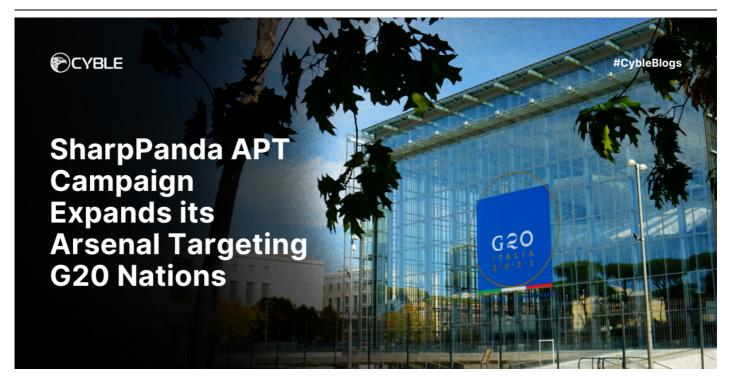
blog.cyble.com /2023/06/01/sharppanda-apt-campaign-expands-its-arsenal-targeting-g20-nations/

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 The APT group utilizes spear-phishing techniques to obtain initial access, employing a combination of outdated Microsoft Office document vulnerabilities, novel evasion techniques, and highly potent backdoor malware.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.

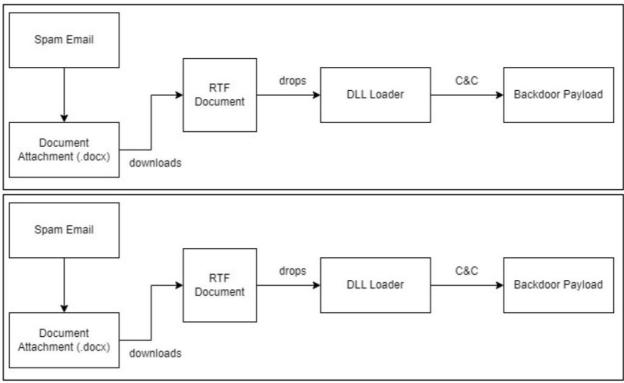


Figure 1 – Infection chain

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.

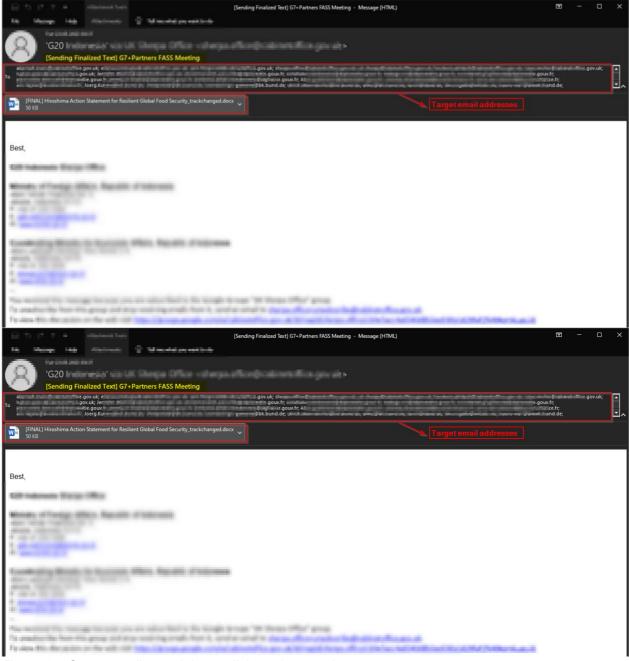


Figure 2 – Spam email containing malicious doc attachment

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.

