As per the last Cyber Threat Alert Level Evaluation on July 11, 2019, the alert level is remaining at Blue (Guarded) due to multiple vulnerabilities in Mozilla Firefox and Microsoft 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

26 July 2019

In The News This Week

Siemens contractor pleads guilty to planting logic bomb in company spreadsheets.

A former Siemens contractor has pled guilty last week to planting logic bombs inside spreadsheets he created for the company. For his crimes, David Tinley, 62, from a city near Pittsburgh, now faces up to 10 years in prison, a fine of $250,000, or both.

According to court documents, Tinley provided software services for Siemens' Monroeville, PA offices for nearly ten years. Among the work he was asked to perform was the creation of spreadsheets that the company was using to manage equipment orders. The spreadsheets included custom scripts that would update the content of the file based on current orders stored in other, remote documents, allowing the company to automate inventory and order management.

But while Tinley's files worked for years, they started malfunctioning around 2014. According to court documents, Tinley planted so-called "logic bombs" that would trigger after a certain date and crash the files. Every time the scripts would crash, Siemens would call Tinley, who'd fix the files for a fee. The scheme lasted for two years, until May 2016, when Tinley's trickery was unravelled by Siemens employees.

According to a report from Law360, the scheme fell apart when Tinley was out of town and had to hand over an administrative password for the spreadsheets to Siemens' IT staff, so they could fix the buggy scripts and fill in an urgent order. Siemens IT employees found the logic bomb, and it all went downhill from there. Tinley was charged this May, and pled guilty last week, on July 19. The contractor's sentencing hearing is scheduled for November 8. Read the full story here: ZDNet Article 1

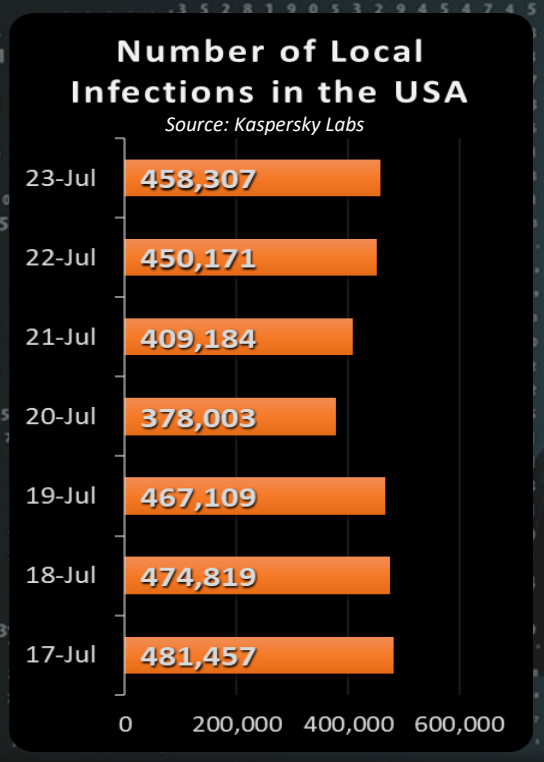
93% of porn sites leak data to a third-party.

In a research paper published this week, academics said that 93% of 22,484 adult websites they analyzed were leaking data to a third-party entity, such as online advertisers or web analytics providers. The list of companies on the receiving end of users' porn browsing habits and sexual preferences includes the likes of Google, Oracle, Facebook, Cloudflare, but also advertisers that were only active in the adult industry. Only 17% of top adult sites have a privacy policy. The research team selected the sites they used for their analysis by scanning the Alexa Top 1 Million list for sites that used the term "porn" in their title or metadata. They identified 22,484 websites, and then analyzed their source code, and looked for the presence of a privacy policy. Inside privacy policies, researchers looked for wording that may indicate if the website is sharing user data with third parties, confirming their source code scans.

"We successfully extracted privacy policies for 3,856 sites, 17% of the total," said the research team, consisting of Elena Maris from Microsoft, Timothy Libert from Carnegie Melon University, and Jennifer Henrichsen from the University of Pennsylvania. "Policies have an average word count of 1,750 and take seven minutes to read," researchers said. "The policies were written such that one might need a two-year college education to understand them." In addition, only 11% of third-parties seen tracking users on an adult web page were also listed in a site's privacy policy, meaning there's a lot of user tracking going on that's not disclosed to users.

TRACKERS EVERYWHERE! But while some sites bothered to set up a privacy policy, some didn't, at all, opting to deploy various trackers in the site's source code or use technology that silently collected data about users' behaviour. Per the research team, Google-related scripts were found on 74% of the 22,484 adult sites, followed by exoClick (40%), Oracle (24%), JuicyAds (11%), and Facebook (10%).

Read the full story here: ZDNet Article 2



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

According to a report by Comparitech, the ransomware attack on the Baltimore City Government in May this year, cost the city over **$18,000,000** to recover. The ransom demanded was only **$76,000** worth of Bitcoin in comparison

SSL/TLS Certificates Explained

Secure Sockets Layer (SSL) and **Transport Layer security** (TLS) are protocols that provide secure communications over a computer network or link. They are commonly used in web browsing and email. In today's tutorial we will look at: (1) TLS and SSL; (2) Public and Private keys; (3) Why we need certificates and what they do; (4) How to get a digital certificate and understand the different common certificate types.

