moderndiplomacy.eu

How the CIA Created the EU - Modern Diplomacy

Published 1 year ago on November 13, 2020

14-18 minutes

In 2021 cyberthreat actors around the world increased the pressure on security issues, and it is no exaggeration to say that 2022 could be the most challenging year ever. With a view to helping security teams better face challenges, security vendor ZeroFox has recently released the 2022 Threat Intelligence Forecast report, which provides predictive analysis of the increasing threats in cyberspace.

Ransomware – a type of malware that restricts access to the device it infects, requiring a ransom to be paid to remove the restriction – will continue to accelerate in 2022. Organisations in the financial, manufacturing, retail and healthcare sectors will continue to face increased risks. Ransomware developers can focus on persistent and sustainable campaigns, including targeting threats to known individuals.

The year 2022 will see a wave of “data kidnapping” attacks (extortion due to the lack of encryption of the victim’s data). “Data kidnapping” means that in the big data era, while people proactively or passively enjoy the benefits and advantages brought by big data, they have to endure the digitisation of every aspect of their lives and the impact on their social lives will entail severe negative effects.

Attacks on the third-party intelligence chains will keep on increasing in frequency, scale and sophistication. In 2022 threat actors are likely to target small third-party vendors and critical events in large supply chains.

Competition among developers of infostealer software – i.e. malware that seeks to steal information – is expected to intensify in 2022, which is likely to spur innovation among developers to create “better”, more complex products and easier-to-use services.

Demand for Initial Access Broker (IAB) services – individuals or groups who band together to gain access to a corporate network or system through means that may include credential theft; aggressive attacks and exploitation of 0-day vulnerabilities (any vulnerability in a piece of software not known to its developers or known to them but not managed); or known but unpatched vulnerabilities – will continue to grow in 2022. Given the low risk of being discovered and the high demand for initial access, an increasing number of IABs or individual actors are trying to sell access to sensitive data to third parties.

Cybercriminals are expected to continue to use automation to foster growth in their sales and licensing of sophisticated phishing-as-a-service suites – an inclusive form of cybercrime that potentially opens the door to everyone – and more cybercriminals will switch from Bitcoin to Monero as their cryptocurrency of choice in the coming year.

It is very likely that ransomware will continue to accelerate in 2022. Without significant changes to security measures to prevent intrusions and possible legal provisions, including international ones, to prevent threat actors from operating in judicial “immunity zones”, it is easy for the ransomware industry to keep on thriving, heading towards organisations of all sizes and across all sectors. Among these, the ransomware threat will severely challenge the financial, manufacturing, retail and healthcare sectors.

Although threat actors will probably continue to focus on SME targets in early 2022, we expect the “big hunt” to reappear in the months ahead. This may take the form of campaigns targeting Managed Security Service Providers and other third-party services as they provide privileged access to multiple customer systems, thus enabling threat actors to infect numerous downstream organisations with a single intrusion.

On the other hand, law enforcement agencies’ crackdowns are unlikely to have a lasting impact on ransomware campaigns. Since the groups targeted by such crackdowns can suspend operations or rename themselves and reopen, and the cycle goes on forever, as there will be new targets (“protected” software) to hit. The threat actors behind the most popular ransomware families of 2021 – DarkSide, Conti, REvil, LockBit and BlackMatter – could come back in 2022 with new identities and improved robbery software.

Considering the trends that emerged in the second half of 2021, threat actors will pay increasing attention to search, encryption and data exfiltration activities. This will entail running search strings to identify and disclose sensitive business data, including industrial espionage; and the “affected” organisations cannot mitigate the impact of such threats with simple security measures, such as creating offline backups or relying on in-house “experts” employed with a fixed salary.

Intelligence about the target may include legal or insurance documents, commercial and financial information, intellectual property or market-sensitive data (such as details of acquisitions or mergers), not to mention the intelligence of some recently pilloried States.

Threat actors can use this intelligence to demand higher ransom payments and put more pressure on victims to give in. Ransomware developers can also focus more on persistent attack campaigns, in which threat actors are able to attack victims again even after the security team believes the initial threat has been removed. Just an illusion or a figment of imagination.

Aggressive law enforcement action against ransomware groups in 2021 pushed some of them to relinquish attacks in favour of data kidnapping schemes that these groups consider less risky. In a data kidnapping operation, attackers/groups obtain data, via phishing, downloading a misconfigured server or other means, and then threatening the victim companies with disclosure of data if they do not pay. This is different from a ransomware attack because victims’ files are not encrypted and victims have full control over their servers and operations, but they may want to avoid reputational damage or fines associated with data breaches.

As threat actors seek more effective means for forcing victims to pay ransom, their extortion tactics may also evolve. Besides disclosing and exploiting sensitive corporate data, threat actors may turn to individuals known to organised crime to push victims to pay. Threats to senior executives and their families, or the executives’ involvement in illegal activities, are possible options. What advice can be given to at least mitigate threats?

1. From an in-depth defence strategy to a zero-trust security strategy. The zero-trust model is based on the principle of “never trust, always check” and relies on other network security methodologies, such as network segmentation and strict access controls. It is an approach to security that assumes the absence of a trusted network perimeter, whereby every network transaction must be authenticated before it can materialise.

2. Segregation of important assets and administrative accounts, also going back to the method of keeping hard copy documents in a safe: a “primitive” method, but immune to malicious attackers who have neither combination nor explosives.

3. Implement multi-factor authentication for remote access and administrative accounts.

4. Monitor threat actors’ communication channels for compromised credentials.

5. Use threat intelligence to focus management on vulnerabilities that the attacker will exploit, provided that intelligence is not – in turn – monitored by the attacker.

6. Disable administration tools for users who do not need them to prevent threat actors from abusing and taking advantage of classic naivety.