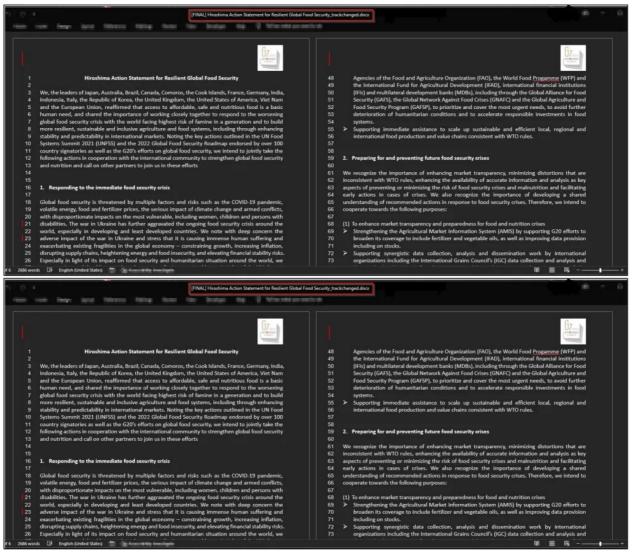


Figure 3 – Opened document attachment from spam email

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.

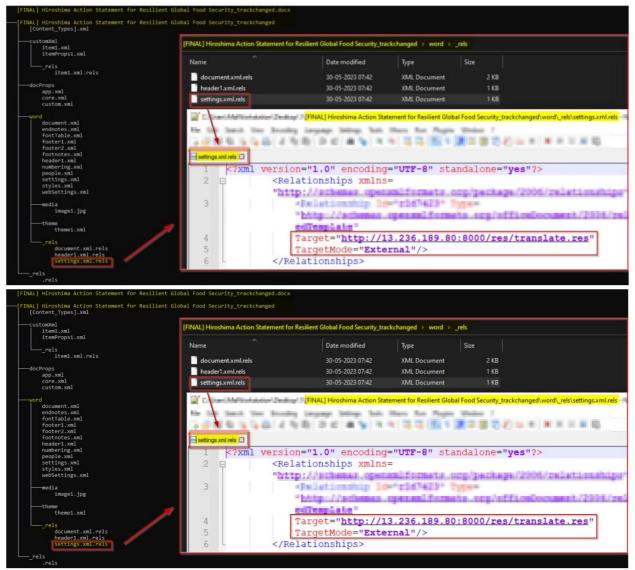


Figure 4 - Payload URL present inside the XML file of the malicious document

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.

