opentext™

2024

Threat hunter perspectives: **Insights from the front lines**

Contents

Executive summary

To understand the current threat landscape, enterprise CISOs need to know not just what types of threats they are up against but in whose hands, when, why, and how. For threat hunters, the connections between these factors can help reveal a more complete understanding of the risks organizations face.

While some attacks occur at arbitrary times, many others are keyed to specific organizational, geopolitical, or cultural events. If the threat actor is a run-of-the-mill cybercriminal with a financial motive, the attack may be timed for maximum leverage, such as a business going through a sensitive merger process or a healthcare organization dealing with a public health emergency. Holidays, major sporting competitions, and other large-scale events offer the potential for high disruption and slower response.

Attacks launched or coordinated by a nation-state are often intended as intimidation or retaliation against actions taken by another nation-state. When defending against such attacks, it's important to realize that they may come in unexpected ways, such as being staged or launched from less secure nations, or targeting supply chains as a way to indirectly impact the primary victim. Considerations like these are especially critical in today's intense geopolitical climate. The ongoing war between Russia and Ukraine is taking place as much in the cyber theater as on physical battlefields. The 2024 US presidential election has already seen signs of attempted hacking.

For CISOs, the question isn't whether attacks will come. It's what form they'll take, and how enterprises can prepare.

This report provides insight from the experts working on the front lines of cybersecurity: OpenText™ threat hunters. The collection of threat intelligence data from millions of endpoints belonging to OpenText customers gives us the ability to triage threats from near-space enterprise network telemetry to the far space of the open internet. Based on this intelligence, we'll share what we're seeing now—and what you need to know about the threats and adversaries targeting your organization.

Key takeaways

- Organized crime rings are supporting attacks by nation-states—possibly through direct collaboration or coordination—by attacking the same targets at the same time.
- Attacks are being keyed to specific events, such as military aid to Ukraine and national elections, making fall 2024 an especially perilous time.
- Evasion, misdirection, and masquerading are helping adversaries get around defenses designed for direct attacks.
- Many attacks are taking advantage of weak security fundamentals, with victims increasing their vulnerability by failing to take basic countermeasures.

Current adversary tactics and trends

Major nation-state players

While several countries have developed sophisticated cyber capabilities, including intelligence-gathering, cyberdefense, and cyberwarfare, two stand out for their involvement in a wide range of attacks with geopolitical motives.

Russia is highly active in launching and supporting cyberattacks, with ongoing operations in Ukraine and cyber espionage activities against NATO members.

China currently focuses its considerable cyber capabilities on countries in the South China Sea region.

Collaboration between nation-states and cybercrime rings

One of the signature trends of the current threat environment is the collaboration or coordination taking place between nation-states and cybercrime rings. In this model, an attack with nation-state characteristics is launched at the same time, or followed closely by, an attack on the same target by an independent for-profit threat actor. Whether this threat actor is taking direction from the nation-state or simply responding to a call for support can't always be known, but the timing of the attacks is too close to attribute to chance.

Russia, for example, has been seen to collaborate with malware-as-a-service gangs including Killnet, Lokibot, Ponyloader, and Amadey. China has entered similar relationships with the Storm0558 and Red Relay cybercrime rings, typically to support its geopolitical agenda in the South China Sea.

Retaliation and intimidation for Ukraine support

Russia's collaboration with cybercrime rings often plays an important role in its attacks against countries supporting Ukraine in the ongoing conflict between the two. A given target that has seen a consistent level of ransomware-as-a-service and DDoS-as-a-service attacks will suddenly experience a massive spike in this activity within 24–48 hours of an announcement of support, an arms shipment, or an endorsement of Ukrainian membership in NATO.

Soft targets, staging grounds, and supply chains

As enterprises and governments implement countermeasures against direct attacks from known adversaries, such as blocking inbound traffic from Russia, nation-state threat actors have turned to more indirect means. Third-party nations with weaker cyberdefense infrastructure can be soft targets for threat actors to gain a foothold from which to stage attacks. Developing nations such as the Democratic Republic of Congo, Argentina, Iran, Nigeria, Sudan, Venezuela, and Zimbabwe have all been leveraged in this way, broadening the range of potential sources for a large-scale attack.

Global supply chains offer another indirect means of inflicting damage. In this type of scenario, the attacker might target the operations of a port or transportation network to disrupt a military aid shipment, punish or intimidate nations whose economies rely on these systems, or otherwise cause mayhem with an indirect but significant impact on the primary target.

Timing factors

While an incident can occur at any time, many adversaries know when an attack will be least convenient for their targets and take advantage of that opportunity. At such moments, the target's attention and resources may be focused on a major event, unrelated disruption or development, or even just the arrival of the weekend.

Popular times for launching an attack include:

Special days such as national holidays, memorial observances, Christmas and other religious festivals, or cultural traditions like Halloween and Valentine's Day.

Sporting events like the Super Bowl, the World Cup, or the Olympics.

A public health emergency such as the COVID-19 pandemic, which was accompanied by a massive and sustained increase in cyberattack activity.

Political and news events like national elections, the announcement of a major Supreme Court decision, or a political scandal.

Business and financial milestones like end-of-quarter or Tax Day.

Cybersecurity events, as when cybercriminals responded to the disclosure of the CrowdStrike vulnerability with phishing emails "from" the security vendor's support organization.

Russia and China also have characteristic preferences for their weekly cadence. Russian cyberattack activity typically follows a Monday through Friday schedule with spikes within 48 hours of an adversarial announcement.

