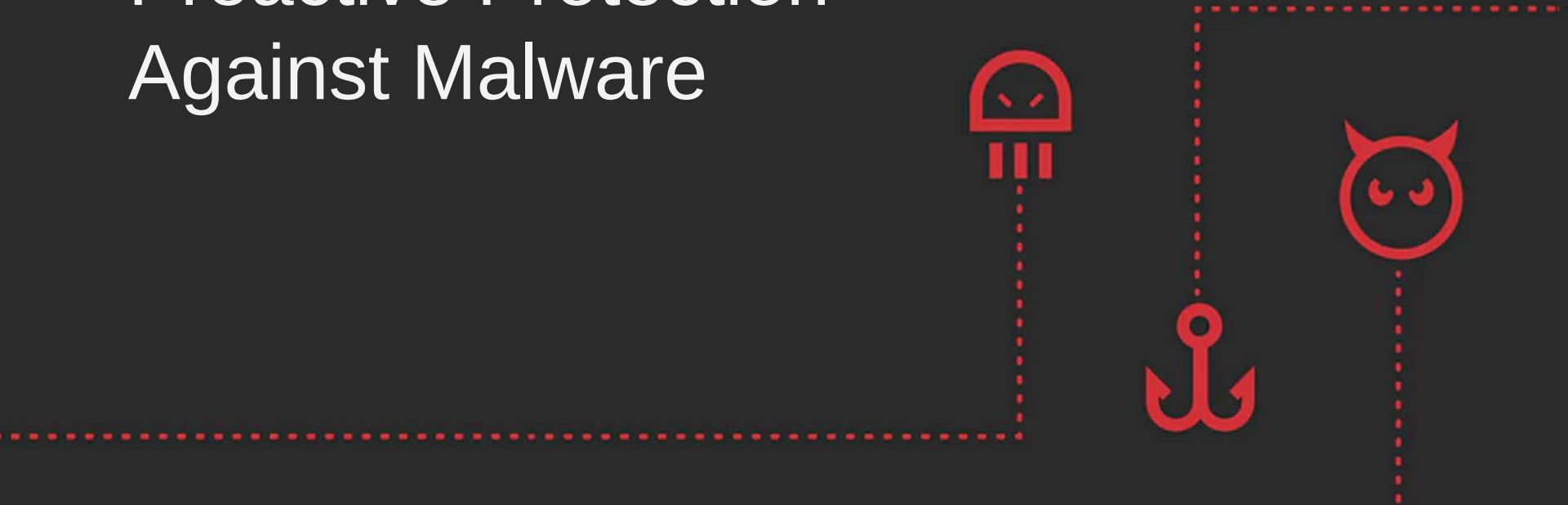
3 Reasons

You Need Proactive Protection Against Malware



We’re here to talk about protecting the existing gaps in your security stack.

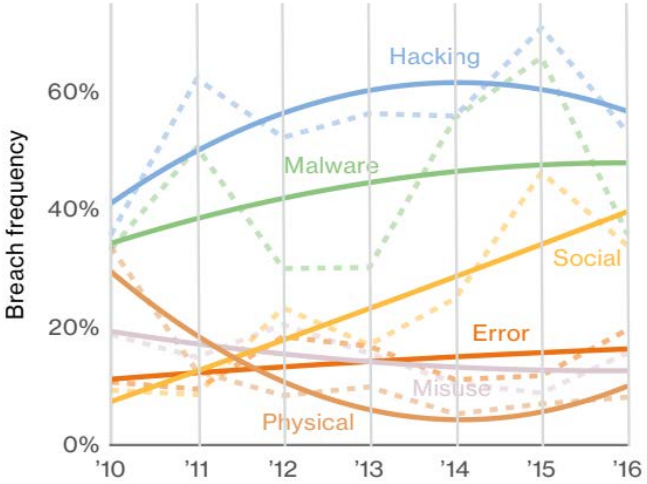
1 Cyber crime is on the rise

Targeted Threats are Increasing and Evolving

The prevalence, volume, and sophistication of targeted threats such as malware, ransomware, data exfiltration, and phishing are rising.

