White Paper

The Insider Threat

Key Takeaways:

- Internal DNS attacks are increasing and ever-evolving
- DNS service is a key indicator of malware presence
- Gartner warns “security organizations must assume they are compromised”
- DNS services play a dual role- as a preferred target and as a threat vector
- Purpose-built DNS security solutions are best to protect your infrastructure

Outline:

Cybercrime is no longer just a hobby for lonely hackers. It has become a real business, driven by organized criminals who hire professionals operating as teams. They indiscriminately target both individuals and organizations of any size. Their main motivation is money and confidential information, and they have become creative and efficient at extorting both. According to recent studies, these criminals can earn more than $500,000 on a daily basis[1].

The number of cyber attacks is constantly increasing year after year. This comes at a significant cost to businesses, which based on the 2015 study provided by the British insurance company Lloyd's[2] is estimated at over $400 billion a year worldwide. Behind this cost, malware is an increasing insider threat for all companies- more than 50 million new malicious programs were identified in 2014[3]. BYOD adoption and the dramatic growth of social media as an attack vector has facilitated their propagation. The single opening of an infected file on a single vulnerable device can generate a malware spread across an entire network, providing attackers with multiple potential entry points, and bypassing several layers of defense. From there, criminals are able to perform a variety of actions, from individual ransoming to large scale coordinated attacks targeting entire businesses. These attacks can lead to the exfiltration of highly valuable confidential data, or to critical service downtimes.

In the context of omnipresent malware, Gartner warns "organizations must assume they are compromised". A new security approach is needed, one which is more integrated with the infrastructure so it can detect suspicious activities within the overall network activity. As a key component of any IP network infrastructure, the DNS protocol is highly valuable for detecting malicious traffic.

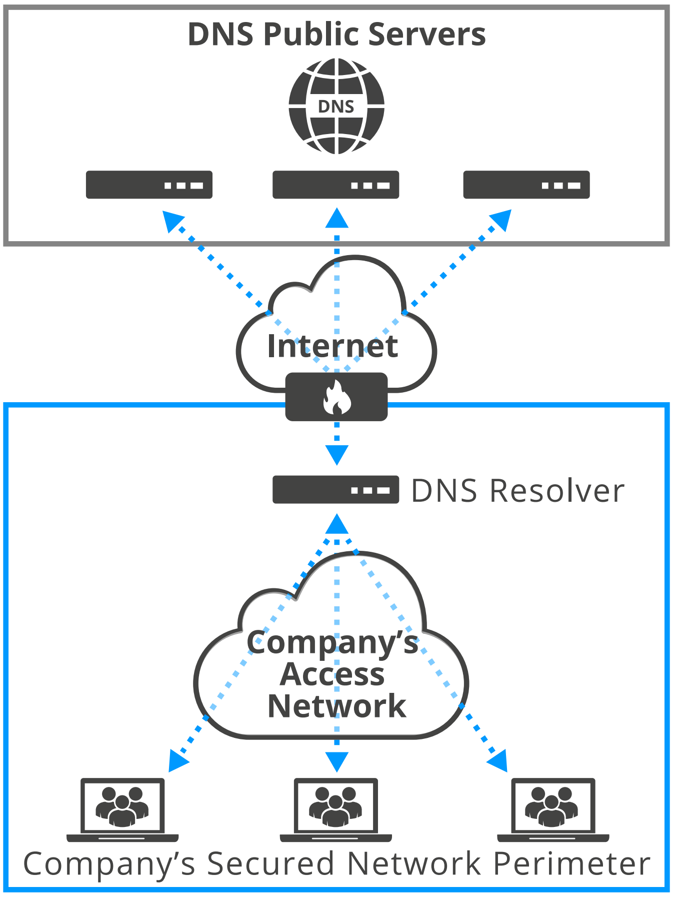
[1] *http://thehackernews.com/2016/07/android-hacking-tool.html*

[2] *http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/*

[3] *2014 Internet Security Team Report - Symantec & Verizon*

DNS: An Open Door

The Domain Name System is a public, hierarchical, decentralized naming system for any resource connected to a network. It provides a worldwide directory service, an essential component of the Internet that permits the association of a computer's network addresses (IP addresses) to readable "human" names commonly used to access network services (e.g. www.efficientip.com).



