Threat Intelligence Digest: TheWizards – Adversary-in-the-Middle Attacks



By Mario Rojas, Senior Security Researcher.

Since mid-2022, the advanced persistent threat (APT) group, TheWizards, has been observed conducting global operations (including observed campaigns against UAE organisations) using an advanced adversary-in-the-middle (AitM) tactic known as IPv6 SLAAC spoofing

By masquerading as legitimate network routers, the group intercepts and redirects software update traffic for widespread third-party applications, deploying the modular WizardNet backdoor.

A recent report by ESET's research team confirms ongoing activity and newly observed UAE targets. In this analysis, we will examine TheWizards' strategic objectives and SLAAC spoofing methodology, catalogue clear indicators of compromise (IoCs), and provide a step-by-step defence strategy to enable UAE defenders to detect, contain and eradicate these stealthy attacks.

Threat actor profile and strategic context

TheWizards emerged in mid-2022 when security teams observed unusual IPv6 traffic anomalies across multiple regions. ESET's analysis associates the group's command-and-control servers with infrastructure maintained by Sichuan Dianke Network Security Technology Co., Ltd., the creators of the DarkNimbus toolkit, suggesting shared development resources.

Rather than relying on phishing or endpoint exploits alone, TheWizards specialises in network-level adversary-in-the-middle operations via IPv6 SLAAC spoofing.

Motivations and tradecraft

- **Espionage focus:** Seeks intelligence on geopolitical policies and commercial projects.
- **Network-native AitM:** Exploits IPv6 SLAAC rather than phishing, reducing detection risk.
- **Modular implantation:** WizardNet's plugin design enables tailored reconnaissance, lateral movement, and data exfiltration per target.

The threat actor has recently refined its SLAAC spoofing frequency and RA packet crafting to bypass security tools and evade behavioural EDR signatures, an evolution that suggests ongoing red-team-style testing and iterative development.

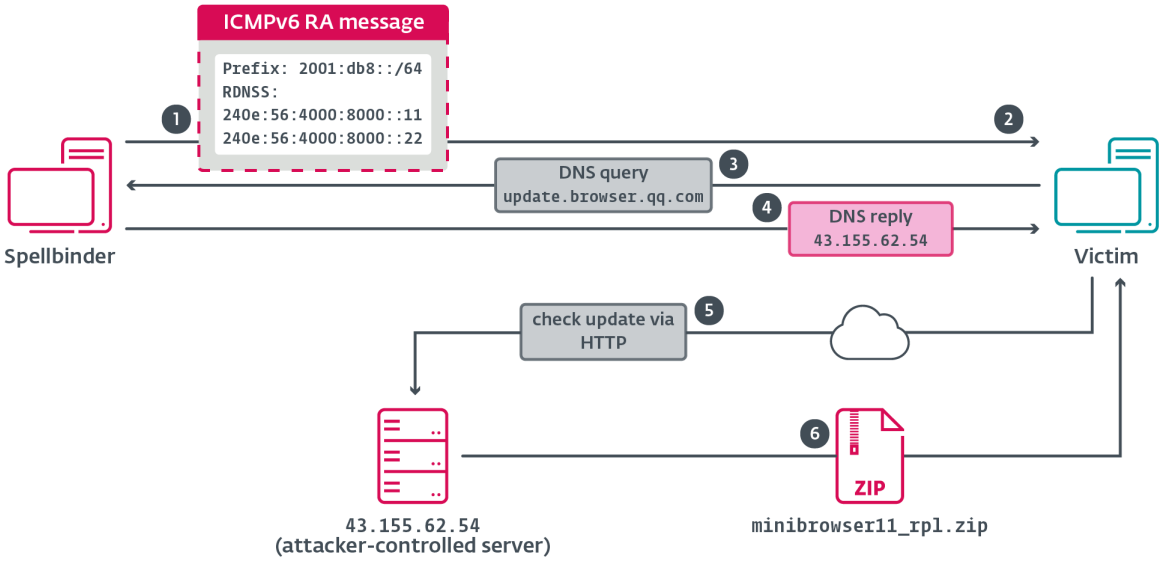
Geographic focus

While ESET confirms that TheWizards has been observed targeting organisations in the UAE, the report does not specify sectors. Their broader campaigns have previously targeted individuals, gambling companies and organisations in other regions, including the Philippines, Cambodia, mainland China, and Hong Kong.

Threat actor's arsenal

Technical analysis

SLAAC spoofing with Spellbinder



1. Spellbinder sends ICMPv6 RA message to all nodes in the network
2. IPv4- and IPv6-enabled machine receives the message, and autoconfigures using SLAAC
3. Victim machine sends DNS request over IPv6 to the machine running Spellbinder
4. Spellbinder replies with the IPv4 address of the malicious server controlled by attackers
5. Software running on victim machine sends HTTP request over IPv4 to malicious server, asking for updates
6. Malicious server replies with the malicious payload

source: welivesecurity

What is SLAAC? Stateless address autoconfiguration (SLAAC) is an IPv6 feature enabling devices to auto-assign addresses based on router advertisements (RAs). The threat actor exploits SLAAC by broadcasting malicious RAs every 200 ms, compelling hosts to adopt attacker-controlled IPv6 prefixes and DNS servers.