What is TLS - TLS is based on SSL and was developed as a replacement in response to known vulnerabilities in SSLv3. SSL is the term commonly used, and today usually refers to TLS.

Security Provided - SSL/TLS provides data encryption, data integrity and authentication. This means that when using SSL/TLS you can be confident that: **No one has read your message, No one has changed your message and You are communicating with the intended person (server)**.

When sending a message between two parties you have two problems that you need to address. First, how do you know that no one has read the message? Second, how do you know that no one has changed the message?

The solutions to these problems are to: Encrypt it– (This makes the content unreadable so that to anyone viewing the message it is just gibberish) and the Sign it – (This allows the recipient to be confident that it was you who sent the message, and that the message hasn't been changed). Both of these processes require the use of keys. These keys are simply numbers (128 bit being common) that are then combined with the message using a particular method, commonly known as an algorithm (e.g. RSA) to either encrypt or sign the message.

Symmetrical Keys and Public & Private Keys - Almost all encryption methods in use today employ public and private keys. These are considered much more secure than the old symmetrical key arrangement. With a symmetrical key, a key is used to encrypt or sign the message, and the same key is used to decrypt the message. This is the same as the keys (door, car keys) we deal with in everyday life. The problem with this type of key arrangement is if you lose the key anyone who finds it can unlock your door.

With Public and Private keys, two keys are used that are mathematically related (they belong as a key pair) but are different. This means a message encrypted with a public key cannot be decrypted with the same public key. To decrypt the message, you require the private key. For example, if this type of key arrangement were used with your car. Then you could lock the car and leave the key in the lock as the same key cannot unlock the car. This type of key arrangement is very secure and is used in all modern encryption/signature systems.

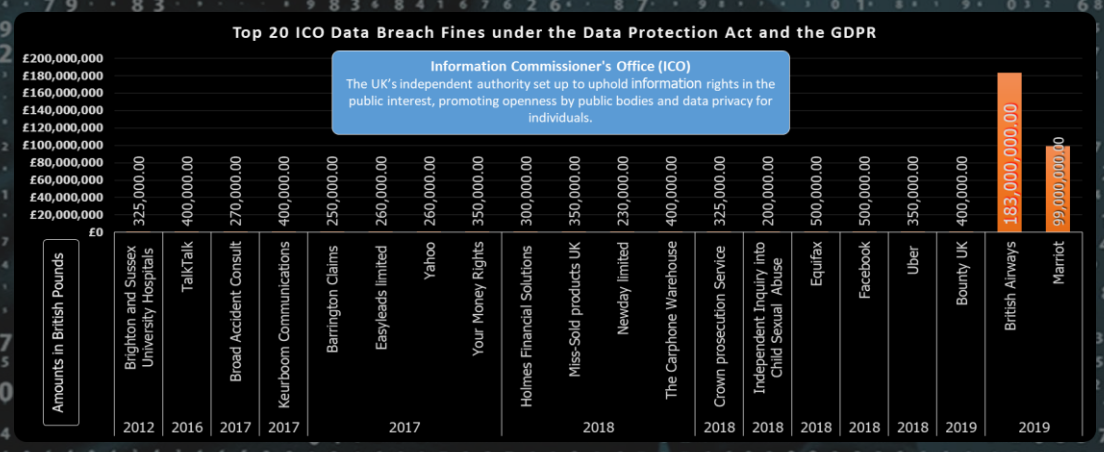
Keys and SSL Certificates - SSL/TLS use public and private key system for data encryption and data Integrity. Public keys can be made available to anyone, hence the term public. Because of this there is a question of trust, and more specifically, how do you know that a particular public key belongs to the person/entity that it claims. For example, you receive a key claiming to belong to your bank, how do you know that it does belong to your bank? The answer is to use a digital certificate. A certificate serves the same purpose as a passport does in everyday life. A passport established a link between a photo and a person, and that link has been verified by a trusted authority (passport office). A digital certificate provides a link between a public key and an entity (business, domain name etc) that has been verified (signed) by a trusted third party (A certificate authority). A digital certificate provides a convenient way of distributing trusted public encryption keys.

Obtaining a Digital Certificate - You get a digital certificate from a recognized Certificate authority (CA). Just like you get a passport from a passport office. In fact, the procedure is very similar. You fill out the appropriate forms add your public keys (they are just numbers) and send it/them to the certificate authority. (this is a certificate Request). The certificate authority does some checks (depends on authority) and sends you back the keys enclosed in a certificate. The certificate is signed by the Issuing Certificate authority, and this is what guarantees the keys. Now when someone wants your public keys, you send them the certificate, they verify the signature on the certificate, and if it verifies, then they can trust your keys.

To illustrate we will look at a typical web browser and web server connection using SSL. (This connection is used on the Internet to send email and when doing online banking, shopping etc.)

START → Browser connects to server Using SSL (https) → Server Responds with Server Certificate containing the public key of the web server. → Browser verifies the certificate by checking the signature of the CA. To do this the CA certificate needs to be in the browser's trusted store → Browser uses this Public Key to agree a session key with the server. → Web Browser and server encrypt data over the connection using the session key.

To read more about Certificate types, Commercial Certificates, Wildcard Certificates, etc. Please visit Steve's Internet Guide where this article was adapted from. You can also look at the 7-Part Blog Series from Entrust to get a better understanding of how digital certificates work.



AUTHOR: CHRIS BESTER
chris.bester@yahoo.com