ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMATII

NR_2_2020

BULETIN CYBERINT

INFO BOX

Hacktivismul reprezintă manifestarea activismului în spațiul cibernetic.
Format prin combinarea cuvintelor „hack” și „activism”, hacktivismul presupune derularea de atacuri cibernetice asupra unor sisteme informatice și pagini web cu scopul de a transmite un mesaj de protest, motivat politic sau social.

INFO BOX

Script kiddie (skiddie/skid/script bunny/lamer/noob) - Persoană, cu cunoștințe reduse de hacking, care folosește diverse aplicații și script-uri create de hackeri pentru a derula atacuri cibernetice. De regulă, nu deține cunoștințe tehnice și provocă daune din teribilism juvenil.

FENOMENUL HACKTIVIST LA NIVEL INTERNAȚIONAL

UNA DINTRE FORMELE DE MANIFESTARE A AMENINȚĂRILOR CIBERNETICE O REPREZINTĂ ATACURILE CIBERNETICE DERULATE DE GRUPĂRI HACKTIVISTE.

Acestea vizează preponderent transmiterea de mesaje de protest, promovarea propriilor idei și obținerea de notorietate, prin derularea unor atacuri cibernetice. De cele mai multe ori, aceste atacuri cibernetice presupun afectarea integrității și disponibilității datelor de pe sistemele informatice vizate.

Țintele predilecte ale acestor actori sunt infrastructurile IT&C din cadrul instituțiilor publice, dar victimele pot face parte chiar și din sfera privată. Preponderent sunt vizate entități cu activitate în domenii de interes social și politic (sănătate, administrație publică, educație, cultură, justiție, securitate națională etc.).

Membrii unor astfel de grupări hacktiviste, atât hackeri, cât și script - kiddies, sunt interesați de obținerea notorietății în mediul online, promovarea grupărilor din care fac parte și expunerea cunoștințelor și capabilităților de care dispun.

În peisajul amenințării hacktiviste, s-a remarcat la nivel internațional gruparea Anonymous, și rețeaua sa transnațională. Originile grupării Anonymous se regăsesc în anul 2003, atunci când Christopher Poole, un tânăr din New York, a lansat site-ul 4chan.org, un forum anonim de discuții unde se puteau posta fotografii și comentarii. Tematica de discuții s-a diversificat în timp, site-ul devenind locul de întâlnire al multor hackeri anonimi, cunoscuți sub denumirea de „anons”, care au început să facă schimb de cunoștințe tehnice și să discute pe subiecte din domenii variate.

În anul 2004, din această comunitate de hackeri anonimi a luat naștere mișcarea ideologică Anonymous, care de-a lungul timpului a instrumentat și promovat în cadrul comunității hacktiviste o serie de operațiuni cibernetice majore la nivel internațional, de susținere a anumitor cauze (Operațiunea Payback, Operațiunea Tunisia, Operațiunea AntiSec, Operațiunea Charlie Hebdo etc.).

Activitatea și evoluția acestor grupări este influențată de existența unor evenimente scena politică, economică și socială care prezintă interes pe agenda acestora.

În prezent, principalele forme de manifestare a amenințării hacktiviste sunt reprezentate de atacurile de tip defacement (prin SQL Injection, shell uploading, php scripting etc.), Denial of Service și Distributed Denial of Service.

Deși, în cele mai multe cazuri exponenții mediului hacktivist nu dețin cunoștințe avansate din punct de vedere tehnic (având multiple niveluri de specializare, de la cunoștințe de hacking peste medie și până la utilizarea unor instrumente basic din open-source), iar atacurile cibernetice pe care le derulează au în general un nivel redus de complexitate, aceștia manifestă preocupare constantă pentru extinderea cunoștințelor, metodelor de compromitere a țintelor.

Un exemplu elocvent îl reprezintă utilizarea de tool-uri de scanare care permit identificarea și exploatarea vulnerabilităților de securitate cibernetică și pentru dezvoltarea rețelelor de boți în vederea instrumentării atacurilor de tip Distributed Denial of Service.

