REPORT

Cyberthreat Predictions for 2024

An Annual Perspective from FortiGuard Labs

FORTINET

Table of Contents

Introduction

Adversaries always discover new ways to compromise networks, yet executing successful attacks hasn't always been straightforward or quick. But today, thanks to the growth of the Cybercrime-as-a-Service (CaaS) market and the rise of generative AI, cybercriminals have more "easy" buttons than ever. The result? Attackers will expand their "work smarter, not harder" approach to cybercrime by relying heavily on the new capabilities in their respective toolboxes.

This year's threat predictions report examines a new era of advanced persistent cybercrime, discusses how AI is changing the attack game, shares fresh trends to watch for in 2024, and more. Here's a look at how we expect the threat landscape to evolve and our best tips for protecting your organization.

The Evolution of Old Favorites

We've been discussing numerous attack trends for years, including in our 2023 threat predictions report, noting how we expect these fan-favorite tactics to evolve in the days ahead. For example, we've witnessed advanced persistent cybercrime become more sophisticated and targeted, the rise of more intense turf wars occurring between cybercrime groups, and a shift in how AI is used to support attacks. Below is a look back at some key 2023 predictions and our thoughts regarding how these longstanding trends across the threat landscape will change in 2024 and beyond.

A new era of advanced persistent cybercrime

For the past several years, we've predicted that the growth of new vulnerabilities combined with more pre-attack activity among adversaries would pave the way for the expansion of the CaaS market. Today, as cybercriminals and advanced persistent threat (APT) groups continue working together (there are more on the dark web than ever), it's safe to say our prediction came true.

Unfortunately for security practitioners, it's only the tip of the iceberg. APT activity is on the rise. In the first half of 2023, we witnessed significant activity among APT groups, with 41 (about 30%) of the 138 groups that MITRE tracks being active during this time. Of those, Turla, StrongPity, Winnti, OceanLotus, and WildNeutron were the most active, according to our FortiGuard Labs malware detections.

Looking ahead, we predict that even more of these APT groups will become more active—even beyond the 138 identified by MITRE and those that CISA outlines with active cycles—likely engaging in dual cybercrime and cyber-espionage activities. We also expect to see a trend in which more APT groups will transition to employing even more stealthy, innovative methods to initiate attacks. Techniques such as HTML smuggling are gaining popularity, and we foresee additional novel methods emerging in the coming year. Their tactics, techniques, and procedures (TTPs) continue to evolve, evading security products with outdated analytics. Alongside what's sure to be a banner year for new Common Vulnerabilities and Exposures (CVEs), we should expect the growth of TTPs and, therefore, the MITRE ATT&CK framework.

In addition to the evolution of APT operations, we predict that cybercrime groups will continue diversifying their targets, looking for hidden (and highly lucrative) gems among a long list of already-compromised organizations. For example, in the operational technology (OT) space, the manufacturing industry has historically been the top target among cybercriminals. Going forward, we expect OT attacks to increasingly reach beyond manufacturing, with malicious actors setting their sights on industries such as healthcare, utilities, finance, oil and gas, and transportation. These attacks will also move beyond data encryption and focus primarily on the extortion of their targets. They'll also continue embracing supply chain attacks, working to disrupt critical services and organizations.

In our 2023 threat predictions report, we also said that edge attacks would go mainstream, and we expect to see even more of this activity in the future. Not only did this happen, but we anticipate that attackers will work to diversify their targets beyond what we typically think of as an edge device. With Flipper Zero and other such tools at their fingertips, money or device mules could hack IoT devices in person by cloning RFID cards or hotel key cards and then running arbitrary commands on devices such as phones and laptops. Recently, Flipper Zero made it possible for attackers to avoid plugging in USB devices in a BadUSB attack. It only takes one employee to connect via Bluetooth before malicious commands get executed. With a zero-day exploit, user interaction may not even be required.

The bottom line: The sheer breadth of potential targets and more left-hand activity in the attack chain ensures a constant stream of victims and profitable payouts for cybercriminals.

