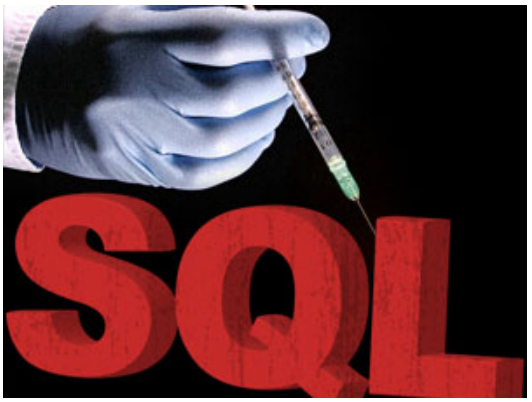
The Last Watchdog
on Privacy & Security
by Byron V. Acohido

FAQ: The rapid spread of SQL injection attacks



A criminal hacker's epiphany: Why not automate SQL inject attacks and use botnets to launch them?

That stroke of genius dawned on a criminal coder, possibly Chinese, a little less than a year ago. The result: in just 10 months, botnet-driven SQL injection attacks have been used to plant infections on multi-millions of webpages. These infections now lurk in wait for anyone who happens to click to what appears to be a reputable website.

Click on a tainted webpage and you won't notice anything amiss. But here's what happens next: A backdoor gets silently implanted on your harddrive. Through that backdoor the attacker will send coding that silently turns your machine into obedient "bot." Your botted PC gets slotted into a bot network of 10,000 or more other bots.

As part of this botnet, your machine may be used to deploy spam, spread infections, steal data, launder stolen funds, participate in extortionist denial of service attacks or wage political warfare against small nations. And for good measure: a datastealer will also get installed on your harddrive; it will clean out your email address book and buddy lists, and thus converting all of your contacts into targets for similar infections. And henceforth any information you type at account logon pages, online banking forms, shopping carts — any webpage with a submit buttion — will will get summarily harvested.

History of SQL injection attacks

SQL injection attacks have been around for years. They require time and skill, and were traditionally done manually. A SQL attack involves querying the databases underlying a web page — until the database hiccups and accepts an injection of malicious code. The intruder then gains full access to the data, and a foothold to roam deeper. Socrates, the meth-addicted hacker I wrote about in *Zero Day Threat,* used a SQL hack to break into a Michigan uniform company's website to steal 3,000 customer profiles, which he gave to his love interest, Hula Girl. This was back in 2005.

At some point in the spring of 2008, a bright hacker "had a Eureka moment," says Ryan Barnett, Breach Security's Director of Research. Instead of trying to steal data from one website at a time, why not use botnets to probe the Interent for webpages whose databases could be easily injected with a small bit of code — just enough to implant backdoor infections.

"It was a brilliant tactical move," says Barnett. "To say, 'if our end goal is to obtain sensitive personal data, hey, wait a minute! Why are we only targeting databases that might hold the information? Why don't we put malware on the sites, and when people go to the legitimate, regular websites; then people will get infected with our javascript? And we can install keystroke loggers and get the data that way.'

"It was pretty crafty," says Barnett.

450,000 webpages attacked daily

LastWatchdog has been unable to get anyone to estimateÃ‚Â how many reputable websitesÃ‚Â have been tainted since then. But the number must beÃ‚Â easily into the multi-millions of webpages. Automated SQL attacks began surfacing last April when 100,000 webpages of the British civil service, United Nations and U.S. Environmental Protection Agency we so hacked.

“The current thinking is the bad guys, thought to be Chinese in origin, use search engines results to identify lik attack targets,” Jeremiah Grossman, White Hat Security founder and CTO told LastWatchdog in spring 2008.Ã‚Â “Next they blindly send in malicious SQL injection traffic to the target websites . . .When someone visits one of these hundreds of thousands of infected web pages, their browser is instructed to connect to a hacker controlled site behind the scenes that exploits their browser and loads their machine with malware.”

For the first five months of 2008 IBM ISS helped large corporations block about 5,000 SQL attacks a day. By mid-June, daily attacks spiked to 25,000; by October they topped 450,000 a day.Ã‚Â And keep this in mind: those blocks only protect corporations that retain IBM ISS to defend their networks. Websites that don’t pay for comparable protection are getting engulfed by the same wave of automated SQL injection attacks, says Holly Stewart, IBM ISS threat response manager.

Cyber crime gangs are “finding tons of sites that have a set of conditions that will allow them to inject malicious software which will infect anyone who visits that site,” says Jack Danahy, founder and CTO of security firm Ounce Labs.