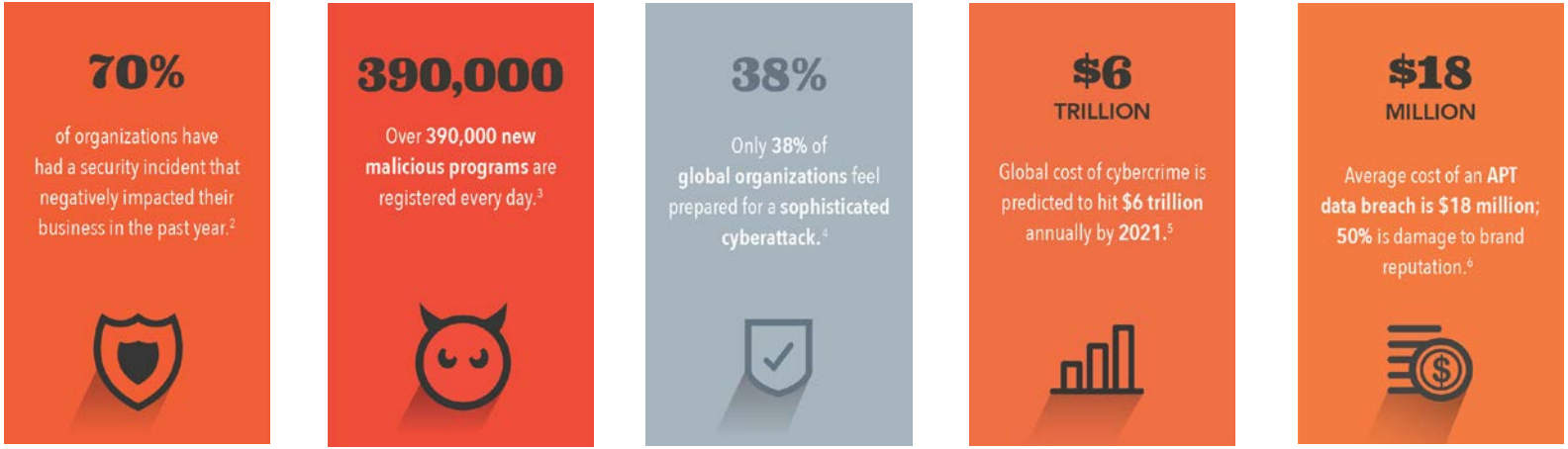
Malicious actors are adapting and evolving to bypass conventional security mechanisms.

Organizations are struggling to effectively deal with this deluge.



Percentage of breaches per threat action category over time[1]

The Realities of Cyber Crime



In 2016, the number of data records lost or stolen was overwhelming:

“A Fortune 1000 company will fail because of a cyber breach.”

Excerpt from Forrester’s *Dynamics That Will Shape The Future In The Age Of The Customer*

2

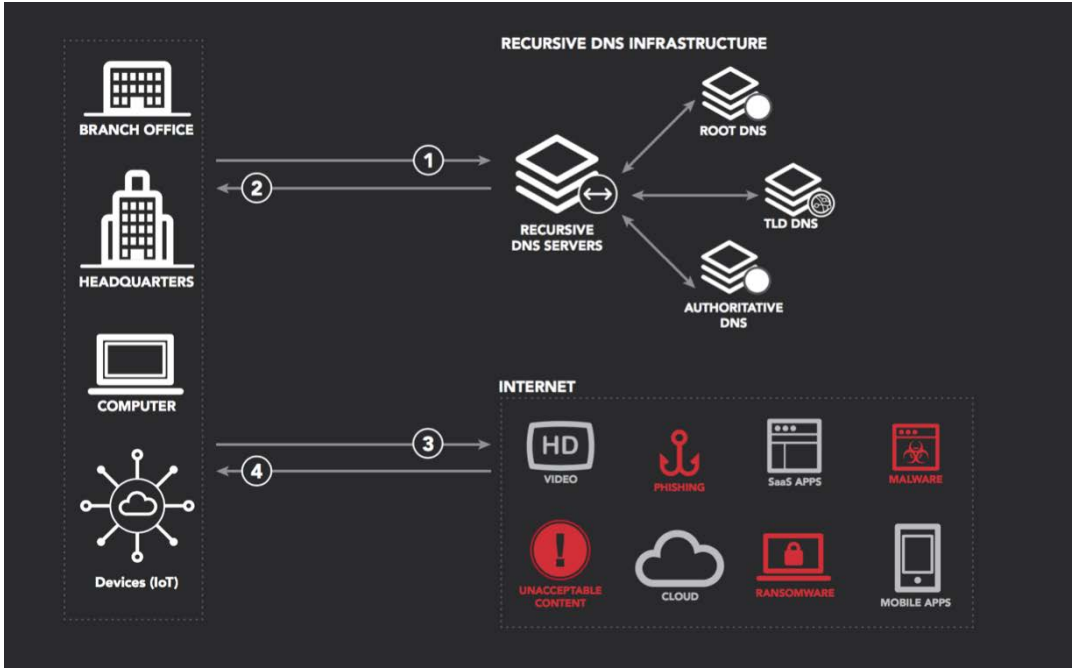
Malicious actors are increasingly using the Domain Name System (DNS) to bypass defenses

