



Protecting Your Network From Evolving DNS-Layer Threats

How to defend against emerging attacks using DNS

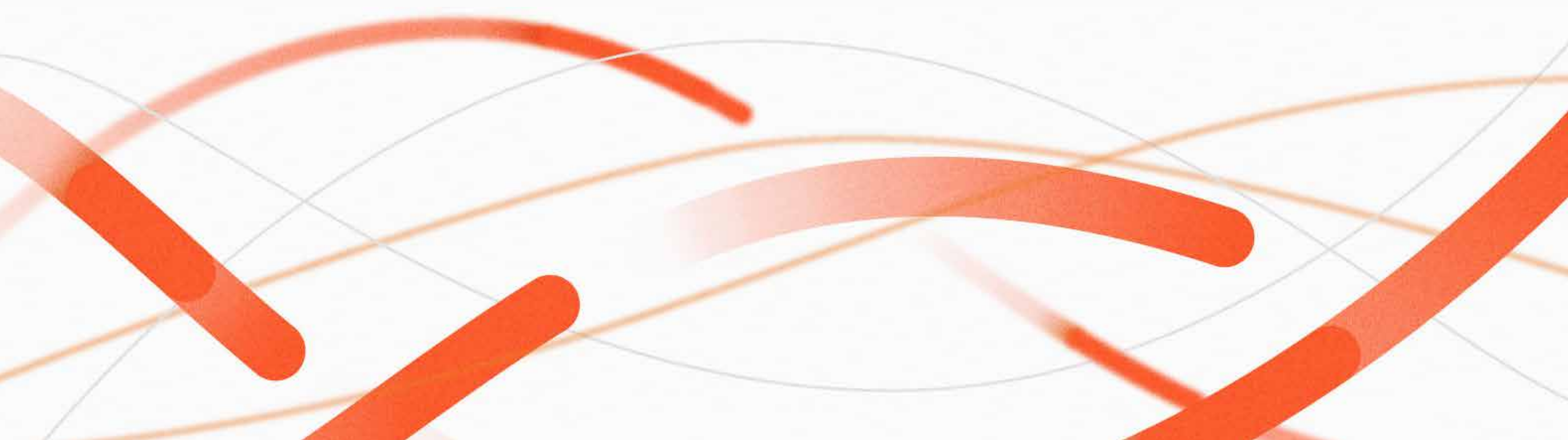


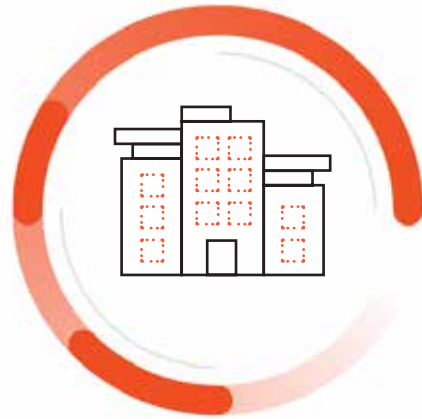
Table of Contents

1. Executive Summary	3
2. Recognizing DNS as an Emerging Threat Vector	4
3. Impact of Attacks Using DNS	5
4. Recent Attacks in the News	6
5. Why Current Security Approaches Fail	7
6. Stopping Attacks Using DNS with Palo Alto Networks	8

Executive Summary

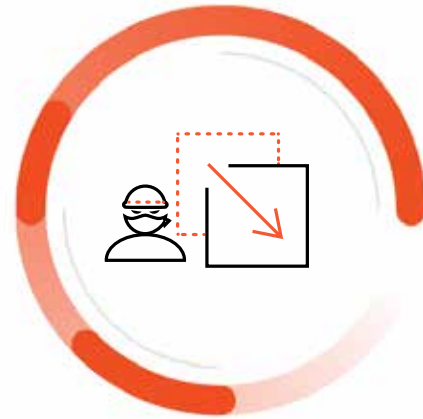
In the age of digital transformation, attackers are finding new ways to successfully breach organizations at scale. Successful attacks are becoming more common as adversaries use highly-evasive and sophisticated techniques to bypass today's security solutions.

