On March 30, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in SonicOS, Google, and Sophos products.
CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
01 Apr 22	488,687,261	6,167,243

Deaths this week: 33,322

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
01 April 2022

In The News This Week

'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider

A "powerful" cyberattack has hit Ukraine's biggest fixed line telecommunications company, Ukrtelecom. Described as the most severe cyberattack since the start of the Russian invasion in February, it has sent the company's services across the country down. Victor Zhora, deputy head of the State Service for Special Communications and Information Protection, confirmed to Forbes that the government was investigating the attack. He said it's not yet known whether Ukrtelecom—a telephone, internet and mobile provider—has been hit by a distributed denial of service (DDoS) attack or a deeper, more sophisticated intrusion. The attack has only been acknowledged by Ukrtelecom in responses to customer comments on Facebook. In one, it responded by saying that services were down as a result of a "powerful cyber attack of the enemy." When Forbes messaged Ukrtelecom over Facebook, an automated response was provided, reading, "Currently, there are difficulties in using the internet service from Ukrtelecom. Read the article by Thomas Brewster here: Forbes

U.S. blacklists Kaspersky antivirus as a risk to national security

Antimalware provider Kaspersky Lab has been blacklisted by the U.S. Federal Communications Commission, adding its name alongside Huawei and ZTE as companies that are deemed a threat to national security. The FCC maintains a list of companies which are "deemed to pose an unacceptable risk to national security or the security and safety of United States persons," and added Kaspersky to the list on Friday. Officially, the list now includes China Mobile International USA Inc., China Telecom (Americas) Corp, and AO Kaspersky Labs, as well as their subsidiaries. FCC Commissioner Brendan Carr said in a statement that adding those companies to the list "will help secure our networks from threats posed by Chinese and Russian state backed entities."
Read the rest of the story by Mark Hachman here: PCWorld

Russia threatens 'grave consequences' over cyberattacks, blames U.S.

Russia signalled Tuesday that it's becoming increasingly aggravated by cyberattacks targeting the country, which have come from numerous directions in connection with its unprovoked assault on Ukraine. In a statement, reported on in the media, Russia's foreign ministry pledged to uncover the sources of the recent "cyber aggression" and hold those sources responsible. Reuters reported that Russia used the statement to blame the U.S. for leading the campaign, involving hundreds of thousands of cyberattacks per day against Russia. The cyberattacks have come as Vladimir Putin's forces continue to attack military, government and civilian targets in Ukraine. The English version of the Tass report quotes the Russian foreign ministry as saying that "no one should have any doubts that the cyber aggression unleashed against Russia will lead to grave consequences for its instigators and perpetrators." Read the rest here: JackOfAllTechs

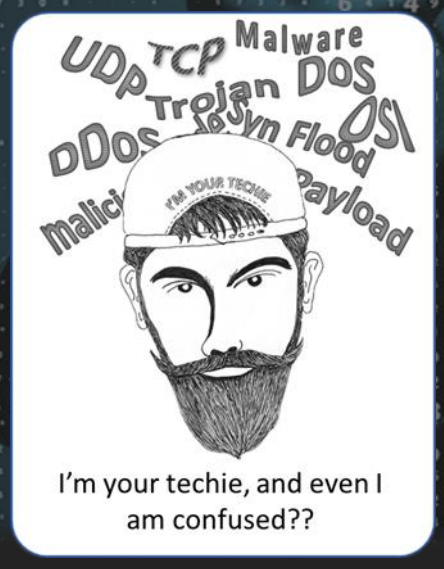
Russia Inches Toward Its Splinternet Dream

For years, the country has been trying to create its own sovereign internet—a goal given new impetus by the backlash to its invasion of Ukraine - RUSSIAN TWITTER USERS noticed something strange when they tried to access the service on March 4: They couldn't. Then came the blackout. Twitter going offline showed how seriously the Russian state took social media's role in amplifying dissent about the country's invasion of Ukraine. And it demonstrated Russia's progress in creating a "splinternet," a move that would effectively detach the country from the rest of the world's internet infrastructure. Read the rest here: Wired

25% Of Workers Lost Their Jobs In The Past 12 Months After Making Cybersecurity Mistakes: Report

For business leaders, there is never a good time for their employees to make mistakes on the job. This is especially true now for workers who have anything to do with the cybersecurity of their companies and organizations. Given the growing risks of cyberattacks across the world and the increased threats posed by Russia in the aftermath of their invasion of Ukraine, these are certainly perilous times. Indeed, a new study released today by email security company Tessian found that one in four employees (26%) lost their job in the last 12 months after making a mistake that compromised their company's security. According to the second edition of Tessian's Psychology of Human Error report, people are falling for more advanced phishing scams—and the business stakes for mistakes are much higher. Read the rest of the article by Edward Segal here: Forbes

For Reporting Cyber Crime in the USA go to the Internet Crime Complaint Center (IC3)



DDoS Attacks in focus

Denial of Service (DoS) attacks has been around for a long time. The first-ever DoS attack occurred in 1974 courtesy of David Dennis, a curious 13-year-old student at University High School, located across the street from the Computer-Based Education Research Laboratory (CERL) at the University of Illinois Urbana-Champaign. The first deliberate DoS-style attack occurred during the week of February 7, 2000, when "mafia boy," a 15-year-old Canadian hacker, orchestrated a series of DoS attacks against several e-commerce sites, including Amazon and eBay. The first known distributed denial of service attack occurred in 1996 when Panix was knocked offline for several days by a SYN flood, a technique that has become a classic DDoS attack. Today, 48 years later, as we see in the media, it is still one of the most prolific cyber attack vectors around. A DoS attack is a denial of service attack where a computer is used to flood a server with TCP and UDP packets (Internet traffic). A Distributed Denial of Service (DDoS) attack on the other hand, is a more sophisticated DoS attack, where the perpetrators will launch an attack from hordes of compromised computers. These compromised computers are computers that were previously infected with a trojan or other type of malicious code, mostly unbeknown to the owner or user of the computer. When the perpetrators start their campaign, and "activate" the compromised machines, it forms a distributed network of machines that can be situated anywhere in the world. These machines could include any networked device like PCs, Servers, or even IoT devices. A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted host server, service or network by overwhelming the target, or its surrounding infrastructure with a flood of Internet traffic from the network of compromised machines. As a simplified illustration, a DDoS attack is like a traffic jam clogging up the highway, preventing regular traffic from arriving at its desired destination.

