unit42.paloaltonetworks.com /three-dns-tunneling-campaigns/

Leveraging DNS Tunneling for Tracking and Scanning

Shu Wang, Ruian Duan, Daiping Liu ⋮ 25-31 minutes ⋮ 5/13/2024

This post is also available in: 日本語 (Japanese)

Executive Summary

This article presents a case study on new applications of domain name system (DNS) tunneling we have found in the wild. These techniques expand beyond DNS tunneling only for command and control (C2) and virtual private network (VPN) purposes.

Malicious actors occasionally employ DNS tunneling as a covert communications channel, because it can bypass conventional network firewalls. This allows C2 traffic and data exfiltration that can remain hidden from some traditional detection methods.

However, we recently detected three recent campaigns using DNS tunneling for purposes outside of traditional C2 and VPN use: scanning and tracking. In scanning, adversaries employ DNS tunneling to scan a victim's network infrastructure and gather information useful for future attacks. In tracking, adversaries use DNS tunneling techniques to track delivery of malicious emails and monitor the use of Content Delivery Networks (CDN).

This article provides a detailed case study that reveals how adversaries have used DNS tunneling for both scanning and tracking. We aim to increase awareness of these new use cases and provide further insight that can help security professionals better protect their networks.

We have built a system to monitor for DNS tunneling, and this detection is embedded in our DNS Security solution. Palo Alto Networks Next-Generation Firewall customers can access this through our DNS Security subscription to help secure their environment against this malicious activity. Customers also receive protection from the threats discussed here through the Advanced URL Filtering subscription.

- Cortex XDR customers receive protection against the DNS tunneling techniques mentioned in this article through our Cortex XDR Analytics Engine.
- Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the IoCs shared in this research.
- Prisma Cloud protects cloud environments against DNS tunneling techniques mentioned in this article.
- If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **DNS Tunneling**, **DNS Security**

Table of Contents

DNS Tunneling

DNS tunneling embeds information into DNS requests and responses in a manner that allows a compromised host to communicate through DNS traffic with a nameserver controlled by an attacker. An example is illustrated below in Figure 1.

A typical use case for DNS tunneling includes the following steps:

- Attackers first register a domain malicious[.]site and then establish a C2 server that uses DNS tunneling as a communication channel. Attackers have many options to set up this C2 channel, such as by abusing Cobalt Strike.
- Attackers can create, develop or acquire malware that communicates with the server as a client and send this malware to a compromised client machine.
- The compromised machine is usually behind a firewall and cannot directly communicate with attackers' servers. However, the malware can encode the data into the subdomain of malicious[.]site and make a DNS query toward the DNS resolver, as shown in Figure 1.
- Due to the unique nature of tunneling fully qualified domain names (FQDNs), the DNS resolver cannot find corresponding records from its cache. As a result, the resolver will then conduct recursive DNS queries toward root nameservers, top-level domain (TLD) nameservers and attacker-controlled authoritative nameservers for this domain.
- Attackers can obtain the decoded data from DNS traffic and manipulate the DNS response to infiltrate malicious data to the client.

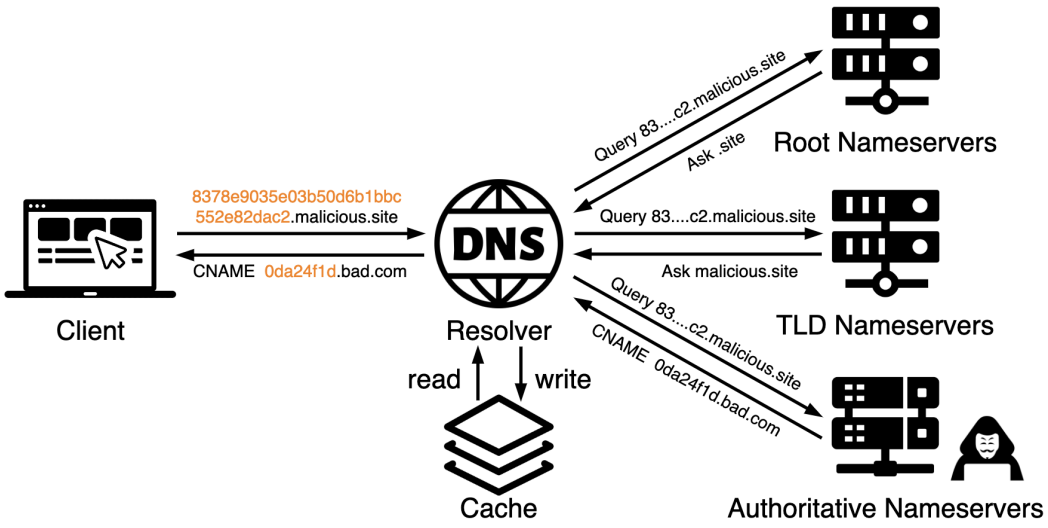

Figure 1. An overview of data exfiltration and infiltration with DNS tunneling.