Its distributed, yet hierarchical design implies that any company's internal DNS resolver[1] has access to any public authoritative server, which is essentially the entire Internet. This is reflected at a firewalling level by permissive accesses regarding DNS traffic on TCP/UDP port 53. Despite the fact that resolvers act like proxies for DNS in a way, they rarely implement filtering capabilities, making them an open door to the Internet for any insider.

[1] Resolvers run local network DNS service, centralizing queries, caching and providing DNS answers. They act like a proxy for DNS.

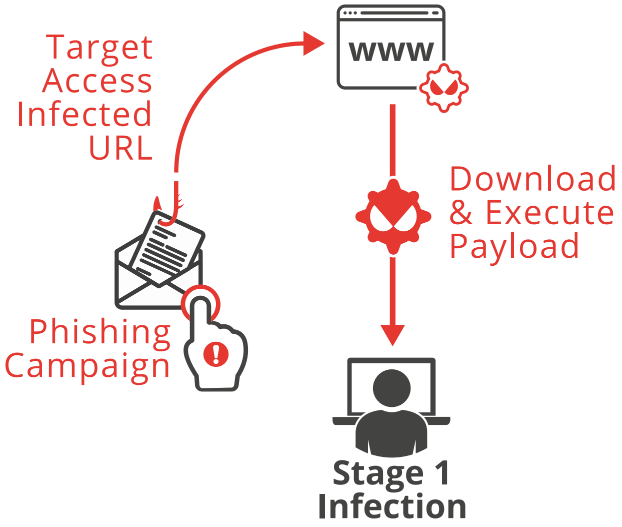
The Hidden Threats from DNS

The open nature and critical role of the DNS service within network infrastructure makes it a very attractive protocol for hackers. Cleverly exploited, DNS resolvers allow indirect communications between any device connected to an IP network and any public authoritative server (making it a useful tool for anyone that wishes to establish communication from a protected, yet connected, device to a specially crafted fake DNS server). Worse, DNS servers are not only an attack vector. They can play a dual role in the kill chain, as they are prime targets that can be leveraged to take down an entire network.

According to Cisco[1], 91% of malware relies on DNS services to communicate with their command and control server, or insidiously redirect users to malicious websites in order to extort their credentials. In more advanced attacks, DNS can even be diverted to exfiltrate confidential data from any compromised device. Yet Cisco cites that while DNS traffic is a good indicator of a network's health, only 32% of the companies monitor the requests going through their resolvers. Among them, very few are likely to go further and implement DNS protection mechanisms.

Malware's Use of DNS

By analyzing the various stages of an attack to highlight the role of DNS in the spread of malware, we can begin understand how DNS can be diverted from its initial purpose to serve the aims of an attacker.



Stage 1: An attack based on malware always relies on the initial infection of at least one device located inside the targeted network. While the initial infection payload is unlikely to be delivered directly from the DNS, it can be used to establish the connection with the infected website. Common strategy to prevent this threat is the use of web filtering, but exceptions are numerous within an information system, and not all devices support the use of proxies (IOT / BYOD). In such cases, DNS is a powerful complementary tool to mitigate the risk of a payload being downloaded and executed. Preventing the initial access to known infected websites and malicious domains is possible by making use of DNS RPZ (Response Policy Zone) combined with a reputation data feed such as SURBL[2]. This constitutes an efficient first layer of defense, actively contributing to the reduction of the attack surface.

