The Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Nagios, Apple, Google, SonicWall, and Microsoft products. See Latest CIS Advisories

Covid-19 Global Statistics

Date	Confirmed Cases	Total Deaths
08 Oct	237,519,284	4,848,652

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

08 October 2021

In The News This Week

Pandora Papers: Massive data leak exposes hidden wealth of world leaders

The secret wealth and dealings of world leaders, politicians and billionaires has been exposed in one of the biggest leaks of financial documents. Some 35 current and former leaders and more than 300 public officials are featured in the files from offshore companies, dubbed the Pandora Papers. They reveal the King of Jordan secretly amassed £70m of UK and US property. They also show how ex-UK PM Tony Blair and his wife saved £312,000 in stamp duty when they bought a London office. The couple bought an offshore firm that owned the building. The leak also links Russian President Vladimir Putin to secret assets in Monaco, and shows the Czech Prime Minister Andrej Babis - facing an election later this week - failed to declare an offshore investment company used to purchase two villas for £12m in the south of France.... Read the full story here: BBC News

Twitch blames server error for massive data leak

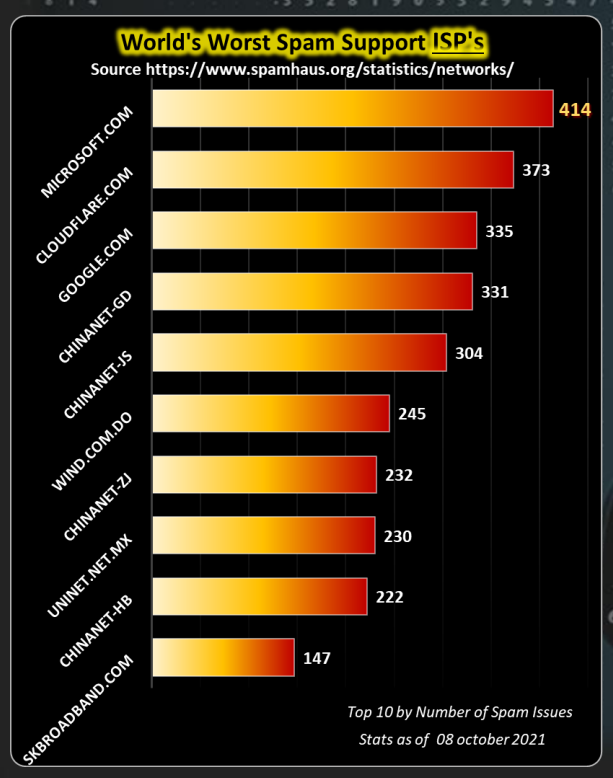
Livestreaming site Twitch says an "error" caused the unprecedented leak that posted vast amounts of sensitive data online this week. The data appeared to include Twitch's internal code and documents, as well as the payments made to thousands of top streamers. Twitch now says the breach was caused by a "server configuration change" that "exposed" some data. But it has not confirmed if all the data posted online is genuine. The Amazon-owned company said the breach had involved "a Twitch server configuration change that was subsequently accessed by a malicious third party". "As the investigation is ongoing, we are still in the process of understanding the impact in detail," it said. But as Twitch streamers and viewers alike scrambled to change passwords, the company also said it: (a) had "no indication" login details were compromised "at this time" (b) did not store users' credit-card information, so that kind of financial information could not have been exposed (c) was resetting all users' stream keys - the unique code used by streaming software to broadcast to the right Twitch account.
Read the full story here: BBC News

Pegasus spyware maker ends contract with UAE after UK high court's hacking ruling

