CRIMINALITATEA INFORMATICĂ – PROVOCĂRI ȘI EVOLUȚII

Mircea Constantin Șcheau*

Banca Națională a României

Rezumat

Noțiunile vehiculate în mediile de comunicare, referitoare la abordările amenințărilor cibernetice, sunt plasate uneori sub presiunea transformărilor etapizate, supuse mecanismului cunoscut sub numele de Fereastră Overton. Articolul încearcă să aducă în atenția opiniei publice și în aceeași măsură a specialiștilor, câteva dintre problemele hibride a căror escaladare poate să producă efecte greu de cuantificat. Setul de propuneri de la finalul studiului se doresc a fi o pledoarie în susținerea ideii de conlucrare interinstituțională și implicare activă a societății civile.

Cuvinte-cheie: instituţie financiară, vulnerabilitate, malware, atac informatic, vector de infecţie, impact, coordonare.

Clasificare JEL: F60, H56, K24, M15, O33.

Introducere

O simplă privire de survol asupra stării actuale în domeniu ne demonstrează că subiectul suscită interes în contextul în care relația de dependență dintre societate și inovație devine tot mai evidentă. Ar fi o greșeală să presupunem că există infrastructuri complet izolate și să ne gândim doar la asocieri particulare ale termenilor specifici cu subdomenii informatizate. Interoperabilitatea presupune interconectivitate, automatizare, și nu de puține ori, sisteme de comandă acționate de la distanță. Dispozitive a căror exploatare este accesibilă mediului domestic sunt utilizate pentru monitorizare în timp real și permit adresarea de resurse cu statut reglementat sau aparținând unei zone clasificate ca fiind componentă dark (e.g. dark web). Într-un simplu smartphone este prezentă tehnologie mai avansată decât într-o navetă spațială din anii ’70.

* Autor de contact, **Mircea Constantin Șcheau**: mirceascheau@hotmail.com

Opiniile exprimate în acest articol aparțin în întregime autorului și nu reflectă poziția oficială a Băncii Naționale a României.

Articol republicat din Revista ”Considerations on challenges and future directions in cybersecurity”, RAISA 2019, cu permisiunea editorului.

În accepțiunea actorilor care se înfruntă pe mai multe planuri, escaladarea conflictelor economice pentru acapararea cotelor de piață justifică apelul la proceduri ce ar putea fi cu ușurință încadrate în zona gri a legislației internaționale. Laboratoarele de cercetare și echipele strategice sunt ținte predilecte ale competitorilor. Tulpinile de virus sunt reinventate pentru a ocoli soluțiile de protecție. Tehnicile moderne vin în completarea manipulărilor de modă veche.

Criminalitatea financiară și activitățile necesare combaterii acesteia sunt diferite de cele asociate, ca exemplu, criminalității informatice din domeniul telecomunicațiilor, dar punctele de intersecție și ariile de suprapunere impun adoptarea de măsuri care să răspundă coordonat în fața agresiunilor. Într-un sondaj anonim, ce a presupus chestionarea a peste 700 de profesioniști în sfera securității din Marea Britanie, Australia, Statele Unite ale Americii, Mexic, Germania și Japonia, nouă din zece repondenți au declarat că organizația pentru care au lucrat a fost afectată ”cu succes” de cel puțin un atac cibernetic în perioada 2016 - 2018, și aproximativ jumătate dintre atacuri au avut ca rezultat înregistrarea unor intervale de nefuncționalitate a sistemelor considerate critice [4].

Cred că una dintre problemele majore cu care se confruntă de multă vreme structurile de securitate este generată de o oarecare lipsă de cultură a consumatorilor obișnuiți, impactul tangibil reflectându-se în exfiltrarea de date personale, compromiterea credențialelor și implicit, posibile pierderi financiare. Aparenta securizare, demontată fără prea mare efort de pasionații black hat hackers sau gray hat hackers, scot la iveală vulnerabilități clasificate în primă instanță ca inofensive. Un grup de experți a descoperit la finalul anului 2018 că există malware ce scanează în mod activ serviciile web și dispozitivele conectate la internet [16] pentru a descoperi eventuale expuneri și parolele prestabilite. Scriptul Xwo Python, legat de familiile de malware cunoscute anterior ca Xbash și MongoLock, combină caracteristici diferite, specifice ransomware, cryptocurrency miners, worms, backdoors etc. Malware-ul a fost atribuit unei grupării criminale Iron Group, a cărei activitate a fost semnalată încă de la începutul anului 2016.

