Bad Bots and Beyond: 2023 State of the Threat

Attack insights from across the Arkose Labs Global Network

2023

Arkose Labs

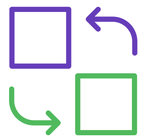
Introduction

As cybercrime continues to evolve, the need for comprehensive insight and protection becomes increasingly urgent. In 2022, the illegal returns of cyberattacks have risen, as bad actors are now able to threaten companies and consumer trust before any transaction takes place. To stay ahead of these evolving threats, Arkose Labs has analyzed billions of sessions to uncover the top attack trends for 2023 and provide businesses with the necessary tools and resources to effectively protect their users.

This 2023 report reflects a chaotic year in cybercrime, which saw attacks reach an all-time high in response to the Russo-Ukrainian war. Setting up policies, systems, and software is not enough to effectively protect against cybercrime. Security must be dynamic and regularly adjusted to stay ahead of attackers, who could exploit any vulnerabilities and cause serious harm if defenses remain stagnant.

2023 Attack Trend Highlights

SHIFTING ATTACK SURFACE



HACKTIVISM

CYBERCRIME-AS-A-SERVICE (CaaS)

RANSOMWARE

MOBILE MALWARE

Chapter One: Shifting Attack Surfaces

The past year brought about significant changes in the attack surface for online entities, with the global pandemic driving many of these shifts. In particular, the move to remote work has forced organizations to adopt new technologies and practices to facilitate communication and collaboration, leading to new vulnerabilities and attack vectors.

Other factors contributing to this expanding shift include

The widespread adoption of cloud-based services and platforms, such as Software as a Service (SaaS) and Infrastructure as a Service (IaaS) has provided cybercriminals with new opportunities to exploit vulnerabilities in cloud infrastructures and attack remote workers.

STATS:

- → 94 % of companies in 2022 used cloud services.
- → As of 2022, roughly 41% of enterprise workloads were in the cloud.
- → There are over 3.6 billion cloud users in the world.

The rise of cryptocurrency and blockchain technology have created new opportunities for threat actors. Decentralized and distributed, cryptocurrencies are a favored form of payment for ransomware attacks. Criminals can take advantage of the anonymity provided they offer, to obscure activities and make it harder for law enforcement to track.

STATS:

- → In 2021, ransomware attacks impacted at least 2,323 local governments, schools, and healthcare providers in the US.
- → According to the World Economic Forum, ransomware attacks increased by 435 percent in 2020 and “are outpacing societies’ ability to effectively prevent or respond to them.
- → In 2021, the agency received 3,729 ransomware complaints with adjusted losses of more than $49.2 million.

The proliferation of Internet of Things (IoT) devices, now a regular part of homes, businesses, and public spaces, are often poorly secured and can be used as entry points for criminals:

STATS:

- → In 2022, 35.37 billion IoT devices were in use, up from 10 billion the year before.
- → By 2025, there will be 152,200 IoT devices connecting to the internet per minute.

The evolution of generative AI, like ChatGPT, has become an enabler for dangerously effective social engineering attacks that reduce barriers and increase efficiency/volume of tailored attacks.

STATS:

- → In 2022, 35.37 billion IoT devices were in use, up from 10 billion the year before.
- → By 2025, there will be 152,200 IoT devices connecting to the internet per minute.

Top 5 Industries Most Vulnerable to Attack

While it's true any industry can be subjected to a cyberattack, the reality is some sectors are more vulnerable than others. The difference between a cyberattack and a cybercrime is usually determined by its potential for financial gain, such as the amount of information that can be taken and/or damage that can be done.

Is your industry included in any of these five categories? If so, take notice:

Fintech | Banks | Financial Services

Hackers have their sights set on the financial services industry, and it's no wonder why. With the average data breach detection being 233 days, cybercriminals have plenty of time to take advantage of vulnerable networks. The fast-paced digital transformation that many financial services businesses are undergoing has also created more opportunity for attack.

Banking apps, cloud storage, and other technologies are becoming more popular, but also more prone to security risks. Fintechs, banks, and financial institutions all face enormous pressure to keep up with these changes and protect their customers' data.

