RANSOMWARE

How did it happen?

ENVISTA FORENSICS

Common Attack Methods

Phishing Attacks

80% of hacked companies in 2016 reported attack entry points were related to phishing emails or social media.

Increased by 109% in the last two years.

Unauthorized Access

With the recent surge of employees working from home, Unauthorized Access Attacks have grown in popularity.

By 2023, 60% of enterprises will phase out most of their VPNs in favor of zero trust network access (ZTNA).

What Will They Do Once They Have Access?

Gather or obtain private information from you

Install malware on your computer

Execute ransomware on your ccompany's network

Typical Steps in a Ransomware Attack

Infection

Once attacked, ransomware executes on the endpoint and likely will encrypt network shares and connected drives.

Key Exchange

The ransomware contacts the server operated by the cybercriminals to generate the keys which will be used on the local, affected system.

Encryption

The ransomware starts encrypting the local system being executed, typically including network shares and physically attached drives.

Extortion

Once the encryption is completed, instructions for payment are provided.

Resolution

Users pay the ransom to decrypt affected files or attempt recovery of infected files and restoration on their own.

If you or a client have been infected with ransomware, contact Envista Forensics Cyber Breach Team.

ENVISTA FORENSICS

EnvistaForensics.com

Please email **Breaches@EnvistaForensics.Com** to submit a case or a claim.