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.

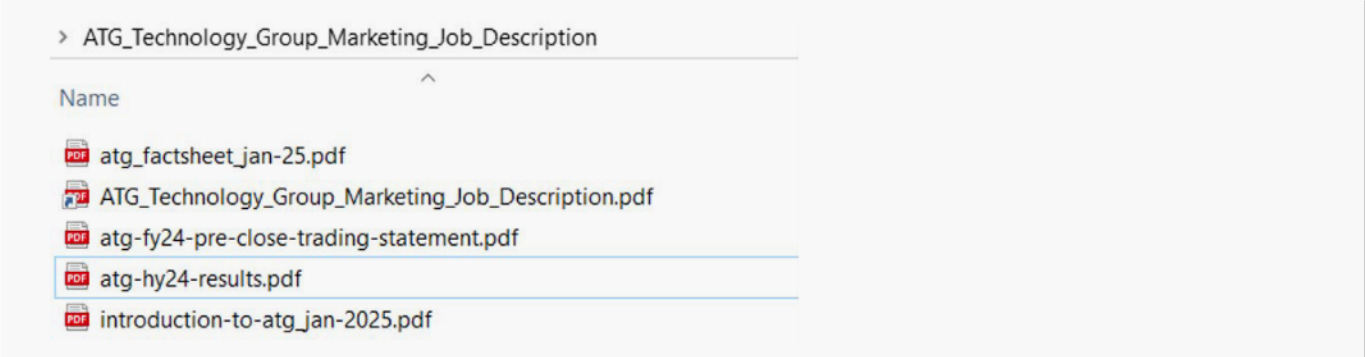

Figure 1: Content of the ZIP files

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.

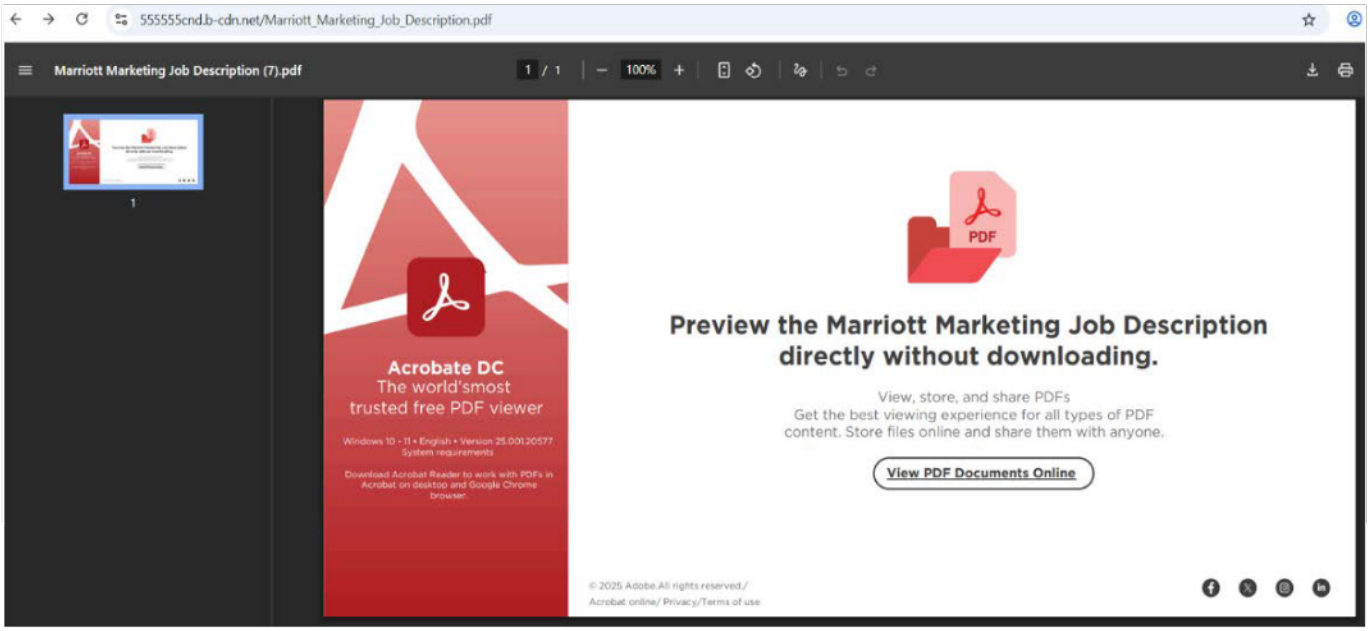

Figure 2: Lure Document

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.