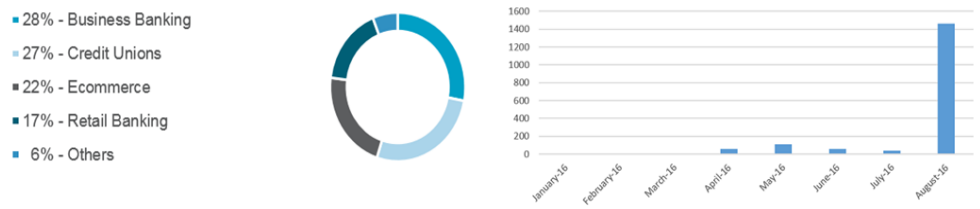


Figura nr. 1. Efectul GozNym [8], [9]

Virușii care s-au afirmat la nivel global, malwares care au atins așteptările inițiatorilor și care au întrunit un număr suficient de mare de aprecieri pentru a fi declarate de succes nu vor fi niciodată abandonați, indiferent de metodele de blocare dezvoltate de echipele de securitate împotriva acestora. Reinventarea lor se aliniază noilor realități tehnologice. Codul sursă este modificat, combinat cu alte coduri sursă și adaptat în așa fel încât să ocolească versiunile îmbunătățite de firewall. Țintele preferate vor fi tot aceleași asupra cărora a fost înregistrat efectul maxim, sau adiacente acestora. Un exemplu elocvent îl reprezintă troianul descoperit inițial în anul 2007 și implicat în perioada 2016 – 2018 în campanii puternice îndreptate împotriva instituțiilor financiar bancare, de asigurări și nu numai. GozNym combină caracteristicile Gozi ISFB și Nymaim. În partea dreaptă a imaginii din figura 1 sunt detaliate sectoarele afectate în anul 2016 din America de nord, iar

în partea dreaptă activitatea din Europa [8], [9]. În 2018, Gozi (Ursnif) a ocupat prima poziție în topul listei cu cei mai activi malware financiari, după un loc trei ocupat în anul 2017.

Unul alt exemplu îl constituie troianul bancar Kronos, a cărui nouă variantă a vizat în anul 2018 mai multe state, principala îmbunătățire fiind reprezentată de sistemul Command & Control, care utiliza în cazul respectiv rețeaua de anonimizare Tor. Chiar dacă s-a încercat o reetichetare sub numele Osiris, asemănările cu vechea versiune sunt evidente: același format webinject, Zeus malware format, același protocol și mecanism de criptare C & C, cod suprapus extensiv și nu în ultimul rând, dimensiunea de 350 Kb, comparabilă cu cea de 351 Kb dintr-o versiune anterioară [13]. Tot în contextul la care am făcut trimitere, un kit de exploatare underminer creat la finalul anului 2017 și lansat la începutul anului 2018, livra un bootkit și un malware de tip cryptocurrency-mining, numit generic Hidden Mellifera, și includea funcționalități de tip criptare asimetrică, randomizare URL etc. [14].
Un alt troian bancar, cunoscut sub numele de BackSwap, și-a făcut simțită prezența în luna martie a anului 2018. Chiar dacă prezintă elemente de noutate referitoare la webinjection, caracteristicile lui sunt foarte asemănătoare cu cele ale unui alt troian cunoscut sub numele de Tinba. Modul de acțiune scoate în relief importanța mecanismelor de autorizare și autentificare, efectele negative înregistrându-se cu mai mult succes în situația instituțiilor ale căror structuri de protecție nu respectau standardelor internaționale în domeniu. O imagine sugestivă prezintă o listă a primilor zece malwari financiari, cu mențiunea că acest clasament poate să difere, depinzând de compania care a realizat studiul de specialitate [10].

