smartwatches, head-mounted displays, body-worn cameras, Bluetooth headsets, and fitness monitors

Tips for protecting your privacy from hackers, spies and government surveillance?

Privacy is what sets us apart from the animals. It's also what sets many countries and citizens apart from dictatorships and despots. People often don't think about their rights until they need them; whether it's when they're arrested at a protest or pulled over for a routine traffic stop. Surveillance is also a part of life, and it's getting progressively more invasive. Government eavesdropping is increasing, carried out in wider secrecy, and it's becoming far more localized. In fact, the last three presidents have pushed for greater surveillance: Clinton introduced mandated wiretapping laws, Bush expanded mass domestic surveillance, and Obama expanded the intelligence service's reach -- just in time for Trump. Now many are concerned about the future of their fundamental freedoms and constitutional rights. There is no such thing as perfect security. But no matter who you are or where you are in the world, there are a lot of things you can do (many of which are simple) to protect yourself in this turbulent time.

THE SIMPLE STUFF - Your privacy, at its core, relies on your data being secure. There are some professions (such as government workers, journalists, and activists) who face far more and complex threats than the average citizen, who should usually only worry about tech companies tracking them to serve up the best kinds of ads, or government bulk data collection of their personal records. But everyone can take this basic advice and modify it on varying degrees.

While most apps and services nowadays secure your data with encryption on their servers to prevent data from being readable if hacked or served with a government subpoena, many more now are providing it "end-to-end." In other words, nobody else can see what's sent, stored, or received, other than you and the person you're talking to -- not even the companies themselves. Usually, the only way to break that "end-to-end" model is to attack an endpoint, such as the device you're using, the internet pipe that the data's traveling along, or the company's servers. If you secure each of those points, you're well on the way in keeping your data private.

SECURE YOUR DEVICES - Your phone is your ultimate endpoint. You carry it everywhere and it usually holds your most personal secrets and sensitive information. iPhones are widely seen as the most secure mainstream device today. Modern and newer Android devices usually come with strong security features, but there isn't a universal implementation of encryption yet. Your iPhone encrypts as soon as you lock your screen (even the feds can't access it), but Android devices have to be shut down entirely. Here's a guide on how to secure your iPhone, and here's another guide for most Android devices.

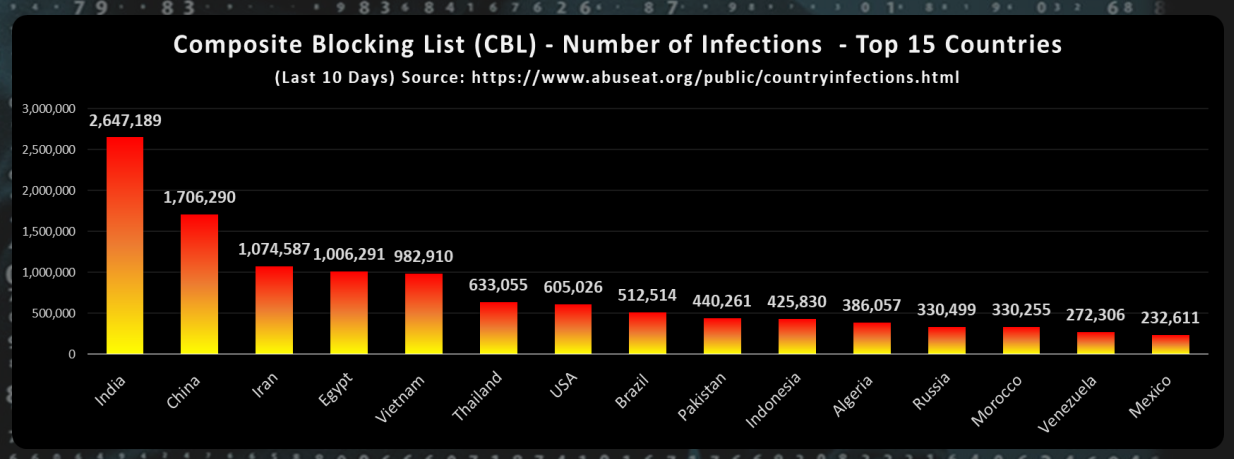
TURN OFF FINGERPRINT PHONE UNLOCK - Your Touch ID or fingerprint sensor is meant to keep your data more secure. But in some cases ***federal agents can force you to unlock your phone with your fingerprint, because the courts have determined that it's not a violation of the Fifth Amendment***, which protects against self-incrimination. The feds however can't force you to turn over your passcode. **(1)** iPhone users - Turn off Touch ID by going to Settings > Touch ID & Passcode > turn off iPhone Unlock. **(2)** Android users - Go to Settings > Security > Lock Screen or Nexus Imprint.

REDUCE YOUR ONLINE FOOTPRINT - There are dozens of websites called data brokers that crawl the web for your personal information, and then post it online for the world to see. If you Google your name along with the city you live in, these data broker sites are always the top search results. Websites like MyLife, Whitepages and Spokeo make millions by selling access to this information. You can use this helpful guide from DeleteMe to remove yourself from each of these data broker websites, but this process can be tedious and time consuming. DeleteMe offers a hands-free service to get you off the web, but at a cost.

SECURE YOUR MESSAGING - Now that your device is secure, you should think about your data in-transit -- that is, as it traverses the waves of the wireless spectrum and the pipes of the internet. SMS messages and phone calls can be intercepted and wiretapped at any time -- it's the law. Police can also use cell-site simulators (known as "stingrays") to force-downgrade your cell connection from LTE to non-encrypted channels to make it easier to snoop on your phone. It's not just the messages you send that you need to worry about; you also have to think about the data that's generated as a result -- so-called metadata, such as who you're talking to, when, and sometimes where. That information alone can tell a lot about your life, which is why it's so important to intelligence services. Metadata is a core pillar of government surveillance. Countering metadata collection isn't easy, but its collection can be limited. The trick? Use the right app. Let's get one myth out of the way: There is no secure email solution -- at least not yet. Other and better instant communications exist.

In ranked order, best first: - **(1)** Use SIGNAL for encrypted messaging, it is by far the simplest and the most secure app when it's used properly. Available for iOS and Android, the end-to-end encrypted messenger was almost universally accepted as the gold standard among security experts and professionals. Signal almost entirely removes itself from the surveillance loop by collecting almost no metadata. **(2)** WhatsApp - If you heard recently that WhatsApp has a "backdoor," that's wrong. So wrong, in fact, that some of the world's foremost security experts and cryptographers have called for the story to be retracted. The Guardian, which published the story, later said "flawed reporting" led the newspaper to "overstate the potential impact on the security of users' messaging. The end-to-end encrypted messenger, owned by Facebook, works on a range of devices, including desktop. At its core, it uses the same protocols as Signal -- so it's secure and neither Facebook, WhatsApp, or anyone else can read your messages. **(3)** Apple's iMessage is also encrypted end-to-end, but you can't verify your keys with the people you're messaging. That's a problem, because you can't ever be sure that your messages aren't being intercepted. Recent developments have shown that the system is vulnerable to man-in-the-middle attacks, so don't rely on the system for critical communications. And again, don't back up your messages to iCloud, because Apple can be forced to turn that data over to law enforcement.

Adapted from an article by Zack Whittaker on ZDNet, please visit this site with loads more information: ZDNet Article2



Author: Chris Bester
chris.bester@yahoo.com