Cybersecurity Illustrated (1)

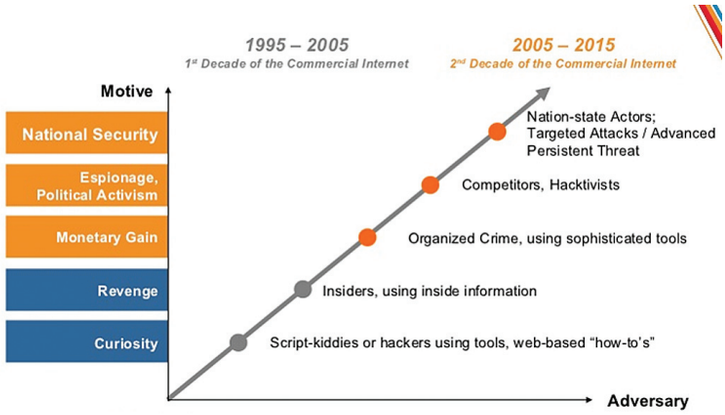
Toma Cîmpeanu,
CEO Asociația Națională
pentru Securitatea
Sistemelor Informatice

autor: Toma Cîmpeanu

În ultimii 25 de ani, de la apariția web-ului, asistăm la formarea unei „lumi paralele", incompletă deocamdată, pentru că nu tot ce există în lumea reală are deja un omolog în spațiul cibernetic. Lumea virtuală a schimbat totul: comunicarea, accesul la informații, învățarea, cercetarea, asistența medicală, comerțul, administrarea afacerilor, transportul și administrația publică, și cel mai important: ne-a schimbat comportamentul. Doar motivațiile se păstrează, pentru că acțiunile își au originea și efectele în lumea reală, chiar dacă mijloacele sunt parțial sau integral electronice.

Civilizația noastră are câteva mii de ani vechime și nu este nici pe departe perfectă, spațiul cibernetic are doar 25 de ani, deci nu putem avea pretenția să fie dominat de echilibru si armonie. Mai mult, nu exista nicio barieră, tehnologică sau morală, care să permită doar aspectelor „bune" ale vieții reale să-și dezvolte un „alte-ego" electronic, și asta ar putea fi o explicație, puțin filosofică, pentru amenințările care nu au întârziat să apară, să se manifeste și să evolueze în spațiul cibernetic.

Venind în completarea multitudinii de articole puternic teoretizate, prin seria de materiale pe care v-o propunem dorim să explicăm și să exemplificăm manifestările și consecințele infracțiunilor cibernetice.



(IBM X-Force)

Dintre principalele evoluții voi menționa aici două:

1 **Entitățile ostile:** în locul programatorului care concepea un virus de „amoru' artei" sau ca să demonstreze „că poate", au apărut grupările de criminalitate informatică, transfrontaliere și multidisciplinare, care urmăresc câștiguri materiale în această „industrie" cu o rată de profitabilitate estimată la 1500%, grupările hacktiviste și teroriste, precum și actorii statali, singurii care dispun de capabilitățile tehnice și resursele financiare pentru realizarea de malware sofisticat. Din acest punct de vedere, România, ca parte a NATO și UE, se confruntă cu aceleași amenințări ca și aliații noștri.

2 „Industria" Cybercrime se maturizează și apare **specializarea**. Identificăm acum finanțatori, proiectanți/dezvoltatori, distribuitori și cumpărători. De asemenea, asistăm la dezvoltarea **Cybercrime-as-a-Service** în tandem cu **finanțele subterane**: o piață neagră pe care se comercializează atât instrumentele de atac cibernetic (care se pot achiziționa sau închiria) cât și rezultatele, să le spunem „roadele" infracțiunilor cibernetice; și pentru că nimic nu este gratis, infractorii cibernetici apelează la instrumente de plată și optează pentru cele care asigură anonimatul, ireversibilitatea si viteza transferului. Pentru că există o astfel de piață, infractorii cibernetici din ziua de azi nu mai au nevoie de cunoștințe tehnice specializate ci doar de un card de credit, putând să achiziționeze malware ca atare sau să angajeze serviciul de exploatare/utilizare al acestuia (mai jos vor fi oferite exemple concrete).

