EUROPOL

IOCTA

EUROPOL SPOTLIGHT

CYBER-ATTACKS: THE APEX OF CRIME-AS-A-SERVICE

Contents

Key terms

AFFILIATES: cybercriminals who carry out ransomware attacks using ransomware-as-a-service platforms (affiliate programs) ran by criminal groups. Affiliates are able to use the tools on the platform in exchange of a percentage of the criminal proceeds they generate.

API SERVER: a server running and relaying commands to an Application Programming Interface.

BULLETPROOF HOSTING: a service offered by some sites or web hosting firms that allows their customers considerable leniency on the content they can upload. Such hosting providers tend not to respond to lawful requests for information.

COMMAND AND CONTROL (C2) SERVERS: a server that is used to send commands to devices connected to the target network.

DROPPERS: programs designed to deliver malicious software to a device. They usually do not have malicious functions themselves and are designed to evade and de-activate the system's security features (e.g. anti-virus, endpoint detection) before installing malware and other malicious tools (i.e. payloads).

END-TO-END ENCRYPTION (E2EE): a method to secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. The data is encrypted on the sender's system/device and only the intended recipient can decrypt it.

FAST-FLUX: a technique used by cybercriminals to increase their infrastructure's resilience by hiding its traffic behind a network of hosts acting as proxies.

KILL-CHAIN: all the different stages of a cyber-attack.

MALSPAM (A PORTMANTEAU OF 'MALWARE' AND 'SPAM'): unsolicited emails containing malware.

STRESSERS: tools designed to test the stress resistance of a network to see if the resources designated to it (e.g. bandwidth, CPU) can withstand additional load.

BOOTERS: illegal stressers criminals provide as-a-service to launch DDoS attacks.

SECURE-SOCKET SHELL (SSH)-TUNNEL CONNECTIONS: (SSH =) a secure connection between a client and an server.

SUPPLY-CHAIN ATTACKS: an attack where the cybercriminals infiltrate a system through an outside partner or service provider that has authorised access to the target's network.

Key findings

Malware-based cyber-attacks, specifically ransomware, remain the most prominent threat with a broad reach and a significant financial impact on industry.

Ransomware affiliate programs have become established as the main form of business organisation for ransomware groups who continue deploying multi-layered extortion methods, with indications that the theft of sensitive information might become the core threat.

Phishing emails containing malware, Remote Desktop Protocol (RDP) brute forcing and Virtual Private Network (VPN) vulnerability exploitation are the most common intrusion tactics used by cybercriminals. Legitimate software and tools built into operating systems are then misused to establish persistence and traverse their victims' networks.

The Russian war of aggression against Ukraine led to a significant boost in Distributed Denial of Service (DDoS) attacks against EU targets. The most noticeable DDoS attacks were politically motivated and coordinated by pro-Russian hacker groups.

Initial Access Brokers (IABs), droppers-as-a-service and crypter developers are key enablers utilised in the execution of a variety of cyber-attacks. High-tier cybercriminals benefit greatly from the increased activity on criminal marketplaces and of IABs selling stolen data.

The war of aggression against Ukraine and Russia's internal politics have uprooted cybercriminals pushing them to move to other jurisdictions.

Introduction

The year 2022 brought forth a number of developments in the cybercrime threat landscape related to the geopolitical turmoil caused by Russia's war of aggression against Ukraine as well as law enforcement actions taken against threat actors and cybercriminal infrastructure.

Ransomware groups have remained the most outstanding threat and have established a clear approach of going after international companies, public organisations, critical infrastructure and essential services. According to the European Union Agency for Cybersecurity (ENISA) and reports from the private sector, ransomware attacks caused most concern for the manufacturing industry[1].

Affiliate programs remain the dominant form of business organisation for ransomware groups. They work closely with other malware-as-a-service groups and initial access brokers (IABs) to compromise high-revenue targets and post huge ransom demands, running into millions of Euros.

Cybercriminals continue targeting Android devices with mobile malware[2], but there were no campaigns as prolific as the ones reported in the IOCTA 2021, thanks to an international law enforcement action in May 2022 that took down the infrastructure of FluBot (mobile info-stealer)[3].

OPERATION VACCINATION

Mobile malware disruption

First spotted in December 2020, FluBot has gained traction in 2021 and compromised a huge number of Android devices worldwide. The malware was installed via text messages which asked users to click a link and install an application to track a package delivery or listen to a fake voice mail message.

