CISCO
SECURE

Security Report
Cisco Public

2022 DNS Discoveries

Using DNS to Uncover Trends and Protect Against Threats

The threat landscape is always changing. Billions of ever-expanding connections are made every day by organizations across the internet. There are more things to protect than ever before. Work patterns are constantly shifting, which means businesses are more vulnerable against increasingly sophisticated attacks.

Cisco Secure has a unique vantage point when it comes to cybersecurity. We know that you can't protect what you can't see. Because we resolve more than 620 billion daily DNS requests, we see more threats, more malware, and more attacks than any other security vendor in the world.

We also power all Cisco Secure services with the threat intelligence of Cisco Talos. Talos is the largest non-governmental threat research organization in the world, made up of an elite group of security experts.

These massive data sets and expert security researchers power our threat research and provide unmatched threat intelligence to stop attacks earlier. It's this foundation that lets us see and understand threats sooner and block them faster.

DNS for Security: An Underrated Part of a Modern Security Posture

The domain name system (DNS) was created to connect, not to protect. It was meant to connect users to websites or applications quickly and correctly, and it forms the foundation of internet. People use DNS thousands of times a day without knowing it – every time a user connects to a website, opens an app on their phone, or updates software, their device queries DNS servers to find the IP address associated with the domain.

The Domain Name System (DNS) allows clients to connect to websites, perform software updates, and use many of the applications organizations rely on.

Since most organizations don't bother to secure the DNS layer, they might be missing opportunities to block cyberattacks.

A recent report by Global Cyber Alliance explored the "Value of DNS Security", and found that:

- 1 in 3 breaches could have been contained by DNS
- Billions of dollars in major losses could have been prevented by DNS-layer security

Many of today's sophisticated attacks rely on DNS activity. This report looks at the top threats that exploited DNS for cyberattacks, as well as how DNS-layer security provides better accuracy and detection of malicious activity and compromised systems.

.

Threat 1: Malware

Definition: Malware is intrusive software that is designed to damage and destroy computers and computer systems. Malware is a contraction for "malicious software." Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware.

- 70% of organizations have users that were served malicious browser ads.
- 48% of businesses found information-stealing malware activity.

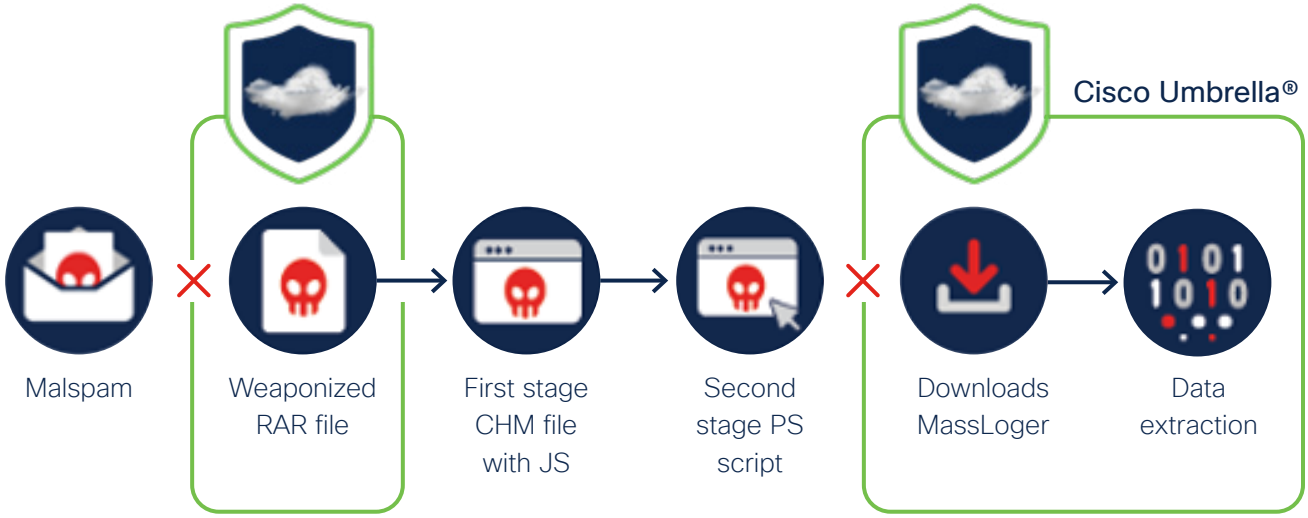
One type of malware, aptly called information stealers, is a shortcut to stealing credentials, passwords, and other sensitive or confidential information. It can compromise email programs, messaging apps, browsers, and more, stealing data and hijacking control of other programs and systems along the way.

