ShelbyC2: Analysis of Espionage Risks Targeting Critical Infrastructure in the UAE

By Mario Rojas, Senior Security Researcher, ORYXLABS

Executive Summary

ShelbyC2, the central backdoor component within the Shelby malware family, was recently discovered by Elastic Security Labs during an investigation into the REF8685 intrusion .campaign

The Shelby malware family comprises two main modules: ShelbyLoader and ShelbyC2. This malware has targeted critical sectors in Iraq and potentially the UAE, with a particular .emphasis on telecommunications and transportation infrastructure

ShelbyC2 distinguishes itself through an innovative yet risky command-and-control (C2) mechanism, leveraging GitHub repositories for C2 operations, data exfiltration, and command retrieval. However, attackers inadvertently exposed sensitive GitHub Personal .Access Tokens (PATs), introducing significant operational security risks

This intelligence summary provides strategic insights into ShelbyC2, its implications for UAE-based organisations, threat analysts, and cybersecurity leadership, along with targeted .mitigation strategies

Threat actor profile and strategic context

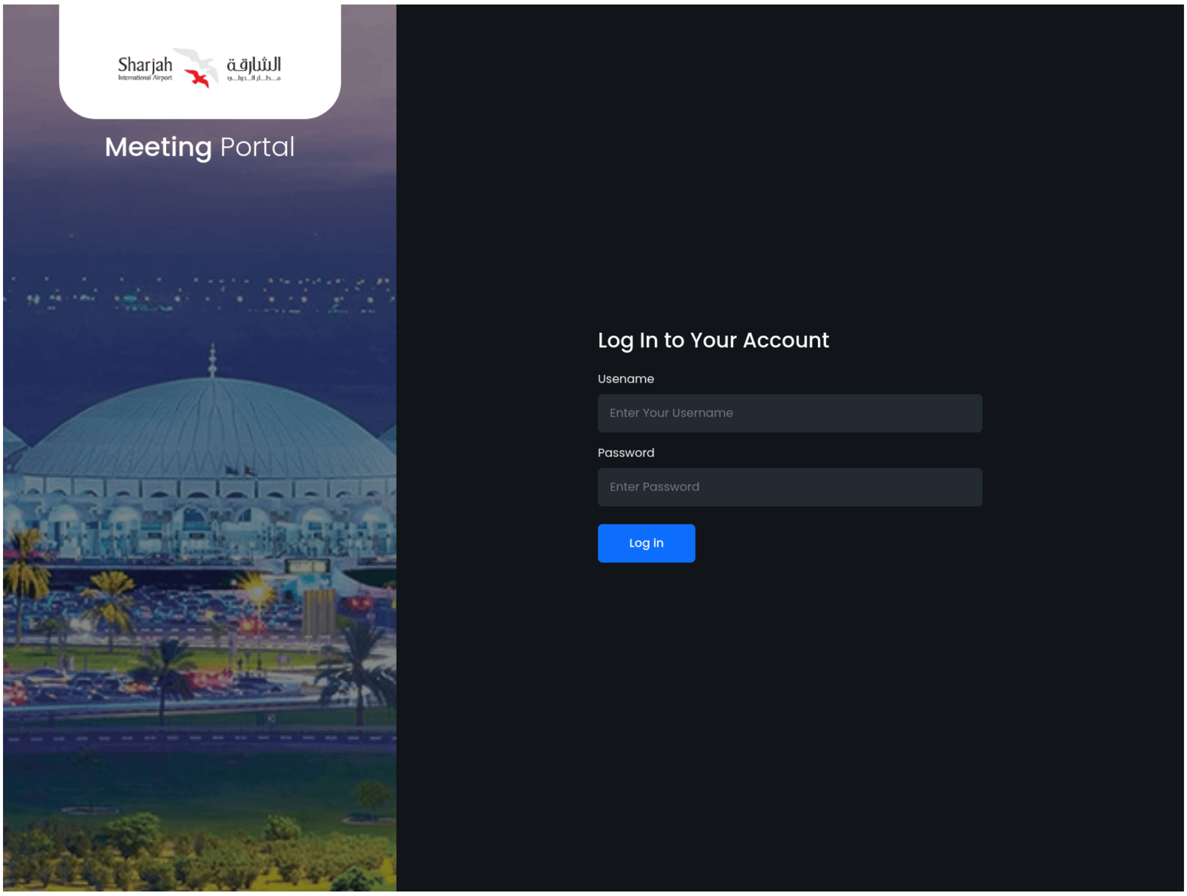
Elastic Security Labs has attributed ShelbyC2 to threat actor REF8685, known for its highly .targeted and sophisticated intrusion campaigns

