THE STATE OF SECURITY (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/)
News. Trends. Insights.

The Top 10 Security Blog Posts of 2015

(HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/DAVID-BISSON/)

DAVID BISSON (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/CONTRIBUTORS/DAVID-BISSON/)

DEC 29, 2015 |
OFF TOPIC (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/TOPICS/OFF-TOPIC/)

(http://www.tripwire.com/state-of-security/off-topic/37192/)

2 7

2015 was a busy year for *The State of Security* blog. Over the past 12 months, we've covered everything from new vulnerabilities to a rundown of computer security films, from the most notorious hacker groups to some of the best conferences in the industry.

As we set our sights for 2016, we know that some of this year's events define 2015 more than others. We also know that these particular developments are likely to shape the security community for years to come.

Provided below is a collection of blog posts whose subjects we feel will have such a lasting impact. (These articles are arranged chronologically.)

WHAT YOU NEED TO KNOW ABOUT SUPERFISH, THE MAN-IN-THE-MIDDLE ADWARE INSTALLED ON LENOVO PCS (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-DATA-PROTECTION/SUPERFISH-LENOVO-ADWARE-FAQ/)

Published: February 19, 2015

Back in February, news broke of an issue called Superfish, a self-signed root certificate installed on Lenovo PCs and laptops that could intercept HTTPS encrypted traffic and insert adverts into users' web browsers. At best, Superfish was a potentially unwanted program (PUP). At worst, it was a potential target for malicious hackers looking to intercept the communication of countless Lenovo customers. Our article explores the problem and includes some relevant resources for affected users.

FORGET BLACKHAT – THE BEST HACKING MOVIES OF ALL TIME (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/OFF-TOPIC/FORGET-BLACKHAT-THE-BEST-HACKING-MOVIES-OF-ALL-TIME/)

Published: February 24, 2015

Following the release of the film *Blackhat*, a review of which can be found here (http://www.tripwire.com/state-of-security/off-topic/blackhat-a-tale-of-cyber-security-buffoonery-and-human-error/), we take a moment to appreciate some of the best hacking movies that came before it. *Wargames*, *The Matrix*, and *Sneakers* are just some of the well-known titles featured in our reminiscence of code-based cinema.

5 SOCIAL ENGINEERING ATTACKS TO WATCH OUT FOR (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-AWARENESS/5-SOCIAL-ENGINEERING-ATTACKS-TO-WATCH-OUT-FOR/)

Published: March 23, 2015

While some attackers use their technical expertise to break into a computer system, others rely on their ability to exploit human weakness. Our article explores the five most common types of social engineering attacks that malicious actors use to exploit human psychology to their advantage, both in the real and digital worlds. Recommendations on how to avoid these types of attacks are also provided.

HOW TO PROTECT YOURSELF FROM CALLER ID SPOOFING (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-AWARENESS/HOW-TO-PROTECT-YOURSELF-FROM-CALLER-ID-SPOOFING/)

Published: April 20, 2015

Caller ID spoofing with intent to defraud, cause harm, and/or wrongfully obtain anything of value is prohibited by the Federal Communications Commission (FCC). However, that doesn't stop telemarketers and scammers from using this technique. Our article serves as a primer on caller ID spoofing, providing readers with an understanding of what the process entails and what you could do if you ever question the number you see on your caller ID.

HOW TO CRASH ANY IPHONE OR IPAD WITHIN WIFI RANGE (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-DATA-PROTECTION/CRASH-IPHONE-WIFI/)

Published: April 22, 2015

One of the highlights of this year's RSA Conference (http://www.tripwire.com/state-of-security/off-topic/rsa-conference-2015-are-you-ready/) in San Francisco was "No iOS Zone," a vulnerability discovered by Skycure's Yair Amit and Adi Sharabani that essentially allows an attacker to crash any and all iOS devices within range of a WiFi hotspot. This vulnerability can be exploited regardless of whether the iOS devices are attempting to connect to WiFi. The only solution? Run and get out of range of the WiFi network.

