Operation PhantomBlu: New and Evasive Method Delivers NetSupport RAT

perception-point.io/blog/operation-phantomblu-new-and-evasive-method-delivers-netsupport-rat/

March 18, 2024

Perception Point security researchers have recently identified a newly surfaced campaign targeting US-based organizations. Dubbed "**PhantomBlu**," the emerging malware campaign employs new TTPs and behaviors to evade detection and deploy the notorious NetSupport RAT. This campaign signifies a sophistication in malware attack methodologies, exploiting the legitimate features of remote administration tools for nefarious purposes.

Teaching an Old RAT Some New Tricks

NetSupport RAT is a spin-off of the legitimate NetSupport Manager, a remote technical support app, exemplifying how powerful IT tools can be misappropriated into malicious software. Engineered for stealthy surveillance and control, it transforms remote administration into a platform for cyber attacks and data theft. This Remote Access Trojan facilitates a spectrum of malicious activities. Once installed on a victim's endpoint, NetSupport can monitor behavior, capture keystrokes (keylogger), transfer files, commandeer system resources, and move to other devices within the network – all under the guise of a benign remote support software.

The PhantomBlu operation introduces a nuanced exploitation method, diverging from NetSupport RAT's typical delivery mechanism by leveraging OLE (Object Linking and Embedding) template manipulation, exploiting Microsoft Office document templates to execute malicious code while evading detection.

This advanced technique bypasses traditional security systems by hiding the malicious payload outside the document, only executing upon user interaction.

Decoding PhantomBlu: A Deep Dive into Advanced TTPs

In the campaign prevented by Perception Point, hundreds of employees in various US-based organizations received email messages seemingly from an accounting service. Using social engineering, threat actors lure recipients into downloading the attached Office Word file

(.docx) to view their “monthly salary report.”

In the body of the email the attacker includes detailed instructions for accessing the password-protected “report.”

Figure 1: Targets are prompted to enter the password “1” and to click “Enable Editing”

By analyzing the Return Path and Message ID of the phishing emails, we observe the utilization of the “SendInBlue” or Brevo service, a legitimate email delivery platform that offers services for marketing campaigns. This choice underscores the attackers’ preference for leveraging reputable services to mask their malicious intent.

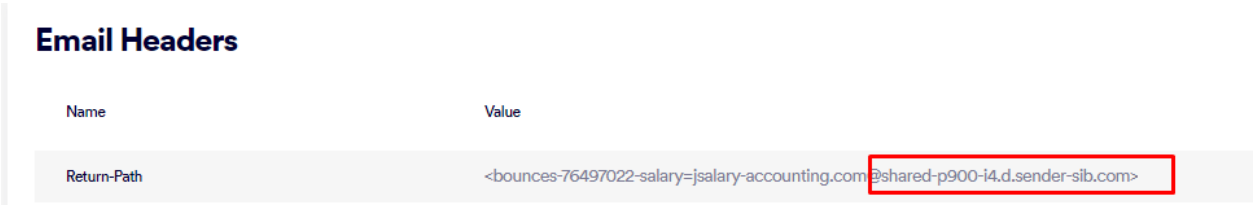

Figure 2: Return path data

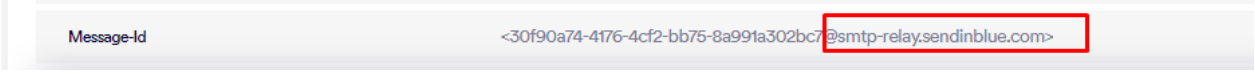

Figure 3: Message ID data

Upon downloading and accessing the attached .docx file targets are asked to insert the provided password.