| render (* 1999) - Stand Stands (* frido) translate.res render (* 2016) - Stand Syndam (* 1999) - Stand Table, set supplementation of the | | | | 00000010: 61 00000020: D0 00000030: 00 | \$ 05 00 00 02 00 07 65 00 00 00 07 11 E0 A1 B 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | 5 00 00 0 9 00 00 0 1 1A E1 0 9 00 00 2 9 00 00 0 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 01 00 03 00 00 00 00 00 | | age. |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| File: 'translate.res' - size: 283670 bytes | | | | | 00 00 00 00 FE FI | | | F3 00 00 00 | |
| id index OLE Object | | | | 00000070: F4 | 00 00 00 FF FF | | F FF FF FF | FF FF FF FF | |
| 0 00002842h format id: 2 (Embedded) class name: b'PACKage' data size: 125952 0LE Package object: Filename: '\x18a' Source path: '' Temp path: '' MOS = 'd41d8cd98f00b204e9800998ecf8427e' | | | | 00000080: FF 0000000A0: FF 0000000A0: FF 0000000C0: FF 0000000C0: FF 0000000C0: FF 000000F0: FF 00000100: FF | FF FF< | F FF FF F | F FF FF FF F FF FF FF | FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF | 3. |
| 1 000408A3h format_id: 2 (Embedded) class name: b'Equation.2\x00\x124Vx\x90\x124VxvT2' data size: 8485 | | | | 00000120: FF 00000130: FF 00000140: FF 00000150: FF | FF FF FF FF FF | F FF FF F F FF FF F F FF FF F F FF FF F | F FF FF FF FF FF FF FF FF FF FF FF FF FF | FF FF FF FF FF FF FF FF FF FF FF FF FF FF | |
| MD5 = 'a0027a66a9081e01907b1fd91ac8613f' | | | | 00000160: FF | | F FF FF F | F FF FF FF | FF FF FF FF | lange and the |
| 2 00040889h Not a well-formed OLE object | | | | 00000170: FF 00000180: FF | FF FF FF FF FF | | F FF FF FF | FF FF FF FF | PATLOAD |
| And a straight and a straight and a straight and a straight a stra | | | | 00000190: FF | FF FF FF FF FF | F FF FF F | F FF FF FF | FF FF FF FF | Dropped |
| 1 Level 1 c= 14 p=00000000 l= 202410 h= 270915; 25198 | | 0 u= | 1591 \rtf1 | 000001B0: FF | FF FF FF FF FF | F FF FF F | | FF FF FF FF | DLL fin |
| | 20 b= 20 b= 2 | 0 u= 0 u= | 27 \fonttbl 5 \f0 | 000001C0: FF | FF FF FF FF FF | F FF FF F | F FF FF FF | FF FF FF FF | |
| 4 Level 4 c= 0 p=00000076 l= 30 h= 20; 2 | 20 b= | 0 u= 0 u= | 0 *\panose | 000001E0: FF | FF FF FF FF FF | F FF FF F | | FF FF FF FF | |
| 6 Level 4 c= θ p=θθθθθθba l= 3θ h= 20; 2 | 20 b= 20 b= | θ u= | 11 \f1 0 *\panose | 00001F0: FF | | F FF FF F | F FF FF FF | FF FF FF FF | |
| | 20 b= | 0 u= | 4 \f2 | 00000210: FF | FF FF FF FF FF | F FF FF F | | FF FF FF FF | ···· |
| 30 Level 3 c= 1 p=00002b1e l= 23 h= 7; 31 Level 4 c= 0 p=00002b25 l= 0 h= 0; | 2 b= θ b= | θ u= θ u= | 7 (| | DE 01 00 02 00 2E 62 00 00 00 | | | 00 63 36 67 63 36 67 74 | # c6gt.b c6g t.bc6gt |
| 32 Level 3 c= 0 p=00002b37 l= 251995 h= 251984; 25190 Name: b'PACKage\x00' Size: 125952 md5: 0cab4269902dlec3f981201a | | 0 0 u= | 0 *\objdata | 00000240: 2E | 62 00 00 DE 0 | 00 82 9 | 1 78 6F DE | E4 30 B8 AF | .bpo0 |
| | 96 b= | 0 u= | 156 \result | | 6F 37 7B 7B 4/ | | | 4A D2 2F CE 8C 71 C6 5A | .o7{{JJ./. /tWcsq.Z |
| | 96 b= 96 b= | 0 u= 0 u= | 156 \rtlch 156 \pict | 00000270: 90 | 58 98 85 E8 A | 6F F9 8 | 33 F9 71 41 | 75 BE 6C 29 | .[qAu.l) |
| \$ rtfobi translate.res | | 0 u= | 120 (pict | | 9A 57 1C F0 B | rtfdump.p | oy -s 32 -H | translate.re | WGR |
| <pre>File: 'translate.res' - size: 283670 bytes id index OLE Object 0 000002842h format id: 2 (Embedded) class name: b PACKage' data size: 125952 OLE Package object: Filename: '\x11a]=\x1aa' Source path: '' Temp path = '' HOS = 'AdJdscd98f00b204e9800998ecf8427e' 000408A3h format_id: 2 (Embedded) class name: b Equation.2\x00\x124Vx\x90\x124VxvT2' data size: 3485 HOS = 'a0027a66a9081c01907b1fd91ac8613f' 2 00040889h Not a well-formed OLE object</pre> | | 1 | | 000000000: 01 00000010: 01 00000010: 01 00000030: 00 00000030: 00 00000030: FF 000000000: FF 00000010: FF | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | translate.re 50 41 43 48 00 EC 01 00 00 00 00 00 FE FF 09 00 02 00 00 00 F1 00 00 00 F1 00 00 00 F1 FF FF FF FF FF FF FF FF FF FF FF FF FF FF | age age |
