RO

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

ianuarie 2019 – aprilie 2020

Ransomware (programele de șantaj digital)

Raportul ENISA privind situația amenințărilor

Prezentare generală

Programele ransomware au devenit o armă populară în mâinile actorilor rău intenționați care încearcă să prejudicieze în fiecare zi guverne, companii și persoane. În astfel de cazuri, victimele programelor ransomware pot suferi pierderi economice fie plătind răscumpărarea cerută, fie plătind costul recuperării pierderii dacă nu dau curs solicitărilor atacatorului. Într-un incident din 2019, Baltimore, Maryland a suferit un blocaj și se preconizează că recuperarea va costa 18,2 milioane USD (aproximativ 15,4 milioane EUR), deși orașul a refuzat să plătească răscumpărarea.[1] Odată cu numărul tot mai mare de incidente, este evident că posibilitatea de a deveni victima unui astfel de incident nu este o chestiune de eventualitate, ci mai degrabă de moment. Cu toate acestea, majoritatea eforturilor țărilor de combatere a programelor ransomware trebuie să includă abordarea mai multor provocări, cum ar fi lipsa de coordonare și colaborare între agenții și autorități și lipsa legislației care incriminează în mod clar atacurile ransomware.

Deși polițele de asigurare cibernetică există de la începutul anilor 2000[2], atacurile ransomware reprezintă unul dintre principalele motive pentru interesul crescut pentru acest tip de asigurare din ultimii 5 ani. În unele dintre incidentele din 2019[7], răscumpărarea sau costurile recuperării au fost acoperite de astfel de contracte. Din păcate, dacă se știe că potențialele ținte ale programelor ransomware sunt asigurate, atacatorii presupun că cel mai probabil vor fi plătiți. Un alt dezavantaj pentru victimă este că furnizorii de asigurări plătesc răscumpărarea în avans pentru a atenua impactul daunelor și pentru a păstra intactă reputația victimei. Cu toate acestea, o astfel de conformare prin plata răscumpărărilor încurajează comunitatea hackerilor și nu garantează nici recuperarea victimei, nici reputația acesteia.[3]

Constatări

*10,1*_miliarde EUR estimate a fi plătite sub formă de răscumpărări în 2019

Cuantumul răscumpărărilor plătite a fost cu 3,3 miliarde EUR mai mare decât în 2018.

*365 %*_creștere a depistărilor în cadrul întreprinderilor în 2019

Depistarea de ransomware în dispozitive din mediile de afaceri a crescut comparativ cu prima jumătate a anului 2018.[22]

*66 %*_din organizațiile din domeniul medical au suferit un atac

Peste 66 % din organizațiile din domeniul medical au suferit un atac de tip ransomware în 2019.[23]

*45 %*_din organizațiile atacate au plătit răscumpărarea

Acesta este procentul de organizații atacate în 2019 care au plătit răscumpărarea, iar jumătate dintre acestea tot și-au pierdut datele.[37]

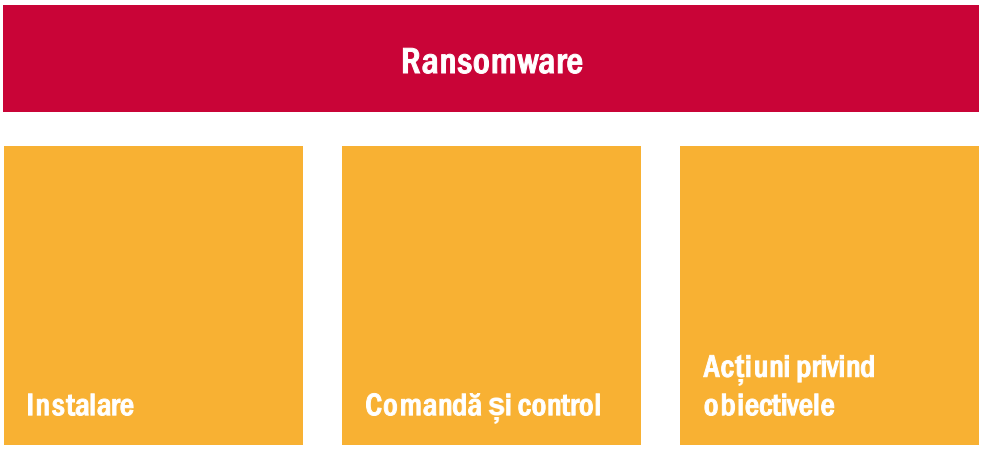
*28 %*_din incidentele de securitate au fost atribuite programelor malware

Programele ransomware au reprezentat a doua cea mai frecventă funcționalitate după malware C2 și au fost asociate cu o treime (28 %) din incidentele de securitate.[32]

Kill chain

Etapă din fluxul de activitate de atac

Amploarea scopului



Cadrul Cyber Kill Chain® a fost dezvoltat de Lockheed Martin, fiind adaptat după un concept militar legat de structura unui atac. Pentru a studia un anumit vector de atac, utilizați această diagramă kill-chain pentru a trasa fiecare etapă a procesului și a face referire la instrumentele, tehnicile și procedurile utilizate de atacator.

MAI MULTE INFORMAȚII

Descriere

_Ransomware țintește mai sus

Atacurile cu ransomware din primul și al doilea trimestru al anului 2019 au fost mai puține decât cele înregistrate în aceeași perioadă din ultimii 3 ani. Cu toate acestea, atacurile ransomware respective s-au concentrat asupra unor ținte de profil înalt. În cursul anului 2018, s-a observat trimiterea troianului de acces la distanță (RAT), a programelor de descărcare și backdoor, dar în acel an respectivul malware a rămas inactiv.[9,10] Acum s-a ajuns la concluzia că software-ul în cauză a oferit atacatorilor informații pentru a identifica ținte vulnerabile importante, dispuse să plătească sume mai mari de răscumpărare. Urmând această direcție, în anul de raportare, ransomware-ul s-a extins în alte sectoare dincolo de industria medicală, vizând întreprinderi din sectorul industrial și manufacturier. Recent, familia de ransomware LockerGoga a fost folosită pentru a deteriora sistemele care controlează echipamentul fizic din fabricile de producție.[11]

