DarkSide Ransomware With Self-Propagating Feature in AD Environments

By ATCP

Published: 2023-02-06 · Archived: 2026-04-05 23:36:45 UTC

In order to evade analysis and sandbox detection, DarkSide ransomware only operates when the loader and data file are both present. The loader with the name “msupdate64.exe” reads the “config.ini” data file within the same path that contains the encoded ransomware and runs the ransomware on the memory area of a normal process. The ransomware is structured to only operate when a specific argument matches. It will then register itself to the task scheduler and run itself periodically.

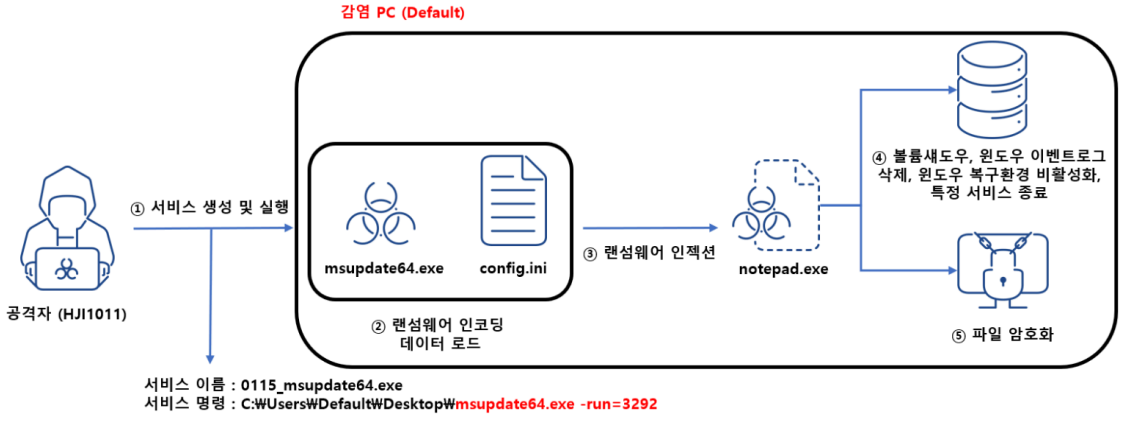

Figure 1. Ransomware operation method

The following are the features of DarkSide ransomware.

1) Ransomware Encryption Target Exception List

After being injected into a normal process, the ransomware encrypts all files aside from those with certain folder and file names. Table 1 and 2 contains the folder paths and filenames excluded from the encryption.

Folder Paths Excluded From Encryption
“AppData”
“Boot”
“Windows”
“WINDOWS”
“Windows.old”
“Ahnlab”
“Tor Browser”
“Internet Explorer”
“Google”
“Opera”
“Opera Software”
“Mozilla”
“Mozilla Firefox”
“$Recycle.Bin”
“ProgramData”
“All Users”
“Program Files”
“Program Files (x86)”
“#recycle”
“..”
“.”
“SYSVOL”
“bootmgr”
“ntldr”

Table 1. List of folder paths excluded from encryption

Filenames Excluded From Encryption
“autorun.inf”
“boot.ini”
“bootfont.bin”
“bootsect.bak”
“bootmgr.efi”
“bootmgfw.efi”

“desktop.ini”
“iconcache.db”
“ntuser.dat”
“ntuser.dat.log”
“ntuser.ini”
“thumbs.db”
“AUTOEXEC.BAT”
“autoexec.bat”
“bootfont.bin”
“bootfont.bin”
“ntldr”
“config.ini”
“begin.txt”
“finish.txt”

Table 2. List of filenames excluded from encryption

2) Force Terminate Running Processes

The ransomware terminates running processes in order to prevent file-handling conflicts during the encryption process. The following is a list of those targets.

Force Terminated Processes
“sql.exe”
“oracle.exe”
“ocssd.exe”
“dbsnmp.exe”
“synctime.exe”
“agntsvc.exe”
“isqlplussvc.exe”
“xfssvccon.exe”
“mydesktopservice.exe”
“ocautoupds.exe”
“encsvc.exe”
“firefox.exe”
“tbirdconfig.exe”
“mydesktopqos.exe”
“ocomm.exe”
“dbeng50.exe”
“sqbcoreservice.exe”
“excel.exe”
“infopath.exe”
“msaccess.exe”
“mspub.exe”

“onenote.exe”
“outlook.exe”
“powerpnt.exe”
“steam.exe”
“thebat.exe”
“thunderbird.exe”
“visio.exe”
“winword.exe”
“wordpad.exe”
“wrapper.exe”
“dbsrv12.exe”
“WinSAT.exe”

Table 3. List of processes to be force terminated

3) Service Termination Targets

The ransomware closes backups and services related to AV products. Table 4 is a list of such targets.

