threatpost

The Kaspersky Lab Security News Service

Spotlight Series

Five Security Predictions for 2012

Featured Articles:

- Facebook And Twitter Erode Your Company's Security From Within. Here's How Stop It.
- Report: FTC Nears Deal with Facebook For Opt-In Privacy Changes
- DHS Official Warns of Security Risks in Supply Chain
- Vodafone-Distributed Handset Found Pre-installed With Mariposa Bot
- Samsung Handsets Distributed With Malware-Infected Memory Cards
- Android Market XSS Bug Allowed Code Execution on Mobile Devices
- DroidDream Again Appears in Android Market Apps
- Google: Spyware Found, Removed from Android Market
- Android Malware, Up 472 Percent, Seeing Fastest Growth Ever
- The Lesson of Stuxnet and Aurora: Get Back to Basics or Get Owned
- Evidence of Infected SCADA Systems Washes Up in Support Forums
- Exposing SCADA Systems With Shodan
- Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System

Stuxnet and the specter of sophisticated, state-sponsored attacks were still dominating the news a year ago, as 2010 ended and we welcomed the New Year. Soon enough, however, there would be a new phenomenon to contend with: hacktivists. As the attack on HBGary Federal and Sony showed, faceless online activists or anarchists can do plenty of damage to even sophisticated and well protected firms. Soon enough, attention shifted from the People's Liberation Army in China to finished basements across the U.S., where disaffected teens were joining the ranks of groups like Anonymous and Lulzsec to exact revenge on firms for slights both real and imagined.

What will 2012 bring? We can't know for sure. Recent years have taught us that, when it comes to computer security, one should expect to be surprised. However, it's equally true that in the realm of computer security, "what's past is prologue," as Shakespeare famously wrote. In other words: the events of the past year have helped to set the stage for the big events (and news stories) of 2012. What are those likely to be? Here's Threatpost's list of 2012 trends:

The Rise of the Chaotic Actor

The past year saw the emergence of a series of cleverly named hacking groups like Anonymous, LulzSec, and TeaMp0isoN. In 2011, these groups brought the fight to corporate America, crippling firms both small (HBGary Federal) and large (Sony). As the year drew to a close these groups noticeably shifted from prank-oriented hacks for laughs (or "lulz"), aligning themselves with political movements like Occupy Wall Street and using their skills to lend material and virtual support to the protests in various cities. It was an Anonymous-linked group, after all, that discovered and leaked the identity of pepper-spraying police officers in both the New York and Davis, California protests. Supporting populist figures like the student protestors at UC Davis is just good PR, but it also plays into the larger Anonymous narrative about using asymmetric force against abuse of individual liberties by corporations and governments. Joshua Corman, of the firm Akamai, has suggested that 2012 will bring further segmentation of what used to be known as "Anonymous," as some elements pursue political and socially constructive ends like income inequality, child exploitation or weeding out corruption, while more extreme elements within Anonymous carry out ever more bold – and alienating – attacks against targets of their choosing.

Facebook Jumps The Shark with IPO, Privacy Backlash

User backlash against Facebook's ever-evolving but always overreaching data privacy plans is almost as old as the site itself. But there's good reason to believe that 2012 will mark a turning point for the fast growing social network. For one thing, Facebook is on track for an IPO (initial public offering), possibly before the end of 2011. Valuations for the 800 million person social network range as high as $100 billion in private markets. With an IPO looming, Facebook is under more pressure than ever to generate outsized revenue from its massive, 800 million strong user base. Queue the new revenue opportunities – and the user backlash against privacy invasions.

In fact, tensions over Facebook's increasingly creepy designs on user data have already flared. Security experts have long charged the company is far too willing to expand sharing opportunities without considering the need for security and user control.

In the legal arena, Facebook and the Federal Trade Commission settled an FTC complaint that alleged the company violated users' privacy by forcing them to opt in to changes to the social network's default privacy settings that cast a trove of previously private user data into the public domain.

But that may not be enough. The UK's Telegraph reports that the European Commission is planning to crack down on Facebook's mining of users' political opinions, religious beliefs, sexual preferences and physical location.

What will we see in 2012? There's little doubt that Facebook's inevitable IPO will be huge and hugely profitable for investors, including Silicon Valley VC firms and longtime employees like CEO Mark Zuckerberg. However, the IPO may be Facebook's moment in the sun. Post IPO, we expect to see a company caught in what military strategists call a "pincer maneuver." On one side will be Wall Street investors with sky high quarterly revenue targets who will push the company to develop new revenue streams. On the other will be regulators and lawmakers in Europe and even the privacy agnostic U.S., where a federal data privacy law looks like it is on the fast track to passage in early 2012, and where regulators are soliciting feedback on changes to landmark laws like the Child Online Privacy Protection Act (COPPA). Expect more tales of woe, including lawsuits, Congressional hearings, new tweaks to the Facebook privacy paradigm and predictable flare ups with its massive user base over the proper use of data they post online, including photos and "likes" (or preferences).

Facebook And Twitter Erode Your Company's Security From Within. Here's How To Stop It.

By Paul Roberts

The "up side" of social networks like Facebook, Twitter and G+ are well known. But the down side of these networks for both users and for organizations that employ them are only now becoming clear. Worms, malware and spam are just the beginning of the security problems engendered by the social net. In this exclusive interview, conducted via e-mail, Threatpost editor Paul Roberts asked Joe Gottlieb, the CEO of security event management firm Sensage, about the many, subtle ways that social networks are eroding organizations' online defenses.

Threatpost: You've spoken about the dangerous phenomenon of social networks "automating trust." Please explain?

Joe Gottlieb: Social fabrics boil relationships down to simple transactions. By automation, I mean that by simply "liking" something, or "friending" someone, you create automated associations that lead to exposure of both good and bad social interactions. The notion of "automated trust" uses the paradigm that by taking those actions, you are prepared for all of the consequences. Users of social networks range from prudent to promiscuous, and every point in between, when it comes to their trust-level and engagements. What's worse is that we have come to trust that messages and interactions in these settings are reaching us because they are relevant in some way (sent by a friend, or because we liked something). This trust makes it even easier for an attack to occur – our defenses are down!

