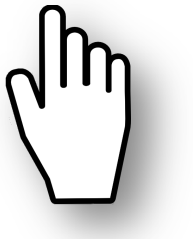

www.attacker.com
Mozilla Firefox
BEST GAME EVER!
PLAY!
twitter
Is this goodbye?
This action is permanent.
Before you deactivate your account, know this:

Using JS to Steal Facebook *Likes*

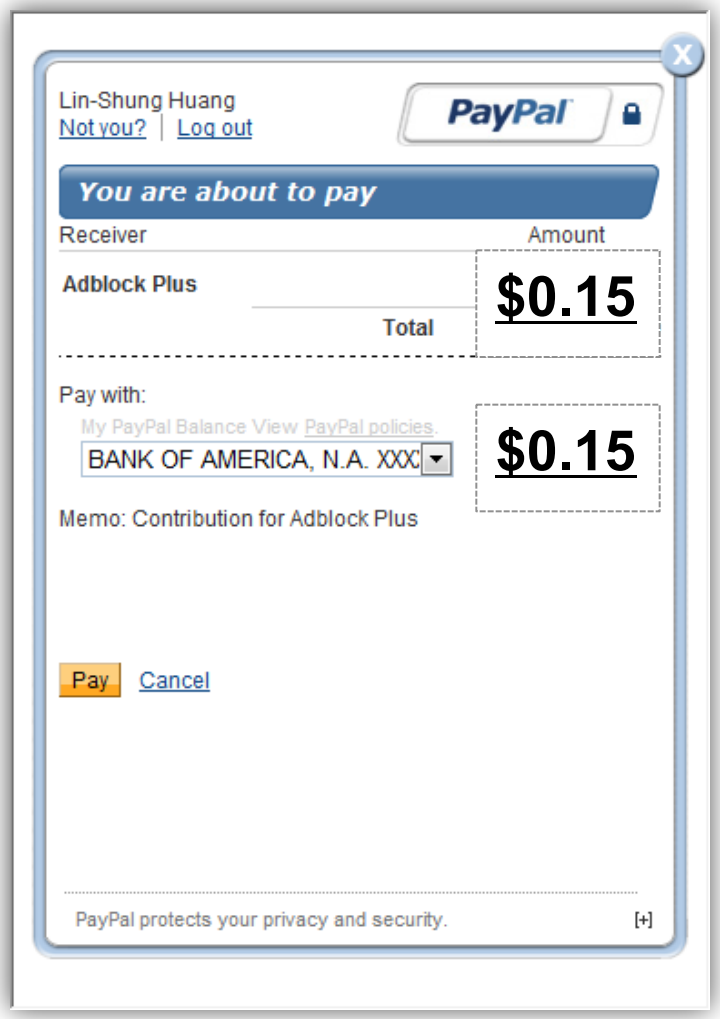


- *Bait-and-switch*
- Note: many of these attacks are similar to *TOCTTOU* (Time of Check to Time of Use) vulnerabilities

From **Clickjacking: Attacks and Defenses**, by Lin-Shung Huang et al, Carnegie Mellon University / Microsoft Research

Compromise visual integrity – target

- Hiding the target
- Partial overlays



Clickjacking to Access the User's Webcam

From **Clickjacking: Attacks and Defenses**, by Lin-Shung Huang et al, Carnegie Mellon University / Microsoft Research

Keychain Access

Click to lock the System Roots keychain.

Keychains
- login
- Micr...ertificates
- System
- System Roots

Category
- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates

A-Trust-Qual-02
Root certificate authority
Expires: Tuesday, December 2, 2014 3:00:00 PM PT
This certificate is valid