How Is DNS Tunneling Hidden?

DNS tunneling is hidden due to three factors.

- Traditional firewalls can reject unauthorized traffic. However, DNS traffic over User Datagram Protocol (UDP) port 53 is ubiquitous and commonly allowed through firewalls and other network security measures.
- DNS tunneling is conducted via a logical channel between the compromised client and the attacker's server, with the implementation of DNS protocol. That means the client machine does not communicate with the attacker's server directly, adding another layer of obscurity.

- Attackers typically encode data sent during exfiltration and infiltration with their own customized methods, which disguises the data within seemingly legitimate DNS traffic.

How Do Adversaries Leverage DNS Tunneling?

The use of DNS tunneling for C2 purposes enables attackers to establish stealthy and resilient communication channels, facilitating malicious activities such as data exfiltration and infiltration. Well-known campaigns such as DarkHydrus, OilRig, xHunt, SUNBURST and Decoy Dog leverage DNS tunneling for C2.

The DNS types used by attackers include:

- IPv4 (A)
- IPv6 (AAAA)
- Mail exchange (MX)
- Canonical name (CNAME)
- Text (TXT) records

Some VPN vendors also use DNS tunneling for legitimate purposes, such as bypassing firewalls to avoid internet censorship or network service charges.

In addition to C2 and VPN purposes, attackers can also use DNS tunneling for tracking and scanning, as we've observed in recent tunneling campaigns.

- DNS tunneling for tracking:
  - Attackers can track victims' activities with regard to spam, phishing or advertisement contents. They do so by delivering malicious domains to victims with their identity information encoded in subdomain payloads.
- DNS tunneling for scanning:
  - Attackers can scan network infrastructure by encoding the IP address and timestamp in the tunneling payloads, with spoofed source IP addresses. Then, the attackers are able to discover open resolvers so that they can exploit resolver vulnerabilities to perform DNS attacks – which can lead to malicious redirection or denial of service.

To better understand these two new use cases, our next sections cover the campaigns we have discovered using DNS tunneling for tracking and for scanning.

DNS Tunneling for Tracking

To track a victim's behavior in conventional C2 communications, a threat actor's malware embeds data from a user's actions in URLs that it transmits to a C2 server through web traffic. In DNS tunneling, attackers accomplish the same result by using subdomains in DNS traffic.

In this application of DNS tunneling, an attacker's malware embeds information on a specific user and that user's actions into a unique subdomain of a DNS query. This subdomain is the tunneling payload, and the DNS query for the FQDN uses an attacker-controlled domain.

An authoritative nameserver for the attacker-controlled domain receives the DNS query. This attacker-controlled nameserver stores all DNS queries for the domain. The unique subdomains and timestamps of these DNS queries provide a log of the victim's activity. This is not limited to a single victim, and attackers can use it to track multiple victims from their campaign.

TrkCdn DNS Tunneling Campaign

We call this campaign "TrkCdn" due to the characteristics of the domain names used for its DNS tunneling. Based on our analysis, we believe the DNS tunneling technique used in the TrkCdn campaign is meant to track a victim's interaction with its email content. Our data indicates the attacker targeted 731 potential victims. This campaign used 75 IP addresses for nameservers, resolving 658 attacker-controlled domains.

Each domain only uses a single nameserver IP address, while one nameserver IP address can serve up to 123 domains. These domains use the same DNS configurations and the same encoding method for their subdomains. The attacker registered all domains under [.]com or [.]info TLDs and set domain names by combining two or three root words, which is a practice attackers use to avoid domain generation algorithm (DGA) detection.