Threatpost: We recently heard about a study in which researchers created "SocialBots" - fake social networking profiles that were still able to assemble very healthy networks of real human beings. What practical steps could Facebook or other social networks take to prevent phony profiles from being created?

Joe Gottlieb: Social media vendors have enjoyed

the ability to serve very indulgent communities with, only recently, the concern for increased controls and security. It will be critical for these proprietors to take a continuous design improvement approach to their security practices, and their responsibility to educate users on the increasingly granular controls that are available, then force users to adopt safe techniques in their community.

Threatpost: It seems as if Facebook looks at user feedback on profiles to spot suspicious activity. Is that too trusting?

Joe Gottlieb: This is a great question – worthy of a live conversation. First, do we want to assume that SocialBots care about durable identities? Or do they act long before end-user commentary engages an alert. In fact, we have seen that these bots are very transient and therefore, "reputation" won't really stop them since they will act and shut down before user feedback catches up. It will be up to vendors to determine how much weight to place on "unlikes," "unfriending," and the like. Automating solely on that feedback is dangerous…which brings us to your next question…and that tests end-user motivation.

Threatpost: Is there any feasible way to police this type of activity since its really relying on human nature to spread, rather than some platform failure?

Joe Gottlieb: End-user motivation alone is questionable. It is a combination of methods – activity monitoring, historical patterns, etc. This is an approach we follow when it comes to security event management. It's never one approach that will detect suspicious events. And there is never consideration that you can fully stop attacks – it's about creating sustainable and repeatable processes for discovering and eradicating risk.

Threatpost: What are some steps that, say, Facebook users should take to protect information?

Joe Gottlieb: Facebook has done a great job of making granular controls available. I am speculating that the average participant does not fully understand or leverage them. So start there – get educated about your online presence and what trust level you want to exhibit. Understand that, outside of the control sphere you create, everything else you share is available to the public.

Use the same prudence in online environments just as you have had to learn to do in your email box – knowing not to click on email that appears to contain a bogus link – now your social media communities can be an attack vector. Be careful who you bring into your network, and don't assume that your wall can't be leveraged for phishing attacks, etc.

Threatpost: Dan Geer, the CISO at In-Q-Tel recently wondered whether having humans in the loop is a failsafe or a liability and, alternately, whether fully automated security to be desired or to be feared. Your thoughts?

Joe Gottlieb: We all enjoy the simplicity of knowing that associations with people we trust drive other desirable interactions. However, we should not be so naïve as to believe that someone won't take the opportunity to capitalize on our interests, if given the opportunity. Humans, who either create no boundaries around their information, or take unnecessary risks on line, will fall prey to those cybercapitalists. In that case, naïve or cocky behavior leads to a level of exposure that makes headlines.

"Trust" can't be fully automated and neither should security. Just as you put controls around who you consider part of your trusted network, you should add a layer of human intuition and security in everything you do. If we rely solely on the social networking engines to secure our digital life, we will lose the ability to spot scams – and that is just lazy behavior on our parts. I liken it to old email phishing scams. We have become so educated about what to look for – and have built-in senses around emails that "just don't seem right." We will need to employ similar senses for social media attacks.

At the same time, automating the "computation of trust context" to the best of our ability can result in better guidance for necessarily human/manual decisions. In the security event monitoring world, automation can help us run statistical filters on vast data sets that we are unable to review manually. In the social networking world, we will most likely see the more security conscious fabrics produce prompts that assemble what can be known about a looming opt-in decision…the current example is how your smartphone asks you if you want to share location information with the app that you just activated.

Future examples might evolve to produce more meaningful context such as secondary considerations like "App xyz is requesting that you share location information with a website whose security certificate does not match that on file with app xyz. Moreover, you a presently occupying a personal residence and so location information sharing may be less valuable or less appropriate at this time."

Threatpost: What can corporations can do about the human and human-plus-Facebook problem?

Joe Gottlieb: Start with education. A smart on-line community member will save you hours of IT support time and reduced risk overall. By understanding the pitfalls of open sharing, random responding, etc., employees will exhibit better behaviors whether on the clock or not. Next, put policies in place around acceptable use, in terms of how, when and where employees can interact with social mediums. And don't assume anything is understood. A launch date may seem like a wonderful thing to share with friends… but could be devastating competitively.

Threatpost: You said in your previous response that they need to create "sustainable and repeatable processes for discovering and eradicating risk," but what does that mean practically?

Joe Gottlieb: Security teams need to build processes that integrate all security events – not just network gear, or endpoint traffic, etc. Build a system that looks for trends – an example would be the number of times each of the marketing employees connects to Facebook per day. Use that trending to set a threshold you can monitor then put an alert that triggers a warning when someone exceeds that threshold. Same with downloads. If it appears that, on average, your sales team downloads 200GB per day in Internet files, look for spikes that show a 2x or 3x that amount, Or suspicious URLs – put filters in place for activities that lead to suspicious website. Then ensure that the system you are using can correlate all those activities – so that, individually, they may appear innocent enough, but when combined with three or four suspicious metrics, lead you to a possible attack.

Report: FTC Nears Deal with Facebook For Opt-In Privacy Changes

By Paul Roberts

The deal will settle an FTC case alleging privacy violations on the social network by forcing users to opt in to any changes to default privacy settings, according to a report in the Wall Street Journal.

The FTC inquiry dates back more than two years, and followed changes to the default privacy settings that pushed some formerly private user information into the public domain, the Wall Street Journal reported. Despite efforts to quell controversy over its privacy policies since then, the company has repeatedly ired consumer advocates and some members of Congress since then. In September, Facebook pushed out changes to its 800 million members that made it easier to share information with their Facebook network and made it easier for applications that run on the platform to track and share users activities, as well.

