keplersafe™

All-in-one Cybersecurity Solution

2023

GLOBAL THREAT REPORT

HEADLINE

*Kepler Safe revolutionizes the Cyber Security Industry by providing cost-effective services to **all Businesses***

FOREWORD

The latest edition of the Kepler Safe Global Threat Report is particularly relevant in today's world as organizations struggle to manage the challenges brought on by remote and hybrid teams, digital transformation, and an uncertain global economy. The report provides critical insights into the growing threat landscape, where adversaries are becoming more sophisticated, relentless, and damaging in their attacks.

The report highlights the growing nation-state attacks by Russia, China, and Iran, which have increased their cyber espionage campaigns and destructive operations using ransomware. These attacks coincide with the ongoing struggle of organizations to manage the explosive landscape of vulnerabilities, which present an open door to attackers.

The report emphasizes the need to understand the adversary, including their motivations, techniques, and targeting strategies to stop breaches. It provides actionable intelligence to help organizations harden their defenses, stay ahead of the adversary, and improve their business resilience.

One of the significant takeaways from this year's report is the doubling down of adversaries on stolen credentials, with a 112% year-over-year increase in advertisements for access-broker services identified in the criminal underground. The report also highlights the emerging class of eCrime threat actors using fileless attacks to target high-profile organizations with devastating campaigns.

The report underscores the need for identity protection to be a core requirement for risk mitigation as adversariesvvvvv ramp up attacks on multifactor authentication. It also reveals how adversaries have created a new "state of the art" for vulnerability exploitation to sidestep patches and why the industry needs to demand more secure software.

As technology continues to innovate, security must mature and match the innovation of the technology running our organizations. The report shows that security must parallel the slope of technology innovation, and with every innovation achieved, the adversary actively seeks ways to expliot it.

At Kepler Safe, the mission is to stop breaches so that customers can move forward. The focus is on delivering the platform, technology, and intelligence needed to keep customers ahead of the adversary. The company has unified and delivered critical protections like endpoint and extended detection and response (EDR and XDR), identity threat protection, cloud security, vulnerability and risk management, threat intelligence, and much more - all from a single platform.

The report provides critical insights and knowledge of the adversaries, their tactics, and the vulnerabilities they exploit. With this knowledge, organizations can improve their security posture, harden their defenses, and move forward with confidence.

SIGNATURE

TABLE OF CONTENT

INTRODUCTION

Throughout 2022, cyber threats persisted with increased target scope and determination, as nation-state, eCrime, and hacktivist adversaries adapted to shifting geopolitical and economic conditions. Nation-state adversaries engaged in constant computer network operations to support their state goals, with Russian and Chinese adversaries dominating the threat landscape. ECrime adversaries proved their ability to adapt and thrive, with a significant increase in demand for access broker services and the use of social engineering tactics. Hacktivists embraced misinformation and capitalized on major geopolitical shifts to promote specific ideologies.

Despite the persistent efforts of adversaries, Kepler Safe Intelligence outpaced them throughout 2022 with expansive reporting and tracking of new actors, introducing its first Syria-nexus adversary and raising the total number of actors tracked to over 200. Kepler Safe continued to empower customers with new services and features, including Intelligence Recon, and a Vulnerability Intelligence module. The Kepler Safe 2023 Global Threat Report summarizes the analysis performed by the Kepler Safe Intelligence team in 2022 and provides anticipatory threat assessments to help organizations prepare for the coming year.

THREAT LANDSCAPE OVERVIEW

EVERY SECOND COUNTS

Kepler Safe tracks the time it takes for attackers to move from one compromised host to another in the victim's environment, which is known as breakout time. Interactive eCrime intrusion activity showed a decrease in average breakout time from 98 to 84 minutes from 2021 to 2022. In order to reduce the impact of an attack, it's important for defenders to respond within the breakout time. To achieve this, security teams are advised to follow the 1-10-60 rule, which means detecting threats within the first minute, comprehending them within 10 minutes, and responding within 60 minutes. It's crucial to act quickly because every second counts in preventing damages and minimizing costs caused by attackers.

