LA-SAFE CYBER DIGEST

July 06, 2018

HACKING INCIDENTS | DATA BREACHES

Cyanweb Solutions Loses Nearly All Website and Backup Data in Hack – **CRN – 07.02.2018:** Digital marketing and web provider Cyanweb Solutions, lost nearly all customer data and backups after a "criminal hacking incident" that compromised one of its servers last week. The company did not have offsite backups in place. According to an advisory posted on its website, " While our server admin was distracted by the DDoS attack, the hackers simultaneously infiltrated the server, escalated their privileges and delivered a seek and destroy payload. This payload located and destroyed all backup disk drives, encrypted all user accounts, and deleted any core WordPress database tables using the default wp_ prefix. An estimated 12 percent of customer data survived the attack.

Analyst Note: Cyanweb Solutions' lack of offsite backup and business continuity planning, resulted in an almost total loss of functionality and customer data. Small businesses and local governments continue to be targets of opportunity for cyber criminals and hacktivist. Organizations need to assess their risks and implement mitigating measures to reduce their vulnerabilities and ensure business continuity. Off-site backups and cloud storage options, protected by well thought out Service Level Agreements (SLAs), are key components.

PHISHING | SOCIAL ENGINEERING | CYBERCRIME

New Smoke Loader Campaign Aims at Stealing Multiple Credentials from Many Applications - **Security Affairs – 07.05.2018:** Researchers from Talos security identified a malware campaign leveraging Smoke Loader to steal credentials from a broad range of applications including web browsers, email clients, and other popular applications. The attack chain starts with messages using a weaponized Word document as an attachment, the hackers attempt to trick victims into opening it and enable the embedded macro. Once executed, the macro downloads the TrickBot banking Trojan used to fetch the Smoke Loader backdoor. This is likely an example of malware-as-a-service, with botnet operators charging money to install third-party malware on infected computers.

Analyst Note: Malware as a Service is a growing industry that enables less sophisticated criminals to engage in malware campaigns. Malware as a Service may also be used by sophisticated organizations to obfuscate the source of the campaign, shifting attribution to the middle man botnet operators.

Cryptocurrency Theft an Increasing Factor in Money Laundering - **Dark Reading – 07.03.2018:** The first half of 2018 saw a threefold increase in cryptocurrency theft compared with the full year of 2017, researchers state in CipherTrace's new "Cryptocurrency Anti-Money Laundering Report" for Q2 2018. Attackers launder digital currencies using a variety of tools and technologies, including mixers, chain hopping, privacy coins, and gambling sites. The increase in theft can be attributed to cyber criminals who traditionally targeted financial institutions with phishing attacks, ransomware, and malware, shifting towards attacking cryptocurrency exchanges. Cybercriminals are using a combination of traditional money laundering techniques such as layering, the buying and reselling of expensive goods, as well cryptocurrency tumbling, a process of mixing cryptocurrency from multiple sources and separating the incoming and outgoing blockchains.

Analyst Note: Cryptocurrency used for criminal means is likely to continue to increase. Due to the decentralized nature of cryptocurrency, effective regulation governing its use and disbursement, will be difficult to develop and enforce. Policy makers and law enforcement will need to be proactive in working together to identify current trends and implementing policy and law that addresses future concerns.

Cyber Policy | Regulation

California Enacts New Privacy Law Similar to European Union's GDPR **- Dark Reading - 07.03.2018:**
On June 28, 2018, California governor Jerry Brown signed into law, AB 375, the California Consumer Privacy Act (CCPA) of 2018. The statute - widely seen as one of the toughest privacy laws in the country - will give consumers in the state unprecedented control over any personal information about them that a company might have collected. Starting Jan. 1, 2020, CCPA confers upon California residents the right to ask a business for all data on them that the business might have collected. It will give consumers the right to ask companies not to sell their personal data to third parties or to ask them to delete all of their personal data.
Analyst Note: California, specifically Silicon Valley, is host to a large number of tech companies and innovators. This focus on the tech industry gives California a disproportionate impact on U.S cyber policy. California's Consumer Privacy Act (CCPA) is likely to have a ripple effect throughout the U.S. similar to the EU's General Data Protection Regulation. These new privacy regulations, due to the distributed and global reach of many modern businesses, will influence many companies to examine how they control data in areas both inside and outside of the geographic boarders of EU and California.

MALWARE AND VIRUSES

Geodo Malware Targets Patriotic Expression **– Cofense – 07.03.2018:**
A classic phishing technique involves timing attacks to match major holidays and other global and regional events. One example of this scenario in a phishing attack captured by Cofense Intelligence™ delivering the Geodo botnet malware on July 3, 2018. In this attack the threat actor appeals to the patriotic nature of the Fourth of July holiday and recipients' sense of patriotism in its content. In these messages, the attacker reminds the recipient of the sacrifices of American service member as part of a narrative designed to entice victims to click on the link in the messages to access an Independence Day-themed greeting card. In doing so, the victim will receive a Microsoft Word document equipped with macro scripting designed to download and run the Geodo malware.

ADVANCED PERSISTANT THREAT

Iranian APT Poses as Cyber Security Company to Phish Victims: **- Bleeping Computer – 07.03.2018:**
An Iranian cyber-espionage group attempted to pose as one of the cyber-security firms that exposed its previous hacking campaigns in an effort to spear-phish people interested in reading reports about it.
The group is known by security researchers under the codenames of Charming Kitten, Newscaster, or Newsbeef. According to Israeli cyber-security firm ClearSky Security, the company says the Iranian APT copied its official website and hosted on a lookalike domain at clearskysecurity.net (the official ClearSky website is located at ClearSkySec.com). The fake site included copied pages from ClearSky's public website and changed one of them to include a 'sign in' that would send the victim's credentials to the attackers.

To report Suspicious Activity, Threats, or Tips,
Please contact LA-SAFE at: lafusion.center@la.gov or 800-434-8007 .