Cybercrime-as-a-Service îmbracă mai multe forme (o clasificare **McAfee**):

- ***Reasearch-as-a-Service*** – în acest caz nu se poate vorbi neapărat de o piață neagră, ci mai degrabă gri. Aici regăsim organizațiile care identifică și prezintă vulnerabilități 0-day către companii selectate după anumite criterii de eligibilitate. Totuși, nu se exclud intermediarii care nu mai aplică aceleași criterii stricte, informația putând ajunge la entități care o folosesc ulterior în scopuri infracționale. De asemenea, în aceeași categorie includem agregarea de informații în baze de date care sunt ulterior folosite în alte scopuri decât cele declarate inițial. Astfel, **în oferta unor adevărate magazine virtuale ilegale găsim:**

Prices for zero-day vulnerabilities.

Adobe Reader	$5,000–$30,000
Mac OS X	$20,000–$50,000
Android	$30,000–$60,000
Flash or Java Browser Plug-ins	$40,000–$100,000
Microsoft Word	$50,000–$100,000
Windows	$60,000–$120,000
Firefox or Safari	$60,000–$150,000
Chrome or Internet Explorer	$80,000–$200,000
IOS	$100,000–$250,000

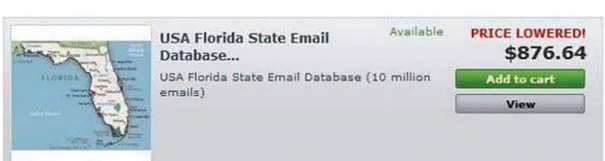


Figure 2. Florida residents email addresses for sale.

Bio - Toma Cîmpeanu

Toma Cîmpeanu a absolvit ca șef de promoție facultatea de matematică și facultatea de automatizări și calculatoare, are doctoratul și un master în sisteme de coordonare și control, precum și un MBA cu o universitate britanică. În ultimii 15 ani a ocupat poziții de conducere în companii de stat și private cum ar fi SN Radiocomunicații, TAROM, Informatica Feroviară, grupul SCOP Computers, eSign România sau TotalSoft. De asemenea, a fost Secretar de Stat în Ministerul pentru Societatea Informațională, reprezentantul României și membru al Boardului ENISA, Președinte al Agenției pentru Serviciile Societății Informaționale și Vicepreședinte al Centrului Național „România Digitală". Și-a legat numele de strategia eRomânia, sistemul național eLicitație și Punctul de Contact Unic al României. Toma Cîmpeanu a activat în domeniul academic la Universitatea din Craiova și a condus operațiunile Institutului de Management și Dezvoltare Durabilă, singura organizație românească care a coordonat la nivel global un grup de lucru al ONU. Din 2015, Toma Cîmpeanu este CEO al Asociației Naționale pentru Securitatea Sistemelor Informatice.

- ***Crimeware-as-a-Service*** – identificarea și dezvoltarea de kit-uri de exploatare, instrumente suport (keyloggers, bots), soluții de mascare a conținutului malware (cryptors, polymorphic builders), roboți și chiar dispositive hardware conexe (skimmers).

- ***Cybercrime Infrastructure-as-a-Service*** – odată ce infractorii cibernetici obțin instrumentele necesare, pentru atacul propriu-zis aceștia pot închiria rețele de calculatoare pentru un atac DDoS, pentru transmiterea cu succes a unui număr uriaș de emailuri, sau pot accesa platforme pe care să-și hosteze conținutul malware.

- ***Hacking-as-a-Service*** – având un cost superior alternativei în care se achiziționează componentele individuale, „cumpărarea" unui atac reprezintă varianta care necesită cele mai puține cunoștinte tehnice. Tot în această categorie regăsim cumpărarea de credențiale, date despre cardurile de credit etc.

Finanțele subterane s-au dezvoltat în special pentru că infractorii (și nu ne rezumăm la cei cibernetici) au nevoie să acceseze **circuite financiare fără trasabilitate**.

