Raport de țară

CRIMINALITATEA CIBERNETICĂ

ÎN ROMÂNIA ÎN 2019. ORIENTĂRI PENTRU 2020

Country Report

CYBERCRIME

IN ROMANIA IN 2019. TRENDS FOR 2020

DE CE ACEST MATERIAL

Raportul face parte din demersurile Serviciului Român de Informații/Centrului Național CYBERINT și ale companiei MANDIANT, de dezvoltare a parteneriatului public-privat. Doar printr-o abordare *whole of society* pot fi prevenite și contracarate amenințările din spațiul cibernetic, printre cele mai prolifice și complexe la adresa securității naționale.

Plus-valoarea raportului constă în faptul că reunește, într-o inițiativă unică până la acest moment, viziunea unui serviciu de informații cu cea a unei organizații private, asupra securității cibernetice naționale, fiecare contribuind cu experiența și perspectiva proprii la cunoașterea și investigarea acelorași amenințări din sfera criminalității cibernetice.

Pentru obținerea unui profit considerabil, atacatorii, grupări sau indivizi, distribuie *malware*-ul fără discriminare, unui număr cât mai mare de potențiale victime - sistemele IT&C ale organizațiilor publice, private și chiar ale utilizatorilor individuali.

Astfel, prin cooperare și schimb de expertiză putem recupera din avantajul pe care atacatorii cibernetici îl au în acest moment față de experții în securitate cibernetică, care trebuie să protejeze interesele organizației pe care o reprezintă, respectiv ale statului din care fac parte.

În fiecare zi “ne luptăm” cu inventivitatea, timpul și resursele pe care atacatorii le alocă dezvoltării de noi capabilități cibernetice, astfel că demersul de colaborare și conlucrare este unul necesar și binevenit.

THE REASON

This report is part of the endeavors the Romanian Intelligence Service/ CYBERINT National Center and MANDIANT are undertaking in order to develop the public-private partnership. Only through a *whole of society* type of approach can cyber threats be prevented and countered, as they are some of the most prolific and complex threats to national security.

The added value of this report is in reuniting, in a so far unique initiative, the perspective of an intelligence service and that of a private entity on national cyber security, each of them contributing with their experience and their own view to identifying and investigating the same cyber crime threats.

In order to gain a considerable profit, the attackers, groups or individuals, distribute malware indiscriminately to the largest possible number of potential victims - IT&C systems of public or private organizations and even individual users.

Therefore, through cooperation and exchange of expertise, cyber security experts who must protect the interests of the organization they represent, namely the interests of their country, can catch up with cyber attackers.

Each day “we fight” against the inventiveness, time and resources the attackers allocate to developing new cyber capabilities, so the initiative to cooperate and work together is a welcome and necessary one.

CARE ESTE SCOPUL RAPORTULUI

Fără a avea pretenția de a fi inclus în acest raport, în mod exhaustiv, toate amenințările cibernetice motivate financiar cu care s-a confruntat România în 2019, materialul este un pas înainte în realizarea acestui deziderat, intenția fiind de a oferi experților în domeniu, din mediul privat și cel public, autorităților de aplicare a legii, dar și publicului larg, un instrument util în cunoașterea și gestionarea acestor provocări.

CUM A FOST GÂNDIT

Deoarece spațiul cibernetic nu ține cont de granițele teritoriale, iar securitatea cibernetică a unui stat nu poate fi abordată independent de situația de la nivel internațional, prima secțiune a raportului prezintă cele mai relevante fenomene care au avut loc în 2019 pe mapamond, riscuri și vulnerabilități în implementarea anumitor tehnologii.

A doua secțiune abordează principalele fenomene și *malware*-uri cu care s-au confruntat mediul public și organizațiile private din țara noastră.

Pornind de la aspectele observate în anul precedent, ultima parte a raportului prezintă elemente ale modului de acțiune a actorilor cibernetici motivați financiar, dar și câteva orientări pentru 2020.

THE PURPOSE

Without claiming to have comprehensively listed in this report all the financially motivated cyber threats Romania faced in 2019, this document is a step forward in achieving this, with the intent of providing public and private experts in this field, law enforcement agencies and the public at large with a useful tool in identifying and managing these challenges.

THE STRUCTURE

Since cyber space is not bound by territorial frontiers and the cyber security of a country cannot be addressed independently of the international situation, the first section of the report encompasses the most relevant phenomena that occurred in 2019 worldwide, risks and vulnerabilities in the implementation of certain technologies.

The second section addresses the main phenomena and malwares that public and private organizations in our country have faced.

Building on aspects observed the previous year, the last part of the report presents modus operandi elements of financially motivated cyber actors, as well as a few guidelines for 2020.

1. CONTEXT GLOBAL ÎN DOMENIUL CRIMINALITĂȚII CIBERNETICE

Grupările de criminalitate cibernetică motivate financiar vizează, de regulă, obținerea de date de autentificare ale utilizatorilor, inclusiv date bancare, compromiterea sistemelor POS și ATM, accesarea portofelelor electronice, derularea de atacuri cu *ransomware* etc. și valorificarea acestor activități pentru obținerea de beneficii materiale.

Pentru realizarea acestui scop sunt utilizate mijloace diverse. Astfel, indivizii sau grupările de criminalitate cibernetică acționează, cel mai adesea, prin derularea de campanii de phishing și spear-phishing, distribuirea de aplicații malware de tip *infostealer, keylogger, loader* și *worm*, troieni bancari, *ransomware, cryptominer* etc.

Criminalitatea cibernetică a avut și are, per total, un **impact major** la adresa mai multor sectoare ale vieții sociale: financiar-bancar, sănătate, administrație publică, învățământ etc.

> Spre exemplu, costurile totale ale gestionării efectelor unui atac cibernetic cu *ransomware,* incluzând aici și costurile de remediere, sunt, de fapt, de câteva ori mai mari decât recompensa efectivă solicitată.

1. CYBER CRIME GLOBAL CONTEXT

Financially motivated cyber crime groups usually aim at obtaining user authentification data, including banking data, compromising POS and ATM systems, accessing electronic wallets, carrying out ransomware attacks, etc. and monetizing these activities in order to gain material benefits.

Various means are used in order to reach this goal. Thus, cyber crime groups or individuals mostly act by carrying out phishing and spear-phishing campaigns, distributing malware applications such as infostealer, keylogger, loader and worm, banking trojans, ransomware, cryptominer, etc.

