BDO THREAT INTEL:

INSIGHTS FROM 2022, AND PREDICTIONS FOR 2023

BDO CONSULTING | Technology & Cyber

BDO THREAT INTEL:

INSIGHTS FROM 2022, AND PREDICTIONS FOR 2023

2022 was almost a year of the same. Ransomware continued to dominate the cyber threat landscape, Supply Chain attacks were still a recurring problem, and other cybercrimes-as-a-service schemes hit organizations around the world. But this was the year of state-sponsored Advanced Persistent Threats (APT), as Russia's invasion of Ukraine gave us remarkably interesting developments that will forever be embedded in the history of cyber warfare and information security. As the BDO Managed Threat Intel team has been busy tracking all of this, here are what we feel are five key trends, developments, and even some predictions.

5 KEY TRENDS

01/05

WE SAW A LOT OF DESTRUCTIVE WIPERS

Wipers and destructive malware are designed by nation-states with considerable sophistication and resources to cause irreversible damage and are largely used for cyberwarfare operations. Since Stuxnet was most famously used in 2010 against the Iranian nuclear project, they have not been commonly observed. However, this year, we saw at least 9, destroying the data of over Ukrainian 100 organizations, ranging from financial services, energy, IT, and aviation sectors.

This unprecedented amount of multiple new wiper families represents a significant uptick in destructive malware activity that was used to destroy thousands of machines, starting with WhisperGate and HermeticWiper at the start of the Russian-Ukrainian. While Wiper attacks were initially exclusive to Ukraine and suggest that they were deployed by Russian APTs, an increase in the use of destructive malwares has been observed in other regions by other groups, including an attack on Albania carried out by Iran.

5 KEY TRENDS

02/05

IABS CREATED A STRONG MARKET FOR RANSOMWARE BUYERS

2022 was a good year for the Initial Access Broker (IAB) market which relied on infostealing malware types mainly deployed through botnets, phishing, obfuscated malware loader/dropper, or the purchase of compromised credentials. Moreover, we observed that the most common method used by ransomware attackers to gain remote access to compromised networks was by purchasing valid accounts harvested by these various infostealer malwares and sold on darkweb and special-access sources.
In this context, IABs have significantly reduced the time and resources ransomware operators would typically need to invest for reconnaissance phases in the attack lifecycle.

While most high-profile IABs operated on top-tier Russian-language forums, including Exploit and XSS, high-access brokers were also found on lower-tier English forums, such as BreachForums. While not as common, some ransomware operators have been observed to directly work with designated IABs off forums, using private ToX and other messaging channels.

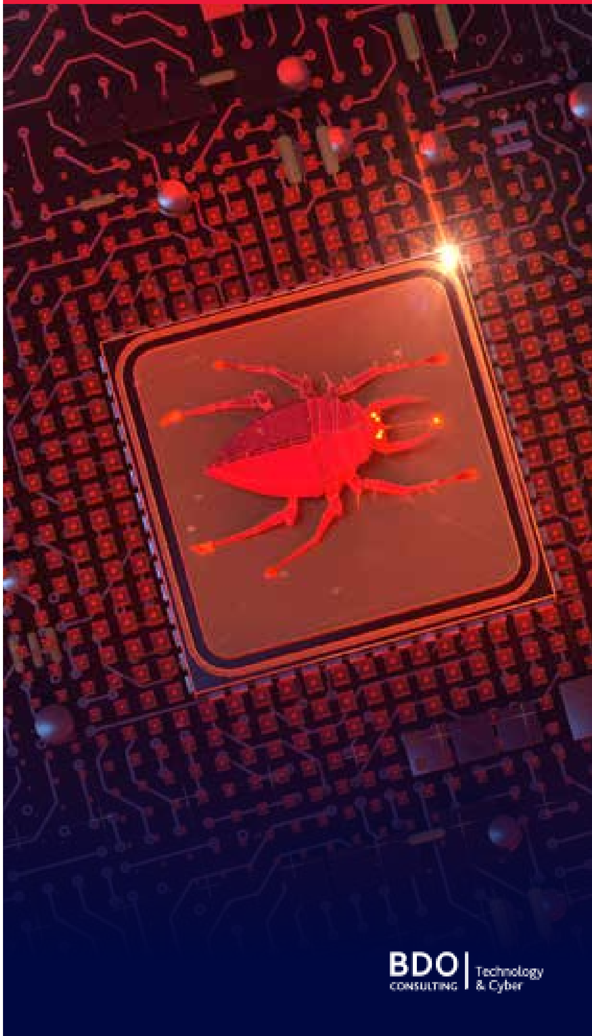
5 KEY TRENDS

03/05

RANSOMWARE PREFERRED EXTORTION OVER ENCRYPTION

This year saw many high-profile ransomware groups opting to skip encryption altogether and go straight to extorting victims by threatening to release their data after managing to exfiltrate company data. Prominent groups such as BlackCat and Lockbit have even taken advantage of this trend by creating searchable data features on their blog site. The shift from encryption to extortion is likely due to several reasons.