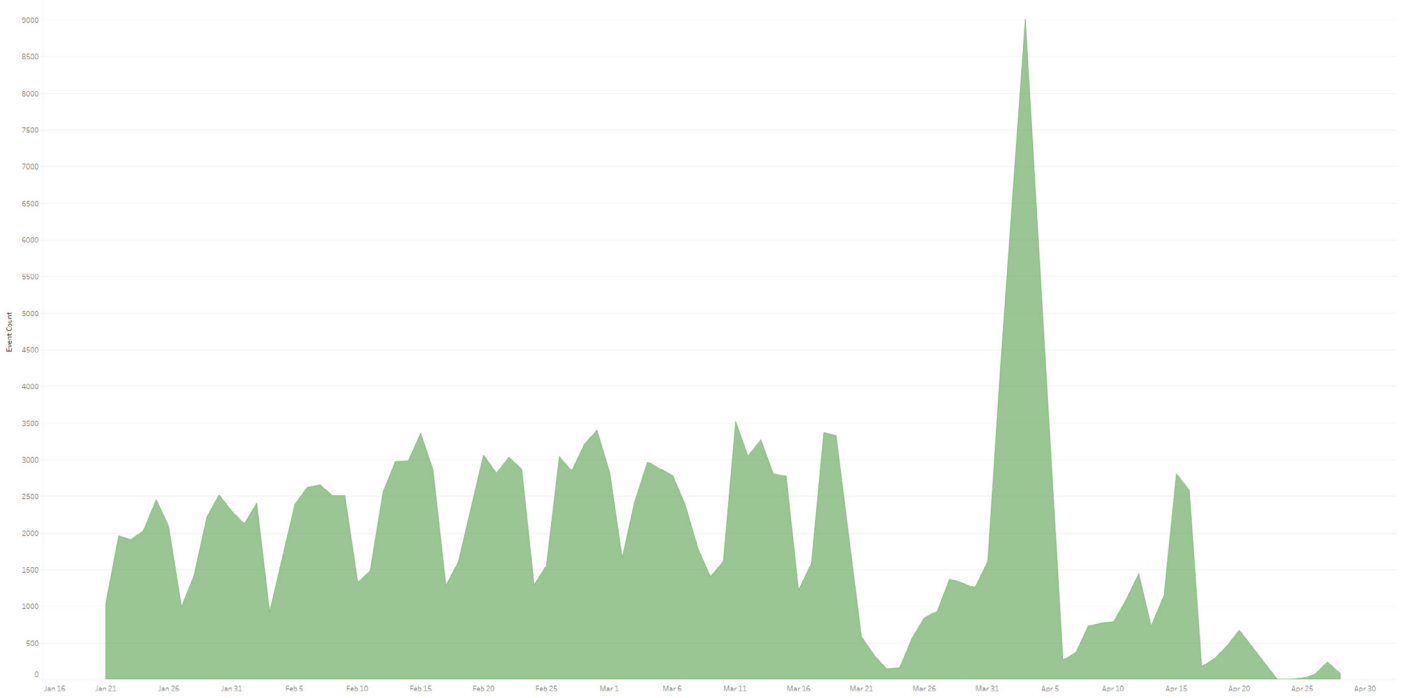


Figure 1 – Russian attacks follow a regular weekly cadence

Chinese attacks don't follow a set schedule, though any data exfiltration is typically slated for Friday afternoons or Saturdays, when it's more likely to be missed, with the data broken into smaller chunks to further reduce suspicion.

