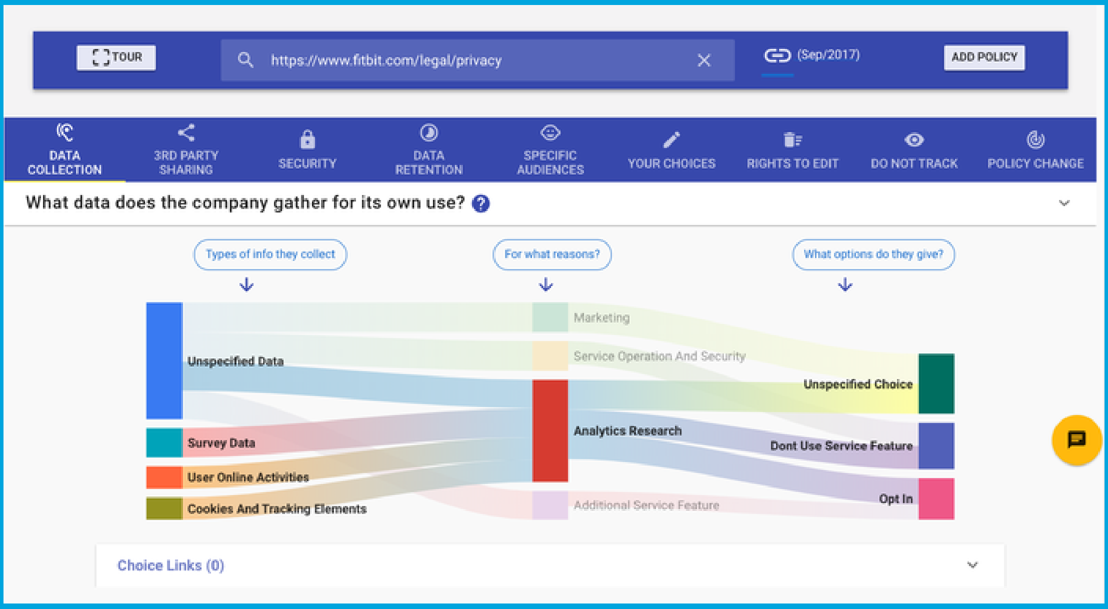
kindred

Security Newsletter

26 February 2018

Subscribe to this newsletter

Pribot Polisis: An A.I. that reads privacy policies so that you don't have to



You don't read privacy policies. And of course, that's because they're not actually written for you, or any of the other billions of people who click to agree to their inscrutable legalese. Instead, like bad poetry and teenagers' diaries, those millions upon millions of words are produced for the benefit of their authors, not readers — the lawyers who wrote those get - out clauses to protect their Silicon Valley employers.

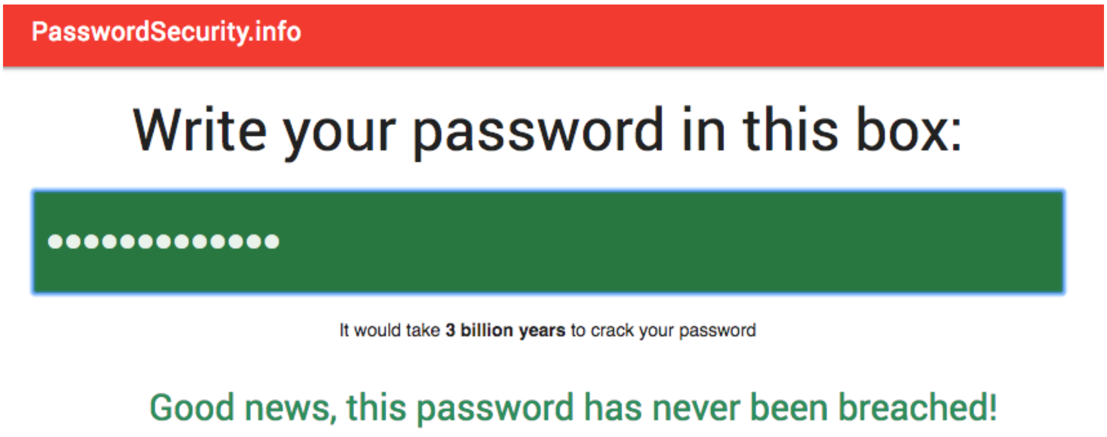
But one group of academics has proposed a way to make those virtually illegible privacy policies into the actual tool of consumer protection they pretend to be: an artificial intelligence that's fluent in fine print. Today, researchers at Switzerland's Federal Institute of Technology at Lausanne (EPFL), the University of Wisconsin and the University of Michigan announced the release of Polisis—short for "privacy policy analysis"—a new website and browser extension that uses their machine-learning-trained app to automatically read and make sense of any online service's privacy policy, so you don't have to.

