مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Eldorado – Ransomware targeting Windows and Linux

Tracking #:432316027

Date:08-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a new ransomware-as-a-service (RaaS) called Eldorado emerged in March and comes with locker variants for Linux and Windows.

TECHNICAL DETAILS:

A new ransomware-as-a-service (RaaS) called Eldorado emerged in March and comes with locker variants for Linux and Windows. The gang has already claimed 16 victims worldwide, in real estate, educational, healthcare, and manufacturing sectors.

Features:

- Eldorado is a Go-based ransomware, with cross-platform capabilities.
- Targets both Windows and Linux platforms.
- Utilizes Chacha20 for file encryption and RSA-OAEP for key encryption12.
- It can encrypt files on shared networks using SMB protocol.
- Ransomware builder requires domain admin password or NTLM hash.
- Affiliate program advertised on RAMP underground forum.

Targeted Platform:

- Windows systems
- Linux

Propagation Methods:

- Network shares via SMB communication protocol.
- Deletion of shadow volume copies on compromised Windows machines

Impact:

- **File Encryption:** Eldorado employs Chacha20 encryption to lock files, rendering them inaccessible. Encrypted files receive the extension .00000001.
- **Double Extortion:** Eldorado combines data exfiltration with encryption. Attackers threaten to leak sensitive data unless the ransom is paid.
- **Business Disruption:** Encrypted files disrupt normal operations, affecting productivity. Recovery can be time-consuming and costly.

INDICATORS OF COMPROMISE:

SHA256	Classification
1375e5d7f672bfd43ff7c3e4a145a96b75b66d8040a5c5f98838f6eb0ab9f27b	Eldorado (32-bit windows)
7f21d5c966f4fd1a042dad5051dfd9d4e7dfed58ca7b78596012f3f122ae66dd	Eldorado (64-bit windows)
cb0b9e509a0f16eb864277cd76c4dcaa5016a356dd62c04dff8f8d96736174a7	Eldorado (64-bit windows)
b2266ee3c678091874efc3877e1800a500d47582e9d35225c44ad379f12c70de	Eldorado (32-bit linux)
dc4092a476c29b855a9e5d7211f7272f04f7b4fca22c8ce4c5e4a01f22258c33	Eldorado (64-bit linux)

IP
173.44.141[.]152

RECOMMENDATIONS:

- **Block the IOCs** on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- **Patch Systems:** Ensure all systems are up-to-date with the latest security patches from operating system and software vendors.
- **Enforce Strong Passwords:** Implement strong and unique passwords for all administrative accounts and enforce multi-factor authentication (MFA) wherever possible.
- **Segment Networks:** Segment network to limit the lateral movement of attackers in case of a breach.
- **Endpoint Detection and Response (EDR):** Deploy EDR solutions to detect and respond to malicious activity on endpoints.
- **Regular Backups:** Maintain regular backups of critical data with offline storage isolated from the production network.
- **Employee Training:** Train employees on cybersecurity best practices, including phishing awareness and social engineering techniques

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.group-ib.com/blog/eldorado-ransomware/