STATS:

- → 70% in banking ranked cybersecurity as a top concern.
- → Cost of cyberattacks is highest in the banking industry, reaching $18.3 million annually per company.
- → Finance reported 703 cyberattack attempts per week in Q4 2021, a 53% increase.
- → On a global scale, the rate of cyber attacks on a fintech is one every 10 seconds.
- → The fintech industry suffered 34% of criminal incidents, with a 12-fold increase in attacks on financial services, making it a more targeted sector than others.

Notable Breach in Financial Services:

The attack on Capital One Financial Corporation in July 2019, was one of the most visible attacks to date. A threat actor managed to access the financial data of over 100 million customers, including names, addresses, phone numbers, birthdates, and Social Security numbers of U.S. and Canadian customers. The hacker also obtained 140,000 Social Security numbers and 80,000 bank account numbers of Capital One customers, and was able to gain access to this information by exploiting a misconfigured web application firewall that was maintained by a third-party vendor.

The attacker was able to steal the data from Capital One's cloud environment. The cloud environment was found to have inadequate security measures in place, allowing the attacker to exploit the vulnerability. Capital One responded to the attack by immediately notifying customers, taking steps to mitigate the risk of further exploitation, and launching an investigation into the incident. The company has since implemented enhanced security measures and is working with law enforcement to investigate the threat.

Finserv | Top 3 Action Items:

- ☐ Implement strong authentication measures to ensure that all accounts are protected with strong methods like two-factor authentication and biometrics.
- ☐ Monitor networks and systems—and implement monitoring solutions to detect suspicious activity on networks and systems.
- ☐ Utilize security solutions and invest in security solutions such as firewalls, anti-virus software, and intrusion detection systems.

2. Healthcare

The healthcare industry is highly vulnerable to cyberattacks due to their extensive storage of Personal Identifiable Information (PII). This information, when compromised, can lead to identity theft and other disastrous outcomes. Healthcare-related ransomware attacks are particularly concerning, as they are capable of directly impacting the health and well-being of patients.

When a hospital's system has been compromised, doctors are unable to access patient records or medical history, leaving them unable to provide the necessary care. This lack of access to important medical data can result in delayed treatments, misdiagnoses, and other potentially life-threatening scenarios. It is essential that healthcare organizations remain vigilant when it comes to cybersecurity, as the consequences of a data breach can be catastrophic.

Notable Breach in Healthcare:

In September 2020, Universal Health Services (UHS) fell victim to a malicious cyberattack that forced them to shut down their computer network in order to contain the threat. The attack included ransomware that encrypts the data of UHS's facilities in the U.S., U.K., and Australia, as well as impacted other technologies, such as patient scheduling and medical record systems. As a result of the attack, UHS had to rely on manual processes to provide patient care—and have yet to fully recover their IT systems.

Healthcare | Top 3 Action Items:

- ☐ Utilize advanced encryption software and technologies to secure data and prevent unauthorized access to systems.
- ☐ Establish a risk management strategy to identify and evaluate potential threats.
- ☐ Invest in automated threat detection and response solutions to quickly detect and respond to threats.

3. Education

The Covid-19 pandemic has had a profound impact on a range of industries, but none more so than the educational sector. The rapid shift to online learning has meant that universities and other educational institutions have had to rapidly open up their networks and systems to a much larger user base.

This situation has presented a ripe opportunity for hackers and cyber criminals to exploit, as many of these institutions often lack the necessary budget to invest in adequate staff and security systems. Indeed, the already diminishing budgets of educational institutions has only been exacerbated by the pandemic, further increasing the risk of a cyberattack.

Notable Breach in Education:

In 2021, the world's largest K-12 school district, Miami-Dade County Public Schools, was the victim of a major cyberattack. The attack, which took place in March, targeted the district's technological infrastructure, including its computer networks and student information systems. The attack caused the district to shut down its entire network, disrupting classes, communication with parents, and access to student data.

The attack was carried out by an unknown group of hackers who used ransomware to encrypt the district's data and demand a ransom payment. The district refused to pay, instead opting to rebuild its systems from backups and take steps to protect against future attacks. The attack is notable for its scale and sophistication, as well as the disruption it caused.

Education | Top 3 Action Items:

- ☐ Train staff to recognize threats, such as spear phishing, ransomware, and other malicious activity, and how to respond appropriately.
- ☐ Regularly backup data to an external hard drive or cloud storage.
- ☐ Utilize two-factor authentication and strong password practices for any employee or student accounts.