| <pre>File: 'translate.res' File: 'translate.res' id index OLE Object 0 00002842h format_id: 2 (Embedded) [class name: b'PACKage' [data size: 125952 [OLE Package object: Filename: '\xllaitxlait' Source path: '\ Temp path = '' MO5 = 'd41d8cd98f00b204e9800998ecf8427e' 1 000408A3h format_id: 2 (Embedded) [class name: b'Equation.2\x00\xl24Vx\x90\xl24Vx\T2' data size: 8485 MO5 = 'a0027a663080e01907b1fd91ac8613f' 2 00040889h Not a well-formed OLE object \$ rffdump.py translate.res</pre> | | 0 | | 00000000000000000000000000000000000000 | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | yy -5 22 -H 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 | $\begin{array}{c} \text{Translate, resp.}\\ \text{Solution}\\ S$ | PACK |
| <pre>File: 'translate.res' - size: 283670 bytes id lindex OLE Object 0 00002842h format_id: 2 (Embedded)</pre> | 84 b= | 0 u= 0 u= | 1591 \rtf1 27 \fonttbl | 000000000: 01 000000010: 51 00000030: 00 0000030: 00 0000030: 72 00000030: 72 00000030: 72 00000030: 74 00000030: 77 00000030: 77 00000030: 77 00000030: 77 00000010: 77 00000100: 77 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | | Translate rr 1 1 0 0 1 1 0 0 0 1 1 0 0 0 0 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | age age |
| <pre>File: 'translate.res' - size: 283678 bytes id jindex OLE Object 0 00002842h format id: 2 (Embedded)</pre> | 84 b= | 1 0 0 u= | 1591 \rtf1 27 \fo1tbl 5 \fo | 000000000: 01 00000002: 00 00000020: 00 00000020: 00 00000000: 00 000000000: 70 000000000: 70 000000100: 70 00000100: 70 00000000000: 70 00000000000000000 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | | | | age age |
| <pre>File: 'translate.res' - size: 283670 bytes id jindex</pre> | 84 b= 20 b= 20 b= 20 b= 20 b= 20 b= | 0 u= 0 u= 0 u= 0 u= 0 u= | 1591 \rtf1 22 \fortbl 5 \fo 0 *\panose 1 *1 | 000000000: 01 00000002: 00 00000020: 00 00000020: 00 00000000: 00 000000000: 70 000000000: 70 000000100: 70 00000100: 70 00000000000: 70 00000000000000000 | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | $ \begin{array}{c} Translate, r = r \\ r = r \\ 0 = t < 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\ 0 = 0 \\$ | age age |
| <pre>File: 'translate.res' - size: 283670 bytes id lindex</pre> | 84 b= 20 b= 20 b= 20 b= 20 b= | 0 u= 0 u= 0 u= 0 u= | 1591 \rtf1 27 \fo1tbl 5 \f0 0 *\panse | 00000000000000000000000000000000000000 | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | | age age |
| File: 'translate.res' - size: 283670 bytes id index OLE Object 0 00002842h format_id: 2 (Embedded) [class name: b'PACKage' 1 006002842h format_id: 2 (Embedded) [class name: b'PACKage' 1 006040843h format_id: 2 (Embedded) [class name: b'Equation.2\x00\x124Vx\x90\x124VxvT2' data size: 4845 1005 = '441d6cd98f00b204e9800998ecf8427e' 2 00040839h Not a well-formed OLE object 2 100040839h Not a well-formed OLE object 2 100040839h Not a well-formed OLE object 1 Level 1 c= 14 perousous t= 254 h= 75; 3 Level 3 c= 1 pe0000051 l= 74 h= 23; 5 Level 3 c= 1 pe0000051 l= 74 h= 23; 7 Level 3 c= 1 pe0000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe0000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe0000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe0000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe0000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe00052 l= 23 h= 7; 3 0 Level 3 c= 1 pe000 | 84 b= 20 b= | 0 U= 0 U= 0 U= 0 U= 0 U= 0 U= 0 U= 0 U= | 1591 \rtf1 27 \fonttbl 5 \f0 0 *\panose 11 \f1 0 *\panose 4 \f2 7 | 00000000000000000000000000000000000000 | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 1 F 1 Gump. 1 1 G 00 0 2 00 00 2 00 00 0 1 A El 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 0 00 0 | yy -5 22 -H 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 10 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | $ \begin{array}{c} From State: r \\ From State: r \\ Sol = It < Sol = S$ | age. PACK age. B B PAYLOAD Umped DLL 0n. |