_Asigurările împotriva riscurilor cibernetice sunt mai populare

În 2019, polițele de asigurare împotriva riscurilor cibernetice au reprezentat o piață de 8 miliarde USD (aproximativ 6,7 miliarde EUR) numai în Statele Unite. Deși astfel de produse există de la bug-ul Y2K sau Millennium, în ultimii ani ele au devenit mai atrăgătoare pentru organizații guvernamentale, orașe, organizații din domeniul medical și alte câteva ținte potențiale cu risc mare de ransomware. Atacul SamSam din Atlanta, Georgia și incidentul din Lake City, Florida, au fost acoperite de astfel de polițe.[16] Pe măsură ce cererile de răscumpărare cresc, polițele de asigurare împotriva riscurilor cibernetice devin din ce în ce mai necesare pentru organizații și companii. Cu toate acestea, bunul simț sugerează că victimele trebuie să evite să cedeze cererilor, dacă este posibil. Atunci când se dă curs cererilor de răscumpărare, atacatorul nu numai că este încurajat să repete actul, dar este posibil și ca victima să nu își recupereze datele, deoarece în multe cazuri atacatorul nu respectă partea sa din înțelegere.

_Protocolul de acces la distanță deschis (Remote Desktop Protocol – RDP) este un risc mare

Mai multe familii de ransomware de succes, cum ar fi SamSam, BitPaymer și CrySiS, vizează serverele RDP pentru a iniția un atac.[20] Din păcate, multe organizații folosesc în continuare RDP în locul rețelei private virtuale (VPN) mai sigure pentru acces la distanță. Problemele cu RDP constau în faptul că suferă de vulnerabilități care pot fi exploatate, iar serviciul RDP se poate baza pe servere care au acces la internet și care sunt ușor de accesat. S-a raportat că peste 800 000 de sisteme cu servicii RDP sunt necorectate și vulnerabile; printre acestea se numără sisteme din gama IP a centrului de date Microsoft Azure.[51] Deși Microsoft a asigurat publicul că aceste sisteme aparțin unui terț, apare o problemă cu privire la securitatea furnizorilor de servicii cloud.

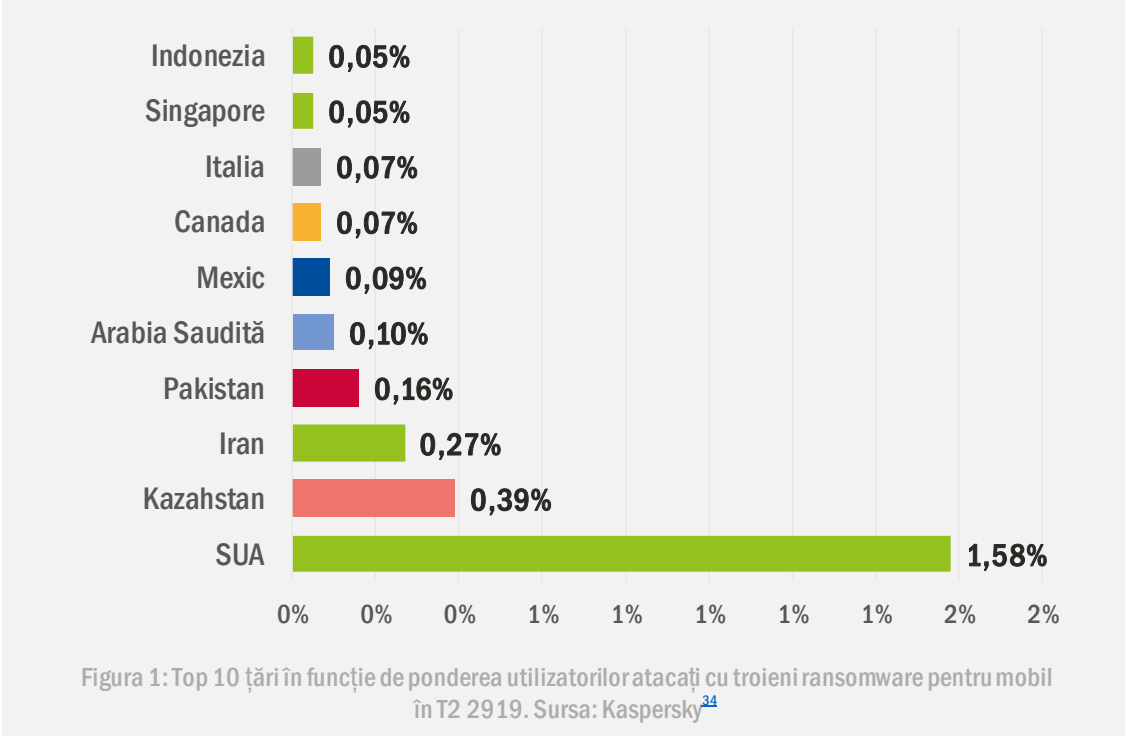


Figura 1: Top 10 țări în funcție de ponderea utilizatorilor atacați cu troieni ransomware pentru mobil în T2 2919. Sursa: Kaspersky[34]

Descriere

_ Cel mai căutat

LOCKERGOGA_ a fost raportat pentru prima dată în ianuarie 2019 într-un atac asupra companiei franceze de consultanță în inginerie Altran Technologies.[40] Rețelele sale informatice și toate aplicațiile au căzut și au fost afectate operațiunile companiei în mai multe țări. LockerGoga este livrat și executat de instrumentul PsExec, care este un înlocuitor ușor de telnet, care poate trece peste unele verificări de securitate ca software semi-valid.[11] Odată instalat, conturile de utilizator din sistemul vizat sunt modificate și sistemul este deconectat forțat. În plus, fișierele cu instrumente sunt auto-redenumite și auto-mutate și, ca urmare, devin aproape imposibil de localizat. În versiunile ulterioare ale LockerGoga, blocarea este atât de completă încât victimele nici măcar nu pot vedea nota de răscumpărare sau instrucțiunile de recuperare, chiar dacă sunt îndeplinite cererile. Doar câteva produse anti-malware și anti-virus sunt capabile să detecteze și să apere sistemele împotriva LockerGoga și nu există un decriptor specific.[10] În afară de Altran Technologies, NorskHydro și două întreprinderi din industria chimică din SUA, Hexion și Momentive au fost vizate de LockerGogain în 2019.[41] Numai pentru atacul NorskHydro, costul pagubelor a fost estimat la 50 de milioane USD (aproximativ 42 de milioane EUR).[21]

KATYUSHA_ este un troian ransomware folosit pentru prima dată în octombrie 2018. Acesta criptează fișierele victimei, șterge copiile-umbră și livrează atașamente prin e-mail. Katyusha folosește exploit-urile EternalBluean și DoublePulsar pentru a se răspândi.[45] Din păcate, încă nu este disponibil niciun instrument sau decriptor pentru apărare.

