CYBER THEORY

The Threats from Unsecured DNS and Domains

A CyberTheory Technology Briefing

CYBER THEORY

We are a full-service cybersecurity marketing advisory firm.
We constantly collect and analyze the latest customer data segmented by security practitioner, industry and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona. With strategic insights from global education services, media providers, intelligence analysts, journalists and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompass all aspects of cybersecurity as well as the related fields of fraud, audit, compliance and risk management.

CONTACT INFORMATION

cybertheory.io

212.518.1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018

Table of Contents

The Threats from Unsecured DNS & Domains

Every day around 4 am, I receive a short essay from my friend and colleague, Andy Jenkinson, the Group CEO at CIP in the UK, lamenting the pending apocalypse that will be brought on by unsecured domains.

He will frequently write something like this:

Domains are a critically important element of internet infrastructure; they are also woefully exposed and exploitable. Their functionality and security rely upon many factors.

Name server delegations introduce complex and subtle interdependencies between domains and their authoritative name servers.

A compromise of any name server in the delegation hierarchy can lead to a hijacking scenario. Targeted name server compromises in the delegation hierarchy can facilitate a complete hijack of a domain or set of domains.

A compromised name server is capable of diverting DNS requests to malicious servers controlled by threat actors and can be weaponized for phishing attacks, MiTM, watering hole vectors or several of many other attack scenarios.

It turns out that over 95% of cyberattacks, malware and bots rely on unsecured DNS to be successful.

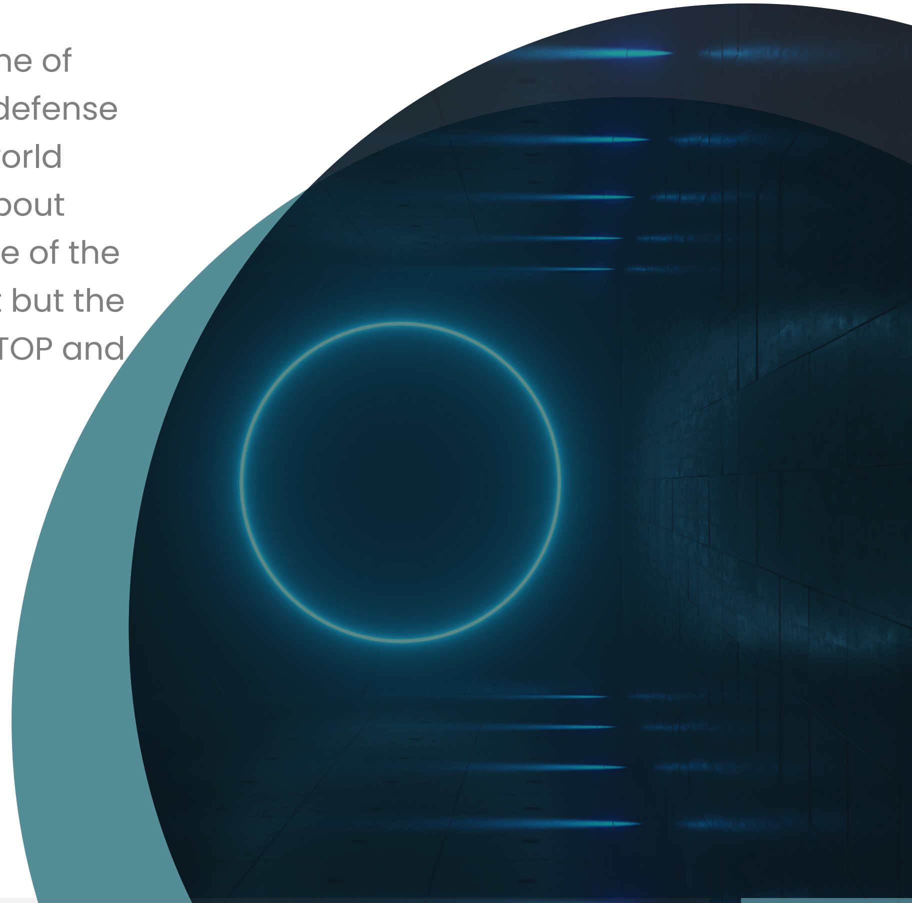
The Smartest Guys in the Room

Dr. Paul Vixie is an American computer scientist who built upon and further developed the Domain Name System (DNS) protocol design and procedure, along with mechanisms to achieve operational robustness of DNS implementations, and the first successful commercial anti-spam service.

Dr. Paul Mockapetris is an American computer scientist and internet pioneer who designed and built the Internet Domain Name System (DNS), wrote the first DNS implementation and serves as Chief Scientist for ThreatSTOP today.

ThreatSTOP, by the way, is one of the smartest cybersecurity defense product companies in the world that understands nothing about marketing. Tom Byrnes is one of the smartest guys on the planet but the difference between ThreatSTOP and Zscaler is Jay Chaudhry.

Vixie and Mockapetris both claim that over 95% of cyberattacks, malware and bots rely upon DNS.



Cybersecurity and Infrastructure **Security Agency (CISA)**

In 2019, CISA authored their first Emergency Directive on domain name security (DNS). In it, CISA directed agencies to take four specific steps over the next 10 days to protect against DNS tampering.

Chris Krebs, the director of CISA, said that “malicious actors obtained access to accounts that controlled DNS records and made them resolve to their own infrastructure before relaying it to the real address. Because they could control an organization’s DNS, they could obtain legitimate digital certificates and decrypt the data they intercepted – all while everything looked normal to users.”

Krebs said DHS is “aware of a number of agencies affected by the tampering campaign and have notified them; though the extent of the impact is limited based on available information. In part, by issuing the directive, CISA seeks to work with agencies to detect and prevent additional impacts on agencies and systems.”

“These types of attacks are not new and in many ways not even that sophisticated,” said John Banghart, the senior director of technology risk management at Venable and the former National Security Council’s director for federal cybersecurity during the administration of President Barack Obama. “We don’t know for sure why DHS is issuing the directive. We can guess they are seeing this occurring and notified some agencies. The worst part about this attack is if it goes unnoticed, which it seemed it did for some time, it’s hard to detect.”

DHS laid out a four step process for agencies to lock their doors:

- Verify their DNS records to ensure they’re resolving as intended and not redirected elsewhere. This will help spot any active DNS hijacks.
- Update DNS account passwords. This will disrupt access to accounts an unauthorized actor might currently have.
- Add multi-factor authentication to the accounts that manage DNS records. This will also disrupt access and harden accounts to prevent future attacks.
- Monitor Certificate Transparency logs for certificates issued that the agency did not request. This will help defenders notice if someone is attempting to impersonate them or spy on their users.

All three experts agreed that three of the four requirements are pretty straight forward, but implementing multi-factor authentication on the accounts to manage DNS records may be more difficult. Best pay attention, you Zero Trust enthusiasts.

According to Andy, overlooking DNS and PKI is like wearing a blindfold, sound blockers and handcuffs while expecting to go about your daily routine. Today, CISA, NSA, DHS, DOD, The White House, EU Commission and many more are driving DNS awareness.

> DNS is a protocol that translates user-friendly domain names...

What is all this DNS stuff

& why do I care?

So, what is DNS, what are Domains, I don't want to have another threat to worry about, and how real is this threat that keeps Andy sending me love notes every morning at 4 am?

Every modern organization requires the Domain Name System (DNS) to run its business, regardless of industry, location, size or products. DNS is a protocol that translates user-friendly domain names, such as cybertheory.io, into machine-usable IP addresses like, 199.123.45.678. Without DNS, we'd have to memorize random strings of numbers, which we can't do. Which is why the most popular password remains 123456.

DNS is fundamental to every single modern organization, all over the world. Network operators cannot block DNS traffic, and firewalls have to let it through. Networks need DNS to function properly.

Domain Hijacking:
Real Threat

Domain hijacking is the act of changing the registration of a domain name without the permission of the original owner, or by abuse of privileges on domain hosting and domain registrar systems.

Domain name hijacking is devastating to the original domain name owner's business with wide ranging effects including financial damages, reputational damage and regulatory impact.

Generally domain hijacking occurs from unauthorized access to, or exploitation of a vulnerability in a domain name registrar; through social engineering; or by gaining access to the domain name owner's email address and then resetting the password to their domain name registrar.

Another common tactic is to gather personal information about the actual domain name owner to impersonate them and persuade the domain registrar to modify registration information or transfer the domain to another registrar they control.

Other methods include email vulnerability, vulnerability at the domain-registration level, key-loggers to steal login creds and phishing attacks.

Your ability to recover a hijacked domain will largely depend on what your registrar can do to reverse the attack. Sometimes registration information can be returned to the original owner. More often, it cannot.

Some Get It

While some CISOs understand the necessity to keep tight controls over DNS and Domains, Andy's daily evidence suggests that most don't realize the ease and prevalence of DNS abuse by attackers. In fact, many security teams don't inspect DNS traffic for threats because they assume queries sent over DNS protocol and port 53 are benign.

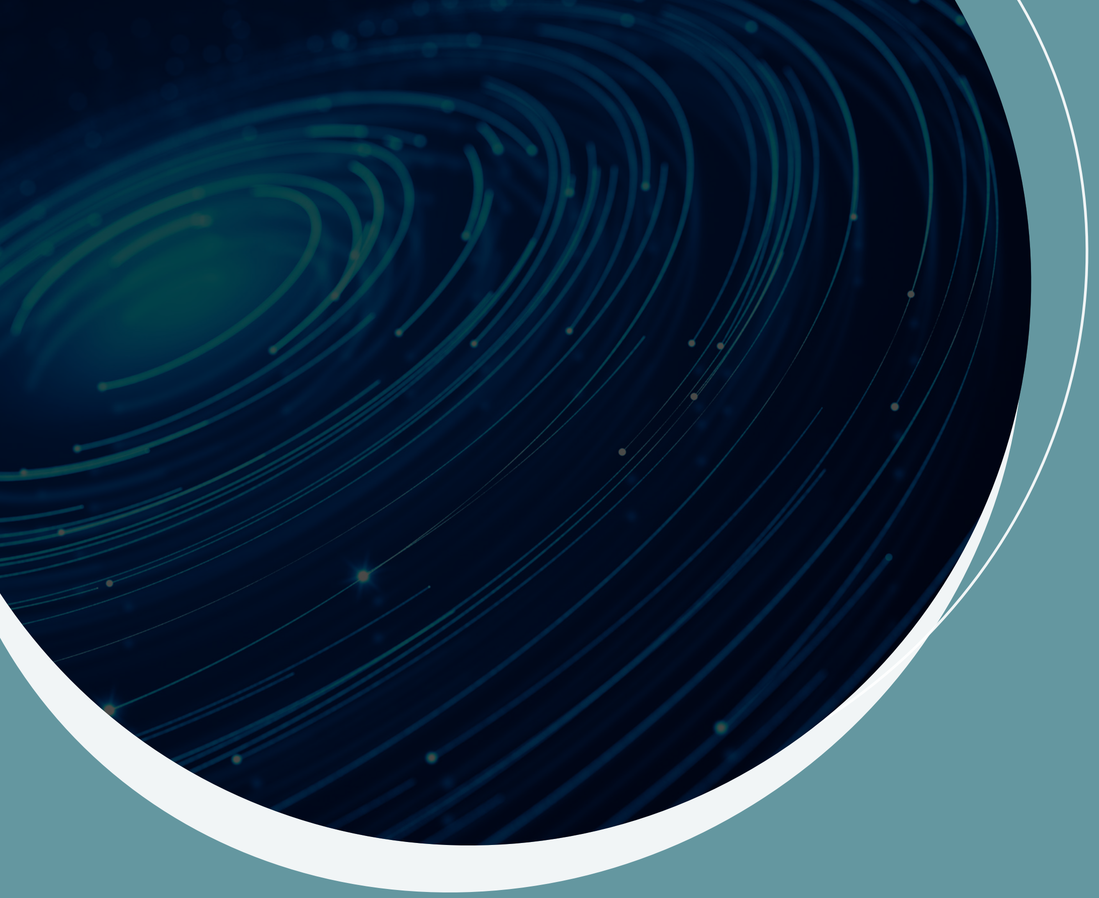
Other organizations don't inspect DNS traffic because the sheer volume of that traffic is overwhelming and looking for a sign of something malicious in that traffic is like looking for a needle in a haystack. This takes a great deal of time and resources—often too great an investment for organizations, especially those that assume DNS does not pose a significant threat.

Andy sends me living examples daily of surprisingly large, savvy companies whose DNS's are unsecured - companies like Boeing, Capital One, Bank of America and Okta for example – LinkedIn has a huge archive that Andy put together over the past year that will likely amaze you.

In fact, DNS is a massive and often overlooked attack surface that requires the same scrutiny and protection given to web and email. It can be used for malware delivery, command and control (C2), or data exfiltration. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack.

According to Palo Alto Networks Unit 42 threat research team, almost 80% of malware uses DNS to initiate C2 procedures. Attackers establish reliable command channels that are difficult to take down or identify since DNS is such a reliable way to maintain a connection to DNS servers. As adversaries increasingly automate their attacks, it becomes almost impossible to identify and stop those threats.

