A CRYPTO CRIME

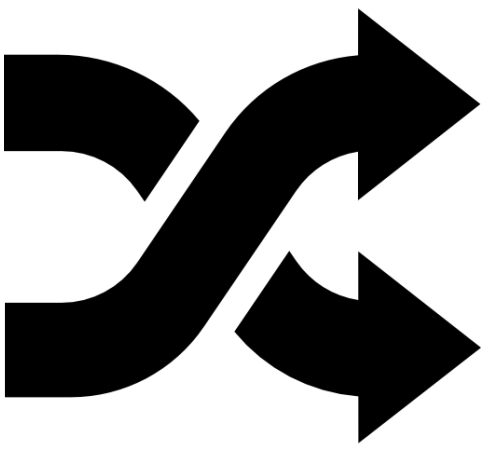
RANSOMWARE

PAST

1989-PRESENT

The original Ransomware was the AIDS trojan, launched in 1989 by Joseph Popp. Ransomware was sparse and ineffective until Bitcoin and related technologies were released in 2009. Since then, ransomware has continued to grow and adapt.

PRESENT

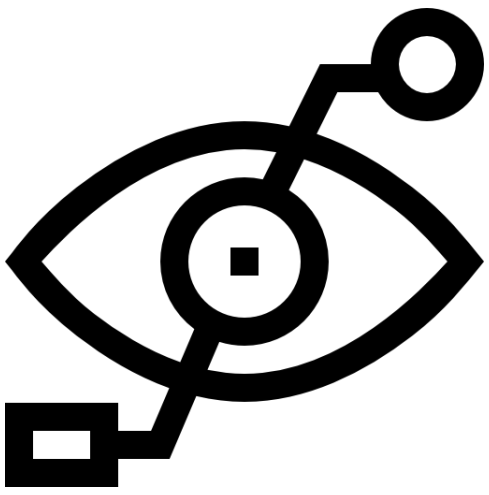


2018

Ransomware Has Evolved In The Following Ways:

- New delivery techniques
- New encryption techniques
- Advanced propagation capabilities
- Harnessing human psychology to improve attacks
- Polymorphic code
- Ransomware as a distraction or attack vehicle
- Multi-threaded attacks

FUTURE



2018+

Ransomware Predictions For The Future:

- Ransomware targeting the internet of things (IoT)
- More doxing
- Creative attacks using ransomware as a distraction
- Attacks on operational technology (OT)
- Ransomware targeting smart transportation
- Increased attacks on the public sector

VULNERABILITIES

- Locating backup servers on network drives
- Failing to establish backup redundancy, including backing up the backup server
- Failing to test the recovery of backed-up data
- Executing inadequate, infrequent backups
- Failing to protect backup servers with anti-virus/anti-malware solutions
- Issuing backup server login credentials to those who don't require access
- Browsing the internet from the backup server

MITIGATION

- Employee ransomware training
- Behavior based threat detection
- Redundant backups in place with copies online, offline, and offsite
- Backup your backup server
- Shutdown Remote Desktop Protocol (RDP) on the internet
- Use a VPN when logging into remote machines
- Don't browse the internet from your backup server unless necessary for software and firmware updates and patches
- Protect your backup servers with anti-virus/anti-malware products
- Test your data recovery know time to recover, and know how much data would be lost in an attack
- Segment your network
- Practice the principle of least privilege
- Decline email messages from languages you don't engage in, which ransomware attackers might leverage for hard-to-detect spoofed URLs
- Establish a ransomware crisis plan

THE SECURITY STRONGHOLD

https://thesecuritystronghold.com

contact@thesecuritystronghold.com

+ (1) 715-347-8979