The researchers' legalese-interpretation apps do still have some kinks to work out. They see their AI engine in part as the groundwork for future tools. They suggest that future apps could use their trained AI to automatically flag data practices that a user asks to be warned about, or to automate comparisons between different services' policies that rank how aggressively each one siphons up and share your sensitive data.

Read More

Pribot Polisis

Troy Hunt Just Launched "Pwned Passwords" V2 With Half a Billion Passwords for Download



PasswordSecurity.info

Write your password in this box:

●●●●●●●●●●●●●

It would take **3 billion years** to crack your password

Good news, this password has never been breached!

Last August, Troy Hunt launched a little feature within Have I Been Pwned (HIBP) called Pwned Passwords. This was a list of 320 million passwords from a range of different data breaches which organisations could use to better protect their own systems. V2 just got released and there's Now 501,636,842 Pwned Passwords, but the biggest improvement is elsewhere. He got a lot of feedback from V1 along the lines of "simply blocking 320M passwords is a usability nightmare". Blocking half a billion, even more so.

In V2, every single password has a count next to it. What this means is that next to "abc123" you'll see 2,670,319 - that's how many times it appeared in my data sources. Having visibility to the prevalence means, for example, you might outright block every password that's appeared 100 times or more and force the user to choose another one (there are 1,858,690 of those in the data set), strongly recommend they choose a different password where it's appeared between 20 and 99 times (there's a further 9,985,150 of those), and merely flag the record if it's in the source data less than 20 times. Of course, the password "acl567" may well be deemed too weak by the requirements of the site even without Pwned Passwords so this is by no means the only test a site should apply.

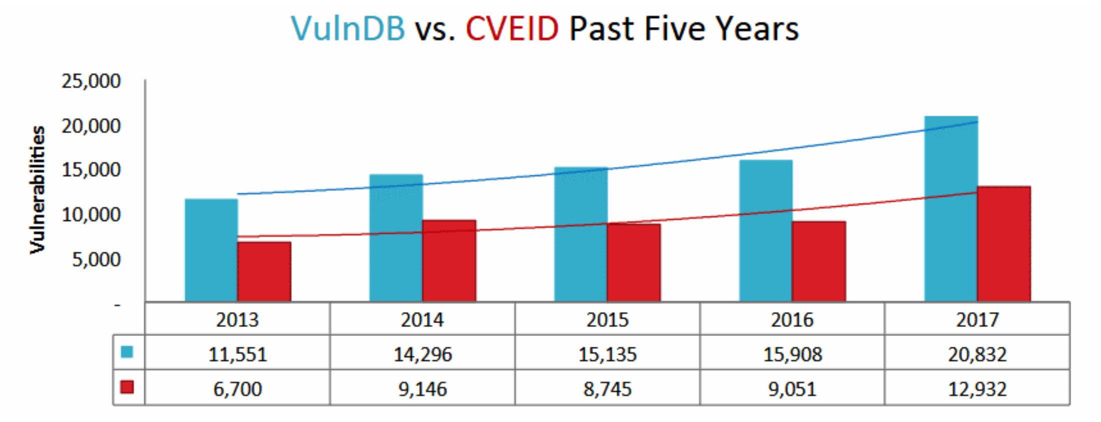
Please note that as per NIST's Special Publication 800-63B, passwords must be checked against blacklists of known breached passwords or weak passwords. The size of the blacklist is critical as a blacklist too big will lead to a very poor user experience and a blacklist too small will not be effective.

