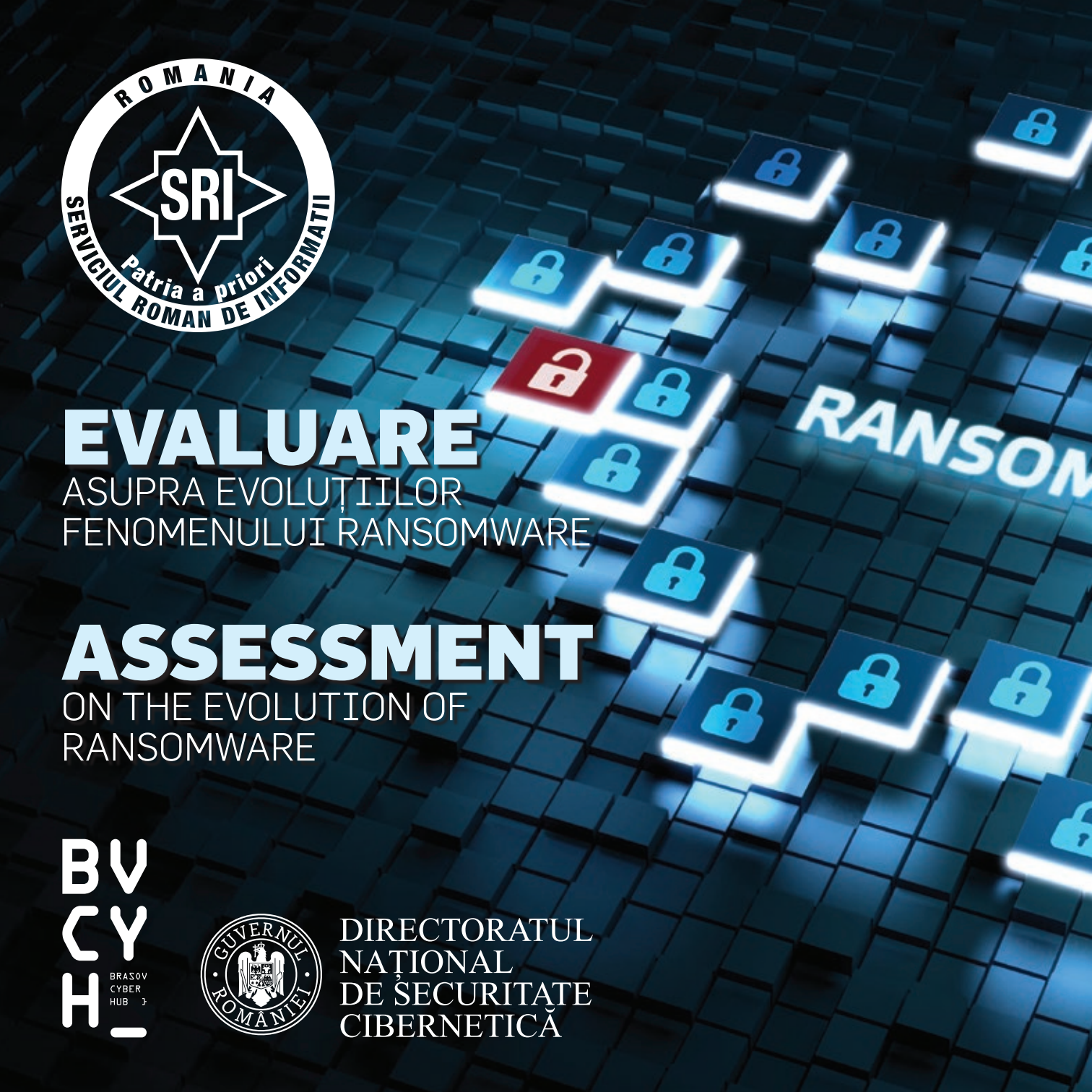

EVALUARE
ASUPRA EVOLUȚIILOR
FENOMENULUI RANSOMWARE

ASSESSMENT
ON THE EVOLUTION OF
RANSOMWARE

BV CY H
BRASOV CYBER HUB

GUVERNUL ROMÂNIEI

DIRECTORATUL
NAȚIONAL
DE SECURITATE
CIBERNETICĂ

SCOPUL MATERIALULUI

Atacurile cibernetice de tip *ransomware* s-au intensificat considerabil începând cu anul 2021, acestea fiind îndreptate atât asupra instituțiilor publice, cât și asupra companiilor private și utilizatorilor individuali.

Materialul a fost realizat în scopul ***sprijinirii eforturilor de consolidare a culturii de securitate cibernetică*** și, implicit, ***reducerii incidenței atacurilor cibernetice de tip ransomware*** asupra instituțiilor publice, companiilor private și utilizatorilor individuali.

Ransomware reprezintă o amenințare pentru toate domeniile de activitate, în special pentru cele critice și esențiale. Amenințările generate de *ransomware* sunt complexe, diversificate și se manifestă nediscriminatoriu, ceea ce impune un răspuns unitar la nivel național. Capacitatea statului de a cunoaște, detecta, preveni, contracara și combate amenințările generate de *ransomware* este direct proporțională cu nivelul de cooperare între sectoarele public, privat și academic.

PĂRȚI IMPLICATE

Materialul a fost realizat prin integrarea a trei viziuni asupra atacurilor de tip *ransomware*: **Centrul Național Cyberint din cadrul Serviciului Român de Informații, Directoratul Național de Securitate Cibernetică (DNSC)** și **Brașov Cyber Hub**.

Prin această formulă este oferită o imagine amplă și de ansamblu asupra fenomenului atacurilor de tip *ransomware*.

SCOPE

Ransomware attacks have intensified considerably since 2021, targeting both public institutions and private companies and individual users.

The material was designed **to support efforts to strengthen the cyber security culture** and, implicitly, **reduce the incidence of ransomware cyber attacks** on public institutions, private companies and individual users.

Ransomware is a threat to all areas of activity, including critical and essential ones. The threats generated by ransomware are complex, diversified and non-discriminatory, which requires a unified response at national level. The capacity of the state to perceive, detect, prevent, counter and combat ransomware phenomenon is directly proportional to the level of cooperation between the public, private and academic sectors.

PARTIES INVOLVED

The material was drawn up by integrating three visions on ransomware attacks: **National Cyberint Center of the Romanian Intelligence Service, National Cyber Security Directorate (DNSC)** and **Brasov Cyber Hub**.

This formula provides a broad and comprehensive picture of the ransomware phenomenon.

➲ **Centrul Național Cyberint** este autoritate națională în domeniul *cyberintelligence*, având atribuții în cunoașterea, prevenirea, combaterea și contracararea atacurilor cibernetice care afectează securitatea națională a României;

➲ **Directoratul Național de Securitate Cibernetică (DNSC)** este autoritatea competentă la nivel național pentru spațiul cibernetic național civil, precum și pentru gestionarea riscurilor și a incidentelor de securitate cibernetică.

➲ **Brașov Cyber Hub** întrunește specialiști, profesori, cercetători, furnizori de servicii, start-up-uri și instituții publice, în scopul identificării de noi soluții în domeniul securității cibernetice, adaptate la specificul fiecărei entități participante.

