Bullwall RansomCare

ARPA Presentation

Stoughton Common Council Meeting

Tuesday July 26, 2022

What is Ransomware?

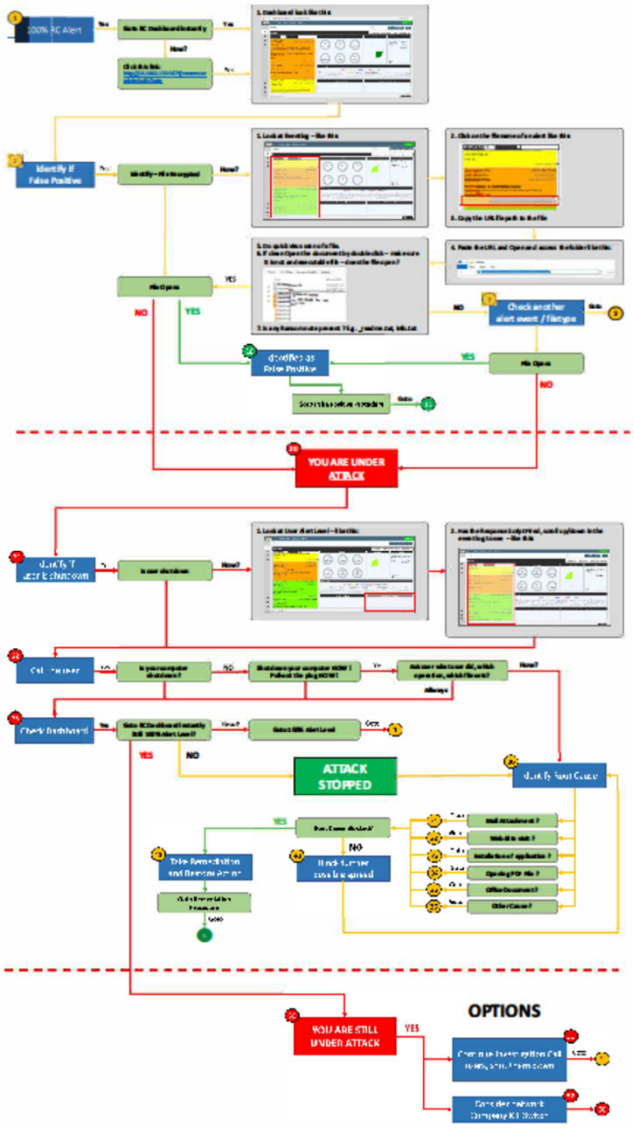
- Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom.
- Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations.

Bullwall Response Workflow

Bullwall is an inline software application that acts as a supplement to our various existing end-point protection.

