Microsoft

Microsoft Digital Defense Report 2022

Executive Summary

Illuminating the threat landscape
and empowering a digital defense.

Introduction by Tom Burt

Corporate Vice President, Customer Security & Trust

> “The trillions of signals we analyze from our worldwide ecosystem of products and services reveal the ferocity, scope, and scale of digital threats across the globe”

A snapshot of our landscape...

Scope and scale of threat landscape

The volume of password attacks has risen to an estimated 921 attacks every second – a 74% increase in just one year.

Dismantling cybercrime

To date, Microsoft removed more than 10,000 domains used by cybercriminals and 600 used by nation state actors.

Addressing vulnerabilities

93% of our ransomware incident response engagements revealed insufficient controls on privilege access and lateral movement.

On February 23, 2022, the cybersecurity world entered a new age, the age of the hybrid war. On that day, hours before missiles were launched and tanks rolled across borders, Russian actors launched a massive destructive cyberattack against Ukrainian government, technology, and financial sector targets. You can read more about these attacks and the lessons to be learned from them in the Nation State Threats chapter of this third annual edition of the Microsoft Digital Defense Report (MDDR). Key among those lessons is that the cloud provides the best physical and logical security against cyberattacks and enables advances in threat intelligence and end point protection that have proven their value in Ukraine.

While any survey of the year’s developments in cybersecurity must begin there, this year’s report provides a deep dive into much more. In the report’s first chapter, we focus on activities of cybercriminals, followed by nation state threats in chapter two. Both groups have greatly increased the sophistication of their attacks which has dramatically increased the impact of their actions. While Russia drove headlines, Iranian actors escalated their attacks following a transition of presidential power, launching destructive attacks targeting Israel, and ransomware and hack-and-leak operations targeting critical infrastructure in the United States. China also increased its espionage efforts in Southeast Asia and elsewhere in the global south, seeking to counter US influence and steal critical data and information.

Foreign actors are also using highly effective techniques to enable propaganda influence operations in regions around the globe, as covered in the third chapter. For example, Russia has worked hard to convince its citizens, and the citizens of many other countries, that its invasion of Ukraine was justified – while also sowing propaganda discrediting COVID vaccines in the West and simultaneously promoting their effectiveness at home. In addition, actors are increasingly targeting Internet of Things (IoT) devices or Operational Technology (OT) control devices as entry points to networks and critical infrastructure which is discussed in chapter four. Finally, in the last chapter, we provide the insights and lessons we have learned from over the past year defending against attacks directed at Microsoft and our customers as we review the year’s developments in cyber resilience.

Each chapter provides the key lessons learned and insights based on Microsoft’s unique vantage point. The trillions of signals we analyze from our worldwide ecosystem of products and services reveal the ferocity, scope, and scale of digital threats across the globe. Microsoft is taking action to defend our customers and the digital ecosystem against these threats, and you can read about our technology that identifies and blocks billions of phishing attempts, identity thefts, and other threats to our customers.

Introduction by Tom Burt

Continued

We also use legal and technical means to seize and shut down infrastructure used by cybercriminals and nation state actors and notify customers when they are being threatened or attacked by a nation state actor. We work to develop increasingly effective features and services that use AI/ML technology to identify and block cyber threats and security professionals defend against and identify cyber-intrusions more rapidly and effectively.

Perhaps most importantly, throughout the MDDR we offer our best advice on the steps individuals, organizations, and enterprises can take to defend against these increasing digital threats. Adopting good cyber hygiene practices is the best defense and can significantly reduce the risk of cyberattacks.

The state of cybercrime

Cybercriminals continue to act as sophisticated profit enterprises. Attackers are adapting and finding new ways to implement their techniques, increasing the complexity of how and where they host campaign operation infrastructure. At the same time, cybercriminals are becoming more frugal. To lower their overhead and boost the appearance of legitimacy, attackers are compromising business networks and devices to host phishing campaigns, malware, or even use their computing power to mine cryptocurrency.

> “The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict.”

