مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Ransomware Campaign- VanHelsing Ransomware

Tracking #:432317285

Date:20-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed FortiGuard Labs has identified and analyzed a new ransomware strain dubbed VanHelsing, which has rapidly gained traction across several geographies and industries.

TECHNICAL DETAILS:

FortiGuard Labs has identified and analyzed a new ransomware strain dubbed VanHelsing, which has rapidly gained traction across several geographies and industries.Operating similarly to other ransomware families, VanHelsing encrypts files on compromised systems and demands a ransom for decryption, using .vanlocker or .vanhelsing file extensions. Victims are redirected to TOR-based negotiation sites, and those who do not comply risk having sensitive data leaked on the group's public data leak site. The ransomware includes several obfuscation and spread mechanisms, including SFTP and SMB credential abuse.

The VanHelsing group demonstrates no apparent restraint in target selection, impacting entities across manufacturing, government, and other sectors.

1. **Infection Vector**
   The precise vector remains unknown, but it likely includes phishing, RDP brute force, or malicious downloads, common to many ransomware operations.

2. **Execution & Spread**
   When executed, the ransomware accepts the following command-line arguments:

   -h : Help
   -v : Verbose
   -sftpPassword : For spreading over SFTP
   -smbPassword : For spreading over SMB
   -bypassAdmin : Locks system without admin
   -noLogs : Disables logging
   -nopriority : Disables CPU and IO priority tweaks

3. **Encryption Behavior**
   - Adds .vanlocker or .vanhelsing extensions to encrypted files.
   - Avoids encrypting critical system and application files to ensure system remains operable for ransom negotiation.
   - Exempted files and extensions include system-related files like ntldr, boot.ini, .exe, .dll, etc.
   - Avoids folders like Windows, Program Files, $Recycle.Bin, Trend Micro, etc.

4. **Registry & Mutex**
   - **Mutex Created:** Global\\VanHelsing
   - May modify registry key: Software\Classes\.vanlocker\DefaultIcon to assign a custom icon.

5. **Ransom Note & TOR Negotiation**
   - Drops ransom note in README.txt.
   - Replaces desktop wallpaper with its branding.
   - Victims instructed to contact attackers via TOR negotiation site.

6. **Victimology & Data Leak Trends**

As of April 2025, the VanHelsing data leak site has listed seven victims:

- Sectors affected: Predominantly manufacturing and municipal governments.
- No target discrimination: Government, industrial, and private entities affected alike.
- Victims removed from site may have paid ransom or negotiated in private.

IOCs:

VanHelsing Ransomware File IOCs(SHA256
86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17
99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98

RECOMMENDATIONS:

- Patch systems and software regularly to close known vulnerabilities.
- Disable SMB v1 and restrict access to SMB/SFTP services from untrusted networks.
- Implement multi-factor authentication (MFA) for remote and administrative access.
- Deploy phishing simulation platforms to train employees on threat recognition.
- Conduct frequent, isolated backups and test restore procedures regularly.
- Maintain immutable backups to prevent tampering by ransomware.
- Apply least privilege access and restrict sensitive folders and data repositories.
- Enable EDR with updated AV and IPS signatures.
- Apply Zero Trust Network Access (ZTNA) policies and micro segmentation.
- Monitor for the mutex “Global\VanHelsing” and other indicators via EDR/XDR tools.
- Develop and test IR playbooks for ransomware scenarios.

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.fortinet.com/blog/threat-research/ransomware-roundup-vanhelsing?lctg=232952123