The challenges with SLAAC often stem from dual-stack environments where IPv4 and IPv6 run side by side. Administrators may focus on IPv4 controls and overlook IPv6 configurations, leaving devices to trust any RA they receive. SLAAC's automatic nature means misconfigured or malicious RAs can silently redirect traffic without triggering traditional IPv4 security alerts.

Spellbinder

- **Function:** Automates ICMPv6 RA spoofing to redirect IPv6 traffic.
- **Evasion:** Crafts RA packets with realistic lifetimes and option fields to mimic legitimate routers and avoid heuristic blocking.

WizardNet backdoor

WizardNet modules deploy via hijacked updates and execute entirely in memory.

- **Payload loader:** Decrypts .NET modules on-the-fly; no disk artefacts.
- **Reconnaissance:** Harvests host telemetry (OS details, installed software, network interfaces).

- **Encrypted C2:** Uses AES over non-standard ports with intermittent beaconing to blend with normal traffic.
- **Evading forensics:** Hooks kernel call-backs to disable AMSI, clear event logs, and mask network sockets.

Attack flow

- **Initial access:** A user endpoint is compromised via phishing or exploitation of a vulnerable updater component, where Spellbinder is delivered under the guise of a legitimate installer.
- **AitM deployment:** Spellbinder broadcasts spoofed ICMPv6 RAs every 200 ms, coercing hosts to auto-configure attacker-controlled IPv6 settings and reroute network and DNS traffic through the malicious host.
- **Update hijack:** Victim machines request software updates from vendor domains (e.g., sogou.com, qq.com). These DNS queries are intercepted and resolved to attacker-controlled IPs, causing the download of malicious payloads instead of genuine patches.
- **Backdoor installation:** The downloaded payload deploys the WizardNet backdoor in memory, establishes persistence via registry keys and mutexes, and disables defences such as AMSI and event logging.
- **Lateral movement and exfiltration:** Using in-memory reconnaissance data (OS versions, network topology), attackers move laterally across network segments, collect sensitive files, and exfiltrate them over encrypted C2 channels to evade detection.

Why is this important for UAE organisations?

The UAE's status as a nexus for global trade, finance, and technology positions its organisations as prime targets for sophisticated cyber espionage and sabotage attacks.

TheWizards' manipulation of network protocols and hijacking of software update processes demonstrate how advanced tactics can bypass traditional defences.

UAE defenders must understand these methods and implement recommended controls to maintain operational resilience and protect critical national and commercial interests.

Indicators of compromise (IoCs)

Infrastructure

File hashes

You can also access the full list of IOCs on ESET's GitHub.

Recommendations for risk mitigation and reduction

1. Network controls

- **RA-Guard enforcement:** Implement at all edge switches to block unauthorised ICMPv6 RAs.
- **IPv6 hygiene:**
  - Disable SLAAC on servers
  - Require authenticated DHCPv6 RAs with RA-Guard policies.
- **Micro segmentation:**
  - Enforce strict IPv6 traffic segmentation
  - Limit host-to-host communication via ACLs.

2. Endpoint and update security

- **Secure update pipeline:** Proxy third-party updates through a signed internal repository with certificate pinning and code-signing verification.
- **Behavioural EDR/XDR:** Tune detections for abnormal ICMPv6 activity, in-memory module loads, and atypical AES traffic patterns.
- **Application whitelisting:** Enforce SHA-256 code-signing policies for all executables and installers.

3. Threat intelligence and operations

- **DNS FIREWALL:** Implement robust DNS defences such as DNS FIREWALL to detect and block malicious domain lookups in real time.
- **Digital risk monitoring:** Use Discovery to track exposed assets and credentials.
- **IoC automation:** Feed IoCs into SOAR for contextual alerts and rapid containment.
- **Tabletop exercises:** Simulate IPv6 AitM scenarios to validate response readiness.

Conclusion

TheWizards' use of IPv6 SLAAC spoofing to hijack software update streams underscores a critical blind spot in many security architectures. UAE organisations must move beyond traditional perimeter defences by first auditing and locking down IPv6 configurations (disable SLAAC where unnecessary and enforce RA policies) to eliminate easy AitM entry points.

At the same time, embedding threat hunting for anomalous ICMPv6 activity would catch early signs of network-level intrusion that would otherwise slip through.

Operationalising DNS FIREWALL as both a blocker and sensor against known malicious domains turns your infrastructure into an active first line of defence.

Lastly, regular tabletop exercises simulating a complete SLAAC spoofing attack—from bypassing RA-Guard to deploying WizardNet—are essential to ensure teams can move beyond theoretical knowledge and respond quickly and effectively with detection, containment, and recovery in real-world situations.

There’s always more intelligence to uncover.