Cyber crime has always had and continues to have an overall **major impact** on several parts of our social life: financial, banking, health, public administration, education, etc.

> For example, the total costs of managing the effects of a ransomware cyber attack, including remedial costs, are, in fact, several times higher than the actual demanded ransom.

2019 a fost marcat de numeroase atacuri ransomware care au afectat, cu precădere, organizații din domeniul sănătății, instituții guvernamentale, infrastructuri critice, servicii publice și instituții de învățământ. Aceste sectoare au fost vizate având în vedere importanța pe care o au în societate, dar și din cauza faptului că atacatorii le-au perceput ca având o probabilitate mai mare de a da curs cererii de recompensă pentru a restabili accesul complet la date și la sistemele IT&C afectate.

DOMENII VIZATE DE GRUPĂRILE DE CRIMINALITATEA CIBERNETICĂ MOTIVATE FINANCIAR

INDUSTRIA FINANCIAR-BANCARĂ

Cuprinde numeroase tipuri de organizații: bănci, instituții de credit, de brokeraj, procesatori de plăți, companii de asigurări etc. **Sistemele și rețelele IT&C ale acestor instituții se confruntă cu o amenințare constantă din partea actorilor cibernetici motivați financiar**, fie că sunt grupări cu capabilități și instrumente foarte sofisticate, fie entități oportuniste, care derulează atacuri cu un nivel de complexitate redus.

Acești actori urmăresc:

- obținerea accesului neautorizat la conturi,
- furtul de credențiale,
- date personale de identificare sau alte informații sensibile (business info),
- furtul de date privind carduri bancare,
- fraude derulate prin accesarea ilegală a rețelei interbancare SWIFT,

2019 saw numerous ransomware attacks which mainly affected public-health organizations, government institutions, critical infrastructures, public services and education establishments. These sectors were targeted both because of their importance in society and because of the fact that the attackers perceived them as most likely to comply with the ransom demand in order to re-establish full access to data and affected IT&C systems.

SECTORS TARGETED BY FINANCIALLY MOTIVATED CYBER CRIME GROUPS

FINANCIAL AND BANKING INDUSTRY

It encompasses numerous types of organizations: banks, credit institutions, brokers, payment processors, insurance companies, etc. **The IT&C systems and networks of these institutions face the constant threat of financially motivated cyber actors**, whether groups with highly sophisticated capabilities and tools, or opportunistic entities which carry out low complexity attacks.

These actors' purpose is:

- gaining unauthorized access to accounts,
- credential theft,
- personal identification data or other sensitive information (business info),
- stealing credit card information,
- frauds by illegally accessing the SWIFT banking network,

- compromiterea ATM-urilor pentru retragerea neautorizată de fonduri,
- transferul de fonduri de la o organizație victimă la un cont controlat de atacatori,
- manipularea criptomonedelor și/sau a burselor etc.

Dintre **grupările care au derulat în 2019 atacuri cibernetice** asupra unor instituții din domeniul financiar-bancar menționăm: FIN6, FIN7, FIN9, FIN10, Cobalt Group, MoneyTaker, iar dintre cele mai distribuite familii de malware au fost Emotet, Nanocore, Pony, LokiBot, Chanitor, GandCrab, Formbook, Dridex, Remcos, AZORult, Qakbot.

> În decembrie 2019, în urma unei investigații derulate în comun, autoritățile americane și cele britanice au luat o serie de măsuri publice cu privire la membrii grupării Evil Corp și la asociați ai acestora, care au dezvoltat și distribuit *malware*-ul DRIDEX, care a cauzat pierderi de milioane de USD instituțiilor financiare din SUA și de la nivel internațional. Aceste măsuri includ: blocarea fondurilor și resurselor deținute de membrii grupării în SUA, interzicerea și sancționarea celor care facilitează tranzacții cu aceste persoane, companiile deținute sunt de asemenea supuse sancțiunilor, iar pentru informații care pot conduce la prinderea liderului grupării este oferită o recompensă consistentă.

Numeroasele raportări publice de incidente și atacuri asupra unor companii, organizații și instituții, la nivel global, indică faptul că **aplicațiile de furt de credențiale** cu cea mai mare prezență la nivel internațional, în 2019, au fost Emotet, Lokibot, Formbook, Nanocore, Pony, Remcos, Azorult și Goznym.

Din analiza statistică a acestor raportări publice, a reieșit că Emotet, Formbook și Nanocore au vizat furtul de credențiale din sisteme și rețele IT&C de pe întreg globul, fără discriminare.

- compromising ATMs for unauthorized cash withdrawals,
- the transfer of funds from a victim organization to an account controlled by attackers,
- manipulating cryptocurrencies and/or stock markets, etc.

Among the **groups that carried out cyber attacks in 2019** on financial and banking institutions were: FIN6, FIN7, FIN9, FIN10, Cobalt Group, MoneyTaker, and some of the most distributed malware families were Emotet, Nanocore, Pony, LokiBot, Chanitor, GandCrab, Formbook, Dridex, Remcos, AZORult, Qakbot.

> In December 2019, following a joint investigation, the US and British authorities implemented a series of public measures regarding Evil Corp group members and their associates, who developed and distributed the DRIDEX malware, which resulted in losses of millions of US dollars for American and international financial institutions. These measures include: blocking funds and resources owned by group members in the US, prohibiting transactions and sanctioning those who facilitate them with these persons. The companies they own are also subjected to sanctions, and there is a substantial reward for any information that can lead to the apprehension of the group leader.

Numerous public reports regarding incidents and attacks on companies, organizations and institutions worldwide indicate that **the credential theft applications** most present internationally in 2019 were Emotet, Lokibot, Formbook, Nanocore, Pony, Remcos, Azorult and Goznym.

The statistics of these public reports show that Emotet, Formbook and Nanocore focused on credential theft from IT&C systems and networks worldwide, indiscriminately.

De asemenea, la nivel global, **atacurile asupra POS-urilor** rămân una dintre metodele principale de compromitere și sustragere a datelor cărților de credit și de debit. De foarte multe ori, atacatorii nu se opresc aici, ci încearcă să se infiltreze inclusiv în rețeaua la care este conectat POS-ul. Potențialii atacatori au oportunități suplimentare de acces atunci când actualizarea software-ului POS-urilor se realizează prin conexiune la Internet sau se realizează de la distanță, de către companiile care asigură mentenanța.

