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

**On January 16, 2019, the Cyber Threat Alert Level was evaluated and is elevated to Blue (Guarded) due to vulnerabilities in PHP and Oracle Products.**

## 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

18 January 2019

## In The News This Week

### Unprotected Government Server Exposes Years of FBI Investigations

A massive government database belonging to the Oklahoma Department of Securities (ODS) was left unsecured on a storage server for at least a week, exposing a whopping 3 terabytes of data containing millions of sensitive files. The unsecured storage server, discovered by Greg Pollock, a researcher with cybersecurity firm UpGuard, also contained decades worth of confidential case files from the Oklahoma Securities Commission and many sensitive FBI investigations—all wide open and accessible to anyone without any password. Other highly sensitive files exposed included emails, social security numbers, names, and addresses of 10,000 brokers, credentials for remote access to ODS workstations, and communications meant for the Oklahoma Securities Commission, along with a list of identifiable information related to AIDS patients. While the researcher doesn't know exactly how long the server was open to the public, the Shodan search engine revealed that the server had been publicly open since at least November 30, 2018, almost a week after (on December 7) Pollock discovered it. The UpGuard research team notified the ODS department the next day, and the state agency removed 'public access' to the unsecured pathway immediately after they were notified, though it is still unclear whether anyone else accessed the unsecured server. The firm also found passwords that could have allowed hackers to remotely access the state agency's workstations, and a spreadsheet containing login information and passwords for several internet services, including popular antivirus software. In response to the incident, the Oklahoma Securities Commission said in a press release published Wednesday that an "accidental vulnerability" of limited duration was discovered and immediately secured in the server and that the department is taking the issue seriously and ordered a forensic investigation. (Read the full story here: https://thehackernews.com/ )

### A Twitter Bug Left Android Users' Private Tweets Exposed For 4 Years

Twitter just admitted that the social network accidentally revealed some Android users' protected tweets to the public for more than 4 years — a kind of privacy blunder that you'd typically expect from Facebook. When you sign up for Twitter, all your Tweets are public by default, allowing anyone to view and interact with your Tweets. Fortunately, Twitter also gives you control of your information, allowing you to choose if you want to keep your Tweets protected. Enabling "Protect your Tweets" setting makes your tweets private, and you'll receive a request whenever new people want to follow you, which you can approve or deny. It's just similar to private Facebook updates that limit your information to your friends only. In a post on its Help Center on Thursday, Twitter disclosed a privacy bug dating back to November 3, 2014, potentially caused the Twitter for Android app to disable the "Protect your Tweets" setting for users without their knowledge, making their private tweets visible to the public. The bug only got triggered for those Android users who made changes to their Twitter account settings, such as changing their email address or phone number associated with their account, using the Android app between November 3, 2014, and January 14, 2019. Apparently, on January 14, 2019, Twitter rolled out an update for Android application to fix the programming blunder. Although Twitter did not specify exactly how many Android users were affected by this issue, 4 years is a long time duration, and it's likely that most users have changed their account settings at least once in that period.

Twitter said the company has reached out to users whom it knows has been affected by the privacy bug. If you are using Twitter for Android app and your tweets are supposed to be protected, it is definitely a good idea to head on to the "Privacy and Safety" settings of your app and double-check the settings. Desktop and iOS users were not affected by the bug. (Read the full story here: https://thehackernews.com/ )

## Understanding Digital Signatures (by the NCCIC)

**What is a digital signature? A digital signature**—a type of electronic signature—is a mathematical algorithm routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document). Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and protect information in digital messages or documents. In emails, the email content itself becomes part of the digital signature. Digital signatures are significantly more secure than other forms of electronic signatures. **Why would you use a digital signature?** Digital signatures increase the transparency of online interactions and develop trust between customers, business partners, and vendors.

**How do digital signatures work?** Before you can understand how a digital signature works, there are some terms you should know: **(1) Hash Function** - A hash function (also called a "hash") is a fixed-length string of numbers and letters generated from a mathematical algorithm and an arbitrarily sized message such as an email, document, picture, or other type of data. This generated string is unique to the file being hashed and is a one-way function—this means a computed hash cannot be reversed to find other files that may generate the same hash value. Some of the more popular hashing algorithms in use today are Secure Hash Algorithm-1 (SHA-1), the Secure Hashing Algorithm-2 family (SHA-2 and SHA-256), and Message Digest 5 (MD5). **(2) Public Key Cryptography** - Public key cryptography (also known as asymmetric encryption) is a cryptographic method that uses a key pair system. One key, called the private key, encrypts the data and is kept secret. The other key, called the public key, decrypts the data and is distributed openly to others. Public key cryptography can be used several ways to ensure confidentiality, integrity, and authenticity. **(3) Public Key Infrastructure** - Public key infrastructure (PKI) consists of the policies, standards, people, and systems that support the distribution of public keys and the identity validation of individuals or entities with digital certificates and a certificate authority. **(4) Certificate Authority** - A certificate authority (CA) is a trusted third party that validates a person's identity and either generates a public/private key pair on their behalf or associates an existing public key provided by the person to that person. Once a CA validates someone's identity, they then issue that person a digital certificate that is digitally signed by the CA. The digital certificate can then be used to verify a person associated with a public key when requested. **(5) Digital Certificates** - Digital certificates are analogous to driver licenses in that their purpose is to identify the holder of a certificate. Digital certificates contain the public key of the individual or organization and are digitally signed by a certificate authority. Other information about the organization, individual, and certificate authority can be included in the certificate as well. **(6) Pretty Good Privacy (PGP)/OpenPGP** - PGP/OpenPGP is an alternative to PKI. With PGP/OpenPGP, users "trust" other users by signing certificates of people with verifiable identities. The more interconnected these signatures are, the higher the likelihood of verifying a particular user on the internet. This concept is called the "Web of Trust."

