CISCO
SECURE

Defending Against Critical Threats

Analyzing Key Incident Trends

Exploring Cybercriminal Patterns

Hazel Burton

(Editor-in-Chief)

Eagles guitarist Joe Walsh once said, "As you live your life, it appears to be anarchy and chaos, with random events smashing into each other....and then later, when you look back on it, it looks like a finely crafted novel."

Unfortunately, that kind of clarity was hard to come by for cybersecurity defenders in 2021 who were (and still are) dealing with so many high-profile threats, including: Log4j, ransomware attacking critical infrastructure, more reported vulnerabilities than in any previous year, supply chain attacks growing in momentum, and Emotet coming back from the dead. And that's on top of generally staying ahead of day-to-day organizational risks.

To analyze the major threat trends from 2021, and help with some of that "finely crafted novel" clarity for defenders, I sat down with six expert threat hunters and analysts from across Cisco Secure. I asked them to tell me about their findings on one specific cybersecurity threat, or incident, from the past 12 months. Each expert chose to discuss a topic that tells us a lot about the current priorities of threat actors.

To give you some additional context, this content was written in January 2022. We don't cover what has been happening in Ukraine, however readers can keep up to date with Talos' threat advisory blog, which is constantly updated with the latest information.

This report also explores predictions and precedents for the year ahead. After what felt like a chaotic 2021, I wasn't sure how we would go about doing this. But when I talked to Matt Olney, Director of Threat Intelligence and Interdiction at Cisco Talos, he gave me this perspective:

> "Broadly speaking, over the last five years, nothing has happened that has fundamentally changed our approach as defenders. We are averaging one or two scary, out-of-nowhere vulnerabilities each year, and then it becomes a race between the adversaries exploiting it, and the defenders seeking to understand it and protect against it."

> "Supply chain attacks and ransomware are certainly a large concern, and this is why we're seeing an escalation in terms of worldwide governmental response here."

The expert analysis you'll read in this report highlights the crucial role of our defenders, and the capabilities that we as an industry have built based on the meticulous study of past attacker behavior.

Read on to learn some great perspectives on how to deal with critical threats, from experts whose job it is to spot cybercriminal patterns.

Table of Contents

Colonial Pipeline:

Moving Beyond Ransomware Thoughts and Prayers

With Matt Olney,
Director of Cisco Talos
Threat Intelligence and Interdiction

From all the threats you could have chosen to talk about from 2021, why did you choose Colonial Pipeline?

There are two things that I found interesting about Colonial Pipeline. One was the real-world impact and what happened to gas supplies on the East Coast of the United States. The attack inspired political pressure, and that subsequently led to an increase in the speed of response from the U.S. government on ransomware activities.

The second aspect is the reaction from the threat actors. It was very much an "Icarus" flying too close to the sun situation. They knew that they had overstepped by attacking critical infrastructure. And there was an immediate and profound response from the threat actor environment.

Things certainly changed after the Colonial Pipeline attack, and they remain changed to this day.

Colonial Pipeline Facts and Figures

- Colonial Pipeline handles 45% of all petroleum delivery on the East Coast of the U.S.
- The pipeline is 29,000 miles long
- The ransom was 75 Bitcoins (~$4.4m)
- 87% of gas stations in Washington D.C. were out of fuel

When did the ransomware attack start and what was the initial response?

To be very clear, Cisco wasn't involved in the Colonial Pipeline response. All my information is from public reporting.

In early May, very early on a Friday morning, a previously infected network at Colonial Pipeline became encrypted, and they essentially lost the entirety of their IT network.

Critical infrastructure environments are typically broken up into IT (information technology) and OT (operational technology), which is where the industrial pieces live. The things that drive the pipeline, pump the gas, and all the monitoring, are in OT.

Reportedly, Colonial Pipeline's OT environment was unimpacted. It was their IT environment that was affected by the encryption. Colonial very quickly paid the ransom of 75 Bitcoin, which on the date was roughly $4.4 million.

However, they found that the tool provided by the threat actor to do the decryption was so slow that it was faster to recover their data through traditional means. I don't think they would say that they got value out of their ransomware payment.

There were reports that because Colonial Pipeline was unable to track the gas and also bill for it (because that capability was in their enterprise IT environment), they chose not to pump gas. Even though the OT network was up and available.

To be clear, on the Colonial side, there were also concerns about ensuring that their OT network was secure. Colonial shut off pipeline operations within an hour of the encryption event. For six consecutive days, they didn't pump any gas at all to the East Coast.

To give you a sense of the significance of that, Colonial Pipeline is responsible for 45% of the East Coast's fuel. And it's not just gasoline for cars – it's also natural gas and aviation fuel.

From the general public's point of view, the response was largely panic buying. As stations began to run out of gas, there was a lot of hoarding, which made the situation worse. There were also some unfortunate incidents of people trying to fill up non-standard containers with gasoline. A government notification was issued to ask people not to put gas in plastic bags.

Even after operations were restored on the following Wednesday, there were still over 10,000 gas stations on the East Coast without gasoline.

There became increasing political pressure on the Biden administration to do something about the supply of gas. If the situation were to go on too much longer (estimates vary between three to four more days), it would have started to have a broader economic impact. Things like mass transit would have been severely impacted, and people would have been unable to get to their jobs.

There was a very real concern about what the longer-term impact would have been.

What do we know about the bad actor side of this attack?

There are a few interesting points here.

Immediately, there was chatter on underground forums and the dark web. Comments were to the effect of, "This looks like a mistake."

Various ransomware groups then issued statements, denying that they had anything to do with the Colonial Pipeline attack. Some groups even rolled out formal policies that stated, "This group does not attack critical infrastructure or hospitals."

We also saw various underground forums initiate rules that people could not advertise ransomware services there, because they wanted to evade the attention of law enforcement that is brought about by being associated with ransomware.

This hasn't gone away in the months since. The bad actors have understood that this event changed the calculus for countries, and how governments would start to treat ransomware actors.

I'm on the Ransomware Task Force (RTF) – an effort to produce a comprehensive set of recommendations to international governments and private-sector partners on how to address this threat. We delivered our findings a couple of weeks before the Colonial attack happened. One of our pieces of advice was that countries should treat ransomware as a national security issue.

As part of this, the Biden administration accelerated some executive orders. We also saw an increase in activity from U.S. Cyber Command, and the FBI recovered some of the ransomware funds.

They recovered 80% of the Bitcoin, but unfortunately by the point they had recovered it, Bitcoin crashed. It was only worth $2.2 million in the end.

You gave a quote in an article just after the attack – "It's time to move beyond ransomware thoughts and prayers." Why did you say that?

Up until this point, a lot of government response involved information sharing – getting the message out. They would rely on traditional law enforcement methodologies to go after ransomware groups.

Unfortunately, it's been clear for a while that this wasn't a viable approach. The arrest record was incredibly poor in contrast with the catastrophic impact that ransomware can cause.

> "The ransomware threat continues to be at a critical level for certain actors, and therefore, you need to treat them as national security threats."

That means you need to bring in the full scope of government response. You need the State Department, you need the Treasury, you need Cyber Command, you need the Department of Justice, and their equivalents across the globe, because this is a global issue.

This situation is no longer solely the province of bulletins and notifications and the occasional law enforcement investigation that finds a dead end somewhere in Eastern Europe.

We saw another ransomware supply chain attack in July by the REvil group on Kaseya. Based on what we've seen this year, what can you tell us about the nature of ransomware and supply chain attacks going into 2022?

With ransomware, we've always been concerned about the breadth that a supply chain attack could bring. In 2017, we saw what a ransomware-like event looked like when delivered through the supply chain, with NotPetya. That caused over $10 billion in damages globally. To be very clear, that was a purely destructive, state-sponsored attack, not ransomware. It was just intended to look like ransomware.

> "Supply chain is the hardest problem in security right now. I can't think of anything else that is as flummoxing."

In the case of Kaseya, this is a company that delivers services to midsize companies, which gives them administration services for their networks and their systems. That's exactly what you want as an attacker. This really did represent a new level of threat.

I'm not going to say it's a common level of threat. It's difficult to pull off because while bad actors attack multiple companies simultaneously, they still need to deliver different sets of decryption keys to each of those environments. If one company pays and gets a key, they need to ensure that the key doesn't unencrypt everything.

I think that's one of the reasons why we haven't seen this type of attack more commonly. Also, they're making plenty of money in the one-by-one method that they're doing now.

What is your advice for defenders who are trying to protect against ransomware attacks?

In the past, we've said things like "patch this" or "make sure you have two-factor authentication installed." And while that's still important, my new main piece of advice is to pay attention.

Working with our Cisco Talos Incident Response team, and watching how actors are getting in with ransomware, there isn't a lot of evolution in terms of their practices. It's rare for us to get a ransomware event where we think, "That's new."

"If you are paying very close attention to the threat landscape, and you are mapping your investments and your time to blocking the avenues that ransomware actors use (i.e., stolen credentials and specific vulnerabilities), you're going to do very well in staying ahead of those actors."

Most of the time, they don't care who they hit. They're just trying to keep the chuckwagon going. If you make yourself a very difficult target, they're far more likely to leave you alone and go after easier prey.

Further Resources:

Read more about the new world of critical infrastructure security in Talos' article about the Colonial Pipeline attack.

Security Debt:

An Increasing Target of Opportunity

With Dave Lewis
Advisory CISO, Cisco Secure

What is security debt and why is it becoming increasingly critical?

Security debt is a term that I started using about 20 years ago, as a result of my time spent working for various power companies. I found that in a lot of those environments, they were using systems that were depreciated, or weren't being properly maintained. As a result, there were many targets of opportunity for an attacker.

I characterize it as technological debt that has manifested as a security issue, either by virtue of time, neglect, or simply an interaction with another system that's been introduced into the environment.

How is security debt manifested?

- Risks are accepted to ensure that projects keep to their deliverable timelines
- There's a continual battle for budget
- Patches are not applied due to systems being behind a firewall

Is there an example from your career that illustrates what security debt looks like?

There are so many different examples I can pull from. But one of the very simple examples is when I worked at a technology company (not Cisco, I might add). In the first week, we did an assessment of all the usernames and passwords within the organization.

We found that there were 10 user accounts that had "super user status" who were no longer part of the organization. Most had left, and in one unfortunate case, a person had passed away in the last five years. However, their account had been used in the last two years.

That account, thankfully, wasn't used for anything malicious. But luck isn't a policy that you want to hang your security program on. Having visibility to see what's happening within your environment is crucial.

From an attacker point of view, how could they exploit security debt within an organization?

For a lot of organizations, it becomes a case of low hanging fruit. For example, they might have vulnerabilities that aren't patched because they don't have the bench strength, or they don't have a trusted third party.

Things also get pushed off the table. Projects are deployed that don't have a sunset provision built into the plan. As a result, some of these projects limp on years past their useful life, which unfortunately introduces security vulnerabilities into the environment.

The attacker can look at it from many different angles. They might use Shodan or scanning, or something as simple as open-source intelligence, such as going through LinkedIn and seeing what people put in their resumes, i.e., that they worked on a certain product.

They can then distil down to the products that were possibly used in that environment, and then compare against vulnerabilities that are either published, or that they can find on the dark web.

What is your advice to organizations who have security debt, and want that debt to be addressed?

It's threefold. First, you need to do your homework to find out what assets are in your environment, who the users are in your environment, and what applications and hardware they are using. Make these inventories readily available.

Secondly, have a risk register to be able to track issues as they are identified. This is not only for tracking purposes, but you can also use it for auditors when they come calling. Your risk register can tell them that you've identified issues, and outline the roadmap you have in place for those issues.

The third, and biggest piece of the puzzle, is to define repeatable processes. I've worked in organizations in the past that when something went wrong, everybody would run around with their hair on fire, trying to figure out who had to do what.

> "Make sure that you have a process in place that can identify the people within your call chain you have to call when something goes wrong, and who takes care of which tasks."

Importantly, don't tag it to an individual by name. Tag it to a role, and that will help solve the problem of when people come and go throughout the organization. When something does go sideways, having those roles identified means you have a path to help remediate it.

How does security debt affect other risk factors?

Security debt impacts your supply chain, not just in the physical sense but in the software sense, as well.

> "If you have applications that are being built by third parties, make sure that they're following a defined, repeatable process that isn't going to introduce vulnerabilities into your environment."

I've lived through that in organizations in the past. Vulnerabilities were introduced, not because of any sense of malice, but because nobody was checking the libraries.

Taking an analytical approach with your environment is always something I'd recommend. Ask, "Are these systems the ones we need?" Or, "Can we do a forklift replacement of these particular bits of hardware?" A tech refresh like that will obviously improve the latency of your devices, and you can also be obviating a lot of security issues that may have been there before.

Also be sure that you're taking an approach where security is democratized. Many countries around the world are dealing with a hybrid workforce and will be for the foreseeable future.

Make sure that you're empowering your end users so that they can get their jobs done safely and securely. We shouldn't expect them to be using tools written by engineers, for engineers.

Further Resources:

For more insights into how to deal with security debt, take a look at the latest Duo Trusted Access report.

The Security Outcomes Study, Volume 2, contains valid data on how organizations have approached this issue.

The Most Critical Vulnerabilities (You Might Not Be Thinking About)

With Jerry Gamblin,
Director of Security Research,
Kenna Security (now part of Cisco)

Can you tell us about the work you do within your team to scope for vulnerabilities?

At Kenna, we closely monitor all published vulnerabilities, and give them a risk score to help our customers understand what they need to focus on first.

To give you a picture of the vulnerability landscape and how it is growing, this year we saw over 20,000 CVEs (Common Vulnerabilities and Exposures) for the first time. That equates to 55 CVEs a day. Most security teams are not staffed to the level of being able to evaluate 55+ CVEs a day to understand which vulnerabilities pose a risk to their environment, and which ones do not.

Popular vulnerability frameworks often require patching any vulnerability with a CVSS (Common Vulnerability Scoring System) score of over 7.0. The problem is we're now sitting at an average CVSS score of 7.1, so that means patching at least half of all CVEs.

We know that this is a problem that is growing larger (we don't like to say "worse" because the vast majority of CVEs are valid vulnerabilities). Part of that is because there's more reporting and visibility. GitHub is a CNA (CVE Numbering Authority) now, and they pushed out the most CVEs last year on open-source projects.

Certain vulnerabilities from 2021 are well known (for example, Log4j and the Microsoft Exchange vulnerabilities). However, a significant number of critical vulnerabilities are less well known and can often go under the radar.

We're seeing a large number of vulnerabilities that affect open-source projects like Chrome and Edge, and vulnerabilities that target Windows such as the PrintNightmare CVEs from this summer.

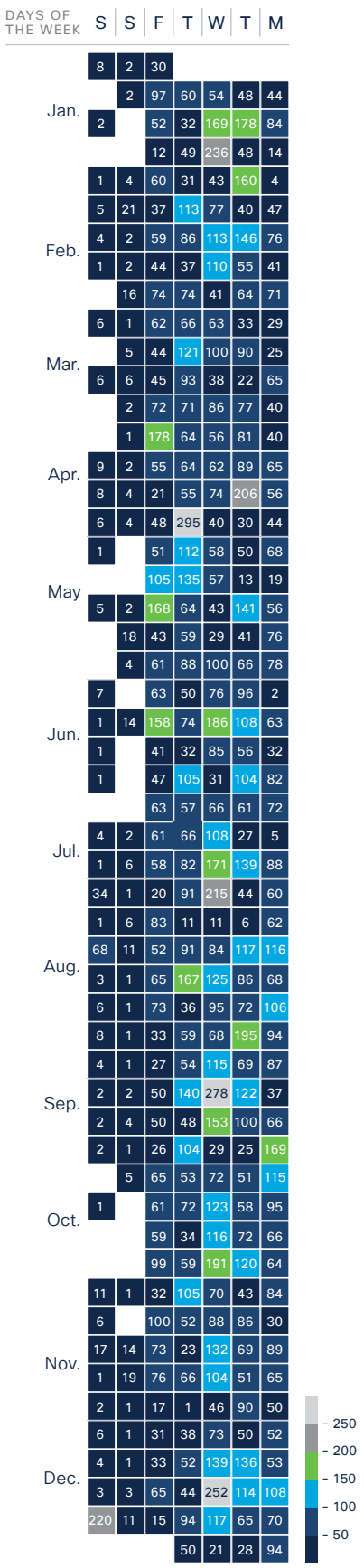
2021 CVE Recap

- Total Number of CVEs: 20,129
- Average CVEs Per Day: 55.3
- Average CVSS Score: 7.1

January 2022 CVE Recap

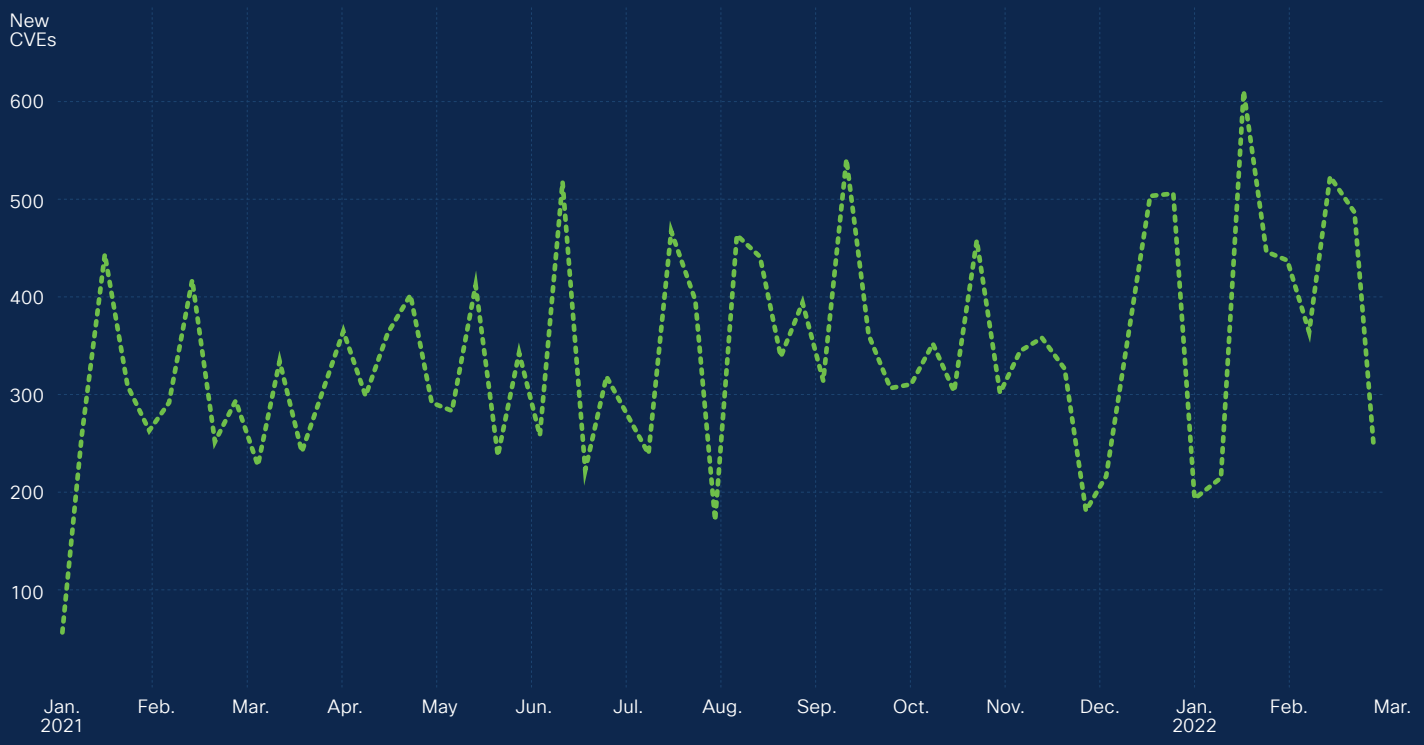
- Total Number of CVEs: 2,020
- Average CVEs Per Day: 65.16
- Average CVSS Score: 6.86
- Growth Over January 2021 (1,523): 32% or +497

CVEs per day 2021



Source: Kenna Security

Number of CVEs per week in 2021:



Source: Kenna Security

Vulnerability disclosures aren't often headline-grabbing news, but can you talk about why they should be getting more attention?

When it comes to vulnerability management, it can be difficult for defenders to get the necessary leadership attention or organizational resources, because it is often CVEs that are not in the news headlines that pose the most risk to their organization.

With over 20,000 CVEs, you will have some that get a lot of media attention. But you are much more likely to have very impactful ones for your organization that miss that media wave of attention.

It's definitely a balancing act when it comes to vulnerability management resources. The news comes at you fast, pressure from stakeholders takes hold, and your whole week gets thrown off when the newest vulnerability is deemed a top priority by intel-lacking resources. This is when risk-based prioritization (and your fix list) has your back to help you keep sight of what really matters.

The Cybersecurity and Infrastructure Security Agency (CISA) is among the influential institutions calling for organizations to evolve their approach to vulnerability remediation. Here's what CISA stated in their Binding Operational Directive 22-01 bulletin in November 2021:

> "Attackers do not rely only on 'critical' vulnerabilities to achieve their goals; some of the most widespread and devastating attacks have included multiple vulnerabilities rated 'high,' 'medium,' or even 'low.' ...Known Exploited Vulnerabilities should be the top priority for remediation."
>
> **- CISA, Binding Operational Directive 22-01**

What occupied your team's time during 2021? Can you highlight some of the key vulnerabilities?

We spent a lot of time on the Chrome V8 engine. Microsoft also made a big change this year when they moved from Internet Explorer to Microsoft Edge, which is based off Chromium, so we are making sure our customers understand the switch to an open-source browser from a closed-source browser.

Virtualization vulnerabilities are also becoming more common. We saw more high-risk VMware ESXi vulnerabilities this year than we have seen in the past.

We're also starting to see the emergence of what we (internally) call "pile-on CVEs" (we really don't have a good term for it yet). A base CVE will come out, and then over the next couple of weeks, you might see more CVEs in the code. Examples of pile-on CVEs include Log4j and PrintNightmare, both of which have multiple unique CVEs assigned to them.

In these situations, it's wise to keep tabs on a vendor's progress in addressing RCE (Remote Code Execution) vulnerabilities, especially vulnerabilities with huge attack surfaces (and substantial potential impact).

Are there any vulnerability trends that you can point to?

The size and scale of vulnerabilities will become an even more acute issue this year. Using the Prophet framework from Facebook, we run a model every night, and it looks like there's going to be over 23,000 CVEs this year. there's going to be over 23,000 CVEs this year.

In addition, what you need to look for generally isn't in the CVSS score. When we launched our latest Priority to Prediction report, we made the news because the report says that Twitter is a better indicator of exploitability.

Our report also discusses how prioritizing vulnerabilities with exploit code that is publicly available is 11 times more effective than CVSS for minimizing exploitability.

If I were to call out one trend in particular, I'd say there's a lot to be gained—or perhaps we should say a lot of risk to be lost - from prioritizing exploited vulnerabilities and predicting what attackers will target next.

"Organizations need to move to a risk-based vulnerability management system, where you look at potential remote code executions, or if there is a released exploit code for it. This is the most crucial thing you can do to identify the key vulnerabilities that might affect your organization."

What is your best practice advice for defenders to gain back the advantage when it comes to vulnerabilities?

Never turn off automatic patching. I spent some time early in my career in IT in both government and private industry, so I know what it is like. Everybody always wants to turn automatic patching off because they don't know what it's going to break. If you leave it all on, you're far more covered.

Let it take care of the routine maintenance, and that will give you time to really dig into the vulnerabilities for which you need to spend a lot of time and effort on testing and patching.

Further Resources:

To keep up to date with vulnerabilities that might not make the news, the Kenna Security blog has those covered.

Jerry also has a personal project that runs a notebook every day at CVE.ICU, which does open-source data analysis on the CVE dataset.

Log4j and How to Plan for Zero-Days

With Liz Waddell,
Practice Lead for Cisco Talos Incident Response

The Cisco Talos Incident Response (CTIR) team was on the front lines of helping our customers tackle the Log4j vulnerability at the end of 2021. Firstly, take us through how the events of Log4j unfolded.

On November 24, 2021, the Alibaba cloud security team alerted Apache that there was a remote code execution (RCE) vulnerability in Apache Log4j2, which is a Java logging library. That's important because it will come into play later.

There are at least 1,800 unique code libraries and projects that are integrated into cloud services and endpoints that have this particular logging library. When Log4j was identified, the exposure of this vulnerability was... well, as papers picked up on, humongous.

On November 30th, an anonymous security researcher with the Twitter handle @p0rz9 shared a GitHub link to a proof of concept. The next day, the first reports came out about the exploitation of organizations around the world.

December 9th was when things really started getting public attention and the first patch was released by Apache. Then, we (Cisco Talos) started seeing exploits and certain odd things popping up. Minecraft users began warning that adversaries could execute malicious code on clients and servers running the Java version of the popular game.

We published our first edition Talos blog on December 10th, and continued to update it with the latest information. In what I now call the "vulnerability mosh pit," this was an incredibly hectic time with a firehose of information coming in.

Defenders were learning how to detect, companies were trying to figure out if they were vulnerable, and researchers were trying to figure out how many people were vulnerable, scanning everything they could find. This is why having a single source of truth for our defenders was so important. Someone needs to cut through all that noise.

"If the past year taught us anything, it's that the first patch for a vulnerable application is never the only one."

Log4j followed this pattern and had three patches that came out before December 18. After last year's holiday-ruining SolarWinds attack, we expected to spend Christmas 2021 in a very similar way. But overall, the number of customers calling us about Log4j over the holidays was light.

Log4j Timeline

TALOS

Nov. 24 2021	Alibaba Cloud security team reported the Apache Log4j2 RCE vulnerability to Apache.
Nov. 30 2021	Github pull request disclosed the vulnerability publicly.
Dec. 01 2021	First exploitation reported.
Dec. 02 2021	First exploitation seen by Cisco.
Dec. 09 2021	Initial patch released by Apache.
Dec. 10 2021	Cisco Talos Blog goes live and initial coverage released. Widespread active exploitation seen, initially delivering miners.
Dec. 11 2021	Activity related to Mirai botnet observed, additional coverage released.
Dec. 13 2021	Cisco Talos finds evidence of email being pursued as attack vector as well as new obfuscations and protocols being abused. Blog updated and additional coverage released in response. CISA released advisory on Log4j2.
Dec. 14 2021	Apcahe released additional patch 2.16.0 advises all users to upgrade. Cisco Talos discovers Log4j2 embedded in a variety of metadata sources including images and word documents. Blog updated and additional coverage released.
Dec. 18 2021	Apache releases additional patch 2.17.0 to address new denial-of-service vulnerability.

This isn't to say nothing was happening. Talos was aware of active exploitation, including activity from miners and other financially motivated attackers. We had reports of nation-state actor activity, and also observed widespread activity in our honeypots and telemetry sources.

The uptick of reported exploitation of the vulnerability began on January 5, when the UK's National Health Service (NHS) reported seeing Log4Shell vulnerabilities in the VMware Horizon servers.

Talos' Incident Response plan for Zero-Days

For organizations dealing with Log4j, and any potential zero-day attacks in 2022, you may find our seven-point action plan useful.

1 Background/Threat Overview

We need a single source of truth for all the information that's coming to us that our customers can use for their own defense planning.

We publish the Talos blog, which always has the latest information.

2 Threat Capabilities

We want to know not only what the vulnerability is, but also what it can be used for. Do we need to worry about the CVE? With Log4j and the Microsoft Exchange vulnerabilities, it was very much a case of "yes."

Can the attackers get control of a system? What can they do with that? Can they move laterally and steal data or deploy ransomware?

Those answers will drive our forensics if we get further down the exploitation path.

3 How Do I Know If I'm Vulnerable?

This is the most frequent question we are asked.

With something like Log4j, the first question we're going to ask is do you know which systems are running Log4j?

There's no single, universal place that an application will be vulnerable with Log4j. Anywhere an application is logging user-controlled data via Log4j should be evaluated as a legitimate vector.

This could manifest as anything from logging user-controlled URIs, incoming user agents and POST parameters, and user-provided files. In many cases, there may be several layers of indirection between the ingest of a user-influenced value and its use by the Log4j framework. This further complicates the task of assessing the risk of a particular pathway.

Also, it's not just your systems that could be affected. It could be your vendors and partners as well. This is why we all started breathing into paper bags when this exploit came out.

4 How Do I Know if I Was Exploited?

There are several resources you can use to determine if your organization has been exploited, and our team has a list we'll run through.

Some of these are specific to Log4j. Others are general things you should have alerts set for. Here's a few examples:

- Search perimeter security device logs (e.g., firewalls, IDS/IPS) for presence of Indicators of Compromise (IOCs).
- Inspect RMI and LDAP protocols and ports at the network perimeter. Blocklist exceptions may be created for known, trusted communications using these protocols when appropriate.
- Inspect operating system event logs for suspicious or malicious HTTP requests.
- Inspect web server logs for related IOCs.
- We can also include any scripts our analysts (or a customer) could use to identify if the application is on a system (e.g., Log4j libraries).

5 What If I Was Vulnerable but Not Exploited?

We identify shareable threat mitigation based on current guidance. Sometimes it is as simple as "patch that system." For example – Log4j: Disable the Java Naming and Directory Interface (JNDI) by updating with the latest patch. Or we investigate other mitigations if patching isn't an option.

6 What If I Was Vulnerable and Exploited?

For the customer, this is situation-dependent, but in the case of Log4j it was fairly straightforward: Do everything in steps 1-5 and activate your organization's incident response plan. And call us.

7 Indicators of Compromise

A list of Indicators of Compromise (IOCs) is one of the best resources to make and update. We pointed everything, including IOCs, to the Talos blog. Typically, the types of IOCs would be IPs, domains, user agents, or specific web shell SHA-256 hashes as in the case of Log4j.

At the time of writing this report (February 2022), what is the situation now with Log4j?

We discovered that the Log4Shell vulnerabilities affecting the NHS were being exploited to establish web shells. Unfortunately, attackers can use web shells to conduct a myriad of unwholesome activities – malware, ransomware, rick roll, and stealing credentials or data.

The bottom line is that adversaries with network access to an impacted VMware product could exploit these issues to gain full control of the target system.

According to Huntress, there are approximately 25,000 VMWare Horizon servers that were internet accessible in January. Also according to Huntress, a large number of those servers are unpatched.

The manipulation of these vulnerabilities is complicated by the fact that several of the executables are excluded from AV and EDR monitoring. We, and several other security firms, have seen this actively leveraged by adversaries.

That's the situation now – the main exploit we are seeing is targeting VMware Horizon servers.

However, we are still being very diligent with how we're monitoring the world and dark web and making sure we can respond as effectively as possible to any changes and further exploitation.

This application is inside a lot of things. Readers can keep up to date with all our findings on the dedicated Talos blog.

How do you think Log4j might make an impact this year?

Log4j is going to continue to make an impact in 2022. We've already seen it with the VMWare Horizon exploit. The key now is being as proactive as possible to determine those potential points of access for an attacker who wants to use this vulnerability to exploit your environment.

What's essential is that organizations are monitoring for other signs of activity that they may not have seen in the initial hunt. Are you seeing signs of lateral movement? Are there indicators that your environment was compromised?

Is there any further advice you can offer for defenders dealing with this vulnerability or potential zero-days this year?

Always remember that during any zero-day emergency, the exploits related to vulnerabilities grow after a vulnerability has been disclosed. Document what you know and then update, update, update.

I wish I could put a quantity on how much time accurately documenting information will save you, based on my experience in customer environments. You'll just have to take my word for it that it's a very large amount.

Further Resources:

Read more about the 2021 Incident Response Trends on the Cisco Talos blog.

If you're experiencing a security emergency, call the Cisco Talos Incident Response Team: US: 1-844-831-7715 | Europe: (44) 808-234-6353

What's Emotet Doing Now?

With Artsiom Holub,
Senior Security Analyst,
Cisco Umbrella

Can you give a history of Emotet in the threat landscape, and how it became a widely distributed threat?

Emotet has quite a history. It first appeared in 2015 as a straightforward banking trojan. Many trojans were around at the time, but Emotet was slightly different because it had a very strong developer team behind it. That meant it was always evolving.

In 2016, it was first reconfigured as a loader. In 2017, we started seeing it being offered as a loader-as-a-service model. That's when Emotet started to really make a wide impact because it would coordinate with malware such as TrickBot and QakBot.

The years 2018-2019 became prolific for this malware and the trio of Emotet, TrickBot and the Ryuk ransomware were used to carry out multiple, high-profile attacks.

The IT network in Frankfurt, Germany, one of Europe's largest financial centers, was brought to a halt by a cyber-attack involving Emotet. Allentown, a city in Pennsylvania, had its critical systems crippled in a malware attack that spread so extensively that it cost the city nearly $1 million USD to mitigate. And the biggest state court in Berlin, Germany suffered from an attack which saw large amounts of confidential data stolen.

To give you a sense of the scale of Emotet, and the collateral malware it was being used with, Cisco Umbrella was blocking up to 4 million requests a month in 2019.

In 2020, there was a consolidated effort in the security industry to take down Emotet. This campaign was moderately successful, and as a result, we saw several periods of inactivity.

However, malicious actors don't give up such a powerful, money-making business so easily. It appears that the breaks in activity served not only to try to evade detection, but also to plan ways to come back stronger than ever.

In late 2020, Emotet returned with a remanufactured code, and new ways to deliver malicious payloads to organizations at scale. It became one of the first big loaders able to get access to enterprise networks, both in private and government sectors.

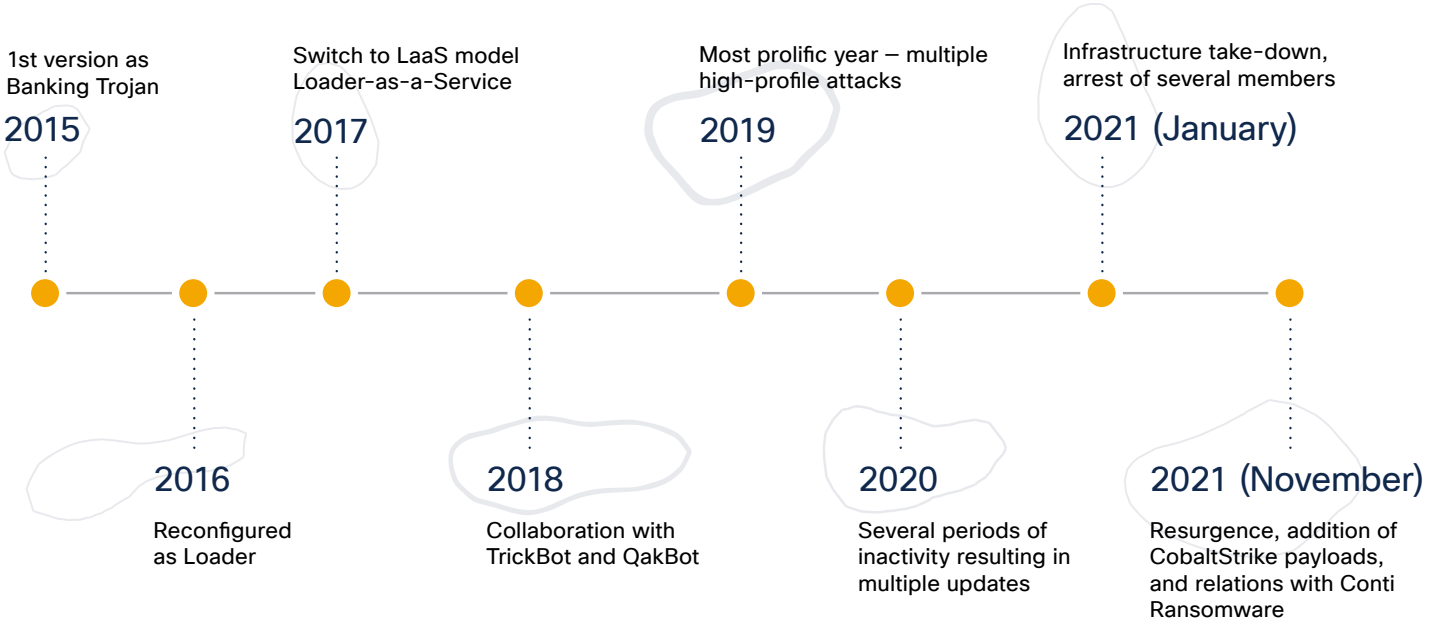
How was Emotet activity addressed in 2021?

In January, with the cooperation of both the private and public sectors, as well as an operation led by Europol and Eurojust (European Union Agency for Criminal Justice Cooperation), the operations of Emotet were disrupted again, and a large part of its infrastructure was taken down.

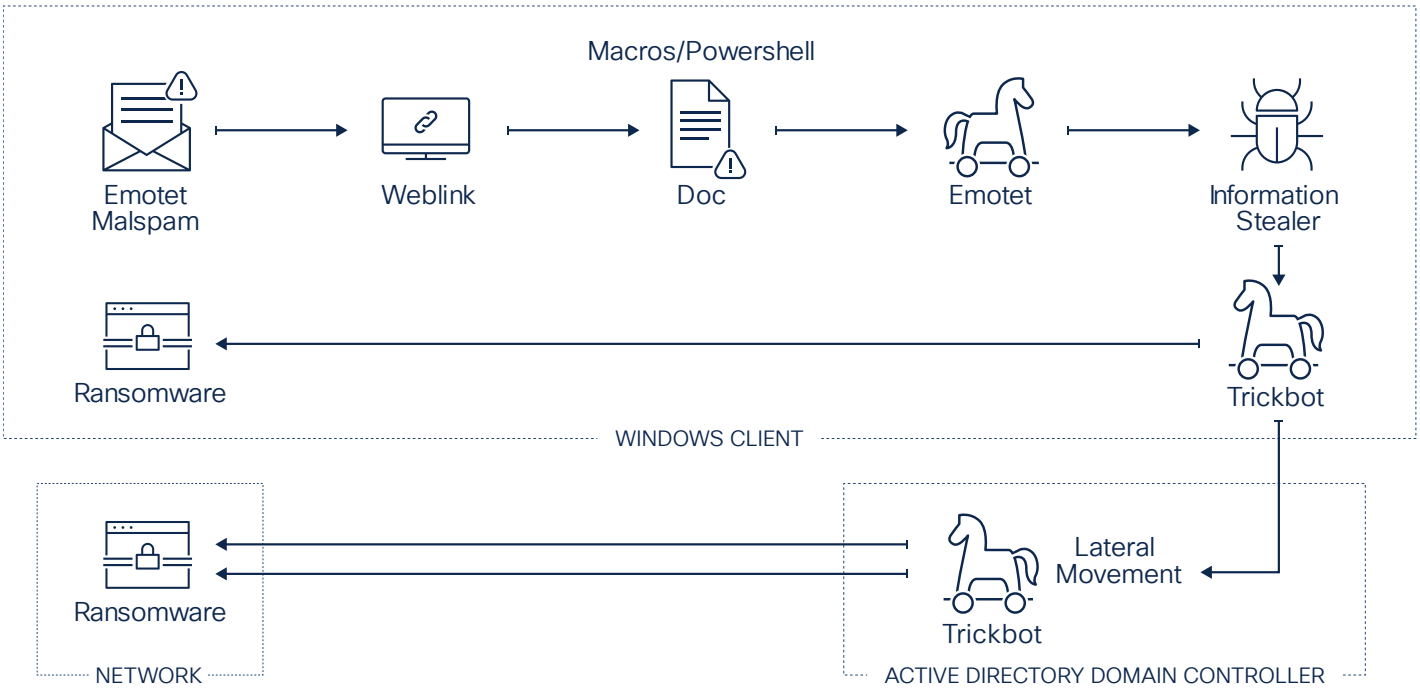
In April, Emotet was uninstalled from all found infected devices. Additionally, there was another successful operation by the Cyber Police of Ukraine, who arrested several gang members believed to be the main developers behind Emotet.

At that time, we'd hoped that this might be the last we heard of Emotet. Unfortunately, that wasn't the case.

Evolution of Emotet



Emotet Changing the Kill Chain for Ransomware



How did Emotet come back from the dead towards the end of 2021?

Due to the nature of the operations, and the profit that this malware was able to generate for the cybercrime community, we did see a resurgence of Emotet. This time it came back with a newly rebuilt infrastructure, which it is continuing to expand today.

The resurgence of Emotet is an illustration of the growing demand for such operations by the ransomware world. It only takes a few highly organized criminal corporations to create endless opportunities for Emotet botnet developers.

The TrickBot and Emotet duo was utilized heavily by Ryuk ransomware, and now Conti is the new logical avenue for the criminals.

Conti organizes highly targeted attacks to maximize revenue. If things continue to head in this direction – with TrickBot and Emotet becoming an exclusive way of distributing Conti ransomware – it is highly likely that these campaigns will become even more rampant and widespread in the upcoming year.

Could you talk a little bit more about that? Based on what we've seen, what are your predictions as to how Emotet might manifest in 2022?

"I believe that Emotet could become the biggest threat of 2022. This is a very powerful loader that has come back to life (again)."

That prediction is based on knowing how much this triad (Emotet, TrickBot, and Ryuk) changed the entire modus operandi of not only themselves, but all other ransomware operators. We've also seen them being used in supply chain attacks as the entry level.

It's a multi-level threat. Firstly, it's about getting the initial foothold in the systems, and building very strong profiles of the affected networks. Then it's about deploying things like TrickBot and Cobalt Strike; a very powerful tool for lateral movement, which can take over entire networks.

Now, having Conti as a highly organized ransomware provider, I predict that we will see high-profile attacks involving this particular kill chain in 2022.

What is your advice for defenders, and how can they protect their organizations from this type of attack?

As with anything in security, there is no silver bullet that is going to stop Emotet. Use a layered approach, know where any weak links in your network might be, and apply security controls at those points.

"As an analyst, I always recommend focusing your defense strategy on detecting lateral movement and data exfiltration to the internet. Pay special attention to the outgoing traffic to monitor for cybercriminal connections."

Finally, use the latest threat intelligence to be aware of the tactics, techniques, and procedures (TTPs) used by threat actors. Their tools and operations might change, but their procedures tend to follow whatever has worked for them in the past.

Further Resources:

Read Cisco Umbrella's report, 'The modern cybersecurity landscape: Scaling for threats in motion'.

Learn more about the re-emergence of Emotet on the Cisco Talos blog.

The Rise of macOS Malware

With Ashlee Benge,
Lead, Strategic Intelligence and Data Unification, Cisco Talos

Could you give us some background on macOS malware and why you wanted to cover it?

This is my own area of research interest. I wanted to cover it in this report because, for too long, we have operated under the assumption that macOS is somewhat impervious to malware. This stereotype has been perpetuated for as long as Mac has been around.

We receive a firehose of information as security researchers. It's my team's job to dig through that enormous amount of data to identify any changes in attacker behavior. Any change starts our hunt for new and emerging threats.

That's been the case recently for macOS malware. It's becoming more of an attractive attack surface, and in 2021, we discovered some new types of macOS malware that were cause for concern.

Increasingly, we're seeing malware that either targets macOS specifically, or that has the capability to target multiple operating systems. Whether it's Linux, Windows, or macOS, an attacker can use the same malware to execute and compromise the system.

At the time of writing, Apple has issued two fixes for zero-day vulnerabilities in iOS and macOS devices within in the first two months of 2022. These vulnerabilities, affecting WebKit, could expose iOS and macOS users to remote code execution attacks.

Vulnerabilities of this severity can be leveraged by attackers to expand their presence across a compromised network. It all depends on what they want to do once they have gained initial access.

Often, we see secondary malware dropped and executed. This malware could be a cryptojacker or ransomware, or perhaps a backdoor.

A backdoor could be used to steal sensitive information that could be used for blackmail, or to otherwise harm the targeted organization. An attacker could also cause a targeted device to become unusable, which would result in a denial of service and interruptions to operations.

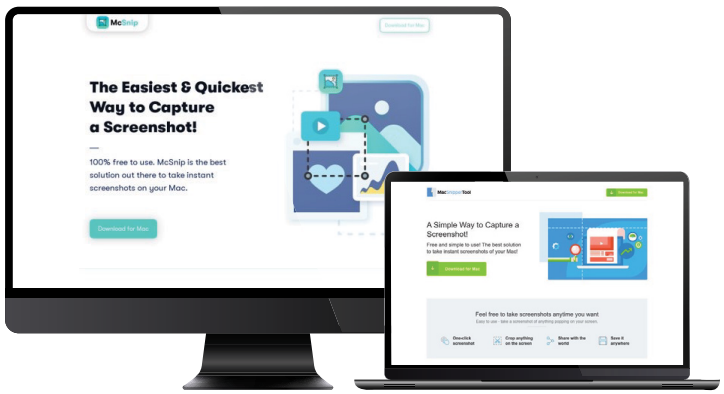
Can you illustrate an example of malware you discovered in 2021 that targets macOS?

One of our most interesting discoveries in August 2021 was the McSnip Backdoor malware.

Our day had started out normally – monitoring attacker behavior, looking for any changes that might help us identify new malware families.

We identified a change in an existing dropper technique, which is one of the methods a particular group of malware actors uses to get the initial binary on a system before exploitation.

We grabbed all the malicious files we could that were associated with this campaign, and then ripped them apart. We found some very interesting things.



Although this binary had the capability to exfiltrate sensitive information, we didn't see those capabilities being leveraged. That set off alarm bells for us.

We found that in the case of McSnip, the malicious binary was impersonating a screenshot tool that could be downloaded directly from a website, rather than from the actual legitimate App Store.