Malware-urile observate în atacuri asupra POS-urilor sunt FastPOS, Alina POS, FrameworkPOS (TRINITY), Backoff POS, BlackPOS, BLUESTEAL, Dexter POS, FIENDCRY, LockPOS, ModPOS, NitlovePOS, TRESOCHO, RAMPAGEPOS și UDPOS.

În plus față de entități criminale cibernetice, există posibilitatea ca sectorul financiar-bancar să prezinte interes inclusiv pentru actorii cibernetici statali.

De ce ar ataca un actor statal instituții din sectorul financiar-bancar? Pentru că acestea dețin, de regulă, date sensibile, care pot fi relevante în planul activităților de spionaj, dar și pentru a-și suplimenta veniturile, demersul fiind util mai ales în situații în care state/ entități sunt supuse unor sancțiuni internaționale.

Pentru atingerea scopurilor, entitățile statele recurg la: campanii de distribuire a mail-urilor de *spear phishing* (sunt vizați membri aflați în poziții de conducere în cadrul unor companii financiare, pentru a obține acces sau date utile), compromiterea site-urilor web prin metoda *watering hole*.

Also, **attacks on POSs** continue to be one of the main methods of compromising and stealing debit and credit card information worldwide. Most of the times, the attackers don't stop there, they also try to infiltrate the network the POS is connected to. The potential attackers have additional access opportunities when the POS software updates are carried out through an Internet connection or remotely by the companies that provide maintenance.

The malware observed in POS attacks are FastPOS, Alina POS, FrameworkPOS (TRINITY), Backoff POS, BlackPOS, BLUESTEAL, Dexter POS, FIENDCRY, LockPOS, ModPOS, NitlovePOS, TRESOCHO, RAMPAGEPOS and UDPOS.

In addition to cyber crime entities, the financial and banking sectors are likely to be of interest to state cyber actors.

Why would a state actor attack financial or banking institutions? Because they usually own sensitive data that can be relevant in espionage activities and with the purpose of increasing their income, this endeavor proving useful especially when states/ entities are under international sanctions.

In order to reach their goals, state entities resort to: spear phishing mail distribution campaigns (the leadership of financial companies is targeted in order to gain access or useful data), compromising web sites through the watering hole method.

SERVICII PUBLICE ESENȚIALE, INCLUSIV ÎN CONTEXTUL SMART CITY

Din dorința de a eficientiza modul în care administrațiile publice asigură servicii esențiale populației (de sănătate, educație, alimentare cu apă/electricitate/gaz, managementul traficului etc.), se apelează tot mai mult la tehnologie, dând naștere conceptului de *Smart City.*

Este atât o evoluție naturală cât și o necesitate, dacă luăm în calcul urbanizarea continuă - extinderea ariilor urbane și creșterea numărului de utilizatori/beneficiari.

Odată cu această tendință de creștere a digitalizării, pe lângă beneficiile incontestabile obținute, au apărut și noi riscuri, de securitate cibernetică, care au un impact semnificativ asupra vieților noastre.

Tehnologizarea pe scară largă a unor servicii publice esențiale și interconectarea acestora în contextul proiectelor de tip *Smart City* creează noi oportunități pentru criminalii cibernetici.

Aceștia urmăresc să își maximizeze profiturile prin accesarea și comercializarea unui volum mai mare de date, inclusiv cu caracter personal, și distribuirea de *ransomware* care poate afecta furnizarea serviciilor către cetățeni.

> Atunci când au apărut inițial, atacurile cu *ransomware* au fost orientate către persoane individuale, dar câștigul astfel obținut nu se compară cu sumele pe care o autoritate publică, un spital etc. le-ar putea plăti pentru a-și recupera datele sau pentru a-și debloca activitatea.

VITAL PUBLIC SERVICES, INCLUDING IN THE CONTEXT OF SMART CITY

Technology is more and more used in order to render more effective the way public administration provides essential services to the population (health, education, water/ electricity/ gas supply, traffic management, etc.), giving rise to the Smart City concept.

It is both a natural evolution and a necessity if we take into account the continuous urbanization - the expansion of urban areas and the increase in the number of users/ beneficiaries.

With this digitalization trend, in addition to its compelling benefits, new cyber security risks have emerged which have a significant impact on our lives.

Large scale technologization of vital public services and their interconnection in the context of Smart City projects creates new opportunities for cyber criminals.

Their purpose is to maximize their profits by accessing and trading a larger data volume, including personal data, and distributing ransomware that can affect the supply of services to citizens.

> When they initially appeared, ransomware attacks were targeting individuals, but the income they obtained this way did not compare to the amounts a public authority, a hospital, etc. would pay in order to recover its data or to unblock its activity.

Trei proiecte de tip *Smart City* prezintă în mod particular oportunități semnificative pentru entitățile cibernetice criminale:

- EXTINDEREA REȚELELOR PUBLICE DE WI-FI

De regulă, acestea nu sunt securizate, facilitând accesul nerestricționat al atacatorilor cibernetici. Aceștia pot exploata datele vehiculate la nivelul rețelei, sau pot utiliza nodul *Wi-Fi* ca parte a unei infrastructuri de atac. Identificarea atacatorului, este, în aceste situații, aproape imposibilă.

- INSTALAREA SISTEMELOR SMART DE MANAGEMENT AL TRAFICULUI

Dacă traficul de date nu este criptat, acestea pot fi compromise foarte ușor.

- CONECTAREA SISTEMELOR DE FURNIZARE A UTILITĂȚILOR PUBLICE LA INTERNET

Suplimentar conectării la Internet a sistemelor care asigură furnizarea utilităților publice, tot mai mult, aceste sisteme preiau și funcții de control operațional și decizional (Industrial Control Systems - ICS). Spre exemplu, în cazul livrării electricității sau a gazului, ICS-urile reglează automat voltajul, volumul sau presiunea, iar contoarele inteligente permit acum utilizarea eficientă a electricității. În astfel de cazuri, există modalități multiple prin care securitatea comunicațiilor poate fi afectată, prin alterarea datelor raportate, sau, și mai îngrijorător, prin întreruperea funcționării sistemelor.

Three Smart City projects particularly present significant opportunities for cyber crime entities:

- EXTENDING PUBLIC WI-FI NETWORKS

They are not usually secured, thus facilitating unrestricted access for cyber attackers. They can exploit the data transferred in the network or they can use the Wi-Fi node as part of the attack infrastructure. In these situations it is almost impossible to identify the attacker.