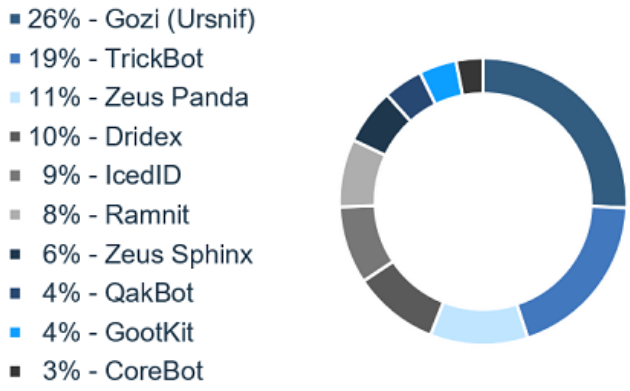


Figura nr. 2. Cele mai relevante familii de malware financiar în 2018 [10]

Un alt episod interesant l-a constituit relansarea spyware-ului Ratopak / Pegasus, cunoscut ca fiind angrenat în anul 2016 în atacuri împotriva unor instituții financiar - bancare. S-a clamat pe forumuri underground că reprezintă o nouă versiune ce conține codul sursă al malware-ului folosit de grupul Carbanak, dar în final a fost atribuit grupului Buhtrap, decizia fiind determinată și de identificarea unui certificat de semnare ce apare în codul binar și care a fost folosit în agresiunile menționate anterior. Modul de acțiune, utilizarea unui modul pentru deplasare laterală, a unei versiuni personalizate, actualizate Mimikatz de „recoltare" a credențialelor, injectarea codului printr-o tehnică „WriteProcessMemory", modul de difuzare PowerShell, SCM, WSH Remote sau RDP Scripts, tehnici diferite care oferă posibilitatea de a rula un script pe o mașină la distanță și

de a prelua controlul asupra acesteia, reprezintă doar câteva dintre caracteristicile cu grad mare de similitudine identificate de cercetători [15].

Cele prezentate anterior induc ideea că zona financiară se afirmă ca țintă predilectă a atacatorilor și trebuie să beneficieze de atenția cuvenită. Poate fi simplu asimilată sectoarelor pentru care trebuie să se asigure protecția și stabilitatea.

1. Transformări și Răspunsuri

Pentru ca tranzacțiile să devină mai sigure, indiferent dacă discutăm despre ordine de plată modeste sau despre transferuri internaționale supuse unui regim standardizat, se depun eforturi în identificarea de soluții care să conducă la o consolidare a blocurilor de apărare. Metodele de autentificare biometrice au fost considerate mai sigure până în momentul în care milioane de profiluri au început să se vândă pe piața neagră cu prețuri variind între cinci și câteva sute de dolari americani. La începutul anului 2019 o companie de securitate cibernetică, care operează de peste 21 de ani, a publicat rezultatele unei investigații privind comercializarea a aproximativ 60.000 de unități prin intermediul unui magazin online, Genesis Darknet marketplace. Accesul se făcea pe bază de invitație și se ofereau cumpărătorilor toate informațiile necesare utilizării produselor [7]. Se înmulțesc semnalele de alarmă referitoare la creșterea varietății și a complexității"oportunităților" din sectorul infracțional, în general și a celui financiar, în particular. Crime-as-a-Service (CaaS) nu mai este doar o expresie dintr-un dicționar. Se pot concatena trunchiuri de malware, se poate obține contra cost acces la baze de date cu clienți pentru care se cunosc și se indică precis punctele slabe, se pot licita vulnerabilități zero-day sau se pot "angaja" echipe dispuse să desfășoare activități malițioase împotriva unei ținte private sau guvernamentale. Paleta este destul de largă, de la viruși personalizați, la living-off-the-land (LoTL) sau infrastructuri criminale partajate. Sunt piețe subterane în continuă dezvoltare deoarece oferta se corelează și în acest caz cu cererea.

Sigur că nivelul de protecție poate să fie incrementat și există companii dispuse să investească în construcții capabile să prelucreze funcții complexe. Machine Learning (ML) nu mai reprezintă o necunoscută. Se afirmă ca ramură importantă a Artificial Intelligence (AI). Ca exemplu, putem să facem referire la elementele primare de identificare ale unei persoane, care se încarcă în sistemele de prelucrare a informației. Analiza comportamentală, gesturile involuntare din timpul deplasării printr-un culoar monitorizat, expresiile faciale, reacțiile la stimuli externi sau fragmentele vocale constituie baza clasificată pe categorii de la care se pornește. Toate acestea sunt comparate cu secvențe înregistrate în timp real de ML și coroborate cu cele injectate ulterior de operatorul uman. Orice inadvertență livrează un semnal de alarmă către echipa de supraveghere, care decide dacă impulsul trebuie asimilat celor inițiale sau trebuie puse imediat în aplicare prevederile planului de securitate.

