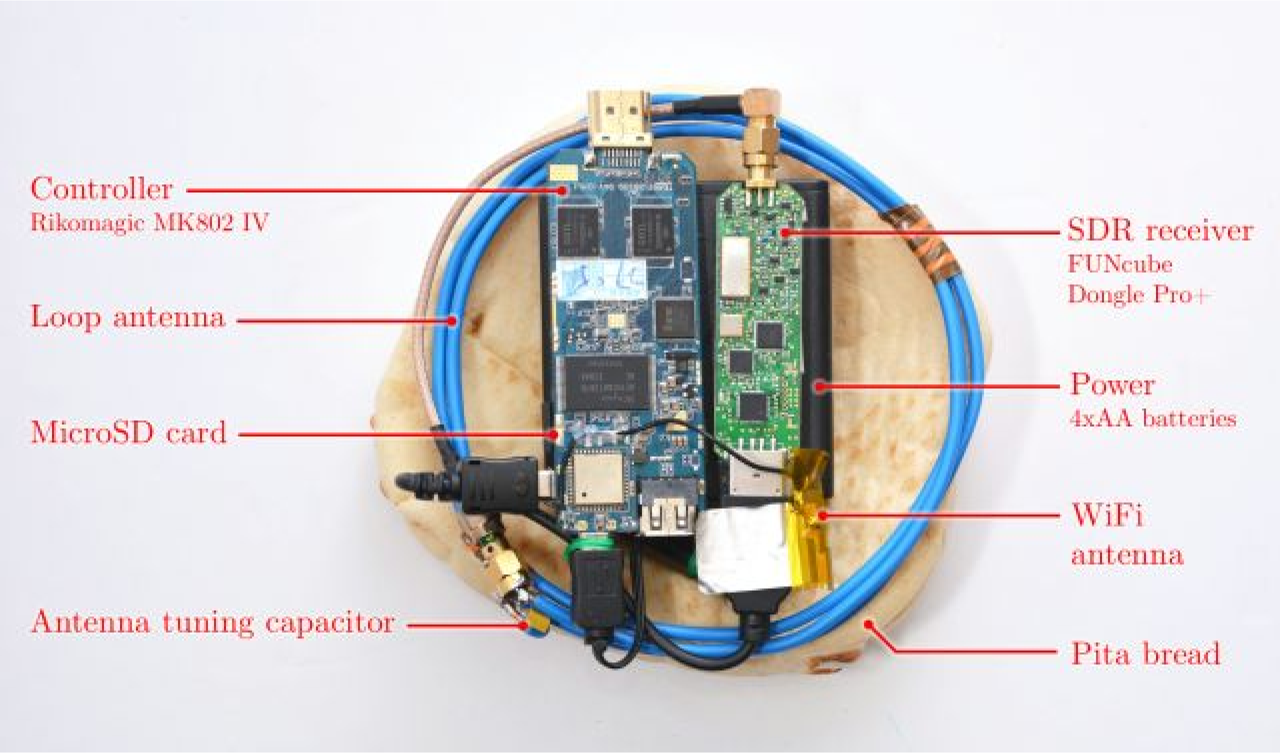
Security Now! #514 - 06-30-15

Tor’s Astoria Client

This week on Security Now!

- Abode issues an emergency out-of-cycle patch for FLASH,
- Microsoft updates its root certificate store and ruffles a few feathers,
- An update to Google's Chrome browser unnerves some,
- Samsung's original solution to driver collision,
- An AM radio that steals nearby Crypto keys,
- A truly FABULOUS siteof Privacy tools,
- New evidence that major ISPs are not being net-neutral,
- Managing NoScript,
- Some miscellaneous notes,
- A look at efforts to increase Tor’s privacy.

Is that Pita Bread spying on you?



