SharpPanda APT Campaign Expands its Arsenal Targeting G20 Nations

: 6/1/2023

Threat Actors Utilize Undetected Loaders for Stealthy Attacks

SharpPanda, an APT group originating from China, has seen a rise in its cyber-attack operations starting from at least 2018. The APT group utilizes spear-phishing techniques to obtain initial access, employing a combination of outdated Microsoft Office document vulnerabilities, novel evasion techniques, and highly potent backdoor malware. This backdoor enables Threat Actors (TAs) to exfiltrate system information, files, and other sensitive data from the targeted victim's machine.

Cyble Research and Intelligence Labs (CRIL) recently observed an ongoing campaign by SharpPanda APT. Previously, this APT group has been observed targeting government officials, particularly in Southeast Asian countries. This latest campaign specifically targets high-level government officials from G20 nations.

The G20, or Group of Twenty, is an international forum comprising 19 countries and the European Union (EU). Established in 1999, its primary objective is to foster global economic cooperation and address key challenges impacting the worldwide economy.

Member countries of the G20 include Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, South Korea, Turkey, the United Kingdom, and the United States. Together, these nations represent a diverse range of economies, constituting a significant share of global GDP and population. The G20 holds annual summits where leaders convene to discuss and coordinate security, economic, and financial policies.

In its latest campaign, the SharpPanda APT group employs a forged document linked to G7 to target various governments within the G20 forum.

The delivery mechanism of the SharpPanda APT attack via a spam email is illustrated in the figure below.