Name	Kind	Expires	Keychain
A-CERT ADVANCED	certificate	Oct 23, 2011 7:14:14 AM	System Roots
A-Trust-nQual-01	certificate	Nov 30, 2014 3:00:00 PM	System Roots
A-Trust-nQual-03	certificate	Aug 17, 2015 3:00:00 PM	System Roots
A-Trust-Qual-01	certificate	Nov 30, 2014 3:00:00 PM	System Roots
A-Trust-Qual-02	certificate	Dec 2, 2014 3:00:00 PM	System Roots
AAA Certificate Services	certificate	Dec 31, 2028 3:59:59 PM	System Roots
AC Raíz Certicámara S.A.	certificate	Apr 2, 2030 2:42:02 PM	System Roots
AddTrust Class 1 CA Root	certificate	May 30, 2020 3:38:31 AM	System Roots
AddTrust External CA Root	certificate	May 30, 2020 3:48:38 AM	System Roots
AddTrust Public CA Root	certificate	May 30, 2020 3:41:50 AM	System Roots
AddTrust Qualified CA Root	certificate	May 30, 2020 3:44:50 AM	System Roots
Admin-Root-CA	certificate	Nov 9, 2021 11:51:07 PM	System Roots
AdminCA-CD-T01	certificate	Jan 25, 2016 4:36:19 AM	System Roots
AffirmTrust Commercial	certificate	Dec 31, 2030 6:06:06 AM	System Roots
AffirmTrust Networking	certificate	Dec 31, 2030 6:08:24 AM	System Roots
AffirmTrust Premium	certificate	Dec 31, 2040 6:10:36 AM	System Roots
AffirmTrust Premium ECC	certificate	Dec 31, 2040 6:20:24 AM	System Roots
America Onli...ation Authority 1	certificate	Nov 19, 2037 12:43:00 PM	System Roots
America Onli...ation Authority 2	certificate	Sep 29, 2037 7:08:00 AM	System Roots
AOL Time W...cation Authority 1	certificate	Nov 20, 2037 7:03:00 AM	System Roots
AOL Time W...cation Authority 2	certificate	Sep 28, 2037 4:43:00 PM	System Roots
Apple Root CA	certificate	Feb 9, 2035 1:40:36 PM	System Roots
Apple Root Certificate Authority	certificate	Feb 9, 2025 4:18:14 PM	System Roots
Application CA G2	certificate	Mar 31, 2016 7:59:59 AM	System Roots
ApplicationCA	certificate	Dec 12, 2017 7:00:00 AM	System Roots