Why is Recursive DNS Exploited?

Almost every action taken on the Internet begins with a Domain Name System (DNS) request that translates domain names to IP addresses.

The DNS protocol is inherently open and unfiltered.

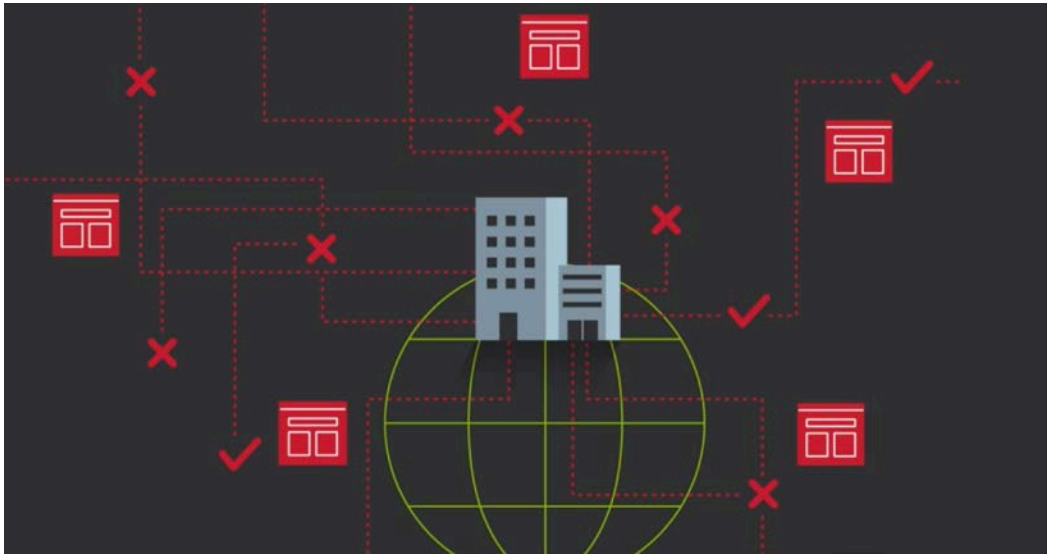
It has no intelligence and will resolve requests for a good or malicious domain.



Why is This an Urgent Problem?