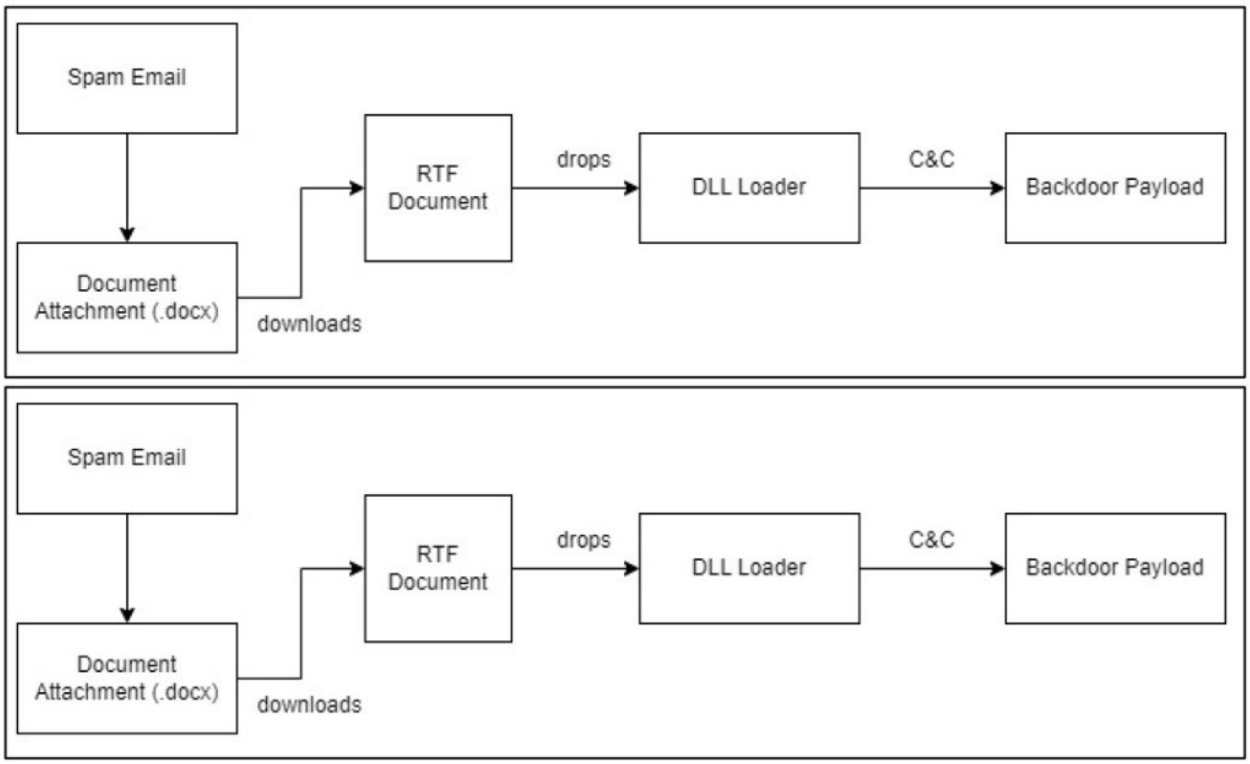

Figure 1 – Infection chain

Technical Details

Initial Infection

The infection process initiates through a spam email comprising an attached MS Office document named *"[FINAL] Hiroshima Action Statement for Resilient Global Food Security_trackchanged.docx."* These emails, with the subject line *"[Sending Finalized Text] G7+Partners FASS Meeting,"* are distributed to multiple employees within government entities across G20 countries, as shown in the figure below.

Figure 2 – Spam email containing malicious doc attachment

The emails contain weaponized versions of seemingly genuine official documents, which employ the remote template injection method to retrieve the next stage of the malware from the TA's Command-and-Control (C&C) server. The attached document in the spam email is shown below.