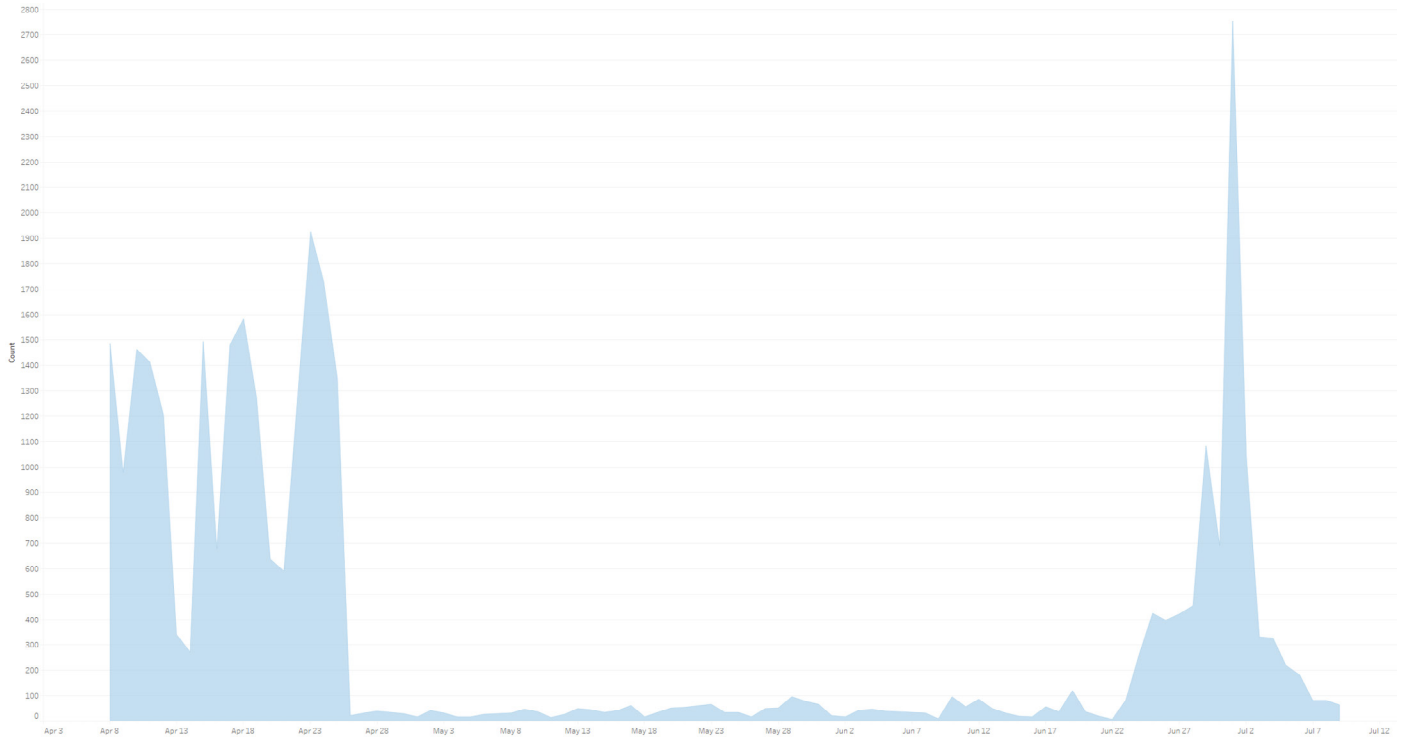
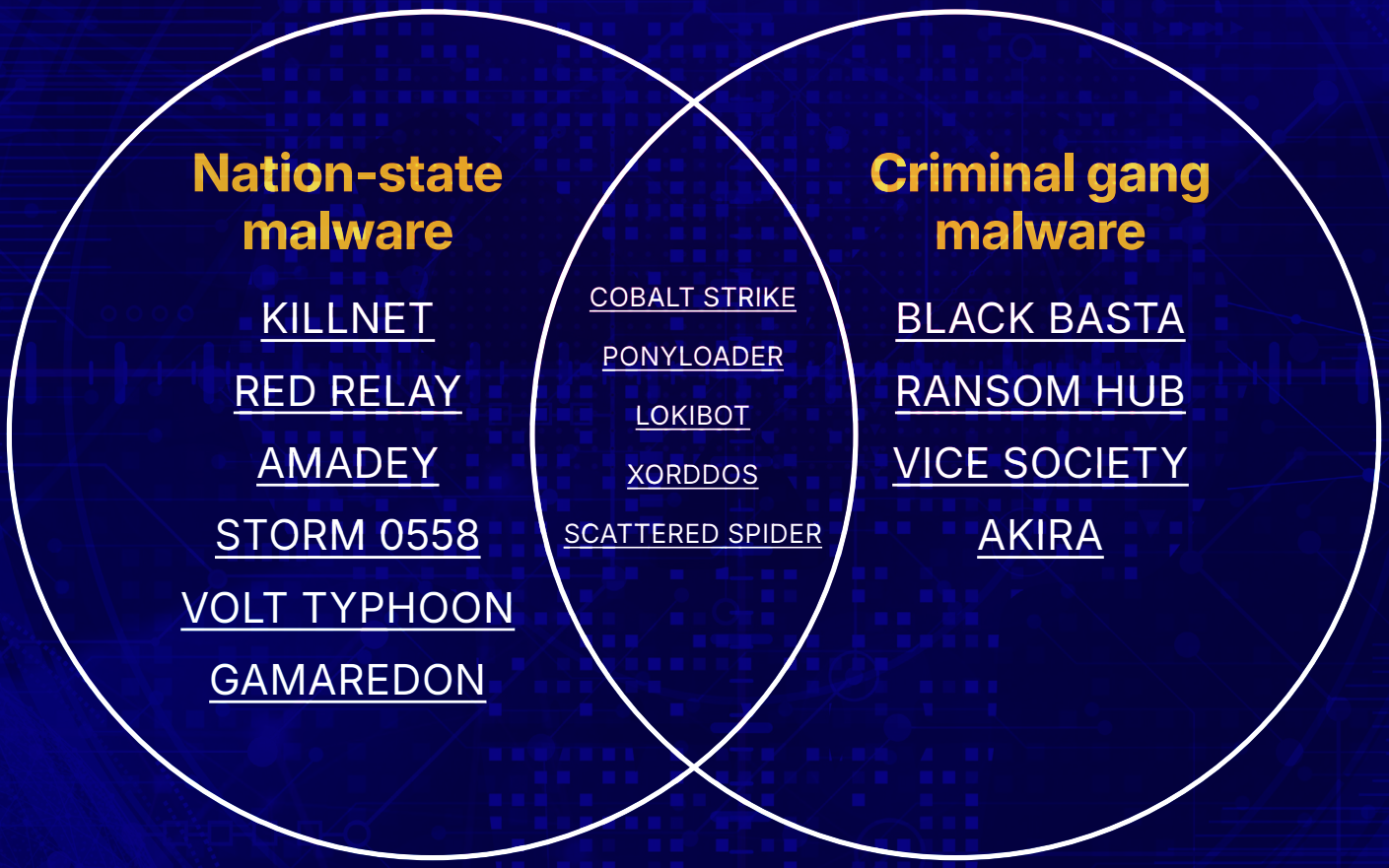


Figure 2 – Chinese attacks can come at any time

Top 15 threats/ threat actors



Threat hunting case studies

Ukraine support brings massive retaliation

A western nation announced material support for Ukraine in early 2023. Within 24–48 hours, a massive wave of attacks hit the systems of its largest railway operator, presumably in order to disrupt the flow of freight through the country. The largest of these attacks were carried out using Ponyloader and Killnet. However, the surge also included uncharacteristic spikes in attack types that are otherwise consistently minimal throughout the year, including lower-level malware-as-a-service campaigns usually launched against enterprise or SMB targets by ransomware gangs like Akira or Black Basta.