Prices for stolen credit card numbers.

	US			EU			CA, AU		Asia	
Visa Classic	$15	$80		$40	$150		$25	$150	$50	$150
Master Card Standard		$90			$140			$150		$140
Visa Gold/Premier	$25	$100	$200	$45	$160	$250	$30	$160	$55	$150
Visa Platinum	$30	$110		$50	$170		$35	$170	$60	$170
Business/Corporate	$40	$130		$60	$170		$45	$175	$70	$170
Purchasing/Signature	$50	$120		$70			$55		$80	
Infinite				$130	$190		$60	$200		$190
Master Card World		$140								
AMEX	$40			$60			$45		$70	
AMEX Gold	$70			$90			$75		$100	
AMEX Platinum	$50									

ANSSI - Partener editorial permanent Cybersecurity Trends

Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI) a fost înființată în anul 2012 ca un liant între sectorul public și mediul de afaceri, pentru promovarea practicilor de succes și facilitarea unei schimbări culturale în domeniul securității informației. Identificarea și sesizarea factorilor cu competențe administrative în cazul eventualelor deficiențe de pe piața IT, precum și pentru coagularea unor forme de parteneriat public-privat care să conducă la creșterea eficienței si operaționalității sistemelor informatice implementate în România au fost preocupări constante ale asociației. ANSSI este o organizație neguvernamentală, nonprofit, profesională și independentă. Ea reunește 40 de membri, companii cu aproximativ 20000 de angajați, reprezentând 25% din totalul salariaților din industria privată de IT și comunicații. Membrii ANSSI, prin spectrul larg și diversitatea de capabilități tehnico-profesionale deținute, formează un grup reprezentativ la nivel sectorial, ale cărui teme de interes reflectă fidel preocupările generale ale domeniului. ANSSI s-a implicat activ, organizând singur sau împreună cu alte autorități, instituții sau ambasade, conferințe și simpozioane naționale dar și internaționale, în domenii conexe, cum ar fi comunicațiile electronice, soluțiile și sistemele de e-guvernare și e-administrație, accesarea instrumentelor structurale, dezvoltarea profesională sau standardele ocupaționale, în care componenta de securitate tehnologică și de infrastructură IT au constituit preocuparea centrală.

Payment purpose	Payment for	Common payment mechanisms	Example
Victim payment	Extorsion	Bitcoins, Bank Transfer, paysafecard	Payment extorted as a result of a ramsonware or DDoS attack
	Fraud	Bitcoins, Bank Transfer, Western Union	Loss to an online fraud/ scam
Criminal to criminal payment	Counter AV	PayPal	Testing of malware against commercial AV products
	Data	Bitcoins, Ukash, Western Union, Webmoney	Purchase of compromosed financial data such as credit cards
	DdoS	Bitcoins	DDoS service for hire
	Hosting	Bitcoins	Purchase of hosting (including bulletproof)
	Malware	Visa, MasterCard, WebMoney, PayPal	Purchase of malware, such as RATS and banking trojans
	Trade on hidden service	Bitcoins, Ukash, paysafecard	Purchase of drugs or weapons
Payment for legitimate service		Bitcoins, Bank transfer, Visa, MasterCard	Hosting, hardware, software, travel, accomodation etc
Money movement		Bitcoins, Bank transfer, Western Union	Movement of money to maintain control of funds or hide/break a financial trail, including „cashing-out" of compromised financial accounts. This also includes exchange to, from or between virtual, digital and fiat currencies

Economia digitală subterană, ca orice economie, se bazează pe fluxul liber de fonduri. Varietatea mecanismelor de plată disponibile și folosite de infractorii cibernetici este diversă, variază față de lumea reală, plățile fizice fiind efectuate către monede digitale nedetectabile.

Multe mecanisme de plată cu aspect important on-line oferă un număr de caracteristici care le face atractive ca și instrument financiar pentru organizațiile criminale - **anonimatul, transferuri rapide, ieftine și ireversibile și tranzacțiile financiare disimulate**.