Get off my lawn: The cybercrime turf wars intensify

We predicted several years ago that we'd see turf wars emerge between cybercrime groups, with multiple adversaries focusing on the same targets.

Today, we're seeing just that, as multiple cybercrime groups try to infiltrate the same target in a short period—sometimes in a matter of 24 hours or less—deploying ransomware variants of AvosLocker, Diamond, Hive, Karakurt, LockBit, Quantum, and Royal in different combinations. Many organizations that experienced this had similar attacks made against them within days, all led by various adversaries. We can assume other cybercriminals closely monitor communications on the dark web and then run the same attack or piggyback off attacks initially executed by rival threat actors. The growth of this emerging trend prompted the FBI to issue a warning to organizations in September 2023, urging security leaders to review and enhance their defenses to guard against ransomware incidents.

We saw that roughly two-thirds of all categorized MITRE ATT&CK techniques were actively used in attacks in the first half of this year, with defense evasion being the top tactic and process injection being used across the board for evasion on compromised systems. Stolen credentials are like an all-access pass for bad actors, enabling them to infiltrate your network to launch ransomware and other attacks. Given how valuable stolen credentials are to threat actors, we predict that the emerging trend of Credential and Initial Access Brokerage service offerings will grow in the future, making it easier for cybercriminals to procure the credentials they need to execute successful attacks (sometimes against the same target). This type of service will likely mature and evolve in the same way that Ransomware-as-a-Service (RaaS) was developed to meet a gap in the market, becoming more commercially available as opposed to being available only on the dark web.

Money laundering services get hung out to dry

We previously predicted that cybercriminals would use Laundering-as-a-Service to wash their ill-gotten funds. As expected, many adversaries used these services to obfuscate ownership of illegal monies, with ChipMixer as an example of a laundering service that was heavily used but then shut down by authorities in March 2023. There are more crypto mixers and tumblers that have come on the scene since. The Killnet threat group, known for their pro-Russia hacktivist activity, also started a crypto exchange and offers mixer services.

However, there also seems to be an active attempt to take down many Bitcoin mixers, and their popularity appears to be declining in tandem. As a result, most telegram groups from hackers are encouraging the use of traditional money laundry schemes instead of tumblers.

Grabbing the (AI) chains to support all attack stages

The weaponization of AI is adding fuel to an already raging threat landscape—it's enabling attackers to enhance every stage of an attack and to do so better and faster than before. As predicted, we're seeing cybercriminals increasingly use AI to support a multitude of malicious activities, ranging from thwarting the algorithms that detect social engineering to mimicking human behavior through activities such as AI audio spoofing and creating other deepfakes.

But adversaries aren't stopping there. We anticipate that cybercriminals will take advantage of AI in additional ways that we haven't seen yet, such as:

- Attackers will use AI to conduct generative profiling—scraping social profiles and other public websites for personally identifiable information—which could easily be turned into an as-a-service offering. This is yet another way for malicious actors to have research done for them to execute an attack.
- We'll see more AI-chained attacks emerge, with cybercriminals using actionable models to make their attack chains more modular. For example, an attacker might use ML during the reconnaissance phase, chain it to an AI-driven weaponized payload, and chain that to the deployment of the weaponized payload. This federated AI approach reduces their time-to-compromise model.
- Cybercriminals will use AI to power up password spraying. Password brute forcing, stuffing, and spraying are popular ways for attackers to identify, steal, and sell credentials. Using AI to identify patterns and themes in passwords will increase this possibility and shorten the time required for attackers to be successful.

- AI poisoning attacks—instances where cybercriminals intentionally tamper with AI model training data and systems themselves—will become common, with malicious actors likely using automated toolkits to execute these hacks. Security teams will need to start protecting against these attacks, relying on an intrusion prevention service and application control to protect an organization's AI assets.