1 ENISA, 2022, ENISA Threat Landscape 2022, accessible at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 ; SEKOIA.IO, 2022, Mid-2022 Ransomware Threat Landscape, accessible at: https://blog.sekoia.io/sekoia-io-mid-2022-ransomware-threat-landscape/

2 HackRead, 2022, Play Store Apps Caught Spreading Android Malware to Millions, accessible at: https://www.hackread.com/play-store-apps-spread-android-malware-millions/

3 Europol, 2022, Takedown of SMS-based FluBot spyware infecting Android phones, accessible at: https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

Once installed, the malicious application, which actually was FluBot, would ask for accessibility permissions. The hackers would then use this access to steal banking app credentials or cryptocurrency account details and disable built-in security mechanisms. This strain of malware was able to spread like wildfire due to its ability to access an infected smartphone's contacts and its ability to self-replicate. In May 2022, an international law enforcement operation involving 11 countries (Australia, Belgium, Finland, Hungary, Ireland, the Netherlands, Romania, Spain, Sweden, Switzerland and the United States) resulted in the takedown of FluBot infrastructure and putting a stop to the destructive spiral. Europol supported the investigation by coordinating the activities, facilitating the information exchange, providing digital forensic support and setting up a virtual command post on the day of the takedown.

According to ENISA, public organisations and digital service providers remained the sectors most targeted by different cyber-attacks in the first half of 2022[4]. The high number of attacks against public administrations is likely influenced by the invasion of Ukraine, which has politicised the hacker underground and brought forth a wave of Distributed Denial of Service (DDoS) attacks against EU countries condemning Russia's actions. The targeting of digital service providers likely illustrates a continued trend reported on in the previous IOCTA of supply-chain attacks increasing in popularity because of the scalability of their attack-surface[5]. Compromising a digital service provider allows criminals to by-pass security features by distributing malware to the clients' networks from a trusted source. This module takes a deeper dive into the specific methods, tools and infrastructure used in cyber-attacks, as well as discusses how the threat actors responsible for them operate.

Cyber-attacks, motivated by both financial gain and political beliefs, are becoming more targeted and continue causing disruptions in all sectors. They can create steep financial set-backs, in terms of incident response and recovery, to businesses and governmental organisations alike. The social impact of cyber-attacks varies based on the target and can range from making (public) services unavailable to hampering critical infrastructure. The by-product of attacks is often people's personal data being stolen or leaked

4 ENISA, 2022, ENISA Threat Landscape 2022, accessible at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

5 The number of different attack vectors a cybercriminal can use to manipulate a network or a system.

online, which damages their privacy and makes them more susceptible to further exploitation by criminal actors.

