Black Friday Edition

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

On November 22, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in 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

29 November 2019

In The News This Week

'Dexphot': A Sophisticated, Everyday Threat

Though this cryptominer has received little attention, it exemplifies the complexity of modern malware, Microsoft says. - Malware threats don't have to have a high profile to be extremely dangerous. Sometimes, even the more common strains can pose big problems. A case in point is "Dexphot," a cryptomining tool that Microsoft has been tracking for the past year and which the company says exemplifies the complexity and fast-evolving nature of even the more everyday threats that organizations now face. Dexphot first surfaced in October 2018 and has since then infected tens of thousands of systems but has received little of the attention that some malware threats receive. Microsoft researchers initially observed the malware attempting to deploy files that changed literally every 20 to 30 minutes on thousands of devices.

The company's subsequent analysis of the polymorphic malware showed it employs multiple layers of obfuscation, encryption, and randomized file names to evade detection. Like many other modern malware tools, Dexphot was **designed to run entirely in memory**. It also hijacked legitimate processes so defenders couldn't easily detect its malicious activity. When Dexphot finally did get installed on a system, it used monitoring services and a list of scheduled tasks to re-infect systems when defenders tried to remove the malware. The authors of the Dexphot have kept upgrading and tweaking the malware in the year since it was first detected, according to Microsoft. Most of the changes have been designed to help the malware evade detection.

What makes Dexphot especially troublesome for defenders is the malware's use of legitimate processes and services for carrying out its activity. In fact, except for the installer that is used to drop the malware on a system, all other processes that Dexphot uses are legitimate system processes, according to a Microsoft blog post. Among them is a process for running programs in DLL files (rundll32[.]exe), another for extracting files from ZIP archives (unzip[.]exe), one for scheduling tasks (schtasks[.]exe), and PowerShell for task automation..

Read the full story by Jai Vijayan here: DARKReading Article

Unsecured Elasticsearch Server Exposed Records of 1.2 Billion

Some 4 terabytes of data on over 1.2 billion individuals - including LinkedIn and Facebook profiles - was exposed to the internet on an unsecured Elasticsearch server, according to an analysis by a pair of independent researchers, Bob Diachenko and Vinny Troia, who discovered the server in October. It's not clear who owns the database or if any of the personally identifiable information it contained has been accessed by hackers or cybercriminals.

The server stored 622 million email addresses, over almost 50 million phone numbers, plus names and profile information from LinkedIn and Facebook, the two researchers told Wired. An examination of the exposed server found that the personal information came from two data enrichment companies, although both said they did not own the cloud-based server, according to the researchers' report. "We regularly look for open Elasticsearch databases and we were just scouring IP address and we found this one and right away we could see that it had 4 terabytes and that it was a pretty large database," Troia told Information Security Media Group. "When we started to dig into it, we found a ton of user profile information and it was just a 'holy wow' moment ... At a glance we saw almost 4 billion user records and once we went through it and did deduplication, we found 1.2 billion unique records and that's pretty momentous." No password or authentication was needed to access the database, the researchers say. Troia told ISMG that he notified the FBI about the database, and then within a few hours, someone pulled the server and the exposed data offline. Troia added that when he examined the IP address further, it appears that the server itself dates from November 2018.

"Due to the sheer amount of personal information included, combined with the complexities identifying the data owner, this has the potential to raise questions on the effectiveness of our current privacy and breach notification laws," Diachenko and Troia write in their report.

Read the full story by Scott Ferguson here: BankInfoSec

The Impact of Artificial Intelligence (AI) on Cyber Security

A few weeks ago, someone asked me about the use of Artificial Intelligence (AI) in cybercrime and the counter balances in place in the security world. Not an easy question to answer but I found this article by Aimee Laurence of CPO Magazine that touches on the subject. Perhaps not a complete answer to the question posed but very informative nonetheless.