JIGSAW_ nu numai că criptează fișierele victimei, dar le și șterge dacă cererile nu sunt îndeplinite , cel mai frecvent, în 24 de ore. Mai mult, dacă victima încearcă, de exemplu, să-și închidă calculatorul, rata de ștergere crește. Nu este un accident că acest ransomware a fost numit după un personaj de film de groază.[45] Cu toate acestea, companiile de securitate lansează în mod constant actualizări pentru un decriptor Jigsaw eficient.[46]

PEWCRYPT_ a fost creat la începutul anului 2019 și, spre deosebire de majoritatea programelor ransomware, singurul său obiectiv este de a forța oamenii să se aboneze la canalul YouTuber-ului PewDiePie. PewDiePie s-a aflat într-o competiție de popularitate cu un canal indian din Bollywood, T-Series, și fanii săi au decis să folosească PewCrypt pentru a spori șansele de câștig ale idolului lor. PewCrypt este un ransomware tipic răspândit prin mesaje spam și reclame online rău intenționate. A fost creat în limbajul de programare Java. În martie 2019, autorul însuși a lansat un instrument de decriptare.[47]

RYUK_ a apărut pentru prima dată în august 2018 și s-a presupus că este asociat cu grupuri de hacking nord-coreene. În curând, autorii Ryuk s-au dovedit a fi același grup care a devenit cunoscut pentru că a utilizat ransomware-ul Hermes furându-i în același timp codul. Principalele caracteristici ale Ryuk sunt utilizarea algoritmilor militari și atacurile sale țintite asupra marilor întreprinderi. Mai mult, majorității victimelor sale li se cere să plătească răscumpărarea în Bitcoin.[45]

DHARMA_ este un virus cripto care a apărut pentru prima dată în 2016, dar în continuare sunt lansate versiuni noi. Dharma nu numai că criptează fișierele victimei, ci și șterge orice copie-umbră. În 2019, acesta a fost răspândit prin fișiere contaminate cu extensii populare, dăunătoare sau legitime, cum ar fi „.gif", „.AUF", „.USA", „.xwx", „.best" și „.heets". În septembrie 2019, un cercetător în domeniul securității a lansat Rakhnidecryptor[42] pentru a ajuta victimele Dharma să-și decripteze fișierele.

GANDCRAB_ a fost utilizat pentru prima dată în ianuarie 2018 și a infectat peste 50 000 de sisteme în mai puțin de o lună, devenind unul dintre cele mai populare programe ransomware din 2018.[43] Acesta exploatează macrocomenzile Microsoft Office, VBScript și PowerShell pentru a ataca fără a fi detectat.[45] GandCrab este similar cu Cerber, se bazează pe modelul ransomware-as-a-service (ransomware ca serviciu)(RaaS) și permite dezvoltatorilor și infractorilor să împartă profitul. O echipă alcătuită de Europol, Poliția Română, Procuratura Generală și Bitdefender a reușit să creeze un instrument de decriptare[44] după ce a piratat serverele GandCrab. Operatorii GandCrab și-au anunțat retragerea în trimestrul doi al anului 2019 după ce au încasat peste 2 miliarde USD în plăți de răscumpărare. Cu toate acestea, ransomware-ul Sodinokibi, care este observat în campanii mici, se presupune a fi succesorul lui GandCrab.[10]

Descriere

_ Cel mai căutat

REVIL sau SODINOKIBI sau SODIN_ a apărut pentru prima dată într-un atac web asupra instrumentului italian WinRAR în iunie 2019. De asemenea, acesta este suspectat că ar fi implicat în trei atacuri MSP și un al patrulea împotriva companiei americane PerCSoft, a cărei clientelă provine în principal din sectorul sănătății.[48] Sodinokibi pare a fi un produs al binecunoscutului grup de spionaj cibernetic FruityArmor, care este activ din 2016. Sodinokibi a afectat mai multe țări din întreaga lume. Taiwan a suferit până în prezent 17,56 % din toate atacurile Sodinokibi înregistrate, devenind astfel țara cea mai vizată de Sodinokibi. În Europa, cele mai vizate țări sunt Germania (8,05 %), Italia (5,12 %) și Spania (4,88 %). Sodinokibi este distribuit de un model RaaS și criptează fișierele necesare pentru ca un atac să aibă loc într-un mod per-sistem. Atacatorii încorporează o „cheie schelet" în codul lor, permițându-le să decripteze fișierele de la distanță, indiferent de criptarea originală.[49] Cu toate acestea, dacă un computer are tastatură rusească, armeană, siriană sau de altă natură, nu este posibil ca Sodinokibi să îl cripteze, fapt care indică probabil originea autorilor.[50]

SAMSAM_ continuă să vizeze infrastructura critică la nivel global pentru al cincilea an consecutiv. Atacurile SamSam se concentrează în principal pe spitale, companii din domeniul sănătății și organizații guvernamentale pentru a asigura plata rapidă a unor răscumpărări mari. Acesta exploatează vulnerabilitățile RDP. Până în prezent, grupul responsabil de distribuirea SamSam a strâns peste 6 milioane USD (aproximativ 5 milioane EUR) în plăți de răscumpărare și le-a costat pe victime peste 30 de milioane USD (aproximativ 25,4 milioane EUR).[45] Numai în urma atacului din 2018 împotriva orașului Atlanta, daunele și costurile de recuperare s-au ridicat la 17 milioane USD (aproximativ 14,4 milioane EUR).[43]

„Sofisticarea capacităților de amenințare a crescut în 2019, mulți adversari folosind exploit-uri, furtul de date de identificare și atacurile în mai multe etape.”