ACCESS BROKER BOOM ACCELERATED IN 2022

In 2022, the market for access brokers, who obtain access to organizations and sell it to other malicious actors, experienced a significant boost in popularity. More than 2,500 advertisements for access were identified, which is a 112% increase from 2021. Some brokers opted for bulk access sales, while others continued to use the one-access-one-auction approach. The tactics employed by brokers to gain access have remained relatively unchanged since 2021, with one particularly popular technique being the misuse of compromised credentials obtained through information stealers or purchased from illegal log shops.

ADVERSARIES CONTINUED TO MOVE BEYOND MALWARE TO GAIN INITIAL ACCESS AND PERSISTENCE

In 2022, attackers continued to move away from using malware as the primary means of gaining initial access and persistence in victim environments. Instead, they relied on malware-free techniques which accounted for 71% of all detections (up from 62% in 2021). One reason for this shift was the widespread exploitation of valid credentials to facilitate unauthorized access. Additionally, the rapid disclosure of new vulnerabilities and the quick exploitation of these vulnerabilities by attackers also contributed to this trend.

INTERACTIVE INTRUSIONS GAINED SPEED AND MOMENTUM

Kepler Safe noted a significant increase in the frequency of interactive intrusion campaigns, which gained momentum throughout 2022, with activity ramping up particularly in the fourth quarter. The technology sector was the most commonly targeted industry vertical, with OverWatch detecting more interactive intrusion activity in this sector than in the top 10 industry verticals combined over the previous year.

2022 THEMES

eCRIME ACTORS GAINED NOTORIETY FOR HIGH-PROFILE ATTACKS

In 2022, eCrime actors gained notoriety for their high-profile attacks, as they constantly search for new ways to increase their revenue and impact. Two newly named adversaries, SLIPPY SPIDER and SCATTERED SPIDER, targeted high-profile victims and affected their employees, customers, and partners. To sustain their operations against multinational and global entities, adversaries need to possess high skill levels and significant resources to evade takedowns, arrests, and potential extradition. SLIPPY SPIDER and SCATTERED SPIDER successfully utilized techniques such as MFA fatigue, vishing, and SIM swapping.

SLIPPY SPIDER

TARGETED TECHNOLOGY GIANTS WITH DATA THEFT AND EXTORTION

Kepler Safe Intelligence observed an increase of 20% in the number of adversaries who conducted data theft and extortion campaigns in 2022 without resorting to ransomware. "Double extortion" has been a common tactic used by big game hunting (BGH) adversaries since 2019. The threat of leaking sensitive information has been as compelling as the disruption caused by ransomware. SLIPPY SPIDER, a newly named adversary, gained notoriety for targeting high-profile technology companies such as Microsoft, Nvidia, Okta, and Samsung in February and March 2022. SLIPPY SPIDER publicly leaked stolen data, including source code, employee credentials, and PII, and made large ransom demands. Despite this, there is no evidence that any of those demands were met. Law enforcement agencies began to focus on SLIPPY SPIDER in mid-2022, and the adversary ceased activity in June of that year.
illegal log shops.

SCATTERED SPIDER

USED SOCIAL ENGINEERING TO OVERCOME MFA

Starting March 2022, SCATTERED SPIDER has been executing social engineering campaigns directed towards companies specializing in customer relationship management and business process outsourcing. Their approach involves creating fraudulent web pages to obtain login credentials for VPNs, Okta, and edge devices. They also employ tactics to trick users into sharing multi-factor authentication codes or overwhelm them with MFA notifications to gain access.

Once inside, SCATTERED SPIDER uses legitimate remote monitoring and management tools, such as PuTTY, to maintain access. They have demonstrated the ability to move laterally across cloud-provider environments and harvest credentials using instance metadata service. To evade detection, they employ various tools to bypass or terminate endpoint security software.

The group targets third-party companies, specifically cellular service providers, for SIM swapping attacks. Their motives are unclear, but the SIM swapping is likely used for follow-on third-party compromise. Additionally, SCATTERED SPIDER steals individual user account data for resale and also targets data relating to cryptocurrency companies. The group has gained notoriety for targeting high-profile victims.