A subset of these domains are as follows:

- simitor[.]com
- vibnere[.]com
- edrefo[.]com
- pordasa[.]info
- vitrfar[.]info
- frotel[.]info

A list of these domains along with sample FQDNs, nameservers, nameserver IP addresses and registration dates are shown below in Table 1. Because this campaign leveraged DNS tunneling only under the trk subdomain and configured a CNAME record under the cdn subdomain, we named this campaign TrkCdn.

Domain	Sample FQDN	Nameservers	Nameserver IP Address	Registration Date
simitor[.]com	04b16bbbf91be3e2fee2c83151131cf5.trk.simitor[.]com	ns1.simitor[.]com ns2.simitor[.]com	193.9.114[.]43	July 6, 2023
vibnere[.]com	a8fc70b86e828ffed0f6b3408d30a037.trk.vibnere[.]com	ns1.vibnere[.]com ns2.vibnere[.]com	193.9.114[.]43	June 14, 2023
edrefo[.]com	6e4ae1209a2afe123636f6074c19745d.trk.edrefo[.]com	ns1.edrefo[.]com ns2.edrefo[.]com	193.9.114[.]43	July 26, 2023
pordasa[.]info	2c0b9017cf55630f1095ff42d9717732.trk.pordasa[.]info	ns1.pordasa[.]info ns2.pordasa[.]info	172.234.25[.]151	Oct. 11, 2022
vitrfar[.]info	0fa17586a20ef2adf2f927c78ebaeca3.trk.vitrfar[.]info	ns1.vitrfar[.]info ns2.vitrfar[.]info	172.234.25[.]151	Nov. 21, 2022
frotel[.]info	50e5927056538d5087816be6852397f6.trk.frotel[.]info	ns1.frotel[.]info ns2.frotel[.]info	172.234.25[.]151	Nov. 21, 2022

Table 1. A subset of the domains used in the TrkCdn campaign.

Tracking Mechanism

We believe the DNS tunneling technique used in the TrkCdn campaign is meant to track a victim's interaction with its email content. Analysis of DNS traffic for simitor[.]com reveals how attackers could achieve this.

Here, we only show the tracking-relevant DNS configurations used by this tunneling domain. 193.9.114[.]43 served as the same IP address for the root domain, nameservers and cdn.simitor[.]com. This behavior is a common indicator for tunneling domains, because attackers need to build a nameserver for themselves while also trying to reduce attack cost. Therefore, they typically use only a single IP address for both domain hosting and name server.

All *.trk.simitor[.]com are redirected to cdn.simitor[.]com via a wildcard DNS record as shown below.

```
simitor[.]com A 193.9.114[.]43
ns1.simitor[.]com A 193.9.114[.]43
ns2.simitor[.]com A 193.9.114[.]43
cdn.simitor[.]com A 193.9.114[.]43
*.trk.simitor[.]com CNAME cdn.simitor[.]com
```

For the TrkCdn campaign, MD5 hash values represent email addresses in the DNS traffic. These MD5 values are subdomains for the DNS queries of a tunneling payload. For example, an email address of unit42@not-a-real-domain[.]com has an MD5 value of 4e09ef9806fb9af448a5efcd60395815. Therefore, the FQDN of a DNS query for the tunneling payload would be 4e09ef9806fb9af448a5efcd60395815.trk.simitor[.]com.

DNS queries for these FQDNs can act as a tracking mechanism for emails sent by the threat actor. For example, if a victim opens one of these emails, embedded content might automatically generate the DNS query, or a victim could click on a link within the email. However this happens, after an infected host generates a DNS query for the FQDN, the DNS resolver will contact the IP address for the authoritative nameserver of the FQDN. Due to its wildcard configuration, the victim's DNS resolver would obtain the following result:

```
4e09ef9806fb9af448a5efcd60395815.trk.simitor[.]com. 3600 IN CNAME cdn.simitor[.]com.
```

cdn.simitor[.]com. 555 IN A 193.9.114[.]43

Hence, even though the FQDNs vary across different targets, they are all forwarded to the same IP address used by cdn.simitor[.]com. This authoritative name server then returns a DNS result that leads to an attacker-controlled server that delivers attacker-controlled content. This content can include advertisements, spam or phishing contents.

For tracking purposes, attackers can query DNS logs from their authoritative nameservers and compare the payload with the hash values of the email addresses. This way, attackers can know when a specific victim opens one of their emails or clicks on a link, and they can monitor campaign performance.

