POLIȚIA ROMÂNĂ

CRIMINALITATEA INFORMATICĂ

ATACURILE MALWARE-FORME ȘI TENDINȚE

POLIȚIA ROMÂNĂ
INSTITUTUL DE CERCETARE ȘI PREVENIRE A CRIMINALITĂȚII
BUCUREȘTI
2022

MALWARE

DEFINIȚIE

MALWARE este un termen generic, care descrie orice tip de program informatic, proiectat intenționat pentru deteriorarea sau infiltrarea într-un sistem informatic – fie el computer, dispozitiv mobil sau chiar o întreagă rețea – și care, de obicei este instalat în sistem fără știrea sau aprobarea utilizatorului.

Program sau software malițios, rău-intenționat sau dăunător sunt termeni care se folosesc alternativ pentru a desemna această categorie de programe informatice. Ele sunt utilizate de către infactorii informatici pentru a inița activități neautorizate în respectivul sistem informatic, exploatând vulnerabilitățile de securitate, în general pentru a-l ajuta pe proprietar să obțină venituri ilicite.

Programele malware variază în funcție de scopul lor, de modul în care infectează un computer, de modul în care se răspândesc și de daunele sau riscurile de securitate pe care le prezintă (troieni, worms/viermi, rootkits, ransomware, ad-ware etc).

Malware as a Service (MaaS) este un serviciu într-o continuă dezvoltare, prin care atacatorii care dezvoltă programe malware le pun la dispoziția celor care nu au cunoștințele tehnice necesare pentru a-și crea propriul program malițios, pentru o anumită sumă de bani sau pentru un procent din câștiguri.
Există atât abonamente lunare, cât și posibilitatea de a cumpăra programul pentru o perioadă nelimitată, astfel încât, cei care îl achiziționează, îl pot folosi pentru atacuri ori de câte ori au nevoie sau până când acesta nu mai este eficient, devenind ușor de detectat de programele antivirus

TIPURI

- ☐ MOBILE MALWARE
- ☐ RANSOMWARE
- ☐ BANKING TROJANS
- ☐ INFOSTEALER
- ☐ KEYLOGGER
- ☐ EXPLOIT

și altele...

MALWARE

STATISTICI

Conform datelor colectate de Direcția Cazier Judiciar, Statistică și Evidențe Operative din cadrul Inspectoratului General al Poliției Române:

- În anul 2021, Poliția Română a fost sesizată cu privire la 1899 infracțiuni contra siguranței și integrității sistemelor și datelor informatice, în creștere cu 37,21% față de anul 2020.
- Dintre acestea, cea mai mare parte (92,58%) a fost reprezentată de accesul ilegal la un sistem informatic, faptă prevăzută la articolul 360 din Codul Penal.
- Sesizările fraudelor comise prin sisteme informatice și mijloace de plată electronice, au crescut considerabil în anul 2021 față de 2020, cu 85,53% (de la 7144 astfel de fapte în 2020 la 13254 în 2021).
- În primele 3 luni ale anului 2022 au fost înregistrate 431 infracțiuni contra siguranței și integrității sistemelor și datelor informatice și 2719 fraude comise prin sisteme informatice și mijloace de plată electronice.

Conform buletinului CYBERINT (semestrul I - 2022) realizat de Serviciul Român de Informații, pe parcursul anului 2021, aplicațiile malware cele mai utilizate de atacatorii cibernetici pentru compromiterea sistemelor critice pentru securitatea națională a României au fost cele de tip InfoStealer (34.27%), Trojan (27.95%), Exploit (13,7%) și Ransomware (12.86%).

MALWARE

Conform unui raport ENISA*, în perioada ianuarie 2019-aprilie 2020, în fiecare zi au apărut aproximativ 230.000 de noi variante de malware, 67% dintre atacurile de tip malware au fost livrate prin intermediul conexiunilor criptate HTTPS, iar în cazul a 71% dintre organizațiile afectate, malware-ul a fost răspândit de la un angajat la altul.

Principalele incidente în U.E. și în lume în perioada aprilie 2019-aprilie 2020*

APRILIE 2019
Facebook a raportat expunerea datelor a 540 de milioane de utilizatori

IUNIE 2019
5 spitale din România au fost atacate de ransomware-ul Badrabbit.