As more businesses move their operations to cloud environments, the rise of cloud-conscious threat actors is anticipated to lead to an increase in cloud exploitation. In 2022, cloud exploitation increased as anticipated, with observed cases growing by 95%, and those involving cloud-conscious actors almost tripling from 2021. These findings indicate that eCrime and nation-state actors are gaining expertise and employing tactics to exploit cloud environments to a greater extent.

TOP CLOUD-CONSCIOUS TTPS OF 2022

In 2022, cloud-conscious threat actors employed a range of tactics, techniques, and procedures (TTPs) to exploit cloud environments. Kepler Safe Intelligence reported that these actors continued to use valid cloud accounts, but also started using public-facing applications to gain initial access. Furthermore, more actors were seen moving towards cloud account discovery for access, as opposed to relying on cloud infrastructure discovery, which was more commonly observed in 2021. In terms of defense evasion tactics, actors were observed shifting away from deactivating antivirus and firewall technologies, and instead focused on modifying authentication processes and attacking identities.

Kepler Safe Intelligence also noted that tactics to gain access to data moved towards exfiltration from information repositories, cloud storage, and local systems. Additionally, threat actors incorporated destructive actions such as account access removal, data destruction, resource deletion, and service stoppage. This trend indicates a growing adoption of knowledge and tradecraft to exploit cloud environments, both by eCrime and nation-state actors.

INITIAL ACCESS

In 2022, attackers who were aware of cloud security mainly gained entry to cloud environments by exploiting public-facing applications such as web servers, using valid accounts or resetting passwords. They also placed webshells or reverse shells on the compromised machine for persistence. Once they had access to a machine, they primarily searched for credentials in files and used the cloud provider's instance metadata services (IMDSs) to gain access. Since cloud workloads are typically short-lived, attackers usually established persistence by using valid cloud accounts that they already had access to or by resetting the password. If they obtained initial access via a web server, they installed webshells or reverse shells for future access.

DISCOVERY

In the initial phase of environment exploration, actors primarily concentrated on cloud accounts for potential persistence and privilege escalation, in addition to identifying reachable network services. They also searched for cloud permission groups, infrastructure, and storage buckets.

LATERAL MOVEMENT

To traverse horizontally within a cloud environment, attackers utilized communication protocols like RDP, SSH, and SMB. Additionally, those with console access leveraged services such as EC2 instance connect and the Systems Manager Session Manager to attain their objective.

PRIVILEGE ESCALATION

The actors elevated their privileges by obtaining access to accounts with higher privileges, which they accomplished either by discovering credentials for these accounts or resetting already existing credentials.

DEFENSE EVASION

To avoid detection, some actors disabled security tools that were running within virtual machines. Others opted to use proxy exits that were in close proximity to their intended victims or gave newly created virtual machines names that were similar to the naming scheme used by their targets.

DATA COLLECTION

Actors sought to gather data by accessing both local systems and internal information repositories, including code repositories, SharePoint, internal tooling, and databases.

IMPACT

Contrary to industry reports that suggested resource hijacking as the prevalent technique, the most widespread method employed by actors to cause an impact in 2022 was actually destructive. The actors resorted to terminating services, removing access to accounts, destroying data, and deleting resources.

Adversaries are widening their scope of attacks to include the cloud as businesses continue to adopt cloud technology. Although their objectives remain similar to those of attacks outside cloud environments, which involve obtaining initial access, persistence, and lateral movement, the dynamic nature of some cloud environments requires a more persistent approach. Kepler Safe Intelligence anticipates that cloud targeting will persist into 2023, based on the observed three-fold increase in such targeting in 2022 and the growing necessity for entities to incorporate the cloud into their daily operations. This assessment is made with a high level of confidence.