CUM A FOST GÂNDIT

Întrucât amenințarea generată de *ransomware* este nediscriminatorie și excedează granițele teritoriale, prima parte a materialului abordează **necesitatea conștientizării amenințărilor cibernetice proiectate de atacurile cibernetice de tip *ransomware***, prin raportare la modalitățile de realizare a infecției, modul de acțiune al *malware*-ului și importanța notei de răscumpărare.

A doua parte a materialului este concentrată pe **evoluția atacurilor cibernetice de tip *ransomware***, pornind de la primul atac de acest tip și ajungând la tacticile, tehnicile și procedurile complexe și diversificate din prezent: *ransomware-as-a-service* și *double extortion*, printre altele. De asemenea, sunt abordate inclusiv inițiativele internaționale de combatere a *ransomware*, precum și impactul generat de evenimente sociale și geopolitice asupra amenințărilor cibernetice asociate *ransomware*.

Ulterior, în cadrul materialului sunt prezentate **cele mai prolifice aplicații *malware* utilizate în atacurile de tip *ransomware***, inclusiv atacurile distructive asupra Colonial Pipeline și Kaseya.

În final, sunt prezentate **trenduri ale fenomenului *ransomware***, urmate de **soluții de contracarare** a acestor atacuri cibernetice și **recomandări** pentru prevenirea lor.

➲ **National Cyberint Center** is a national authority in the field of cyberintelligence, with attributions in knowing, preventing, combating and countering cyber attacks that affect Romania's security;

➲ **National Cyber Security Directorate (DNSC)** is the national competent authority for the national civil cyberspace, as well as for the management of cyber security risks and incidents;

➲ **Brasov Cyber Hub** brings together specialists, teachers, researchers, service providers, start-ups and public institutions, in order to identify new solutions in the field of cyber security, adapted to the specifics of each participating entity.

FRAMEWORK

Since the threat generated by ransomware is non-discriminatory and exceeds territorial boundaries, the first part of the document addresses **the need to raise awareness regarding cyber threats posed by ransomware cyber attacks**, by referring to the methods to deliver infection, the manner in which the malware functions and the importance of the ransom note.

The second part of the material focuses on **the evolution of ransomware attacks**, starting from the first attack of this type and reaching today's complex and diversified tactics, techniques and procedures: ransomware-as-a-service and double-extortion among others. It also addresses international initiatives to combat ransomware, as well as the impact generated by social and geopolitical events on ransomware-related cyber threats.

Subsequently, the material presents **the most prolific malware applications used in ransomware attacks**, including the destructive attacks on Colonial Pipeline and Kaseya.

Finally, **trends of the ransomware phenomenon** are presented in the material, followed by **solutions to counter** these cyber attacks and recommendations for prevention.

NECESITATEA
CONȘTIENTIZĂRII
AMENINȚĂRILOR
CIBERNETICE
GENERATE DE ATACURILE DE
TIP RANSOMWARE

THE NEED FOR
AWARENESS REGARDING
THE CYBER THREATS
GENERATED BY
RANSOMWARE
ATTACKS

INFO BOX

RANSOMWARE

aplicație care criptează fișierele de pe sistemele informatice infectate, afectând integritatea și disponibilitatea datelor din cadrul acestora. Scopul actorilor cibernetici care derulează atacuri de tip ransomware este obținerea de beneficii financiare, pentru decriptarea datelor fiind solicitată plata unei răscumpărări în criptomonedă. Raportat la anul 2022, amenințarea generată de atacurile ransomware vizează inclusiv exfiltrarea datelor criptate și targetarea concretă a unor tipare organizaționale, care se potrivesc obiectivelor financiare ale atacatorilor.

CUM SE REALIZEAZĂ INFECȚIA INIȚIALĂ?

Cea mai întâlnită modalitate de distribuire a unui *ransomware* este utilizarea de **tehnici de inginerie socială**:

- **campanii de *phishing*** – presupun transmiterea de e-mailuri care simulează a fi transmise de către persoane fizice, instituții sau companii legitime. Acestea conțin elemente care determină potențialele victime să acceseze *link*-uri, respectiv să descarce documente cu conținut *malware*.
- **site-uri compromise** – atacatorii compromit un site, pe care îl utilizează pentru a distribui aplicația *malware*.
- **reclame web** – anunțurile agresive de publicitate pot fi primul pas în realizarea infecției cu *ransomware*.

Pe lângă utilizarea tehnicilor de inginerie socială pentru realizarea infecțiilor cu *ransomware*, atacatorii apelează la compromiterea credențialelor aferente *Remote Desktop Protocol* (RDP), precum și la vulnerabilități ale acestuia.

RDP este un protocol de comunicații proprietar Microsoft, care permite unui utilizator accesul și gestionarea unui alt dispozitiv, de la distanță, printr-o interfață grafică.

INFO BOX

RANSOMWARE

an application that encrypts files on infected computer systems, affecting the integrity and availability of data within them. The purpose of the cyber actors who carry out ransomware attacks is to obtain financial benefits, as they request a ransom paid in cryptocurrency in exchange for data decryption. Talking about 2022, the threats posed by ransomware attacks also refer to data exfiltration and the targeting of specific organizational patterns, according to the cyber actor's financial objectives.

HOW THE INITIAL INFECTION IS DELIVERED

The most common method to spread ransomware is using **social engineering techniques**:

- **phishing campaigns** – involve sending e-mails that pretend to be sent by legitimate individuals, institutions or companies. They contain elements that urge potential victims to access links, respectively to download documents with malware content.
- **Compromised websites** – attackers compromise a site that they use in order to disseminate the *malware*.
- **Web ads** – the aggressive commercial ads can be the first step in spreading a *ransomware* infection.

Besides using social engineering techniques to generate *ransomware* infections, attackers also resort to compromising the credentials associated to *Remote Desktop Protocol* (RDP), as well as to the latter's vulnerabilities.

RDP is a Microsoft proprietary communications protocol that allows users to access and manage another device remotely by way of a graphical interface.

ETAPELE UNUI ATAC DE TIP RANSOMWARE

Pentru asigurarea succesului unui atac cibernetic de tip *ransomware*, atacatorii parcurg următorii pași:

1. STABILIREA VICTIMEI ȘI OBȚINEREA DE DATE DESPRE ACEASTA

Majoritatea atacatorilor distribuie *ransomware* prin e-mailuri de tip *phishing*. Aceștia își **pot alege victimele în mod aleatoriu**, utilizând adrese e-mail achiziționate de pe forumuri *cybercrime*, compromise anterior de alții, sau **pot alege în mod expres anumite victime din companii pe care le vizează**.

De cele mai multe ori, atacatorii creează e-mailurile de *phishing* utilizând date obținute de pe site-uri sau date pe care utilizatorii le fac publice pe rețele de socializare.

2. ATACUL INIȚIAL

În această etapă, *malware*-ul este transmis către victimă ca atașament sau *link* în cadrul e-mailului de *phishing*, fiind necesară intervenția utilizatorului pentru ca infecția să fie inițiată. De asemenea, atacatorii pot utiliza site-uri compromise anterior, pe care postează fișierul cu conținut *malware*, utilizatorii fiind direcționați să descarce acest fișier. Fișierul conține adesea un **script integrat** (de exemplu, în macrocomenzile unui document Word) utilizat **pentru a crea o conexiune la serverul C2** (Command and Control).