SEPTEMBRIE 2019
În Belgia, datele a aproximativ 90.000 de clienți Mastercard din Europa au fost furate.

IANUARIE 2020
Ministerul de Externe al Austriei a fost victima unui atac cibernetic.

APRILIE 2020
Peste 500.000 de conturi de utilizatori ale platformei Zoom au fost găsite la vânzare pe site-urile pe care atacatorii informatici fac schimb de informații

*European Union Agency for Cybersecurity, 2020. Main Incidents in the EU and Worldwide

MALWARE

*ȘTIAI CĂ...

În 2020, victimele atacurilor cibernetice au pierdut 4.2 miliarde de dolari.

Costul mediu al criminalității informatice pentru companii a fost de aproximativ 13 milioane de dolari în 2019.

70% dintre fraudele online au loc prin intermediul dispozitivelor mobile.

Peste 75% dintre atacurile cibernetice au fost inițiate prin email.

De la începutul pandemiei de COVID-19, FBI a observat o creștere de 300% a raportărilor privind criminalitatea informatică.

În 2020, atacul asupra echipamentelor unui spital din Germania a condus la moartea unui pacient.

*Sursa:https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

MOBILE MALWARE

MOBILE MALWARE presupune infectarea dispozitivelor mobile cu aceleași tipuri de malware existente și în cazul atacurilor cibernetice care țintesc alte tipuri de dispozitive.

Securitatea telefoanelor este de obicei neglijată de utilizatori. Foarte puțini dintre aceștia folosesc soluții de securitate pe dispozitivele mobile, deși acestea conțin informații importante: aplicații bancare, conturi ale aplicațiilor utilizate, documente legate de viața personală și profesională etc.

Foarte multe persoane folosesc telefonul în interes de serviciu, astfel că acestea sunt o țintă „atrăgătoare" pentru atacatori.

Conform Raportului „Internet Organised Crime Threat Assessment 2021" realizat de Europol, în anul 2021, acest tip de malware a redevenit o amenințare critică, numărul sesizărilor privind infectarea dispozitivelor mobile crescând considerabil.

RANSOMWARE

CINE POATE DEVENI VICTIMĂ?

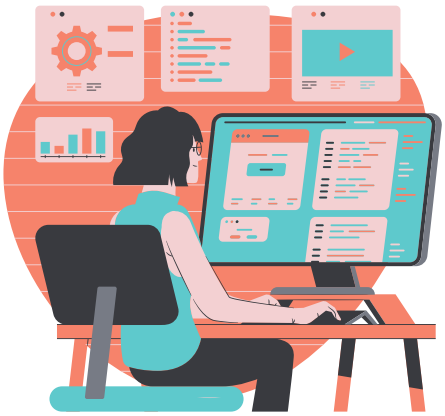
Oricine care utilizează un dispozitiv conectat la internet poate fi victimă a acestui tip de atac, fie că este vorba de o persoană fizică, o instituție publică sau o companie comercială

EVOLUȚIE

În ultimii 2 ani, atacurile s-au concentrat pe companii comerciale, prin comparație cu persoanele fizice, întrucât șansa de a primi bani este mai mare. Acest lucru este posibil deoarece companiile gestionează date, care, odată compromise, le pot aduce prejudicii pe care sunt interesate să le stopeze. Aceste prejudicii pot ajunge la valori extrem de mari, într-un interval foarte scurt, astfel încât compania atacată este tentată să plătească răscumpărarea cât mai rapid posibil.

CE ESTE?

Ransomware-ul este un program din familia mai mare a malware-ului, care blochează dispozitivele (atât computerele, cât și dispozitivele mobile) sau criptează fișierele de pe dispozitivele respective. Atacatorii vă informează că puteți recăpăta accesul la dispozitiv sau la datele de pe acesta doar dacă plătiți o răscumpărare și vă îndrumă pas cu pas ce aveți de făcut pentru a plăti, în vederea obținerii cheii de decriptare.



