DNS Data Exfiltration
Gianluca Silvestri, System Engineer - Exclusive Networks Italy
15/03/2017
Infoblox Solutions

Core Network Services

DNS, DHCP, Authoritative IPAM
Integrated DDI for physical and virtual environments

Secure DNS

External & Internal DNS Security
Threat visibility, protection, and response

Cloud Network Automation

DDI Cloud Automation & Visibility
Provisioning critical network services for cloud deployments

Centralized Management
Patented Grid™ Technology
Reporting and Analytics
Why is DNS an Ideal Target?

- DNS is the cornerstone of the Internet used by every business and government.
- DNS as a protocol is easy to exploit.
- Traditional protection is ineffective against evolving threats.

DNS Outage = Business Downtime
DNS is #1 protocol during 1st 60 Seconds of Malware

“There are no surprises in the top protocols used. Just over 15,000 samples utilized DNS. It makes sense a majority of the samples utilize DNS to locate their [malicious home] network resources. This provides resiliency to their network and allows them to utilize techniques such as fast-flux networks”
APT/Malware uses DNS as Control Plane
Easy to Let in, Touch to Get Out

91%
Of malware uses DNS to carry out campaigns¹

431M
New unique pieces of malware in 2015²

#1
Malware C&C is #1 responsible vector for crimeware³

- Intruders rely on DNS to infect devices, propagate malware and exfiltrate data
- Malware is designed to spread, morph and hide within your IT infrastructure
- Longer it takes to discover, the higher the cost of damage

DNS query

- DNS needs to pass through Firewalls
- This leaves a big security gap in your defensive strategy
Need to ungroup and rotate text, add question text and reformat some text boxes, realign lines and regroup.
Motion of Malware through Networks: “PIE”

APT/malware uses DNS at every stage

**Penetration**
Query malicious domains and report to C&C

**Infection**
Download malware to the infected host

**Exfiltration**
Transport the data offsite

![Diagram showing the motion of malware through networks: Penetration, Infection, Exfiltration, with DNS server and End-User Host.]
DNS - Leading Culprit for Data Exfiltration

One Byte is Too Much

$3.8M

46%

45%

• DNS tunnels are commonly used to send sensitive information out
• Data can also be exfiltrated by embedding it directly in DNS queries

1. Source: Ponemon Institute, 2015 Cost of Data Breach Study
Exfiltrating Data via DNS Tunneling

- Uses DNS as a covert communication channel to bypass firewalls
- Attacker tunnels other protocols like SSH, or web within DNS
- Enables attackers to easily insert malware, pass stolen data or tunnel IP traffic without detection
- A DNS tunnel can be used as a full remote-control channel for a compromised internal host

Examples:
- Iodine
- OzymanDNS
- SplitBrain
- DNS2TCP
Using Signatures to Detect Tunneling

- Implemented in Advanced DNS Protection
- Most standard DNS Tunneling toolkits (like Iodine) have well known signatures
- Infoblox Internal DNS Security has 12 different threat protection rules that use these signatures to detect tunneling attempts
- Allows immediate blocking without any thresholds
- As new signatures become available, customers get automatic updates through the threat intelligence service
  - OzymanDNS
  - SplitBrain
  - DNS2TCP
Data Exfiltration over DNS Queries
Malware Steals File Containing Sensitive Data

- Infected endpoint gets access to file containing sensitive data
- It encrypts and converts info into encoded format
- Text broken into chunks and sent via DNS using hostname.subdomain or TXT records
- Exfiltrated data reconstructed at the other end
- Can use spoofed addresses to avoid detection
Examples of data exfiltration

100000ff51cf3f640038c742012057c038c742405.notashutin.com
8b0211040037508b0a01040005860d0b8400ff51c04f6400ff51d0db84008b8c.notashutin.com
42411000008e24863000184c8110000000c8cccccccccccccccccccccccccccccccc.notashutin.com
b844424065b84742c07c6000000001887c00010000005781b80401388fb1475.notashutin.com
388f9057b08e0abd40007c6010000000e52c8000cccccccccccccccccccccccccccc.notashutin.com
65b8474280586f47d2b84442c0580c4752b844210184542411565a6f05a60.notashutin.com
25667c600000ff518f64007fb8d10c326ce52c0100330ce52c0100cccccccccccc.notashutin.com
8bcd7f64003c00cccccccccccccccccccccccccccccccccccccccccccccccccccccccc.notashutin.com
e59e1e6b4000cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc.notashutin.com
058e83086000cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc.notashutin.com
72vVDE6L0g3orDtdzmUqIDKVW3CihcDh77gHhzATHLYxPlUtyn.com
kgTfHv3FBSyUs6B8iOqFkQEgSOBbOzTwc2EqBw ygJx21YNGIQE.y.com
HkBOcoGWSRDFa43NyrtTF3kgWAqGqsycpawyDA6Rxqm1OAR6P.y.com
NvX8PtEA75yAXnR2KtnoKprQJRhs75CsdTge0dnKPntsDXk0cN.y.com
rTNmolUwp1yW8AOPIUbdEwkuYuKfCrSOwGme3AWTWFJcbVsWY.com
NZrhKG2KQNP1Ya2QY6k5xuimLeFE76krZ0j1XlywoSe6DVGrX.y.com
UTuOhSTxDxLISGTs14WLPjradQztKFHnRTSVW6yoyIB04AzSQ.y.com
6X6YXk0VDG6Ud6vsYsk6iFup7cnqW23LigxMRFmm0zo8w52Vhg.y.com
TMDT18cMKREkOxcm1aQdDXHqE2K1g3LeLiUbnDW8RKRbBxfv.y.com
XoBmOzQ6fQghkKQRBDnzBiiY9v1u2KPWokQUjOZerhRXM89dta.y.com
Not Examples of DNS Tunneling