This incident illustrates several of the key themes of 2024: Russian retaliation and intimidation for Ukraine support, collaboration between a nation-state and criminal gangs, and an attack against a private sector company within a critical supply chain in order to inflict damage on its nation-state.

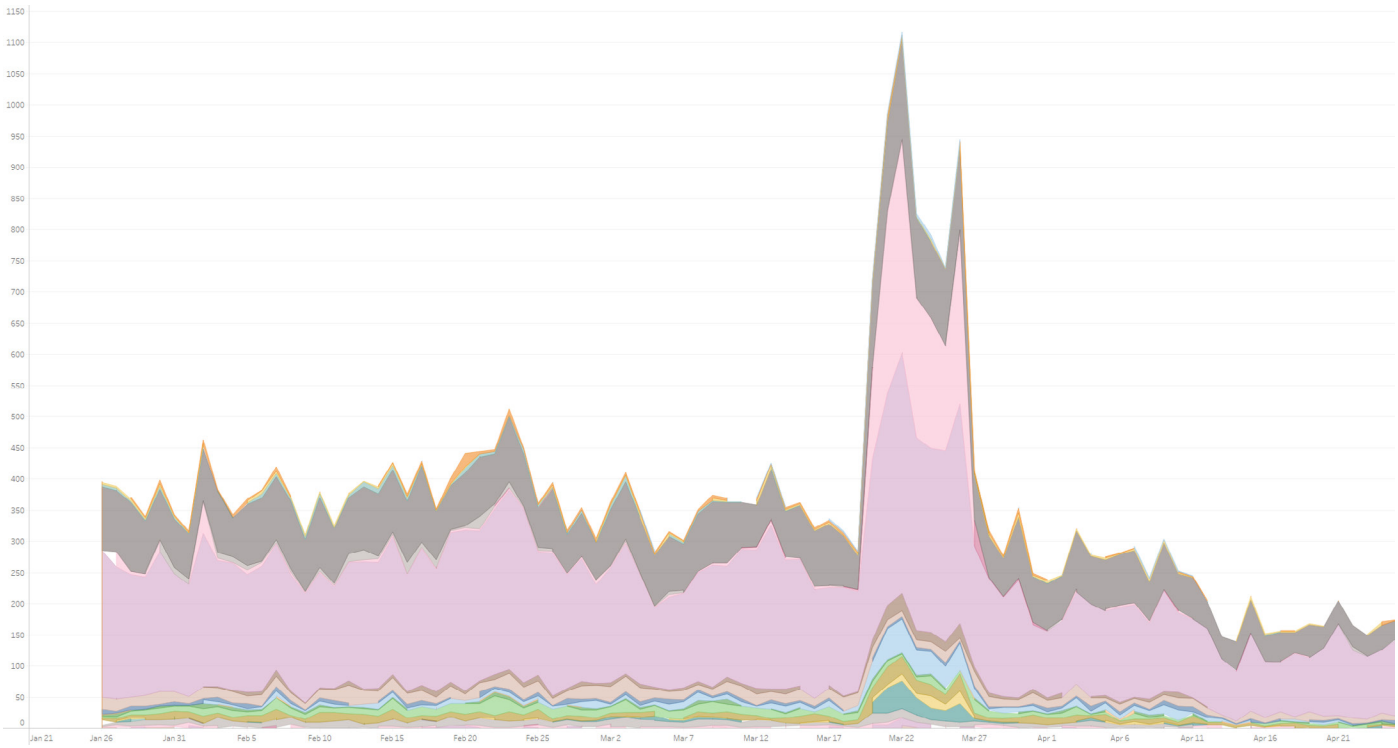


Figure 3 – An announcement of military aid was met promptly with collaborative attacks March 15 "Support for Ukraine Announced"

This is a stunning example of data correlation. To connect a news event to a network response to full and deep attribution of that signal all the way to named criminal and nation-state actors is powerful and transformative.

—Stephan Jou, sr. director of software engineering, OpenText

Non-public shipment targeted

In this incident, OpenText threat hunters learned of the previously undisclosed attack from our own threat intelligence data. When a global network of sensors detected a spike in activity against a national multimodal transportation service in Eurasia, we contacted the company and asked them for context. The target revealed that a shipment had been underway related to a military project. While the nature of the shipment had not been revealed publicly, its adversaries had gained knowledge of it and attempted an attack to potentially paralyze the company's distribution center.

In addition to the spike in activity associated with the initial attack, our threat data showed elevated levels of suspicious inbound connections and traffic over the following months, suggesting that the target may have been compromised and now hosts ongoing command and control activity.