FACTORI FAVORIZANȚI ÎN DERULAREA **ATACURILOR CIBERNETICE**

01
VULNERABILITĂȚI DE SECURITATE CIBERNETICĂ

Persistența vulnerabilităților de securitate cibernetică la nivelul infrastructurilor IT&C din România oferă hacktiviștilor oportunitatea de a derula atacuri cibernetice împotriva acestora. Un eventual atac cibernetic major lansat asupra infrastructurilor IT&C aparținând instituțiilor guvernamentale poate afecta atât imaginea și credibilitatea instituției în cauză, cât și buna funcționare a activității curente a acesteia.

02
ACCES LA INSTRUMENTE ȘI CUNOAȘTERE

Activitatea acestor entități se desfășoară în cadrul unor grupuri constituite la nivelul forumurilor și rețelelor de socializare unde sunt diseminate tool-uri, metode de atac și know-how-ul necesar planificării și derulării de atacuri cibernetice. Totodată, obținerea instrumentelor și a cunoașterii necesare derulării atacurilor cibernetice este obținută și de la nivelul platformelor open-source specifice și din mediul Dark Web.

03
EVENIMENTE CU POTENȚIAL DE MOBILIZARE

Atacurile cibernetice derulate de exponenți ai unor grupări hacktiviste asupra website-urilor care aparțin unor instituții publice, au loc cu precădere în contextul unor evenimente sociopolitice cu impact la nivel național sau internațional.

Un exemplu în acest sens îl reprezintă pandemia generată de răspândirea bolii COVID-19, context în care exponenți ai mediului hacktivist au derulat atacuri cibernetice asupra infrastructurilor IT&C administrate și utilizate la nivelul instituțiilor cu atribuții pe linia adoptării unor măsuri de diminuare a efectelor crizei epidemiologice.

ACTIVITĂȚI SUBSUMATE FENOMENULUI **HACKTIVIST ÎN ROMÂNIA**

Începând cu luna ianuarie 2020 au fost identificate mai multe atacuri cibernetice de tip defacement și SQL Injection asupra mai multor website-uri ale unor instituții din România, realizate de către o grupare de hackeri autohtoni. Motivația acestei grupări este una ideologică, scopul fiind de a promova mesaje prin intermediul atacurilor cibernetice.

În urma investigațiilor derulate de instituțiile abilitate, a fost stabilit faptul că entitatea hacktivistă a derulat și acțiuni premergătoare infectării cu ransomware și remote acces trojan a unor instituții publice, cu precădere din domeniul sănătății. În contextul epidemiologic actual, materializarea unei astfel de intenții ar fi putut afecta grav capacitatea de funcționare a instituțiilor vizate, cu rol central în gestionarea crizei.

Astfel, organele de urmărire penală au dispus percheziții și arestarea preventivă a membrilor grupării, prevenind materializarea intențiilor acestora, în caz contrar, generând, atât prejudicii de imagine pentru victimele atacurilor cibernetice, cât și disfuncții în activitatea derulată de acestea.

RANSOMWARE DOUBLE EXTORTION

PENTRU SPORIREA „VENITURILOR" OBȚINUTE ȘI PENTRU CREȘTEREA RATEI DE SUCCES A ACȚIUNILOR LANSATE ÎN SPAȚIUL CIBERNETIC, ATACATORII ÎȘI DIVERSIFICĂ, ÎN MOD CONSTANT, MODUL DE OPERARE ȘI INSTRUMENTELE UTILIZATE ÎN CADRUL CAMPANIILOR DERULATE.

Începând cu 2019, a fost observat un nou trend în planul campaniilor de distribuire de ransomware ce constă în double extortion / dubla extorcare a victimelor. Mai mult, acest trend s-a intensificat considerabil în 2020, tot mai multe grupări fiind observate că utilizează această tactică în campanii lansate atât asupra instituțiilor publice, cât și asupra unor companii și entități private.

INFO BOX

La nivel internațional, primele campanii de acest tip au fost observate în cazul grupării care utilizează ransomware-ul Maze, ulterior, un număr din ce în ce mai mare de grupări/atacatori împrumutând acest mod de lucru.