3. COMUNICARE CU ATACATORUL

După ce infecția a fost realizată, aplicația *malware* va încerca să comunice cu un server de comandă și control al atacatorului, pentru a transmite date relevante despre sistemul infectat. În unele situații, atacatorii realizează comunicări cu sistemele victimă pentru încărcarea unor aplicații *malware* adiționale, care vor fi utilizate în următoarele faze ale atacului. În anumite

THE STAGES OF A RANSOMWARE ATTACK

To ensure the success of a *ransomware* cyber attack, the attackers go through the following stages:

1. IDENTIFYING THE VICTIM AND OBTAINING DATA ABOUT IT

Most attackers disseminate *ransomware* through *phishing* emails. They **can choose their victims randomly**, using email addresses acquired from *cybercrime* forums that have already been compromised by others, or they **can choose their victims specifically from targeted companies**.

Most frequently, attackers create the *phishing* emails using data obtained from websites or data that users make public on social media.

2. THE INITIAL ATTACK

At this stage, the *malware* is sent to the victim as an attachment or as a link with the *phishing* email, user intervention being required in order to initiate the infection. Moreover, attackers can use websites that have already been compromised, on which they post the *malware*-containing file, and users are being led to download the file. Often, the file contains an **integrated script** (e.g. in the Word macro commands) used **in order to connect to the C2 server** (Command and Control).

3. COMMUNICATION WITH THE ATTACKER

After the infection has been achieved, the *malware* application will try to communicate with the attacker's command and control server, in order to transmit relevant data about the infected system. In some cases, attackers communicate with the victim systems for the purpose of uploading additional malware applications meant to be used in the subsequent stages of the

situații, cheia de criptare este generată pe serverul C2 și transmisă către sistemul victimă, fiind ulterior demarat procesul de criptare a fișierelor.

4. MIȘCARE LATERALĂ

În cadrul campaniilor *ransomware*, mișcarea laterală se derulează, în unele situații, prin intermediul unei aplicații malware adiționale instalate anterior de către atacator. Foarte puține aplicații dețin capabilități de propagare la nivelul unei rețele după infectarea unui sistem informatic. Cu toate acestea, atacatorii cu capabilități tehnice avansate au dezvoltat ceea ce specialiștii în securitate cibernetică numesc *CryptoWorms*, o aplicație *malware* ce are capabilitatea de a se autoreplica în interiorul rețelei și de a cripta datele utilizatorilor, având posibilitatea de a infecta toate dispozitivele din aceeași rețea.

5. EXFILTRARE DE DATE

Mulți atacatori cibernetici implicați în atacuri de tip *ransomware* apelează la exfiltrarea datelor pentru a constrânge victimele să plătească răscumpărarea. Există situații în care aceștia reușesc să exfiltreze date despre dispozitiv și date din browser-ele web (inclusiv conturi de acces pe anumite platforme și parolele aferente), dar și situații în care sunt exfiltrate cantități considerabile de fișiere aflate pe sistemul informatic infectat.

6. CRIPTAREA DATELOR

În această etapă, aplicația *malware* începe procesul de criptare a datelor, acesta fiind diferit și dependent de nivelul de cunoștințe tehnice al atacatorului. Fișierele pot fi criptate individual, la nivel de sistem, sau pot fi criptate sisteme multiple din aceeași rețea. După finalizarea procesului de criptare, utilizatorii nu mai pot accesa datele și/sau nu mai pot utiliza dispozitivul infectat.

NOTA DE RĂSCUMPĂRARE

Ulterior criptării datelor, pe ecranul dispozitivului infectat este vizibilă nota de răscumpărare, prin care victimei i se solicită plata unei anumite sume, în criptomonedă, pentru a recăpăta accesul la propriile date. Există situații în care atacatorii solicită plata răscumpărării într-un anumit interval

attack. In certain cases, the encryption key is being generated on the C2 server, and then sent to the victim system. Afterwards, the file encryption process is being launched.

4. LATERAL MOVEMENT

Throughout ransomware campaigns, the lateral movement takes place in some cases, by means of an additional malware application previously installed by the attacker. Hardly any applications have network dissemination capacities after an IT system has been infected. However, attackers with advanced technical capabilities have developed the malware application known by cyber security experts as *CryptoWorms*, which has the ability to replicate itself within the network, and to encrypt the users' data, thus being capable of infecting all the devices within the same network.

5. DATA EXFILTRATION

Many cyber attackers involved in *ransomware* attacks resort to data exfiltration in order to coerce victims to pay ransom. There are cases when they succeed in exfiltrating data about the device and data from the web browsers (including access accounts on certain platforms and the associated passwords). But there are also situations when significant volumes of files are being exfiltrated from the infected system.

6. DATA ENCRYPTION

At this stage, the malware application starts the data encryption process, which differs from case to case and depends on the level of technical knowledge of the attacker. Files can be encrypted individually, at system level, or multiple systems can be encrypted within the same network. After the encryption process ends, the users cannot access the data and/or cannot use the infected device anymore.

THE RANSOM NOTE

Following data encryption, the ransom note can be seen on the display of the infected device, and the victim is required to pay a certain sum, in cryptocurrency, in order to regain access to his/her own data. In some cases, the attackers require the ransom to be paid within a certain period

de timp, în caz contrar, cheia de decriptare fiind ștearsă, datele exfiltrate fiind postate pe site-uri dedicate scurgerilor de date (*DLS*), forumuri *cybercrime* pentru comercializare, iar victima se află în imposibilitatea de a-și recupera datele.

Nota de răscumpărare marchează finalizarea procesului de criptare a datelor, fiind momentul în care victima conștientizează că nu își mai poate accesa datele.

Nota de răscumpărare reprezintă modul prin care atacatorii comunică, indirect, cu victimele, solicitând plata unei sume de bani, în criptomonede, pentru decriptarea datelor. Aceasta a suferit multiple îmbunătățiri de-a lungul timpului, atacatorii urmărind să identifice noi metode de determinare a victimelor să realizeze plățile.

Cele mai întâlnite tipuri de note de răscumpărare sunt:

- utilizarea unei casete de mesaj pe sistemul informatic al victimei;
- crearea unor fișiere de tip text în care este detaliat modul prin care poate fi plătită răscumpărarea;
- blocarea ecranului victimei și afișarea notei de răscumpărare.

În funcție de aplicația *malware* utilizată, detaliile cu privire la plata pentru răscumpărarea datelor sunt oferite în moduri diferite:

- suma în criptomonedă și portofelul electronic sunt menționate în nota de răscumpărare;
- atacatorii solicită victimelor să acceseze o adresă de Tor (.onion), unde se autentifică folosind o cheie menționată în nota de răscumpărare; ulterior, victimelor le este vizibilă nota de răscumpărare;
- atacatorii solicită victimelor să îi contacteze prin e-mail pentru a afla detalii despre modalitatea în care pot decripta datele proprii.

of time, failing which, the decryption key is being deleted, the exfiltrated data is being posted on dedicated leak sites (*DLS*), cybercrime forums for commercial purposes, and the victim is unable to retrieve his/her data. The ransom note marks the completion of the data encryption process, as the victims realize they can no longer access their data.