Following the change, users noticed that the company was collecting data not only when users were logged on, but also when they were visiting other sites online, by way of a Facebook plug-in that continued to operate even when there was no active Facebook session. Congressmen Ed Markey (D-MA) and Joe Barton (R-TX), co-Chairs of the Congressional Bi-Partisan Privacy Caucus, sent a letter in September to the FTC to investigate the company's use of tracking cookies.

The exact terms of the rumored settlement aren't known, but reports suggest it would go a long way towards ending those kinds of practices. For one, Facebook would submit to independent privacy audits for 20 years settlement and to get user consent before making retroactive policy changes to its privacy. The agreement will not require users to expressly agree to all changes and feature additions on the site.

In August, Facebook introduced a slew of privacy changes that gave users more control over how their information is used.

Facebook has been the frequent target of privacy complaints from its massive user base, which is subject to spam and other scams. Researchers have also noted how information shared on Facebook and other social networks can be used to link anonymous video and photos with online identities and social graphs.

Those complaints took on new life once Google+ debuted, with its "Circles" feature, that allows users to present different slices of their social profile to different groups of followers. In recent months, Facebook has sought to tamp down with a series of improvements to its security features and strict requirements for Facebook application developers.

Pre-Owned Hardware

Counterfeit and "certified pre-owned" hardware is nothing new, but we think 2012 will see this issue morph from a sideshow in the cyber security world to center stage, with new revelations about contamination of the global supply chain by hardware and software components of dubious origin and possibly malicious intent. Government agencies, militaries and commercial firms in the U.S., Europe and elsewhere will increasingly worry that gear they purchased with confidence may, in fact, contain components of dubious origin that could provide an attacker with access to critical networks or systems, or that could be funneling sensitive information to parties hostile to their organization.

A DHS official warned lawmakers earlier this year that DHS was aware of software and hardware manufactured overseas that had arrived in the U.S. with "security risks" preloaded on them. That was a vaguely ominous kind of warning, but there are other, more concrete examples. In March, 2010, HTC mobile phones running Google's Android operating system were found pre-installed with malware linked to the Mariposa botnet. A similar incident affected Samsung handsets, which shipped with malware infected memory cards. There have been other signs that officials are becoming more concerned about hacked gear and embedded devices. A report in 2010 from SAFECode, an independent consortium of independent software vendors (ISVs) found that security risks in the software supply chain were poorly understood and called for more research and development on supply chain security. Commerce Department, for example, forbade Chinese telecommunications firm Huawei from bidding on a new national wireless network for first responders in the U.S. The concerns of U.S. intelligence officials over bugged technical equipment. With more scrutiny of threats in mobile and embedded devices and vulnerabilities in the global supply chain, expect more stories about pre-owned hardware in 2012.

DHS Official Warns of Security Risks in Supply Chain

By Dennis Fisher

In a House committee hearing on cybersecurity threats Thursday, a DHS official said he was aware of some cases in which software and hardware manufactured overseas had arrived in the U.S. pre-loaded with security bugs. However, the official did not say that those cases involved vulnerabilities or backdoors planted intentionally.

In response to a question from Rep. Jason Chaffetz of Utah, Greg Schaffer, the acting deputy undersecretary of the National Protections and Programs directorate at the Department of Homeland Security, said that he knew of instances in which PC components and software had come to the U.S. with security vulnerabilities in them. The hearing of the House Committee on Oversight and Government Reform was mainly focused on information sharing between the government and the private sector, but Chaffetz began to press Schaffer on the issue of compromised foreign components entering the supply chain of U.S. companies.

"Are you aware of components, software or hardware, coming to the United States of America that have security risks already embedded into those components?" Chaffetz asked.

Schaffer had already balked at answering the question a minute before and seemed hesitant, but after asking Chaffetz eventually to rephrase it, he did answer.

"I am aware that there have been instances where that has happened," he said.

Identifying a vulnerability in an application that was planted specifically and intentionally by a foreign supplier or third party would be a difficult task, to say the least. It's generally accepted that every piece of software that hits the shelves contains security flaws, and while a lot of development is outsourced now, tying a specific bug to an intentional operation would be problematic.

There have been plenty of examples in recent years of hardware devices such as USB flash drives and even digital picture frames being pre-loaded with malware.

Chaffetz did not press Schaffer any further on the issue or ask him whether he meant that there had been examples of software and hardware found to have been rigged with intentional vulnerabilities in an effort to weaken defenses at U.S.-based companies and government agencies. Chaffetz instead moved on to the information-sharing topic again.

Schaffer said that the DHS and Department of Defense have a joint task force that is charged with looking at ways to ensure the strength and integrity of the U.S. supply chain over the long term. Schaffer, a former computer crime prosecutor at the Department of Justice and security officer in the private sector, said that the lack of control of the supply chain and threats to its security is one of the more difficult challenges facing the country at this moment.

Vodafone-Distributed Handset Found Pre-installed With Mariposa Bot

By Dennis Fisher

Security researchers have found the Mariposa bot client pre-installed on a mobile phone handset distributed in Europe, and say that the malware looks to have been installed on the phone's memory card.

The phone, the HTC Magic, runs the Google Android mobile operating system, and is a low-priced handset distributed by Vodafone. A researcher at Panda Security received one of the handsets recently, and upon attaching it to her PC, found that the phone was pre-loaded with the Mariposa bot client. Mariposa has been in the news of late thanks to some arrests connected to the operation of the botnet.

However, that was not the only malware the Panda researcher found on the phone.

"Interestingly enough, the Mariposa bot is not the only malware I found on the Vodafone HTC Magic phone. There's also a Conficker and a Lineage password stealing malware. I wonder who's doing QA at Vodafone and HTC these days," Pedro Bustamante of Panda wrote in a blog post on the incident. The phone was purchased new in Spain.