| <pre>File: 'translate.res' - size: 283670 bytes id jindex</pre> | 84 b= 220 b= 220 b= 220 b= 220 b= 220 b= 220 b= 2 b= | 0 u= 0 u= 0 u= 0 u= 0 u= 0 u= 0 u= 0 u= | 1591 \rtf1 27 \fonttbl 5 \f0 0 *\panose 1 \f1 0 *\panose 1 \f1 0 *\panose 4 \f2 7 | 00000000000000000000000000000000000000 | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 | | Translate rr 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 | BACK egg. BACK BACK BACK BACK BACK BACK BACK BACK |
| <pre>File: 'translate.res' - size: 283670 bytes id [index 0LE Object 0 100002842h format id: 2 (Embedded) 1 [class name: b'PACKage'] 1 [data size: 123952 2 [0LE Package object: 1 Filename: '\xllai's\xlai' 3 Source path: '' 1 Temp path = '' 1 [000408A3h format id: 2 (Embedded) 1 [class name: b'Equation.2\x00\xl24Vx\x90\xl24Vx\r2' 1 [000408A3h format id: 2 (Embedded) 1 [class name: b'Equation.2\x00\xl24Vx\x90\xl24Vx\r2' 1 [000408A3h format id: 2 (Embedded) 1 [class name: b'Equation.2\x00\xl24Vx\x90\xl24Vx\r72' 1 [000408A3h format id: 2 (Embedded) 1 [class name: b'Equation.2\x00\xl24Vx\x90\xl24Vx\r72' 1 [000408A3h format id: 2 (Embedded) 1 [class name: b'Equation.2\x00\xl24Vx\x90\xl24Vx\r72' 1 [data size: 8485 1 [dut a well-formed OLE object 2 [000408B9h Not a well-formed OLE object 3 Level 2 c= 4 p=00000050 l= 26 h= 27, 15 3 Level 3 c= 1 p=0000050 l= 30 h= 20; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 1 p=00002252 l= 23 h= 7; 3 Level 3 c= 0 p=00002252 l= 23 h= 7; 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=0002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=0002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002252 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002552 l= 25195 h= 251984; 25197 3 Level 3 c= 0 p=00002552 l= 25195 h= 251954; 25197 3 L</pre> | 84 b= 22 b= 22 b= 22 b= 22 b= 22 b= 22 b= 84 b= | 0 u= 0 u= 0 u= 0 u= 0 u= 0 u= 0 u= 0 u= | 1591 \rff1 27 \fonttbl 5 \f0 0 *\panose 11 \f1 0 *\panose 4 \f2 7 0 *\panose 4 \f2 8 | 000000000: 01 00000002: 00 00000020: 00 00000020: 00 00000002: 00 00000000: 00 00000000: 00 00000000: 00 00000000 | $\begin{array}{c} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 &$ | $\begin{array}{cccccccccccccccccccccccccccccccccccc$ | | $ \begin{array}{c} \mbox{translate}, \mbo$ | BACK BE BE BE BE BE BE BE BE BE BE |
| <pre>File: 'translate.res' - size: 283678 bytes id [index OLE Object 0 00002842h format id: 2 (Embedded)</pre> | 84 b= 20 b= 20 b= 20 b= 20 b= 20 b= 20 b= 2 b= 0 b= 2 b= 0 b= 2 b= 0 b= | | 1591 \rtf1 22 \fonttbl 5 \fo 0 *\spanse 11 \f1 0 *\spanse 4 \f2 7 0 *\objdsta | 00000000000000000000000000000000000000 | $\begin{array}{c} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 &$ | 1 F 1 Gump. 1 1 G 00 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 2 0 0 <tr< td=""><td>yy s. 2. - H 10 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 17 17 17 17 17 17 17 17 17 17<!--</td--><td>$\begin{array}{c} From State: \\ From State: \\ Sol = LC \le Sol$</td><td>B age B B B B B B B B B B B B B B B B B B B</td></td></tr<> | yy s. 2. - H 10 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 17 17 17 17 17 17 17 17 17 17 </td <td>$\begin{array}{c} From State: \\ From State: \\ Sol = LC \le Sol$</td> <td>B age B B B B B B B B B B B B B B B B B B B</td> | $ \begin{array}{c} From State: \\ From State: \\ Sol = LC \le Sol $ | B age B B B B B B B B B B B B B B B B B B B |