Copy

167 items

News

Solo Iranian hacker takes credit for Comodo certificate attack

Security researchers split on whether 'ComodoHacker' is the real deal

By Gregg Keizer

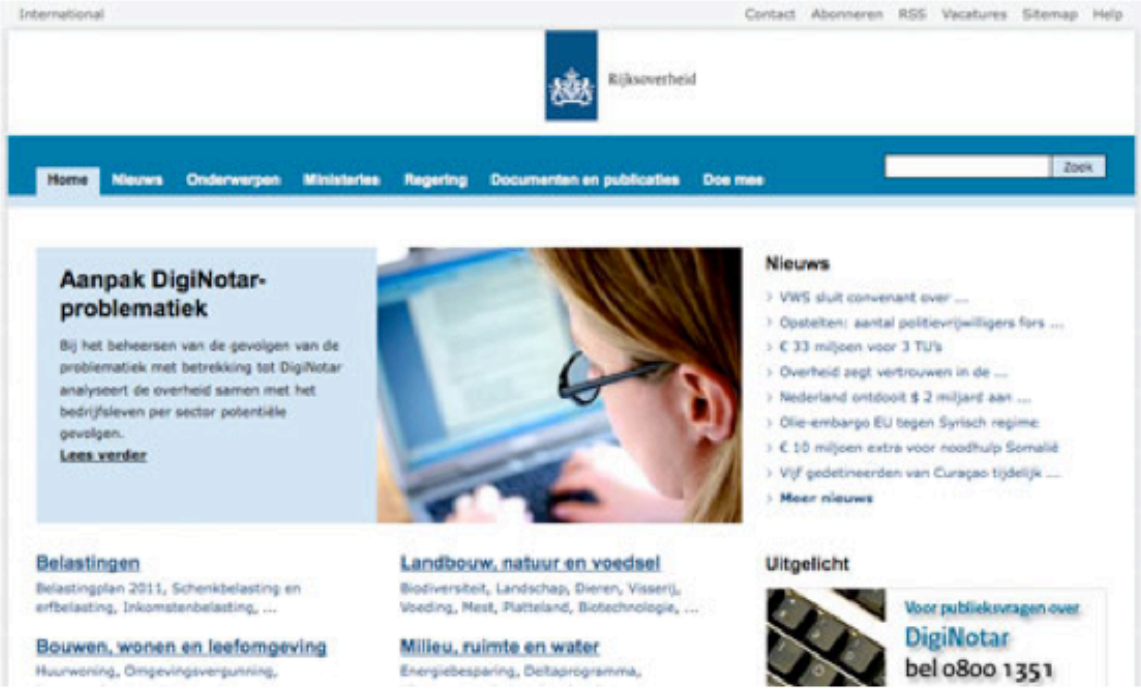
March 27, 2011 08:39 PM ET

Computerworld - A solo Iranian hacker on Saturday claimed responsibility for stealing multiple SSL certificates belonging to some of the Web's biggest sites, including Google, Microsoft, Skype and Yahoo.

Early reaction from security experts was mixed, with some believing the hacker's claim, while others were dubious.

Last week, conjecture had focused on a state-sponsored attack, perhaps funded or conducted by the Iranian government, that hacked a certificate reseller affiliated with U.S.-based Comodo.

On March 23, Comodo acknowledged the attack, saying that eight days earlier, hackers had obtained nine bogus certificates for the log-on sites of Microsoft's Hotmail, Google's Gmail, the Internet phone and chat service Skype and Yahoo Mail. A certificate for Mozilla's Firefox add-on site was also acquired.



The Dutch government has revoked all trust in digital certificates issued by DigiNotar

The Dutch government says hackers who broke into a web security firm in the Netherlands last month issued hundreds of bogus security certificates that could be used on websites including the CIA and Israel's Mossad, as well as internet giants such as Google, Microsoft and Twitter.

More than 500 fake certificates, including some which could be used to send fake Windows updates to computers, and others which could be used when connecting to the CIA's site, were fraudulently issued in the hack, which occurred in July.

The Dutch government took the exceptional step of calling a press conference at 1.15am on Saturday morning to announce that it was revoking all trust in digital certificates issued by DigiNotar, which until then had been used for all online tax returns filed in the Netherlands.

Law Enforcement Appliance Subverts SSL

By Ryan Singel March 24, 2010 | 1:55 pm | Categories: Surveillance, Threats

That little lock on your browser window indicating you are communicating securely with your bank or e-mail account may not always mean what you think its means.

Normally when a user visits a secure website, such as Bank of America, Gmail, PayPal or eBay, the browser examines the website's certificate to verify its authenticity.

At a recent wiretapping convention, however, security researcher Chris Soghoian discovered that a small company was marketing internet spying boxes to the feds. The boxes were designed to intercept those communications — without breaking the encryption — by using forged security certificates, instead of the real ones that websites use to verify secure connections. To use the appliance, the government would need to acquire a forged certificate from any one of more than 100 trusted Certificate Authorities.

The main take-away from the above graph is that ATLAS data shows **no statistically significant increase** for either AS4134 or AS23724. While we did observe modest changes in traffic volumes for carriers within China, the BGP hijack had limited impact on traffic volumes to or from the rest of the world.

As a couple readers of my blog observed (link to comments), traffic volumes provide an awkward measure of the security implications of a BGP hijack. In particular, the volume of hijacked traffic change depends on:

If the intent was to hijack traffic for a small set of sensitive US government machines, then we might see TCP connections diverted for only a few machines in a man-in-the-middle attack, relatively low volumes of diverted traffic, and thousands of bogus routes announced as a smokescreen (credit for this scenario to my colleague Danny McPherson in a NYTimes interview). In other words, basically close to what we observed on April 15th.

Or maybe, of course, this was just a typo in a configuration file.

Keychain Access

Click to lock the System Roots keychain.