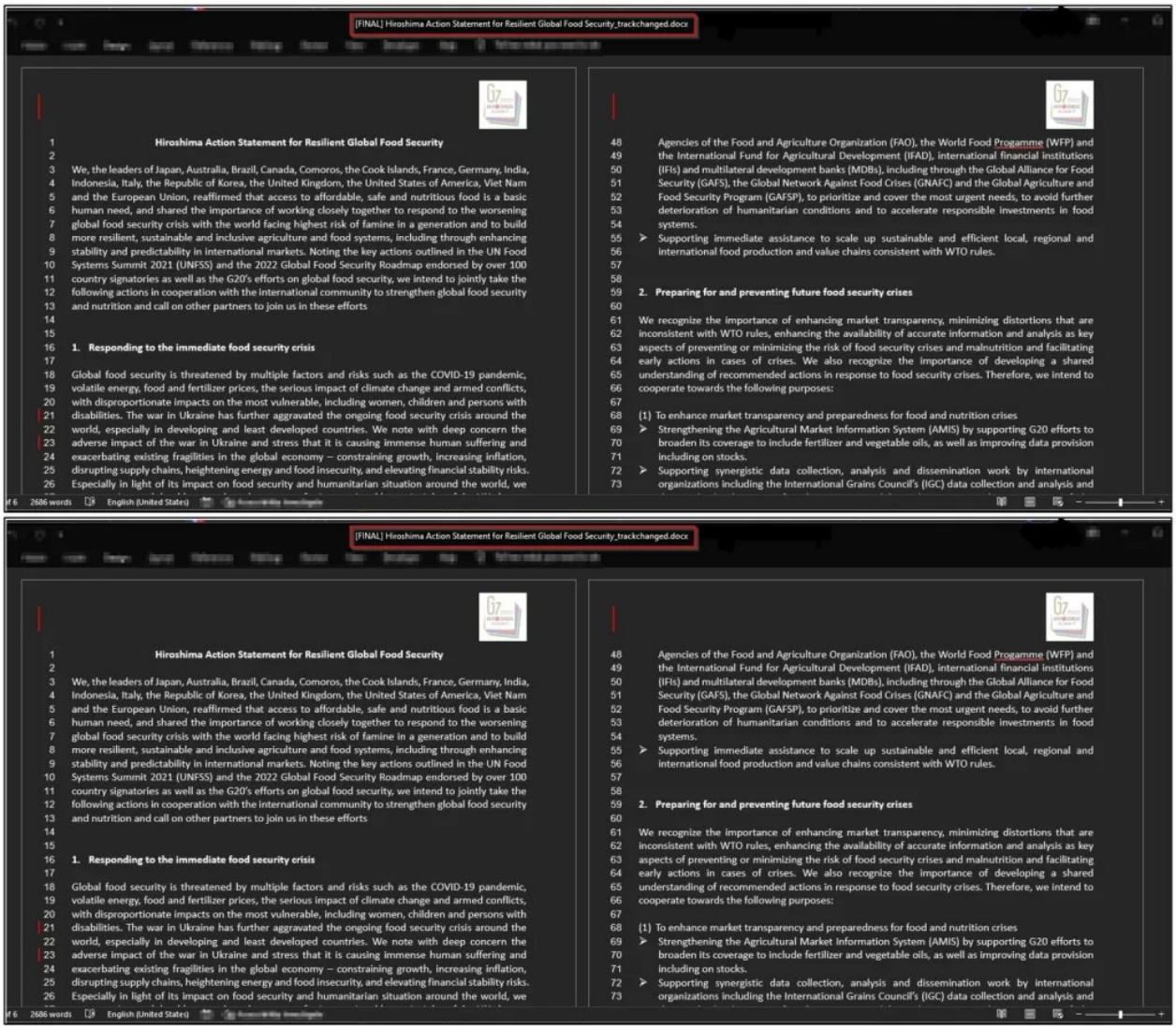

Figure 3 – Opened document attachment from spam email

Upon opening the document, it initiates the download of a new payload from the attacker's remote server (*hxxp[:]//13[.]236[.]189[.]80:8000/res/translate[.]res*), which is RTF file serving as the next-level payload.

