SWITCHcert Security Report

November 2014

SWITCH

I. The «long tail» effect of Shellshock, Heartbleed & co.

«We're just at the beginning of a cycle of vulnerabilities being found in the software we rely on every day.» This is the conclusion drawn by Martin McKeay, Senior Security Advocate at Akamai, following the discovery of two major security loopholes – Heartbleed and Shellshock – in the same year.

As mentioned in June's Security Report, Heartbleed is a vulnerability in the almost universally used OpenSSL software library that can be exploited, for example, to access passwords or SSL keys.

In September, a French developer discovered a leak in Bash, a fundamental component of UNIX and Linux systems that is over 20 years old. The Bash bug, which became widely known as Shellshock, is a threat not only to UNIX and Linux servers, but also OS X, network devices such as routers and webcams and a wide range of other hardware connected to the Internet.

Even months after Heartbleed and Shellshock came to light, the consensus among security experts is that they have still not been fixed on thousands of computers. Criminal hackers are now using Shellshock to gain access to mail servers, for instance,

so that they can set up and run botnets. OpenVPN-encrypted network connections are not immune to Shellshock either.

While most system administrators react quickly and install all available updates as soon as they become available, it will nevertheless be many years before all devices that are potentially at risk have been patched or, if necessary, replaced.

McKeay believes that the next Shellshock is just around the corner, pointing out that security loopholes like Heartbleed and Shellshock are hidden in program code developed in an era when such problems were not yet relevant. This code has survived and been integrated, be it partially or in its entirety, into the latest software. The only way to eliminate as many of these vulnerabilities (which have in fact existed for a very long time) as possible is by checking billions of lines of code and replacing it where necessary with new code that meets today's security standards.

Another aspect of this «legacy» can be seen in the POODLE attack on SSL/TLS-encrypted connections that was recently published by Google researchers. Here, the attacker attempts to downgrade a connection's security level to the outdated and insecure SSLv3 protocol in order to hack it. Unlike Heartbleed and Shellshock, POODLE exploits a vulnerability not in old programme code, but in an old protocol that has long since outlived its purpose.

Read more here:

http://securityintelligence.com/heartbleed-and-shellshock-the-new-norm-in-vulnerabilities

http://www.switch.ch/export/sites/default/all/cert/downloads/secrep/_files_secrep/SecurityReport_Juni2014.pdf

http://www.spiegel.de/netzwelt/web/sicherheitsluecke-shellshock-bedroht-linux-rechner-und-macs-a-993688.html

http://www.csoonline.com/article/2839054/vulnerabilities/report-criminals-use-shellshock-against-mail-servers-to-build-botnet.html

http://www.heise.de/security/meldung/Angriff-auf-Verschluesselung-Reaktionen-auf-die-Poodle-Luecke-2425244.html

http://blog.erratasec.com/2014/10/some-poodle-notes.html

II. Malvertising: hackers learning from advertising professionals

Invincea, an IT security firm based in the US state of Virginia, has dubbed a particularly devious form of malvertising «Operation DeathClick». The company reported in mid-October that it had seen evidence of malvertisers moving away from broad-based attacks and instead profiling their victims using specific target-group characteristics and delivering manipulated advertisements to them through a process called real-time ad bidding. This is where advertisers bid for space on a website in real time while it is loading. As with normal analogue and digital advertising, the target audience can be segmented using regional, economic or sociological criteria and sometimes even more precisely using individual profiles.

«Operation DeathClick» was aimed at staff of aerospace and defence companies. As in legal advertising, it would appear that a clearer distinction is being drawn between broad business-to-customer (B2C) advertising and more carefully targeted business-to-business (B2B) advertising.

Malvertising that casts a wide net to lure all manner of users into clicking on manipulated advertisements on sites like Yahoo or AOL and downloading ransomware is still commonplace and remains an expensive problem for its victims. This is especially the case when ransomware encrypts the entire server infrastructure, which recently happened to a large organisation in the US.

