Feed Journal

Issue #6 for AUEB CIS - 3/29/2011 feedjournal.com

Iranian hackers obtain fraudulent HTTPS certificates: How close to a Web security meltdown did we get?

(EFF.org Updates)

Submitted at 3/23/2011 8:08:37 PM

On March 15th, an HTTPS/TLS Certificate Authority(CA) was tricked into issuing fraudulent certificates that posed a dire risk to Internet security. Based on currently available information, the incident got close to — but was not quite — an Internet-wide security meltdown. As this post will explain, these events show why we urgently need to start reinforcing the system that is currently used to authenticate and identify secure websites and email systems.

There is a post up on the Tor Project's blog by Jacob Appelbaum, analyzing the revocation of a number of HTTPS certificates last week. Patches to the major web browsers blacklisted a number of TLS certificates that were issued after hackers broke into a Certificate Authority. Appelbaum and others were able to cross-reference the blacklisted certificates' serial numbers against a comprehensive collection of Certificate Revocation Lists (these CRL URLs were obtained by querying EFF's SSL Observatory databases) to learn which CA had been affected.

The answer was the UserTrust "UTN-USERFirst-Hardware" certificate owned by Comodo, one of the largest CAs on the web. Comodo has now published a statement about the improperly issued certs, which were for extremely high-value domains including google.com, login.yahoo.com and addons.mozilla.org (this last domain could be used to trojan any system that was installing a new Firefox extension, though updates to previously installed extensions have a second layer of protection from XPI signatures). One cert was for "global trustee" — not a domain name. That was probably a malicious CA certificate that could be used to flawlessly impersonate any domain on the Web.

Comodo also said that the attack came primarily from Iranian IP addresses, and that one of the fraudulent login.yahoo.com certs was briefly deployed on a webserver in Iran. 1 What should we do about these attacks?

Discussing problems with the revocation mechanisms that should (but don't) protect users who don't instantly get browser updates, Appelbaum makes the following assertion:

If the CA cannot provide even a basic level of revocation, it's clearly irresponsible to ship that CA root in a browser. Browsers should give insecure CA keys an Internet Death Sentence rather than expose the users of the browsers to known problems.

Before discussing whether or not such a dramatic conclusion is at all warranted, it is worth considering what the consequences of blacklisting Comodo's UserTrust CA certificate would have been. We used the SSL Observatory datasets to determine what had been signed by that CA certificate. The answer was that, as of August 2010, 85,440 public HTTPS certificates were signed directly by UTN-USERFirst-Hardware. Indirectly, the certificate had delegated authority to a further 50 Certificate Authorities, collectively responsible for another 120,000 domains. In the event of a revocation, at least 85,000 websites would have to scramble to obtain new SSL certificates.

The situation of the 120,000 other domains is more complicated — some of these are cross-certified by other root CAs or might be able do obtain such cross-certifications. In most — but not all — cases, these domains could continue to function without updating their webserver configurations or obtaining new certs.

The short answer, however, is that the Comodo's USERFirst-Hardware certificate is too big to fail. If the private key for such a CA were hacked, by the Iranians or by anybody else, browsers would face a horrible choice: either blacklisting the CA quickly, causing outages at tens or hundreds of thousands of secure websites and email servers; or leave all of the world's HTTPS, POP and IMAP deployments vulnerable to the hackers for an extended period of time.

Fortunately, Comodo has said that the master CA private keys in its Hardware Security Modules (HSMs) were not compromised, so we did not experience that kind of Internet-wide catastrophic security failure last week. But it's time for us to start thinking about what can be done to mitigate that risk. Cross-checking the work of CAs

Most Certificate Authorities do good work. Some make mistakes occasionally, 2 but that is normal in computer security. The real problem is a structural one: there are 1,500 CA certificates controlled by around 650 organizations, 3 and every time you connect to an HTTPS webserver, or exchange email (POP/IMAP/SMTP) encrypted by TLS, you implicitly trust all of those certificate authorities!

What we need is a robust way to cross-check the good work that CAs currently do, to provide defense in depth and ensure (1) that a private key-compromise failure at a major CA does not lead to an Internet-wide cryptography meltdown and (2) that our software does not need to trust all of the CAs, for everything, all of the time.

For the time being, we will make just one remark about this. Many people have been touting DNSSEC PKI as a solution to the problem. While DNSSEC could be an improvement, we do not believe it is the right solution to the TLS security problem. One reason is that the DNS hierarchy is not trustworthy. Countries like the UAE and Tunisia control certificate authorities, and have a history of compromising their citizens' computer security. But these countries also control top-level DNS domains, and could control the DNSSEC entries for those ccTLDs. And the emergence of DNS manipulation by the US government also raises many concerns about whether DNSSEC will be reliable in the future.

We don't think this is an unsolvable problem. There are ways to reinforce our existing cryptographic infrastructure. And building and deploying them may not be that hard. Look for a blog post from us shortly about how we should go about doing that.