- INSTALLING SMART TRAFFIC MANAGEMENT SYSTEMS

If the data traffic is not encrypted, it can be easily compromised.

- CONNECTING THE PUBLIC UTILITIES SUPPLY SYSTEMS TO THE INTERNET

In addition to connecting the systems that ensure the supply of public utilities to the Internet, these systems increasingly take on operational and decisional control functions (Industrial Control Systems - ICS). For example, in the case of electricity or gas supply, the ICSs automatically adjust the voltage, volume or pressure, and smart meters now allow an efficient use of electricity. In these cases, there are multiple ways in which communication security can be affected, by altering reported data or, even more worrisome, by disrupting the functioning of the systems.


CYBER ATTACK
VIRUS DETECTED

2. SITUAȚIA DE SECURITATE CIBERNETICĂ LA NIVEL NAȚIONAL

Ca urmare a extinderii proceselor de digitalizare și tehnologizării, țara noastră este atât o țintă a atacurilor cibernetice, cât și spațiu pe care se regăsesc elemente din infrastructura de atac, utilizată de diverși actori cibernetici ca urmare a creșterii exponențiale a numărului de data center-uri prezente pe teritoriul României.

Și în 2019, atacatorii și-au menținut interesul pentru realizarea de atacuri cibernetice asupra infrastructurilor IT&C cu valențe critice pentru securitatea națională, în multe situații, problema principală fiind neaplicarea sau nerespectarea unor politici de securitate cibernetică de bază (neinstalarea unor soluții antivirus, spre exemplu).

Campaniile de *phishing* și *spear phishing* s-au aflat în top în ceea ce privește distribuirea de *malware*. Acestea reprezintă o metoda de infecție cu o rată de succes ridicată, la care apelează, pentru atingerea scopurilor, atât actori cu motivație financiară cât și cei cu motivație strategică, fie ei statali sau non-statali. De regulă, campaniile de acest fel reprezintă o primă etapă, care creează condițiile favorabile pentru derularea unor atacuri cibernetice mai complexe (fraude financiare, exfiltrare de date sau chiar preluarea sub control a sistemelor informatice compromise etc.).

2. THE NATIONAL CYBER SECURITY SITUATION

As a consequence of the expansion of digitalization and technologization, our country is both a target of cyber attacks and an arena where attack infrastructure elements ca be found. They are used by various cyber actors because of the exponential increase in the number of data centers on Romanian soil.

In 2019, attackers continued to show interest in carrying out cyber attacks on IT&C infrastructure of critical importance for national security, in most cases the main problem consisting of failure to apply or comply with basic cyber security policies (for example, failing to install an antivirus solution).

Phishing and spear phishing campaigns were the top choice for distributing malware. In pursuit of their goals, both financially motivated actors and those with a strategic purpose, whether state or non-state actors, resort to this highly successful infection method. These campaigns generally represent a first stage which creates the pre-requisites for more complex cyber attacks (financial fraud, data exfiltration or even taking control of the compromised IT systems, etc.).

Printre provocările din 2019, inclusiv în România, au fost cele la adresa **sistemului financiar-bancar**, care a continuat să fie vizat de grupările de criminalitate cibernetică, fiind un domeniu care poate aduce câștiguri substanțiale. Acest sector s-a confruntat în ultimii ani cu atacuri în care au fost utilizate tehnici APT, atacuri DDoS, campanii de *spear phishing* pentru distribuire de *malware*, derulate atât împotriva clienților cât și a angajaților instituțiilor, cu scopul obținerii de credențiale, inclusiv bancare și/sau date despre sistemul infectat, campanii de malspam etc.

> **Cobalt Group**, a targetat în ultimii doi ani instituții bancare de pe tot globul, inclusiv din țara noastră.

În 2019, entități publice și private din România au fost afectate de atacuri cibernetice de tip *ransomware* și de campanii de minare neautorizată de criptomonedă, prin utilizarea infrastructurii IT&C fără acordul proprietarului.

Efectele unui atac *ransomware* sunt diverse, în cazul instituțiilor din domeniul sănătății fiind posibilă, spre exemplu, inclusiv indisponibilizarea infrastructurii IT&C a unui spital și afectarea calității serviciilor medicale furnizate populației. Infecțiile s-au realizat, de regulă, prin utilizarea tehnicilor de inginerie socială sau prin dezactivarea soluției antivirus.

În 2019, activitățile de minare neautorizată de criptomonedă s-au menținut la un nivel de intensitate medie, fiind în continuare o metodă utilizată de atacatori cibernetici. Au fost identificate atât atacuri de tip *cryptojacking*, cât și activități de utilizare, în mod direct, a unei infrastructuri fără acordul proprietarului, pentru generarea de profit prin activități de minare.

Among the challenges of 2019, including in Romania, those against the **financial and banking system** are noteworthy. They continued to be targeted by cyber crime groups since it's a sector that can bring substantial income. In the last few years, this sector has faced APT attacks, DDoS attacks, spear phishing campaigns for the distribution of malware, conducted both against clients and employees with the purpose of obtaining credentials, including banking and/ or data about the infected system, malspam campaigns, etc.

> **Cobalt Group** targeted banking institutions all over the world in the last two years, including in our country.

In 2019, public and private entities in Romania were affected by ransomware cyber attacks and unauthorized cryptocurrency mining, using IT&C infrastructures without the owner's consent.

The effects of a ransomware attack are diverse. In the case of public-health institutions, for example, they include the disruption of a hospital's IT&C infrastructure and the quality of medical services supplied to the population. The infections were conducted mainly through the use of social engineering techniques or by disabling the antivirus software.

In 2019, unauthorized cryptocurrency mining remained at a medium intensity level, and it continues to be a method used by cyber attackers. Both cryptojacking and the direct use of an infrastructure without the owner's consent in order to generate profit through mining activities were identified.

Au fost descoperite mai multe pagini *web* compromise de scripturi de minare în *browser*, în vederea obținerii de criptomonedă (ex. MONERO). Printre acestea s-au aflat și pagini *web* aparținând unor instituții publice, din domeniul administrației publice, sănătății etc.