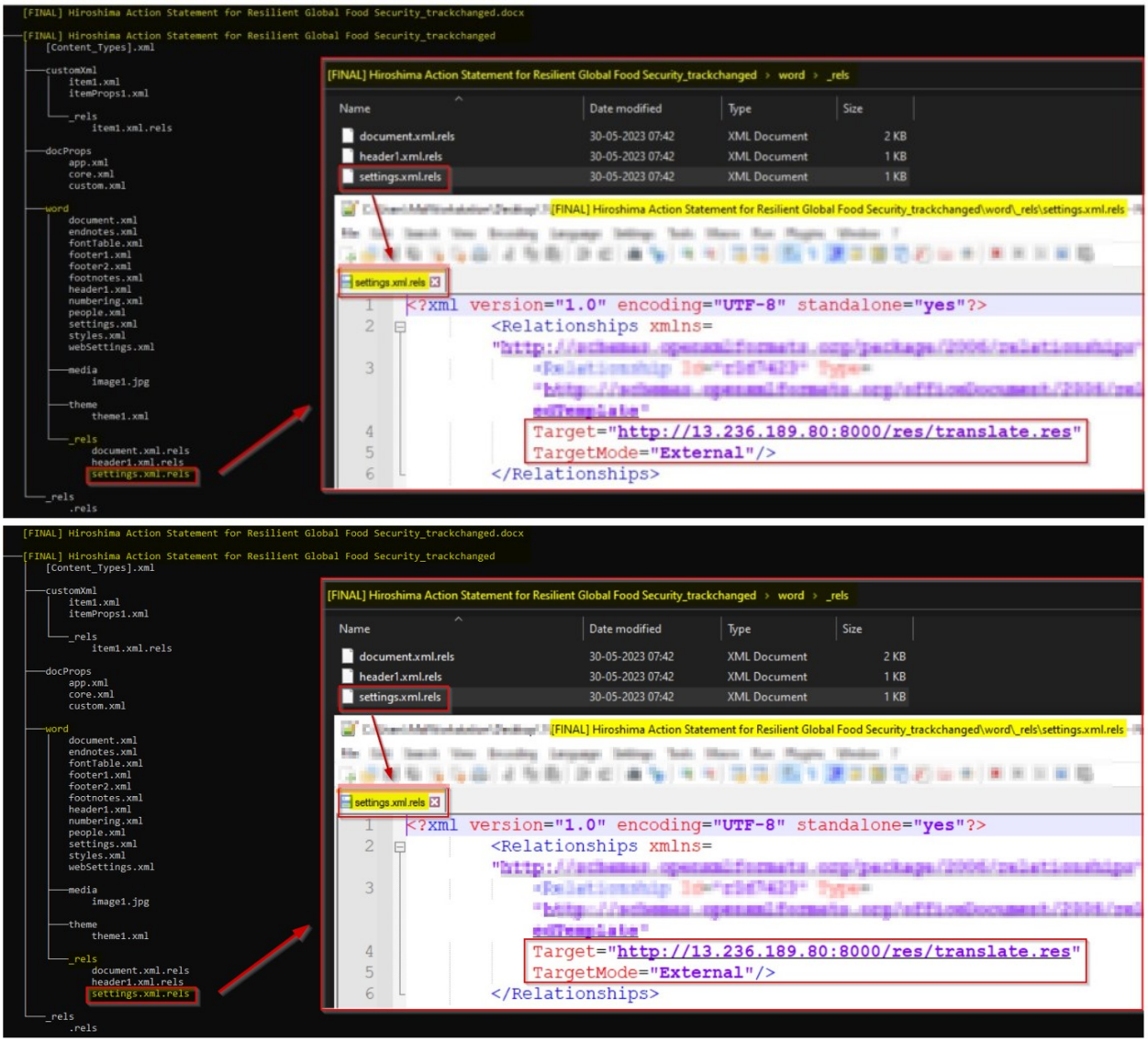

Figure 4 – Payload URL present inside the XML file of the malicious document

The RTF file is weaponized using a tool called RoyalRoad. This tool enables the TAs to create customized documents containing embedded objects that exploit vulnerabilities in Microsoft Word's Equation Editor.

RoyalRoad leverages a specific set of vulnerabilities, including CVE-2018-0802, CVE-2018-0798, and CVE-2017-11882, within the Equation Editor of Microsoft Office. The TAs integrate anti-analysis and anti-debugging techniques into their loaders to avoid being detected while also utilizing the older Equation Editor exploits.

The RTF file includes both an encrypted payload and shellcode. Once the RTF file is executed, it proceeds to decrypt and drops an embedded payload, which is a DLL file saved under the name "c6gt.b" in the %temp% directory.

After decryption, the shellcode facilitates the establishment of a persistence mechanism. It achieves this by creating a scheduled task entry, which executes the export function "StartA" from the DLL "c6gt.b" using rundll32.exe on a daily basis.

The figure below illustrates the presence of embedded content within the RTF document.