Unique Attack Trends to Watch for in 2024 and Beyond

Cybercriminals will continue to rely on specific fan-favorite tactics that have enabled them time and time again to achieve their goals. However, modern attackers have more tools at their disposal today than ever before, including a growing number of CaaS offerings and AI-driven technologies to help them work smarter and faster at every stage of an attack.

As the cybercrime industry evolves, we'll see distinct new attack trends emerging in 2024 and beyond. Here's a look at several anticipated developments that will keep security teams everywhere on their toes.

Next-level playbooks

If there was a popularity contest among types of cyberattacks, ransomware would surely earn top marks. Over the past few years, the volume of ransomware attacks worldwide has skyrocketed, making every organization, regardless of size or industry, a target. According to our 1H 2023 FortiGuard Labs Threat Landscape report, ransomware activity was 13 times higher at the end of the first half of 2023 than at the start of the year. And despite 78% of business leaders saying they felt prepared to defend against ransomware, half still fell victim to an attack.

Attackers continue to up the ante by embracing more sophisticated and complex strains to infiltrate networks—including highly destructive disk-wiping malware, which we covered in our 2023 predictions report—largely thanks to the rapid expansion of RaaS operations. However, as an increasing number of cybercriminals launch ransomware attacks in hopes of achieving a lucrative payday, cybercrime groups are quickly pivoting from smaller, easier-to-hack targets.

As a result, we anticipate that cybercriminals will become more aggressive and expand both their respective target lists and their playbooks. We'll see adversaries looking for big payouts turn their focus to critical industries such as healthcare, utilities, manufacturing, and finance, seeking out targets that, if successfully disrupted, would have a substantially adverse impact on society. In addition to setting their sights on higher-value targets, attackers will move beyond the plays they've built already. Their playbooks will become more aggressive and destructive in nature, shifting away from encryption and instead focusing on denial of service and extortion.

Despite going after high-value targets, at some point, this list of targets will dry up. This begs the question of who (or what industry) cybercriminals will set their sights on next. As adversaries are forced to adjust their strategies, cyber insurers may become attractive targets. Over the past few years, we've seen a trend in which organizations were compensating for gaps in their strategy by loading up on cyber insurance. But as ransomware intensifies, cyber insurers are becoming more particular regarding when and how they distribute payouts. That money will eventually become restricted as cyber insurers become increasingly stringent and ransom payouts become less frequent. We haven't observed cyber-insurance companies being targeted directly by attackers yet, but it's possible the industry could be viewed as a high-value target in the future, particularly as insurance companies restrict those payments downstream.

A new (and more lucrative) day for zero days

As organizations continue to expand the number of platforms, applications, and technologies they rely on to support daily business operations, cybercriminals have ample new opportunities to uncover and exploit software vulnerabilities. Case in point: We've observed a record number of zero days and new CVEs emerge in 2023, and that count is still rising. This lengthy list includes the MOVEit Transfer hack that impacted at least 60 million individuals, dubbed the "largest hack of the year so far." New zero days discovered are quite profitable, but because they're so valuable, we expect many to go unreported. Unreported

zero days are understandably more valuable to attackers—they can make more money exploiting a zero day that most aren't even aware of yet—which means security teams will need to become increasingly vigilant. And let's not forget about the rise of N-days, which we think of as zero days with an extended shelf life. These vulnerabilities could pose a risk for a long time, even several years. Although N-days are known vulnerabilities, they still present a risk for organizations if they haven't been patched or don't have a patch available.

Zero-day attacks won't be slowing anytime soon; in fact, we expect to see zero-day brokers—cybercrime groups selling zero days on the dark web to multiple buyers—emerge among the CaaS community. The rise of zero-day brokers will pave the way for cybercriminals to scale their efforts and reach a broader attack surface through more coordinated campaigns. We'll see this shift occur due to a growing attack surface with non-hardened products, which allows attackers to operationalize exploits for the tens of thousands of CVEs that are bound to be discovered.