Nation state threats

Nation state actors are launching increasingly sophisticated cyberattacks designed to evade detection and further their strategic priorities. The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict. Russia has also supported its war with information influence operations, using propaganda to impact opinions in Russia, Ukraine, and globally. Outside Ukraine, nation state actors have increased activity and have begun using advancements in automation, cloud infrastructure, and remote access technologies to attack a wider set of targets. Corporate IT supply chains that enable access to ultimate targets were frequently attacked. Cybersecurity hygiene became even more critical as actors rapidly exploited unpatched vulnerabilities, used both sophisticated and brute force techniques to steal credentials, and obfuscated their operations by using opensource or legitimate software. In addition, Iran joins Russia in the use of destructive cyberweapons, including ransomware, as a staple of their attacks.

These developments require urgent adoption of a consistent, global framework that prioritizes human rights and protects people from reckless state behavior online. All nations must work together to implement norms and rules for responsible state conduct.

Devices and infrastructure

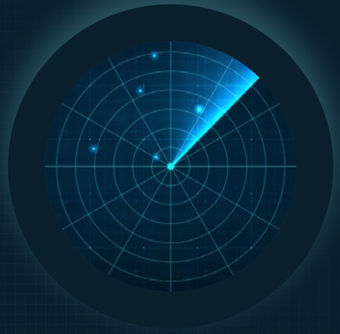
The pandemic, coupled with rapid adoption of internet-facing devices of all kinds as a component of accelerating digital transformation, has greatly increased the attack surface of our digital world. As a result, cybercriminals and nation states are quickly taking advantage. While the security of IT hardware and software has strengthened in recent years, the security of IoT and OT devices security has not kept pace. Threat actors are exploiting these devices to establish access on networks and enable lateral movement, to establish a foothold in a supply chain, or to disrupt the target organization’s OT operations.

Introduction by Tom Burt

Continued

Cyber influence operations

Nation states are increasingly using sophisticated influence operations to distribute propaganda and impact public opinion both domestically and internationally. These campaigns erode trust, increase polarization, and threaten democratic processes. Skilled Advanced Persistent Manipulator actors are using traditional media together with internet and social media to vastly increase the scope, scale, and efficiency of their campaigns, and the outsized impact they are having in the global information ecosystem.
In the past year, we have seen these operations used as part of Russia's hybrid war in Ukraine, but have also seen Russia and other nations, including China and Iran, increasingly deploy propaganda operations powered by social media to extend their global influence on a range of issues.



Cyber resilience

Security is a key enabler of technological success. Innovation and enhanced productivity can only be achieved by introducing security measures that make organizations as resilient as possible against modern attacks. The pandemic has challenged us at Microsoft to pivot our security practices and technologies to protect our employees wherever they work. This past year, threat actors continued to take advantage of vulnerabilities exposed during the pandemic and the shift to a hybrid work environment. Since then, our principal challenge has been managing the prevalence and complexity of various attack methods and increased nation state activity. In this chapter, we detail the challenges we have faced, and the defenses we have mobilized in response with our more than 15,000 partners.

Our unique vantage point

43tn
signals synthesized daily, using sophisticated data analytics and AI algorithms to understand and protect against digital threats and criminal cyberactivity.

8,500+
engineers, researchers, data scientists, cybersecurity experts, threat hunters, geopolitical analysts, investigators, and frontline responders across 77 countries.

15,000+
partners in our security ecosystem who increase cyber resilience for our customers.

37bn
email threats blocked

34.7bn
identity threats blocked

2.5bn
endpoint signals analyzed daily

July 1, 2021 through June 30, 2022

Introduction by Tom Burt

Continued

We believe Microsoft—independently and through close partnerships with others in private industry, government, and civil society—has a responsibility to protect the digital systems that underpin the social fabric of our society and promote safe, secure computing environments for every person, wherever they are located. This responsibility is the reason we have published the MDDR each year since 2020. The report is the culmination of Microsoft's vast data and comprehensive research. It shares our unique insights on how the digital threat landscape is evolving and the crucial actions that can be taken today to improve the security of the ecosystem.

We hope to instill a sense of urgency, so readers take immediate action based on the data and insights we present both here and in our many cybersecurity publications throughout the year. As we consider the gravity of the threat to the digital landscape—and its translation into the physical world—it is important to remember that we are all empowered to take action to protect ourselves, our organizations, and enterprises against digital threats.

