International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 2, March- April 2024 |

DOI:10.15662/IJEETR.2024.0602010

Ransomware Resilience for Pipeline Operators

Vilas Shewale

Independent Cybersecurity Researcher, USA

ABSTRACT: The Colonial Pipeline breach in May 2021 effectively rendered ransomware against pipeline operators a real concern. In the 3 years since the breach, BlackCat, LockBit, the CL0P group with their MOVEit data theft exploit, Play Ransomware and Akira Ransomware, amongst others, have all attacked pipeline operators. Simultaneously, authorities such as the TSA have issued new requirements and the SEC's cyber disclosure ruling took effect in December 2023. This paper investigates the nature of the ransomware threat today, the anatomy of a ransomware incident impacting a pipeline and outlines an architecture of defense-in-depth based on five essential capabilities: Prevention, Limitation, Detection, Response and Recovery. Finally, it addresses critical issues affecting pipeline ransomware incident response: reliance on manual operational procedures, the decision-maker responsible for ransom payment and the regulatory compliance and reporting deadlines imposed in parallel to incident response activities.

KEYWORDS: ransomware, pipeline cybersecurity, recovery, incident response, SEC disclosure, TSA directives.

I. INTRODUCTION

The ransomware risk to U. S. Critical infrastructure has grown since Colonial Pipeline was crippled three years ago. As the 2024 pipeline ransomware threat has evolved, attackers, new tools, expanded targets and tightening regulation have converged to force pipeline operators into managing a different set of challenges. The problem remains, of course, fundamentally recognizable, but the operational circumstances have been transformed. A pipeline operator faces it now, 3 years later, the circumstances that drove the decisions and activities that this paper advocates and explains were far less developed in 2021.

This paper covers three core topics. Section 2 surveys ransomware attacks against U. S. Pipeline operators since 2021, I show how attackers' modus operandi, tools and victims have changed, as have defensive activities and approaches. Section 3 dissects how ransomware attacks specifically impact pipeline operators and their unique responses. I explore attack surfaces and impact zones, operational constraints during incident response and how the different parts of a pipeline's control system are susceptible to attack. Section 4 explains a defensive posture we have termed "defense-in-depth resiliency. " Section 5 discusses how responding to ransomware is fundamentally different in pipeline-specific operations versus general IT settings. Finally, I briefly speculate on the current and projected direction of the pipeline industry's response to this ongoing menace.

II. THE RANSOMWARE ERA FOR PIPELINES

This trend did not start and stop with Colonial. Ransomware attacks do not always target pipeline operators. The attack that shut down Colonial in the first place happened to its IT network ransomware operation (which incidentally resulted in Colonial deciding to shut down its pipeline [1]). We have seen many events since then with similar narratives: a ransomware group hacks an IT environment, jumps from that to an OT network common between both systems and the pipeline company faces the tough decision to pause operations to contain damage.

The most dominant ransomware services in that time include LockBit (active before disruption in February 2024)[2], one of the largest active affiliate networks, which affected oil & gas and manufacturing organizations. BlackCat/ALPHV targeted critical infrastructure operators and has become notable for the MGM incident in 2023 (both FBI and CISA put out advisories throughout the year)[3]. CL0P launched attacks through exploitation of zero-days on the Progress MOVEit product in May & June of that year. They eventually hacked data from hundreds of organizations[4]. Royal, Play, Akira all ran various other campaigns, CISA issued an alert in December 2023 detailing ransomware activity carried out by the Play group targeting critical infrastructure.[5]