în ETL 2020

Descriere

_ Sectoare vizate

STATELE-NAȚIUNE SUNT ÎNCĂ ÎN CENTRUL ATENȚIEI_ În 2018, ransomware-ul a fost folosit pentru a viza organizații ale statelor-națiune ca instrument de a face bani. Această tendință a continuat în 2019, când națiunile sau grupurile naționale și-au deghizat identitatea utilizând aceleași instrumente create de alte grupuri sau actori ai statului-națiune. Această manipulare a instrumentelor permite ca originea atacatorului să rămână ascunsă și ca națiunea lor să evite orice consecințe diplomatice, mai ales atunci când ținta este o organizație guvernamentală sau de stat.

În 2019, au avut loc mai multe atacuri împotriva organizațiilor guvernamentale sau de stat, cum ar fi cel în care orașului californian Lodi[4] i s-a cerut să plătească 400 000 USD (aproximativ 340 000 EUR) ca răscumpărare pentru a deblocarea liniilor telefonice ale Departamentului de poliție, liniei de urgență a Departamentului de lucrări publice, numerelor primăriei și ale sistemelor financiare și de date de plată ale orașului. Orașul a refuzat să se conformeze și și-a revenit din atac folosind copii de rezervă. În august 2019, Departamentul de resurse informaționale din Texas a raportat un atac ransomware coordonat asupra a 23 de mici organizații guvernamentale.[5] Costul pentru ținutul Texas a fost estimat la 3,25 milioane USD (aproximativ 2,75 milioane EUR). Baltimore a suferit un atac RobbinHood care a provocat un prejudiciu de 18,2 milioane USD (aproximativ 15,4 milioane EUR), în timp ce Lake City din Florida a fost victima unui atac Ryuk care a provocat o pierdere de 460 000 USD (aproximativ 389 768 EUR). Orașul New Bedford din Massachusetts a fost lovit, de asemenea, de un atac de răscumpărare în iulie 2019(6) și i s-a cerut plata unei răscumpărări de 5,3 milioane USD (aproximativ 4,4 milioane EUR). Orașul a refuzat să plătească răscumpărarea și a cheltuit în schimb 1 milion USD pentru a-și reveni după atac.[7]

INSTITUȚIILE DE ÎNVĂȚĂMÂNT SE ALĂTURĂ VICTIMELOR_ În cursul anului 2019, s-a observat o reorientare a atacurilor către instituțiile de învățământ. Conform unui raport publicat de compania de securitate Emsisoft, 1 051 de școli și colegii au fost victimele unui număr de 62 de incidente ransomware. În 2018, doar 11 incidente au afectat instituții de învățământ. În raport se afirmă că școlile americane au constituit a doua cea mai frecventă categorie de victime după municipalitățile locale.[8]

SECTORUL SĂNĂTĂȚII CONTINUĂ SĂ SUFERE_ Organizațiile din domeniul medical au fost ținta preferată a atacatorilor ransomware în toți anii precedenți și această tendință a continuat și în 2019. Furnizorii californieni de servicii medicale Wood Ranch Medical au fost atacați în timpul verii, iar fișele medicale electronice ale companiei au fost complet distruse (inclusiv copiile de rezervă) ca urmare a refuzului acestora de a plăti răscumpărarea. Incidentul a forțat Wood Ranch Medical să anunțe că va înceta să funcționeze până la sfârșitul anului.[12] În aprilie 2019, aceeași succesiune exactă de evenimente a vizat un alt furnizor de servicii medicale, Centrul Brookside ENT and Hearing din Michigan[13], care, de asemenea, a fost forțat să înceteze activitatea. Mai mult, în Australia, au fost atacate două grupuri de spitale : GippslandHealth Alliance și South West Alliance of Rural Health. Rezultatul a fost că spitalele din mai multe orașe, inclusiv Warrnambool, Colac, Geelong, Warragul, Sale și Bairnsdale, nu au putut efectua pacienților procedurile normale deoarece sistemele lor s-au deconectat pentru a limita expunerea.[14] În acest sector, pierderea de date este la fel de dăunătoare ca pierderea financiară. De exemplu, informațiile protejate privind sănătatea a peste 300 000 de pacienți au fost dezvăluite ca urmare a unui atac ransomware lansat în iunie 2019 împotriva grupului Premier Family Medical din Utah.[15]

MSP AU PICAT_ Numeroase industrii se bazează pe furnizorii de servicii gestionate (MSP) și furnizorii de servicii cloud (CSP) pentru a găzdui informații sensibile, care sunt esențiale pentru operațiunile lor. De asemenea, acestea se bazează pe astfel de furnizori pentru integritatea datelor și prevenirea accesului neautorizat la acestea.[17] Cu toate acestea, programele ransomware GandCrab și Sodin vizează vulnerabilitățile din MSP-urile care le expun infrastructura și datele pe care le găzduiesc și, în cele din urmă, permit ca atacul ransomware să se răspândească la întreaga clientelă MSP. Webroot2FA, un instrument MSP comun, încorporează astfel de vulnerabilități și a fost utilizat în mai multe cazuri în cursul anului 2019.[18] Anul acesta, într-o perioadă de doar trei luni au fost atacați mai mulți MSP, cum ar fi PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. și IT By Design.[19]

Vectori de atac

_ Cum

Un nou ransomware numit Sodinokibi exploatează vulnerabilitatea recent anunțată CVE-2019-2725 Oracle WebLogic Server pentru a obține capacități de executare a codului la distanță. Victima este infectată fără a face nimic. Au fost lansate, de asemenea, patch-uri oficiale pentru versiunile Oracle WebLogic Server 10.3.6.0 și 12.1.3.0.[51] Același atac exploatează vulnerabilitatea CVE-2018-8453 pentru a obține mai multe privilegii de utilizator (ridicate), a sista procese de pe lista neagră, a șterge fișierele de pe lista neagră și a elimina informațiile despre gazdă.[48]