Understanding how adversaries abuse DNS is the first step to stopping attacks on your network and minimizing your cybersecurity risks. Here are the top three ways cybercriminals abuse DNS to mask their C2 activity so they can deliver additional malware or steal data.



Malware Using DNS for C2

This is one of the most typical ways attackers take advantage of DNS. Attackers use common network protocols, including DNS, to spread malicious code. Malware can be sent to users through online ads, malicious URLs in emails or other means. Once a user's computer is infected, the system sends a DNS request back to the attacker's control server.

And the genius is that now the infected computer becomes a bot the attacker can control.

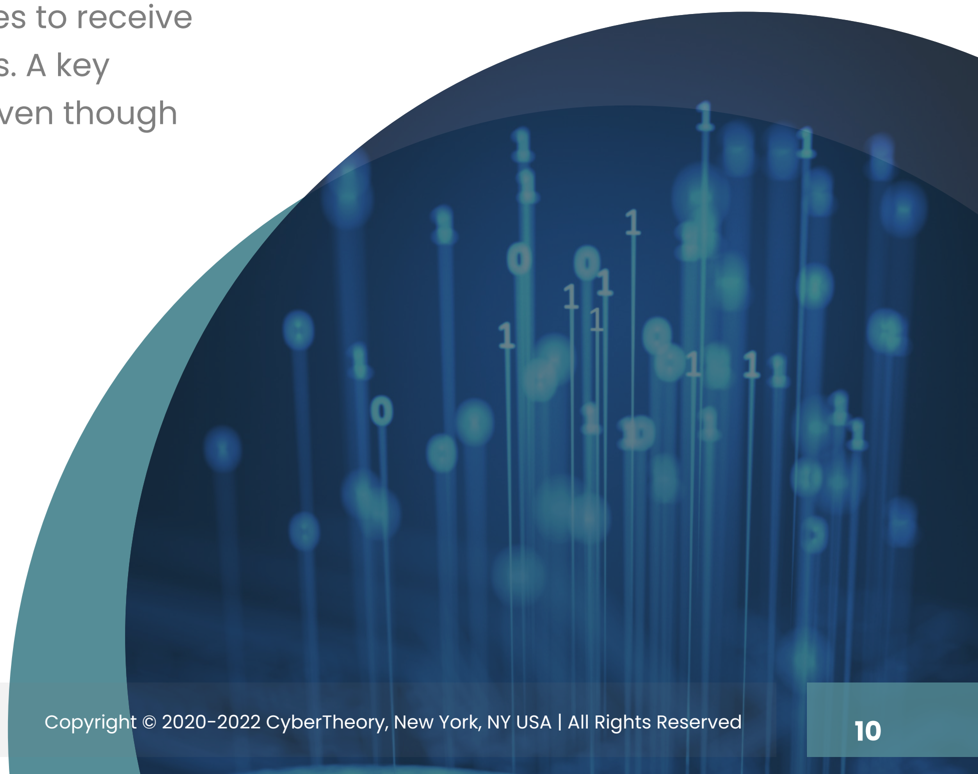
The malware can then steal personal or financial data and spread very quickly by issuing instructions to scan the network for other computers.