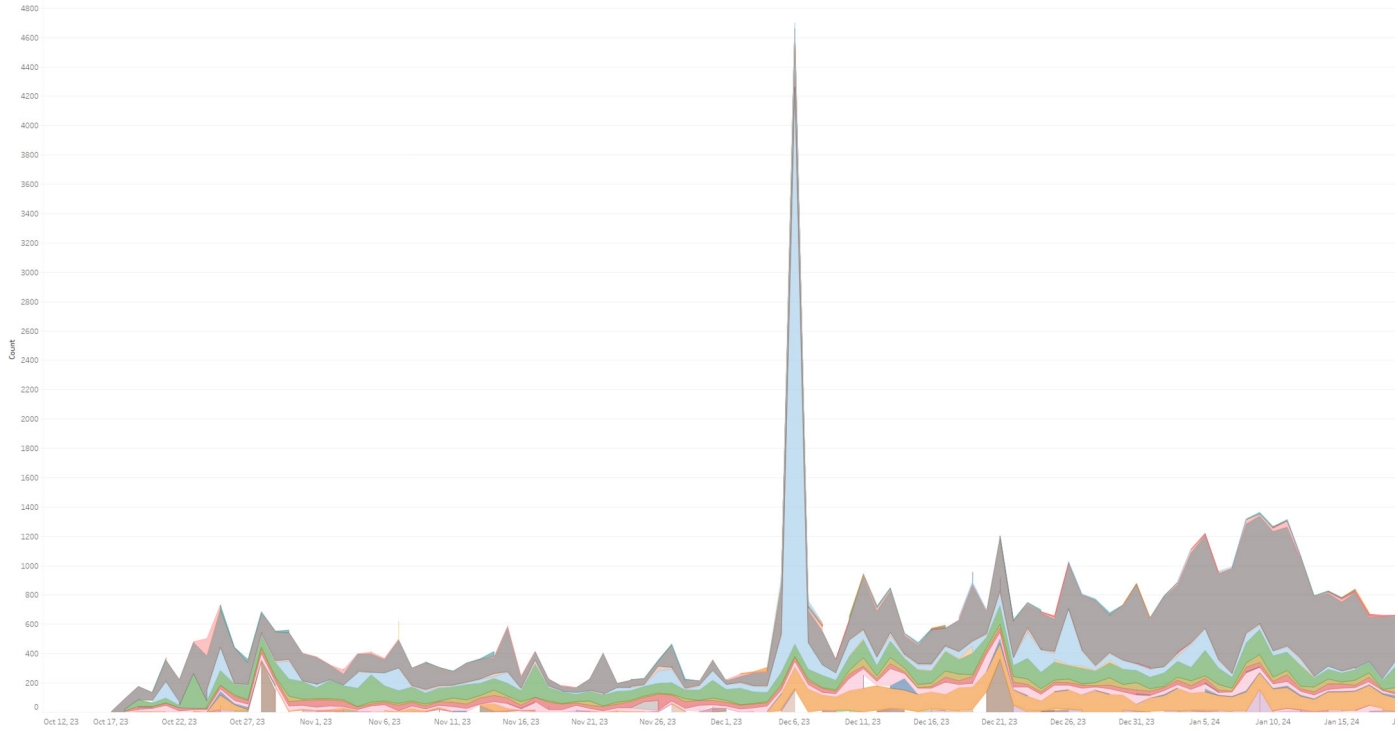


Figure 4 – An initial attack was followed by a sustained increase in suspicious inbound traffic

Manual disinformation campaign disrupts public services

Not every successful attack relies on sophisticated technologies. In the course of an ongoing territorial dispute between two nation-states, one of the countries launched an attack against the other government's website for citizen interaction. Over a five-day period, thousands of bogus reports, apparently manual, flooded the system and strained the target's resources. At the same time, Storm 0558 uploaded compromised data, divided into chunks to avoid suspicion, through a video streaming edge device.

Finnish elections targeted after NATO membership

Finland's application for NATO membership was ratified on March 30, 2023. Given the 800-mile border the country shares with Russia, and coming at a time when tensions between the two were high over the war in Ukraine, the subsequent retaliation hardly came as a surprise. The next Finnish national election was held in two phases on January 28 and February 11, 2024. Each of those days saw a two-pronged spike in cyberattack operations persisting 24–48 hours, with an extended period of attack following the final phase.

Following the election, Finland announced its first participation in NATO military exercises to take place from March 4–16, 2024. OpenText threat intelligence showed significant attack activity from Russia during this time, as well as additional operations from China via Volt Typhoon.