Terminated Services
vss
sql
svc$
memtas
mepocs
sophos
backup
GxCIMgr
DefWatch
ccEvtMgr
ccSetMgr
SavRoam
RTVscan
QBFCService
QBIDPService
Intuit.QuickBooks.FCS
QBCFMonitorService
YooBackup
zhudongfangyu
stc_raw_agent
VSNAPVSS
VeeamTransportSvc
VeeamDeploymentService
VeeamNFSSvc

PDVFSService BackupExecVSSProvider BackupExecAgentAccelerator BackupExecAgentBrowser BackupExecDiveciMediaService BackupExecJobEngine BackupExecManagementService BackupExecRPCService AcrSch2Svc AcronisAgent CASAD2DWebSvc CAARCUpdateSvc

Table 4. List of services to be terminated

4) Delete Volume Shadows, Suspend Windows Event Logging, and Deactivate Windows Recovery

The threat actor uses tools such as vssadmin.exe to perform acts like deleting volume shadow copies, but they manage to bypass command line-based behavior detection by using the following method.
Each process is run in SUSPEND mode, but garbage values like “11111111” are given as command line arguments. Afterward, the address of the command line is obtained by reading the PEB from the corresponding process memory and finding the RTL_USER_PROCESS_PARAMETERS struct.
Finally, by using WriteProcessMemory() to rewrite the actual command line argument in the obtained address, tools like vssadmin.exe can perform normally by using the newly transmitted argument.

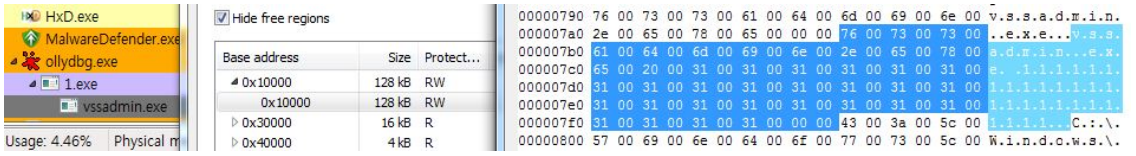

Figure 2. Original command line

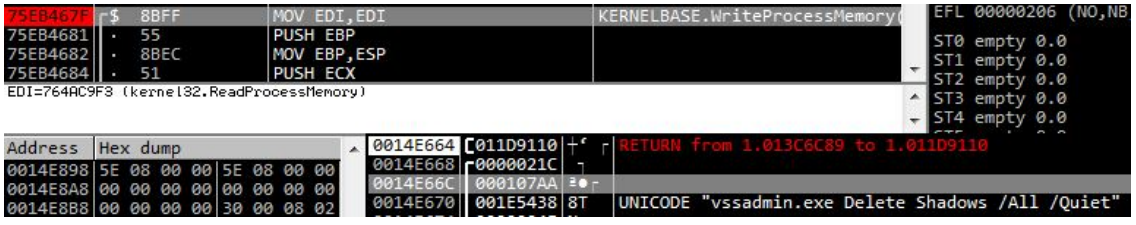

Figure 3. Command line argument being changed

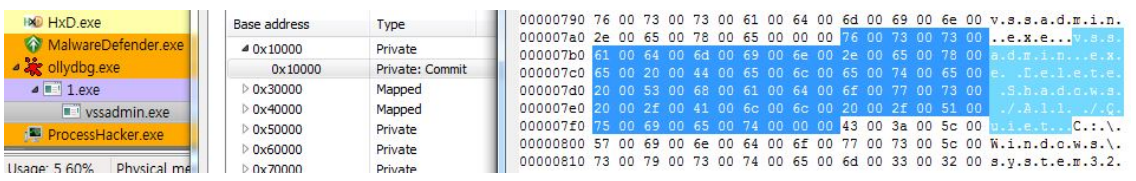

Figure 4. Changed command line argument

Process Execution Log	Actual Command Line

vssadmin.exe 111111111111111111111111	vssadmin.exe Delete Shadows /All /Quiet
bcdedit.exe 11111111111111111111111111111111	bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe 1111111111111111111111111111111111111111111111111	bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin.exe 11111111111111111111	wbadmin.exe DELETE SYSTEMSTATEBACKUP
wbadmin.exe 1111111111111111111111111111111111111	wbadmin.exe DELETE SYSTEMSTATEBACKUP -deleteOldest
wbadmin.exe 11111111111111111	wbadmin.exe delete catalog -quiet
wbadmin.exe 1111111111111	wbadmin.exe delete backup
wbadmin.exe 1111111111111111111111111111111111111111	wbadmin.exe delete systemstatebackup -keepversions:0
wevtutil.exe 11111111111111111111	wevtutil.exe clear-log Application
wevtutil.exe 1111111111111111	wevtutil.exe clear-log Security
wevtutil.exe 111111111111111	wevtutil.exe clear-log System
wevtutil.exe 1111111111111111111111111111	wevtutil.exe clear-log “windows powershell”
wmic.exe 111111111111111111111111	wmic.exe SHADOWCOPY /nointeractive
net.exe 1111111111	net.exe stop MSDTC
net.exe 1111111111111111111	net.exe stop SQLSERVERAGENT
net.exe 111111111111111	net.exe stop MSSQLSERVER
net.exe 11111111	net.exe stop stop vds
net.exe 11111111111111	net.exe stop SQLWriter

net.exe 111111111111111	net.exe stop SQLBrowser
net.exe 1111111111111111	net.exe stop MSSQLSERVER
net.exe 1111111111111111111	net.exe stop MSSQL$CONTOSO1
netsh.exe 11111111111111111111111111111111111111111	netsh.exe advfirewall set currentprofile state off
netsh.exe 111111111111111111111111111111111	netsh.exe firewall set opmode mode=disable

