Espionage fuels global cyberattacks

Oct 5, 2023 | Tom Burt - Corporate Vice President, Customer Security & Trust

In the past year, cyberattacks have touched 120 countries, fueled by government-sponsored spying and with influence operations (IO) also rising. At times, nearly half of these attacks targeted NATO member states, and more than 40% were leveled against government or private-sector organizations involved in building and maintaining critical infrastructure. While headline-grabbing attacks from the past year were often focused on destruction or financial gain with ransomware, data shows the predominant motivation has swung back to a desire to steal information, covertly monitor communication, or to manipulate what people read. For example:

- Russian intelligence agencies have refocused their cyberattacks on espionage activity in support of their war against Ukraine, while continuing destructive cyberattacks in Ukraine and broader espionage efforts

Related Stories

Sep 7, 2023 | Clint Watts

China, North Korea pursue new targets while honing cyber capabilities >

Sep 1, 2023 | Clint Watts

Russia's African coup strategy >

Aug 16, 2023 | Michelle Patron

Advocating for decarbonization of the power sector >

Related Blogs

Oct 2, 2023 | Jenny Lay-Flurrie

Creating a more disability-inclusive workplace >

Sep 21, 2023 | Brad Smith

- Iranian efforts, once focused on taking down the networks of their targets, are also inclined today to amplify manipulative messages to further geopolitical goals or tap into data flowing through sensitive networks
- China has expanded its use of spying campaigns to gain intelligence to fuel its Belt and Road Initiative or regional politics, to spy on the U.S. including key facilities for the U.S. military, and to establish access to the networks of critical infrastructure entities
- North Korean actors have been trying to covertly steal secrets; they've targeted a company involved in submarine technology, while separately using cyberattacks to steal hundreds of millions in cryptocurrency

These are some of the insights from the fourth annual Microsoft Digital Defense Report, which covers trends between July 2022 and June 2023 across nation-state activity, cybercrime, and defense techniques.

More countries, sectors under attack

While the U.S., Ukraine, and Israel continue to be most heavily attacked, the last year has seen an increase in the global scope of attacks. This is particularly the case in the Global South, especially Latin America and sub-Saharan Africa. Iran increased its operations in the Middle East. Organizations involved in policymaking and execution were among the most targeted, in line with the shift in focus to espionage.

The most targeted nations by region* were:

Europe	Middle East & North Africa	Asia Pacific
1. Ukraine (33%)	1. Israel (38%)	1. Korea (17%)
2. United Kingdom (11%)	2. United Arab Emirates (12%)	2. Taiwan (15%)
3. France (5%)	3. Saudi Arabia (9%)	3. India (13%)
4. Poland (5%)	4. Jordan (6%)	4. Malaysia (6%)
5. Italy (4%)	5. Iraq (5%)	5. Japan (5%)
6. Germany (3%)	6. Bahrain (4%)	6. Australia (5%)

*Fuller data breakdown can be found in the report

Russia and China increase focus on diaspora communities

Business, labor, and others join to support Microsoft's position in FTC appeal ›

Sep 12, 2023 | Brad Smith

Developing and deploying AI responsibly: Elements of an effective legislative framework to regulate AI ›

More Cybersecurity Stories

Standing up for democratic values and protecting stability of cyberspace: Principles to limit the threats posed by cyber mercenaries ›

April 11, 2023

Digital Crimes Unit: Leading the fight against cybercrime ›

May 3, 2022

Keeping your vote safe and secure: A story from inside the 2020 election >

June 22, 2021

Both Russia and China are increasing the scope of their influence operations against a variety of diasporas. Russia aims to intimidate global Ukrainian communities and sow mistrust between war refugees and host communities in a range of countries, especially Poland and the Baltic states. By contrast, China deploys a vast network of coordinated accounts across dozens of platforms to spread covert propaganda. These directly target global Chinese-speaking and other communities, denigrating U.S. institutions, and promoting a positive image of China through hundreds of multilingual lifestyle influencers.

Convergence of influence operations with cyberattacks

Nation state actors are more frequently employing IO alongside cyber operations to spread favored propaganda narratives. These aim to manipulate national and global opinion to undermine democratic institutions within perceived adversary nations – most dangerously in the contexts of armed conflicts and national elections. For example, following its invasion of Ukraine, Russia consistently timed its IO operations with military and cyberattacks. Similarly, in July and September 2022, Iran followed destructive cyberattacks on the Albanian government with a coordinated influence campaign which is still ongoing.

Trends by nation state

While there has been an increase overall in threat activity, trends have been observed with the most active nation state actors.

- **Russia targets Ukraine's NATO allies**
  Russian state actors expanded their Ukraine-related activities to target Kyiv's allies, principally NATO members. In April and May 2023, Microsoft observed a spike in activity against Western organizations, 46% of which were in NATO member states, particularly the United States, the United Kingdom, and Poland. Several Russian state actors posed as Western diplomats and Ukrainian officials, attempting account access. The goal was to obtain insights into Western foreign policy on Ukraine, defense plans and intentions, and war crimes investigations.

- **China targets US defense, South China Sea nations and Belt and Road Initiative partners**
  China's expanded and sophisticated activities reflect its dual pursuits of global influence and intelligence collection. Their

targets are most commonly U.S. defense and critical infrastructure, nations bordering the South China Sea (especially Taiwan) and even China's own strategic partners. In addition to the multiple sophisticated attacks on U.S. infrastructure detailed in the report, Microsoft has also seen China-based actors attack China's Belt and Road Initiative partners such as Malaysia, Indonesia, and Kazakhstan.

