Effectively Combating Zero-Day Ransomware

DECEPTION TECHNOLOGY + EDR
Growing Ransomware Threat

It's a big problem that is getting bigger, and the data indicates a lack of protection from this type of malware in organizations, but that can be stopped.

Verizon DBIR 2020 on Ransomware

...Using indicators of compromise (IOCs) alone to determine impact from these threats is not a durable solution, as most of these ransomware campaigns employ “one-time use” infrastructure for campaigns, and often change their tools and systems once they determine the collection capabilities of their targets...

Microsoft blog
Data backups are no longer a safety net for Ransomware threats.
Data Exfiltration and Extortion added to Crypto-Ransomwares

Sodinokibi Ransomware Publishes Stolen Data for the First Time

Lawrence Abrams
2-3 minutes

For the first time, the operators behind the Sodinokibi Ransomware have released files stolen from one of their victims because a ransom was not paid in time.

Since last month, the representatives of the Sodinokibi, otherwise known as REvil, have publicly stated that they would begin to follow Maze’s example and publish data stolen from victims if they do not pay a ransom.

Allied Universal Breached by Maze Ransomware, Stolen Data Leaked

Lawrence Abrams
7-9 minutes

After a deadline was missed for receiving a ransom payment, the group behind Maze Ransomware has published almost 700 MB worth of data and files stolen from security staffing firm Allied Universal. We are told this is only 10% of the total files stolen and the rest will be released if a payment is not made.

Nemty Ransomware to Start Leaking Non-Paying Victim’s Data

Lawrence Abrams
3 minutes

The Nemty Ransomware has outlined plans to create a blog that will be used to publish stolen data for ransomware victims who refuse to pay the ransom.

A new tactic started by the Maze Ransomware and now used by Sodinokibi is to steal files from companies before encrypting them. If a victim does not pay the ransom, then the stolen data will be leaked little-by-little until payment has been made or it has all been

Data Backups no longer a safety net

Copyright 2020. Acalvio Technologies Inc.
Targeted and APT Style Attacks

• Leverage advanced techniques
  • Deep understanding of security layers
    • Avoid using vssadmin
    • Proxy execution of commands
    • Avoid sinkholing
    • Anti debugging techniques
    • Avoid blocking by IPS
  • Living of the land techniques
  • Very Stealthy

• Often human assisted

Maze is a ransomware created by skilled developers

Ransomware adopts Deception

All Mitre Tactics
Maze Ransomware: 30+ Victims in 1 year

Maze Ransomware to cost Cognizant $50-$70 million, impact to continue beyond Q2

Maze ransomware operators have infected computers from Medical Diagnostic Laboratories (MDLab) and are releasing close to 9.5GB of data stolen from infected machines.

US aerospace services provider breached by Maze Ransomware

Business services giant Conduent hit by Maze Ransomware

Chubb Cyber Insurer Allegedly Hit By Maze Ransomware Attack

Maze ransomware fails to encrypt Pitney Bowes, steals files

The actor also followed through with leaking an additional cache of files belonging to another of its victims that did not pay the ransom, Southwire, a wire and cable manufacturer from Carrollton, Georgia.
Can the next Maze or Ryuk Ransomware version be stopped on day zero?

YES.

USING A UNIQUE COMBINATION OF ADVANCED DECEPTION AND EDR
Advanced Deception Technology

AN ACE UP THE THREAT DEFENSE SLEEVE
What is Advanced Deception Technology?

**ADD TO NETWORK**
- End points
- Applications
- IoT devices
- Cloud Decoys (S3)

**LEAD TO DECOYS**
- Credentials
- URLs
- AD
- Network Traffic

**TRIP WIRES**
- Beaconing Docs
- Processes
- Tools

**MAKE DECEPTIONS ATTRACTIVE**
- Vulnerabilities
- Mis-configurations
- Default/weak credentials

**Modern Deception Platform**
- Rich Deception Palette
- Extensible & Customizable
- Automation

**Advanced Deception Tech**
- Intelligent (AI-based)
- Dynamic Deceptions (SDN)
- Autonomous
- Active System
#1 Fighting Fire with Fire

- Attackers rely on Deceptions besides heavy Automation
  - Ransomwares like Maze, Sodinokibi, Ryuk and Ragnar Locker
  - Deep Fakes like CEO voice
  - Phishing Emails

- Defenders can now fight back with Advanced Deceptions to stop known as well as Zero-Day Ransomware
# 2 Advanced Deception Tech is *game changer*

- **Dynamically change the landscape**
  - Observe & Analyze

- **Give Attackers the Opportunity they seek**

- **Ferret Latent Threats**
Acalvio Ransomware Kill Chain

Concept:
• Using Advanced Deceptions give opportunity for Ransomware at each step
• Combined observations by Acalvio and CrowdStrike
• Detects and Confirms Ransomware Threats even zero-day
Detect Ransomware Threats
- Known and Zero-Day
- Combined Deception & ML based approaches
- Inside Corp network, OOO, @HOME
- Built-in Threat Confirmation

Automated, Real Time Response
- Threat Detection with precision and speed enables automated response

Responses
- Detect Ransomware
- Deploy Deceptions
- Baits
- Decoys
- Lures
- Watch deception
- Combine observations
- Raise Alert
- Notification
- Isolate Device(s)
- Protect VLANs
- Kill Process
- Protect files on endpt
Acalvio and CrowdStrike are both Cloud-based SaaS

Detect and Mitigate known and zero-day ransomware everywhere