SUSPECTED PANDA BECOMING CLOUD-CONSCIOUS

The exploitation of CVE-2022-29464 can result in remote code execution and unrestricted file uploads. Shortly after the disclosure of the vulnerability affecting various WSO2 products, exploit code was publicly released, and adversaries wasted no time taking advantage of the situation. The OverWatch's threat hunters identified numerous exploitation incidents in which adversaries utilized techniques, infrastructure, and tools that were consistent with China-related activity. There is mounting evidence to suggest that adversaries are becoming more comfortable using traditional endpoints to move laterally to cloud infrastructure.

THE 2022 VULNERABILITY INTELLIGENCE LANDSCAPE

In order to accomplish exploitation in 2022, Kepler Safe Intelligence saw attackers recurrently focusing on already proven attack pathways and components. This strategy may be continued in one of two ways by attackers looking to construct an exploit once a vulnerability is found. To attack other goods that are equally susceptible, the attackers can tweak or even reapply the same exploit. As an alternative, the discovery process might spot a possible target and motivate attackers to concentrate on known-vulnerable components while also avoiding patching by investigating other exploit pathways (see Figure 3). This is especially true for edge devices, which are frequently exposed to arbitrary file-delivery vulnerabilities and a variety of injection tactics.

VULNERABILITY DISCOVERY AND REDISCOVERY

The discovery of vulnerabilities across multiple products in 2022 was exemplified by the widespread and prolonged exploitation of Log4Shell. Initially, actors targeted vulnerable products opportunistically. However, with variations of the exploit, targeting other fields and leveraging different protocols, CVE-2021-44228 exploitation was tailored for other products where exploitation was not initially possible. This sustained interest in Log4Shell exploitation was reflected in continued discussions among threat actors in the criminal underground, as observed by Intelligence Recon.

Similarly, the PwnKit exploit targeted the Polkit package on most Linux platforms to manage permissions through privilege escalation vulnerability CVE-2021-4034. Although open-source projects are more likely to be affected by vulnerability exploitation, the integration of vulnerable packages from external sources also contributed to proprietary software exploitation throughout 2022.

CIRCUMVENTION OF EARLIER PATCHES

When a vulnerability is disclosed, especially one that has already been exploited in the wild, it reveals potential avenues for future attacks. In 2022, both zero-day and N-day vulnerabilities demonstrated how threat actors could use specialized knowledge to bypass mitigations implemented through previous patches, allowing them to target the same vulnerable components.

For instance, the ProxyLogon and ProxyShell campaigns in 2021 targeted proxy mechanisms to compromise Microsoft Exchange. In Q4 2022, these mechanisms were targeted again using an authenticated variation known as ProxyNotShell (CVE-2022-41040 and CVE-2022-41082). However, ransomware-affiliated actors were able to bypass ProxyNotShell's mitigations by exploiting an alternative vector that abused CVE-2022-41080 to achieve the same goals.

A similar pattern emerged among a series of zero-day exploits related to the Windows Common Log File System (CLFS) driver observed between March and August 2022. In this case, the developers of the CVE-2022-37969 exploit used a technique to bypass mitigations intended for an earlier CLFS vulnerability (CVE-2022-24521), demonstrating their proficiency in the field.

RUSSIAN CYBER OPERATIONS ARE SUPPORTING THE WAR IN UKRAINE

The year 2022 saw the start of the Russia-Ukraine war, which has witnessed an unprecedented level of cyber capabilities employed throughout the ongoing military conflict. Kepler Safe Intelligence has observed a range of activities linked to Russia in relation to this conflict, including extensive intelligence gathering, information operations aimed at influencing public opinion, and destructive attacks against government and commercial networks. These operations, which occurred alongside a backdrop of patriotic hacktivism aligned with Russian objectives, frequently targeted Western entities that Russian state-linked adversaries currently appear unwilling to pursue.

Although the Kremlin had integrated cyber capabilities into its military campaigns before 2022, often involving distributed denial-of-service (DDoS) attacks, the activities in 2022 demonstrated the breadth of tools that Russia is willing to use to accomplish its objectives, with varying degrees of success. Figure 5 provides an overview of how Russia-nexus operational activity levels evolved during 2022, categorized by intelligence collection, information operations, and destructive motivations.