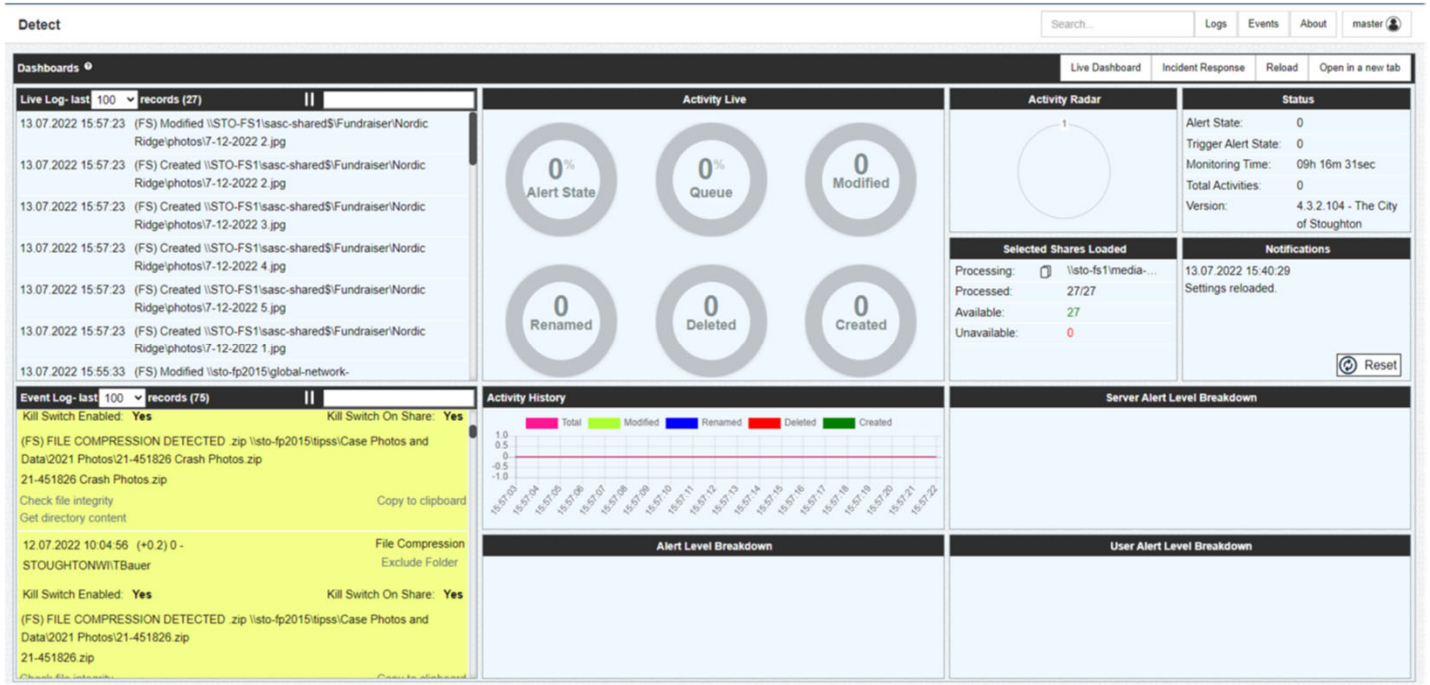
Barracuda and Symantec guard against and filter many of the obvious threats but does not however take action once a threat has been introduced. As you will see, Bullwall has the means to effectively prevent a malware threat from taking hold of our file systems.

The flowchart to the right follows a logic plan of ‘if-then-else’ to filter out normal activity from false positives.



