Cyber Intelligence si Operatiuni APT

Ce este Cyber Threat Intelligence?

- Colectarea, analizarea și diseminarea informațiilor despre amenințările actuale și potențiale la care este expusă o organizație, persoana, sau o tara
- Aceste date pot fi utilizate pentru a îmbunătăți capabilitățile defensive ale organizației

Obiective Cyber Threat Intelligence

- Conștientizarea volumului de amenințări, inclusiv metode, vulnerabilități, ținte și tipuri de actori actori malitiosi.
- Proactivitate în fața viitoarelor amenințări de securitate cibernetică prin implementarea datelor de Threat Intelligence in instrumentele defensive ale organizatiei
- Menținerea departamentelor de management și utilizatorilor la curent cu cele mai recente pericole și efectele pe care le pot avea asupra organizației.
- Impartasirea acestor informații cu organizații terte pentru a colabora în îmbunătățirea performanței detecției atacurilor cibernetice la nivel de industrie

Tipuri Comune de Amenintari

- Malware & Ransomware
- Phishing/Spear Phishing
- DoS/DDoS
- Spyware
- Adware
- Drive-by Download
- Exploatare de Vulnerabilitati Cunoscute (CVE-uri)
- Zero-Days
- Inginerie Sociala
- Cryptojacking
- Formjacking

Ce este OSINT?

- “Open-Source Intelligence” = OSINT
- Colectarea, analizarea și corelarea de date publice

Ce putem descoperi folosind OSINT?

- Posibile date confidențiale expuse pe Internet
- Tranzacții frauduloase
- Potențiale amenințări teroriste
- Impersonare de brand/identitate
- Vulnerabilitati
- Activele unei organizatii expuse pe Internet
  - Servere
  - Domenii & Subdomenii
- Informatii despre persoane
  - Profiling
  - Locatii Vizitate
  - Interese
  - Conexiuni
  - Numar telefon, email, data nastere, etc.
- Informatii despre organizatii
  - Angajati
  - Adrese email

Domenii de activitate OSINT

- Securitate Cibernetica
- Jurnalism
- Spionaj & Agentii de Intelligence
- Anti-Terorism
- Investigatii Criminale
- Investigarea Fraudelor
- Afaceri - Investigarea Concurentei

Studiu de caz - Operațiunea “Christmas Gift” -Charming Kitten (APT35) - IRGC

Localizare	Persoanele Țintă	Trăsătură comună	Obiective operaționale
• Statele Unite ale Americii • Uniunea Europeană • Țările din Golful Persic	• Activiști de mediu • Profesori Universitari • Experți în Orientul Mijlociu • Membrii ai centrelor de cercetare politică	• Opozanți ai Iranului • Oameni de interes pentru strategiile Iranului	• Compromiterea contului țintei • Monitorizare a activității tintei.

https://blog.certfa.com/posts/charming-kitten-christmas-gift/

Supreme Leader of Iran (رهبر معظم ایران)
Head of State - Political and religious authority

IRGC
~230,000 active duty

- Ground Forces
- Aerospace Force
- Navy
- Quds Force (special operations and military intelligence)
- Basij (volunteer militia)

Armed Forces
~420,000 active duty

- Ground Forces

- Air Defense Force

- Air Force

- Navy

Detalii operaționale

Atacatorii au folosit două metode pentru a-și executa atacurile:

1) SMS Phishing

1) Email Phishing

Elementul cheie al acestei faze inițiale a atacului este discreția. Obiectivul atacatorilor a fost să rămână ascunși și să nu lase urme.

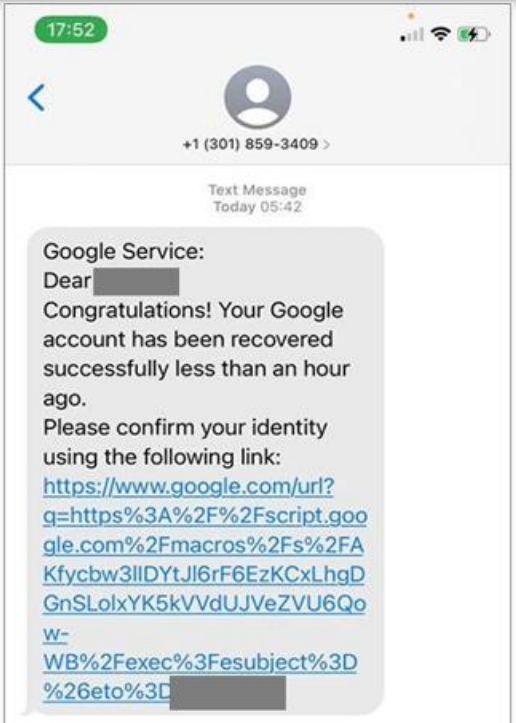
După ce au reușit compromiterea contului, atacatorii nu au blocat accesul victimei la propriul cont.