For example, a graph showing the cumulative distribution function (CDF) of DNS queries for FQDNs from the TrkCdn campaign is shown below in Figure 2. This graph shows the total percentage of DNS queries for TrkCdn FQDNs from 0 to 30 days. The graph indicates that approximately 80% of victims view the campaign's emails only once, while an additional 10% view the messages again within approximately one week. Attackers can view this FQDN data from their authoritative nameservers in the same manner.

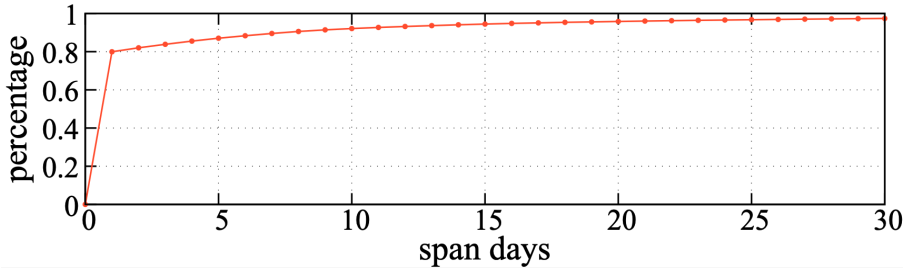

Figure 2. The CDF of FQDN span days in the TrkCdn campaign.

Domain Lifecycle

By investigating an older domain pordasa[.]info, we conclude that the TrkCdn domain lifecycle goes through four distinct phases. These four phases are as follows:

- Incubation phase (two to 12 weeks)
  - After the domain registration, attackers only configure the DNS settings and do nothing else, attempting to avoid malicious newly registered domain detection.
- Active phase (two to three weeks)
  - Attackers actively distribute thousands of FQDNs to the corresponding victims' email addresses.
- Tracking phase (nine to 11 months)
  - Victims query the FQDNs, while attackers track their behaviors by obtaining DNS logs.
- Retirement phase (one year after registration)
  - Attackers typically stop updating the domain registration after one year.

Below, Figure 3 shows an example of this lifecycle for pordasa[.]info. An attacker used this domain for DNS tunneling-style tracking, originally registering it on Oct. 12, 2022.

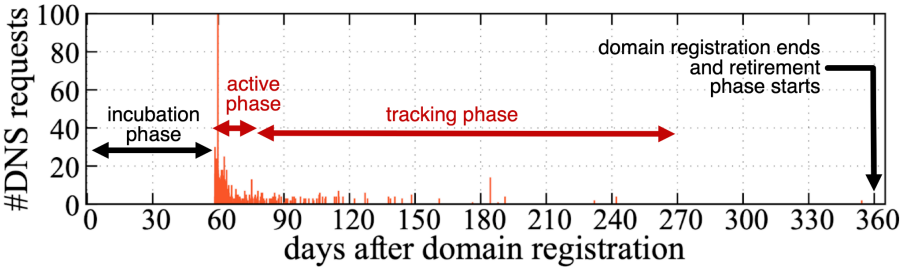

Figure 3. The lifecycle of the pordasa[.]info domain.

TrkCdn Persistence

Until February 2024, we found adversaries using new IP addresses and registering new domains for their authoritative nameservers associated with TrkCdn activity. Attackers registered these domains between Oct. 19, 2020, and Jan. 2, 2024. We analyze the timeline of domain registration and the domain's first use across different IP addresses.

Figure 4 tracks the use of TrkCdn domains associated with 49 IP addresses. As noted in Figure 4, the majority of IP addresses used for TrkCdn's authoritative nameservers lie within the 185.121.0[.]0/16 or the 146.70.0[.]0/16 subnets. This indicates that the threat actor behind TrkCdn tends to use specific hosting providers.