4. Energy | Utilities

Sometimes hackers are interested in much more than just financial gain and data theft. A massive power outage, capable of disrupting the lives of millions, demonstrates how much control these malicious actors can wield over our daily lives. If hackers are able to infiltrate entire power grids or nuclear facilities, the consequences could be catastrophic.

According to industry reports, there is an increased risk of attack from "hacktivists," or cybercriminals with political and social agendas, targeting energy companies in response to any controversies. The ever-growing reliance on technology has made critical infrastructures increasingly vulnerable. As a result, it's essential for businesses to invest in the latest cyber security tools and techniques in order to protect their networks and systems from attack.

Notable Breach in Energy Sector:

In February of 2022, a group of threat actors known as the Black Sun Collective launched a large-scale cyberattack in the energy sector. The attack targeted several energy providers in both the U.S. and Europe. The attack resulted in the disruption of power to over a million people, and cost hundreds of millions of dollars in damages. It found success using a combination of phishing and ransomware tactics to gain access to the energy providers' networks, and to encrypt their data.

The hackers were able to successfully steal data and cause significant damage before the attack was neutralized. It is believed that the attack was motivated by political and economic reasons, and it is still unclear who was behind it. Fortunately, the attack was eventually stopped and the stolen data was recovered. The incident served as a wake-up call for energy providers to take more proactive steps to protect their systems.

Energy & Utilities | Top 3 Action Items:

- ☐ Utilize advanced threat detection capabilities to detect and respond to cyberattacks in realtime.
- ☐ Establish a secure backup of critical systems to ensure data can be quickly restored in case of an attack.
- ☐ Regularly test systems and automate patch management to address vulnerabilities as soon as they are identified.

Chapter Two: Hacktivism

Hacktivists develop tools for politically motivated actions that eventually become adopted by for-profit criminals, leading to an increase in the strength and duration of attacks.

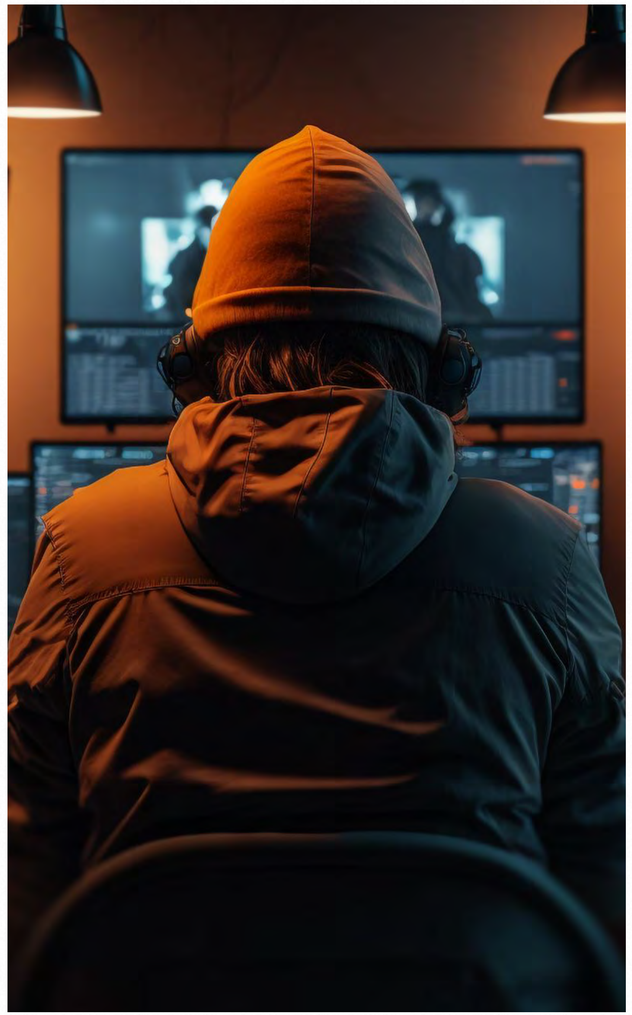
Traditionally, hacktivism referred to politically or socially motivated cyberattacks carried out by loosely managed entities, like Anonymous. These groups were often disorganized and ad hoc, with individuals cooperating for various agendas. However, in the past year, the hacktivist landscape has matured, particularly due to the Russian-Ukrainian conflict. Hacktivist groups have become more organized and sophisticated in their operations, conducting military-like campaigns that include recruitment, training, sharing intelligence and tools, and selecting targets.