SMS Phishing

Servicii folosite: Google, Yahoo, Instagram, Outlook

Cel mai important aspect în această metodă de livrare este structura link-ului: hxxps://www.google[.]com/url?q=https://script.google.com/xxxx.

După mai multe redirecționări, ținta era în cele din urmă condusă către un link similar cu mobile[.]recover-session-service[.]site



Redirecționare

Parametrul “url” era folosit pentru a redirecționa ținta către un alt site.

În situația noastră, atacatorii au folosit acest mecanism pentru a face site-urile lor să pară legitime. În realitate, atacatorii au redirecționat ținta către un script găzduit prin serviciul Google Apps Script care se executa odată ce utilizatorul făcea clic pe link.

Scriptul verifica valoarea atribuită în variabila **eto** pentru a-și da seama dacă actorul care a dat click pe link a fost ținta reală sau o altă terță parte.

Atacatorii au folosit și servicii terțe, cum ar fi IP Logger, pentru a detecta dacă actorul care a dat click pe link a fost sau nu un serviciu de control automat.

Același serviciu a fost folosit pentru tactical reconnaissance pentru a obține date precum numărul de clickuri pe link, adresa IP a țintei, datele de localizare geografică etc..

Unele dintre site-urile de credential harvesting care se aflau la sfârșitul lanțului de redirecționare au fost găzduite de furnizori de servicii de găzduire din Iran.

Studiu de caz - Operațiunile “Pawn Storm” - APT28 aka Fancy Bear - GRU

Perioada 2014-2016 a fost una foarte tensionată pentru afacerile externe ale Rusiei:
• conflictul și anexarea ilegală a Crimeei
• desfășurarea de forțe pentru operații speciale NATO în Europa de Est.
• la sfârșitul anului 2014, Vladimir Putin a declarat „consolidarea” forțelor NATO în apropierea granițelor ruse drept principala amenințare militară la nivel național.

Creșterea interesului Rusiei pentru America Latină în acea perioadă:
• la două luni după inaugurarea lui Bachelet în martie 2014, ministrul rus de externe Lavrov a efectuat o vizită oficială în Chile. Șase luni mai târziu, președintele Bachelet s-a întâlnit cu Putin la Beijing. Această întâlnire a dus la angajamentul ministrului chilian de externe Heraldo Munoz de a călători în Rusia pentru a urmări problemele ridicate anterior. (*source: THE NEW RUSSIAN ENGAGEMENT WITH LATIN AMERICA: STRATEGIC POSITION, COMMERCE, AND DREAMS OF THE PAST by R. Evan Ellis)*
• în 2013, Mexicul a fost al șaselea cel mai mare partener comercial al Rusiei în regiune, aproape întreaga relație fiind achiziții de produse rusești de către Mexic. (*source: THE NEW RUSSIAN ENGAGEMENT WITH LATIN AMERICA: STRATEGIC POSITION, COMMERCE, AND DREAMS OF THE PAST by R. Evan Ellis)*

Ministry of Defence

General Staff of the Armed Forces

GRU (or GU)
Main Directorate of the General Staff

6th Directorate
Electronic & Signals Intelligence (ELINT & SIGINT)

85th Special Services Center
Military Unit 26165

Operațiunea Chile Air Force

Unitatea militară GRU 26165 a vizat Forțele Aeriene din Chile cu o campanie de phishing din 10 septembrie 2014 până în 12 decembrie 2014.

Atacatorii au copiat identitatea portalului oficial de webmail al FACh (Chile Air Force) găzduit la **mail.fach.mil.cl** prin înregistrarea unui domeniu la adresa **mail.fach.rnil.cl**.

Scopul operațiunii a fost compromiterea conturilor prin colectarea credentialelor.

În timpul operațiunii, merită menționate câteva evenimente geopolitice cheie, cum ar fi Ziua Forțelor Armate ale Chile din 19 septembrie 2014, care a inclus o paradă militară și mai multe vizite ale unor oficiali străini, precum și exercițiul forțelor aeriene din America de Sud Salitre III, antrenament comun de luptă aeriană în octombrie 2014, organizat de FACh.

Operațiunea ce a vizat guvernul din Mexic

GRU a vizat serverul de e-mail al Guvernului Mexicului în două campanii separate, una în noiembrie-decembrie 2013 și cealaltă în noiembrie-decembrie 2014.