Real-life threat: Masslogger

The malware campaign Masslogger focuses on business users and is delivered by email. The malicious email contains an RAR file with a compiled HTML (.chm) attachment.

When the user opens the attachment, it launches the chain of exploitation, which results in MassLogger malware being installed on the workstation.

This version of Masslogger retrieves credentials from applications such as Pidgin messenger client, FileZilla FTP client, Discord, NordVPN, Outlook, FoxMail, Thunderbird, FireFox, QQ Browser, and Chromium-based browsers (Chrome, Chromium, Edge, Opera, Brave).



Information stealer that arrives as an email with a RAR attachment containing a malicious .chm file.

Potential damage:

Can steal credentials from email clients, messaging applications, browsers, VPN, and FTP clients, which can be used to take over further systems.

Threat 2: Phishing

Definition: Phishing is the practice of sending fraudulent communications that appear to come from a reputable source. These attacks are usually performed through email. The goal is to steal sensitive data like credit card and login information or install malware on the victim's machine.

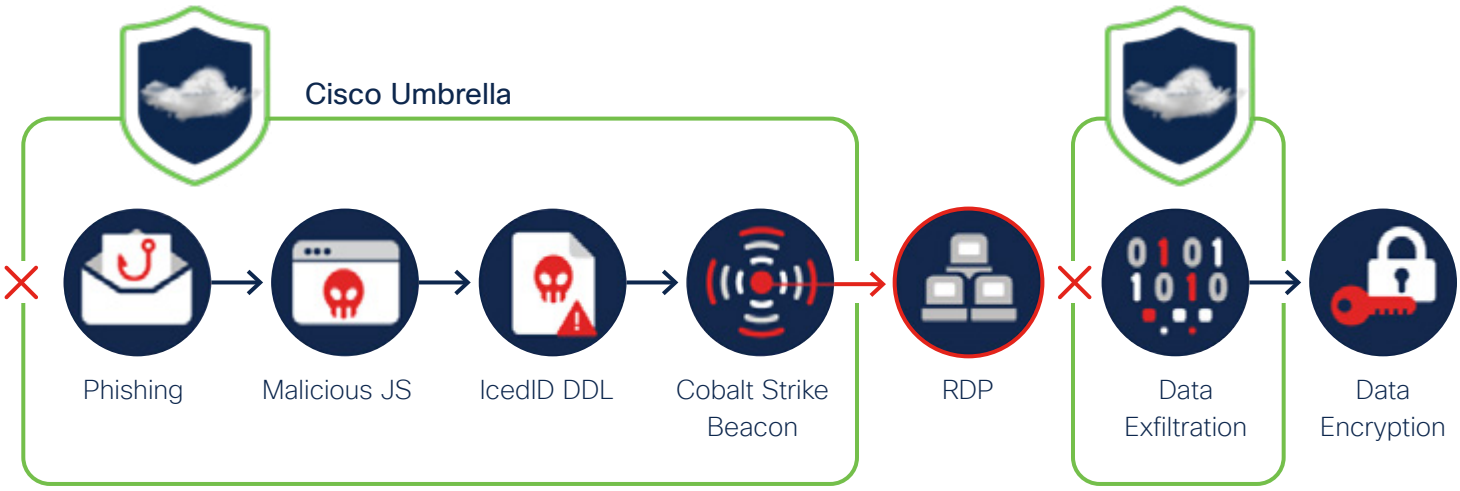
- 86% of organizations have had at least one user try to connect to a phishing site
- Phishing attacks account for 90% of data breaches

Real-life threat: Conti ransomware

Conti ransomware infection often begins with delivery of a malicious JavaScript file as an attachment in a phishing email.