A critical element of this campaign involved compromising legitimate email credentials from within targeted organisations, enabling internally originated phishing attacks that .bypass traditional security controls

The target selection indicates potential espionage motivations rather than financial gain, .specifically focusing on critical infrastructure in the Middle East

:Known targets include

- .An Iraq-based telecommunications company as the primary target
- .Potentially Sharjah Airport, a key international air transport hub in the UAE



Log In to Your Account

Usename

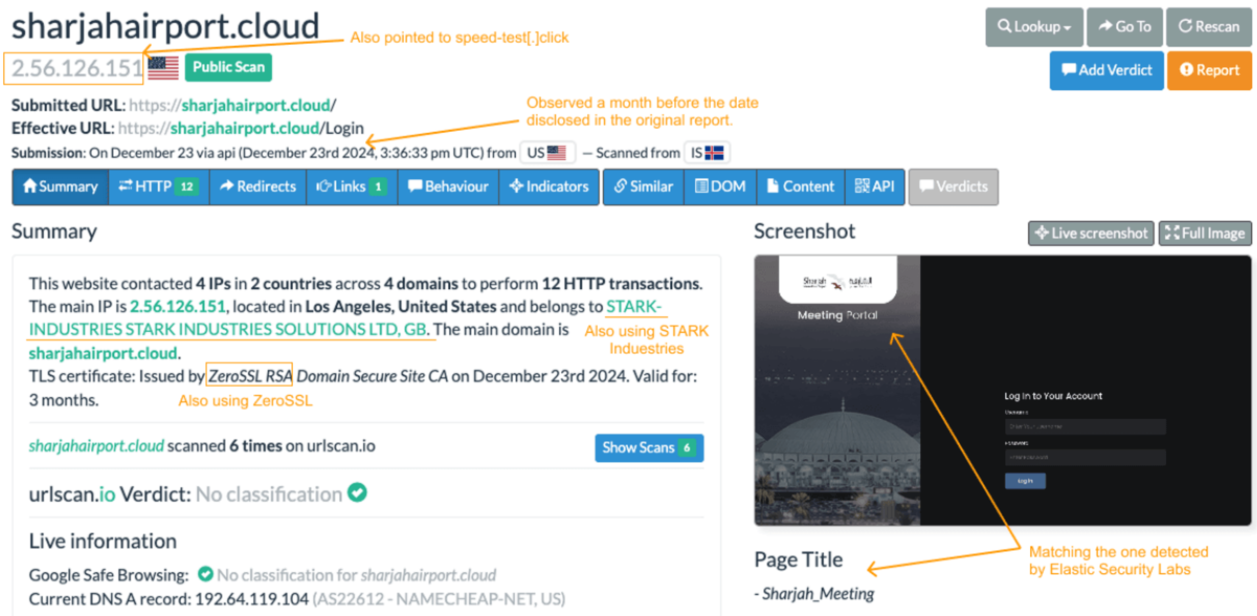
Enter Your Username

Password

Enter Password

It is important to clarify that the identification of phishing pages targeting Sharjah Airport does not confirm an actual breach or successful attack, but rather raises awareness of a .potential risk that should be closely monitored

Elastic Security Labs identified the subdomain portal.sharjahairport[.]cloud directing traffic briefly to IP 2.56.126[.]188 between 23–25 January 2025, before switching to IP 172.86.68[.]55. However, independent analysis has uncovered earlier activity indicating sharjahairport.cloud pointing to IP 2.56.126[.]151 as early as 23 December 2024. This expands the potential operational timeline and suggests prolonged planning and .reconnaissance phases



sharjahairport.cloud

2.56.126.151

Also pointed to speed-test[.]click

Submitted URL: https://sharjahairport.cloud/

Effective URL: https://sharjahairport.cloud/Login

Submission: On December 23 via api (December 23rd 2024, 3:36:33 pm UTC) from US — Scanned from IS

Observed a month before the date disclosed in the original report.

