BIZ & IT —

Why passwords have never been weaker—and crackers have never been stronger

Thanks to real-world data, the keys to your digital kingdom are under assault.

DAN GOODIN - 8/20/2012, 9:00 PM

Aurich Lawson / Thinkstock

In late 2010, Sean Brooks received three e-mails over a span of 30 hours warning that his accounts on LinkedIn, Battle.net, and other popular websites were at risk. He was tempted to dismiss them as hoaxes—until he noticed they included specifics that weren't typical of mass-produced phishing scams. The e-mails said that his login credentials for various Gawker websites had been exposed by hackers who rooted the sites' servers, then bragged about it online; if Brooks used the same e-mail and password for other accounts, they would be compromised too.

The warnings Brooks and millions of other people received that December weren't fabrications. Within hours of anonymous hackers penetrating Gawker servers and exposing cryptographically protected passwords for 1.3 million of its users, botnets were cracking the passwords and using them to commandeer Twitter accounts and send spam. Over the next few days, the sites advising or requiring their users to change passwords expanded to include Twitter, Amazon, and Yahoo.

"The danger of weak password habits is becoming increasingly well-recognized," said Brooks, who at the time blogged about the warnings as the Program Associate for the Center for Democracy and Technology. The warnings, he told me, "show [that] these companies understand how a security breach outside their systems can create a vulnerability within their networks."

The ancient art of password cracking has advanced further in the past five years than it did in the previous several decades combined. At the same time, the dangerous practice of password reuse has surged. The result: security provided by the average password in 2012 has never been weaker.

A new world

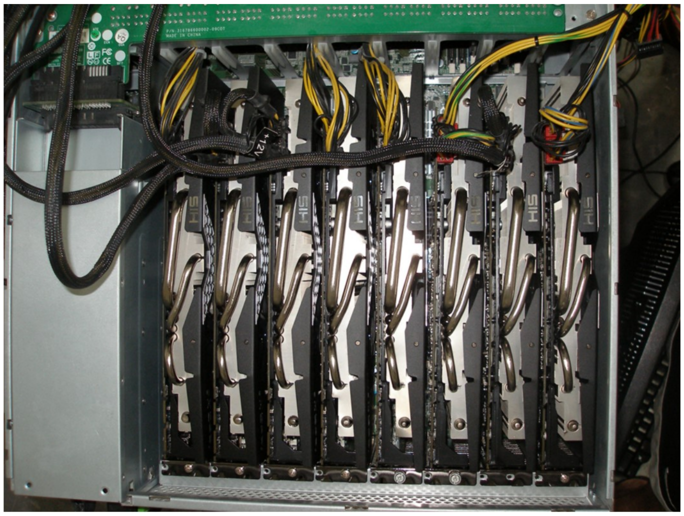
The average Web user maintains 25 separate accounts but uses just 6.5 passwords to protect them, according to a landmark study (PDF) from 2007. As the Gawker breach demonstrated, such password reuse, combined with the frequent use of e-mail addresses as user names, means that once hackers have plucked login credentials from one site, they often have the means to compromise dozens of other accounts, too.

Newer hardware and modern techniques have also helped to contribute to the rise in password cracking. Now used increasingly for computing, graphics processors allow password-cracking programs to work thousands of times faster than they did just a decade ago on similarly priced PCs that used traditional CPUs alone. A PC running a single AMD Radeon HD7970 GPU, for instance, can try on average an astounding 8.2 billion password combinations each second, depending on the algorithm used to scramble them. Only a decade ago, such speeds were possible only when using pricey supercomputers.

The advances don't stop there. PCs equipped with two or more $500 GPUs can achieve speeds two, three, or more times faster, and free password cracking programs such as oclHashcat-plus will run on many of them with little or no tinkering. Hackers running such gear also work in tandem in online forums, which allow them to pool resources and know-how to crack lists of 100,000 or more passwords in just hours.

Most importantly, a series of leaks over the past few years containing more than 100 million real-world passwords have provided crackers with important new insights about how people in different walks of life choose passwords on different sites or in different settings. The ever-growing list of leaked passwords allows programmers to write rules that make cracking algorithms faster and more accurate; password attacks have become cut-and-paste exercises that even script kiddies can perform with ease.