If run on a Windows system, a DLL of IcedID is installed and the system starts beaconing to C2 servers. The C2 connections are the only activity for a few days, then a Cobalt Strike beacon is installed.

Within hours, threat actors use the IcedID DLL and Cobalt Strike payloads to explore the system, escalate privileges, move laterally, exfiltrate data, and finally encrypt all systems with AES-256 using the Conti ransomware. While encrypting files, Conti continues attempting to connect to other systems using SMB.



Threat 3: Command & Control

Definition: A command-and-control [C2] server is a computer controlled by an attacker which is used to send commands and remotely control compromised systems.

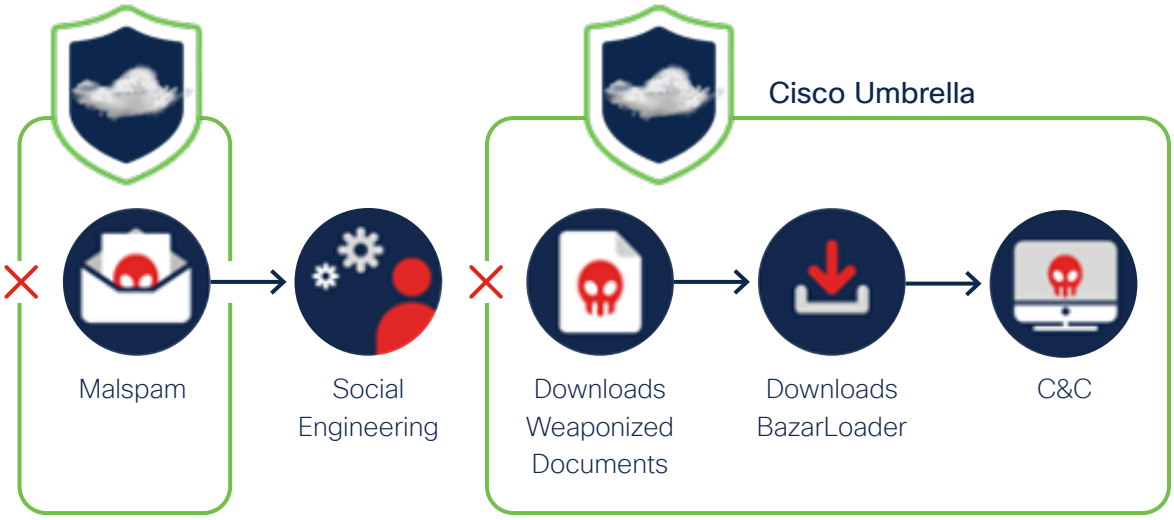
Cisco Umbrella threat intelligence detected an increase in command-and-control traffic starting in April 2021, which increased to a 31% higher than average rate by July 2021.

Real-life threat: BazarLoader

While BazarLoader has used a variety of tactics over the years, this particular malspam campaign sends emails that claim recipients need to unsubscribe from a trial service to avoid credit card charges. The attack leads to a legitimate-looking website operated by the threat actors.

When a user tries to unsubscribe, the page delivers a malicious Excel or Word document, which ultimately downloads BazarLoader. This malware strain uses C2 domains with the .bazar and hosting that is designed to make it very difficult, if not impossible, for law enforcement to take over these domains.

C2 activities include – but are not limited to – profiling, downloading additional payloads, executing PowerShell scripts, killing processes and services, and deleting itself. After that, follow-up malware (such as commodity trojans like Trickbot, infostealers, and ransomware) is downloaded on the compromised systems.



Loader used to gain a foothold in compromised networks.

Potential damage:

Can deliver wide variety of secondary payloads, such as ransomeware, infostealers, or tools providing further control of network.

Threat 4: Malicious Cryptomining

Definition: Malicious cryptomining malware is a browser or software-based threat that enables bad actors to hijack system resources to generate cryptocurrencies.

- The technology sector sees far more cryptomining traffic than any other industry
- Cryptomining generated the most DNS traffic out of any individual category. It's relatively noisy on the DNS side, as it regularly pings mining servers for more work.