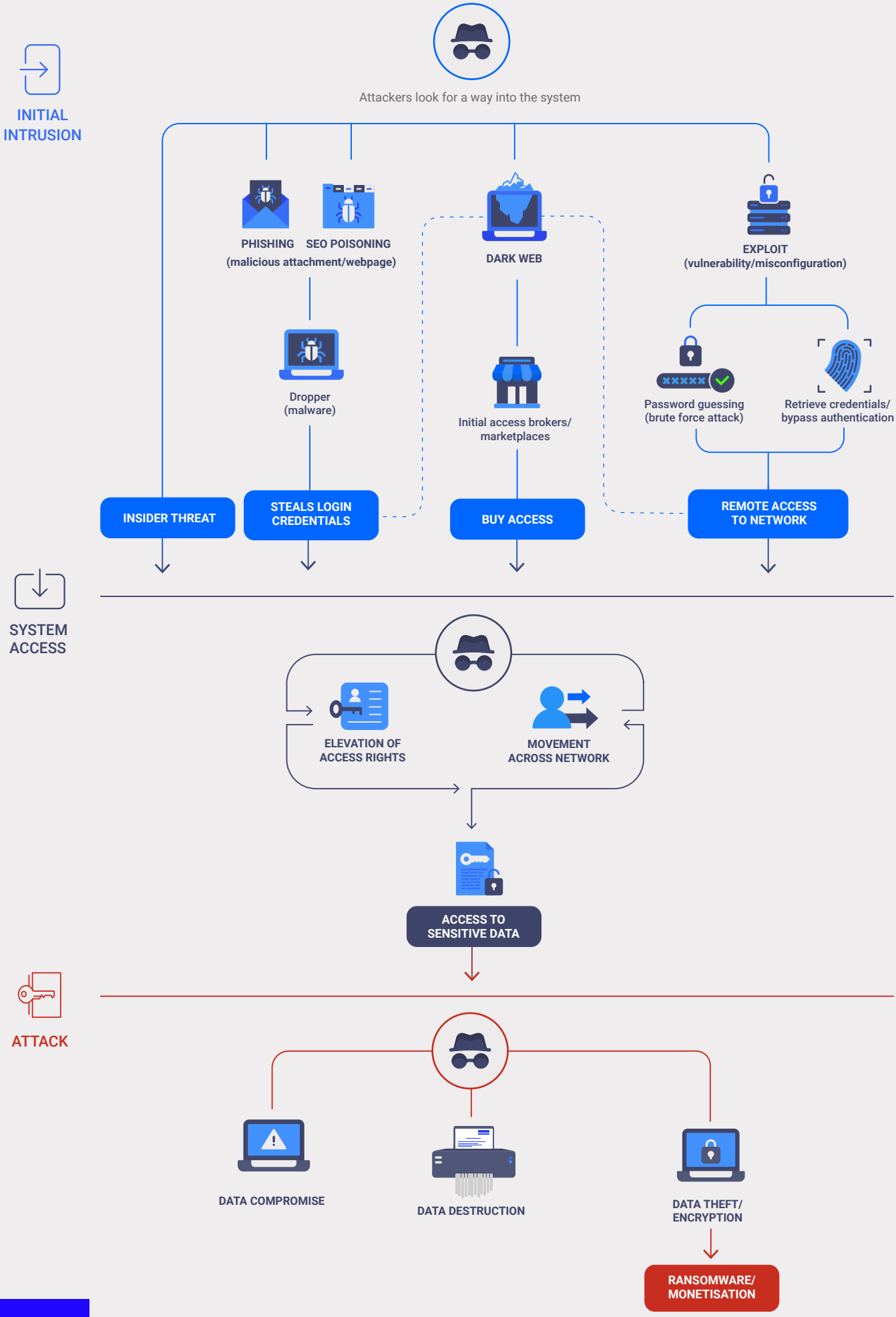
Criminals fleeing the war

The war of aggression launched against Ukraine, Russia's mass mobilisation and Western sanctions (including boycotts by tech companies) have uprooted criminals in the region and created opportunities for law enforcement to arrest high-ranking threat actors previously outside their reach. A prolific Ukrainian cybercriminal fled the country in March 2022 and was arrested soon after by Dutch authorities. The suspect was under investigation for having created and sold RacoonStealer, a data theft malware in existence since 2019. The malware was sold as–a-service to other criminals (malware-as-a-service), with clients paying USD 200 per month in cryptocurrencies. It is believed to have been used to steal personal data through browsers, applications and cryptocurrency wallets from more than two million victims[6].

Malware attacks

Malware based cyber-attacks remain the most prominent threat and consist of multiple types of malware and intrusion techniques being deployed in conjunction in different attack stages. Malware based attacks are usually categorised based on their end impact (e.g. ransomware deployment = ransomware attack), with ransomware continuing to be the top threat. It is important to note that regardless of the end result, the same intrusion patterns can lead to a number of different forms of exploitation depending on the main focus of the attacker (e.g. data theft/ espionage, selling or using access for profit, disruption of service for ideological/political end goal).

6 Krebs on Security, 2022, Accused 'Raccoon' Malware Developer Fled Ukraine After Russian Invasion, accessible at: https://krebsonsecurity.com/2022/10/accused-raccoon-malware-developer-fled-ukraine-after-russian-invasion/


INITIAL INTRUSION
Attackers look for a way into the system
PHISHING
SEO POISONING
(malicious attachment/webpage)
DARK WEB
EXPLOIT
(vulnerability/misconfiguration)
Dropper
(malware)
Initial access brokers/
marketplaces
Password guessing
(brute force attack)
Retrieve credentials/
bypass authentication
INSIDER THREAT
STEALS LOGIN CREDENTIALS
BUY ACCESS
REMOTE ACCESS TO NETWORK
SYSTEM ACCESS
ELEVATION OF ACCESS RIGHTS
MOVEMENT ACROSS NETWORK
ACCESS TO SENSITIVE DATA
ATTACK
DATA COMPROMISE
DATA DESTRUCTION
DATA THEFT/ ENCRYPTION
RANSOMWARE/ MONETISATION

Initial intrusion

Cybercriminals usually gain initial access through compromised user credentials or by exploiting vulnerabilities in the targeted infrastructure. Compromised credentials are a commodity that can be acquired from IABs, who sell them on criminal platforms or can be gathered in bulk through phishing and dropper services. Droppers offered as-a-service use cracked websites and their network of infected computers (botnet) for malspam campaigns to deliver their customer's malware (e.g. an info-stealer) to a victim's system. These services are widely used and facilitate a variety of different forms of cybercrime.