The ransom note is the way in which the attackers communicate, indirectly, with the victims, asking for a sum of money in cryptocurrency, in exchange for data decription. It has undergone many improvements over time, the attackers seeking to identify new methods of determining victims to make the payments.

The most common types of ransom notes are:

- using a message box on the victim's computer system;
- generating text files detailing how the ransom can be paid;
- locking the victim's screen and displaying the ransom note.

Depending on the malware application being used, payment details for data ransom are provided in different ways:

- the amount in cryptocurrency and the electronic wallet are specified in the ransom note;
- the attackers ask the victims to access a Tor address (.onion), where they authenticate using a key specified in the ransom note; subsequently, the victims can see the ransom note;
- the attackers ask the victims to contact them by e-mail to find out how they can decrypt their data.

EFECTE ȘI IMPACT

Atacurile de tip *ransomware* compromit toate cele trei valori fundamentale ale datelor, respectiv confidențialitatea, integritatea și disponibilitatea acestora.

Compromiterea acestor valori poate cauza prejudicierea companiilor din punct de vedere:

- reputațional (inclusiv pierderea clienților);
- financiar;
- legal.

În ceea ce privește entitățile publice, un astfel de atac poate genera efecte ce transcend prejudiciile financiare, existând posiblitatea apariției unor consecințe mai grave (cu titlu de exemplu, se poate face referire la o instituție medicală, la nivelul căreia un atac *ransomware* poate genera inclusiv pierderi de vieți omenești).

Indiferent de impactul atacurilor cu *ransomware*, **plata răscumpărării NU reprezintă o garanție a faptului că atacatorii vor furniza cheile de decriptare**, respectiv vor renunța la utilizarea datelor exfiltrate. Prin urmare, **plata răscumpărarii nu este recomandată în cazul unui atac de tip ransomware**.

CONSEQUENCES AND IMPACT

Ransomware attacks affect the three fundamental qualities of data: confidentiality, integrity and availability.

Affecting these values can inflict damage from several angles, such as:

- reputation (including the loss of clients);
- financial losses;
- legal repercursions.

Regarding public entities, such an attack can generate effects that go beyond financial losses, with more serious consequences being a risk (for instance, talking about a medical institution, a ransomware attack can even lead to human deaths).

Regardless of the impact of *ransomware* attacks, the payment of the **ransom is not a guarantee that the attackers will provide the decryption keys** and will waive the use of exfiltered data. Therefore, **the payment of the ransom is not recommended in case of a ransomware attack**.

PEISAJUL AMENINȚĂRII CIBERNETICE GENERATE DE **ATACURILE RANSOMWARE**

THE FRAMEWORK OF CYBERTHREATS GENERATED BY **RANSOMWARE ATTACKS**

Actorii cibernetici motivați financiar își diversifică în mod constant tacticile, tehnicile și procedurile utilizate, astfel încât să își maximizeze profiturile, utilizând un număr cât mai limitat de resurse.

În acest sens, atacurile cibernetice de tip *ransomware* reprezintă o soluție facilă, atât prin prisma gradului ridicat de comercializare a aplicațiilor *malware* specifice la nivelul forumurilor de criminalitate cibernetică, cât și prin prisma efectelor generate de acestea și a numărului mare de victime care achită răscumpărarea solicitată de atacatori.

INFO BOX

Deși la prima vedere atacurile ransomware par a fi o consecință a gradului ridicat de digitalizare a secolului XXI, acestea au fost observate pentru prima data la finalul anilor '80. Mai exact, primul atac ransomware a avut loc în 1989, când cercetătorul Joseph PoPP a participat la conferința găzduită de Organizația Mondială a Sănătății pentru combaterea SIDA.
Cercetătorul a distribuit participanților 20.000 suporturi de memorie de tip „floppy disk", care, conform acestuia, conțineau un chestionar privind cercetările referitoare la tema conferinței. În realitate, acestea conțineau o aplicație malware, care era instalată la nivelul sistemului informatic în momentul rulării suportului de memorie, dar nu era executată decât în momentul celei de-a 90-a pornire a sistemului. În acel moment, accesul utilizatorului la sistemul informatic era blocat, fiind solicitată transmiterea sumei de 189$ către o cutie poștală din Panama pentru deblocarea acestuia.

Din 1989 și până în prezent atacurile ransomware s-au dezvoltat, direct proporțional cu evoluțiile tehnologice și creșterea numărului de actori cibernetici motivați financiar. Concret, dacă la început atacurile *ransomware* vizau blocarea utilizării unui sistem informatic, **atacatorii s-au reorientat către criptarea datelor sau chiar exfiltrarea acestora pentru a șantaja victimele să achite recompensa solicitată**.

Financially motivated cyber players constantly diversify their tactics, techniques and procedures so as to maximize their profits, using as little resources as possible.

In this respect, *ransomware* cyber attacks are an facile solution, both because lots of specific malwares are marketed on cybercrime forums, and due to their effects and the large number of victims who pay the ransom requested by the attackers.

INFO BOX

Although at first sight the ransomware attacks appear to be a consequence of the high digitization of the 21st century, they were first observed in the late 80s." Specifically, the first ransomware attack took place in 1989, when researcher Joseph PoPP attended the conference hosted by the World Health Organization to fight AIDS.
The researcher distributed to the participants 20,000 "floppy disks", which according to him contained a questionnaire on the reserches related to the conference topic. In reality, they contained a malware, which was installed on the computer system at the time of running the memory support, but was executed only when the system was started for the 90th time. At that point, the user's access to the computer system was blocked, and he was requested to send the sum of $189 to a Panama mailbox to unblock it.

Since 1989, ransomware attacks have developed, directly proportional to the technological developments and the increase in the number of financially motivated cyber players. Specifically, if ransomware attacks initially aimed at blocking the use of a computer system, **the attackers have turned to data encryption or even their exfiltration in order to blackmail victims to pay the requested ransom.**

DOUBLE EXTORTION & TRIPLE EXTORTION

Astfel, actorii cibernetici au dezvoltat noi tactici privind derularea atacurilor *ransomware*, precum *double extortion*. Aceasta presupune exfiltrarea datelor din cadrul sistemelor informatice infectate, anterior criptării. Datele exfiltrate sunt utilizate ulterior de către atacatori pentru a amenința victimele cu publicarea/utilizarea acestor date, solicitând achitarea recompensei solicitate.

Mai mult, actorii cibernetici au identificat o nouă tactică de a obține beneficii financiare atât de la entitatea vizată de atacul *ransomware*, cât și de la beneficiarii serviciilor acestora sau alte entități partenere prin șantajarea acestora cu publicarea unor date confidențiale sau compromițătoare. Această tactică este cunoscută în mediul specialiștilor de securitate cibernetică sub denumirea de *triple extortion*.

