Introducing:
The ORDINAL Dataset

Operational Research Data from Internet NAmespace Logs

DNS Namespace Collisions: a (very) quick history

- As old as the DNS itself
- Researched since ~2003
- New interest related to ICANN's new gTLD Program
- Result when resolving party is other than the one anticipated
- "Squatting" and "drop catching" seek to leverage collisions
- Machine-to-machine traffic is more interesting
- Exacerbated by complex/aggressive DNS search path processing
- Misuse of the DNS for Authentication

(known) Violators that Misuse the DNS for Authentication (1)

Protocols/Applications that lack server authentication

- Server authentication is hard, think https/tls/x.509, and ssh
- Especially in scenarios where there is no pre-existing trust
- Legacy protocols (FTP, POP, etc) mostly punt

SMTP

- Identification by DNS MX record; no cryptographic authentication
- Few use SMTP over TLS to add cryptographic authentication (used for transp
- Most email honeypots leverage this behavior

(known) Violators that Misuse the DNS for Authentication (2)

Microsoft Active Directory, SMB/CIFS

- Active Directory namespaces are DNS namespaces
- Locates URL/UNC resources via DNS; trusts the response (!!)
- \\SYSVOL, \\NETLOGON (!!)
- \\users\jschmidt and *smb://users/jschmidt*
- SMB/CIFS will downgrade to WebDAV over http (SharePoint) (!!)
- Crux of JASBUG/CVE_2015_0008/MS15-011,014
- Trivially exploitable (Responder and SMBRelay)
- Microsoft's response, SMB Signing, adds cryptographic authentication
- "PROPFIND /USERS/michaelw HTTP/1.1" 405 240 "-" "Microsoft-WebDAV-MiniRedir/10.0.10586"
- "PROPFIND /SYSVOL/XXX/Policies/%7B87DF. . . 48FA9EC%7D HTTP/1.1" 405 293 "-" "Microsoft-WebDAV-Mi 6.1.7601"

(known) Violators that Misuse the DNS for Authentication (3)

Microsoft Distributed File System (DFS)

- DFS Namespaces are DNS Namespaces
- "PROPFIND /DFSRoot02/05_0139/10_General/30_Communication/02_Management_People/info%20in%20verband%20met%20nieuwe%20CAT%20systeem%20in%20EMS HTTP/1.1" 405 338 "-" "Microsoft-WebDAV-MiniR 6.1.7601"

WPAD

- http://wpad.microsoft.com/wpad.dat (and iterations/subdomains)
- No authentication; very bad; trivially exploitable (Responder has a module)
- "GET /wpad.dat HTTP/1.1" 404 206 "-" "WinHttp-Autoproxy-Service/5.1"

(known) Violators that Misuse the DNS for Authentication (4)

Microsoft System Center Configuration Manager (SCCM)

- Formerly Systems Management Server (SMS); widely deployed
- Uses http and custom method: CCM_POST
- No discernable server authentication
- "CCM_POST /ccm_system/request HTTP/1.1" 501 214 "-" "ccmhttp"
- "GET /SMS_MP/.sms_aut?SITESIGNCERT HTTP/1.1" 404 213 "-" "SMS CCM 5.0"
- "HEAD /SMS_DP_SMSPKG$/4885f087-977b-4a79-b1b6-e4370a25492c HTTP/1.1 "-" "SMS CCM 5.0"

Microsoft "OutlookAnywhere"

- Uses http and custom methods: RPC_IN_DATA, RPC_OUT_DATA
- "RPC_IN_DATA /rpc/rpcproxy.dll?d89b673c-38b0-483c-b906-89e992c88c12@XXX.com:6001 HT 501 215 "-" "MSRPC"
- "RPC_OUT_DATA /rpc/rpcproxy.dll?d89b673c-38b0-483c-b906-89e992c88c12@XXX.com:6001 1.1" 501 216 "-" "MSRPC"
- No discernable server authentication

(known) Violators that Misuse the DNS for Authentication (5)

Other/Custom Applications

- "GET /system/transSession.asp?loginusername=KylieXXX&ucomp=01&sysnar
  Freight%20Payment%20System HTTP/1.1" 404 221 "http://
  epayment.XXX.corp.com/system/login.aspx" "Mozilla/5.0 (Windows NT 6.1;
  WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 S
  537.36"

- "GET /sm_login/sm_login.asp?user_
  id=phemingXXX&password=<muchsadness>&ismd5=1&app_id=cmwin
  19.45.1602.0&timeout=30 HTTP/1.1" 404 219 "-" "-"

(known) Violators that Misuse the DNS for Authentication (6)

Just plain Evil

- "PROPFIND /SysVol/XXX.corp.com/scripts/IR/IRD/ChangePassword.vbs HTTP/1.1" 4
"-" "Microsoft-WebDAV-MiniRedir/6.1.7600”
- "PROPFIND /it/Installs/Work%20Station/Standard%20Applications/GPINSTALL/Loca
%20Admin%20Password%20Change HTTP/1.1" 405 310 "-”
- "PROPFIND /home/deebXXX/passwords/keepass HTTP/1.1" 405 257 "-”
- "GET /Citrix/XenApp/site/changepassword.aspx HTTP/1.1" 404 236 "-" "Mozilla/5.0
CPU iPhone OS 7_0 like Mac OS X)
- “PROPFIND /Wallpaper/SCREENSAVER.jpg HTTP/1.1 "-”