- 1. This is strong circumstantial evidence that the attack was perpetrated by Iranians, though it also possible that the perpetrators used compromised systems in Iran in order to frame Iran.
- 2. A few previous examples.
- 3. These numbers are from the SSL Observatory. Before we performed those scans, we are unsure that anybody knew how many CAs were trusted by our browsers and operating systems, because CAs regularly delegate authority to subordinate CAs without announcing this publicly

Can cell phone exposure cause bone weakening?

(Hack In The Box)

Submitted at 3/27/2011 8:32:36 PM

Electromagnetic radiation from cellular phones may adversely affect bone strength, suggests a study in the March Journal of Craniofacial Surgery. Men who routinely wear their cell phone on their belt on the right side have reduced bone mineral content (BMC) and bone mineral density (BMD) in the right hip, according to the study by Dr. Fernando D. Sravi of National University of Cuyo, Mendoza, Argentina. He writes, "The different patterns of right-left asymmetry in femoral bone mineral found in mobile cell phone users and nonusers are consistent with a nonthermal effect of electromagnetic radiofrequency waves not previously described." Dr. Sravi measured BMC and BMD at the left and right hip in two groups of healthy men: 24 men who did not use cell phones and 24 men who carried their cell phone in a belt pouch, on the right side, for at least one year. Measured using a test called dual-energy x-ray absorptiometry, BMC and BMD are standard markers of bone strength. Average hip BMC and BMD measurements were not significantly different between groups. However, men who did not use cell phones had higher BMC in the right femoral neck (near the top of the thigh bone): a normal left-right difference that was absent in cell phone users. Thus men who wore their cell phones on the right side had a relative reduction in femoral neck BMC in that hip.

Are Facebook Comments the Death of Anonymity?

by F-Secure Antivirus Research Team (mailto:weblog\@PLEASE-REMOVE-THIS.f-secure.com) (F-Secure Antivirus Research Weblog)

Facebook recently announced a major overall of their comments system. The new changes will allow Facebook users to comment on third-party websites using their profiles. Supporters of the new system hope that it will help in combating Internet trolls and comment spam because Facebook accounts typically use real names. Critics of the system argue that it's a threat to free speech.

A number of critics have cited this quote by Mark Zuckerberg, from The Facebook Effect: " You have one identity. The days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly ... Having two identities for yourself is an example of a lack of integrity."

Reactions among social activists have not been positive. But really, why? Is having only one identity really such a strange concept?

Other than The Batman, who really needs more than one identity?

I only have one identity. I also have an alias on Twitter,@FSLabsAdvisor, and you can probably tell based on its name, it's a work related account and primarily reflects my work persona as a public spokesperson of F-Secure. It's directly connected to my identity, but only represents a particular side of my personality.

I have multiple aliases on the Internet, a couple of them are anonymous, but I only need one identity.

Maintaining identity, privacy and integrity on the Internet can be a tricky thing — take Sarah Palin for example. About three weeks ago, Jack Stuef at Wonkette wrote that Palin maintained a personal Facebook account using the name "Lou Sarah". (Palin's middle name is Louise.) Stuef's take on the story was that Palin had a "secret" account to praise her "Sarah Palin" account. And he doesn't seem to take her Lou Sarah account as a sign of great integrity.

It was quite a good catch, but Stuef didn't get it entirely right. The Sarah Palin account is not a "profile". It is a special type of hybrid "page" for celebrities that behaves as a profile. But it's really just a page and part of Sarah Palin's personal brand. It's very likely that the page is entirely administered by her public relations team.

A lot of people wanting to manage their privacy create anonymous Facebook accounts. Many people clearly want aliases. I suspect that a great deal of the backlash directed at Zuckerberg is due to the fact that having multiple accounts per individual is a violation of Facebook's Terms of Service, and Zuck says stuff that makes them sound like criminals.

I think some of the backlash is deserved.

Facebook's corporate line is that you should only friend people that you actually know. But Facebook makes a lot of money from partnerships with social game companies such as Zynga. Social gaming is a form of casual gaming, and casual gaming encourages the formation of casual friendships. Facebook profits are in part driven by the formation of casual friendships.

You can't have your cake and eat it too.

I've seen lots of examples where people have created secondary accounts to play Facebook games with "virtual" friends. As long as Facebook profits from casual friendships, they need to find a way to better protect their users' privacy. Facebook needs to step up and offer users some sort of aliases, or else they need adjust their TOS.

I'm not holding my breath.

But how about Facebook's new commenting system?

Is it the death of anonymity and free speech?

Probably not. There's a "backdoor" method which is already being used to comment anonymously.

Pages.

TechCrunch buried this lead in their initial story: " Incidentally, it's also now possible to leave a comment on an external site as a Facebook Page, which means we could see brands use Facebook to leave 'official' comments on blog posts."

So here's an example of what you can do — create a fictional character.

My character is named "Jaajo Jantteri". And I hold the copyright so I'm in full compliance with Facebook's Page Terms.

Next, visit a site testing the new comments, such as TechCrunch. Select the alias of your choice.

And comment.