Tot ca parte a *triple extortion*, există situații în care, ulterior exfiltrării și criptării datelor, atacatorii amenință victimele cu realizarea unui atac de tip DDoS asupra rețelelor și sistemelor informatice utilizate, în vederea blocării sau epuizării resurselor aferente.

RANSOMWARE-AS-A-SERVICE (RaaS)

Acest model de business, bazat pe principiul afilierii, presupune comercializarea, la nivelul forumurilor de criminalitate cibernetică, a aplicațiilor de tip *ransomware* precum și a unor instrumente și elemente de infrastructură necesare pentru derularea atacurilor. Acest fenomen permite derularea de atacuri *ransomware* inclusiv de către persoane care dețin capabilități și cunoștințe reduse.

Deseori, grupările care derulează atacuri ransomware inițiază programe de afiliere, prin care, persoanelor interesate li se pun la dispoziție toate instrumentele necesare în schimbul unei sume de bani sau al unui procent din veniturile obținute în urma atacurilor derulate.

DOUBLE EXTORTION &TRIPLE EXTORTION

Cyber actors have developed new tactics for conducting ransomware attacks, such as *double extortion*. This involves the exfiltration of the data from the infected IT&C systems prior to the encryption. The exfiltered data are then used by the attackers to threaten the victims with the publication/use of these data, asking for the required ransom to be paid.

Moreover, cyber actors have identified a new approach to obtain financial benefits both from the entity targeted by the ransomware attack, as well as the beneficiaries of their services or other partner entities by blackmailing them to publish confidential or compromising data. This method is known in the field of cyber security experts as “triple extortion”.

Also, as part of “triple extortion”, there are situations in which, after exfiltration and encryption of data, attackers threaten victims with a DDoS attack on the networks and computer systems used, in order to block or diminish the related resources.

RANSOMWARE-AS-A-SERVICE (RaaS)

This business model, based on affiliation principle, involves the commerce, at the level of cybercrime forums, of ransomware applications, as well as of some tools and infrastructure elements necessary for carrying out the attacks. This phenomenon allows ransomware attacks to be conducted even by people with limited skills and knowledge.

Often, groups that carry out ransomware attacks initiate affiliate programs, through which interested persons are provided with all the necessary tools in exchange for a specific sum of money or a percentage of the income obtained from the attacks.

INFO BOX

INIȚIATIVE INTERNAȚIONALE

Entitățile responsabile pentru combaterea atacurilor cibernetice de tip ransomware derulează constant inițiative menite să ajute victimele acestor tipuri de atacuri sau să prevină derularea de campanii ransomware.

Printre cele mai importante inițiative din anul 2021 a fost ***Inițiativa de Combatere a Ransomware*** (*Counter Ransomware Initiative - CRI*), propusă de Statele Unite ale Americii. România este unul dintre cele 31 de state care au participat la reuniunea multilaterală pe tema atacurilor cibernetice de tip ransomware, organizată în perioada 13-14.10.2021 de Consiliul Securității Naționale din SUA (NSC), sub coordonarea Casei Albe.

O altă inițiativă la nivel internațional este ***No More Ransom*** (*NMR*), creată la nivelul Centrului European dedicat criminalității cibernetice din cadrul Europol, printr-un parteneriat public-privat între unitatea dedicată criminalității cibernetice din cadrul poliției din Țările de Jos (*The National High Tech Crime Unit of the Netherlands' Police*) și compania de securitate cibernetică McAfee.

Rolul acestei inițiative este de a ajuta victimele atacurilor ransomware în decriptarea datelor, fără a fi nevoie să achite recompensa cerută de atacatori. Acesta a fost lansată încă din anul 2016, punând la dispoziția victimelor datele tehnice necesare decriptării fișierelor.

Până în prezent, peste 6 milioane de persoane au fost sprijinite pentru minimizarea efectelor negative ale unui atac *ransomware*, peste 170 de noi parteneri din mediul privat, public și academic alăturându-se inițiativei. Resursele puse la dispoziție pot fi accesate în 37 de limbi diferite și includ peste 120 de instrumente capabile să remedieze atacurile derulate cu aproximativ 150 de familii de *ransomware* diferite.

INFO BOX

INTERNATIONAL INITIATIVES

Entities responsible for countering ransomware cyber attacks are constantly running initiatives to help victims of these types of attacks or to prevent ransomware campaigns.

Among the most important initiatives in 2021 was the US ***Counter Ransomware Initiative*** (CRI). Romania is one of the 31 states that participated in the multilateral meeting on ransomware cyber attacks, organized on October 13–14, 2021 by the US National Security Council (NSC), coordinated by the White House.

Another international initiative is ***No More Ransom*** (*NMR*), created at the European Center for Cybercrime within the Europol, through a public-private partnership between the Dutch cybercrime unit (*The National High-Tech Crime Unit of the Netherlands' police*) and the cyber security company McAfee.

The role of this initiative is to help victims of ransomware attacks in decrypting data, without having to pay the reward requested by the attackers. It has been launched since 2016, providing victims with the technical data needed to decrypt files.

So far, more than 6 million people received support to minimize the negative effects of a ransomware attack, with more than 170 new private, public and academic partners joining the initiative. The available resources can be accessed in 37 different languages and include over 120 tools capable of fixing attacks with about 150 different ransomware families.

APLICAȚII MALWARE
UTILIZATE ÎN ATACURI DE TIP RANSOMWARE

MALWARE APPLICATIONS
USED IN RANSOMWARE ATTACKS

CONTI

***Ransomware*-ul CONTI** este dezvoltat de gruparea de criminalitate cibernetică Wizard, fiind identificat pentru prima dată la începutul anului 2020. Acesta este cunoscut pentru viteza cu care dezvoltatorii actualizează codul sursă, în prezent existând o creștere cu 27,3% a numărului de variante Conti.

Ransomware-ul este comercializat în sistem *RaaS* și este operat de diferiți atacatori.Aplicația poate fi controlată manual de către un atacator și folosește tehnica de *double extortion*.

Vectorul de infecție este, de obicei, un e-mail de tip *phishing* care conține atașamente cu conținut *malware*, ce include adesea un script integrat (preponderent în macrocomenzile unui document Word), utilizat pentru a crea o conexiune de la sistemele vizate către serverul de comandă și control (C2). Având o conexiune activă, atacatorii pot descărca ulterior *ransomware*-ul Conti.

La sfârșitul lunii februarie 2022, un cercetător în domeniul securității cibernetice a publicat pe contul de Twitter *@contileaks* o serie de date interne ale grupării, reprezentând conversații dintre membrii. Ulterior, acesta a continuat publicarea de date, incluzând elemente de infrastructură de atac, identități reale ale atacatorilor și portofele electronice utilizate.

Cercetătorul care a publicat datele este de origine ucraineană, acțiunea sa reprezentând modul prin care își susține țara în cadrul conflictului ruso-ucrainean, dat fiind faptul că gruparea anunțase anterior că va derula operațiuni pentru susținerea Rusiei.

CONTI

CONTI ransomware is developed by the cybercrime group Wizard, being identified for the first time in early 2020. It is known for the speed with which developers update the source code; currently there is a 27.3% increase in the number of Conti variants.

