مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

OilRig Cyber Espionage Threat

Tracking #:432316669

Date:26-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that OilRig, also known as APT34 or Helix Kitten, is a threat actor targeting critical sectors in the Middle East through sophisticated cyber espionage campaigns. This advisory outlines their tactics, techniques, and procedures (TTPs) to help organizations enhance their defenses.

TECHNICAL DETAILS:

OilRig, also known as APT34 or Helix Kitten, is a threat actor that has been active since at least 2016. OilRig specializes in advanced cyber-espionage, particularly targeting critical sectors such as government entities, energy, and technology providers in the Middle East. The group employs highly adaptive tactics, techniques, and procedures (TTPs), leveraging sophisticated malware, zero-day vulnerabilities, and supply chain compromises to achieve its geopolitical objectives.

1. **Evolution of Tools and Tactics**:
   - **Initial Toolset**: Early campaigns featured the Helminth backdoor, enabling stealthy access and long-term persistence.
   - **Advanced Payloads**: Recent use of malware like QUADAGENT, ISMAgent, and STEALHOOK demonstrates technical sophistication and adaptability.
   - **Vulnerability Exploitation**: Exploits of vulnerabilities, such as CVE-2024-30088 (Windows Kernel), provide SYSTEM-level access for deploying custom tools.
2. **Notable Campaigns**:
   - **Supply Chain Attacks**: Utilizing compromised accounts within technology providers for broader infiltration.
   - **QUADAGENT Campaign (2018)**: Leveraged PowerShell-based malware for stealthy network infiltration.
3. **TTP Highlights**:
   - **Initial Access**: Spearphishing via platforms like LinkedIn to steal credentials.
   - **Execution**: PowerShell scripting for stealthy command execution.
   - **Persistence**: Scheduled tasks and obfuscated payloads for enduring access.
   - **Defense Evasion**: Techniques like base64 encoding and Invoke-Obfuscation bypass detection systems.
   - **Credential Access**: Use of tools like Mimikatz and LaZagne for extracting plaintext credentials.
   - **Exfiltration**: Alternative protocols, such as FTP and DNS tunneling, for undetected data extraction.

Indicators of Compromise (IOCs):

File Name	Hash (SHA256)
QUADAGENT	d7130e42663e95d23c547d57e55099c239fa249ce3f6537b7f2a8033f3aa73de
OilRig ThreeDollars	1f6369b42a76d02f32558912b57ede4f5ff0a90b18d3b96a4fe24120fa2c300c
mscom.exe	0ca0febadb1024b0a8961f21edbf3f6df731ca4dd82702de3793e757687aefbc
People List.xls	9f31a1908afb23a1029c079ee9ba8bdf0f4c815addbe8eac85b4163e02b5e777
Dell.exe	5db93f1e882f4d7d6a9669f8b1ab091c0545e12a317ba94c1535eb86bc17bd5b

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures
- Implement robust email filtering and user awareness training
- Regularly patch and update systems, especially for critical vulnerabilities
- Deploy endpoint detection and response (EDR) solutions
- Monitor for suspicious PowerShell and scripting activities
- Implement strong access controls and multi-factor authentication
- Conduct regular security assessments and penetration testing

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.picussecurity.com/resource/blog/oilrig-exposed-tools-techniques-apt34