CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

MS-ISAC Effectiveness Against Ransomware

Introduction

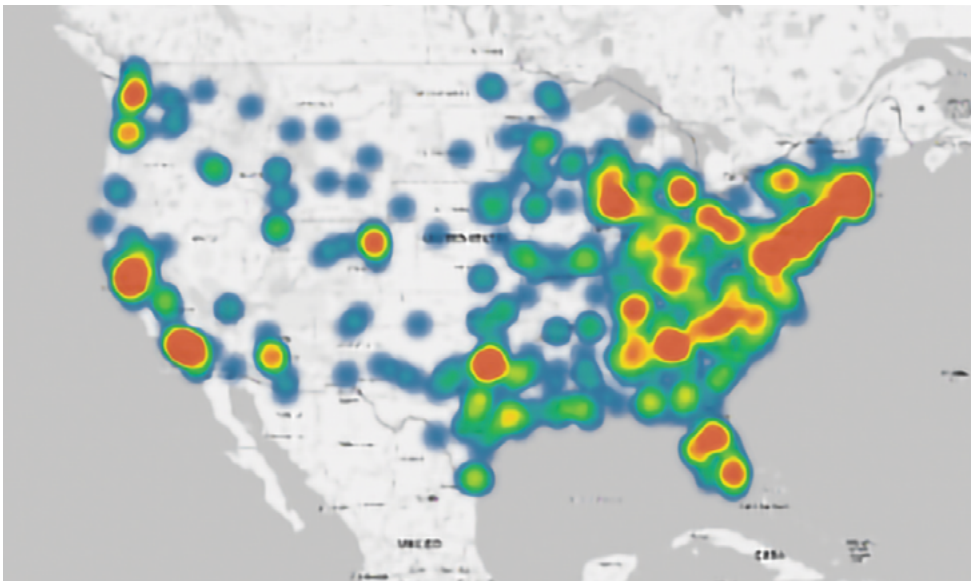
Ransomware has quickly become one of the most destructive, disruptive, and costly cybersecurity issues in history. Given the simplicity of its operation, easily automated deployment, and the high potential of success, ransomware has become the preferred method for cyber criminals. This is particularly the case for State, Local, Tribal and Territorial (SLTT) governments.

According to Trend Micro, ransomware attacks have increased 363% since 2018. In addition, specific strains of ransomware, including "Ryuk,", appear to be targeting state and local governments. (Source: Trend Micro)

The biggest SLTT ransomware news-maker thus far for 2019 is the Baltimore City government. The city's computer system was hit with ransomware in May 2019 that crippled the city's government for more than one month. Estimates put the cost to recover at over $18 million dollars. The attack shut down city employees' emails, halted credit card payments for city services and fines, and froze the property market. (Source: Baltimore Sun)

Around one year earlier, the Atlanta city government spent over $17 million to recover from a ransomware attack. In recent weeks, Louisiana school systems and 23 local government organizations in Texas have been hit with ransomware attacks. (Source: CNBC)

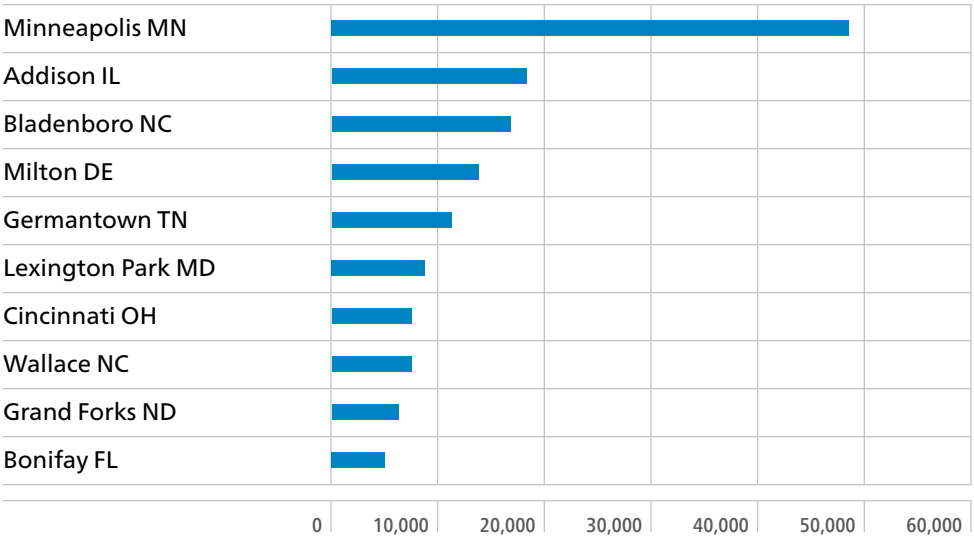
While many choose to pay the ransom, paying does not guarantee that encrypted files will be recovered.