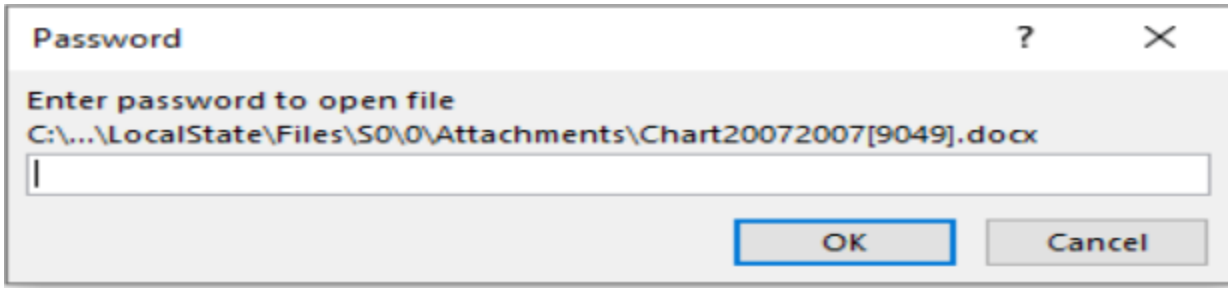

Figure 4: Enter password to open file

The content of the document further instructs the targets to click “enable editing” and then to click the image of the printer embedded on the document in order to view their “salary graph.” The clickable printer is actually an OLE package, a feature in Microsoft Windows that allows embedding and linking to documents and other objects. Its legitimate use enables users to create compound documents with elements from different programs.

With this step PhantomBlu’s campaign leverages a TTP called OLE **template manipulation**(Defense Evasion – T1221), exploiting document templates to execute malicious code without detection. This advanced technique bypasses traditional security measures by hiding the payload outside the document, only executing upon user interaction.

This is the first recorded time T1221 was observed in an attempt to deliver NetSupport RAT via email.

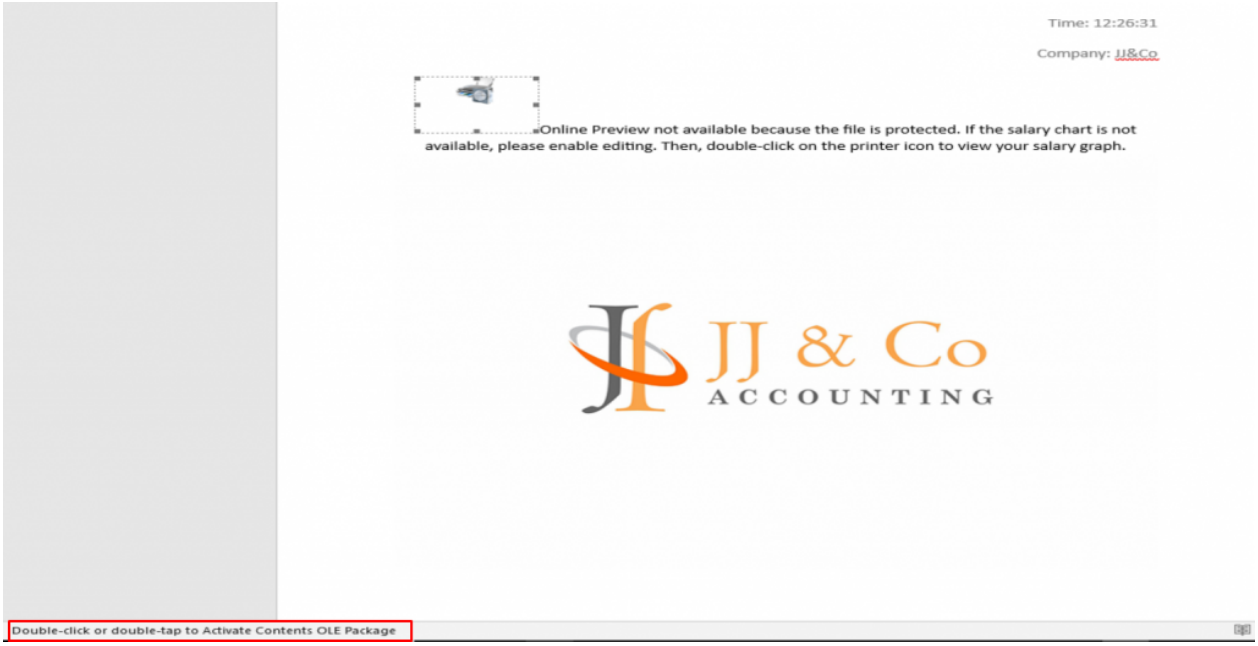

Figure 5: “Online Preview not available because the file is protected. If the salary chart is not available, please enable editing. Then, double-click the printer icon to view your salary graph”

Clicking the printer icon opens an archive .zip file containing **one LNK file**.