În multe privințe, unele mecanisme de plată pot oferi un nivel de anonimat **similar banilor lichizi**, dar într-un mediu on-line. **Europol** a realizat o statistică privind mijloacele de plată preferate pentru anumite tipuri de operațiuni:

Exemplu – economia phishing-ului

Phishingul este una dintre cele mai des întâlnite infracțiuni informatice, urmărind obținerea unor informații personale care ulterior să fie folosite pentru obținerea de foloase materiale. Phishingul imbracă multe forme, în exemplu ne vom referi la situația unui infractor fără cunoştințe tehnice profunde dar cu abilități de navigare în darknet, acolo unde se găsesc magazinele virtuale amintite mai sus (este un exemplu mult simplificat, care surprinde însă principalele aspecte specifice).

Am văzut că acesta poate achiziționa o bază de date de **10 milioane de adrese de mail din Florida** cu mai puțin de **1000 dolari**. Către aceste adrese transmite un mesaj email în care pretinde că este un reprezentant al statului, dintr-o instituție de supraveghere bancară reală, şi solicită cetățenilor să-şi introducă datele privind contul și cardul, pentru a valida informațiile transmise de bănci. Un astfel de mail este în general blocat de filtrele anti-spam în proporție de 99% (conform **CISCO Annual Report 2015**), aşa că, pentru a

diminua efectul filtrelor, subiectul nostru achiziționează cu aproximativ **5000 dolari** un mecanism de livrare emailuri de pe un număr mare de adrese IP (volum mic per adresă IP; așa numitul **spam snowshoe**). Rata de succes în acest caz este de 10% (filtrele opresc doar 90%, sursă www.getcybersafe.ca).

Evident, nu e suficient ca email-ul să ajungă la destinatar, ci trebuie să fie suficient de credibil (și destinatarul suficient de naiv) ca să-l determine să-și transmită datele. **Jumătate din mail-uri sunt deschise** și **10 % dintre destinatari dau click pe link-ul din mail (www.getcybersafe.ca)**.

Așadar, infractorul din acest exemplu trebuie sa-și construiască o **pagină web** care să semene cat mai mult cu cea originală, a instituției de supraveghere bancara a carei identitate o asumă, iar **numele de domeniu** sa fie de asemenea foarte asemănător. Pentru toate acestea considerăm un cost de **10.000 dolari**. Pe această pagină, destinatari care au fost păcăliți își vor lăsa datele privind cardurile și conturile lor.

Dintre cei care ajung pe pagina web, doar **10% își completează datele, natura infomațiilor îi descurajează pe cei mai prudenți 90% (www.getcybersafe.ca)**.

În cazul nostru concret, infractorul fără studii de specialitate obține **5.000 de seturi de date privind carduri bancare**, pe care le comercializează, la rândul său, de data aceasta de pe poziția de vânzător și nu de cumpărător (ca până acum), prin magazinele virtuale ilicite din darkweb, obținând în medie 60 dolari/buc conducând la un total de **300.000 dolari**.

Conform statisticilor **Europol**, în acest caz plățile se fac cel mai adesea în **Bitcoin**. ■

Așadar:

- **10 milioane de adrese mail – achiziționate inițial cu 1000 dolari**
- **1 milion de mail-uri ajung la destinație (10%, prin spam snowshoe, cost expediere 5000 dolari)**
- **500.000 mail-uri sunt deschise (jumatate dintre cele care trec de filtre)**
- **50.000 de destinatari acceseaza adresa web din email (10% dintre cei care deschid mail-ul)**
- **5.000 de destinatari introduc datele solicitate în pagina web (10% dintre cei care ajung pe pagina web falsă)**
- **Cost pagină web 4=10.000 dolari**
  Obs. Procentul celor păcăliți este de 0.05% din totalul destinatarilor
- **5.000 de seturi de date privind carduri bancare = 300.000 dolari (60 dolari/buc)**

Sumarizând:

- **Total investiție = aproximativ 16-20.000 dolari ()**
- **Venituri = 300.000 dolari**
- **Profit = 1500%!**

183 x 123 mm