Amongst the different types of cyberthreats today, attacks using DNS (Domain Name System) are growing at an alarming rate, which comes at no surprise. The combination of organizations failing to secure their DNS traffic and the ubiquity of DNS makes it an adversary's most powerful tool.



87%

of organizations experienced one or more attacks using DNS in 2021. An increase of 8% from 2020¹.



85%

of modern threats today abuses DNS for malicious activity².



42%

of organizations do not use a dedicated DNS security solution¹.

Recognizing DNS as an Emerging Threat Vector

DNS is a bi-directional and internet facing protocol that carries a tremendous amount of data, making it an adversaries greatest tool to carry out attacks. **And many organizations today lack the proper tools to protect against these attacks.** While they do have solutions that inspect and secure areas like their network, web traffic and email, these solutions are unable to perform a deep inspection of their DNS traffic, leaving them vulnerable to the many threats today that abuse DNS.

Not only do some organizations lack the proper security tools to secure their DNS traffic, but many of them don't have any DNS security solution at all.

DNS being ubiquitous and often unprotected makes it an extremely tempting target for attackers. **Palo Alto Networks Unit 42 threat research team has identified that 85% of modern threats today abuse DNS for malicious activity².** And this rate will continue to rise if organizations don't have the proper security solutions in place to defend against modern day attacks.

Reasons why organizations don't secure their DNS traffic:



Organizations **lack awareness** of the many types of techniques attackers can use to infiltrate their network.



Organizations **mistakenly view** DNS as a basic protocol that cannot be used for harm.

