Ministerul Afacerilor Externe (MAE) - Ținta unui atac cibernetic în desfășurare

Așa cum am menționat în articole anterioare, infractorii cibernetici au ca scop comun obținerea de câștiguri financiare, direct sau indirect. Am scris infractori, deoarece atacurile cibernetice lansate de aceștia se aseamănă cu infracțiunile cunoscute în viața de zi cu zi.

Atacului cibernetic asupra Ministerului Afacerilor Externe nu îi putem atribui o astfel de descriere, pentru că în acest caz nu mai putem discuta despre infracțiune financiară, scopul atacatorilor fiind foarte definit... și anume accesul în infrastructura Ministerului.

1. Primele indicii

Ca specialist în securitate cibernetică, consider că pe lângă activitățile mele profesionale, trebuie să contribui la protejarea infrastructurii informaționale din România și pe cât posibil la cea europeană.

Prin monitorizarea constantă a evenimentelor din zona de securitate cibernetică, am observat că pe una dintre platformele online(urlscan.io) a apărut o creștere semnificativă a scanărilor asupra domeniului mae.ro, mai exact a subdomeniilor acestuia. Scanările pot fi făcute manual sau posibil să fi fost adăugat în lista unui software care folosește baza de date a acestei platforme

Cert este că în ultimele săptămâni acest domeniu a apărut a fi scanat destul de des.

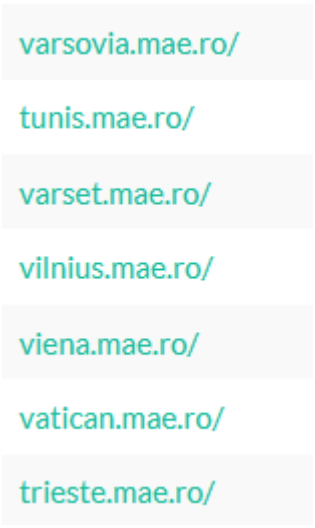

Fig.1: urlscan.io

Un aspect important în analizarea informațiilor, este concentrarea asupra elementelor care uneori par irelevante și atenția la detalii.. De aceea voi atașa următoarea imagine, în care deși este un domeniu cunoscut, parametrii incluși fac diferența/

Fig.2: urlscan.io

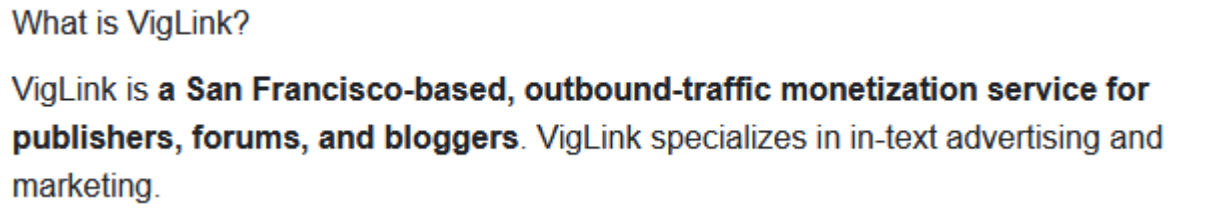

Fig.3: Google search

Mai pe scurt, nu are legătură cu infrastructura din România, cu MAE sau orice altceva relevant...

2. Analiza informațiilor

Diferența o face redirecționarea stabilită prin parametrii acestei adrese, deoarece ne trimite spre ceva foarte interesant.

Fig.4: urlscan.io

Ce observăm în conținutul noii adrese web?

- **xn—f1a** – adresa folosește pentru subdomeniu caracterul unui alfabet non latin, mai exact este alfabetul chirilic (știm cine în folosește...)
- domeniul principal se termină înainte de primul ”**/”,** cel principal este abc.aa/ și nu mae.ro.

Accesarea directă a adresei care conține acel *mail.mae.ro* ne trimite pe o pagină goală și din experiență știm că poate fi o pagină care are conținutul șters de către atacator/ administrator pagină(deoarece a fost marcată ca fiind malițioasă) sau... pentru a fi accesat conținutul trebuie ca vizitatorul să vină cu anumiți parametri de recunoaștere.

În urma decriptării primei adrese, care conține un șir lung de caractere ” MJRDWY%2E%76%64%31%6C%2E%70%69%63%73%2FWMK%2FTAXUID%2F WlhKbGRtRnVRRzFoWlM1eWJ3PT06Y2JnbGZmYXFwbQ==&drKey=173&HCYTPJ OCRBKSPFYHMLFX” se poate observa prezența următoarelor:

- **o nouă adresă** – aqyelnotn(editat)bysmjrdwy.vd1l.pics (IP Asia)
- **un parametru criptat**: *WlhKbGRtRnVRRzFoWlM1eWJ3PT06Y2JnbGZmYXFwbQ==*
  Decriptat: *ZXJldmFuQG1hZS5ybw==:*cbglffaqpm
  Decriptat: ***erevan@mae.ro***
- **o cheie:** drKey=173&HCYTPJOCRBKSPFYHMLFX

erevan@mae.ro este adresa folosită de Ambasada României din Armenia

Fig.5: Google search

Accesarea adresei cu acești parametri direcționează vizitatorul(victima) spre o nouă adresă(cea care apare mai sus *.vd1l.pics), după care îl trimite pe pagina falsă creată.

Toate acestea creează conținutul cu care vizitatorul poate vedea conținutul paginii, dar fiecare accesare conține anumite schimbări(imagine, subdomeniu, port). Acestea fiind vizibile la fiecare accesare.

```
'host:-login.mae.ro:8341
'host:-login.mae.ro:2137
'host:-web.mae.ro:3452
'host:-webmail.mae.ro:4123
'host:-web.mae.ro:0514
```

Fig.6: Analiză proprie

Una dintre accesări conține atașată prima pagină a domeniului oficial mae.ro, având o serie de articole, atenționări etc, plus forma de acces, dar există și varianta simplă care seamănă cu pagina unui server de email.