For one, RaaS operators began to develop intermittent encryption, which allows for at least partial file encryption, probably because RaaS developers are competing for affiliates by selling faster encryption methods that limit the probability of detection. Moreover, the successes of the Lapsus$ and Karakurt group extortion tactics showed that complex operations involving encryption are not necessary. Additionally, the recent trend of targeting poorly defended healthcare organizations has led many RaaS actors to recommend that their affiliates not encrypt critical areas that can harm patients, as with the case of healthcare hunting Hive ransomware, which was observed to have made efforts to not disable critical healthcare systems.



04/05

MOST CYBERATTACKS WERE TRACED BACK TO COMMON MISCONFIGURATIONS

Most cyberattacks shared common exploits of not only poor credential hygiene, but misconfigurations that allowed entry and privilege escalation points in an organizational environment. A configuration error occurs when the security settings are not properly configured to deal with evolving threats, and most vulnerabilities are introduced due to misconfiguration.

Capable and experienced attackers have good knowledge of common network configurations and use it to their advantage to identify misconfigurations. In August, Microsoft released a report claiming that more than 80% of ransomware attacks were tracked back to common configuration errors in software and devices. This concern was voiced by IBM which also confirmed that cloud misconfigurations have also increased by 28% since last year, with a 200% increase in cloud accounts offered on the dark web in the same timeframe.

05/05

DDOS ATTACKS SURGED IN SCALE AND SCOPE

While not nearly as destructive as wipers, 2022 saw a significant increase in distributed denial-of-service (DDoS) attacks, most of which were carried out by pro-Russian hacktivists. At the beginning of the year, most DDoS instances were primarily focused on various Ukrainian critical infrastructure targets. However, later in the year, DDoS attacks began spilling over into other countries following their announced support for Ukraine and intentions to sanction Russian assets, as well as businesses pressured to pull out of Russian markets.

Despite DDoS attacks decreasing somewhat toward the end of the year, and the fact that it has relatively limited impact in the form of short outages lasting for minutes and hours, some attacks were observed to be more innovative and lasted for days.

5 SIGNIFICANT DEVELOPMENTS

01/05

RUSSIAN ATTACKS ON UKRAINIAN GIVES PRECEDENCE TO FULL-SCALE CYBER CAPABILITIES THAT SPILL OVER INTO EUROPE, HIGHLIGHTING CRITICAL INFRASTRUCTURE WEAKNESSES

Since the beginning of Russia's war on Ukraine, Russia's cyberwarfare capabilities have shown us how vulnerable communications SATCOM networks and Global Navigation Satellite Systems (GNSS) are, both of which spilled over into European neighbors with the attack on Viasat. The war also brought forth the resurgence of DDoS attacks, which while a relatively older method, have since grown in type and scale, with 2022 reporting record-sized DDoS attacks. The worst of all was the threat of wipers, which, unlike ransomware, gives us a looming threat where organizations will not be able to recover their data.

While Russia's intent on using the cyber capability to meet its interests hardly comes as a surprise, the sheer type and scale of its cyber means has never been seen before and gives precedent to other "Big Four" nations like China, Iran, and North Korea when forming strategies in future wars. Moreover, it will likely inspire cybercriminal groups who often refer to the technical prowess of APT groups for inspiration for their profit-generating operations. This is especially considerable given the alleged connection between many so-called "hacktivist" groups (more likely "faketivists") supporting Russia, who engaged in operations supporting the Russian war effort and have alleged ties to the most high-profile ransomware players.

5 SIGNIFICANT DEVELOPMENTS

02/05

CONTI SHUTS DOWN COSTA RICA, RANSOMWARE CAUSES A COUNTRY TO DECLARE A STATE OF "NATIONAL EMERGENCY" FOR THE FIRST TIME

Conti leaks did not just give us unprecedented insight into one of the most highly capable ransomware operations, they also showed us how dynamic and resilient they can be. Only a few weeks after the so-called internal feud that would see the end of the group, it disrupted the banking operations and Finance Ministry of Costa Rica and managed to also cripple its import and export industry.

While this was not the first-time ransomware targeted a government, it was the first time it did so to such an extent that it declared a national crisis, an unprecedented event. In May the country also suffered a similar attack on its Social Security Fund at the hands of the Hive ransomware, whose authorship is also associated with the Russian-speaking ransomware group.