Heat Map of Public Entity Ransomware Attacks, YTD 2019 (Source: Malwarebytes Labs)

According to Malwarebytes Labs, a leading malware research organization, most victims of ransomware do not become media stories like Baltimore and Atlanta. The table below illustrates the cities most affected by ransomware in the first half of 2019.

Top 10 Cities in US for Business Ransomware Detection. (January–May 2019) (Source: Malwarebytes Labs)



Other important ransomware figures include the following:

- According to Cybersecurity Ventures, global ransomware damages were predicted to top $11.5 billion in 2019. (Source: Cybersecurity Ventures)
- After getting hit by the SamSam ransomware in March 2018, Atlanta, Georgia, spent more than $5 million rebuilding its computer network, including spending nearly $3 million hiring emergency consultants and crisis managers. (Source: Statescoop)
- New York State's capital was hit with a ransomware attack in 2019 that took several key services offline. (Source: CNET)
- The city of Riviera Beach in Florida paid a $600,000 ransom in June 2019 to recover files following a ransomware attack. (Source: CBS News)
- On average, businesses that experienced ransomware lost around $8,500 per hour due to ransomware-induced downtime. (Source: Govtech)

Albert Effectiveness in Detecting Ransomware

While ransomware has been proven highly lucrative and is growing as a threat, there are ways for organizations to defend themselves. The keys to ransomware survival are twofold:

1 early detection and mitigation; and

2 effective data backups in case ransomware is successfully executed.

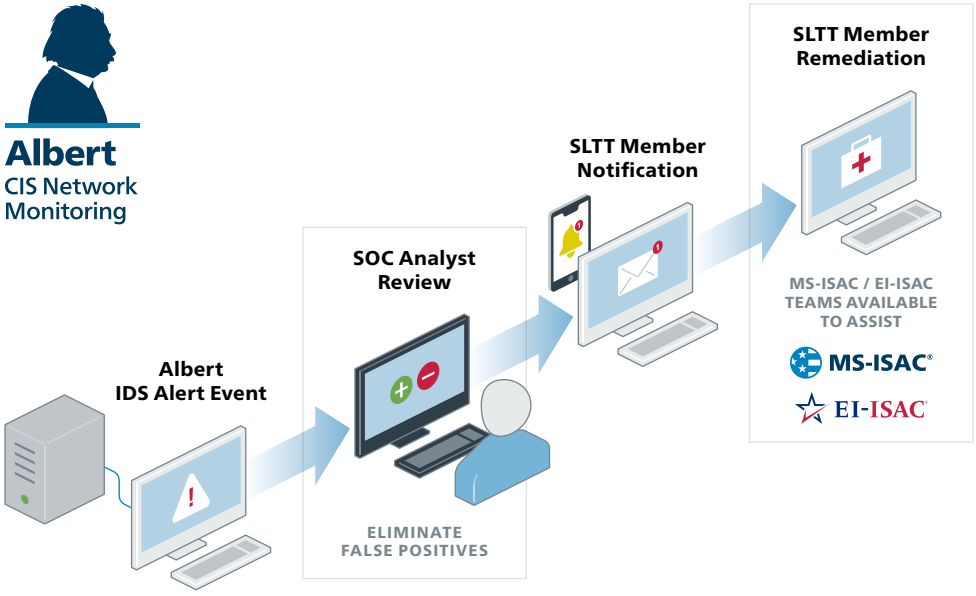
The Center for Internet Security® (CIS®)[1] has developed and deployed a network monitoring system called "Albert" that plays a critical role in early detection of ransomware and other malicious attacks against SLTT government entities.

Albert is a custom-designed Intrusion Detection System (IDS) and network traffic-monitoring sensor developed by CIS specifically for monitoring SLTT networks. Albert consists of a combination of open source, government-owned, and CIS-developed software that performs malicious intrusion detection as well as network flow analysis. CIS has deployed hundreds of Albert sensors to help protect SLTT critical and elections infrastructure.

Albert's specialty is detection of malicious network activity, which makes it particularly effective against certain ransomware attacks.