Plata răscumpărării nu garantează recuperarea accesului la date sau dispozitive și, mai mult, le arată atacatorilor că inițiativa lor a avut succes, garantându-le în acest fel reputația, pentru a-și putea vinde mai departe „afiliaților" programul malițios.

RANSOMWARE

Răspândirea unui ransomware și infectarea dispozitivelor se produce prin mai multe metode, printre care: accesarea unui website infectat sau chiar a unuia ilegal, accesarea unui fișier atașat infectat sau a unui link dintr-un email, accesarea unui link dintr-o reclamă sau chiar alt malware care infecta deja sisemul, fără știrea utilizatorului.

Se constată, în paralel, două modalități principale prin care atacatorii acționează: pe de o parte, așa cum am spus mai sus, atacurile sunt lansate la modul general, astfel încât orice utilizator poate deveni o victimă a unui astfel de program malițios, de la un copil care accesează calculatorul sau telefonul părinților, până la un adult sau un vârstnic, care este predispus să dea click pe o reclamă la un produs de întreținere a sănătății. În același timp, există și atacuri țintite asupra anumitor companii comerciale, selectate intenționat de către atacatori în funcție de cifra de afaceri, profit, număr de angajați etc., date pe care le pot găsi din surse publice.

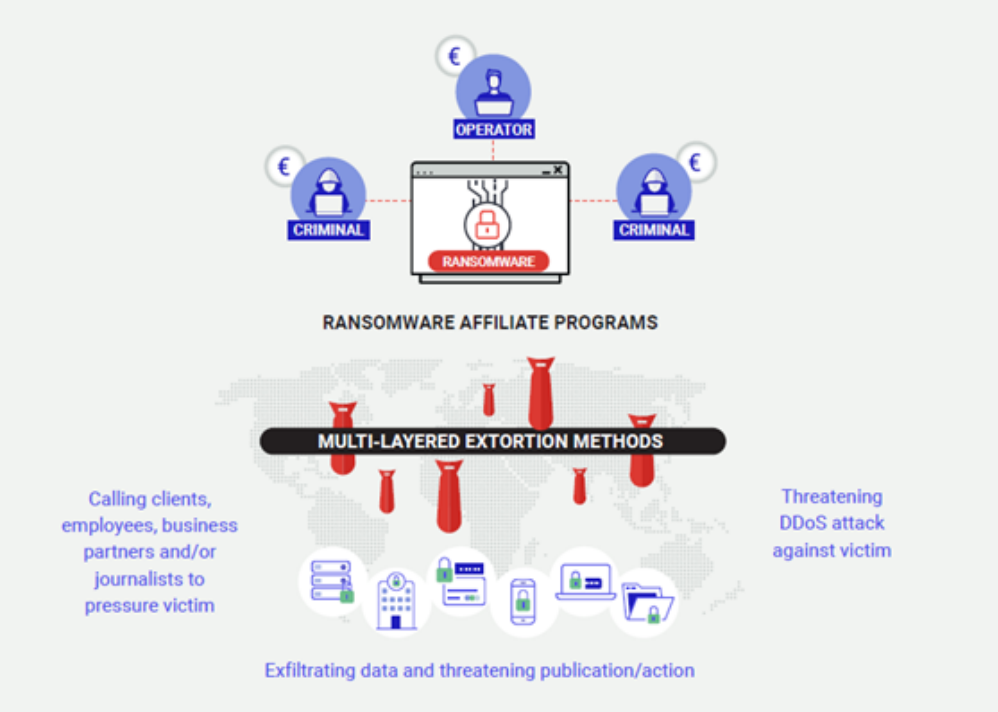
Atacatorii vizează astfel orice breșă de securitate a sistemului sau rețelei, de la credențiale slabe pentru autentificare (user și parolă), până la sisteme de operare neactualizate, aplicații neactualizate, lipsa unui antimalware, conectarea la rețele Wi-fi care nu sunt de încredere, accesul la infrastructura companiei prin intermediul unor dispozitive nesecurizate, accesarea unor link-uri sau atașamentele ale emailurilor care infectează sistemul.

RANSOMWARE

RANSOMWARE ÎN ROMÂNIA

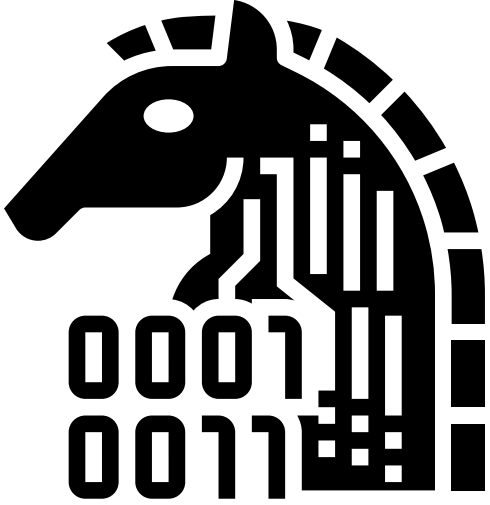
S-a constatat că atacatorii din România sunt, de cele mai multe ori, afiliați ai unor rețele internaționale mult mai mari, ei primind doar un procent din plățile făcute de victime. Aceștia sunt persoane care, în cea mai mare parte a lor, au deja un profil infracțional dinaintea reprofilării pe atacuri de tip ransomware, ocupându-se anterior tot de infracțiuni din domeniul informatic (de exemplu phishing, carding etc.). Așa cum arată investigatorii, ransomware-ul este mai periculos pentru victime, dar mult mai profitabil pentru atacatori.

Raportul „Internet Organised Crime Threat Assessment 2021" realizat de Europol confirmă dezvoltarea modelului Ransomware as a Service, folosit de infractorii din întreaga lume pentru a orchestra atacuri cibernetice, aceștia neavând nevoie de cunoștințe tehnice foarte avansate. De asemenea, în urma atacurilor, autorii infracțiunilor cibernetice exfiltrează datele o dată cu blocarea acestora, șantajând victimele cu publicarea acestora în cazul în care nu vor plăti răscumpărarea.



Sursa: Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

BANKING TROJANS



După cum o sugerează numele, principala țintă a troienilor bancari este reprezentată de datele atașate conturilor și aplicațiilor bancare, fiind vizată atât infrastructura IT de la nivel de companie, dar cu o mai mare preponderență, utilizatorii de rând. Nu au un istoric îndelungat, existența și dezvoltarea acestora fiind concomitentă și direct proporțională cu dezvoltarea soluțiilor digitale de banking.

Asemeni categoriei mari a troienilor care acționează sub „acoperirea" unui soft legitim, softurile malițioase din categoria troian bancar vizează date precum: credențiale, număr de cont bancar, date de card, tranzacții și sume disponibile, etc..

Desigur, efectele nu se limitează doar la simplul acces și stocarea datelor bancare, urmărindu-se realizarea unor tranzacții fără aprobarea sau știința utilizatorului, și deturnarea fondurilor acestuia.

Troienii bancari pot fi ascunși în spatele unor jocuri, aplicații de mesagerie, aplicații de utilitate generală (web browsing) sau pot fi regăsți în conținutul mesageriilor digitale (ex.: email) sub forma unui link sau atașament contaminat, care permite eludarea sistemelor de securitate ale dispozitivelor pe care sunt instalate.

Troienii bancari nu reprezintă în mod imperativ un produs unic atribuit, gestionat de un singur individ sau o grupare fixă. Nu în puține cazuri, codurile sursă ale acestora sunt publicate și date spre vânzare persoanelor interesate. Prin urmare, apariția unor subvariante și derivații rezultate dintr-un cod sursă conduce la ceea ce putem intitula o familie malware.

Pe fondul migrației către dispozitivele portabile, tip smartphone, în dauna stațiilor desktop, specificul amenințărilor malware include orientarea către zona mobilă, primul troian bancar adaptat dispozitivelor mobile fiind detectat în 2014.

Una dintre cele mai populare tehnici este „overlay-malware", constând în afișarea unor ferestre false (imitative) peste aplicațiile utilizate, colectând astfel informațiile introduse în fereastra ce pare a fi cea pe care utilizatorul a dorit să o acceseze.

Mai mult, au capacitatea de a intercepta mesajele text (SMS), reușind astfel să treacă de soluțiile de siguranță implementate pentru autorizarea tranzacțiilor.