5 SIGNIFICANT DEVELOPMENTS

03/05

LAPSUS$ SUPPLY CHAIN ATTACK, BREACH OF MULTIPLE GIANTS SHOWS RANSOMWARE IS NOT THE ONLY THREAT

In February of 2022, Lapsus$, a group known of loosely based hackers that included teenagers, began a string of attacks on high-profile targets including the world's largest semiconductor manufacturer Nvidia, Ubisoft, Samsung, T-Mobile, EA Games, Microsoft, and identify and access management (IAM) vendor Okta in a Supply Chain Attack. Interestingly, Lapsus$ gained access to Okta's network via a third-party supplier, Sitel, before accessing Okta's customer information. At the time, Okta had more than 15 thousand customers, with at least 375 customers being affected by the attack.

While being mislabeled as a ransomware group, their operating model is extortion where access is most often gained through phishing before exfiltrating sensitive data, without encrypting data. The Lapsus$ attacks were highly notable given their list of victims, lack of financial motivation, and apt use of social media to gain attention, even running polls to vote on whose data they should publish next. However, the most notable part is when British police apprehended two teenagers aged 16 and 17 years old as part of seven people arrested. This shows that even amateurs can compromise multiple organizations, and how many of them, including industry giants, are susceptible to overlooked risks in the supply chain.

04/05

MICROSOFT MISCONFIGURATION LED TO DATA LEAKS FOR MORE THAN 65,000 ORGANIZATIONS

In November 2022 Microsoft confirmed that it inadvertently exposed the information of thousands of customers following a misconfiguration that left an endpoint publicly accessible over the internet without any authentication controls. Unauthenticated access to data included business transaction data between Microsoft and prospective customers, including the planning or potential implementation of several Microsoft services. While they did not reveal the scale of the data leak, according to security researchers, the misconfiguration affected more than 65,000 entities in 111 countries and exposed over 2.4 terabytes of data which consists of invoices, product orders, signed customer documents, partner ecosystem details, etc.

05/05

ATTACK ON MARQUARD & BALHS SHUTS DOWN FUEL IN GERMANY, SHOWS ENERGY IS VULNERABLE

The war in Ukraine has also correlated with a significant uptick in attacks on various European energy providers following sanctions that came in response to the invasion. In February 2022, German energy giant Marquard & Balhs was attacked and saw more than 200 gas stations across Germany closed after its IT infrastructure was destabilized. The attack was attributed to the Russian-linked BlackHat gang, which has previously targeted energy pipelines and resembled the Colonial Pipeline attacks in the United States in 2021. This attack was just one against many German energy firms which lasted throughout the year, with the country's cyber agency the BSI warning that the threat situation is 'higher than ever' in its annual report released in October.

More concerning, the attack reflects an increase in attacks on global multiple energy providers in 2022, including Luxembourg's Encevo, Italian energy giant ENI and its national energy agency GSR, Indian power company TATA, and oil refining hub of Amsterdam-Rotterdam-Antwerp (ARA), which disrupted the movement of refined cargo throughout the region.

The impact of this attack was also felt throughout the global supply chain, as the energy sector is a critical element of the global supply chain which is essential to the constant operation of various critical industries, including Transport and Logistics, Chemicals, Food and Beverage, etc.

5 SIGNIFICANT DEVELOPMENTS

5 PREDICTIONS FOR 2023

01/05

APTS WILL DICTATE THE GEOPOLITICAL CYBER THREAT LANDSCAPE

The Russian invasion of Ukraine has caused significant disruption and disinformation in the rest of the Western world, as the unprecedented circumstance of a major cyber power has, together with its hacktivist fronts, significantly increased disruptive attacks, and cyber espionage. Russia's continued resolve is likely to lead to the proliferation of data destruction wipers and the use of all cyber means, such as reinvented DDoS attacks, outside of Ukraine and its neighbors.

Moreover, this precedence will likely inspire other APTs from other pariah states facing sanctions, such as Iran, which seek to grow cyber capabilities that offset limitations to kinetic operations. In this context, the distinction between the motivations of nation-states, cybercriminals, and hacktivists, will be increasingly difficult to distinguish. State-linked groups will continue to diversify their capabilities to improve current TTPs to reinforce targeted attacks, with state "faketivist" groups likely to use ransomware in 2023.

As Russia's activity has also increased concerns of European energy suppliers to deter countries involved from sanctions and reduce their reliance on Russian energy, this will continue to make the energy sector a prime target for APT groups of nations in conflict who seek to retaliate with ostensibly anonymous deterrent measures. As European energy suppliers start to rethink energy policy, energy extortion based on dependency on Russian energy poses a complex issue in the face of the changing geopolitical, economic, social, and cyber threat landscape. Moreover, such attacks may reveal vectors for cybercriminals who seek opportunities to similarly compromise highly profitable targets.

