As last reviewed On June 19, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in Mozilla Thunderbird and Firefox 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

05 July 2019

In The News This Week

IoT vendor Orvibo gives away treasure trove of user and device data (2 Billion Items).

Two billion items of log data from devices sold by China-based smart IoT device manufacturer Orvibo was found by researchers at web privacy review service vpnMentor, who discovered the data in an exposed ElasticSearch server online. Orvibo has been selling products for smart homes, businesses, and hotels since 2011, ranging from HVAC systems through to home security, energy management, and entertainment systems. The back-end database appears to have been logging system events from lots of them.

Researchers Noam Rotem and Ran Locar found logs from Orvibo devices in China, Japan, Thailand, the US, the UK, Mexico, France, Australia, and Brazil, vpnMentor said in its report.

This data provides insights into the lives of Orvibo's customers, creating potential security risks, it warned. "With over 2 billion records to search through, there was enough information to put together several threads and create a full picture of a user's identity". The logs discovered by the vpnMentor team contained various pieces of personal information, including email addresses, usernames, user IDs, and passwords. Orvibo's developers had used the notoriously insecure MD5 hashing mechanism to protect the passwords. It had also failed to use a salt, which is a random string combined with the password that makes hashed passwords far more difficult to recover.

The log data also included codes required for users to reset their accounts. The company said: "With this code accessible in the data, you could easily lock a user out of their account, since you don't need access to their email to reset the password." The code enables people to reset their email addresses too, meaning that an attacker could deny a user any chance of regaining their passwords.

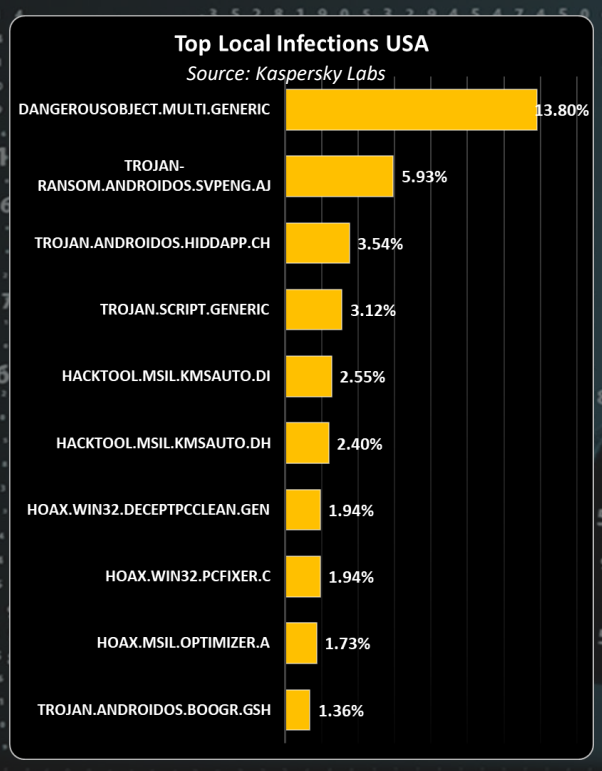
If I can throw in my personal 2 cents worth, I believe if you spend a little bit of time doing research on the products you want to use in your environment, more often than not, you'll come across something that sets of the security alarm bells. Be vigilant before you buy.

Read the full story here: NakedSecurity

Hacker who launched DDoS attacks on Sony, EA, and Steam gets 27 months in prison.

Six years later, DerpTrolling, the hacker who started all the Christmas DDoS attacks, gets prison time. A 23-year-old man from Utah was sentenced this week to 27 months in prison for a series of DDoS attacks that took down online gaming service providers like Sony's PlayStation Network, Valve's Steam, Microsoft's Xbox, EA, Riot Games, Nintendo, Quake Live, DOTA2, and League of Legends servers, along with many others. Named Austin Thompson, but known online as DerpTrolling, the man is the first hacker who started a trend among other hackers and hacking crews -- namely of launching DDoS attacks against gaming providers during Christmas, which they later justified using ridiculous reasons such as "to spoil everyone's holiday," "to make people spend time with their families," or "for the lulz". The hacker's DDoS attacks were extremely successful at the time, in 2013, in a time when most companies didn't use strong DDoS mitigation services. At the time, Thompson used the @DerpTrolling Twitter account to announce attacks and take requests for services users wanted him to take down. While the hacker had been active since 2011, his most famous stretch of activity was between December 2013 and January 2014, when most of his high-profile DDoS attacks took place, before the account going inactive. The attacks caused many online gaming services to go offline, and after seeing DerpTrolling success and the media coverage the hacker got, many other hacking crews followed suit in subsequent years.

Read the full story here: ZDNet Article



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

As per Statista, 2019, In **2017** alone,

269 billion

emails were sent and received each day. This figure is expected to increase to over

333 billion

daily emails in **2022**

What is a DDoS Attack?

In many of the news articles I mentioned in this bulletin, we read about DDoS attacks and today I want to spend some time giving a high level overview or anatomy of such an attack.

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with 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 a network of online machines in order to carry out an attack. Computers and other machines (such as IoT devices) are infected with malware, turning each one 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.

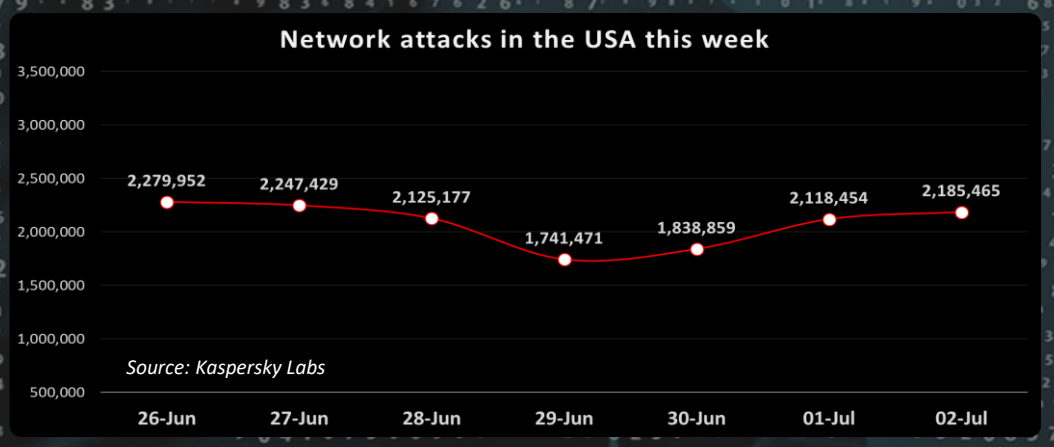
What are common types of DDoS attacks? Different DDoS attack vectors target varying components of a network connection. In order to understand how different DDoS attacks work, it is necessary to know how a network connection is made. A network connection on the Internet is composed of many different 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, I'll start with one)*

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 one or multiple different attack vectors, or cycle attack vectors potentially based on counter measures 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 a 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.

Adapted from an article by CloudFlare that you can find here: CLOUDFLARE Article



Author: Chris Bester
chris.bester@yahoo.com