În ceea ce privește atacurile de tip *cryptojacking* au fost sesizate campanii de distribuire a BitCoinMiner.XMR ("xmrzig.exe"), *malware* ce minează ilegal monedă virtuală Monero, utilizând resursele infrastructurii afectate.

Problematic în cazul minării neautorizate cu criptomonedă este incidentul de compromitere în sine, care semnifică, în fapt, infiltrarea atacatorului în infrastructura IT&C, ceea ce poate permite instrumentarea și derularea altor atacuri cibernetice.
Date de cunoaștere despre malware-urile cu cea mai mare prezență la nivel internațional, unele dintre acestea fiind observate inclusiv în România:

Emotet - este un troian care urmărește, în primul rând, colectarea de date de autentificare la conturi deschise la instituții financiare. Este un malware modular, deoarece descarcă și execută diverse module, cu funcționalități diferite, care sunt încărcate direct din memorie și includ: tool-uri pentru obținerea de credențiale din browser-ul web și clientul de email, scraper de email pentru Microsoft Outlook etc.

LokiBot - este un *malware* care fură credențiale (parole, date de autentificare stocate în browser-ul web, FTP/SSH, date de autentificare introduse în *browser*-ul web, portofele de criptomonede etc.). Poate descărca, încărca și executa alte coduri *malware* în sistemul IT&C infectat. De asemenea, este proiectat să colecteze date private pe care le transmite atacatorului printr-un server de C2. De asemenea, este proiectat să funcționeze pe mașini care au sistemul de operare Windows XP, Vista 7, 8 sau Linux.

Several web pages compromised by mining scripts in the browser were discovered, aiming at obtaining cryptocurrency (i.e. MONERO). Among these, there were web pages belonging to public institutions from the public administration sector or public-health, etc.

As regards cryptojacking attacks, campaigns to distribute BitCoinMiner.XMR ("xmrzig.exe") were identified, a malware which illegally mines for Monero cryptocurrency by using the resources of the affected infrastructure.

What poses a problem in the case of unauthorized cryptocurrency mining is the compromising itself, which actually means the attacker has infiltrated the IT&C infrastructure, which can allow for the instrumentation and conducting of cyber attacks.
Information on the malwares that are most present internationally, some of them observed in Romania:

Emotet - is a trojan that aims, first of all, at collecting authentification data to accounts open with financial institutions. It is a modular malware, because it downloads and executes various modules with different functionalities, which are loaded directly from memory and include: tools for obtaining credentials from the web browser and the email client, email scraper for Microsoft Outlook, etc.

LokiBot - is a *malware* that steals credentials (passwords, authentication data stored in the browser, FTP/SSH, authentication data entered in the browser, cryptocurrency wallets etc.). It can download, upload and execute other malware codes on the infected IT&C system. It is also designed to collect private data which are then sent to the attacker via a C2 server. It can be run on computers with Windows XP, Vista, 7, 8 or Linux.

GozNym – este un *troian bancar* utilizat pentru obținerea de beneficii financiare care vizează bănci, platforme de e-commerce și conturi de business. Acesta realizează fraudele prin infectarea browserelor web (ex. Google Chrome, Mozilla Firefox), fără a fi detectat de soluțiile antivirus.

FormBook - este un *malware* care fură date de autentificare. Se injectează în diferite procese care rulează pe sistem și deține capabilități pentru înregistrarea cuvintelor tastate de utilizator și extragerea datelor din sesiunile HTTP. *Malware*-ul poate executa și comenzi primite de la un server de C2: descărcarea și executarea de fișiere, inițierea unor procese, închiderea și rebootarea sistemului, colectarea cookie-urilor și a parolelor locale. De asemenea, are capacitatea de a-și asigura persistența.

NanoCore - este un troian prin care se poate realiza accesul de la distanță (Remote Access Trojan - RAT), disponibil public și cu rol de *backdoor*. Utilizează comunicații criptate și are următoarele capabilități: poate accesa de la distanță desktop-ul, camera web și microfonul sistemului, poate adapta plugin-urile, poate transfera, descărca și executa fișiere.

CUTWAIL – este un malware de tip botnet, care afectează doar sistemele de operare Windows, fiind distribuit prin troianul Pushdo. Acesta transformă sistemele infectate în spamboți, care se conectează direct la serverele de comandă și control, primesc informații despre email-urile pe care trebuie să le trimită și, după ce își termină task-ul trimit serverelor o statistică privind numărul email-urilor transmise și erori întâmpinate.

GozNym – is a *banking Trojan* used to obtain financial benefits by targeting banks, e-commerce platforms and business accounts. It commits frauds by infecting the browsers (e.g. Google Chrome, Mozilla Firefox) while going undetected by antivirus products.

FormBook - is a *malware* that steals authentication data. It is injected into different processes running on the system and has capabilities for recording words typed by users and extracting data from HTTP sessions. The *malware* can also execute commands received from a C2 server: downloading and executing files, inititating processes, shutting down and rebooting the system, collecting cookies and local passwords. It is also able to maintain persistence.

NanoCore - is a publicly available Trojan that can provide remote access (Remote Access Trojan - RAT), with a *backdoor* function. It uses encrypted communications and has the following capabilities: it can remotely access the desktop, the webcam and the system's microphone, it can adapt the plugins, it can transfer, download and execute files.

CUTWAIL – is a botnet malware that affects only Windows operating systems and is distributed via the Pushdo Trojan. It turns the infected systems into spambots, which connect directly to the command and control servers, receive information about the e-mails to send and, after completing the task, they send statistical data to the servers about the number of sent e-mails and encountered errors.

Remcos - este un RAT configurabil, scris în limbajul C++ și are mai multe funcționalități, printre care: managementul fișierelor, capturi de ecran, accesarea arbitrară a fișierelor, preluarea controlului asupra mouse-ului. Remcos poate fi utilizat și ca un tool de supraveghere de la distanță, prin care se accesează camera și microfonul calculatorului.

NetWire - este tot un RAT, capabil să: colecteze un număr mare de date de autentificare, date tastate, informații despre sistem, capturi de ecran etc. Instrumentul este disponibil public.

Azorult – este un malware utilizat pentru furtul informațiilor din sistemele IT&C, precum istoricul browselor web, cookie-uri, credențiale de acces, informații privind criptomonedele și altele. Acesta poate acționa și ca downloader pentru alte aplicații malware.

