مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Beast Ransomware Campaign

Tracking #:432316432

Date:24-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Beast Ransomware, also known as Monster, targeting various organizations and operating across multiple operating systems, including Windows, Linux, and VMware ESXi servers.

TECHNICAL DETAILS:

Beast Ransomware, also known as Monster, has emerged as a sophisticated Ransomware-as-a-Service (RaaS) platform actively targeting organizations since 2022.

- **Multi-Platform Targeting**: Beast can infect Windows, Linux, and VMware ESXi systems.
- **Customizable Payloads**: Affiliates can tailor binaries for specific environments and attack scenarios.
- **Offline Builder**: Added in August 2024, allows payload creation without internet connectivity.
- **Self-Propagation**: Performs SMB scans to spread across networks automatically.
- **Geofencing**: Avoids encrypting systems in Commonwealth of Independent States (CIS) countries.

Windows Version:

- Uses Elliptic-curve cryptography and ChaCha20 encryption
- Multithreaded queue for faster file encryption
- Terminates critical services before encryption
- ZIP wrapper mode embeds ransom notes in .zip files

Linux and ESXi Version:

- Shuts down virtual machines before encryption
- Targets critical VMware-related files and logs

Anti-Recovery Measures:

- Deletes shadow copies to prevent system restore
- Executes IWbemServices::ExecQuery to query and remove backups

Attack Vector:

- **Initial Access**: Phishing, malicious downloads, or exploiting vulnerabilities
- **Privilege Escalation**: Targeting ESXi hosts or vCenter credentials
- **Access Validation**: Enabling SSH on ESXi servers if direct access is blocked
- **Ransomware Deployment**: Execution on ESXi hosts, encrypting '/vmfs/volumes'
- **Backup Compromise**: Targeting backup systems to prevent recovery
- **Additional Spread**: Possible deployment to non-virtualized systems

Indicators of Compromise (IOCs):

IOC	IOC type	Description
iplogger[.]co/1v1i85[.]torrent	Domain Name	Geofencing IP query
4c44ac1eea4bc7f4ea542d611b5658d7ac2729d79abe750da83f1581cd832eaf	SHA-256	Beast Windows Encryptor
369034bf1d793fe56ea4d683a156722d825ad9829fc128117f82a26bc1d0480b	SHA-256	Beast Windows Encryptor
e01f5c7067dc984dceb883b10444b1a5b0f22ebd500baf9d9a88207f5033285d	SHA-256	Beast Windows Encryptor

dd09a2ef31d018fd83f186e3eaaccccdaa8a8c8779ced668abb06dc934d89a2d	SHA-256	Beast Windows Encryptor
dbbe792e6c804518909f8990a836552573522d126547429d6cd3fcb1f60d542c	SHA-256	Beast Windows Encryptor

RECOMMENDATIONS:

- Review the Indicators of Compromise (IOCs) and implement the necessary security measures.
- **Implement Multi-Factor Authentication**: Especially for privileged accounts
- **Patch Management**: Keep all systems and software up-to-date
- **Network Segmentation**: Isolate critical systems and limit lateral movement
- **Backup Strategy**: Maintain offline, encrypted backups and test restoration processes
- **Endpoint Protection**: Deploy and maintain updated anti-malware solutions
- **Access Control**: Implement least-privilege principles and regularly audit access
- **Monitoring**: Enable logging and implement real-time threat detection
- **Employee Training**: Conduct regular phishing awareness and security training
- **Incident Response Plan**: Develop and regularly test an incident response plan
- **VMware-Specific Hardening**: Follow VMware's security best practices for ESXi environments

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.cybereason.com/blog/threat-analysis-beast-ransomware