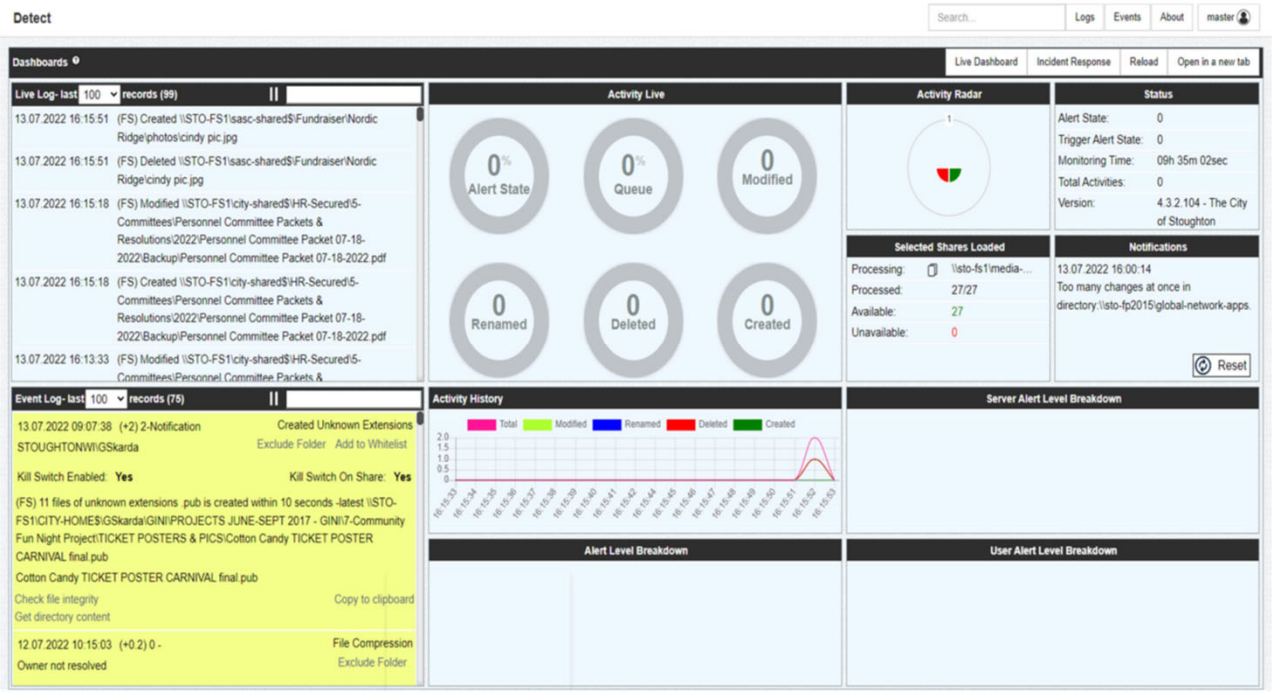
Passive State

Bullwall passively monitors all network shares to ensure file integrity and detects any usual file changes.



Active State

Several thresholds exist that trigger a reaction within the software algorithms. Each trigger raises the awareness threat level.



Active attack executed

The IT department launched an attack manually against a network user's computer.

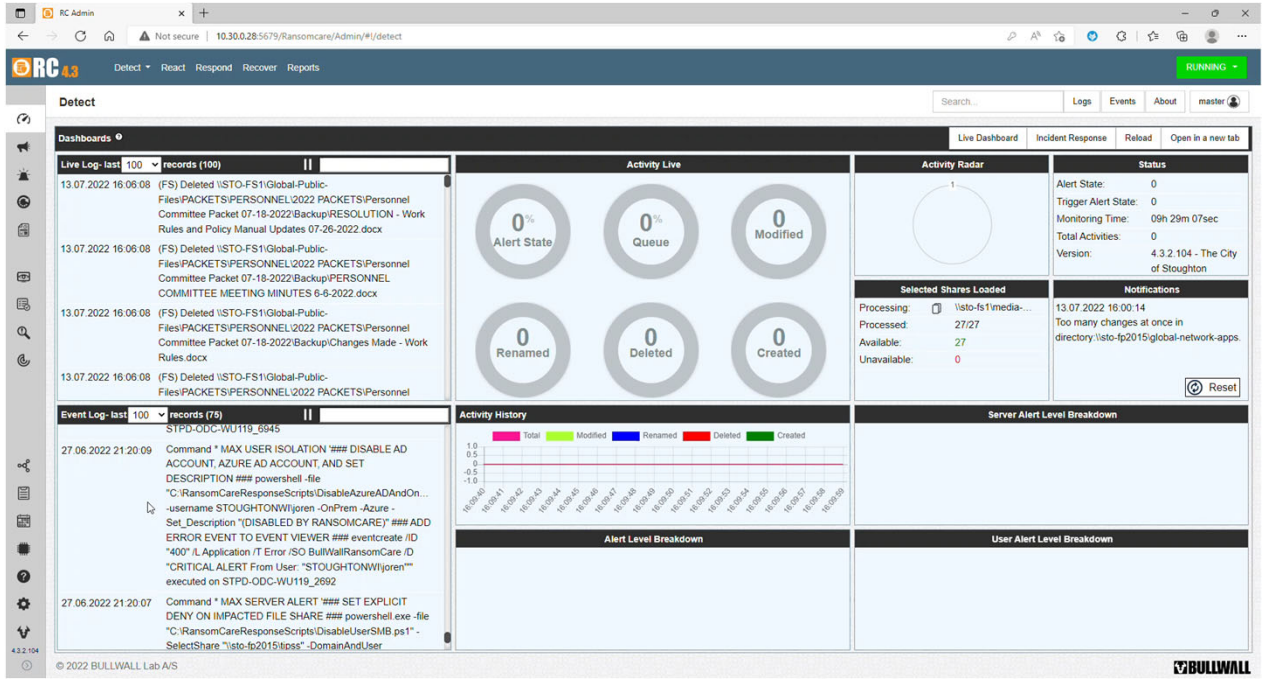
The files attacked in this exercise were stored on one file server that contains:

All city department H:\, S:\ drives and T:\. (excluding PD)

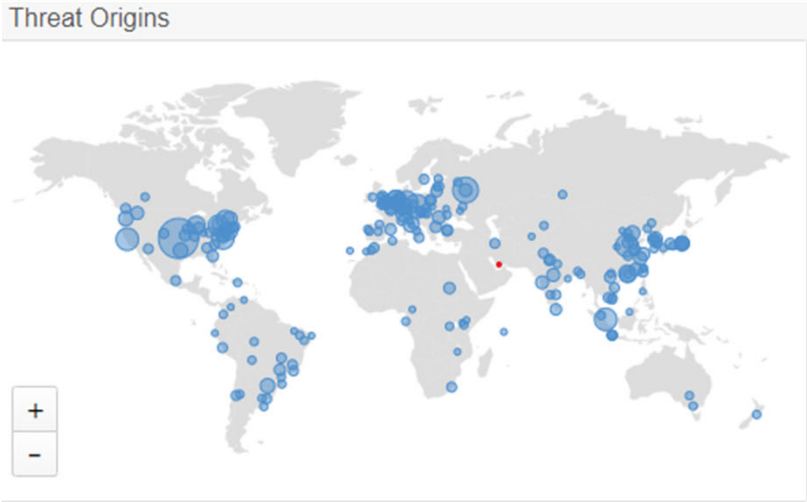
871 GB of data
835,153 files
70,337 folders

In this exercise, only 27 files were encrypted before the user was:

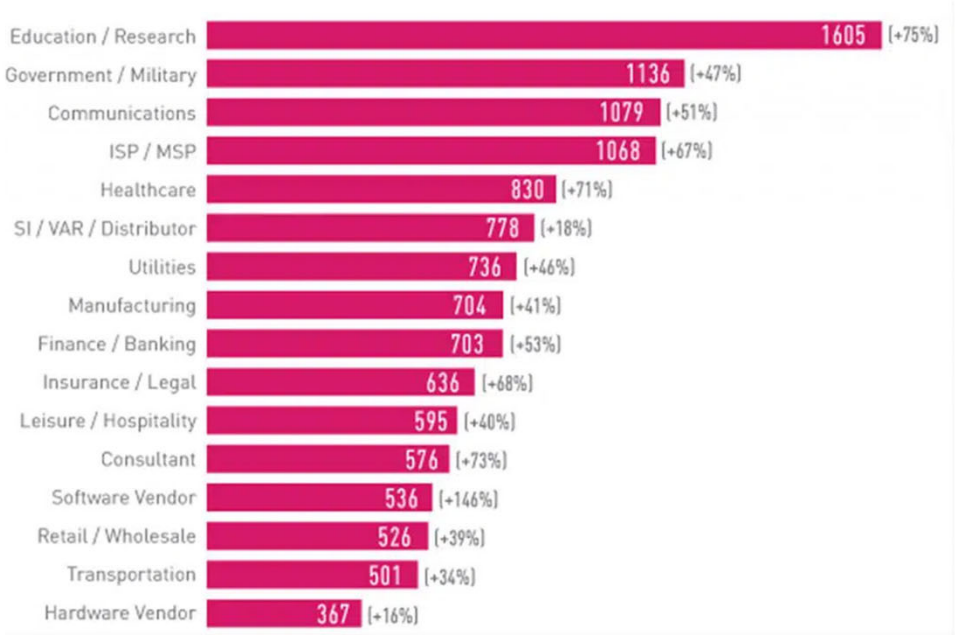
1. Locked out of all shared folders
2. Removed from Active Directory (the domain).
3. Their workstation powered off