O altă vulnerabilitate, CVE-2019-0708, este utilizată, de asemenea, pentru instalarea programului ransomware. Aceasta permite conexiunea neautorizată prin protocolul desktop la distanță (RDP) al Microsoft. În mai 2019, Microsoft a lansat patch-uri pentru versiunile curente ale sistemului de operare (OS), precum și pentru versiunile care nu mai sunt acceptate.[51]

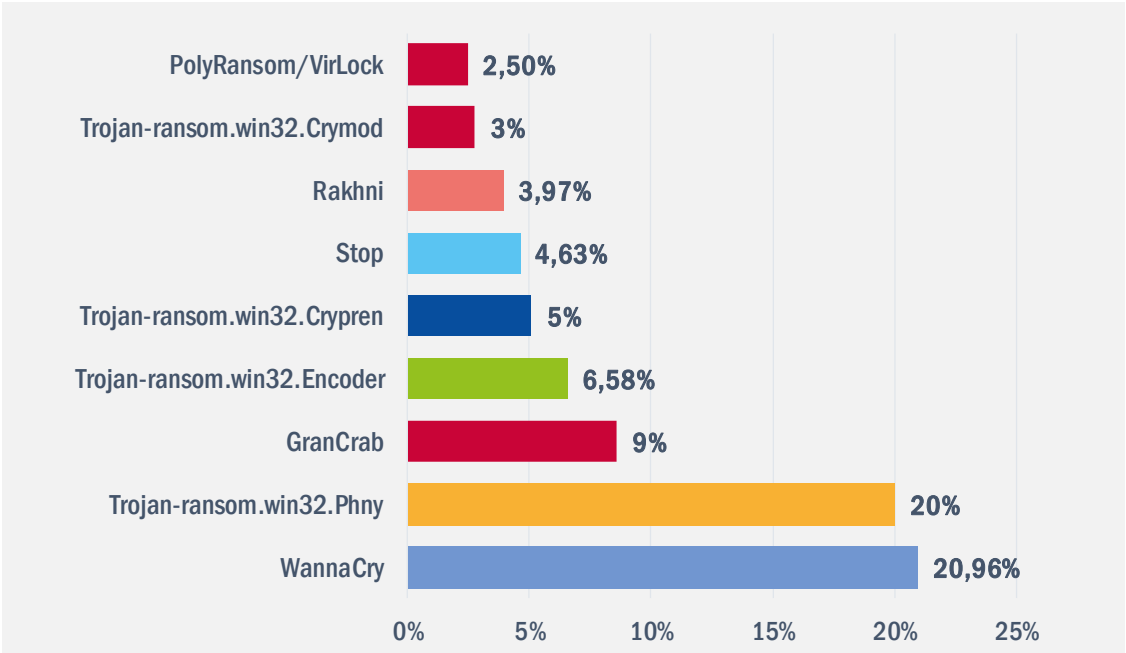


Figura 2: Cele mai importante atacuri ransomware din 2019. Sursa: Kaspersky[39]

Incidente

- Incidentul Baltimore County[1]
- Atacul de la spitalele din Alabama[7]
- Incidentul din orașul Lodi, California[4]
- Incidentul din Texas (Departamentul pentru resurse informaționale din Texas)[5]
- Atacul Ryuk din Lake City (Florida)[7]
- Incidentul din New Belford (Massachusetts)[6]
- Atacuri ransomware la peste 500 de școli și universități[8]
- Cazul Wood Ranch Medical (California)[12]
- Incidentul de la Centrul Brookside ENT and Hearing din Michigan[13]
- Incidentele de la Gippsland Health Alliance și South West Alliance of Rural Health (Australia)[14]
- Incidentul de la grupul Premier Family Medical (Utah)[15]
- Incidentele de la MSPs PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. și IT By Design[19]
- Incidentul de la centrul de date Microsoft Azure[51]
- Atacul de la Altran Technologies LockerGoga[40]
- Atacul de la Norsk Hydro LockerGoga[7]
- Atacurile de la Hexion și Momentive LockerGoga[41]
- Incidentul Albany IT[60]
- Incidentul din Jackson County (Georgia)[61]
- Incidentul Riviera Beach (Florida)[62]
- Incidentul din New Orleans[63]
- Atacul de la producătorul danez de aparate auditive Demant[64]

Măsuri de atenuare

Acțiuni propuse

- Păstrarea de copii de siguranță fiabile care respectă regula 3-2-1 (adică păstrarea a cel puțin trei copii, în două formate diferite, păstrând una dintre copii în afara sediului).[5]
- Investirea într-o poliță de asigurare cibernetică care acoperă daunele provocate de atacurile ransomware.[21]
- Utilizarea segmentării rețelei, criptarea datelor, controlul accesului și aplicarea politicilor pentru a asigura expunerea minimă a datelor.
- Folosirea de metode precum monitorizarea pentru a identifica rapid infecțiile.
- Monitorizarea accesului și a stării infrastructurii publice utilizate.
- Crearea unui centru de operațiuni de securitate (SOC) cu personal calificat în domeniul securității în cadrul fiecărei organizații sau companii.
- Utilizarea de instrumente adecvate și actualizate pentru prevenirea ransomware-ului.
- Definirea exactă și aplicarea unui set minim de drepturi de acces la datele utilizatorului pentru a minimiza impactul atacurilor (adică mai puține drepturi, mai puține date criptate).
- Aplicarea unui management robust al vulnerabilității și al patch-urilor.
- Aplicarea filtrării conținutului pentru a filtra atașamentele nedorite, e-mailurile cu conținut rău intenționat, spamul și traficul de rețea nedorit.
- Instalarea de protecție a punctului final prin intermediul programelor antivirus, dar și prin blocarea executării fișierelor (de exemplu, blocarea execuției în folderul Temp).
- Utilizarea unor politici pentru a controla dispozitivele externe și accesibilitatea portului.
- Utilizarea listei albe pentru a preveni executarea executabilelor necunoscute la punctele finale.
- Realizarea de investiții în creșterea gradului de conștientizare a utilizatorilor cu privire la ransomware, în special referitor la comportamentul de navigare securizat.

