US Congress Rules Huawei a 'Security Threat'

Posted by timothy on Monday October 08, @07:06AM from the q-in-tel-is-totally-a-different-story dept.

dgharmon writes with the lead from a story in the Brisbane Time:

"Chinese telecom company Huawei poses a security threat to the United States and should be barred from US contracts and acquisitions, a yearlong congressional investigation has concluded. A draft of a report by the House Intelligence Committee said Huawei and another Chinese telecom, ZTE, 'cannot be trusted' to be free of influence from Beijing and could be used to undermine U.S. security."

Entire Cities In World of Warcraft Dead, Hack Suspected

Posted by timothy on Sunday October 07, @05:40PM from the just-some-reamde-plotlines-nothing-to-worry-about dept.

hypnosec writes

"Entire cities in the World of Warcraft have been destroyed with no one spared, not even the NPCs. About 13:00 GMT, forums on WOW started getting the first comments from users regarding players and NPCs dying on the Ragnaros-EU realm in Orgrimmar. Users of the online game started reporting that Draenor had a similar sight to offer. Some of the other realms where this was reported include Tarren Mill, and Twisting Nether."
DNS and BGP

CS642: Computer Security

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu
DNS and BGP

DNS
Attacking the DNS system
BGP
BGP attacks
Defense mechanisms
We don’t want to have to remember IP addresses

Early days of ARPANET: manually managed hosts.txt served from single computer at SRI
Hierarchical domain name space

Top Level domains (TLD)
- org
- net
- edu
- com
- tv
- ca

Second Level domains
- wisc
- ucsd
- davis

ICANN (Internet Corporation for Assigned Names and Numbers)
- cs
- ece

root nameservers and authoritative nameservers

Zone: subtree

max 63 characters
Resolving names

From
## Example DNS query types

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>address (get me an IPv4 address)</td>
</tr>
<tr>
<td>AAAA</td>
<td>IPv6 address</td>
</tr>
<tr>
<td>NS</td>
<td>name server</td>
</tr>
<tr>
<td>TXT</td>
<td>human readable text, has been used for some encryption mechanisms</td>
</tr>
<tr>
<td>MX</td>
<td>mail exchange</td>
</tr>
</tbody>
</table>
Caching

• DNS servers will cache responses
  – Both negative and positive responses
  – Speeds up queries
  – periodically times out. TTL set by data owner
DNS packet on wire

Query ID is 16-bit random value

We’ll walk through the example from Friedl’s document

From Friedl explanation of DNS cache poisoning, as are following diagrams
Query from resolver to NS

<table>
<thead>
<tr>
<th>IP</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>src IP = 68.94.156.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dst IP = 192.26.92.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>src port = 5798</td>
<td>dst port = 53</td>
<td></td>
</tr>
<tr>
<td>UDP length</td>
<td>UDP checksum</td>
<td></td>
</tr>
<tr>
<td>QID = 43561</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Question count = 1</td>
<td>Answer count = 0</td>
<td></td>
</tr>
<tr>
<td>Authority count = 0</td>
<td>Addl. Record count = 0</td>
<td></td>
</tr>
</tbody>
</table>

**QU** What is A record for www.unixwiz.net?
Response contains IP addr of next NS server (called “glue”)

Response ignored if unrecognized QueryID
**IP**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>src IP</td>
<td>68.94.156.1</td>
</tr>
<tr>
<td>dst IP</td>
<td>64.170.162.98</td>
</tr>
</tbody>
</table>

**UDP**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>src port</td>
<td>5798</td>
</tr>
<tr>
<td>dst port</td>
<td>53</td>
</tr>
</tbody>
</table>

**QID = 43562**

- Question count = 1
- Authority count = 0
- Answer count = 0
- Add1. Record count = 0

**Qu**
What is A record for www.unixwiz.net?

- RD=1 - recursion desired
- OP=0 - standard query
- QR=0 - this is a query
**bailiwick checking:**
response is cached if it is within the same domain of query (i.e. a.com cannot set NS for b.com)
Here we go again...

- What security checks are in place?
  - Random query ID’s to link responses to queries
  - Bailiwick checking (sanity check on response)
- No authentication
  - DNSsec is supposed to fix this but no one uses it yet
- Many things trust hostname to IP mapping
  - Browser same-origin policy
  - URL address bar
What are clear problems?

• Corrupted nameservers
• Intercept & manipulate requests
  – BGP route hijacking (stay tuned)
• Other obvious issues?
DDoS against DNS

• Denial of Service
  – take down DNS server, clients can’t use Internet
  – Feb 6, 2007 attack against 6 of 13 root servers:
    • 2 suffered very badly
    • Others experienced heavy traffic

• DoD purportedly has interesting response:
  – “In the event of a massive cyberattack against the country that was perceived as originating from a foreign source, the United States would consider launching a counterattack or bombing the source of the cyberattack, Hall said. But he noted the preferred route would be warning the source to shut down the attack before a military response.”
  – http://www.computerworld.com/s/article/9010921/RSA_U.S._cyber_counterattack_Bomb_one_way_or_the_other
DNS cache poisoning

Clients

Victm DNS server

Internet

bankofsteve.com 10.1.1.1

Attacker site 10.9.9.99

goodguy.com IP = 10.9.9.9

goodguy.com IP = 10.1.1.1

How might an attacker do this?
Assume DNS server uses predictable UDP port
1. IP for www.BankOfSteve.com?
2a. Forged answers: IP = 10.9.9.99
2b. QID=1000
   IP for www.bankofsteve.com?
3. QID=1000
   referral to ns1.bankofsteve.com
4. QID=1001
   IP for www.bankofsteve.com?
5. QID=1001
   IP = 10.1.1.1
6. www.bankofsteve.com is 10.9.9.99
Simultaneously
Another idea:
- Poison cache for NS record instead
- Now can take over all of second level domain

