דוח מספר 6

מגיש – דור לבקוביץ 203565015

שם התרחיש – Infected device

תהליך ההתקפה – בדיעבד הסתבר שעובד בחברה הכניס דיסק נגוע. לאחר בירור מעמיק גילינו שבדיסק הנגוע יש קובץ שמופעל באופן אוטומטי (AUTORUN) שיוצר BACKDOOR לבן אדם שמפעיל סקריפט שישלח קבצים זדוניים לשאר העובדים בארגון. ההאקר בעצם עשה PING SWEEP שבעצם נתן לו אופציה לדעת אילו מחשבים מחוברים לרשת וכמה.

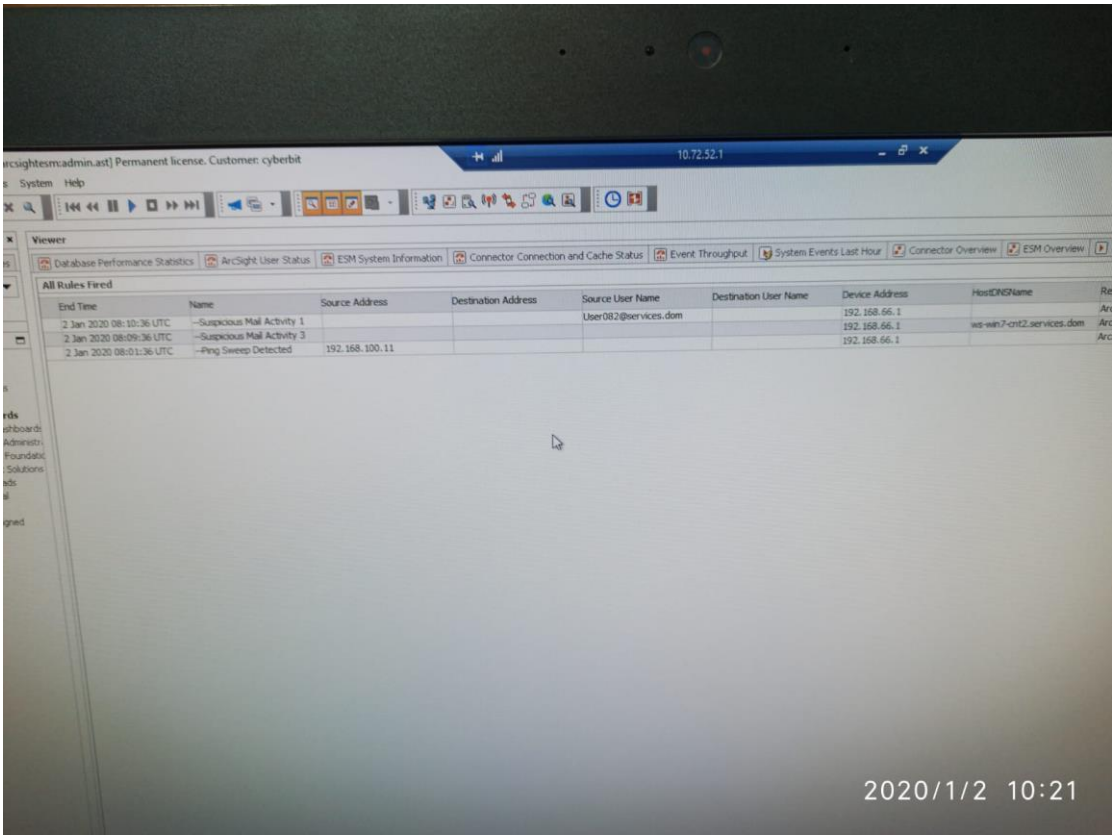
בעזרת ה- BACKDOOR שהוא יצר הוא יכל לחפש מידע רגיש כמו סיסמאות ומיילים לדוגמה.