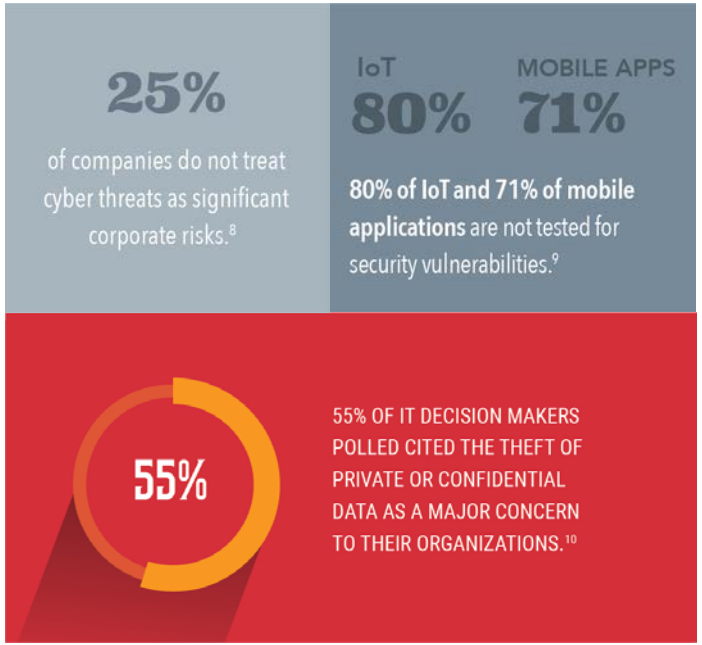
Cyber criminals have realized just how simple it is to exploit this unprotected security gap to get malware onto the network and extract sensitive data.

The number of attacks utilizing this vector are increasing quickly.



Why Are These Attacks Flourishing?

Despite the acknowledged vulnerability of the DNS infrastructure, the pressure to protect consumer and proprietary data, and the growing number of connected devices, few CIOs and IT teams make protecting the DNS infrastructure a priority.



3

Securing this vector is difficult

Imagine all the ways malware can enter your network...

All it takes is one employee or visitor on your network to:

Access a link in a phishing email
Click a malware-laden advertisement
Open a compromised URL in a social post
Navigate to a typosquatter's site
Access a homographic domain
Share infected computer storage media
Succumb to a social engineering tactic

Over 90% of malware uses DNS to spread the infection, take control of your network, and/or exfiltrate data.[11]

Volume of Traffic Poses a Problem

There are thousands of devices on a network: laptops, mobile phones, desktops, tablets, printers, projectors, guest Wi-Fi, “smart” IoT devices, and more.

They make hundreds of thousands of DNS requests a day.

This volume often obfuscates abnormal activities. There is often too much good and too little bad traffic to warrant the resources necessary to monitor DNS logs.

Visibility into Global Trends is Vital

Even if you allocate the resources to constantly monitor and dissect your DNS logs, it's highly unlikely you'll identify and mitigate an intrusion before it inflicts damage.

This is because your company's sample size is too small to identify global Internet trends and threats.

Existing security point solutions and appliances aren’t enough.

They’re often ineffective, inconsistent, and reactive.

Layers of Defense are Critical

Products like firewalls, Secure Web Gateways, endpoint anti-virus, and threat intelligence services rely heavily on blacklists, manual updates, reactive adjustments, and 100% user compliance.

They are often only as good as the providers' threat intelligence database.

It’s a Cat and Mouse Game

Given the rate of evolution of malware and the evasive measures bad actors employ to avoid detection—using non-standard ports and protocols, domain generation algorithms (DGAs), fast flux, and DNS exfiltration to name a few—most defense mechanisms lack the agility to adapt alongside a targeted threat and are quickly rendered obsolete.

There is a better way

Akamai
Enterprise Threat Protector

Sources

1. Verizon 2017 Data Breach Investigations Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

2. RSA Cybersecurity Poverty Index 2016, https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016

3. https://www.av-test.org/en/statistics/malware/

4. ISACA 2015 Global Cybersecurity Status Report, http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf

5. Cybersecurity Ventures, 2016 Cybercrime Report, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016

6. Ponemon Institute, The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN

7. www.cyberark.com/noteworthy-cyber-security-statistics/

8. MMC Cyber Handbook 2016, http://www.mmc.com/content/dam/mmc-web/Global-Risk-Center/Files/MMC-Cyber-Handbook_2016-web-final.pdf

9. Arxan, 2017 Study on Mobile and Internet of Things Application Security, https://www.arxan.com/2017-Ponemon-Mobile-Iot-Study

10. www.securityweek.com/nearly-50-percent-organizations-hit-dns-attack-last-12-months-survey

11. Cisco 2016 Annual Security Report