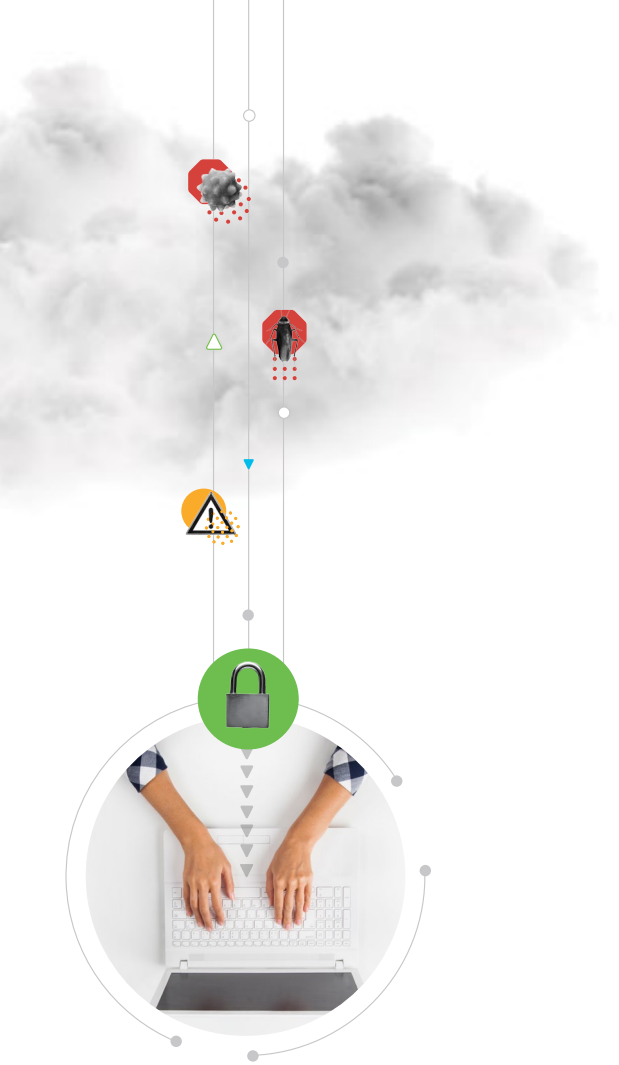
Cisco Umbrella

February 2021

Top cybersecurity trends 2021

Spotlight: Cryptomining



Introduction

For the majority of 2020, in the face of a global pandemic, the entire world grappled with massive change – in how we lived, how we worked, how we connected. But one area that's always been dynamic and rapidly evolving is the cyberthreat landscape.

Here at Cisco, we saw firsthand how commonplace threats quickly evolved into complex, multi-stage attacks that use tried-and-true malware methodology paired with innovative new tactics to cover their tracks.

In the face of these new threats, InfoSec teams have been feeling increasingly overwhelmed. The right information, however, can prepare you for what's out there.

Cisco Umbrella identified a number of major threat trends in 2020 that will have serious implications for years to come:

Trend spotlight: Cryptomining opened the door to other types of cyberthreats.