How does a DDoS attack work?

A DDoS attack requires an attacker to gain control of this network of compromised online machines in order to carry out an attack. Computers and other devices that were infected with malware, are now turned into a bot (or zombie). The attacker then has remote control over the group of bots, which is called a botnet. Once a botnet has been established, the attacker is able to direct the machines by sending updated instructions to each bot via a method of remote control. When the IP address of a victim is targeted by the botnet, each bot will respond by sending requests to the target, potentially causing the targeted server or network to overflow capacity, resulting in a denial-of-service to normal traffic. Because each bot is a legitimate Internet device, separating the attack traffic from normal traffic can be difficult.

What are common types of DDoS attacks?

Different DDoS attack vectors target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made. A network connection on the Internet is composed of many different components or "layers". Like building a house from the ground up, each step in the model has a different purpose. The OSI model is a conceptual framework used to describe network connectivity in 7 distinct layers.
These layers are: (These are normally listed in reverse order as a stack but for the sake of this article, we'll list them in chronological order)

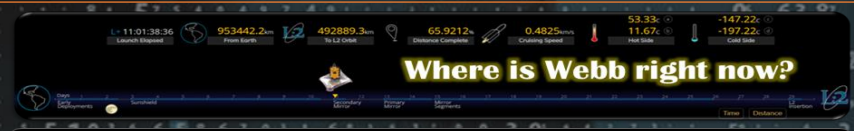
1. PHYSICAL LAYER – Transmits raw bit stream over the physical medium. In other words, the physical stuff like cables and connectors etc. that makes up a network.
2. DATALINK LAYER – Defines the format of the data on the network.
3. NETWORK LAYER – Decides on which physical path the data will travers on the network.
4. TRANSPORT LAYER – Transmitting data using transmission protocols like TCP, UDP etc.
5. SESSION LAYER – Maintains connections and is responsible for controlling ports and sessions.
6. PRESENTATION LAYER – Ensures that data is in a usable format and is where encryption takes place.
7. APPLICATION LAYER – Human to computer interaction layer, where applications can access the network services.

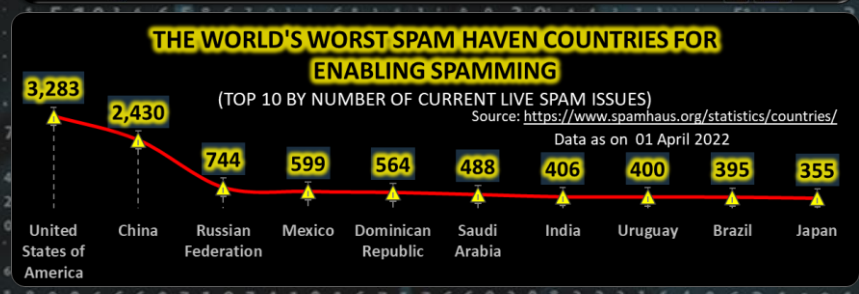
While nearly all DDoS attacks involve overwhelming a target device or network with traffic, attacks can be divided into three categories. An attacker may make use of one or multiple different attack vectors, or cycle attack vectors potentially based on countermeasures taken by the target. **(A) Application Layer Attacks** - Sometimes referred to as a layer 7 DDoS attack, the goal of these attacks is to exhaust the resources of the target. The attacks target the layer where web pages are generated on the server and delivered in response to HTTP requests. A single HTTP request is cheap to execute on the client-side and can be expensive for the target server to respond to as the server often must load multiple files and run database queries in order to create a web page. Layer 7 attacks are difficult to defend as the traffic can be difficult to flag as malicious. **(B) Protocol Attacks** - Protocol attacks, also known as "state-exhaustion" attacks, cause a service disruption by consuming all the available state table capacity of web application servers or intermediate resources like firewalls and load balancers. Protocol attacks utilize weaknesses in layer 3 and layer 4 of the protocol stack to render the target inaccessible. **(C) Volumetric Attacks** - This category of attacks attempts to create congestion by consuming all available bandwidth between the target and the larger Internet. Large amounts of data are sent to a target by using a form of amplification or another means of creating massive traffic, such as requests from a botnet. An example of a volumetric attack is DNS Amplification. A DNS Amplification is like if someone were to call a restaurant and say "I'll have one of everything, please call me back and tell me my whole order," where the call-back phone number they give is the target's number. With very little effort, a long response is generated. By making a request to an open DNS server with a spoofed IP address (the real IP address of the target), the target IP address then receives a response from the server. The attacker structures the request such that the DNS server responds to the target with a large amount of data. As a result, the target receives an amplification of the attacker's initial query.

Resources: Radware, Cloudflare, A10

Other Interesting News and Cyber Security bits:

- Ukrainian software developers share their stories and photos from the war zone
- The Hydrogen Powered Car Is Alive: Sales Up By 84 Percent In 2021
- Anonymous Affiliate Hacks State-Run Russian Broadcaster
- SANS Daily Network Security Podcast (Storm cast)





AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com