

MAGNET AXIOM CYBER™

FOR RANSOMWARE

THE CHALLENGE:

Frequency and complexity of ransomware has risen dramatically.

Attempted ransomware attacks increased 435% in 2020 compared to 2019.¹ Cybercrime Magazine predicts that a ransomware attack will happen every 10 seconds, compared to one every 14 seconds in 2019, and one every 40 seconds in 2016.²

It's not a matter of if a ransomware attack will be successful, but when.

The most common initial point of compromise for a ransomware attack originates from a malicious link or document in a phishing email. Phishing emails are designed to be highly convincing and unfortunately have a high success rate: 74% of organizations reported successful phishing attacks.³

Once a bad actor has gained access to an enterprise's network, typical attack behaviors include:

- Laying dormant and researching where the most sensitive files and data are stored, this could be months that a bad actor has free reign over a business' network.
- Mandiant reports in their 2021 M-Trends threat report that the global median dwell time that bad actors have on a network is 24 days.⁴ While this number is trending down, bad actors only need days to successfully deliver their ransomware payload and cripple businesses.
- Bad actors will move laterally through a network using remote desktop internally to gain user credentials and ultimately access to main databases and SQL servers.

¹ <https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-----what-you-need-to-know-for-2021/?sh=1d74f5fc58d3>

² <https://safeatlast.co/blog/ransomware-statistics/#gref>

³ <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>

⁴ <https://www.darkreading.com/threat-intelligence/global-dwell-time-drops-as-ransomware-attacks-accelerate/d-d-id/1340663#:~:text=In%20their%202021%20M%2DTrends,has%20fallen%20to%2024%20days.>

MAGNET FORENSICS' SOLUTION

Magnet AXIOM Cyber can acquire and ingest images and memory from data sources (Windows, Macs, and Linux) for forensic analysis to identify and validate the initial point of compromise of a ransomware attack and use that information to improve an organization's security posture.

Using powerful analytics features like Timeline, Magnet AXIOM Cyber enables forensic examiners to immediately begin their investigation with a known event (such as the execution of a malicious file or creation of a ransomware note) and then build a timeline of events to work backward to the root point of compromise.

Using an artifacts-first approach, AXIOM Cyber will surface relevant artifacts that will help an examiner identify behavior common to ransomware attackers. Artifacts which are especially helpful for ransomware investigations include:

- **Remote Desktop Protocol:** Since bad actors will often leverage RDP to move laterally through a network, having an at-a-glance view of all RDP events helps an examiner narrow their focus and get to the evidence they need.

The screenshot displays the Magnet AXIOM Cyber interface. On the left, a sidebar lists various artifact categories with their counts: MATCHING RESULTS (3,632), WEB RELATED (17), DOCUMENTS (470), OPERATING SYSTEM (3,145), \$LogFile Analysis (1,182), AmCache File Entries - Legacy (3), Remote Desktop Protocol (12), Shellbags (2), Startup Items (1), UserAssist (7), and Windows Event Logs (1,938). The 'Remote Desktop Protocol' category is selected. The main area shows 'MATCHING RESULTS (12 of 45)' in a table format. The table has columns for Event ID, Created Date, Registry Path, Directory, and Event Description Summary. Several rows are highlighted in blue, indicating matches for Remote Desktop Protocol events.

| Event ID | Created Date | Registry Path | Directory | Event Description Summary |
|----------|-----------------------|---------------|-----------|---|
| 25 | 10/30/2019 2:06:38 PM | | Incoming | |
| 25 | 10/30/2019 2:06:38 PM | | Incoming | |
| 25 | 10/30/2019 2:06:38 PM | | Incoming | |
| 4648 | 10/30/2019 2:06:38 PM | | Incoming | A logon was attempted using explicit credentials. |
| 4624 | 10/30/2019 2:06:38 PM | | Incoming | An account was successfully logged on. |
| 4648 | 10/30/2019 2:06:38 PM | | Incoming | A logon was attempted using explicit credentials. |
| 4624 | 10/30/2019 2:06:38 PM | | Incoming | An account was successfully logged on. |
| 4648 | 10/30/2019 2:06:38 PM | | Incoming | A logon was attempted using explicit credentials. |
| 4624 | 10/30/2019 2:06:38 PM | | Incoming | An account was successfully logged on. |
| 1149 | 10/30/2019 2:06:38 PM | | Incoming | |
| 1149 | 10/30/2019 2:06:38 PM | | Incoming | |
| 1149 | 10/30/2019 2:06:38 PM | | Incoming | |

- **Evidence of Timestomping:** When timestamps of files are altered, it's a common indication that these files were involved in a malicious attack. AXIOM Cyber is able to identify files that demonstrate evidence of timestomping giving investigators another way to expedite ransomware attacks.
- **Email:** The Email artifact is another extremely useful artifact to help pinpoint how a malicious file was delivered to an email inbox and its origin. A preview of the email is viewable in addition to details about the email itself that are forensically relevant.
- Many other artifacts such as Prefetch Files, Windows Event Logs, and \$LogFile activity are insightful as they empower an examiner with the information they need to quickly and thoroughly investigate a ransomware attack.

Lastly, AXIOM Cyber's reporting capabilities make it easy for examiners to share their findings with relevant parties so key findings can be socialized and then later incorporated into future cybersecurity prevention and remediation practices.

Learn more at magnetforensics.com