Crypto ransomware targets called by name in spear-phishing blast

Once the domain of espionage, personalized scams embraced by profit-driven scammers.

by Dan Goodin - Apr 6, 2016 10:07am CDT

Thu 3/10/2016 3:39 PM

Jamie Byrom <motellanancy@aol.com>

Incident at [redacted] - For the attention of [redacted] - Message (HTML)

To [redacted]

FILE MESSAGE

Dear [redacted]

I have been told to contact you in reference to the conflict that happened at [redacted] (BENTONVILLE, AR, [redacted]) on Tuesday. Please see the enclosed document for comprehensive details on the incident.

Would you mind if I asked you to view the complaint and respond with your thoughts on this?

Good Luck!

Jamie Byrom

Enlarge / An e-mail targeting a retail company to deliver point-of-sale malware.

Proofpoint

For the past decade, spear phishing—the dark art of sending personalized e-mails designed to trick a specific person into divulging login credentials or clicking on malicious links—has largely been limited to espionage campaigns carried out by state-sponsored groups. That made sense. The resources it takes to research the names, addresses, and industries of large numbers of individuals was worth it when targeting a given organization that had blueprints or some other specific piece of data prized by the attacker. But why go through the trouble to spread crypto ransomware or banking trojans to the masses when a single scam e-mail could do the trick?
network security
* Domain name system (DNS)
* CIDR
* Border Gateway Protocol
<table>
<thead>
<tr>
<th>Domain Name</th>
<th>IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.amazon.com">www.amazon.com</a></td>
<td>54.239.25.208</td>
</tr>
<tr>
<td>theverge.com</td>
<td>172.111.64.124</td>
</tr>
<tr>
<td>goglemail-smtp.l.google.com</td>
<td>74.125.193.16</td>
</tr>
<tr>
<td>hosted-cdn.statuspage.io</td>
<td>23.235.40.65</td>
</tr>
<tr>
<td>p05-calendars.icloud.com</td>
<td>17.172.100.13</td>
</tr>
<tr>
<td>print-gw.cs.wisc.edu</td>
<td>128.105.123.66</td>
</tr>
</tbody>
</table>

Which one is easier to remember?

**Domain Name System (DNS)**

translates domain names->IP addresses
Hierarchical domain name space

ICANN (Internet Corporation for Assigned Names and Numbers)

root nameservers and authoritative nameservers

Zone: subtree
Name Servers

Recrusively hunts down an answer

Authoritative name servers
Programmed by an original source

Caching

• DNS servers will cache responses
  – Both negative and positive responses
  – Speeds up queries
  – Entries expire periodically. Time-to-live (TTL) set by data owner
Example DNS query types

<table>
<thead>
<tr>
<th>Query Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>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</td>
</tr>
<tr>
<td>MX</td>
<td>mail exchange</td>
</tr>
</tbody>
</table>
DNS packet on wire

Query ID is 16-bit random value
Query from resolver to NS

<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>192.26.92.30</td>
</tr>
<tr>
<td>src port</td>
<td>5798</td>
</tr>
<tr>
<td>dst port</td>
<td>53</td>
</tr>
</tbody>
</table>

The query is for the A record of www.unixwiz.net.
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>src IP</td>
<td>192.26.92.30</td>
</tr>
<tr>
<td>dst IP</td>
<td>68.94.156.1</td>
</tr>
<tr>
<td>src port</td>
<td>53</td>
</tr>
<tr>
<td>dst port</td>
<td>5798</td>
</tr>
<tr>
<td>QR</td>
<td>1</td>
</tr>
<tr>
<td>AA</td>
<td>0</td>
</tr>
<tr>
<td>RA</td>
<td>0</td>
</tr>
<tr>
<td>QID</td>
<td>43561</td>
</tr>
<tr>
<td>Question</td>
<td>What is A record for <a href="http://www.unixwiz.net">www.unixwiz.net</a>?</td>
</tr>
<tr>
<td>Authority</td>
<td>2</td>
</tr>
<tr>
<td>Additional</td>
<td>2</td>
</tr>
<tr>
<td>ttl</td>
<td>120</td>
</tr>
</tbody>
</table>

**Response contains IP addr of next NS server (called “glue”)**

**Response ignored if unrecognized QueryID**
<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>
<tr>
<td>src port</td>
<td>5798</td>
</tr>
<tr>
<td>dst port</td>
<td>53</td>
</tr>
<tr>
<td>QID</td>
<td>43562</td>
</tr>
<tr>
<td>Question count</td>
<td>1</td>
</tr>
<tr>
<td>Answer count</td>
<td>0</td>
</tr>
<tr>
<td>Authority count</td>
<td>0</td>
</tr>
<tr>
<td>Additional Record count</td>
<td>0</td>
</tr>
</tbody>
</table>

**Question:** What is A record for www.unixwiz.net?
**bailiwick checking:**

Response is cached if it is within the same domain of query (i.e. *a.com* cannot set NS for *b.com*)
DNS Security

• What security checks are in place?
  – Random query ID’s to link responses to queries
  – Bailiwick checking (sanity check on response)
• No authentication
• Many things trust hostname↔IP mapping
  – Browser same-origin policy
  – URL address bar
  – Every application that accesses the internet
DNSsec