Phishing campaigns

Criminals use phishing services to distribute emails containing documents (e.g. Excel, Word) with malicious macros, infected container files (e.g. Zip, RAR) or URLs that lead to webpages that initiate a drive-by download of malware. Interacting with these sources often results in a dropper being introduced into the victim's system. According to some research, criminals have shifted their preference of using malicious macros in favour of container files[7] after Microsoft blocked macros delivered over the Internet in their applications[8]. Emotet and Bazarloader are two prominent examples of droppers used for malware distribution. The main distribution vector for both services is email campaigns.

Victims can also be infected with droppers through internet search-engines, where users are lured with search engine optimisation (SEO) key words to download malware disguised as a legitimate program or tool[9]. In some cases, criminals use search-engine advertising tools to direct users to web pages masquerading as download sites for popular software programs, which actually deliver malware to the victim's system. Furthermore, smart-devices can become compromised through malicious applications uploaded to legitimate App Stores[10].

7 Proofpoint, 2022, How Threat Actors Are Adapting to a Post-Macro World, accessible at: https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world

8 Microsoft, 2023, Macros from the internet will be blocked by default in Office, accessible at: https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

9 Mandiant, 2022, Zoom For You — SEO Poisoning to Distribute BATLOADER and Atera Agent https://www.mandiant.com/resources/blog/seo-poisoning-batloader-atera

10 MalwareBytesLab, 2022, Malware on the Google Play store leads to harmful phishing sites, accessible at: https://www.malwarebytes.com/blog/news/2022/11/malware-on-the-google-play-store-leads-to-harmful-phishing-sites

Criminal groups running droppers-as-a-service cooperate closely with other criminal malware-as-a-service providers like ransomware affiliate programs, who use the botnets for access, malware distribution and also in some cases victim monitoring. Both of the aforementioned criminal services also have a close working relationship with crypter developers. Crypters are pieces of software that obfuscate and encrypt malicious payloads, making them less detectable by traditional anti-virus programs.

Crypters are a key component in malware development operations and creating them requires a very specific skillset.

The sophistication of the crypter directly influences the success rate of the malware delivery and execution, which makes them a very sought after commodity on cybercriminal markets.

Droppers-as-a-service are used to deliver a variety of different payloads like info-stealers, crypto-miners, remote access tools (RATs) and penetration tools. One of the more common primary payloads identified in 2022 was the QakBot (Qbot)[11] modular information stealer that gathers data from the infected system (browser data, keystrokes and credentials) and also acts as a loader to retrieve a secondary payload from its command-and-control (C2) servers (e.g. Cobalt Strike).

Exploitation of vulnerabilities and misconfigurations

Exploitation of vulnerabilities in Virtual Private Network (VPN) software, the Microsoft Exchange Server and misconfigurations in the Remote Desktop Protocol (RDP) are common intrusion tactics deployed by cybercriminals.

Remote Desktop Protocol (RDP) brute forcing[12] – Cybercriminals perform automated scans on the Internet for open RDP ports. If configured incorrectly, the protocol presents many opportunities for intrusion. Examples of misconfiguration include not enabling (multi-factor) authentication, employing simplistic credentials or not using a firewall to filter access to the machine. These missteps open the door for brute-force attacks or exploitation of vulnerabilities enabling access and remote code execution in popular software like AnyDesk or TeamViewer.

11 Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, accessible at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

12 Axios, 2023, Ransomware gangs are starting to ditch encryption, accessible at: https://www.axios.com/2023/01/13/ransomware-gangs-cut-out-encryption

ProxyShell[13] is the name given to a collection of vulnerabilities in the Microsoft Exchange Server. For example, exploiting these vulnerabilities enables the attacker to use the Exchange server to distribute phishing emails to user accounts from a trusted source.

Virtual Private Networks (VPN) – This category of remote access software is heavily targeted by cybercriminals to get a good foothold inside the victim's network.

