Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS Center for Internet Security
By
Chris Bester

On November 28, 2018, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). The MS-ISAC released a Cyber Alert regarding the recent evolution of Business Email Compromise (BEC) scams targeting direct deposit accounts through emailed change requests being sent to Human Resources or Finance departments.

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

07 December 2018

In the news this Week

Marriott – The Starwood Guest Reservation Database Security Incident

On September 8, 2018, Marriott received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database. Marriott quickly engaged leading security experts to help determine what occurred. Marriott learned during the investigation that there had been unauthorized access to the Starwood network since 2014. Marriott recently discovered that an unauthorized party had copied and encrypted information, and took steps towards removing it. On November 19, 2018, Marriott was able to decrypt the information and determined that the contents were from the Starwood guest reservation database.

Marriott has not finished identifying duplicate information in the database, but believes it contains information on up to approximately **500 million** guests who made a reservation at a Starwood property. For approximately **327 million** of these guests, the information includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128). There are two components needed to decrypt the payment card numbers, and at this point, Marriott has not been able to rule out the possibility that both were taken. For the remaining guests, the information was limited to name and sometimes other data such as mailing address, email address, or other information. Marriott reported this incident to law enforcement and continues to support their investigation. We have already begun notifying regulatory authorities.

Marriott deeply regrets this incident happened. From the start, we moved quickly to contain the incident and conduct a thorough investigation with the assistance of leading security experts. Marriott is working hard to ensure our guests have answers to questions about their personal information with a dedicated website and call center. We are supporting the efforts of law enforcement and working with leading security experts to improve. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network.

Dedicated Call Center

Marriott has established a dedicated call center to answer questions you may have about this incident. The call center is open seven days a week and is available in multiple languages.

Email Notification

Marriott began sending emails on a rolling basis on November 30, 2018 to affected guests whose email addresses are in the Starwood guest reservation database. *(Read the whole story here - https://answers.kroll.com/)*

TOP - LOCAL INFECTIONS IN THE LAST WEEK (USA)

#	KNOWN AS	(%)
1	DangerousObject.Multi.Generic	22.69%
2	Trojan.Script.Generic	4.67%
3	Hoax.Win32.Uniblue.gen	3.61%
4	Trojan.MSOffice.SAgent.gen	3.58%
5	Trojan-Ransom.Win32.Blocker.gen	2.83%
6	Trojan-Ransom.AndroidOS.Svpeng.ah	2.42%
7	Exploit.MSWord.Agent.gen	2.25%
8	HackTool.Win64.HackKMS.b	1.75%
9	Hoax.Win32.PCRepair.b	1.58%
10	Hoax.MSIL.Optimizer.a	1.28%

Source: Kaspersky Labs

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

According to Europol IOCTA

2018

Darknet Market AlphaBay (Taken down in 2017) was one of the largest criminal marketplaces to date, hosting over **200 000** users and **40 000** vendors. There were over 250 000 listings for illegal drugs and toxic chemicals on AlphaBay and over **100 000** listings for stolen and fraudulent identification documents, counterfeit goods, malware and other computer hacking tools, firearms and fraudulent services. The site was conservatively estimated to have had USD 1 billion pass through its ledgers since it opened its doors in 2014.

(Read the Report for details)

Avoiding The Security Pitfalls of Online Trading By Mindi McDowel

What is online trading? - Online trading allows you to conduct investment transactions over the internet. The accessibility of the internet makes it possible for you to research and invest in opportunities from any location at any time. It also reduces the amount of resources (time, effort, and money) you have to devote to managing these accounts and transactions.

What are the risks? - Recognizing the importance of safeguarding your money, legitimate brokerages take steps to ensure that their transactions are secure. However, online brokerages and the investors who use them are appealing targets for attackers. The amount of financial information in a brokerage's database makes it valuable; this information can be traded or sold for personal profit. Also, because money is regularly transferred through these accounts, malicious activity may not be noticed immediately. To gain access to these databases, attackers may use Trojan horses or other types of malicious code. Attackers may also attempt to collect financial information by targeting the current or potential investors directly. These attempts may take the form of social engineering or phishing attacks (see Avoiding Social Engineering and Phishing Attacks for more information). With methods that include setting up fraudulent investment opportunities or redirecting users to malicious sites that appear to be legitimate, attackers try to convince you to provide them with financial information that they can then use or sell. If you have been victimized, both your money and your identity may be at.

