CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

Les principales menaces en 2022 (et 2023)

Philippe.Bourgeois@cert-ist.com

www.cert-ist.com

CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

Plan

- Les menaces 2021 se poursuivent en 2022
- De nouvelles tendances marquent l'année 2022
  - Des états plus agressifs
  - Les attaques visant l'identité
  - La montée en puissance des attaques SCADA

Des menaces toujours présentes

Ce que l'on a observé en 2021 s'est poursuivi en 2022, en particulier :

- Ransomware et chantages à la fuite de données
  - De multiples attaques observées (Lockbit, etc.)
  - Le Conti-leak a montré l'envers de cette industrie
- Attaques via la Supply-chain
  - Beaucoup de cas de compromissions de librairies logicielles (ex. sur le dépôt NPM)
  - L'incident OKTA / Lapsus$ (janvier 22) est un exemple d'attaque via la sous-traitance

2022 : Des états plus agressifs (1/2)

- Le cyber dans la guerre RU-UA
  - Difficile de mesurer l'importance réelle du Cyber
    - Pas de cyber-Armageddon
    - Mais beaucoup d'actions de cyber-sabotage (Wiper) et d'influence (fake news)
  - La guerre rend possible des scénarios improbables (cyber-sabotage d'infrastructures critiques)
- Les USA annoncent faire du « Hunt-Forward » pour devancer l'éventualité d'un cyber-incident
  - Envoi d'équipes de défense là où une attaque cyber pourrait se produire
  - Rumeur : les USA auraient volé des outils d'attaques SCADA avant qu'ils ne soient utilisés (Dreampipe)

2022 : Des états plus agressifs (2/2)

- Le cyber est utilisé comme une « force douce » contre les pays rivaux
  - Iran vs Israël (attaques de « wipers »)
  - Chine vs pays concurrents (soupçons d'attaques 0-days)
  - Corée du nord contre l'embargo
- Le cyber est utilisé comme un outil d'oppression contre les opposants
  - Ex. 4 pays européens ont utilisés des spywares de type Pegasus contre des journalistes ou des opposants
    (cf. le comité PEGA créé par la commission européenne)

2022 : Les attaques visant l'identité (1/3)

- Les intrusions au moyen de comptes volés se multiplient
  - Historiquement :
    - Attaques en force brute sur des mots de passe faible (SSH, RDP)
    - Phishing et vol de base de données utilisateurs
    - Password stuffing : rejouer les mots de passe déjà volés sur de nouveaux accès
  - En 2022, le marché des Info-Stealers a explosé
    - + 80% = nombre de mots de passe volés en 7 mois en 2022 par rapport au 10 derniers mois de 2021 (rapport Group-IB)
- Info-Stealer - Botshop/Logshop - Initial Access Brokers (IAB)
  - Info-Stealer : Racoon, Redline, etc. :
    - Infectent des ordinateurs et volent un ensemble de données (un LOG) : password, cookie, données techniques (CPU, RAM, etc)
  - Bot-shop : Genesis, Russian Market, 2Easy et Amigos
    - Vendent les LOG collectés par les Info-Stealers

2022 : Les attaques visant l'identité (2/3)

- Certains attaquants sont des chasseurs de mots de passes
  - Voler des identifiants et mots de passe demandent des compétences spécifiques
    - Connaissance des fournisseurs d'identités (ex. OKTA)
    - De d'ingénierie sociale et de la technique (ex. contacter la victime via WhatsApp)

Exemple : Incident OKTA / Twillio en août 2022

- Incident baptisé Oktapus par Groupe-IB et Scatterwine par Okta
- Phishing SMS OKTA -> Intrusion chez Twilio -> vol des comptes MailChimp -> Intrusion chez Digital Ocean

2022 : Les attaques visant l'identité (3/3)

- Les attaques contre les MFA se multiplient
  - SIM swap (2016 / 2018) via des attaques visant les opérateurs Telco (Engineeering Social ou Insider)
  - Phishing MFA (décembre 2018) au moyen d'outils MiTM comme Modlishka (2019) ou EvilProxy (2022)
  - Pass-the-cookie (2022) en utilisant les cookies volés par les Info-Stealers
  - MFA fatigue (2022) en submergeant l'utilisateur de Push-notifications MFA (attaque Uber septembre 2022)
- Rappel : depuis fin 2020 (SolarWind) les attaquants avancés visent les systèmes SSO
  - SolarWind (2020) : l'authentification Azure et Microsoft 365 (attaques Golden SAML).
  - ADCS (2021) : Attaque de la PKI de Microsoft

2022 : La montée en puissance des attaques SCADA (1/2)

- Toolkit d'attaque PIPEDREAM (Dragos) / INCONTROLLER (Mandiant).
  - Annoncé en avril 2022 par la CISA, Dragos et Mandiant
  - Malware SCADA dans la lignée de Stuxnet (2010), Industroyer (2016) et TRITON (2017).
  - Pourrait être un malware volé au laboratoire russe (le TsNIIKhM) supposé avoir mis au point TRITON
- Selon Dragos, Pipedream a des fonctions avancées
  - Toolkit modulaire
  - Connait les protocoles industriels : OPC-UA, CoDeSys, Modbus
  - Bypasse les firewall (par ex. en utilisant des requêtes CoDeSys pour identifier les PLC présents)
  - Assemblé pour une attaque Omron et Schneider visant la production de gaz liquéfié

2022 : La montée en puissance des attaques SCADA (2/2)

- Dragos recommande (en autres)
  - De créer des équipes de réponse sur incident capables de remplacer les équipements attaqués
  - Surveiller le trafic réseau pour détecter les anomalies

Et 2023 ? (1/2)

- La poursuite des tendances 2022 (les chantiers de fond)
  - Ransomware & Data extorsion
  - Attaques Supply-chain
  - La sécurisation des environnements SCADA
- Des évolutions à plus long termes difficiles à anticiper
  - La guerre RU-UA va sans doute faire évoluer les pratiques cyber
  - L'internet semble se segmenter en blocs : Chine, Russie, Autres

Et 2023 ? (2/2)

- Il faut continuer à protéger les identités
  - Lutter contre les Info-Stealers
    - Mettre en garde contre les mauvaise pratiques (téléchargement de logiciels et mots de passe stockés dans les navigateurs web)
    - Renforcer la détection, et peut-être faire du « Hunt Forward »
  - Continuer à déployer des solutions de MFA
  - Attention à ne pas faire du ZeroTrust baclé…
    - La tendance ZTA est de donner accès à tout partout (dé-périmétrisation)
    - Cela est OK pour des solutions conçues ZTA
    - Mais dangereux sur des applications « legacy » si le ZTA est mis en place « parce qu'il le faut »
- Maintenir à jour les systèmes

CERT-IST
INDUSTRIE | SERVICES | TERTIAIRE

Merci