[1] 2016 Cisco Security Report

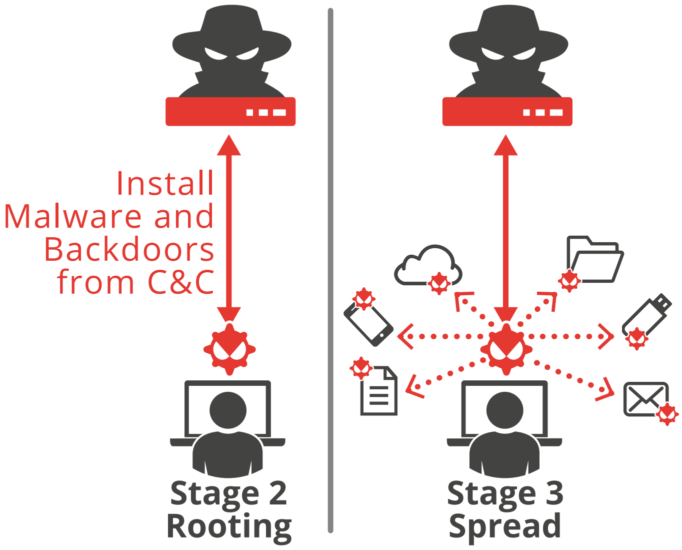
[2] http://www.surbl.org/

Stage 2: Once a device is infected, the code embedded in the payload calls home, trying to reach its command and control servers (C&C) to notify the attacker of the infiltration success. It then starts its malicious tasks. Depending on the malware, the action schema that follows may vary according to the aim of the attack. Still, it generally installs all the necessary backdoors and rootkits used by the attackers to take remote control of the device, and starts spreading across the entire network. At this stage, DNS is leveraged in two ways:

- For regular Internet services, using DNS to contact the C&C Servers allows attackers to dynamically modify- on regular basis (FastFlux)- the IP addresses used to reach their servers relying on other protocols such as HTTP/IRC to communicate. This circumvents the filtering policy, as firewalls are designed to filter flows based on IP prefixes and UDP/TCP ports, not according to the Domain Name(s) associated with IP addresses
- In a more advanced setup, DNS can provide a simple yet reliable protocol to communicate directly with the C&C Servers, making use of DNS resource records such as TXT to encapsulate commands and data

As a result, monitoring DNS traffic with the appropriate tools could:

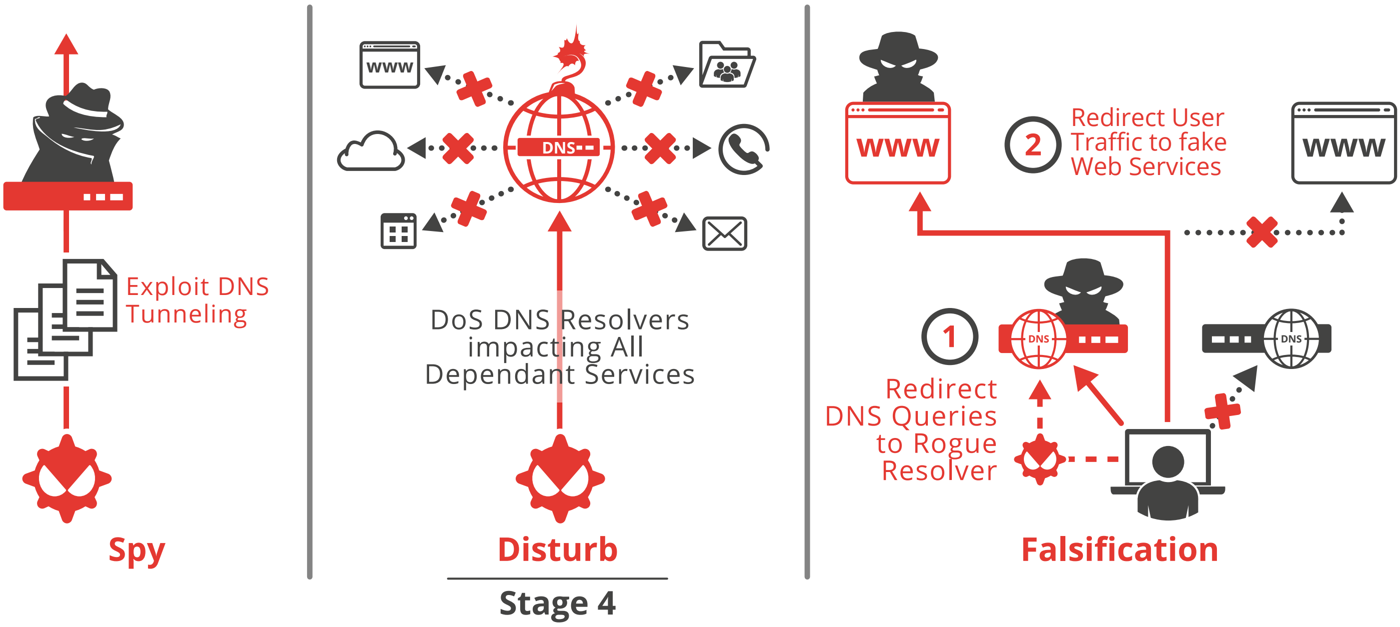
- Permit detection access to command and control servers, triggering a warning for administrators to take the proper actions, and potentially put suspect devices into quarantine
- Stop the malware from communicating with its remote control servers, preventing it from operating properly and avoiding further damages



