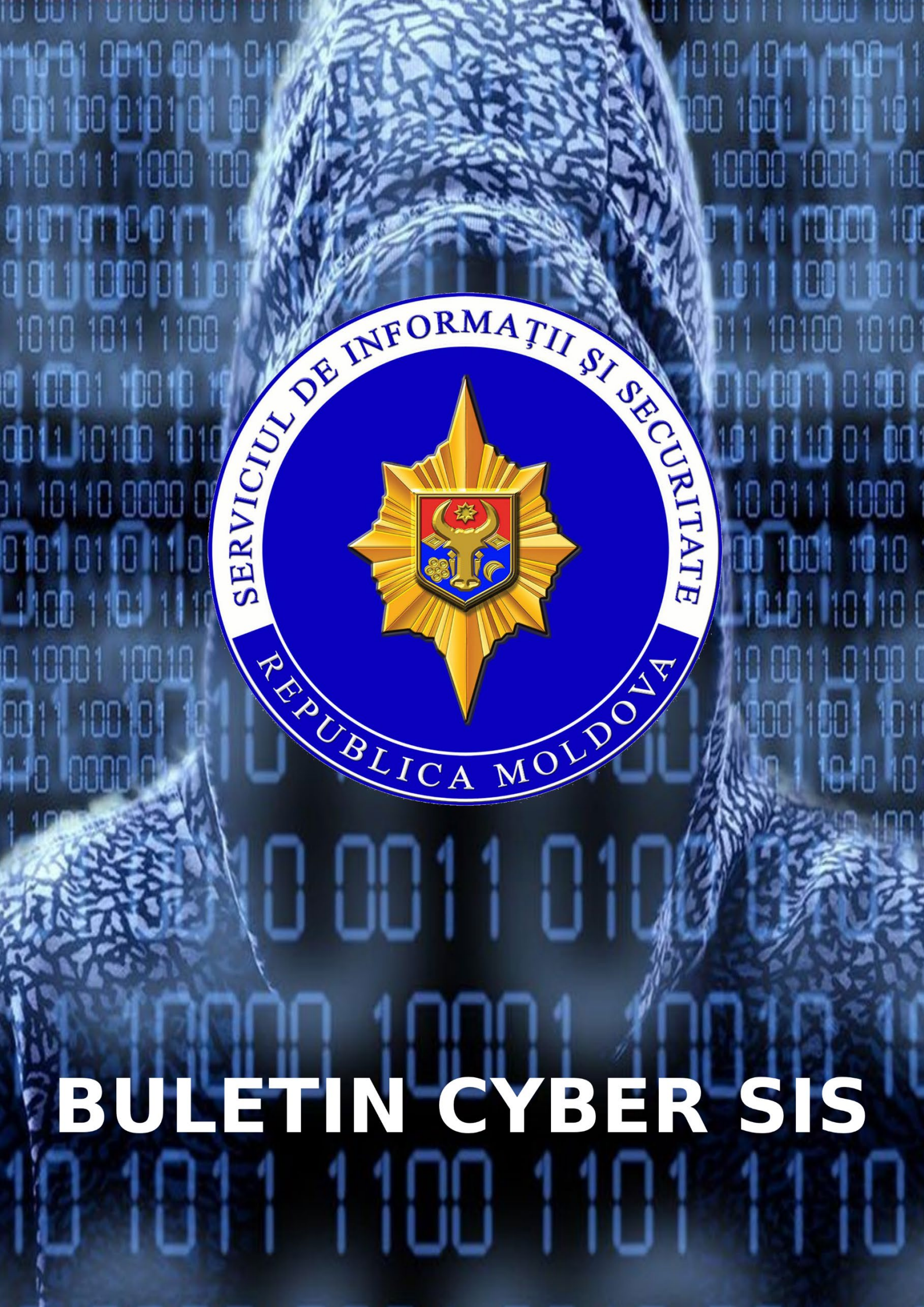


BULETIN CYBER SIS

NOTIFICARE

Serviciul de Informații și Securitate al Republicii Moldova vine cu un avertisment pentru operatorii obiectivelor infrastructurii critice naționale în legătură cu unele riscuri de securitate cibernetică la nivel regional și internațional.

Evoluția informațiilor indică faptul că anumiți actori statali explorează opțiuni pentru potențiale atacuri cibernetice la adresa obiectivelor infrastructurii critice și infrastructurilor IT&C cu valențe critice.
Operațiunile cibernetice recente sponsorizate de actorii statali au inclus atacuri distribuite de refuz a serviciului (DDoS), iar operațiunile mai vechi au inclus dezvoltarea mecanismelor și utilizarea aplicațiilor malițioase distructive în scopul:

- menținerii accesului pe termen lung și persistent la rețelele IT;
- exfiltrației datelor sensibile din rețelele IT și rețelele de tehnologie operațională (OT – SCADA/PLC/DCS/CNC/BMS/BAS);
- perturbării sistemelor critice de control industrial (ICS).