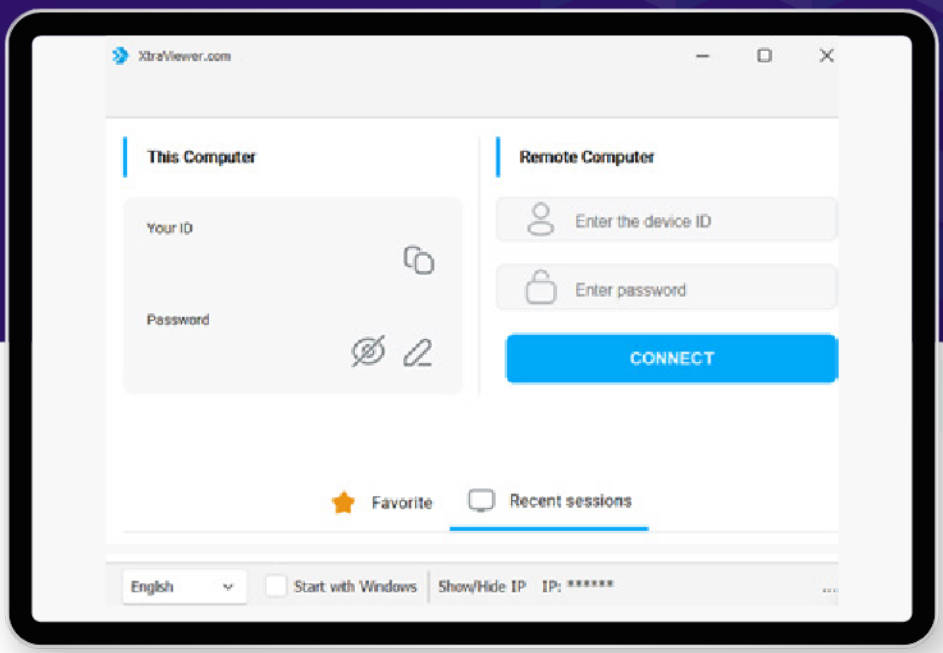

Figure 3 - XtraViewer Login Page

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.