Real-life threat: The lifecycle of a malicious cryptomining attack chain

Malicious cryptomining attacks often infiltrate networks by exploiting public-facing infrastructure that's not fully protected. Once these unpatched systems are accessed, the threat actors use the processing power of business-critical infrastructure to mine cryptocurrency, making money by using others' resources for their own gains.

Unauthorized cryptomining in your network can lead to performance degradation, increased energy consumption, or disruption of productivity. Plus, once an attacker has a foothold in your network, they can deploy other malware.

Malicious Cryptomining Attack Chain

1. A vulnerability is discovered in software frequently found running on publicly accessibile company servers.
2. Malicious actors develop and share exploits.
3. Attackers scan the internet to identify vulnerable infrastructure.
4. When vulnerable infrastructure is found, attackers do the following:
   - Use the exploit against company servers.
   - Deploy malicious scripts from C2 servers
5. Automation takes over, and:
   - Scripts download cryptocurrency miners
   - Cryptominers contact mining pools

Additional ways Cisco Umbrella leverages DNS to protect organizations

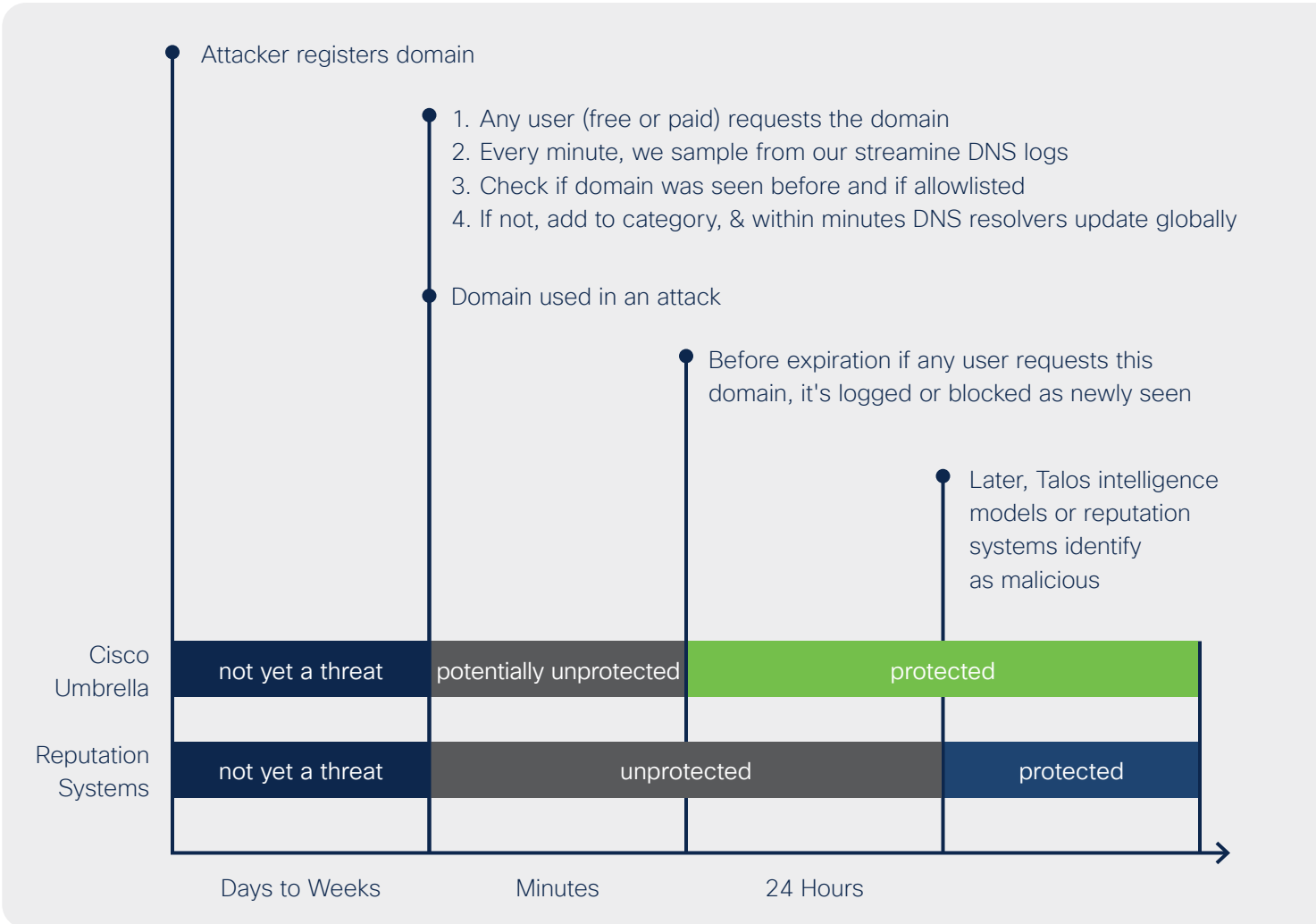
Cybersecurity is about more than just protecting what's "happening now", but also about what's "happening next." Our DNS data sources are massive and diverse; it represents many markets, geos, and protocols. The research models are continuously run against this data so we can uncover malicious domains, IPs, and URLs before they're even used in attacks. Our security researchers are always innovating and creating new models to provide better threat detection and classification.

