On December 12, 2018, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in multiple Google, Adobe, Apple, PHP, Microsoft, and Mozilla 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
21 December 2018

In the news this Week

Huawei to spend $2bn over five years in cyber security push

Huawei Technologies on Tuesday said it would spend $2 billion over the next five years to focus on cyber security by adding more people and upgrading lab facilities, as it battles global concerns about risks associated with its network gear. The typically secretive Chinese technology giant made the comments at one of its most in-depth press conferences at its Dongguan offices, after welcoming about two dozen international journalists into its new campus in the southern Chinese city. Huawei has been in the news these past weeks for the arrest of its chief financial officer Meng Wanzhou - also the daughter of its billionaire founder Ren Zhengfei - in Canada at the request of the United States. This has exacerbated the woes of the Chinese firm, which has already been virtually locked out of the US market and has been prohibited by Australia and New Zealand from building 5G networks amid concerns its gear could facilitate Chinese spying.
Read the full story here: https://www.itweb.co.za/

Mayday! NASA Warns Employees of Personal Information Breach

Another day, another data breach. This time it's the United States National Aeronautics and Space Administration (NASA) On Wednesday NASA confirmed a data breach that may have compromised personal information of some of its current and former employees after at least one of the agency's servers was hacked. In an internal memo sent to all employees on Tuesday, NASA said the unknown hackers managed to gain access to one of its servers storing the personally identifiable information (PII), including social security numbers, of current and former employees. The agency said NASA discovered the breach on October 23 when its cybersecurity personnel began investigating a possible breach of two of its servers holding employee records. After discovering the intrusion, NASA has since secured its servers and informed that the agency is working with its federal cybersecurity partners "to examine the servers to determine the scope of the potential data exfiltration and identify potentially affected individuals." However, NASA said this process "will take time." According to the agency, any NASA Civil Service employee who joined, left, or transferred within the agency from July 2006 to October 2018 may have had their personal data compromised. NASA currently employs roughly 17,300 people. It should be noted that no space missions were jeopardized by the cyber incident, the agency said. Read the full story at https://thehackernews.com/

Know your Malware - Backdoor.DoublePulsar

DoublePulsar is a backdoor implant tool developed by the U.S. National Security Agency's (NSA) Equation Group that was leaked by The Shadow Brokers in early 2017. This Trojan is a configurable implant found in a data dump released to the public by the Shadow Brokers attack group. It is highly active currently and infection rates are high. When the Trojan is executed, it creates the following file: Doublepulsar-1.3.1.exe. The Trojan communicates with the attacker using either of the RDP or SMB protocols. DoublePulsar runs in kernel mode, which grants cybercriminals a high level of control over the computer system. Once installed, it uses three commands: ping, kill, and exec, the latter of which can be used to load and run any malicious executable file on your system, or even create privileged accounts.

TOP SPAM FOR THE LAST WEEK IN THE USA

#	KNOWN AS	(%)
1	Shikari	68.23%
2	Analysis of Formal Attributes	20.29%
3	Linguistic Analysis	10.48%
4	Other	0.43%
5	Signature Analysis	0.42%
6	Graphical Content Analysis	0.06%
7	Enforced Anti-Spam Update Service	0.04%

Source: Kaspersky Labs

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

According to the Cyren Cyber Threat Report 2018
Nearly **20%** Phishing sites are gone within 3 hours!, **50%** are gone within a day, only about **40%** sticks around for over 2 days

What should you know about the Bitcoin Email Extortion Scam?

A stranger threatens to reveal embarrassing information about you and will remain silent in exchange for a ransom.