Este indiscutabil faptul că evaluările periodice sunt deosebit de utile în identificarea deficiențelor politicii interne de securitate și contribuie la actualizarea programelor existente. Red team și testele de penetrare pot să ofere o imagine de ansamblu asupra obiectivului cheie, de evaluare a eficacității capabilităților de detecție, prevenire și răspuns. Un e-mail de tip phishing produce dovezi reziduale și de aceea regia se orientează uneori către scenarii de inginerie socială, bazată pe apeluri mai greu detectabile. Ca exemplu, după ce se studiază infrastructura clientului și conexiunea acestuia cu mediul public online, se poate clona portalul de autentificare și se poate chiar falsifica întreaga

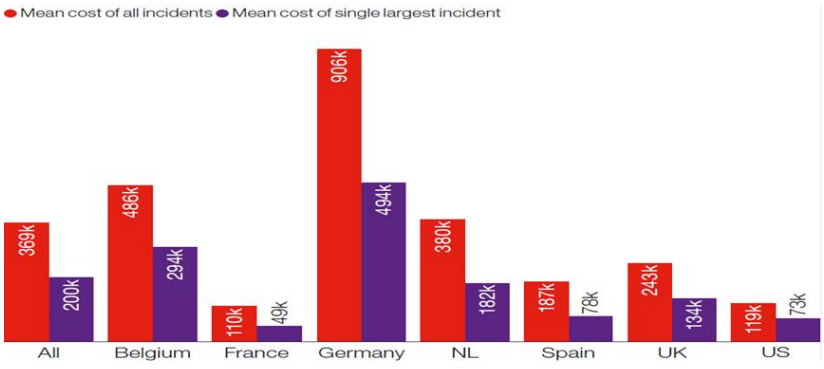
structură, inclusiv numărul de telefon pentru asistență IT. Se trimite o informare în conformitate cu care mail-urile au fost migrate pe un nou server și se solicită angajaților să se conecteze la portalul OWA clonat. Pentru a se evita orice suspiciune, sunt imediat redirectați după autentificare către portalul OWA legitim, dar folosind această metodă red team capturează suficiente credențiale pentru a stabili un punct de sprijin în rețeaua internă. Compromiterea conturilor privilegiate, coroborată cu lipsa unei segmentări judicioase, oferă în scurt timp acces total [1]. Astfel de exerciții se recomandă a se efectua simultan pentru toate structurile interconectate. Se pot evidenția vulnerabilitățile comune și cele particulare, inclusiv cele care pot să migreze.

Industry	Users Targeted (%)
Mining	38.4%
Wholesale Trade	36.6%
Construction	26.6%
Non-classifiable Establishments	21.2%
Retail Trade	21.2%
Agriculture, Forestry & Fishing	21.1%
Manufacturing	20.6%
Public Administration	20.2%
Transportation & Public Utilities	20.0%
Services	11.7%
Finance, Insurance & Real Estate	11.6%

Figura nr. 3. Email-uri malițioase pe industrii de utilizatori [3]

În condiții ideale este imposibilă detecția de malware, prezența putând fi semnalată doar datorită efectelor. Acest aspect presupune apariția unor pierderi în intervalul parcurs între momentul infecţiei și al implementării soluţiei [5].

Victimele pot fi simpli utilizatori, companii multinaționale sau organizații ale statului: ministere, obiective militare agenții de informații, grupuri producătoare de energie etc. Nimeni nu trebuie să se considere protejat total. Oricine poate fi atacat direct sau prin intermediul unui terț colaborator. Riscul de contaminare este destul de mare. Aceiași vectori de infecție și aceleași tehnici pot să fie folosite pentru medii diferite, așa cum se vede și din statistica din figura 3, valabilă pentru anul 2019. Platformele Web sunt folosite mai intens și mediile cu sisteme preinstalate sunt mult mai accesate pentru că este dificilă identificarea operatorilor din spatele acțiunii.