"It has been night and day, the amount of improvement," said Rick Redman, a penetration tester for security consultants KoreLogic and organizer of the Crack Me If You Can password contest at the past three Defcon hacker conferences. "It's been an exciting year for password crackers because of the amount of data. Cracking 16-character passwords is something I could not do four or five years ago, and it's not because I have more computers now."



d3ad0ne

Enlarge / This $12,000 computer, dubbed Project Erebus v2.5 by creator d3ad0ne, contains eight AMD Radeon HD7970 GPU cards. Running version 0.10 of oclHashcat-lite, it requires just 12 hours to brute force the entire keyspace for any eight-character password containing upper- or lower-case letters, digits or symbols. It aided Team Hashcat in winning this year's Crack Me If You Can contest.

At any given time, Redman is likely to be running thousands of cryptographically hashed passwords though a PC containing four of Nvidia's GeForce GTX 480 graphics cards. It's an "older machine," he conceded, but it still gives him the ability to cycle through as many as 6.2 billion combinations every second. He typically uses a dictionary file containing about 26 million words, combined with programming rules that greatly extend its effectiveness by adding numbers, punctuation, and other characters to each list entry. Depending on the job, he sometimes uses a 60 million-strong word list and something known as "rainbow tables," which are described later in this article.

As a penetration tester who gets paid to pierce the defenses of Fortune 500 companies, Redman tries to spot weaknesses before criminal hackers exploit them on his customers' networks. One of the key ways he stays ahead is by downloading hash lists that are dumped almost every day on pastebin.com and other sites to see if any belong to the organizations he is contracted to protect.

Recently, he recovered a 13-character password that he had spent several months trying to crack. To protect the account holder, he declined to reveal the precise combination of characters and instead made up the imaginary passphrase "Sup3rThinkers" (minus the quotation marks) to illustrate his breakthrough. "Sup3rThinkers" follows a number of patterns that have become common: it opens with a common, five-letter word that begins with a capitalized letter and substitutes a 3 for an E, followed by a common, seven-letter word that also begins with a capital letter. While the speed of his system didn't hurt, cracking the password was largely the result of the collective codebreaking expertise developed online over the past few years.

The most important single contribution to cracking knowledge came in late 2009, when an SQL injection attack against online games service RockYou.com exposed 32 million plaintext passwords used by its members to log in to their accounts. The passcodes, which came to 14.3 million once duplicates were removed, were posted online; almost overnight, the unprecedented corpus of real-world credentials changed the way whitehat and blackhat hackers alike cracked passwords.

Page: 1 2 3 4 Next →

READER COMMENTS

SHARE THIS STORY

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

WATCH

Nintendo's Corey Olcsvary plays your...

Nintendo's Corey Olcsvary plays your Super Mario Maker 2 levels

Corey Olcsvary from Nintendo Treehouse joins us to play through a selection of user-generated Super Mario Maker 2 levels. Watch as he talks us through his strategies for clearing each stage and offers his impressions of what works and doesn't with each level's design. Corey then goes behind the scenes to explain the design ideas behind a custom course created by Nintendo Treehouse.

Nintendo's Corey Olcsvary plays your Super Mario Maker 2 levels

Bioware answers unsolved mysteries of the Mass Effect universe

Civilization: It's good to take turns | War Stories

SITREP: DOD Resets Ballistic Missile Interceptor program

More videos

← PREVIOUS STORY

NEXT STORY →

Related Stories

- Leak of >1,700 valid passwords could make the IoT mess much worse
- Anatomy of a hack: How crackers ransack passwords like "qeadzcwrsfxv1331"
- How the Bible and YouTube are fueling the next frontier of password cracking
- Bitcoin-only poker site resets user credentials after 42,000 passwords leak

Today on Ars

Dealmaster: More Black Friday deals are now live, including AirPods for $129 [Update]

MediaTek and Intel team up to bring 5G networking to laptops and PCs

CT scans confirm 17th-century medical mannikins are mostly made of ivory

UN report card: Carbon-emissions cuts are way behind schedule

Hacker's paradise: Louisiana's ransomware disaster far from over

Galaxy S11+ renders show off world's most disorganized camera array

Netflix cancels its *Mystery Science Theater 3000* revival

State ignored worker death to lure Amazon business, report says

STORE
SUBSCRIBE
ABOUT US
RSS FEEDS
VIEW MOBILE SITE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS

NEWSLETTER SIGNUP

Join the Ars Orbital Transmission mailing list to get weekly updates delivered to your inbox.

SIGN ME UP →