The ransomware is marketed in the *RaaS* system and is operated by various attackers.The application can be manually controlled by an attacker and uses the double extortion technique.

The infection vector is usually a phishing email that contains attachments with malware content, which often includes an integrated script (mostly in the macros of a Word document), used to create a connection from the targeted systems to the command and control server. With an active connection, attackers can later download Conti ransomware.

In late February 2022, a cyber security researcher posted on the Twitter page *@contileaks* a series of internal data of the group, representing conversations among members. Subsequently, it further published data, including elements of the attack infrastructure, real identities of the attackers and the electronic wallets that were used. The researcher who published the data is of Ukrainian origin, this action being his way of supporting his country in the Russian-Ukrainian conflict, given that the group had previously announced that it would carry out operations to back Russia.

REvil

Ransomware-ul REvil a fost observat pentru prima dată în 2019, fiind inclusiv disponibil în sistem RaaS. În funcție de preferința atacatorului care îl achiziționează, REvil poate fi distribuit prin mesaje de *phishing* sau prin tehnici specifice, precum utilizarea unor *kit*-uri de exploatare sau a unor aplicații *malware* de tip *backdoor*, respectiv compromiterea credențialelor RDP prin *brute-force*.

După criptarea datelor, atacatorii afișează pe sistemele infectate nota de răscumpărare, suma solicitată variind între 1.500 de dolari și 42 de milioane de dolari, în funcție de specificul victimei. Actorii cibernetici solicită până la 9% din veniturile anuale ale victimei, iar în situația în care plata nu este realizată la timp, suma se dublează.

În 2020, REvil a introdus *double extortion* în strategia de atac, prin urmare, dacă cerințele nu sunt îndeplinite, aceștia amenință victima cu publicarea datelor furate pe site-ul propriu, "*The Happy Blog*".

După ce a fost printre **cele mai active familii de ransomware în 2021** (17,8% dintre atacurile *ransomware* din 2021 au fost cu o variantă REvil), **atacurile cu REvil au fost oprite o perioadă**, ca urmare a unor operațiuni de arestare a unor operatori REvil derulate în perioada noiembrie 2021 - februarie 2022. Operațiunile au fost derulate atât de către o echipă comună formată din reprezentanți ai Europol, Eurojust și INTERPOL, cât și de către Serviciul Federal de Securitate din Rusia (FSB), la cererea autorităților americane.

Cu toate acestea, în aprilie 2022, a fost observată reluarea atacurilor cibernetice cu aplicația *malware* Revil, atacatorii creându-și o infrastructură nouă și dezvoltând o altă modalitate de criptare.

REvil

The REvil ransomware was first noted in 2019 and it is also available as a RaaS. Depending on the attacker's wish, REvil can be distributed through phishing messages or other specific techniques, such as using exploit kits or backdoor malware applications, namely by compromising the RDP credentials by brute-force.

After the encryption of the data, the attackers display the ransom note on the infected systems, the amount varying between USD 1500 and 42 million depending on the nature of the victim. Cyber actors demand up to 9% of the victim's yearly income and, if the payment is not made on time, the amount is doubled.

In 2020, REvil introduced double extortion in its attack strategy. Thus, if their demands are not met, they threaten the victim with publishing the stolen data on their own site, "The Happy Blog".

After it became one of **the most active ransomware families of 2021** (17.8% of the 2021 *ransomware* attacks used a REvil version), **the REvil attacks stopped for a while**, because of operations carried out in November 2021 – February 2022 to arrest REvil operators. The operations were carried out both by a joint team made up of Europol, Eurojust and INTERPOL representatives, as well as by the Russian Federal Security Service (FSB), at the request of American law enforcement agencies.

However, in April 2022, the cyber attacks using the Revil malware application resumed, the attackers creating a new infrastructure and developing a new encryption method.

HIVE

A fost observat pentru prima dată în iunie 2021, fiind utilizat în atacuri asupra sectorului de sănătate, organizațiilor non-profit, distribuitorilor de bunuri/servicii și furnizorilor de energie.

Hive a fost dezvoltat astfel încât să infecteze cu ușurință sistemele informatice indiferent de sistemul de operare al acestora: Windows, Linux sau macOS.

Vectorii de infecție utilizați de Hive sunt ***e-mailurile de tip phishing cu atașamente ce conțin malware*** și exploatarea RDP-ului.

De asemenea, atacatorii folosesc ***tactica de double extortion***, amenințând cu publicarea datelor victimei pe site-ul TOR propriu, „*HiveLeaks*".

LOCKBit

Cunoscut anterior sub numele de ABCD *ransomware*, LockBit a fost identificat pentru prima dată în 2019 și a fost îmbunătățit treptat în ultimii ani pentru a deveni una dintre cele mai ingenioase familii de *ransomware* în prezent. Versiunea LockBit 2.0 este cunoscută pentru faptul că prezintă cel mai rapid și eficient proces de criptare a fișierelor. Ulterior, la finalul lunii iunie 2022 operatorii LockBit au dezvoltat și comercializat versiunea 3.0 a aplicației *malware*.

Atacatorii care operaționalizează LockBit recrutează angajați din companii de securitate cibernetică și organizează concursuri pe forumuri *cybercrime* în scopul angrenării hackerilor talentați în procesul de identificare de posibile vulnerabilități ale malware-ului.

Fișierul de criptare executabil este disimulat într-un fișier tip imagine (cu extensia .PNG). LockBit are capabilități de mișcare laterală la nivelul unei rețele, prin instrumente tipice, cum ar fi

HIVE

It was first noted in June 2021, when it was used in attacks against the public health sector, Non-Government Organizations, goods/services distributors and energy suppliers.

Hive was developed to easily infect IT systems regardless of their operating system: Windows, Linux or macOS.

The infection vectors used by Hive are **phishing e-mails with attachments containing malware** and by exploiting the RDP.

Also, the attackers **use the double extortion tactic** and threaten to publish the victim's data on their own TOR site," HiveLeaks".

LOCKBit

Previously known as ABCD ransomware, LockBit was first identified in 2019 and it has been gradually improved over the last years so that it became one of the most ingenious ransomware families to date. The LockBit 2.0 version is known for the fact that it offers the fastest and most efficient file encryption process. During the later June 2022, LockBit operators developed and commercialized 3.0 version of the malware.

The attackers that operate LockBit recruit employees from cyber security companies and organize competitions on cybercrime forums in order to recruit talented hackers and identify possible vulnerabilities in the malware.

The executable encryption file is concealed in an image file (with the extension .PNG). LockBit has lateral movement capabilities it can use within a network, such as Windows PowerShell and

Windows PowerShell și SMB (Server Message Block). În faza inițială, atacatorul infectează manual un singur sistem informatic, iar ulterior *malware*-ul se răspândește la nivelul rețelei, fără intervenție umană.

ALPHV BlackCat

Cunoscut anterior ca DarkSide/BlackMatter, ALPHV BlackCat este un *ransomware* observat la mijlocul lunii noiembrie 2021 ce poate fi achiziționat în sistem RaaS și poate fi adaptat cu ușurință de atacatori pentru a rula atât pe sistemul de operare Windows, cât și pe Linux.

