ATTIVO NETWORKS DATACLOAK, INNOVATIONS FOR HIDING DATA AND DENYING ACCESS TO ATTACKERS

INTRODUCTION

Despite layers of security, attackers are still successfully breaching organizations and gaining access to critical data to steal intellectual property or extort with ransomware demands. Given the APT-style tactics that attackers use, they can take valuable intellectual property and command massive payments from their victims. Businesses now pay more than 50% of the time as they frantically attempt to secure their data and restore operations. There are detection gaps in every security control that tries to stop them, and the attackers know these well. It's time to change the game.

Attivo Networks innovation delivers the ability to hide and deny access to the data that attackers seek – from files, folders, removable storage, and cloud and network shares to the Active Directory information they need to gain privileges. This novel approach is unlike any other security control that cybercriminals have seen before, and it is sure to derail their efforts and stop them in their tracks.

The Attivo DataCloak concealment framework works hand-in-hand with a layered defense strategy and prevents attackers from discovering the data they are seeking. Attackers cannot find nor access data from files, folders, mapped network and cloud shares, removable drives, or Active Directory. The solution goes one step further than detection to prevent the threat actor from advancing their attack by providing them with fake data that guide their paths straight into a decoy. Here, the decoys gather attack telemetry, and native integrations automatically isolate the infected system.

To follow are specific use cases for derailing ransomware activity, Active Directory attacks, and threat reconnaissance.

SCENARIO 1

- Ransomware infects the endpoint system
- Attempts to encrypt files, cloud folders, and shares and steal credentials
- Attivo hides and denies unauthorized access to real files, folders, shares, and credentials
- Endpoint Detection Net protects the data and raises alerts in the dashboard

WHAT IT DOES

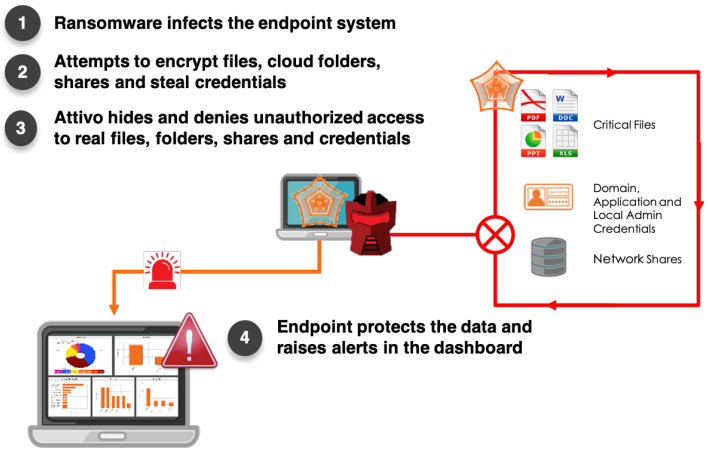
- Detects the known & unknown
- Prevents Data Destruction
- Exploit Blocking
- Lateral Movement Blocking
- Discovery Blocking

This is particularly useful because you can prevent lateral ransomware propagation and prevent local folder/file encryption.

© 2021 Attivo Networks. All rights reserved.

Some of the things that can be hidden:

- DFS and network shared drives from untrusted applications
- Local folders and files from untrusted applications
- Removable disks from untrusted applications