Summary

This website contacted **4 IPs** in **2 countries** across **4 domains** to perform **12 HTTP transactions.** The main IP is **2.56.126.151**, located in **Los Angeles, United States** and belongs to STARK-INDUSTRIES STARK INDUSTRIES SOLUTIONS LTD, GB. The main domain is **sharjahairport.cloud**.

Also using STARK Industries

TLS certificate: Issued by *ZeroSSL RSA Domain Secure Site CA* on December 23rd 2024. Valid for: 3 months.

Also using ZeroSSL

sharjahairport.cloud scanned **6 times** on urlscan.io

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for *sharjahairport.cloud*

Current DNS A record: 192.64.119.104 (AS22612 - NAMECHEAP-NET, US)

Screenshot

Page Title

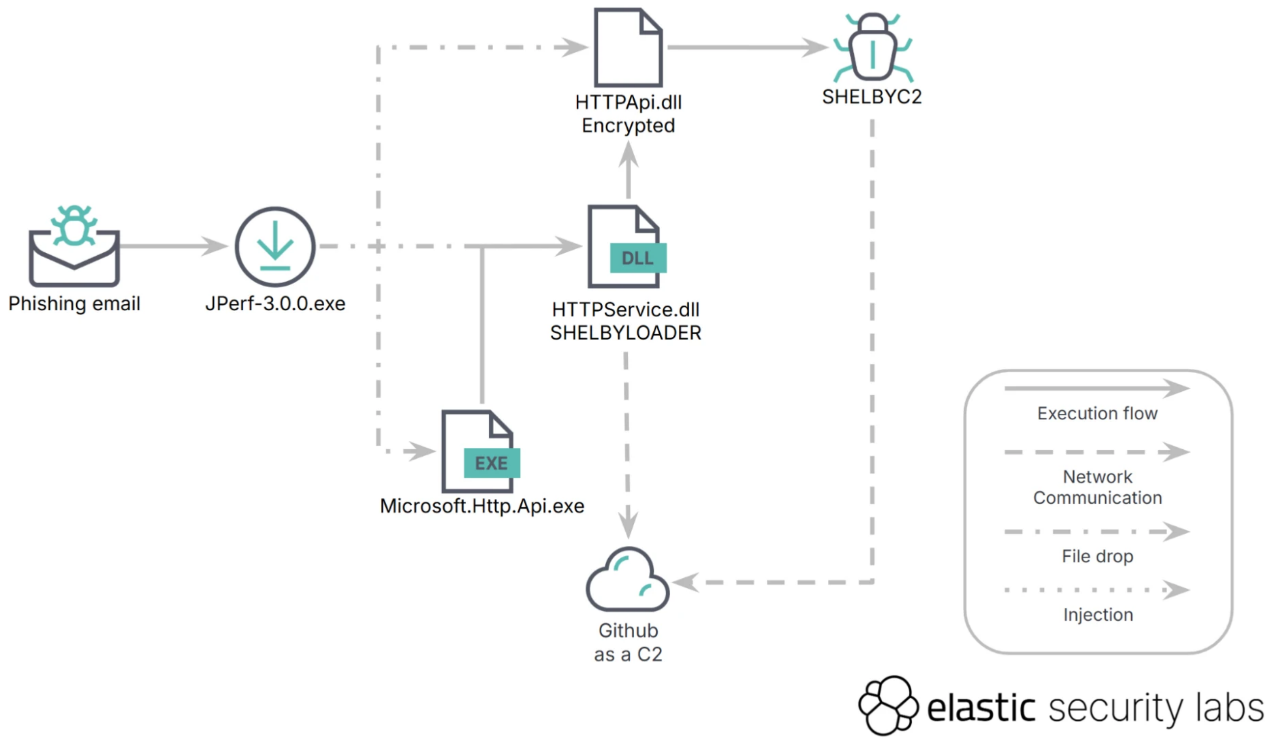
- *Sharjah_Meeting*

Matching the one detected by Elastic Security Labs

ShelbyC2 leverages hosting infrastructure predominantly sourced from Stark Industries (AS44477), highlighting intentional reliance on providers known for leniency and ".anonymity, which we describe as "dangerous neighbourhoods

Technical analysis of the attack chain

ShelbyC2 employs highly tailored spear-phishing emails containing malicious ZIP files as .initial infection vectors