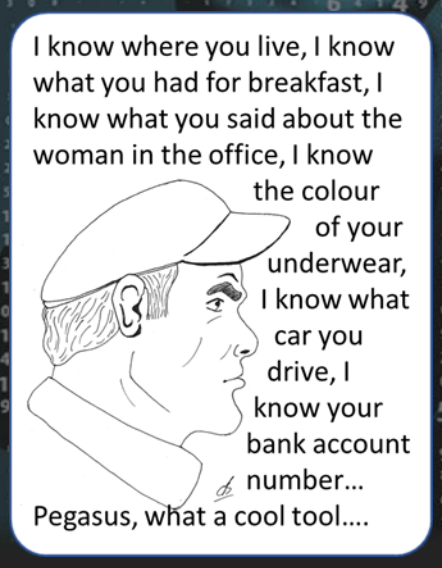
The Israeli manufacturer of Pegasus spyware said Thursday it had terminated its contract with the United Arab Emirates (UAE) in the wake of a ruling by England's high court that Dubai's ruler hacked his ex-wife's phone using the software. Andrew McFarlane, the UK's most senior family court judge, said in his ruling on Wednesday that Sheikh Mohammed bin Rashid al-Maktoum used agents of Dubai and the UAE to hack into and monitor the phones of his ex-wife Princess Haya bint al-Hussein, her legal advisers, and staff, during an ongoing child custody battle concerning their two children using Pegasus software licensed to Dubai and the UAE by the NSO Group.
"Whenever a suspicion of a misuse arises, NSO investigates, NSO alerts, NSO terminates. NSO is proud to prove its commitment to protect human rights," the company's statement read. "The Court expressed its appreciation of NSO's cooperation which was given although NSO is not within the jurisdiction of the court."
Read the full story here: CNN

Iranian Hacking Group Discovered Targeting Aerospace and Telecom

A newly discovered hacking group with alleged ties to the Iranian government has waged a year long campaign to steal information from aerospace and telecommunications companies in the Middle East, the U.S., Europe and Russia, according to cybersecurity researchers. The hacking group, dubbed MalKamak by the researchers, disguised its activities by using the U.S.-based file storage service Dropbox Inc. as the "command and control" server from which it orchestrated hacking operations, according to a report published by Cybereason Inc. on Wednesday. The use of Dropbox helped conceal the hackers' activity, making it look like the network traffic from compromised computers was associated with legitimate uploads and downloads from the Dropbox website, Cybereason found. While the group has carried out a targeted spying operation since 2018, Cybereason said it only recently discovered it after identifying the group's involvement in a hack on a Middle Eastern company.
A representative for Dropbox said it had disabled an account identified by Cybereason as belonging to the hackers. A representative for the Iranian government didn't respond to requests for comment..
Read the story here: Bloomberg



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



The World's Most Notorious Spyware

Spyware is in the news. In a press release this week, Amnesty International talks about Togo activists that were targeted by shadowy cyber-mercenaries using a Spyware Variant Of Chat App produced by the Indian-based DoNot APT Group. Last week I reported how "FinSpy", a product of German-based FinFisher, uses 4 layers of obfuscation to hide its existence and protect itself from discovery on mobile communication devices. This triggered some curiosity and I decided to share some insights into known spyware and some of its capabilities. I said, "known" spyware because we simply don't know if something else is lurking around that has not been discovered yet. To clarify, if I say "spyware", I'm not talking about the run-of-the-mill adware, system monitors, or web tracking trojans, we are talking about physically spying on someone to get the inner details of their daily exitance. Below is a summary of some of the most notorious ones.

FINSPY

Although a desktop version of the spyware exists (not only for Windows, but also for macOS and Linux), the greatest danger largely comes from mobile implants: FinSpy can be installed on both iOS and Android, with the same set of functions available for each platform. The app gives an attacker almost total control over the data on an infected device. The malware can be configured individually for each victim and in such a way that provides the attack mastermind with detailed information about the user, including contacts, call history, geolocation, texts, calendar events, and so on. But that's not all. FinSpy can record voice and VoIP calls, and intercept instant messages. It has the ability to eavesdrop on many communication services — WhatsApp, WeChat, Viber, Skype, Line, Telegram, as well as Signal and Threema.
Getting infected with FinSpy happens the same as with most types of malware. It's most often a case of clicking a link in a malicious e-mail or text message. Android device owners are traditionally in the risk zone, and if their gadgets are also rooted, that greatly facilitates the task of the malware. If, however, the user does not have root access, but a rooting app is installed on the smartphone (as happens when superuser rights are required for installation of some other app), FinSpy can exploit this to obtain the root. Even if a smartphone isn't rooted, and has no rooting apps installed, the spyware can get root access using the DirtyCow exploit. Apple users have a slightly easier time. The iOS version of the spyware requires a system jailbreak. More detail about FinSpy can be found here.