The Impact of Artificial Intelligence (AI) on Cyber Security - There is currently a big debate raging about whether Artificial Intelligence is a good or bad thing in terms of its impact on human life. With more and more enterprises using AI for their needs, it's time to analyze the possible impacts of the implementation of AI in the cyber security field.

The positive uses of AI for cyber security - Biometric logins are increasingly being used to create secure logins by either scanning fingerprints, retinas, or palm prints. This can be used alone or in conjunction with a password and is already being used in most new smartphones. Large companies have been the victims of security breaches which compromised email addresses, personal information, and passwords. Cyber security experts have reiterated on multiple occasions that passwords are extremely vulnerable to cyber-attacks, compromising personal information, credit card information, and social security numbers. These are all reasons why biometric logins are a positive AI contribution to cyber security.

AI can also be used to detect threats and other potentially malicious activities. Conventional systems simply cannot keep up with the sheer number of malware that is created every month, so this is a potential area for AI to step in and address this problem. Cyber security companies are teaching AI systems to detect viruses and malware by using complex algorithms, so AI can then run pattern recognition in software. AI systems can be trained to identify even the smallest behaviours of ransomware and malware attacks before it enters the system and then isolate them from that system. They can also use predictive functions that surpass the speed of traditional approaches. Systems that run on AI unlock potential for natural language processing which collects information automatically by combing through articles, news, and studies on cyber threats. This information can give insight into anomalies, cyber-attacks, and prevention strategies. This allows cyber security firms to stay updated on the latest risks and time frames and build responsive strategies to keep organizations protected.

AI systems can also be used in situations of multi-factor authentication to provide access to their users. Different users of a company have different levels of authentication privileges which also depend on the location from which they're accessing the data. When AI is used, the authentication framework can be a lot more dynamic and real-time and it can modify access privileges based on the network and location of the user. Multi-factor authentication collects user information to understand the behaviour of this person and make a determination about the user's access privileges.

To use AI to its fullest capabilities, it's important that it's implemented by the right cyber security firms who are familiar with its functioning. Whereas in the past, malware attacks could occur without leaving any indication on which weakness it exploited, AI can step in to protect the cyber security firms and their clients from attacks even when there are multiple skilled attacks occurring.

Drawbacks and limitations of using AI for cyber security - The benefits outlined above are just a fraction of the potential of AI in helping cyber security, but there are also limitations which are preventing AI from becoming a mainstream tool used in the field. In order to build and maintain and AI system, companies would require an immense amount of resources including memory, data, and computing power. Additionally, because AI systems are trained through learning data sets, cyber security firms need to get their hands on many different data sets of malware codes, non-malicious codes, and anomalies. Obtaining all of these accurate data sets can take a really long time and resources which some companies cannot afford.

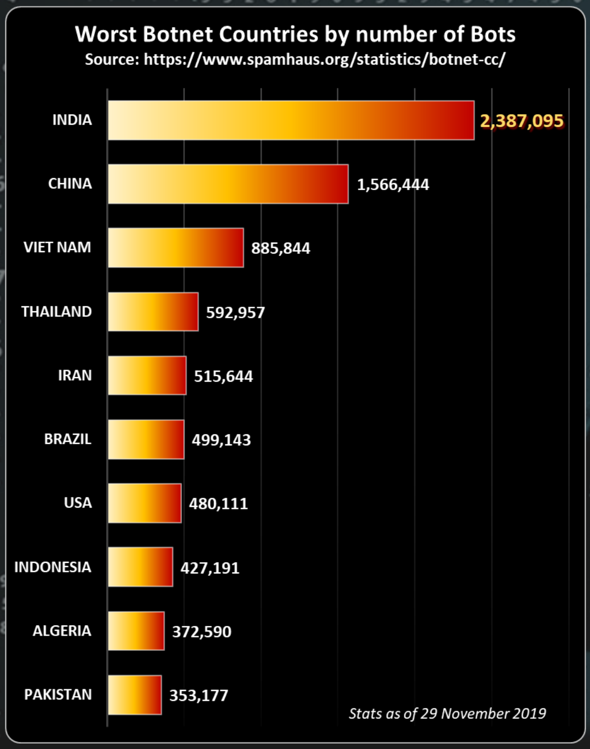
Another drawback is that hackers can also use AI themselves to test their malware and improve and enhance it to potentially become AI-proof. In fact, an AI-proof malware can be extremely destructive as they can learn from existing AI tools and develop more advanced attacks to be able to penetrate traditional cyber security programs or even AI-boosted systems.