Security News

Adobe issues emergency (out-of-cycle) FLASH player update

- https://www.fireeye.com/blog/threat-research/2015/06/operation-clandestine-wolf-adobe-flash-zero-day.html
- Operation Clandestine Wolf – Adobe Flash Zero-Day in APT3 Phishing Campaign
- In June, FireEye's FireEye as a Service team in Singapore uncovered a phishing campaign exploiting an Adobe Flash Player zero-day vulnerability. The attackers' emails included links to compromised web servers that served either benign content or a malicious Adobe Flash Player file that exploits the vulnerability (CVE-2015-3113).
- CVE-2015-3113:
    - Heap-based buffer overflow in Adobe Flash Player before 13.0.0.296 and 14.x through 18.x before 18.0.0.194 on Windows and OS X and before 11.2.202.468 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in June 2015.
- APT3
    - The China-based threat group FireEye tracks as APT3, aka UPS, is responsible for this exploit and activity. This group is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of introducing new browser-based zero-day exploits (e.g., Internet Explorer, Firefox, and Adobe Flash Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts, and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.
- Overview
    - In the last several weeks, APT3 actors launched a large-scale phishing campaign against organizations in the following industries:
        - Aerospace and Defense
        - Construction and Engineering
        - High Tech
        - Telecommunications
        - Transportation

    - Upon clicking the URLs provided in the phishing emails, targets were redirected to a compromised server hosting JavaScript profiling scripts. Once a target host was profiled, victims downloaded a malicious Adobe Flash Player SWF file and an FLV file, detailed below. This ultimately resulted in a custom backdoor known as SHOTPUT being delivered to the victim's system.

- Exploit Details
    - The attack exploits an unpatched vulnerability in the way Adobe Flash Player parses Flash Video (FLV) files. The exploit uses common vector corruption techniques to bypass Address Space Layout Randomization (ASLR), and uses Return-Oriented Programming (ROP) to bypass Data Execution Prevention (DEP). A neat trick to their ROP technique makes it simpler to exploit and will evade some ROP detection techniques.

Shellcode is stored in the packed Adobe Flash Player exploit file alongside a key used for its decryption. The payload is xor encoded and hidden inside an image.

The Adobe Flash Player exploit is packed with a simple RC4 packer. The RC4 key and ciphertext are BinaryData blobs that the packer uses to decrypt the layer 2 Adobe Flash Player file. Once decrypted, layer 2 is executed with loader.loadBytes.

Layer 2 uses a classic Adobe Flash Player Vector corruption technique to develop its heap corruption vulnerability to a full relative read/write available to ActionScript3. In this technique, the attacker sprays Adobe Flash Player Vectors to the heap, and triggers a write vulnerability to change the size of one of the vectors. The attacker can then perform subsequent reads and writes to memory outside the intended boundaries of the corrupted Vector object from AS3.

Once the attacker has limited read/write access to memory, they choose to corrupt a second Vector to increase their access to a range of 0x3FFF FFFF bytes. This second Vector is used for the remainder of the exploit.

The attackers use a ROP chain to call kernel32!VirtualAlloc to mark their shellcode as executable before jumping to their shellcode. Instead of writing their ROP chain to the heap along with their shellcode and payload, they used a different technique. Usually, exploit developers will corrupt a built-in Adobe Flash Player object such as a Sound object. Instead, the attackers chose to define their own class in AS3 with a function that takes a lot of arguments:

```
class CustomClass {
        public function victimFunction(arg1:uint, arg2:uint, …, arg80:uint):uint
}
```

Then, the attackers can simply overwrite the function pointer with a gadget that adds to the stack pointer and returns to pivot to ROP.

- Users can check if their installation of Flash is up to date by visiting the Adobe website - the current latest version is 18.0.0.194.
- https://www.adobe.com/software/flash/about/

Microsoft quietly pushes 17 new trusted root certificates

- http://hexatomium.github.io/2015/06/26/ms-very-quietly-adds-18-new-trusted-root-certs/
- RCC (Local Root Certificate Auditing Tool) -- tiny EXE -- Win7 or later.
  - http://www.wilderssecurity.com/threads/rcc-check-your-systems-trusted-root-certificate-store.373819/
  - http://trax.x10.mx/apps.html
  - RCC is a tool that quickly inspects the root certificates trusted by Windows and Mozilla Firefox, and pinpoints possible issues. For instance, it is able to detect funky root certificates installed by Superfish or other unknown threats.
  - RCC does not require admin rights.