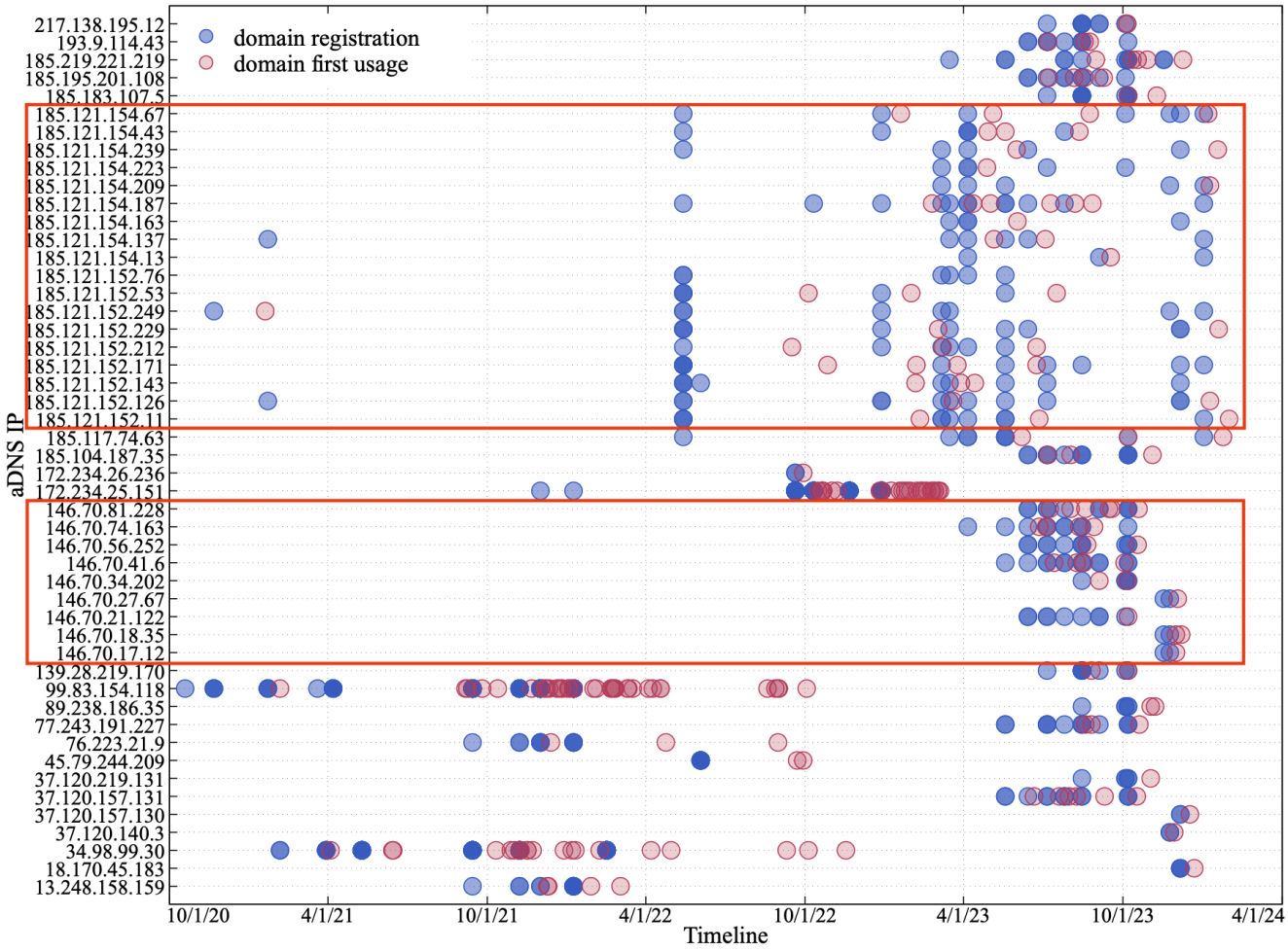

Figure 4. The timeline of TrkCdn domain registration and usage across different IP addresses.

SpamTracker DNS Tunneling Campaign

Our second example is a campaign using DNS tunneling to track spam delivery. Because this campaign uses DNS tunneling for spam tracking, we have nicknamed this campaign "SpamTracker."

This campaign uses a similar tracking mechanism as the TrkCdn campaign. This campaign is related to 44 tunneling domains that have an IP address of 35.75.233[.]210 for its authoritative nameservers.

These domains share the same DGA naming method and subdomain encoding method used by the TrkCdn campaign. Nameservers for the A records of these domains are hosted on IP addresses that fall into the 103.8.88[.]64/27 subnet. This campaign originated from Japan, and most of the targets were part of educational institutions.

This campaign employs emails and website links to deliver spam and phishing content that covers the following subjects:

- Fortune-telling services
- Fake package delivery updates
- Secondary job offers
- Lifetime free items

Figure 5 shows an example of these emails. The intent of the campaign is to lure victims to click on the links behind which threat actors have concealed their payload in the subdomains.

