WANNACRY DAY-3

It targeted computers running the Microsoft Windows operating system by encrypting data and demanding a ransom payment in Bitcoin for its decryption.

Threat

The threat was a ransomware attack aiming to encrypt victims' data and demand a ransom for its decryption.

1. Ransomware WannaCry: All you need to know - Kaspersky

www.kaspersky.com

Vulnerability

The primary vulnerability exploited was the EternalBlue exploit, a tool developed by the NSA to target vulnerabilities in Microsoft's SMB protocol. This exploit allowed attackers to remotely execute code on vulnerable systems.

1. EternalBlue Exploit: What It Is And How It Works - SentinelOne

www.sentinelone.com

Attack

The WannaCry ransomware attack leveraged the EternalBlue exploit to spread rapidly across networks, infecting vulnerable systems. Once installed, it encrypted files and displayed a ransom demand.

1. CRITICAL ALERT: Wannacry/ WannaCrypt Ransomware - Cyber Swachhta Kendra

www.csk.gov.in

Risk

The risk was significant, including data loss, financial loss due to ransom payments, business disruption, and reputational damage for affected organizations.

WANNACRY DAY-3

1. WannaCry Ransomware Attack Underscores Cyber Risks to the Construction Industry

www.stites.com

Exploit

The EternalBlue exploit was the primary tool used to spread the ransomware.

Asset

The assets targeted by the attack were data stored on vulnerable systems.

Impact

The impact was widespread, affecting individuals, businesses, and critical infrastructure. Hospitals, schools, and businesses were forced to shut down operations, causing significant economic losses. The attack also highlighted the global nature of cyber threats and the need for improved cybersecurity practices.

1. Comprehensive Guide to WannaCry Ransomware Attacks - Tata Communications

www.tatacommunications.com