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 2, March- April 2024 |

DOI:10.15662/IJEETR.2024.0602010

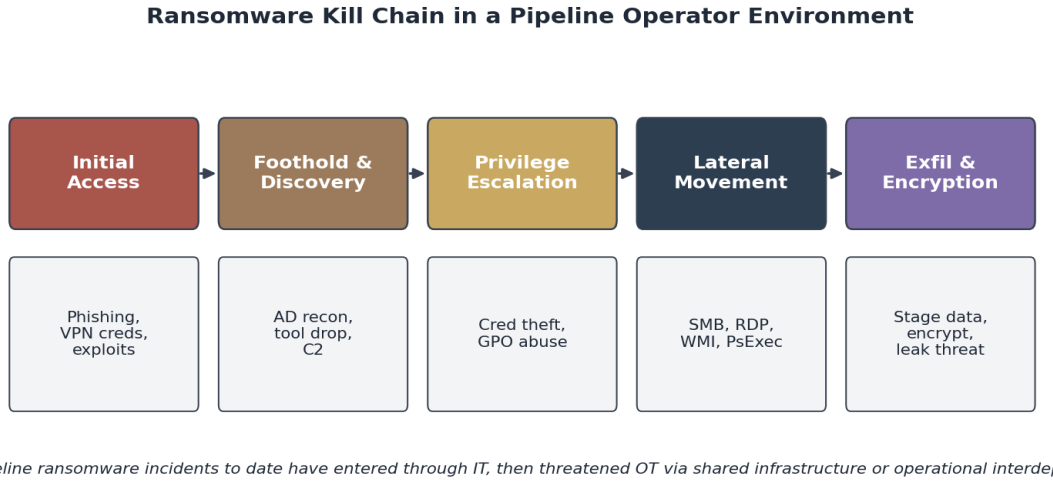

Figure.1. Ransomware kill chain in a pipeline operator environment. Most pipeline ransomware incidents enter through IT and threaten OT via shared infrastructure or operational interdependence.

Two themes emerged strongly from this assessment. OT-specific ransomware capability is scarce, most OT outages occur as a byproduct of an IT attack that infects the OT network via shared infrastructure or from operator intervention during a non-specific ransomware crisis, than through ransomware that is designed to encrypt PLCs and cause OT disruption. It is a fact that double-extortion has become a default tactic of ransomware criminals, in addition to encrypting data, the threat is to leak it to the public. While this may reduce the incentive to pay ransoms, it also introduces an exposure risk for pipeline operators. It poses the possibility that attackers may be able to extract and hold data and this cannot be mitigated with backups alone.

III. ANATOMY OF A PIPELINE RANSOMWARE INCIDENT

As shown in Figure 1, CISA and the security firms Dragos and Mandiant recently confirmed that many recent hacks against the energy sector followed such an attack. The typical first entry is via phishing emails, open Remote Desktop Protocol (RDP) ports or VPNs, unpatched flaws in routers, firewalls or perimeter services or malware placed on user devices [6]. Once a breach occurs, intruders carry out recon on AD, dump Cobalt Strike or equivalent tooling, install backdoors and secure their communication channels over the internet.

The privilege-escalation phase follows quickly and usually comes as a result of stealing credentials or the abuse of AD, GPO and local operating system vulnerabilities. The lateral-movement stage increases pressure on operators. Adversaries navigate through the network via protocols like SMB, RDP, WMI, PsExec and other methods to find important servers, such as those backing up critical files and systems that connect IT to OT networks.

Attackers will try to target the backup infrastructure in particular to cripple an operator. Encryption is carried out swiftly and ransomware groups often start exfiltrating data from victims before encrypting it, sometimes this continues for hours or even days. They also leave messages that detail instructions for paying, opening communication channels. Operators are left with a set of increasingly complex decisions.

IV. DEFENSE-IN-DEPTH RESILIENCE ARCHITECTURE

The resilience architecture in Figure 2 organizes capabilities into five layers: prevent, limit, detect, respond, recover. Each layer is necessary; none is sufficient. The composition is what produces resilience.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 2, March- April 2024 |