Read the report in full

Thank you for taking the time to review this year's Microsoft Digital Defense Report. We hope you will find that it provides valuable insight and recommendations to help us collectively defend the digital ecosystem.

Tom Burt
Corporate Vice President,
Customer Security & Trust

Our objective with this report is twofold:

1. To illuminate the evolving digital threat landscape for our customers, partners, and stakeholders spanning the broader ecosystem, shining a light on both new cyberattacks and evolving trends in historically persistent threats.
2. To empower our customers and partners to improve their cyber resiliency and respond to these threats.

An overview of

The State of Cybercrime

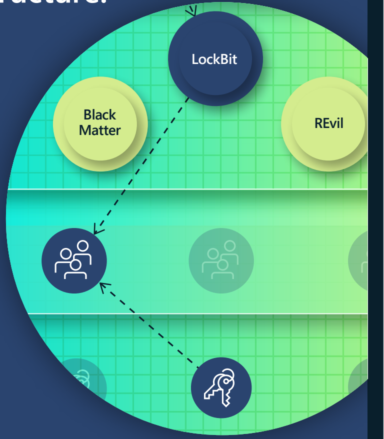
As cyber defenses improve and more organizations are taking a proactive approach to prevention, attackers are adapting their techniques.

Cybercriminals continue to act as sophisticated profit enterprises. Attackers are adapting and finding new ways to implement their techniques, increasing the complexity of how and where they host campaign operation infrastructure. At the same time, cybercriminals are becoming more frugal. To lower their overhead and boost the appearance of legitimacy, attackers are compromising business networks and devices to host phishing campaigns, malware, or even use their computing power to mine cryptocurrency.

Learn more in the full report
The State of Cybercrime chapter

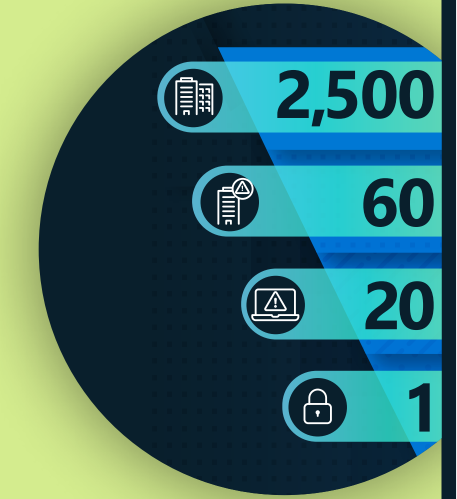
Cybercrime continues to rise as the industrialization of the cybercrime economy lowers the skill barrier to entry by providing greater access to tools and infrastructure.

The threat of ransomware and extortion is becoming more audacious with attacks targeting governments, businesses, and critical infrastructure.

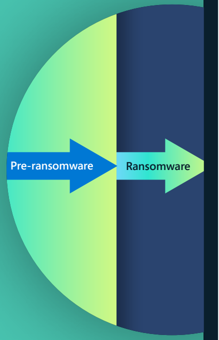


Attackers increasingly threaten to disclose sensitive data to encourage ransom payments.

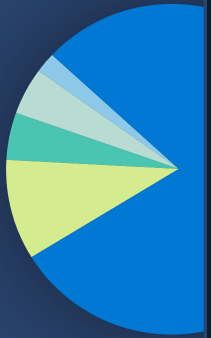
Human operated ransomware is most prevalent, as one-third of targets are successfully compromised by criminals using these attacks and 5% of those are ransomed.



The most effective defense against ransomware includes multifactor authentication, frequent security patches, and Zero Trust principles across network architecture.



Credential phishing schemes which indiscriminately target all inboxes are on the rise and business email compromise, including invoice fraud, poses a significant cybercrime risk for enterprises.



To disrupt the malicious infrastructures of cybercriminals and nation state actors, Microsoft relies on innovative legal approaches and our public and private partnerships.

An overview of

Nation State Threats

Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities. The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict.

