مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

ConnectWise RAT Malware Campaign

Tracking #:432317118

Date:24-04-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers reported a sophisticated malware campaign exploiting the ConnectWise remote access platform is actively targeting users worldwide.

TECHNICAL DETAILS:

ThreatMon has identified and analyzed a continuing malware campaign leveraging the ConnectWise remote access platform, now active into April 2025. The attackers are impersonating the U.S. Social Security Administration (SSA) to deliver malicious payloads via phishing emails and fraudulent websites. The campaign distributes a malicious executable file named tax_details202504-pdf.Client.exe under the guise of SSA documentation, which upon execution enables full system compromise and unauthorized remote access.

Key Observations:

- **Delivery Method**: Phishing emails and fake SSA-themed websites.
- **Payload**: Malicious file masquerading as a PDF (e.g., tax_details202504-pdf.Client.exe).
- **Infection Strategy**: Exploits Microsoft's ClickOnce technology and uses process hollowing with dfsvc.exe.
- **Persistence Mechanism**: Installs as a Windows service and modifies registry for Safe Mode execution.
- **Command & Control (C2)**: Communicates with C2 at admin.ratoscreenconne[.]com (IP: 45.81.23[.]35).
- **Capabilities**: Remote desktop access, screen/video capture, credential harvesting, and command execution.
- **Targets**: Government agencies, healthcare providers, legal and insurance firms, and educational institutions.

RECOMMENDATIONS:

- Deploy Advanced Email Filtering: Use secure email gateways with phishing, spoofing, and malware detection capabilities.
- Conduct Regular Phishing Simulations: Train staff to identify and report suspicious emails.
- Install and Maintain EDR/XDR: Use endpoint detection and response systems that can detect behaviors such as process injection, abnormal DLL usage, or suspicious file activity.
- Keep Systems Patched: Ensure operating systems, browsers, and third-party applications are up to date.
- Implement Least Privilege Principle: Users should have only the access necessary for their roles and use MFA for all remote access and privileged accounts.
- Block Known Malicious IPs and Domains: Use threat intelligence feeds to update network-level defenses.

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.

Indicators of Compromise:
Attached File

REFERENCES:

- https://github.com/ThreatMon/ThreatMon-Reports-IOC/tree/main/ConnectWise