În acest sens organizațiile, instituțiile și întreprinderile ce fac parte din infrastructura critică națională sunt îndemnate să se pregătească și să atenueze potențialele amenințări cibernetice prin:
(1) actualizarea imediată a software-ului;
(2) aplicarea MFA (Multifactor Authentication);
(3) securizarea și monitorizarea conexiunilor RDP și altele servicii cu potențial risc.
(4) educarea, instruirea și conștientizarea utilizatorilor finali privind respectarea regulilor de igienă cibernetică.

1) Actualizați software-ul, inclusiv sistemele de operare, aplicațiile și firmware-ul, pe activele IT din rețea. Acordați prioritate aplicării pachetelor de remediere pentru vulnerabilitățile exploatate cunoscute și vulnerabilitățile cu statut critic(critical) și major (high), care permit executarea codului la distanță sau refuzarea serviciului pe echipamentele cu acces la Internet.

Luați în considerare utilizarea unui sistem centralizat de gestionare a remedierilor. Pentru rețelele OT, utilizați o strategie de evaluare bazată pe risc pentru a determina activele și zonele rețelei OT care ar trebui să participe la programul de gestionare a remedierilor.

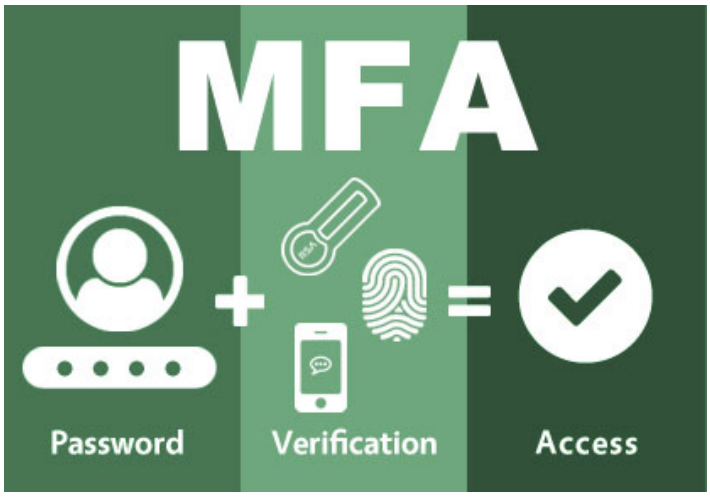
Exploatarea vulnerabilităților aplicațiilor cunoscute (T1190), compromiterea aplicațiilor des utilizate la fel este populară tehnica ce se utilizează de către hackeri la faza inițială a atacului cibernetic. La momentul actual frecvent sunt exploatate următoarele vulnerabilități:

- CVE-2018-13379 (Fortinet FortiOS)
- CVE-2018-10939 (Zimbra mail)
- CVE-2019-2725 (Oracle WebLogic Server)
- CVE-2019-0708 (Microsoft Remote Desktop Protocol)
- CVE-2020-5902 (BIG-IP)
- CVE-2020-0688 (Microsoft Exchange Server)

Pentru a se apăra ar trebui să respectați următoarele recomandări:

- Scanați în mod regulat sistemele care sunt accesibile din internet pentru identificarea vulnerabilităților existente (M1016);
- Remediați imediat vulnerabilitățile critice identificate. Actualizați aplicațiile în mod regulat (M1051);

Monitorizați jurnalele *Application Log* (DS0015) pentru a identifica orice comportamente anormale ce indică o încercare sau o exploatare reușită.



2) Aplicați mecanisme de autentificare cu mai mulți factori (MFA) în cea mai mare măsură posibilă și solicitați autentificare printr-o parolă puternică pentru toate conturile, inclusiv conturile de serviciu. Nu permiteți utilizarea/reutilizarea aceleași parole în mai multe conturi sau stocarea lor într-un sistem la care un adversar poate avea acces. Actorii cibernetici sponsorizați de state străine (APT) și-au demonstrat capacitatea de exploatare protocoalelor MFA implicite și vulnerabilitățile cunoscute, organizațiile, instituțiile și întreprinderile ar trebui să asigure revizuirea politicilor de configurare a serviciilor MFA pentru a se proteja împotriva scenariilor de „deschidere eșuată” și reînscriere. Un eventual scenariu fiind descris mai jos.