Stage 3: The next stage of the attack is to spread across the network in order to maximize the number of infected devices, to access the maximum amount of information and gain higher privilege access. To do so, the malware shares its infectious payload through any means- emails, USB keys or shared network drives, repeating Stage 1 and 2 on as many devices as possible. Such behavior can be detected through DNS analytics, generating identifiable patterns as suspicious domains suddenly begin to be requested by a large number of devices.

Stage 4: As soon as they reach this point, attackers can (depending on their goal) trigger several actions- among which at least three are related to DNS:

- They can divert DNS protocol to exfiltrate confidential information relying on DNS Tunneling. As described previously, this is a suitable means to silently exfiltrate data from secure networks using a specially-crafted authoritative DNS server controlled by the attacker. This makes it an evasion technique closely tied to the concept of Advanced Persistent Threats (APT)
- They can install and operate rogue DNS services, to launch phishing campaigns and temporarily redirect users to rogue web services, extorting credentials such as bank account passwords in the process
- Or, they can easily take down internal recursive DNS services to seriously impact the information system (email, web services and cloud services access, TOIP, etc.), within an entire business. Two points should be considered on Denial of Service attacks. First, some can make use of a zero-day exploit, and silently take down the entire recursive DNS cluster with just a few requests (security alert CVE-2015-5477). Secondly, recursive DNS servers have, by design, limited capacity to process unknown requests. Most of them generally handle around 10,000 recursive requests per second, while a standard computer can generate a few hundred thousand, quickly overloading the targeted server.

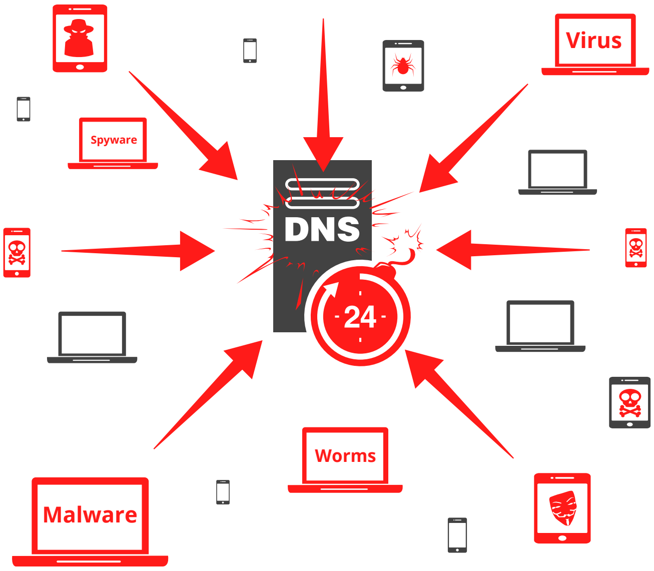

Exploit DNS Tunneling
Spy
www
DNS
DoS DNS Resolvers impacting All Dependant Services
Disturb
Stage 4
www
2
Redirect User Traffic to fake Web Services
www
1
DNS
DNS
Redirect DNS Queries to Rogue Resolver
Falsification