Russia has also supported its war with information influence operations, using propaganda to impact opinions in Russia, in Ukraine, and globally. This first full-scale hybrid conflict has taught other important lessons. First, the security of digital operations and data can be best protected – both in cyberspace and in physical space – by moving to the cloud. Initial Russian attacks targeted on-premises services with wiper malware, and targeted physical data centers with one of the first missiles launched.

Ukraine responded by rapidly moving workloads and data to hyperscale clouds hosted in data centers outside Ukraine. Second, advances in cyber threat intelligence and endpoint protection powered by the data and advanced AI and ML services in the cloud have helped Ukraine defend against Russian cyberattacks.

Elsewhere, nation state actors have increased activity and are using advancements in automation, cloud infrastructure, and remote access technologies to attack a wider set of targets. Corporate IT supply chains that enable access to ultimate targets were frequently attacked. Cyber security hygiene became even more critical as actors rapidly exploited unpatched vulnerabilities, used both sophisticated and brute force techniques to steal credentials, and obfuscated their operations by using opensource or legitimate software. And Iran joins Russia in use of destructive cyberweapons, including ransomware, as a staple of their attacks.

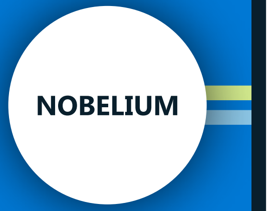
These developments require urgent adoption of a consistent, global framework that prioritizes human rights and protects people from reckless state behavior online. All nations must work to implement agreed upon norms and rules for responsible state conduct.

> Defending Ukraine: Early Lessons from the Cyber War — Microsoft On the Issues

> Learn more in the full report Nation State Threats chapter

Increased targeting of critical infrastructure particularly IT sector, financial services, transportation systems, and communications infrastructure.

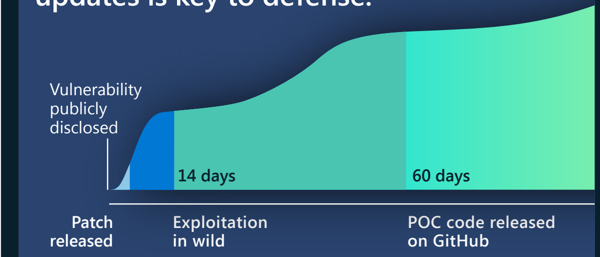
IT supply chain being used as a gateway to access targets.



China expanding global targeting especially smaller nations in Southeast Asia, to gain intelligence and competitive advantage.

Iran grew increasingly aggressive following power transition, expanded ransomware attacks beyond regional adversaries to US and EU victims, and targeted high profile US critical infrastructure.

Identification and rapid exploitation of unpatched vulnerabilities has become a key tactic. Rapid deployment of security updates is key to defense.



North Korea targeted defense and aerospace companies, cryptocurrency, news outlets, defectors, and aid organizations, to achieve regime's goals: to build defense, bolster the economy, and ensure domestic stability.

Cyber mercenaries threaten the stability of cyberspace as this growing industry of private companies is developing and selling advanced tools, techniques, and services to enable their clients (often governments) to break into networks and devices.

An overview of

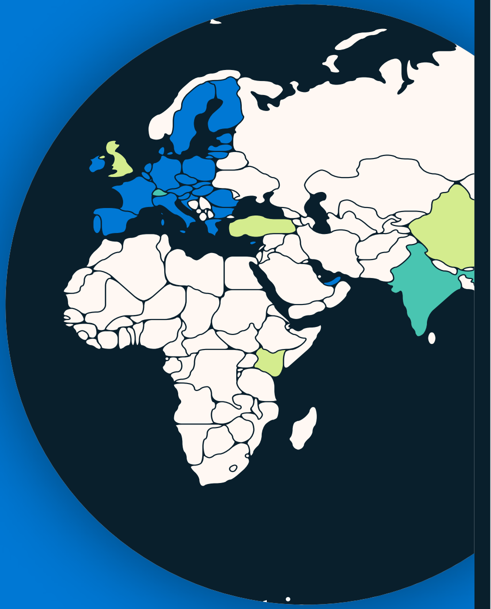
Devices and Infrastructure

The pandemic, coupled with rapid adoption of internet-facing devices of all kinds as a component of accelerating digital transformation, has greatly increased the attack surface of the digital world.