- It is compatible with Windows 7 and later (clients) and Windows 2008 and later (servers).
- Please note that RCC currently uses a (non-elevated) PowerShell command to enumerate the system certificate root store.

Google starts listening to everyone without permission (or did they?)

- https://www.privateinternetaccess.com/blog/2015/06/google-chrome-listening-in-to-your-room-shows-the-importance-of-privacy-defense-in-depth/
- chrome://voicesearch/
  - Microphone: Yes
  - Audio Capture Allowed: Yes
- Installed and ENABLED by default?? No, actually.
  - Google: This is not "opt-in default". If you do not explicitly opt in (using the "Enable Ok Google" setting in chrome://settings), then this module will not run.
- But apparently this was not true for Debian users who noticed their webcam light turning on.
- Chromium users were upset: "Black Box" without any provided sourcecode.
- "Ok Google"... then what's said is sent elsewhere...
- Chromium Bug tracking:
  - https://code.google.com/p/chromium/issues/detail?id=491435#c4
  - “Add build flag to disable hotwording.”
  - Hotwording downloads a shared module from the web store containing a NaCl module. There is a desire to build and distribute Chromium without this happening. This change adds an "enable_hotwording" build flag that is enabled by default, but can be disabled at compile time.
  - A build-time flag has been added for anyone that wants to build chromium without hotwording. To disable hotwording, pass "enable_hotwording=0" in your GYP_DEFINES, or "enable_hotwording = false" in your GN config. This will prevent the shared module from being downloaded, and also prevent the option from showing up in settings.
  - May I ask why this extensions is hidden from the extension list at chrome://extensions/ , although the page chrome://voicesearch/ shows it as an enabled extension? I suggest that sensitive functionality intended to process data from the surroundings (sound input,video input, etc.) should be presented in an open and transparent way, with easy to find controls.
  - This weirds me out as well. The whole behaviour of hotword is pretty conspicuous: Opt-in default, downloading a binary blob without notification, extension being hidden, ability to record audio .. I almost fell out of my chair when I saw that. Great strategy to erode trust of any user who is even slightly concerned with security (which, I assume, a lot of chromium users are).

Samsung OEM crapware silently disabling Windows Update

- http://bsodanalysis.blogspot.com/2015/06/samsung-deliberately-disabling-windows.html
- http://arstechnica.co.uk/information-technology/2015/06/samsung-silently-disabling-windows-update-on-some-computers/

- http://venturebeat.com/2015/06/23/samsung-is-actively-disabling-windows-update-on-at-least-some-computers/
- Some Samsung machines contain: Disable_Windowsupdate.exe
- Part of Samsung's SW Update system.
- Samsung's support team "explains":
  - When you are enable Windows updates, it will install the Default Drivers for all the hardware no laptop which may or may not work. For example if there is USB 3.0 on laptop, the ports may not work with the installation of updates. So to prevent this, SW Update tool will prevent the Windows updates.
- Microsoft is unhappy with this news and is "working with Samsung."

Radio can steal Laptop Crypto Keys ... or: Is that Pita Bread spying on you??

- "Tempest in a teapot?... on in a Pita Bread!
- http://www.tau.ac.il/~tromer/radioexp/
- To be presented at the Workshop on Cryptographic Hardware and Embedded Systems, 2015 in September 2015.
- http://www.wired.com/2015/06/radio-bug-can-steal-laptop-crypto-keys-fits-inside-pita/
- Quote: We successfully extracted keys from laptops of various models running GnuPG (popular open source encryption software, implementing the OpenPGP standard), within a few seconds. The attack sends a few carefully-crafted ciphertexts, and when these are decrypted by the target computer, they trigger the occurrence of specially-structured values inside the decryption software. These special values cause observable fluctuations in the electromagnetic field surrounding the laptop, in a way that depends on the pattern of key bits (specifically, the key-bits window in the exponentiation routine). The secret key can be deduced from these fluctuations, through signal processing and cryptanalysis.
- Refinement beyond Pita Bread:
  - Consumer radio attack. Despite its low price and compact size, assembly of the Pita device still requires the purchase of an SDR device. As discussed, the leakage signal is modulated around a carrier circa 1.7 MHz, located in the range of the commercial AM radio frequency band. We managed to use a plain consumer-grade radio receiver to acquire the desired signal, replacing the magnetic probe and SDR receiver. We then recorded the signal by connecting it to the microphone input of an HTC EVO 4G smartphone.