Lateral movement and privilege escalation

After stealing a user's credentials or exploiting a vulnerability to access the target's (organisation) system, the attackers need to map the network, move laterally and escalate their privileges to gain access to as many parts of the system as possible before exfiltrating data and executing the attack.

Most of the tools in the hackers' arsenal are not malicious by design, but regular system administration and pen-testing tools like Cobalt Strike that can be utilised for carrying out the attack after the initial compromise.

As the first step, attackers establish persistence within the compromised system by creating an encrypted channel to their own infrastructure (i.e. a back-door) in case the initial intrusion is detected. For this purpose, cybercriminals commonly use SystemBC and legitimate remote access applications.

Attackers usually map out the network, its devices and users using tools like BloodHound in order to design their attack-steps. This includes identifying operating systems, understanding the network structure and host-naming conventions.

Once the attacker has identified critical areas that they need to access, they will start gathering credentials to escalate their privileges by utilising tools like Mimikatz and Rubeus.

These different tools are used in conjunction with each other based on the compromised system specifics. Most of the tools (e.g. Cobalt Strike and

13 SentinelLabs, Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection, accessible at: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

Mimikatz) are multi-functional and can be utilised in different attack stages. The end result of the phase is that the attackers have access to the sensitive data and assets within the victim's system.

Exfiltration and exploitation

Attackers then move the extracted data from the victim's network to a cloud-based hosting service or to rented servers for its exploitation. This includes, for example, using the threat of publishing it for extortion[14] or selling it on criminal markets.

In case of a ransomware attack, samples of the extracted data are posted on leak-sites hosted on the dark web (.onion sites) as well as the clear web. This is generally accompanied by a threat to publish or auction off the data if the ransom demand is not met. This is a common way to prove the legitimacy of a threat and to add more pressure to the victim to comply with the demands. Data theft has become a key-component in ransomware groups' criminal process because it bolsters the success rate of receiving a pay-out. This is supported by the fact that in some instances ransomware operators have started opting to not encrypting the victim's files and purely leverage the stolen information against them in the ransom negotiation[15]. A possible explanation for this trend could be that organisations have become more systematic in backing up their systems on a regular basis so the threat of not decrypting their data is no longer sufficient for making them succumb to the ransom demand. If true, this could be an indication of an upcoming shift in the threat landscape, where theft of sensitive data becomes the central goal of cyber-attacks, which inadvertently would also further feed the growing criminal market of personal information.

After exfiltrating the data, attackers can deploy ransomware (or other malware) to the system encrypting the files and leaving behind a ransom note on how to contact the attackers or pay for the decryption key. Additionally, more ransomware groups have started using partial encryption

14 Europol, 2021, Internet Organised Crime Threat Assessment (IOCTA) 2021, accessible at: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

15 Axios, Ransomware gangs are starting to ditch encryption, accessible at: https://www.axios.com/2023/01/13/ransomware-gangs-cut-out-encryption

algorithms to speed up the process and to make it less detectable by the system[16].

In addition, compromised organisations can be exposed to several simultaneous or consecutive cyber-attacks because the IABs usually do not offer exclusivity of their assets to the buyers. Due to this, the same compromised credentials can be used by different cybercriminals[17]. Although ransomware remains a top-threat, law enforcement should not ignore the criminal groups and services in the rest of the attack kill-chain that enable a variety of attack forms to be executed.

Ransomware groups

Business structure

Ransomware groups and affiliate programs continue to plague international enterprises, public organisations, critical infrastructure and essential services. Affiliate programs have become established as the staple form of ransomware-as-a-service (RaaS) because of their streamlined processes as well as the scalability of their activities. Their business model is based on developing a platform, which affiliates can use for deploying ransomware, posting exfiltrated data and laundering the criminal proceeds. The administrators of the platform (ransomware group) receive a percentage of all the payments made to criminals using their service.

