we secure



Operation “Silent Portal”: How We Secure Eradicated a Stealthy Keylogger Campaign

October 2025

BACKGROUND

In mid-2025, *We Secure* was engaged by a **public sector organization** that began noticing **unusual login patterns across its internal infrastructure**.

The organization was **not an existing We Secure client** at the time and sought immediate support from our **Digital Forensics and Incident Response (DFIR)** team to investigate and contain the incident.
Due to confidentiality requirements, **the client's identity cannot be disclosed**.

During the engagement, the **We Secure DFIR team aligned with the customer's existing security stack**, which was built on **Microsoft technologies**.

Case Information	
Category	Incident Response & Digital Forensic
Technology stack	Microsoft
Industry	Public Sector
Region	Europe
Engagement Type	Emergency Response (Non-Retainer Client)

Summary of Findings

- The attacker remained undetected for approximately **30 days**.
- Initial access was gained via **SQL injection** on a public web application.
- **ShadowPad-style DLL loading** used to deploy a keylogger and multiple backdoors.
- Attribution consistent with **APT41** activity patterns.
- Reverse-proxy tunnels were established for covert communication.

We Secure Response Timeline

Timeframe	Action
0-12 hours	Initial triage, containment of compromised accounts, and preservation of forensic evidence
12-36 hours	Deep-dive investigation, IOC discovery, and reconstruction of intrusion chain
36-72 hours	Eradication of malware and backdoors, web application patching, credential resets, and post-incident validation

Key Achievements

- Complete containment and remediation achieved in **under 72 hours**.
- All **Indicators of Compromise (IOCs)** identified and validated.
- **No disruption** to business operations during the response.
- **Vulnerable web application patched** and proactive monitoring implemented.

Outcome

Within three days of engagement, the **We Secure DFIR** team eliminated the attacker's presence and restored full confidence in the infrastructure.
All malicious DLL loaders, backdoors, and reverse-proxy tunnels were eradicated.
The exploited web application was remediated, credentials rotated, and continuous monitoring implemented.

Post-incident validation confirmed no **lateral movement, data exfiltration, or ongoing compromise**.

Lessons Learned

- Unusual login activity often serves as the earliest and most valuable indicator of compromise.
- Advanced threat groups such as APT41 combine stealthy web exploitation with long-term persistence mechanisms.

Conclusion

Operation Silent Portal demonstrates the power of coordinated incident response and forensic precision.
Although **We Secure** was not a managed service provider for the organization, our **DFIR team's structured approach and 72 hour response window** turned a month long intrusion into a verified, secure recovery.

Through disciplined investigation and mastery of modern security technologies, We Secure restored operational integrity and confidence proving that even advanced, state-linked intrusions can be eradicated when expertise meets speed.

Need Emergency Support?

If your organization is facing a cybersecurity incident and needs immediate response assistance, **contact the We Secure Incident Response Team**.
Our experts are available 24/7 to help you contain threats, recover safely, and protect your environment.

we-secure.eu