The Dangerous Game of DNS

Peter Silva, 2016-26-04

The Domain Name Service (DNS) is one of the most important components in networking infrastructure, enabling users and services to access applications by translating URLs (names) into IP addresses (numbers). Because every icon and URL and all embedded content on a website requires a DNS lookup, loading complex sites necessitates hundreds of DNS queries.

And because of that, DNS is a precious target and only lags behind http as the most targeted protocol.

DDoS-ing DNS is an effective way to make the service unavailable. As the flood of malicious DNS requests hit the infrastructure, the service can become unresponsive if there is not enough capacity. Organizations can add more servers or turn to their cloud-based security provider for help. One of the strategies cloud-based security providers use to shield DNS is DNS redirection. Cloud providers will divert incoming traffic to their own infrastructure, which is resilient enough to detect and absorb these attacks. The success of this strategy however depends on how well the website's original IP address can be shielded. If the bad guy can find that IP address, then they can get around the protection.

So is DNS redirection effective? Researchers decided to find out.

Scientists from KU Leuven in Belgium built a tool called CLOUDPIERCER, which automatically tries to retrieve websites' original IP address, including the use of unprotected subdomains. Almost 18,000 websites, protected by five different providers, were part to the team's DNS redirection vulnerability tests. In more than 70% of the cases, CLOUDPIERCER was able to retrieve the website's original IP address - the precise info needed to launch a successful attack.

Researchers did share their findings with those cloud-based providers and have made CLOUDPIERCER freely available for organizations to test their own DNS infrastructure.

In another DNS scam, a new version of the NewPosThings PoS (point of sale, not…) malware is using DNS rather than http/https/ftp to extract data from infected PoS terminals. This is an interesting twist since most security solutions monitor http/https traffic for suspicious activity. Anti-virus doesn't necessarily watch DNS and admins cannot simply turn off DNS since they need it to resolve hostnames and domains. Seems like a clear shot.

The newest version of NewPoSThings is nicknamed MULTIGRAIN and it only targets (and infects) one specific type of PoS platform: The multi.exe process, specific to a popular electronic draft capture software package. If the multi.exe process is not found the malware moves on. Once inside, the malware waits for the Track 2 credit card data and once it has the data, it encrypts and encodes it before sending to the bad guy via a DNS query.

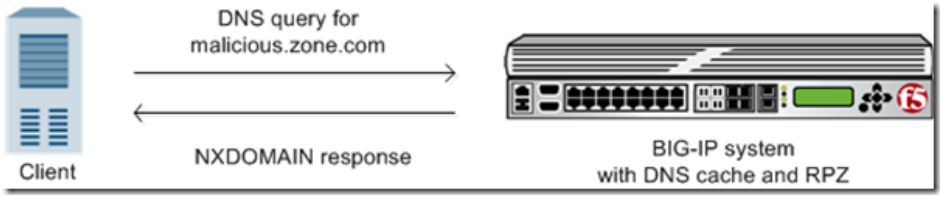
The use of DNS for data exfiltration on PoS devices is not new and shows not only how attackers can adjust to different environments but also, that organizations need to be more aware of their DNS traffic for potential anomalies.

BIG-IP could also help in both instances.

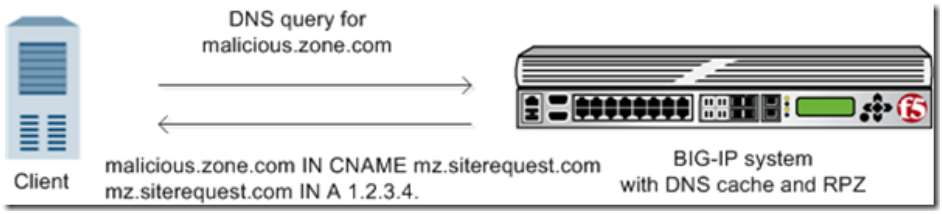
For the redirection issue, BIG-IP or our Silverline Managed Service offers Proxy mode with DNS redirection. With Routed Mode, we offer BGP to Silverline then Generic Routing Encapsulation (GRE) tunnels or L2VPN back to the customer to mask the original IP address.

For the PoS malware, BIG-IP can utilize a DNS response policy zone (RPZ) as a firewall or outbound domain filtering mechanism. An RPZ is a zone that contains a list of known malicious Internet domains. The list includes a resource record set (RRset) for each malicious domain and each RRset includes the names of the malicious domain and any subdomains of the domain.

When the BIG-IP system receives a DNS query for a domain that is on the malicious domain list of the RPZ, the system responds in one of two ways based on your configuration. You can configure the system to return an NXDOMAIN record that indicates that the domain does not exist or return a response that directs the user to a walled garden.



BIG-IP returns NXDOMAIN response to DNS query for malicious domain



BIG-IP forwards DNS query for malicious domain to walled garden

DNS is one of those technologies that is so crucial for a functioning internet, especially for human interaction. Yet is often overlooked or seems to only get attention when things are broken. Maybe take a gander today to make sure your DNS infrastructure is secure, scalable and ready to answer each and every query. Ignoring DNS can have grave consequences.

ps

Related:

- "Multigrain" PoS Malware Exfiltrates Card Data Over DNS
- NewPosThings Has New PoS Things
- New point-of-sale malware Multigrain steals card data over DNS
- Commonly used strategy for website protection might not work
- Cloudpiercer Discovery Tool
- Application Layer DNS Firewall

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com