Table 5. Actually executed command lines

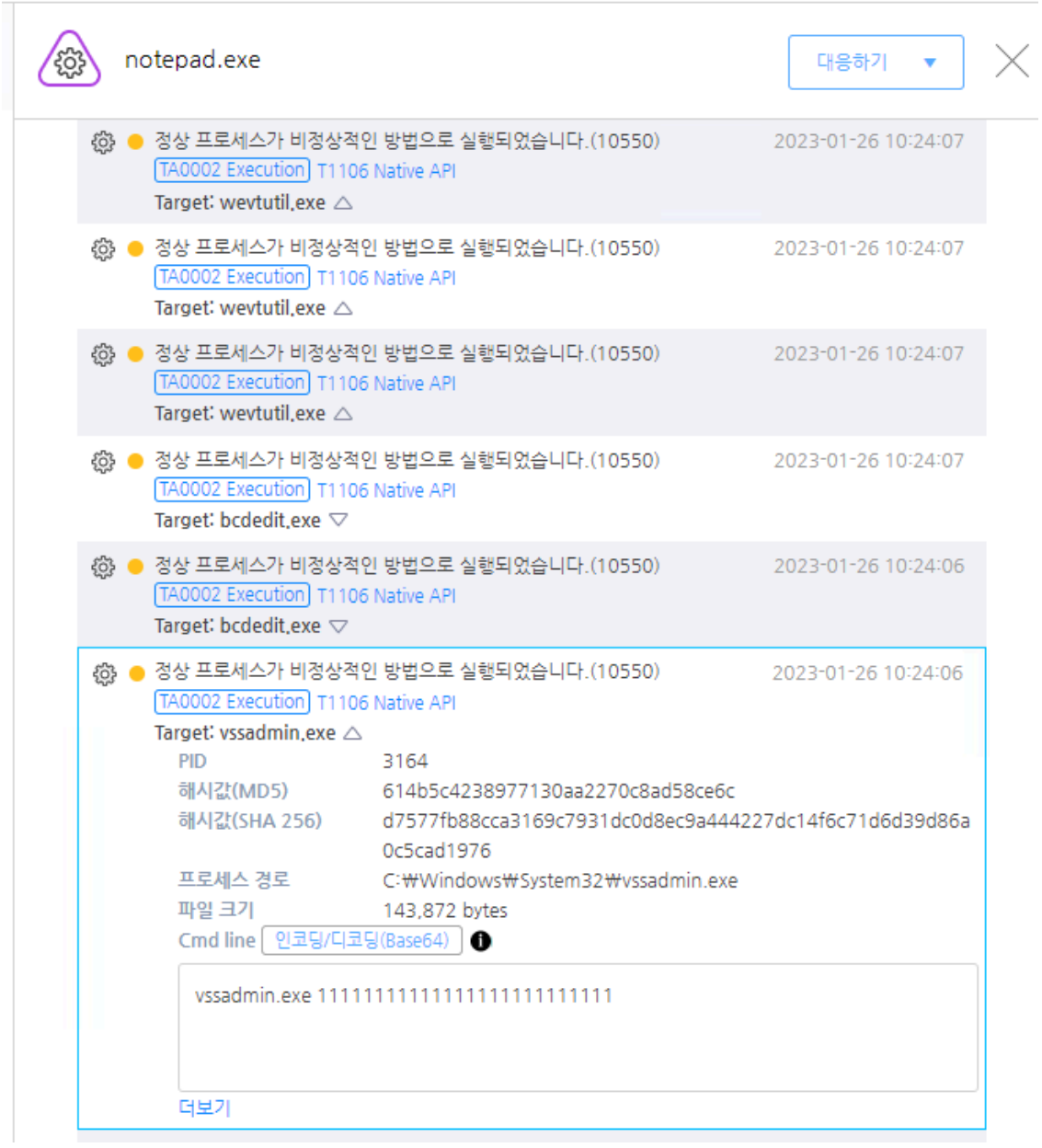

Figure 5. AhnLab EDR detecting abnormal process executions from Table 5

Figure 6. AhnLab MDS detecting execution and data written in memories

The AhnLab EDR/MDS line of products considers executions like the ones above as abnormal executions. MDS products can also check the data that's written on target process memories.

Written data
76 00 73 00 73 00 61 00 64 00 6d 00 69 00 6e 00 2e 00 65 00 78 00 65 00 20 00 44 00 65 00 6c 00 65 00 74 00 65 00 20 00 53 00 68 00 61 00 64 00 6f 00 77 00 73 00 20 00 2f 00 41 00 6c 00 6c 00 20 00 2f 00 51 00 75 00 69 00 65 00 74 00
What command the above data means
vssadmin.exe Delete Shadows /All /Quiet

Table 6. Command written in the memory

5) Ransom Note and File Encryption Extension

The ransomware generates a ransom note file called "_r_e_a_d_m_e.txt", like the one shown in Figure 7, in each encrypted folder.