02/05

SECURING CRITICAL INFRASTRUCTURE WILL REMAIN A KEY ISSUE

The energy crisis in Europe highlights a key weakness in global cybersecurity in the last two years, critical infrastructure. While, Critical infrastructure is already at risk of destructive cyber-attacks when nations are in conflict, not just the energy supply crisis, but the supply chain crises which worsened in 2022. Both APT and ransomware campaigns will focus on disrupting not just the energy and power supply, but food supply, transport industries, and critical manufacturing. This will also likely be extended to the production of essential manufacturing components such as semiconductors, which has seen a considerable uptick in attacks in 2022 and is likely to see a similar rise in the next year.

5 PREDICTIONS FOR 2023

That said, hackers of all motivations are also likely to exploit the growing list of outdated ICS and OT vulnerabilities that were never designed with security in mind. Already in the first month of 2023, an Anonymous-affiliated hacker group shared on Twitter that it conducted a "first-ever" ransomware attack against an RTU (remote terminal unit), a device that is typically deployed across industrial control system (ICS) environments. More importantly, the motivation for developing the RTU attack was political, in this case in support of Ukraine. However, as with all other attacker developments, TTPs of politically motivated actors, state, or hacktivist, will no doubt be adopted by financially motivated threat actors. This is troubling given the state of OT/ICS security of many manufacturers, most of which play critical roles in various supply chains.

5 PREDICTIONS FOR 2023

03/05

RANSOMWARE WILL REMAIN THE SINGLE GREATEST CYBER THREAT, BUT WITH MORE EXTORTION

Ransomware operators continue to evolve their activities and capabilities, and besides nation-state APTs, remain not just the cutting edge in cybercrime, but the main drivers of the cybercrime-as-a-service market. For example, 2022 saw more malcode being re-written in more obscure languages and targeting more OS environments.

Beyond the encrypting capabilities, ransomware groups will continue to focus on other opportunities to diversify their profit-generating operations, mainly by managing leak sites or blogs, where threat actors post details of their victims. Ransomware groups' reliance on valid accounts will also lead to the further development of IABs in the coming year, with harvesting and sale of credentials likely to increase. While ransomware began as a method of encrypting and later moved to also leaking victims' data if they refused to pay (the double extortion method) 2023 will likely see more data leak-based schemes. The most active group, LockBit 3.0 for example, offered visitors and victims the chance to destroy or purchase stolen data, or even extend the timer counting down to publication. LockBit in general will likely remain the dominant ransomware variant in the next 12 months. Auctioning of data, releases based on subscriptions, and schemes where news of the breach itself will not be made public if victims pay to protect falling stock prices, for example, may make many organizations complicit in breaking data breach laws.

04/05

MISCONFIGURATIONS AND CLOUD-NATIVE THREATS ARE EXPECTED TO INCREASE SUBSTANTIALLY

The rise in misconfigurations will see threat actors who know how to take notice, especially aspiring cybercriminals, using similar exploit methods. As more and more organizations move to the cloud, misconfigurations, especially cloud-native threats are expected to rise in the coming years, meaning more cloud migration programs will likely need to implement stronger configuration management strategies. Regardless, cloud-native threats will likely become not only the target of the incident but the source of the threat in the form of poor configuration of access management.

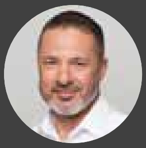
05/05

SUPPLY CHAIN ATTACK WILL CONTINUE TO GROW

Supply Chain attacks will continue to accelerate in 2023 as most companies do not implement effective risk management and security controls that gives visibility to risks emanating from third party components. This is especially concerning given many organizations manage projects in external repositories, and often lack visibility and control within their supply chains, much less understanding where there are security gaps.

As Supply Chain attacks are designed to exploit trust relationships between an organization and external parties, mainly third-party software vendors. This may lead to further investments in Third Party Risk Management (TPRM) threat intelligence and attack surface management programs. Regardless, threat actors will likely continue designing campaigns compromising single organizations to gain access to multiple organizations' environments.

FOR MORE
INFORMATION:



NOAM HENDRUKER

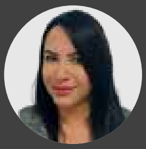
Partner
Head of Cyber Consulting Group
BDO Cybersecurity Center

Tel: +972 50-675-7703
noamh@bdo.co.il

YEHOUD MARCIANO

Senior Manager
Head of Offensive Cyber Security Advisory
BDO Cybersecurity Center

Tel: +972 52-471-6089
yehoudm@bdo.co.il



OSHRIT ATIAS

Sales Manager
BDO Cybersecurity Center

Tel: +972 52-581-4484
oshrita@bdo.co.il

BDO CONSULTING | Technology & Cyber