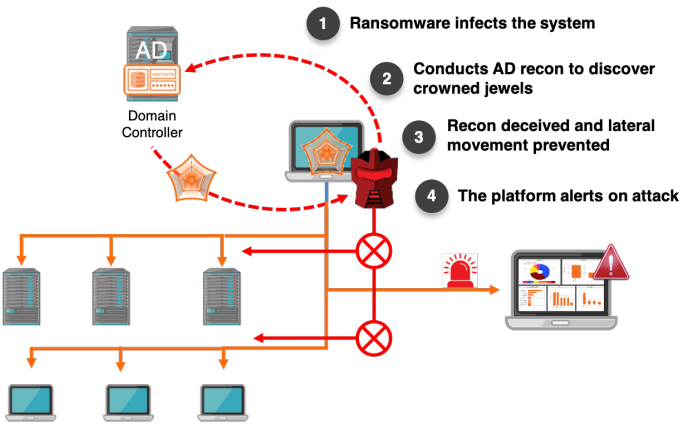


SCENARIO 2

- Ransomware infects the endpoint system
- Conducts Active Directory recon to discover crown jewels
- Recon deceived, and lateral movement prevented
- Alerts in the dashboard
- Infected endpoint automatically isolated
- Plus, you have now fed the attacker fake AD objects that steer them to decoys

WHAT IT DOES

- Hides info, protects critical objects
- Returns deceptive objects to the attacker
- Supports popular AD objects (admin, service, critical computers, net sessions)
- Telemetry for visibility & hunting
- No changes to production AD
- Ultimate protection against AD recon and Local Administrator privilege escalation



© 2021 Attivo Networks. All rights reserved.

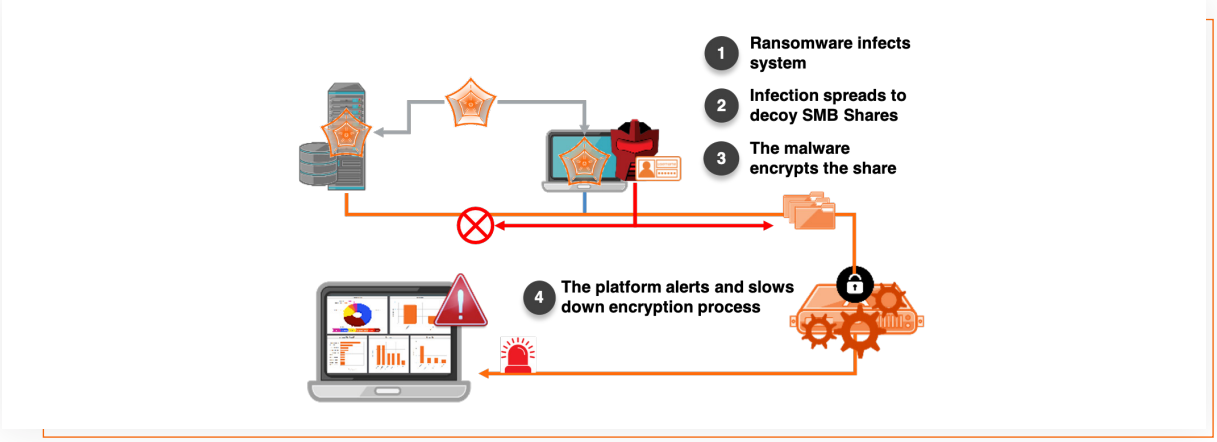
SCENARIO 3

- Ransomware infects the endpoint system
- Infection spreads to decoy SMB Shares
- The malware encrypts the decoy share
- The solution feeds attacker fake data and throttles down the encryption process
- Alerts in the dashboard
- Infected endpoint automatically isolated

WHAT IT DOES

- Discovery blocking
- Lures malware to decoy drives
- Feeds fake data
- Slows the encryption process
- Automates isolation

Collectively, these solutions will dramatically reduce the ability of an attacker to find their targets, move laterally, and escalate their privileges. This functionality in the Attivo ThreatDefend Platform is also available within the standalone Endpoint Detection Net Suite and ADSecure protection solution.



ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in preventing identity privilege escalation and detecting lateral movement attacks, delivers a superior defense for countering threat activity. ThreatDefend® Platform customers gain unprecedented visibility to risks, attack surface reduction, and speed up attack detection. Patented innovative defenses cover critical points of attack, including at endpoints, in Active Directory (AD), in the cloud, and across the entire network. Concealment technology hides critical AD objects, data, and credentials. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys derail lateral movement activities. Attivo has won over 150 awards for its technology innovation and leadership. www.attivonetworks.com.

© 2021 Attivo Networks. All rights reserved.