_Decriptori

EUROPOL și 163 de parteneri au realizat progrese semnificative[7] cu proiectul „No more ransom”[71]. Portalul a adăugat 28 de instrumente în 2019 și în prezent poate decripta 140 de tipuri diferite de infecții cu ransomware.[65] Au fost dezvoltați câțiva decriptori de ransomware și mulți alții au fost actualizați. Mai jos sunt enumerate câteva exemple.

RANSOMWARE	DECRIPTOR
Aurora[52], Muhstik[53], Ryuk[54]	Emsisoft
Rakhni, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Democry, TeslaCrypt, Chimera, Crysis, Jaff, Dharma, Cryakl, Yatron, FortuneCrypt,[55,56]	Kaspersky Lab
GandCrab[44]	Europol, Poliția Română și GPO, Bitfender
Jigsaw[46]	Avast
Mira[57]	F-Secure
Nemty[58]	Tesorion
PewCrypt[47]	autorul PewCrypt

Referințe

1. „Washington idle as ransomware ravages cities big and small" (Washingtonul nu face nimic, în timp ce ransomware-ul distruge orașe mari și mici), 28 septembrie 2019. Politico. https://www.politico.com/news/2019/09/28/ransomware-cities-washington-007376

2. „What you – and your company – should know about cyber insurance" (Ce ar trebui să știți dumneavoastră – și compania dumneavoastră – despre asigurările cibernetice), 20 august 2019. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

3. „The State of Ransomware in 2019" (Situația ransomware-ului în 2019),

17 iunie 2019. IT Pro Today. https://www.itprotoday.com/threat-management/state-ransomware-2019

4. „California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware" (California City confirmă întreruperile liniei telefonice și ale sistemului de date financiare cauzate de ransomware). 2 august 2019. Trend Micro. https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware

5. „Coordinated Ransomware Attack Cripples Local Government Organizations in Texas" (Atac ransomware coordonat blochează organizații guvernamentale locale din Texas), 19 august 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coordinated-ransomware-attack-cripples-local-government-organizations-in-texas

6. „The State of Ransomware in the US: Report and Statistics 2019" (Situația ransomware-ului în SUA: raport și statistici 2019). 12 decembrie 2019. EMSISOFT blog. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

7. „Alabama hospitals have been hit by a massive ransomware attack" (Spitalele din Alabama au fost lovite de un atac ransomware masiv), 3 octombrie 2019. https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

8. „500+ Schools Have Been Affected by Ransomware in 2019" (Peste 500 de școli au fost afectate de ransomware în 2019), 4 octombrie 2019. Campus Safety, https://www.campussafetymagazine.com/safety/500-schools-ransomware-2019/

9. „Latest Quarterly Threat Report - Q1 2019" (Ultimul raport trimestrial privind amenințările – T1 2019), 2019. Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

10. „Proofpoint Q2 2019 Threat Report - Emotet's hiatus, mainstream impostor techniques, and more" (Raport Proofpoint T2 2019 privind amenințările – discontinuitatea Emotet, tehnicile impostor tradiționale și altele). 9 septembrie 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques

11. „6 of the Biggest Cybersecurity Crises of 2019 (So Far)" [6 dintre cele mai mari crize de securitate cibernetică din 2019 (până acum)], 24 septembrie 2019. Blogul Consiliului EC. https://blog.eccouncil.org/6-of-the-biggest-cybersecurity-crises-of-2019-so-far/

12. „Ransomware Attacks Double in 2019: Medical Providers Can't Recover and Shut Down" (Atacurile ransomware se dublează în 2019: furnizorii medicali nu se pot reface și încetează activitatea), 3 octombrie 2019. https://www.natlawreview.com/article/ransomware-attacks-double-2019-medical-providers-can-t-recover-and-shut-down

13. „Michigan's Brookside ENT and Hearing Center forced to close due to a Ransomware Attack" (Centrul Brookside ENT and Hearing din Michigan este obligat să înceteze activitatea din cauza unui atac ransomware), 23 aprilie 2019. SPAM Fighter. https://www.spamfighter.com/News-22154-Michigans-Brookside-ENT-and-Hearing-Center-forced-to-close-due-to-a-Ransomware-Attack.htm

14. „Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack" (Spitale din statul Victoria din Gippsland, Geelong și Warrnambool au fost lovite de un atac ransomware). 1 octombrie 2019. https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

15. „Ransomware Attack Affects 300,000 Patients in Utah" (Atac ransomware afectează 300 000 de pacienți din Utah). 12 septembrie 2019. CISO Mag. https://www.cisomag.com/ransomware-attack-affects-300000-patients-in-utah/

16. „The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks" (Economia extorsiunii: cum asigură companiile de asigurări o creștere a numărului de atacuri ransomware). 27 august 2019. ProPublica. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

17. „CYBER THREATSCAPE REPORT" (Raportul privind peisajul amenințărilor cibernetice). 2019. Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

18. „Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread" (Numărul de programe ransomware crește de 3 ori în T2 pe măsură ce Ryuk și Sodinokibi se răspândesc). 2019. Coveware. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

19. „Armor Identifies 15 New Ransomware Victims in the Last 2 Weeks, All of them Educational Institutions – Threat Intelligence" (Armor identifică 15 noi victime ale programelor ransomware în ultimele 2 săptămâni, toate fiind instituții de învățământ – informații despre amenințări). 20 septembrie 2019. Armor. https://www.armor.com/resources/armor-identifies-10-new-ransomware-victims-in-the-past-9-days/

20. „4 Ransomware Trends to Watch in 2019" (4 tendințe ransomware de urmărit în 2019). 13 februarie 2019. https://www.recordedfuture.com/ransomware-trends-2019/

21. „BDO Cyber Threat Insights - 2019 2nd Quarter Report" (Analiza BDO privind amenințările cibernetice – Raportul pentru al doilea trimestru din 2019), iulie 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

22. „BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare" (Raportul BDO din toamna anului 2019 privind amenințările cibernetice: accent pe asistența medicală). Octombrie 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