Throughout 2022, Kepler Safe Intelligence observed multiple instances of Ukrainian entities being targeted in operations associated with Russia state-nexus, Russia-aligned, or presumably Russia-origin adversaries. The operations carried out by the Main Intelligence Directorate (GRU), in line with Russia's military priorities, were responsible for most of the attacks on Ukraine. However, the Federal Security Service (FSB) also played a role in supporting the war effort through intelligence-gathering activities.

In 2022, various adversaries, including FANCY BEAR, EMBER BEAR, VOODOO BEAR, PRIMITIVE BEAR, and GOSSAMER BEAR, along with the RepeatingUmbra and LostPotential activity clusters, targeted Ukraine extensively. Additionally, unattributed campaigns also focused on Ukrainian organizations and individuals, likely for intelligence gathering purposes, using credential phishing techniques to access their targets' email accounts.

Before Russia's invasion of Ukraine, a series of EMBER BEAR operations, including website defacements and the deployment of WhisperGate wiper malware, disrupted and caused damage to Ukrainian targets. These attacks likely intended to undermine the Ukrainian government's ability to function and create a sense of insecurity among Ukrainian citizens about their protection from the upcoming military campaign.

Psychological operations escalated in February 2022, with several DDoS attacks on Ukrainian government portals and financial institutions aimed at disrupting routine activities such as accessing banking services, likely in an attempt to pressure Ukrainian citizens. Western government sources later attributed some of these attacks to the GRU.

EMBER BEAR

THE PUBLIC FACE OF DESTRUCTIVE OPERATIONS IN UKRAINE

Several covert operations conducted by Russia against Ukrainian networks since the invasion have aimed to prevent Ukrainian citizens from accessing specific resources, such as energy supply or government databases, without attracting public attention. On the other hand, EMBER BEAR's destructive operations between January and February 2022 were carried out publicly, with government websites being defaced to announce data destruction and public information leaks. The attackers used the guise of hacktivism to mislead attribution. This new approach to destructive operations suggests that EMBER BEAR may use it in specific situations where psychological impact is crucial.

In February 2022, Russian-aligned adversaries launched multiple attacks on Ukrainian network infrastructure, deploying new wiper malware families and continuing website defacements. The use of AcidRain, deployed soon after Russian President Vladimir Putin's announcement of a "special military operation," disrupted Viasat satellite communications network segments, affecting at least three internet service providers across Europe and wind turbine network communications in Germany.

Despite a reduction in tooling variety and capability, VOODOO BEAR activity remained high, including CaddyWiper deployments and attacks against the Ukrainian energy sector using a new CrashOverride variant and scripts designed to wipe Linux and Solaris systems. This suggests the complexity of effectively leveraging cyber operations compared to well-established kinetic military doctrine.

From February 2022, Russia-nexus adversaries launched multiple attacks on Ukrainian network infrastructure, deploying destructive malware families and carrying out website defacements. The attacks intensified with the onset of Russia's military invasion on February 24, 2022. The use of AcidRain was significant, as it was designed to disrupt Viasat satellite communications network segments that connected Ukraine.

While the true impact of these early attacks remains unclear, at least three internet service providers across Europe were affected, resulting in outages for thousands of customers and the disruption of wind turbine network communications in parts of Germany. Russia's offensive cyber operations continued at a highly elevated pace, but with a reduction in capability and tooling variety after the first week of the war. However, VOODOO BEAR's activities stood out, which included spear-phishing and credential-phishing operations against Ukrainian targets.

During the second half of 2022, Russia's cyber activities shifted to intelligence-collection operations, indicating increasing Russian military and Kremlin requirements for situational awareness as their advances into Ukraine stalled and reversed. However, Russia returned to using fake ransomware in October and November 2022, suggesting its intent to widen its targeting to include sectors and regions in which destructive operations are considered politically risky.

Overall, Russia's cyber operations within the context of the 2022 Ukraine invasion have demonstrated inherent wartime limitations, particularly in the case of destructive attacks. Ukraine's improved defensive capabilities and significant assistance from the international community have potentially influenced the course of Russian military strategy in this conflict. While attacks against core sectors have not been as extensive as predicted, future targeting of currently unaffected sectors is possible as the war progresses and potentially changes course.

CHINA-NEXUS ADVERSARIES SIGNIFICANTLY INCREASED 2022 OPERATIONAL SCALE

According to Kepler Safe Intelligence, China-linked threat groups were the most active in targeted intrusions in 2022. These groups, as well as those using similar tactics, were observed targeting almost all 39 industry sectors and 20 geographic regions tracked by Kepler Safe Intelligence. These attacks were likely aimed at gathering strategic intelligence, stealing intellectual property, and enhancing surveillance of targeted groups, which align with the intelligence goals of the Chinese Communist Party.

Throughout 2022, China-linked threat groups primarily targeted organizations in the government, technology, and telecommunications sectors based in East Asia, Southeast Asia, Central Asia, and South Asia. Around two-thirds of the China-linked targeted intrusion activity confirmed by Kepler Safe Intelligence in 2022 occurred in these regions. European and North American organizations were targeted in approximately one-fourth of the activity, while Africa, South America, and Oceania were targeted in the rest.

It is highly likely that government-sector targeting in countries neighboring China represents a continuous intelligence collection mission for China-linked threat groups. Telecommunications and technology entities in these regions are also high-priority targets, albeit for different reasons. Technology entities are the targets of ongoing economic espionage campaigns that seek to steal research and development data, proprietary information, and trade secrets. Telecommunications entities provide adversaries with direct access to foreign telecommunications infrastructure, which can be used to amplify intelligence collection or surveillance efforts.

TARGET REGION – TAIWAN

During 2022, Kepler Safe Intelligence observed that China-nexus adversaries heavily targeted technology organizations based in Taiwan. Despite the inflammatory rhetoric and military drills by China in response to a high-level state visit by U.S. Speaker of the House Nancy Pelosi, there was no significant increase in China-nexus targeting of Taiwan observed by Kepler Safe Intelligence. However, there was a noticeable rise in nationalist hacktivist activity affiliated with China targeting Taiwanese organizations with DDoS attacks and web defacements during this period.

Throughout 2022, Kepler Safe Intelligence observed that China-nexus adversaries continued to exploit web-facing services to gain initial access to targeted organizations. This included the use of both zero-day exploits and publicly released exploits. Zero-day exploits were most commonly used to target North American organizations in the aerospace, legal, and academic sectors. Additionally, zero-day exploits were delivered using weaponized Microsoft Office documents to likely target the Philippines defense sector, Nepalese telecommunications sector, and Russian government sectors, as well as groups associated with Tibetan independence movements.

Enterprise software remained a high-priority target for China-nexus adversaries, who identified and exploited zero-day vulnerabilities in products such as CITRIX ADC and Citrix Gateway, Microsoft Exchange Server, Microsoft Support Diagnostic Tool, and Atlassian Confluence Server and Confluence Data Center. Furthermore, Kepler Safe Intelligence observed multiple instances of suspected but unconfirmed China-nexus adversary exploitation of vulnerabilities on web-facing services throughout 2022.

KEPLER SAFE ECRIME INDEX

The eCrime Index (ECX) by Kepler Safe® monitors various aspects of eCrime, such as botnet and spam activity, and calculates the total number of ransomware victims observed. The overall trends in 2022 were similar to those of 2021, with a peak in March and April. The increase in activity was likely due to the invasion of Ukraine by Russia, which led to increased eCrime activity by SALTY SPIDER, SCULLY SPIDER, and other actors who used the invasion as a theme for social engineering lures. Access broker activity also increased, with PrivateLoader by HERMIT SPIDER distributing over 900 unique payloads in March 2022.

Another peak was observed in September 2022, which could be attributed to an increase in corporate access advertisements and BGH victims published on dedicated leak sites. However, the overall ECX value in 2022 was lower than in 2021 due to WIZARD SPIDER closing their Conti RaaS after damaging leaks and HERMIT SPIDER ceasing their PrivateLoader operations, which affected ECX factors such as BGH victims and malware distribution.

Despite these setbacks, Kepler Safe Intelligence believes that ECX values will likely return to 2021 levels or higher in 2023 as new enabling adversaries such as COMPASS SPIDER, LILY SPIDER, BRAIN SPIDER, and Black Basta continue to emerge. Established adversaries such as BITWISE SPIDER, ALPHA SPIDER, and MALLARD SPIDER also continue to make significant malware maintenance efforts. Moreover, the core members of WIZARD SPIDER remain active and may return in some capacity. Finally, adversaries are adjusting their TTPs, with BGH operations increasing data extortion intrusions without using ransomware, which may affect the ECX in 2023.

CONCLUSION

In 2022, adversaries in the targeted intrusion, eCrime, and hacktivist landscapes demonstrated relentless determination in achieving their goals. They continued to employ novel techniques to bypass security measures, hinder research analysis, and refine their tactics.

Kepler Safe Intelligence predicts that eCrime adversaries will maintain their high activity levels in 2023, with BGH remaining the dominant threat and shifting towards the use of RaaS networks. These adversaries are also likely to pursue data theft and extortion without using ransomware, and access brokers may become dedicated brokers to RaaS partnerships.

As organizations implement countermeasures against eCrime operators, adversaries are expected to use new tactics like increased social engineering and direct engagement with victims. The threat to the cryptocurrency market will continue to be a concern, with operational tempo fluctuating with cryptocurrency values. Additionally, formjacking will remain a credible threat for eCrime actors to steal and exploit victim PII.

Big game hunting is predicted to remain the primary eCrime threat to organizations in most geographic regions and industry sectors in 2023.

While Russia's invasion of Ukraine provided a window into cyber operations during wartime, most targeted intrusion activity in 2022 was driven by traditional espionage motives. Cyber activity remains most effective in roles associated with intelligence operations, such as deniable disruption, information operations, and currency generation. Kepler Safe Intelligence expects targeted intrusion adversaries to predominantly pose data theft threats in 2023. However, state-nexus adversaries from Russia and Iran may present disruptive or destructive threats in connection to geopolitical developments, while North Korean adversaries may pose a threat to currency theft. China-nexus targeted intrusion activity is not expected to decrease in 2023, as cyber espionage remains critical in supporting the CCP's strategic and economic ambitions.

Kepler Safe Intelligence has observed that in 2022, adversaries across different threat landscapes such as targeted intrusion, eCrime, and hacktivism have been relentless in their pursuit of bypassing security measures and refining their techniques. In 2023, eCrime adversaries are expected to continue operating at a high rate, with BGH remaining the dominant threat and shifting to the use of RaaS networks.

In terms of targeted intrusion activity, data theft threats will likely remain predominant for most sectors and geographies, with Russian and Iranian state-nexus adversaries presenting outsized threats of disruptive or destructive activity in connection to geopolitical developments. Hacktivism is expected to continue supporting political ideals, particularly in countries experiencing civil unrest or war, while vulnerability threats and mobile-based social engineering techniques in intrusion attempts will remain relevant in 2023.

To address these threats, Kepler Safe Intelligence offers industry-leading adversary tracking, malware analysis, geopolitical trend analysis, and real-time campaign trend analysis through its suite of reporting products, covering different threat landscapes. This will help customers stay informed and stay ahead of the adversary in 2023.

RECOMMENDATIONS

GAIN VISIBILITY INTO YOUR SECURITY GAPS

To ensure complete security, it's essential to protect all assets, and for that, it's necessary to have visibility into them. Cyber attackers are continually targeting vulnerabilities, and hence, organizations should prioritize enforcing IT hygiene and visibility across their entire asset inventory. With the Kepler Safe platform, you can get comprehensive visibility and protection for your assets, including endpoints, identities, cloud, and data. By cataloging your assets and understanding their risk level, you can ensure their protection. With the increasing adoption of cloud technology, enterprises have expanded their digital footprint, which has led to a surge of unknown exposed assets and increased attack surface. External Attack Surface Monitoring (EASM) solutions can provide an outside-in view of the enterprise, allowing organizations to identify areas of exposure and close security gaps.

PRIORITIZE IDENTITY PROTECTION

As attackers increasingly rely on tactics such as social engineering to obtain access and credentials, traditional endpoint-only solutions are no longer sufficient. To protect against these threats, it is important to prioritize identity protection and implement integrated solutions that correlate endpoints, identities, and data. This should include conditional risk-based access policies to reduce the burden of MFA for legitimate users, while also identifying unexpected or unusual network behavior. CISA's Shields Up initiative highlights the importance of enforcing MFA and quickly assessing any suspicious activity. Look for solutions that not only extend MFA to legacy and unmanaged systems, but also offer real-time detection and prevention of lateral movement, misuse of service accounts, and other suspicious behavior.

Prioritize cloud protection

Protection of cloud infrastructure should be a top priority as adversaries are constantly targeting it. In 2022, there was a 95% increase in observed cases of cloud exploitation, with attackers utilizing various tactics, such as credential theft and misconfigurations, to compromise vital business data and applications. To prevent such breaches, it's crucial to have agentless capabilities that safeguard against control plane and identity-based attacks and misconfigurations, along with runtime security to shield cloud workloads.

Know your adversary

When it comes to cyberattacks, it's important to understand the adversary you're up against. Without this knowledge, organizations may find themselves unprepared and spending significant resources on ineffective measures. Many organizations struggle to identify the "who, why and how" behind attacks, leaving them vulnerable to persistent threats. To address this, it's important to invest in threat intelligence that goes beyond just providing indicators of compromise. This intelligence should also identify the individuals behind the attacks, their motivations, capabilities, and tools. Armed with this information, security teams can prioritize their defenses and take action to protect their assets. The Kepler Safe Adversary Universe is a valuable resource that provides insights into the threat landscape and can help organizations identify which adversaries are most likely to target them.

Practice makes perfect

Although technology is vital in detecting and preventing intrusions, security teams play a vital role in thwarting breaches. Regularly conducting tabletop exercises and red/blue teaming can help security teams identify vulnerabilities and weaknesses in their cybersecurity practices and response, making practice an essential component of their success. Additionally, user-awareness programs should be implemented to combat the ongoing threat of phishing and other social engineering tactics.

KEPLER SAFE PRODUCT AND SERVICES

KEPLER SAFE OFFERS YOU ALL IN ONE CYBER SECURITY SERVICES

Kepler Safe provides a comprehensive suite of products and services that offer all-in-one protection for your organization's digital assets. With the ever-increasing number of cyber threats targeting businesses of all sizes, it's critical to have a robust and reliable security solution in place.

Our products and services are designed to address the full range of cyber threats, from traditional malware and ransomware to sophisticated nation-state attacks. We provide advanced threat detection and response capabilities, backed by our team of highly skilled security experts who are available 24/7 to provide rapid incident response and remediation.

In addition to our threat detection and response capabilities, we also offer comprehensive identity and access management solutions to help organizations manage user access and permissions across their entire network. This includes multi-factor authentication, conditional access policies, and real-time monitoring of user activity.

At Kepler Safe, we understand that no two businesses are alike, which is why we offer customized solutions tailored to meet the unique needs of each organization we work with. Our team works closely with our clients to understand their specific security requirements and develop a tailored solution that provides maximum protection while minimizing disruption to business operations.

Whether you're a small business looking to improve your cybersecurity posture or a large enterprise with complex security requirements, Kepler Safe has the products and services you need to stay protected from cyber threats. Contact us today to learn more about how we can help you keep your business safe.

keplersafe™

All-in-one Cybersecurity Solution

Secure your digital world with our all-in-one cyber security seirvices!

Book a Demo Session now!

Don't wait until it's too late. Book our demo cyber-security session and see how Kepler Safe can satisfy your cybersecurity needs.

+1 (855) 653-7537 info@keplersafe.com www.Keplersafe.com