Astfel, în cadrul acestui nou mod de lucru, anterior criptării datelor identificate la nivelul unui sistem informatic, atacatorii le exfiltrează pe cele de interes cu scopul de a le utiliza mai apoi în determinarea victimei de a plăti răscumpărarea solicitată.

Atacatorii cibernetici amenință victimele cu publicarea datelor exfiltrate, de multe ori acestea fiind informații sensibile cu privire proiecte ale companiei/instituției, date personale ale unor angajați și/sau clienți, precum și orice alte date care, prin publicare, ar aduce prejudicii victimei.

Ca parte a modului de lucru, grupările care operează diverse aplicații ransomware au creat platforme/site-uri dedicate publicării datelor exfiltrate. Mai mult, pentru a demonstra că se află în posesia datelor pe care amenință că le vor publica, aceștia postează un set restrâns din cele exfiltrate.

În cazul în care datele exfiltrate includ adrese de email sau certificate pentru nume de domenii, grupările amenință cu utilizarea acestora în viitoare campanii de atac, prin impersonarea victimei, fapt ce ar aduce un prejudiciu de imagine acesteia.

În acest context, victimele unor atacuri de tip ransomware, în care atacatorii recurg la double extortion, resimt o presiune mult mai mare și vor fi mai înclinate să achite suma solicitată pentru a preîntâmpina publicarea datelor sensibile și pentru a redobândi accesul la sistemele afectate.

Cu toate acestea, plata răscumpărării NU reprezintă o garanție a faptului că atacatorii vor furniza cheile de decriptare, respectiv vor renunța la utilizarea datelor exfiltrate.

INFO BOX

Cea mai bună soluție pentru incidentele cibernetice de acest gen este preîntâmpinarea lor, prin asigurarea unui nivel adecvat de securitate cibernetică a sistemelor și rețelelor utilizate.

De asemenea, este necesară crearea și consolidarea unei culturi de securitate cibernetică adecvată în rândul angajaților, întrucât cele mai multe atacuri cibernetice sunt derulate prin utilizarea unor tehnici de inginerie socială.

ȚIȚEICA

SISTEMUL NAȚIONAL DE PROTECȚIE A INFRASTRUCTURILOR IT&C DE INTERES NAȚIONAL ÎMPOTRIVA AMENINȚĂRILOR PROVENITE DIN SPAȚIUL CIBERNETIC

Complexitatea mediului de securitate cibernetică și evoluția rapidă a trendurilor și tehnologiilor subsumate acestui domeniu reclamă necesitatea consolidării capabilităților investigative ale unui serviciu de informații. Fie că vorbim de actori motivați strategic, financiar sau ideologic, activitatea în domeniul cyberintelligence, prin caracterul preponderent tehnic al amenințării la adresa securității naționale, presupune inclusiv derularea de activități specifice unui Security Operations Center (SOC).

Un Security Operations Center reprezintă o facilitate formată din experți în securitate cibernetică responsabili cu monitorizarea, analizarea și reacția la evenimente de securi-

tate cibernetică. Zonele de competență ale unui SOC sunt rețelele, serverele, echipamentele de tip endpoint, bazele de date, aplicațiile, site-urile web și a alte sisteme, în scopul detectării anomaliilor care se pot constitui în incidente de securitate cibernetică.

Pentru derularea unor investigații cât mai aprofundate, care să reliefeze concluzii relevante necesare demersurilor de mitigare a riscurilor de securitate cibernetică, la nivelul Serviciului Român de Informații, prin Centrul Național CYBERINT (CNC), se derulează activități specifice unui SOC, precum analiză forensics, analiză malware, audituri de securitate cibernetică și management al incidentelor de securitate cibernetică.

Principalul instrument tehnic prin care CNC obține cunoașterea necesară derulării de investigații asupra atacurilor cibernetice care vizează infrastructurile IT&C cu valențe critice pentru securitatea națională (IVC) este „Sistemul național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic" (ȚIȚEICA). Acest proiect este realizat prin finanțare din fonduri europene și este contractat de SRI, în parteneriat cu STS, CERT-RO, MApN și MAI.