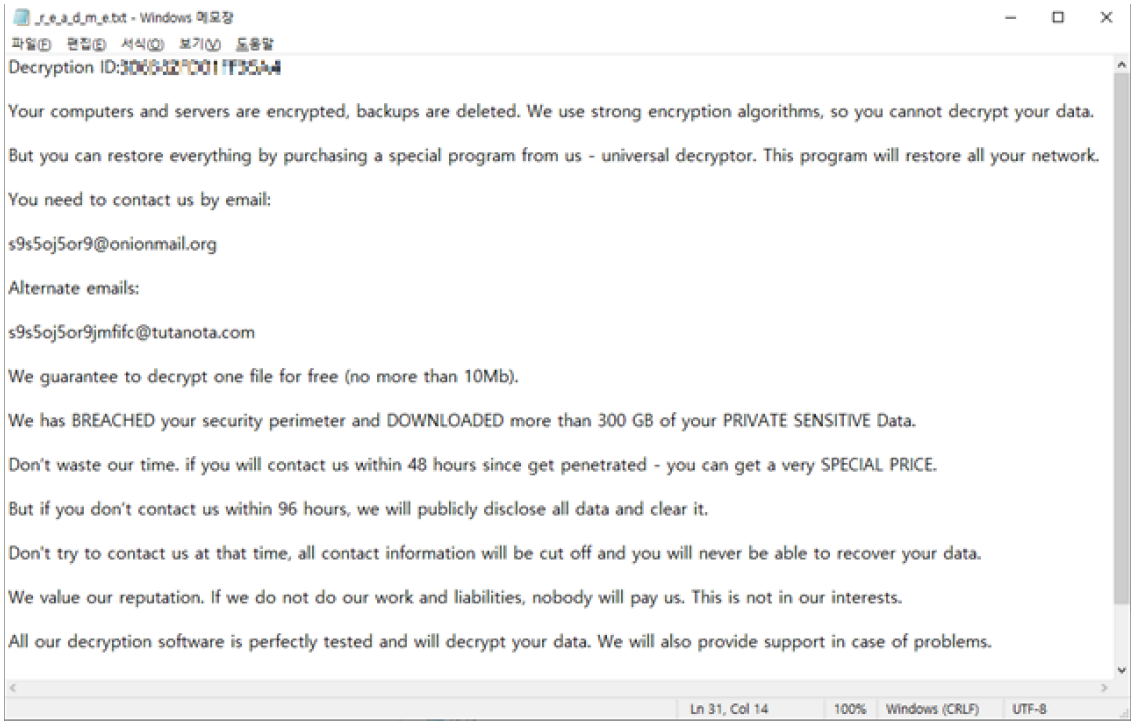

Figure 7. Ransom note

Additionally, the ransomware changes the extension format of encrypted files to ".s1s2s3[number of encrypted files]".

6) Self-deleting Ransomware

After the ransomware finishes its actions, it attempts to delete itself through the following command.

Self-deletion Command
"C:\Windows\System32\cmd.exe" /c ping 127.0.0.1 -n 3 && del /f/q "C:\Users\Default\Desktop\msupdate64.exe"