Digital signatures work by proving that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed. Digital signatures do this by generating a unique hash of the message or document and encrypting it using the sender's private key. The hash generated is unique to the message or document and changing any part of it will completely change the hash. Once completed, the message or digital document is digitally signed and sent to the recipient. The recipient then generates their own hash of the message or digital document and decrypts the sender's hash (included in the original message) using the sender's public key. The recipient compares the hash they generate against the sender's decrypted hash; if they match, the message or digital document has not been modified and the sender is authenticated.

**Why should you use PKI or PGP with digital signatures?** Using digital signatures in conjunction with PKI or PGP strengthens them and alleviates the possible security issues connected to transmitting public keys, validating that the key belongs to the sender, and verifying the identity of the sender. The security of a digital signature is almost entirely dependent on how well the private key is protected. Without PGP or PKI, proving someone's identity or revoking a compromised key is impossible, and could allow malicious actors to impersonate someone without any method of repudiation. Through the use of a trusted third party, digital signatures can be used to identify and verify individuals and ensure the integrity of the message. As paperless, online interactions are used more widely, digital signatures can help you secure and safeguard the integrity of your data. By understanding how digital signatures work, you are in a position to better protect your information, documents, and transactions.

*Read the full article here:* https://www.us-cert.gov/ncas/tips/ST04-018

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

| # | KNOWN AS | (%) |
|---|---|---|
| 1 | DangerousObject.Multi.Generic | 23.89% |
| 2 | Trojan.Script.Generic | 4.70% |
| 3 | Trojan-Ransom.AndroidOS.Svpeng.ah | 4.11% |
| 4 | Worm.MSIL.Agent.vho | 3.57% |
| 5 | Hoax.MSIL.Optimizer.a | 2.90% |
| 6 | Trojan.PDF.Alien.gen | 2.77% |
| 7 | Hoax.Win32.Uniblue.gen | 1.57% |
| 8 | HackTool.Win64.HackKMS.b | 1.50% |
| 9 | Trojan-Ransom.Win32.Agent.autj | 1.46% |
| 10 | Trojan-Downloader.MSOffice.SLoad.gen | 1.25% |

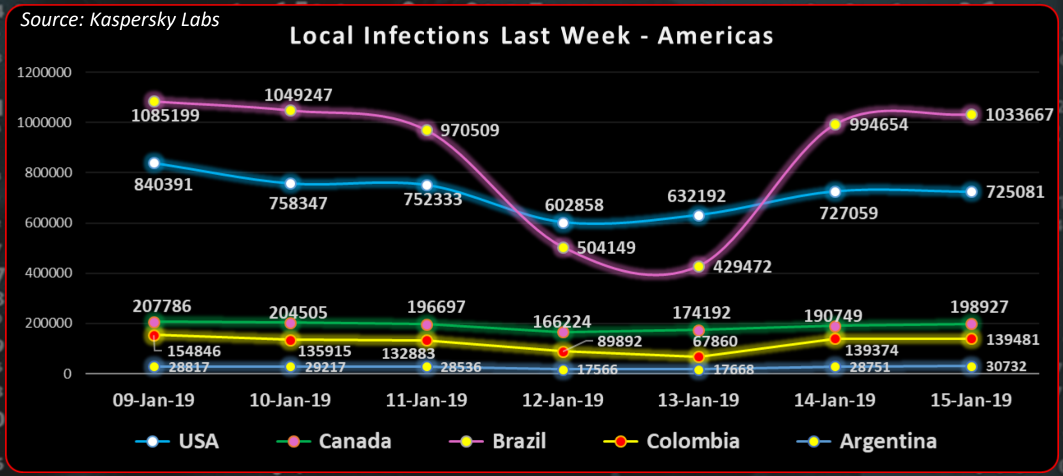
*Source: Kaspersky Labs*

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

**One of Forbes' 60 Cyber Security Predictions for 2019 states:**

"With fraud attack rates expected to continue to increase in 2019, costing e-commerce retailers billions of dollars, **AI** is poised to play a huge role in stopping bad actors in real-time before they strike.

*Source: Kaspersky Labs*



Author: Chris Bester