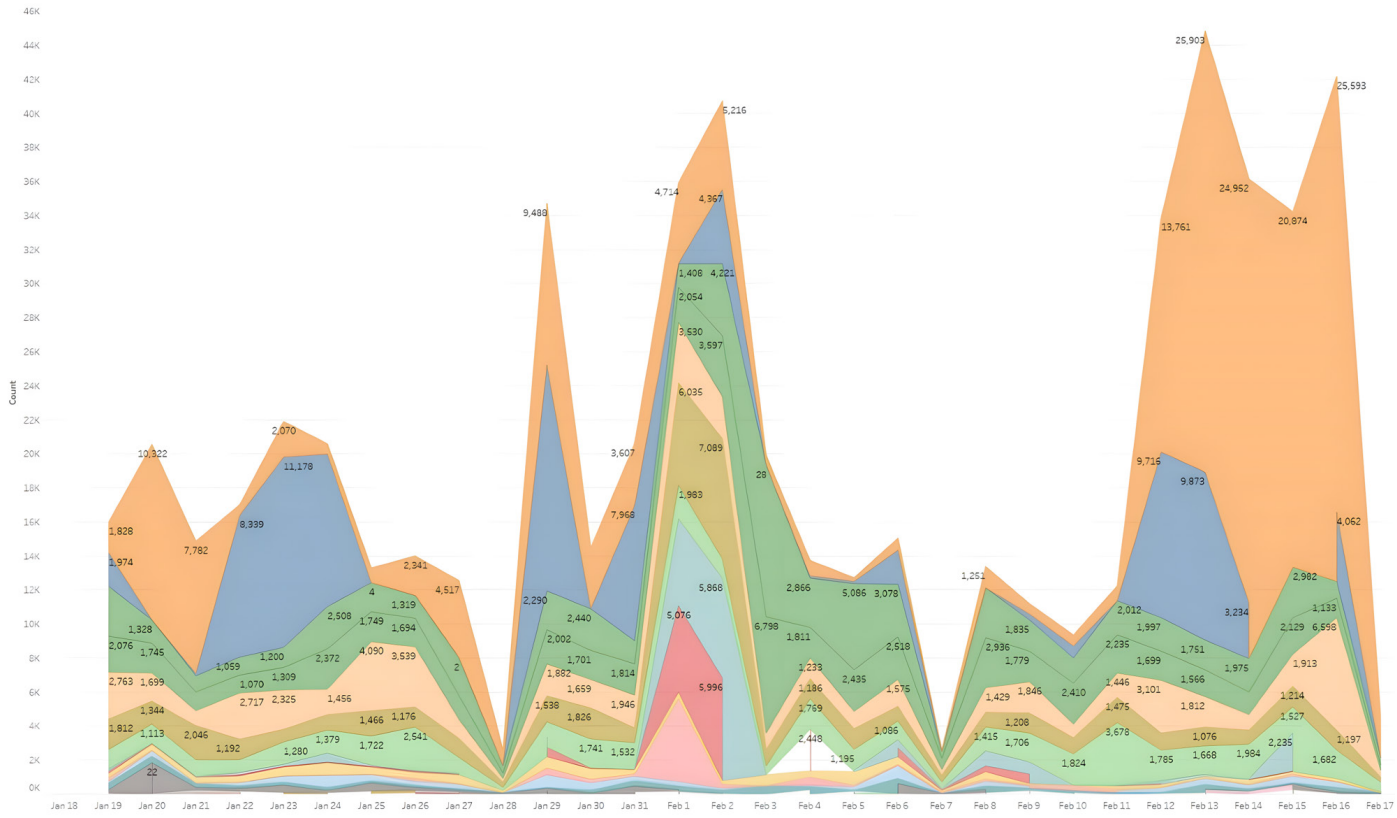


Figure 5 – Each phase of Finnish voting saw a double-peaked increase in cyberattacks

Predictions for fall 2024

The US election will be a hotbed of activity

Both US presidential campaigns have already been targeted by cybercriminals, one of them successfully—and that's only what's been reported in the media. Behind the scenes, nation-states are doubtlessly planning attacks to take advantage of the many distractions of a contentious election to sow misinformation, advance geopolitical agendas, and lay the groundwork for longer-term operations. DDoS attacks are a particularly popular method to impede access to information, so we can expect a high level of such activity in the months to come.

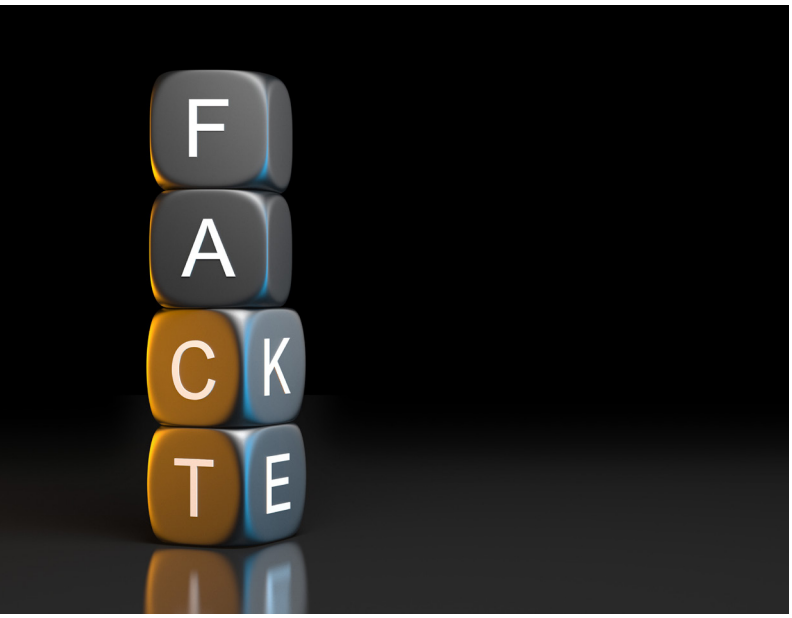
While it's too early to forecast the winner of the election, threat hunters are already contemplating the implications of either outcome. A Republican win might bring a reduction or withdrawal of US support for Ukraine, in which case an easier path to Russian victory might lead that country to refocus its cyber operations elsewhere. On the other hand, the US might continue to play an active role in Ukraine's cyberdefense even as materiel support lessens due to the value these activities provide for US cyber operations. A win by the Democratic candidate might increase the likelihood of US cyber operations against Iran given Russia's ongoing distractions in Ukraine. Only time will tell how either scenario will play out, but the identity and priorities of the next administration will help shape the global threat environment in the years to come.

The cyber arms race will escalate—including terrorists

It's common knowledge in the cybersecurity community that nation-states actively hoard zero-day vulnerabilities as weapons. Unknown to researchers and undetectable by signature-based threat detection technologies, these threats could be unleashed during a conflict—cyber or physical—to disable an adversary's industrial systems such as water purification, power and energy, transportation, GPS networks, and other critical infrastructure. Other cyber weapons in these arsenals are designed for espionage, stealing information for intelligence purposes. This arms race undermines security for the entire global community, but it shows no signs of slowing.

Meanwhile, non-state actors are building their cyber capacity as well. As systems and devices become ever more interconnected and remotely operated, black-hat hackers are gaining new ways to breach defenses, hijack operations, and wreak havoc. Damaging ransomware attacks against critical institutions and infrastructure such as hospitals, fuel pipelines, telecommunications networks, government agencies, and more have shown the vulnerability of these targets and the impact a breach can have. Terrorist groups and cybercriminals alike will have every reason to exploit the opportunities they offer.

Misinformation will reach alarming new levels



In the generative AI era, impersonation, fraud, and distortion have become almost comically simple to perpetrate. A photo or two and a few sentences of recorded speech can be enough to create a convincing deepfake video at minimal cost with an easy-to-use app. For public figures like political leaders, celebrities, and religious figures for whom extensive footage is freely available, the level of realism achievable with these tools can fool even the most discerning observer. In an environment of partisan conflict, conspiracy theories, and looming existential threats, the potential for misinformation-based schemes is clear. Many people will fall for the fakes; others will become jaded and struggle to trust even legitimate information sources.