Scranos - identificat în 2019, este un *malware* multifuncțional (rootkit/backdoor/infostealer), care își asigură persistența și poate prelua sub control total sistemele infectate. Acesta este distribuit prin aplicații software modificate/compromise anterior de către atacatori. Scranos are următoarele capabilități: extrage cookie-uri, fură credențiale introduse în câteva tipuri de browsere web și pe platforma Steam, exfiltrează conturi prin care s-au făcut plăți pe Amazon, Airbnb și Facebook, trimite mesaje de *phishing* către prietenii asociați conturilor de Facebook compromise, descarcă și execută *malware*, precum și multe alte activități malițioase. Dacă inițial Scranos a fost distribuit în China, ulterior a fost extinsă aria de acțiune, fiind infectate sisteme din întreaga lume, cele mai multe fiind raportate în România, Brazilia, Franța, India, Indonezia și Italia.

Remcos - is a configurable RAT written in C++ and has various functionalities, among which: file management, screenshots, arbitrary accessing of files, taking control of the mouse. Remcos can also be used as a remote surveillance tool, as it is able to access the computer's camera and microphone.

NetWire - is also a RAT malware capable of: collecting a large number of authentication data, entered data, system information, screenshots etc. The tool is publicly available.

Azorult – is a malware used to steal information from IT&C systems, such as browsing history, cookies, access credentials, cryptocurrency information and so on. It can also download other malware applications.

Scranos - identified in 2019, it is a multifunctional malware (rootkit/backdoor/infostealer), which maintains persistance and can gain full control over the infected systems. It is distributed via software applications that were previously modified/compromised by the attackers. Scranos has the following capabilities: extracting cookies, stealing credentials entered into several types of browsers and on the Steam platform, exfiltrating accounts through which payments were made on Amazon, Airbnb and Facebook, sending phishing messages to friends associated with compromised Facebook accounts, downloading and executing malware, as well as many other malicious activities. Although Scranos was initially distributed only in China, its scope was later expanded to infect systems around the world; most cases were reported in Romania, Brazil, France, India, Indonesia and Italy.

Citadel – este un malware de tip troian, care utilizează capabilități de keylogger pentru a fura credențialele stocate în fișiere de tip password manager. Mai mult, Citadel construiește o rețea de boți din sistemele infectate și poate executa alte aplicații malware pe acestea, de tip ransomware și scareware.

Retefe – este un troian bancar care afectează sistemele pe care rulează Windows, având capacitatea de a instala malware adițional prin Windows PowerShell. Pe sistemele infectate, Retefe afectează setările DNS și instalează un certificat local root, care permite atacuri de tip man-in-the-middle pentru interceptarea și modificarea traficului de rețea către băncile utilizatorilor.

GlobeImposter - aplicație de tip *ransomware* care se răspândește prin intermediul campaniilor de tip spam. Poate executa comenzi pentru evitatea restaurării datelor criptate (întruperea funcționării programelor antivirus sau a altor setări de securitate etc.).

Maoloa - aplicație *ransomware* de tip troian, diseminată în principal prin distribuirea de email-uri *spam* cu atașamente infectate. Fișierelor criptate de acest *malware* le este adăugată extensia ".maoloa".

Dharma - face parte dintr-o familie de *ransomware* care care a apărut în 2016 și de atunci se află în continuă dezvoltare. Principalele metode de distribuție includ: livrarea ca atașament *malware* la mail-uri spam, distribuirea prin executarea fișierelor de instalare ale unor aplicații legitime sau prin exploatarea RDP.

Citadel – is a Trojan-type malware that uses keylogger capabilities to steal credentials stored in password manager files. Moreover, Citadel builds a network of bots made up of the infected systems and can run other malware applications on them, such as ransomware or scareware.

Retefe – is a banking Trojan that affects Windows operating systems and is able to install additional malware via Windows PowerShell. Retefe affects the DNS settings of the infected systems and installs a local root certificate, which enables man-in-the-middle attacks in order to intercept and modify network traffic to the users' banks.

GlobeImposter - a *ransomware* application that is distributed by means of spam campaigns. It can execute commands to avoid the restoration of encrypted data (interrupting the operation of antivirus programs or of other security settings etc.).

Maoloa - a Trojan-type *ransomware* application, mainly disseminated by distributing spam e-mails with infected attachments. Files encrypted by this *malware* receive the ".maoloa" extension.

Dharma - is part of a *ransomware* family that emerged in 2016 and has been developing ever since. The main methods of distribution include: delivery as malicious attachment to spam e-mails, distribution as a result of executing installation files of legitimate applications or by exploiting the RDP protocol.

Phobos - aplicație *ransomware* care prezintă similitudini cu Dharma. Se răspândește prin intermediul campaniilor de tip spam, prin exploatarea vulnerabilităților protocolului RDP, respectiv prin descărcarea unor aplicații de gaming din mediul online. Aplicația criptează fișierelor care au extensiile *.doc, .docx, .xls, .pdf* etc.

Pony - este un Remote Acces Trojan, cu funcționalități de *spyware*, care urmărește furtul de credențiale și alte date cu caracter personal existente pe sistemele infectate.

Houdini - *malware* care vizează furtul de date bancare ale victimelor, fiind distribuit prin intermediul mail-urilor de phishing.

Pentru prevenirea și gestionarea cu succes a acestor amenințări, orice organizație ar trebui să aibă în vedere implementarea și respectarea unor politici de securitate cibernetică care să cuprindă:

- instalarea unor soluții antivirus;
- implementarea unor politici corespunzătoare de *back-up* al datelor;
- actualizarea permanentă a aplicațiilor și sistemelor utilizate pentru eliminarea posibilelor vulnerabilități;
- restricționarea accesului din mediul Internet către sistemele interne (restricționarea accesului RDP și implementarea autentificării în doi pași - *two factor authentication*, închiderea porturilor neutilizate pentru sistemele IT&C expuse etc.);

Phobos - a *ransomware* application similar to Dharma. It is spread via spam campaigns, by exploiting the vulnerabilities of the RDP protocol or by downloading gaming applications from the Internet. The application encrypts files with the *.doc, .docx, .xls, .pdf* etc. extensions.

Pony - is a Remote Acces Trojan with *spyware* functionalities, aimed at stealing credentials and other private data from the infected systems.

Houdini - *malware* aimed at stealing banking data, which is distributed via phishing e-mails.

