Threat Hunter Team
Symantec

POSTED: 14 APR, 2022 | 9 MIN READ |
THREAT INTELLIGENCE

TRANSLATION: 日本語

Lazarus Targets Chemical Sector

Continuation of Operation Dream Job sees North Korea-linked APT target orgs in espionage campaign.

Symantec, a division of Broadcom Software, has observed the North Korea-linked advanced persistent threat (APT) group known as Lazarus conducting an espionage campaign targeting organizations operating within the chemical sector. The campaign appears to be a continuation of Lazarus activity dubbed Operation Dream Job, which was first

under th

Ope

Operatic

victims i

eventua

Past Dream Job campaigns have targeted individuals in the defense, government, and engineering sectors in activity observed in August 2020 and July 2021.

Recently targeted sectors

In January 2022, Symantec detected attack activity on the networks of a number of organizations based in South Korea. The organizations were mainly in the chemical sector, with some being in the information technology (IT) sector. However, it is likely the IT targets were used as a means to gain access to chemical sector organizations.

There is sufficient evidence to suggest that this recent activity is a continuation of Operation Dream Job. That evidence includes file hashes, file names, and tools that were observed in previous Dream Job campaigns.

A typical attack begins when a malicious HTM file is received, likely as a malicious link in an email or downloaded from the web. The HTM file is copied to a DLL file called scskapplink.dll and injected into the legitimate system management software INISAFE Web EX Client.

The scskapplink.dll file is typically a signed Trojanized tool with malicious exports added. The attackers have been observed using the following signatures: DOCTER USA, INC and "A" MEDICAL OFFICE, PLLC

Next, scskapplink.dll downloads and executes an additional payload from a command-and-control (C&C) server with the URL parameter key/values "prd_fld=racket".

This step kicks off a chain of shellcode loaders that download and execute arbitrary commands from the attackers, as well as additional malware, which are usually executed from malicious exports added to Trojanized tools such as the Tukaani project LZMA Utils library (XZ Utils).

The attackers move laterally on the network using Windows Management Instrumentation (WMI) and inject into MagicLine by DreamSecurity on other machines.

In some instances, the attackers were spotted dumping credentials from the registry, installing a BAT file in a
configured to run as a

The attackers were als
used to take screensh
intervals (SiteShoter).
protocol used to turn c

copier (FastCopy), and the File Transfer Protocol (FTP) executed under the MagicLine process.

Case study

The following is a case study detailing step-by-step attacker activity on an organization in the chemical sector.

January 17, 2022

00:51 – A malicious HTM file is received:

- e31af5131a095fbc884c56068e19b0c98636d95f93c257a0c829ec3f3cc8e4ba - csidl_profile\appdata\local\microsoft\windows\inetcache\ie\3tygrjkm\join_06[1].htm

The HTM file is copied to a DLL file:

- rundll32.exe CSIDL_PROFILE\public\scskapplink.dll,netsetcookie Cnusrmgr

This DLL file is injected into the legitimate system management software INISAFE Web EX Client. The file is a signed Trojanized version of the ComparePlus plugin for Notepad++ with malicious exports added.

01:02 – The file is run and downloads and executes a backdoor payload (final.cpl - 5f20cc6a6a82b940670a0f89eda5d68f091073091394c362bfcaf52145b058db) from a command-and-control (C&C) server with the URL parameter key/values "prd_fld=racket".

The file final.cpl is a Trojanized version of the Tukaani project LZMA Utils library (XZ Utils) with a malicious export added (AppMgmt).

The malware connects to, downloads, decodes, and executes shellcode from the following remote location:

- hxxp[:]//happy[.]nanoace.co.kr/Content/rating/themes/krajee-fas/FrmAMEISMngWeb.asp

01:04 – Another CPL file (61e305d6325b1ffb6de329f1eb5b3a6bcafa26c856861a8200d717df0dec48c4) is executed. This file, aga
export.

01:13 – The shellcode l

01:38 – Commands are
registry hives.

Over the next several hours, the attackers run unknown shellcode via final.cpl at various intervals, likely to collect the dumped system hives, among other things.

06:41 – The attackers create a scheduled task to ensure persistence between system reboots:

- schtasks /create /RU [REDACTED].help\175287 /ST 15:42 /TR "cmd.exe /c C:\ProgramData\Intel\Intel.bat" /tn arm /sc MINUTE

The scheduled task instructs the system to execute 'Intel.bat' as user '[REDACTED].help/175287' starting at 15:42 then every minute under the scheduled task name 'arm'. It's unclear if this was an account that was cracked via the dumped registry hives or an account the attackers were able to create with admin rights.