Read More

Validating leaked passwords with k-anonymity

How developers got password security wrong

Nearly 8,000 Security Flaws Did Not Receive a CVE ID in 2017



	2013	2014	2015	2016	2017
🟦	11,551	14,296	15,135	15,908	20,832
🟥	6,700	9,146	8,745	9,051	12,932

A record-breaking number of 20,832 vulnerabilities have been discovered in 2017 but only 12,932 of these received an official CVE identifier last year, a Risk Based Security (RBS) report reveals. This means that 7,900 security bugs remained without a CVE-2017-XXXXX number, and were left off the databases of many security scanners because of it.

Furthermore, this also means that many security bugs remained buried on forums and personal blogs —places where attackers might have the time to scout, but where many IT security departments will never look. The reasons are plenty, but one of them is the explosion of security bugs in IoT devices, which has made it harder for Mitre and NVD staffs to keep up with all the bugs.

Furthermore, almost 7,000 2917 vulnerabilities received a RESERVED CVE status, with no public details available, despite 1,342 of them having a public disclosure. "This seems to indicate that MITRE is more focused on assigning and increasing the number of IDs, and not ensuring the quality of data," RBS experts concluded.

Read More

Hacker Group Makes $3 Million by Installing Monero Miners on Jenkins Servers

A hacker group has made over $3 million by breaking into Jenkins servers and installing malware that mines the Monero cryptocurrency.

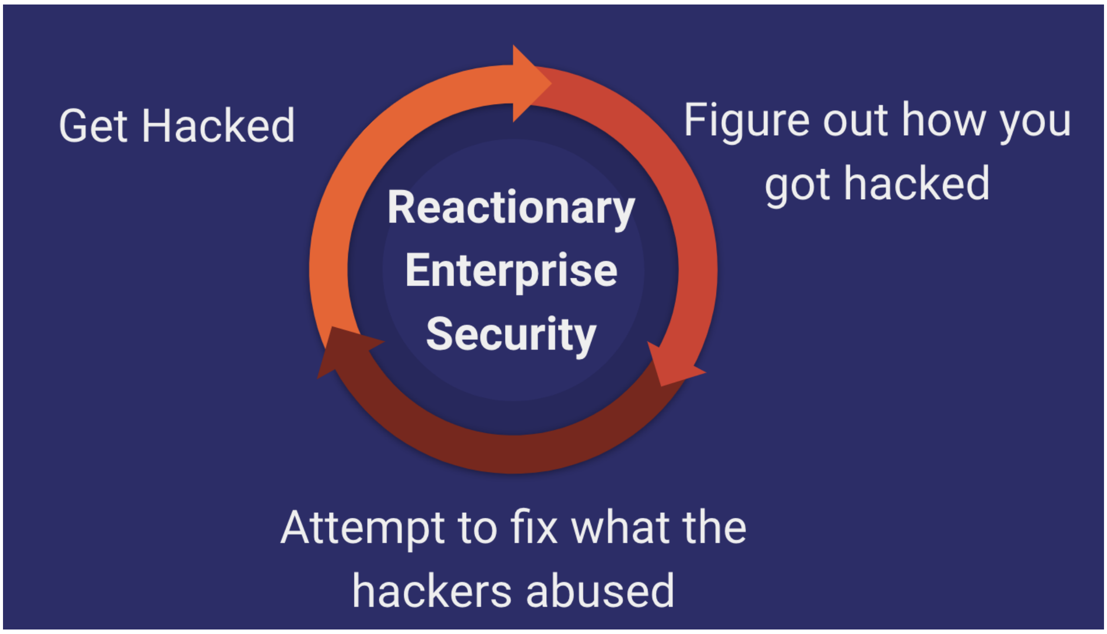
Hackers are targeting Jenkins, a continuous integration/deployment web application built in Java that allows dev teams to run automated tests and execute various operations based on test results, including deploying new code to production servers. Because of this, Jenkins servers are extremely popular with both freelance web developers, but also with large enterprises.