Atacatorii ce utilizează *ransomware*-ul ALPHV BlackCat folosesc inclusiv tactica **triple extortion.** În numeroase situații, dacă victima refuză să se conformeze cerințelor atacatorului, acesta insistă ca victima să plătească răscumpărarea, amenințând, în caz contrar, că va efectua un atac DDoS asupra infrastructurii vizate.

Canalul de comunicare utilizat de ALPHV BlackCat pentru negocieri este diferit în comparație cu practicile obișnuite, deoarece chat-urile pot fi accesate numai de către cei care dețin un *token* de acces sau un ID al notei de răscumpărare, cu scopul de a evita implicarea unor terți.

KHONSARI

Khonsari este unul dintre primele *ransomware*-uri care au exploatat vulnerabilitatea Log4Shell, descoperită la jumătatea lunii decembrie 2021.

Log4Shell este o vulnerabilitate software a Apache Log4j 2, o bibliotecă Java populară pentru jurnalizarea mesajelor de eroare în aplicații. Exploatarea vulnerabilității permite unui atacator să preia controlul de la distanță asupra unui dispozitiv de pe internet care rulează anumite versiuni de Log4j 2. În comparație cu alte aplicații *ransomware*, Khonsari nu este disponibilă în sistem RaaS, dezvoltatorii aplicației fiind singurii care operaționalizează atacurile.

SMB (Server Message Block). Initially, the attacker manually infects a single IT system, and later the malware spreads within the network, without human intervention.

ALPHV BlackCat

Previously known as DarkSide/BlackMatter, ALPHV BlackCat is a ransomware observed in mid-November 2021 which can be purchased as a RaaS and can be easily adapted by the attackers to run both on Windows and Linux operating systems.

The attackers that use the ALPHV BlackCat ransomware also use the **triple extortion** tactic. On numerous occasions, if the victim refuses to comply to the attacker's demands, the latter insists that the victim pay the ransom, or else they carry out a DDoS attack on the targeted infrastructure.

The communication channel used by ALPHV BlackCat for negotiations is unlike the usual practices because the chats can be accessed only by those who have an access token or the ID of the ransom note, with the purpose of avoiding third parties from getting involved.

KHONSARI

Khonsari is one of the first ransomwares that have exploited the Log4Shell vulnerability, discovered mid-December 2021.

Log4Shell is a software vulnerability of Apache Log4j 2, a Java library popular for its applications error log. By exploiting vulnerabilities, an attacker can remotely take over the control of a device on the Internet that runs certain Log4j 2 versions. Unlike other ransomware applications, Khonsari is not available as a RaaS. The application's developers are the only ones that can carry out attacks.

ATACURI DISTRUCTIVE
CU RANSOMWARE

DESTRUCTIVE
RANSOMWARE **ATTACKS**

INDUSTRIA DE PETROL ȘI GAZE

În luna mai 2021, compania americană **Colonial Pipeline**, cel mai mare operator de conducte petroliere din Statele Unite ale Americii și-a oprit activitatea ca urmare a unui atac cibernetic de tip *ransomware* cu aplicația *malware* Darkside. Activitatea companiei a fost întreruptă pentru aproximativ 5 zile, ceea ce a condus la o criză a combustibilului pe coasta estică a SUA, a determinat schimbarea zborurilor pentru companii aeriene și a destabilizat economia țării.

Actorul cibernetic care a operaționalizat atacul asupra Colonial Pipeline a fost gruparea Darkside, scopul fiind unul pur financiar, fără a urmări afectarea infrastructurii fizice a companiei. În urma atacului a fost exfiltrată o cantitate considerabilă de date (100 GB).

Pentru a putea obține cheia de decriptare necesară reluării proceselor de business, compania a plătit o răscumpărare de 5 milioane de dolari în BTC. Ulterior, în luna iunie 2021, FBI a reușit recuperarea, dintr-un portofel electronic utilizat de atacatori, a sumei de 4,4 milioane de dolari din răscumpărarea plătită de Colonial Pipeline.

SECTORUL SĂNĂTĂȚII

În luna mai 2021, **HSE (*Health Service Executive*) din Irlanda**, responsabilă pentru furnizarea serviciilor de sănătate publică în spitale și comunități din Irlanda, a fost victima unui atac cibernetic de tip *ransomware* cu aplicația *malware* Conti. Aplicația *malware* a fost distribuită printr-un e-mail de tip *phishing*, al cărui atașament a fost deschis de un angajat al HSE. În urma atacului a fost limitat accesul la dosarele medicale de diagnosticare, cauzând timpi de răspuns lenți la vizitele medicale. De asemenea, au fost exfiltrate aproximativ 700 GB de date. Atacatorii au solicitat o răscumpărare în valoare de 20 de milioane de dolari, pe care HSE a refuzat să o plătească.

OIL AND GAS INDUSTRY

In May 2021, the American company **Colonial Pipeline**, the largest oil pipeline operator in the United States, stopped its activity as a result of a ransomware cyber attack with the malware Darkside. The company's activity was interrupted for about 5 days, which led to a fuel crisis on the United States' East Coast, caused airlines to change their flight schedule and destabilized the country's economy.

The cyber actor that perpetrated the attack against Colonial Pipeline was a group called Darkside and the purpose was a purely financial one, with no intention to damage the company's physical infrastructure. The hackers managed to exfiltrate a considerable amount of data (100 GB).

In order to obtain the decryption key needed to resume its business processes, the company paid 5 million dollars in BTC. Subsequently, in June 2021, the FBI managed to recover, from an electronic wallet used by the attackers, the amount of 4.4 million dollars from the ransom paid by Colonial Pipeline.

HEALTHCARE INDUSTRY

In May 2021, **the Irish HSE (Health Service Executive)**, responsible for providing healthcare services to Irish hospitals and communities, was the victim of a ransomware cyber attack with the malware application Conti. The malware was distributed via a phishing e-mail, whose attachment was opened by an HSE employee. Following the attack, access to medical records was limited, causing slow response times to medical visits. At the same time, 700 GB of data was exfiltrated. The attackers demanded a 20-million-dollar ransom, which the HSE refused to pay.

SECTORUL IT

În iulie 2021, compania **Kaseya** a fost victima unui atac ransomware de tip „*supply chain*”, în care a fost utilizată aplicația *malware* REvil.

Atacatorii **au exploatat o vulnerabilitate de tip *zero-day*** a *software*-ului Kaseya Virtual System Administrator (VSA), o platformă bazată pe *cloud* care permite furnizorilor să efectueze gestionarea *patch*-urilor și monitorizarea clienților.

Inițial, **atacatorii au reușit să ocolească mecanismele de autentificare** în interfața web a serverului Kaseya VSA și au obținut o sesiune validă. Ulterior, aceștia au realizat un atac de tip SQL injection, în scopul transmiterii de actualizări cu conținut *malware* la nivelul serverului.

În urma atacului, operatorii REvil au solicitat o răscumpărare de 70 de milioane de dolari în BTC, una dintre cele mai mari răscumpărări cerute până în prezent.

Atacul a afectat sute de companii la nivel global. După nouăsprezece zile de la atac, Kaseya a obținut cheia universală de decriptare, fără a plăti răscumpărarea. De asemenea, toți clienții compromiși au primit sprijin pentru decriptarea propriilor fișiere.