PrivacyTools.io

Mike Liljedahl (@lij1954) Maybe you have seen this privacy site...nice aggregation privacytools.io
https://www.privacytools.io/

- Headline: You are being watched. Private and state-sponsored organizations are monitoring and recording your online activities. privacytools.io provides knowledge and tools to protect your privacy against global mass surveillance.
- Private Search
- Why is it not recommended to choose an US based service?
  - Services based in the United States are not recommended because of the country’s surveillance programs, use of National Security Letters (NSLs) and accompanying gag orders, which forbid the recipient from talking about the request. This

combination allows the government to secretly force companies to grant complete access to customer data and transform the service into a tool of mass surveillance.

- VPN providers with extra layers of privacy - No Affiliates
  - Jurisdiction / Logs? / Encoding / Bitcoin / # of servers / P2P / Cost / Warrant Canary
- Browser Recommendation
  - (Firefox) and the Tor/Firefox browser bundle
- Browser Fingerprint - Is your browser configuration unique?
- Excellent Firefox Privacy Addons
  - Disconnect
  - uBlock Origin
  - Fingerprint spoofer
  - Cookie Deletion
  - HTTPS Everywhere
  - NoScript
- Firefox: Privacy Related "about:config" Tweaks
- Privacy-Conscious Email Providers - No Affiliates
  - Outside the US and supporting SMTP TLS
  - Where, Much much storage, Free? / Cost / Bitcoin / Encryption
- Email Clients
- Email Alternatives
- Encrypted Instant Messenger
- Encrypted Video & Voice Messenger
- Encrypted Cloud Storage Services
- Self-Hosted Cloud Server Software
- Secure File Sync Software
- Password Manager Software
- File Encryption Software
- Decentralized Social Networks
- Domain Name System (DNS)
- PC Operating Systems
- Live CD Operating Systems
- Mobile Operating Systems
- Open Source Router Firmware

- Participate with suggestions and constructive criticism
  - **Talk to us please.** Join our subreddit and start a discussion. This is a community project and we're aiming to deliver the best information available for a better privacy. We are also using /r/privacy and /r/VPN. Thank you for participating.

Major internet providers slowing traffic speeds for thousands across US
http://www.measurementlab.net/blog/interconnection_and_measurement_update
http://www.theguardian.com/technology/2015/jun/22/major-internet-providers-slowing-traffic-speeds

- <Quoting The Guardian> In Atlanta, for example, Comcast provided hourly median download speeds over a CDN called GTT of 21.4 megabits per second at 7pm throughout the month of May. AT&T provided speeds over the same network of ? of a megabit per second. When a network sends more than twice the traffic it receives, that network is required by AT&T to pay for the privilege. When quizzed about slow speeds on GTT, AT&T told Ars Technica earlier this year that it wouldn’t upgrade capacity to a CDN that saw that much outgoing traffic until it saw some money from that network (as distinct from the money it sees from consumers).

Should we trust NoScript?

- Matthew Bryant
- http://thehackerblog.com/the-noscript-misnomer-why-should-i-trust-vjs-zendcdn-net/
- NoScript comes with a LARGE bunch of pre-trusted domains.
- "zendcdn.net" was ON the trust list... but had expired.
- <Matthew> I contacted Giorgio Maone about the vulnerability and the response time was incredibly quick. Within hours he had a patch out on his site and less then two days later the patch was pushed to all NoScript users. This is by far some of the fastest response and patch times I’ve ever seen – so hats off to him for that! Please note: This stray domain is no longer in the default whitelist for NoScript users.