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.

| | c6gt.b | | | | | | | | |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------------------|------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|---|
| | Member | | Offs | Offset Size | | Val | | Value | |
| E File: c6gt.b | Characteristics | | 0001 | 00019580 Dwo | | rd 0000 | | 00000 | |
| - P I Nt Headers | TimeDateStamp | | 00019584 Dwo | | rd | 645 | 8ADE9 | | |
| File Header G I Optional Header | MajorVersion | | 0001 | 00019588 Wor | | d | 000 | 0 | |
| Data Directories [x] | MinorVersion | | 0001 | 001958A Wor | | d 0000 | | 0 | |
| Section Headers [x] | Name | | 0001 | 0001958C Dwo | | ord 0001 | | 1A7D0 | |
| Export Directory | Base | | 00019590 Dwg | | Dwo | ord 00 | | 00000001 | |
| - Orienter Desites | NumberOfFunctions | | 00019594 Dv | | Dwo | Dword | | 00004 | |
| - Consider Sectors | NumberOfNames | | 00019598 D | | Dwo | Dword | | 00004 | |
| - States Consta | AddressOfFunctions | | 0001959C Dwo | | ord 0001 | | 1A7A8 | | |
| - Constant Rates | Ordinal | Function | RVA Name Or | | dinal Name RV | | A Name | | - |
| - Stanta | | runction | | Name On | | TVarrie KVA | • | Ivanie | _ |
| - State Recently | (nFunctions) | Dword | | Word | | Dword | T | szAnsi | 1 |
| - Statute | 00000001 | 00007660 | | 0000 | | 0001A7EF | + | md5lnit | t |
| Contraction former | 0000002 | 000076A0 | | 0001 | | 0001A7F7 | + | md5Update | H |
| | 00000003 | 00007750 | | 0002 | | 0001A7DF | + | StartA | H |
| | 00000004 | 000079E0 | | 0003 | | 0001A7E6 | + | md5Final | H |
| | 00000004 000079E0 | | | | | | | in a standar | |
| | | | | | | | | | |
| | c6gt.b | | | | | | | | |
| | <mark>66gt.b</mark> Member | | Offs | et | Size | | Val | ue | |
| File: c6gt.b | | | | et 9580 | Size Dwo | ord | - | ue | |
| Dos Header Il Dos Header Il Nt Headers | Member | , | 0001 | (1971) | | | 000 | | |
| B Dos Header B Nt Headers B File Header | Member Characteristics |) | 0001 | 9580 | Dwo | rd | 000 | 000000 8ADE9 | |
| B Dos Header B Nt Headers B File Header B Optional Header B Data Directories [x] | Member Characteristics TimeDateStamp | , | 0001 0001 0001 | 9580 9584 | Dwo | rd d | 000 645 | 000000 ISADE9 IO | |
| I Dos Header I Dos Header I Nt Headers I I File Header I Optional Header I Data Directories [x] I Section Headers [x] | Member Characteristics TimeDateStamp MajorVersion | > | 0001 0001 0001 0001 | 9580 9584 9588 | Dwo Dwo Wor | rd d | 000 645 000 000 | 000000 ISADE9 IO | 4 |
| B Dos Header B Nt Headers B File Header B Optional Header B Data Directories [x] | Member Characteristics TimeDateStamp MajorVersion MinorVersion | > | 0001 0001 0001 0001 0001 | 9580 9584 9588 958A | Dwo Dwo Wor Wor | rd d d rd | 000 645 000 000 | 000000 8ADE9 10 | - |
| B Dos Header B Nt Headers B File Header B Optional Header B Data Directories [x] B Section Headers [x] Export Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name | | 0001 0001 0001 0001 0001 0001 | 9580 9584 9588 958A 958C | Dwo Dwo Wor Wor | rd d d rd rd | 000 645 000 000 000 | 000000 8ADE9 10 10 11A7D0 | |
| B Dos Header B File Header B File Header Dotional Header Data Directories [x] Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base | tions | 0001 0001 0001 0001 0001 0001 | 9580 9584 9588 958A 958C 9590 | Dwo Dwo Wor Dwo Dwo Dwo | rd d rd rd rd | 000 645 000 000 000 000 | 000000 8ADE9 00 100 11A7D0 000001 | |
