

"Compilation of cyber-related media reports for the purpose of promoting situational awareness in the government." "This is not vetted intelligence."

NOTE: Please email: james.twist@usma.edu if you wish to be added or removed from the distribution list.

ARMY CYBER INSTITUTE

Weekly Threat Report



ACI-THREAT ANALYSIS CELL for 16 JAN 17 to 31 JAN 17

Yahoo's Email Scan Draws More Questions from European Commission.

Item of Interest: Government Surveillance / Privacy Rights

The European Commission has more questions about the Yahoo email scan. The commission said that the U.S. government has not satisfied its concerns about Sunnyvale-based Yahoo's scan of all users' incoming emails for U.S. intelligence, according to Reuters. Yahoo built software that searched all incoming Yahoo email for specific words or phrases at the request of U.S. intelligence officials. The collection was authorized by a warrant issued FISA, according to a Reuters report late last year. The request was issued under a provision known as Section 702, which is set to expire on Dec. 31, 2017 unless it is renewed by lawmakers.

>>Yahoo's Role in Surveillance. >> Yahoo.gov?

No Hiding From This New Web Fingerprinting Tech: One Browser Can Still Hide Your ID

Item of Interest: Cyber Security / Computer Forensics

Researchers have significantly improved the ability to generate a unique fingerprint for your computer by reading how the operating system and hardware respond to certain browser actions. Cookies used to be the preferred way to track users online, but the same result can be achieved with browser fingerprinting, which uses characteristics of the browser when it visits a site to create a unique identifier for the user. A group of researchers from France's INRIA last year revealed how they could use the configuration of a user's browser and OS when they visit a website to uniquely identify 90 percent of desktops. >>[Browser Fingerprinting](#). >> [99% ID](#).

WhatsApp Encryption Has Backdoor, Facebook Says its "Expected Behavior".

Item of Interest: Encryption / Cyber Security / Privacy Rights

WhatsApp is believed to be one of the most secure messaging applications, considering that it has the ability to encrypt messages in conversations and its founders have said that not even they can access them. However, it seems that a backdoor allows WhatsApp messages to be disclosed. >>[Backdoor to End to End Encryption](#). >> [Backdoor Subverts Encryption](#).

Watson For Cybersecurity.

Item of Interest: Artificial Intelligence / DCO / Analytic Tools

IBM has announced that 40 companies around the world have signed up for its IBM Watson's Beta Cybersecurity Program. The companies will test the ability of IBM's cognitive computing technology to help in the battle against cybercrime. The trial will include representatives of the banking, healthcare, insurance, education and other key industry sectors. Watson for Cyber Security uses technologies such as machine learning and natural language processing, which is being trained to understand the language of security. >> [AI Guarding Cyber Infrastructure](#). >> [AI in Charge of Security?](#)

China Makes VPNs Illegal, Boosts Internet Censorship.

Item of Interest: Government Surveillance / Privacy Rights / Cyber Policy

Chinese authorities have decided to gain even more control over the Internet by restricting the use of virtual private networks. What does this mean? Well, it means that governmental Internet censorship has just been taken to the next level. Up until now, China was known for the "great firewall" on top of the local landmarks. This firewall was used by authorities to block access to large websites they deemed unfit for the local users, such as Twitter, Facebook, YouTube, and many others. In response, local alternatives have been built, which are quite popular among users. >>[More Barriers to Free Speech and Access in China](#). >> [Increased State Control](#).

TECH TRENDS: VULNERABILITIES<LINKS

- Symantec revokes faulty security certificates. [Certs](#).
- Increased Use of Behavioral Analytics. [Way of the Future?](#)
- Driverless Future Won't Start with Driverless Cars. [Logistics](#).
- GitHub Secret Key Finder Released to Public. [TruffleHog](#).
- Mobile Hacking Firm Cellebrite Confirms Server Breach. [High Profile Security Co. Breached](#).
- First came mass MongoDB ransacking: Now copycat ransoms hit Elasticsearch. [Campaign Vs. Servers](#).
- Detroit Car Makers Allegedly Hacked. [Big 3 Hit](#).
- Fired IT worker changed password, wants \$200K. [Data & Services for Ransom by Insider](#).
- Samsung's Smartcams Can Be Hacked to Gain Root Access. [Latest Security Flaw](#).
- Changing Other People's Flight Bookings Is Just Too Easy. [Air Transportation Vulnerabilities](#).
- Don't fall for this new Chrome malware scam. [Trick to Poke Holes in Browser](#).
- US-CERT Warns of Zero-Day Windows Exploit Owned by Shadow Brokers. [0 Day at Large](#).
- CyberDeception Technology. [New Strategy for Defense?](#)
- USAF Cyber Systems Ready for War. [USAF DCO Tools](#).
- HummingBad Malware Is Back and It's Worse than Before. [HummingWhale Haunting Android](#).
- Chinese Data Brokers. [Physical Security Risk](#).

STATS of the WEEK

82% of executives experienced a fraud incident in the past year.

SOURCE:

Heise Security.