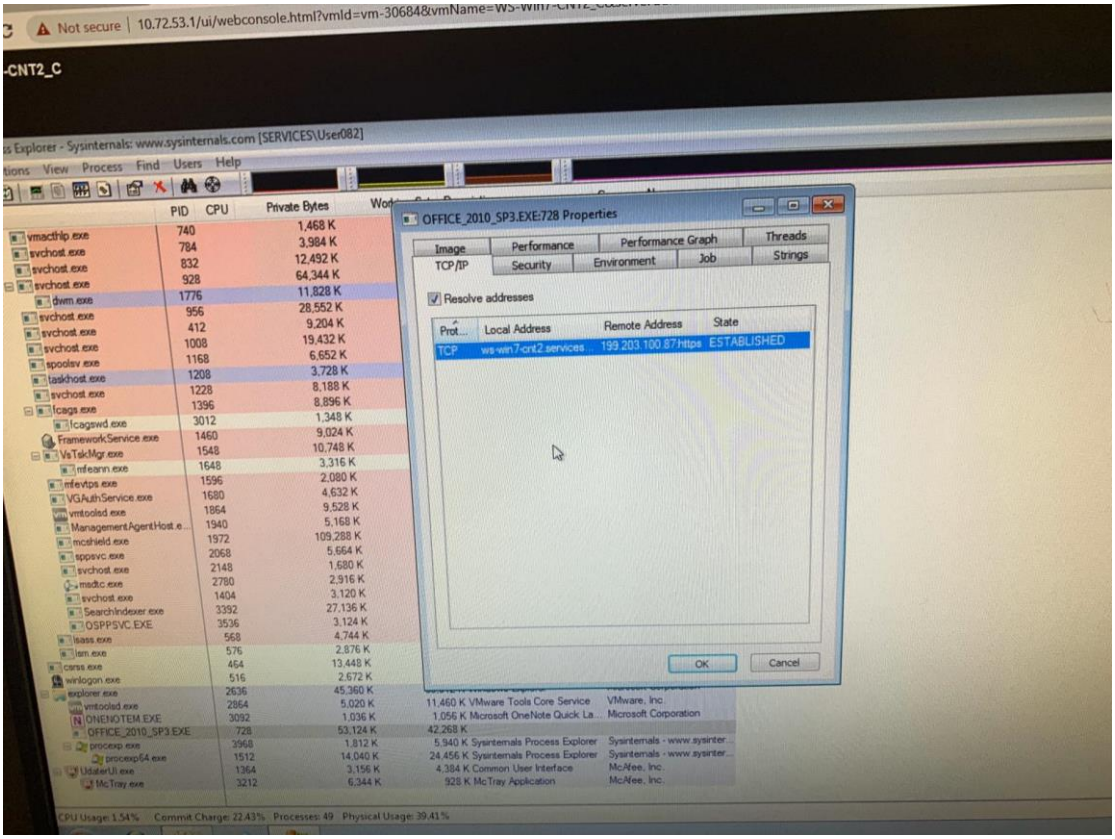
תהליך הזיהוי – התקבלה התרעה על בדיקת פינגים באמצעות ה- ARKSIGHT ולאחר זמן קצר גם מיילים חשודים שיוצאים. לאחר בדיקה מעמיקה נמצא שמישהו מהעובדים הכניס דיסק שהסתבר כנגוע. מבדיקה בפרוססים הצלחנו לעלות ה- BACKDOOR שנוצר עקב הקובץ האוטומטי שרץ ע"י הדיסק.

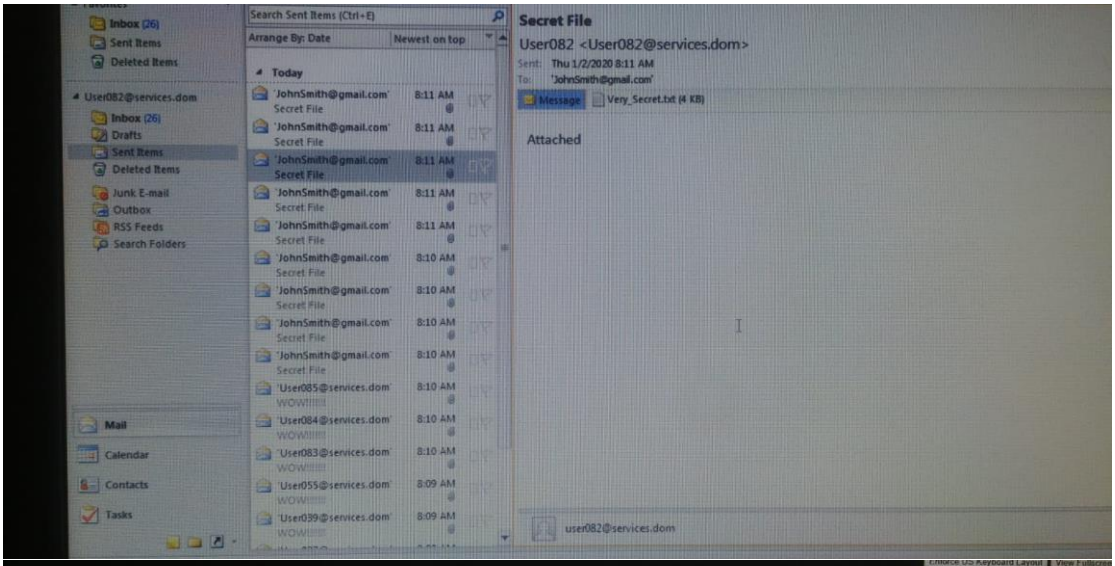
תהליך הגנה ראשוני – התחברות לשרת המיילים לאחר ההתראה על המיילים ולראות את המיילים החשודים ולמה זה מתריע. לבדוק מאיפה נוצר ה-BACKDOOR ולנסות לחסום אותו ואז לברר מה הנזק שנגרם.