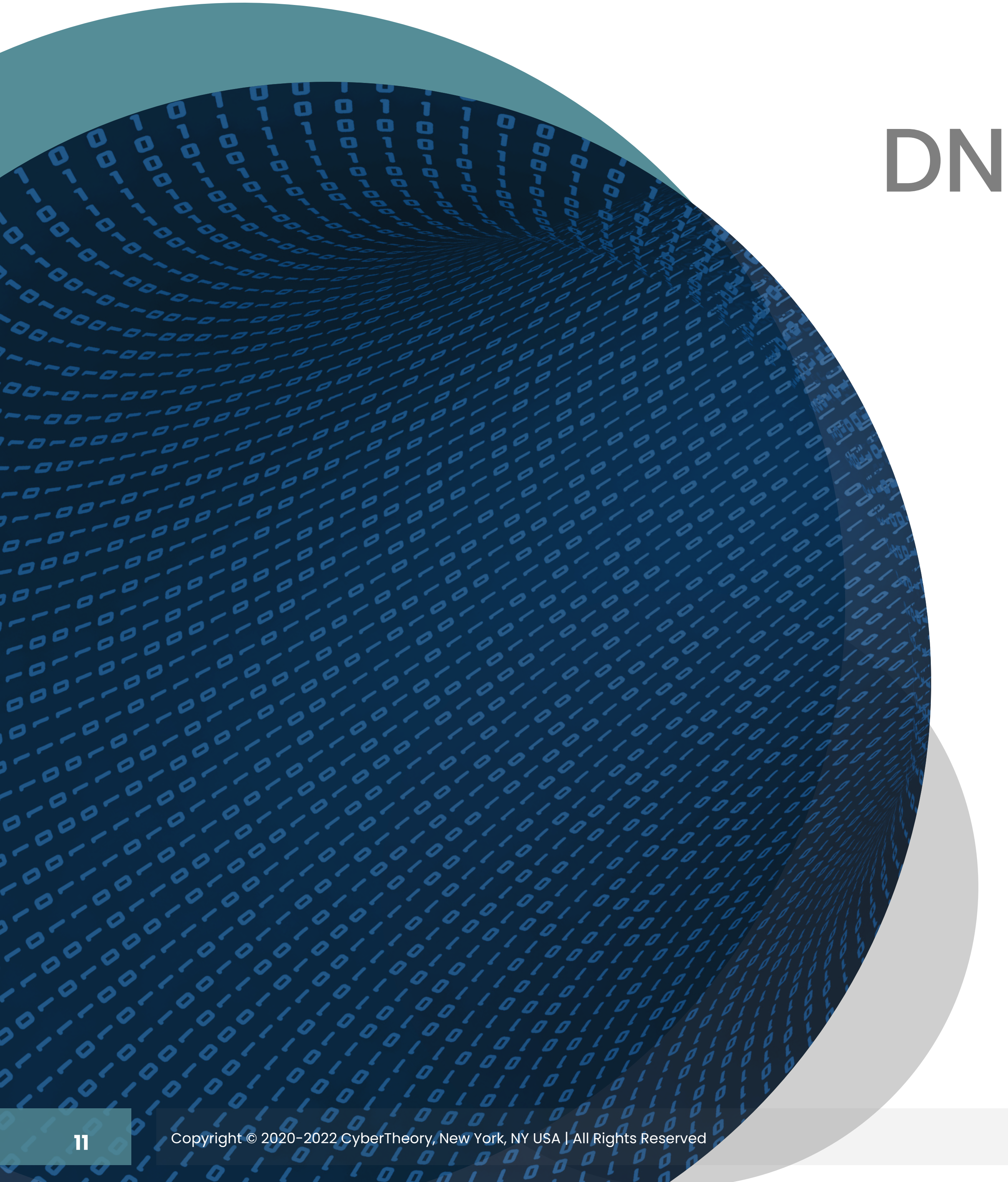
Malware Using Domain Generation Algorithms

Domain generation algorithms (DGAs) randomly generate large numbers of slightly different domain names. A DGA can, for instance, create thousands of domains in a day that are each a slight variation of www[.]badguys[.]com. Attackers developed DGAs so that malware can generate these domains and use them for C2. Unit 42 has observed that 18% of malware uses DGAs to automatically create thousands of C2 domains every day—of which attackers may use one—so that defenders can't block them.

Malicious domains controlled by attackers enable rapid movement of C2 channels from point to point, bypassing traditional security controls like blacklists or web reputation filtering.

Infected computers contact some of these new domain names to receive commands and updates. A key aspect of DGAs is that, even though thousands of domains can be generated in short order, not all of them need to be registered. Eighty percent of malware uses DNS to initiate C2 procedures that can be used to steal data and spread malware.





DNS Tunneling

This technique, increasingly used by advanced persistent threat (APT) actors, lets attackers encode their payloads in small chunks within DNS requests to bypass security controls. Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. Once a victim's device is compromised, the infected device sends a request within the DNS traffic. The DNS server is instructed to connect to the cybercriminals' server, establishing a channel through which to steal and transmit data. With DNS tunneling, DNS requests pass through the normal DNS server, inside and outside a company's firewall. However, tunneled data hidden in the DNS requests goes unnoticed. Attackers have used DNS tunneling extensively in recent years because it works.

Why Current Security Approaches Fail

I could make a joke here, but I won't. Current approaches to blocking malware attacks that use DNS are inadequate for several reasons. To begin with, it is difficult to address the many ways attackers can use DNS to compromise an organization. Many organizations focus solely on protecting their DNS infrastructure—and rightfully so. If DNS goes down, they can no longer access the internet.

