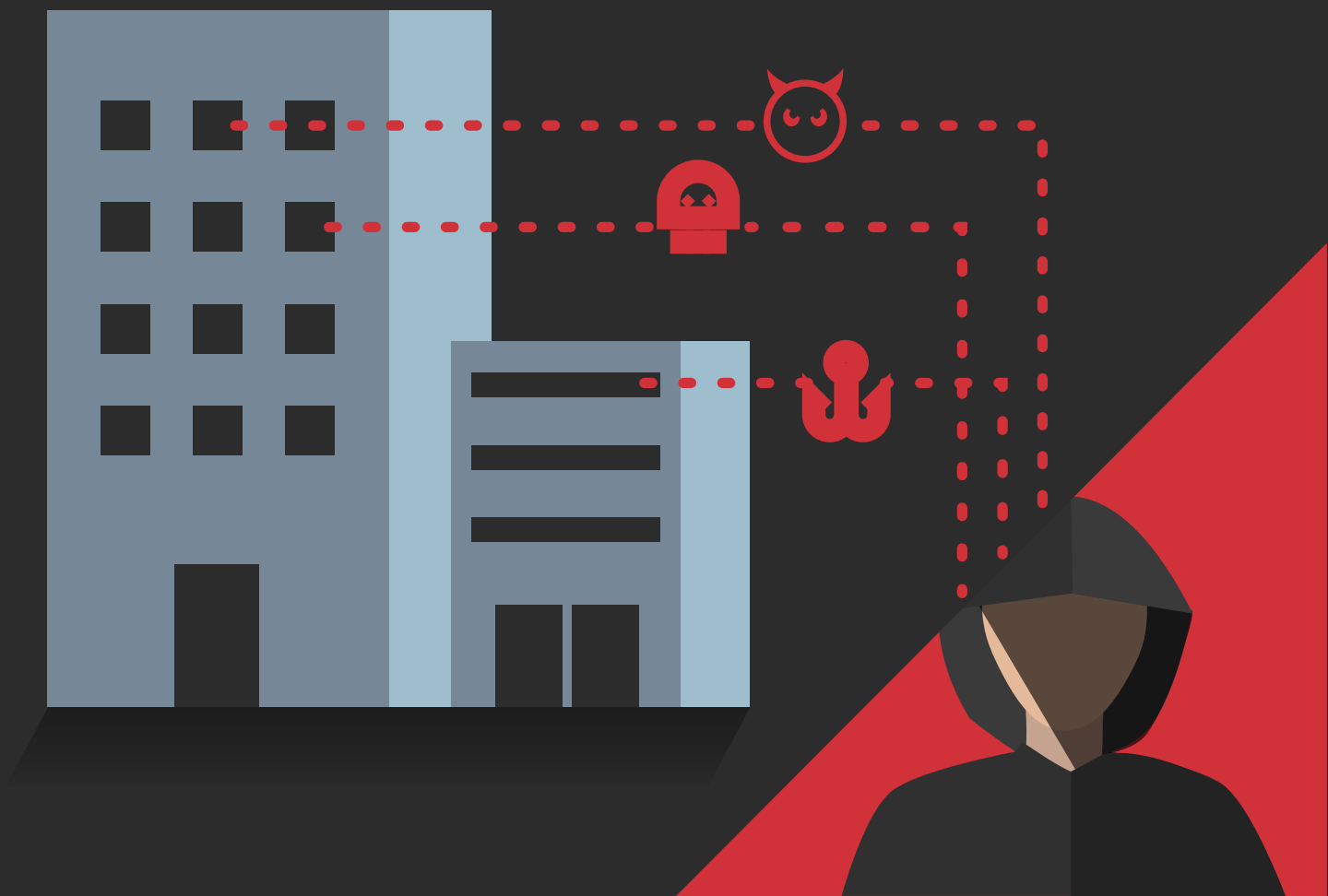
AKAMAI
SOLUTIONS
BRIEF

TARGETED THREAT PROTECTION IN THE CLOUD



PROACTIVELY PROTECT YOUR BUSINESS AGAINST TARGETED THREATS

The majority of security professionals agree that it's not a question of if, but when your company will fall prey to a targeted attack involving malware, ransomware, or phishing. In fact, 70% of organizations reported a security incident that negatively impacted their business in the past year,[1] a figure consistent with the reality that more than 390,000 malicious programs are registered every day.[2] Given the burgeoning number of connected devices and the growing financial incentives for cybercriminals, the prevalence, volume, and sophistication of targeted threats is only increasing.

As the stakes are raised for criminals and as companies react to attacks, the enterprise threat landscape is pushed forward. Bad actors are evolving their targeted threats and are finding vulnerabilities in companies' security defenses. One area that is increasingly drawing the attention of cybercriminals is the domain name system (DNS). DNS, and recursive DNS in particular, is the perfect cyberattack target because it is ubiquitous, open, and often unprotected. The number of targeted threats taking advantage of this threat vector is rising.

WHY IS DNS EXPLOITED?

Almost every action taken on the internet begins with a DNS request that maps domain names to IP addresses. While DNS makes the internet fast, efficient, and navigable, it is inherently ripe for exploitation due to its open and ubiquitous nature. DNS itself has no intelligence and, as a result, will resolve requests for both good and malicious domains. Cybercriminals are capitalizing on this vulnerability to launch targeted threats such as phishing attacks, malware and ransomware campaigns, and data exfiltration against enterprises.