There are many steps organizations can take today to guard against zero-day vulnerabilities, such as using next-generation firewalls, conducting vulnerability scanning, and implementing a smart patch management strategy. Yet these tools and activities are all designed to guard against vulnerabilities only after they're discovered. Engineering teams have an opportunity to help slow the growth of zero-day exploits by enhancing their software development life-cycle (SDL) methodologies. While cybercriminals use fuzzing—an automated software testing technique designed to uncover software bugs—to find new vulnerabilities to exploit, development teams can also use fuzzing to beat attackers at their own game. Developers should consider incorporating fuzzing into their SDL processes, which can help with hardening products and enhancing security and finding and fixing potential bugs before the adversaries do.

The inside game

In response to the evolving threat landscape, many enterprises are leveling up their security controls and adopting new technologies and processes to strengthen their defenses. These enhanced controls make it more difficult for attackers to infiltrate a network externally, requiring cybercriminals to find new ways to reach their targets.

Given this change, we predict that attackers will continue to shift left with their tactics, reconnaissance, and weaponization, with groups beginning to recruit from inside target organizations for initial access purposes. For example, cybercriminals could easily use generative AI to clone the voices of executives or trusted individuals, using those recordings to compel an unsuspecting target to execute commands, disclose passwords or data, or release funds. We could easily see Recruitment-as-a-Service evolve as the next phase of this trend, allowing attackers to gain access to more information to profile their targets.

While some targets may unknowingly fall victim to a cybercrime scheme, other employees may view a one-time collaboration with cybercriminals as a way to augment their salaries with quick cash.

"We the people" attacks

In 2024, we expect to see attackers take advantage of more tailored and event-driven opportunities, such as the 2024 United States elections and the Paris 2024 games. While adversaries have worked to disrupt major events in the past or take advantage of geopolitical happenings, cybercriminals now have new tools at their disposal, particularly generative AI, to aid their efforts. Officials are already offering warnings about AI's threat to the upcoming elections, talking about the role this technology will likely play in accelerating the spread of disinformation online. Attendees and viewers of the upcoming Paris games can expect to be bombarded with scams targeting fan loyalties. And as the games increasingly rely on technology to time, manage, and broadcast events, there is a growing likelihood that those systems may become targets.

But there are more opportunities for causing mayhem than just these significant events. While resource-constrained state and local governments have long been targets of cyberattacks, we predict that malicious actors will find new ways to infiltrate these entities as well. For example, cybercriminals could easily use ML and AI to regionalize attacks, translating associated communications to local languages using large-language models.

Narrowing the TTP playing field

We anticipate that attackers will inevitably continue to expand the collection of TTPs they use to compromise their targets. Yet by narrowing the playing field and finding ways to disrupt those activities, defenders can gain an advantage.

While most of the day-to-day work done by cybersecurity defenders is related to blocking indicators of compromise, there's great value in taking a closer look at the TTPs attackers regularly use to improve their playbooks and find points at which we

can disrupt their attack models. While attackers may have a broad toolkit for executing ransomware or phishing campaigns, their techniques are often similar. As defenders, we can map what attackers are doing, share that intelligence among the security community, and mitigate specific techniques.

The Attack Flow Project, led by the MITRE Engenuity Center for Threat-Informed Defense in collaboration with several partners, including Fortinet, offers security practitioners the chance to narrow the TTP playing field. Project contributors are creating a data model designed to help the security community find choke points on the chessboard by documenting the steps a malicious actor takes as part of an attack. As cybercriminals advance their operations and become more adept at evading traditional detection measures, identifying where we can potentially disrupt their activities will become even more vital.

Playing the (Attacker) Long Game

Edge devices such as OT systems were once considered nontraditional targets for cybercriminals. However, over the past decade, we've seen a rise in the sophistication and volume of attempted attacks against these targets. Several years ago, we predicted that threat actors would increasingly use Edge-Access Trojans to target edge environments, and we saw several examples of this come to fruition.

With Lynk Global, 5G, direct-to-device connectivity is now a reality. In addition, the low earth orbit satellite space is becoming crowded, which means there is more connectivity to devices that previously were not online. Simply put, more connected devices offer attackers a larger attack surface, and this presents endless opportunities for compromise. A successful attack against 5G infrastructure could easily disrupt critical industries such as oil and gas, transportation, public safety, and healthcare.