The cryptocurrency payments received from victims are deposited directly to the wallet of the ransomware group, where they are usually funnelled through a mixer and distributed automatically between the administrators, the affiliate carrying out the attack and the service providers. The split of the profit received by the affiliate is based on their rank, which is determined by the success rate of their attacks and the criminal profits generated. At entry level the affiliate shares are low (around 20-40 % of the ransom), but at higher ranks they can receive up to 80 % of the profits

16 SentinelLabs, Crimeware Trends | Ransomware Developers Turn to Intermittent Encryption to Evade Detection, accessible at: https://www.sentinelone.com/labs/crimeware-trends-ransomware-developers-turn-to-intermittent-encryption-to-evade-detection/

17 SOPHOS, 2022, Multiple attackers: A clear and present danger, accessible at: https://news.sophos.com/en-us/2022/08/09/multiple-attackers-increase-pressure-on-victims-complicate-incident-response/

0

AFFILIATE PROGRAM

1

CORE GROUP

- Senior managers
- Back-end developers

2

SECOND TIER

- Pen-testers
- Developers
- Decrypters
- Reverse-engineers
- System administrators
- Human resource department
- Recruiters
- Legal teams
- Ransom negotiators

3

THIRD TIER

- Bullet-proof hosting and VPN services
- Money laundering services
- Initial access brokers
- Dropper and botnet services
- Crypter developers

because they have proven to be a lucrative business partner for the criminal groups running the service. The business process of a ransomware affiliate program is similar to a legitimate tech company with dedicated teams working on development projects and support services[18].

The core of ransomware groups usually consists of cybercriminals with experience in different areas of cybercrime and a long history of collaboration. They usually operate in closed environments (e.g. privately hosted forums and chatrooms). The members of the core group are senior managers (e.g. data managers) and back-end developers who oversee the operation, manage the groups' assets and develop the service platform by adding new features, increasing operational security (OpSec) and resilience.

Core members can also be a part of different ransomware groups because of the short life-expectancy of ransomware families. Law enforcement action and internal disputes can force ransomware operations to disperse or rename themselves to cover their tracks, which leads to establishment of new groups involving the same managers/administrators[19].

The second tier of ransomware group members consists of recruited specialists, who fulfil specific functions in running the affiliate program. They can include developers, pentesters, reverse-engineers, system administrators, negotiators, recruiters, human resource managers and legal experts. Their profile can be more diverse, but a majority come from Russian-speaking backgrounds as it is the lingua franca of the cybercriminal ecosystem. They form technical and support teams with their own budget and middle-management structures[20].

The third tier is composed of external service providers the group cooperates with and affiliates who are responsible for carrying out the attacks. The most common service providers include IABs, crypter developers, dropper, money laundering and bullet-proof hosting services. Affiliates and service providers sometimes work simultaneously with several ransomware groups. Ransomware groups, similar to other criminal

18 Forescout Vedere Labs, 2022, Analysis of Conti Leaks, accessible at: https://www.forescout.com/resources/analysis-of-conti-leaks/

19 BleepingComputer, 2022, BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs, accessible at: https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/

20 Krebs on Security, 2022, Conti Ransomware Group Diaries, Part II: The Office, accessible at: https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/

syndicates, are distrustful and prefer to collaborate with criminal actors that they have worked with previously.

Some affiliate programs, like LockBit 2.0[21], aim to make the process of infection as easy and fast as possible (e.g. using partial encryption[22]). They have automated most of the features in their service platform (e.g. privilege escalation, data encryption and exfiltration) that enable the malware to propagate with minimal human oversight after the initial intrusion, making it possible to target a larger number of victims simultaneously. This makes LockBit 2.0 attractive for lower-level cybercriminals whose only role is to secure initial access into the victim's network, which explains why it is one of the most widely encountered ransomware strains in 2022[23]. The new LockBit variant, similar to many other ransomware families (e.g. RagnarLocker), is also able to encrypt Linux systems. Linux based systems are often used in devices running administrative servers for enterprises, governmental institutions and web service providers, which means they hold critical data for the organisation.

Infrastructure

The infrastructure of cybercrime services is built to be resilient to law enforcement tracing and disruption. The admin panel of a service platform (back-end infrastructure) is usually hosted on a dedicated server with a bulletproof provider located in an uncooperative jurisdiction and is managed by the group's administrators. The panel contains among other things the source code for the ransomware builder, affiliates' information, details of victims, overview of compromised computer systems and the addresses of the cryptocurrency wallets used by the group.