In the comments of the post, Bustamante says that the malware was found on the memory card and not the phone's file system. The bot was found on one phone, although Bustamante said that the company is buying some more of the Magic handsets to see if the malware shows up on others.

In a statement, HTC said they believe the problem was contained.

"HTC operates rigorous quality assurance testing of all products entering the market. We believe this was an isolated incident but are working closely with Vodafone to investigate thoroughly," the company said.

John Leyden at The Register reports that Vodafone has investigated the incident and found it to be a local, isolated problem. "Following extensive Quality Assurance testing on HTC Magic handsets in several of our operating companies, early indications are that this was

an isolated local incident," Vodafone told Leyden in a statement.

After the researcher plugged the HTC phone into the PC, the Mariposa client began trying to infect other PCs in the local network and also started trying to contact a remote server. The Panda researcher found that the client was not being run by the same group of alleged Spanish hackers who were arrested last week, but by someone named "tnls."

Pre-installing malware on hardware devices such as phones, digital photo frames, USB keys and others has become a favored attack vector for criminals. It simply takes one weak link in the supply chain, which can include dozens of countries around the globe, to plant the malware on thousands or millions of devices.

The main Mariposa botnet was shut down recently, and security researchers have taken control of the botnet's command-and-control channels. The takedown was a large cooperative effort among various security companies, including Panda and Defence Intelligence, and law enforcement agencies, a paradigm that is becoming more common in recent months as experts continue to focus their attention on the massive botnet epidemic.

Researchers at Microsoft, working closely with law enforcement officials, recently shut down the Waledac botnet, a smaller operation that had been peppering user's of Microsoft's Hotmail service with billions of spam messages for some time.

**This story has been updated to clarify that the malware was found on the memory card, not the file system, and to add Vodafone's statement to The Register. The headline also was updated to reflect the new information.*

Samsung Handsets Distributed With Malware-Infected Memory Cards

By Dennis Fisher

Another mobile-phone manufacturer has fallen victim to an increasingly common attack in which phones' memory cards are infected with malware during the manufacturing process and then shipped out to customers. The latest victim is Samsung, which has acknowledged that the microSD cards in a batch of its S8500 Wave mobile phones sold in Germany were infected with an autorun Trojan.

The Samsung incident comes just three months after a similar attack in which the memory cards on a group of HTC Magic handsets distributed in Spain by Vodafone were found to be pre-loaded with the client for the Mariposa botnet. As in the Vodafone incident, the malware pre-loaded on the Samsung phones is generally detected by most anti-malware suites.

The malware loaded on the microSD cards in the S8500 Wave handsets is an autoRun virus that executes automatically if the card is inserted into a PC that has the autoRun feature enabled, according to an analysis by Michael Oryl of MobileBurn.com, who received one of the infected handsets.

It appears that Samsung has accidentally allowed a malware program called slmvsrv.exe onto the 1GB microSD memory card that is shipping with the new bada-powered Samsung S8500 Wave smartphone. This Windows-based application, known as Win32/Heur, appears with an Autorun.inf file in the root of the memory card and will install itself when it is inserted into any Windows PC that has the autorun feature enabled.

Oryl notified Samsung of the infection, and the company responded that only the first production run of S8500 Waves shipped to Germany was infected with the malware. However, the company didn't specify exactly how many handsets that initial production run included.

Malware targeted at specific smartphone platforms is still a relatively rare phenomenon, but attacks such as those against the HTC and Samsung handsets, in which the malware is pre-loaded on memory cards, are increasingly common. There have been other incidents in which other pieces of malware have been found pre-loaded on USB memory sticks, digital photo frames and other devices not typically thought of as targets for attackers.

For attackers, these types of attack vectors can be an efficient way of getting malware on a large number of devices with a minimum effort. Security experts say these attacks often are executed by attackers paying an employee working in the factory that manufacturers the device or memory card, who installs the malware on the devices during the production process. It's a pay once, infect many business model.

Google's Day of Reckoning

Adoption of Google's Android operating system is accelerating faster than a run-away train. That's good news for Google, which always saw Android as a potential iPhone killer. But the events of the past year also make it clear that the company will be forced to deal head on with a dirty little secret: both the Android operating system and the Android Marketplace have become the preferred platform for malicious software authors interested in compromising mobile devices.

Thus far, Android's gangbuster adoption has exposed a few weaknesses. While the mobile platform itself has stood up well, the Android Marketplace has been shown to be susceptible to manipulation. – The by-product of structural problems and a policy that abjures application testing of any kind. Notably, the DroidDream malware cropped up in compromised Marketplace apps a number of times during 2011. Other incidents saw the Plankton spyware crop up on the Marketplace, and a version of the Zeus banking Trojan for Android phones. Though mobile phone malware is a niche problem, what mobile malware there are these days is being written for the Android platform – a 472% increase in just the last year. As Tim Armstrong of Kaspersky Lab recently pointed out, there's good reason to be skeptical of alarmism about mobile malware – it's not a big problem relative to Windows malware, and many of the most pressing threats (like SMS Trojans) are rarely seen by mobile phone users in the U.S. One Google executive has even gone so far as to call security researchers who warn about mobile threats "hucksters." Regardless, there's little doubt that the mobile malware train is gaining speed, that threats – though few in number – are growing at an alarming rate, and that Google, as the maker of the most popular mobile operating system, is becoming a target of choice. Angry protests aside, we expect to see a range of new threats for Android in 2012 including, but not limited to, new threats affecting mobile payments features. In response, look for Google to institute new policies to combat mobile threats, including (but not limited to) pre-release mobile application auditing a la its chief rival, Apple.

Android Market XSS Bug Allowed Code Execution on Mobile Devices

By Dennis Fisher

A simple, trivially exploitable persistent cross-site scripting bug on the Google Android Web Market allowed anyone to upload an app that could be used to later run arbitrary code on the user's Android device. The vulnerability, which Google has patched, enabled an attacker to silently install his malicious app and then get any and all permissions on the device.