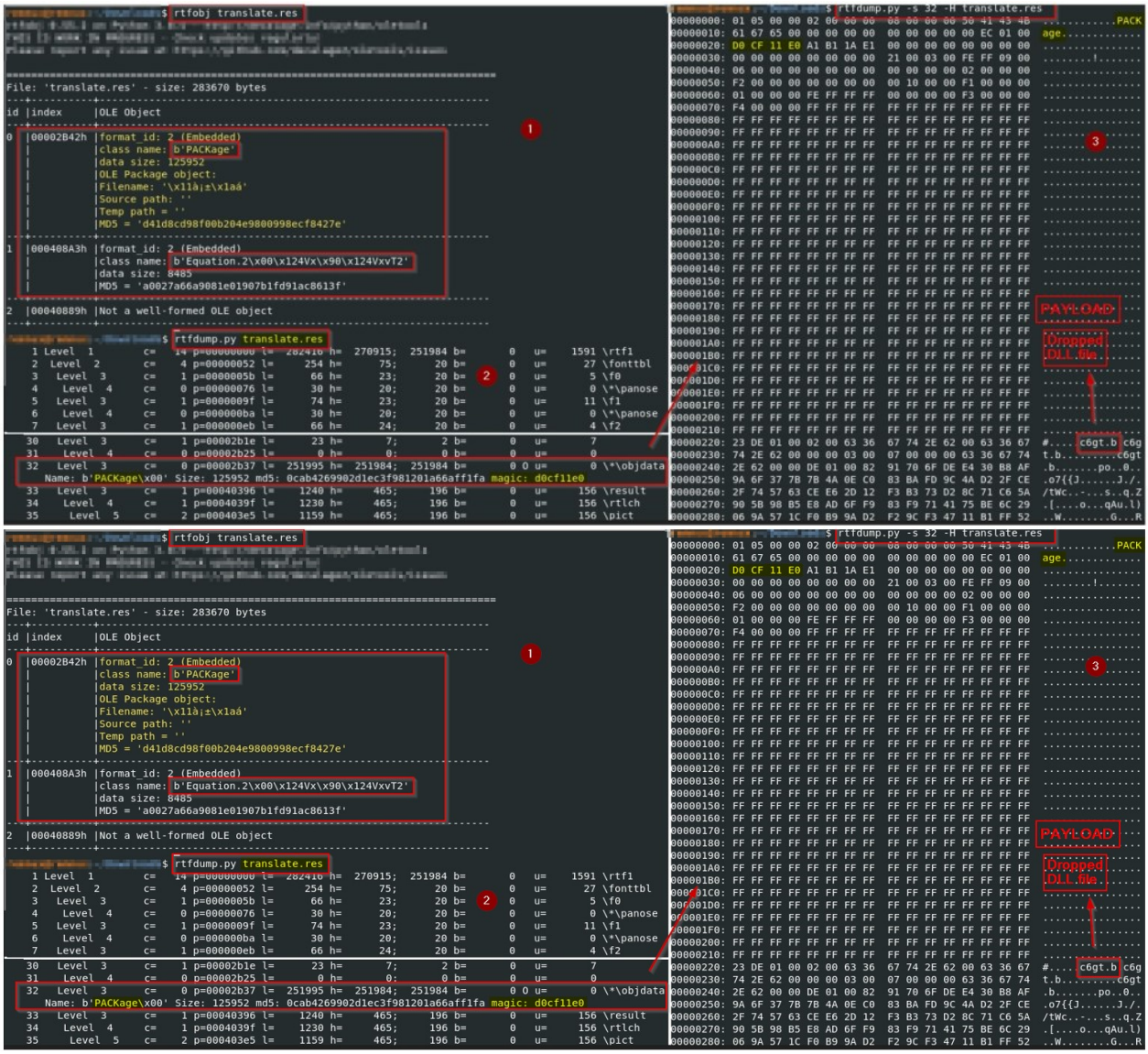

Figure 5 – Embedded payload in RTF file

Once the persistence is established, the RTF file proceeds to execute the downloaded DLL payload by utilizing the “rundll32.exe” command as follows:

- *rundll32.exe C:\Users<Admin>\AppData\Local\Temp\c6gt.b StartA*

DLL Downloader (“c6gt.b”)

The DLL file’s original name is “Downloader.dll.” It contains four export functions, as depicted below.