- **Iran brings new attacks to Africa, Latin America, and Asia** The past year has seen some Iranian state actors increase the complexity of their attacks. Iran has not only targeted Western countries it believes are fomenting unrest within Iran, but it has also expanded its geographical reach to include more Asian, African, and Latin American countries. On the IO front, Iran has pushed narratives that seek to bolster Palestinian resistance, sow panic among Israeli citizens, foment Shi'ite unrest in Gulf Arab countries, and counter the normalization of Arab-Israeli ties. Iran has also made efforts to increase the coordination of its activities with Russia.

- **North Korea targets Russian organizations among others** North Korea has increased the sophistication of its cyber operations in the last year, especially in cryptocurrency theft and supply-chain attacks. Additionally, North Korea is using spear-phishing emails and LinkedIn profiles to target Korean peninsula experts around the world to gather intelligence. Despite the recent meeting between Putin and Kim Jong-Un, North Korea is targeting Russia, especially for nuclear energy, defense, and government policy intelligence collection.

AI creates new threats – and new opportunities for defense

Attackers are already using AI as a weapon to refine phishing messages and improve influence operations with synthetic imagery. But AI will also be crucial for successful defense, automating, and augmenting aspects of cybersecurity such as threat detection, response, analysis, and prediction. AI can also enable large language models (LLMs) to generate natural language insights and recommendations from complex data, helping make analysts more effective and responsive.

We are already seeing AI-powered cyber-defense reversing the tide of cyberattacks; in Ukraine, for example, AI has helped defend against Russia.

As transformative AI reshapes many aspects of society, we must engage in Responsible AI practices crucial for maintaining user trust and privacy, and for creating long-term benefits. Generative AI models require us to evolve cybersecurity practices and threat models to address new challenges, such as the creation of realistic content – including text, images, video, and audio – that can be used by threat actors to spread misinformation or create malicious code. To stay ahead of these emerging threats, we remain committed to ensuring that all our AI products and services are developed and used in a manner that upholds our AI principles.

The state of cybercrime

The game of cat and mouse between cybercriminals and defenders continues to evolve. While threat groups have significantly accelerated the pace of their attacks over the last year, built-in protections across Microsoft products have blocked tens of billions of malware threats, thwarted 237 billion brute-force password attack attempts, and mitigated 619,000 distributed denial of service (DDoS) attacks that aim to disable a server, service, or network by overwhelming it with a flood of internet traffic.

Criminals are also looking to increase their anonymity and effectiveness, by using remote encryption to cover their traces more effectively as well as cloud-based tools such as virtual machines. But stronger private and public partnerships mean that they are increasingly finding themselves in the crosshairs of law enforcement. For example, the ransomware operator known as Target was outed, and arrests and indictments were successfully made. But criminals continue to look for the points of easiest entry to systems and a continuous and accelerating effort is required to stay one step ahead of them.

Ransomware attacks increase in sophistication and speed

Microsoft's telemetry indicates organizations saw human-operated ransomware attacks increase 200% since September 2022. These attacks are generally a "hands on keyboard" type of attack rather than an automated one, typically targeting a whole organization with customized ransom demands.

Attackers are also evolving attacks to minimize their footprint, with 60% using remote encryption, thereby rendering process-based remediation ineffective.

These attacks are also notable for how they attempt to gain access to unmanaged or bring-your-own devices. More than 80% of all compromises we observed originate from such unmanaged devices. Ransomware operators are increasingly exploiting vulnerabilities in less common software, making it more difficult to predict and defend against attacks.

Ransomware criminals also threaten disclosure of stolen information to pressure victims and extract payment. Since November 2022, we have observed a doubling of potential data exfiltration instances after threat actors compromised an environment. But not all data theft is associated with ransomware; it can also be for credential harvesting or nation-state espionage.

Password-based and Multifactor Authentication (MFA) fatigue attacks skyrocket

MFA is the increasingly common authentication method that requires users to provide two or more "factors" of identification to gain access to a website or application – such as a password along with facial recognition or a one-time passcode. While deploying MFA is one of the easiest and most effective defenses organizations can deploy against attacks, reducing the risk of compromise by 99.2%, threat actors are increasingly taking advantage of "MFA fatigue" to bombard users with MFA notifications in the hope they will finally accept and provide access.

Microsoft has observed approximately 6,000 MFA fatigue attempts per day over the past year. Additionally, the first quarter of 2023 saw a dramatic tenfold surge in password-based attacks against cloud identities, especially in the education sector, from around 3 billion per month to over 30 billion – an average of 4,000 password attacks per second targeting Microsoft cloud identities this year.

The only secure defense will be a collective defense

The scale and nature of threats outlined in the Microsoft Digital Defense Report can appear dispiriting. But huge strides are being made on the technology front to defeat these attackers and at the same time, strong partnerships are being forged that transcend borders, industries, and the private-public divide. These partnerships are having ever greater success in keeping us all safe and this is why it is vital we continue to broaden and

deepen them. Some 75% of eligible citizens in democratic nations have the opportunity to vote in the next year and a half. Keeping elections safe and democratic institutions strong is a cornerstone of our collective defense.

Tags: China, cyber influence, cyberattacks, cybercrime, cybersecurity, Iran, NATO, Russia