Enhancing Our Collective Resilience Against the Evolving Threat Landscape

Cybercriminals will constantly find new, more sophisticated ways to hack organizations. Still, we can take plenty of actions in the security community to better anticipate their next moves and disrupt their activities. From greater public-private collaboration to more stringent incident reporting standards, here are several ways to collectively fight back against cybercrime.

Partnerships are crucial to fighting cybercrime

Cybercrime impacts everyone, and the consequences of a breach are often far-reaching. One of the most impactful actions we can take as an industry is to build partnerships to facilitate easier information sharing.

Many efforts are underway to share knowledge and best practices across the public and private sectors to disrupt threat actors. However, there is more work to be done, and everyone has a role to play. Fortinet invests meaningful resources in various global partnerships and actively contributes to the World Economic Forum's (WEF) Partnership Against Cybercrime. Additionally, we worked with WEF earlier this year to launch the Cybercrime Atlas, a project designed to assist industry, law enforcement, and government agencies in disrupting attackers by providing a new level of visibility into the global cybercrime ecosystem and infrastructure.

Policy changes on the horizon

Strong partnerships are only one piece of the puzzle in effectively fighting cybercrime. In 2024 and beyond, we expect to see a few proposed policy changes come to light, from mandating better cyber defenses across select industries to implementing more robust standards for incident reporting.

As governments worldwide begin to better understand the fragility and interconnectivity of critical infrastructure, expect to see more systems defined as critical. Given that the private sector operates most critical infrastructure, we expect new, more stringent requirements to be introduced, forcing critical infrastructure operators to maintain better cyber defenses.

Additionally, we're encouraged to see government agencies recognize the need for standardized incident reporting and take steps to harmonize reporting requirements. Early next year, the Cybersecurity and Infrastructure Security Agency (CISA) will introduce incident report requirements under the Cyber Incident Reporting for Critical Infrastructure Act of 2022. Recently, the U.S. Department of Homeland Security (DHS) issued a report that includes a working template for how government

agencies might create a common reporting platform using consistent terminology, ultimately enabling better information sharing. We'll be watching to see how the reporting regulations and templates evolve and what role the DHS report might play in CISA's final requirements.

Implementing regulations that focus on aspects of cybersecurity, such as reporting and responsible disclosure, is essential to disrupting cybercriminal operations. We can point to numerous examples where a lack of regulation allows companies to sell tools and services designed for nefarious purposes. For example, consider NSO Group and its rival QuaDream, both of which sell high-end surveillance software to customers anywhere in the world, including those who use them for nefarious purposes.

Organizations play a vital role in disrupting the cybercrime ecosystem

While collaborative partnerships and strong regulations are vital to fighting against global cybercrime, every organization plays an integral part in disrupting the ecosystem. This starts with creating a culture of cyber resilience—making cybersecurity everyone's job—by implementing ongoing initiatives such as enterprisewide cybersecurity education programs and more focused activities like tabletop exercises for executives. Finding ways to shrink the cybersecurity skills gap, such as tapping into new talent pools to fill open roles, can help organizations navigate the combination of overworked IT and security staff as well as the growing threat landscape. And threat sharing will only become more important in the future, as this will help enable the quick mobilization of protections.

Responding to threats collectively as an ecosystem has a greater effect on the disruption of cybercrime and attacks, and it's vital that organizations understand their important role in this disruption.

About FortiGuard Labs

Founded in 2002, FortiGuard Labs is Fortinet's elite cybersecurity threat intelligence and research organization. A pioneer and security industry innovator, FortiGuard Labs develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. FortiGuard Labs data is collected through telemetry gathered from Fortinet's millions of sensors (6M+ devices deployed globally), giving FortiGuard Labs visibility into the real-world threats that organizations face today.

November 7, 2023 11:46 AM

2387910-0-0-EN