THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

VanHelsing Ransomware

Threat Actor Malware

Description

VanHelsing Ransomware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Data Theft and Espionage
- Financial Losses
- Data Encrypted for Impact
- Inhibit System Recovery

A newly discovered ransomware strain dubbed VanHelsing has been observed targeting organizations across various sectors. This ransomware is designed specifically for Windows systems and uses advanced encryption to lock files, appending a ".VanHelsing" extension.

VanHelsing also incorporates double extortion tactics not only encrypting files but also exfiltrating data and threatening public release if the ransom is not paid. Its ability to evade detection and establish persistent access emphasizes the critical need for robust preventive measures, incident response planning, and threat monitoring.

THREAT OVERVIEW: VANHELSING RANSOMWARE:

The VanHelsing ransomware variant has been observed encrypting files and demanding cryptocurrency payments for decryption. It changes the desktop background and drops a ransom note titled README.txt.

Key Features

- Encrypts data with a unique .vanhelsing extension.
- Drops ransom note explaining the breach and payment demands.
- Exfiltrates sensitive information before encryption.
- Threatens public disclosure of stolen data (double extortion).
- Uses anonymous communication channels via the Tor network.

Ransom Note Summary:

The note notifies victims of system compromise and the encryption of data, including financial documents, personal records, and other sensitive files. It demands payment in Bitcoin and warns that non-compliance may lead to data leaks. Victims are advised against attempting recovery on their own, as it may lead to permanent data loss.

Indicator of Compromise

MD5

5c254d25751269892b6f02d6c6384aef
3e063dc0de937df5841cb9c2ff3e4651
2b8cb32a74e16be7c30e1e605c0ed6ba

SHA-1

79106dd259ba5343202c2f669a0a61b10adfadff
e683bfaeb1a695ff9ef1759cf1944fa3bb3b6948
4211cec2f905b9c94674a326581e4a5ae0599df9

SHA-256

86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17
99959c5141f62d4fbb60efdc05260b6e956651963d29c36845f435815062fd98
8c272d63d9a37651b81283f0273609db8b9cd7af0b20e917529c7c9ca8687d59

Remediation

Strategic Actions

- Implement strong access controls, encryption policies, and strict user authentication mechanisms.
- Maintain up-to-date offline backups of all critical data and systems.
- Incorporate ransomware-specific playbooks into your organization's incident response plan.

Management-Level Actions

- Define a formal breach response plan that includes data classification, regulatory compliance, and external communication protocols.
- Enforce **Zero Trust principles** and enable **Multi-Factor Authentication (MFA)** for all remote and privileged access.
- Conduct regular **security awareness training** to build a security-conscious workforce.

Tactical Actions

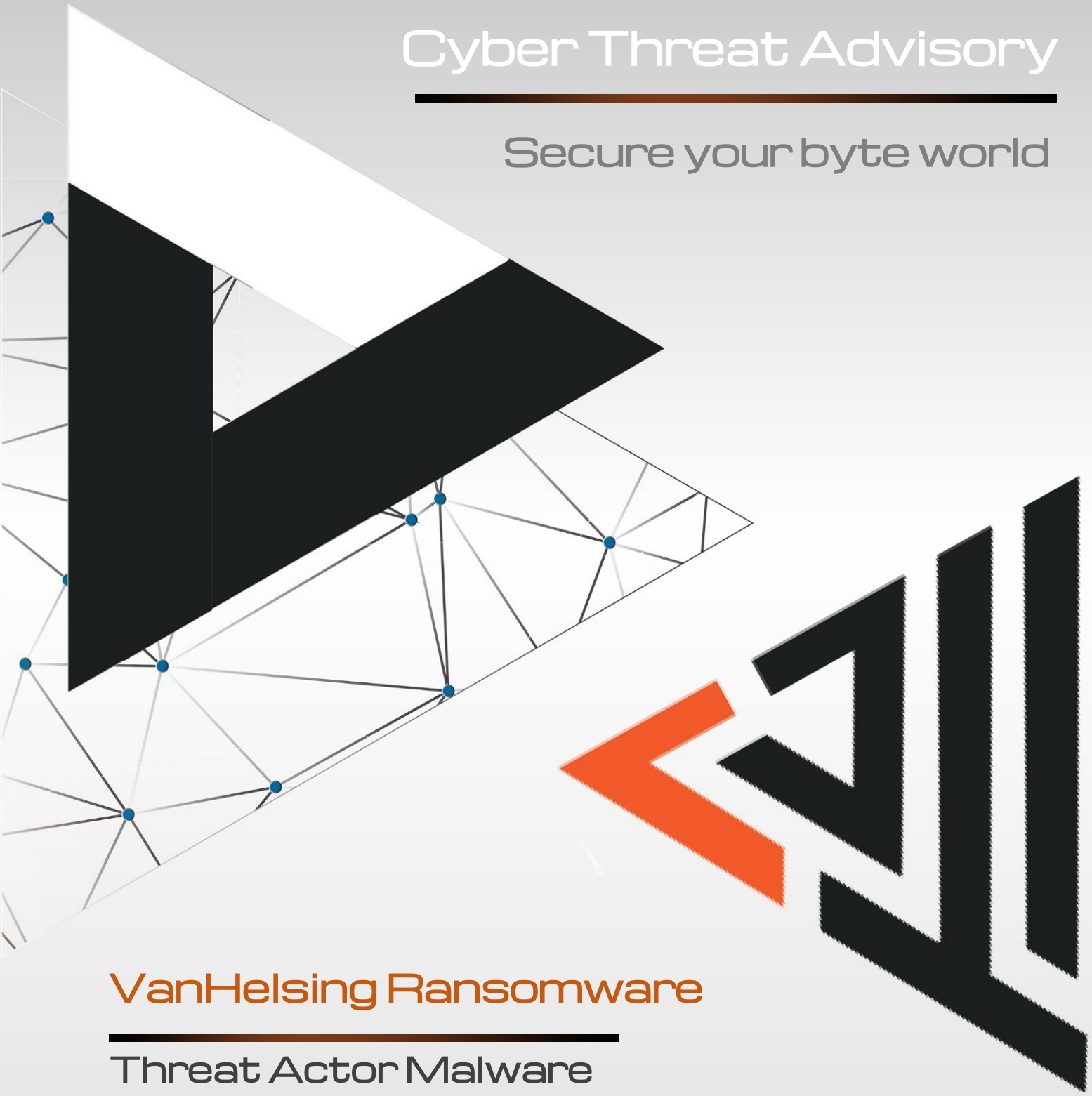
- Apply the latest security patches and software updates across all systems and applications.
- Monitor and block known IOCs at network, endpoint, and perimeter levels.

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world



VanHelsing Ransomware

Threat Actor Malware

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:
• Website: www.threatcure.net
• Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE