Security Now! #501 - 03-31-15

Q&A #209

This week on Security Now!

- The ongoing GitHub / GreatFire.org DDoS attack.
- A bad vulnerability discovered in Hotel / Convention center / Visitor routers.
- What a detailed analysis of 10 million passwords reveals.
- 10 great questions. comments, and thoughts from our terrific audience.

Security News

GitHub DDoS attack

- On March 27 The following message was posted on the official GitHub blog:
  We are currently experiencing the largest DDoS (distributed denial of service) attack in github.com's history. The attack began around 2AM UTC on Thursday, March 26, and involves a wide combination of attack vectors. These include every vector we've seen in previous attacks as well as some sophisticated new techniques that use the web browsers of unsuspecting, uninvolved people to flood github.com with high levels of traffic. Based on reports we've received, we believe the intent of this attack is to convince us to remove a specific class of content.

- How it works:
  - Millions of global internet users, visiting thousands of websites hosted inside and outside China, randomly receive malicious code used to launch an attack against GreatFire.org's websites, hosted by Amazon's cloud services.
  - Baidu's Analytics code (h.js) was one of the files replaced by malicious code which launches the attacks. Baidu Analytics, similar to Google Analytics, is used by thousands of websites. Any visitor to any website using Baidu Analytics or other Baidu resources would have been exposed to the malicious code.
  - That malicious code is sent to any browser globally without distinguishing that user's geographical location. Chinese authorities did not just launch this attack using Chinese internet users - they compromised internet users and websites everywhere in the world.
  - The tampering takes places someplace between when the traffic enters China and when it hits Baidu's servers. This is consistent with previous malicious actions and points to the Cyberspace Administration of China (CAC) being directly involved in these attacks.

- The attack:
  - (Was generating 2.6 BILLION requests per hour -- an increase of x2500.)
  - A user is browsing the Internet from outside China.
  - A website the user visits loads JavaScript from a server in China, for example the Badiu Analytics script that often is used by web admins to track visitor statistics (much like Google Analytics).
  - The web browser's request for the Baidu javascript is detected by the Chinese passive infrastructure as it enters China.
  - The requested JavaScript is replaced on-the-fly with malicious JavaScript that tells the user's browser to continuously reload two specific pages on GitHub.com.

- The two targeted URLs are:
  - github.com/greatfire
  - github.com/cn-nytimes

- These are mirror sites for GreatFire.org and the Chinese New York Times. GreatFire and NYT both use GitHub to circumvent the online censorship performed by the Great Firewall of China (GFW).

- Good technical analysis:
  - http://www.netresec.com/?page=Blog&month=2015-03&post=China%27s-Man-on-the-Side-Attack-on-GitHub
  - https://drive.google.com/file/d/0ByrxblDXR_yqeUNZYU5WcjFCbXM/view?pli=1
  - https://nakedsecurity.sophos.com/2015/03/20/greatfire-org-faces-daily-30000-bill-from-ddos-attack/

- Greatfire.org:
  - <quote> Because of the number of requests we are receiving, our bandwidth costs have shot up to US$30,000 per day. Amazon, which is the service we are using, has not yet confirmed whether they will forgo this.

Common Hotel WiFi router very insecure:

- InnGate routers by ANTlabs of Singapore used in US, European and everywhere else.
- Unauthenticated Rsync Daemon running on TCP 873.
- The instance of rsync included with the InnGate firmware is incorrectly configured to allow the entire filesystem to be read/write without authentication. A remote unauthenticated attacker may read or modify any file on the device's filesystem.
- Attackers gain direct access to the root file system.
- 277 Internet-accessible devices in 29 countries.
    - More than 100 quickly found throughout the U.S.

- http://blog.cylance.com/spear-team-cve-2015-0932
    - The severity of this issue is escalated by how little sophistication is required for an attacker to exploit it.

    - An attacker exploiting the vulnerability would have the access to launch attacks against guests on the affected hotel's WiFi. Targets could be infected with malware using any method from modifying files being downloaded by the victim or by directly launching attacks against the now accessible systems. Given the level of access that this vulnerability offers to attackers, there is seemingly no limit to what they could do.

      Let's assume an attacker has compromised an InnGate device at a hotel with this vulnerability, and has obtained shell access via SSH and an account they created for themselves with root access. The attacker could then simply run tcpdump, which is present on these devices, to dump all network traffic going through them. This would allow an unsophisticated attacker to gather any plaintext communication sent through the gateway of the affected hotel, convention center or data center.

      A slightly more sophisticated attacker could use a tool such as SSLStrip to attempt to downgrade the transport layer encryption to increase the amount of plaintext credentials gathered. This attack gives the threat actor significant leverage over their targets including making OpenSSL vulnerabilities easier to exploit.

A look at 10 million passwords

- http://wpengine.com/unmasked/
- Fabulous analysis

Miscellany:

"Active SETI" -- Proactively sending out a signal ??

SpinRite:

Filipe R in Portugal
Subject: Q&A/SpinRite: Running SR on brand new drives

Hello Steve. Thanks for Security Now.
Here's a quick question: Do you recommend running SpinRite on brand new HDD (or SSD) drives? What level would be adequate to find a possible problem with new drives?
Cheers!