OCTOBER 26, 2023

UT LAW CLE

TEXAS Law
The University of Texas at Austin
School of Law

RANSOMWARE: TO PAY OR NOT TO PAY

WILL DAUGHERTY
Partner, Head of Cybersecurity, U.S.
Norton Rose Fulbright
Houston, TX

JASEN ORME
Special Agent, Cyber Task Force
FBI
Houston, TX

Ransomware Introduction

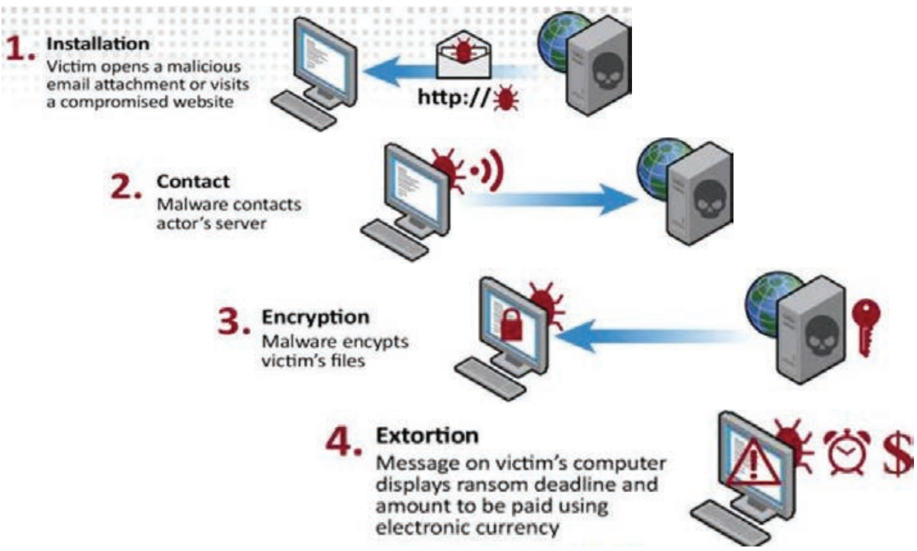
Ransomware is malware that infects computers, networks, and services

- Victim’s computer is infected with malware
- Malware encrypts victim's data and/or systems, making them unreadable
- Actor demands payment to decrypt files or network
- Numerous variants and threat actor groups that launch the attacks

Ransomware Continues to Evolve

- **Ransomware-as-a-service**: business model where operators develop ransomware encryptor and supporting infrastructure (leak site; victim chat function) where affiliates launch the attacks with tools developed by the operator and they split the ransom payment.
  - Affiliates are moving between RaaS operators more frequently, complicating detection and response
- **Timed Wiper Malware**: threat actors install wiper malware before ransomware deployment and if payment is not made within the time the wiper malware is installed, it will execute to delete organization data. Increased pressure tactics from Threat Actor to force victim payments (e.g., DDoS attacks, shame sites, direct calls to employees) and increase in re-extortion after payment
- **Dual Ransomware attacks**: certain threat actors are launching multiple attacks after the first ransomware attack by a different ransomware variant to disrupt remediation efforts
- **Supply-Chain attacks**: Increased focus on targeting cloud infrastructure, managed services providers, industrial processes and software supply chain

Stages of Ransomware



Stages of Ransomware

5. Double Extortion
Posting proprietary information to online marketplaces, only partially unlocking the system and demanding more money, simultaneously employing BEC

UT LAW | CLE   TEXAS Law

Common Traits: Ransom Page

Title search: To Pay or Not to Pay: Issues and Considerations for a Ransomware Response

Also available as part of the eCourse
To Pay or Not to Pay: Issues and Considerations for a Ransomware Response

First appeared as part of the conference materials for the
2023 Essential Cybersecurity Law session
"To Pay or Not to Pay: Issues and Considerations for a Ransomware Response"