Table 7. Self-deletion command

Figure 8. AhnLab MDS detecting self-deletion command

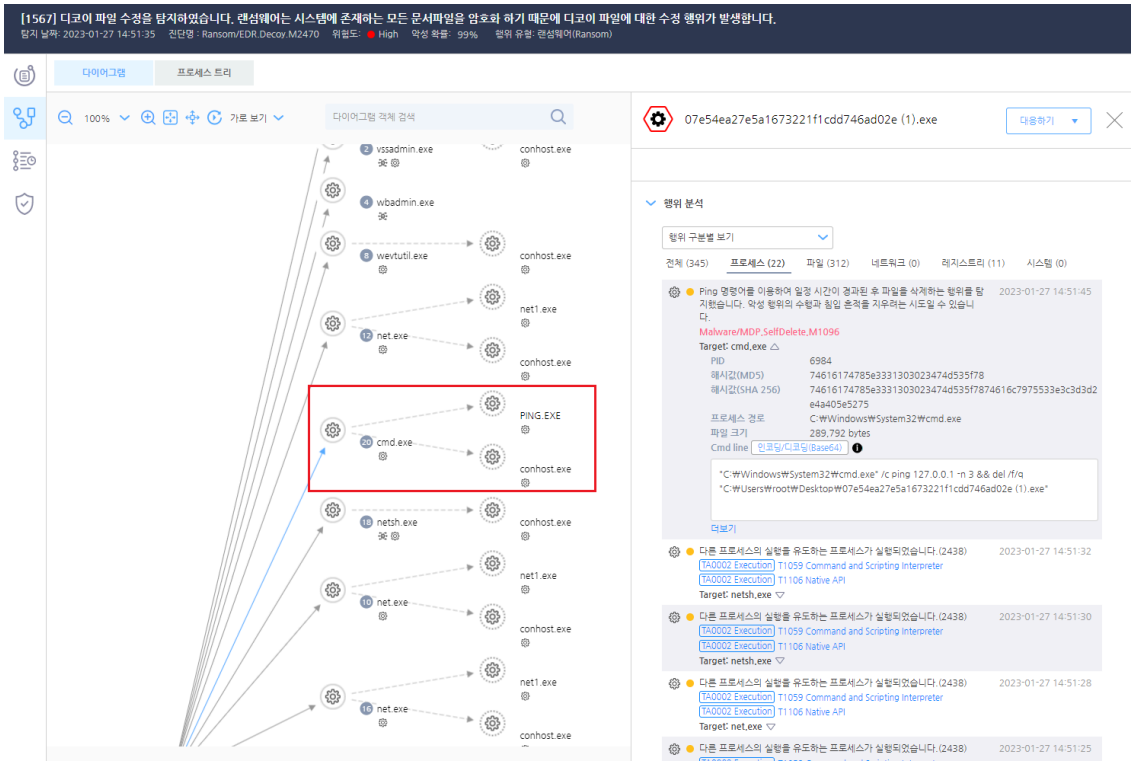

Figure 9. AhnLab EDR detecting self-deletion command

Internal Propagation (Ransomware Distribution Method Through Domain Controller)

When this ransomware becomes active on the domain controller of an AD server, it creates a group policy as shown in Figure 9 to distribute the ransomware to other PCs linked to the current domain.

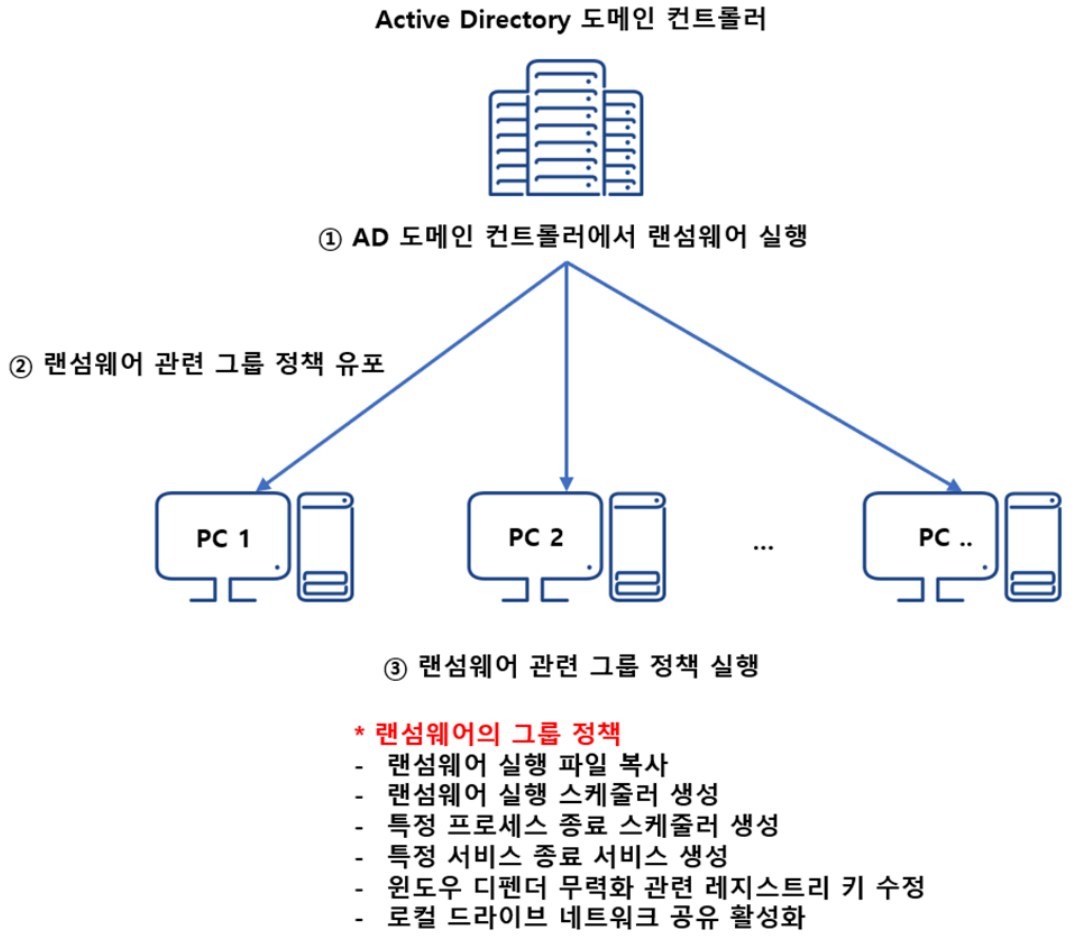

Figure 10. Ransomware distribution method through domain controller

Table 8 shows a file-related group policy which gives the command to copy the executable file within the ransomware's domain controller to the desktops of infected PCs with the name format "[Distribution Date]_[Ransomware Filename].exe".