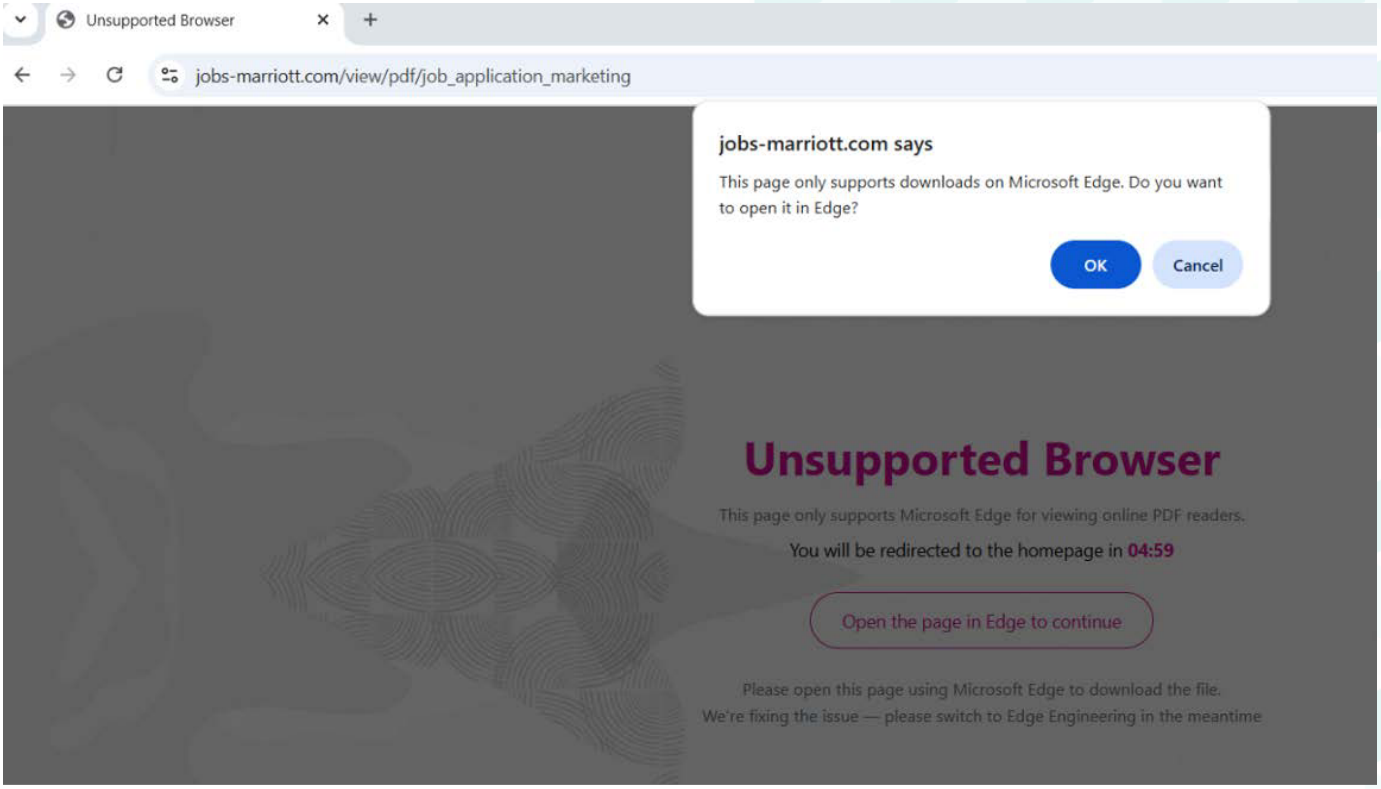

Figure 4 - Unsupported Browser Page

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.