PEGASUS

End-to-end encryption is technology that scrambles messages on your phone and unscrambles them only on the recipients' phones, which means anyone who intercepts the messages in between can't read them. This kind of encryption is good for protecting your privacy, but governments don't like it because it makes it difficult for them to spy on people, whether tracking criminals or snooping on protesters and journalists. This is where the Israeli technology firm, NSO Group comes into play. The company's flagship product is Pegasus, spyware that can stealthily enter a smartphone and gain access to everything on it, including its camera and microphone. Pegasus is designed to infiltrate devices running Android, Blackberry, iOS, and Symbian operating systems and turn them into surveillance devices. The company says it sells Pegasus only to governments and only for the purposes of tracking criminals and terrorists. (Yeah right!).
How it works - Earlier versions of Pegasus were installed on smartphones through vulnerabilities in commonly used apps or by spear-phishing, which involves tricking a targeted user into clicking a link or opening a document that secretly installs the software.
It can also be installed over a wireless transceiver located near a target, or manually if an agent can steal the target's phone.
Since 2019, however, Pegasus users have been able to install the software on smartphones with a missed call on WhatsApp, and can even delete the record of the missed call, making it impossible for the phone's owner to know anything is amiss. Another way is by simply sending a message to a user's phone that produces no notification. This means the latest version of this spyware does not require the smartphone user to do anything. All that is required for a successful spyware attack and installation is having a particular vulnerable app or operating system installed on the device. This is known as a zero-click exploit. Once installed, Pegasus can theoretically harvest any data from the device and transmit it back to the attacker. It can steal photos and videos, recordings, location records, communications, web searches, passwords, call logs and social media posts. It also has the capability to activate cameras and microphones for real-time surveillance without the permission or knowledge of the user. Read more here

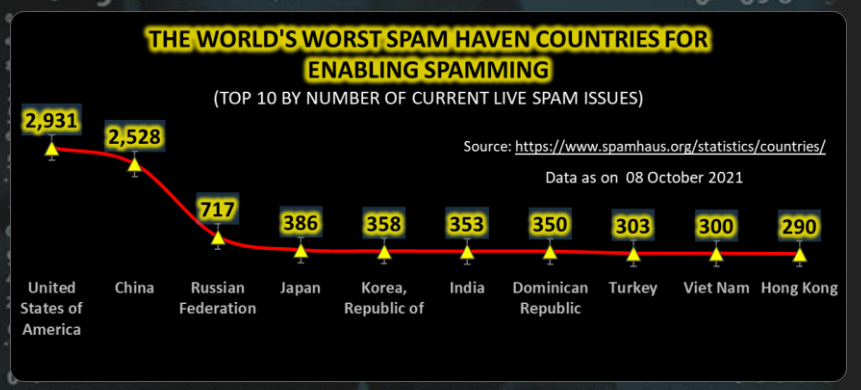
Other Rivals

Further to Pegasus and FinSpy, a host of other similar tools has been seen around which includes the following:
Exodus - This spyware was created by an Italy-based surveillance company eSurv. Unlike Pegasus that needs complex machinery, Exodus follows a two-step process. The malware, which infected phones through an app was to be downloaded by the user. Once downloaded, the hacker can get hold of data ranging from a list of apps, a phone's contact list and even the pictures on the device.
P6-GEO - The surveillance segment is a popular space for Israeli companies. Another company called Picsix has designed a product that can find a person's location, just by using their mobile number. P6-GEO, like its rivals, is most likely used by intelligence agencies.

That is all that I have space for this week. Other References: The Quint, News Nine, Fast Company, WikiLeaks, Anti-Interception

Other Interesting News and Cyber Security bits:

- Facebook down for six hours: Here's what happened
- 58% of Nation-State Cyberattacks Come From Russia
- 5 Best Cybersecurity Videos To Watch In 2021



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