{D6C45CD3-BCB9-4D6C-A16C-FD416DAA1C47}\User\Preferences\Files\Files.xml
<?xml version="1.0" encoding="utf-8"?> <Files clsid="{215B2E53-57CE-475c-80FE-9EEC14635851}"><File clsid="{50BE44C8-567A-4ed1-B1D0-9234FE1F38AF}" name="[Distributed Date]*[Ransomware Filename].exe*" *status="[Distribution Date]*[Ransomware Filename].exe" image="2" changed="*[Distribution Date]*" uid="{1F86D6A8-6640-47D8-A26B-E263CAECE394}" bypassErrors="1">

Table 8. Group policy that generates ransomware executable file

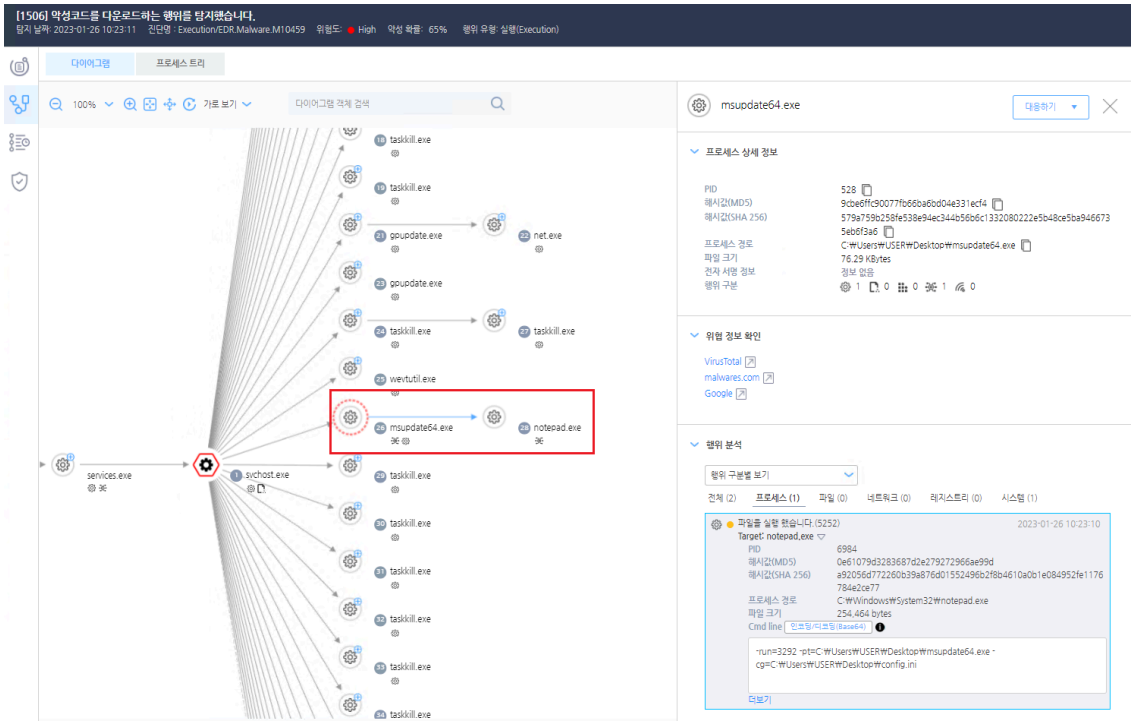

Figure 11. AhnLab EDR detecting the execution of ransomware generated through a group policy

DarkSide will not operate if a certain argument to prevent replication and analysis does not match. However, as shown in Figure 10, AhnLab EDR detects ransomware strains generated through group policies in AD environments. It is also possible to check the arguments at the point of execution.

For continuous propagation, the ransomware distributes group policies with the following command.

PowerShell command
powershell.exe -Command “Get-ADComputer -filter * -Searchbase ‘DC=ahnlabs,DC=com’ | foreach{ Invoke-GPUpdate -computer $_.name -force -RandomDelayInMinutes 0}”