The C2 servers (separate ones for malware, penetration tools, data extraction etc.) from where the different attack stages are orchestrated are managed by the affiliates and usually run on virtual private servers (VPS) provided by bulletproof hosters in Eastern-European countries. These hosting providers often rent the servers from legitimate and well-

21 PacketLabs, 2022, LockBit's Automated Ransomware Processes Present Unique Challenges, accessible at: https://www.packetlabs.net/posts/lockbit-automated-ransomware/

22 Bleeping Computer, Ransomware gangs switching to new intermittent encryption tactic, accessible at: https://www.bleepingcomputer.com/news/security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic/

23 Unit 42, LockBit 2.0: How This RaaS operates and how to protect against it, accessible at: https://unit42.paloaltonetworks.com/lockbit-2-ransomware/; SEKOIA.IO, SEKOIA.IO Mid-2022 Ransomware Threat Landscape, accessible at: https://blog.sekoia.io/sekoia-io-mid-2022-ransomware-threat-landscape/

known service providers in Europe and North-America, which means that cybercriminals do not necessarily know where parts of the attack infrastructure are physically hosted. Sometimes separate VPSs as also used as stepping-stones for connecting to an infected device to make tracing and mapping more difficult.

The C2 servers control the different components through SSH-tunnel connections[24]. The tools themselves are hosted on separate domains rented from a bulletproof hoster and introduced to the victim's device/system through droppers or manual delivery after the initial intrusion.

Ransomware groups sometimes rent separate servers for victim data exfiltration, but are increasingly moving toward using legitimate cloud-storage providers to store the data gathered from the victim. This seems to be mostly for cost-efficiency since they do not have to rent additional infrastructure and most services today offer built-in privacy features like end-to-end encryption (E2EE) sought by the criminals.

Dedicated leak-sites, where the victim data is posted, can be hosted on the dark web (.onion sites) or on the clear web using bulletproof domain hosts and are managed by the administrators as a part of the main service infrastructure.

DDoS attacks

Criminal groups

The pro-Russian hacktivist group Killnet, that ramped up its activities since the Russian war of aggression against Ukraine, claimed responsibility for the most outstanding DDoS attacks launched in 2022 against targets in the EU and beyond. These attacks include the one launched against the European Parliament and many others targeting the infrastructure of EU countries[25]. The impact of these attacks has been moderate, mostly causing limited disruption.

24 SSH, SSH Tunneling: Examples, Command, Server Config, accessible at: https://www.ssh.com/academy/ssh/tunneling-example

25 Avertium, 2022, An in-depth look at Russian threat actor, Killnet, accessible at: https://www.avertium.com/resources/threat-reports/an-in-depth-look-at-russian-threat-actor-killnet

Killnet's main goal seems to be mobilising and coordinating low-skilled hacktivists to launch DDoS attacks on ideological grounds. They encourage people to post about outstanding targets in their home countries on Killnet's dedicated Telegram channels and try to orchestrate attacks against those targets.

The attacks themselves are executed using widely available DDoS services on the internet (booter and stresser services[26]).

Another hacking group pushing the pro-Russian agenda through DDoS attacks in 2022 was NoName057[27]. They launched the DDosia project, which enables users downloading the tool to lend their machine's computational resources for launching DDoS attacks. This essentially means building a botnet of volunteered devices. The project also payed users for successful attacks.

Infrastructure

The infrastructure of a DDoS service is not very different from other cybercriminal services. It consists of an admin panel, C2 servers, API servers and botnets. The service providers can build their own botnets, but often the botnet infrastructure is bought from other criminal groups specialising in the service.

The API servers connected to the botnet are used to prepare attacks based on the given parameters and can be hosted on other compromised devices. Criminals also use fast-flux[28] in their networks, which allows them to frequently change the IP address of their servers by moving them between different hosters and compromised machines making it harder to disrupt. The C2 servers that are usually hosted on VPSs are connected to the API server and the botnet and are used to launch the attack.

The business model of booter and stresser services consists of acquiring a botnet and building a user-panel through which criminals can launch a

26 Cloudflare, What is a DDoS booter/IP stresser? | DDoS attack tools, accessible at: https://www.cloudflare.com/en-gb/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/

27 Avast, 2023, Beware of DDosia, a botnet created to facilitate DDoS attacks, accessible at: https://blog.avast.com/ddosia-project

28 Unit 42, 2021, Fast Flux 101: How Cybercriminals Improve the Resilience of Their Infrastructure to Evade Detection and Law Enforcement Takedowns, accessible at: https://unit42.paloaltonetworks.com/fast-flux-101/

designated attack for a small fee (depends on attack type and duration). The service itself is very easy to use – the customer wishing to launch a DDoS attack only has to input the destination (IP-address and port), attack type (e.g. UDP, SYN, ping flood) and duration. Different attack types are chosen based on what kind of system you are targeting (web-page, email server etc.), which also determines what protocol layer of the system you are trying to overwhelm[29]. Before deciding on an attack path, criminals scan the target network for vulnerabilities and find open ports.