Now we just need to hope that trolls and spammers won't want to do the same.

But hey, if Facebook wants to move the battleground within their walled garden, I say, let them.

Regards,

####

On 16/03/11 At 06:38 PM

Where's EFF? Why EFF Is Sometimes Quiet About Important Cases

(EFF.org Updates)

Submitted at 3/28/2011 1:34:41 PM

When legal issues light up the Internet, people turn to EFF for answers. Whether it's attacks on coders' rights, overreaching copyright claims online, or governments' efforts to censor or spy on people, we are often among the first to hear about troubling events online, and we're frequently the first place people turn to for legal help.

So why are there times when EFF is involved in an important case but is silent or gives only limited information about it? Usually it's for one of three reasons: to protect the people who have asked us for help, because of a specific court requirement or because we're putting the strategy into place.

First, the legal protections for attorney/client communications and attorney work product allow lawyers and their prospective or existing clients to speak frankly with each other and to honestly evaluate the strengths and weaknesses of their cases. But these communications and notes must be kept strictly confidential in order to remain protected. If the confidentiality is broken, the person or a person's attorney can be required to reveal their communications, legal strategies, and evaluations to their opponents – including to prosecutors who can put them in jail or opposing civil lawyers. Breaching these privileges can hurt the people who ask us for help and undermine our chances of winning a case, so we are very careful to avoid doing so.

Other times, a court limits our ability to speak. A recent example of this is when the government demanded information from Twitter as part of its Wikileaks investigation, where we were subjected to a court sealing order. In this Twitter records case, we are representing Birgitta Jonsdottir, one of the Twitter users whose records are being sought by the U.S. government. Initially, the fact of our representation was the only thing we could acknowledge publicly. The court documents in the case were filed under seal, and we could not even discuss the hearing we were preparing for, leading to many awkward and frustrating conversations with EFF members as well as reporters. However, we asked the judge to unseal the court records, and she ultimately did unseal nearly all filed documents in the case to be released to the public, including news of the hearing. In such cases, we press as hard as we can to get the legal proceedings made public, especially for cases involving important personal privacy and free speech implications.

Finally, there are times when we are simply not finished investigating a case to determine whether to take it, or are taking the initial steps to put a strategy into place. Here's a page outlining some of the things we consider when making those decisions. This often involves not only gathering background information, but also conducting a legal and technological analysis of the situation. We also try to help people find other lawyers for cases we can't take. While working through this process, the worst thing we could do is to talk publicly before a legal strategy is in place and before EFF has solidified our role. This is especially true when the legal situation is in flux, as when emergency legal relief is sought or when some of the people potentially involved have not yet been notified or identified. We've had a few of those recently – close watchers of EFF may have some guesses about specific instances where this has been the situation.

However, none of this should keep EFF members, the press, or the public from emailing us at info@eff.org when something is happening that potentially requires EFF's involvement. EFF members and the general public are an essential part of our early warning system – a form of crowdsourcing that helps us have a much broader view of what's going on and where the important cases are occurring. But we hope you will understand if we answer your call or email with limited detail or if we hold back from commenting extensively in the press or on our blog. We believe strongly that everyone's rights online should be vigorously protected, and sometimes that requires us to be silent.

Met officer mulls legal action over phone-hack reports

(Hack In The Box)

Submitted at 3/29/2011 12:19:09 PM

Senior Metropolitan Police officer John Yates has taken legal advice about starting libel proceedings over "unfair reporting" of the tabloid phone hacking row, it emerged today. The acting Met deputy commissioner told a parliamentary committee this morning that he was not pursuing any actions at the moment but had "sought authority" to do so. Yates told MPs on the home affairs select committee that he was "entitled to defend" his integrity and the "the corporate soul" of the Met, following a number of stories about the force's handling of the News of the World hacking claims. "There is fair comment and fair reporting and there is unfair comment and unfair reporting," he said. "All I have said is I'm protecting my position and I'm not undertaking any legal proceedings against anybody at the moment."

Report on Declarations of War

by Richard Bejtlich (TaoSecurity)

Submitted at 3/24/2011 12:24:00 PM

Similar to my post Report on Instances of US Forces Abroad, I again thank Steven Aftergood for his post No-Fly Zones: Considerations for Congress. He points to a new report titled Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications(.pdf). This is a good resource for those trying to determine what is war, what isn't war, and what happens in each situation. From the report summary:

From the Washington Administration to the present, Congress and the President have enacted 11 separate formal declarations of war against foreign nations in five different wars. Each declaration has been preceded by a presidential request either in writing or in person before a joint session of Congress. The reasons cited in justification for the requests have included armed attacks on United States territory or its citizens and threats to United States rights or interests as a

sovereign nation.

Congress and the President have also enacted authorizations for the use of force rather than formal declarations of war. Such measures have generally authorized the use of force against either a named country or unnamed hostile nations in a given region. In most cases, the President has requested the authority, but Congress has sometimes given the President less than what he asked for.