Mean cost of all incidents by sector ($)

	Pharma and health	Travel and leisure	Financial services	Transport	TMT
2019	726,000	703,000	628,000	530,000	464,000
2018	103,000	148,000	400,000	157,000	349,000

Mean cost of largest single incident by sector ($)

	Pharma and health	Travel and leisure	Financial services	Transport	TMT
2019	388,000	427,000	301,000	229,000	288,000
2018	11,000	29,000	83,000	38,000	52,000

Figura nr. 4. Costul mediu al incidentelor cibernetice ($) [6]

Se previzionează o creștere cu 1,5 miliarde $ a profitului obținut din criminalitate informatică și atingerea pragului de 70% până în anul 2021 din volumele de crypto-monede alocate industriei subterane. Pierderile înregistrate vor depăși șase trilioane $ anual, în condițiile în care peste 146 de miliarde de înregistrări se estimează că vor fi exfiltrate până în anul 2023 [3]. Impactul financiar, costul total, frecvența și intensitatea atacurilor cresc și implicit trebuie incrementat nivelul de informare și pregătire. Deși există diferențe în ceea ce privește pierderile datorate cyber crime, un studiu de specialitate scoate în evidență temele comune din jurul prevalenței atacurilor și a costului recuperării [6]. Indicii de interes ai agresorilor reprezintă în cazul de față repere de proiecție pe termen scurt, mediu și lung. Rapoartele sunt dinamice și graficele pot să înregistreze mediane de valori diferite, ceea ce face și mai dificilă trasarea coordonatelor previzionare.

Este adevărat că ascensiunea Artificial Intelligence / Machine Learning permite în prezent examinarea și identificarea cu destul de mare precizie a stilului de codare al unei persoane sau chiar al unui grup de persoane care lucrează împreună la un același proiect, dar rezultatul poate fi util mai mult în sens reactiv decât anticipativ. Chiar dacă nu se poate discuta despre standardizare sau o acceptare unanimă a unei metode consacrate, anonimizarea și plagiatul în materie de programare poate să devină în curând doar o simplă sintagmă teoretică. Testele au relevat faptul ca nivelul de experiență al unui informatician, coroborat cu numărul de produse elaborate și cu gradul de dificultatea al acestora, este direct proporțional cu gradul de precizie al identificării acestuia. Mai exact, cu cât un informatician are mai multă experiență, cu cât a participat la construcția mai multor produse și cu cât gradul de dificultate a fost mai ridicat, cu atât a crescut procentul de acuratețe al dezanonimizării. Stilometria se afirmă ca sferă de activitate ce poate fi înglobată în mai

multe subdomenii, răspunsurile fiind unele dintre cele mai surprinzătoare [11]. Pasionații computer security, care și-au dezvoltat abilitățile și sunt dispuși să depună un efort în acord cu provocările, au nevoie uneori doar de câteva indicii care să-i ajute la formularea unui riposte de tip KickBack. În funcție de natura agresiunii, după identificarea fragmentelor de start, se implementează strategia de abordare împreună cu organele de aplicare a legii [12].

Concluzii și Propuneri

Privite din exterior, scenariile pot fi percepute ca apocaliptice și seamănă mai mult cu nuvele science-fiction decât cu realitatea crudă. Pe aceasta se bazează și infractorii. Pe sentimentul că ”mie nu mi se poate întâmpla” sau ”de ce să mi se întâmple tocmai mie, dacă nu prezint niciun interes pentru nimeni?”. Fiecare dintre noi putem să devenim o simplă piesă într-un joc de GO sau putem să fim antrenați într-un vârtej de figuri geometrice care își schimbă forma și plasamentul continuu. Tot ceea ce putem să facem este să nu renunțăm nicio secundă la prevenție și să încercăm să schimbăm mentalitatea celor din jurul nostru. Cu douăzeci de ani în urmă încuiam ușa cu cheia și nu deschideam decât persoanelor cunoscute. Nu cu mult timp în urmă, când cunoșteam doar monedele cu care puteam să achiziționăm bunuri uzuale, nu ne gândeam că va veni momentul în care crypto-monedele vor încerca să se impună ca o alternativă. Lipsa de reglementare în domeniu favorizează însă economia subterană și fără politici coerente este dificil de combătut fenomenul infracțional. Granița criminalității informatice poate fi considerată sinonimă cu limita imaginației și în acest caz, este bine să conștientizăm cât mai rapid că agresorul, care altă dată încerca să ne invadeze prin metode brute spațiul personal, acum o poate face invitat chiar de noi.