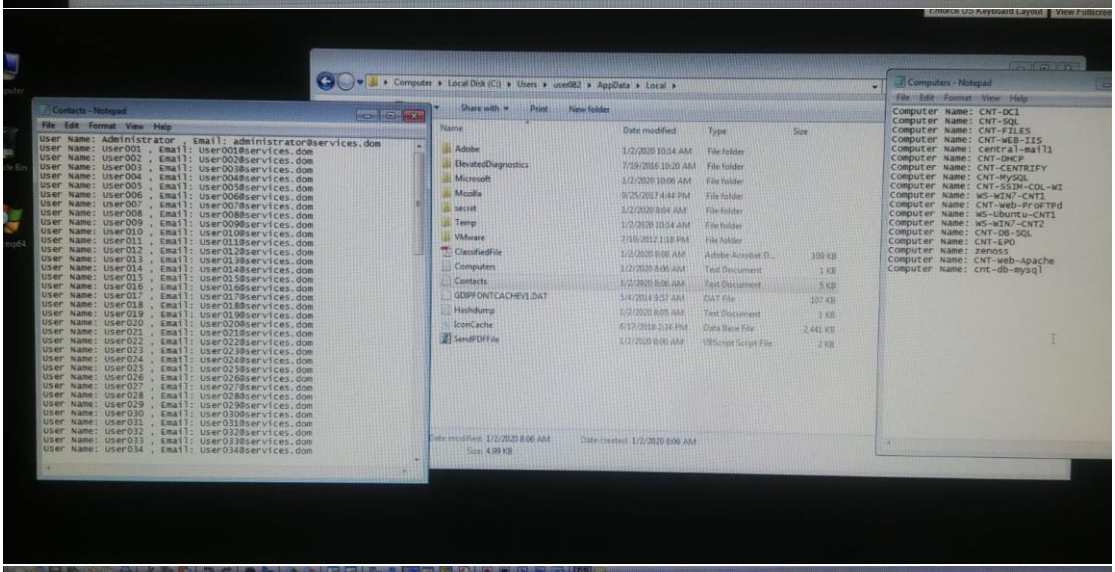
תהליך הגנה מונעת- לחדד נהלים מול העובדים ולאסור על הכנסת חומרה חוץ אירגונית ולחברה למחשבים בארגון במיוחד שמדובר על מחשבים רגישים. לחסום גישה ממחשבים בין המחשבים על מנת שלא יהיה אפשרות לגנוב מידע רגיש.