THE TOP 10 HIGHEST PAYING JOBS IN INFORMATION SECURITY – PART 1 (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/OFF-TOPIC/THE-TOP-10-HIGHEST-PAYING-JOBS-IN-INFORMATION-SECURITY-PART-1/)

Published: May 4, 2015

The first of a two-part series, our article provides job descriptions, required skills, and salary information on the five highest-paying jobs in information security. This article specifically discusses the following positions: Chief Information Security Officer (CISO), Security Architect, Security Director, Security Manager, and Security Engineer. The second part (http://www.tripwire.com/state-of-security/security-awareness/the-top-10-highest-paying-jobs-in-information-security-part-2/) of our series relates information for Incident Responders, Security Consultants, Computer Forensic Experts, Malware Analysts, and Security Specialists.

TOP 10 INFORMATION SECURITY CONFERENCES (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-AWARENESS/TOP-10-INFORMATION-SECURITY-CONFERENCES/)

Published: May 6, 2015

Security personnel love conference season, so we thought we would make their lives a little easier. Our article provides an overview of some of the biggest names in the infosec conference world, including Black Hat USA, BSides, and DEF CON. In a separate article (http://www.tripwire.com/state-of-security/security-awareness/5-lesser-known-gems-in-the-world-of-information-security-conferences/), we also discuss five lesser-known conferences that come highly recommended among infosec professionals.

HOW TO STALK SOMEONE'S LOCATION ON FACEBOOK MESSENGER (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-DATA-PROTECTION/CYBER-SECURITY/STALK-LOCATION-FACEBOOK-MESSENGER/)

Published: May 28, 2015

Marauder's Map, a tool released back in May, allows Facebook users to stalk their contacts by scraping the location data shared from their Facebook Messenger page. This information is plotted on a map, the latitude and longitude lines of which have more than five decimal places of precision. Such accuracy enables users to build a profile of where their contacts work, live, and hang out. Our article discusses this tool and provides step-by-step instructions on how concerned users can disable location sharing in Facebook messenger.

DD4BC GROUP TARGETS COMPANIES WITH RANSOM-DRIVEN DDOS ATTACKS (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/SECURITY-DATA-PROTECTION/CYBER-SECURITY/DD4BC-GROUP-TARGETS-COMPANIES-WITH-RANSOM-DRIVEN-DDOS-ATTACKS/)

Published: June 14, 2015

Earlier this year, news broke about a group called DD4BC that leverages distributed denial-of-service (DDoS) attacks as a means to extort victims into paying ransoms. If the victim does not pay, the group conducts a large-scale DDoS attack against them. Our article explores the history of this group, observes DD4BC's tactics, and provides some information on how companies can protect against DDoS ransom attacks.

IE UNDER ATTACK! MICROSOFT RELEASES EMERGENCY OUT-OF-BAND PATCH (HTTP://WWW.TRIPWIRE.COM/STATE-OF-SECURITY/VULNERABILITY-MANAGEMENT/IE-UNDER-ATTACK-MICROSOFT-RELEASES-EMERGENCY-OUT-OF-BAND-PATCH/)

Published: August 18, 2015

In August, Microsoft published an emergency advisory on CVE-2015-2502, a zero-day vulnerability that could allow an attacker to assume control of a computer if users visited an infected webpage with any version of Internet Explorer. If attackers successfully convinced users to visit a booby-trapped site, they would assume full control of the computer and could then do whatever they wanted with it. Microsoft noted in its advisory that it would release a fix outside of its Patch Tuesday cycle–a clear indication of this vulnerability's severity.