Solutions to AI limitations - Knowing these limitations and drawbacks, it's obvious that AI is a long way from becoming the only cyber security solution. The best approach in the meantime would be to combine traditional techniques with AI tools, so organizations should keep these solutions in mind when developing their cyber security strategy:

- Employ a cyber security firm with professionals who have experience and skills in many different facets of cyber security.
- Have your cyber security team test your systems and networks for any potential gaps and fix them immediately.
- Use filters for URLs to block malicious links that potentially have a virus or malware.
- Install firewalls and other malware scanners to protect your systems and have these constantly updated to match redesigned malware.
- Monitor your outgoing traffic and apply exit filters to restrict this type of traffic.
- Constantly review the latest cyber threats and security protocols to get information about which risks you should be managing first and develop your security protocol accordingly.
- Perform regular audits of both hardware and software to make sure your systems are healthy and working.

Following these steps can help mitigate many of the risks associated with cyber-attacks, but it's important to know that your organization is still at risk of an attack. Because of this, prevention is not enough, and you should also work with your cyber security team to develop a recovery strategy.

As the potential of AI is being explored to boost the cyber security profile of a corporation, it is also being developed by hackers. Since it is still being developed and its potential is far from reach, we cannot yet know whether it will one day be helpful or detrimental for cyber security. In the meantime, it's important that organizations do as much as they can with a mix of traditional methods and AI to stay on top of their cyber security strategy.



Worst Botnet Countries by number of Bots

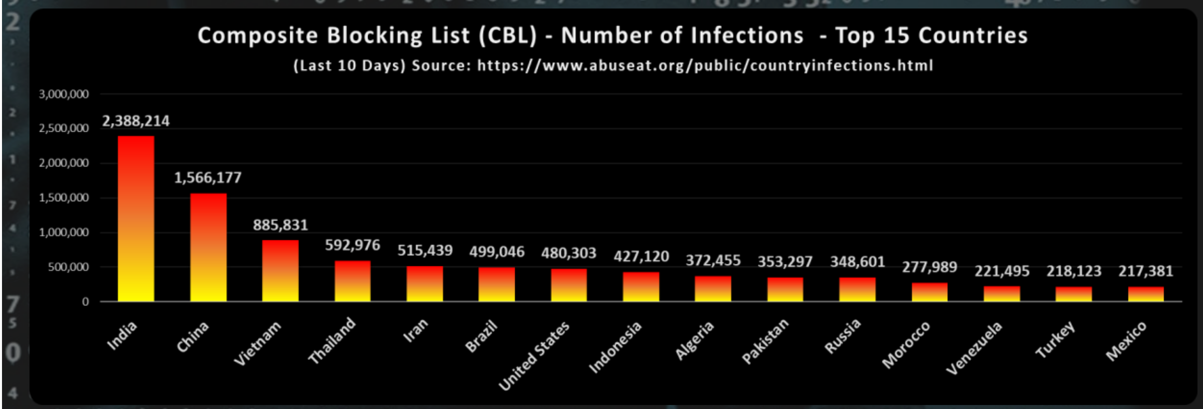
Source: https://www.spamhaus.org/statistics/botnet-cc/

Stats as of 29 November 2019

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

Black Friday

Be careful with your online shopping, make sure your credentials are protected!



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

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

Author: Chris Bester
chris.bester@yahoo.com