The attackers were also observed installing Cryptodome (PyCrypto fork) Python encryption modules via CPL files.

A clean installation of BitDefender was also installed by the attackers. While unconfirmed, the threat actors may have installed an older version of this software (from 2020) with a vulnerability that allowed attackers to run arbitrary commands remotely.

January 18

00:21 – The final.cpl file is executed again.

00:49 – A new CPL file called wpm.cpl (942489ce7dce87f7888322a0e56b5e3c3b0130e11f57b3879fbefc48351a78f6) is executed.

- CSIDL_COMMON_APPDATA\finaldata\wpm.cpl Thumbs.ini 4 30

This file contains, and connects to, a list of IP addresses and records whether the connections were successful.

01:11 – Again, the final.cpl shellcode loader is executed multiple times, executing some unknown shellcode. This activity continued intermittently until 23:49.

23:49 – The file name of the CPL file changes to 'ntuser.dat'. The file location and command-line argume

January 19

00:24 – The CPL shell
multiple times.

00:28 – The attackers
persistence:

- schtasks /create /RU [REDACTED]\i21076 /ST 09:28 /TR "cmd.exe /c C:\ProgramData\Adobe\arm.bat" /tn arm /sc MINUTE

The command is used to schedule a task named 'arm' to run the file 'arm.bat' starting at at 09:28 then every minute after that under the user account '[REDACTED]\i21076'.

00:29 – A file named arm.dat (48f3ead8477f3ef16da6b74dadc89661a231c82b96f3574c6b7ceb9c03468291) is executed with the following command line arguments:

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\adobe\arm.dat,packageautoupdater LimitedSpatialExtent_U_f48182 -d 1440 -i 10 -q 8 -s 5

The arm.dat file is a tool used to take screenshots of web pages viewed on the compromised machine every 10 seconds (SiteShoter), as determined by the command line arguments. The screenshots are saved in appdata\local with the date at the top of the file.

06:50 – The shellcode loader (final.cpl) is executed several times.

07:34 – A new CPL file named addins.cpl (5f20cc6a6a82b940670a0f89eda5d68f091073091394c362bfcaf52145b058db) is executed multiple times, which again is another shellcode loader and has the same command line arguments as seen with final.cpl:

- CSIDL_SYSTEM\rundll32.exe CSIDL_COMMON_APPDATA\addins.cpl, AppMgmt EO6-CRY-LS2-TRK3

07:39 – A scheduled task is created:

- sc create uso start= auto binPath= “cmd.exe /c start /b C:\Programdata\addins.bat” DisplayName= uso

The task is used to auto-start and execute addins.bat each time the system is booted. The task uses the service name 'uso' (a file name previously used in older Dream Job campaigns targeting security researchers).

The attacker runs addi
delete the service dire

- CSIDL_SYSTEM\r
  AppMgmt EO6-CR
- sc start uso (via cm
- sc delete uso

The following commands were then executed to collect information pertaining to network configuration, current user the attackers are logged in as, active users on the machine, available shared drives, and the contents of the 'addins' directory.

- ipconfig /all
- whoami
- query user
- net use
- dir CSIDL_WINDOWS\addins

07:41 – The file addins.cpl is executed again multiple times before a scheduled task is created to run addins.bat again, start the service, and immediately delete the service:

- sc create uso start= auto binPath= "cmd.exe /c start /b C:\Windows\addins\addins.bat" DisplayName= uso
- sc start uso
- sc delete uso

January 20

The attackers execute addins.cpl again with the same command line as before.

No further activity is observed.

The Lazarus group is likely targeting organizations in the chemical sector to obtain intellectual property to further North Korea's own pursuits in this area. The group's continuation of Operation Dream Job, as witnessed by Symantec and others, suggests that the operation is sufficiently successful. As such, organizations should ensure they have adequate security in place and remain vigilant for attacks such as this.