件名:受け取れるはずのお金たくさんあるのになぜか上手くいきませんよね?
Subject: You should receive lots of money, but it didn't happen due to some reason
貴方の金運は今、最高潮にあります。
人生で一番強いといって差し支えありません。
Your financial luck is currently at its peak. It's safe to say it's the strongest it has ever been in your life.
だからこそたくさんのお金に関する話が舞い込んできているはずです。
That's why you should expect to receive a lot of money-related discussions.
なのに受け取れない。どうして? なぜ? そう思われていませんか?
However, you can't receive it. Why? How come? Don't you think so?
理由はあります。貴方がその素晴らしい金運を正しい方法で使えていないからです。
たったそれだけの理由なんです。
There is a reason: you're not utilizing your wonderful financial luck in the right way. That's the only reason.
当サイトの先生がそれを見抜き、放っておけないと仰っています。
こちらから先生のお言葉を聞き、あふれ出る金運を使いこなして下さい。
Our website's teacher has seen through this and says they can't ignore it. Please listen to the teacher's words and make the most of the overflowing financial luck.
すぐに億万長者になれます。
You can become a millionaire or billionaire soon.
http://dzrsqnd6a3ata.wzbhk2ccghtshr.com/fi814kst/w3r

Figure 5. An email example (and English translation) used in the SpamTracker campaign.

Victims will be redirected to websites containing fraudulent information, such as the fortune-telling services shown in Figure 6.

Figure 6. A fake fortune-telling website in the SpamTracker campaign.

Table 2 lists six domains from this campaign along with an example of FQDNs, the nameservers, nameserver IP addresses and registration times.

Domain	Sample FQDN	Nameservers	Nameserver IP Address	Registration Time
wzbhk2ccghtshr[.]com	21pwt2otx07d3et.wzbhk2ccghtshr[.]com	ns01.wzbhk2ccghtshr[.]com ns02.wzbhk2ccghtshr[.]com	35.75.233[.]210	May 15, 2023
epyujbhfhbs35j[.]com	y0vkmu2eh896he7.epyujbhfhbs35j[.]com	ns01.epyujbhfhbs35j[.]com ns02.epyujbhfhbs35j[.]com	35.75.233[.]210	May 15, 2023
8egub9e7s6cz7n[.]com	q8udswcmvznk34q.8egub9e7s6cz7n[.]com	ns01.8egub9e7s6cz7n[.]com ns02.8egub9e7s6cz7n[.]com	35.75.233[.]210	May 15, 2023
hjmpfsamfkj5m5[.]com	run0ibnpq8r34dj.hjmpfsamfkj5m5[.]com	ns01.hjmpfsamfkj5m5[.]com ns02.hjmpfsamfkj5m5[.]com	35.75.233[.]210	May 15, 2023

uxjxfg2ui8k5zk[.]com	vfct3phbmc8qsx2.uxjxfg2ui8k5zk[.]com	ns01.uxjxfg2ui8k5zk[.]com ns02.uxjxfg2ui8k5zk[.]com	35.75.233[.]210	May 15, 2023
cgb488dixfxjw7[.]com	htujn1rhh3553tc.cgb488dixfxjw7[.]com	ns01.cgb488dixfxjw7[.]com ns02.cgb488dixfxjw7[.]com	35.75.233[.]210	May 15, 2023

Table 2. The list of the domains used in the SpamTracker campaign.

DNS Tunneling for Scanning

Network scanning, which seeks vulnerabilities within network infrastructures, is usually the first stage of cyberattacks. However, the use case of DNS tunneling for network scanning is understudied. As a result, uncovering the scanning applications of tunneling campaigns can help us prevent cyberattacks at an early stage, mitigating potential damage.

SecShow DNS Tunneling Campaign

We found a new campaign in which threat actors leverage tunneling to periodically scan a victim's network infrastructure, and then they typically perform reflection attacks. Their malicious actions include the following:

- Seeking open resolvers
- Testing resolver delays
- Exploiting resolver vulnerabilities
- Obtaining time-to-live (TTL) information.

This campaign generally targets open resolvers. As a result, we find victims mainly come from education, high tech and government fields, where open resolvers are commonly found. This campaign contains three domains, leveraging various subdomains to achieve different network scanning.

We list these three domains along with examples of FQDNs, nameservers, nameserver IP addresses and registration times in Table 3. These domains share the nameserver IP address of 202.112.47[.]45. We named this campaign "SecShow" due to the domain names the attackers used.