Prin intermediul ȚIȚEICA, 54 de instituții publice au beneficiat de echipamente și expertiză în scopul securizării IVC-urilor.

Rolul ȚIȚEICA și implicit al echipamentelor implementate la nivelul instituțiilor beneficiare este de a identifica în timp real tentative ale atacatorilor cibernetici de compromitere a IVC-urilor. Raportat la misiunile Serviciului Român de Informații ș i la atribuțiile deținute în domeniul cyberintelligence, sistemul ȚIȚEICA este utilizat pentru:

➡ Cunoaștere - sistemul furnizează suportul informațional necesar elaborării măsurilor proactive și reactive în vederea asigurării securității cibernetice. Astfel, se vizează cunoașterea pe scară largă a riscurilor și amenințărilor derivate din activitățile ostile desfășurate în spațiul cibernetic, precum și a modului de prevenire și contracarare a acestora.

➡ Prevenție - constă în totalitatea acțiunilor întreprinse pentru eliminarea breșelor de securitate, înainte ca acestea să fie exploatate, în scopul prevenirii furtului, distrugerii sau alterării datelor.

➡ Detecție - alertează persoanele abilitate la nivelul IVC că anumite evenimente neautorizate sau nedorite au avut loc.

➡ Investigare - constă în identificarea cauzelor incidentului, analiza sistemelor afectate, identificarea daunelor și stabilirea măsurilor de protecție împotriva unor activități similare viitoare.

➡ Corecție - constă în totalitatea acțiunilor necesare pentru remedierea unei vulnerabilități sau a unei breșe de securitate identificată în cadrul rețelei informatice IVC și pot consta în aplicarea unor actualizări pentru anumite aplicații sau sisteme, efectuarea unor modificări de configurație, sau oprirea unor servicii vulnerabile.

În vederea consolidării capabilităților de detecție ale CNC, s-a demarat implementarea proiectului ȚIȚEICA 2.0, care are ca obiectiv principal actualizarea sistemului de protecție existent, prin modernizarea sistemelor de securitate deja implementate, și includerea în cadrul acestuia a 4 noi instituții din arcul guvernamental. Proiectul se află în curs de implementare și are ca beneficiari un număr de 59 de instituții publice.

NECESITATEA ASIGURĂRII SECURITĂȚII CIBERNETICE A **ORAȘELOR INTELIGENTE**

ÎN ULTIMII ANI S-AU INTENSIFICAT PREOCUPĂRILE LA NIVEL INTERNAȚIONAL PENTRU EFICIENTIZAREA UNOR PROCESE ȘI SERVICII FURNIZATE CETĂȚENILOR PRIN ÎNCURAJARE DEZVOLTĂRII ORAȘELOR INTELIGENTE (SMART CITIES).

Conceptul de smart city presupune un grad ridicat de tehnologizare și interconectare, care facilitează dezvoltarea sustenabilă a vieții sociale și economice, ceea ce se transpune în creșterea calității vieții cetățenilor. Smart city se bazează pe tehnologii cloud, artificial intelligence și internet of things pentru a stoca, analiza și coordona modalitatea de utilizare a datelor în timp real. Smart city ar putea fi implementat în: distribuția de energie, colectarea selectivă deșeurilor, decongestionarea traficului și îmbunătățirea calității aerului.

Proiectele smart city aduc o serie de avantaje, precum accesul facil la produse și servicii de calitate, la sisteme de educație și sănătate moderne, reducerea birocrației, simplificarea fluxurilor informaționale, dezvoltarea de parteneriate public-private.

Pe de altă parte, operaționalizarea unor proiecte de acest tip generează o serie de provocări inclusiv din perspectiva asigurării unui nivel adecvat de securitate cibernetică. Astfel, pe fondul utilizării și interconectării unui spectru variat de echipamente și tehnologii, problema securității cibernetice a sistemelor/ rețelelor reprezintă o reală provocare pentru toate statele comunitare, inclusiv pentru România.