Source: Elastic Security Labs

:Key insights into its operational tactics include

- **GitHub-based command-and-control:** Unlike traditional malware relying on dedicated infrastructure, ShelbyC2 uses GitHub repositories to host commands, exfiltrate data, and dynamically retrieve operational instructions, presenting a .significant detection and mitigation challenge
- **Reflective payload execution:** Payloads are dynamically decrypted and executed .directly in memory, effectively bypassing many endpoint protection mechanisms
- **Advanced anti-analysis techniques:** ShelbyC2 integrates sandbox evasion methodologies such as detailed system enumeration, process monitoring, and .environment checks, further complicating detection and analysis

Interestingly, attackers' operational sophistication is undermined by embedding sensitive GitHub PAT tokens within their malware, highlighting operational immaturity and offering .unique counter-threat intelligence opportunities

Additionally, ShelbyC2's dynamically generated domain patterns resemble Domain .Generation Algorithms (DGA), a detection gap for many current DNS security solutions

?Why is this important for UAE organisations

The UAE's strategic positioning in global trade, aviation, and telecommunications makes it a .prime target for cyber espionage and sabotage campaigns

The sophisticated operational characteristics of ShelbyC2, including the targeting of local .critical infrastructure, signal potential high-impact breaches

Understanding ShelbyC2's unique characteristics and operational shortcomings is crucial .for UAE organisations to proactively enhance defences and maintain operational resilience

(Indicators of compromise (IoCs

Malicious domains and C2 infrastructure

Indicator	Type
arthurshelby[.]click	Domain
speed-test[.]click	Domain
sharjahairport[.]cloud	Domain
151[.]2.56.126	IPv4
188[.]2.56.126	IPv4
55[.]172.86.68	IPv4
58[.]195.16.74	IPv4

GitHub accounts

Indicator
github[.]com/johnshelllby
github[.]com/arturshellby

File hashes

Hash	Indicator
0e25efeb4e3304815f9e51c1d9bd3a2e2a23ece3a32f0b47f829536f71ead17a	details.zip
feb5d225fa38efe2a627ddfbe9654bf59c171ac0742cd565b7a5f22b45a4cc3a	JPerf-3.0.0.exe
0354862d83a61c8e69adc3e65f6e5c921523eff829ef1b169e4f0f143b04091f	HTTPService.dll
fb8d4c24bcfd853edb15c5c4096723b239f03255f17cec42f2d881f5f31b6025	HTTPApi.dll
472e685e7994f51bbb259be9c61f01b8b8f35d20030f03215ce205993dbad7f5	JPerf-3.0.0.zip
5c384109d3e578a0107e8518bcb91cd63f6926f0c0d0e01525d34a734445685c	Setup.exe
e51c6f0fbc5a7e0b03a0d6e1e1d26ab566d606b551c785bf882e9a02f04c862b	NewrozSpeedtest.zip

Recommendations for mitigation and risk reduction

:Organisations should adopt a proactive, intelligence-led defensive posture

- **Credential breach monitoring:** Leverage digital attack surface management solutions such as Discovery to proactively identify compromised credentials leveraged .in phishing campaigns
- **Enhanced DNS security:** Implement robust DNS defences such as DNS Firewall to .detect and block anomalous, DGA-like domain resolution attempts
- **Endpoint behaviour analytics:** Utilise advanced endpoint protection solutions capable of identifying memory-based reflective code execution and sandbox evasion .behaviours
- **GitHub API traffic monitoring:** Continuously monitor GitHub-related API .interactions to swiftly identify anomalous activities indicative of ShelbyC2 operations
- **Infrastructure provider intelligence:** Conduct targeted assessments of hosting providers historically associated with malicious activities, incorporating findings into .proactive threat-hunting initiatives

Conclusion

ShelbyC2 exemplifies the evolving threat landscape through its sophisticated yet .operationally risky approach

For UAE organisations, it underscores the imperative to transition toward proactive and intelligence-driven cybersecurity strategies. Recognising attacker behaviours and adapting .defences accordingly is essential

The discovery and analysis of ShelbyC2 highlight how attackers continue to evolve, blending novel techniques with traditional espionage objectives. UAE-based organisations must not only anticipate increasingly sophisticated technical threats but also adapt to adversaries’ evolving operational security practices. Effective cybersecurity requires .understanding the attacker’s mindset, methods, and mistakes

.Remember, there’s always more intelligence to uncover