Fiecare producător recomandă efectuarea de update-uri ca parte a proceselor de îmbunătățire a securității produselor sau ca vaccinare preventivă, metaforic vorbind și modificarea parolelor inițiale cu unele care să respecte criteriile legate de lungime și combinații de taste, ridicând astfel o primă barieră în fața atacatorilor. Internet of Things (IoT) reprezintă practic suportul pentru Internet of People (IoP) și împreună evoluează rapid către Internet of Everything (IoE). Wifi Protected Access (WPA), protocol lansat de Wi-Fi Alliance pentru autentificarea dispozitivelor conectate fără suport fizic de transmitere a informației (fără fir) utilizând Advanced Encryption Standard (AES), s-a dovedit că prezintă lacune de securitate, în pofida creșterii puterii criptografice și în condițiile în care devine din ce în ce mai dificilă separarea dintre personal și profesional, o companie poate să ajungă foarte ușor victimă. Un atac ar putea avea succes, cu ajutorul unui angajat care nu tratează corect un e-mail de tip phishing sau care încalcă altă normă de securitate internă. Un episod de acest gen poate fi catalogat ca eșec uman. În aceste circumstanțe, trebuie valorizate motivații specifice pentru a îngusta cât mai mult canalele de penetrare și pentru a micșora suprafețele expuse posibilelor agresiuni. Trebuie plasate în prim plan și susținute rațiunile de creștere a gradului de intoleranță la risc.

Pentru a rezista presiunii concurențiale, companiile trebuie să înțeleagă tendințele disruptive cu influențează evidentă asupra pieților, comportamentelor și așteptărilor clienților, în aceeași măsură cu cele ale angajaților. Oportunitățile de creștere stimulează eforturile de modernizare a infrastructurii și deschid noi perspective evoluției transformărilor digitale. Se stabilesc priorități în construcția unei culturi inovative și în acest context, trebuie recunoscută importanța deosebită a factorului uman în dezvoltarea colaborărilor transfrontaliere [2].

La nivelul Uniunii Europene consider necesară constituirea de grupuri comune de lucru care să analizeze cele mai bune practici (de securitate) pentru fiecare domeniu sau minister, în vederea implementării unitare pe baza unui calendar a măsurilor de aliniere la aceleași standarde. Apelurile către serviciile de suport primar sau către echipele pregătite să răspundă la incidente de natură informatică, chiar și cele din aria civilă, ar trebui să beneficieze de sprijin pe tot cuprinsul Uniunii Europene, să fie contorizate și raportate în așa fel încât să conducă la o mai rapidă identificare a schemelor de atac și a agresorilor.

Conceptul unei structuri (securizate) de comunicații cu acoperire europeana, cu sistem centralizat Artificial Intelligence sau gestionat pe module, poate fi dezvoltat numai în condițiile uniformizării legislativ, care să statueze schimbul de informații interinstituționale, interstatale și modelul de colaborare dintre furnizorii de servicii și autorități [17]. În această conjunctură, transmiterea cu celeritate către organismele abilitate a informațiilor referitoare la orice eveniment de tip cyber crime este vitală pentru asigurarea rezilienței și trebuie să reprezinte o prioritate pentru organisme oficiale sau persoane juridice private, indiferent de industria în care activează.

Pentru a pune în aplicare propunerile de mai sus, consider de asemenea ca fiind necesară inițierea la nivel european, în mediul educațional, a unui concept de familiarizare cu noțiunile primare de securitate informatică și chiar de aprofundare a acestora. Pe lângă programele generale de informare susținute în parteneriat public - privat, pornind de la ciclul gimnazial și până la finalizarea cursurilor medii, liceale, curricula școlară ar trebui să permită includerea de capitole specifice acestui subiect. O societate informată în ansamblul ei poate să reacționeze în fața agresiunilor și să contribuie activ la limitarea și chiar la prevenirea pierderilor.

Declarație

Opiniile exprimate în acest articol aparțin în întregime autorului și nu reflectă poziția oficială a Băncii Naționale a României.

Articolul original a fost publicat în limba engleză, în cadrul studiului „Considerations on Challenges and Future Directions in Cybersecurity”, ISBN 978-606-11-7004-3.

Bibliografie

[1] A. Rahman and C. Antolik, “Finding Weaknesses Before the Attackers Do,” *Threat Research*, FireEye, 08 April 2019. [Online]. Available: https://www.fireeye.com/blog/threat-research/2019/04/finding-weaknesses-before-the-attackers-do.html.

