
**On January 2, 2019, the Cyber Threat Alert Level was evaluated and is being lowered to Green (Low). Organizations and users are advised to update and apply all appropriate vendor security patches to vulnerable systems and to continue to update their antivirus signatures daily.**

### 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

## 11 January 2019

## In The News This Week

### Cyber Security Concerns amid Government Shutdown Due to Lapse of Congressional Appropriations

The partial government shutdown has widespread implications for the country's Cyber Security capability as various government funded agencies are halted and services stalled. Agencies such as the Cybersecurity and Infrastructure Security Agency's (CISA), has furloughed nearly half the staff as they are dealing with this major setback to protecting vulnerabilities in federal infrastructure. Former Department of Homeland Security (DHS) officials and lawmakers fear the shutdown, now in its 21st day, could have both short- and long-term effects, hurting the new Cybersecurity and Infrastructure Security Agency's (CISA) efforts to get off the ground and potentially pushing existing talent out the door. Other agencies Like the National Institute of Standards and Technology (NIST) posted the following on their website ***"NOTICE: Due to a lapse in government funding, this and almost all NIST-affiliated websites will be unavailable until further notice. NIST websites for programs using non-appropriated funds (NVLAP and PSCR) or those that are excepted from the shutdown (such as NVD) will continue to be available and updated"***
Cyber experts warn foreign adversaries and domestic criminals could take advantage of the shutdown now that fewer resources are working to prevent their hostile and criminal efforts. If the situation does not change soon, the country could face a catastrophic Cyber Defence lapse that could have major implications across the world.

### Massachusetts man gets 10 years in prison for hospital cyberattack

Reuters report that a Massachusetts man was sentenced on Thursday to more than 10 years in prison for carrying out a cyberattack on a hospital on behalf of the hacking activist group Anonymous to protest the treatment of a teenager in a high-profile custody dispute. Martin Gottesfeld, 34, was sentenced by U.S. District Judge Nathaniel Gorton in Boston nearly three years after he was rescued from a disabled powerboat off the coast of Cuba by a Disney Cruise Line ship after fleeing the United States amid a federal investigation. A federal jury in August found him guilty of two counts, including conspiracy to damage protected computers related to cyberattacks he carried out in 2014 on Boston Children's Hospital and another facility. "Make no mistake, your crime was contemptible, invidious and loathsome," Gorton said. Gottesfeld, who beyond serving 121 months in prison must also pay nearly $443,000 in restitution, has been in custody since February 2016. He said he planned to appeal but had no regrets. "I wish I could have done more," he said!
Read the whole story here: www.reuters.com

### Manufacturers Struggle with IoT and Finding Skilled Cybersecurity Staff

Though the manufacturing sector does not attract the sheer volume of total cyberattacks as other areas of the economy, research has shown that coordinated cyber espionage targets manufacturing more than any other sector. A new ISACA and the Digital Manufacturing and Design Innovation Institute (DMDII) survey show that manufacturers face security concerns, including those related to Internet of Things (IoT)-integrated devices and employee error, and that they continue to struggle with finding skilled cybersecurity staff and may be underspending on security training. Some points the survey reveals is that of the 75% of organisations that have an awareness program in place, 37% believe it is totally ineffective. It also reveals that Finding skilled cyber-staff remains challenging; a 1.8 million worker shortage is anticipated by 2022. Read the full story here: www.securitymagazine.com

## Defending Against Illicit Cryptocurrency Mining Activity

The popularity of cryptocurrency, a form of digital currency, is rising; Bitcoin, Litecoin, Monero, Ethereum, and Ripple are just a few types of the cryptocurrencies available. Though cryptocurrency is a common topic of conversation, many people lack a basic understanding of cryptocurrency and the risks associated with it. This lack of awareness is contributing to the rise of individuals and organizations falling victim to illicit cryptocurrency mining activity.

**What is cryptocurrency?** Cryptocurrency is a digital currency used as a medium of exchange, similar to other currencies. However, unlike other currencies, cryptocurrency operates independently of a central bank and uses encryption techniques and blockchain technology to secure and verify transactions.

**What is cryptomining?** Cryptocurrency mining, or cryptomining, is simply the way in which cryptocurrency is earned. Individuals mine cryptocurrency by using cryptomining software to solve complex mathematical problems involved in validating transactions. Each solved equation verifies a transaction and earns a reward paid out in the cryptocurrency. Solving cryptographic calculations to mine cryptocurrency requires a massive amount of processing power.

