Security Newsletter

10 March 2017

What WikiLeaks' massive CIA Leak tells us about cybersecurity

This week, WikiLeaks returned with a further installment dubbed “Vault 7/Year Zero” that exposes the first cache of 7,818 partly redacted web pages and 943 attachments that make up some of the CIA’s most precious software riddles.

Year Zero introduces the scope and direction of the CIA’s global covert hacking program, its malware arsenal and dozens of zero day weaponized exploits against a wide range of US and European company products, include Apple’s iPhone, Google’s Android and Microsoft’s Windows and even Samsung TVs, which are turned into covert microphones.

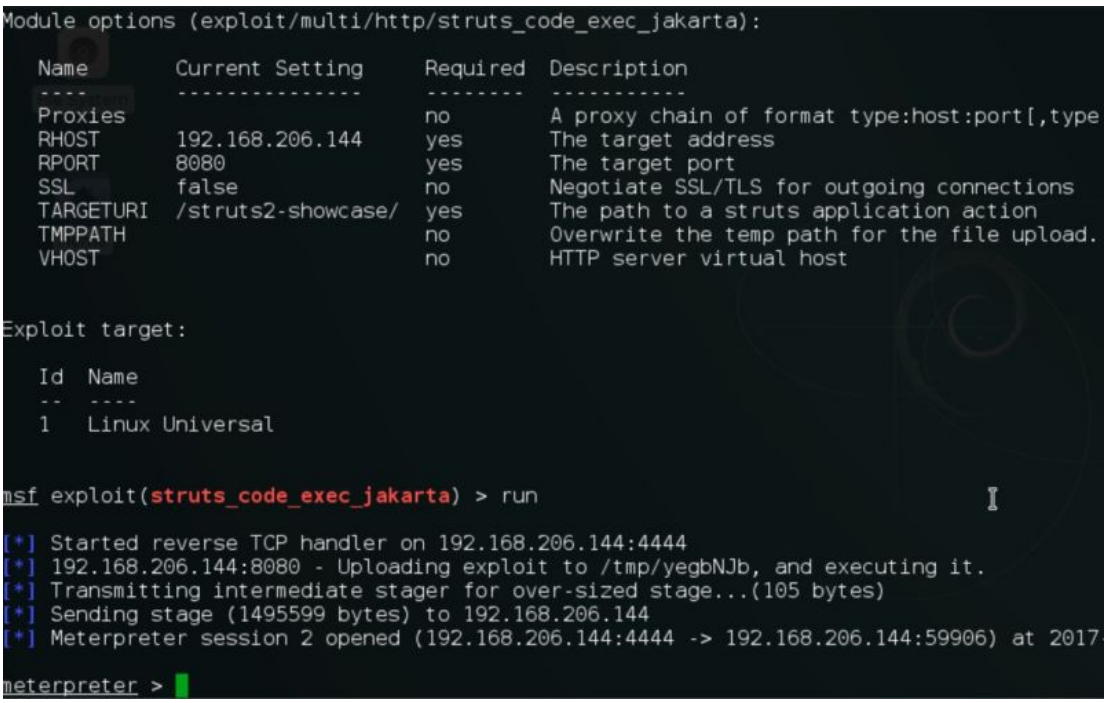
While a lot of its content won't surprise most people working in cybersecurity, these kind of leak confirm some important facts:

- Secure messaging app doing end-to-end encryption look to be robust enough so that even the CIA does not even try to break the encryption. What they do is that they break into the system hosting the app and intercept the messages before it gets encrypted.
- The CIA routinely put false flags into their exploits so that people analysing it think it comes from other countries.
- While a lot of those operations are highly technical, a lot of them still make an extensive use of social engineering techniques to get into the system and inject the malwares. Security awareness among employees is still a key cybersecurity protection.
- Their documentation explaining how to evade most Antivirus detections shows how those products are just one layer of our security. They are necessary, but they don't suffice.
- Those documents seemed to have leaked from some of the many contractors the CIA used over the years. They have been shared internally before one of them decided to send it to Wikileaks. That shows how important it is to manage third parties effectively.

Read More

Even More

Hackers exploit Apache Struts vulnerability to compromise corporate web servers, patch now!



Apache Struts is an open-source web development framework for Java web applications. Security experts today urged enterprises using Apache Struts2 for Web applications to upgrade to either versions 2.3.32 or 2.5.10.1 as soon as possible after researchers from Cisco Talos disclosed an easily exploitable bug in all other versions of the open-source framework.

