ATTACKS/BREACHES

6/12/2014
12:00 PM

Dave Piscitello

Connect Directly

3 COMMENTS
COMMENT NOW

Login

0% 100%

EDUCATIONAL RESOURCES

Monitor DNS Traffic & You Just Might Catch A RAT

Criminals will exploit any Internet service or protocol when given the opportunity. Here are six signs of suspicious activity to watch for in the DNS.

IT admins have the thankless task of having to watchdog devices, hosts, and networks for signs of malicious activity. Host intrusion detection and endpoint protection may be “must have” security measures for many organizations, but there’s nothing like monitoring DNS traffic if you’re looking to expose a RAT, rootkit, APT, or other malware that’s taken residence on your networks.

Why DNS?

Criminals will exploit any Internet service or protocol when given the opportunity, and this includes the DNS. They register disposable domain names for spam campaigns and botnet administration, and they use compromised domains to host phishing or malware downloads. They inject malicious queries to exploit name servers or disrupt name resolution. They inject crafty responses to poison resolver caches or amplify denial of service attacks. They even use DNS as a covert channel for data exfiltration or

malware updates.

You may not be able to keep pace with every new DNS exploitation but you can be proactive by using firewalls, network IDS, or name resolvers to report certain indicators of suspicious DNS activity.

What are you looking for?
DNS query composition or traffic patterns offer signs that suspicious or malicious activity is emanating from your networks. For example:

DNS queries from spoofed source addresses or addresses that you have not authorized for use but are not egress filtering especially when observed in conjunction with unusually high DNS query volume or DNS queries that use TCP rather than UDP) may indicate that infected hosts on your network are engaged in a DDoS attack.

Malformed DNS queries may be symptomatic of a vulnerability exploitation attack against the name server or resolver identified by the destination IP address. They may also indicate that you have incorrectly operating devices on your network. The causes for problems of these kinds may be malware or unsuccessful attempts to remove malware.

DNS queries that request name resolution of known malicious domains or names with characteristics common to domain generation algorithms (DGA) associated with criminal botnets and queries to resolvers that you did not

authorize for use in many cases are dead giveaway indicators of infected hosts on your networks.

DNS responses also offer signs that suspicious or malicious data are being delivered to hosts on your networks. For example,length or composition characteristics of DNS responses can reveal malicious or criminal intent. For example, the response messages are abnormally large (amplification attack) or the Answer or Additional Sections of the response message are suspicious (cache poisoning, covert channel).

DNS responses for your own portfolio of domains that are resolving to IP addresses that are different from what you published in your authoritative zones, responses from name servers that you did not authorize to host your zone, and positive responses to names in your zones that should resolve to name error (NXDOMAIN) may indicate a domain name or registration account hijacking or DNS response modification.

DNS responses from suspicious IP addresses, e.g., addresses from IP blocks allocated to broadband access network, DNS traffic appearing on non standard port, unusually high number of response messages that resolve domains with short Times to Live (TTL) or unusually high number of responses containing "name error"

(NXDOMAIN) are often indicators of botnet-controlled, infected hosts running malware.

Various forms of DNS monitoring can expose these threats, many in real time. In my next blog, I'll look at how you can implement mechanisms to detect these at Internet firewalls, using network intrusion systems, traffic analysis, or log data.

Dave Piscitello has been involved with Internet technologies (broadband access, routing, network management, and security) for over 35 years. He left private sector consulting and his company, Core Competence, to provide security and ICT coordination for security and policy ... *View Full Bio*

COMMENT | EMAIL THIS | PRINT | RSS

MORE INSIGHTS

Webcasts

- Enterprise Mobile Security Report 2016: From the Front Lines
- Surviving 2016: Protecting Your Business From Advanced Cyber Threats