Not all authorizations for the use of force have resulted in actual combat. Both declarations and authorizations require the signature of the President in order to become law. In contrast to an authorization, a declaration of war in itself creates a state of war under international law and legitimates the killing of enemy combatants, the seizure of enemy property, and the apprehension of enemy aliens.

While a formal declaration was once deemed a necessary legal prerequisite to war and was thought to terminate diplomatic and commercial relations and most treaties between the combatants, declarations have fallen into disuse since World War II.

The laws of war, such as the Hague and Geneva Conventions, apply to circumstances of armed conflict whether or not a formal declaration or authorization was issued. With respect to domestic law, a declaration of war automatically triggers many standby statutory authorities conferring special powers on the President with respect to the military, foreign trade, transportation, communications, manufacturing, alien enemies, etc. In contrast, no standby authorities appear to be triggered automatically by an authorization for the use of force, although the executive branch has argued, with varying success, that the authorization to use force in response to the terrorist attacks of 2001 provided a statutory exception to certain statutory prohibitions.

Most statutory standby authorities do not expressly require a declaration of war to be actualized but can be triggered by a declaration of national emergency or simply by the existence of a state of war; however, courts have sometimes construed the word "war" in a statute as implying a formal declaration, leading Congress to enact clarifying amendments in two cases.

Declarations of war and authorizations for the use of force waive the time limitations otherwise applicable to the use of force imposed by the War Powers Resolution.

This report provides historical background on the enactment of declarations of war and authorizations for the use of force and analyzes their legal effects under international and domestic law. It also sets forth their texts in two appendices.

The report includes an extensive listing and summary of statutes that are triggered by a declaration of war, a declaration of national emergency, and/or the existence of a state of war. The report concludes with a summary of the congressional procedures applicable to the enactment of a declaration of war or authorization for the use of force and to measures under the War Powers Resolution.

Tweet

Ultimate guide to Windows 7 security

(Hack In The Box)

Submitted at 3/28/2011 10:09:15 PM

Windows 7 has been warmly received and swiftly adopted by businesses, with the result that many IT admins are now struggling with the platform's new security features. In addition to changes to User Account Control, BitLocker, and other features inherited from Windows Vista, Windows 7 introduces a slew of security capabilities that businesses will want to take advantage of. Windows 7 improves on Vista with a friendlier UAC mechanism, the ability to encrypt removable media and hard drive volumes, broader support for strong cryptographic ciphers, hassle-free secure remote access, and sophisticated protection against Trojan malware in the form of AppLocker, to name just a few. In this guide, I'll run through these and other significant security enhancements in Windows 7, and provide my recommendations for configuring and using them. I'll pay especially close attention to the new AppLocker application control feature, which may be a Windows shop's most practical and affordable way to combat socially engineered Trojan malware.

It's Time for the Recording Industry to Stop Blaming "Piracy" and Start Finding A New Way

(EFF.org Updates)

Submitted at 3/25/2011 5:42:13 PM

As many — EFF included— have been saying for years, filesharing is not the reason that the recording industry has fallen on hard financial times. In fact, the recording industry's complaints that the sky is falling really only apply to the recording industry, and not musicians and the fans, who have seen increased music purchases, increased artist salaries, and the availability of more music than ever before. And now two new reports further debunk the recording industry's myth.

First, the London School of Economics released a paper finding that while filesharing may explain some of the decline in sales of physical copies of recorded music, the decline "should be explained by a combination of factors such as changing patterns in music consumption, decreasing disposable household incomes for leisure products and increasing sales of digital content through online platforms." And even if the sales of recorded music are down, there is an important distinction to draw: the recording industry may be hurting, but the music industry is thriving. For example, the LSE paper points out that in the UK in 2009, the revenues from live music shows outperformed recorded music sales.

We've also seen more and more artists making a go of it on their own. Rebecca Black, a 13-year-old, is reportedly netting nearly $25,000 a week from digital downloads of her hit song, "Friday." The band OK Go famously made a name for itself by self-producing widely popular music videos and then leaving a big record label that failed to"recognize the basic mechanics of the Internet" by attempting to prohibit embedding of the band's video content. As the lead singer noted, "[c]urbing the viral spread of videos isn't benefiting the company's bottom line, or the music it's there to support." Even bands with record deals are finding different ways to make money. For example, the popular band the Black Keys makes 85% of its money from live shows.

Another recent study, this one by the Social Science Research Council, delves into international aspects of "piracy," especially in emerging markets, and finds unauthorized filesharing in some developing economies has actually created opportunities for media companies to come up with innovative business models that allow legal and widespread access to media goods. For example, in India, "where large domestic film and music industries dominate the national market, [large media companies] set prices to attract mass audiences, and in some cases compete directly with pirate distribution." The impact of this cannot be understated: in many of these emerging markets, the new business models are improving legal access to music and art that was previously unaffordable for many people.

The SSRC report also points out that, despite the content industry's dire predictions, the media business is still thriving: "Software, DVD, and box office revenues in most middle-income countries have risen in the past decade — in some cases dramatically. Sales of CDs have fallen, but the overall music business, including performance, has grown."

