
**On June 5, 2019, the Cyber Threat Alert Level was evaluated and is being raised to Blue (Guarded) due to multiple vulnerabilities in Google Android OS and Chrome.**

### 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

## 14 June 2019

## In The News This Week

### Huawei Represents Massive Supply Chain Risk

A new report from threat intelligence firm Recorded Future says the Chinese technology giant Huawei's enormous product and service footprint gives it access to more data than almost any other single organization in the world and portrays the technology giant as presenting a substantially bigger threat to US interests and organizations than currently perceived.

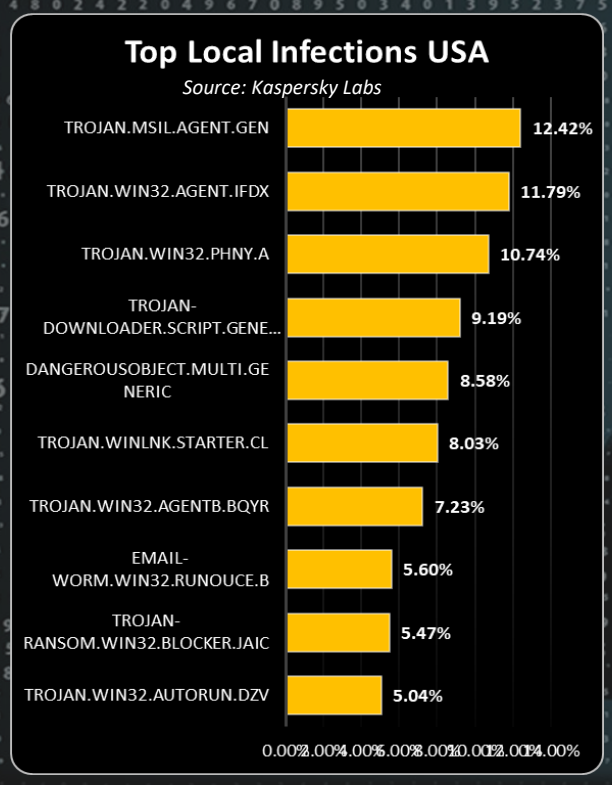
According to the firm, Huawei's enormous range of technologies and products and its global customer base has put the company in a position to access an unprecedented amount of information on organizations, governments, and people worldwide. Huawei's obligations to the Chinese government under various national security and related statutes puts that data at risk of interception and compromise. "The position that Huawei occupies in China and its obligations under that government's laws and regulations cannot be minimized," warns Priscilla Moriuchi, director of strategic threat development at Recorded Future.

"Huawei, as a Chinese company, is not inherently malign," she acknowledges. "However, the people that compose Huawei will at some point likely be forced into making decisions that could compromise the integrity or corporate ambitions of their customers."

President Trump last month signed an executive order that effectively bans US government agencies from buying technologies that are owned by, controlled by, or subject to the laws of foreign adversaries. (Read the executive order here - TrumpExecOrder ) The order cited concerns over the potential for foreign governments to force such vendors to use their technology to spy on US organizations and to conduct widespread espionage — via backdoors, for instance. The executive order also requires contractors that work with the federal government to jettison Huawei technologies from their infrastructure in a phased manner. Read the full story here – DarkReading Article01

### For two hours, a large chunk of European mobile traffic was rerouted through China

For more than two hours on Thursday, June 6, a large chunk of European mobile traffic was rerouted through the infrastructure of China Telecom, China's third-largest telco and internet service provider (ISP). The incident occurred because of a BGP route leak at Swiss data center colocation company Safe Host, which accidentally leaked over 70,000 routes from its internal routing table to the Chinese ISP. The Border Gateway Protocol (BGP), which is used to reroute traffic at the ISP level, has been known to be problematic to work with, and BGP leaks happen all the time. However, there are safeguards and safety procedures that providers usually set up to prevent BGP route leaks from influencing each other's networks. But instead of ignoring the BGP leak, China Telecom re-announced Safe Host's routes as its own, and by doing so, interposed itself as one of the shortest ways to reach Safe Host's network and other nearby European Telco's and ISPs. For the subsequent hours, until China Telecom operators "realized" what they have done, traffic meant for many European mobile networks was rerouted through China Telecom's network. "Some of the most impacted European networks included Swisscom of Switzerland, KPN of Holland, Bouygues Telecom and Numericable-SFR of France," said Doug Madory, Director of Oracle's Internet Analysis division (formerly Dyn). "Often routing incidents like this only last for a few minutes, but in this case many of the leaked routes in this incident were in circulation for over two hours," Madory added. It was China Telecom, again. The same ISP accused last year of "hijacking the vital internet backbone of western countries. Read the full story here: ZDNet Article




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

According to the latest Nokia Threat Intelligence report, global malware infections on phones & IoT devices shows the following:

Android 47.15%
Windows 35.82%
IoT 16.17%
iPhones <1%

## Smartphone Security (Part 5 of 5)

### 9. The ninth layer of protection: install an antivirus.

Install a trustworthy antivirus solution on your smart phone. Although they are generally not as potent as their desktop versions, it's still a better alternative than having no antivirus solution installed, especially if you have an Android device. Also ensure that your antivirus solution on your PC is up to date, if your PC is infected with a virus and you connect your phone to it via USB, then your phone will also be infected. Be careful not to connect your smartphone to unknown computers. They might be infected with malware and end up infecting your mobile too.