What they don't focus on is the hidden threat: attackers using DNS itself to spread malware or steal data. Some organizations do nothing to protect DNS, leaving it wide open for attackers. Many organizations don't have DNS monitoring and instead only block malicious domains, essentially doing nothing to address malware that abuses DNS.

Static Lists.

Other security teams take a blacklisting approach to blocking attacks that use DNS, relying on relatively static threat feeds that work off known bad domains. However, as malware's use of DGA grows, the effectiveness of blocking known malicious domains alone becomes more limited. Using a list of randomly generated domains for C2 can overwhelm the signature capability of legacy tools and traditional security approaches.

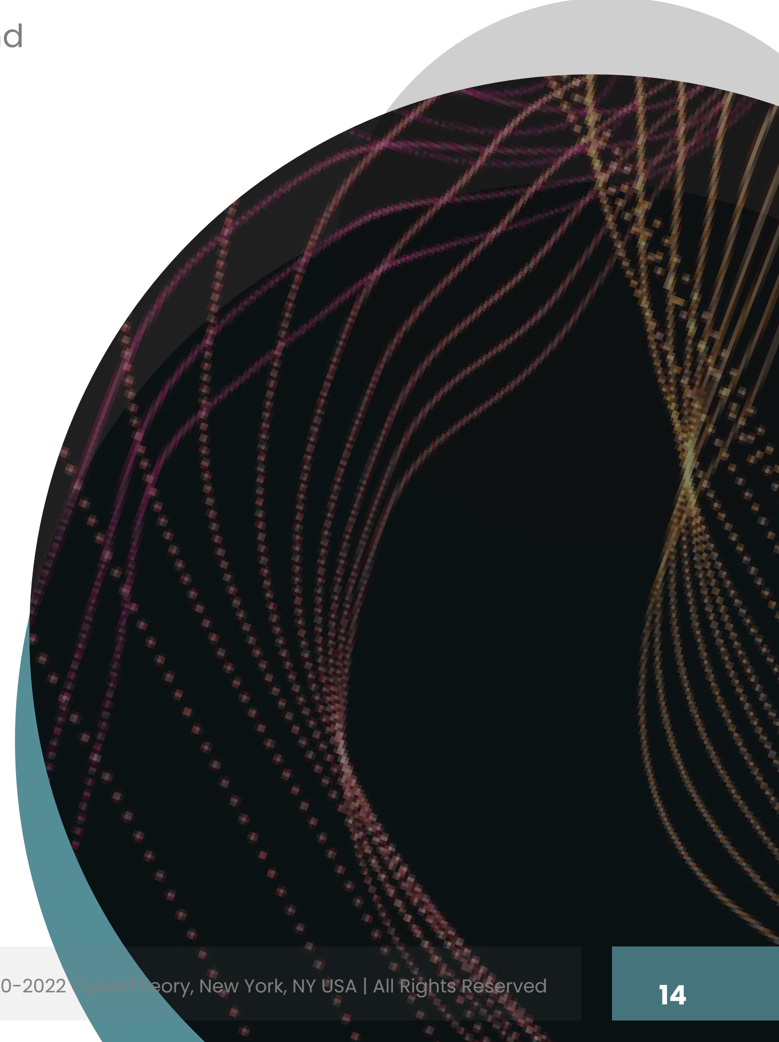
A limited set of signatures simply cannot scale to meet the growing threat of DNS-based attacks. Additionally, relying on static lists limits the amount of context defenders can access to fully understand the attacks against their network. Although threat intelligence feeds are regularly updated with indicators or artifacts derived from a source outside the organization, daily or even hourly updates are too slow to keep up with the massive amount of DNS data.

Volume

The sheer volume of DNS traffic often means defenders simply lack the visibility or resources to universally inspect it for threats. With a traditional approach, security teams don't have the resources to be proactive or scale their DNS security.

Some organizations use standalone point products to address threats to their DNS. These tools may adequately address specific facets of DNS security, but even "best-in class" technologies come with limitations. For instance, these tools often require changes to DNS infrastructure if they are to work effectively. Disparate products also create siloes of threat intelligence and data that may not work with other areas of an organization's security structure. As a result, overwhelmed teams drown in uncoordinated data from independent tools. Multiple tools become more things to own and manage, adding complexity and drain on already limited human resources.

> "With a traditional approach, security teams don't have the resources to be proactive..."



Stop Attackers from

Using DNS

How can you regain control of your DNS traffic and prevent attackers from using DNS to attack your organization?