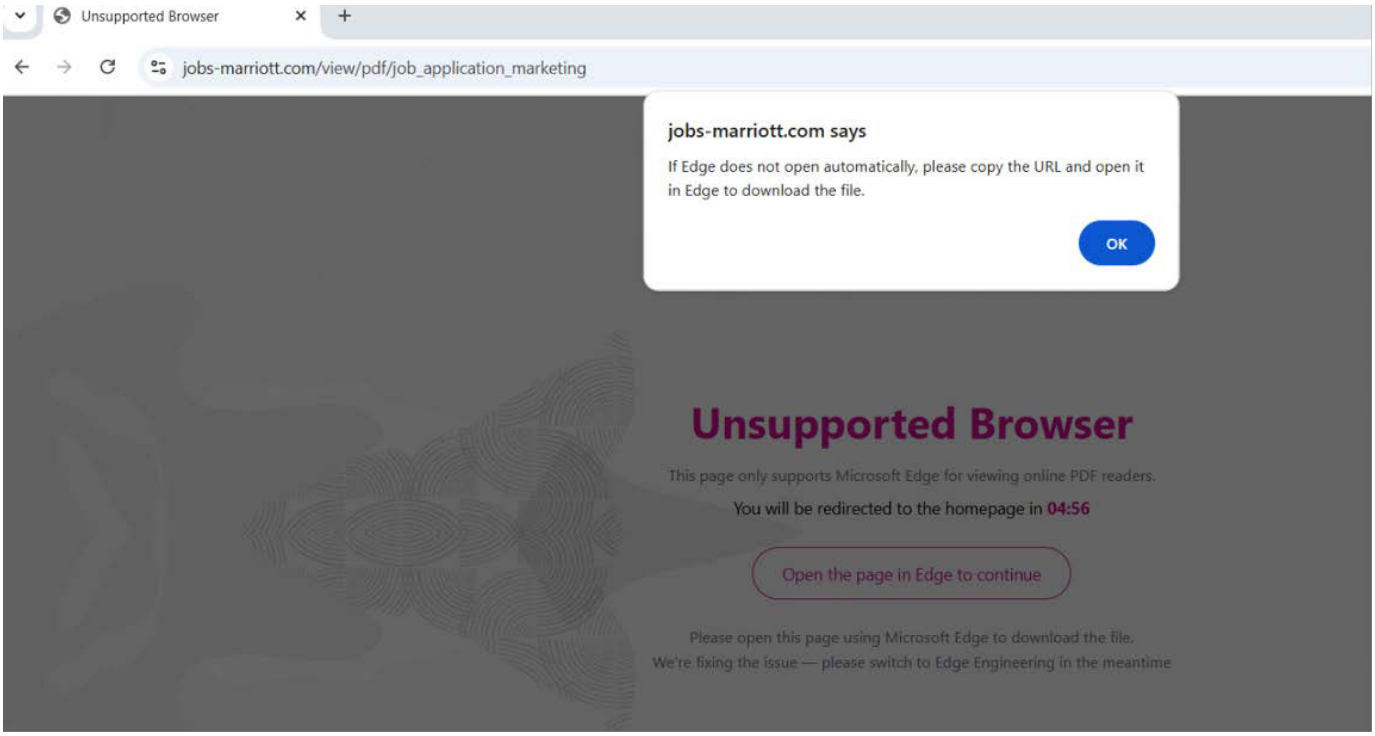

Figure 5- Unsupported Browser Page

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.

