Once the surveillance research has revealed a preferred attack vector, cybercriminals will execute the initial attack by preying upon an organization’s vulnerabilities and relying upon ransomware’s advanced obfuscation to thwart detection.

Phase 1: Surveillance
Cybercriminals will scan the target’s website and capture executive names, email configurations, and contact information and will analyze servers and networks for vulnerabilities.

Phase 2: Ransomware Deployment
Once the surveillance research has revealed a preferred attack vector, cybercriminals will execute the initial attack by preying upon an organization’s vulnerabilities and relying upon ransomware’s advanced obfuscation to thwart detection.

Phase 3: Command & Control Server Connection
When the ransomware is deployed, it connects to its command and control server via secure communication protocols.

Phase 4: Encryption Key Generation
The command and control server will generate the encryption keys (public and private). Today’s ransomware has evolved to utilize more sophisticated encryption, making it very difficult to decrypt with traditional tools.

Phase 5: Encryption Key Deployment
The ransomware then utilizes the public key from the command and control server to encrypt files that are accessible to the user.

Phase 6: Data Exfiltration
Some of the latest ransomware variants encrypt and exfiltrate data, allowing cybercriminals to sell it on the black market. This creates a data breach as defined by most regulatory authorities.

Phase 7: Bitcoin Demand
Infected users receive messages on their home screens and are instructed to pay the bitcoin fee in exchange for the private key that initiates file decryption.

Phase 8: Ransom Negotiation
Ransomware threat actors often provide communication channels to facilitate negotiation. Most reports indicated that infected businesses have been successful in reducing ransoms.

Phase 9: Payment
Once the negotiated ransom is paid, usually in bitcoin, the private key is deployed and file decryption will commence. However, payment does not guarantee file recovery.

Phase 10: Repeat
Successful ransomware attacks position victims to be targeted again. Deploying a next-generation anti-virus solution which draws on industry-leading ransomware detection and quarantine efficacy, like X by Invincea, enterprises can prevent recurrent attacks.

www.invincea.com/testdrive
CLICK HERE TO TEST DRIVE