Criminals also use DDoS-as-a-service platform to launch low-volume attacks against company websites and demand ransom payments threatening to cripple the service otherwise. This low cost and effort modus operandi was also reported in IOCTA 2021 and DDoS for ransom (rDDoS) continues to persist thanks to the widely available criminal services. To mitigate this threat, Europol has coordinated several international law enforcement operations to take down DDoS services with the latest one dismantling around 50 of the world's largest providers.

OPERATION POWER OFF 3

Take-down of DDoS service providers

Some 50 of the world's biggest booter services, designed to enable users to launch crippling DDoS attacks against critical online infrastructure, were taken down in December 2022 as part of an international crackdown against DDoS service providers. The operation involved authorities from Germany, the Netherlands, Poland, the United Kingdom, the United States and the activities in Europe were coordinated by the Joint Cybercrime Action Taskforce (J-CAT)[30]. As part of this action, seven administrators have been arrested in the United States and the United Kingdom, with further actions planned against the users of these illegal services. The most prolific of them, IP-stresser, had been used to launch over 30 million attacks before it was taken down[31].

29 CloudFare, How do layer 3 DDoS attacks work? | L3 DDoS, accessible at: https://www.cloudflare.com/en-gb/learning/ddos/layer-3-ddos-attacks/

30 The J-CAT was launched in September 2014. Located at Europol's European Cybercrime Centre (EC3), it helps fighting cybercrime within and outside the EU. Its objective is to drive intelligence-led, coordinated action against key cybercrime threats and targets by facilitating the jont identification, prioritisation, preparation, initiation and execution of cross-border investigations and operations by its partners. See also https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce

31 Europol, 2022, Global crackdown against DDoS services shuts down most popular platforms, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-against-ddos-services-shuts-down-most-popular-platforms

Europol's response in fighting cyber-attacks

Cyber-attacks are expected to further increase as a criminal threat affecting the EU. Cybercriminals are likely to further embrace new technologies and maximise the reach of their services, with sensitive data as a core target. The crime-as-a-service ecosystem will further develop in order to service a wider criminal base.

Europol's mission is to support EU Member States and cooperation partners in preventing and combating all forms of serious international and organised crime, cybercrime and terrorism. In 2013, Europol set up the European Cybercrime Centre (EC3) to provide dedicated support for cybercrime investigations in the EU and thus to help protect European citizens, businesses and governments from online crime. EC3 offers operational, strategic, analytical and forensic support to Member States' investigations, including malware analysis, cryptocurrency-tracing training for investigators, and tool development projects. EC3's dedicated Analysis Project Cyborg, focused on the threat of cyber-attacks, supports international investigations and operations into cyber criminality affecting critical computer and network infrastructures in the EU.

IOCTA

The Internet Organised Crime Threat Assessment (IOCTA) is a strategic analysis report that provides a law enforcement-centric assessment of the latest online threats and the impact of cybercrime within the EU. It serves to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, with a view to updating the operational focus for EU law enforcement authorities.

The IOCTA is chiefly informed by operational information shared with Europol by EU Member States and third partners, combined with expert insights and open source intelligence.

This ninth edition of the IOCTA appears in an updated format. A summary presents the main overarching findings concerning the major typologies of cybercrime, namely cyber-attacks, online fraud schemes, and online child sexual exploitation. This report “Cyber-attacks: The apex of crime-as-a-service” is the first in a series of spotlight reports covering each of these crime areas in-depth as part of the IOCTA 2023.

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report. Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Headquartered in The Hague, the Netherlands, Europol supports the 27 EU Member States in their fight against terrorism, cybercrime and other serious and organised forms of crime. We also work with many non-EU partner states and international organisations. From its various threat assessments to its intelligence-gathering and operational activities, Europol has the tools and resources it needs to do its part in making Europe safer.

EUROPOL SPOTLIGHT - CYBER-ATTACKS: THE APEX OF CRIME-AS-A-SERVICE

PDF | ISBN 978-92-95220-87-4 | ISSN 2600-2760 | DOI: 10.2813/30058 | QL-AN-23-002-EN-N

Luxembourg: Publications Office of the European Union, 2023

Cite this publication: Europol (2023), Cyber-attacks: the apex of crime-as-a-service, Europol Spotlight Report series, Publications Office of the European Union, Luxembourg.

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu