Navigating the Evolving Threat Landscape

Resilient Cybersecurity Tactics for CISOs

EXECUTIVE ADVISORY

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

Incident response used to be simpler. If you were compromised, it was mostly your problem to solve. You could tell who you were up against. You could expect cybercriminals to give up and move on if they encountered resistance. Advanced persistent threats (APTs) used custom tools and recognizable tactics and procedures. Botnets sent spam. Worst case, your incident might affect a few of your business partners or suppliers.

Today, those distinctions are blurring. We see cybercrime actors using processes and playbooks. When they were discovered by incident responders, rather than abandoning the attack, they fought back.

We've seen the APT groups using testing tools that were meant to improve defenses, not malware. Sometimes, they don't leave enough evidence behind to figure out what they may have taken.

And incidents affect more than just their target. Sometimes, a lot more.

This isn't all bad news. When different groups of attackers do similar things, comprehensive defenses give you more bang for your buck. Defenders can prevent, frustrate, or reveal multiple threats with fewer but more comprehensive defense tools.

In effect, cybersecurity defense today can be a total-value question, not just a technical one.

Savvy security leaders do a few things to win. You prioritize having the defenses that maximize protection with minimum spend and invest in building your own capabilities for the defenses that are unique to your organizations. And you purchase capabilities that others can provide more cost-effectively than you could yourself.

Of course, Unit 42 can help you too. But we'll get to that later.

02 WHAT YOU SHOULD DO

Here are three recommendations Unit 42 consultants frequently advise our clients to consider.

01

Establish the Right Expectations

First, change your board of directors' or CEO's view of success.

How you respond to active threats determines your success. Nobody can prevent everything bad from happening—even with the best security technology—so, making full prevention a measure of success isn't wise.

Use prevention to lower the noise floor. Stop the uncomplicated stuff. Slow down the attacker and make them trip alarms. And back it up with detailed visibility so you can determine at what and how an attacker succeeded.

Think of your defense as something that gives your defenders room and time to maneuver. Attackers already make room for themselves in their targeted networks—box them in and reduce their freedom. The less time and access the attacker has, the more opportunity for you to respond and contain them.

02

Optimize and Standardize Your Defenses

Second, streamline your defense so it's faster and more repeatable. Attackers aren't giving up when they encounter resistance anymore. You'll need to run your defense playbooks more than once. And your life will be a lot easier if you're not making it up as you go. Even easier if you have automation applied to the processes that are well-suited to machines.

Increase the time pressure on attackers. (Everyone makes more mistakes when they're rushed.) Have a practiced 24/7 security operations center or managed detection and response (MDR) provider to handle alerts around the clock. Add a threat hunting capability, in-house or outsourced, to find attacker activity that didn't set off detections. And then, you can focus your in-house defenders on the work that is unique to defending your organization. Have them concentrate on the systems and processes that nobody else can defend.

Provide your defenders a way to measure and reduce your external attack surface, giving attackers fewer opportunities in the first place. Similarly, determine what's "normal" for the inside of your network and preemptively block otherwise-legitimate tools used by attackers that your organization doesn't need.

03

Empower Your Technical Leadership

Third, empower your technical leadership. Give the Technical Appendix of this advisory to your technical lead. It's intended to give them a head start on what we know about several important attack groups. We share a little about their tactics and things you could look for to determine if you should be further concerned.

We would also be happy to discuss the intelligence with you in more detail, helping you tailor your strategies more closely to emerging threats.

03 ATTACKER TRENDS FOR THE EXECUTIVE

A few trends in the last 18 months have arisen from Unit 42 Incident Response engagements and threat intelligence analysis. Here are the ones we think are most relevant to security executives.

Cybercriminals Are Becoming More Tenacious

Once upon a time, you could expel a criminal attacker just by taking basic remediation actions, like deleting their malware. It was much easier for them to go attack someone else rather than engage in a fight with you. But that's not as true as it used to be.

Unit 42 security consultants investigated over 600 intrusions for organizations globally over the past year. In many of them, the attacker was clearly using automation, organization, playbooks, and repeatable operations. It makes them faster and more efficient, and every enterprise (even criminal ones) needs to be more efficient, right? It also meant they could fight back against defenders, keeping the access they had worked hard (or paid a lot) to achieve.

We're also seeing criminal attackers try to remain undetected, avoiding using malware and instead misusing legitimate software. This tactic is called "living off the land," and we explain it in this article if you're not already familiar with the term.

Once discovered, cybercriminals now try to persist in the environment rather than give up and go away. A criminal group we call Muddled Libra fights back against defenders. They've disabled or uninstalled security tools and avoided setting off monitoring systems. Sometimes, they've cleared alerts of their own activity from their targets' security tools or even used those security tools for the attackers' own purposes.

Listen to the Unit 42 Threat Vector podcasts, as our cybersecurity experts Stephanie Regan and Kristopher Russo reveal effective strategies to counter the enigmatic Muddled Libra threat actor group.

THREAT VECTOR PODCAST

Listen here

State-Sponsored Attacks Extend Beyond Governments

Foreign intelligence services have extended their targeting beyond solely governmental entities for quite some time. Today, some of them also attack businesses and critical infrastructure providers... in addition to their years of state-sponsored economic espionage.

For example, a Russian adversary group we call Trident Ursa has long conducted operations against the government of Ukraine. In 2022, they also attempted to compromise a petroleum refining company within a NATO member nation. This group has a history of creating access to its targets and gathering information from them.

We also saw a Chinese adversary group, which we call Alloy Taurus, expand its mission. They had previously focused on compromising telecommunication companies, and then expanded to financial institutions and government entities. And they even had time to build and use a new remote access Trojan.

And in May 2023, the governments of the US, Australia, Canada, and the UK published a remarkable Joint Cybersecurity Advisory about a group they called Volt Typhoon, which they said was targeting organizations in "the communications, manufacturing, utility, transportation, construction, maritime, government, information technology, and education sectors." This attacker group put significant focus on remaining undetected after establishing access, which makes them harder to defend against.

The notable aspect of these examples is restraint. Threat actors are establishing and maintaining access to their targets, but not using that access right away.

What This Means for You

Okay, cool stories, but what do they mean?
A few things:

01

First, thoughtful defense against tactics fights both kinds of threat actors at once. You get more value from your defensive investments when different types of attackers are doing the same things.

02

Second, threat actors are being more tenacious, quieter, and harder to find, and faster at initial compromise. There isn't as much "noisy and easily ejected" activity as there used to be, and the window of opportunity between an attacker's initial access and causing damage is shorter.

03

Third, malware-only defenses aren't sufficient anymore. But you can still catch attacker activity using other detection vectors, such as XDR, SOAR, and SecOps platforms, in the hands of capable security responders.

Tactics We Recommend

Given those trends and what they mean at a more strategic level, there are a few tactics Unit 42 consultants routinely recommend to security leaders.

Prioritize your defenses against what would do the most damage to your organizational value. Sure, this seems like common sense, but many times we see cyber defense organized around bottom-up technology stacks rather than top-down assessment of the effect a successful threat actor would have.

Build or buy a capability that can operate as fast as attackers do. If you're able to build an in-house, full-scope team, that's great. Make sure you equip them with the tools and information they need to be most effective. If you can't build the whole thing yourself, consider engaging an MDR provider for the basics and then focus your staff on your unique-to-you needs. They'll be less distracted and more effective, and they'll be better able to respond when your provider alerts you of a real problem.

Begin to evolve toward being a Zero Trust Enterprise. Zero Trust is a security strategy that eliminates implicit trust and validates everything. It's not a product, it's a methodology and a journey—and you can take a few steps right away. Here are a few steps that we often recommend to clients.

First, consider infrastructure trust. Identify the devices and workloads that should be on your network. Create and maintain an asset inventory to the best of your ability. When the alert goes up, knowing where and how important the asset is will help your responders move quickly to containment and response. It will also help with response exercises, alert prioritization, and other SOC transformation and operations.

Second, strengthen user identity, another key Zero Trust concept. Validating users with strong authentication is a critical defense against contemporary attacks. Implement phishing-resistant multifactor authentication (MFA) and single sign-on. Consider tightening failed-authentication and lockout policies, because the help desk reset calls will probably be less expensive than even the triage stage of the incident response that would otherwise result. And look through the executive summary of the Cyber Safety Review Board's second review for more on this topic. We contributed to it.

Third, assess your attack surface from the outside. Measure it, then plan on how to reduce it. Palo Alto Networks Cortex® Xpanse™ researchers found almost half the organizations they surveyed had a Microsoft® Remote Desktop server open to the internet. And Unit 42 consultants often discover internet-facing systems our incident response clients didn't know were there.

There are a lot more steps along the Zero Trust path, and we'd be happy to consult with you about them.

Finally, assume the attackers will be able to fight even a capable incident response team. Have assistance on call, including an incident response retainer and both inside and outside counsel. Practice using them, too, so you can move quickly and authoritatively when it matters.

> **Sometimes, the internet thinks you own something you don't think you own. And that's reputational risk, rather than technical risk.**
>
> We use Cortex Xpanse to identify systems that look like they belong to you. Even if you tell me "we sold that part of the business two years ago," the data may show it's still using your certificate, your domain, your IP addresses.
>
> And if that gets attacked, it will look to the world like you got compromised.
>
> We help you find these exposures, so you can ensure the internet reflects what you own, as opposed to what you may have owned five, ten, or twenty years ago.

DOMINIQUE KILMAN
Consulting Director
Unit 42

04 CONCLUSION

Sometimes, there's good news, even in security. Today, the growing similarities between cybercriminal and advanced persistent threat actors mean your defense is getting more valuable against both.

At the same time, some attackers aren't giving up as easily as they used to. Match their determination and equipment with your own.

Defense is like a profit and loss activity: invest in capabilities that create value for your organization, and purchase that that others can provide for you more cost-effectively.

How Palo Alto Networks Unit 42 Can Help You

Unit 42 and other Palo Alto Networks products and services can help you in many ways. We provide proactive and reactive consulting services, from attack surface assessment through full-scope reactive incident response. We're familiar and experienced with responding to threat actors, from APT to ransomware, in environments that include the largest Global 2000 firms. Our Unit 42 Threat Intelligence team includes threat hunters, malware reverse engineers, and threat modeling experts who can help you apply a threat-informed approach to defense.

If you think an attacker has compromised your environment, contact the Unit 42 Incident Response team at unit42-investigations@paloaltonetworks.com or +1 (866) 4-UNIT42. We'll help immediately.

If you don't think you have a current incident but would like to know for sure, we can perform a Compromise Assessment and find the truth. And if you'd like to measure your exposure, an Attack Surface Assessment will help you see yourself through the eyes of an attacker.

Many of our clients maintain a Unit 42 Retainer or access our services through their outside counsel or cyber insurer to work with us on an ongoing basis.

In addition to Unit 42, the Palo Alto Networks consolidated platform integrates cyber capabilities to coordinate and automate prevention, detection, and response across network, cloud, and endpoint. Using shared intelligence, our security platform gives SecOps teams the data to help close security gaps and fully secure their attack surfaces.

Security has a lot of challenges. We'd love to work with you to solve yours.

Want help preparing for an incident? Connect with our elite incident response advisors today.

Contact us

05 TECHNICAL APPENDIX

Here are some pointers to our previous work that are relevant to this advisory.

Understand Top Cyberthreats

Unit 42 tracks a wide variety of threat actors. Here are a few pointers to the ones that deserve priority attention.

Muddled Libra is one of the highest-profile groups. They present a significant risk even to organizations with well-developed defenses. If you only click through one link in this appendix, click this one. They are a fluid, adaptable adversary who are adept at social engineering and understand enterprise networking and defense. They fight back against incident responders, and we believe some members of the group speak English as a first language.

The main focus of a recent MITRE ATT&CK evaluation, Pensive Ursa (aka Turla, Uroburos, Snake) is a group that's linked to the Russian Federal Security Service (FSB). Our threat group assessment contains extensive analysis of their tools and tactics. While it can be tempting to think "why would the FSB target us," this threat group's activity has national security and geopolitical ramifications. We recommend prioritizing your investments to guard against them.

In May 2023, a Joint Cybersecurity Advisory was published by multiple intelligence agencies they called Volt Typhoon. We track this threat actor as Insidious Taurus. They've been attributed to the People's Republic of China (PRC), conducting operations for espionage purposes.

Noteworthy: these attackers put significant focus on remaining undetected. Our threat brief includes some hunting queries for Cortex XDR® that you can use to search for signs of their activity.

Black Basta is an interesting ransomware as a service that has been active since 2022. It's used along with double extortion techniques: encrypting files and exfiltrating sensitive data to threaten victims.

If you've been around Chinese cyberespionage incidents, you're probably familiar with PlugX. It's been around for over a decade and has been used in some high-profile attacks. But did you know we saw a USB-portable variant in 2022? We also published a decrypter for certain PlugX payload files.

Research Reports

We've mapped commonly observed tools, tactics, and procedures (TTPs) from ransomware and extortion cases in the Mitigating Cyber Risks with MITRE ATT&CK guide. It also has recommendations for practical actions you can take to defend your organization against these TTPs.

In our Ransomware and Extortion Report, we survey some trends, predictions, and best practices to protect against this common, but evolving, attack. Having backups is no longer enough.

Explore Unit 42 Threat Research Center

paloalto NETWORKS | UNIT 42

3000 Tannery Way
Santa Clara, CA 95054

Main +1.408.753.4000
Sales +1.866.320.4788
Support +1.866.898.9087

www.paloaltonetworks.com/unit42