In order to successfully prevent and manage these threats, any organization should implement and enforce certain cyber security policies, including:

- installing antivirus products;
- implementing appropriate data back-up policies;
- permanently updating applications and systems in order to eliminate any potential vulnerabilities;
- restricting access from the Internet to internal systems (restricting RDP access and implementing *two factor authentication*, closing unused ports on exposed IT&C systems etc.);

- modificarea cu regularitate a parolelor și asigurarea unui nivel de complexitate ridicat al acestora;
- stabilirea unei politici de awareness privind activități subsumate ingineriei sociale (*phishing, spear phishing*);
- segmentarea rețelelor IT&C;
- stabilirea unui plan de răspuns la incidente de securitate cibernetică în vederea creșterii nivelului de reziliență a sistemelor și rețelelor IT&C din cadrul organizației;
- instruirea și testarea reacției angajaților la incidente cibernetice.

- regularly changing passwords and making sure they have a high level of complexity;
- implementing an awareness policy in terms of social engineering activities (*phishing, spear phishing*);
- segmenting the IT&C networks;
- building a cyber security incident response plan in order to increase the resilience of the organization's IT&C systems and networks;
- training the employees and testing their reaction to cyber incidents.


CYBER
RISK
Threat
hacker

3. ELEMENTE DE EVALUARE ȘI TREND ÎN CEEA CE PRIVEȘTE CRIMINALITATEA CIBERNETICĂ ÎN 2020

ANALIZÂND MODUL DE OPERARE AL ATACATORILOR CIBERNETICI CU MOTIVAȚIE FINANCIARĂ, ÎN 2019 AU FOST OBSERVATE URMĂTOARELE:

■ mai multe grupări de criminalitate cibernetică utilizează aceleași metode, îngreunând suplimentar procesul de atribuire al unui atac.

> Această colaborare dintre diferite grupări de criminalitate cibernetică constă atât în utilizarea în comun a anumitor elemente de infrastructură (IP-uri, servere de C2 etc.) sau *tool*-uri, cât și în distribuirea aceluiași *malware*.

■ o mare varietate de *tool*-uri și servicii cibernetice sunt comercializate pe forumuri, publice, cu acces restricționat, sau pe cele din Dark Web, fapt care oferă unor actori cu capabilități și cunoștințe reduse posibilitatea de a derula atacuri cibernetice. Acest fenomen este cunoscut ca *cybercrime-as-a-service* (CaaS) și generează venituri atât

3. ASSESSMENT AND TRENDS IN CYBER CRIME FOR 2020

AFTER ANALYZING THE MODUS OPERANDI OF FINANCIALLY-MOTIVATED CYBER ATTACKERS IN 2019, THE FOLLOWING TRENDS WERE DISCOVERED:

■ several cybercrime groups use the same methods, further complicating the process of attributing attacks.

> This cooperation between different cybercrime groups consists both in the shared use of certain infrastructure elements (IPs, C2 servers etc.) or tools, as well as in the distribution of the same *malware*.

■ a large variety of cyber tools and services are sold on public forums, restricted access forums or on the Dark Web, which gives low-skilled actors the opportunity to carry out cyber attacks. This phenomenon is known as *cybercrime-as-a-service* (CaaS) and it generates revenue both for the person who rents/sells the malware product /provides

celui care închiriază/vinde *malware*-ul/furnizează expertiza sau infrastructura necesare derulării atacului cibernetic, cât și celui care derulează efectiv atacul.

> Odată cu proliferarea fenomenului Ransomware-as-a-Service (RaaS), parte a CaaS, derularea unui atac *ransomware* este mult mai facilă. De asemenea, servicii de realizare a atacurilor Distributed Denial of Service (DDoS), operațiuni de *phishing* sau de minare neautorizată de criptomonedă pot fi contractate de pe diverse website-uri specializate.

■ o altă modalitate la care criminalii cibernetici au apelat pentru a-și spori substanțial veniturile constă în compromiterea bazelor de date, copierea conținutului, ștergerea datelor de pe serverul victimei și solicitarea unei recompense pentru restaurarea acestora; un astfel de atac poate fi monetizat suplimentar, prin punerea la vânzare a conținutului bazelor de date pe diverse forumuri underground;

■ macro-urile documentelor sunt utilizate pentru obfuscarea *malware*-ului;

■ atacatorii folosesc tool-uri legitime sau disponibile public, fapt care reduce costurile necesare pentru derularea atacului și îngreunează eforturile de atribuire;

■ exploatarea vulnerabilităților *Remote Desktop Protocol* (RDP) a fost o metodă des utilizată de criminalii cibernetici pentru realizarea infecției;

■ în scopul evitării detecției și îngreunării investigațiilor, atacatorii utilizează metode *anti-forensics*, precum ștergerea completă a log-urilor, criptarea log-urilor aplicațiilor de administrare de la distanță etc;

the expertise or infrastructure needed to carry out the attack, as well as for the person who actually carries out the attack.

> With the prolideration of Ransomware-as-a-Service (RaaS), as part of CaaS, carrying out a ransomware attack has become much easier. Likewise, services for carrying out Distributed Denial of Service (DDoS) attacks, phishing or unauthorized cryptocurrency mining can be found on various specialized websites.

■ another method used by cyber criminals to substantially increase their income is to compromise databases, copy content, delete data from the victim's server and request a reward for restoring them; such an attack can be further monetized by selling the content of databases on various underground forums;

■ document macros are used for malware obfuscation purposes;

■ the attackers use legitimate or publicly available tools, which reduces the costs necessary for carrying out the attack and hinders the efforts to attribute such attacks;

■ exploiting *Remote Desktop Protocol* (RDP) vulnerabilities has been a method often used by cyber criminals to achieve the infection;

■ in order to avoid detection and to hinder investigations, the attackers use anti-forensics methods, such as complete deletion of logs, encryption of logs of remote administration applications etc.;

■ pentru a asigura succesul unui atac cu *ransomware*, atacatorii pot șterge copiile de siguranță ale datelor, opresc serviciile care asigură realizarea de *back*-up și modifică regulile soluțiilor de antivirus/*firewall*, înainte de a rula aplicația *malware*.

ÎN CEEA CE PRIVEȘTE ANUL 2020 ESTIMĂM URMĂTOARELE TREND-URI ÎN CEEA CE PRIVEȘTE FENOMENUL CRIMINALITĂȚII CIBERNETICE:

■ Organizațiile, publice sau private, care dețin și gestionează date cu caracter personal sau care furnizează servicii esențiale populației, vor fi cele mai vizate de atacatorii cibernetici în căutare de câștiguri financiare.