Cybercriminals and nation-states are quickly taking advantage. While the security of IT hardware and software has strengthened in recent years, the security of Internet of Things (IoT) and Operational Technology (OT) devices has not kept pace. Threat actors are exploiting these devices to establish access on networks and enable lateral movement, to establish a foothold in a supply chain, or to disrupt the target organization's OT operations.

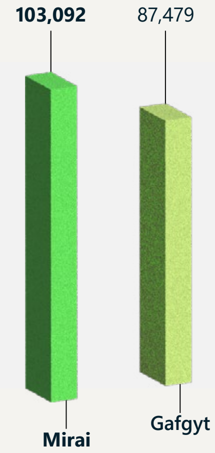
Learn more in the full report Devices and Infrastructure chapter

Governments worldwide are moving to protect critical infrastructure by improving IoT and OT security.



Globally consistent and interoperable security policies are needed to ensure broad adoption.

Malware as a service has moved into large scale operations against exposed IoT and OT in infrastructure and utilities as well as corporate networks.



Attacks against remote management devices are on the rise, with more than 100 million attacks observed in May of 2022—a five-fold increase in the past year.

Attackers are increasingly leveraging vulnerabilities in IoT device firmware to infiltrate corporate networks and launch devastating attacks.

32% of firmware images analyzed contained at least 10 known critical vulnerabilities.

An overview of

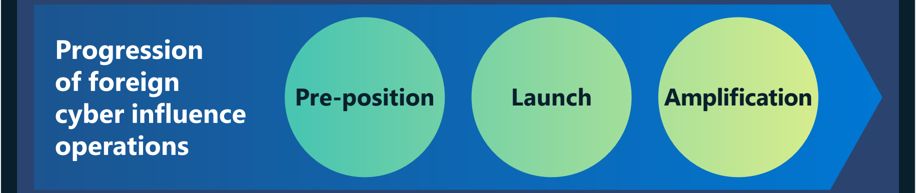
Cyber Influence Operations

Today's foreign influence operations utilize new methods and technologies, making their campaigns designed to erode trust more efficient and effective.

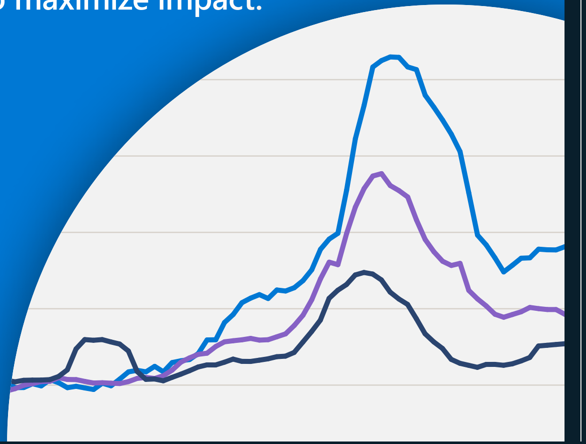
Nation states are increasingly using sophisticated influence operations to distribute propaganda and impact public opinion both domestically and internationally. These campaigns erode trust, increase polarization, and threaten democratic processes. Skilled Advanced Persistent Manipulator actors are using traditional media together with internet and social media to vastly increase the scope, scale, and efficiency of their campaigns, and the outsized impact they are having in the global information ecosystem. In the past year, we have seen these operations used as part of Russia's hybrid war in Ukraine, but have also seen Russia and other nations, including China and Iran, increasingly turning to social-media powered propaganda operations to extend their global influence.

Learn more in the full report
Cyber Influence Operations chapter

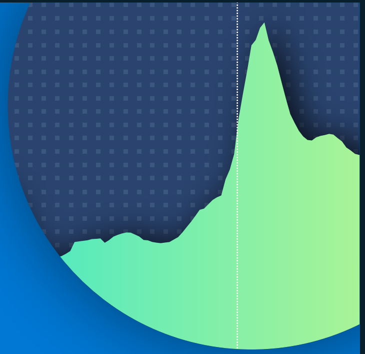
Cyber influence operations are becoming increasingly sophisticated as more governments and nation states are using these operations to shape opinion, discredit adversaries, and promote discord.