However, security experts Adam Caudill and Brandon Wilson have shown that classic promotional giveaways can also be used for a form of malvertising. They published a piece of software that allows USB sticks – a very popular promotional gift – to upload malware and hijack a computer as soon as they are plugged into it.

Read more here:

https://threatpost.com/apts-target-victims-with-precision-ephemeral-malvertising/108906

http://www.csoonline.com/article/2838025/data-protection/disaster-as-cryptowall-encrypts-us-firms-entire-server-installation.html

http://www.enigmasoftware.com/cryptowall-ransomware-updated-version-2-new-obfuscator

http://www.nzz.ch/mehr/digital/badusb-stick-adam-caudill-und-brandon-wilson-1.18396488

III. Legitimate defence of the right to protection versus opening Pandora's box

The September edition of the SWITCH Security Report mentioned ongoing network blocking lawsuits against Austrian Internet service providers. Since then, the websites kinox.to and kino4k.to have been blocked in Austria. Now that the European Court has been called into proceedings, commentators fear that a Europe-wide online censorship infrastructure may become established. It seems that they are right to be concerned. Six websites offering fake Cartier watches were recently blocked in the UK on the grounds that they infringed trademark rights rather than copyright. If the UK prosecutors have their way, 46,000 more sites will be blocked. Austria's anti-piracy association VAP also wants a further 100 sites blocked. With an estimated cost of EUR 6,300 per site, this would mean a huge financial hit for the ISPs.

The targeted reform of European and Swiss intellectual property law (in which the AGUR12 working group plays a key role) looks like sparking wider debate on Internet freedom.

Meanwhile, moves are being made somewhere else entirely: a new draft law in Austria with the unassuming name «Second Tax Amendment Act 2014» provides for the Austrian financial authorities to demand information on Internet access and traffic from telecom providers if there is even a suspicion of financial crime.

Read more here:

https://netzpolitik.org/2014/netzsperren-ab-heute-in-oesterreich-bald-in-ganz-europa

http://futurezone.at/netzpolitik/netzsperren-fuer-seiten-mit-gefaelschten-cartier-uhren/93.087.367

http://futurezone.at/netzpolitik/finanz-will-auskunft-zu-ip-adressen/92.820.502

http://www.nzz.ch/aktuell/digital/agur-12-urheberrecht-1.18319514

IV. Taxing the Net: a Hungarian posse gets serious

The failure of Hungarian Prime Minister Viktor Orbán's attempt to impose a tax of 150 forints (about CHF 0.59) per gigabyte on data traffic – with a maximum bill of 700 forints (about CHF 2.78) a month for private individuals – could be seen as amusing, were this not such a serious subject. Hungary's citizens and the European Commission saw the planned tax not only as a financial burden, but also as a restriction of democratic freedoms. Their mass protests have now caused Orbán to abandon his plans, but the Hungarian government still intends to tax revenues made on and with the Internet. Have Hungary's financial authorities, like Austria's (see III. above), turned to the Net as a new cash cow?

Read more here:

http://www.zeit.de/politik/ausland/2014-10/ungarn-orb-n-zieht-umstrittene-internet-steuer-zurueck

http://www.budapester.hu/2014/10/26/zehntausende-demonstrieren-gegen-internetsteuer

http://www.computerworld.ch/news/it-branche/artikel/widerstand-gegen-internetsteuer-66676

http://ec.europa.eu/avservices/video/player.cfm?ref=I094641

The Clipboard: Interesting Presentations, Articles and Videos

Securing SSL/TLS certificates with DNSSEC: an interesting talk on DANE by Carsten Strotmann (in German):

https://www.youtube.com/watch?v=KZiW-7jXda4

Something for everyone: 122 presentations from this year's RIPE69 in London:

https://ripe69.ripe.net/presentations/presentation-archive/

A «chat» between US cryptography expert Whitfield Diffie and NSA Director Michael Rogers:

https://www.youtube.com/watch?v=yhwy2ZWi_y8

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.