Security researcher Jon Oberheide discovered the vulnerability recently and developed an exploitation scenario in which an attacker who could entice a user into clicking on a URL in the Web Market could force the user to install his malicious app. The attacker could then use one of a couple of methods to gain arbitrary code execution with the malicious app on the Android device. By inserting a small bit of HTML code in the field that developers use to describe their apps when their publishing them, an attacker can trigger the XSS vulnerability on a user's browser when he clicks on the link the Web Market to install an app.

The Android Web Market includes functionality that enables users who are browsing the Market on a desktop machine to automatically install apps on their devices simply by clicking on a link in the Market. The Android OS doesn't give users a prompt on the device to confirm an app install, which makes the attack scenario simpler.

"Since there is no on-device prompt or confirmation for these INSTALL_ASSET requests pushed to your

phone, an attacker can silently trigger an malicious app install simply by tricking a victim into clicking a link while logged in to their Google account on their desktop or on their phone. The malicious app delivered to the victim's phone can use any and all Android permissions, allowing for all sorts of evil behavior," Oberheide said. "Simply installing the app does not result in code execution since apps do not auto-start upon install on Android. However, we can easily emulate this functionality effectively to auto-start our app and gain code execution."

There are two methods that an attacker could use to gain code execution once his app is installed. The first scenario involves having the app register for the PACKAGE_ADDED broadcast intent in Android. One that's done, the malicious app will run anytime another app is installed on the device, and because the attacker can control the user's browser via the XSS bug, he can force another app install and then use this method. The second way to gain code execution uses the mobile browser.

"Alternately, if our XSS is taking place within the browser of the mobile device itself, we can simply insert a hidden IFRAME in our XSS payload, continually set the src of the IFRAME to something like 'trigger://blah', and then have our installed malicious app register an intent filter on the 'trigger://' URI scheme," Oberheide said. "This will cause our malicious app to be triggered and gain code execution as soon as it is finished installing."

The vulnerability that Oberheide discovered, which Google has now patched, was present since the Android Web Market launched in February. It is just the latest issue to affect the security of the Android Market and comes just a week after researchers discovered that more than 50 apps had been uploaded to the Market that were infected with the DroidDream Trojan. That malware was designed to steal data about the infected phone and then download further malicious code.

Google removed the apps from the Market and is using its remote-wipe capability to delete them from infected Android devices as well. The company said over the weekend that it was pushing a fix for the Android vulnerability that the DroidDream attack leveraged and also is adding some unspecified new security measures to the Android Market to prevent future attacks like this.

DroidDream Again Appears in Android Market Apps

By Dennis Fisher

For Android users, the refrain must be getting a little tiresome: Researchers have found another batch of apps in the Android Market that were infected with malware. Once again, it was the DroidDream malware family causing the trouble, but this time, it was just a handful of apps and they were only in the market for a little while.

This is the third known incident in which a variant of DroidDream has been found in a group of infected apps in the Android Market. And it's the second warning in two days for Android users about malware-infected apps. Just yesterday, researchers at NC State University identified a new SMS Trojan that was in Android apps in unofficial markets in China. Now comes the news of a strain of DroidDream infecting four apps in the Android Market.

Researchers at Lookout found that the apps contained a version of the malware known as DroidDream Light, which is the same variant that was found in a batch of apps in June, as well. They estimate that the malware-loaded apps only were downloaded by fewer than 5,000 users before Google removed them.

"Four applications in the Android Market published by a developer named "Mobnet" were found to contain malware that is nearly identical to DroidDream Light. Though our analysis is still underway, these applications are likely published by the same author as the original DroidDream malware. Similar to the first samples of DroidDream Light found, these samples are not reliant on the manual launch of the infected application to start," the researchers wrote.

The affected apps are Scientific Calculator, Quick Fall-Down, Bubble Buster and Quick Compass and Leveler. The infected compass app has a name that's very similar to a legitimate app, the researchers said, with the difference being that the infected one uses capital letters in the name.

The version of DroidDream Light found in these four apps has a variety of remote-control and other capabilities, including the ability to download other apps and display prompts on the notification bar on the phone's screen, directing the user to a URL, which is likely malicious. DroidDream Light also can download a new APK for the infected app, and then download an updated version of the malware.

As malware authors have focused more and more on mobile devices, Android has emerged as their preferred platform for mischief. The platform's open architecture and the ease of getting apps into the official Android Market have made it a prime target for attackers in recent months. The Apple iPhone so far has been spared most of this unwanted attention from malware authors.

Google: Spyware Found, Removed from Android Market

By Paul Roberts

Google says it has suspended a number of suspicious applications from the Android Market after researchers at NC State announced they had discovered a new and particularly stealthy piece of spyware, dubbed "Plankton," lurking in Android applications there.

According to a report by computer science professor Xuxian Jiang, the Plankton spyware represents an evolution in Android malware by attempting to obscure itself using a native class loading capability, rather than trying to gain root access to Android phones. The NC State team claims this sort of exploitation is the first of its kind.

Ten Android apps in the Official Android Market are known to infected, but many more could be victims of the Plankton Trojan. Jiang claims that early variants of the Trojan have evaded detection for as long as two months.

A Google spokesman said the company has already taken action to remove the malicious applications.

"We're aware of and have suspended a number of suspicious applications from Android Market," a Google spokesperson told Threatpost. "We remove apps and developer accounts that violate our policies."

Plankton works like a parasite: latching onto its host applications as a background service which has no affect on that apps intended purpose. When a user runs an infected application on their Android phone, Plankton collects information such as the device ID and list of granted permissions and sends them via HTTP POST message to a remote update server, the NC State researchers found.

That remote server returns a URL pointing to an executable file for the device to download. Once downloaded, the jar file is dynamically loaded. In this way, the payload evades static analysis and is difficult to detect.