7. Disable unnecessary or obsolete Windows and Linux components.

8. Remove remote access solutions that are no longer needed.

9. Prepare for breaches by constantly building and maintaining relations with law enforcement agencies.

It is likely that the use of TCP – the transmission control protocol, which is part of the Internet protocol suite dealing with transmission control, i.e. making online data communication between sender and receiver reliable – as a vehicle for ransomware distribution is increasing, because it lowers barriers to entry for threat actors, and puts malware in multiple operators' hands. Ransomware attacks, however, can generate much media coverage, which could be a mitigating factor, as threat actors do not want to attract authorities' attention.

The continued expansion of the software supply chain could also lead to an increase in TCP attacks. Small third-party vendors in large supply chains will be seen as weak links through which threat actors can target high-value, security-conscious organisations. Therefore, organisations cannot focus only on strengthening their own defences, but must also protect their supply chains. Threat actors are also likely to increase attacks on vulnerabilities in teleworking and cloud infrastructure.

"Non-State" hackers – i.e. those operating across national borders – could also increase. These attackers could target key media events in 2022, such as the World Championship in Qatar, etc., causing disruptions and reputational damage to event organisers and sponsors. Moreover, as was the case with the 2020 US presidential election, the 2022 mid-term elections could further highlight the risks associated with third-party vendors.

Throughout 2022, the underground crime market will continue to provide a lucrative channel for all types of cybercriminals to peddle credentials stolen from an organisation's network. The surge in the use of intelligence thieves – such as RedLine, Vidar, Azorult, Raccoon, Grand Stealer, Vikro Stealer, or even open source products such as Sorano and AdamantiumThief – will continue to drive and well pay its developers and the community.

Moreover, given the effectiveness and prevalence of their attacks, the multi-dimensional capabilities that these infostealing software already possess are likely to expand and grow further. Competition among developers of infostealing software will intensify, which is bound to spur innovation among developers to create “better”, more complex products and easier-to-use services, with personal and “employer” profits far beyond any imagination.

Infostealing software significantly lowers the barriers to entry for low-level threat actors by providing botnet logs that help attackers gain additional access to other services by collecting credentials, obtaining confidential information or assisting in the distribution of other payloads.

Botnet is a network of computers, usually PCs, controlled by a botmaster and composed of devices infected with specialised malware, called bots or zombies. Zombie is a computer or mobile device connected to the Internet that, without the user’s knowledge, has been compromised by a cracker or infected with a virus in such a way as to enable unauthorised people to take partial or full control of it.

The versatility of infostealing software and its ability to steal large amounts of sensitive data make it a threat to every organisations in all sectors. The growing “symbiotic relationship” between access brokers and ransomware operators will see the demand for IAB services continue to grow. This will exacerbate physical attacks across multiple sectors to simplify the cyber intrusion process, enabling threat actors to operate more quickly and effectively. Considering the low risk and high demand for initial access, more groups or threat actors will engage and attempt to sell access to various organisations.

Based on the trends observed in 2021, it is believed that vulnerabilities in packages bundled and imported into various applications will continue to attract threat actors seeking to maximise the effectiveness of their attacks. They may invest time finding consistent inputs from various applications that eventually lead to the same vulnerable functionality in commonly used computer libraries. This could enable attackers to develop effective exploit tools for various applications, increasing the number of potential targets and reducing the workload. Furthermore, threat actors gaining access from the breach will further compromise systems, extract personal identification data and implement data extortion schemes. As early as January 2022, threat actors have begun advertising access to hundreds of thousands of servers.

Cybercriminals will continue to use sophisticated and automated phishing kits in 2022 to take cybercrime to the next level. These types of kits may vary in sophistication and be purchased through clandestine criminal networks, covert channels and sometimes even transparent online platforms operating on the dark and deep web.

The operators purchasing kits from these platforms usually have most – if not all – of the necessary resources provided by the kit creator. These include tools to quickly distribute and deploy landing pages, detection evasion tools and even interfaces to generate obfuscated HTML templates that bypass anti-spam or phishing email controls and successfully reach recipients' mailboxes.

It has been found that threat actors involved in distributing phishing kits can advertise their products through underground criminal networks and covert channels, and even automate transactions using bots to sell the leaked data. As security technologies designed to detect phishing kits and websites continue to improve and evolve, threat actors are constantly changing their tactics, methods and procedures to avoid detection and maintain their operations.

“Remittance-intensive” economies will switch to digital currencies at a faster pace in 2022, especially in the Middle East and Central Europe. The threat posed by cryptocurrencies to “long-lived” currencies such as the dollar and euro could increase regulation of the sector.

As cryptocurrencies are known to avoid sanctions, launder money and disrupt dollar-based economic systems, further regulation of the sector could come from traditional economic powers, such as the United States last year, which introduced new tax return requirements. The EU is also exploring a digital euro to compete with cryptocurrencies in the coming years.

Besides causing financial losses to victims, threat actors may also look for opportunities to expose user data, as these companies collect large amounts of data from customers for security purposes.

As cybercriminals find new ways to steal investors’ financial resources, and attacks on cryptocurrencies become more targeted, the opportunity to exploit digital currencies will not only attract cybercriminals, but in 2022 State hackers will probably continue to carry out ever more high-speed attacks in the cryptocurrency sector as a way to raise funds for governments to circumvent various international controls.

Furthermore, as mentioned above, cybercriminals may accelerate the transition from Bitcoin to Monero as the cryptocurrency of choice to facilitate transactions and respond to more aggressive actions by the law enforcement agencies, as well as controls by governments and various related intelligence. The use of Monero in the threat actor community is estimated to increase significantly by the end of 2022, as observed on the darknet markets, namely Silk Road, AlphaBay and White House Market.