You need massive quantities of real-world security data, either that you collect yourself or gather through threat intelligence or cyber-threat alliances. With data from a large and expanding intelligence-sharing community, your protection will continue to grow.

Analytics,

Cloud & Automation

Your security teams need to be able to run analytics on that data. To address the dynamic nature of domains or DNS tunneling, your teams must employ machine learning to dynamically identify unknown bad domains. Without analytics, it is impossible to predict highly dynamic malicious domains. Behavioral analytics can also help determine a baseline of activity, understand general patters and find what is normal. When defenders see signals that require action, analytics can help determine how manual or automated that action should be. Analytics can also understand which signals need to be acted upon, helping your teams prioritize time and resources.

Because many DNS-based attacks happen so quickly, it is imperative that security teams spend less time manually responding to attacks. To stand a chance, defenders need automation. Automation can help quickly determine infected machines, automate responses, and contain threats before they spread to other areas of a network. Security teams need integrated innovations that extend the value of existing security investments without complicating operations.

Using the cloud, your DNS protections can scale infinitely and always stay up to date, giving you a critical new control point from which to stop attacks that use DNS. Cloud-based innovations enable your defenders to develop and deploy new detection techniques that your organization can take advantage of instantly. Cloud-based protections update instantly without requiring you to update or make changes to software, which means less work for your security operations center (SOC) teams.

Full Visibility & Context for DNS Traffic

To protect against threats over DNS, you need superior detection combined with analytics to empower your security personnel with the context to quickly and effectively craft policies and respond to threats. Visibility into your DNS traffic enables you to identify malicious and benign traffic and trends. Context around security events allows you to understand why a domain was blocked and the history of that domain.

You can use this intelligence to optimize your policies and security posture as well as identify the nature and scope of any malicious activity so you can quickly move to remediate any issues.

No Extras

Your security teams must avoid deploying disparate tools that are poorly integrated or require changes to DNS routing. Many of these tools weren't designed for automation, forcing your analysts to manually stitch together insights from multiple disparate sources before acting. These products also don't automatically share data or insights, and they won't let you coordinate alerts across your entire security stack. As a result, your teams can't approach protection holistically, resulting in slower responses to threats.

Category-Based Actions

Not all threats over DNS are equal, and each may require a different response. For example, malware may require simple blocking and alerting, while C2 requires sink-holing as well as identification, quarantining, and inspection of potentially infected endpoints. In addition, dynamic DNS or newly registered domains—while not explicitly threats— can be considered higher risks to which certain systems on your network should not be exposed.

Automated responses based on DNS traffic categories enable fine-grained control over your DNS traffic to more quickly and efficiently mitigate threats while also reducing your risk exposure.

DNS Security
Best Practices

In addition to deploying the right technology, there are other best practices your organization can follow to protect your network from DNS-based threats.

Implement a security education and awareness program to train your staff on what to look for in suspicious emails. Encourage them to take care when following links to avoid installing malware. Phishing training can help them learn to recognize, avoid, and report email-based attacks.

Understand the threat landscape and set up a threat intelligence program to understand what threats and techniques exist. With this knowledge, you can ensure you have the right technology stack to keep your network safe.

Don't just look at DNS traffic. Collecting DNS logs has little value unless you understand what you're looking at, what the data is telling you and what you can do to secure your network from DNS-based attacks.

If a DNS server is compromised, it may feed you false responses meant to direct your traffic to other compromised systems or enable a man-in-the-middle attack.

Develop a strategy for your mobile employees as they can put company data at risk. Warn them against using unsecured, free or public Wi-Fi, as adversaries can easily put themselves between employees and the connection point. Integrate multi-factor authentication. Assume a high risk of devices being lost or stolen, and have a plan in place.

Approach Network
Security Holistically

Don't rely on a single product that promises to solve all your security problems. Instead, take a holistic approach to network security and ensure you have all the right tools to combat modern threats. Look at your security tools' capabilities and whether you can use them together effectively. You need tools with multiple capabilities that address various threat vectors, including intrusion prevention, URL filtering and file blocking.

When evaluating vendor solutions, it's important to make direct comparisons in proofs of concept.

Every environment is different, and independent vendor-neutral testing for DNS-layer security has not yet been established.

Require automated response, not just signals or alerts. Threats move so fast that alerts or signals alone are ultimately not helpful. By the time an analyst has prioritized an alert, confirmed a threat and identified the threat and its source, it is likely too late. Your security systems must be able to automatically determine threats and quarantine potentially infected systems before more damage is done.

