On June 10, 2020, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Zoom, Google, IBM, 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

12 June 2020

In The News This Week

SMBleed: A New Critical Vulnerability Affects Windows SMB Protocol

Cybersecurity researchers today uncovered a new critical vulnerability affecting the Server Message Block (SMB) protocol that could allow attackers to leak kernel memory remotely, and when combined with a previously disclosed "wormable" bug, the flaw can be exploited to achieve remote code execution attacks. Dubbed "SMBleed" (CVE-2020-1206) by cybersecurity firm ZecOps, the flaw resides in SMB's decompression function — the same function as with SMBGhost or EternalDarkness bug (CVE-2020-0796), which came to light three months ago, potentially opening vulnerable Windows systems to malware attacks that can propagate across networks.

The newly discovered vulnerability impacts Windows 10 versions 1903 and 1909, for which Microsoft released security patches this week as part of its monthly Patch Tuesday updates for June. The development comes as the US Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory last week warning Windows 10 users to update their machines after exploit code for SMBGhost bug was published online last week. SMBGhost was deemed so serious that it received a maximum severity rating score of 10.

Read the full story here: The Hacker News

'CallStranger' vulnerability affects billions of UPNP devices

A newly disclosed vulnerability named "CallStranger" affects billions of connected devices and can be exploited to steal data or initiate large-scale DDoS attacks. CallStranger was disclosed Monday by Yunus Çadırcı, senior cybersecurity manager at EY Turkey. The vulnerability affects the Universal Plug and Play (UPNP) protocol, which is widely used by a variety for devices, from enterprise routers and IoT devices to video game consoles and smart TVs. "The vulnerability -- CallStranger -- is caused by a Callback header value in the UPnP SUBSCRIBE function that can be controlled by an attacker and enables an SSRF [server-side request forgery]-like vulnerability, which affects millions of Internet facing and billions of LAN devices," Çadırcı wrote on the research site. The vulnerability, CVE-2020-12695, can allow unauthorized users to bypass security products such DLP and exfiltrate data or abuse connected devices for DDoS attacks that use TCP amplification.

Read the full article by Rob Wright here: TechTarget

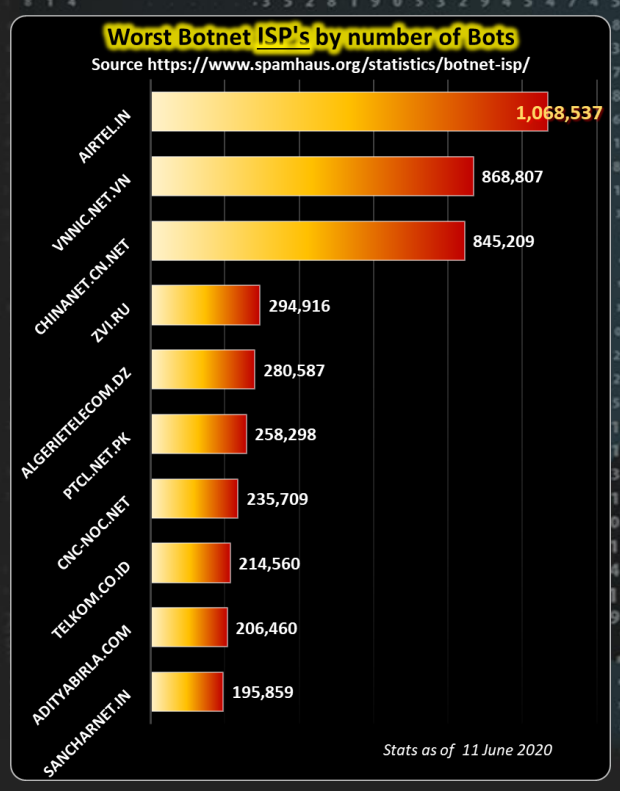
Dark Basin, a hack-for-hire group that remained under the radar for 7 years