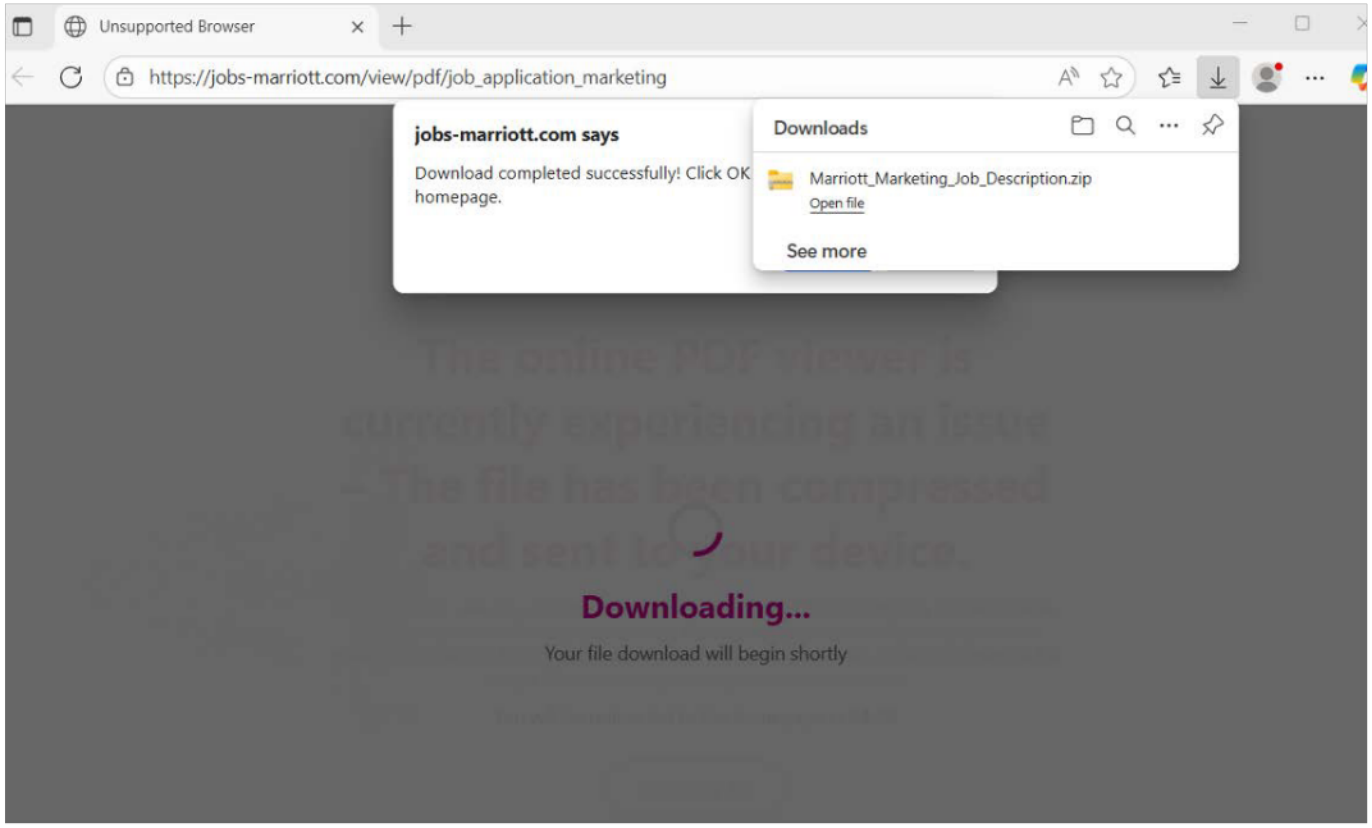

Figure 6 - Malicious ZIP file Download

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.

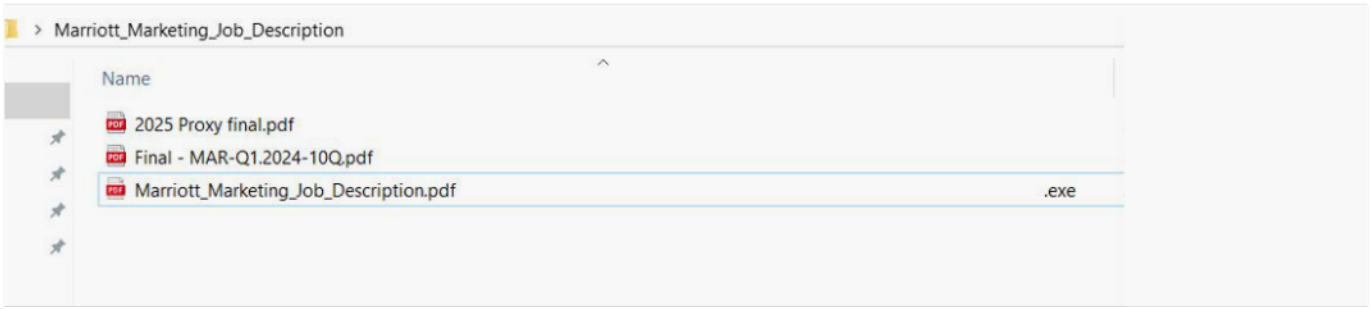

Figure 7 - Content of the zip file

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.

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”.