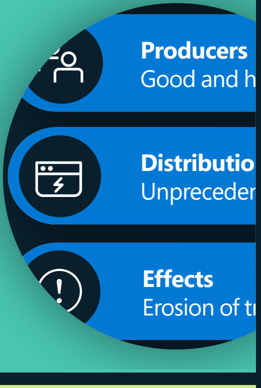
Russia's invasion of Ukraine demonstrates cyber influence operations integrated with more traditional cyberattacks and kinetic military operations to maximize impact.



Russia, Iran, and China employed propaganda and influence campaigns throughout the COVID-19 pandemic often as a strategic device to achieve broader political objectives.



Synthetic media is becoming more prevalent due to the proliferation of tools which easily create and disseminate highly realistic artificial images, videos, and audio. Digital provenance technology that certifies media asset origin holds promise to combat misuse.



A holistic approach to protect against cyber influence operations

Microsoft is building on its already mature cyber threat intelligence infrastructure to combat cyber influence operations. Our strategy is to detect, disrupt, defend, and deter propaganda campaigns by foreign aggressors.

An overview of

Cyber Resilience

Cyber security is a key enabler of technological success. Innovation and enhanced productivity can only be achieved by introducing security measures that make organizations as resilient as possible against modern attacks.

The pandemic has challenged us to pivot our security practices and technologies to protect Microsoft's employees wherever they work. This past year, threat actors continued to take advantage of vulnerabilities exposed during the pandemic and the shift to a hybrid work environment. Since then, our principal challenge has been managing the prevalence and complexity of various attack methods and increased nation state activity.

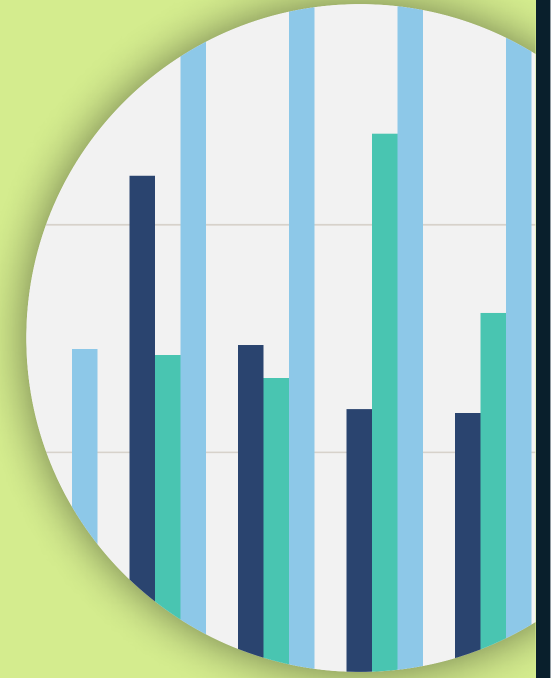
Learn more in the full report Cyber Resilience chapter

Effective cyber resiliency requires a holistic, adaptive approach to withstand evolving threats to core services and infrastructure.

Modernized systems and architecture are important for managing threats in a hyperconnected world.

Basic security posture is a determining factor in advanced solution effectiveness.

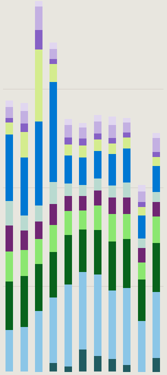
While password-based attacks remain the main source of identity compromise, other types of attacks are emerging.



The human dimension of resilience to cyber influence operations is our ability to collaborate and cooperate.

The vast majority of successful cyberattacks could be prevented by using basic security hygiene.

Over the past year, the world experienced DDoS activity that was unprecedented in volume, complexity, and frequency.



Microsoft

Illuminating the threat landscape
and empowering a digital defense.

Learn more: **https://microsoft.com/mddr**

Dive deeper: **https://blogs.microsoft.com/on-the-issues/**

Stay connected: **@msftissues and @msftsecurity**