Domain	Sample FQDN	Nameservers	Nameserver IP Address	Registration Time
secshow[.]net	6a134b4f-1.c.secshow[.]net	ns1.c.secshow[.]net. ns2.c.secshow[.]net.	202.112.47[.]45	July 27, 2023
secshow[.]online	1-103-170-192-121-103-170-192-9.f.secshow[.]online	ns.secshow[.]online.	202.112.47[.]45	Nov. 5, 2023
secdns[.]site	0-53aa2a46-202401201-ans-dnssec.l-test.secdns[.]site	ns1.l-test.secdns[.]site. ns2.l-test.secdns[.]site.	202.112.47[.]45	Dec. 13, 2023

Table 3. The list of the domains used in the SecShow campaign.

SecShow Tunneling Use

SecShow uses different subdomain values for different scanning purposes. Here, we present four use cases to show how attackers scan the networks.

Case 1: bc2874fb-1.c.secshow[.]net

In this FQDN, bc2874fb is a hexadecimal encoding for IP address 188.40.116[.]251 and -1 is a counter to make the FQDN unique while the nameserver domain is c.secshow[.]net.

Attackers first spoof a random source IP address (e.g., 188.40.116[.]251) and make a DNS query to a candidate IP address for the encoded FQDN (bc2874fb-1.c.secshow[.]net). Once the attackers' authoritative nameserver (c.secshow[.]net) receives a DNS query, they can obtain the incoming resolver's IP address and the encoded source IP address used for this query.

Attackers repeat this process with different spoofed IP addresses and discover the open resolvers in the networks and the IP addresses that these open resolvers service. This can be the first step for DNS spoofing, DNS cache poisoning or DNS amplification attacks.

Case 2: 20240212190003.bailiwick.secshow[.]net

This FQDN type only appears every Monday at 19:00:03 UTC. The payload indicates a timestamp (e.g., on Feb. 12, 2024, at 19:00:03 UTC) that is the generation time for this FQDN.

Attackers spoof a source IP address and query this FQDN from a resolver IP address. Attackers can perform the following activities:

- Test the query delays for this resolver
- Check whether their domain is blocked and the query is forwarded to a sinkhole
- Exploit the vulnerabilities of this resolver

Attackers achieve the first two objectives by analyzing logs from their authoritative nameserver. To exploit the vulnerabilities of the resolver, the response of this query contains an A record for another domain:

```
20240212190003.bailiwick.secshow[.]net. 3600 IN A 202.112.47[.]45

afusdnfysbsf[.]com. 3600 IN A 202.112.47[.]45
```

In the above code, afusdnfysbsf[.]com was a malicious domain that had been revoked. However, its record can still be cached by resolvers. Therefore, attackers might leverage some resolver's cache vulnerabilities in older software versions (for example, CVE-2012-1033) to prevent domain name revocation.

Case 3: 1-103-170-192-121-103-170-192-9.h.secshow[.]net

The payload starts with a counter padding of 1 followed by two IP addresses of 103.170.192[.]121 and 103.170.192[.]9 that are the spoofed source IP address and the resolver's destination IP address.

This FQDN type is similar to Case 1. However, the A record of this FQDN is a random IP address that varies along with query attempts, with a long TTL of 86400. This feature could be exploited to perform the following activities:

- DNS amplification distributed denial-of-service (DDoS) attacks
- DNS cache poisoning attacks
- Resource exhaustion attacks

Case 4: 0-53ea2a3a-202401201-ans-dnssec.l-test.secdns[.]site

The payload contains a pre-padding of 0 followed by a hex-encoded IP address (53ea2a3a), a date (20240120), and post-padding (1). We observe that attackers use this type of FQDN to obtain the following information:

- Max/min TTL
- Timeout
- Query speed information

These are useful for some DNS threats such as Phoenix Domain [PDF] and Ghost Domain Names.

Mitigation

The DNS tunneling domains used in these campaigns can be detected by Palo Alto Networks firewall products. However, we also suggest the following measures to reduce the attack surface of DNS resolvers.

- Control the service range of resolvers to accept necessary queries only
- Promptly update the resolver software version to prevent N-day vulnerabilities

Conclusion

DNS tunneling techniques can be leveraged by adversaries to perform various actions not normally associated with DNS tunneling. Despite the conventional impression that tunneling is used for C2 and VPN purposes, we also find that attackers can use DNS tunneling as a vehicle for victim activity tracking and network scanning.