Table 9. Propagation command

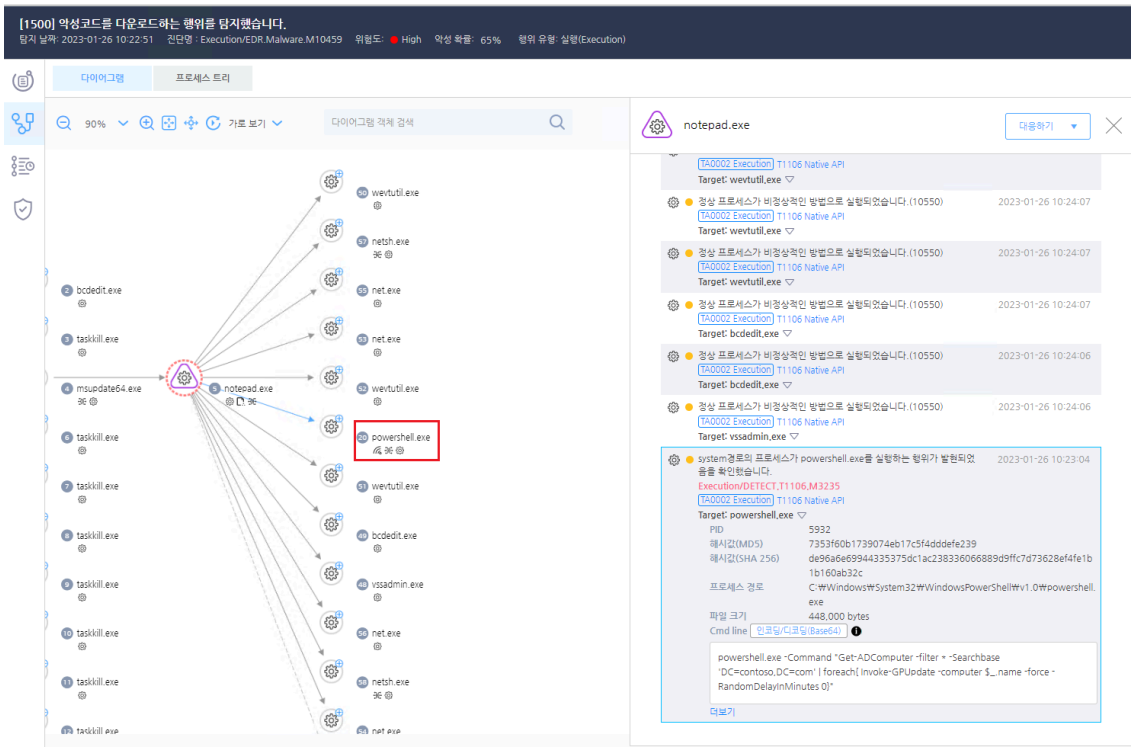

Figure 12. AhnLab EDR detecting the distribution of group policies using PowerShell

The threat actor that performs an ATP attack on the AD environments of companies for monetary gain distributes their malware after checking the detection of all AV products based on existing signatures.

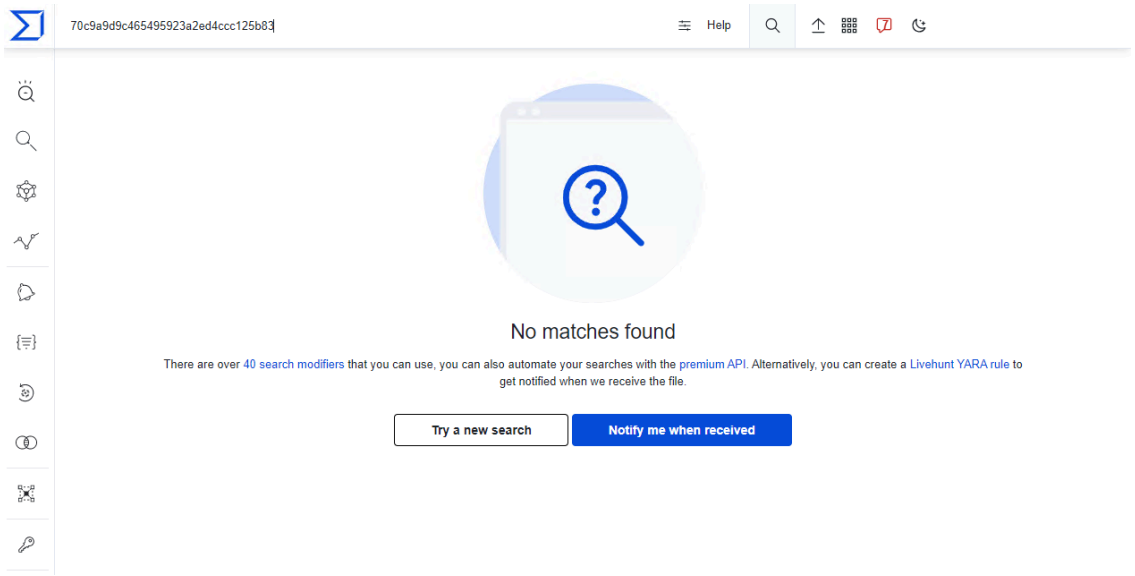

Figure 13. DarkSide ransomware not found by VirusTotal

As shown in the above Figure 13, there is a great chance that DarkSide ransomware can evade being detected by AV products based on existing signatures since it cannot be collected by even VirusTotal.

The importance of an APT detection solution like MDS and EDR, which records and reports all suspicious behaviors in endpoints, becomes clear when it comes to trying to detect this threat effectively.