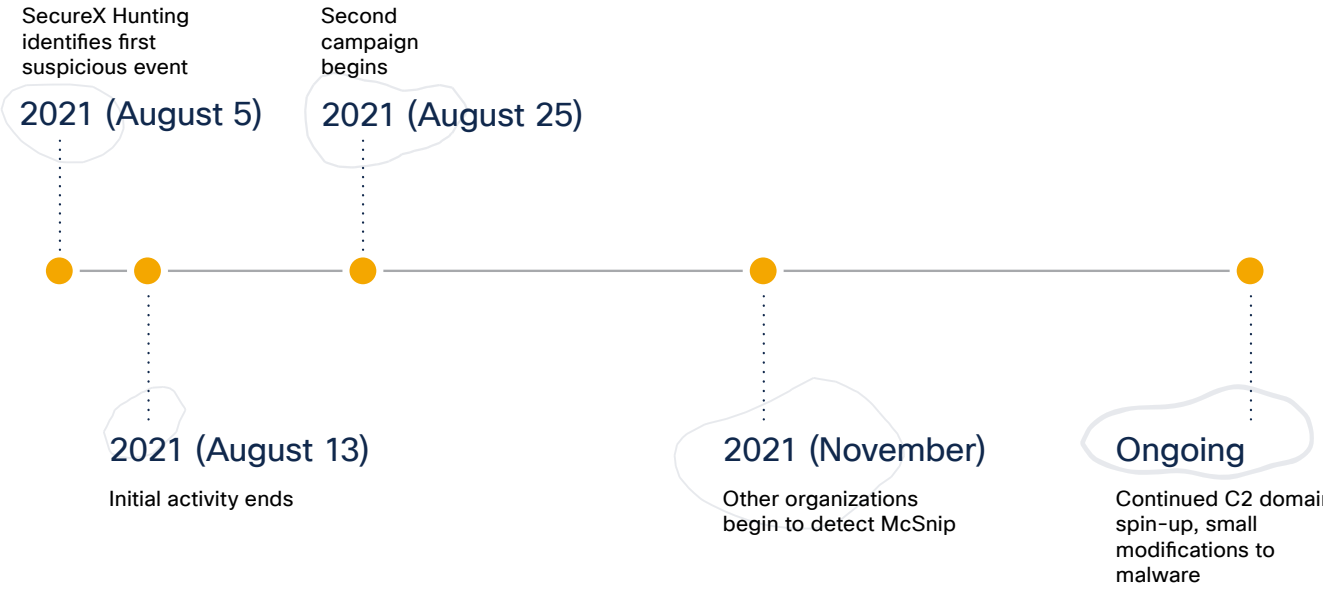
We developed hunts for this malware to ensure that there were no active campaigns. Soon afterwards, the attempts to compromise systems using the McSnip method died down.

Later in November, other security organizations began to detect McSnip as well. Around the same timeframe, we saw a secondary campaign. Small updates had been made to the malware we saw in August, and it was leveraging these new malicious capabilities for data exfiltration.

We think we saw the initial testing stage in August. The attacker behind this malware was looking to ensure that the dropping mechanism worked as planned, and that they were able to drop binaries on targeted devices. Their actual campaign kicked off in November when they were looking to use McSnip to actively compromise systems.

We're still seeing McSnip being leveraged, or attempting to be leveraged, against customers in the wild. But because of our active hunting efforts and the work that we do on my team, we're able to block actual execution of these malicious files.

McSnip Backdoor



What is your advice for defenders protecting their endpoints in 2022?

Ensuring that you have a good understanding of your attack surface is my biggest piece of advice. That may involve doing threat modeling, and ensuring that you're communicating across multiple teams, so that you really understand where you're vulnerable.

"In terms of endpoint, active hunting exercises are very useful. Look for changes in behavior and patterns and ensure that you're not just relying on what is known. Look for the unknown, and that will really help you to fill in any potential gaps."

Further Resources:

Learn more about threat modelling via our 'What is threat modelling?' resource page.

How Cisco Secure Can Help

For defenders looking to build security resiliency, and protect the integrity of their organizations amidst unpredictable threats or change, Cisco Secure can help. We partner with customers to close security gaps and anticipate what's next, while empowering companies to strengthen their institutional-wide resilience investments.

Delivering machine-scale observation to a human-level understanding, Cisco Secure helps you see more and detect threats faster. When coupled with Cisco Talos' unrivaled actionable intelligence for known and emerging threats, defenders can stay one step ahead. Learn more about our platform approach:

Cisco SecureX

Bring your security defense together in one place with Cisco SecureX, a cloud-native, built-in platform experience within our portfolio.

Cisco SecureX is integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency to secure your network, endpoints, cloud, and applications.

Explore Cisco SecureX

Cisco Talos Incident Response

Our customer-facing incident response team helps organizations find out if they have been compromised, and if so, determine exactly what happened. We then guide each organization to be back up and running as quickly as possible.

In November 2021, Cisco Talos Incident Response was recognized as a leader in the 2021 IDC MarketScape for Worldwide Incident Readiness Services.

Explore Cisco Talos Incident Response

Find a Cisco Secure solution:

Secure access service edge (SASE)

Combine network and security functionality in a single, cloud-delivered service.

Explore SASE

Extended detection and response (XDR)

Boost productivity using a cloud-native platform with analytics and automation built in.

Explore XDR

Zero trust

Balance security and usability while protecting users, networks, and applications.

Explore zero trust

Secure hybrid work

Enable security everywhere, so you can empower work anywhere.

Explore hybrid work

Ransomware defense

Prevent and respond to attacks across a range of critical control points.

Explore ransomware defense

Further Resources

A Word on Burnout

We couldn't round off this report without some thoughts on what defenders might be going through from a personal standpoint. In our recent eBook, 'Creating Safe Spaces in Cybersecurity,' we asked 20 people from across the cybersecurity industry to share their stories about avoiding burnout and managing mental health. Be sure to check out the eBook if you or someone you know is currently struggling.

Maximizing the Top Five Security Practices

In the Cisco Security Outcomes Study, Volume 2, we explore five essential practices that can help you build a world-class cybersecurity program. Read the report to gain practical insight and get started on building a more secure and efficient working environment.

Talos Threat Source Newsletters

Subscribe to Talos Threat Source – a regular intelligence update from Cisco Talos, highlighting the biggest threats and other top security news each week.

Cisco Secure Blog

Read Cisco's security blog to stay up to date on Cisco Secure product announcements, industry news, and thought leadership.

Security Stories Podcast

Listen to the Security Stories podcast for unique, inspiring, and often amusing stories behind what it takes to lead cybersecurity efforts in an organization.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA), Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands


cisco
SECURE