IT INDUSTRY

In July 2021, the company **Kaseya** was the victim of a “supply chain” ransomware attack using the malware application REvil.

The attackers **exploited a zero-day vulnerability** in the Kaseya Virtual System Administrator (VSA), a cloud-based platform that allows vendors to manage patches and monitor customers.

Initially, **the attackers managed to bypass the authentication mechanisms** on the web interface of Kaseya’s VSA server and obtained a valid session. Subsequently, they carried out a SQL injection attack, in order to send updates with malware content to the server.

Following the attack, the REvil operators demanded a 70-million-dollar ransom in BTC, one of the **largest ransoms ever demanded**.

The attack affected hundreds of companies worldwide. Nineteen days after the attack, Kaseya obtained the universal decryption key, **without paying** the ransom. At the same time, all compromised customers received support in order to decrypt their own files.


TENDINȚE DE EVOLUȚIE ALE
FENOMENULUI RANSOMWARE.
EVALUARE & RECOMANDĂRI
EVOLUTIONARY TRENDS OF THE
RANSOMWARE PHENOMENON.
EVALUATION & RECOMMENDATIONS

Atacurile cibernetice de tip *ransomware* s-au menținut la un nivel ridicat în 2021 și în prima parte a anului 2022, fiind exploatat contextul pandemic pentru asigurarea succesului campaniilor cibernetice. Având în vedere că acest tip de atac cibernetic a generat venituri consistente actorilor cibernetici motivați financiar, este de așteptat ca aceștia să continue să deruleze campanii *ransomware*, având același scop: obținerea beneficiilor financiare.

În același timp, se poate estima că actorii cibernetici motivați financiar **vor exploata contextul internațional generat de conflictul dintre Federația Rusă și Ucraina**, în vederea asigurării compromiterii inițiale a unor sisteme informatice,ca parte a unor campanii *ransomware*.

Numărul ridicat de atacuri cibernetice de tip *ransomware* este o consecință a disponibilității crescute a acestui tip de malware la nivelul forumurilor de criminalitate cibernetică. Concret, **comercializarea acestor aplicații în sistem *Ransomware-as-a-Service* generează posibilitatea menținerii acestor campanii cibernetice la un nivel ridicat,** din perspectiva obținerii unor beneficii financiare ridicate cu utilizarea de resurse reduse.

Cu toate acestea, pe parcursul anului 2021 a fost observată o evoluție a atacatorilor cibernetici ce derulează campanii *ransomware* în ceea ce privește tacticile, tehnicile și procedurile utilizate. Mai exact, tranziția de la atacurile *ransomware* clasice la adoptarea tacticii *double extortion*, iar mai apoi chiar *triple extortion*,a generat creșterea presiunii exercitate de atacatorii cibernetici asupra victimelor în vederea convingerii acestora pentru a achita suma solicitată. Întrucât creșterea gradului de amenințare asupra victimelor generează un avantaj semnificativ atacatorilor cibernetici, este de așteptat ca atacurile cibernetice de tip *double extortion* și *triple extortion* să se mențină pe un trend ascendent în perioada următoare.

SOLUȚII DE CONTRACARARE A ATACURILOR RANSOMWARE. RECOMANDĂRI DE SECURITATE CIBERNETICĂ

- realizarea periodică de scanări la nivelul rețelei în scopul determinării unor potențiale stații infectate, respectiv izolarea acestora;
- implementarea unei politici de schimbare periodică a parolelor, precum și stabilirea unui nivel ridicat de complexitate al acestora, care să implice utilizarea obligatorie de simboluri și cifre;
- activarea, acolo unde este posibil, a autentificării în doi pași;
- utilizarea de soluții antivirus, anti-*ransomware*, *firewall* și mecanisme de filtrare web;
- realizarea zilnică de copii de siguranță (BACK-UP) pentru principalele sisteme din rețea care stochează date, dar și pentru serverele care găzduiesc domenii importante;

The number of ransomware attacks remained high in 2021 and in early 2022, taking advantage of the pandemic context to ensure the success of cyber campaigns. Given that this type of cyber attack has generated consistent revenue for financially motivated cyber actors, it is expected that they will continue to run ransomware campaigns with the same goal: to obtain financial benefits.

At the same time, we estimate that financially motivated cyber actors **will exploit the international context generated by the conflict between the Russian Federation and Ukraine** in order to compromise computer systems, as part of ransomware campaigns.

The high number of ransomware attacks is a consequence of the increased availability of this type of malware on cybercrime forums. In other words, **the marketing of these applications based on the Ransomware-as-a-Service model generates the possibility of maintaining these cyber campaigns at a high level,** from the perspective of obtaining high financial benefits while using limited resources.

However, in 2021 an evolution of cyber attackers conducting ransomware campaigns was noted in terms of tactics, techniques and procedures used. More precisely, the transition from classic ransomware attacks to the adoption of *double extortion* tactics, and later even *triple extortion*, has led to an increase in the pressure exerted by cyber attackers on victims in order to convince them to pay the required amount. **As the increasing threat to victims generates a significant advantage for cyber attackers**, it is expected that cyber attacks such as *double extortion* and *triple extortion* will continue on an upward trend in the coming period.

SOLUTIONS TO COUNTER RANSOMWARE ATTACKS. CYBER SECURITY RECOMMENDATIONS

- periodic network scans meant to identify and also isolate potential infected workstations;
- implementing a policy of periodic password changes, as well as establishing a high level of complexity involving the mandatory use of symbols and numbers;
- enabling two-step authentication where possible;
- use of antivirus, anti-*ransomware*, firewall and web filtering solutions;
- making daily backups for the main network systems that store data, but also for the servers that host important domains;

- folosirea celui mai redus nivel de privilegii necesare pentru executarea acțiunilor/operațiilor, atât pentru aplicații, cât și pentru utilizatori;
- în cazul în care este utilizat un router Wi-Fi pentru conectarea la internet, este necesară schimbarea parolei inițiale, actualizarea *firmware*-ului și instalarea *patch*-urilor de securitate;
- utilizarea unui furnizor de servicii de e-mail ce oferă o filtrare puternică anti-*spam*;
- actualizarea permanentă a aplicațiilor și sistemelor utilizate pentru eliminarea posibilelor vulnerabilități;
- instruirea permanentă a angajaților cu privire la necesitatea respectării politicilor de securitate cibernetică;
- stabilirea unui plan de răspuns la incidente de securitate cibernetică în vederea creșterii nivelului de reziliență a rețelelor și sistemelor informatice din cadrul instituției.

- using the lowest level of privileges required to perform actions/operations, both for applications and users;
- if a WI-FI router is used to connect to the internet, it is necessary to change the initial password, update the firmware and install security patches;
- using an e-mail service provider that offers strong anti-spam filtering;
- constantly updating the applications and systems used to eliminate possible vulnerabilities;
- continuous training of employees on the need to comply with cyber security policies;
- establishing a response plan for cyber security incidents in order to increase the resilience level of the network and IT systems within the institution.

WWW.SRI.RO/CYBERINT