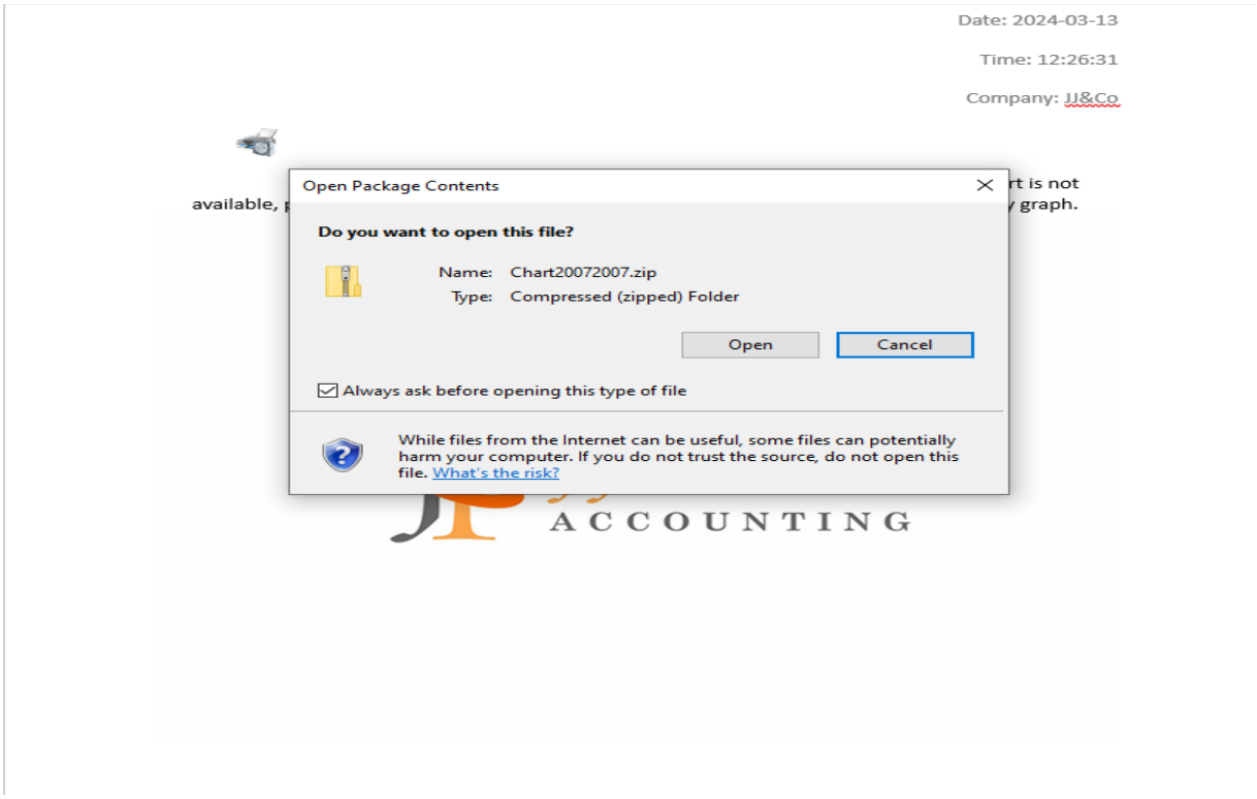

Figure 6: Opening the hidden content

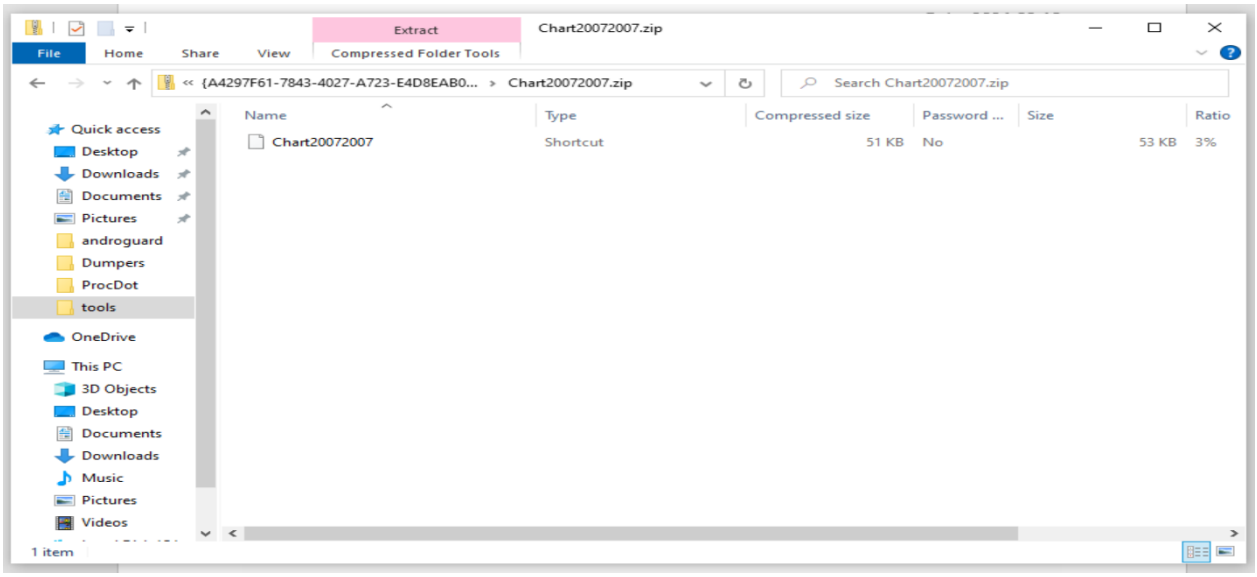

Figure 7: A look into the zip containing LNK file

Dissecting the Malware: From Lure to Control

In our forensic analysis of the LNK file, we dissected its payload and execution behavior. The file was identified as a PowerShell dropper, crafted to retrieve and execute a script from a specified URL.