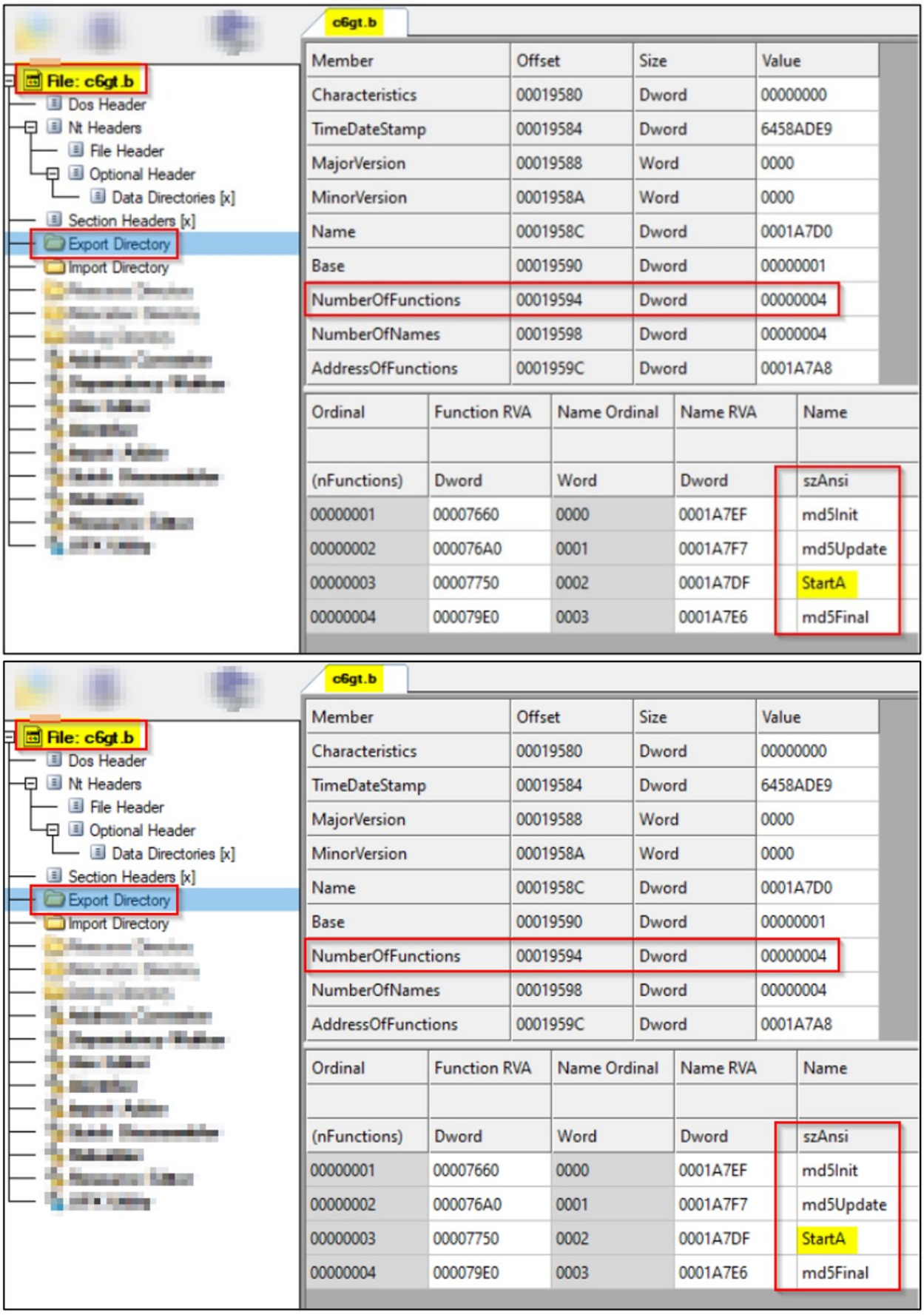

Figure 6 – Export functions of the DLL loader

When the loader is executed through rundll32.exe, it collects various data from the victim's computer. This includes the hostname, operating system name, OS version, username, Internet information, as well as the presence of any installed anti-virus software on the machine.

Subsequently, the loader encrypts the collected information using RC4 encryption with the key “xkYgv127” and encodes it using base64. The encrypted data is then exfiltrated using the below C&C URL:

- *hxxps://13[.]236[.]189[.]80:8001/G0AnyWhere_up[.]jsp?Data=[redacted]*

The figure below illustrates the exfiltrated data sent to the C&C server, as well as the decrypted/decoded stolen information obtained from the victim’s machine.