Many of these groups now have a consistent and clearly defined political ideology that aligns with governmental narratives. Others may be less politically motivated but still operate in a professional and organized manner. Either way, hacktivism has graduated to a major player on the geopolitical stage.

Unlike Anonymous, who accept individuals regardless of skill level or agenda, the new era of hacktivists implement a screening process to ensure applicants meet specific requirements. This requirement helps to minimize the risk of exposing their operations to outsiders. Organized hacktivist groups invest in the development of their members' technical proficiency and tools. While their activities often focus on defacement and distributed denial-of-service (DDoS) attacks using botnets, some groups have also begun using more advanced and destructive tools.

The Why & How of Hacktivism

Hacktivism refers to the use of hacking or cyber attacks for political or social activism purposes. The ongoing battle among hacktivist groups extends beyond causing damage through cyber attacks. These groups recognize the significance of media coverage and use communication channels to publicize reports of their successful attacks to maximize their impact. For instance, Killnet is an active group that utilizes its Telegram channel to share details of their attacks, recruit new members, and distribute attack tools. With over 89,000 subscribers, Killnet's activities are extensively covered by major Russian media outlets to highlight their achievements in cyberspace and validate the impact of their successful attacks.

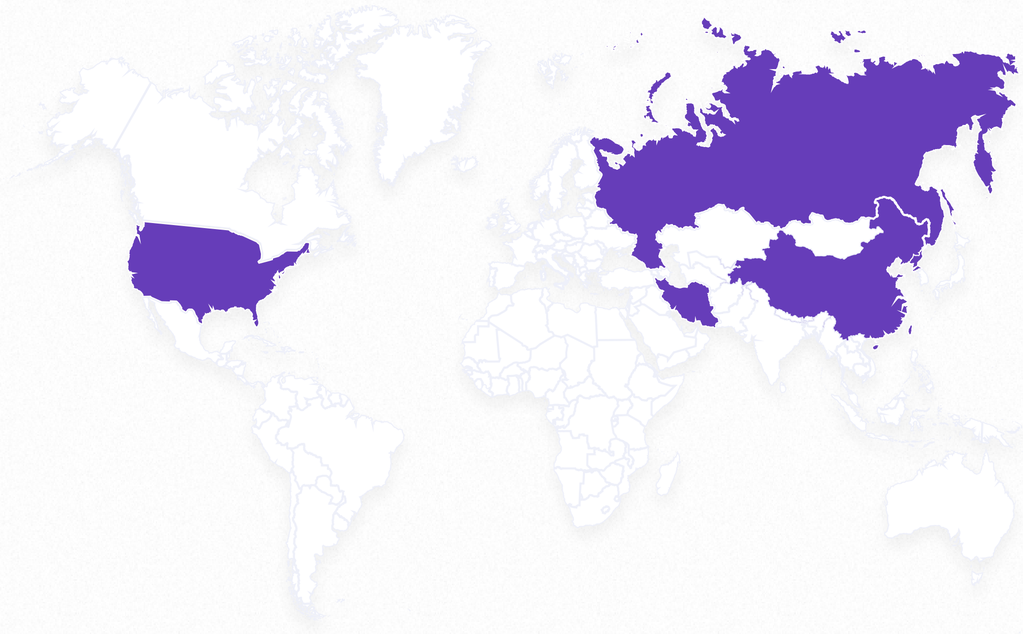


Highly organized and coordinated hacktivist groups also leverage their resources to collaborate with other entities. The evolution of the hacktivism landscape is not confined to particular national conflicts or geographical areas. Nowadays, major corporations and governments in Europe and the United States are being targeted by this new breed of hacktivism. These groups are mobilized based on political narratives and have achieved strategic and widespread objectives with greater success rates and more significant public impact than ever before.

The trend of increased organization and specialization among hacktivist groups is not solely focused on political motives. Hacktivist operations, which previously were characterized by an anarchic and loosely coordinated approach, have been influenced by state-run cyber campaigns and have adopted more structured management approaches. This enhanced level of coordination has led to improvements in infrastructure, manpower, tools, and capabilities, which have resulted in more efficient and destructive operations. Initially, this trend emerged in certain conflict zones, but it has quickly spread worldwide, and it is likely to inspire hacktivist groups with a more diverse range of agendas.