Attackers were leveraging CVE-2017-1000353, a vulnerability in the Jenkins Java deserialization implementation that allows attackers to run malicious code remotely without needing to authenticate first. The attackers have been active for months. Researchers say the group appears to have compromised mostly Jenkins instances running on Windows operating systems. Attackers aren't the only ones who've noticed the large number of Jenkins servers available online. In mid-January, security researcher Mikail Tunç published research highlighting that there were over 25,000 Jenkins servers left exposed to Internet connections at the time of his research.

Read More

Even More

Introducing the Adversary Resilience Methodology


Get Hacked
Figure out how you got hacked
Reactionary Enterprise Security
Attempt to fix what the hackers abused

In this post, the authors illustrate some of the current challenges enterprises face when trying to secure their Active Directory environment. Then, they detail a new methodology that uses the untapped power of BloodHound’s attack graph to efficiently achieve an Active Directory that is highly resilient against the most attacks most likely to be discovered and executed by an adversary.

Even in a perfect world, where all remediations were applied, only one attack path of many was stopped. The techniques and procedures used change, as vendors and defenders add security measures, but attackers continue to succeed. For many reasons, enterprises get stuck in this endless loop of responding to attacker behaviors and capabilities, hardly ever having time to try and get a leg up on adversaries.

Read More

Botched npm Update Crashes Linux Systems, Forces Users to Reinstall

A bug in npm (Node Package Manager), the most widely used JavaScript package manager, will change ownership of crucial Linux system folders, such as /etc, /usr, /boot.

Changing ownership of these files either crashes the system, various local apps, or prevents the system from booting, according to reports from users who installed npm v5.7.0. —the buggy npm update. Users who installed this update —mostly developers and software engineers— will likely have to reinstall their system from scratch or restore from a previous system image.

The bug was first reported a week ago but was left without an answer from npm developers. Users filed a new bug report after last night's release, and the npm team has released npm v5.7.1, a version that removes the buggy code.

Read More

Cutting room floor

- Learn How to Turn On 2FA Now!
- Windows 10 null character flaw keeps malware hidden from security scanning tools
- Microsoft Fixes Windows 10 Privilege Escalation bug But forgot an edge case
- Amazon AWS Servers Might Soon Be Held for Ransom, Similar to MongoDB
- uTorrent Client Affected by Some Pretty Severe Security Flaws
- Hackers are selling legitimate code-signing certificates to evade malware detection
- North Korean Reaper (APT 37) uses zero-day vulnerabilities to spy on governments
- Meet Coldroot, a nasty Mac trojan that went undetected for years
- Intel rolls out Spectre updates for 7th and 8th-gen Core chips
- Chromebook update boosts security, but wipes all data in the process
- Cryptojacking Scripts Could Soon Invade Your Word Documents
- Anchor CMS Sites May Be Spewing Their Database Passwords
- NIST Working on Global IoT Cybersecurity Standards
- Life-saving Pacemakers, Defibrillators Can Be Hacked and Turned Off
- Google drops new Edge zero-day as Microsoft misses 90-day deadline
- AWS Single Sign-On Now Enables Command Line Interface Access for AWS Accounts Using Corporate Credentials
- Center for Internet Security (CIS) released CIS Top20 Controls version 7

#Tech and #Tools

- CSS Keylogger
- Assessing the Effectiveness of Hash-based Application Whitelisting Blacklist Rules
- Tearing Apart the Undetected (OSX)Coldroot RAT
- Check if you’re public on Shodan
- Docker Layer 2 ICC Bug
- GitLeaks: Check git repos for secrets and keys
- Secure Coding: Understanding input validation

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.

You can access the previous newsletters at https://news.infosecgur.us