SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

Ransomware
Ghid Informativ

Ce reprezintă un Ransomware

Ransomware este un tip de malware conceput pentru a compromite datele unei victime și a restricționa accesul la ele, cerând o răscumpărare pentru deblocare. Organizațiile cele mai expuse atacurilor ransomware gestionează date sensibile, cum ar fi informații personale, date financiare sau proprietate intelectuală.

În timp, atacurile ransomware au evoluat de la simple cereri de răscumpărare pentru cheia de decriptare, la tactici mai sofisticate, precum dublă și triplă extorcare, sporind semnificativ impactul asupra victimelor.

Modul de infectare sau distribuție

Tehnica	Cod MITRE	Descriere
Phishing și inginerie socială	T1566	Atacurile de inginerie socială păcălesc victimele să descarce și să ruleze fișiere executabile care se dovedesc a fi ransomware.
Exploatarea aplicațiilor	T1190	Exploatarea vulnerabilităților unui server web pentru a lansa un atac ransomware.
Credențiale valide	T1078	Atacatorii obțin sau sparg acreditări (inclusiv prin RDP) și le folosesc pentru acces neautorizat în rețea, de unde pot implementa direct ransomware.
Transfer Instrument Ingress	T1105	Alte programe malware descarcă și rulează ransomware pe sistemul compromis

Cum Funcționează

Pasul 1. Vectori de infecție și distribuție

După compromitere, ransomware-ul rulează discret, atacă fișierele și poate accesa sau modifica acreditări, lăsând sistemul sub controlul atacatorului.

Pasul 2. Criptarea datelor

Ransomware-ul criptează fișierele folosind o cheie controlată de atacator, înlocuind originalele cu versiuni criptate.

Pasul 3. Cererea de răscumpărare

După criptare, ransomware-ul afișează nota de răscumpărare, fie pe fundalul desktop-ului, fie în fișiere text din directoarele afectate.

Tipuri de atac

Unele tipuri importante de ransomware și amenințări conexe includ:

- **Criptarea tradițională:** datele victimei sunt criptate, accesul fiind condiționat de plata unei sume de bani.
- **Double Extortion:** Dubla extorcare, combină criptarea datelor cu furtul de date. Această tehnică a apărut ca reacție la refuzul unor organizații de a plăti: atacatorii amenință să publice datele furate dacă nu primesc răscumpărarea.
- **Triple Extortion:** Extorcarea triplă presupune, pe lângă criptarea și scurgerea datelor, aplicarea unei presiuni suplimentare – de exemplu, solicitarea de răscumpărări clienților sau partenerilor ori executarea unui atac DDoS.
- **Locker Ransomware:** Ransomware-ul Locker nu criptează fișierele dar computerul , făcându-l inutilizabil pentru victimă.
- **Crypto Ransomware:** Crypto ransomware este un alt nume pentru ransomware care subliniază faptul că plățile ransomware sunt plătite în mod obișnuit în criptocurrency.
- **Wiper:** O formă de malware care este legată, dar distinctă de ransomware. Deși pot utiliza aceleași tehnici de criptare, scopul este de a refuza permanent accesul la fișierele criptate
- **Ransomware as a Service (RaaS):** În modelul RaaS, dezvoltatorii de ransomware furnizează malware-ul către afiliați, care îl utilizează pentru a compromite victime. Veniturile din răscumpărări sunt apoi împărțite între afiliați și dezvoltatori.

Cum să te protejezi împotriva unui atac

1. **Patching:** Este esențial ca organizațiile să se asigure că toate sistemele au cele mai recente patch-uri aplicate
2. **Instalați Antivirus Protection.** Protecția antivirus este una dintre cele mai puternice și mai simple soluții în lupta împotriva malware-ului.
3. **Backup-uri de date continue:** Backup-urile automate și protejate permit unei organizații să se recupereze după un atac cu o pierdere minimă de date și fără a plăti o răscumpărare.
4. **Educarea utilizatorilor**. Instruirea utilizatorilor cu privire la modul de identificare și evitare a potențialelor atacuri ransomware.
5. **Autentificarea utilizatorilor**: Utilizarea autentificării puternice a utilizatorilor poate face mai dificil pentru un atacator să folosească o parolă ghicită sau furată.

Detectare și Eliminare

Multe atacuri ransomware sunt detectate abia după ce fișierele au fost criptate și apare nota de răscumpărare. În acest caz, urmați imediat pașii:

1. **Izolați dispozitivul:** Pentru a împiedica răspândirea ransomware-ului la unități sau alte computere.
2. **Lăsați computerul pornit:** Criptarea poate destabiliza sistemul, iar oprirea poate duce la pierderea memoriei volatile.
3. **Copiați fișierele criptate:** Salvați-le pe suporturi externe pentru a putea încerca decriptarea fără a plăti răscumpărarea.
4. **Verificați decriptori disponibili:** Consultați Proiectul No More Ransom și testați un decriptor pe copia fișierelor.
5. **Cereți ajutor specializat**: Experții pot recupera copii de rezervă sau date ascunse de malware.
6. **Ștergeți și restaurați:** Folosiți un backup sigur pentru a elimina complet malware-ul și a restaura sistemul.

Variante Populare de Ransomware

Există zeci de variante de ransomware, fiecare cu propriile caracteristici unice. Iată câteva din ele:

1.**Ransomhub:** un grup proeminent RaaS, care a apărut în februarie 2024, a crescut rapid în importanță prin atragerea de afiliați din grupuri perturbate precum ALPHV și LockBit.

2.**Akira:** o variantă de ransomware identificată pentru prima dată în 2023, vizează atât sistemele Windows, cât și cele Linux folosind criptarea ChaCha2008. Se infiltrează în sisteme prin e-mailuri de phishing și vulnerabilități VPN, apoi folosește tactici precum LOLBins și dumpingul de acreditare pentru a evita detectarea și a obține privilegii.

3.**Play Ransomware Group**, cunoscut și sub numele de Play sau Playcrypt, a apărut ca o entitate criminală cibernetică semnificativă din 2022, compromițând cu succes peste 300 de organizații la nivel global, inclusiv ținte de profil înalt precum Microsoft Cuba, Orașul Oakland și guvernul elvețian. Acest grup utilizează tactici unice, cum ar fi criptarea intermitentă, care criptează numai părți selective ale fișierelor și extorcarea dublă.

4.**Clop** este o variantă a malware-ului Cryptomix. Este o amenințare sofisticată care funcționează ca un RaaS și vizează în primul rând industriile care gestionează date sensibile, cum ar fi asistența medicală și finanțele. Acesta folosește o strategie de dublu extorcare și este cunoscut pentru codul său semnat digital, cerințele de răscumpărare ridicate, utilizarea SDBOT pentru auto-propagare și o preferință pentru rețelele corporative.

5.**Qilin** operează ca un proeminent RaaS, utilizând un ransomware extrem de personalizabil pentru a viza organizații din diferite sectoare la nivel global. Acest grup a câștigat o tracțiune semnificativă în aprilie 2025, fiind în fruntea listei pentru atacurile ransomware. Qilin utilizează o tehnică de dublă extorcare.