În scopul creșterii utilității acestor proiectelor smart city și al diminuării riscurilor de securitate cibernetică asociate, în procesul de implementare este importantă analizarea următoarelor aspecte:

➔ **orașele au diferite tipuri de nevoi,** motiv pentru care nu există un model unic de dezvoltare. Ca urmare, nevoile reale ale cetățenilor trebuie să reprezinte baza în proiectarea și dezvoltarea smart city.

Alba Iulia reprezintă un proiect pilot al conceptului de smart city, din perspectiva faptului că oferă un pachet de peste 100 de soluții pentru o serie de facilități care să fie puse la dispoziția cetățenilor. La nivelul orașului există soluții smart în domenii precum planificare urbană, mobilitate urbană, utilități publice, mediu, siguranță publică, sănătate, sustenabilitate a patrimoniului, educație, turism, administrație publică și mediul de afaceri local.

➔ **inițierea și dezvoltarea unui dialog între instituțiile publice, companiile din sectorul privat și societatea civilă** în proiectarea, dezvoltarea și operaționalizarea unor orașe inteligente. Implicarea tuturor actorilor ar facilita înțelegerea și evaluarea riscurilor ce decurg din implementarea unor proiecte smart city.

➔ **în proiectarea, dezvoltarea și operaționalizarea proiectelor de tip smart city** este necesar să fie avută în vedere securitatea cibernetică a infrastructurilor IT&C utilizate, dar și interoperabilitatea și proprietatea datelor.

Conform Ghidului Smart City pentru România trebuie asigurată securitatea cibernetică pe următoarele paliere:

⇢ comunicarea persoană-persoană (P2P) ce reprezintă suportul de bază în funcționarea rețelelor de socializare, aplicațiilor de gestiune, aplicații de ghidare etc.;
⇢ comunicarea persoană-mașină (P2M) ce se bazează pe tehnologia cloud;
⇢ comunicarea mașină-mașină (M2M) prin care se realizează legătura între Internet of Things, unde regăsim obiecte, dispozitive, senzori statici și dinamici și internetul datelor, ce reprezintă conectarea interoperabilă a tuturor bazelor de date.

➔ **necesitatea realizării unui buget realist** care să asigure cheltuielile aferente resurselor umane și materiale.

➔ **necesitatea elaborării unor standarde de implementare a smart city.** Lipsa acestora poate afecta armonizarea tehnologiilor și aplicațiilor integrate în smart city.

STATISTICI

TOP 10 CAMPANII MALWARE ÎN ROMÂNIA (Ianuarie 2020 - Iulie 2020)

1	INFOSTEALER.MSIL.AGENTTESLA	2267
2	TROJAN.SALITY	899
3	EXPLOIT.IOT.MIRAI	714
4	EMOTET_CAMPAIGN_TREND	451
5	TROJAN_AUTOIT	430
6	TOOL.COINMINER	423
7	TROJAN.DOWNLOADER	382
8	EXPLOIT.IOT.GENERIC	337
9	TROJAN.FORMBOOK	302
10	MALICIOUSWEBCRYPTOMINER	196

FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE PHISHING

IANUARIE	6291
FEBRUARIE	1609
MARTIE	243
APRILIE	156
MAI	157
IUNIE	26774

CELE MAI FRECVENTE TIPURI DE ATACURI

TROJAN	33.73%
INFOSTEALER	30.15%
EXPLOIT	23.14%
BACKDOOR	5.86%
TOOL	5.19%
WORM	1.93%

APLICAȚII NELEGITIME ÎN CONTEXTUL **COVID-19**

ÎN CONTEXTUL PANDEMIEI DE COVID-19 AU FOST DEZVOLTATE MAI MULTE APLICAȚII MOBILE MENITE SĂ VINĂ ÎN SPRIJINUL CETĂȚENILOR.

Acestea au fost realizate cu scopul de a informa utilizatorii cu privire la numărul de infectări, pentru transmiterea de rapoarte zilnice pe acest subiect sau pentru evaluarea riscului expunerii acestora. În acest context, anumite aplicații mobile solicitau permisiuni de acces la locația dispozitivelor mobile, pentru identificarea persoanelor care au frecventat aceleași zone sau permisiuni necesare monitorizării istoricului de plăți.

