مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Abyss Ransomware Threat

Tracking #:432316449

Date:29-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed the Abyss Ransomware, also known as Abyss Locker, has emerged as a significant cybersecurity threat since its introduction in 2023.

TECHNICAL DETAILS:

Abyss Ransomware, also known as Abyss Locker, has emerged as a significant cybersecurity threat since its introduction in 2023. This ransomware group employs advanced tactics to infiltrate and disrupt Windows and Linux systems across various sectors, including finance, manufacturing, and healthcare. Their multi-extortion approach, characterized by sophisticated encryption and data exfiltration, poses serious risks to organizations worldwide.

Abyss Ransomware employs a variety of sophisticated Tactics, Techniques, and Procedures (TTPs):

1. **Initial Access Vectors**:
   - **Phishing**: Utilizing deceptive emails to trick users.
   - **SSH Exploits**: Brute-force attacks on weak SSH configurations.
   - **Vulnerability Exploitation**: Leveraging known vulnerabilities in exposed servers.
2. **Windows Version**:
   - **Service and Process Termination**: Shutting down critical services to facilitate encryption.
   - **Volume Shadow Copy Deletion**: Preventing file recovery through deletion commands.
   - **Boot Configuration Changes**: Modifying recovery settings to hinder restoration efforts.
   - **File Encryption**: Utilizing the Salsa_20 encryption algorithm, appending unique extensions to files.
3. **Linux Version**:
   - **Targeting Virtual Machines**: Using the esxcli tool to manage VMs effectively.
   - **Selective Encryption**: Excluding critical directories to maintain some system functionality.
   - **Advanced Persistence Techniques**: Establishing daemon processes to ensure continued operation post-reboot.
4. **Multi-Extortion Tactics**: Threatening to publicly release stolen data if ransom demands are not met.

The most targeted industries include:

- Manufacturing
- Finance and Insurance
- Professional, Scientific, and Technical Services
- Health Care and Social Assistance
- Construction

INDICATORS OF COMPROMISE(IOCs):

Attached in Excel File

RECOMMENDATIONS:

1. **Implement Advanced Anti-Malware Solutions**: Deploy comprehensive anti-malware tools and Endpoint Detection and Response (EDR) systems to enhance real-time threat detection and prevention.
2. **Conduct Regular Security Audits and Vulnerability Assessments**: Perform routine evaluations of network configurations and system vulnerabilities. Establish a continuous vulnerability management program to address potential weaknesses proactively.
3. **Enforce Strong Authentication and Access Controls**: Implement Multi-Factor Authentication (MFA) and regularly review access controls to reduce unauthorized access risks.
4. **Establish Comprehensive Backup and Disaster Recovery Plans**: Schedule regular backups of critical data and test restoration processes frequently to ensure quick recovery in the event of an attack.
5. **Utilize Dark Web Monitoring**: Employ advanced monitoring tools to track unauthorized data transfers and potential threats linked to Abyss Ransomware, allowing for preventive action.
6. **Conduct Continuous Employee Training and Awareness Programs**: Educate staff on identifying phishing attempts and suspicious activities. Use simulated phishing exercises to reinforce training and increase awareness.
7. **Develop an Incident Response Plan**: Create a detailed incident response plan outlining steps to take during a ransomware incident. Regularly test and update this plan to ensure effectiveness.

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://socradar.io/dark-web-profile-abyss-ransomware/