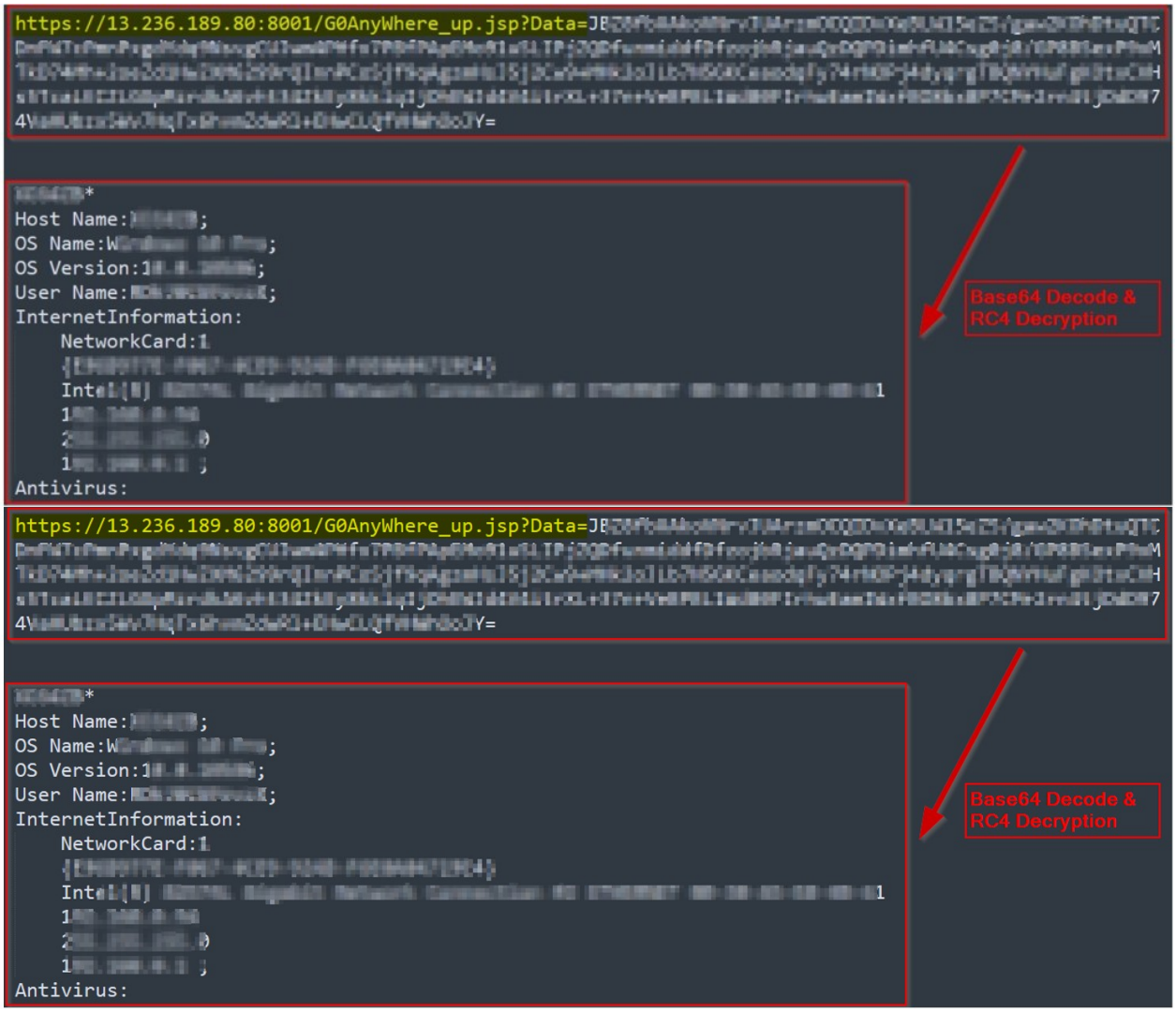

Figure 7 – Exfiltrated data to C&C server

Final Payload

Once the victim’s information is sent to the remote server, the TA checks the information. If they deem the victim’s machine to be intriguing, the C&C server responds with the next stage executable. During the final phase of the infection chain, the malicious loader in the SharpPanda APT campaign is specifically designed to download a backdoor module. However, during our analysis, no response was received from the remote server.

In previous SharpPanda APT campaigns, the loader establishes a connection with a C&C server in the final stage of the attack. Subsequently, it downloads and executes a malicious backdoor.