> Actorii cibernetici sponsorizați de state străine au obținut acces inițial [TA0001] la organizația victimei prin intermediul acreditărilor compromise [T1078] și prin înscrierea unui nou dispozitiv în Duo MFA al organizației. Actorii au obținut acreditările [TA0006] printr-un atac de ghicire a parolei cu forță brută [T1110.001], permițându-le acces la un cont de victimă cu o parolă simplă, previzibilă. Contul victimei avea a fost dezactivat din Duo din cauza

unei perioade lungi de inactivitate, dar nu a fost dezactivat în Active Directory. Întrucât setările implicite de configurare ale Duo permit reînregistrarea unui nou dispozitiv pentru conturile latente, actorii au putut să înregistreze un nou dispozitiv pentru acest cont, să completeze cerințele de autentificare și să obțină acces la rețeaua victimei.

Folosind un cont compromis, actorii cibernetici au efectuat escaladarea privilegiilor [TA0004] prin exploatarea vulnerabilității „PrintNightmare" (CVE-2021-34527) [T1068] pentru a obține privilegii de administrator. Actorii au modificat, de asemenea, un fișier controler de domeniu, ***c:\windows\system32\drivers\etc\hosts***, redirecționând apelurile Duo MFA către localhost în loc de serverul Duo [T1556]. Această modificare a împiedicat serviciul MFA să-și contacteze serverul pentru a valida autentificarea MFA — acest lucru a dezactivat efectiv MFA pentru conturile de domeniu active, deoarece politica implicită a Duo pentru Windows este „deschiderea eșuată" (fail open) dacă serverul MFA nu este accesibil. După dezactivarea efectivă a MFA, actorii cibernetici sponsorizați de stat au putut să se autentifice cu succes în rețeaua virtuală privată (VPN) a victimei ca utilizator non-administrator și să realizeze conexiuni Remote Desktop Protocol (RDP) la controlerele de domeniu Windows [T1133]. Actorii au executat comenzi pentru a obține date de autentificare pentru conturi de domeniu suplimentare; apoi, folosind metoda descrisă în paragraful anterior, au schimbat fișierul de configurare MFA și au ocolit MFA pentru aceste conturi noi compromise. Actorii au folosit în mare parte instrumentele interne ale SO Windows deja prezente în rețeaua victimei pentru a efectua această activitate. Folosind aceste conturi compromise fără aplicarea MFA, actorii cibernetici sponsorizați de stat au putut să se deplaseze lateral [TA0008] la conturile de e-mail și spațiul de stocare în cloud ale victimei și să acceseze conținutul dorit.

INDICATORI DE COMPROMITERE

Au fost executate următoarele fișiere:

ping.exe − Un proces central al sistemului de operare Windows utilizat pentru a efectua Transmiterea Control Protocol (TCP)/comanda IP Ping; folosit pentru a testa conexiunea la rețea la o gazdă la distanță [T1018] și este folosit frecvent de actori pentru descoperirea rețelei [TA0007].

regedit.exe − Un fișier executabil standard de Windows care deschide editorul de registry încorporat [T1112].

rar.exe − Un instrument de compresie, criptare și arhivare a datelor [T1560.001] cyber rău – intenționat actorii au căutat în mod tradițional să compromită protocoalele de securitate MFA, așa cum ar face acest lucru oferiți acces la conturi sau informații de interes.

ntdsutil.exe − Un instrument de linie de comandă care oferă facilități de gestionare pentru Active Directory Servicii de domeniu. Este posibil ca acest instrument să fi fost folosit pentru a enumera utilizatorii Active Directory conturi [T1003.003].

Actorii cibernetici au modificat fișierul ***c:\windows\system32\drivers\etc\hosts*** pentru a preveni comunicarea cu serverul Duo MFA:
127.0.0.1 api-<redacted>.duosecurity.com

Următoarele adrese IP ale dispozitivelor utilizate de actorii cibernetici au fost identificate până în prezent:
45.32.137[.]94
191.96.121[.]162
173.239.198[.]46
157.230.81[.]39

Pentru mai multe informații, consultați [AA22-074A].