BANKING TROJANS

TIPURI

ZEUS

Apărut în 2007, este primul malware de tip bancar. Acesta colecta credențielele utilizatorilor și îi redirecționa pe aceștia către pagini web false, care imitau portalurile puse la dispoziție de către instituțiile bancare. Acesta a fost adaptat sistemelor de operare Microsoft. Fiind primul malware din această categorie, coroborat cu accesibilitatea îndelungată a codului acestuia, s-a ajuns la numeroase forme derivate ale acestuia, fără a fi detectate de noile sisteme de protecție și, implicit cu noi manifestări. În acest ultim câmp menționăm posibilitatea unor variante de a genera profit pentru atacatori prin sistemul pay-per-click. Zeus este strămoșul multor dintre troienii bancari actuali.

GOZI

Specializat în a încuraja utilizatorii să efectueze tranzacții în conturi care nu le aparțin. În varianta sa inițială, Gozi se folosea de componente tip rootkit (cod software care dă posibilitatea atacatorului de a utiliza un sistem din postura de administrator; totodată, acesta face posibilă accesarea sistemului de la distanță) pentru a-și ascunde activitatea, devenind nedetectabil. Precum în cazul Zeus, publicarea codului său sursă a condus la numeroase, noi și adaptate variante, actualmente fiind unul dintre troienii bancari cei mai longevivi.

BANKING TROJANS

TIPURI

SPYEYE

Descoperit în 2009, se baza pe înregistrarea secvenței de taste apăsate de utilizator (keylogger), respectiv colectarea datelor utilizatorilor prin intermediul generării de formulare. Specificul său este dat de tentativa de eliminare a altor troieni bancari (ex.: Zeus) de pe dispozitivele unde activa.

DYRE

Printre cele mai distructive soft-uri malițioase din această categorie, este cunoscut pentru daunele de zeci de milioane de dolari provocate unor bănci din S.U.A.. A fost primul troian care a utilizat pagini de logare în totalitate false, arhitectură modulară și care avea capacitatea de a replica răspunsurile emise de serverele bancare.

SHYLOCK

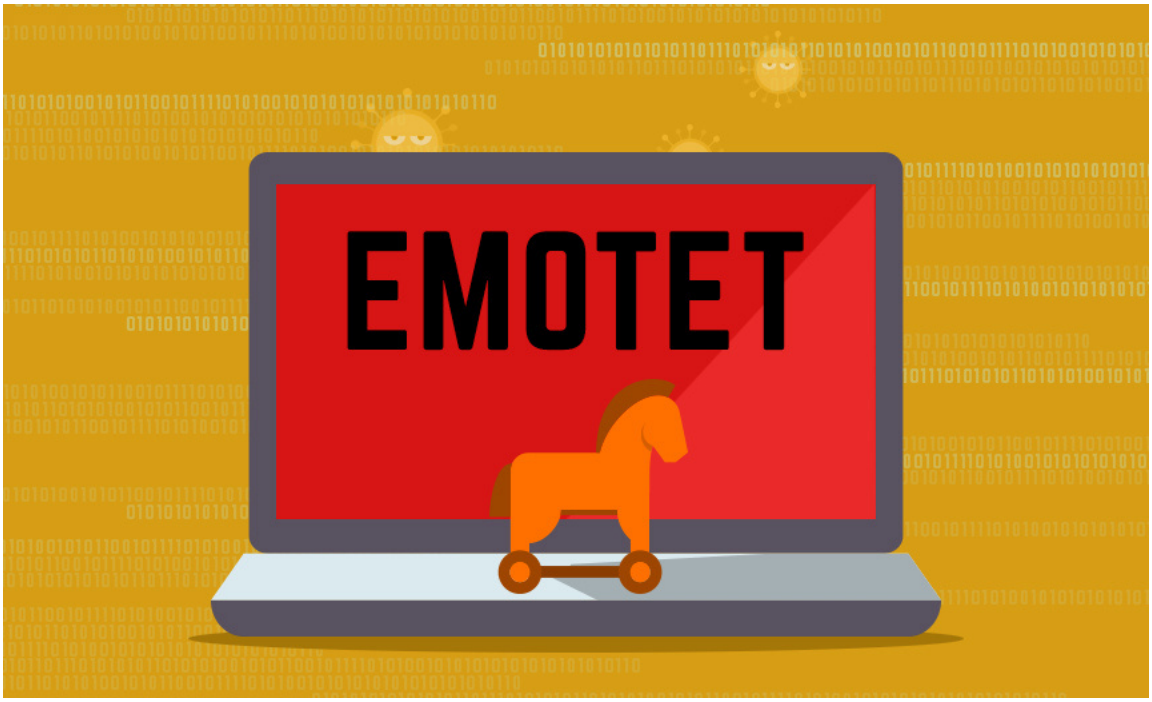
Campania a debutat în 2011 și s-a bazat pe colectarea datelor bancare ale utilizatorilor și înșelarea acestora pentru a transfera fonduri în conturile controlate de răufăcători. Spre deosebire de alte softuri malițioase din această sferă, Shylock a fost o proprietate privată, fără a fi supus comercializării pe piețe subterane. Totodată, arealul său de activitate a fost în mare restrâns la instituțiile bancare din Marea Britanie și S.U.A.. Creatorii săi l-au folosit după modelul unei afaceri/companii, care funcționa în baza unui program de lucru activitatea desfășurtându-se în intervalul orar 09 – 17.