With its extensive capabilities, this backdoor possesses the ability to perform a variety of operations, including:

- Capture screenshots of victims’ system
- Obtain information about processes and services running on the machine
- Create or terminate processes

- Delete/Create/Rename/Read/Write files and retrieve file attributes
- Retrieve TCP/UDP tables
- Retrieve information about registry keys
- Obtain titles of all top-level windows
- Trigger a shutdown of the targeted computer
- Gather computer-specific information such as computer name, username, gateway address, network adapter details, Windows version, and user type

Conclusion

The SharpPanda APT group is comprised of exceptionally sophisticated cyber-TAs who execute targeted and extended attacks against specific targets, including governments, organizations, and industries, with the objectives of spying, disruption, or monetary gain. SharpPanda has been associated with multiple cyber espionage campaigns, employing strategies such as spear-phishing, manipulation through social engineering, and exploiting zero-day vulnerabilities to gain illicit access to networks.

Previously, this group has been observed targeting government officials, particularly in Southeast Asian countries. However, as evidenced in this recent campaign, their focus has shifted to high-level government officials from G20 countries in Europe, North America, and South Asia. The APT group consistently adapts its techniques and incorporates new tools into its arsenal as it evolves.

CRIL actively monitors the latest APT attacks, phishing attempts, and circulating malware strains, consistently releasing informative blog posts that offer valuable insights and practical guidance to safeguard users against these widely recognized attacks.

Our Recommendations

We have listed some essential cybersecurity best practices that create the first line of control against attackers. We recommend that our readers follow the best practices as mentioned below:

- Avoid downloading pirated software from warez/torrent websites. The “Hack Tool” present on sites such as YouTube, torrent sites, etc., mainly contains such malware.
- Use strong passwords and enforce multi-factor authentication wherever possible.
- Turn on the automatic software update feature on your computer, mobile, and other connected devices.
- Use a reputed anti-virus and internet security software package on your connected devices, including PC, laptop, and mobile.
- Refrain from opening untrusted links and email attachments without first verifying their authenticity.
- Educate employees on protecting themselves from threats like phishing/untrusted URLs.
- Block URLs that could be used to spread the malware, e.g., Torrent/Warez.
- Monitor the beacon on the network level to block data exfiltration by malware or TAs.
- Enable Data Loss Prevention (DLP) Solutions on the employees’ systems.

MITRE ATT&CK® Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566	Spear-phishing Attachment
Execution	T1204	User Execution
	T1203	Exploitation for Client Execution
Persistence	T1053	Scheduled Task
Defense Evasion	T1497	Virtualization/Sandbox Evasion

	T1027	Obfuscated Files or Information
Discovery	T1082	System Information Discovery
	T1518	Security Software Discovery
	T1016	System Network Configuration
Collection	T1006	Data from Local System
Command And Control	T1065	Uncommonly Used Port
	T1071	Application Layer Protocol
	T1105	Ingress Tool Transfer

Indicators Of Compromise

Indicators	Indicator Type	Description
f39442edc4a96ce729e50f66901263e1	MD5	Spam email
734b1cd163937e9509ea616f5f7ff8870f7be8e5	SHA1	
1fb22c38c781495018deda70af49bda17269203547620c140ee9eee68cecc016	SHA256	
ea889308acb4249af92807cc7d70f084	MD5	Document attachment
92c8f9ea9b6555e1b9c42cd7302f7caf62eb83e6	SHA1	
57b64a1ef1b04819ca9473e1bb74e1cf4be76b89b144e030dc1ef48f446ff95b	SHA256	
92d994be99ea43c121ac4f4ddfacbf75	MD5	RTF document
f14afd2856dab6183150f6e269f5bb6f4a2e3f50	SHA1	
180f5a0f9210698b54dcafb9a230b12e3eaf199889e5377a2acb7124c2d48d69	SHA256	
09bf850be5da44a1c3629a1f62813a83	MD5	DLL loader
a4e89d1f060e4dfd5f0fd4e7ba8be96967b39ac7	SHA1	
21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e6	SHA256	
hxxp[:]//13[.]236[.]189[.]80:8000/res/translate[.]res	URL	RTF payload download
13[.]236[.]189[.]80:8000	IP: Port	C&C