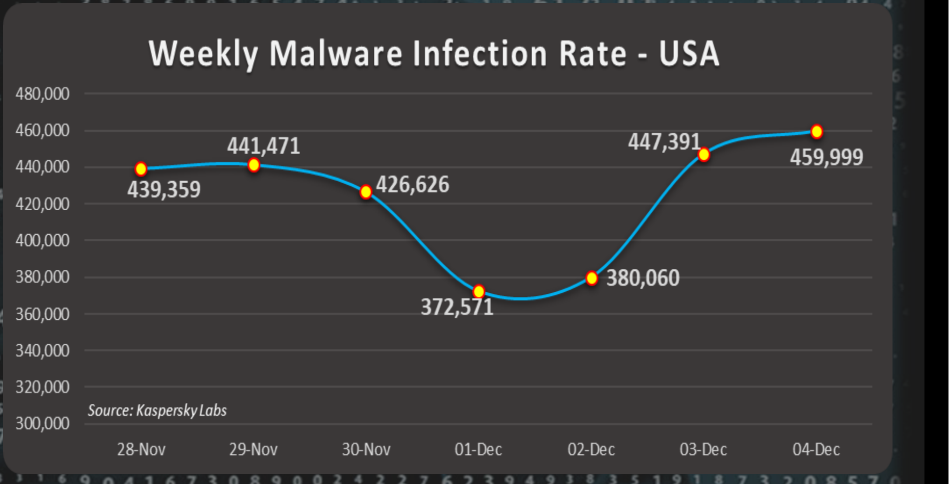
How can you protect yourself? (1) Research your investment opportunities – Take advantage of resources such as the U.S. Securities and Exchange Commission's EDGAR database and your state's securities commission to investigate companies. (2) Be wary of online information – Anyone can publish information on the internet, so try to verify any online research through other methods before investing any money. Also be cautious of "hot" investment opportunities advertised online or in email. (3) Check privacy policies – Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used. (4) Conduct transactions on devices you control – Avoid conducting transactions on public resources such as internet kiosks, computers in places like libraries, and other shared computers and devices. Other users may introduce security risks. (5) Make sure that your transactions are encrypted – When information is sent over the internet, attackers may be able to intercept it. Encryption prevents the attackers from being able to view the information. (6) Verify that the website is legitimate – Attackers may redirect you to a malicious website that looks identical to a legitimate one. They then convince you to submit your personal and financial information, which they use for their own gain. Check the website's certificate to make sure it is legitimate . (7) Monitor your investments – Regularly check your accounts for any unusual activity. Report unauthorized transactions immediately.

(8) Use strong passwords – Protect your computer, mobile devices, and accounts with passwords that cannot easily be. Use different passwords for each account. (9) Use and maintain anti-virus software – Anti-virus software recognizes and protects your computer against most known viruses. However, because attackers are continually writing new viruses, it is important to keep your virus definitions current. (10) Use anti-spyware tools – Spyware is a common source of viruses, and attackers may use it to access information on your computer. You can minimize the number of infections by using a legitimate program that identifies and removes spyware. (11) Keep software up to date – Install software updates so that attackers can't take advantage of known problems or vulnerabilities. Enable automatic updates if the option is available. (12) Evaluate your security settings – By adjusting the security settings in your browser, you may limit your risk of certain attacks

The following sites offer additional information and guidance:

- U.S. Securities and Exchange Commission – https://www.sec.gov/investor/pubs/cyberfraud.htm
- National Consumers League – http://www.fraud.org/scams/general-fraud/investment-fraud
- Local & International Stock Market web sites

Main Source: https://www.us-cert.gov/ncas/tips/ST06-004



Author: Chris Bester