EXHIBIT 7

July 14, 2008 9:12 AM PDT

Column: The man who changed Internet security

Posted by Robert Vamosi 14 comments

Programming note: *As of Friday, July 11, 2008, Defense in Depth will now only carry my weekly column plus additional commentary on the state of computer security. My security news blogs will instead appear under the CNET News Security banner going forward. And my CNET News Security Bites podcasts can be found at here. All of these can be subscribed to via RSS.*

While security researcher Dan Kaminsky still won't comment on the specific nature of a flaw within the Domain Name System--for fear that criminal hackers might exploit it before the worldwide network of name servers worldwide and client systems that contact them can be updated--he nonetheless went public on July 8 with some details, backed by simultaneous patch releases from Microsoft, Cisco, and others.

There have been other multiparty patch releases, but never has there been one on such a massive scale. It took someone with the gravitas and reputation of Kaminsky to pull together the affected parties.

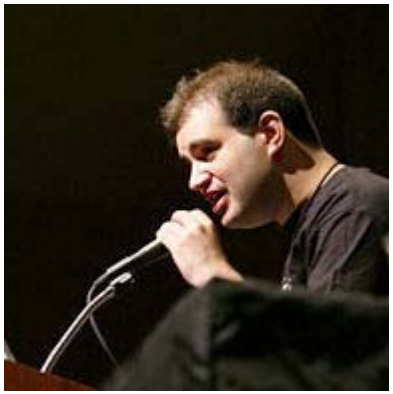
What he and others he took into his confidence did over the last
few months was not only responsible but extraordinary. The flaw that Kaminsky discovered could allow criminal hackers to guess the transaction ID of any request to a DNS server for a particular domain, such as one used for a bank or an e-commerce site, and then redirect that request to another site, a phishing site. It would do so silently, evading most anti-phishing technology because

About Defense in Depth

Covering computer viruses and computer crime, Robert Vamosi goes beyond the hype to provide you with expert interviews of the top security researchers, as well as offeri the hands-on, nontechnical advice you'll need to stay safe online.

Subscribe via RSS
Click this link to view as XML.

the change would be made not at the desktop level but at the DNS server itself. Certainly this is big, and certainly one would want to get the news out as soon as possible--but Kaminsky took the time to inform the proper vendors and authorities and, only after they were ready with patches, did he disclose some of what he'd discovered.



Dan Kaminsky at DefCon in 2006.

(Credit: Declan McCullagh/CNET News)

That isn't to say what Kaminsky did was perfect; he himself admits there are lessons to be learned and improved upon the next time this happens. Whether you agree with the severity of the flaw Kaminsky disclosed last Tuesday, I do think all future vulnerability disclosures could benefit from his example.

Kaminsky, director of penetration testing at IOActive, is no stranger to vulnerabilities. Over the years he's found a fair share and says that in the case of the DNS flaw he wasn't looking for it. In this week's Security Bites podcast, Kaminsky told me that after three days of testing he knew he had something important. At that point, early in 2008, he had a few options.

One was to tell the vendor (or, in this case, vendors) directly. Ari Takanen of Codenomicon told me he prefers that security researchers keep vulnerabilities between them and the vendor. Vendors, Takanen said, have their own development cycles, and for a researcher to burst into a room or go public and demand that everyone work on his or her vulnerability is unrealistic. While Kaminsky was willing to work with the vendors, he wasn't willing to give them forever.

Another option was to sell the vulnerability to a third party like TippingPoint's Zero Day Initiative. ZDI acts as the middleman, talking with the vendor and communicating with the researcher. The advantage here is that a researcher with no connections to the affected vendor can communicate the problem clearly.

ZDI has been credited with several vulnerabilities, such as those announced by Apple and Microsoft. Kaminsky has no qualms with those who opt for this method, although he said he didn't understand why a company would pay for this information. (I know the answer: TippingPoint uses the vulnerability data it purchases to protect its customers first, thereby giving it a competitive advantage in the vulnerability assessment space).

Another option for Kaminsky was to go public, to announce the vulnerability and publish details, including an exploit, on, say, Bugtraq. A few researchers have gone this route, but often as a last resort after getting a cold shoulder from the vendor. A few researchers have published flaw details first without contacting anyone, taking both the public and the vendor by surprise. But such moves are unwise since they give the bad guys all the information they need while everyone is vulnerable.

Finally, as Kaminsky reminded me, there's the option of selling your vulnerability to the criminal underside of the Internet.