Having created this problem, technology—or more accurately, its innovators—will also bear the burden of addressing it. A definitive solution is probably beyond reach, but models for detecting altered images continue to improve in accuracy. The development of such tools will continue to lag behind what's needed, but we can hope to at least mitigate the damage.

AI expectations will come into alignment with reality

After more than a year of breathless excitement by analysts and rampant AI-washing by technology vendors, expectations for the latest AI innovations are finally coming back to earth. This will be seen as clearly in the security operations center as anywhere else in the enterprise.

While AI can play a transformative role in cybersecurity, CISOs are beginning to think more realistically about both its value and its limitations. For one thing, it's important to keep in mind that enterprises don't have a monopoly on the technology. Our adversaries are studying AI as avidly as any other organization, and their sophistication, especially at the level of nation-state threat actors, can equal any target. A deep understanding of how ML-based security tools work and what they look for can help attackers evade detection—for example, by making a threat look enough like a legitimate file, or ensuring that their malicious behavior doesn't register as an anomaly.

In that light, it's clear that AI isn't a magic bullet that can eliminate risk or enable fully automated security. Rather, it's a powerful way to enhance and augment human effort to keep pace with rising threats. AI can speed root cause analysis, enhance threat detection and response, analyze threat data at scale, and improve analyst productivity, among many other promising use cases, but human expertise and judgment will remain essential elements of cybersecurity for the foreseeable future.

At the end of the day, AI is just a tool. Just like how cryptography can be used for good (securing your browser communications) and bad (ransomware encrypting your hard drives), so too can AI.

—Stephan Jou, sr. director of software engineering, OpenText

Security recommendations for enterprise CISOs

As our predictions for fall 2024 make clear, enterprises will be facing a daunting threat environment in the months ahead. The recommendations that follow can make a significant difference in improving your organization's security posture and lowering the risk of disruption.

Eat your security vegetables

We'll get this one out of the way first. If it seems tiresome to still be harping on security basics in 2024, trust us—we're as tired of this topic as anyone else. But the fact remains that many attacks succeed due to neglected fundamentals like endpoint protection, email security, patch management, security awareness training, and backup and disaster recovery planning. Any gap in your security posture leaves you exposed to potential data theft, privacy violations, ransomware, service disruption, and other attacks. By ensuring that these unglamorous but essential best practices are in place, CISOs can rob threat actors of many of their favorite tactics to abuse networks and businesses.

Be aware of your operational cadences

As discussed earlier, many cyberattacks are timed for moments of distraction or vulnerability. Enterprise CISOs need to be aware of important go-live events, movements of important goods or components, key transactions, and other organization-specific dates, as well as national and cultural holidays and events. By exercising heightened vigilance during these times, you can safeguard data and systems more effectively—and mount a more rapid and effective response to any incidents that occur.

Use signal analysis to strengthen cyberdefense

Signal analytics is a critical capability for modern security operations. By gaining visibility and insight into network activity within and beyond your organization, you can discover malicious traffic and reveal adversarial behaviors, early warning signs, and sophisticated attack paths. This insight can in turn help you attribute attacks to specific threat actors to better understand where, why, and how they're attempting to breach you. Defining digital genealogies within your network can help you identify misconfigurations and vulnerabilities to better defend against future attacks.

Know your supply chains

Supply chains can often hide weak links in an enterprise security posture. Supply chain risk management practices can help you identify potential vulnerabilities across the partners and suppliers with whom you do business to ensure that any attacks they face don't spread into your own network. The remote monitoring and management (RMM) tools used by managed service providers (MSPs) offer a classic example of this scenario. Used by MSPs to deliver services and resolve issues for their customers, RMM tools are whitelisted and granted a high level of access to perform functions such as patch management, network monitoring, and direct messaging. As a result, a compromise of the RMM can allow attackers to push threats to the customer as easily as the MSP would apply a patch. Understanding and verifying the security posture of every MSP you work with is a critical element of enterprise security.

Know your software stack

The highly modular nature of enterprise software, often incorporating numerous open source projects, can make it difficult for organizations to understand which common vulnerabilities and exposures (CVEs) pose a risk. A comprehensive, continuously updated software bill of materials detailing all the software used in the business can help you identify whether a newly identified CVE is relevant to your environment so you can react and remediate the vulnerability promptly. Tools for application discovery and dependency mapping, attack surface management, and cloud attack surface management can play a similarly important part in understanding and protecting your entire enterprise estate.

Of course, as this year's CrowdStrike incident illustrated, disruption isn't always the result of cyberattacks. Unforced errors can be just as devastating—whether triggered internally or by a vendor. Be ready for anything.

Understand the human element of attacks

Even as cybercrime grows more and more technologically sophisticated, the most critical element of a breach often comes in human form. Malicious insiders can collaborate with criminals to facilitate data theft or undermine security controls. Well-intentioned employees can fall victim to social engineering schemes—in fact, tactics like phishing and pretexting play a role in the overwhelming majority of successful attacks. User education programs and security hygiene policies are of course essential, as are behavioral analytics to detect suspicious activity, but they're only part of a complete strategy.

By now, every CISO is well-versed in the Zero Trust principle of assuming you'll be breached and acting accordingly. That includes using identity and access management (IAM) tools to enforce least privilege, limit the data accessible to a given user at a given time, and thus contain the damage that either a malicious insider or careless employee could do. IAM is a cornerstone of compliance with regulations like GDPR and CPPA, and for good reason.

