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

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

11 October 2019

In The News This Week

Twitter: We accidentally used security data to target users with ads

Twitter announced Tuesday 8 October that email addresses and phone numbers used to secure accounts had accidentally been used for advertising purposes. In a blog post, the company says the addresses and numbers were used in its "Tailored Audiences" product, which allows advertisers to target ads to customers based on the advertiser's own marketing lists. "When an advertiser uploaded their marketing list, we may have matched people on Twitter to their list based on the email or phone number the Twitter account holder provided for safety and security purposes," the blog states. "This was an error and we apologize." Twitter does not know how many people were impacted by the error. The company says no data was shared with third parties that used the Tailored Audiences feature. Twitter users share phone numbers with the company for security purposes, particularly for its two-factor authentication feature. With that feature, Twitter sends a code to the stored phone number via SMS, which is then used to further authenticate a user's login. Security experts have frowned upon using SMS in the two-factor authentication process, mainly due to SIM hijacking, which typically involves hackers posing as their victim in order to transfer a phone number from one device to another. Other social media networks have moved away from using phone numbers in their two-factor authentication process. In May 2018, Facebook moved away from requiring a phone number to use the service to sign into the company's platform. However, Facebook also never explicitly told users it was using those numbers for advertising purposes. That act was among the many reasons the Federal Trade Commission issued a $5 billion fine against the company in July.

Read the full article here: CyberScoop

Apple can uphold basic human rights or become a Beijing accomplice: HK lawmaker

Member of the Hong Kong Legislative Council, Charles Mok, the representative of its Information Technology functional constituency, has called on Apple to lift its ban on HKmap.live.

Apple removed the app from its store on Thursday, stating that the app could be used to ambush police. Writing to Apple, Mok said the company has the ability to "uphold its commitment to free expression and other basic human rights, or become an accomplice for Chinese censorship and oppression". Mok said the app, which crowdsources information to allow people in Hong Kong to know where police are active, helps people avoid police brutality.

"HKmap.live helps HK residents, journalists, tourists etc. identify 'danger zones' and avoid being hurt by tear gas, rubber bullets, baton, bean-bag rounds, and water cannon that the Hong Kong police claims to be 'minimum force', and get real-time updates of public transport, who rely on the app to avoid being harassed and beaten up by police for no reason," Mok wrote. "If sharing information on a real-time basis equates to encouraging criminal activity ... the same standard should also be applied to review social media apps such as Facebook, WhatsApp, Twitter, Telegram, and Instagram, where people share similar information in real-time." Responding to news of its decision to ban HKmap.live, CEO Tim Cook reportedly sent an email to Apple employees backing the ban.

"The app was being used maliciously to target individual officers for violence," Cook reportedly said. "We built the App Store to be a safe and trusted place for every user ... In this case, we thoroughly reviewed [the facts], and we believe this decision best protects our users."

The app is still available on the Google Play Store, and is viewable through its website.

Read the full article here: ZDNet Article

Machine learning–aided scams

Kaspersky Labs reported this on October 4, 2019 and I thought it would be great to share it in my bulletin. Thank you to my good friend Yazan Shapsugh who pointed me in the direction of the story.

New technologies are clearly changing the world, but not the human psyche. As a result, evil geniuses are devising new technological innovations to target vulnerabilities in the human brain. One vivid example is the story of how scammers mimicked the voice of an international CEO to trick the head of a subsidiary into transferring money to shady accounts.

What happened?

The details of the attack are unknown, but the Wall Street Journal, citing insurance firm Euler Hermes Group SA, describes the incident as follows:

1. Answering a phone call, the CEO of a U.K.-based energy firm thought he was speaking with his boss, the chief executive of the firm's German parent company, who asked him to send €220,000 to a (fictitious, as it later turned out) Hungarian supplier within an hour.
2. The British executive transferred the requested amount.
3. The attackers called again to say the parent company had transferred money to reimburse the U.K. firm.
4. They then made a third call later that day, again impersonating the CEO, and asked for a second payment.
5. Because the transfer reimbursing the funds hadn't yet arrived and the third call was from an Austrian phone number, not a German one, the executive became suspicious. He didn't make the second payment.

How was it done?

Insurers are considering two possibilities. Either the attackers sifted through a vast number of recordings of the CEO and manually pieced together the voice messages, or (more likely) they unleashed a machine-learning algorithm on the recordings. The first method is very time-consuming and unreliable — it is extremely difficult to assemble a cohesive sentence from separate words without jarring the ear. And according to the British victim, the speech was absolutely normal, with a clearly recognizable timbre and a slight German accent. So, the main suspect is AI. But the attack's success had less to do with the use of new technologies than with cognitive distortion, in this case submission to authority.

Psychological post-mortem

Social psychologists have conducted many experiments showing that even intelligent, experienced people are prone to obeying authority unquestioningly, even if doing so runs counter to personal convictions, common sense, or security considerations.

In his book The Lucifer Effect: Understanding How Good People Turn Evil, Philip Zimbardo describes this type of experiment, in which nurses got a phone call from a doctor asking them to inject a patient with a dose of medicine twice the maximum allowable amount. Out of 22 nurses, 21 filled the syringe as instructed. In fact, almost half of nurses surveyed had followed a doctor's instructions that, in their opinions, could harm a patient. The obedient nurses believed they had less responsibility for the orders than a doctor with the legal authority to prescribe treatment to a patient.