According to Nokia's latest threat intelligence report, Android devices are nearly fifty times more likely to be infected by malware than Apple devices. Cyber-criminals are aiming at the largest crowd. Currently, there are more than two billion devices operating the Google-created Android platform making it the most popular end-user OS in the world. The fact that Android is open source makes it a fantastic OS option for many vendors. However, granting companies with the ability to modify the Google-owned OS increase the chances for human error. Small tweaks in the OS can end up being potential security holes.

Apple is strict on getting its users to keep their OS up-to-date. Many are unhappy that Apple always finds a way to make them update and generally want to control everything that appears on the platform. However, it is a fact that if Android users were more diligent in updating their OS, Android-enabled devices would've not been topping the list of most malware-infected products in the world. Making sure that your OS is up-to-date is the first step towards securing your device. Download: Nokia_Threat_Intelligence_Report_2019 here

### 10. The tenth layer of protection: use a secure connection.

Only use secure wireless connections. That means no free or public wi-fi, especially when you're accessing sensitive data (yes, we're talking about that Starbucks connection. And the airport wi-fi or in-store wi-fi also falls under this warning!). Information sent via public networks can be accessed by anyone who knows how to view it. Use your mobile data instead – it will cost you more, but the risk of your data being compromised will be greatly reduced.

A VPN can also protect you – that's short for Virtual Private Network, a network created to protect your activity, that will encrypt your internet traffic and data. You can easily set up a VPN on today's smartphones. Comparitech also has handy guides showing the best VPNs for Android phones and ITProPortal list the best iOS VPN's.

You should also keep your **Bluetooth** turned off when not in use – it's not a secure way to communicate. Enable it only when necessary. Perpetrators can hack into your phone via Bluetooth when they are in close proximity like in a restaurant or coffee shop and most often this will happen without you even knowing it. The average time for a hacker to get into your phone via Bluetooth is 10 seconds.

Adapted from various sources and an article by Cristina Chipurici, which you can find here - HEIMDAL SECURITY

## Malware Report

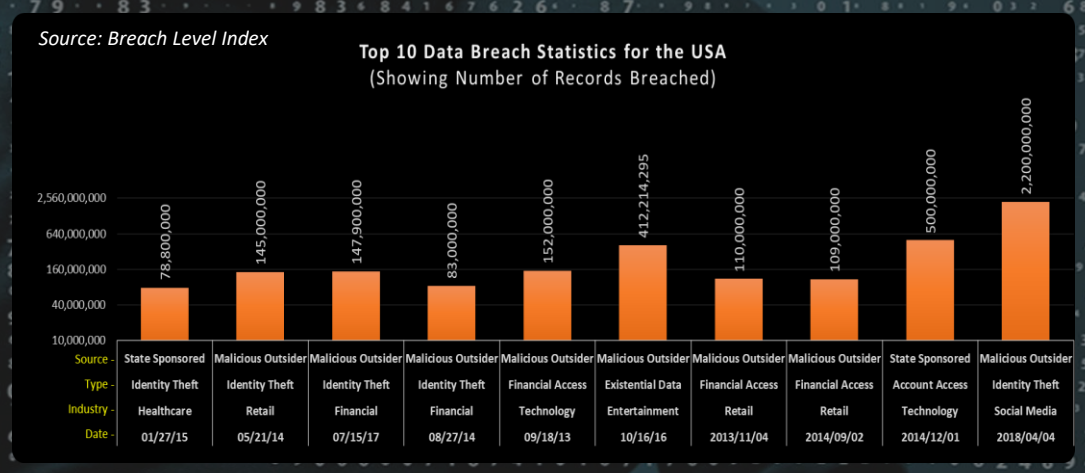
### Buran - New Ransomware Variant

A BleepingComputer posting reports on a new variant of the Vega ransomware which is named Buran. The ransomware is being delivered using the RIG exploit kit. Once installed on to the victim system, the ransomware is written to a file (ctfmon.exe), then executes and begins the encryption process. As is typical of ransomware, there is a list of certain directories, files and file extensions which are not to be encrypted. Files that are encrypted have the victim's unique ID appended as the file extension and the word "Buran" prepended to the head of the file. Further information in the article linked in the Reference section.

Indicators of Compromise:

1. **Hash** (Type SHA256) - 0bed6711e6db24563a66ee99928864e8cf3f8cff0636c1efca1b14ef15941603
2. **Ransomware Executable File**: **ctfmon.exe** (%APPDATA%\microsoft\windows\ctfmon.exe)
3. **Registry Keys**:
   [HKEY_CURRENT_USER\Software\Buran] "Knock"=dword:0000029a
   [HKEY_CURRENT_USER\Software\Buran\Service] "Public"="" "Private"=""
4. **Email Addresses**: polssh1@protonmail.com, polssh@protonmail.com

Reference: xForce(1) & BleepingComputer




**Author: Chris Bester**