O serie de actori cibernetici au considerat contextul oportun pentru a derula activități ilegale de obținere a datelor cu caracter personal sau beneficii financiare. Printre modalitățile de acțiune utilizate frecvent se numără:

➡ dezvoltarea unor aplicații aparent legitime, care prin utilizare infectau dispozitivele mobile cu malware;

➡ impersonarea unor aplicații oficiale, astfel încât prin accesarea acestora să se realizeze infectarea dispozitivului.

COVID 19 TRACKER:

COVID 19 Tracker este o aplicație dezvoltată pentru terminalele mobile care rulează sistemul de operare Android. Aceasta conține un malware de tip ransomware, CovidLock, care deține capabilități de blocare a ecranului dispozitivului și de criptare a fișierelor existente pe acesta. În schimbul deblocării / redobândirii accesului se solicită în termen de 48 de ore, suma de 0.011BTC (aproximativ 100$). În cazul neplății, atacatorul cibernetic amenință utilizatorul prin ștergerea datelor stocate pe dispozitiv (fișiere multimedia, agendă telefonică etc.) și prin expunerea datelor personale în mediul online (credențiale, conturi utilizate în social media etc.)

Funcționalitatea aparent legitimă a aplicației vizează informarea utilizatorilor cu privire la posibile persoane infectate prezente în zona în care se află dispozitivul mobil. Odată deschisă aplicația, aceasta afișează două mesaje, prin care se cere permisiunea utilizatorilor de a primi alerte de la aplicație cât timp ecranul este blocat și permisiunea de a oferi aplicației acces în funcția de Accesibilitate a device-ului pentru monitorizarea activă a statisticilor. În realitate, utilizatorul oferă atacatorului rolul de administrator al dispozitivului, fiind inițiate automat operațiile de blocare a ecranului și criptare a fișierelor stocate.

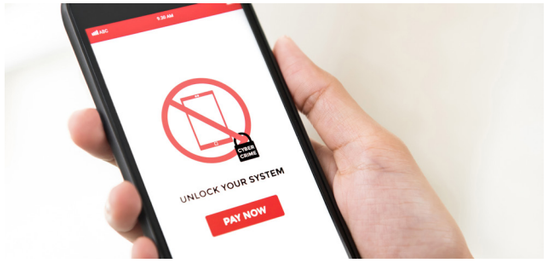
CovidLock a utilizat următoarele TTP-uri (tactici, tehnici și proceduri):

➡ Drive-by Compromise T1 (T1456) - presupune obținerea accesului pe un dispozitiv prin accesarea unui website nelegitim.

➡ App Auto-Start Device Boot (T140) - asigură activarea funcțiilor unei aplicații mobile odată cu pornirea dispozitivului, fără să fie nevoie de accesarea acesteia de către utilizator.

➡ Device Lockout (T1446) - presupune indisponibilizarea dispozitivelor pentru o perioadă determinată de timp.

În plus, ransomware-ul CovidLock realiza interogări Domain Name Server (DNS), prin care se făceau trimiteri la două link-uri asociate platformei Pastebin (https://pastebin[.]com/zg6rz6qT și https://pastebin[.]com/GK8qrfaC). În cadrul acestora se regăseau instrucțiunile pentru realizarea plății.



De asemenea, atrage atenția faptul că portofelul electronic Bitcoin al atacatorului nu figurează cu nicio tranzacție realizată, ceea ce denotă faptul că niciun utilizator atacat nu a achitat răscumpărarea. Acest lucru se datorează în primul rând activității experților în securitate cibernetică, întrucât au publicat cheia necesară decriptării ("4865083501") pe mai multe site-uri de specialitate.

Contextul social actual a demonstrat încă o dată faptul că securizarea dispozitivelor și aplicațiilor mobile reprezintă o necesitate prin prisma evoluțiilor de la nivelul spațiului cibernetic. În această perioadă, atacatorii cibernetici au exploatat deficiențele unor dispozitive devenite vulnerabile, atât din cauza factorului tehnologic, dar mai ales din cauza celui uman.