- Authenticated DNS protocol
- Used by TLDs :) 
- But no one else :( 

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Total Domains</th>
<th>DNSSEC Enabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>internet2</td>
<td>Internet2 Members</td>
<td>267</td>
<td>26 (9.7%)</td>
</tr>
<tr>
<td>esnet</td>
<td>ESNet community</td>
<td>11</td>
<td>9 (81.8%)</td>
</tr>
<tr>
<td>ivyleague</td>
<td>The Ivy League</td>
<td>8</td>
<td>1 (12.5%)</td>
</tr>
<tr>
<td>nysernet</td>
<td>NYSERNet members</td>
<td>30</td>
<td>0 (0.0%)</td>
</tr>
<tr>
<td>gigapop</td>
<td>Internet2 GigaPoPs</td>
<td>20</td>
<td>3 (15.0%)</td>
</tr>
<tr>
<td>usnews_20</td>
<td>US News Top 20 universities</td>
<td>20</td>
<td>2 (10.0%)</td>
</tr>
<tr>
<td>times_hied_50</td>
<td>Times Higher Ed Top 50</td>
<td>50</td>
<td>8 (16.0%)</td>
</tr>
<tr>
<td>techcom</td>
<td>Top Tech Companies</td>
<td>53</td>
<td>5 (9.4%)</td>
</tr>
<tr>
<td>tld</td>
<td>Top Level Domains</td>
<td>1272</td>
<td>1111 (87.3%)</td>
</tr>
<tr>
<td>new_gtld</td>
<td>New GTLD</td>
<td>957</td>
<td>957 (100.0%)</td>
</tr>
<tr>
<td>cc_tld</td>
<td>Country-Code Top Level Domains</td>
<td>292</td>
<td>137 (46.9%)</td>
</tr>
</tbody>
</table>

What are obvious problems?

- Corrupted nameservers
- Intercept & manipulate requests (on-path active attacker)
- Other obvious problems?
DNS cache poisoning

How might an attacker do this?
What security features must an attacker overcome?

- Packet spoofing
- Guess UDP port
- Guess QID

Assume SRC port spoofing
Assume predictable UDP port
QID=1000
IP for www.bankofsteve.com?

QID=1000
referral to ns1.bankofsteve.com

QID=1001
IP for www.bankofsteve.com?

QID=1001
IP = 10.1.1.1

Simultaneously

Forged answers:
IP = 10.9.9.99

QID=1000 - mismatch
QID=1001 - success!
QID=1002 - mismatch

www.bankofsteve.com is 10.9.9.99

IP for www.BankOfSteve.com?
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
- Good chance of success
Brazilian Boletos Stolen Through DNS Cache Poisoning

Crooks compromise DNS resolution of local ISP network

Feb 12, 2015 14:13 GMT · By Ionut Ilascu

Cybercriminals in Brazil have resorted to a new method to steal the much coveted boletos, a nation-wide payment method, by poisoning the domain name system (DNS) entry used by a bank’s website so that the IP address to the legitimate location point to a site controlled by the cybercriminals.

Boleto payments are highly popular in Brazil. They consist in a voucher generated by banks that can be used instead of payment cards. An expiration date is set for each of them, defining a time frame during which merchants can accept it.

When they expire, the customer can re-generate another one, with a different identification number, through online banking services.

When a website is accessed, its name is converted into its IP address by a DNS server maintained by the ISP (Internet Service Provider). If the DNS server is compromised, attackers can assign any website an address under their control, in order to point visitors to malicious content.
Defenses

- Query ID size is fixed at 16 bits
- Repeat each query with fresh Query ID
  - Doubles the space
- Randomize UDP ports
- DNSsec
  - Cryptographically sign DNS responses, verify via chain of trust from roots on down
- Other problems?
Phishing is common problem

• Typo squatting:
  • www.LansdEnd.com
  • www.goggle.com
  • secure.bank0fAmerica.com
  • wíkipedia.org
• Phishing attacks
  – Trick users into thinking a malicious domain name is the real one
ip routing
CIDR addressing

Prefixes used to setup hierarchical routing:
- An organization assigned a.b.c.d/x
- It manages addresses prefixed by a.b.c.d/x

Classless inter-domain routing (CIDR)
Network prefix
MSBs
Host address
x LSBs

...111001
10110... 1100011
ISP2
5.6.7.8
...111011
10110... 1110000
ISP1
backbone
10110... 1110011
10110... 1110000
Network prefix
MSBs
Host address
x LSBs
Autonomous systems (AS) are organizational building blocks
- Collection of IP prefixes under single routing policy
- wisc.edu
Within AS, might use RIP (Routing Information Protocol)
Between AS, use BGP (Border Gateway Protocol)
• **Stub:** connected to only one other AS
• **Multi-homed:** connected to multiple other AS
• **Transit:** routes traffic through its AS for other AS's
BGP and routing

wisc.edu

charter.net

BGP (exterior BGP)

defense.gov

OSPF within AS’s (Open shortest-path first)
Border Gateway Protocol (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 does not respond well to frequent node outages
2008: 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 via BGP
  - more specific, prefix hijacking
Internet thinks youtube.com is in Pakistan
Outage resolved in 2 hours...
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
recap

- DNS
  - DNS insecurity
  - DNS cache poisoning
  - Typosquatting

- CIDR, BGP
  - IP route hijacking

- Exit slips
  - 1 thing you learned
  - 1 thing you didn't understand