Say it with me:

DNS is for Identification

NOT

Authentication

(no, DNSSEC doesn't solve this problem)

What is in the ORDINAL Dataset

CORP.COM
02PROXY.COM
ANAMS1.COM
ANAMS2.COM
ANAMS3.COM
ANAMS4.COM
ANAMS5.COM
ANAMS6.COM
DEFAULT-FIRST-SITE-NAME.COM

- IISPROXY.COM
- LVFS1-2K.COM
- OAUTHPROXY.COM
- SIPEXTERNAL.NET
- SIPINTERNAL.NET
- VLAN01.COM
- VLAN101.COM
- VLAN141.COM
- VLAN142.COM
- VLAN143.COM
- VLAN144.COM
- VLAN145.COM
- VLAN400.COM
- VLAN403.COM
- VLAN404.COM
- VLANB.COM
- WNADROOT.COM

(And There's More!)

DNS Search Path ala Microsoft

"Devolution is a Windows DNS client feature. Devolution is the process by which Windows DNS clients resolve DNS queries for single-label unqualified hostnames. Queries are constructed by appending PDS to the hostname. The query is retried by systematically removing the left-most label in the PDS until the hostname + remaining PDS resolves or only two labels remain in the stripped PDS. For example, Windows clients looking for "Single-label" in the western.corp.contoso.co.us domain will progressively query Single-label.western.corp.contoso.co.us, Single-label.corp.contoso.co.us, Single-label.contoso.co.us, and then Single-label.co.us until it finds a system that resolves. This process is referred to as devolution."

- Microsoft

(https://technet.microsoft.com/library/security/971888

Why some names (corp.com) are special

Microsoft long ago suggested folks name Active Directories “CORP”

AD hosts and resources have DNS records : <stuff>.corp

SRV qnames we see at corp.com (among millions of others):

- _kerberos._tcp.dc._msdcs.Fareast.Microsoft.corp.com
- _kerberos._tcp.dc._msdcs.redmond.microsoft.corp.com
- _kerberos._tcp.NA-WA-EXCH._sites.dc._msdcs.Fareast.Microsoft.corp.com
- _kerberos._tcp.NA-WA-RED._sites.dc._msdcs.redmond.microsoft.corp.com
- _ldap._tcp.dc._msdcs.middleeast.microsoft.corp.com
- _ldap._tcp.dc._msdcs.redmond.microsoft.corp.com
- _ldap._tcp.microsoft.corp.com
- _ldap._tcp.NA-WA-RED._sites.microsoft.corp.com

More qnames we actually see at corp.com
(just for fun)

wpad.partners.microsoft.corp.com

wpad.redmond.microsoft.corp.com

boxcontroltower.microsoft.corp.com

satap.redmond.microsoft.corp.com

gproxy.northamerica.microsoft.corp.com

gproxy.redmond.microsoft.corp.com

UCIS-CXXX.redmond.microsoft.corp.com

UnifiedSearchCube.partners.microsoft.corp.com

A few stats… one month in 2016

Unique v4 IP addresses sending DNS queries to corp.com authoritative DNS nameservers	**182,612** (Mainly from public and corporate recursives)
Unique v4 IP addresses requesting WPAD configurations from the HTTP server hosted at corp.com	**379,403** (IPs of specific end machines received over HTTP)
Unique v4 IP addresses requesting information from the HTTP/WebDAV server hosted at corp.com related to NETLOGON or SYSVOL – the most dangerous items as described in MS15- 011/014	**75,272** (IPs of specific end machines received over HTTP)
Unique v4 IP addresses requesting information from the HTTP/WebDAV server hosted at corp.com related to USERS – home directory file system mounts	**27,051** (IPs of specific end machines received over HTTP)
Unique v4 IP addresses sending ns1.labs.jasadvisors.com unsolicited DNS UPDATE queries	**140,643** (Mainly IPs specific Microsoft Active Directory Member Machines taken off-site)
Volume of email received per day	**~ 2.5 GB** (Some spam/phishing, some not)

What do we collect in the ORDINAL Dataset

- DNS querylogs (named logs)
- Email metadata (verbose Postfix logs)
- Email delivered to the domain (maildir/ format)
- Port 80 and 443 requests (httpd log)
- Pcaps
- Source IP addresses (hashed where possible)
- IPv4 and IPv6 served here
- Open to running experiments (based on risk assessment)

What do we hope to accomplish?

- Raise awareness of the ”Misuse of the DNS for authentication” issue
- Improve protocol and application design
- Help software vendors identify and fix problems
- Help system administrators identify and fix problems
- Provide data to spam/phishing/malware researchers

How to access the data

- All access via DHS S&T IMPACT Program
- Vetted researchers only
- Commitment from researcher to publish and otherwise “Better the Internet”
- ordinal-dataset@jasadvisors.com
- https://ordinal.jasadvisors.com