Implementing a secure DNS policy based on existing security tools, combined with an efficient modern DNS solution, would allow for:

- The detection and blocking of DNS tunneling attacks used to exfiltrate information, allowing administrators to act quickly in response
- Designing a proper filtering policy, allowing only company's official DNS resolvers to access public authoritative DNS servers. This would reduce the risk of users relying on rogue DNS resolvers that redirect to fake web sites, preventing credentials extortion
- Leveraging a hybrid DNS architecture combining different DNS engine technologies for mitigating DoS attacks based on zero-day exploits
- Real time DNS traffic analysis for detecting and blocking attacks on the DNS recursive service

It's Not Just About Malware

Internal resources are responsible of 41% of malicious attacks[1]. Malware is not the only threat to focus on- it is important to keep in mind that an information system's own users are not always trustworthy. The most basic attacks can have significant impact, and some businesses might be willing to trigger one against their competitors. When one in five employees are willing to sell their internal password for less than $100[2], how much would it cost to convince them to run a single binary targeting a critical service within an information system? DNS is a perfect target in such a case, where the potential to disrupt an entire information system is high, and requires very few resources.



In the long term, intellectual property theft is likely an even greater threat. A motivated insider is just as likely to steal confidential documents as an external hacker, but he will most likely know exactly what to look for. Many companies invest to prevent such leaks, but very few think about DNS in such context. Anyone with a moderate level of computer knowledge can execute a DNS tunnel following online tutorials, and then silently exfiltrate any proprietary knowledge or private information.

Organizations need to acknowledge these risks and take action to protect critical DNS infrastructures.

[1] *IBM 2015 Security Report*

[2] *http://fortune.com/2016/03/30/passwords-sell-poor-sailpoint/*

Conclusion

Cybercrime is a rising threat to organizations of any size, and has already generated huge amounts of money from extortion and confidential data theft. As a result, malware is spreading like never before, and is considered the go-to tool for initiating the compromise of any information system[1].

In this context, the recent increase in successful cyber attacks makes it clear that organizations must consider this threat and adapt their security policies. DNS service does not have to be leveraged by attackers only. Its criticality makes it the perfect place to scrutinize network health and activity. Implementing secure DNS services can enhance an organization's ability to stand against internal attacks. This can be achieved through embedding DNS security components such as high performance cache, DNS firewall, and real-time DNS traffic analysis capable of triggering adaptive countermeasures.

The EfficientIP 360° Security solution offers such game-changing technologies. Patented security innovations ensure unmatched continuity of mission-critical DNS services without the risk of blocking legitimate clients, or requiring complex configuration and laborious filtering rules. The solution is fast to deploy, easy to maintain, immediately capable of protecting against new threats, and highly cost-effective.

[1] *http://www.infosecurity-magazine.com/news/malware-irole-wildly-overstated/*

REV: C-1708

As one of the world's fastest growing DDI vendors, EfficientIP helps organizations drive business efficiency through agile, secure and reliable network infrastructures. Our unified management framework for DNS-DHCP-IPAM (DDI) and network configurations ensures end-to-end visibility, consistency control and advanced automation. Additionally, our unique 360° DNS security solution protects data confidentiality and application access from anywhere at any time. Companies rely on us to help control the risks and reduce the complexity of challenges they face with modern key IT initiatives such as cloud applications, virtualization, and mobility. Institutions across a variety of industries and government sectors worldwide rely on our offerings to assure business continuity, reduce operating costs and increase the management efficiency of their network and security teams.

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752