VDCPENDEP001.kdc.capitalone.com
KDCPENDEPO02.cof.ds.capitalone.com
MDCPENDEP002.dqa.capitalone.com
MDCPENDEP002.osd.dev.capitalone.com
latency_check.perftest_latency9u16190.n1.netalyzr.icsi.berkeley.edu
latency-set.perftest-latency3u16190.n1.netalyzr.icsi.berkeley.edu
ir5soq-bn1305.files.1drv.com
ir5wew-bn1305.files.1drv.com
ir5wew-bn1305.files.1drv.com
0.data.fantlab.ru_-.images_-.editions_-.small_-.112413.6250.ko-146501.url.esoft.com
0.data.fantlab.ru_-.images_-.editions_-.small_-.121387.6250.ko-146501.url.esoft.com
0.data.fantlab.ru_-.images_-.editions_-.small_-.127370.6250.ko-146501.url.esoft.com
How DNS Threat Insight Works

- Looks at payload: hostname.subdomain, TXT records, A, AAAA records
- Uses sophisticated and complex Analytics algorithms
- Certain attributes add to a threat score, others subtract from it
- All attributes are evaluated and weighted
- After all attributes are evaluated, a final score will classify a request as exfiltration or not
- If the finding is exfiltration, the destination DNS server is added to a special RPZ zone in the Infoblox DNS Firewall that contains the block, log, redirect policy
Tools to Exfiltrate Data via DNS & Infoblox DNS Threat Insight Demonstration
DNS Data Exfiltration Portal
You receive an invitation email from your Infoblox Channel Partner to use

WARNING – YOU WILL BE MOVING DATA OUT THE NETWORK!!!
Data Exfiltration Demo Portal
There are three tools that you can use to exfiltrate data via DNS queries

Example: DNS text Decoder tool
Simply hex encodes your text and formats it into DNS query commands for you to cut and paste in shell/command prompt

Step 1: An infected endpoint has access to company data.
Step 2: Malware encodes the data, breaks it into chunks and sends it out as DNS queries.
Step 3: The encoded queries are logged and re-assembled on the far end.
Data Exfiltration Demo Portal – Hexify Tool

https to portal to download file by clicking on View the file
Data Exfiltration Demo

Internet

dex.infoblox.com

Internet Firewall

External Recursion

Virtual Infoblox DNS Server (VMware)

DNS Packet Query Flow

VPN to Test Lab Environment

Recursive Layer

Turn Threat Insight DNS Analytics ON/OFF

VPN Server
What should be your course of action?

“Something is better than nothing”
“Addressing priorities does not mean striving for perfection, but rather ensuring, at least, that critical exposures are remediated.”*  

*Gartner 2016*
“Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms. All organizations should now assume that they are in a state of continuous compromise.”

*Neil MacDonald and Peter Firstbrook Designing an Adaptive Security Architecture for Protection From Advanced Attacks (Gartner)
DNS Security Solution

Common Concerns:

- Avoid Outages/Downtime
- Reputation and Brand Protection against breach
- Compliance – HIPPA, PCI, other

Risks

- Port 53 may be wide open or limited to only select DNS servers
- No inspection/enforcement of data loss through port 53 using typical DNS platforms (Microsoft, BIND)
- Limited capability to prevent establishing communication with known malware
Internal DNS Security Deployment

Secure DNS Proxy

Internal users query internal DNS which forwards to a secure cache proxy

- Port 53 filtered to allow only select internal systems to forward to Secure DNS Proxy
- Internal queries all handled inside the protected areas of the network
- Client identification of possible infected/compromised systems possible
- Local enforcement of port 53 protection policies possible

- Port 53 filtered to allow only the Secure DNS proxy to request external resolution
- Ideal choke point for behavior and signature-based port 53 protection
- Last opportunity for reputation-based port 53 protection

App Offerings
Salesforce.com
Office 365
Workday – HR
SAP
Infoblox Secure DNS

Protect Your DNS Infrastructure

Detect & Find Infected Devices

Prevent Data Exfiltration
Infoblox SPIFF Program

Our new SPIFF Program rewards partners that identify new opportunities with new & existing customers, through initiating Security Assessments or Data Exfiltration (DEX) Demos.

<table>
<thead>
<tr>
<th>What Qualifies?</th>
<th>Activity Type</th>
<th>End Customer Company Size</th>
<th>Opportunity Creation Incentive Via Amazon e-gift card</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Opportunities</td>
<td>Security Assessment OR DEX Demo</td>
<td>1,000 + employees</td>
<td>300 USD</td>
</tr>
<tr>
<td>New or Existing</td>
<td></td>
<td>5,000+ employees</td>
<td>600 USD</td>
</tr>
<tr>
<td>Customers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Submit your SPIFF Claim today via Partner Central!

https://infoblox-partners.force.com/partners/sitelogin
Q&A
or
Thank you