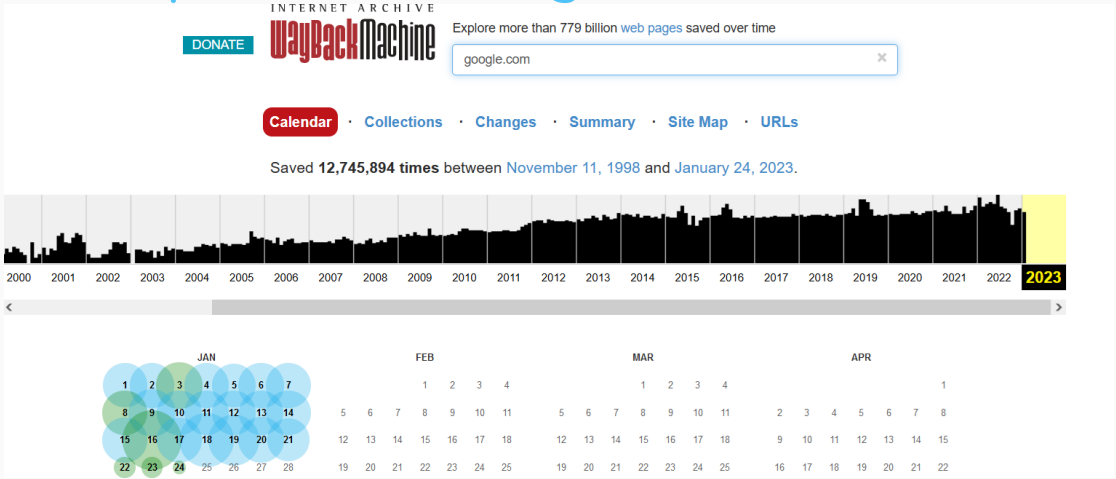
Atacatorii au copiat identitatea portalului oficial de webmail găzduit la **mx1.gob.mx** prin înregistrarea unui domeniu la adresa **g0b.mx**

Scopul operațiunii a fost compromiterea conturilor prin colectarea credentialelor.

Pe perioada operațiunii merită menționate câteva evenimente geopolitice cheie, cum ar fi aprobarea Senatului pentru privatizarea parțială a industriei petrolului/energiei, discuțiile și planurile legate de energie și aprobarea anuală a bugetului guvernului.

Wayback Machine

- Motor de cautare a versiunilor precedente a unei pagini web
- https://archive.org/web/

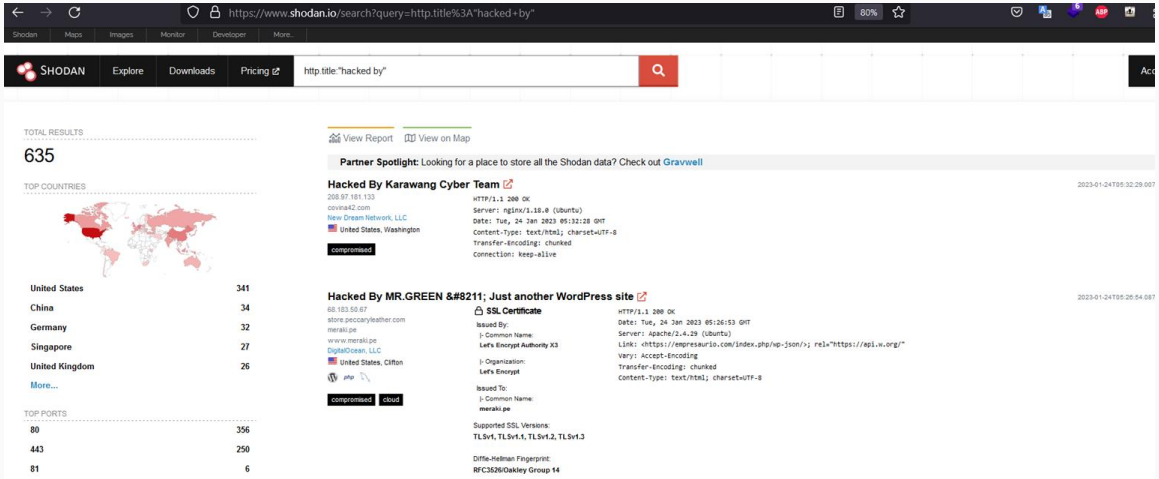


UrlScan

- Website scanner ce verifica undeva la 100,000 URL-uri pe zi.
- Util in investigarea campaniilor de phishing.
- https://urlscan.io/

Shodan

- Motor de cautare pentru dispozitivele conectate la Internet
- https://www.shodan.io/



Canary Tokens

- Instrument prin care putem afla adresa IP a unei ținte.
- canarytokens.org

Q&A