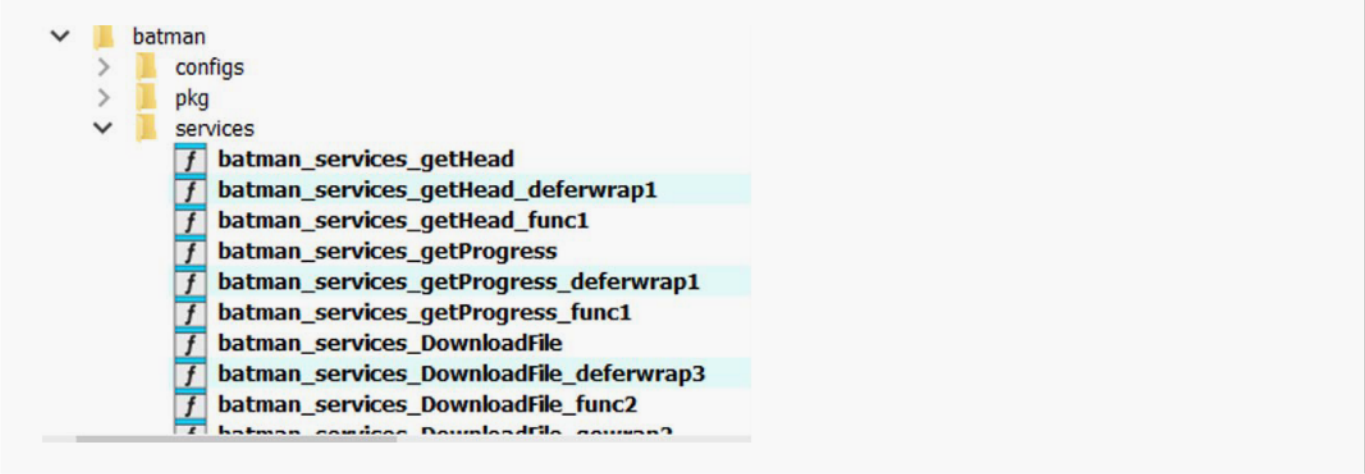

Figure 10 - Vampire Bot Functions

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.

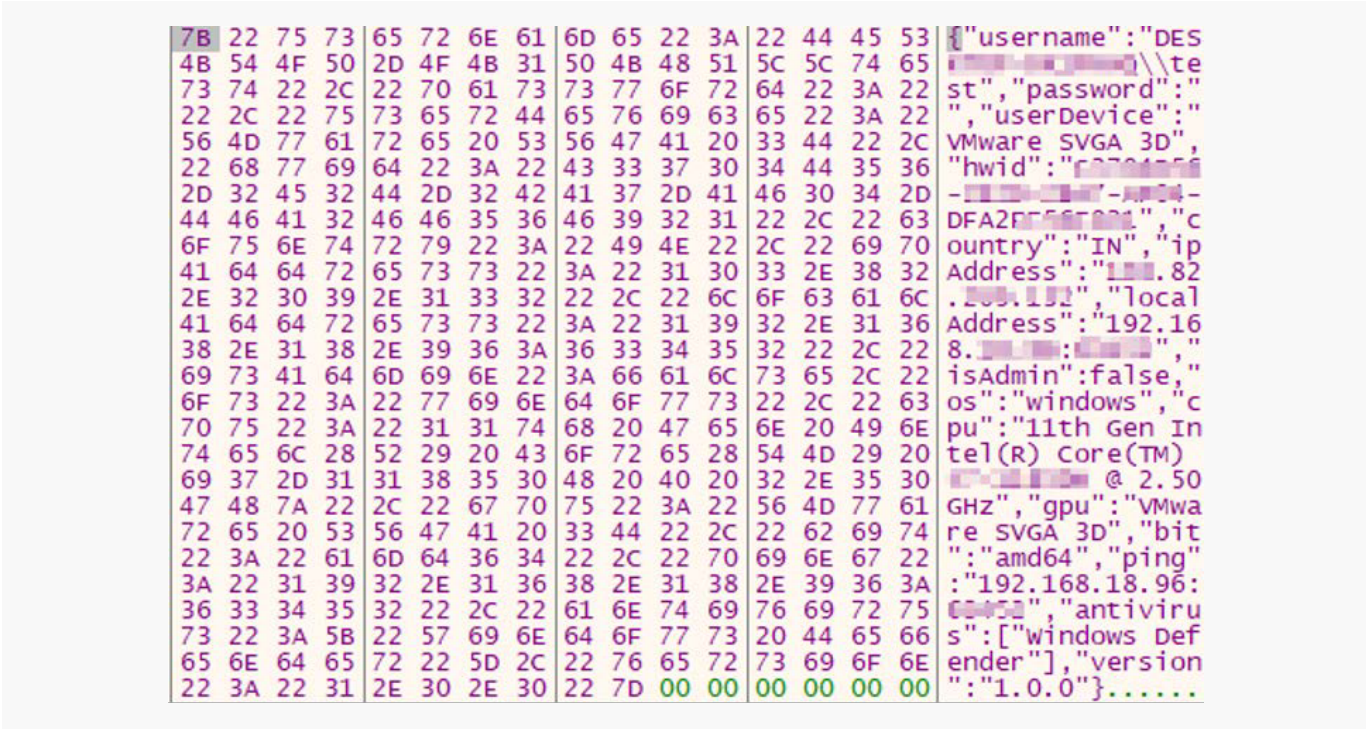

Figure 11 – Initial Beacon

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.