With the DNS flaw, Kaminsky was in a very weird position. What he found wrong with DNS, the servers that translate a Web site's common name to its IP address, wasn't just within one vendor's product, it cut across various products, from various vendors. He said he consulted with DNS expert Paul Vixie, and together they decided they had to convene a meeting, and do so within a few weeks of the discovery.

Whether or not Kaminsky knocks the socks off of everyone at Black Hat seems considerably less important than the responsible nature of his disclosure.

That meeting occurred at Microsoft's Redmond, Wash., headquarters on March 31, 2008. There, representatives from 16 vendors sat down and listened to Kaminsky's pitch. After deciding this was a real and exploitable problem, the vendors decided they would have little choice but to agree to release simultaneously their respective patches.

At some point, July 8, 2008, was agreed upon as the date,

perhaps because it coincided with Microsoft's monthly Patch Tuesday. The date was significant in other ways: for example, it fell roughly 30 days before Kaminsky was scheduled to speak at Black Hat in Las Vegas.

Between March and July, there was considerable back and forth among Kaminsky and the vendors, and then, as the date neared, he decided to share the details with a few others.

In retrospect, Kaminsky confessed that he really should have told more people. He had gone through great pains to inform the DNS community, the specific vendors, and few researchers. He did so to keep word from getting out.

But within hours of making his announcement, Kaminsky faced a chorus of public ridicule by other security researchers, most hearing about the flaw for the very first time. The complaints, at times, trivialized the announcement, with fellow researchers citing that similar claims had been made against DNS 3 to 10 years before or even longer. Some suggested Kaminsky was simply trying to advertise his talk at Black Hat next month.

Most vocal was Matasano Security researcher Thomas Ptacek, who blogged his doubts. But Kaminsky called Ptacek and he retracted his comments. He now says, "Dan has the goods. Patch now, ask questions later."

Whether or not Kaminsky knocks the socks off of everyone at Black Hat seems considerably less important than the responsible nature of his disclosure. He could have, as Ptacek notes, made thousands of dollars off this DNS thing. Instead, Kaminsky has set a high mark for future disclosures. He has changed Internet security, and done so for the better of us all.

TOPICS: **Security**
TAGS: **security**, **column**, **Security Watch**, **Dan Kaminsky**, **DNS patch**
BOOKMARK: Digg Del.icio.us Reddit Yahoo! Buzz

August 8, 2008 5:35 AM PDT

Between a rock and YouTube, video execs see promise
Posted in News - Digital Media by Stefanie Olsen
August 8, 2008 4:00 AM PDT

Targeted for hacking by reporters at my table
Posted in News - Security by Elinor Mills
August 8, 2008 1:00 AM PDT

All News.com headlines »

Featured blogs

Beyond Binary by Ina Fried
Coop's Corner by Charles Cooper
Defense in Depth by Robert Vamosi
Geek Gestalt by Daniel Terdiman
Green Tech
One More Thing by Tom Krazit
Outside the Lines by Dan Farber
The Iconoclast by Declan McCullagh
The Social by Caroline McCarthy
Underexposed by Stephen Shankland

Recent posts from Defense in Depth

Black Hat 2008: Notes from the field

Column: Finally, ID fraud protection that works

Column: Will you be ditching your antivirus app anytime soon?

A real simple answer to password protection

Despite patch, today's systems still vulnerable to 2002 flaw

ADD A COMMENT **(Log in or register)**

14 comments (Page 1 of 2)

by inachu July 14, 2008 7:55 AM PDT

I miss the days where most govt agencies had their own BBS.
Using telnet and going into various areas just exploring.
I went from my local library to MIT then onto NIST then onto some tokyo university BBS retracing mysteps it went all the way around the world through nasa then loggen back into my library.
Sad to see we can't do that anymore. No more wild jungle.

Reply to this comment

by tekwiz4u July 14, 2008 11:17 AM PDT

It's commendable what he did. He wasn't in it for bragging rights, like most of the hackers out

there. The exploit would have been bad for all of us. But he took it upon himself to be responsible to benefit the greater whole. Good job.

Reply to this comment

by n3td3v July 14, 2008 11:28 AM PDT

Media hype and clever marketing for Blackhat security conference.

Let's find out who is making the money, this vulnerability is over hyped.

Reply to this comment

by The_Decider July 14, 2008 12:10 PM PDT

Responsible? Only because the parties involved took it seriously.

If they had not and Kaminsky hadn't disclosed it would have been irresponsible. The black hats would have found it eventually leaving everyone at the mercy of them.