Despite these realities, the policy debate continues to focus on enforcement and "strengthening intellectual property," which, SSRC rightly points out, is incredibly counterproductive and comes at a high social cost. Instead of discussing ways to make sure artists get paid for their work and fans have access to media goods, time and energy is wasted debating how to continue an enforcement policy that has failed to actually curb unauthorized filesharing.

We are encouraged to see studies like these that challenge policy makers to shift the tone of the debate to a more productive conversation about how to innovate and use new technologies to benefit artists and their fans. Because the bottom line is this: those who find ways to capitalize on new technologies will be the ones to succeed going forward.

Has Apple infiltrated the jailbreak community?

(Hack In The Box)

Submitted at 3/29/2011 12:15:16 PM

If you canâ€™t beat them, join them. At least that seems to be Appleâ€™s new mantra when it comes to patching jailbreak bugs according to Comex. One of the more influential hackers in the jailbreak community, Comex believes Apple may have planted a hacker on the iPhone Dev Team. The move, if it turns out to be true, would explain Appleâ€™s ability to patch jailbreak exploits before the iPhoneÂ Dev Team could release their software to the public. Comex pointed out on Twitter that Apple managed to patch an exploit that was slated to be used in JailbreakMe 2.0. The weird thing is that the exploit has been around since 4.0.2 through until iOS 4.3, but Apple managed to patch it with iOS 4.3.1.

ACLU and EFF Appeal Ruling In Case Challenging Government Attempt To Obtain Private Data in WikiLeaks Investigation

(EFF.org Updates)

Submitted at 3/25/2011 4:47:07 PM

Alexandria, VA - The Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) today appealed a ruling that the government can collect the private records of three Twitter users as part of its investigation related to WikiLeaks. The ruling further held that the users cannot learn which other Internet companies were ordered to turn over information about them to the government. EFF and the ACLU are challenging the ruling on behalf of Birgitta Jonsdottir, an Icelandic parliamentarian who is appealing jointly with fellow Twitter users Jacob Appelbaum and Rop Gonggrijp.

The secret government demands for information about the subscribers' communications came to light only because Twitter took steps to ensure its customers were notified and had the opportunity to respond. The ACLU and EFF have also asked the court to make public any similar orders to any other companies.

"Except in very rare circumstances, the government should not be permitted to obtain information about individuals' private Internet communications in secret. This is not one of those circumstances," said Aden Fine, staff attorney with the ACLU Speech, Privacy and Technology Project. "If the ruling is allowed to stand, our client might never know how many other companies have been ordered to turn over information about her, and she may never be able to challenge the invasive requests."

"Services like Twitter have information that can be used to track us and link our communications across multiple services including Facebook and Gmail," said EFF Legal Director Cindy Cohn. "The Magistrate's ruling that users have no ability to protect that information from the U.S. government is especially troubling."

The ruling was issued by U.S. Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia. It is being appealed to a U.S. District Judge in the Eastern District of Virginia.

Attorneys for Jonsdottir are Fine and Benjamin Siracusa Hillman of the ACLU, Rebecca Glenberg of the ACLU of Virginia, and Cindy Cohn, Lee Tien, Marcia Hofmann and Kevin Bankston of EFF. The motions were joined by attorneys from the law firm Keker & Van Nest LLP and the Law Office of John D. Cline on behalf of Appelbaum and Gonggrijp, respectively, as well as local counsel in Virginia.

For the full brief:
https://www.eff.org/files/Objections.pdf

For more on this case:
https://www.eff.org/cases/government-demands-twitter-records

Contacts:
Rebecca Jeschke
Media Relations Director
Electronic Frontier Foundation
press@eff.org
Rachel Myers
Media Relations
American Civil Liberties Union
media@aclu.org

What Location Tracking Looks Like

(EFF.org Updates)

Submitted at 3/29/2011 12:46:36 PM

Your cell phone company knows everywhere you go, twenty-four hours a day, every day. How concrete is this fact for you?

It's very concrete for Malte Spitz, a German politician and privacy advocate. He used German privacy law — which, like the law of many European countries, gives individuals a right to see what private companies know about them — to force his cell phone carrier to reveal what it knew about him. The result? 35,831 different facts about his cell phone use over the course of six months. As the German newspaper website Zeit Online reports:

This profile reveals when Spitz walked down the street, when he took a train, when he was in an airplane. It shows where he was in the cities he visited. It shows when he worked and when he slept, when he could be reached by phone and when was unavailable. It shows when he preferred to talk on his phone and when he preferred to send a text message. It shows which beer gardens he liked to visit in his free time. All in all, it reveals an entire life.

To show just how extensive this data is, Spitz chose to make it all available to the public; Zeit Online used it to prepare a remarkable interactive map, which animates Spitz's movements, moment by moment, over the course of half a year. It's correlated with information Spitz willingly posted on the web, and, according to him and the newspaper, is remarkably, eerily accurate. Try it out.