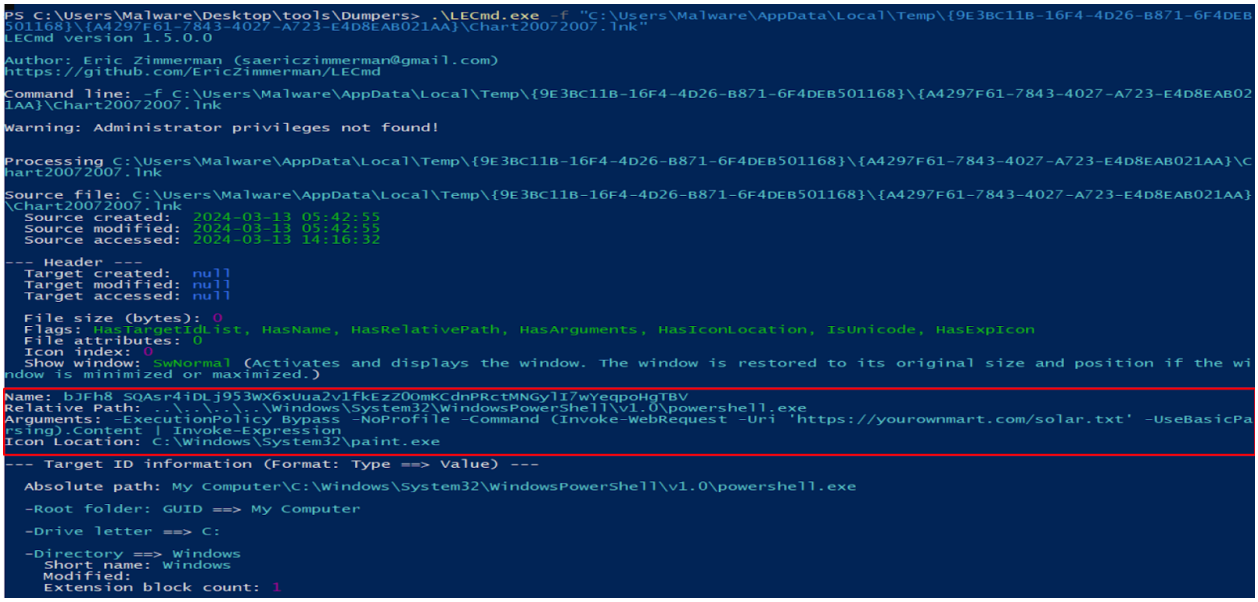

Figure 8: Examining the link's code

This script, upon closer examination, was obfuscated to mask its true intentions, containing elements such as another URL, a ZIP file, an executable for the NetSupport RAT, and a registry key designed for keeping the RAT alive.

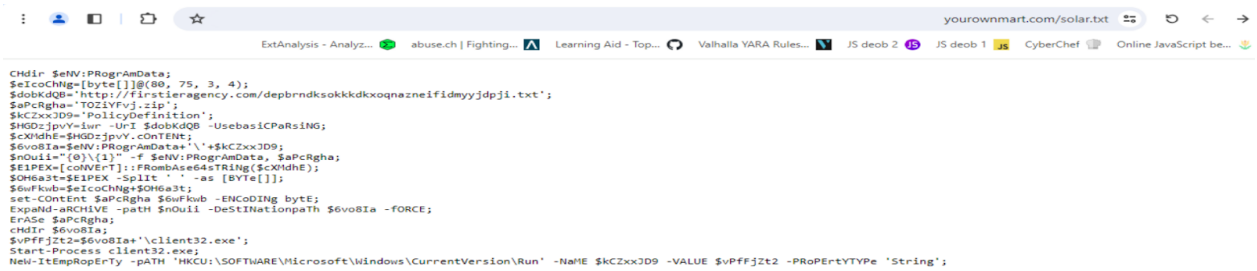

Figure 9: Obfuscated PowerShell extracted from the URL

Delving deeper, we de-obfuscated the PowerShell script to elucidate its operations. It meticulously orchestrates the creation of a secondary ZIP file from a fetched URL, unpacks it, and navigates to the extracted directory to activate the NetSupport RAT. This process culminates in the establishment of a new registry key within "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run", ensuring the malware's AutoStart and thereby its persistence.

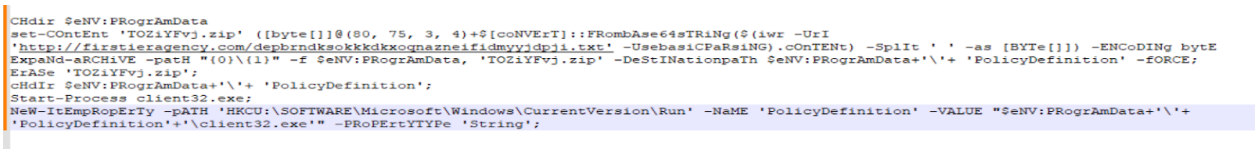

Figure 10: De-obfuscating the code

Our investigative efforts extended to accessing the secondary URL, revealing a user-agent gated payload delivery. Bypassing this, we obtained the payload through PowerShell, mirroring the attackers' approach.