Top Attacking Countries

While cybercrime can originate from anywhere in the world, certain countries are known for being hotspots for launching attacks. In 2023, five countries stand out for their aggressive cyber activity. These countries have been identified by cybersecurity experts as being among the most prolific sources of cyberattacks globally. Understanding the sources and motivations behind cyberattacks is crucial for developing effective strategies to prevent and respond to them.



CHINA is widely recognized as one of the top countries in launching cyberattacks, particularly because of its sheer size and sophisticated cyber capabilities. China has invested heavily in developing cyber infrastructure, with a strong focus on gathering intelligence and targeting foreign entities. Thanks to relaxed laws around security, threat actors in China are able to operate with relative impunity.

NORTH KOREA has solid notoriety for aggressive cyber activities, which are now believed to be carried out by a specialized unit within its military. North Korea's cyber capabilities have been attributed to its reliance on cyber operations as a means of achieving its strategic objectives, as well as its relative isolation from the international community, which has made it less susceptible to traditional forms of retaliation.

IRAN has become a big player in the global cyber landscape, with its cyber operations targeting both domestic and foreign entities. Iran's cyber activities are often focused on gathering intelligence and carrying out attacks against its adversaries in the region. They invest heavily in cyber capabilities, and it shows.

RUSSIA has long been known for its advanced cyber capabilities, and remains one of the top countries launching cyberattacks in 2023. Russia's cyber operations are believed to be coordinated by the government and carried out by many, including state-sponsored hackers and criminal groups.

UNITED STATES now ranks among the top countries launching attacks in 2023. Cyber operations in the U.S. are carried out by various groups, from government agencies to military units and private contractors—and are often focused on disrupting or gathering intelligence on foreign adversaries.

Chapter Three: Cybercrime-as-a-Service (CaaS)

Cybercrime caused $6 trillion in damages last year and is projected to result in 33 billion breached accounts in 2023.

The term "Cybercrime-as-a-Service" (CaaS) refers to the outsourcing of cyberattacks to other criminals, who offer their services and expertise on the dark web, as well as the basic internet. In recent years, the prevalence of CaaS has surged due to the increasing demand for cyberattacks by non-technical criminals and a rise in skilled actors willing to sell their services to the highest bidder. This development has made it more accessible and cost-effective for individuals with little technical knowledge to become a threat.

In 2023, the CaaS market is thriving and continues to evolve. The range of services on offer has expanded beyond traditional hacking tools such as malware and phishing kits to include more sophisticated services such as ransomware-as-a-service (RaaS) and distributed denial-of-service (DDoS) attacks. Criminals can now easily rent botnets, hire hackers to create custom malware, and buy stolen data and credentials on the web. The demand for these services is high, with cybercriminals using CaaS to launch attacks on businesses, governments, and individuals worldwide.

Despite the efforts of law enforcement agencies to crack down on CaaS providers, the market continues to grow. The anonymity provided by the dark web and the use of cryptocurrency for payment have made it difficult to track down and prosecute those involved in the trade. In response, some CaaS providers have begun to adopt more sophisticated operational security measures, such as the use of encrypted communication channels and the use of code words to avoid detection.

The rise of CaaS has fundamentally changed the landscape of cybercrime, making it easier for anyone with a motive and a bit of money to launch an attack, and has made it even more difficult for law enforcement to keep up with the ever-evolving tactics of cybercriminals.

SPOTLIGHT ON INTELLIGENT BOTS

The evolution of intelligent bots is having a significant impact on the CaaS world. Bots, which are automated programs that can perform a wide range of tasks, are becoming an increasingly popular tool for cybercriminals to use in their attacks.

One of the ways that bots are affecting CaaS is by making it easier and more efficient for threat actors to carry out attacks. Automated bots are often relied upon to complete a range of tasks, from scanning for vulnerabilities in systems to launching large-scale attacks on targeted networks. This automation can make it easier for cybercriminals to scale their operations and launch attacks more efficiently than ever before.

Another way that bots are affecting CaaS is by enabling new types of attacks that were previously not possible. For example, bots can be used to carry out credential stuffing attacks, where stolen usernames and passwords are tested against multiple websites in order to gain unauthorized access. These attacks can be carried out on a massive scale with the help of bots, potentially leading to widespread data breaches and other security issues.

