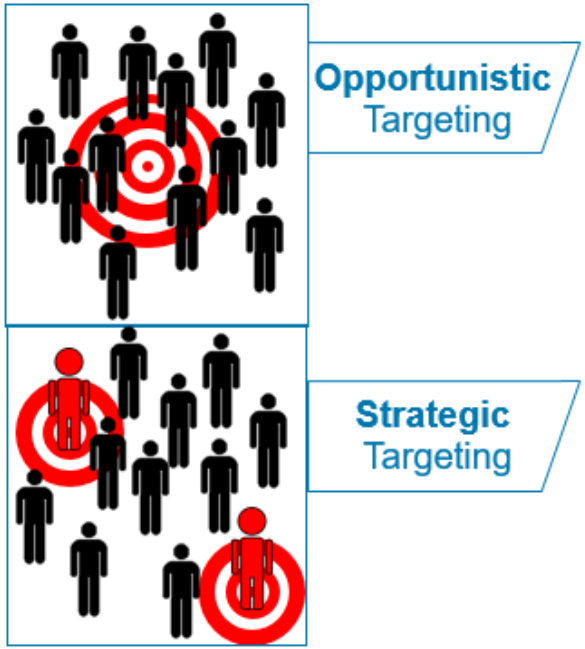
What is Ransomware?

Ben Spear
Director, EI-ISAC
January 31, 2020

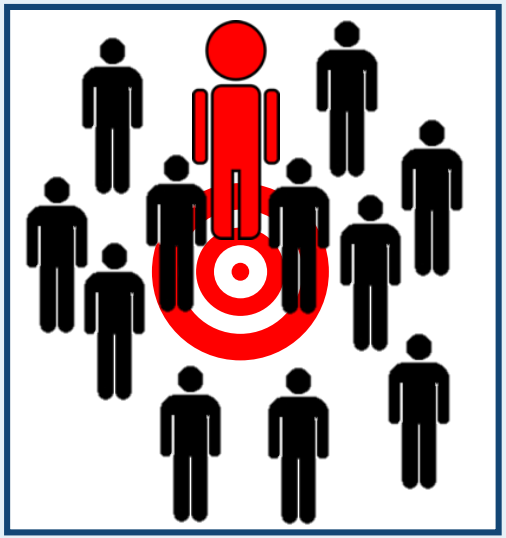
Ransomware Overview

- Malware that blocks access to a system, device, or file until a ransom is paid
- The ransom is typically demanded in the form of cryptocurrency (e.g., Bitcoin)
- The amount demanded can range from several hundred dollars up to and exceeding $1 million

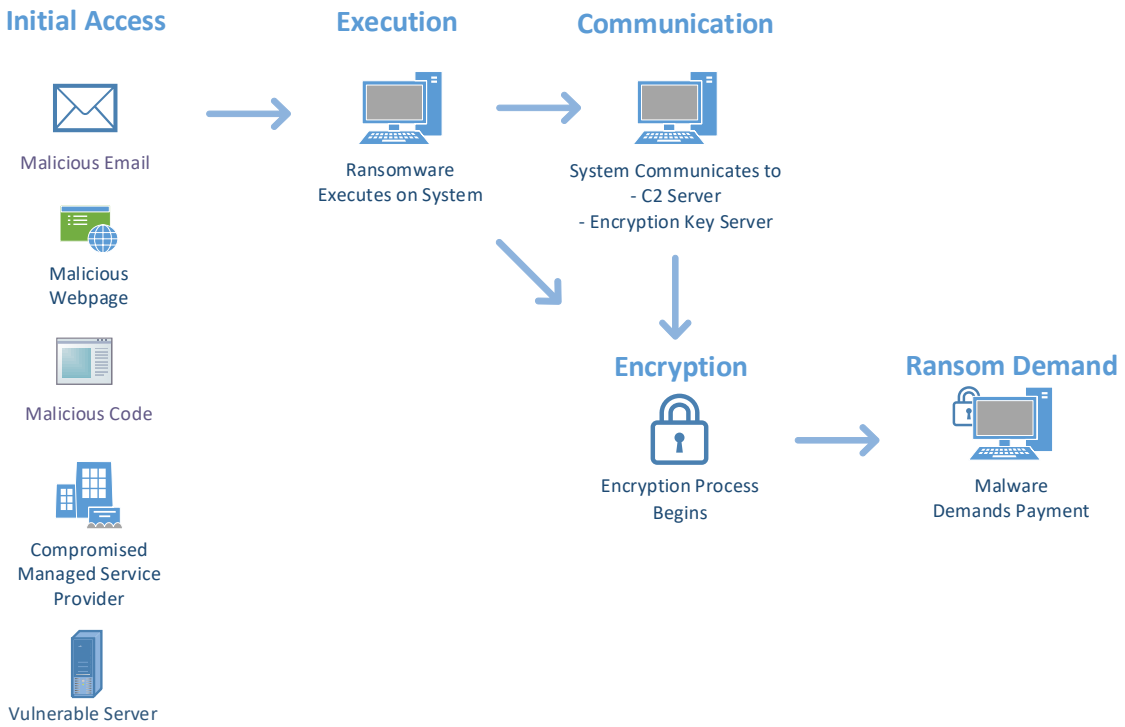
Opportunistic and Strategic Campaigns



Opportunistic Targeting
Leading to
Strategic Targeting



Ransomware Lifecycle



Current SLTT Ransomware Trends

In recent months, K-12 schools were the most impacted SLTT sector

- IT and cybersecurity is typically under-resourced
- Flat network architecture
- Lots of targets
- Reports of school districts paying ransoms

Ransomware attack forces Richmond Schools to extend holiday break

Schools closed until Monday

School officials: Ransomware prompts school closure in Flagstaff

Students with the Flagstaff Unified School District will have the day off Thursday.

