مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Threat Actors targeting the Middle East with fake Palo Alto VPN

Tracking #:432316209

Date:02-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new malware campaign targeting users in the Middle East by disguising itself as the Palo Alto Networks GlobalProtect VPN client.

TECHNICAL DETAILS:

A new malware campaign has been observed targeting users in the Middle East, posing as the Palo Alto Networks GlobalProtect VPN tool. This malware presents a significant risk to organizations in the region due to its advanced capabilities and stealthy operations.

- **Malware Characteristics:**
  - The malware executes remote PowerShell commands, downloads and exfiltrates files, encrypts communications, and bypasses security measures like sandbox solutions.
  - It employs a two-stage process that allows it to connect to a command-and-control (C2) infrastructure, masquerading as a legitimate VPN portal.
- **Intrusion Vector:**
  - The precise method of initial intrusion is unknown but is suspected to involve phishing techniques to persuade users to install the fake GlobalProtect agent.
- **File Deployment:**
  - The malware installs a primary backdoor named GlobalProtect.exe, which initiates a "beaconing" process to alert the operators about the system's status.
  - Config files (RTime.conf and ApProcessId.conf) are created for sending system information to the C2 server, such as IP address and operating system details.
- **Evasion Techniques:**
  - This malware uses evasion techniques against behavior analysis and sandbox detection by checking file paths before executing its payload.
- **Infrastructure and Tactics:**
  - The malware employs a domain that resembles a legitimate VPN portal, seamlessly blending its activities with expected network traffic and enhancing its stealth.

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

- Review the attached Indicators of Compromise (IOCs) and implement the necessary security measures.
- **User Awareness:** Educate employees about the risks of phishing and the significance of verifying software origins before installation.
- **Maintain Updated Security Measures:** Ensure all security systems and software are up to date to recognize and block malicious activities.
- **Monitor Network Traffic:** Implement stringent monitoring for unusual network activities, especially connections to unknown URLs.
- **Incident Response Planning:** Have a response strategy in place should users

inadvertently install the malware, including isolating affected systems and analyzing network traffic.

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.trendmicro.com/en_us/research/24/h/threat-actors-target-middle-east-using-fake-tool.html