That means we can see more and use all the patterns, trends, and telemetry that we see every day to know what to pay attention to and protect going forward.

Detect and block newly seen domains

New domains are created and published every day, but they aren't all used for legitimate purposes. Bad actors use new domains to host and deliver spam, malware, or botnets, often in the first minutes of the new domain being created

Newly seen domain category reduces risk of the unknown



Newly seen domain example (mcorecari.com)

A domain named mcorecari.com was discovered by Umbrella, categorized as Newly Seen Domain on Wednesday, September 22, 2021 6:14 AM. “Newly Seen Domains” (NSD) is a security category that identifies domains that have been queried for the first time within the past 24 hours by any user of Cisco Umbrella’s DNS service. Domains stay in the list for a period of 24 hours.

Later that same day, at 10:44 PM, the mcorecari.com domain was used in a phishing attack, impersonating a large bank in Japan. It was subsequently categorized as Phishing and blocked by Cisco Umbrella.

DNS tunneling

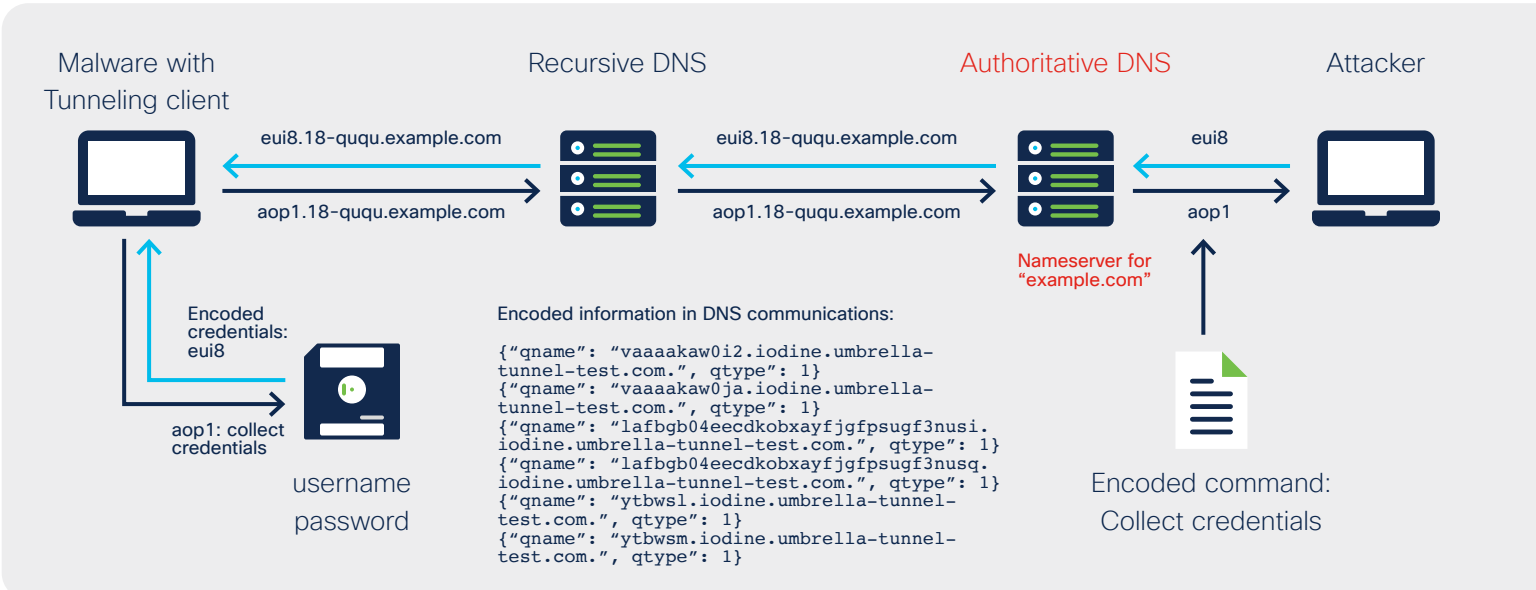
Because DNS traffic is widely used, it is often blindly trusted. DNS tunneling allows malware authors to communicate in a covert channel. Threat actors use DNS tunneling techniques to exfiltrate sensitive data out of corporate networks or to send malicious commands to be executed as part of an attack chain. DNS tunneling can also be used to circumvent security controls and even obtain free WIFI by bypassing authentication steps.