DOI:10.15662/IJEETR.2024.0602010

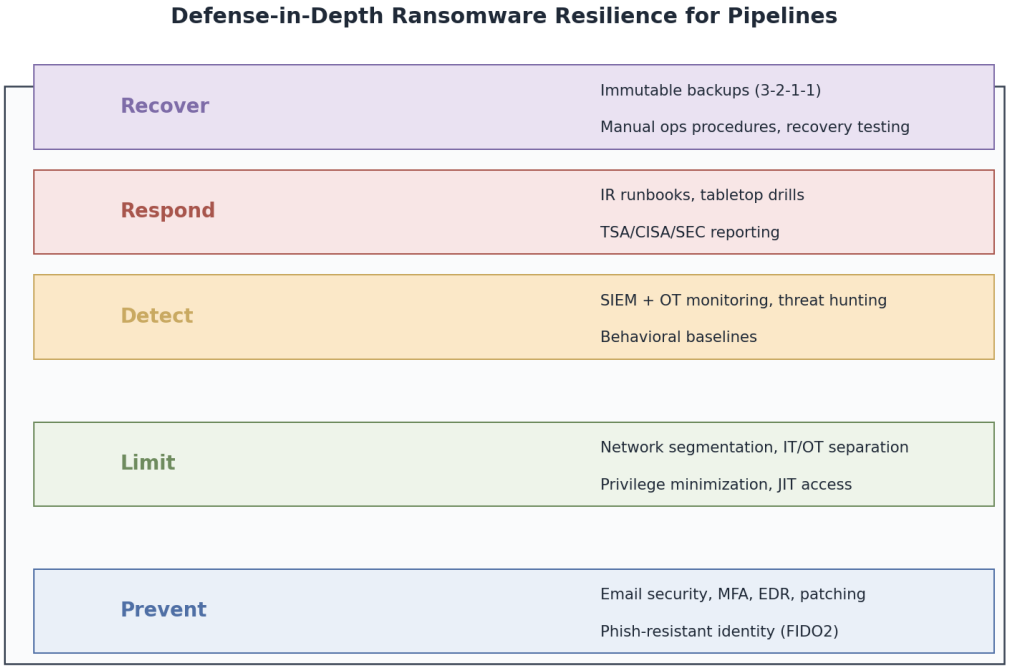

Figure2. Defense-in-depth ransomware resilience model for pipeline operators

4.1 Prevent

Your preventive measures target the main entry vectors exploited by malicious actors in incidents affecting the pipeline sector. When you equip all remote connections with phish-resistant multi-factor authentication, you mitigate credential theft, a tactic behind a significant number of these attacks. Furthermore, installing endpoint detection and response on engineers' computers, plus security for corporate email accounts, lays the foundational framework. Keeping up with patches is crucial, especially for outward-facing servers, CISA's catalog of Known Exploited Vulnerabilities serves as a helpful reference to determine priorities [7].

4.2 Limit

Limitation, in this context, means making sure your first move does not eventually compromise you completely. Isolating your IT systems from your OT systems with carefully planned and strictly monitored interfaces stops an IT compromise snowballing into an OT issue through implied security. Limiting privilege means nobody should have administrator rights they are not using right now (Just-In-Time Access). Nobody should ever have sitting administrator rights at all and administrative users should not use their email or do their browsing with those accounts. An attacker stealing an administrator password only gets a limited amount of utility out of it if there are no administrators on the OT network they are interested in.

4.3 Detect

The ransomware detection coverage should focus on both OT and IT, emphasizing actions relevant to ransomware behavior: credential theft tool usage, command-and-control (C2) communications, large-scale mass file modification and shadow copy removal. In addition to comprehensive IT security coverage by SIEM, operators of significant size are expected to have OT monitoring in place that is aware of OT protocols and devices, coordinated through an incident response plan across both sectors. Threat hunting should be conducted regularly to uncover undetected malicious activity.

4.4 Respond

Ability to respond comes from standard playbooks. These playbooks have been practiced many times both in exercises and real-world emergencies, as well as tied into reporting that has quadrupled since 2021. Companies are already reporting to TSA due to various TSA directives [8], reporting to CISA due to the Cyber Incident Reporting for Critical

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 2, March- April 2024 |

DOI:10.15662/IJEETR.2024.0602010

Infrastructure Act and companies which are registrants for the SEC have been mandated to report by the SEC's cybersecurity disclosure rule, which came into effect in December 2023 [9].

4.5 Recover

Recovery, therefore, dictates whether a system owner pays ransoms or refuses payment. To recover effectively, backups must be immutable (cannot be changed or deleted), physically separated from primary systems and routinely tested. A standard practice known as the "3-2-1-1 backup strategy" involves maintaining three copies of data, two on different types of storage media, one copy stored offsite and the last one being immutable. The 3-2-1-1 pattern is widely adopted by operational technology operators. Recovery planning must extend beyond mere restore-from-backup drills, it needs to account for all the steps required to reconfigure systems and validate their security status once systems have been recovered from a compromise affecting the domain controller. Manual operating procedures to maintain safe operations during recovery periods must be part of the disaster recovery plan, not something conceived in the heat of the moment.