Posted September 5, 2019

'Ransomware' Attack Locks San Bernardino City Unified School District Computer System

POSTED 7:31 PM, OCTOBER 20, 2019, BY BRIAN DAY, *UPDATED AT 09:49AM, OCTOBER 21, 2019*

Hackers target Wakulla Schools, shut down district-wide emails in ransomware attack

James Call, Tallahassee Democrat Published 1:45 p.m. ET Sept. 10, 2019 | **Updated 8:55 p.m. ET Sept. 10, 2019**

Ryuk

- First appeared in August 2018
- Most reported ransomware for SLTTs in 2019
- Leverages the TrickBot botnet for network access
- Highly impactful and costly ransomware attacks
- Targets backups and shadow copies

https://www.cisecurity.org/white-papers/security-primer-ryuk/

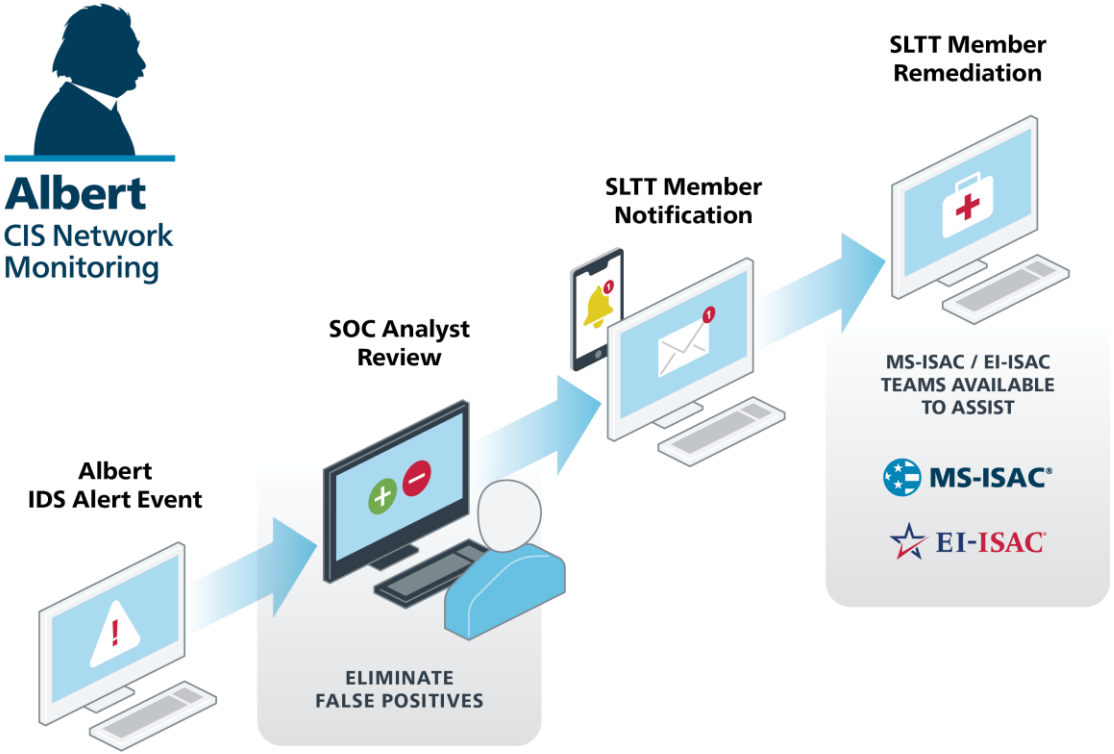
Recent Ransomware Incidents

- Pensacola, FL – December 2019
- Louisiana – July and November 2019
- Alabama Hospitals (3) – October 2019
- School District in Arizona – September 2019
- Texas (22 towns) – August 2019
- Greenville, NC – April 2019
- Baltimore – May 2019
- Atlanta – March 2018

EI-ISAC & Ransomware

- 24 x 7 Incident Reporting via Security Operations Center
  - 1-866-787-4722
  - soc@cisecurity.org
- Incident response, digital forensics and malware analysis via Computer Emergency Response Team
- Albert Network Intrusion Detection – Monitoring and Analysis

Albert Event Generation and Analysis



Albert – Ransomware Detection

- Albert detects Ransomware in four ways
  - Ransomware executable download
  - Establishment of Command-and-Control
  - Encryption keys download
  - Periodic check-in traffic
- Average time from Albert sensor detection to customer notification is 5 minutes
- Actionable information provided to affected entity for action and system remediation
- To find out more about network security monitoring, contact us at services@cisecurity.org

CIS Services®

Albert
CIS Network Monitoring

Thank You

Ben Spear

518.880.0705

Ben.spear@cisecurity.org

Join the MS-ISAC

https://learn.cisecurity.org/ms-isac-registration