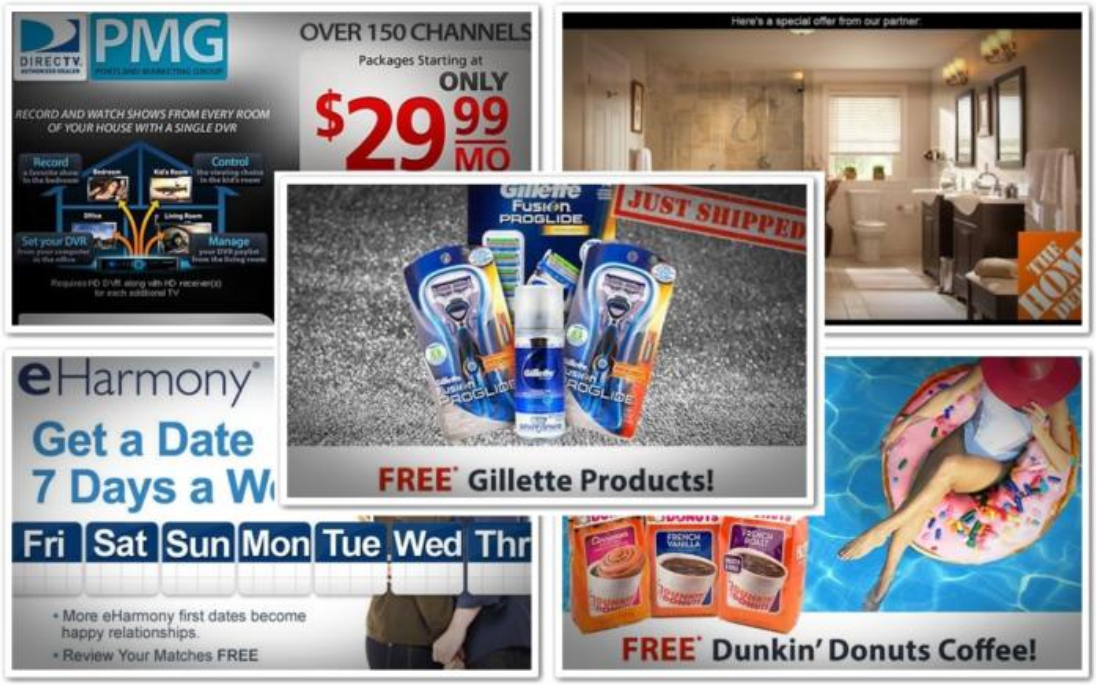
It's widely used to build corporate websites. Exploits for the flaw are already available in the wild and attackers are using them to actively look for and target vulnerable Web servers. Most of the attacks appear to be taking advantage of a proof-of-concept exploit that was released publicly.

The remotely executable flaw exists in something called the Jakarta Multipart parser in Struts. It allows attackers to inject malicious commands into certain HTTP requests, which are then executed by the Web server. **What makes the vulnerability especially dangerous is that it allows attackers unauthenticated remote access to insert malicious commands and payloads of their choice into HTTP requests.**

Read More

For the brave

Spammers expose their entire operation through backups mistakenly disclosed to the public



On Monday, Salted Hash covered the story of how faulty Rsync backups exposed River City Media (RCM), an organization known to Spamhaus. The data breach exposed 1.34 billion email addresses used by RCM to send offers, or emails that most of the public would consider spam. Some of those email records included personal information, compounding the issue.