One critical component of the recovery process that is often overlooked by operators: The speed of data recovery is primarily influenced not by the speed of backup throughput, but by the extent of the verification process. Reintroducing a system to production from a clean backup necessitates a thorough check of all affected components to ensure no evidence of an attack remains within the restored data. For a medium-to-large operational technology system, these checks can extend for several days. Operators that focus solely on the efficiency of backups while neglecting the associated validation costs often express surprise when their real-time recovery durations exceed expectations. Pre-emptively documenting these validation procedures and practicing them during recovery drills is the key to transforming a passive backup plan into a proactive recovery strategy.

V. OPERATIONAL AND REGULATORY CONSIDERATIONS

Pipeline ransomware incidents differ from generic enterprise incidents in several ways that the architecture above does not, on its own, address.

5.1 Manual Operating Procedures

Pipeline operations can, in many cases, continue at reduced capacity through manual procedures if SCADA visibility is lost. Maintaining those procedures, training operators on them, and exercising them as part of the resilience program is not optional. An operator who has never run a section of pipeline without telemetry will discover the limits of their procedures under the worst possible conditions.

5.2 Ransom Decision Authority

In the same fashion, a Ransom policy exists which a Board decision, not an operational decision, can decide on whether they want to negotiate payment. Each firm must have a policy in advance on ransomware and should define who will be authorized to decide the ransom negotiation on a given attack. Factors considered are operational cost to recover, amount of stolen data, sanctions risk, amount of cyber liability coverage and who the firm consults. Treasury advisories viaOFAC in regard to payment ransomware continually increase the risk of paying [10].

5.3 Regulatory Reporting Timelines

TSA is by far the quickest on their heels. After CISA (under CIRCIA) would come anything required from an SEC registrant. Note the 8-K Item 1.05 filingclock is not tied to detection of an incident but the determination of its materiality [9]. This leads to the dilemma of needing to act both swiftly and defensibly-the material determination cannot be ignored too long without facing a negative legal consequence, nor can it be rushed to closure without creating a negative operational problem.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 2, March- April 2024 |

DOI:10.15662/IJEETR.2024.0602010

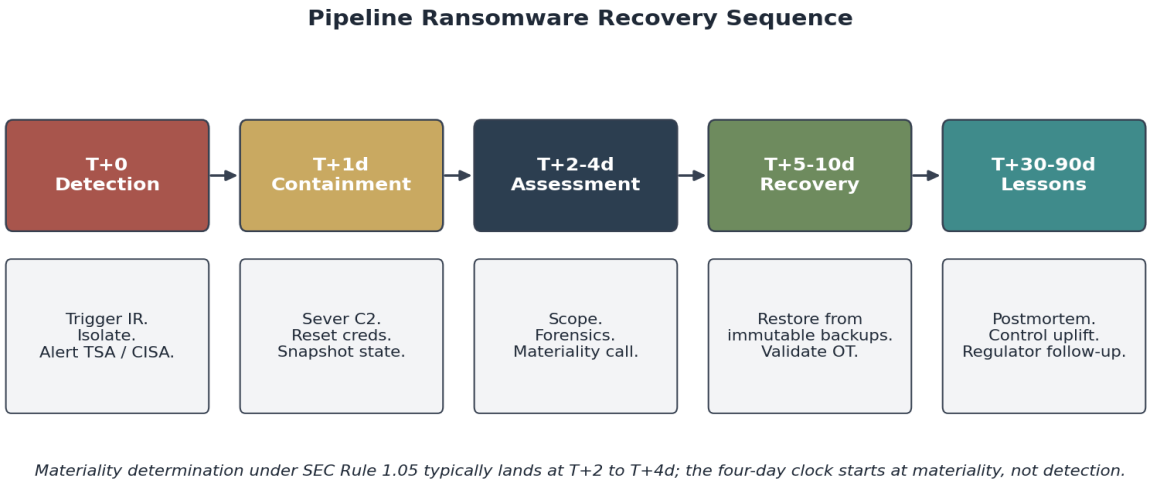

Figure.3 Pipeline ransomware recovery sequence with regulatory reporting clocks overlaid.