A report in the New York Times on Saturday described the data release, which it called "astounding", and put it in a U.S. context, quoting EFF's Kevin Bankston. The Times tried to find out whether U.S. mobile phone carriers have similar data about their subscribers, but it said "[t]he major American cellphone providers declined to explain what exactly they collect and what they use it for."

EFF has been following this issue for years and has worked extensively to limit government access to location data about individuals; government agents have increasingly sought to use this information, using questionable legal arguments to get carriers to turn it over. Still, it's remarkable to see an actual location data set about a real person. (According to the Times, German carriers have, for legal reasons, now stopped routinely storing this data. However, like all mobile phone carriers, they still have the technical ability to collect it at any time.)

Malte Spitz explains why he worked to obtain this information: to help educate the public about some of what's at stake in the German and worldwide debates about telecommunications data retention. All around the world, including the United States, proposed laws would force carriers to retain enormous quantities of personal information. As Spitz and Zeit Online have shown, these troves of information can give a detailed picture of each person's private life.

Firefox 4 sets unofficial download record

(Hack In The Box)

Submitted at 3/27/2011 10:12:30 PM

Mozilla set an unofficial record for software downloads on the second day of Firefox 4's launch, the company said Friday. In the 24 hours from early Wednesday to early Thursday, users downloaded 8.75 million copies of the new browser, an uptick from the 7.1 million logged by Firefox 4 its first day. Last week's one-day tally broke the record established by Firefox 3.0 in mid-2008 when that browser was downloaded more than 8 million times within 24 hours. Then, Mozilla ran a "Download Day" campaign that resulted in a certified Mozilla launched the final version of Firefox 4 around 6:30 a.m. PT Tuesday after more than a year of development.

Although Firefox 4's downloads bested Firefox 3's record, the achievement won't be official. In 2008, a Guinness representative monitored Mozilla's download servers to audit the number; no on-site official was present at Mozilla last week, a company spokeswoman said.

Microsoft Shuts off HTTPS in Hotmail for Over a Dozen Countries

(EFF.org Updates)

Submitted at 3/25/2011 6:21:15 PM

UPDATE (3/26/11): HTTPS is again available for those in the countries discussed below. Microsoft denies deliberately blocking access to HTTPS, blaming the problem on a bug:

We are aware of an issue that impacted some Hotmail users trying to enable HTTPS. That issue has now been resolved. Account security is a top priority for Hotmail and our support for HTTPS is worldwide – we do not intentionally limit support by region or geography and this issue was not restricted to any specific region of the world.

If you've been waiting for a golden opportunity to download EFF's HTTPS Everywhere Firefox add-on, this is it.

Microsoft appears to have turned off the always-use-HTTPS option in Hotmail for users in more than a dozen countries, including Bahrain, Morocco, Algeria, Syria, Sudan, Iran, Lebanon, Jordan, Congo, Myanmar, Nigeria, Kazakhstan, Uzbekistan, Turkmenistan, Tajikistan, and Kyrgyzstan. Hotmail users who have set their location to any of these countries receive the following error message when they attempt to turn on the always-use-HTTPS feature in order to read their mail securely:

Your Windows Live ID can't use HTTPS automatically because this feature is not available for your account type.

Microsoft debuted the always-use-HTTPS feature for Hotmail in December of 2010, in order to give users the option of always encrypting their webmail traffic and protecting their sensitive communications from malicious hackers using tools such as Firesheep, and hostile governments eavesdropping on journalists and activists. For Microsoft to take such an enormous step backwards undermining the security of Hotmail users in countries where freedom of expression is under attack and secure communication is especially importantis deeply disturbing. We hope that this counterproductive and potentially dangerous move is merely an error that Microsoft will swiftly correct.

The good news is that the fix is very easy. Hotmail users in the affected countries can turn the always-use-HTTPS feature back on by changing the country in their profile to any of the countries in which this feature has not been disabled, such as the United States, Germany, France, Israel, or Turkey. Hotmail users who browse the web with Firefox may force the use of HTTPS by defaultwhile using any Hotmail location settingby installing the HTTPS Everywhere Firefox plug-in.

Initial Thoughts on RSA "APT" Announcement

by Richard Bejtlich (TaoSecurity)

Submitted at 3/17/2011 8:29:00 PM

Today RSA's Art Coviello announced the following:

Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA...

Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT).

Our investigation also revealed that the attack resulted in certain information being extracted from RSA's systems. Some of that information is specifically related to RSA's SecurID two-factor authentication products.

While at this time we are confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers, this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack...

This is one of the problems with debates over terminology. If we all accepted the actual definition of APT as created by the Air Force in 2006, we would know what Mr Coviello is describing. Without that clarity we're left wondering if he means any threat on the planet that he and RSA choose to describe as "APT."

Without knowing anything more than what is printed in the RSA announcement, I can offer the following opinion. It is not outside the realm of APT methodology and targeting to attack RSA in order to access internal details on their authentication technology. We know APT actors have attacked other technology companies to steal their intellectual property, ranging from software to algorithms to private keys, all to better infiltrate other targets.