A hack-for-hire group tracked as Dark Basin targeted thousands of journalists, advocacy groups, and politicians worldwide over 7 years. - Researchers from Citizen Lab uncovered the operations of a hack-for-hire group tracked as Dark Basin that targeted thousands of journalists, elected and senior government officials, advocacy groups, and hedge funds worldwide over 7 years. Dark Basin is a group of cyber mercenaries that conducted commercial espionage for its customers, the researchers from Citizen Lab linked it to BellTroX InfoTech Services ("BellTroX"), an Indian technology company. "We give the name Dark Basin to a hack-for-hire organization that has targeted thousands of individuals and organizations on six continents, including senior politicians, government prosecutors, CEOs, journalists, and human rights defenders." reads the report published by Citizen Lab. "Over the course of our multi-year investigation, we found that Dark Basin likely conducted commercial espionage on behalf of their clients against opponents involved in high profile public events, criminal cases, financial transactions, news stories, and advocacy." The report published by the experts provides detailed info on several clusters of targets hit by the group. Read the full article by Pierluigi Paganini here: SecurityAffairs

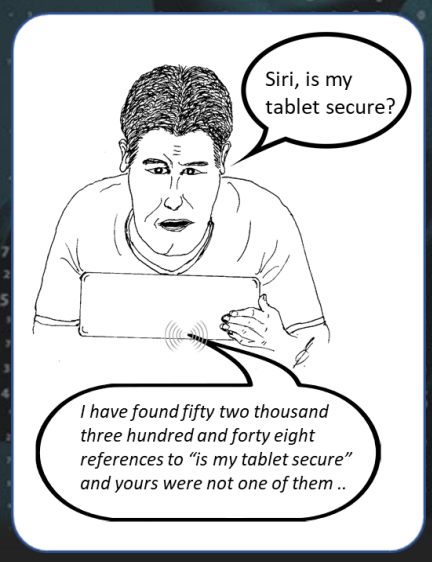
NSA: Russia's Sandworm Hackers Have Hijacked Mail Servers

In a rare public warning, the US spy agency says the notorious arm of Russian military intelligence is targeting a known vulnerability in Exim. - When that warning comes from the National Security Agency, and the hackers are some of the most dangerous state-sponsored agents in the world, run-of-the-mill email server hacking becomes significantly more alarming.

Read the full story here: Wired



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



Anatomy of a Ransomware Attack

With Ransomware making headlines this week with attacks on Honda, NHS, Life Healthcare Group and others, I though it apt to put it under the looking glass this week. The exabeam threat report give an excellent analysis on the Ransomware phenomena and it is packed with useful information that is easy to understand. Below then is an adapted extract of parts of the report but do yourself a favour and read the full report, you will not be sorry. It gives insights on the inner workings of the Ransomware Business and how to deal with Ransomware once hit, etc.

Adapted Exabeam Threat Report Extract

One of the most glaring differences between typical malware and ransomware is that the second ransomware finishes its activity; it announces its presence to the user. It does this because it has already taken the victim's machine and files hostage and wants to demand ransom in exchange for the return of these assets. The confluence of various factors sparked our interest in researching ransomware behavior.

DEFINING THE RANSOMWARE KILL CHAIN

After detonating 86 strains of ransomware in our lab, we were able to narrow down the phases of the ransomware's activity to six stages that assemble the "Ransomware Kill Chain". These six stages were ubiquitous across all the strains we tested, and consistent in the face of permutations or improvements to any specific strain. The main stages of the Ransomware Kill Chain are as follows:

CAMPAIGN → INFECTION → STAGING → SCAN → ENCRYPT → PAYDAY

DISSECTING THE KILL CHAIN: ACTIVITY AND ARTIFACTS

After careful analysis of all 86 ransomware specimens, we found a surprising amount of commonality in their behavior. Ultimately, because these strains share a common goal of demanding ransom, the activities they must perform to reach this goal are the same. We assembled the following Ransomware Kill Chain from the six stages which are shared by all ransomware strains:

DISTRIBUTION CAMPAIGN

The first stage in the kill chain is distribution of the installation software to potential victims. During the distribution campaign, users are tricked or forced into downloading and activating a malicious dropper or payload via an email, a watering-hole attack, an exploit kit, or a drive-by-download. This dropper is responsible for kicking off the infection.

INFECTION

Once on the victim's machine, the dropper phones home to download an .exe or other camouflaged executable by connecting to a predefined list of IP addresses that host the C2 server, or by using DGA to connect via pseudo random domains. From this point, the dropper usually copies the malicious executable to a local directory such as Temp folder or %AppData%/local/temp. Finally, the dropper script is terminated, removed, and the malicious payload is executed.