Everything you should know about SQL injection attacks

Below is a FAQ on SQL injection attacks compiled by LastWatchdog with guidance from — and gratitude extended to — Breach Security, WhiteHat, IBM ISS, Guardium and Ounce Labs.

Q: What is a SQL injection attack?

A: SQL refers to the layer of databases underlying most websites.Ã‚Â SQL attacks involves an unauthorized party injecting coding into one of these databases — coding that should not be there. An intruder can can do this by typing coding into the browser URL address line, or into any box of any webform, such as those found on account logon pages or shopping carts.

Q: How are SQL injection attacks typically carried out?

A: Prior to the spring of 2008, SQL attacks were done manually. The hacker would try different database queries from the browser or from pages displayingÃ‚Â web forms, until he successfully injected code into the underlying database. These types of attacks are still done, but on a smaller scale compared to the automated SQL infection/attacks that have come on strong.

Major banks and online merchants are putting up strong defenses, says Phil Neray, Guardium vice-president of security strategy, at Guardium. But regional banks and credit unions, smaller online retailers, and many government agencies remain highly vulnerable to manual, targeted SQL attacks.

As cited above, someÃ‚Â 100,000 webpages of the British civil service, United Nations and U.S. Environmental Protection Agency we so hacked in spring 2008. More recently, Commerce Bank, a small Midwest bank that operates 360 branches in Missouri, Illinois and Kansas, Scarborough & Tweed, a New Hampshire-based company that sells corporate gifts online, and a Rhode Island government Web siteÃ‚Â got hit, according toÃ‚Â Neray.

Q: Are manuul SQL injections still a big concern?

A: Yes. Manual, one-off SQL injection hackers are still out there making a living. Not only can theseÃ‚Â intruders clean out a customer database, they can get a foothold inside of the corporate network serving up the company’s website.

“We’ve seen numerous instances in which attacks leveraged SQL vulnerabilities in order to get inside of corporate networks and gtet access to internal systems and information that was not supposed to be exposed to the Internet,” says Tom Cross, Manager, X-Force Advanced Research, at IBM ISS. “When we first started seeing this kind of attack occurring, it was pretty amazing how simple and straightforward it was, yet how deep the intruder could infiltrate the infrastructure and be relatively unseen.

“The bad guys are getting in and are not being detected,” Cross continued. “They’re finding and taking what they want and leaving, not bothering to clean up.”

Q: What was the breakthrough that enabled automated SQL attacks?

A: In the spring of 2008, a criminal coder discovered that Microsoft SQL databases would accept javascript, the shorthand coding that enables cool website features. Microsoft contends in this SQL security alert that there is nothing wrong with its database products. Instead, the software giant blames sloppy coding by web application developers who write the programs that tap into the underlying databases.

This discovery touched off a gold rush by white hat, black hat and grey hat researchers to find security holes in widely-used, off-the-shelf web applications. In 2008, researchers found 134% more web application vulnerabilities than in 2007. To be more precise, these were flaws that could enable the injection of javascript into Microsoft databases, according to IBM ISS.

What's worse, to date 74% of these recently revealed SQL security holes have no available security patch.

Keep in mind those metrics apply to garden-variety web applications. Many websites use custom made web applications; and these more sophisticated programs are even more susceptible to SQL attacks, says IBM's Stewart.

Q: So the bad guys discovered javascript could be injected into Microsoft databases via poorly written web applications. How did they make hay of that development?

A: First, the bad guys developed tools to search out SQL vulnerabilities in off-the-shelf and custom web applications being used by web sites all across the Internet. "Automated tools that search for SQL injection vulnerabilities are able to find these vulnerabilities in standard and custom web applications alike," says IBM's Stewart.

Second, the bad guys began to instruct their botnets to inject malicious javascript into Microsoft databases, via flawed web applications, by the tens of thousands. "They figured out a way to scale it, and make it a broad attack," says Barnett, of Breach Security.

The javascript didn't do anything terribly invasive. It simply embedded an infection, so that anyone clicking to the tainted webpage thereafter got a backdoor installed — effectively turning full control of the machine overÃ‚Â to the intruder.

Q: What are the bad guys doing with all of this stolen personal data?

A: ID theft, of course, begins with stolen data. And millions of tainted websites lurking to silently infect visitors with data stealers appear to be swelling the gigantic pool of stolen identity data, along with viral spam campaigns, such as Waledec and KoobFace. And let's not forget big data heists, such as the recent breach at Heartland Payments Systems.