BANKING TROJANS

TIPURI

EMOTET

Activitatea sa a fost observată începând cu 2014, fiind unul dintre troienii bancari cu cea mai mare adaptabilitate și inovativitate.
Acesta era livrat prin emailuri care conțineau linkuri sau fișiere atașate infectate. Odată instalat, computerul infectat era închiriat către alți atacatori care puteau instala alte tipuri de malware.
De asemenea, Emotet era un troian care își schimba codul după fiecare instalare, fiind imposibil de detectat de programele antimalware.
În ianuarie 2021, autoritățile de aplicare a legii din mai multe state au reușit să elimine botnet-ul Emotet.



INFOSTEALER

DEFINIȚIE

INFOSTEALER este un tip de troian proiectat să adune informații precum nume de utilizator și parole de la diverse conturi ale utilizatorului afectat, pe care le transmite ulterior către un alt sistem informatic.

METODE DE OBȚINERE A DATELOR

- Utilizarea browserului sau a altor aplicații pentru a fura datele introduse de utilizator
- Utilizarea web injection scripts, care adaugă noi câmpuri în formularele deja existente, informații ce odată introduse, sunt transmise către serverele atacatorilor
- Furtul informațiilor identificate în ferestrele pe care utilizatorul le are deschise
- Memorarea tastelor și a ordinii acestora pentru a accesa diferite conturi (keylogging)
- Furtul parolelor care sunt salvate în sistem și datele aferente fișierelor de tip cookies

INFOSTEALER

DATE CE POT FI FURATE

- Informațiile de pe cardul bancar, fie pentru a fi utilizate direct, fie pentru a fi vândute către alții
- datele de login de pe diverse aplicații pentru a fura achizițiile trecute și a le revinde (precum datele de autentificare ale jocurilor care au opțiunea de a face in-game purchases)
- datele de conectare de pe aplicații de cumpărături, plăți sau servicii online, în care cardul a fost asociat pentru facilitarea plăților ulterioare, atacatorii preluând astfel controlul asupra cardului și putând achiziționa servicii sau produse, fără a avea nevoie de informațiile scrise pe acesta
- datele de acces pot fi vândute în pachet către alți atacatori cibernetici care pot găsi noi metode de valorizare a acestora
- fotografii sau documente care pot fi utilizate pentru șantaj sau valorificate în alt mod
- datele de acces la crypto wallets

TOP INFOSTEALERS

- RedLine - distribuit prin campanii de phishing ce făceau referire la pandemia de COVID-19
- Raccoon - foarte popular în rândul atacatorilor deși nu este complex
- Agent Tesla - capabil să exfiltreze datele din browser, are capacități de keylogging și posibilitatea de a face screenshot-uri

OPERAȚIUNI DE SUCCES

Lupta împotriva criminalității informatice este esențială pentru asigurarea securității tot mai multor indivizi, companii, instituții publice sau servicii esențiale. Infractorii găsesc noi modalități de atac, iar instituțiile de aplicare a legii trebuie să evolueze constant pentu combaterea fenomenului.