MORE WEBCASTS

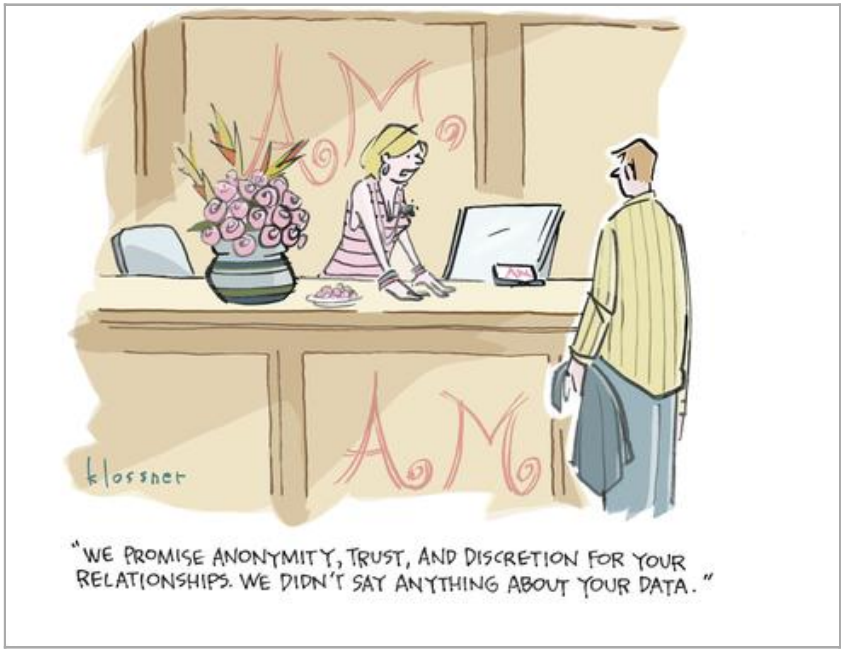
White Papers

- The New BYOD: Best Practices for a Productive BYOD Program
- Negotiating with Cybercriminals

MORE WHITE PAPERS

Reports

- The Forrester Wave:



Latest Comment: nice one good

CARTOON ARCHIVE

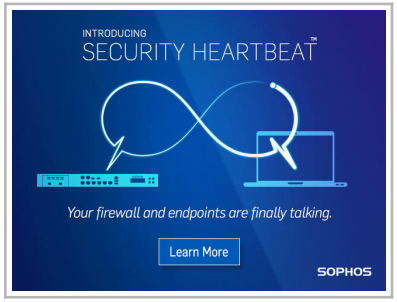
CURRENT ISSUE

Digital Experience Platforms, Q4 2015

- [InformationWeek & Dark Reading Report] 2015 Strategic Security Survey Results

MORE REPORTS

SPONSORED CONTENT



Introducing Sophos Security Heartbeat

Synchronized Security links network and endpoint security to deliver unparalleled protection by automating threat discovery, analysis and response. With synchronized security you can get better protection from advanced threats and significantly reduce the time and complexity of responding to security incidents. Are you ready to join the revolution?

Sponsored by SOPHOS

COMMENTS

NEWEST FIRST | OLDEST FIRST | THREADED VIEW

Randy Naramore,
User Rank: Ninja
6/16/2014 | 3:21:34 PM

Login

E-Commerce Security: What Every Enterprise Needs to Know

The mainstream use of EMV smartcards in the US has experts predicting an increase in online fraud. Organizations will need to look at new tools and processes for building better breach detection and response capabilities.

DOWNLOAD THIS ISSUE!

BACK ISSUES | MUST READS

FLASH POLL

What's missing from your incident response plan? (Pick all that apply.)

- ☐ Access to activity logs
- ☐ An up-to-date network diagram
- ☐ Blueprint for public disclosure
- ☐ Hostname-IP address maps
- ☐ IR fire drills before the event
- ☐ Plan for finding malicious files after the breach
- ☐ We don't have an incident response plan
- ☐ Other (Please explain in the comments)

Submit

100% 0%

Re: Know Your Enemy
Very interesting post, DNS is the key to discovering your network. If hackers can get to the DNS servers perform a transfer then you are had. This is the reason DNS is not allowed in controlled environments such as DMZ's. The specific tool set you mentioned (Kali-Linux) is a good one indeed.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

Robert McDougal,
User Rank: Ninja
6/13/2014 | 4:09:26 PM

Login
100% 0%

Re: Know Your Enemy
Very good points Christian! I would like to add that Nagios provides a plugin for DNS monitoring as well.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

Christian Bryant,
User Rank: Ninja
6/12/2014 | 1:00:52 PM

Login
100% 0%

Know Your Enemy
I try not to name specific tools unless I'm doing an analysis, but for Enterprise-level network monitoring I rather prefer OpenNMS network management application platform and Nagios IT monitoring with its solid DNS monitoring solution. But I have to say to all network engineers, also grab a copy of a penetration

ALL POLLS

SLIDESHOWS

The Internet of Private 'Things'

testing distribution like Kali Linux and understand what cyber criminals are looking for, how they search for it, and what the raw data and DNS traffic looks like. With highly configurable DNS monitoring tools, you can start tailoring the monitoring to specific types of traffic (if the tool isn't already - Nagios is pretty hefty in that regard) based upon your research. With tips like the ones in this article, some first-hand experience and solid tools, you will maintain a more secure network environment.

REPLY | POST MESSAGE | MESSAGES LIST | START A BOARD

1 COMMENTS | READ | POST A COMMENT

Boldest Cybersecurity Predictions For 2016 5

Tech Gifts That Security Pros Will Probably Return 0 COMMENTS

MORE SLIDESHOWS

TWITTER FEED

Tweets about "from:DarkReading OR @DarkReading OR #DarkReading"

BUG REPORT

ENTERPRISE VULNERABILITIES
From DHS/US-CERT's National Vulnerability Database

- **CVE-2013-7445**
  PUBLISHED: 2015-10-15
  The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles requests for Graphics Execution Manager (GEM) objects, which allows context-dependent attackers to cause a denial of service (memory consumption) via an application that processes graphics data, as demonstrated b...

- **CVE-2015-4948**
  PUBLISHED: 2015-10-15
  netstat in IBM AIX 5.3, 6.1, and 7.1 and VIOS 2.2.x, when a fibre channel adapter is used, allows local users to gain privileges via unspecified vectors.

- **CVE-2015-5660**

PUBLISHED: 2015-10-15

Cross-site request forgery (CSRF) vulnerability in eXtplorer before 2.1.8 allows remote attackers to hijack the authentication of arbitrary users for requests that execute PHP code.

- **CVE-2015-6003**

PUBLISHED: 2015-10-15

Directory traversal vulnerability in QNAP QTS before 4.1.4 build 0910 and 4.2.x before 4.2.0 RC2 build 0910, when AFP is enabled, allows remote attackers to read or write to arbitrary files by leveraging access to an OS X (1) user or (2) guest account.

- **CVE-2015-6333**

PUBLISHED: 2015-10-15

Cisco Application Policy Infrastructure Controller (APIC) 1.1j allows local users to gain privileges via vectors involving addition of an SSH key, aka Bug ID CSCuw46076.

DARK READING RADIO

Archived Dark Reading Radio

The Changing Role of the Chief Information Security Officer

Join Dark Reading community editor Marilyn Cohodas in a thought-provoking discussion about the evolving role of the CISO.

FULL SCHEDULE | ARCHIVED SHOWS

InformationWeek DARKReading

ABOUT US
CONTACT US
CUSTOMER SUPPORT
SITEMAP
REPRINTS

TWITTER
FACEBOOK
LINKEDIN
GOOGLE+
RSS

UBM

UBM TECH BRANDS

Black Hat
Cloud Connect
Dark Reading
Enterprise Connect
Fusion
GDC
GTEC
Gamasutra
HDI
InformationWeek
Interop
Network Computing
No Jitter
Tower & Small Cell Summit

COMMUNITIES SERVED

Enterprise IT
Enterprise Communications
Game Development
Information Security
IT Services & Support

WORKING WITH US

Advertising Contacts
Event Calendar
Tech Marketing
Solutions
Contact Us
Licensing