Infoblox DNS Firewall Evaluation

Gregor

2,052
Queries analyzed from the traffic capture

28
Suspicious queries found by DNS Firewall (0.39%)

This traffic is associated with:
14 Critical Threats (50 hits)
7 Moderate Threats (43 hits)
12 Minor Threats (63 hits)

Critical threats found - use DNS Firewall to protect your DNS queries.

8 Unique Suspicious Destinations:

go to **Threat Descriptions**
go to **Reputation Feeds**

Destination IP / Network	Destination Domain	Threat Level	Occurrences	Threat Categories
112.78.0.0/20	blackhorsemodel.com.vn	Critical	1	Advanced-ru, Web attackers, Zeus, Advanced, Alienvault, Botnets-ru, Botnets, Finshun, Unix server-ru, Alienvaultscanspam, Unix server, Community, Phishtank, Dshield block list, China, Dshield top 4000, Ssh crackers, Autoshun, Modified itar, Denyhosts, Vietnam, Itar
117.121.0.0/17	cm.ipinyou.com	Critical	1	Advanced, Alienvault, Advanced-ru, Alienvaultscanspam, Unix server, Unix server-ru, Itar, Denyhosts, Autoshun, Modified itar, Ssh crackers, Dshield top 4000, China
203.162.0.0/16	ns1.matbao.vn	Critical	1	Advanced-ru, Web attackers, Alienvault, Advanced, Finshun, Unix server-ru, Alienvaultscanspam, Unix server, Community, Phishtank, Dshield block list, Dshield top 4000, Autoshun, Vietnam, Itar, Denyhosts
211.80.0.0/12	bae.jomodns.com	Critical	2	Alienvault, Advanced, Advanced-ru, Community, Dshield block list, Unix server-ru, Alienvaultscanspam, Unix server, Russian business network, Autoshun, Modified itar, Denyhosts, Itar, China, Parasites, Dshield top 4000, Ssh crackers
61.128.0.0/10	hm.e.shifen.com	Critical	4	Web attackers, Basic, Advanced-ru, Dshield top 10, Basic-ru, Botnets, Shell shock attackers, Finshun, Zeus, Botnets-ru, Advanced, Alienvault, Shadowserver, Alienvaultscanspam, Unix server, Russian business network, Unix server-ru, Community, Phishtank, Dshield block list, Ssh crackers, Voip abuse, China, Dshield top 4000, Parasites, Denyhosts, Malware domain list, Itar, Autoshun, Modified itar
115.224.0.0/12	static.n.shifen.com	Critical	3	Advanced, Alienvault, Botnets, Tscritical general , Basic-ru, Finshun, Dshield top 10, Advanced-ru, Basic, Web attackers, Dshield block list, Phishtank, Community, Unix server-ru, Unix server, Alienvaultscanspam, Russian business network, Modified itar, Autoshun, Denyhosts, Itar, Spamhaus edrop, Malware domain list, China, Parasites, Dshield top 4000, Ssh crackers, Voip abuse
123.112.0.0/12	fe.lvyou.n.shifen.com	Critical	7	Web attackers, Advanced-ru, Finshun, Alienvault, Advanced, Russian business network, Alienvaultscanspam, Unix server, Unix server-ru, Community, Dshield block list, Voip abuse, Ssh crackers, Dshield top 4000, Parasites, China, Itar, Denyhosts, Autoshun, Modified itar
180.76.0.0/14	hiphotos.wshifen.com	Critical	9	Advanced, Finshun, Advanced-ru, Unix server-ru, Unix server, Modified itar, Itar, Denyhosts, Dshield top 4000, China

