Mobile Attacks More Vicious Than Ever, New Blue Coat Report Shows
Mobile Attacks More Vicious Than Ever, New Blue Coat Report Shows

Submitted by: Blue Coat
Wednesday, 28 October 2015

Uptick in Insidious and Malicious Attack Types Turns Mobile Device Users into Cyber Hostages Among Other Manipulations; Sounds Alarm for Both Individuals and Organizations to Strengthen Defenses

SUNNYVALE, Calif., October 28, 2015 – As mobile devices become more deeply woven into the fabric of our personal and work lives, cyber criminals are taking increasingly vicious and disturbingly personal shots at us, according to the 2015 State of Mobile Malware Report (http://dc.bluecoat.com/Mobile_Malware_Report) from Blue Coat Systems (https://www.bluecoat.com/), Inc., a market leader in enterprise security. Cyber blackmail (mobile ransomware attacks) leads the way as a top malware type in 2015, along with the stealthy insertion of spyware on devices that allows attackers to profile behavior and online habits. The new Blue Coat report, available here (http://dc.bluecoat.com/Mobile_Malware_Report), describes the latest trends and vulnerabilities in mobile malware, provides advice for strengthening corporate defenses and educating mobile device users, and offers predictions about the future of mobile threats.

“As we sleep, exercise, work and shop with our mobile devices, cyber criminals are waiting to take advantage of the data these devices collect, as evidenced by the types of malware and attacks we’re seeing,” said Dr. Hugh Thompson, CTO and senior vice president, Blue Coat. “The implications of this nefarious activity certainly carry over to corporate IT as organizations rapidly adopt cloud-based, mobile versions of enterprise applications, opening up another avenue for attackers. A holistic and strategic approach to managing risk must extend the perimeter to mobile and cloud environments—based on a realistic, accurate look at the problem—and deploy advanced protections that can prioritize and remediate sophisticated, emerging and unknown threats.”

Summary of Findings:

- Pornography returned as the number one threat vector after dropping to number two last year.
- The three top types of malware in this year’s report are Ransomware, Potentially Unwanted Software (PUS), and Information Leakage.
- The mobile threat landscape is becoming more active.

Get Your Cyber Flu Shot: Top Infection Vectors of 2015

1- Pornography
Porn isn't just back on top—it's bigger than ever—jumping from 16.55 percent in 2014 to over 36 percent this year. That is, when we see a mobile user's traffic heading to a malicious site, 36 percent of the time that user is following a link from a porn site. To put this in some perspective: when porn led the pack in the 2013 report, it was with a market share of just 22.16 percent.

3 - WebAds
Dropped from almost 20 percent last year (2014) to less than five percent this year. These include both

malvertising attacks and sites that host Trojan horse apps designed to appeal to porn site visitors. Blue Coat has also tracked and defined suspicious WebAd networks that are heavily involved in malware, scams, Potentially Unwanted Software (PUS), and other shady activities.

Bitcoin Payment Now or Lose Your Smartphone Contents: Top Malware Types of 2015

1- Ransomware
The world of mobile ransomware has grown dramatically over the past year. While some varieties that run on Android devices cause little damage beyond convincing victims to pay the cyber hostage-taker, many have adopted more sophisticated approaches common to ransomware in the Windows environment. With the increased performance capabilities of modern smartphones, it was only a matter of time before more advanced cryptographic ransomware, such as SimpleLocker, started showing up on mobile devices. These threats render music files, photographs, videos, and other document types unreadable—while typically demanding an untraceable form of payment such as Bitcoin—and employing a strict time limit for payment before the files become permanently inaccessible to the owner.

2- Potentially Unwanted Software
Generally, this class of program exhibits behavior typical of “adware” or “spyware”—spying on users’ on-line activity and personal data—or serving extra ads. Blue Coat researchers have seen a major shift in the volume of such software in the traditional malware space—and this is also true of the mobile space—as the number of junk mobile apps hosted on sites the researchers classify in this category has been rising steadily. This type of mobile app, notable for its dubious utility, frequently finds its way onto a mobile device through the use of deceptive advertising, or other social engineering attacks designed to deceive the victim into installing the unwanted program.

3- Information Leakage
Most people are unaware that apps on their mobile device may be watching them—and reporting out—on a 24x7x365 basis. This information leakage is usually a minor drip, showing the version of their phone's operating system, the manufacturer, the specific app or browser being used, and similar information. Complicating matters is the fact that there are typically no included system tools available for users to see or know what data is going out of their devices. Whether on an Android or iOS device, leaky data is often openly revealed in the “User Agent” string.

The Future of Mobile Security:

With no signs of slowing down, the market for mobile devices is booming. Anticipating that millions more of these devices will hit the street in the coming years, Blue Coat makes the following observations and predictions about the future of this trend.

1- Mobile payment systems
Mobile payment systems are set to grow, and services including contactless payment methods will incorporate additional security features, such as biometrics or two-factor authentication.

2 - Support for traditional PC and mobile platforms
There are already too many mobile devices vulnerable to a host of threats in use. These devices will

almost certainly not receive needed OS updates, and that will drive a market in security solutions that can support both traditional PC and mobile platforms.

3- OTA updates to vulnerable devices
Mobile carriers and handset makers are already working on plans to fast-track critical OTA updates to vulnerable devices, but the work is slow and it may be some time before this segment of the mobile market matures.

To download the Blue Coat Mobile Malware report, including tips for staying safe and advice for strengthening corporate defenses, please visit: www.bluecoat.com/mobile-malware (www.bluecoat.com/mobile-malware)

About Blue Coat Systems

Blue Coat is a leader in advanced enterprise security, protecting 15,000 organizations every day, including 88 of the 100 largest global companies. Through the Blue Coat Security Platform, Blue Coat unites network, security and cloud, providing customers with maximum protection against advanced threats, while minimizing impact on network performance and enabling cloud applications and services. Blue Coat was acquired by Bain Capital in March 2015. For additional information, please visit www.bluecoat.com (www.bluecoat.com).

# # #

Media Contacts
Marika Mousseau|Jenny Davis
Positive Marketing
bluecoat@positivemarketing.com
+44 203 637 0640