Psychologist Stanley Milgram likewise explained the unquestioning obedience to authority using the theory of subjectivity, the essence of which is that if people perceive themselves as tools for fulfilling the wills of others, they do not feel responsible for their actions.

What to do?

You simply cannot know with 100% certainty who you are talking to on the phone — especially if it's a public figure and recordings of their voice (interviews, speeches) are publicly available. Today it's rare, but as technology advances, such incidents will become more frequent.

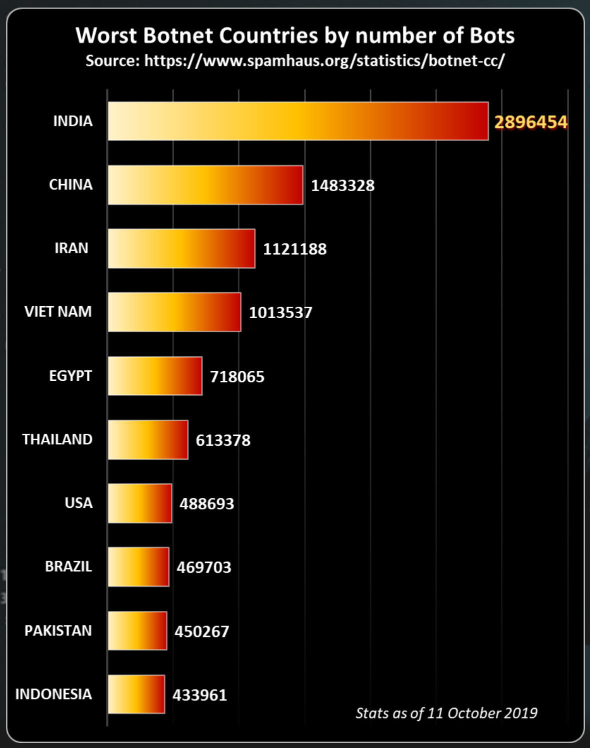
By unquestioningly following instructions, you might be doing the bidding of cybercriminals. It's normal to obey the boss, of course, but it's also critical to question strange or illogical managerial decisions.

We can only advise discouraging employees from following instructions blindly. Try not to give orders without explaining the reason. That way, an employee is more likely to query an unusual order if there's no apparent justification.

From a technical point of view, we recommend:

- Prescribing a clear procedure for transferring funds so that even high-ranking employees cannot move money outside of the company unsupervised. Transfers of large sums must be authorized by several managers.
- Train employees in the basics of cybersecurity and teach them to view incoming orders with a healthy dollop of scepticism.

Read the article here: Kaspersky



Worst Botnet Countries by number of Bots

Source: https://www.spamhaus.org/statistics/botnet-cc/

Country	Bots
INDIA	2896454
CHINA	1483328
IRAN	1121188
VIET NAM	1013537
EGYPT	718065
THAILAND	613378
USA	488693
BRAZIL	469703
PAKISTAN	450267
INDONESIA	433961

Stats as of 11 October 2019

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

According to AV-Test.org, this is total number of

Malware

over the last three years

2017

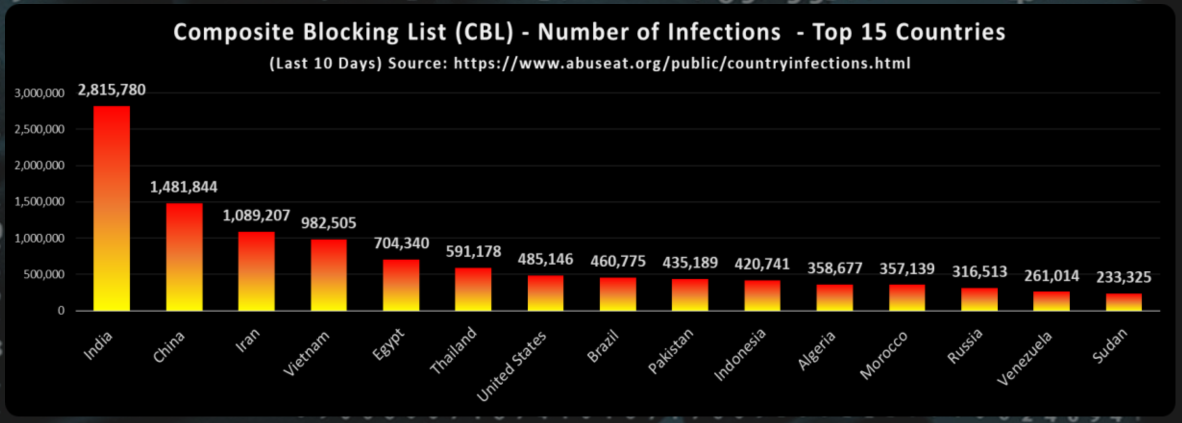
719.15 Million

2018

856.62 Million

2019 (so far)

960.35 Million



Composite Blocking List (CBL) - Number of Infections - Top 15 Countries

(Last 10 Days) Source: https://www.abuseat.org/public/countryinfections.html

Country	Infections
India	2,815,780
China	1,481,844
Iran	1,089,207
Vietnam	982,505
Egypt	704,340
Thailand	591,178
United States	485,146
Brazil	460,775
Pakistan	435,189
Indonesia	420,741
Algeria	358,677
Morocco	357,139
Russia	316,513
Venezuela	261,014
Sudan	233,325

Author: Chris Bester
chris.bester@yahoo.com