| B Dos Header B File Header B File Header Dotional Header Data Directories [x] Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc | tions | 0001 0001 0001 0001 0001 0001 0001 | 9580 9584 9588 958A 958C 9590 9594 | Dwo Dwo Wor Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd | 000 645 000 000 000 000 000 | 000000 8ADE9 00 00 01A7D0 000001 000004 | |
| B Dos Header B File Header B File Header Dotional Header Data Directories [x] Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfFunc | tions | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 9598 | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd | 000 645 000 000 000 000 000 000 | 000000 8ADE9 00 00 01A7D0 000001 000004 01A7A8 | |
| B Dos Header B File Header B File Header Dotional Header Data Directories [x] Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfNam | tions tions | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd rd | 000 645 000 000 000 000 000 000 | 000000 8ADE9 10 10 11A7D0 100001 100004 100004 | |
| B Dos Header B File Header B File Header Dotional Header Data Directories [x] Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfFunc | tions tions | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 9598 | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd rd | 000 645 000 000 000 000 000 000 | 000000 8ADE9 00 00 01A7D0 000001 000004 01A7A8 | |
| B Dos Header B File Header B File Header Dotional Header Data Directories [x] Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfFunc Ordinal | tions tions Function I | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 9592 Name Ord | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd Name RVA | 000 645 000 000 000 000 000 000 | 000000 8ADE9 00 00 00 00 00 00 00 00 00 0 | |
| B Dos Header B File Header B File Header B Optional Header B Data Directories [x] B Section Headers [x] Export Directory Import Directory | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfFunc Ordinal (nFunctions) | tions tions Function I Dword | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 959C Name Ord | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd rd Dword | 000 645 000 000 000 000 000 000 | 000000 8ADE9 00 11A7D0 100001 100004 11A7A8 Name szAnsi md5lnit | |
| B Dos Header B Nt Headers B File Header B Optional Header B Optional Header B Section Headers [x] B Section Headers [x] B Section Headers [x] D Inport Directory D Inport Dinport Directory D Inport Directory D I | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfFunc Ordinal (nFunctions) 00000001 | tions tions Function f Dword 00007660 | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 959C Name Ord Word 0000 | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d rd rd rd rd rd Dword 0001A7EF | 0000 645 0000 0000 0000 0000 0000 | 000000 8ADE9 00 00 01A7D0 000001 000004 000004 000004 01A7A8 Name szAnsi | |
| B Dos Header B Nt Headers B File Header B Optional Header B Optional Header B Section Headers [x] B Section Headers [x] B Section Headers [x] D Inport Directory D Inport Dinport Directory D Inport Directory D I | Member Characteristics TimeDateStamp MajorVersion MinorVersion Name Base NumberOfFunc NumberOfFunc Ordinal (nFunctions) 00000001 00000002 | tions tions Function I Dword 00007660 000076A0 | 0001 0001 0001 0001 0001 0001 0001 000 | 9580 9584 9588 958A 958C 9590 9594 9598 9592 Name Ord 0000 0001 | Dwo Dwo Wor Dwo Dwo Dwo Dwo Dwo Dwo | rd d Mame RVA Dword 0001A7EF 0001A7F7 | 0000 645 0000 0000 0000 0000 0000 | 000000 8ADE9 0 0 11A7D0 000001 000004 11A7A8 Name szAnsi md5lnit md5lnit | |