**What is cryptojacking?** Cryptojacking occurs when malicious cyber actors exploit vulnerabilities—in webpages, software, and operating systems—to illicitly install cryptomining software on victim devices and systems. With the cryptomining software installed, the malicious cyber actors effectively hijack the processing power of the victim devices and systems to earn cryptocurrency. Additionally, malicious cyber actors may infect a website with cryptomining JavaScript code, which leverages a visitor's processing power via their browser to mine cryptocurrency. Cryptojacking may result in the following consequences to victim devices, systems, and networks: **(1)** Degraded system and network performance because bandwidth and central processing unit (CPU) resources are monopolized by cryptomining activity; **(2)** Increased power consumption, system crashes, and potential physical damage from component failure due to the extreme temperatures caused by cryptomining; **(3)** Disruption of regular operations; and **(4)** Financial loss due to system downtime caused by component failure and the cost of restoring systems and files to full operation as well as the cost of the increased power consumption.
Cryptojacking involves maliciously installed programs that are persistent or non-persistent. Non-persistent cryptojacking usually occurs only while a user is visiting a particular webpage or has an internet browser open. Persistent cryptojacking continues to occur even after a user has stopped visiting the source that originally caused their system to perform mining activity.
Malicious actors distribute cryptojacking malware through weaponized mobile applications, botnets, and social media platforms by exploiting flaws in applications and servers, and by hijacking Wi-Fi hotspots.

**What types of systems and devices are at risk for cryptojacking?** Any internet-connected device with a CPU is susceptible to cryptojacking. The following are commonly targeted devices:

- Computer systems and network devices – including those connected to information technology and Industrial Control System networks;
- Mobile devices – devices are subject to the same vulnerabilities as computers; and
- Internet of Things devices – internet-enabled devices (e.g., printers, video cameras, and smart TVs).

**How do you defend against cryptojacking?** The following cybersecurity best practices can help you protect your internet-connected systems and devices against cryptojacking: **(1)** Use and maintain antivirus software. **(2)** Keep software and operating systems up-to-date. **(3)** Use strong passwords. **(4)** Change default usernames and passwords **(5)** Check system privilege policies. **(6)** Apply application whitelisting. **(7)** Be wary of downloading files from websites. **(8)** Recognize normal CPU activity and monitor for abnormal activity. **(9)** Disable unnecessary services. **(10)** Uninstall unused software. **(11)** Validate input. **(12)** Install a firewall. **(13)** Create and monitor blacklists.

*Read the full article with description of defences here:* **https://www.us-cert.gov/ncas/tips/ST18-002**

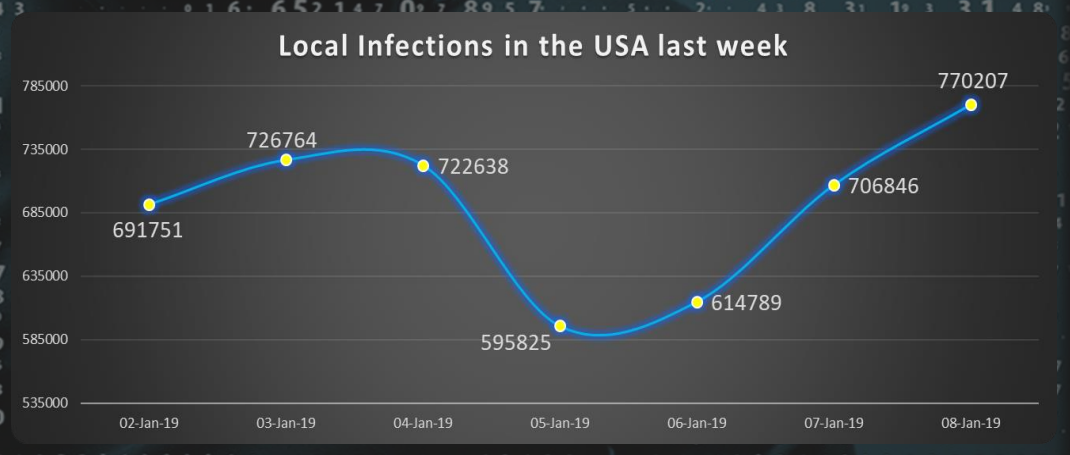
### TOP local Infections registered for last week in the USA

| # | KNOWN AS | (%) |
|---|---|---|
| 1 | DangerousObject.Multi.Generic | 19.08% |
| 2 | Trojan.Script.Generic | 7.45% |
| 3 | Trojan-Ransom.AndroidOS.Svpeng.ah | 5.30% |
| 4 | Trojan-Downloader.MSOffice.SLoad.gen | 2.75% |
| 5 | Hoax.Win32.Uniblue.gen | 2.21% |
| 6 | Hoax.MSIL.Optimizer.a | 1.80% |
| 7 | HackTool.Win64.HackKMS.b | 1.72% |
| 8 | Trojan.PDF.Alien.gen | 1.68% |
| 9 | Trojan-Downloader.OSX.Shlayer.a | 1.51% |
| 10 | Trojan.Win32.Hosts2.gen | 1.22% |

*Source: Kaspersky Labs*

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

According to Dimention Data's Technology Trends 2019 report
The compound annual growth rate of the identity and access management market are predicted to grow from
USD 8.09 billion
USD 14.82 billion
by 2021




Author: Chris Bester