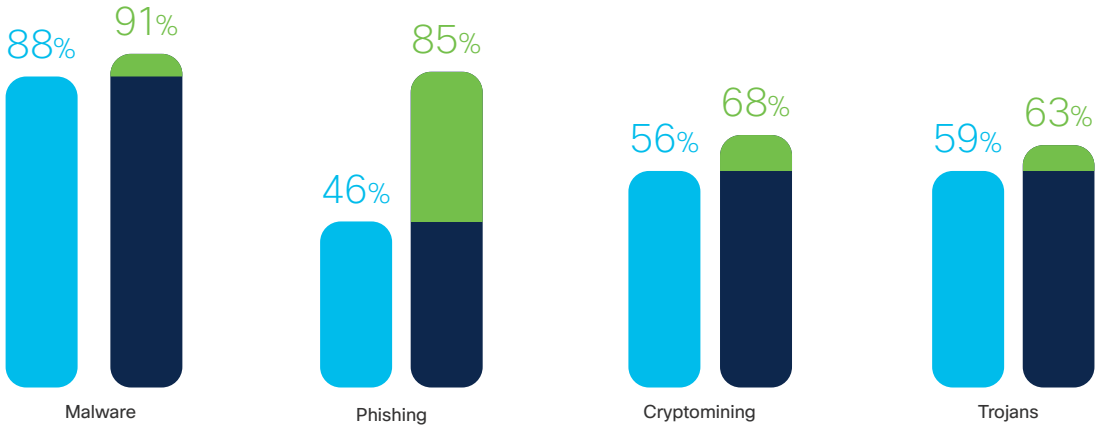
Before we dive in, let's take a look at the overall threat landscape and what's changed in the recent past.

The threat landscape in 2020

Phishing was on the rise as second most common threat.

Top cyberthreats found on Cisco Umbrella global cloud architecture

2019 ▸▸▸▸ 2020



Looking at the broad threats Cisco Umbrella's customer base encountered in the first nine months of 2020:

91%
of customers saw a domain linked to **malware**.

85%
saw a domain linked to **phishing**.

68%
saw a domain linked to **cryptomining**.

63%
saw a domain linked to **trojans**.

From 2019 to 2020, trojans and phishing swapped spots – in 2019, trojans were the number two threat at 59%, and phishing was in fourth with 46% impacted. In 2020, phishing rose by nearly 40%. Why the shift? One reason was connected to the pandemic – a huge increase in malicious phishing that preyed on people's fears about the virus.

Malicious cryptomining was once again the top form of attack.

Top cyberattacks on Cisco Umbrella global cloud architecture

2019	2020
1. Cryptomining	1. Cryptomining
2. IcedID	2. Emotet
3. Emotet	3. Ursnif/Gozi
4. Locky	4. COVID-19
5. Necurs	5. IcedID
6. Andromeda	6. Andromeda

In terms of the specific attacks and infiltrations we saw in 2020, it's no surprise that cryptomining was #1, having taken the top spot in 2019 as well. Why did cryptomining continue to be the most prevalent form of attack? Key reasons included:

- The relative ease with which criminals could monetize their activities
- Cryptomining's relatively small footprint was easier to hide
- A misperception that cryptomining was less dangerous than other threats – more a nuisance than a real danger to your environment

So, where did the data come from? A closer look at Cisco Umbrella

At Cisco, we believe it's better to predict and prevent cyberattacks than to respond and remediate after they strike. And doing that means we need data.

Every day, Cisco Umbrella's 33+ data centers process more than 350 billion internet requests from across 190 countries. This real-time DNS data is further enriched with data from both private feeds and a handful of public ones.

With such a massive and diverse data set, our threat analysis can uncover patterns that signal malicious behavior. This analysis is based on aggregated DNS query logs paired with scrubbed and anonymized customer demographic information. Together, they give us a unique perspective on global DNS traffic, which helps us see the trends and defend against potential threats.

Cisco Umbrella protects against more than 7 million malicious domains and IPs, while discovering over 60,000 new malicious destinations (domains, IPs, and URLs) every day. Each node of attack infrastructure is an opportunity to identify and neutralize threat architecture before it can be used for new attacks.

Leveraging data from Cisco Talos, one of the largest commercial threat intelligence teams in the world, Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files being used in attacks. We also feed huge volumes of global internet activity into statistical and machine learning models to identify new attacks being staged. Tapping into anti-virus engines, Cisco Advanced Malware Protection (AMP), and sandboxing with Cisco Threat Grid, Umbrella takes advantage of intelligence from millions of daily malware samples to provide the most effective defense against malicious files.

Learn more about Cisco Umbrella, the intelligence that powers it, and the protection it provides.