■ Având în vedere disponibilitatea crescută a aplicațiilor de tip *ransomware*, în sistem *Ransomware-as-a-Service* și popularitatea în rândul criminalilor cibernetici, activitățile de distribuire a acestui tip de *malware* vor continua și în 2020. Va crește în mod special ponderea atacurilor *ransomware* targetate, care pot genera pagube mai mari spre deosebire de cele cu adresabilitate generală, mai populare în trecut.

> Prin atacuri *ransomware* targetate ne referim la cele în care *pay*load-ul *malware* este distribuit ulterior etapei de compromitere a infrastructurii IT&C a victimei. În prima fază atacatorul se infiltrează în rețea și derulează activități de recunoaștere, fapt care maximizează efectele etapei a doua, de distribuire efectivă a *ransomware*-ului.

■ Derularea de *third party attacks*, cu subcategoria *supply-chain attacks*, care exploatează încrederea pe care utilizatorii o acordă relației cu alte companii, produse și servicii furnizate pe căi legitime.

■ to ensure the success of a ransomware attack, the attackers can delete data backups, interrupt the services that ensure the backup and change the rules of the antivirus/ firewall solutions, before running the malware application.

FOR 2020 WE ESTIMATE THE FOLLOWING TRENDS IN TERMS OF CYBERCRIME:

■ Public or private organizations that hold and manage personal data or provide essential services to the population will be the most targeted by cyber attackers in search of financial gains.

■ Given the increased availability of *Ransomware-as-a-Service* and its popularity among cyber criminals, the distribution of this type of malware will continue in 2020.
We'll witness an increase in targeted ransomware attacks, which can cause greater damage than the ones with general addressability, which were more popular in the past.

> By targeted *ransomware* attacks we mean the attacks in which the malware payload is distributed after the victim's IT&C infrastructure has been compromised. In the first stage, the attacker infiltrates the network and carries out reconaissance activities, which maximize the effects of the second stage, during which the ransomware is actually distributed.

■ Conducting *third party attacks*, including *supply-chain attacks*, which exploit the users' trust in their relations with other legitimate companies, products and services.

Metoda este una atractivă pentru atacatori, deoarece este greu de detectat și de prevenit și este foarte eficientă, având în vedere că printr-o singură activitate de compromitere pot fi atacate mai multe victime.

> Luând aceste aspecte în calcul, orice organizație are, într-un fel sau altul, legătură cu o posibilă țintă. Chiar dacă entitatea este de dimensiuni mici și nu are un profil semnificativ, dar este furnizor, vânzător terț sau are o legătură cu o organizație mai mare/cu un rol important în societate, atunci acea entitate este foarte probabil să fie ținta unui atac cibernetic prin care să se încerce accesarea țintei finale. Evaluarea nivelului de securitate cibernetică și adoptarea măsurilor necesare trebuie realizate, prin urmare, luând în calcul inclusiv poziția în ecosistemul social.

■ Exploatarea RDP va fi în continuare o metodă preferată de atacatori pentru infiltrarea în sistemul IT&C al victimei și distribuirea de *malware*. Cel mai probabil, aceștia vor viza serverele configurate deficitar prin RDP, sau vor urmări exploatarea vulnerabilităților asociate RDP.

■ Includerea în rețele de boți pentru automatizarea atacurilor. Compromiterea și includerea într-o rețea de boți a unui sistem IT&C constituie un efect negativ în sine, dar impactul negativ este multiplicat prin utilizarea rețelei de boți în derularea de alte atacuri: DDoS, *phishing*, furt de credențiale, care ulterior vor fi utilizate în alte tipuri de activități malițioase. Acest fenomen are efecte negative inclusiv în planul imaginii unui stat sau chiar a unei companii, prin asocierea IP-urilor acestora cu atacuri cibernetice.

■ Și în 2020 ne vom confrunta cu furtul de credențiale, inclusiv date bancare, atât ale clienților cât și ale angajaților, prin transmiterea de mail-uri de *phishing* sau *spear phishing*, sau prin compromiterea POS-urilor.

The method is an attractive one for attackers, because it is difficult to detect and prevent and it is very efficient, considering that several victims can be attacked simultaneously.

> Taking these aspects into account, any organization is, in one way or another, connected to a possible target. Even if the entity is small and does not hold a significant position, but is a supplier, third party seller or has a connection with a larger organization /an organization playing an important role in society, that entity is very likely to be the target of a cyber attack seeking access to the final target. The evaluation of the cyber security level and the adoption of appropriate measures must therefore take into account, among other things, the organization's position in the social ecosystem.

■ RDP exploitation will continue to be one of the preferred methods of attackers for infiltrating the victim's IT&C system and distributing malware. Attackers will most likely target poorly configured RDP servers or exploit the vulnerabilities associated with RDP.

■ Assimilation into bot networks for the purpose of automating the attacks. Compromising and assimilating an IT&C system into a bot network is a negative effect in itself, but the negative impact is multiplied due to the exploitation of the bot network for carrying out other attacks, such as DDoS, *phishing*, credential theft, which will subsequently be used in other types of malicious activities. This phenomenon has negative effects in terms of the reputation of a state or even a company, since their IPs are associated with cyber attacks.

■ In 2020 we will continue to deal with credential theft, including banking data, both of customers and employees, by means of phishing or spear phishing e-mails or compromised POSs.

Phishing-ul/*spear phishing*-ul vor fi în continuare metode preferate pentru distribuirea de *malware*, având în vedere rata mare de succes a acestui mecanism, generată, în mare parte, de neaplicarea politicilor de securitate precum și de cultura de securitate, inclusiv cibernetică, insuficientă a utilizatorilor.

Se vor extinde intruziunile complexe vizând crearea unor breșe de securitate la nivelul *point-of-sale* (POS), principalii actori fiind grupările de criminalitate cibernetică care vizează domeniul financiar.

Phishing/*spear phishing* will continue to be among the preferred methods for malware distribution, given the high success rate of this mechanism, which is largely due to the failure to enforce security policies and to the users' poor security culture, including in the field of cyber security.

Complex intrusions aimed at creating security breaches at the *point-of-sale* (POS) level will expand; the main actors will be cybercrime groups targeting the financial sector.

www.sri.ro
www.fireeye.com