Make strategic use of AI

While AI won't entirely replace existing security solution sets, there are many ways it can be used to enhance SOC effectiveness. Use cases like proactive threat hunting, anomaly detection, incident and vulnerability prioritization, and automated incident response can all help organizations detect and protect against threats more successfully. Improved security analytics and visualization, workflow automation, and task automation can help SOC teams work more quickly and efficiently, easing skills shortages and analyst burnout.

Be a good cyber citizen

The US Cybersecurity & Infrastructure Security Agency (CISA) leads federal efforts in partnership with private industry to defend against threats to cyber and physical infrastructure. A perennial challenge for CISA is knowing where to invest their focus and which threat actors to go after. Businesses can help CISA maximize its impact by coming forth when they are attacked and sharing the experience so that the community can learn, and government agencies can take action.

At DEF CON 2024, the world's largest hacker conference, a project was launched to create a volunteer army to help protect vulnerable water systems and schools in the US as well as broaden public access to cybersecurity research. Efforts like these can help harness the nation's full collective cyber expertise more effectively to counter rising threats like those described above.

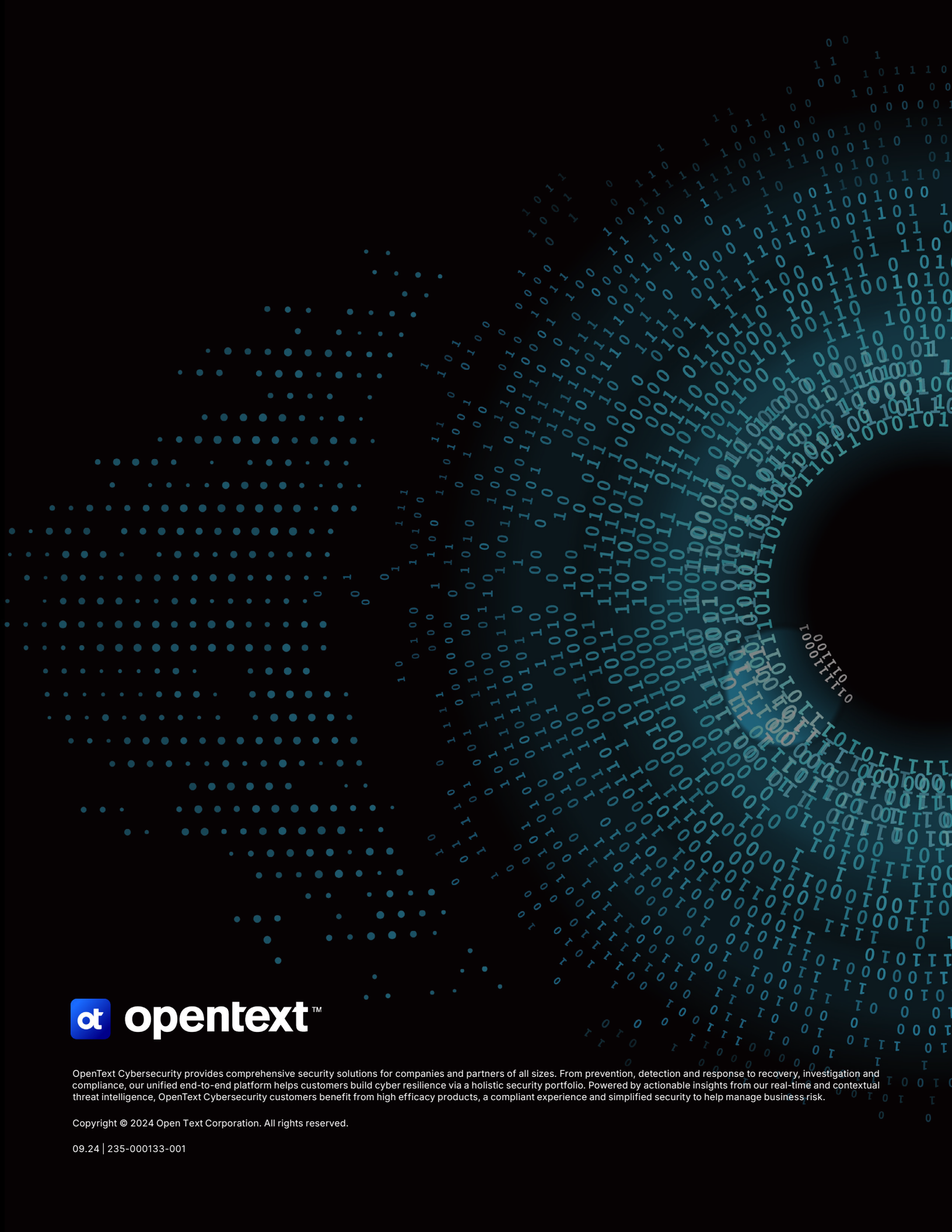
Timing is everything for cyber adversaries. By launching attacks at moments of maximum disruption, whether during a critical business event or a national holiday, they demonstrably increase their chances of success. This calls for vigilance, even during expected lulls.

—Tyler Moffitt, sr. security analyst, OpenText

It feels good being a threat hunter and protecting businesses from the risks they face. However, it is very frustrating how often a breach is discovered as the result of a basic security failure. Not using MFA for remote access to your network? Why not? Not educating your employees on how to spot a phishing campaign? Foolish! We need to make the job of our adversaries as difficult as possible, which starts with eating your cybersecurity veggies and ensuring the basics are covered.

—Grayson Milbourne, security intelligence director, OpenText

Want to learn more? Contact one of our experts here.



opentext™

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.

09.24 | 235-000133-001