Hack Attack

Categoría: articulos / Noticias/News
Autor: editor
Publicado: 25 Jun, 2011 - 08:11 AM

time.com

Thursday, Jun. 23, 2011
Hack Attack
By Bill Saporito

So who would you like to hack today? A bank, a website, a corporation or perhaps a government agency that's rubbing you the wrong way? The hacktivist group LulzSec is taking requests. Or maybe you'd like to get your hands on some stolen credit-card accounts to boost your personal spending level or purchase some malware that will divert a business's payments from its vendors to you. A malware seller called Zeus not only can do that but also provides customer support. Hacking has become a service and entertainment business — and in a quantity and at a quality never before reached.

Hacktivists, pranktivists, idealists and malware coders are oozing past the circa-2000 network-security gates of corporations and governments with ease. Among the biggest hacks was the one that brought down Sony's PlayStation Network. Some fingered the politically motivated group Anonymous, and authorities in Spain have arrested several purported members. But Anonymous has said, Not us.

When Sony announced that it had finally restored service, the gang of merry hacksters called LulzSec began to trample through its websites, including Sony Pictures. LulzSec, which makes a point of pointing out holes in Web security, used a hack called an SQL injection, then tweeted about it: "We accessed EVERYTHING. Why do you put such faith in a company that allows itself to become open to these simple attacks?" It has since broken into gaming companies such as Bethesda Softworks and Minecraft. It used a hack called a distributed-denial-of-service attack to lock up the CIA's website; it accessed account information from Citibank. (See if hackers are getting smarter.)

LulzSec may be the headline hacker, but it's not the most malevolent. The black-hat, criminal side of the practice is booming by adopting a similar approach. Cyberthieves have shifted their focus to social networks. Instead of attacking corporate firewalls head-on, they are breaching corporate sites using social engineering, convincing someone within a company that an e-mail is from a friend or colleague. It's a technique called spear phishing: the idea is to identify vulnerable targets — say, someone in human resources or finance — and, through them, burrow into corporate networks. They are feasting on small and medium-size businesses like wolves on lambs.

There is also a real cyberwar being waged by nations. Reports of cybersecurity incidents from federal

agencies have increased 660% over the past five years, to 41,776 in 2010, according to the Government Accountability Office's information-security-issues director. The networks of the Department of Defense (DOD) are probed millions of times every day. More than 100 foreign intelligence agencies have attempted to penetrate DOD networks or those of military contractors — attacks characterized as APTs, or advanced persistent threats. At least one got into the Pentagon via Lockheed Martin by cracking the RSA security token, the random-number-generating device that many companies use for secure access to computer networks.

To experts, this is just another sign that the older technology that protected IT is passé. "User-named passwords are breakable now. They weren't when they first started," says Bill Conner, CEO of Entrust, an IT-security firm. "Tokens have been around a long time. One lockmaker has now been breached. Even tokens aren't good against some of the new-age cybercrimes." (See whose emails were exposed in a LulzSec hack.)

The New Threat Matrix

It adds up to an entirely different threat matrix bubbling up on the Web. The hacker community that once operated in its dark recesses has broken the surface, embracing social networks and exploiting them to expand in all directions, legal and otherwise. "What we are seeing is beyond a technical improvement," says Dave Jevans, chairman of the Web-security firm IronKey. "They have a social element to bring people together [via the network] to create more sophisticated attacks than we've ever seen. That's what makes it accelerate."

And it's not just Nigerian spammers and post-Soviet computer jocks anymore. In the past quarter, the IT-security company AVG traced hack attacks tied to about 700 -command-and-control servers — servers that take over computers infected by botnets — used by various hackers around the world. "About 30% of the hackers were in the U.S.," says CEO J.R. Smith. "This is a shocking experience to see the data being stolen — medical data, business data. The volume of data being stolen is constantly increasing." So is his business, since the thieves are also expanding into cell phones. Smith says his company blocks 10,000 malicious mobile-app downloads every day.

See the 140 Best Twitter Feeds.

LulzSec and Anonymous have been proving with alarming regularity that the data we've entrusted to corporations and institutions isn't as safe as we'd like. If information privacy wasn't our first concern, it's now in the top slot. Anonymous evolved from the fringy website 4chan, where posters frequently signed in as anonymous, and gained acclaim as the hacking force that attacked MasterCard, Amazon and PayPal for canceling Wiki-Leaks' accounts after WikiLeaks released a trove of U.S. diplomatic cables. LulzSec is thought to be a splinter group of former Anonymous members.

LulzSec's name is a play on the texting abbreviation LOL, as in laugh out loud, which is what LulzSec has been doing at the networks (it claims to do it "for the lulz") that in its view aren't protecting users. Its members are skillful enough to hack into an FBI affiliate site and, according to LulzSec, leak its user base as well, always with a tweet. When an IT-security firm offered $10,000 to anyone who could hack its website, LulzSec did it — and refused the money. (See why a U.K. hacker was charged for an attack claimed by LulzSec.)

But it seems LulzSec might be shedding its Robin Hood persona in favor of more nefarious activity. Recently it announced via Twitter that it is teaming with Anonymous to steal and share data. In announcing Operation Anti-Security (#AntiSec), LulzSec stated plans "to steal and leak any classified government information, including email spools and documentation. Prime targets are banks and other high-ranking establishments."

In a missive it released after its 1,000th tweet, LulzSec explained a bit of its philosophy: "Yes, yes, there's always the argument that releasing everything in full is just as evil, what with accounts being stolen and abused, but welcome to 2011. This is the lulz lizard era, where we do things just because we find it entertaining." In the meantime, counterhackers are vowing to track down LulzSec's membership.