23. „Healthcare Cyber Heists in 2019" (Furturi cibernetice în domeniul sănătății în 2019), 3 octombrie 2019. VMWare. https://www.carbonblack.com/resources/threat-research/healthcare-cyber-heists-in-2019/

24. „Australia | Global Threat Report | Defender Power On The Rise" (Australia | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/australia-global-threat-report-defender-power-on-the-rise/

25. „France | Global Threat Report | Defender Power On The Rise" (Franța | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/france-global-threat-report-defender-power-on-the-rise/

26. „Italy | Global Threat Report | Defender Power On The Rise" (Italia | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/italy-global-threat-report-defender-power-on-the-rise/

27. „Japan | Global Threat Report | Defender Power On The Rise" (Japonia | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/japan-global-threat-report-defender-power-on-the-rise/

28. "Canada | Global Threat Report | Defender Power On The Rise" (Canada | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/canada-global-threat-report-defender-power-on-the-rise/

29. "Singapore | Global Threat Report | Defender Power On The Rise" (Singapore | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/singapore-global-threat-report-defender-power-on-the-rise/

30. "UK | Global Threat Report | Defender Power On The Rise" (Regatul Unit | Raport privind amenințările globale | Capacitatea Defender este în creștere). 2019. VMWARE. https://www.carbonblack.com/land/uk-global-threat-report-defender-power-on-the-rise/

31. „Anticipating the Unknowns" (Anticiparea necunoscutelor). Martie 2019. Cisco. https://ebooks.cisco.com/story/anticipating-unknowns/

32. „2020 Data Breach Investigations Report" (Raportul de investigații privind încălcarea securității datelor din 2020), 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

33. „IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks" (Studiul de securitate IBM: contribuabilii se opun guvernelor locale care plătesc hackerii în atacuri ransomware). 5 septembrie 2019. IBM. https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks

34. „IT threat evolution Q2 2019 statistics" (Statistici privind evoluția amenințărilor informatice în T2 2019), 2019 Kaspersky, https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

35. „IT threat evolution Q1 2019 statistics" (Statistici privind evoluția amenințărilor informatice în T1 2019), 2019 Kaspersky, https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

36. „The state of industrial cybersecurity" (Situația securității cibernetice industriale). Iulie 2019. Kaspersky. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

37. „2019 Cyberthreat Defense Report" (Raportul privind apărarea împotriva amenințărilor cibernetice 2019), Cyber Edge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

38. „Evasive Threats, Pervasive Effects" (Amenințări evazive, efecte extinse). 27 august 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

39. „IT threat evolution Q3 2019 statistics" (Statistici privind evoluția amenințărilor informatice în T3 2019), 2019 Kaspersky, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

40. „What You Need to Know About the LockerGoga Ransomware" (Ce trebuie să știți despre ransomware-ul LockerGoga). 20 martie 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

41. „BDO Cyber Threat Insights - 2019 2nd Quarter Report" (Analiza BDO privind amenințările cibernetice – Raportul pentru al doilea trimestru din 2019), iulie 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

Referințe

42. Instrumente de decriptare ransomware, Kaspersky https://noransom.kaspersky.com/

43. „ENISA Threat Landscape Report 2018" (Raportul ENISA privind situația amenințărilor din 2018). 28 ianuarie 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

44. „New GandCrab v5.1 Decryptor Available Now" (Noul decriptor GandCrab v5.1 este acum disponibil), 19 februarie 2019. Bitdefender LABS. https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

45. „10 Ransomware Attacks You Should Know About in 2019" (10 atacuri ransomware despre care ar trebui să știți în 2019), 28 aprilie 2019. Allot. https://www.allot.com/blog/10-ransomware-attacks-2019/

46. Instrumente de decriptare ransomware. Avast. https://www.avast.com/ransomware-decryption-tools

47. Sursa ransomware-ului PewCrypt. GitHub. https://github.com/000JustMe/PewCrypt

48. „Are the REvil, GranCrab Ransomware Families Related?" (Familiile de ransomware REvil și GranCrab sunt înrudite?). 25 septembrie 2019. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/revil-gandcrab-related/

49. „Threat Landscape Report" (Raportul privind situația amenințărilor), Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf

50. „Sodin Ransomware includes exploit for Windows CVE-2018-8453 bug" (Ransomware-ul Sodin include un exploit pentru bug-ul Windows CVE-2018-8453). 4 iulie 2019. Security Affairs. https://securityaffairs.co/wordpress/87944/malware/sodin-ransomware-cve-2018-8453.html

51. "Threat Landscape Report" (Raportul privind situația amenințărilor), 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

52. „Emsisoft Decryptor for Aurora" (Decriptorul Emsisoft pentru Aurora), 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/aurora

53. „Emsisoft Decryptor for Muhstik" (Decriptorul Emsisoft pentru Muhstik), 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/muhstik

54. „Caution! Ryuk Ransomware decryptor damages larger files, even if you pay" (Atenție! Decriptorul ransomware-ului Ryuk deteriorează fișierele mai mari, chiar dacă plătiți). 9 decembrie 2019. Emsisoft. https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

55. „RakhniDecryptor tool for defending against Trojan-Ransom.Win32.Rakhni ransomware" (Instrumentul RakhniDecryptor pentru apărare împotriva ransomware-ului Trojan-Ransom.Win32.Rakhni). Kaspersky. https://support.kaspersky.com/10556

56. „Another two bite the dust: Kaspersky updates decryption tool to fight ransomware pair" (Încă două au fost învinse: Kaspersky actualizează instrumentul de decriptare pentru a combate două programe ransomware). 27 septembrie 2019. The Online Citizen. https://www.theonlinecitizen.com/2019/09/27/another-two-bite-the-dust-kaspersky-updates-decryption-tool-to-fight-ransomware-pair/

57. „Mira Ransomware Decryptor" (Decriptorul ransomware-ului Mira), 1 aprilie 2019. F-Secure. https://blog.f-secure.com/mira-ransomware-decryptor/

58. „Nemty update: decryptors for Nemty 1.5 and 1.6" (Actualizare Nemty: decriptori pentru Nemty 1.5 și 1.6), Tesorion. https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/