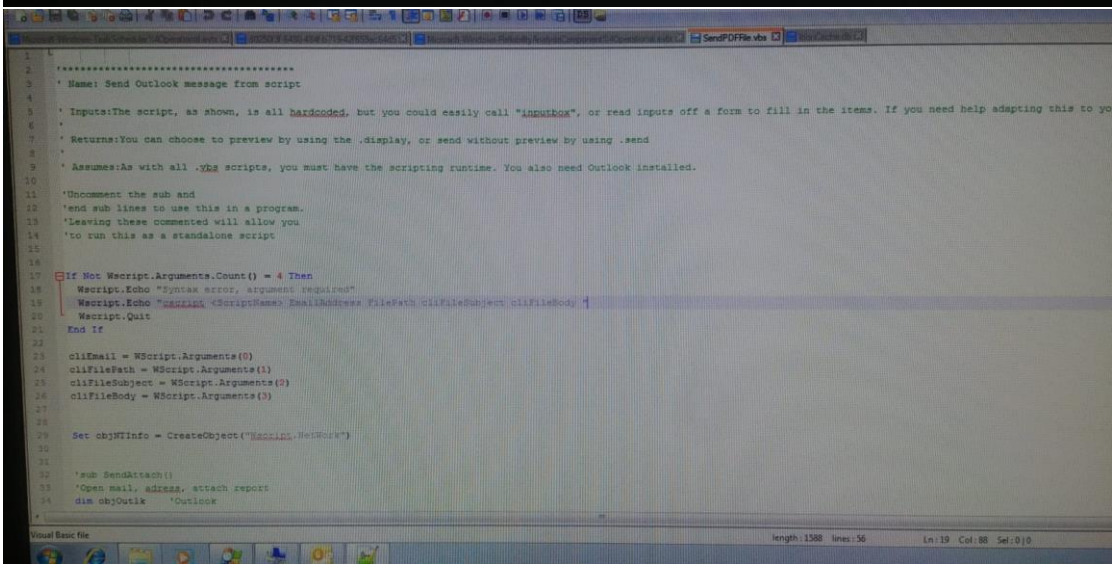
כלים חדשים שהשתמשתם – PROCEXP.


10.72.52.1
System Help
Viewer
Database Performance Statistics
ArcSight User Status
ESM System Information
Connector Connection and Cache Status
Event Throughput
System Events Last Hour
Connector Overview
ESM Overview
All Rules Fired
End Time
Name
Source Address
Destination Address
Source User Name
Destination User Name
Device Address
HostDNSName
2 Jan 2020 08:10:36 UTC
Suspicious Mail Activity 1
User082@services.dom
192.168.66.1
2 Jan 2020 08:09:36 UTC
Suspicious Mail Activity 3
192.168.66.1
ws-win7-cnt2.services.dom
2 Jan 2020 08:01:36 UTC
Ping Sweep Detected
192.168.100.11
192.168.66.1
2020/1/2 10:21


Not secure
10.72.53.1/ui/webconsole.html?vmId=vm-30684&vmName=WS-WIN7-CNT2_C
-CNT2_C
Explorer - Sysinternals: www.sysinternals.com [SERVICES\User082]
View Process Find Users Help
PID CPU Private Bytes
OFFICE_2010_SP3.EXE:728 Properties
Image Performance Performance Graph Threads
TCP/IP Security Environment Job Strings
Resolve addresses
Prot... Local Address Remote Address State
TCP ws-win7-cnt2.services... 199.203.100.87:https ESTABLISHED
OK Cancel


Inbox (26)
Sent Items
Deleted Items
User082@services.dom
Inbox (26)
Drafts
Sent Items
Deleted Items
Junk E-mail
Outbox
RSS Feeds
Search Folders
Mail
Calendar
Contacts
Tasks
Search Sent Items (Ctrl+E)
Arrange By: Date
Newest on top
Today
'JohnSmith@gmail.com' Secret File 8:11 AM
'JohnSmith@gmail.com' Secret File 8:11 AM
'JohnSmith@gmail.com' Secret File 8:11 AM
'JohnSmith@gmail.com' Secret File 8:11 AM
'JohnSmith@gmail.com' Secret File 8:11 AM
'JohnSmith@gmail.com' Secret File 8:10 AM
'JohnSmith@gmail.com' Secret File 8:10 AM
'JohnSmith@gmail.com' Secret File 8:10 AM
'JohnSmith@gmail.com' Secret File 8:10 AM
'User085@services.dom' WOW!!!!!! 8:10 AM
'User084@services.dom' WOW!!!!!! 8:10 AM
'User083@services.dom' WOW!!!!!! 8:10 AM
'User055@services.dom' WOW!!!!!! 8:09 AM
'User039@services.dom' WOW!!!!!! 8:09 AM
Secret File
User082 <User082@services.dom>
Sent: Thu 1/2/2020 8:11 AM
To: 'JohnSmith@gmail.com'
Message
Very_Secret.txt (4 KB)
Attached
user082@services.dom