The following chart details the typical phases in a ransomware attack:

Albert Ransomware Detection



1 CIS is a nonprofit organization that operates the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (the MS-ISAC® and the EI-ISAC® respectively) in support of the Department of Homeland Security.

Albert sensors are loaded with the "signatures" of many malicious threats. These signatures are derived from many sources including commercial threat providers, federal organizations, and unique MS-ISAC and EI-ISAC threat intelligence indicators of malicious activity. Threat signatures for Albert sensors are updated multiple times a day. Threat "alerts" are generated by the Albert sensors based on a match against one or more of the threat signatures. These alerts are automatically passed to the Security Operations Center (SOC), a 24/7/365 analysis and response facility operated by CIS.

The Albert events are individually reviewed by SOC analysts who validate the malicious activity and initiate the appropriate action. In the case of a validated ransomware attack, the SOC analyst would immediately contact the affected SLTT organization.

The average time from threat detection by an Albert sensor to SOC notification to an affected organization is sufficiently rapid that, in most instances, the affected SLTT is able to mitigate the ransomware attack before it begins execution or certainly before it does significant damage.

Albert Effectiveness

Using Albert sensors to monitor SLTT networks, the MS-ISAC has been proven enormously effective in detecting and defeating entirely or minimizing the impact of most strains of ransomware. The combination of Albert sensors deployed, with custom and commercial ransomware signatures, and the CIS SOC are extremely effective in detecting known ransomware.

In 2018, the MS-ISAC alerted and the SOC successfully acted on, hundreds of ransomware-related attacks. Through July 2019, the MS-ISAC has already identified, analyzed, and communicated approximately half of the total number of 2018 ransomware-related attacks to the affected SLTT organization. To the MS-ISAC's knowledge, none of the ransomware-related attacks from January 2018 through July 2019 have resulted in a successful ransomware incident in which files were encrypted or there was significant impact to an SLTT's network requiring additional incident response support from the MS-ISAC CERT team. These MS-ISAC services result in very significant cost-avoidance benefits for members.

Cost avoidance occurs in the following areas:

- **Downtime not incurred:** Organizations that detect ransomware attacks early are more likely to respond and recover quickly, minimizing organizational disruption and downtime.
- **Upgrades and replacements not needed:** Organizations that detect ransomware attacks early are less likely to require upgrading and replacement of hardware, software, networks, and other assets.
- **Ransoms not paid:** Organizations that detect ransomware attacks early are more likely to minimize spread and reduce impact, therefore making it less necessary to consider ransom payment.

According to the Coveware's 2019 Q1 Ransomware Market Report (the latest report on ransomware costs), the average cost of a ransomware infection was $71,378 in 2018 and $77,407 in 2019.

The following data provides an example of how MS-ISAC monitoring of federally-funded Albert sensors has helped SLTT entities with cost avoidance related to ransomware over the past 19 months.

Ransomware Cost Avoidance

Period	*MS-ISAC Defeated Ransomware Infections	**Average Cost of a Ransomware Infection	Total Ransomware Cost Avoidance
2018 (Calendar Year)	200	$71,378	$14,275,600
2019 (January – July)	100	$77,407	$7,740,700
Total	**300**		**$22,016,300**

* These numbers are not actual statistics and represent a subset value, simplified for calculation, of ransomware infections that were detected by MS-ISAC Albert network monitoring that were partially or completely defeated through detection, rapid escalation and effective response efforts.

** Includes costs of ransom(s) and downtime, does not include costs for infrastructure upgrades or professional services.

Conclusion

The Albert network monitoring system coupled with the SOC operated by CIS is an extremely effective and enormously cost-efficient investment in protecting SLTT organizations against malware threats, including ransomware. While this paper examined the specific benefits against ransomware, there are a large number of other malware threats that are similarly detected and mitigated by Albert and the SOC. As one customer noted: *"The MS-ISAC might be the most effective and efficient defense against cyber-attacks in the entire government."*

References

SOURCES

- Coveware Q1 Ransomware Market Report

  https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases

SUPPORTING SOURCES

- Symantec 2019 Internet Security Threat Report

  https://www.symantec.com/security-center/threat-report

- Statescoop

  https://statescoop.com/ransomware-local-government-pays-10-times-more/

- TrendMicro 2019 Ransomware Report

  https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/narrowed-sights-bigger-payoffs-ransomware-in-2019

- Malwarebytes Labs

  https://blog.malwarebytes.com/ransomware/2019/05/ransomware-isnt-just-a-big-city-problem/

- Comparitech

  https://www.comparitech.com/antivirus/ransomware-statistics/