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.

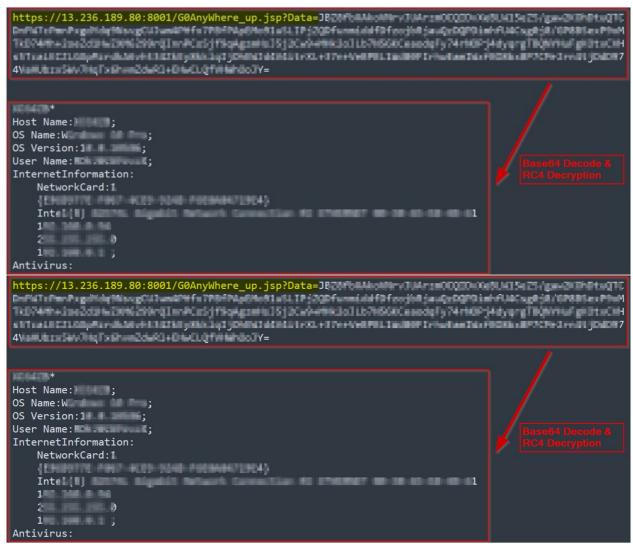


Figure 7 – Exfiltrated data to C&C server

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 |
| Execution | T1203 | Exploitation for Client Execution |
| Persistence | T1053 | Scheduled Task |
| Defense Evasio | on T1497 | Virtualization/Sandbox Evasion |

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

Indicators Of Compromise

| Indicators | Indicator Type | Description |
|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|----------------------------|
| f39442edc4a96ce729e50f66901263e1 734b1cd163937e9509ea616f5f7ff8870f7be8e5 1fb22c38c781495018deda70af49bda17269203547620c140ee9eee68cecc0 | MD5 SHA1 16 SHA256 | Spam email |
| ea889308acb4249af92807cc7d70f084 92c8f9ea9b6555e1b9c42cd7302f7caf62eb83e6 57b64a1ef1b04819ca9473e1bb74e1cf4be76b89b144e030dc1ef48f446ff95b | MD5 SHA1 SHA256 | Document attachment |
| 92d994be99ea43c121ac4f4ddfacbf75 f14afd2856dab6183150f6e269f5bb6f4a2e3f50 180f5a0f9210698b54dcafb9a230b12e3eaf199889e5377a2acb7124c2d48d6 | MD5 SHA1 9 SHA256 | RTF document |
| 09bf850be5da44a1c3629a1f62813a83 a4e89d1f060e4dfd5f0fd4e7ba8be96967b39ac7 21f173a347ed111ce67e4c0f2c0bd4ee34bb7ca765da03635ca5c0df394cd7e | MD5 SHA1 6 SHA256 | DLL loader |
| hxxp[:]//13[.]236[.]189[.]80:8000/res/translate[.]res | URL | RTF payload download |
| 13[.]236[.]189[.]80:8000 | IP: Port | C&C |