If you aren't sure whether your organization is implementing best practices in your DNS security strategy, you should conduct a Best Practice Assessment to assure yourself, your board and your C-suite that you are on the right track. There are lots of companies who can help you do this. We think Palo Alto Networks has one of the most comprehensive and best offerings on the market, but you should also consider Andy Jenkinson's company and their Whitethorn Shield® offering as an actionable alternative – they are experts in DNS and Domain security.

The Danger in
“Not Secure” Domains

It is a Fact. A “Not Secure” domain acts as beacon for cybercriminals.

Websites that use https create an encrypted SSL connection between the web server and your browser. Encrypting the connection prevents a third party from intercepting communications and helps provide a degree of privacy in transit.

The best analogy for this is a postcard vs. an envelope. Http – a regular unencrypted website – is like a postcard. Anyone in between your computer and the web server can see what data you’re exchanging. Https – an encrypted website – is like an envelope. It also has the side benefit of helping – but not guaranteeing – to ensure that you’re actually visiting the real website and not a cloned copy set up to trick you. (The website operator has to pay money to get the certificate needed for https. While it’s not impossible for a bad guy to get a certificate, it’s generally less likely.)

Https is simply using an envelope. It provides privacy for your data while it is in transit. Really, though, that’s all it provides. Https doesn’t do anything to improve your security once you’re on the website. It can still be infected with malware. The website operators can still mishandle your data. They can still use trackers of various sorts. They can still be hacked. In other words, an https site can be just as dangerous as an http site.

The difference is that you’re not going to get mugged en route.

Not Secure domains are flagged up as being insecure, and OSINT technology provides this information to anyone willing to subscribe. A cybercriminal can readily identify common vulnerabilities and exposures (CVEs) and utilize known exploits to attack its target. The lack of basic security fundamentals allows successful attacks, which are completely avoidable.

A Common
Case Study:

A distribution and logistics company based in Delaware with annual revenue of $250m, a seasoned executive team and a very experienced CISO managing security with a competent and fully staffed team, was the recent victim of a stage one ransomware attack.

They have been in business for 28 years and have never had a security disruption. Then, suddenly one day, their systems get locked down and they are held to ransom for their data. The business is halted, and crisis calls (both internal and external) ensue to derive how this issue has manifested.

The attackers, who turn out to be based in Asia, have never even heard of the target company until they set up the attack – to the attackers, the Delaware Company is simply a vulnerable opportunity.

They learned of the company's vulnerability by virtue of the OSINT technology that flagged Not Secure URLs, which was originally developed to provide visibility, and when actioned, security. This flag acted as a beacon and notified the cybercriminals to scan their internet-facing domains services and infrastructure.

By being flagged as Not Secure and facing the internet, this messaging provided the threat actors with several attack options to exploit and discover the most effective using one of several unpatched software exploits, including cross site scripting. This, in conjunction with simple social engineering, and the attackers were in and moving laterally through the target's network, completely unbeknown to the target.

When the threat actors had ensured sufficient exfiltration of unencrypted data, whilst also encrypting the files on the target's infrastructure, the victim was then informed that the data would be shared unless a payment was made, thus initiating the simplest form of a stage one ransomware attack.

How did this happen? In this case, an expired digital certificate set off the notification alarms, but not to the owners. Digital certificates provide encryption, authentication and data integrity. They frequently expire, and when they do and are not properly managed, the situation is alerted to OSINT, and the information is sharable in the public domain.

Whitethorn Shield®

Whitethorn Shield® was developed by CIP to provide complete, proactive, defensive internet-facing security and capability. Currently, cybercriminals have a distinct advantage as they simply need to find a single access point, and by subscribing to the OSINT functionality, they can receive alerts and notification of insecurities and vulnerabilities on which to launch attacks.

CyberTheory's objective in this White Paper is to draw attention to the often overlooked hygiene requirement, the risks associated and to identify some alternative solutions available to organizations who need help addressing the issues.

Our objective is not to promote solutions, though we are comfortable mentioning CIP and PAN, as we have long and trusted relationships with both companies and know that their solutions provide solid value. We are not compensated in any way, nor do we share in any equity plan offered by CIP or Palo Alto Networks.

For more information about Whitethorn Shield®, Palo Alto Networks or other third-party sources for system solutions and DNS/Domain security in general, please contact:

Steve King
sking@cybertheory.io

CYBER THEORY

cybertheory.io
212.518.1579 • info@cybertheory.io
530 7th Avenue, New York, NY 10018