Contacts - Notepad
File Edit Format View Help
User Name: Administrator , Email: administrator@services.dom
User Name: User001 , Email: User001@services.dom
User Name: User002 , Email: User002@services.dom
User Name: User003 , Email: User003@services.dom
User Name: User004 , Email: User004@services.dom
User Name: User005 , Email: User005@services.dom
User Name: User006 , Email: User006@services.dom
User Name: User007 , Email: User007@services.dom
User Name: User008 , Email: User008@services.dom
User Name: User009 , Email: User009@services.dom
User Name: User010 , Email: User010@services.dom
User Name: User011 , Email: User011@services.dom
User Name: User012 , Email: User012@services.dom
User Name: User013 , Email: User013@services.dom
User Name: User014 , Email: User014@services.dom
User Name: User015 , Email: User015@services.dom
User Name: User016 , Email: User016@services.dom
User Name: User017 , Email: User017@services.dom
User Name: User018 , Email: User018@services.dom
User Name: User019 , Email: User019@services.dom
User Name: User020 , Email: User020@services.dom
User Name: User021 , Email: User021@services.dom
User Name: User022 , Email: User022@services.dom
User Name: User023 , Email: User023@services.dom
User Name: User024 , Email: User024@services.dom
User Name: User025 , Email: User025@services.dom
User Name: User026 , Email: User026@services.dom
User Name: User027 , Email: User027@services.dom
User Name: User028 , Email: User028@services.dom
User Name: User029 , Email: User029@services.dom
User Name: User030 , Email: User030@services.dom
User Name: User031 , Email: User031@services.dom
User Name: User032 , Email: User032@services.dom
User Name: User033 , Email: User033@services.dom
User Name: User034 , Email: User034@services.dom
Computer ▸ Local Disk (C:) ▸ Users ▸ user082 ▸ AppData ▸ Local ▸
Share with
Print
New folder
Name
Date modified
Type
Size
Adobe
ElevatedDiagnostics
Microsoft
Mozilla
secret
Temp
VMware
ClassifiedFile
Computers
Contacts
QBPFONTCACHEV1.DAT
Hashdump
IconCache
SendPDFFile
Computers - Notepad
File Edit Format View Help
Computer Name: CNT-DC1
Computer Name: CNT-SQL
Computer Name: CNT-FILES
Computer Name: CNT-WEB-IIS
Computer Name: central-mail1
Computer Name: CNT-DHCP
Computer Name: CNT-CENTRIFY
Computer Name: CNT-MySQL
Computer Name: CNT-SSIM-COL-WI
Computer Name: WS-WIN7-CNT1
Computer Name: CNT-web-PrOFTPd
Computer Name: WS-Ubuntu-CNT1
Computer Name: WS-WIN7-CNT2
Computer Name: CNT-DB-SQL
Computer Name: CNT-EPO
Computer Name: zenoss
Computer Name: CNT-web-Apache
Computer Name: cnt-db-mysql


SendPDFFile.vbs
'***
' Name: Send Outlook message from script
' Inputs:The script, as shown, is all hardcoded, but you could easily call "inputbox", or read inputs off a form to fill in the items. If you need help adapting this to yo
' Returns:You can choose to preview by using the .display, or send without preview by using .send
' Assumes:As with all .vbs scripts, you must have the scripting runtime. You also need Outlook installed.
'Uncomment the sub and
'end sub lines to use this in a program.
'Leaving these commented will allow you
'to run this as a standalone script
If Not Wscript.Arguments.Count() = 4 Then
Wscript.Echo "Syntax error, argument required"
Wscript.Echo "wscript <ScriptName> EmailAddress FilePath cliFileSubject cliFileBody "
Wscript.Quit
End If
cliEmail = WScript.Arguments(0)
cliFilePath = WScript.Arguments(1)
cliFileSubject = WScript.Arguments(2)
cliFileBody = WScript.Arguments(3)
Set objNTInfo = CreateObject("Wscript.NetWork")
'sub SendAttach()
'Open mail, adress, attach report
dim objOutlk 'Outlook
Visual Basic file
length : 1588 lines : 56
Ln : 19 Col : 88 Sel : 0 | 0