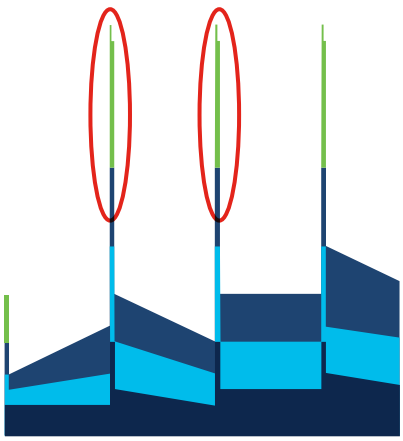
Trend spotlight

Cryptomining opened the door to other types of cyberthreats.

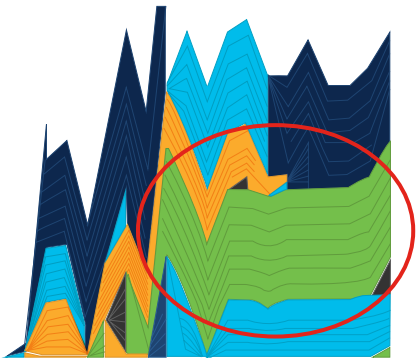
Of all the trends we saw in 2020, the fact that cryptomining remained the top threat was the least surprising news — it's been a well-documented trend across a variety of sources. However, because cryptomining is inherently chattier than other activities — i.e., it produces more DNS queries to properly sync with the blockchain network to successfully mine cryptocurrency — its strong lead in query volume over various forms of cyberattack is not as impressive as it appears. It's the consistently high volumes of DNS traffic over time that indicates a malicious party may be involved.

In addition, it's been argued that cryptomining isn't really an attack you actually need to worry about. This line of thinking, however, generally only considers *web-based* cryptomining, which only occurs while a user is on an infected web page; close the page and the threat is gone, so there's little risk of damaging hardware. Too often, though, organizations overlook *software-based* cryptomining, in which mining software installed on a machine operates any time the machine is on and connected to the Internet. Here, there is a much higher risk of damaging hardware. This could be considered an indicator of compromise (IOC).

Web-based vs. software-based malicious cryptomining



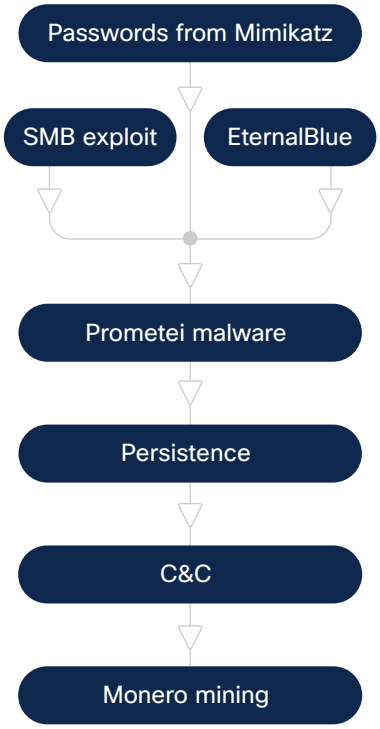
Web-Based Miners



Software-Based Miners

The Prometei botnet

The Prometei botnet has more than 15 executable modules.



With cryptomining software running on your machines or in your public cloud, you're footing the bill for electricity, internet service, web services, and hardware replacement (if your machine wears out faster than it would otherwise). However, that might only be the beginning.

In a more recent trend, cryptomining software running in your environment can also be just the first step in a multi-staged attack on your infrastructure. Malicious third parties can infiltrate your environment, then set up a miner to make passive income while they peruse your infrastructure to exfiltrate data or perform other malicious activities.

So, what can a multi-staged cryptomining attack look like? Meet Prometei, a cryptocurrency-mining, multi-modular botnet recently discovered by Cisco Talos. Employing multiple methods to spread across a network – including SMB with stolen credentials, PsExec, and WMI and SMB exploits – Prometei drops a payload focused on mining Monero cryptocurrency for the attacker. The software then uses a variety of crafted tools that help the botnet increase the number of systems that participate in the mining.