Analysis of the payload shows that the virus does not provide root exploits, but supports a number of bot-related commands. One interesting function is that the virus can be used collect information on users' accounts.

The team discovered the new malware while conducting research on two existing pieces of Android malware, DroidKungFu and YZHCSMS. These and other pieces malware such as DroidDream are indicative of a trend toward targeting Android devices with online attacks.

Google has historically taken a hands-off approach to policing the Android Marketplace. It will suspend and remove suspicious or malicious applications when they're reported, but does not vet applications prior to posting them, as Apple does with its AppStore. A growing population of Android users and burgeoning Android Marketplace, however, may challenge that approach.

A company spokesman said that the company has security measures in place to insure the integrity of Android applications.

"We are committed to providing a secure Android Market experience for consumers. Our approach includes clearly defined Android Market Content policies that developers must adhere to, plus a multi-layered security model based on user permissions and application sandboxing. Applications in violation of our policies are removed from Android Market," he said in an e-mail message.

Android Malware, Up 472 Percent, Seeing Fastest Growth Ever

By Christopher Brook

As Android market share has shot up in recent months, so has the volume of malware designed for the mobile platform. There's been a whopping 472 percent increase in Android malware samples in the last three months alone, according to research from Juniper Networks.

While September saw a 28 percent jump in malware samples, in particular, the numbers for the months of October and November are trending upwards and might translate into the fastest growth of Android malware the platform's ever seen. October's numbers spiked up to a 110 percent increase over September, a 171 percent increase from what was collected up to July of this year, the company said on its Global Threat Center blog.

Juniper's research found the bulk of Android malware is behaving one of two ways: 55 percent was disguised as spyware while 44 percent hijacked phones and utilized a SMS Trojan to send expensive messages without the user's knowledge.

The Android Market has seen a tremendous surge in malware-laden apps that have this year, namely those infected with the DroidDream family of malware.

Malware targeting Android was "more than triple the amount that targeted Java Micro Edition and far more than any other mobile platform, such as Symbian or BlackBerry," according to a McAfee study earlier this year.

Juniper credits this influx to Google's rather lax submission process. The lack of code signing and a formal application review process makes apps in the open Android Market easier targets for malware and in turn, unsuspecting users, than the iTunes App Store, which included app review and other restrictions.

For the rest of Juniper's research and an infographic summing it up, head here.

Stuxnet part II, III and IV

The nation-state sponsored malware arms race is on. Stuxnet may have been the "Shot heard round the world" but we think its likely that 2012 will witness a number of other skirmishes, with malware linked to foreign governments hostile to (or allied with) U.S. and Western nations infecting and disrupting critical infrastructure from power generation to telecommunications to water treatment. The warning signs are already there – evidence of infected SCADA systems can readily be found online. Internet facing SCADA and industrial control systems are readily identifiable using tools like the (free) Shodan scanner, while hackers and gray hat security researchers have used targeted attacks to expose poorly secured or mis-configured industrial control systems. Cyber war would be a stretch, but expect more Stuxnet-like proof of concept attacks in 2012 – perhaps even within the U.S. - that ratchet up international tensions.

The Lesson of Stuxnet and Aurora: Get Back to Basics or Get Owned

By Dennis Fisher

SAN FRANCISCO--It's often said that after decades of work and technological advances, the security industry hasn't actually solved any problems or made things any better. But that's not entirely true. The industry has in fact perfected the art of exploiting the scare 'em and snare 'em, threat-of-the-moment mentality that's turned security into a perpetual cash-generation machine. And it's all for naught.

Nowhere is the state of this art clearer or on more flagrant display than at the RSA Conference here every year, a week-long industry love-in during which thousands of sales and marketing executives descend upon the city to mingle with dozens of actual security professionals. The agenda for the week is clear: Hammer home the fact that your product protects enterprises against <insert threat here>. The flavor of the week this time around was Stuxnet/Aurora/Iran/China/terrifying professional adversary.

For the most part, the idea that Product A, which was designed to address Threat A seven years ago, is now being touted as a perfect countermeasure to Threat B is treated as a harmless joke in the industry. Everyone does it. Threats come and go, so companies that want to stick around need to adapt. The threat from professional or state-sponsored attackers using super-sophisticated custom malware to compromise government agencies, banks, Google, nuclear plants and other high-profile targets is simply the latest iteration of that.

But the problem with this evolution is that attacks such as Stuxnet or Operation Aurora or GhostNet are not what most enterprises and organizations need to be worried about. The plain fact is that most organizations are falling far short in protecting against the same threats that they've faced for the last 10 years. SQL injection, phishing, malicious attachments, social engineering. Old, every one of them. And yet, still incredibly effective at compromising networks in some of the best-known and theoretically best-protected companies.

In other words, Stuxnet and Aurora have been owning networks around the world, without ever touching them.

Security researcher Michal Zalewski points out that all of the discussion in recent months of these highly targeted attacks has obscured the fact that this kind of attack not only is nothing new, it's not even worth worrying about for most organizations.

"It is tempting to frame the constant stream of high-profile failures as a proof for the evolution of your adversary. But when you realize that almost every single large institution can probably be compromised by a moderately skilled attacker, this explanation just does not ring true. The inability to solve this increasingly pressing problem is no reason to celebrate - and even less of a reason to push for preposterous, unnecessary spending on silly intelligence services, or to promote overreaching and ill-defined regulation. If anything, it is a reason to reflect on our mistakes and perhaps go back to the drawing board," Zalewski wrote in a blog post recently.

His point is well-made. And while it may be tempting to dismiss this line of thinking as just a thought exercise or hair-splitting about who the attackers are, that would be a mistake. Focusing on shadowy, highly-funded and motivated attackers that may be targeting your organization can divert your resources and personnel away from the less sexy and headline-worthy attackers who most definitely are targeting you.