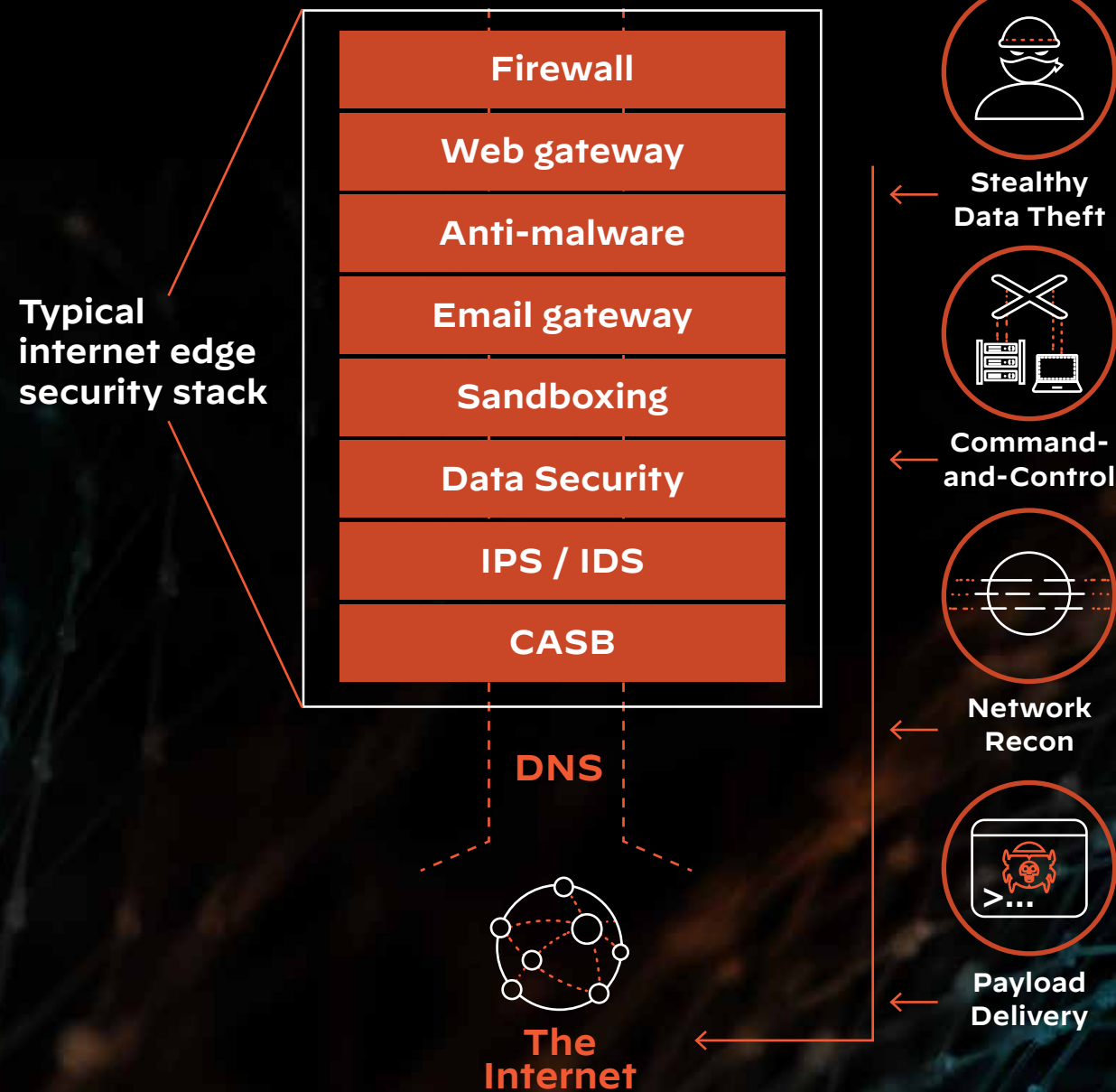


Identifying malicious threats with the high volume of DNS traffic and countless domains is **extremely difficult** and requires a great deal of time and resources.

DNS is an attacker's most powerful tool

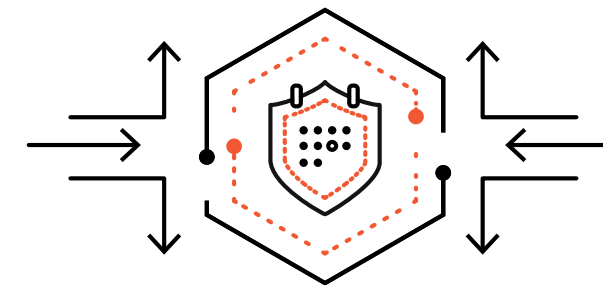


Your Network
(Users, devices, apps, & data)



Impact of Attacks Using DNS

Adversaries are taking advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack. **DNS is a massive and often overlooked attack surface** that requires the same level of protection that organizations use for web and email, but as long as organizations continue to neglect securing their DNS traffic, the attack surface will continue to grow. This means more organizations will fall victim to data theft, phishing and other malicious attacks using DNS.



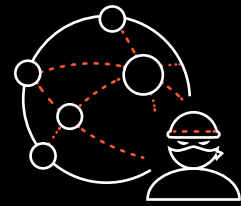
Average cost of a data breach in 2021 was

\$4.24M

DNS is your network's first line of defense against attacks that use ransomware, malware and data theft.

Source: <https://www.ibm.com/security/data-breach>

Attacks in The News



Solar Winds

On December 13, 2020, SolarWinds, a company who provides IT management tools and services for network and infrastructure monitoring to over 33,000 customers worldwide, were the victims of a supply chain attack on their SolarWinds Orion® software. In early 2020, nation-state hackers infiltrated malicious code into SolarWinds software which was later sent out to over 18,000 customers. The attackers were able to gain access into the networks, systems and data of these customers, allowing them to spread malware and steal sensitive information.

The SolarWind attackers, also known as Nobelium, used a number of different attacks using DNS to successfully carry out this historic cyberattack such as compromised DNS zones and strategically aged domains.