Despite the challenges that bots pose to security, there are also efforts underway to use bots for good. For example, security researchers are using bots to detect and report vulnerabilities in systems, and some companies are using bots to improve their own cybersecurity defenses. As the use of bots continues to evolve, it will be important to find ways to leverage their capabilities for positive outcomes while mitigating their potential risks.

Cybercrime-as-a-Service (CaaS): Common Tricks & Tactics

At the core of cybersecurity protection lies the ability to identify and prevent malicious behavior and tools before they can wreak havoc. However, threat actors have become increasingly sophisticated and are evolving their attack techniques to counter cybersecurity solutions. Instead of relying on custom malware, they are turning to non-signature tools to exploit built-in operating system capabilities, popular IT management tools, and even off-the-shelf pentesting and Red Team tools. These tools are already installed on target systems, making them less likely to arouse suspicion when detected.

Although this practice is not new, it was once limited to sophisticated actors. Today, it has become a phenomenon known as cybercrime-as-a-service (CaaS), where perpetrators rely on a wide range of tactics to commit their cybercrimes. Some of the more common types of CaaS offerings include:

Ransomware-as-a-Service (RaaS): In 2023, ransomware attacks have become more sophisticated and widespread, with a growing trend towards RaaS that enables anyone to launch an attack, regardless of technical skills or experience. RaaS refers to a business model in which cybercriminals rent out ransomware tools and infrastructure to other cybercriminals, who use them to launch attacks on unsuspecting victims.

- → In 2022, 71% of global businesses felt the impact of ransomware trends.
- → A total of 62.9% of the ransomware victims paid the ransom.

Phishing Kits: They continue to be one of the most common methods used by cybercriminals to steal sensitive information such as login credentials, financial data, and personal information. To make the process of launching a phishing attack more efficient, many cybercriminals are using a pre-packaged set of tools called phishing kits, which include everything necessary to create a convincing phishing email or website, including templates, code, and images.

Distributed Denial-of-Service (DDoS): These attacks are a major threat to individuals and organizations worldwide. They overload servers or networks with traffic, making them unavailable to legitimate users. The frequency and scale of these attacks have increased dramatically in recent years, and they are becoming more sophisticated, making them harder to detect and stop.

- → Overall, there was a 74% YoY increase in the number of DDoS attacks in 2022.
- → In 2022, e-commerce faced 17% of DDoS attacks, with a 53% YoY rise.

Malware-as-a-Service: This type of attack involves the sale or rental of pre-packaged malware that can be used for various cyberattacks, such as ransomware, banking Trojans, or spam campaigns. The buyer can customize the malware with their own branding and choose the target.

Chapter Four: Ransomware

In the world of ransomware, there is a shift happening from encryption to data extortion. Today, threat actors use multiple-extortion tactics to increase the pressure on their victims. They encrypt data on the victims' systems and release decryption keys only after receiving the ransom payment. Companies are aware that if they do not pay, their data may be publicly released, sold, or used to directly extort their employees and customers. Some ransomware affiliates have become more dominant and skilled at identifying sensitive information in victims' networks. As a result, they no longer rely on encryption and instead solely threaten to publish the data to generate ransom payments. This new approach could have serious implications for defense mechanisms, attribution, and future analysis of the ransomware ecosystem.

In the past, ransomware attacks were carried out by individuals who would distribute large numbers of automated payloads to random victims, collecting small amounts of money from each successful attack. However, in 2022, these attacks have evolved into human-operated processes, conducted by multiple entities over several weeks. Attackers now carefully select their victims based on specific criteria and use various tactics to extort significant amounts of money. Threats of exposing sensitive data have proven particularly effective, as victims fear the potential for large fines, lawsuits from employees and customers, and damage to their stock prices and reputation.

The Evolution of Ransomware-as-a-Service (RaaS)

The management of ransomware attacks has evolved in response to the rise of threat actors that use a Ransomware-as-a-Service (RaaS) model through affiliates. Affiliates, who may participate in multiple RaaS programs simultaneously and choose from various encryption tools, have become the "producers" who initiate attacks and pay a portion of the revenue back to the RaaS operator.

To further streamline their operations, affiliates often purchase stolen credentials or network access from access-brokers. This fragmented approach to ransomware attacks makes it difficult to attribute attacks to specific individuals or criminal organizations. Additionally, the tactics, techniques, and procedures (TTPs) used to gain initial access to a system are not necessarily connected to the affiliate or the RaaS payload later deployed, further complicating the tracking of criminal entities.