STAGING

During the Staging phase, the ransomware performs various housekeeping items to ensure smooth operation, such as moving itself to a new folder then dissolving, checking the local configuration and registry keys for various rights, such as proxy settings, user privileges, accessibility, and other potentially meaningful information. The ransomware also performs several persistence steps into the system, such as running at boot, run when in recovery mode, disabling recovery mode, etc. Finally, it uses various commands to delete shadow copies of the files from the system. Ransomware also communicates with C2 at this stage to either get the ransomware's public key negotiated, or to perform recon on the user/system using online IP analytic tools to determine whether or not they are an applicable target.

SCANNING

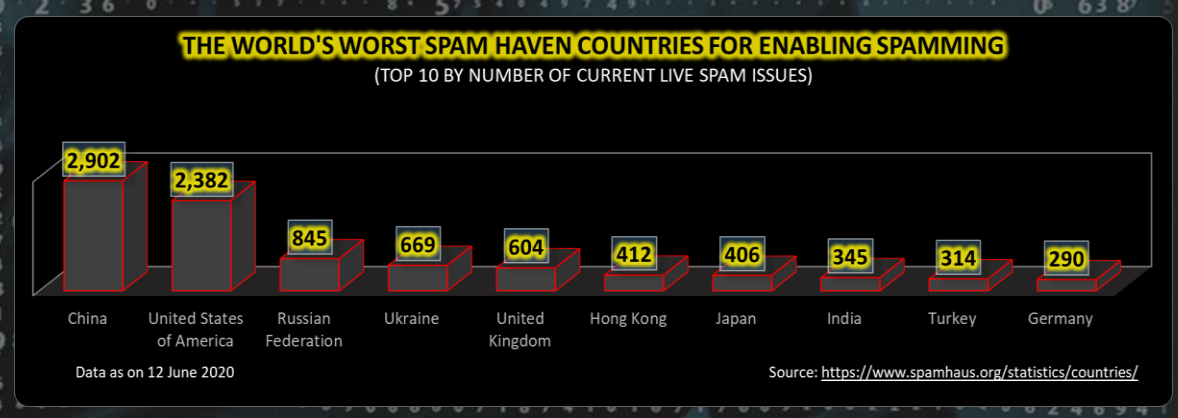
Now that the ransomware has set itself up, and is equipped to persist in the face of shutdowns or reboots, it prepares to take files hostage. To do this, the Ransomware enumerates both the local system and network-accessible systems, searching for a predefined list of file extensions of interest. The ransomware scans and maps the locations containing those files, both locally and on both mapped and unmapped network-accessible systems as well as cloud file storage repositories such as Dropbox, and others; which may also be included. The scanning phase presents security analysts with the first real opportunity to interrupt the Ransomware Kill Chain. While scanning the local machine and synced cloud folders can be accomplished in seconds, mapping out a large corporate network, investigating the results of the scan, checking for read and write permissions, etc. can take minutes to hours depending on the amount of information which must be assessed.

ENCRYPTION

Until the encryption phase, nothing potentially irreversible has happened. The ransomware has simply unpacked itself and performed reconnaissance on the system within which it exists. Beginning with the Encryption phase, control of the situation begins to tilt in favor of the hacker as the ransomware begins to encrypt all of the files it discovered while scanning. All encryption happens locally on the infected machine, meaning that for each file that must be encrypted, the ransomware must fetch the file, encrypt it, upload the newly encrypted version to the original location, and then delete the original file. For every location where files have been found and encrypted, copies of auto-generated ransom notes are created in multiple formats, including .html, .txt, and scripts.

PAYDAY

Once encryption is complete, the ransomware explicitly displays a ransom note to the victim in various ways. With its mission complete, the last task the ransomware usually performs is to terminates and delete itself. At this point, hackers simply wait for ransom to be paid to a bitcoin wallet they own. Victims on the other hand must decide whether to pay the ransom or part ways with the files which were encrypted by the ransomware. As noted during the payment section of this paper, many types of ransomware are pre-configured to have timeout thresholds where the ransom price increases or the software begins to delete encrypted files. After ransom has been paid, victims are typically provided with a link they can use to download a key or decryption program.



Author: Chris Bester (CISA,CISM)
chris.bester@yahoo.com