Pegasus

Pegasus is a spyware that can be covertly installed on iOS and Android devices to collect user information such as call and geolocation history. But as of 2022, Pegasus expanded the type of information they can get with their spyware by expanding their capabilities to also read text messages, track calls, collect passwords, track location, access the microphone and camera of devices, and harvest other user information from applications.

Pegasus was able to accomplish all of this by leveraging two DNS-layer threats, Strategically Aged Domains and Domain Generation Algorithms (DGAs). They used command-and-control (C2) domains that they registered in 2019 and waited 2 years before launching in order to bypass any security reputation checks, as well as several DGA subdomains to carry C2 traffic and relay encoded system information to the attacker.

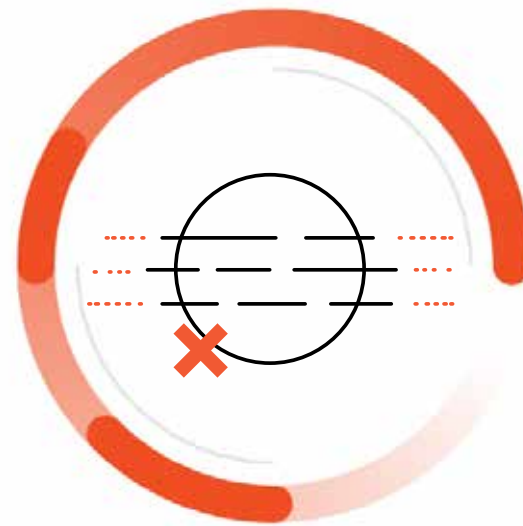
Why Current Security Approaches Fail

Existing security solutions fail to defend against attacks using DNS simply because they are unable to keep up with the innovation of modern day threats. Organizations tend to focus on securing their DNS infrastructure while ignoring the traffic that flows through it, leaving it wide open for attackers to spread malware and steal data.



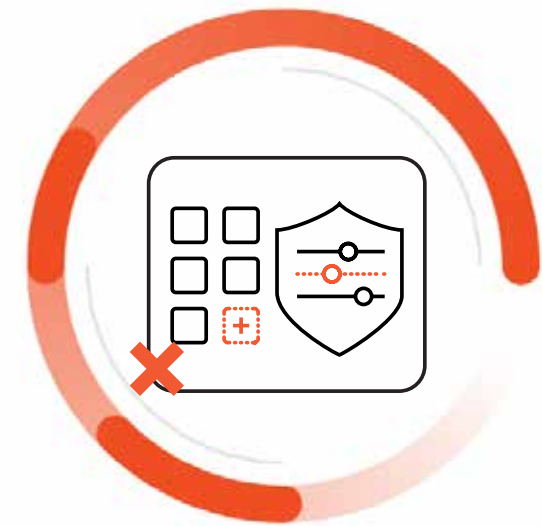
Static lists are slow and do not scale

Static domain block lists limit the amount of context defenders can access to understand attacks and lack real-time data analysis, making it difficult to scale and protect against emerging threats.



Analytics is required to predict malicious domains

In order to scale protection, security teams need to be able to run analytics on real-world security data using machine learning in order to detect unknown bad domains.



Security can be bypassed

DNS settings of resolver-based security solutions can easily be changed, meaning there is no place to enforce security, thus allowing security to be bypassed.

Stopping Attacks Using DNS With Palo Alto Networks

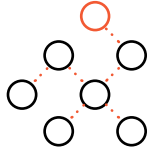
As DNS-layer attacks become more sophisticated, it becomes critical that security solutions continue to innovate to protect against these threats. In order to prevent being the next victim of a DNS-layer attack, organizations need a solution that can offer complete visibility and comprehensive coverage of their DNS traffic.