As always, users should be wary of clicking links or downloading files even if they come from seemingly trustworthy sources.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of

SHA-256

164f6a8f7d2035ea475

18686d04f22d3b593c

1cb8ea3e959dee9882

2dd29b36664b28803819054a59934f7a358a762068b18c744281e1589af00f1f

32bfdf1744077c9365a811d66a6ea152831a60a4f94e671a83228016fc87615f

35de8163c433e8d9bf6a0097a506e3abbb8308330d3c5d1dea6db71e1d225fc3

4277fcaada4939b76a3df4515b7f74837bf8c4b75d4ff00f8d464169eede01e3

4446efafb4b757f7fc20485198236bed787c67ceffc05f70cd798612424384ce

48f3ead8477f3ef16da6b74dadc89661a231c82b96f3574c6b7ceb9c03468291

4a2236596e92fa704d8550c56598855121430f96fe088712b043cba516f1c76c

54029bd4fcc24551564942561a60b906bee136264f24f43775b7a8e15095a9e0

56da872e8b0f145417defd4a37f357b2f73f244836ee30ac27af7591cda2d283

5e7edc8f1c652f53a6d2eabfbd9252781598de91dbe59b7a74706f69eb52b287

5f20cc6a6a82b940670a0f89eda5d68f091073091394c362bfcaf52145b058db

61e305d6325b1ffb6de329f1eb5b3a6bcafa26c856861a8200d717df0dec48c4

67f1db122ad8f01e5faa60e2facf16c0752f6ab24b922f218efce19b0afaf607

7491f298e27eb7ce7ebbf8821527667a88eecd5f3bc5b38cd5611f7ebefde21e

79b7964bde948b70a7c3869d34fe5d5205e6259d77d9ac7451727d68a751aa7d

7aa62af5a55022fd89b3f0c025ea508128a03aab5bc7f92787b30a3e9bc5c6e4

8769912b9769b4c11aabc523a699d029917851822d4bc1cb6cc65b0c27d2b135

8aace6989484b88abc7e3ec6f70b60d4554bf8ee0f1ccad15db84ad04c953c2d

942489ce7dce87f7888322a0e56b5e3c3b0130e11f57b3879fbefc48351a78f6

a881c9f40c1a5be3919cafb2ebe2bb5b19e29f0f7b28186ee1f4b554d692e776

bdb76c8d0afcd6b57c8f1fa644765b95375af2c3a844c286db7f60cf9ca1a22a

d815fb8febaf113f3cec82f552dfec1f205071a0492f7e6a2657fa6b069648c6

e1997d1c3d84c29e02

e31af5131a095fbc884

ef987baef9a1619454b

f29d386bdf77142cf24

f7359490d6c141ef7a9ee2c03dbbd6ce3069e926d83439e1f8a3dfb3a7c3dc94

f8995634b102179a5d3356c6f353cb3a42283d9822e157502486262a3af4447e

ff167e09b3b7ad6ed1dead9ee5b4747dd308699a00905e86162d1ec1b61e0476

Network

52.79.118.195

61.81.50.174

[URL]/[FOLDER]/[FILENAME]asp?prd_fld=racket

happy.nanoace[.]co.kr

hxxp://happy.nanoace[.]co.kr/Content/rating/themes/krajee-fas/FrmAMEISMngWeb.asp

hxxps://mariamchurch[.]com/board/news/index.asp

hxxps://www.aumentarelevisite[.]com/img/context/offline.php

mariamchurch.com

www.aumentarelevisite[.]com

www.juneprint[.]com

www.jungfrau[.]co.kr

www.ric-camid[.]re.kr

File names

addins.cpl

dolby.cpl

ezhelp.cpl

final.cpl

officecert.ocx

wpm.cpl

Services

arm

uso

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

Related Blog Posts

POSTED: 22 OCT, 2024 | 5 MIN READ

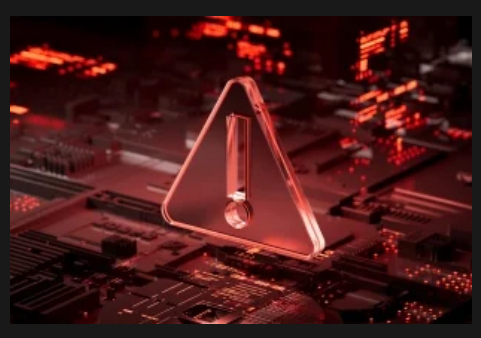
Exposing the Danger Within: Hardcoded Cloud Credentials in Popular Mobile Apps

POSTED: 17 OCT, 2024 | 3 MIN READ

Ransomware: Threat Level Remains High in Third Quarter

POSTED: 2 OCT, 2024 | 5 MIN READ

Stonefly: Extortion Attacks Continue Against U.S. Targets



POSTED: 12 SEP, 2024 | 3 MIN READ

Ransomware: Attacks Once More Nearing Peak Levels

SUBSCRIBE FOLLOW