WHY IS THIS AN URGENT PROBLEM?

If recursive DNS is left unmonitored, it's only a matter of time before one of the hundreds of thousands of daily Internet requests made from your network resolves to a malicious download. This could happen in any number of ways: An employee clicks on a link in a phishing email, selects a malware-laden advertisement, opens a compromised URL in a social post, navigates to a typosquatter's site, accesses a homographic domain, shares infected computer storage media, or succumbs to a social engineering tactic.

One compromised device quickly becomes a gateway for companywide infections that can slow or crash your network, spy on business activities, steal information, delete data and files, turn devices into "zombie computers" that host illegal content and engage in DDoS attacks, and more.

Additionally, once on your network, the vast majority of malware will send a request back to its command and control (CnC) server for further instructions. As DNS traffic is necessarily unfiltered and open, these malicious communications will go undetected, bypassing all network-level security. Through this DNS tunneling, bad actors can exfiltrate financial records, social security numbers, credit card information, intellectual property, and other sensitive data. These data packets are encrypted, compressed, and chopped, and then transmitted outside of your network.

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

The potential business impact of these targeted threats is extensive. According to the Ponemon Institute, the cost associated with protecting and remediating an attack can be broken down into four cost centers: technical support, lost productivity, forfeited revenue, and brand damage. Combined, these total an average of more than $18 million per attack.[3] Interestingly, the cost associated with damage to brand and reputation is almost $9.5 million, three times that of each of the other categories.[4] If your company experiences a data breach as a result of a targeted threat, Ponemon estimates another $4 million for mitigation.[5] The various expenditures rolled into that total can include: customer and crisis management, incident response, investigation, security audits, employee turnover, talent acquisition for hiring new CISO and security staff, legal fees and settlements, and regulatory fines.

It is estimated that cybercrime currently costs the global economy $450 billion and will climb to a projected $6 trillion by 2021.[6] In light of this, it is even more imperative that enterprises shore up their defenses, layering solutions, products, and tools into their existing security stack to reinforce known network vulnerabilities and attack vectors such as recursive DNS.

THE CHALLENGE: SECURING THIS ATTACK VECTOR IS DIFFICULT

Existing security solutions are often ineffective and inconsistent at protecting the recursive DNS infrastructure. Network-level security measures are unable to detect threats entering or data exfiltration happening via recursive DNS as they're originating outside of your company's perimeter. Products like firewalls, secure web gateways, antivirus programs, and threat intelligence services rely heavily on blacklists, manual updates, reactive adjustments, and 100% user compliance, and are often only as good as the providers' database.

Additionally, most security services only inspect HTTP and HTTPS protocol over ports 80 and 443; bad actors have become wise to this and are using alternative ports and protocols. Given the rate of evolution of malware and the evasive measures bad actors employ to avoid detection — slow drip, IP spoofing, domain generation algorithms (DGAs), and fast flux to name a few — most defense mechanisms lack the agility to adapt alongside a targeted threat and are quickly rendered obsolete.

Perhaps most difficult is the fact that your DNS security decisions are being made in a vacuum. Given the number and variety of DNS requests on your network — originating from laptops, mobile phones, desktops, tablets, printers, projectors, guest Wi-Fi, not to mention all the "smart" connected devices — it's difficult to know what constitutes normal, even if you allocate resources to constantly monitor and dissect your DNS logs. This is because your company's sample size is too small to effectively flag irregular DNS traffic. You must have an understanding of global patterns to efficiently and consistently identify threats.

AKAMAI PROACTIVELY PROTECTS THE ENTERPRISE WITH SIMPLE, FAST, AND CONVENIENT CLOUD-BASED SECURITY

Akamai's new Enterprise Threat Protector proactively protects your enterprise against targeted threats by modifying your existing recursive DNS setup. As every web request from the enterprise begins with DNS, it's the perfect control point to secure companywide visibility into web requests and apply security policy.

A cloud-based solution, Enterprise Threat Protector is quick to configure, easily scalable, and simple to deploy with no hardware or software and zero downtime. Security and acceptable use policy (AUP) rules and updates can be enforced unilaterally across all branches, employees, and devices in minutes. The cloud portal allows agile central management, and the dashboard provides drill-down into DNS traffic, threat events, and AUP activities. Enterprise Threat Protector also easily integrates with other security products and reporting tools, allowing your company to maximize investments across all layers of your defense-in-depth strategy.

Most importantly, Enterprise Threat Protector is built on Akamai's carrier-grade Intelligent Platform and powered by real-time intelligence from Akamai's Cloud Security Intelligence (CSI). Our extensive DNS domain knowledge, 100% availability SLA, and proven AnswerX service coupled with insights gleaned from managing 30% of global web traffic and 150 billion daily DNS queries means unmatched visibility into global traffic and threats, as well as unprecedented protection for your company and employees.

Want more information on Enterprise Threat Protector? Read the product brief and view a product demo by visiting akamai.com/etp.

SOURCES

1. RSA Cybersecurity Poverty Index 2016, https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016
2. https://www.av-test.org/en/statistics/malware/
3. Ponemon Institute: The Economic Impact of Advanced Persistent Threats, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WGL03060USEN
4. Ibid
5. Ponemon Institute: 2016 Cost of a Data Breach Study, http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
6. Cybersecurity Ventures: 2016 Cybercrime Report, http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/