6 things your DNS Security solution needs to protect against modern day threats



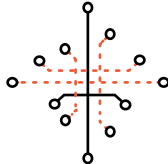
Security Data

Massive quantities of real-world security data from threat intelligence or cyberthreat alliances. With data from a large and expanding intelligence-sharing community, organizations are better equipped to protect themselves from attacks using DNS.



No Standalone Point Products

Disparate tools that are poorly integrated weren't designed for automation, meaning security teams are forced to manually stitch together insights from multiple disparate sources before taking action on threats.



Analytics and Machine Learning

Security teams must be able to run analytics inline on real-world security data and pair it with machine learning to identify unknown bad domains.



Full Visibility and Context for DNS Traffic

Visibility into DNS traffic allows security teams to identify malicious and benign traffic and trends. With context around these events, organizations are able to optimize policies and security posture.



Cloud-Based Protection

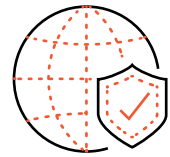
Using the cloud allows DNS protections to scale infinitely and always stay up to date. These cloud-based innovations allow defenders to develop and deploy new detection techniques instantly.



Category-Based Actions

Different types of DNS-based threats will require a different course of action. Security teams need automated responses based on DNS traffic categories to enable fine-grained control over DNS traffic more quickly, allowing them to efficiently mitigate threats and reduce risk exposure.

Palo Alto Networks DNS Security is the industry's most comprehensive DNS security solution that offers:



Unparalleled Protection

Predict, identify and disrupt new and advanced DNS-layer attacks with machine learning-powered detections.



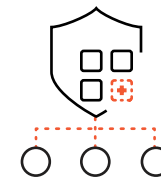
Visibility and Security Across All DNS Traffic

Secure all DNS traffic in your network, including unexpected DNS resolvers and malicious DNS servers.



Native Integration with Palo Alto Networks Next Generation Firewall (NGFW) and Prisma Access

Deploy DNS Security across all users and locations with no changes to your DNS infrastructure.



Ease of Deployment

Simply turn on and manage your subscription through your NGFW without the need to reroute your DNS traffic or endure lengthy change management processes.



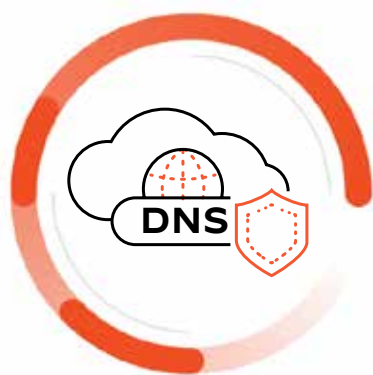
Security That Can't Be Bypassed

DNS Security is resolver agnostic, meaning security cannot be bypassed with simple changes to DNS settings.



Maximized Operational Efficiency

Secure your DNS traffic through a single platform and eliminate the need for independent tools, saving you an average of \$9.9 million per year of infrastructure costs.



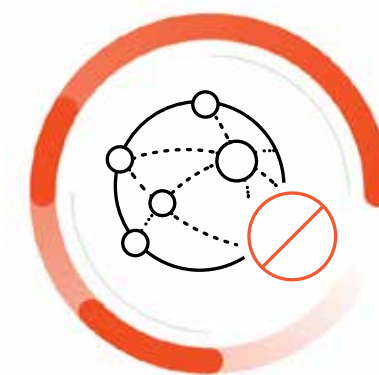
40% more

DNS-layer threat coverage than any other solution available



6X faster

detection of malicious newly registered domains than other leading public scanners

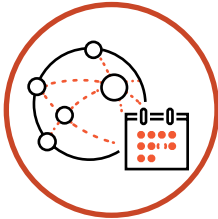


19M


malicious domains blocked per day

Threats Prevented by Palo Alto Networks DNS Security

Modern day threats using DNS are becoming more sophisticated than ever and are growing at an alarming rate. With adversaries constantly coming up with different types of attacks, they are becoming more capable of bypassing today's legacy security solutions. Palo Alto Networks is constantly adding protections to its DNS Security solution to prevent organizations from being a victim of modern attacks using DNS.