Master Password

- https://ssl.masterpasswordapp.com/
- iPHone / iPad / Mac / Desktop (Java) / Android (Beta) / Web (Beta)
- https://itunes.apple.com/app/id510296984
- Your Full Name
- Your ONE Master password
- Integer to allow per-domain variations
- These deterministically key a hash of the domain name to produce high-quality passwords.

Google Contributor:

- https://www.google.com/contributor/welcome/
- $2, $5, $10

Miscellany:

The World's "Leap Second"

- 11:59:60! Huh???
- 5pm PDT / 8pm EDT
- Due to the Earth's slowing rotation, we have to pause the clocks for a second.
- (Don't ya just hate it when the Earth's rotation slows down?)
- Ars Technica reports:
  - In June 2012, when the last leap second was applied, reddit crashed, Gawker went down, lots of Linux servers fell over, and Australian airline Qantas had some

computer problems that caused up to 50 delayed flights.
- Google is choose to "smear" the second across all of today.

Mr. Robot was so popular… it was renewed before the 1st episode officially aired.

"Halt and Catch Fire" season #2 is fun if you like the characters.

SpinRite:

Discuss SpinRite's partial sector recovery technology when full recovery is impossible.

Tor's AsTORria Client

Quick refresher on Tor -- The Onion Router
The underlying problem is that nothing about the way the Internet was designed provides a strong guarantee of privacy. It was just never designed with that in mind. The designers were just struggling to make it work at all!... and back then it was interconnecting a few university and government sites.

Traffic Correlation Attacks.
The Tor network has grown from 33 nodes to over 6,000!

http://www.dailydot.com/politics/tor-astoria-timing-attack-client/
http://arxiv.org/pdf/1505.05173.pdf

"Measuring and mitigating AS-level adversaries against Tor"
<quote> The popularity of Tor as an anonymity system has made it a popular target for a variety of attacks including blocking, denial of service, and traffic correlation attacks. In this paper, we focus on traffic correlation attacks which are no longer solely in the realm of academic research with recent revelations about the NSA and GCHQ actively working to implement them in practice.

When an Entry and Exit node are within the same AS (autonomous system), traffic correlation attacks can deanonymize Tor users very quickly.

Remember!... packets coming IN and going OUT have NO Tor protection

How bad is standard Tor today?

- Up to 58% of circuits constructed by the current Tor client are vulnerable to network-level attackers.
-
- Up to 43% of all sites in the local Alexa Top 500 of Brazil, China, Germany, Spain, France, England, Iran, Italy, Russia, and the United States had main content that was not reached via a safe path i.e., a path that was free from network-level attackers.
-

- Connections from China were found to be most vulnerable to network-level attackers with up to 85.7% of all Tor circuits and 78% of all main content requests to sites in the local Alexa Top 500 being vulnerable to colluding network-level attackers.
-
- For up to 8% of requests generated within China, there were no network-level attacker free circuits that could have been built { i.e., it was impossible to construct a safe circuit to serve 8% of our generated requests, regardless of the relay selection algorithm used.

Fundamentally,

- Astoria considers the history of node performance and requires nodes to "earn" trust over time.
- The Tor client was modified to perform offline IP to ASN mapping using a database downloaded from APNIC for every incoming request. Since the entire database (9 MB) is downloaded, the client does not reveal its intended destination to any lookup services.
- Astoria then uses IP-to-AS mapping to deliberately route BETWEEN AS's.

Usability of Astoria:

From our evaluation of Astoria, it is clear that the performance-security trade-off is favorable only in its higher security configurations. At high security configurations, Astoria is able to perform good load balancing, achieve reasonable throughput, avoid asymmetric colluding attackers whenever possible, and even handle situations where safe circuits are not possible.

However, at lower security configurations, the performance offered by Tor is clearly better, and its security, only slightly worse. Therefore, Astoria is a usable substitute for the vanilla Tor client only in scenarios where security is a high priority.