Here's the threat delivered to your email: They've infected your system with remote computer control malware. Pay a ransom in bitcoin or they'll release evidence of you watching adult material. They show your password, or part of it, to prove their case. Is this threat credible? No, it's a scam. The bad guys got your information from a breach and are using it to shake you down. The evidence is many-fold:

It's an untargeted, mass email scam
The scammers are not targeting specific individuals. Your inbox is one of thousands in a database. They're only hoping to capitalize on panic and embarrassment to force some small number of people to pay the ransom. Their goal is making fast cash from the volume of people who give in, they're not interested in running high effort blackmail. We know this because the content of the email is nearly identical in many, many reports. Not only is there no concrete proof offered, the scammers actively dissuade the would-be victim from looking for evidence. There's no mention of which adult website you had visited. Your full name often does not appear in the email. There are no images or videos of you attached or linked to.

No malware detected
The emails also claim to have installed malware through which they gathered this incriminating material - yet, malware scans reveal no threats. True, malware scanners vary in accuracy when it comes to more subtle infections. Software capable of remotely accessing your system is not one of those.

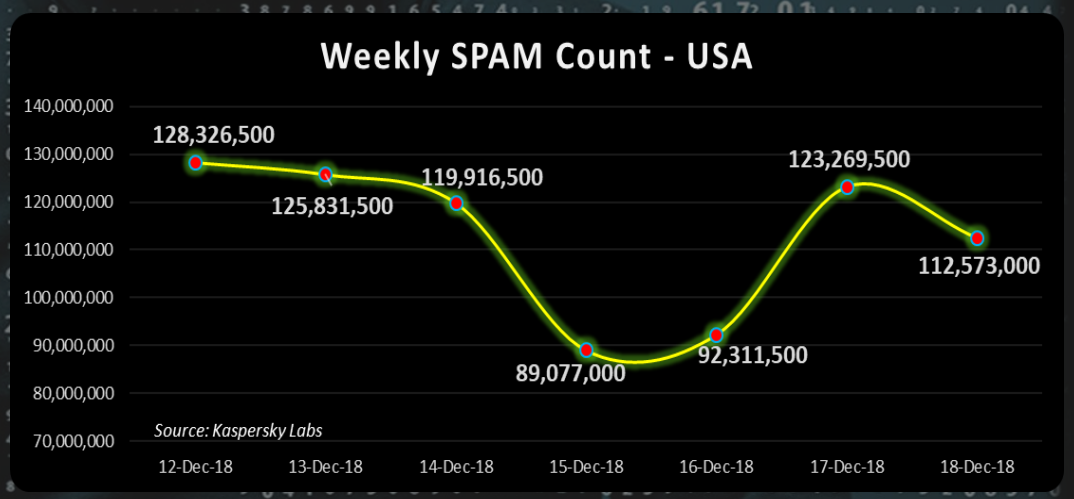
Nothing new under the sun
The history of this threat is also a clue to it being a scam. These reports have been floating around since the end of 2017. The nature of their threat, the amount of money they're demanding and the method of 'evidence' collection has changed but it is essentially the same scam.

So, what should you do?
First, you should not pay this ransom. You should definitely see this as a big wakeup call about your data security. This data was pulled from one of the many data breaches that've been popping up in the last several years. That means that your email and password have been compromised.

Next, act:

1) Whichever password appeared in the email: change it, everywhere and never use it again. You can check if your password has ever appeared in a breach. If it has, never use it again.
2) Adhere to good password practices when creating new passwords. (**Length is far stronger than complexity**, Follow best practices).
3) Run a malware scan on your system - (Malware Bytes or another tool you are familiar with).
4) Consider cloud-based password vaults like 1Password or LastPass. (If you only have to remember **1** master Password, you can make it as secure and strong as possible).
5) Create long and high-strength passwords by forming a memorable phrase, then adding capitalization and punctuation. (It would take a computer running a brute force password cracker approximately 2 Sexdecillion years to crack "Iwaswanderingthroughthetulips1day!" - that's a 2 followed by 96 zeros.)

(Adapted from a Blog published by Julian) - Find the BLOG here: https://www.xenomedia.com/blog/what-should-you-know-about-bitcoin-email-extortion-scam



Author: Chris Bester