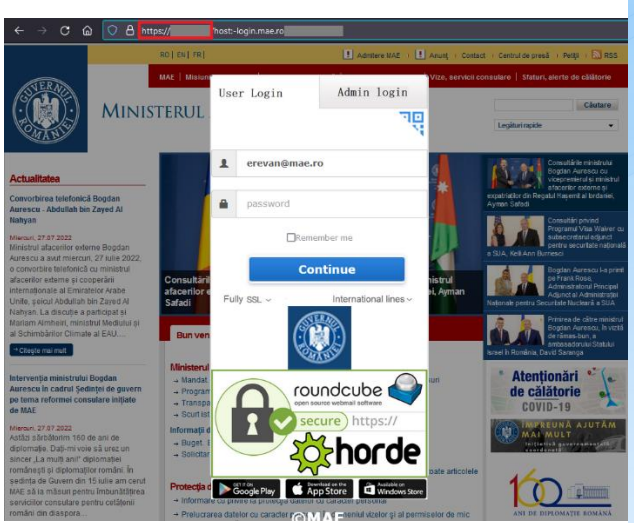

Fig.5: Analiză proprie

Fig.6: Analiză proprie:

Analizând conținutul formei de acces pe serverul de email observăm o serie de semnale de alarmă. Butoane/ meniuri false și desigur prezența caracterului chirilic...

Fig.7: Analiză proprie

3. Resurse

Urmărind traficul la accesarea domeniului putem observa resursele obținute din surse externe

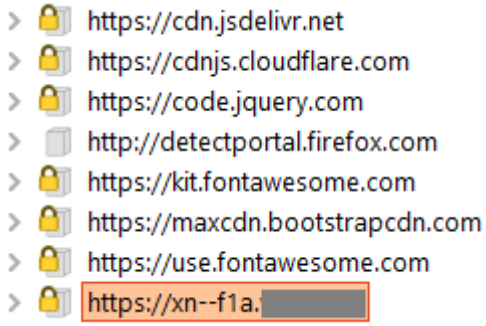

Fig.8: Analiză proprie

Pentru cei care au avut răbdare să citească până aici, pot spune că domeniul cu pagina falsă este web.app (Firebase/ Google), totul trecând prin serverele Cloudflare. Drept urmare pagina falsă este:

hxxps://xn--f1a.web.app/host:-mail.mae.ro:3187 - hxxps://ж.web.app/host:-login.mae.ro:3187

De reținut că portul se schimbă la fiecare accesare.

4. … și după ce obține acces?

Așa cum am observat, foarte mulți utilizatori nu conștientizează pericolul accesării ilegale a unui cont de email, considerând că ”mare lucru nu găsește acolo”, deși în cazul unei adrese de email al unei instituții de acest nivel nu cred că se mai poate pune problema astfel.

Accesul la serverul de email înseamnă mult mai mult decât citirea sau ștergerea mesajelor. Deși în cazul nostru, interceptarea mesajelor este un risc extrem.

Atacatorul poate folosi această adresă pentru a interacționa cu:

- Superiori,
- Colegi,
- Utilizatori ai platformelor instituției,
- Parteneri instituționali.

Având libertatea de a folosi adresa compromisă atacatorul poate lansa multiple atacuri cibernetice, folosindu-se de identitatea instituției:

- Atac phishing, pentru a compromite și alte adrese,
- Distribuire de malware, pentru a compromite dispozitivele celor cu care interacționează,
- Extragere de informații de la colegi și parteneri ai instituției,
- Fraudă financiară,
- Propagarea de știri false.

5. Educație. Profesionalism. Etică

Succesul atacurilor cibernetice depinde de acțiunile utilizatorului înainte de atac și modul în care reacționează atunci când este atacat.

Educația cibernetică și pregătirea utilizatorilor în combaterea atacurilor cibernetice este un factor important. Acesta trebuie să cunoască sistemul pe care îl folosește, să poată identifica un atac cibernetic sau măcar să reacționeze atunci când apare o situație diferită și suspect.

Respectarea politicilor și procedurilor de lucru este esențială! Acestea au ca scop prevenirea unor astfel de incidente și/ sau modalitatea de răspuns la acestea.

Nu în ultimul rând, utilizatorul trebuie să fie un profesionist, indiferent de situație. Chiar și atunci când, din neatenție, a greșit… acesta trebuie să respecte pașii care trebuie urmați în caz de incident cibernetic și să anunțe departamentul responsabil. Încercând să ascundem un incident, putem crea mult mai multe probleme.

Eu am trimis informațiile către **Directoratul Național de Securitate Cibernetică** și sunt convins că echipa @dnsc va trata subiectul cu aceiași seriozitate și profesionalism ca de fiecare dată.

Ceea ce vreau să subliniez și să fie luat în considerare este faptul că aceste informații sunt doar ceea ce am găsit eu și 100% atacul nu se rezumă la această adresă de email sau la această pagină falsă!

Acel parametru criptat, în care apare adresa de email a Ambasadei din Armenia, poate fi înlocuit cu oricare altă adresă a instituției... sau prin schimbarea celorlalți parametrii atacul poate imita/ clona oricare altă instituție sau firmă privată.

Atenție sporită la situațiile care ies din tiparele cunoscute!
Atenție la detaliile ”situațiilor urgente”!

Dacă situația depășește nivelul de pregătire, nu ezita să ceri ~~ajutor~~ o a doua părere!

Siguranța în mediul online este o responsabilitate comună și necesită implicarea tuturor!