On November 18, 2018, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in WordPress, PostgreSQL, Google Chrome, Adobe, and VMWare.

Breaking News Today!! Marriott Says 500 Million guest records could be leaked!! Read full report next week.

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

30 November 2018

In the news this Week

Dell Resets All Customers' Passwords After Potential Security Breach

Multinational computer technology company Dell disclosed Wednesday that its online electronics marketplace experienced a "cybersecurity incident" earlier this month when an unknown group of hackers infiltrated its internal network. On November 9, Dell detected and disrupted unauthorized activity on its network attempting to steal customer information, including their names, email addresses and hashed passwords. According to the company, the initial investigation found no conclusive evidence that the hackers succeeded to extract any information, but as a countermeasure Dell has reset passwords for all accounts on Dell.com website whether the data had been stolen or not. Dell did not share any information on how hackers managed to infiltrate its network at the first place or how many user accounts were affected, but the company did confirm that payment information and Social Security numbers were not targeted. "Credit card and other sensitive customer information were not targeted. The incident did not impact any Dell products or services," Dell says. You are affected if you have ever created an account on the Dell website to purchase any of their products or to access the online support. "Upon detection of the attempted extraction, Dell immediately implemented countermeasures and initiated an investigation. Dell also retained a digital forensics firm to conduct an independent investigation and has engaged law enforcement," the company said. *(Read the whole story at https://thehackernews.com)*

FBI Shuts Down Multimillion Dollar – 3ve – Ad Fraud Operation

Google, the FBI, ad-fraud fighting company WhiteOps and a collection of cyber security companies worked together to shut down one of the largest and most sophisticated digital ad-fraud schemes that infected over 1.7 million computers to generate fake clicks used to defraud online advertisers for years and made tens of millions of dollars in revenue. Dubbed 3ve (pronounced "Eve"), the online ad-fraud campaign is believed to have been active since at least 2014, but its fraudulent activity grew last year, turning it into a large-scale business and earning their operators more than $30 million in profit. Meanwhile, the United States Department of Justice (DoJ) also unsealed Tuesday a 13-count indictment against 8 people from Russia, Kazakhstan, and Ukraine who allegedly ran this massive online advertising scheme. The 3ve botnet scheme deployed different tactics, such as creating their own botnets, creating fake versions of both websites and visitors, selling fraudulent ad inventory to advertisers, hijacking Border Gateway Protocol (BGP) IP addresses, using proxies to hide real IP addresses, and infecting user's PCs with malware — all to create or generate fake clicks over online ads and get paid. 3ve involved 1.7 million computers infected with malware, over 80 servers in generating fake internet traffic, more than 10,000 counterfeit websites to impersonate legitimate web publishers, and over 60,000 accounts selling ad inventory via more than one million compromised IP addresses to generate 3 to 12 billion of daily ad bid requests at its peak.

"Tech-savvy fraudsters try to produce fake traffic and fraudulent ad inventory to trick advertisers into believing that their ads are being seen by actual, interested users," WhiteOps researchers said.

(Read more about 3ve operations at https://thehackernews.com)

Avoiding Social Engineering and Phishing Attacks

Author - Cybersecurity and Infrastructure Security Agency (CISA)

What is a social engineering attack? - In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack? - Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as natural disasters (e.g., Hurricane Katrina, Indonesian tsunami), epidemics and health scares (e.g., H1N1), economic concerns (e.g., IRS scams), major political elections, holidays.

How do you avoid being a victim? – (1) Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claim to be from a legitimate organization, try to verify his or her identity directly with the company. (2) Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information. (3) Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email. (4) Don't send sensitive information over the internet before checking a website's security (Check if there is a little lock displayed on the URL line). (5) Pay attention to the Uniform Resource Locator (URL) of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). (6) If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group. (7) Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic. (8) Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim? – (a) If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity. (b) If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account. (c) Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future. (d) Watch for other signs of identity theft. (e) Consider reporting the attack to the police, and file a report with the Federal Trade Commission or the Internet Crime Compliant Center (IC3).

Source - https://www.us-cert.gov/ncas/tips/ST04-014

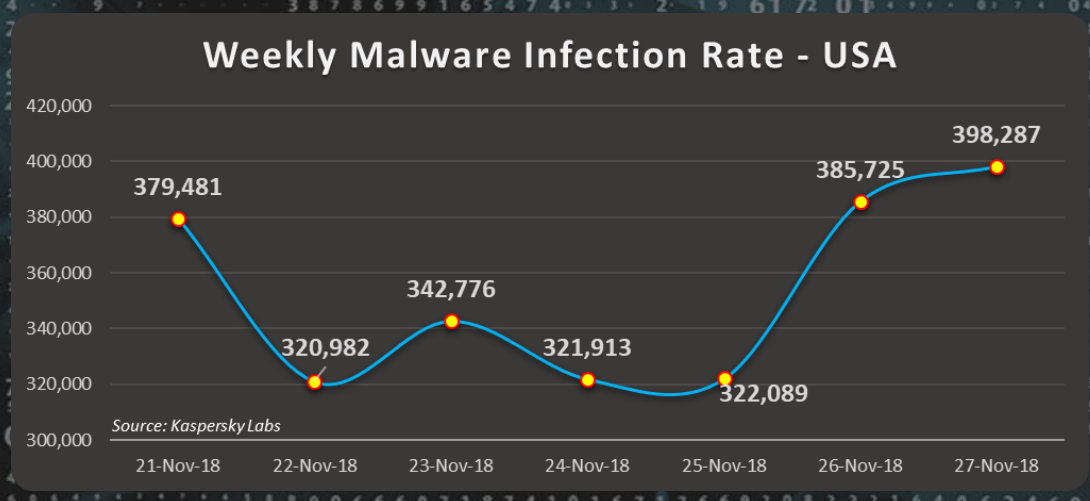
TOP - LOCAL INFECTIONS IN THE LAST WEEK (USA)

#	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 navigate to the Internet Crime Compliant Center (IC3) www.ic3.gov

According to Europol IOCTA 2018 The amount of detected online Child Sexual Exploitation Material(CSEM) continues to grow, creating serious challenges for investigations and victim identification efforts. (Read the Report for details)



Author: Chris Bester (CISA, CISM)