It's not a coincidence that identity theft is also rising. Nearly twice as many people — 7.5% of all U.S. adults — lost money as part of some sort of financial fraud in 2008 according to this survey by Gartner banking analyst Avivah Litan.Ã‚Â Last Fall, Litan surveyed 5,000 consumers. She found 70% had never been a victim of identity theft fraud; 14% had had their credit card information used to charge purchases or get money; 7% said their debit card was used; 6% said a new account had been opened in their name; 5% had money transferred out of their account; and 4% had had checks forged.

"It's not getting better, it's getting worse," says Litan. "I think this coming year will be more severe. A lot of stolen data has yet to be used."

Q: What can the average person do to avoid getting one of these infections?

A: Do your homework and be ready to give up convenience. There are numerous consumer tools designed to assess the goodness of the Web page you are about to click to, and tell you whether it's safe. AVG LinkScanner, ScanSafe, McAfee SiteAdvisor,Ã‚Â Enigma SpyHunter andÃ‚Â Authentium SafeCentral are browser-based security tools worth checking out.

And here's a tip: WinPatrol offers very powerful protection. It's a terrific free tool, popular with techies since it was created 10 years ago by Bill Pytlovany, one of the original designers of AOL and a longtime open-source practitioner. The premier version, called WinPatrol Plus, costs just $30 for a lifetime subscription, which includes all updates, and is designed for the average consumer. WinPatrol takes a snapshot of your Windows run registry, and from then on blocks and alerts you to any new executable program, such as a malicious backdoor, that tries to install itself on your hard drive.

But that's not enough. You must do all of your software updates promptly. Most SQL infectionsÃ‚Â work by exploiting long-ago discovered security flaws in your browser –Ã‚Â and in the programs that serve up Web-hosted video, music, photos, documents and work files. Keeping all of these web applications up to date will go a long way toward innoculating you.

This includes keeping current on updates for Internet Explorer, Firefox, Safari, Opera, Chrome, Adobe Flash, Adobe Reader, iTunes, QuickTime, Windows Media Player and RealPlayer. Microsoft and Mozilla do a credible job of alerting

users to security updates for the IE and Firefox browsers, respectively.Ã‚Â But the rest of the software vendors don't make it clear the updates increasingly include security patches.

–by Byron Acohido

Photos of Ryan Barnett, Obama, Avivah Litan, Jeremiah Grossman

March 17th, 2009 | For consumers | For technologists | Imminent threats | Obama watch | Steps forward | Top Stories | USAToday stories

Discuss this Article

12 Comments on "FAQ: The rapid spread of SQL injection attacks"

Notify of

new follow-up comments

Email

›

Join the discussion

Sort by: newest|oldest|most voted

Guest

Ray Dickenson

Nice coverage of an important story. We routinely scan the 15,000+ banking and shopping websites in the SafeCentral directory, looking for malicious code. I recently called a credit union to warn them a hidden iframe had been added to every page of their online banking web site. The iframe contained a Javascript tag pointing to China. This was a remarkable example of a banking website distributing malware that could, in turn, steal banking credentials. The general manager of the credit union reassured me, saying, "Oh, that's not a virus, it's just a pop-up that offers to sell antivirus." The notorious… Read more »

0

8 years 11 months ago

Guest

Eric Schultze

This is a scary problem that isn't going away anytime soon. Were there a simple way to 'fix' webservers and SQL servers to protect them from this attack, we might see a decline, over time, from this type of threat. The last two paragraphs of your story are central to protecting against becoming a bot. They best thing users can do to protect their computers from hijack is to install the latest available patches for their computer. As you mention, web browser patches are at the top of the list, but don't forget to do Operating System patches (MS09-006 is… Read more »

0

8 years 11 months ago

Author

bacohido

Ray: Were you able to determine whether the hidden iframes on this credit union's webpages were, indeed, primarily related to selling fake antivirus/antispyware? Please look over this excerpted chapter from my book (see link) about the iframebiz cash gang, and their activities, led by Andrey Sporaw, way back in 2005. http://lastwatchdog.com/selling-fake-antivirus-start/ Some other questions: Are these the same guys? Why does selling fake antivirus appear to be stronger than ever? What metrics or anecdotes can I use to describe just how prevalent fake antivirus campaigns are in the mix of bad stuff on the Internet? What other delivery methods are… Read more »