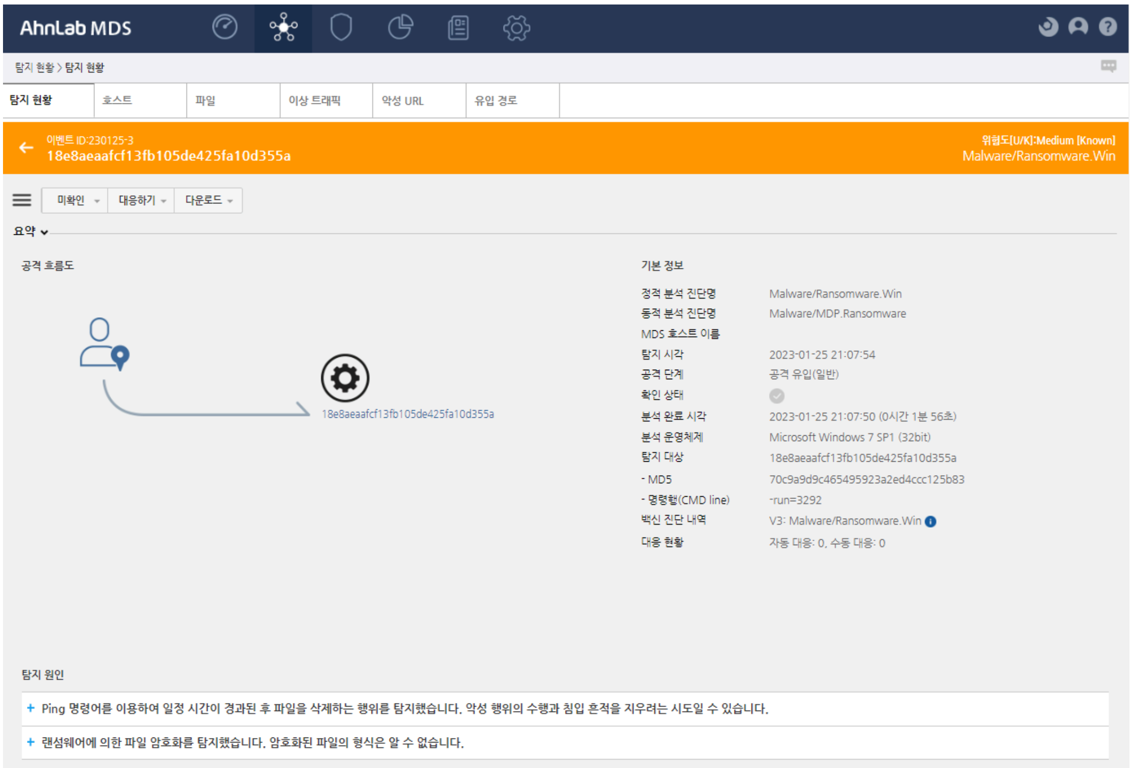

Figure 14. DarkSide ransomware detected on AhnLab MDS

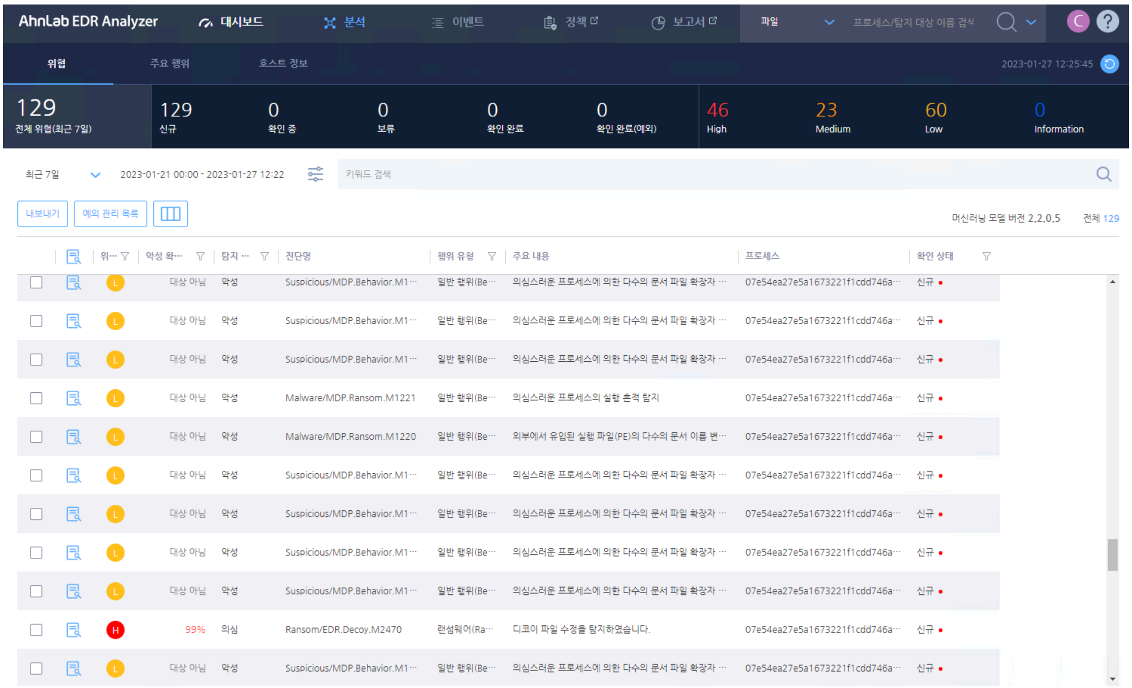

Figure 15. DarkSide ransomware detected on AhnLab EDR

DarkSide ransomware attacks correspond to the following techniques in the MITRE ATT&CK framework.

- T1486 Data Encrypted for Impact[1]
- T1484.001 Domain Policy Modification: Group Policy Modification[2]
- T1053.005 Scheduled Task/Job: Scheduled Task[3]
- T1562.001 Impair Defenses: Disable or Modify Tools or T1489 Service Stop[4]

- T1489 Service Stop[5]
- T1021.002 Remote Services: SMB/Windows Admin Shares[6]
- T1562.001 Impair Defenses: Disable or Modify Tools[7]

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.