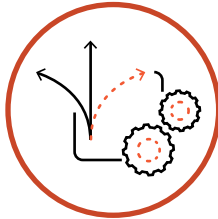


Strategically Aged Domains

 Attackers register domains months or even years before it is used for an attack. By lengthening the life of the domain, it is easier for the attacker to bypass reputation-based checks done by security vendors.

Objective:

-  Data exfiltration
-  Phishing



Wildcard DNS


 Wildcard DNS records allow attackers to redirect users to malicious hosts via a nearly infinite number of domains they registered in bulk.

Objective:

-  Malware
-  Phishing



Malicious NRD (Newly Registered Domains)


 A domain is considered newly registered if it has been registered or had a change in ownership within the last 32 days. The actors behind malicious NRDs often create slight variations of legitimate brand domains to fool users into visiting them. Many of these domains stay active only for short periods, which makes them hard to detect.

Objective:

-  Malware
-  C2
-  Phishing



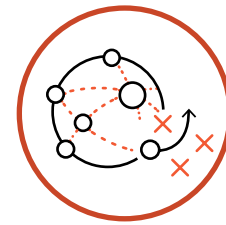
Domain Squatting

 Attackers register malicious domains that appear related to legitimate brand domains, with the intent of tricking users into believing that the malicious domain is owned by a reputable brand.


Objective:

 Malware

 Phishing



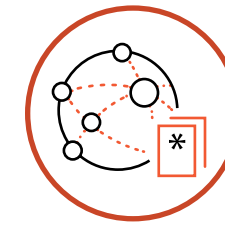
Compromised DNS Zone

 Attackers hack legitimate domains to create subdomains and use them to launch phishing and malware attacks to users who think they are visiting a safe site.


Objective:

 Malware

 Phishing

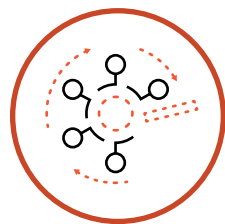


DNS Infiltration


 Attackers use another DNS-layer attack technique, DNS Tunneling, to download malicious payloads in small chunks within DNS packets to bypass security.

Objective:

 Infiltrate malicious payload

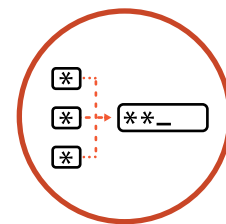


NXNS Attack


 NXNS attack, also known as NoneXistent Name Server attack, is used to paralyze a DNS resolver, making it impossible for users to access internet resources.

Objective:

 DDoS Attacks



Random Domain Generation Algorithms (DGA)


 Attackers continuously generate a number of domain names made up of random characters that stay valid for minutes or even seconds, allowing them to bypass legacy firewalls which are unable to keep up with the volume of domains as well as the rate in which they change.

Objective:

 C2



DNS Tunneling

 Attackers exfiltrate sensitive data in small chunks within DNS requests to bypass security. With the amount of DNS traffic and requests a network typically sees, attackers are able to easily hide data theft.

Objective:

 Data exfiltration



Dangling DNS

🚀 Attackers hijack stale DNS zone entries that point to expired domains, allowing them to impersonate legitimate domains and redirect traffic to their own site for malicious activities.

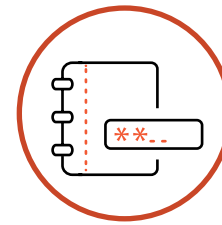
Objective:

👤 Malware

📄 C2

🕸 Phishing

👥 Social Engineering



Dictionary DGA

🚀 Attackers continuously generate a number of domain names made up of dictionary words, to resemble legitimate domains and evade detections. These domains stay valid for only minutes or seconds in order to bypass legacy firewalls.