Sony didn't find hacking particularly entertaining when its PlayStation Network was shut down on April 20. For more than a month, Sony had to take the network down, leaving about 100 million players without their fun and no doubt forcing parents to pay more attention to their children, and vice versa, until the company got it going again at the beginning of June — at a cost of $173?million. The PlayStation Network had barely returned to action when LulzSec barreled into many of Sony's more than 10,000 websites worldwide. Yet when Sega's site was hacked by an unknown interloper, LulzSec signaled that it would track down the culprit. (See how LulzSec compromised 1.3 million user accounts.)

LulzSec's beef with Sony — indeed, with just about everybody — is that the company's Internet security isn't good enough, so it must be named and shamed. Within Sony, the reaction was as much frustration as anger. It was not as if PlayStation owners were launching cruise missiles at endangered animals. The PlayStation Network was a community that willingly shared information; it depended upon a certain level of civil behavior. Nonsense, said LulzSec.

The Black Hats Are Winning

In that same release, LulzSec also warned the public about what it wasn't noticing: the everyday hacking of banks, businesses and individuals, incidents that the IT-security experts concede are growing rapidly. Black-hat hackers are adapting social networks to establish an evil ecosystem while exploiting its vulnerabilities to steal data and money. Their tool kit includes social-engineering techniques that dupe you into coughing up passwords. Their malware is getting better: botnets (networks of infected computers) are growing, as are "man in the middle" schemes that redirect your Web traffic.

It's a new plug-and-play environment as hackers specialize, link with other specialists as needed and offer a variety of goods and services. You don't even have to be a hacker to use some of the available products. There's 24/7 customer support. Malware consortiums like Zeus produce botnets that let you invade and infest computer systems. You can obtain specific parts of botnet code that you can customize for your own use to hack individual bank accounts. Need a "mule" to set up an account to transfer stolen money into? That service can be provided too. "There's a whole supply chain here," says AVG's Smith. "The guys who develop it, update, use it, and people who have to get the money. It's hard to find the guy."

See the top 10 Internet blunders.

Not that the cops aren't looking. Zeus suffered a major hit when the U.S. charged 70 people with involvement in the cybercrime ring in September 2010. Its response was to merge with SpyEye, another botnet maker. The point, as with any other merger, is to improve efficiency and profits. The combined Zeus-SpyEye, for example, is making an even more damaging bot called "browser in the middle" that allows thieves to manipulate the data that a user sends to a bank. The bank may see six authorizations for payment when the user thinks she's sending one. When the bank acknowledges the six authorizations, the browser intercepts and shows the user only one.

Hackers have discovered that small and medium-size businesses (SMBs) are far more vulnerable than major corporations. SMBs can't afford the kinds of costly defenses the big guys can erect if they choose. The stakes are higher too. If someone hacks your personal bank account, you'll be made whole. But courts in many states

have ruled that if someone hacks a business account and the bank followed standard security protocols, the business is on the hook for the money. (See "A Small Victory in the Fight Against Cybercrime.)

Hackers haven't forgotten about you either. While the Web has encouraged sharing via Facebook and LinkedIn, those networks have become portholes to problems. Friend the wrong person and go to that unknown friend's recommended website, and you are asking for trouble, buddy. A Facebook bug called Koobface that takes over your account is infecting a million accounts daily, says IronKey's Jevans. As for LinkedIn, he says, "I can make a very authentic-looking LinkedIn invite."

Hackers are also using the data gamed from social-network sites to build credible individual identities with which they can infiltrate corporations and websites. Even if you don't have a Facebook account, someone could create one for you — as happened to the head of Interpol.

The Counterattack

The good guys aren't standing still, of course. The focus now is to disconnect a person's e-mail and browser from the rest of the network with a variety of security layers. Companies are also figuring out new ways to protect themselves from employees who work at home beyond the corporate firewall and from the growing threats via mobile devices, including iPads and other tablet computers. Until then, corporations and government agencies are well advised to keep the doors locked, change the default settings and train employees to be on guard for spear phishing and social engineering. (See a brief history of the computer.)

We think in terms of Moore's law — that computing speed doubles every 18 months. But "hackers are thinking in days," says Entrust's Conner. There are things you can do to help protect yourself: not just changing your passwords but also making them long enough and complex enough to be a meaningful deterrent. But at a more basic level, it's about not oversharing with people you may or may not know and being a little more cautious even with people you think you know. It takes a little of the social out of social networks, but it's safer.

"The main thing is that it's going social. If you look at Lulz, would you believe a hacking group has a p.r. office, a Twitter account and a request line?" asks Jevans. "It's crazy. It's creating a whole new culture of people who feel they are entitled to do it."

That's sort of how LulzSec feels. It has prodded the public for its watching-the-train-wreck attitude toward hacking. But even LulzSec doesn't know how long it can last. British officials recently arrested a hacker who may be part of the group. "We'll continue creating things that are exciting and new until we're brought to justice, which we might well be," says LulzSec. "But you know, we just don't give a living f--- at this point. You'll forget about us in three months' time when there's a new scandal to gawk at."

At the rate the hackers are moving, it may be even sooner than that. It's the damage that could be lasting.

Click to Print

Find this article at:
http://www.time.com/time/business/article/0,8599,2079423,00.html

Este artículo viene de culturas de archivo
http://culturasdearchivo.org/

La URL de esta historia es:
http://culturasdearchivo.org/modules.php?op=modload&name=News&file=article&sid=805