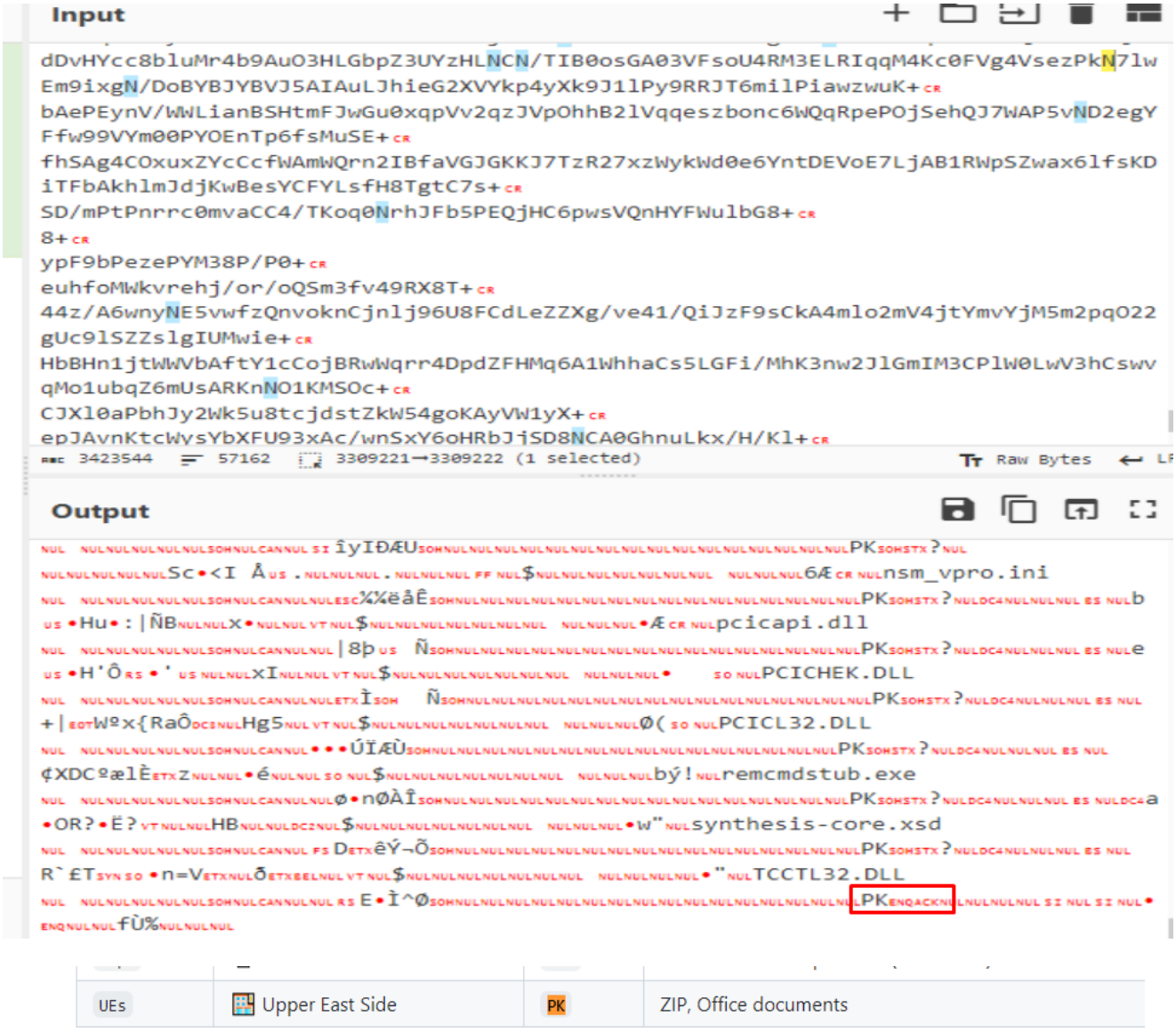

Figure 11: Retrieving the hidden content – a second zip file

Further analysis of the extracted contents confirmed the deployment of a ZIP file, as delineated in the script. The execution of the secondary PowerShell script, sans the deletion routine, yielded the "Client32.exe" file — the NetSupport RAT. An examination of its configuration files unveiled the command and control (C2) servers, underscoring PhantomBlu's communication backbone and operational directives.