Full disclosure is always better than those idiots who think there is any merit to security through obscurity.

Reply to this comment

by RobertinOhio July 14, 2008 12:44 PM PDT

As a security professional whom is certified I still do not see the value of this "admiral approach" to

releasing of security incidents and vulnerabilities. Yeah Dan Kaminsky has made a name for himself in the security community. If he was just some other schmo...then he would have never seen the inside of any vendor's office. My name does not mean jack so I know I am not going to pick up the phone and get a meeting at Cisco or Microsoft in a couple of days to discuss the issue with them. I am going to put my discovery on Bugtraq and if the internet gets shut down in North America as a result...oh well.

BUT...if I do sit on it and a hacker finds the exploit and then I come out afterward, I get nailed for not sharing it. D-amned if I do and d-amned if I don't. The good guys always loose.

Another thing I have learned is usually the hacker will almost always win. All you can do is contain, eradicate, and learn from attacks and exploits to make it harder for them to break in. Not sharing your discoveries from the general public and only with vendors is most certainly NOT the way to resolve these issues however. I do not commend Dan Kaminsky for his actions, he is setting a BAD precedent. One that unfortunately Infragard, another organization with a history of one way traffic with information, follows.

Reply to this comment

by DanKaminsky July 14, 2008 2:13 PM PDT

Robert--

The vendors have become pretty good at responding to stuff -- and, of course, if you do find something of technical value, please feel free to contact me and I will be happy to help. I'm trying to find a balancing point between not releasing (which leads to no patches, and/or no deployment of patches) and releasing in a problematic manner (i.e. even those places that are responsible, and do maintain their security, are still hit). Maybe this isn't perfect, but please give me the benefit of the doubt until you know just what I've found.

Reply to this comment | View all 2 replies

by DanKaminsky July 14, 2008 2:17 PM PDT

Decider--

I agree. It's only because the vendors were so amazingly responsive that this path could be taken at all. If they'd been lame, we'd be screaming at them for being so. So, they weren't lame, in all fairness they deserve some appreciation for that.

Reply to this comment

by n3td3v July 14, 2008 3:47 PM PDT

Dan Kaminsky is making money out of this there is no doubt.

If he hadn't circled his disclosure around a profiteering security conference I wouldn't bash this **** so much.

Because he has circled his disclosure around a big security conference, I know his motivation is money.

I don't know who he has been shaking hands with and what money has been exchanged, but this is something for the government to wire tap on.

Reply to this comment

by mehap July 14, 2008 11:12 PM PDT

So what if he is making/indulging in making money?

Your whole system is geared on making money.

How do you survive mate?

Reply to this comment

by DanKaminsky July 15, 2008 3:45 PM PDT

n3td3v--

Dude, did you miss the fact that Defcon is like three days later? Black Hat is just practice for Defcon  Seriously, the last big talk was Seattle Toorcon. Rickrolling the Internet isn't exactly profit source number one.

Reply to this comment

1 | 2 | Next 10 Comments >>

Register to submit a comment

Already have an account? Log in now

Join the CNET community To continue, we ask that you first complete the free registration.

Choose a username

E-mail address

Choose a password (6 characters minimum)

Retype password

I agree to CNET's Terms of Use

CONTINUE

Need help? »

Powered by Jive Software

August 7, 2008 9:07 AM PDT

Kaminsky provides the why of attacking DNS

Posted by Robert Vamosi 6 comments

LAS VEGAS--Speaking before a packed audience, researcher Dan Kaminsky explained the urgency in having everyone patch their systems: virtually everything we do on the Internet involves a Domain Name System request and therefore is vulnerable.

Expectations were running high before Wednesday morning as Kaminsky, director of penetration testing for IOActive, had revealed little about his DNS vulnerability up till then. That didn't stop others from trying to figure it out. But that actually helped Kaminsky in the end; it meant during his speech, he was able to skip the what and go directly to the why.

Security researchers always thought it was hard to poison DNS records, but Kaminsky said to think of the process as a race, with a good guy and bad guy each trying to get a secret number transaction ID. "You can get there first," he said, "but you can't cross finish line unless you have the secret number."

The question is why would someone bother? Well, Kaminsky talked about how deeply embedded DNS is in our lives. Kaminsky said there are three ages in computer hacking. The first was attacking servers (for example FTP and Telnet). The second was attacking the browsers (for example Javascript and ActiveX). We're now about to enter the third age, where attacking Everything Else is possible.