As I Tweeted on March 10th, it's public knowledge that validated APT actors have targeted public key infrastructure for several years. Besides PKI, enterprises of all types rely heavily on two-factor systems such as those created by RSA. Stealing technology and examining it for weaknesses, or identifying ways to exploit the supply chain, or otherwise gain an advantage over RSA users are all valid APT interests.

Hopefully we will learn more about this issue as time passes.

Adobe Releases Flash Player Update

by US-CERT (US-CERT Current Activity)

Submitted at 3/21/2011 1:22:13 PM

Adobe has released an update for Flash Player to address multiple vulnerabilities. These vulnerabilities affect Adobe Flash Player 10.1.102.64 and earlier versions for Windows, Macintosh, Linux, and Solaris, and Adobe Flash Player 10.1.106.16 and earlier versions for Android. Exploitation of these vulnerabilities may allow an attacker to cause a denial-of-service attack or execute arbitrary code.

US-CERT encourages users and administrators to review Adobe Security Advisory APSB11-05 and apply any necessary updates to help mitigate the risks.

US Tax Season Phishing Scams and Malware Campaigns

by US-CERT (US-CERT Current Activity)

Submitted at 3/16/2011 10:32:25 AM

In the past, US-CERT has received reports of an increased number of phishing scams and malware campaigns that take advantage of the United States tax season. Due to the upcoming tax deadline, US-CERT reminds users to remain cautious when receiving unsolicited email that could be part of a potential phishing scam or malware campaign.

These phishing scams and malware campaigns may include, but are not limited to, the following:

- information that refers to a tax refund
- warnings about unreported or under-reported income
- offers to assist in filing for a refund
- details about fake e-file websites

These messages which may appear to be from the IRS, may ask users to submit personal information via email or may instruct the user to follow a link to a website that requests personal information or contains malicious code.

US-CERT encourages users and administrators to take the following measures to protect themselves from these types of phishing scams and malware campaigns:

- Do not follow unsolicited web links in email messages.
- Maintain up-to-date antivirus software.
- Refer to the IRS website related to phishing, email, and bogus website scams for scam samples and reporting information.
- Refer to the Recognizing and Avoiding Email Scams(pdf) document for more information on avoiding email scams.
- Refer to the Avoiding Social Engineering and Phishing Attacks document for more information on social engineering attacks.
- Review the Wall Street Journal blog post " Cybercrooks Digging for Tax Data" for additional suggestions for protecting against these types of attacks.

Another New Study Shows That Filesharing Doesn't Deter Artists From Making Music

(EFF.org Updates)

Submitted at 3/28/2011 12:20:04 PM

Further proof that the recording industry's oft-repeated claims of the downfall of the entire music industry hold no water: a new report finding that filesharing has led directly to "reduced costs of bringing works to market and a growing role of independent labels." In other words, in the past decade, we have seen more music from independent outlets and at lower prices – something that consumers and music fans should all be happy about.

The study, by University of Minnesota economist Joel Waldfogel, proves just what we've been saying as recently as last week– that filesharing (unauthorized or not) has led more artists to create more music, and – just as importantly – more different music. U.S. copyright law is based on a compromise recognized in the Constitution that grants authors (or artists, or musicians) a limited monopoly designed to give those authors an incentive to make their creative works. As we've long known and as this study makes clear yet again, even in the face of filesharing, those incentives still exist.

Serious security gaps found in NASA's computer network

(Hack In The Box)

Submitted at 3/28/2011 10:11:23 PM

NASAâ€™s internal computer network is full of holes and is extremely vulnerable to an external cyberattack, an audit by the agency's Office of the Inspector General has

SERIOUS page 6

Japan Quake Malware Again

(Securelist / Blog)

Submitted at 3/25/2011 9:29:28 AM

The earthquake and tsunami related crisis in Japan is still far from over - so is the appearance of new cyber threats trying to exploit that same crisis. Tens of thousands of people in Japan have lost their homes, and many their loved ones too. On top of that, radiation leaks are still a major concern for the country and its observers , while new tremors remind everyone of nature's power on an almost daily basis. (At time of writing, a Magnitude 6.2 quake shook the place!). Today we investigated another malicious webpage. This one states in Portuguese: "Novo tsunami atinge a região de Sendai e Japão declara estado de emegência em usina nuclear", which roughly translated means "New tsunami reaches the area of Sendai, Japan declares state of emergency at nuclear power plant".

Requesting Comments on Open Information Security Foundation

by Richard Bejtlich (TaoSecurity)

Submitted at 3/18/2011 2:00:00 PM

Thank you to anyone who voted for me to join the board of the Open Information Security Foundation. They are most famous for their Suricata intrusion detection engine, but I expect additional outputs as time passes. I appreciate those of you who supported my goal to join their board. I will try to provide fair and useful input to the project.

I believe we will have our first board phone call next week. Are there any issues you would like me to raise, or consider for future meetings?