How many tries does this require?
- Try 256 different QIDs
- Do about 256 attempts
Does happen in the wild

**HD Moore pwned with his own DNS exploit, vulnerable AT&T DNS servers to blame**

By Dancho Danchev | July 30, 2008, 8:08am PDT

*Summary:* A week after |)ruid and HD Moore release part 2 of DNS exploit, HD Moore’s company BreakingPoint has suffered a traffic redirection to a rogue Google site, thanks to the already poisoned cache at AT&T servers to which his company was forwarding DNS traffic: “It happened on Tuesday morning, when Moore’s company, BreakingPoint had some [...]”

Defenses

• Query ID size is fixed at 16 bits
• Repeat each query with fresh Query ID
  – Doubles the space
• Randomize UDP ports
  – Dan Bernstein’s DJBDNS did this already
  – Now other implementations do, too
• DNSsec
  – Cryptographically sign DNS responses, verify via chain of trust from roots on down
Phishing is more common

• Typo squatting:
  – www.ca.wisc.edu
  – www.goggle.com

• Other shenanigans:
  – www.badguy.com/(256 characters of filler)/www.google.com

• Phishing attacks
  – These just trick users into thinking a malicious domain name is the real one
As our thanks to you, our visitors, please select a *Free* gift!

*Free* Apple iPad 2©  ·  *Free* Apple iPhone 4S©
Other abuses, so-called DNS pharming

First case of "drive-by pharming" identified in the wild

By Ellen Messmer, Network World
January 22, 2008 02:24 PM ET

The theory is now a reality. Symantec reported Tuesday that drive-by pharming, in which a hacker changes the DNS settings on a customer's broadband router or wireless access point and directs the link to a fraudulent Web site, has been observed in the wild.
An anonymous reader writes

"There is an interesting story over at the SANS Internet Storm Center that shows details on about 50 organizations that have had new machine names added to their DNS zone information. These were then pointed to sites used to boost the search engine cred of pharma, personals, and porn sites. If you outsource your DNS, how would you ever catch something like this?"
DNS piggybacking

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>IP Address</th>
<th>Domain Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>buy-cialis.sacmetrofire.ca.gov</td>
<td>74.220.215.210</td>
<td><a href="http://www.sacmetrofire.ca.gov">www.sacmetrofire.ca.gov</a></td>
<td>66.147.240.176</td>
</tr>
<tr>
<td>buy-viagra.sacmetrofire.ca.gov</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>drugs.sacmetrofire.ca.gov</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mgdrugs.sacmetrofire.ca.gov</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rxdrugs.sacmetrofire.ca.gov</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

From https://isc.sans.edu/diary/What+s+In+A+Name+/11770

Attackers maliciously added extra domain lower level domain names to valid domain name

This is helpful for search engine optimization
BGP and routing

BGP (exterior BGP)

OSPF within AS’s (Open shortest-path first)
BGP

• Policy-based routing
  – AS can set policy about how to route
    • economic, security, political considerations
• BGP routers use TCP connections to transmit routing information
• Iterative announcement of routes
• 2, 7, 3, 6 are Transit AS
• 8, 1 are Stub AS
• 4,5 multihomed AS
• Algorithm seems to work OK in practice
  – BGP is does not respond well to frequent node outages
IP hijacking

• BGP unauthenticated
  – Anyone can advertise any routes
  – False routes will be propagated

• This allows IP hijacking
  – AS announces it originates a prefix it shouldn’t
  – AS announces it has shorter path to a prefix
  – AS announces more specific prefix
Malicious or misconfigurations?

• AS 7007 incident in 1997
  – “Okay, so panic ensued, and we unplugged *everything* at 12:15PM almost to the second.” [sic]

• China Telecom hijacks large chunks of Internet in 2010
  – [http://bgpmon.net/blog/?p=282](http://bgpmon.net/blog/?p=282)
Youtube incident

• Pakistan attempts to block Youtube
  – youtube is 208.65.152.0/22
  – youtube.com = 208.65.153.238

• Pakistan ISP advertises 208.65.153.0/24
  – more specific, prefix hijacking

• Internet thinks youtube.com is in Pakistan

• Outage resolved in 2 hours…
BGPsec

- Route announcements must be cryptographically signed
  - AS can only advertise as itself
  - AS cannot advertise for IP prefixes it does not own
- Requires a public-key infrastructure (PKI)
- Still in development:
Internet Security

• Recurring themes:
  – Built without any authenticity mechanisms in mind
  – Functionality mechanisms (sequence #’s) become implicit security mechanisms
  – New attempts at backwards-compatible security mechanisms
    • IP -> IPsec
    • DNS -> DNSsec
    • BGP -> BGPsec
Shady Reshipping Centers Exposed

Posted by timothy on Thursday October 13, @08:52AM from the shady-shipping-containers-make-cool-houses dept.

Dynamoo writes

"Ever wondered how criminals can spirit away the products they buy with stolen credit cards? The answer is that they use surprisingly sophisticated but very shady reshipping centers to launder the goods on their way to Eastern Europe. The bad guys make the money, but it's the mules doing the reshipping who will eventually get caught."

Read the 86 comments