Cooperarea internațională este indispensabilă în această luptă având în vedere că atacatorii cibernetici pot acționa de oriunde, oricând, fără să fie necesar ca aceștia să locuiască sau să acționeze în spațiul geografic al unei singure țări.

În noiembrie 2020, Poliția Română, alături de alți parteneri externi, a condus o operațiune în urma căreia doi suspecți care ar fi condus serviciile de criptare CyberSeal și Dataprotector au fost arestați.
Serviciile oferite de aceștia au fost achiziționate de peste 1560 de atacatori cibernetici.
Cei doi administratori gestionau și serviciul Cyberscan, ce le permitea clienților acestora să își testeze programele de malware, pentru a se asigura că nu vor fi detectate de programe antivirus.

OPERAȚIUNI DE SUCCES

În luna noiembrie 2021, în cadrul operațiunii GOLD DUST, Poliția Română, împreună cu D.I.I.C.O.T. – Structura Centrală, a efectuat percheziții domiciliare la persoane bănuite de implicare în distribuirea aplicațiilor malițioase de tip ransomware Sodinokibi/Revil și GandCrab, doi dintre bănuiți fiind reținuți.

Persoanele bănuite au aderat încă din 2018 la mai multe grupări internaționale de criminalitate organizată, constituite online, ce funcționează după modelul Ransomware as a Service (RaaS).

Cele două „familii de ransomware" GandCrab și Revil/ Sodinokibi au fost două dintre cele mai prolifice de acest gen și au afectat numeroase victime din toată lumea, atât din sectorul public, cât și din cel privat, membrii grupării reușind să obțină câștiguri ilicite estimate la ordinul zecilor de milioane de dolari.

Totodată, în urma acestei investigații au fost dezvoltate instrumente de decriptare a fișierelor afectate de aceste tipuri de ransomware, ce au fost ulterior puse la dispoziția victimelor prin intermediul site-ului dezvoltat de Europol „No More Ransom".

OPERAȚIUNI DE SUCCES

În decembrie 2021, Poliția Română, cu sprijinul F.B.I. și al Centrului European de Criminalitate Cibernetică (EC3) al Europol, a arestat o persoană suspectată că ar fi compromis rețeaua unei mari companii de IT românești care livrează servicii clienților din sectoarele de retail, energie și utilități, prin intermediul malware-ului de tip ransomware, acesta fiind afiliat al unei rețele ce dezvolta astfel de aplicații.

Acesta ar fi furat date sensibile de la clienții companiei IT din România și din străinătate, criptându-le ulterior fișierele. Informațiile obținute includeau date financiare ale companiilor, informații personale despre angajați, detalii ale clienților și alte documente importante. Suspectul ar fi cerut apoi o răscumpărare considerabilă în criptomonede, amenințând că va divulga datele aflate în posesia sa pe forumurile de criminalitate cibernetică în cazul în care cerințele nu sunt îndeplinite.

OPERAȚIUNI DE SUCCES

În luna aprilie 2022, în cadrul operațiunii TOURNIQUET, unul dintre cele mai mari forumuri pentru hackeri pe care aceștia îl foloseau pentru schimbul de date și pentru orchestrarea altor atacuri, a fost închis. Această operațiune a putut fi realizată după un an în care instituțiile de aplicare a legii din Statele Unite ale Americii, Marea Britanie, Suedia, Portugalia și România au colaborat sub coordonarea Europol pentru a identifica și stabili ce roluri jucau în cadrul rețelei fiecare dintre membri. Urmare a acestei operațiuni, administratorul forumului și doi complici au fost arestați.

Sursa: https://www.europol.europa.eu/media-press/newsroom/news/one-of-world%E2%80%99s-biggest-hacker-forums-taken-down

POLIȚIA ROMÂNĂ

Pentru mai multe informații, accesați
https://sigurantaonline.ro