ActZero

The Rise of Double Extortion Ransomware

Exponentially illustrates importance of ransomware detection

Cyber crime is continuously evolving. New tactics and techniques are being evaluated and used be adversaries to attack businesses like yours. One of the most dangerous changes is the rapid adoption of the double extortion tactic - the adversary's blunt attempt to kick you while you're down.

The Rise of Double Extortion

The double extortion practice is a two-stage attack: 1. The adversary extorts money for the ransomware attack, and 2. they extort money again through giving a second ransomware notice for the data it had stolen. The practice was somewhat unknown until late 2019 when the Maze ransomware caught the world's attention as the first high-profile case of double extortion. Since then, it is being seen used in practice by countless adversaries.

Why Back-ups aren't enough

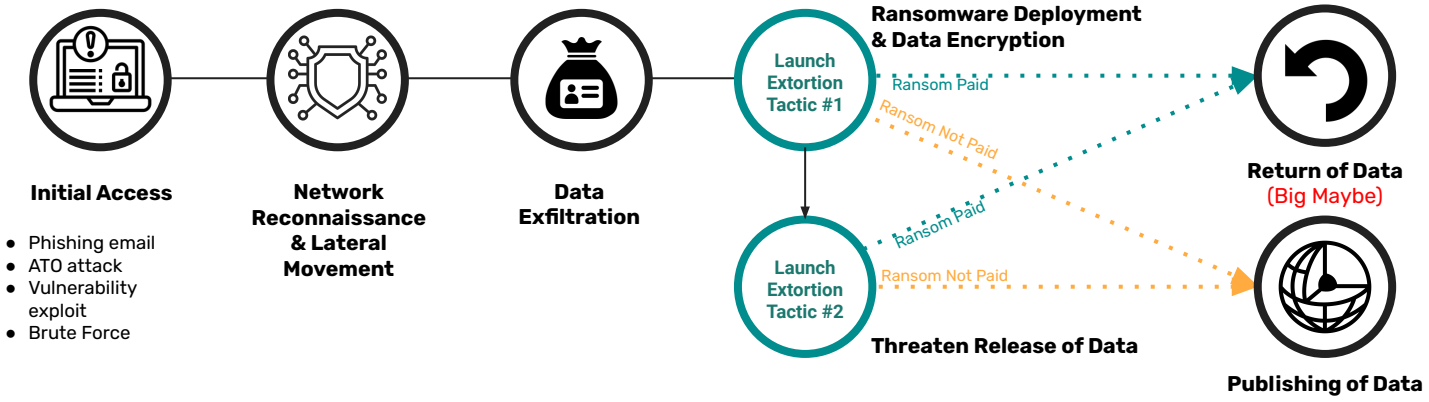
Many organizations feel they're protected against double extortion because they have backed up their data and can recover it. This simply isn't true, and can lead to a false sense of security. Sure, recovery of the data is a good thing, but usually only results in 90% restoration, The greater problem is, there is never a guarantee that payment will result in your data being released to you. In fact, 92% of the time, it won't be.

92%
of organizations don't get all their data back, even if a payment was forthcoming

Regardless of whether or not you can recover from back-ups, your 'unreturned' data or documents—classified, proprietary, or even containing personally identifiable information (PII) — is now circulating in the black market, putting your organization, customers, partners and even investors at risk. This practice is often referred to as 'Doxing'.

How does it work?

Hackers generally do their homework, tailoring any attack to the targetted company. They know where to hit your weak spots. Once inside, they Move quickly and stealthily, exfiltrating data before locking down systems for Tactic 1. Regardless of whether or not a victim pays, once the systems are unlocked, they'll then shift to Tactic 2, threatening the release of data that they'd early stolen, unbeknownst to you.



Defending Against Double Extortion

Defending against these attack tactics isn't a one and done step. It's a continuous effort that includes:

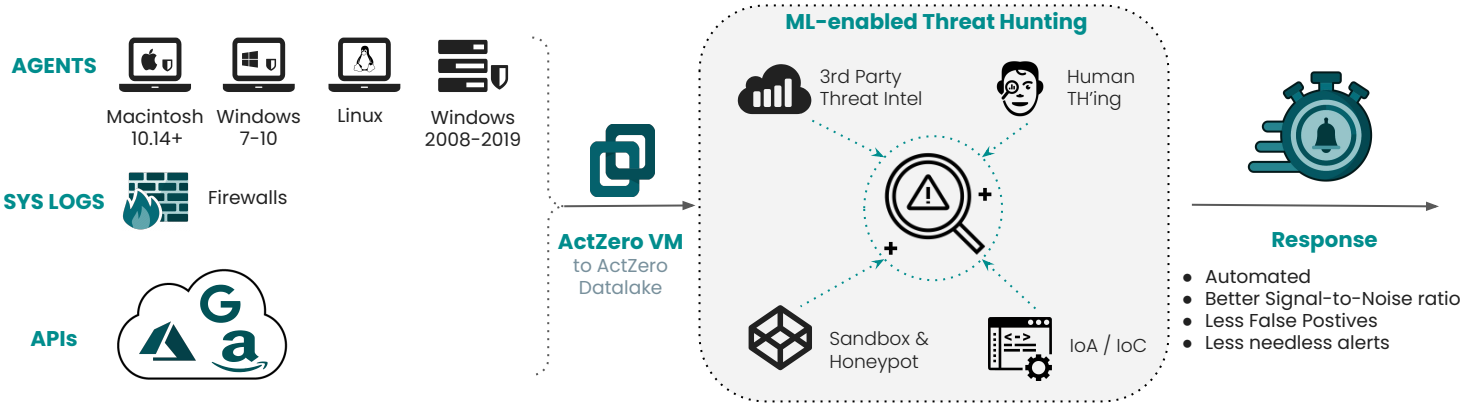
- Proper cyber security hygiene - keeping systems current and expeditiously patched
- Having robust back-ups to ensure full restores, if you can't recover everything
- Having a security solution in place that can detect, isolate, and mitigate threats early before they propagate
- Employing aggressive response measures to be able to quickly address issues as they arise
- Considering cyber insurance to cover financial losses from operational disruptions, loss of business, fines and even lawsuits

Why Machine-Learning enabled Detection and Response is critical

Detecting and identifying potential ransomware threats requires human and technological elements to be effective.

To help solve the challenge facing customers in battling ransomware, ActZero launched a new detection in December 2021 that combines threat signals from multiple signals to enhance the utility of the individual vectors in predicting and stopping ransomware attacks. Machine learning modeling and multiple-source detections will be used to enhance this detection in the near future. This new detection capabilities focus on:

- Combining high-fidelity detections for ransomware and exploits to specifically defeat double-extortion threats
- Integrating broader, and lower-fidelity detections to correlate the results with the first part of the feature, and generalize the results



Only with a deep, comprehensive, and evolving understanding of your organization's environment can ActZero offer such real-time detection and response to sophisticated ransomware attacks.