Real-life threat: DNS-tunneling example

Here, an attacker has incorporated a DNS tunneling kit into an authoritative DNS nameserver and installed malware with a DNS tunneling client on a compromised system. DNS tunneling attacks are particularly difficult to block as they only occur at the DNS layer, so many other security tools don’t block these.

- The attacker issues an encoded command (“aop1”) that will tell the malware on the compromised computer to collect credentials.
- The command is added to the domain (“aop1.18-ququ.example.com”) and sent over DNS.
- The malware receives the command and collects the credentials.
- The malware encodes them and sends them back over DNS. (“eui8”)

DNS-Tunneling example



DNS-layer security benefits

- Simplify security management: Cisco Umbrella's DNS-layer protection reduces the number of infections and alerts you see from other security products by stopping threats at the earliest point. With no hardware to install or software to manually update, ongoing management is simple.
- Improve internet performance: Umbrella has a highly resilient network that boasts 100% business uptime since 2006. Our carrier-neutral data centers worldwide use Anycast routing so requests are transparently sent to the fastest available connection with automatic failover.
- Block malware: By enforcing security at the DNS layer, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established.
- Increase visibility: Monitoring DNS requests provides better accuracy and detection of compromised systems and improves security visibility and network protection.
- Proactively respond to threats: Umbrella logs all DNS activity to simplify investigations. Umbrella Investigate provides context to prioritize incidents and speed up response. Cisco SecureX automates insights across Cisco products for quick answers.

> "After deploying Umbrella, we were able to reduce malware infections by more than 90% and the airline has not experienced any security incidents."
>
> Brett Stone, Network Operations Manager
> Cape Air

Why Cisco Umbrella

Cisco Umbrella analyzes internet activity to uncover known and emergent threats to protect users anywhere they go.

Most predictive intelligence

Our unparalleled intelligence enables us to uncover malicious domains, IPs, and URLs before they're even used in attacks.

Easiest deployment

There's no hardware to install or software to manually update, and customers can leverage their existing Cisco footprint to provision thousands of network devices and laptops.

Most open platform

Leveraging our bi-directional API, customers can easily integrate Umbrella with existing tools to automatically add to our platform or enhance another system – extending protection and enhancing information.

"Umbrella has given us visibility into our DNS traffic that we've never had before, enabling us to quickly respond to malware, command-and-control attacks, and more."

Brandon Wood, Information Security Officer
University of Alaska Anchorage

Schedule a personalized demo to see our DNS defense capabilities for yourself.