Title image courtesy of ShutterStock (http://www.shutterstock.com/)

2 7

CATEGORIES Featured Articles (http://www.tripwire.com/state-of-security/topics/featured/), Off Topic (http://www.tripwire.com/state-of-security/topics/off-topic/)

TAGS Blogs (http://www.tripwire.com/state-of-security/tag/blogs/), Infosec (http://www.tripwire.com/state-of-security/tag/infosec/), security (http://www.tripwire.com/state-of-security/tag/security/), Top 10 (http://www.tripwire.com/state-of-security/tag/top-10/)

About David Bisson

(http://www.tripwire.com/state-of-security/contributors/david-bisson/)

David Bisson (http://www.tripwire.com/state-of-security/contributors/david-bisson/) has contributed 445 posts to The State of Security.

View all posts by David Bisson (http://www.tripwire.com/state-of-security/contributors/david-bisson/) >

Follow @DMBisson

(http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)
Security Configuration Management
For Dummies (http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

Download Now (http://www.tripwire.com/scm/?utm_source=sos&utm_medium=sb-bnr&utm_content=pdf&utm_campaign=scm-for-dummies)

Latest Security News (/state-of-security/topics/latest-security-news/)

ProxyBack Malware Transforms Infected Systems Into Internet Proxies DEC 29, 2015

Adobe Releases Security Update for 19 'Critical' Vulnerabilities in Flash Player DEC 29, 2015

Database Containing 191 Million US Voters' Personal Data Leaked Online DEC 28, 2015

GOTPass Seeks to Replace Passwords with Images and Patterns DEC 28, 2015

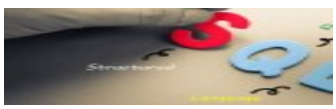
Hyatt Hotels Investigates Malware Found on Payment Processing Systems DEC 24, 2015

POPULAR | FEATURED | RECENT

(http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/a-holiday-nightmare-cryptolocker2-delivered-by-postnord-email-scams/)

A Holiday Nightmare: Cryptolocker2 Delivered by PostNord Email Scams (http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/a-holiday-nightmare-cryptolocker2-delivered-by-postnord-email-scams/)

DECEMBER 27, 2015



(http://www.tripwire.com/state-of-security/security-awareness/rising-danger-from-sql-injection-attacks/)

Rising Danger From SQL Injection Attacks (http://www.tripwire.com/state-of-security/security-awareness/rising-danger-from-sql-injection-attacks/)

DECEMBER 23, 2015

(http://www.tripwire.com/state-of-security/latest-security-news/database-containing-191-million-us-voters-personal-data-leaked-online/)

Database Containing 191 Million US Voters' Personal Data Leaked Online (http://www.tripwire.com/state-of-security/latest-security-news/database-containing-191-million-us-voters-personal-data-leaked-online/)

DECEMBER 28, 2015

Safety – Part of Information Security (http://www.tripwire.com/state-of-security/security-awareness/safety-part-of-information-security/)

DECEMBER 27, 2015

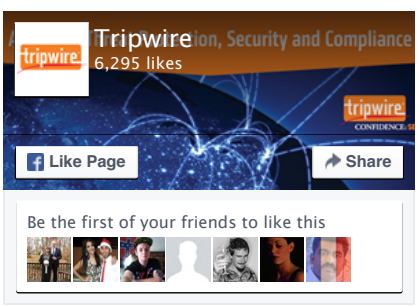
(http://www.tripwire.com/state-of-security/security-awareness/safety-part-of-information-security/)

Hyatt Hotels Investigates Malware Found on Payment Processing Systems (http://www.tripwire.com/state-of-security/latest-security-news/hyatt-hotels-investigates-malware-found-on-payment-processing-systems/)

DECEMBER 24, 2015

(http://www.tripwire.com/state-of-security/latest-security-news/hyatt-hotels-investigates-malware-found-on-payment-processing-systems/)

(http://bit.ly/1Kb6rne)



Topics (/state-of-security/topics/)

- Government
- ICS Security
- Incident Detection
- IT Security and Data Protection
- Latest Security News
- Off Topic
- Regulatory Compliance
- Risk-Based Security for Executives
- Security Awareness
- Security Slice
- This Week in Security
- Tripwire News
- Vulnerability Management

FOLLOW US