RaaS providers are competing for the attention of affiliates and usually charge a fee of 10% to 20% of the ransom payment for their services. One of their primary selling points is the speed of the encryption module, which allows attackers to reduce the time it takes to encrypt the data and decrease the likelihood of detection. RaaS providers strive to shorten encryption times by offering various encryption modes from which affiliates can choose or by even providing intermittent encryption, where only certain files are encrypted. Other groups have opted to forego the encryption phase entirely and instead rely solely on threats of data exposure to extract ransom payments.

Opting to rely solely on data publication for extortion is understandably appealing to attackers for several reasons. Firstly, it allows for quick deployment without the need for a lengthy and potentially risky encryption process, reducing the risk of detection. Managing victims also becomes simpler, as there is no need to provide individual decryption keys and operate a complex "customer support" system. Additionally, this approach frees affiliates from their reliance on larger RaaS actors, who often demand a share of the income.

Chapter Five: Mobile Malware

In 2023, mobile malware is on the rise and becoming an increasingly dangerous threat to both individuals and businesses. Mobile malware refers to malicious software that targets mobile devices such as smartphones, tablets, and smartwatches. These types of malware exploit vulnerabilities in mobile operating systems and phone technology. While not as prevalent as malware that attacks traditional workstations, mobile malware is a growing threat to consumer devices. As attacks become more frequent and powerful, the mobile security industry is facing increasing challenges in combating these threats.

As the use of mobile devices continues to rise, so does the number of threats posed by malicious software. Mobile malware is particularly dangerous because it can be spread quickly and stealthily, and it can be used to compromise personal and corporate data, steal money, and even to spy on users.

The number of malicious applications infiltrating Google and Apple stores has significantly increased. These applications are often disguised as seemingly harmless apps such as QR readers, external Bluetooth apps, flashlights, or games to avoid detection. Hiding mobile malware in "unofficial" versions of popular applications has become a new trend. Usually, these are modified versions (known as Mods) distributed through third-party app stores and downloaded by users who prefer unofficial versions for various reasons. While this is not a new threat, 2022 witnessed numerous attacks utilizing well-known, trusted, and widely used applications.

SPOTLIGHT ON MOBILE MALWARE ATTACKS

There have been many notable instances of mobile malware attacks in recent years, but one of the most significant was the Pegasus spyware attack that came to light in July 2021. Pegasus is a sophisticated spyware developed by the Israeli company NSO Group that can infect iPhones and Android devices without the user's knowledge. Once installed, Pegasus can steal a variety of information from the infected device, including contacts, messages, emails, call records, and location data.

The attack was discovered by the cybersecurity research group Citizen Lab, who found evidence that Pegasus had been used to target human rights activists, journalists, politicians, and government officials in several countries around the world. The spyware was installed on victims' devices through a technique called "zero-click" exploitation, which allows attackers to install the malware without any interaction from the user. The attack was particularly notable for its scale, sophistication, and impact on human rights.

The Pegasus attack highlights the growing threat of mobile malware and the need for stronger mobile security measures. It also raises important questions about the role of governments and private companies in developing and deploying advanced cyberweapons, and the need for greater transparency and accountability in the cybersecurity industry.

Facing the State of the Threat with Arkose Labs

In 2023, businesses face an ever-evolving landscape of threats, including DDoS attacks, bots, and other forms of cybercrime. Arkose Labs provides businesses with the tools they need to fight back against these threats, using advanced AI and machine learning technology to detect and block attacks in real-time. By partnering with Arkose Labs, businesses can stay ahead of the curve and keep their systems and data safe from harm in an increasingly dangerous online environment.

The mission of Arkose Labs is to create an online environment where all consumers are protected from online spam and abuse. Recognized by G2 as 2023 Leader in Bot Detection and Mitigation, with the highest score in customer satisfaction and largest market presence four quarters running, Arkose Labs offers the world's first $1M credential stuffing and SMS toll fraud warranties. Its AI-powered platform combines powerful risk assessments with dynamic attack response to undermine the strategy of attack, all the while improving good user throughput. Headquartered in San Mateo, CA with offices in London, Costa Rica, and Brisbane, Australia, Arkose Labs protects enterprises from cybercrime and abuse.

Offices

San Francisco
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

United Kingdom
167-169 Great Portland Street, 5th
Floor, London, W1W 5PF

Schedule Demo