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.

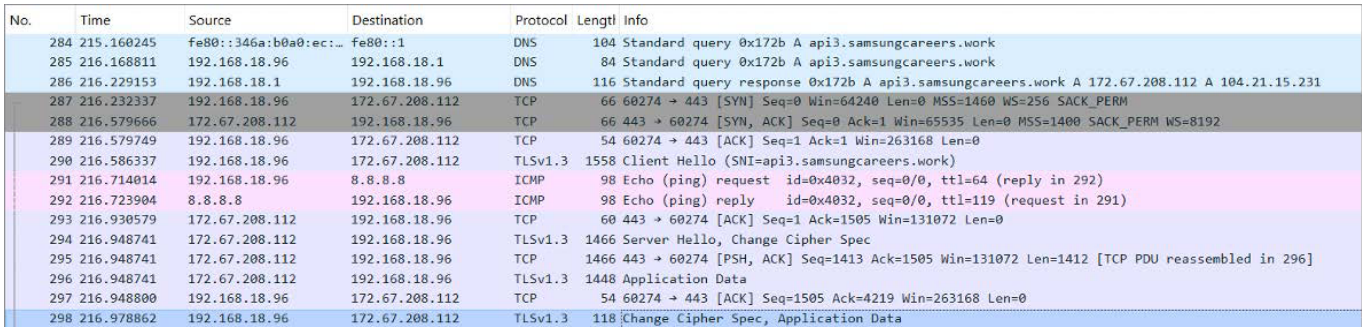

Figure 13 - Exfiltration

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.

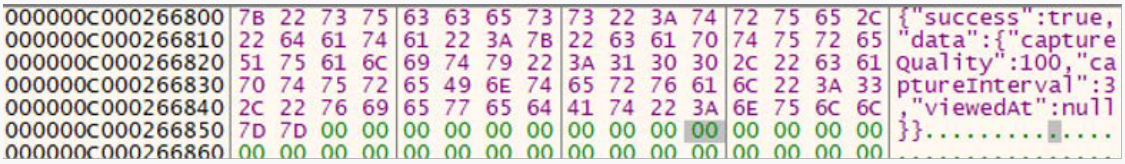

Figure 14 -Configuration Details

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.