I am personally interested in OISF because I think they bring a level of enthusiasm, openness, and innovation to the open source network security monitoring space, alongside tools like Bro and Snort and others I mentioned in my January post Seven Cool Open Source Projects for Defenders.

OISF is also a US nonprofit, a 501c(3) group, so I like the idea of helping that sort of organization.

Review of Kingpin Posted

by Richard Bejtlich (TaoSecurity)

Submitted at 3/25/2011 9:00:00 PM

Amazon.com just posted my four star review of Kingpin by Kevin Poulsen. I read this book by checking it out of my library! From the review:

I've read and reviewed almost all of the non-fiction computer crime and espionage books written since the 1980s. Kingpin by Kevin Poulsen is one of my favorites. I will recommend this book to fellow digital security professionals and those who would like insights into our world. Kingpin's coverage of Max Ray Butler's (MRB) constant entanglement with the dark side is a lesson for anyone contemplating using their skills for evil.

On a related note, in late 2007 I posted Max Ray Butler in Trouble Again and followed that in 2010 with Max Ray Butler Sentenced (Again).

Fraudulent SSL Certificates

by US-CERT (US-CERT Current Activity)

Submitted at 3/23/2011 12:54:38 PM

US-CERT is aware of public reports of the existence of fraudulent SSL certificates. These fraudulent SSL certificates could be used by an attacker to masquerade as a trusted website. Multiple web browser vendors have provided updates to recognize and block these fraudulent SSL certificates.

Mozilla has updated Firefox 4.0, 3.6, and 3.5. Additional information can be found in the Mozilla Security Blog.

Microsoft has released updates for various platforms in Microsoft Knowledge Base Article 2524375. Additional information can be found in Microsoft Security Advisory 2524375.

US-CERT encourages users and administrators to apply any necessary updates to help mitigate the risks. US-CERT will provide additional information as it becomes available.

SERIOUS

continued from page 5

found. Even worse, it appears that several of the vulnerabilities were known about for months yet remained unpatched. â€œSix computer servers associated with IT [information technology] assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable,â€ the audit report released Monday by Inspector General Paul K. Martin said. "The attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASAâ€™s operations," the report continued. "We also found network servers that revealed encryption keys, encrypted passwords, and user account information to potential attackers."

Paul Baran, one of the founding fathers of the internet dies at 85

(Hack In The Box)

Submitted at 3/29/2011 12:23:15 PM

One of the men who laid the foundations of the internet died on Saturday at the age of 85. US Scientist Paul Baran was one of the first to look into how telecommunication networks would work in the future. His work with packaging data in the 1960s has been credited with playing a key role in the later development of the internet. Vinton Cerf is another founder of the internet and tells BBC Radio 5 live Up All Night's Giles Dilnot that Baran was a "prolific inventor".

Ransomware: Fake Federal German Police (BKA) notice

(Securelist / Blog)

Submitted at 3/24/2011 9:42:10 AM

Kaspersky Lab is still monitoring malicious websites involved in the recent Japan spam campaigns.

For those who may have missed the two first blogs, you can read them here and here However, today we discovered than some of the payloads were not the usual Trojan-Downloader.Win32.CodecPack.*.

Malvertizing Continued - Spotify's Ad Networks Outed

(Securelist / Blog)

Submitted at 3/25/2011 4:52:48 PM

Over the past couple months, some advertising networks have been distributing ads that redirect browsers to sites hosting exploits.

Spotify's advertising network was most recently outed(note that it is the third party banner ads rotating through the client's ad frames). Most of the redirections we have been been monitoring have sent users to a variety of servers in the .cc TLD. We have been working with providers to ensure the ads aren't on their networks, but the groups have been active in rotating malvertizing banners through multiple networks.

Ransomware: GPCode strikes back

(Securelist / Blog)

Submitted at 3/25/2011 4:05:31 PM

Back in November 2010, we wrote a blog post about a new variant of the Gpcode Ransomware.

Kaspersky lab discovered a new variant today, in the form of an obfuscated executable. Please review the technical details for further information. The threat was detected automatically thanks to the Kaspersky Security Network as UDS:DangerousObject.Multi.Generic.

Specific detection has been added and the threat is now detected as Trojan-Ransom.Win32.Gpcode.bn

VideoLAN Releases VLC Media Player 1.1.8

by US-CERT (US-CERT Current Activity)

Submitted at 3/25/2011 6:43:40 AM

VideoLAN has released VLC Media Player 1.1.8 to address two vulnerabilities. These vulnerabilities are due to the improper handling of .AMV and .NSV files. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.

US-CERT encourages users and administrators to review the release notes for VLC Media Player 1.1.8 and apply any necessary updates to help mitigate the risks.

Google Releases Chrome 10.0.648.204

by US-CERT (US-CERT Current Activity)

Submitted at 3/25/2011 6:43:43 AM

Google has released Chrome 10.0.648.204 for Windows, Mac, Linux, and Chrome Frame to address multiple vulnerabilities. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code.

US-CERT encourages users and administrators to review the Google Chrome Releases blog entry and apply any necessary updates to help mitigate the risks.