The script kiddies that were defacing web sites and playing DDoS tag 10 years ago didn't go away; they moved on to more profitable activities such as spear phishing and planting malware on your home page to exploit visitors. Doesn't sound serious? Keep in mind that many of the victims of Operation Aurora were compromised through malicious PDFs attached to emails. None of these attacks is a joke and if you're compromised, you don't much care who did it in many cases. You just care that you're owned.

But it's important to remember when trying to discern the signal from the noise that determined attackers have always existed and they've always had the advantage. That's not likely to change anytime soon, regardless of what scary mask they may be wearing at the moment or may don in the future.

Evidence of Infected SCADA Systems Washes Up in Support Forums

By Paul Roberts

While security experts and lawmakers debate the seriousness of cyber threats to critical infrastructure, one security researcher says that evidence that viruses and spyware already have access to industrial control systems is hiding in plain sight: on Web based user support forums.

Close to a dozen log files submitted to a sampling of online forums show evidence that laptops and other systems used to connect to industrial control systems are infected with malware and Trojan horse programs, including one system that was used to control machinery for UK based energy firm Alstom UK, according to industrial control systems expert Michael Toecker.

Toecker said he has uncovered almost a dozen log files from computers that are connected to industrial control systems (ICS) while conducting research online. The configuration log files, captured by the free tool HijackThis by Trend Micro, were willingly submitted by the computer's operator in an effort to weed out pesky malware infections. The random sampling suggests that critical infrastructure providers are vulnerable to attacks that take advantage of mobile workers and contractors that bring infected laptops and mobile devices into secure environments.

Toecker circulated his findings via Twitter and discussed them in a blog post for Digital Bond, a consulting firm that specializes in work with firms in the control systems space. He discovered the links between infected Windows systems and industrial control systems by analyzing the HijackThis logs posted on the forums, which reveal detailed configuration information about the systems in question, the organization it belonged to, and even the role of the individual who owned the system.

In one case, posted on a UK based support forum in 2008, Toecker said the HijackThis logs reveal that a system belonging to the UK energy firm Alstom had been infected with the Trojan Zlob and that DNS queries from the system were being redirected to two Ukrainian DNS servers that were known to redirect users to malicious, drive by download sites.

The system contained references to an alstom.com domain associated with the company's power conversion division, and shows the laptop was managing a number of ICS systems including GE's Proficy, Intellution and FANUC products and Alspa Pilot, Alstom's controller interface and programming software.

The logs don't reveal how the system became infected with the Zlob trojan, but other forum posts make it clear how infections happened.

"I downloaded what it (sp) seemed to be a video codec to play a video through a website. Now I constantly get an annoying pop up message appear every time I open Internet Explorer, or even search for something in Google," wrote a user named EmerickAguilera in a 2008 post to the experts-exchange.com forum. Details from the HijackThis configuration log revealed an entry for a SCADA application installed in a directory named "\Development\Dubai\PalmJumeirah," an apparent reference to one of three famous palm-shaped man-made islands in Dubai.

Public evidence of infected systems that have direct access to industrial control systems - and potentially to critical infrastructure - shouldn't be surprising, Toecker writes. However, it should prompt critical infrastructure owners to rethink how truly "closed" their networks are, and to increase scrutiny of all the systems that access to them, including mobile systems used by vendors, contractors and full time employees.

Exposing SCADA Systems With Shodan

By John C. Matherly

"The sad truth is that Shodan is just scratching the surface of unprotected or misconfigured SCADA devices...And, of course, the search engine merely finds systems. It doesn't expose the myriad of bad security practices that seem to be rampant amongst

vendors and operators."

Editor's Note: The U.S.'s Industrial Control System Computer Emergency Response Team (ICS-CERT) recently issued a warning to its members about the ability of attackers to discover ICS systems using a simple search on Shodan, a public search engine that is used to locate systems accessible from the public Internet. In this column, Shodan's creator, John Matherly, writes that the ICS-CERT warning just scratches the surface of SCADA and ICS System insecurity, and provides suggestions for shielding these systems from the attentions of search engines, curious netizens or would-be attackers.

The recent ICS-CERT alert on the ability to find Supervisory Control and Data Acquisition (SCADA) systems using Shodan has received a lot of attention, mostly by people who were surprised to hear about the apparent lack of security on systems that run much of our nation's critical infrastructure. For many security experts, though, these security issues were well known and long-standing - the proverbial elephant in the living room. Now it seems Shodan, a search engine that I created, has brought the security issues plaguing SCADA and ICS systems into the daylight by making it possible to discover Internet facing ICS systems with a simple Web search.

For people unfamiliar with Shodan (http://www.shodanhq.com), it's a web service that scans the entire Internet for specific services (HTTP, HTTPS, Telnet, SMTP, SSH and FTP). If it finds an IP that responds to an initial search, it proceeds to grab a banner that contains information about the service. Finally, the IP gets correlated with other sources of data, such as geographic location, to complete the picture.

To cloak a computer from Shodan, systems should simply refrain from responding to either the first crawl or subsequent connection attempts by configuring their firewall to block unknown sources from connecting. I should note that this is not the same as trying to hide the computer from search engine crawling by configuring a robots.txt file to tell Google, Yahoo, Bing, etc. to leave you alone. That might be an instinctual first step for IT staff, but would only mask and delay the real problem. The truth is that SCADA and industrial control systems should not have a public IP address. If the security of a service depends on that service remaining hidden (a.k.a. "security through obscurity,"), then that's a problem.

I launched Shodan nearly a year ago, and right off the bat people started finding systems that are discussed in the ICS alert. It ranged from a cyclotron at the Lawrence Berkeley National Laboratories to infrastructure-level network switches and water treatment facilities. Even now, a quick search for openly accessible Cisco switches returns almost 7,000 results.

The sad truth is that Shodan is just scratching the surface of unprotected or misconfigured SCADA devices. Since it mostly looks for computers running a web server, it misses any device that relies on a custom daemon operating on a different port. That doesn't mean that such systems are undiscoverable. It just means

that Shodan isn't looking for them. And, of course, the search engine merely finds systems. It doesn't expose the myriad of bad security practices that seem to be rampant amongst vendors and operators.