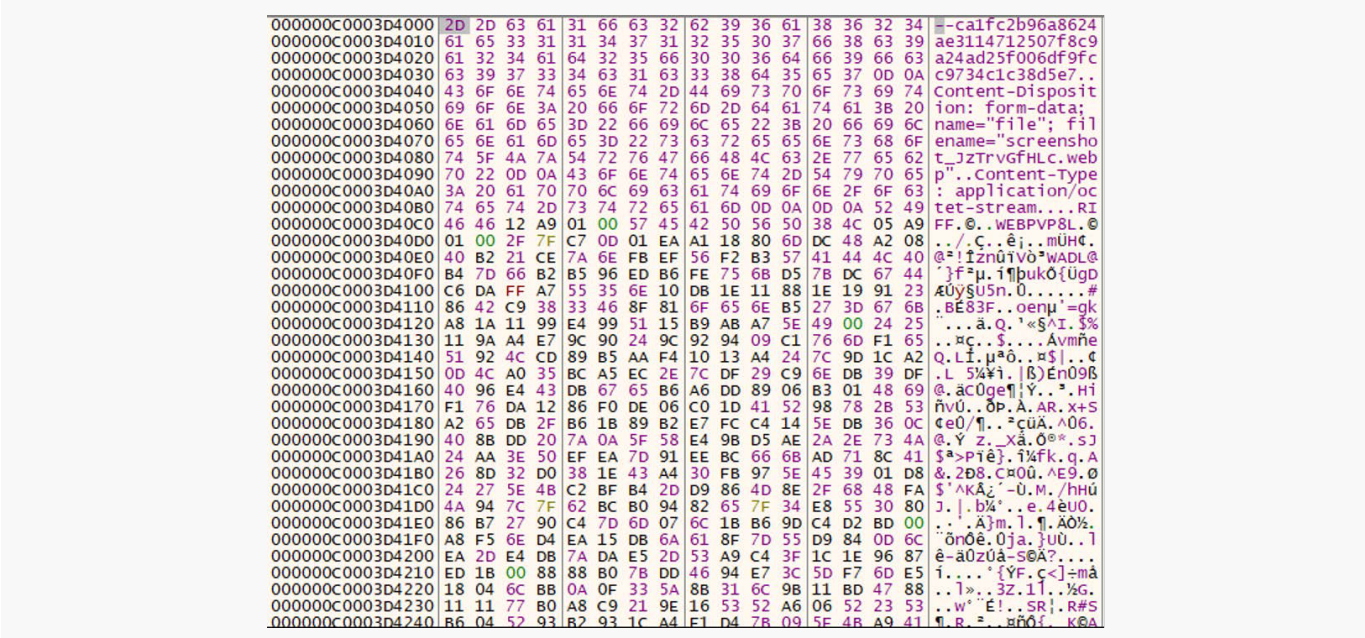

Figure 15 – Stolen Images Staged for Exfiltration

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.

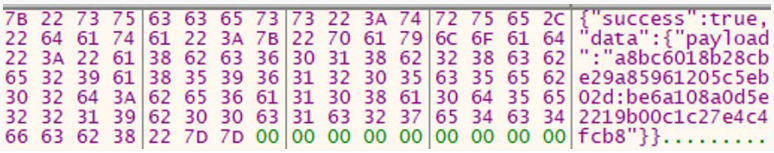

Figure 16 - C&C Response

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.

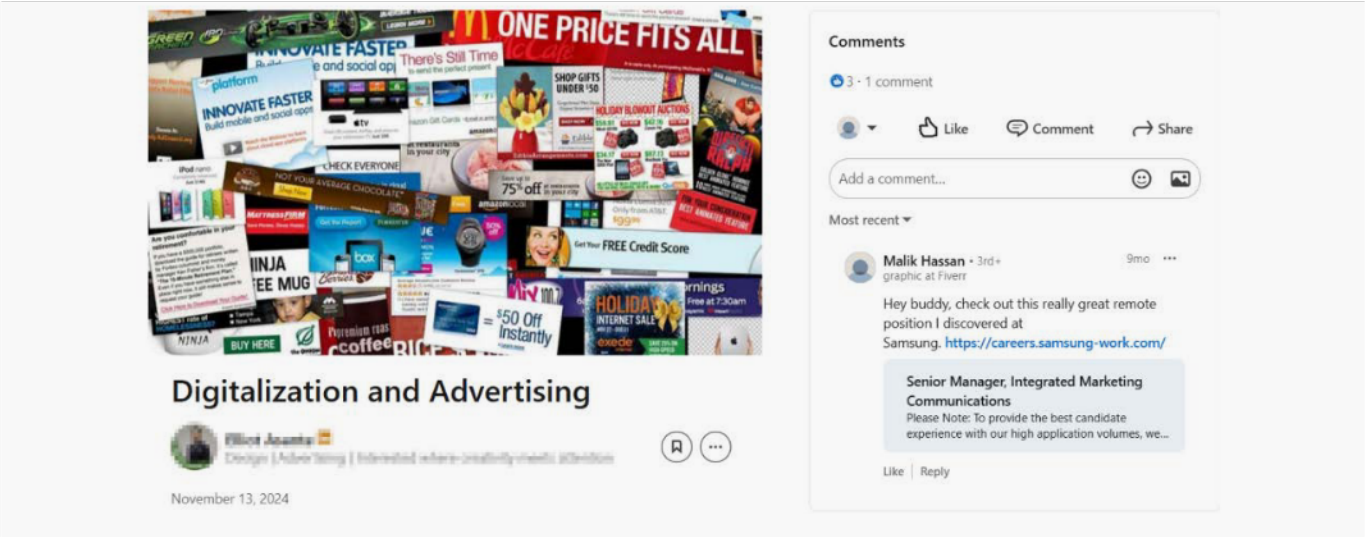

Figure 18 - Download from URL and Execute

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