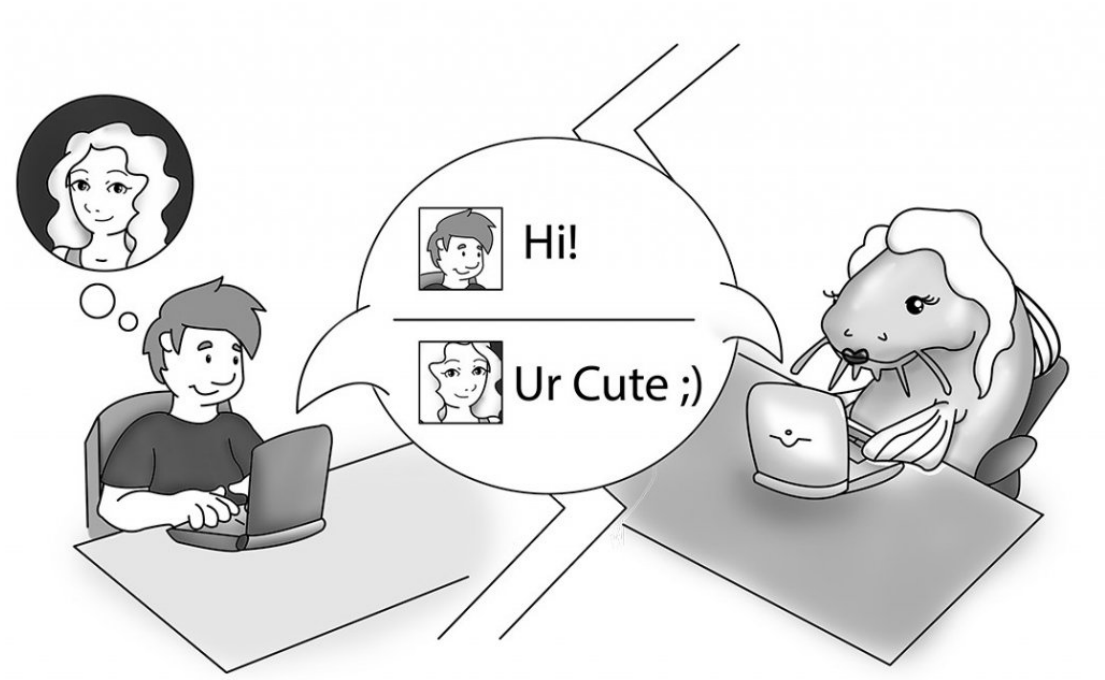
This leak allows us to discover how spammers operate:

- How do they collect emails
- How do they maintain this list to check who receives their spam, who opens it, who clicks on links and who actually gets scammed
- How they cheat email providers into not flagging their messages as spam
- How do they recover from their domain name being flagged as spammer

Read More

Follow Up

How to spot phishing and scams on social media

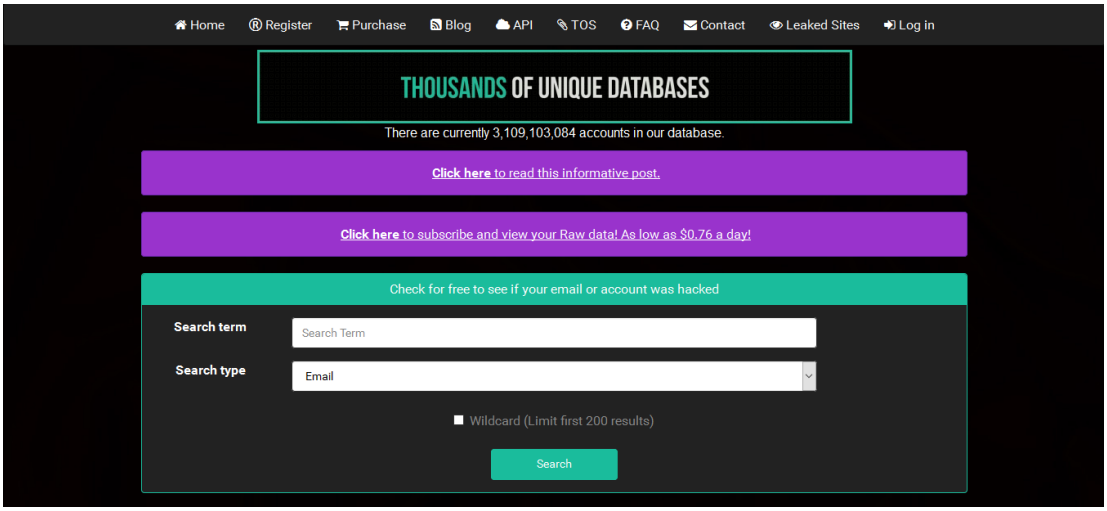


We spend a lot of time on social media, and for good reason. It has collapsed the communication distance between us and other people, bringing us closer. However, this category of “other people” includes persons you would never want to meet: scammers, blackhat hackers, and other such online criminals.

In this article, you will learn how you can identify a fake online profile, and avoid any of their scamming attempts. You will also learn about social media specific phishing techniques, such as Catphishing and Like-farming.