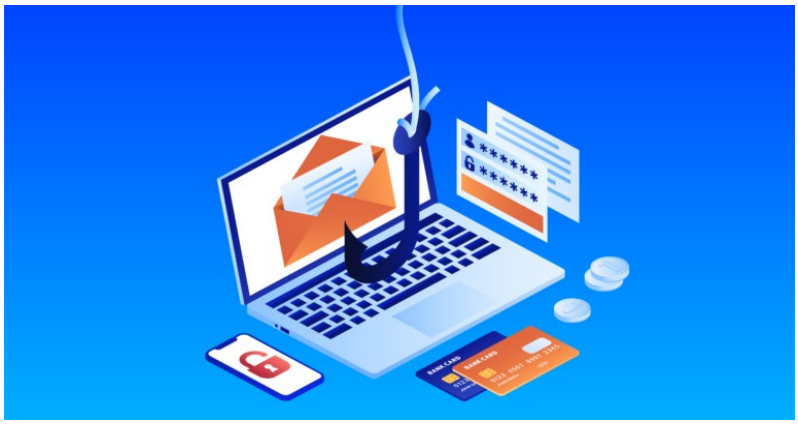
3) Dacă utilizați RDP și/sau alte servicii potențial riscante, asigurați-le și monitorizați-le îndeaproape. Exploatarea RDP este unul dintre cei mai buni vectori de infecție inițială pentru ransomware, iar serviciile riscante, inclusiv RDP, pot permite accesul neautorizat la sesiunea dvs. folosind un atacator pe cale.
Limitați accesul la resurse prin rețelele interne, în special prin restricționarea RDP și utilizarea infrastructurii desktop virtuale. După evaluarea riscurilor, dacă RDP este considerat necesar din punct de vedere operațional, restricționați sursele de origine și solicitați MFA să atenueze furtul și reutilizarea datelor de autentificare. Dacă RDP trebuie să fie disponibil extern, utilizați un privat virtual rețea (VPN) sau alte mijloace pentru a autentifica și securiza conexiunea înainte de a permite RDP să se conecteze la dispozitivele interne. Monitorizați jurnalele de acces la distanță/RDP, impuneți blocarea contului după un număr specificat de încercări de a bloca încercările de forță brută, înregistrați încercările de conectare RDP și dezactivați accesul la distanță/porturile RDP neutilizate.
Asigurați-vă că dispozitivele sunt configurate corect și că funcțiile de securitate sunt activate. Dezactivați porturile și protocoalele care nu sunt utilizate în scopuri comerciale (de exemplu, portul 3389 RDP Transmission Control Protocol).

Serverele RDP, accesibile din internet (T1133) sunt des utilizate de către grupările cibernetice criminale sponsorizate de actori statali (APT28, APT29) pentru a efectua

accesul inițial la sistemele informatice. Multe atacuri succese au fost efectuate utilizând următoarele tehnici *brute force* (T1110.001) – atacatorul încearcă să se autentifice cu parole aleatorii, făcând acest lucru poate chiar și de milioane de ori; *password spraying* (T1110.003) – este o altă variantă a atacurilor tip brute force în care un atacator încearcă aceeași parolă pe mai multe conturi de utilizator; sau *credential stuffing* (T1110.04) – este similar unui atac de tip brute force, cu excepția faptului că încearcă să utilizeze date de autentificare deja compromise pentru autentificare și aceste date pot fi găsite în domeniul public, pe forumurile de hacking și pe dark web. Pentru a se apăra mai bine împotriva atacurilor ar trebui să respecte următoarele recomandări:

- Utilizați parole complexe pentru toate conturile de admin / user care se pot accesa prin RDP (M1027);
- Implementați o politică de "maximum 3 încercări eșuate de autentificare" via Group Policy (M1036);
- Utilizați autentificare multifactorială (M1032);

Monitorizați jurnalele de autentificare *User Account* (DS0002) și *Application Log* (DS0015).



4) Asigurați educarea, instruirea și conștientizarea utilizatorilor finali pentru a ajuta la prevenirea campaniilor de succes de inginerie socială și spearphishing. Phishing-ul este unul dintre cei mai importanți vectori de infecție pentru ransomware, iar actorii cibernetici au desfășurat campanii de succes de spearphishing pentru a obține datele de acces pentru rețele țintă.

- Asigurați-vă că angajații sunt conștienți de potențialele amenințări cibernetice și de metodele de livrare.
- Asigurați-vă că angajații știu ce trebuie să facă și pe cine să contacteze atunci când primesc un e-mail suspect (phishing) sau suspectează un incident cibernetic.

Metodele de detectare a atacurilor de inginerie socială pot fi separate în două tipuri de detecție, detecție bazată pe factorul uman și detecție bazată pe tehnică și tehnologii. Detecția bazată pe factorul uman se realizează prin: educație, instruire și conștientizare, implementarea politicilor de securitate și audit al activității. Detecția bazată pe tehnică și tehnologii presupune utilizarea: biometriei, inteligenței artificiale, honeypot-urilor și al senzorilor.

Nu în ultimul rând îndemnăm să atrageți atenția asupra tehnicilor și tacticilor utilizate în cadrul campaniilor/atacurilor cibernetice realizate de către următoarele grupări/actori:

Turla [G0010]
Dragonfly [G0035]
APT29 [G0016]
APT28 [G0007]
Sandworm Team [G0034]
Temp.Veles [G0088]
Gamaredon Group [G0047]

Momentan, asemenea atacuri nu au fost semnalate în Republica Moldova.

În cazul apariției unor situații descrise în notificare, solicităm respectuos să ne contactați:

Date de contact:
022239393
067433899
069055446
069142969

https://antiteror.sis.md