[2] B. Solis, “Seven Priorities To Accelerate Digital Transformation Maturity and Success,” Forbes, 09 January 2019. [Online]. Available: https://www.forbes.com/sites/briansolis/2019/01/09/seven-priorities-to-accelerate-digital-transformation-maturity-and-success/amp/.

[3] C. Crane, "80 Eye-Opening Cyber Security Statistics for 2019," The SSL Store, 10 April 2019. [Online]. Available: https://www.thesslstore.com/blog/80-eye-opening-cyber-security-statistics-for-2019/.
[4] *D. Simmons,* "Cyber-attacks 'damage' national infrastructure," BBC News, Technology, 04 April 2019. [Online]. Available: https://www.bbc.com/news/amp/technology-47812479.
[5] F. Cohen, *Computer Viruses - Theory and Experiments*, Computers & Security, vol. 6, pp. 22—35, 1987.
[6] Hiscox Ltd, "Hiscox Cyber Readiness Report 2019," [Online]. Available: https://www.hiscox.com/documents/2019-Hiscox-Cyber-Readiness-Report.pdf.
[7] Kaspersky Lab, "Kaspersky Lab uncovers Genesis: The underground e-shop with tens of thousands of digital doppelgangers for sale to bypass financial anti-fraud solutions," Press Release, 09 April 2019. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2019_kaspersky-lab-uncovers-genesis-new.
[8] L. Kessem, "GozNym's Euro Trip: Launching Redirection Attacks in Germany," *SecurityIntelligence*, IBM X-Force, 23 August 2016. [Online]. Available: https://securityintelligence.com/goznyms-euro-trip-launching-redirection-attacks-in-germany/.
[9] L. Kessem and L. Keshet, "Meet GozNym: The Banking Malware Offspring of Gozi ISFB and Nymaim," *SecurityIntelligence*, IBM X-Force, 14 April 2016. [Online]. Available: https://securityintelligence.com/meet-goznym-the-banking-malware-offspring-of-gozi-isfb-and-nymaim/.
[10] L. Kessem and T. Agayev, "BackSwap Malware Now Targets Six Banks in Spain," *Analysis and Insight for Information Security Professionals, Security Intelligence*, IBM, 22 August 2018, [Online]. Available: https://securityintelligence.com/backswap-malware-now-targets-six-banks-in-spain/.
[11] L. Matsakis, "Even Anonymous Coders Leave Fingerprints," Wired, 10 August 2018. [Online]. Available: https://www-wired-com.cdn.ampproject.org/c/s/www.wired.com/story/machine-learning-identify-anonymous-code/amp.
[12] M. Ramilli, "Hacking The Hacker. Stopping a big botnet targeting USA, Canada and Italy**,**" *Cyber Crime, Hacking*, Security Affairs, 31 August 2018. [Online]. Available: https://securityaffairs.co/wordpress/75782/cyber-crime/hacking-hacker-botnet.html.
[13] P. Paganini, "Kronos Banking Trojan resurrection, new campaigns spotted in the wild," *Cyber Crime*, Security Affairs, 26 July 2018. [Online]. Available: https://securityaffairs.co/wordpress/74764/malware/kronos-banking-trojan-variants.html.
[14] P. Paganini, "Underminer Exploit Kit spreading Bootkits and cryptocurrency miners," *Cyber Crime*, Security Affairs, 29 July 2018. [Online]. Available: https://securityaffairs.co/wordpress/74860/malware/underminer-exploit-kit.html.
[15] Tanya_K, "Source Code of Ratopak/Pegasus Spyware Targeting the Financial Sector Recently Leaked," Cyber Threat Insider Blog, 27 August 2018. [Online]. Available: https://blog.sensecy.com/2018/08/27/source-code-of-ratopak-pegasus-spyware-targeting-the-financial-sector-recently-leaked/.

[16] T. Hegel, J. Blasco and C. Doman, "Xwo - A Python-based bot scanner," AT&T Business, 02 April 2019. [Online]. Available: https://www.alienvault.com/blogs/labs-research/xwo-a-python-based-bot-scanner.
[17] Trend Micro Research, Europol's and European Cybercrime Centre (EC3), "Cyber-Telecom Crime Report 2019," Report, 2019. [Online]. Available: https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019.