The infection starts with the main botnet file – which is copied from other infected systems by means of the SMB protocol, using passwords retrieved by a modified Mimikatz module and exploits like EternalBlue. From there, the botnet has more than 15 executable modules that are all downloaded and driven by the main module, which constantly communicates with the command-and-control (C2) server over HTTP. At the same time all of this is happening, Prometei also tries to recover administrator passwords; any discovered passwords are sent to the C2, then reused by other modules, which attempt to verify their validity on other systems using SMB and RDP protocols.

In short, cryptomining – already the most common threat – can also expand the potential attack surface, demanding a new type of security solution that can fight on multiple fronts.

Summary

The world is changing, threats are changing, and you should be changing too.

With the rise of the pandemic – and the accompanying move to remote work for most of the global workforce – 2020 was a time of dramatic upheaval in work, education, governance, and more. The risk profile of individuals working at home is considerably different than it is with the security infrastructure provided by organizations in an office setting. As a result, the threat landscape evolved – and will continue to evolve – but the bottom line is that malicious actors are still working hard to infiltrate your environment in a variety of new and changing ways. The pandemic may slow them down, but it won't stop them, and it shouldn't stop you either.

As attackers increasingly use complex, orchestrated attacks that leverage proven tactics, techniques, and procedures (TTPs), the cyber defender's job only grows more challenging. Throwing more time and more bodies at the problem no longer works – if it ever did. It's time to leverage novel solutions – like machine speed and predictive intelligence – to scale and adapt defenses to meet rising threats.

Here are a few recommendations for defending against these new threats:

- Implement scalable first-line-of-defense tools, like cloud security platforms and Secure Access Service Edge (SASE) solutions.
- Ensure your information security policies adhere to an internationally recognized information security management system (ISMS) like ISO 27001 or NIST.
- Employ network segmentation to help reduce outbreak exposures.
- Leverage timely, accurate threat intelligence that allows for such data to be incorporated into security monitoring.
- Fully embrace automated event sequencing and intelligent machine-generated analysis through machine learning.
- Existing Cisco Umbrella customers should enable the optional cryptomining policy in security settings.

About our experts

The data and analysis for this report were brought to you by the Cisco Umbrella Security Analytics and Research Teams. Recognized experts in the threat landscape, they identify new threats to help add to our intelligence, identify the latest attacker trends, and develop new processes and systems for locating malicious destinations. The research team takes a different approach to addressing threats; rather than waiting for them to hit, they proactively use Umbrella's predictive intelligence to spot the attackers.

Contributors to this report include:
Austin McBride | Shyam S. Ramaswami | Artsiom Holub

About our research methods

Using our massive and diverse dataset — collected across the more than 100 million users on our global cloud architecture — our world-class team of engineers, mathematicians, and security researchers work to apply statistical and machine learning models that can predict what threats are coming next.

Together, the team is able to statistically score the "guilt" of domains and IPs to determine if they're part of an attacker's infrastructure. More than a reputation score (which merely focuses on the past), we analyze both historical and live data — using statistical models to automatically score and classify that data so we can detect anomalies and uncover known and emerging threats. (In addition to automated classifiers, our security analyst team also adds malicious domains to block lists.) In essence, our research is able to predict the likelihood of whether a domain, IP address, or entire ASN is going to originate an attack or pose a security threat before they can actually do so.

Cisco Umbrella

About Cisco Umbrella

Cisco Umbrella delivers the most secure, most reliable, and fastest internet experience to more than 100 million users daily. By unifying multiple security solutions into a single service, Cisco Umbrella helps businesses embrace direct internet access, secure cloud applications, and extend protection to roaming users and branch offices.

Learn more about how to protect yourself from threats:

View a live demo