59. „McAfee Labs Threats Report" (Raportul McAfee Labs privind amenințările), August 2019. McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

60. „The 10 biggest ransomware attacks of 2019" (Cele mai mari 10 atacuri ransomware din 2019), CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/2

61. „The 10 biggest ransomware attacks of 2019" (Cele mai mari 10 atacuri ransomware din 2019), CRN. https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/3

62. „The 10 biggest ransomware attacks of 2019" (Cele mai mari 10 atacuri ransomware din 2019), CRN https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/6

63. „The 10 biggest ransomware attacks of 2019" (Cele mai mari 10 atacuri ransomware din 2019), CRN https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/7

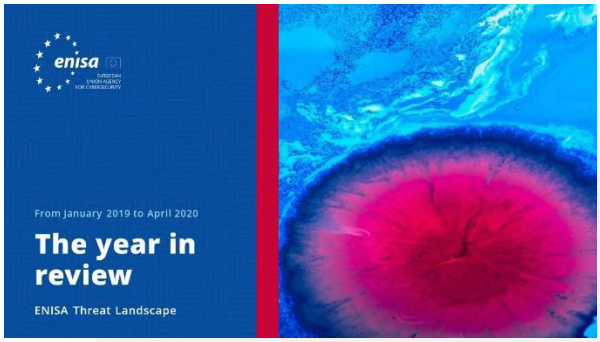
64. „The 10 biggest ransomware attacks of 2019" (Cele mai mari 10 atacuri ransomware din 2019), CRN https://www.crn.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/11

65. https://www.nomoreransom.org/

„CTI s-a impus ferm în domeniul securității cibernetice ca instrument esențial pentru îmbunătățirea agilității și eficienței în apărarea împotriva atacurilor cibernetice.”

în ETL 2020

Documente conexe



Raportul ENISA privind situația amenințărilor **Trecerea în revistă a anului**

Rezumat al tendințelor de securitate cibernetică pentru perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Lista celor mai importante 15 amenințări

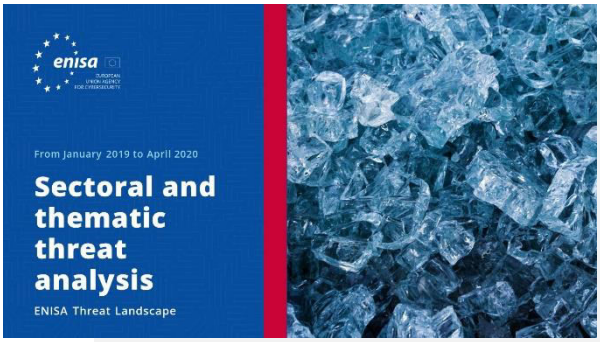
Lista ENISA a celor mai importante 15 amenințări din perioada ianuarie 2019 – aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Teme de cercetare

Recomandări privind teme de cercetare în diferite sectoare din securitatea cibernetică și informațiile privind amenințările cibernetice.

CITIȚI RAPORTUL



CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Analiza sectorială și tematică a amenințărilor**

Analiza contextualizată a amenințărilor în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor **Tendințe emergente**

Principalele tendințe în securitatea cibernetică observate în perioada ianuarie 2019 - aprilie 2020.

CITIȚI RAPORTUL

Raportul ENISA privind situația amenințărilor
Prezentare generală a informațiilor privind amenințările cibernetice

Situația actuală a informațiilor privind amenințările cibernetice în UE.

Despre

_Agenție

Agenția Uniunii Europene pentru Securitate Cibernetică, ENISA, este agenția Uniunii dedicată realizării unui nivel comun ridicat de securitate cibernetică în întreaga Europă. Înființată în 2004 și consolidată prin Regulamentul UE privind securitatea cibernetică, Agenția Uniunii Europene pentru Securitate Cibernetică
contribuie la politica cibernetică a UE, sporește credibilitatea produselor, serviciilor și proceselor TIC cu ajutorul sistemelor de certificare a securității cibernetice, cooperează cu statele membre și organismele UE și ajută Europa să se pregătească pentru provocările cibernetice viitoare. Prin schimbul de cunoștințe, consolidarea capacităților și campanii de sensibilizare, agenția colaborează cu părțile interesate cheie pentru a consolida încrederea în economia conectată, pentru a spori reziliența infrastructurii Uniunii și, în cele din urmă, pentru a menține securitatea digitală a societății europene și a cetățenilor. Mai multe informații cu privire la ENISA și activitatea sa sunt disponibile la adresa www.enisa.europa.eu.

Contribuitori

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) și *toți membrii Grupului părților interesate al ENISA CTI:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) și Thomas Hemker.

Editori

Marco Barros Lourenço (ENISA) și Louis Marinos (ENISA).

Date de contact

Pentru întrebări privind această lucrare, vă rugăm să utilizați adresa enisa.threat.information@enisa.europa.eu.

Pentru întrebări din partea mass-media despre această lucrare, vă rugăm să utilizați adresa press@enisa.europa.eu.

Dorim să aflăm părerea dumneavoastră despre acest raport!
Vă rugăm să acordați câteva momente pentru completarea chestionarului. Pentru a accesa formularul, faceți clic aici.

Aviz juridic

Trebuie luat în considerare faptul că această publicație reprezintă punctele de vedere și interpretările ENISA, cu excepția cazului în care se prevede altfel. Această publicație nu trebuie interpretată ca o acțiune juridică a ENISA sau a organismelor ENISA, cu excepția cazului în care aceasta a fost adoptată în conformitate cu Regulamentul (UE) nr. 526/2013. Această publicație nu reprezintă neapărat stadiul actual al tehnologiei și ENISA o poate actualiza periodic.

Sursele terțe sunt citate corespunzător. ENISA nu este responsabilă pentru conținutul surselor externe, inclusiv al site-urilor externe menționate în această publicație.

Această publicație are doar scop informativ și trebuie să fie accesibilă în mod gratuit. Nici ENISA și nici persoanele care acționează în numele său nu sunt responsabile pentru modul în care ar putea fi utilizate informațiile conținute în această publicație.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Grecia
Telefon: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

https://www.enisa.europa.eu