We know that if we type a name.com into a browser, the DNS resolves it to its numerical address. But what we don't realize is that same process occurs when we send e-mail or when we log onto a Web site. These also require DNS lookup.

Kaminsky then detailed how various security methods on the Web can be defeated if one owns the DNS. For example, if a site wants to establish a Trust Authority Certificate with the Certificate Authorities, they use e-mail to confirm the identity of the requester. He also said that it's possible to poison Google Analytics and even Google AdSense, which also rely on DNS lookup.

Prior to the patch, the bad guy had a 1 in 65,000 chance of getting it because the transaction ID is based, in part, on the port number used. With the patch, the chances decrease to 1 in 2,147,483,648. Kaminsky said it's not perfect, but it's a good enough start.

Click here for full coverage of Black Hat 2008.

TOPICS: **Vulnerabilities & attacks**, **News**
TAGS: **Security**, **Black Hat 2008**, **Dan Kaminsky**, **DNS**
BOOKMARK: Digg Del.icio.us Reddit Yahoo! Buzz

Recent posts from News - Security

Targeted for hacking by reporters at my table

Black Hat expels reporters in network snooping

Microsoft to seek credit for finding vulnerabilities

Wall of Sheep comes to Black Hat

Is Check Point's security profile the broadest?

News - Security topics

Corporate & legal
Privacy & data protection
News
Vulnerabilities & attacks

Most popular stories

Kaminsky provides the why of attacking DNS

IKEA to sell solar panels?

Photos: More spins from the Oshkosh air show

Images: Scientists develop eye camera

Black Hat a sure bet to be big, bold in Vegas

Latest tech news headlines

Between a rock and YouTube, video execs see promise
Posted in News - Digital Media by Stefanie Olsen
August 8, 2008 4:00 AM PDT

Targeted for hacking by reporters at my table
Posted in News - Security by Elinor Mills
August 8, 2008 1:00 AM PDT

Google sours on $1 billion AOL investment
Posted in News - Digital Media by Steven Musil
August 7, 2008 9:20 PM PDT

ADD A COMMENT (**Log in or register**)

6 comments (Page 1 of 1)

by One Mark Bliss August 7, 2008 10:04 AM PDT

Actually, the chances decrease, since the one is divided by the increased number. Consider that the concept of chance being used in the article represents the random likelihood that someone will guess the secret code in one attempt.
It seems that a similar confusion exists in another concept nothing to do with chance, namely turning the air conditioning up, or down. Which makes the room colder? In that case it depends on whether the concept being referred to is the amount of the flow of cold air, in which case it would be up, or the numerical representation of temperature, in which case it would be down.
The only way a similar confusion can arise with chance is whether it is couched as the chance of guessing something randomly, or the chance of not guessing it. So, in the article, the chance would only increase if it were the chance of a hacker randomly NOT getting the secret code.

Reply to this comment | View reply

by conobs August 7, 2008 11:20 AM PDT

instead of giging them on symantecs
WHERE IS THE MEAT?
how dos it work?

this would qualify more as a story about a story, not an actual news story
take it up a notch
thx
bob

All News.com headlines »

Featured blogs

Beyond Binary by Ina Fried
Coop's Corner by Charles Cooper
Defense in Depth by Robert Vamosi
Geek Gestalt by Daniel Terdiman
Green Tech
One More Thing by Tom Krazit
Outside the Lines by Dan Farber
The Iconoclast by Declan McCullagh
The Social by Caroline McCarthy
Underexposed by Stephen Shankland

Resource center from News.com sponsors

Reply to this comment

by conobs August 7, 2008 11:25 AM PDT

i dont know maybe i am wrong and overly harsh

Reply to this comment

by frazmann August 7, 2008 12:55 PM PDT

@conobs - the crux of the hack are that you send a DNS request to a server, knowing that the server will send a request to it's DNS master server to obtain the translation, and then bombard the server with fake responses, hoping to guess the transaction id that it used when making the request. If you get it right before the master server's response arrives then you have planted a fake DNS entry in your server, and the real response is thrown away. If you do this from your comcast account then you can re-direct all your neighbors to a fake google.com that sits on your PC. Seems so simple I'm surprised no-one tried it before....

Reply to this comment

by benjaminstraight August 8, 2008 3:14 AM PDT

Good article.

Reply to this comment

Register to submit a comment

Already have an account? Log in now

Join the CNET community To continue, we ask that you first complete the free registration.

Choose a username

E-mail address

Choose a password (6 characters minimum)

Retype password

I agree to CNET's Terms of Use

CONTINUE

Need help? »