DNS Changer Update

[What was the US DoJ Victim Letter all about]

Update for the NANOG Security BoF
February 6, 2012

Merike Kaeo
merike@isc.org

What Is The DNS Changer Takedown ?

- The "DNS Changer" (aka ‘Ghost Click’) crew that has been hijacking your constituent's DNS configs were arrested, infrastructure seized, and a major data center shutdown.
- Law Enforcement Details:
  - http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911

What does DNS Changer Do?

- Installs malware on PCs and MACs, changes the DNS, and tries to reconfigure the home gateway's DNS.
- Points the DNS configurations to DNS resolvers in specific address blocks (see below) and use it for their criminal enterprise.

Home Routers

- Initial analysis show the following router types might be violated:
  - UTSTARCOM routers from BNSL (India)
  - D-Link
  - Linksys
  - OpenWRT/DD-WRT
  - A-Link
  - Netgear
  - ASUS ZVMODELVZ Web Manager
  - SMC
- No evidence of “changing code,” only config
- No evidence of changing the existing password.

Netblocks Involved

- IP Address Blocks:
  - 85.255.112.0/20 (85.255.112.0 through 85.255.127.255 /20)
  - 67.210.0.0/20 (67.210.0.0 through 67.210.15.255)
  - 93.188.160.0/21 (93.188.160.0 through 93.188.167.255)
  - 77.67.83.0/24 (77.67.83.0 through 77.67.83.255)
  - 213.109.64.0/20 (213.109.64.0 through 213.109.79.255)
  - 64.28.176.0/20 (64.28.176.0 through 64.28.191.255)

Initial Takedown Remediation

- As part of the operation, clean DNS resolvers under the control of the investigative team have replaced the criminal's DNS resolvers.
- All of your constituents who might be infected are now going to trusted DNS resolvers.
- Your customers might still be infected, but at least they are not going to rogue DNS server or having their DNS service stopped.
- This "DNS resolver replacement" was done to prevent customer's DNS from breaking and having a surge of help desk calls.

What's Happening to 'Bad' Netblocks

- All the involved netblocks are advertised as /24s to minimize risk of hijacking by the bad guys.

- All the involved netblocks are locked down at the RIRs (ARIN and RIPE). You will now see things like this:

```
remarks:
##############################################
remarks:        #Based on an order from the Dutch authorities #
remarks:        #changes to this record are not possible from #
remarks:        #8 November 2011 till 22 March 2012      #
remarks:
##############################################
```

What is Next?

- Remediation!
  - The industry is now working on remediation (cleaning up the malware).
  - Logs from the clean DNS resolvers with the SRC/DST IP addresses, ports, and time stamps are being fed to remediation groups.
  - ISPs should work with these groups to get feeds to see who in their ASes are infected and help remediate. List is located at: http://www.dcwg.org/cleanup.html
- The current court order has the clean DNS servers enabled until March 8, 2012

Tools to Clean Up Infections

- Analysis of the infected computers show that they have multiple infections with boot sector infections.
  - The infections varied over the past five years ranging from the “codex” infections (Zlob) to today’s Alureon.
- Unfortunately, this is not an easy "just use this tool to clean it up."
- The anti-malware community working on tools.

Monitoring

- If you have the ability, please enable Netflow and see what customer traffic may be communicating with the rogue netblocks.
- It might be a way to find more of the C&C and shutdown cyber-criminal infrastructure.
- If you see something, please contact an appropriate CSIRT team so that information can be passed to the security community for remediation.

Tools (Follow Vendor Instructions)

- NPE
  - http://security.symantec.com/nbrt/npe.aspx?lcid=1033
- TDSSKiller
  - http://support.kaspersky.com/faq/?qid=208280684
- fixmbr, Microsoft Recovery Console
  - http://support.microsoft.com/kb/314058
- Microsoft MSRT
  - http://support.microsoft.com/kb/890830
- FixTDSS
  - http://www.symantec.com/security_response/writeup.jsp?docid=2010-090608-3309-99
- McAfee Stinger
  - http://www.mcafee.com/us/downloads/free-tools/stinger.aspx
- Trend Micro Housecall
  - http://housecall.trendmicro.com

Register as a Victim!

- The FBI is working to collect as many victims as possible.
- Go to the FBI Site and let them know you were victimized:
  - http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911

Some More Links

- DNS Changer Infrastructure and TDSS/Alureon/ TidServ/TDL4 Malware
  - http://www.publicsafety.gc.ca/prg/em/ccirc/2011/in11-002-eng.aspx
- A video from sunbelt showing how DNS Changer works and what it does
  - http://www.youtube.com/watch?v=bzNQ0OxNX8E
- Wikipedia entry on the zlob family of malware
  - http://en.wikipedia.org/wiki/Zlob_trojan

Remediation So Far

- Lukewarm at best
- DoJ notification mistakes are a lesson learned for ENTIRE industry
  - Who you notify and how is not easy when potentially millions of global users involved
- Some global ISP are leaders in helping their customers and overall community
  - dealing with lots of cross functional groups and senior management who had to reach agreement
- Lots of FUD but reality is you make mistake, learn, improve, move forward…

If You Do NOT Help with Remediation

- When ISC DNS Servers no longer available
  - The infection remains, and alurion is capable of downloading other plugins beyond just DNS-Changer.
  - Anyone who redirects routes from the involved IP blocks at a regional (non-monitored) level will have a ready supply of DNS victims, and such attacks may not be on ad sales alone. (bank or social or online services URL jacking.)
  - If this address space is later reassigned then the new operator of this space is going to see far more "internet background radiation" than is normal -- so this is a toxic waste dump.
- Should you act on the victim notification letter?

Positive ISP Lessons Learned

- Some ISPs have gone through learning curve and next time the processes are in place
  - Do you have a process in place?
- Why haven't folks been doing this before?
  - No one to force issue
- Recent trends are to participate in self-regulation efforts
- Senior management type people who need to buy are more cognizant of criticality for business
  - Reputation
  - Avoiding down time and user calls

Still To Figure Out

- RIR Policy issues for what to do with bad address space
- March 8, 2012 is when court ordered ISC run DNS servers (as appointed by court order) will no longer be available – what happens to non remediated devices?
- What are YOUR next steps?