ADOPT DNS BEST PRACTICES **TO PROACTIVELY PROTECT AGAINST MALWARE**

390,000

More than **390,000 new malicious programs** are registered every day.[1]

The cyber threat landscape is dynamic and accelerating. 2017 has already seen several large-scale ransomware attacks that crippled private and public organizations across the globe. More than 390,000 malicious programs continue to be registered every day.[1] And significant data breaches have been reported since January, revealing the sensitive personal information of billions of customers to date.[2] While it is estimated that cyber crime currently costs the global economy $450 billion, this figure is projected to climb to $6 trillion by 2021.

Clearly, cyber crime is an enduring challenge. With ever-evolving tactics and growing financial incentives, hackers have know-how and reason to seek out vulnerabilities in your security stack. The Domain Name System (DNS) is one such gap in many organizations' defenses, and malicious actors are increasingly utilizing the recursive DNS infrastructure to launch damaging phishing attacks, malware and ransomware campaigns, and data exfiltration against companies.

Shoring up this well-recognized security back door is imperative given the financial and reputational ramifications. According to the Ponemon Institute, the cost associated with remediating an attack is about $18 million,[3] with an additional $4 million if your company experiences a subsequent data breach.[4] So imminent and dire are the consequences that Forrester Research predicts a Fortune 1000 company will cease to exist in 2017 because of a cyber breach.[5]

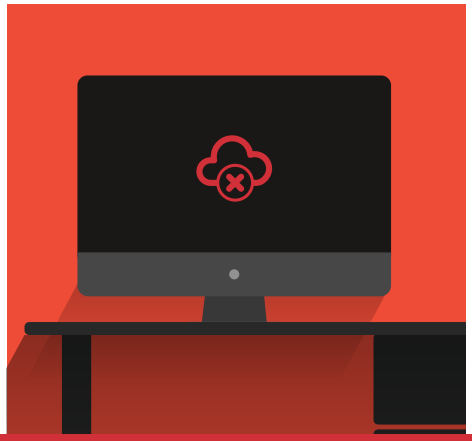
$18 MILLION

Cost associated with **remediating an attack is about $18 million**.[3]

Proactively protecting your company against malware, ransomware, and phishing at the DNS control-point, as opposed to retroactive triage and remediation, simply makes sense. A cloud-based solution is ideal given ease of configuration and deployment, limiting exposure time and ensuring 100% compliance across all branches, employees, and devices on your network near instantaneously.

However, layering an enterprise DNS security solution into your defense stack should be done in conjunction with enforcing DNS best practices. The following are industry standards that will help prevent DNS exploitation and, when coupled with an enterprise threat protection service, will aid you in identifying, blocking, and mitigating threats, as well as enforcing Acceptable Use Policies across your organization.

1. **Lock down systems to prevent changes to local DNS settings.**
   Enterprise threat protection systems block requests to known malicious sites. But end users may want to circumvent this feature and go to the site anyway, to see a photo or read an article, for example. Employees, people on your guest Wi-Fi, and other users on your network can easily reach a restricted site by simply using a free resolver (such as Google) to bypass the DNS settings on their local device. Organizations should therefore lock down any devices they provide or distribute to prevent end users from changing local DNS settings. An easy way to accomplish this is to create a group policy in your Active Directory.



2. Lock down systems to prevent installation of third-party VPNs.

When organizations secure their communications over the Internet, they have the option to use two types of VPN tunnels:

- **Split VPN tunnels:** The DNS query hits the local system and the local system makes an outbound query that adheres to company policies set by the administrator. The query might be directed to an ISP or to the local DNS server in the enterprise.
- **No-split VPN tunnels:** The DNS query goes over the tunnels themselves. If an employee or end user were to download a free or paid third-party, no-split VPN service, he or she could bypass the enterprise threat protection filters installed by the organization.

Best practice is to lock down systems to prevent employees, people on your Wi-Fi, and other end users from installing third-party VPNs that can bypass enterprise threat protection or network firewalls. Such a lockdown denies remote VPN access from any workstations unless they meet business requirements.

3. Lock down your firewall to allow DNS queries from local DNS systems only.

Best practice is to use a firewall to deny outbound traffic on DNS port 53 unless it's from a trusted source (e.g., the local DNS forwarder) and bound to a trusted destination (e.g., the resolver virtual IP [VIP] that the enterprise threat protection system assigns to you). That local DNS forwarder uses the enterprise threat protection system to look up all local queries for the enterprise to ensure that they only go to specified, legitimate addresses.

4. Look for questionable patterns in your DNS logs.

Suspicious patterns in DNS logs indicate the presence of malware. Malicious patterns can include:

- **Queries outside of normal business hours:** If a query comes from an employee's laptop at 2 a.m., chances are it is not the employee working late, and as such, should be viewed as a suspicious query.
- **Queries that use non-standard naming conventions:** Malicious actors use domain names with non-standard naming conventions because they know that these domain names will not be taken or registered. They can register these names on the fly. So, examine the domains' naming conventions and try to rationalize them.
- **Long-tail log queries:** To locate queries at the tail of the log, first sort all of the domain names alphabetically and eliminate any duplicates to ensure that all of the domain names are unique. Then count the number of requests to each domain name. Look at the tail end of the log and you will find a number of domain names that are accessed only once or twice. These domains are also often accessed outside of normal business hours and use non-standard naming conventions. You should investigate these suspicious domains to determine the owner and how long the domain has been registered. If, for example, it was only registered 10 hours ago and accessed 30 minutes later, it is likely not legitimate.

5. Separate your user traffic from data center traffic.

Separate your outbound traffic from your data center traffic, and have them egress from different points in your network. This allows you to set much stricter controls over the traffic leaving your data center. In addition, look at the DNS traffic exiting your data center to make sure that it is not going to a suspicious domain.

6. Beware of Tor.

The Tor network is a group of volunteer-operated servers that allow organizations and individuals to improve the privacy and security of information on the Internet. While the Tor network has many legitimate uses, there is no good reason to use Tor on a corporate network. If a connection is observed going to a Tor entry node, it's likely malicious. Many targeted threats use Tor to communicate with their CnC servers, and as a result, it is good practice to block Tor entry nodes at the edge firewall. Do this either by blocking all Tor entry nodes (based on publicly available lists of entry nodes) or doing deep packet inspection (DPI) on HTTPS traffic in your firewall.

For more information about proactively protecting your business against malware and other targeted threats, watch this short video, Spotlight on ETP, and visit akamai.com/etp.

Sources

1. https://www.av-test.org/en/statistics/malware/
2. https://www.identityforce.com/blog/2017-data-breaches
3. Ponemon Institute: The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN
4. Ponemon Institute: 2016 Cost of a Data Breach Study, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
5. Forrester's 2017 Predictions: Dynamics That Will Shape The Future In The Age Of The Customer, https://go.forrester.com/wp-content/uploads/Forrester-2017-Predictions.pdf