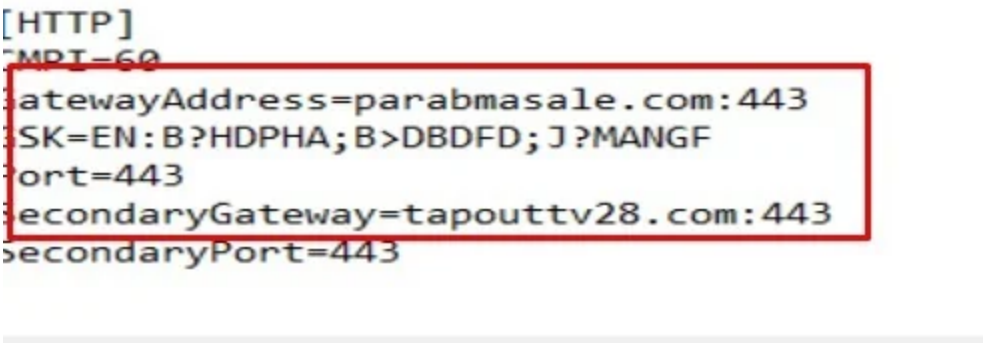

Figure 12: the NetSupport RAT's C2 servers

Beyond Evasion: The "Recursive Unpacker" Unravels PhantomBlu's Stealth

By using encrypted .docs to deliver the NetSupport RAT via OLE template and Template Injection (T1221), PhantomBlu marks a departure from the conventional TTPs commonly associated with NetSupport RAT deployments. Historically, such campaigns have relied more directly on executable files and simpler phishing techniques, which showcases PhantomBlu's innovation in blending sophisticated evasion tactics with social engineering.

Perception Point's proprietary anti-evasion model, the Recursive Unpacker, meticulously deconstructed the multi-layered obfuscation and evasion techniques employed by the PhantomBlu threat actors. From the email itself down to extracting the last LNK file hidden behind the template manipulation.

Figure 13: PhantomBlu "Attack Tree" unpacked by Perception Point's advanced detection engines

Check out the Perception Point blog to learn more about developing attack trends.

TTPs

Remote Access Software (T1219) — https://attack.mitre.org/techniques/T1219/

Windows Management Instrumentation(T1047) — https://attack.mitre.org/techniques/T1047/

Hide Artifacts: Hidden Files and Directories(T1564/003) — https://attack.mitre.org/techniques/T1564/003/

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder(T1547/001) — https://attack.mitre.org/techniques/T1547/001/

Hide Artifacts: Hidden Window(T1564/003) — https://attack.mitre.org/techniques/T1564/003/

Modify Registry(T1112) — https://attack.mitre.org/techniques/T1112/

Obfuscated Files or Information: Software Packing(T1406/002) — https://attack.mitre.org/techniques/T1406/002/

System Network Connections Discovery(T1049) — https://attack.mitre.org/techniques/T1049/

Template Injection (T1221) – https://attack.mitre.org/techniques/T1221/ (The new TTP!)

IOCs

Hashes (SHA-256)

Email – 16e6dfd67d5049ffedb8c55bee6ad80fc0283757bc60d4f12c56675b1da5bf61

Docx – 1abf56bc5fbf84805ed0fbf28e7f986c7bb2833972793252f3e358b13b638bb1

Injected ZIP – 95898c9abce738ca53e44290f4d4aa4e8486398de3163e3482f510633d50ee6c

LNK file – d07323226c7be1a38ffd8716bc7d77bdb226b81fd6ccd493c55b2711014c0188

Final ZIP – 94499196a62341b4f1cd10f3e1ba6003d0c4db66c1eb0d1b7e66b7eb4f2b67b6

Client32.exe – 89f0c8f170fe9ea28b1056517160e92e2d7d4e8aa81f4ed696932230413a6ce1

URLs and Hostnames

yourownmart[.]com/solar[.]txt

firstieragency[.]com/depbrndksokkkdkxoqnazneifidmyyjdpji[.]txt

yourownmart[.]com

firstieragency[.]com

parabmasale[.]com

tapouttv28[.]com

IP Addresses

192[.]236[.]192[.]48

173[.]252[.]167[.]50

199[.]188[.]205[.]15

46[.]105[.]141[.]54

Others

Message ID contains: “sendinblue.com”

Return Path contains: “sender-sib.com”