Keychains

- login
- Micr…ertificates
- System
- System Roots

Category

- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates

CNNIC ROOT

Root certificate authority

Expires: Friday, April 16, 2027 12:09:14 AM PT

This certificate is valid

Name	Kind	Expires	Keychain
Class 1 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 1 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 1 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Primary CA	certificate	Jul 6, 2019 4:59:59 PM	System Roots
Class 2 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 2 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi…fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi…fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 3 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 4 Publi…on Authority – G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
CNNIC ROOT	certificate	Apr 16, 2027 12:09:14 AM	System Roots
Common Policy	certificate	Oct 15, 2027 9:08:00 AM	System Roots
COMODO Certification Authority	certificate	Dec 31, 2029 3:59:59 PM	System Roots
Deutsche Telekom Root CA 2	certificate	Jul 9, 2019 4:59:00 PM	System Roots
DigiCert Assured ID Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Global Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Hig…rance EV Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiNotar Root CA	certificate	Mar 31, 2025 11:19:21 AM	System Roots
DoD CLASS 3 Root CA	certificate	May 14, 2020 6:13:00 AM	System Roots

Copy

167 items

Keychain Access

Click to lock the System Roots keychain.

Keychains

- login
- Micr...ertificates
- System
- System Roots

Category

- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates

CNNIC ROOT

Root certificate authority

Expires: Friday, April 16, 2027 12:09:14 AM PT

This certificate is marked as not trusted for all users

Name	Kind	Expires	Keychain
Class 1 Publi...fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 1 Publi...fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 1 Publi...on Authority - G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Primary CA	certificate	Jul 6, 2019 4:59:59 PM	System Roots
Class 2 Publi...fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 2 Publi...fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 2 Publi...on Authority - G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi...fication Authority	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 3 Publi...fication Authority	certificate	Aug 2, 2028 4:59:59 PM	System Roots
Class 3 Publi...on Authority - G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
Class 4 Publi...on Authority - G2	certificate	Aug 1, 2028 4:59:59 PM	System Roots
CNNIC ROOT	certificate	Apr 16, 2027 12:09:14 AM	System Roots
Common Policy	certificate	Oct 15, 2027 9:08:00 AM	System Roots
COMODO Certification Authority	certificate	Dec 31, 2029 3:59:59 PM	System Roots
Deutsche Telekom Root CA 2	certificate	Jul 9, 2019 4:59:00 PM	System Roots
DigiCert Assured ID Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Global Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiCert Hig...rance EV Root CA	certificate	Nov 9, 2031 4:00:00 PM	System Roots
DigiNotar Root CA	certificate	Mar 31, 2025 11:19:21 AM	System Roots
DoD CLASS 3 Root CA	certificate	May 14, 2020 6:13:00 AM	System Roots

Copy

167 items

Security Warning: Do you trust the Russian government?

Firefox has detected that your connection to this website is probably not secure. If you are attempting to access or transmit sensitive data, you should **stop** this task, and try again using a **different Internet connection**.

Firefox has detected a potential security problem while trying to access www.bankofamerica.com, a website visited at least 131 times in the past by persons using this computer.

In these previous browsing sessions, www.bankofamerica.com provided a security certificiate verified by a company in the **United States**.

However, this website is now presenting a different security certificate verified by a company based in **Russia**.

If you do not trust the government of Russia with your private data, or think it unlikely that Bank of America would obtain a security certificate from a company based there, this could be a sign that someone is attempting to intercept your secure communications.

Click here to learn more about security certificiates and this potentially risky situation.

If you trust the government of Russia and companies located there to protect your privacy and security, click here to accept this new certificate and continue with your visit to the site.

Get me out of here!

```
static OSStatus
SSLVerifySignedServerKeyExchange(SSLContext *ctx, bool isRsa, SSLBuffer signedParams,
                                 uint8_t *signature, UInt16 signatureLen)
{
        OSStatus        err;
        ...

        if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
                goto fail;
        if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
                goto fail;
                goto fail;
        if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
                goto fail;
        ...

fail:
        SSLFreeBuffer(&signedHashes);
        SSLFreeBuffer(&hashCtx);
        return err;
}
```

reason	occurences
NULL	921683
Affiliation Changed	41438
CA Compromise	248
Certificate Hold	80371
Cessation Of Operation	690905
Key Compromise	73345
Privilege Withdrawn	4622
Superseded	81021
Unspecified	168993

https://www.eff.org/deeplinks/2011/10/how-secure-https-today