Securitate ofensiva Tema 1. Analiza a grupărilor de hackeri

1. Cobalt Group

Scurt istoric: Cobalt Group este o grupare criminală cibernetică activă din 2016, cunoscută pentru atacurile asupra instituțiilor financiare din Europa de Est și alte regiuni. Grupul a devenit notoriu pentru utilizarea troianului Carbanak și a tehnicii „cash-out” prin ATM-uri compromise, reușind să fure milioane de dolari.

Instrumente utilizate: Cobalt Strike (Trojan): Un instrument de testare pentru penetrare folosit pentru exploatarea vulnerabilităților din rețelele bancare.

Carbanak: Un troian bancar utilizat pentru controlul de la distanță al sistemelor și furtul de date.

Ținte frecvente: Gruparea atacă bănci și companii fintech, cu scopul de a fura fonduri și informații confidențiale.

Metodologie de atac:

Phishing (T1566): E-mailuri phishing sunt folosite pentru a păcăli angajații și a obține acces inițial.

Exploatarea vulnerabilităților software (T1190): Vulnerabilitățile din software-urile bancare sunt exploatate pentru a compromite sistemele interne.

MiTM (Man-in-the-Middle) (T1557): Interceptarea comunicațiilor pentru a fura date critice.

Măsuri de protecție: Implementarea soluțiilor EDR (Endpoint Detection and Response) pentru detectarea și răspunsul rapid la atacuri. Educația angajaților pentru recunoașterea phishing-ului. Monitorizarea traficului de rețea pentru detectarea activităților suspecte, inclusiv a atacurilor MiTM.

2. Volt Typhoon

Scurt istoric: Volt Typhoon este o grupare de hackeri sponsorizată de stat, activă din 2021, și atribuită Chinei. Gruparea este cunoscută pentru activitățile sale de spionaj cibernetic, vizând infrastructura critică din SUA și alte țări occidentale, în special în domeniile energetic și telecomunicații.

Instrumente utilizate: Utilizare preponderentă a instrumentelor personalizate și a tehnicilor living off the land (LOLbins) pentru a folosi comenzi legitime din sistem, evitând astfel detectarea.

PowerShell (T1059.001) și WMI (T1047): Utilizarea acestor instrumente native pentru a executa comenzi fără a ridica suspiciuni.

Ținte frecvente: Gruparea vizează sistemele energetice și companiile de telecomunicații din SUA, cu scopul de a culege informații sensibile și de a monitoriza activitățile infrastructurii critice.

Metodologie de atac: Living off the Land (T1105): Folosirea unor comenzi și scripturi legitime din sistemele vizate pentru a evita detectarea. Exfiltrarea datelor prin criptare (T1022): Datele sunt extrase și criptate pentru a împiedica detectarea atacului.Furt de date de autentificare (T1555): Gruparea capturează datele de autentificare pentru a accesa și compromite infrastructura vizată.

Măsuri de protecție: Limitarea utilizării PowerShell și WMI și monitorizarea activităților acestora.

Implementarea autentificării multi-factor (MFA) pentru protejarea conturilor.

Segmentarea rețelei și monitorizarea comportamentului anormal în rețelele critice.

3. DarkSide

Scurt istoric: DarkSide este o grupare de ransomware activă din 2020, cunoscută mai ales pentru atacul asupra Colonial Pipeline din SUA, care a avut un impact major asupra infrastructurii energetice. Gruparea funcționează ca un serviciu de ransomware-as-a-service (RaaS), oferind software de ransomware altor grupuri criminale.

Instrumente utilizate: Ransomware DarkSide (T1486): Software de ransomware care criptează datele victimelor și extrage informații pentru a forța plata răscumpărărilor.

Ținte frecvente: Gruparea vizează companii energetice, instituții din sănătate și alte sectoare critice, în special din America de Nord.

Metodologie de atac: Exploatarea vulnerabilităților IT (T1190): Gruparea exploatează vulnerabilitățile din infrastructura IT pentru a obține acces inițial la rețele. Phishing (T1566): E-mailurile de phishing sunt utilizate pentru a păcăli angajații și a compromite sistemele vizate. Exfiltrarea datelor (T1020): Datele sunt extrase din sistemele compromise înainte de a fi criptate pentru a șantaja victimele cu dublu risc (furt de date și criptare).

Măsuri de protecție: Backup regulat al datelor pentru a preveni pierderea acestora în cazul unui atac de ransomware. Aplicarea constantă a actualizărilor de securitate pentru a închide vulnerabilitățile exploatabile. Implementarea autentificării multi-factor (MFA) pentru a proteja accesul la conturi și sisteme critice.