The good news is that a few, simple security precautions would prevent the problems mentioned in the ICS alert: multiple layers of defense are important and expected of an organization containing sensitive equipment or information. Such measures include the use of strong passwords, removing default user accounts, setting up a VPN for remote access, properly configuring the firewall and having emergency response procedures in place, constantly testing network security and monitoring for file system changes. Operators should use Shodan to check whether their systems have been indexed.

Finally, there's an API for Shodan that lets system administrators periodically check whether any of their machines are publicly accessible.

The bad news is that getting ICS vendors and their customers to understand and implement these common-sense measures is an uphill battle.

A few weeks ago at the Toorcon conference, security researcher Jeremy Brown gave a talk on exploiting SCADA systems that showed just how little some vendors care about security.

Brown related his experience trying to convey information about a serious, remotely exploitable hole in a common SCADA platform to the vendor responsible for the software. Brown told the audience about how he struggled to explain the concept and implications of remotely exploitable vulnerabilities to the vendor's security contact, only to be told to "stop wasting their time."

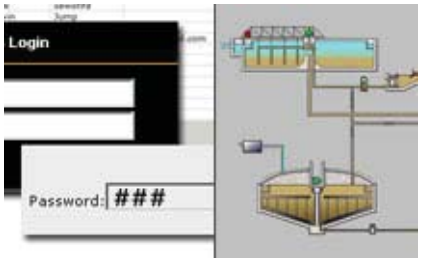
It wasn't until Brown went public with his findings and aroused the interest of the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) that a vendor patch was issued.

Hopefully the Stuxnet incident as well as recent ICS alerts will convince vendors and operators alike to allocate more resources to security and make it a central component of their infrastructure.

Hacker Says Texas Town Used Three Character Password To Secure Internet Facing SCADA System

By Paul Roberts

In an e-mail interview with Threatpost, the hacker who compromised software used to manage water infrastructure for South Houston, Texas, said the district had HMI (human machine interface) software used to manage water and sewage infrastructure accessible to the Internet and used a password that was just three characters long to protect the system, making it easy picking for a remote attack.



The hacker, using the handle "pr0f" took credit for a remote compromise of supervisory control and data acquisition (SCADA) systems used by South Houston, a community in Harris County, Texas. Communicating from an e-mail address tied to a Romanian domain, the hacker told Threatpost that he discovered the vulnerable system using a scanner that looks for the online fingerprints of SCADA systems. He said South Houston had an instance of the Siemens Simatic human machine interface (HMI) software that was accessible from the Internet and that was protected with an easy-to-hack, three character password.

"This was barely a hack. A child who knows how the HMI that comes with Simatic works could have accomplished this," he wrote in an e-mail to Threatpost.

"I'm sorry this ain't a tale of advanced persistent threats and stuff, but frankly most compromises I've seen have been have been a result of gross stupidity, not incredible technical skill on the part of the attacker. Sorry to disappoint."

In a public post accompanied by screenshots taken from the HMI software, the hacker said he carried

out the attack after becoming frustrated with reports about an unrelated incident in which an Illinois disaster response agency issued a report claiming that a cyber attack damaged a pump used as part of the town's water distribution system.

A report by the Illinois Statewide Terrorism and Intelligence Center on Nov. 10 described the incident, in which remote attackers hacked into and compromised SCADA software in use by the water utility company. The hackers leveraged the unauthorized access to pilfer client user names and passwords from the SCADA manufacturer. Those credentials were used to compromise the water utility's industrial control systems, according to Joe Weiss, a security expert at Applied Control Solutions, who described the incident on ControlGlobal.com's Unfettered Blog.

"You know. Insanely stupid. I dislike, immensely, how the DHS tend to downplay how absolutely (expletive) the state of national infrastructure is. I've also seen various people doubt the possibility an attack like this could be done," he wrote in a note on the file sharing Web site pastebin.com.

The system that was compromised was protected by a three character password, pr0f claimed - though not necessarily the default password for the device.

Siemens Simatic is a common SCADA product and has been the subject of other warnings from security researchers. The company warned about a password vulnerability affecting Simatic programmable logic controllers that could allow a remote attacker to intercept and decipher passwords, or change the configuration of the devices.

In July, Siemens advised customers to restrict physical and logical access to its Simatic Industrial Automation

products. The company warned that attackers with access to the product or the control system link could decipher the product's password and potentially make unauthorized changes to the Simatic product.

At the Black Hat Briefings in August, security researcher Dillon Beresford Dillon Beresford unveiled a string of other software vulnerabilities affecting Siemens industrial controllers, including a serious remotely exploitable denial of service vulnerability, the use of hard-coded administrative passwords, and an easter egg program buried in the code that runs industrial machinery around the globe.

About Threatpost

Threatpost, Kaspersky Lab's Security News Service, is dedicated to helping IT security professionals succeed by delivering the most important and immediate security news and analysis available. Threatpost off ers a fresh approach to providing up-to-the minute news and information for IT security and networking professionals. Threatpost editors cover today's most relevant security news and the most pressing security issues of the day. They break important original stories, off er expert commentary on high-priority news aggregated from other sources, and engage with readers to discuss how and why these events matter. Threatpost's global editorial activities are driven by industry-leading security journalists Dennis Fisher and Paul Roberts. They are assisted by Ryan Naraine, a widely-followed security journalist and regular contributor to Threatpost.

Collectively they bring over thirty years of experience to their mission of delivering insight into the issues that aff ect the lives of security professionals every day. Threatpost has expanded with Latin American editions in both Spanish and Portuguese. These editions are led by local, veteran editorial teams dedicated to covering security news and analysis vital to the region.

Make Threatpost your first stop for security news and analysis.
www.threatpost.com