Objective:

📄 C2

👤 Infiltrate Malicious Payload



DNS Rebinding

🚀 Attackers manipulate resolution of domain names and cause users to run a client-side script that attacks machines elsewhere in the network.

Objective:

👤 Data Exfiltration

👤 DoS

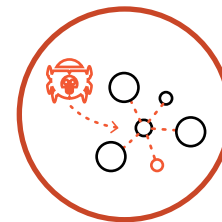


Ultra-slow DNS Tunneling

🚀 Attackers exfiltrate sensitive data in small chunks and distribute them to multiple domains under their control at a very slow rate to evade detection.

Objective:

👤 Data exfiltration



Malware Domains

🚀 Malware domains host and distribute malware. These domains are different from C2 domains in that they deliver malicious payloads into your network via external source.

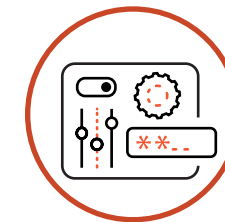
Objective:

👤 Malware

📄 C2

🕸 Phishing

👥 Social Engineering



Command-and-Control Domains

🚀 Command-and-control includes URLs and domains used by malware or compromised systems to communicate with an attacker's remote server and receive malicious commands or exfiltrate data, or deplete resources on a target authoritative DNS server.

Objective:

📄 C2

👤 Data Exfiltration

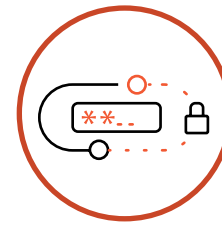


Botnet Domains


 These domains connect to an attacker controlled domain for C2 activities.

Objective:

 C2



Fast-flux Domains

 Attackers generate numerous IP addresses per malicious domain and change them in quick succession, allowing them to bypass legacy security solutions.

Objective:

 Malware

 Scams

 Phishing

 Botnet Operations



Proxy Avoidance


 Proxy avoidance is traffic to services that are used to bypass content filtering policies

Objective:

 Bypass Security

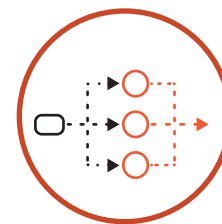


Parked Domains


 Parked domains are inactive websites that host limited content, often in the form of click-through ads which may generate revenue for the host entity, but generally do not contain content that is useful to the end user.

Objective:

 Malware

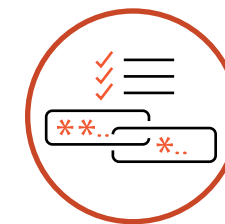


Grayware Domains


 Grayware domains are used to facilitate vectors of attacks, produce various undesirable behaviors, or contain questionable and offensive content. These include websites that attempt to trick users into granting remote access, promote illegal activities or scams and other malicious activities.

Objective:

 Host Risky Content



Dynamic DNS

 Dynamic DNS (DDNS) provides real-time mapping between host names and IP addresses, allowing attackers to infiltrate a network by using DDNS to change the IP addresses that host command-and-control servers.

Objective:

 C2

Palo Alto Networks DNS Security Solution

Palo Alto Networks DNS Security protects you from these DNS-layer threats while continuing to add protections that will defeat any new attacks. With ML-powered engines that prevent attacks in real time and added detections, Palo Alto Networks offers 40% more DNS threat coverage than any other vendor and can disrupt 85% of modern attacks that use DNS for malicious activity, without requiring any changes to your infrastructure.