Threat origins 6/15 – 7/14, 2022



Average weekly attacks per organization, by industry 2021, compared to 2020



Source: Checkpoint Research

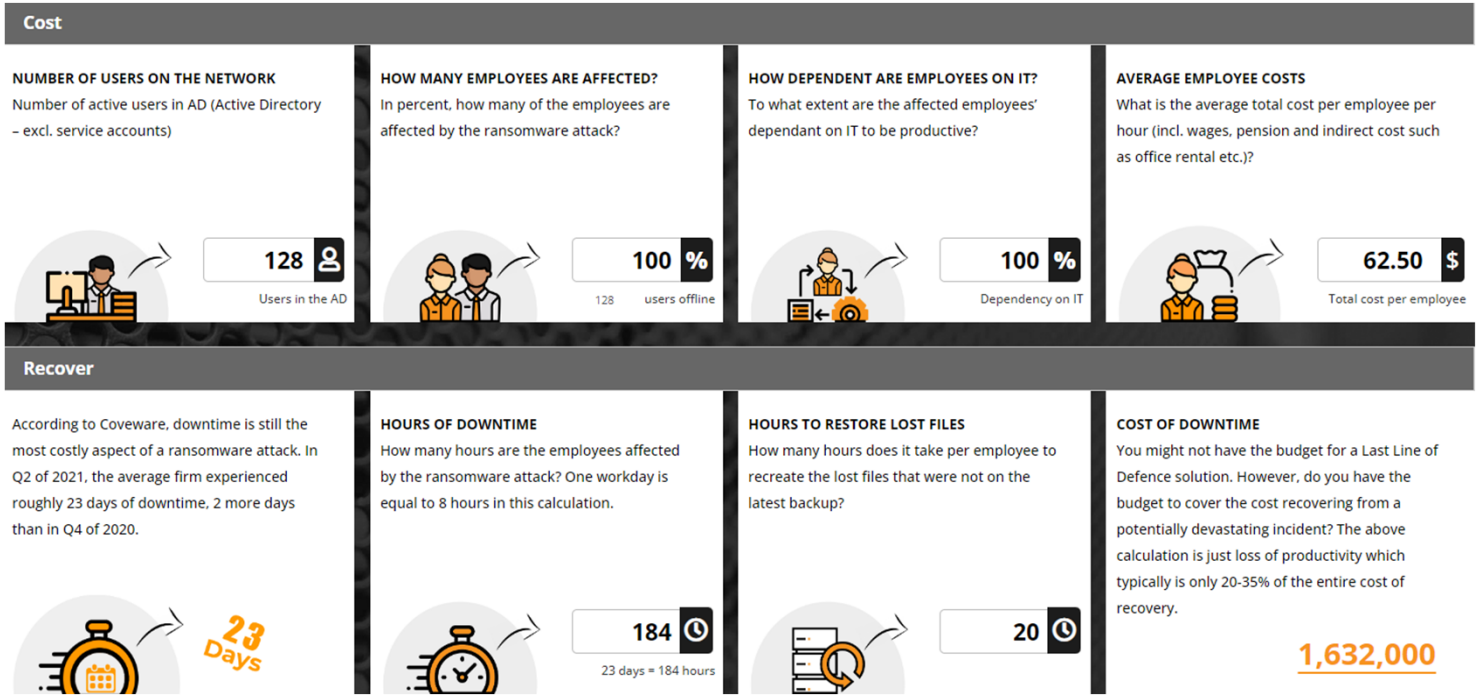
Cost of a Ransomware Attack

IT ARPA REQUEST

The example shown is based on both hard and soft costs of a recovery from a ransomware attack.

The cost of this software for year one is $13,288.32 and one year agreement. Each additional year would be $9,688.32 unless a multi-year agreement is executed.

Considering the loss potential I am requesting ARPA funds be provided and applied to the first year.



CITY OF STOUGHTON
DEPARTMENT OF INFORMATION
TECHNOLOGY AND MEDIA SERVICES
321 S. Fourth Street
Stoughton, WI 53589

JOHN T. MONTGOMERY
DIRECTOR
jmontgomery@ci.stoughton.wi.us

Thank you for your consideration.