33 Unique Threat Categories:

go to **Suspicious Destinations**
go to **Reputation Feeds**

Threat Category	Threat Level	Occurrences	Description
Advanced	Critical	8	IP addresses identified as a currently active source of malware, network attacks, fast-flux botnets, crime hosting networks, phishing and browser hijacking sites or as a member of the current Cymru Bogon List.
Advanced-ru	Critical	8	IP addresses identified as a currently active source of malware, network attacks, fast-flux botnets, crime hosting networks, phishing and browser hijacking sites or as a member of the current Cymru Bogon List.
Alienvault	Critical	7	IP addresses identified as AlienVault Malware Droppers and Botnet C2 insfrastructure
Alienvaultscanspam	Moderate	7	List of ip addresses and networks detected as scanning for vulnerabilities or sending spam by AlienVault's Open Threat Exchange program. These addresses are normally a problem for servers but outbound contacts to these IP addresses is also suspicious.
Autoshun	Minor	7	Currently active attacker (generally against servers)
Basic	Critical	2	IP addresses that are the worst current sources of attacks, spam, and malware, as well as currently active Botnet Command and Control servers. If a system inside your network attempts to connect out to these addresses, it is most likely infected with malware and needs to be cleaned.
Basic-ru	Critical	2	IP addresses that are the worst current sources of attacks, spam, and malware, as well as currently active Botnet Command and Control servers. If a system inside your network attempts to connect out to these addresses, it is most likely infected with malware and needs to be cleaned.
Botnets	Critical	3	IP addresses of known active C&C addresses of major botnets such as ZeuS and SpyEye. If a system inside your network attempts to connect out to these addresses, it is most likely infected with malware and needs to be cleaned.
Botnets-ru	Critical	2	IP addresses of known active C&C addresses of major botnets such as ZeuS and SpyEye. If a system inside your network attempts to connect out to these addresses, it is most likely infected with malware and needs to be cleaned.
China	Minor	7	IP addresses in the Peoples Republic of China
Community	Moderate	6	The worst IP addresses and subnets according to DShield
Denyhosts	Minor	8	Attackers of linux/unix servers
Dshield block list	Moderate	6	The worst IP addresses according to DShield
Dshield top 10	Critical	2	The 10 absolute worst IP addresses according to DShield
Dshield top 4000	Minor	8	IP addresses reported as malicious by DShield, usually attacking servers
Finshun	Critical	6	IP Addresses that have been auto-blocked by a finiancial institution in the last week
Itar	Minor	8	IP Addresses in countries on the ITAR sanction list. Currently this is Afghanistan, Belarus, Cuba, Cyprus, Eritrea, Fiji, Iran, Iraq, Cote d'Ivoire, Lebanon, Libya, North Korea, Syria, Vietnam, Myanmar, China, Haiti, Liberia, Rwanda, Somalia, Sri Lanka, Republic of the Sudan (Northern Sudan), Yemen, Zimbabwe, Venezuela, Democratic Republic of the Congo.
Malware domain list	Minor	2	IP address hosting malware as identified at http://www.malwaredomainlist.com/
Modified itar	Minor	7	IP addresses in countries that are generally suspected of industrial espionage and potentially other acts against US interests. Currently this list contains: China, Brazil, Russia, India, Korea (both), Vietnam, Ukraine, Cuba, Czech Republic, Estonia, Georgia, Iran, Latvia, Lithuania, Moldova, Romania, Pakistan, Serbia, Somalia, Venezuela, Yemen

Parasites	Minor	4	Ethically suspect advertisers etc. Some advertisers end up serving malware
Phishtank	Moderate	4	Known phishing sites
Russian business network	Moderate	4	IP addresses ontrolled by known cyber-criminals
Shadowserver	Critical	1	List of botnet command and control hosts from ShadowServer
Shell shock attackers	Critical	1	IP address actively seeking to exploit servers vulnerbale to the bash vulnerability CVE-2014-6271
Spamhaus edrop	Minor	1	Spamhaus Extended Don't Route or Peer List containing ISPs known to host spammers, serve malware etc.
Ssh crackers	Minor	6	Attackers of linux/unix servers via SSH
Tscritical general	Critical	1	Addressses that ThreatSTOP has determined are a current active threat that are not in a specific feed
Unix server	Moderate	8	Ip addresses that attack linux/unix servers and other devices via SSH and/or Telnet. It also contains hosts that have been seen scanning for the Heartbleed openSSL bug.
Unix server-ru	Moderate	8	Ip addresses that attack linux/unix servers and other devices via SSH and/or Telnet. It also contains hosts that have been seen scanning for the Heartbleed openSSL bug.
Vietnam	Minor	2	IP addresses known to be located in Vietnam.
Voip abuse	Minor	3	IP addresses that have been noted as attacking VOIP infrastructure such as IP PBXes.
Web attackers	Critical	5	Attackers of web servers seeking to explit various vulnerabilities.
Zeus	Critical	2	ZeuS is a trojan that steals bank details

Reputation feed used in this evaluation:

go to **Suspicious Destinations**
go to **Threat Descriptions**

DNS Firewall Feed	Description
malware.rpz.infoblox.local	A comprehensive list of malware hosts/domains/name servers. Contains known botnet C&C domains/IPs and dropboxes as well as name servers that are known to be used solely by malicious entities. In addition to active botnets, this also includes resources used to sinkhole contact attempts by botnets that have been taken down by law enforcement and/or security researchers (e.g. conficker), the sites (IPs/domains/name servers) for known malware dropper sites and other places that can infect a computer that visits it, networks and entire autonomous systems that are on the "Do not Route Or Peer" (DROP) list, known active phishing sites, and other threats.

Report created on Tuesday, April 21, 2015