0

8 years 11 months ago

Guest

Ray Dickenson

It's not clear who is/was behind the iframe injection on the credit union site I mentioned. We're focusing on protecting consumers during their online banking sessions. Fake antivirus campaigns are clever because they prey on user fear, have a clear call-to-action, and cause the user to voluntarily use their credit card on their own computer to purchase the software. The criminals do not have to use credit card information to create a fraudulent transactions. Regarding their prevalance and other delivery methods, I see even today that the tragic death of actress Natasha Richardson is being used to distribute fake antivirus… Read more »

0

8 years 11 months ago

Guest

Bill Carey

Great article. One of the many things the bad guys are stealing as part of these ID Theft scams is your passwords. People typically let Internet Explorer remember their passwords which is not secure or save them in a Word or Excel document, which can be stolen

as youÃ¢â‚¬â„¢ve outlined above. In addition many users have keyloggers unknowingly installed which steal your passwords as you type them. Our software will help prevent ID theft by storing userÃ¢â‚¬â„¢s passwords in secure, encrypted files and then logging users into websites automatically so users donÃ¢â‚¬â„¢t need to type their passwords. Using secure passwords… Read more »

0

8 years 11 months ago

Guest

Mike Kilroy

Byron — Just started susbscribing to your blog. You really should twitter each new post. FYI, I tweeted your blog to my followers http://twitter.com/mike_kilroy

0

8 years 11 months ago

Guest

Uri Rivner

Byron, Excellent article! The SQL injection self-expanding botnet was indeed a stroke of breakthrough creativity, and I'd say its timing was just right for the fraud community. In the last couple of years, Trojans Ã¢â‚¬â€œ once the tools of the very savvy high end of cyber crime Ã¢â‚¬â€œ have become cheaper and easier to use, but there was one thing missing: scale. In order to really capitalize on Trojan technology, fraudsters had to look for ways to distribute their malware to a huge amount of victims. Now these criminals have the scalability they needed. No wonder RockPhish, the mammoth Phishing… Read more »

0

8 years 11 months ago

Guest

Razvan Stoica

Neat article, Mr. Acohido. You make an especially important point about updating your web-facing apps. At BitDefender, we routinely come across e-threats like this password stealer trojan. Compromised pages are set up to run literally dozens of exploits against machines that visit one of the SQL-injected sites – Flash player vulnerabilities, old Explorer bugs, you name it, they have it, waiting for an unpatched machine to come along. It's all set up neatly so that exploits are tried based on user agent information about what might work. This particular trojan is set up to steal game accounts – a type… Read more »

0

8 years 11 months ago

Guest

Paul Davie

We were alerted to automated SQL injection attacks when a customer was compromised last year, causing them significant problems from data corruption. The initial round of attacks from last spring and summer were largely small but wide-scale attempts at installing malware. However, automated SQL injection has the potential for much more serious consequences, since SQL is the way in which the database is both queried and managed. We have advised all clients to keep their web content databases hosted on a separate server from any commercial or sensitive data, as this is an important step in protecting data. The potential… Read more »

0

8 years 11 months ago

Guest

Uri Rivner

Excellent article! The SQL injection self-expanding botnet was indeed a stroke of breakthrough creativity, and I'd say its timing was just right for the fraud community. In the last couple of years, Trojans Ã¢â‚¬â€œ once the tools of the very savvy high end of cyber crime Ã¢â‚¬â€œ have become cheaper and easier to use, but there was one thing missing: scale. In order to really capitalize on Trojan technology, fraudsters had to look for ways to distribute their malware to a huge amount of victims. Now these criminals have the scalability they needed. No wonder RockPhish, the mammoth Phishing operation… Read more »

0

8 years 11 months ago

Guest

Ken Pappas

Great down to Earth article on SQL. The only caution I have is that network threats are coming from many creative means, SQL being one of them. Network IT folks need to think beyond what they are seeing and hearing. They need to look around them and think about what is possible. When I look at threats and say "Hey this is possible", it then become eminent that the threat is real. I study and forecast tomorrow's threats and there are some real freaky things going on out in Cyber Space.
ken

0

8 years 11 months ago

Guest

Hiroyuki Shigematsu

According to the IPA (INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN) and LAC(Little eArth Corporation Co., LTD.), SQL injection attacks against servers in Japan have increased rapidly in 2008. Specifically, in December 2008, SQL injections were 60 times the previous figure. And as mentioned in your blog, botnet attacks are also rapidly increasing. Further, SQL injections and Cross site Scripting makes up 65% of the total vulnerabilities of websites in Japan. This data also signifies that countermeasures for SQL injection are extremely important. There are many end users in Japan who misunderstand that Network Firewalls and IDS(Intrution Detection Systems)/IPS(Intrution Prevention Systems) can protect… Read more »

0

8 years 11 months ago