For more resources and information

about Palo Alto Networks DNS Security solution, visit

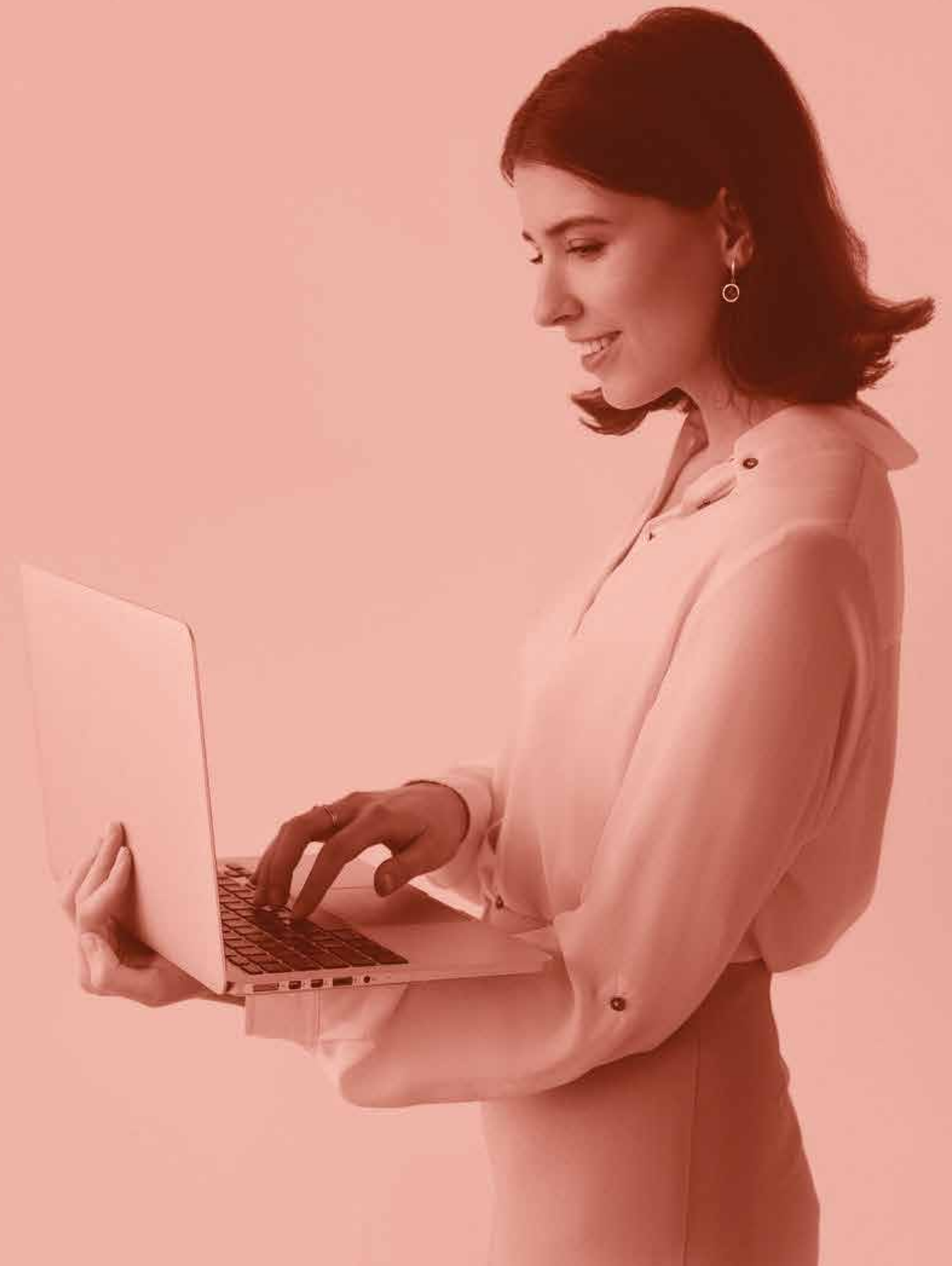
[Palo Alto Networks DNS Security](#)

To learn how the DNS Security service

can stop modern day attacks with machine learning and predictive analytics, sign up for a 90-day DNS Security free trial and benefit from the best-in-class DNS-layer threat detection and prevention service.

[DNS Security](#)

[90 Day FREE Trial](#)





www.paloaltonetworks.com

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

© 2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks>. All other marks mentioned herein may be trademarks of their respective companies.