Read More

How hackers find your reused passwords: LeakedSource Clone Pops Up on Russian Domain



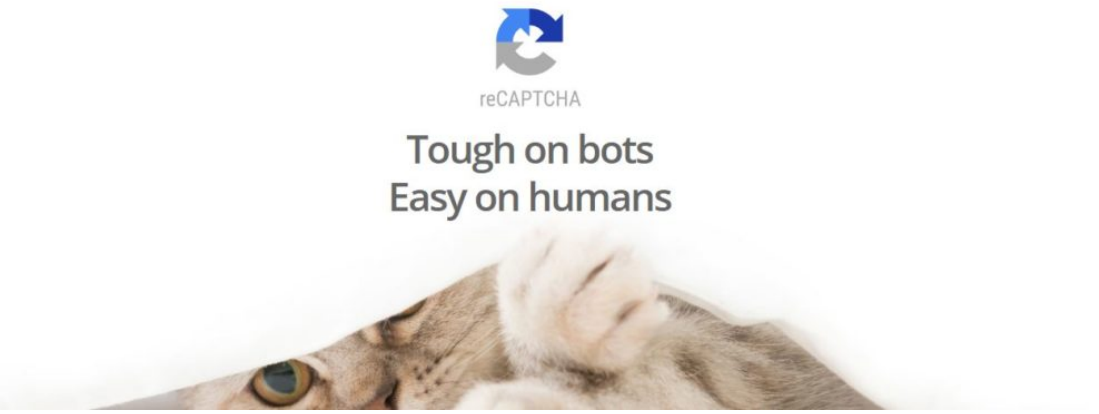
The original LeakedSource launched in late 2015, and it became known worldwide after it disclosed mega data breaches affecting services such as LinkedIn, MySpace, Dropbox, and many others. The original LeakedSource went down on January 25, this new website, currently hosted at LeakedSource.ru, claims to be a continuation of the official LeakedSource service.

At the same time, the site also became extremely popular with amateur hackers because, for a small fee, it allowed anyone to view cracked passwords from user accounts included in these breaches.

While it is very likely that this version is a scam, real copycats will eventually show up and take back this business. That's why it's very important to use strong, UNIQUE passwords on each service.

Read More

Google finally releases it's new, invisible reCAPTCHA



Google's reCAPTCHA is the leading CAPTCHA service (that's "Completely Automated Public Turing test to tell Computers and Humans Apart") on the Web. You've probably seen CAPTCHAs a million times on sign-up pages across the Web; to separate humans from spam bots, a challenge will pop up asking you to decipher a picture of words or numbers, pick out objects in a grid of pictures, or just click a checkbox.

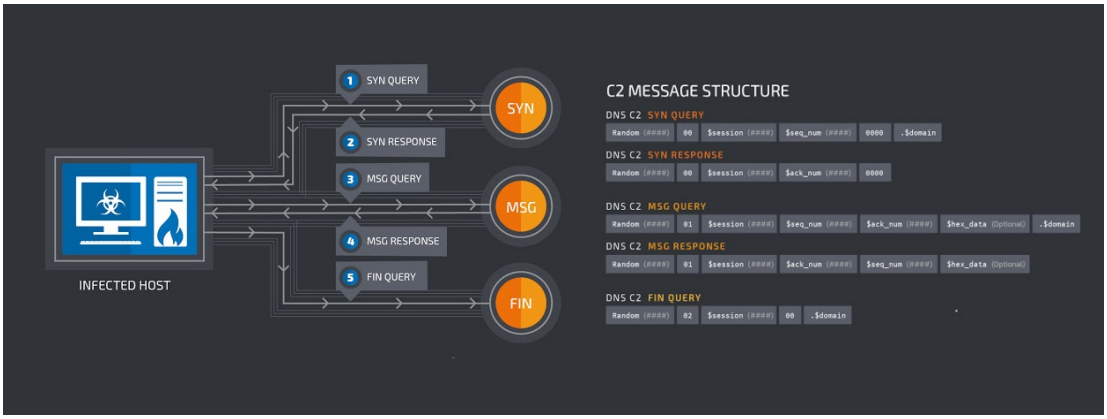
Now, though, **you're going to be seeing CAPTCHAs less and less, not because Google is getting rid of them but because Google is making them invisible.** It works invisibly in the background, somehow, to identify bots from humans. Google doesn't go into much detail on how it works, only saying that the system uses "a combination of machine learning and advanced risk analysis that adapts to new and emerging threats." More detailed information on how the system works would probably also help bot-makers crack it, so don't expect details to pop up any time soon.

To use it, just click on Get reCaptcha and select "Invisible reCAPTCHA".

Read More

Dev HowTo

Malware Retrieves PowerShell Scripts from DNS Records



Malware researchers have come across a new Remote Access Trojan (RAT) that uses a novel technique to evade detection on corporate networks by fetching malicious PowerShell commands stored inside a domain's DNS TXT records.

Most of today's enterprise and home security products monitor HTTP/S traffic primarily. Cisco says that because the malware used DNS queries to hide its activity, unless the target company was monitoring DNS traffic, the infection would have never been picked up.

Read More

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with over 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and as an innovation driven company that builds on trust.