Palo Alto Networks Next-Generation Firewall customers receive protections against malicious indicators (domain, IP address) mentioned in this article via Advanced URL Filtering and our DNS Security subscription services.

- Palo Alto Networks Cortex XDR analytics customers receive protection against DNS tunneling techniques mentioned in this article via the DNS tunneling analytics detector.
- Advanced WildFire machine-learning models and analysis techniques have been reviewed and updated in light of the IoCs shared in this research.
- Prisma Cloud can detect, analyze and alert on malicious DNS traffic within cloud environments.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America Toll-Free: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- Japan: +81.50.1790.0200

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Indicators of Compromise

Domains used for DNS tunneling

- 85hsyad6i2ngzp[.]com
- 8egub9e7s6cz7n[.]com
- 8jtuazcr548ajj[.]com
- anrad9i7fb2twm[.]com
- aucxjd8rrzh7xf[.]com
- b5ba24k6xhxn7b[.]com
- cgb488dixfxjw7[.]com
- d6zeh4und3yjt9[.]com
- epyujbhfhbs35j[.]com
- hhmk9ixaw9p3ec[.]com
- hjmpfsamfkj5m5[.]com
- iszedim8xredu2[.]com
- npknraafbisrs7[.]com
- patycyfswg33nh[.]com
- rhctiz9xijd4yc[.]com
- sn9jxsrp23x63a[.]com
- swh9cpz2xntuge[.]com
- tp7djzjtcs6gm6[.]com
- uxjxfg2ui8k5zk[.]com
- wzbhk2ccghtshr[.]com
- y43dkbzwar7cdt[.]com
- ydxpwzhidexgny[.]com
- z54zspih9h5588[.]com
- 3yfr6hh9dd3[.]com
- 4bs6hkaysxa[.]com
- 66tye9kcnxi[.]com
- 8kk68biiitj[.]com
- 93dhmp7ipsp[.]com
- api536yepwj[.]com
- bb62sbtk3yi[.]com
- cytceitft8g[.]com
- dipgprjp8uu[.]com
- ege6wf76eyp[.]com
- f6kf5inmfmj[.]com
- f6ywh2ud89u[.]com
- h82c3stb3k5[.]com
- hwa85y4icf5[.]com
- ifjh5asi25f[.]com
- m9y6dte7b9i[.]com
- n98erejcf9t[.]com
- rz53par3ux2[.]com
- szd4hw4xdaj[.]com
- wj9ii6rx7yd[.]com
- wk7ckgiuc6i[.]com
- secshow[.]net
- secshow[.]online
- secdns[.]site

IP addresses associated with this activity

- 35.75.233[.]210
- 202.112.47[.]45

Additional Resources

- DNS Tunneling Archives – Unit 42, Palo Alto Networks
- Understanding DNS Tunneling Traffic in the Wild – Unit 42, Palo Alto Networks
- DNS Tunneling: how DNS can be (ab)used by malicious actors – Unit 42, Palo Alto Networks
- SolarStorm Timeline: Details of the Software Supply-Chain Attack – Unit 42, Palo Alto Networks
- DarkHydrus delivers new Trojan that can use Google Drive for C2 communications – Unit 42, Palo Alto Networks
- DNS Tunneling in the Wild: Overview of OilRig's DNS Tunneling – Unit 42, Palo Alto Networks
- OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory – Unit 42, Palo Alto Networks
- xHunt Campaign: Newly Discovered Backdoors Using Deleted Email Drafts and DNS Tunneling for Command and Control – Unit 42, Palo Alto Networks
- xHunt Campaign: New PowerShell Backdoor Blocked Through DNS Tunnel Detection – Unit 42, Palo Alto Networks
- Dog Hunt: Finding Decoy Dog Toolkit via Anomalous DNS Traffic – Infoblox
- CVE-2012-1033: Ghost Domain Names: Revoked Yet Still Resolvable – Internet Systems Consortium (ISC)
- Ghost Domain Reloaded: Vulnerable Links in Domain Name Delegation and Revocation [PDF] – NDSS Symposium

Updated May 13, 2024, at 10:15 a.m. PT to correct Table 2 and 3.

Most Read Articles