5.4 Insurance and Legal Posture

Yes, the cyber insurance landscape has matured from Colonial Insurance Company to Alliant Insurance Brokers and, currently, Arctic Wolf. The questionnaires are now granular. We get asked about: What is the multifactor authentication solution being used for access to all sensitive systems, cloud and on-premise? What endpoint detection response tools are in use to monitor for malicious activity? What solutions are being used for immutable backups for critical systems, servers, etc.? Do you retain a third-party cybersecurity incident response provider on retainer, ready to activate immediately? Is there a contractual exclusion from the policy against covering payments to sanctioned individuals or entities as listed by any sanctions regime, such as the United States Treasury? Is the ransomware-specific insurance sub-limited? Use the application like the control questionnaire you answer as accurately as possible to create a list of your known weaknesses, these answer sheets are more informative and drive your priorities better than the insurance policy itself. The last part is the most important part as I discussed earlier, but many miss it: Legal prep includes pre-retained breach counsel, forensic firm retainer and a solid grasp of which communications during an event have attorney-client privilege. It is the height of inefficiency-and of high costs-to start searching for that on hour two of your first breach response.

5.5 Tabletop Exercises and Live Drills

No one tests incident plans when things are running fine, so those plans typically do not fare too well when an incident actually occurs. Mature security organizations regularly conduct tabletop exercises that test the process (every quarter for core responders, once a year for the executive group) and follow them with hands-on drills that practice the technical restoration steps. The best exercises are the tricky ones, those that involve an anomaly such as an unsuccessful restore from a backup, a regulatory timer that kicks in earlier than expected or an employee account that provides backdoors to the network. Organizations that drill only for standard cases will learn during a real incident that all of the hardest issues, which require far more complex interventions, are also the kinds of problems they encounter.

The mid-2023 MOVEit campaign showed a scenario that almost no operators had practiced before: the attacker actually exploited vulnerabilities at an innocent third-party vendor, not at the victim operator, but the operators themselves bore the immediate consequences of exposed data, the need to notify authorities of a breach and communicating it to their clients [4]. Training exercises in the future must include such a scenario wherein the organization is not a direct attack victim but a downstream affected entity, training will be essential so that responders coordinate with (but do not always lead) their internal technical support team.

VI. CONCLUSION

By now, they know that much more can be done. The set of technical controls, applicable regulations and a solid response posture expected by cybersecurity stakeholders now looks overmatched for a ransomware event to anyone who lived through 2020. However, since 2020, threat actors have gotten richer. Regulations have tightened on cybersecurity. Each incident has gotten worse by almost every definition. The pipeline operators that are building

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 6, Issue 2, March- April 2024 |

DOI:10.15662/IJEETR.2024.0602010

resilience programs and not merely a compliance project and those operators who are rigorously testing under circumstances that might come close to reflecting a real-world event, are less likely to have significant regrets. That does not guarantee that there will not be another ransomware incident. It guarantees that if there is another, the operator will have options to get ahead of it.

REFERENCES

[1] U.S. Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, "DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks," Joint Advisory AA21-131A, May 2021.
[2] U.K. National Crime Agency, U.S. Department of Justice, and partners, "Operation Cronos: International Disruption of LockBit Ransomware," February 2024.
[3] U.S. Cybersecurity and Infrastructure Security Agency, "#StopRansomware: ALPHV Blackcat," Joint Advisory AA23-353A, December 2023, with updates from earlier in the year.
[4] U.S. Cybersecurity and Infrastructure Security Agency, "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," Joint Advisory AA23-158A, June 2023.
[5] U.S. Cybersecurity and Infrastructure Security Agency, "#StopRansomware: Play Ransomware," Joint Advisory AA23-352A, December 18, 2023.
[6] Mandiant, "M-Trends 2023: Cyber Security Insights," April 2023.
[7] U.S. Cybersecurity and Infrastructure Security Agency, "Known Exploited Vulnerabilities Catalog," ongoing, established November 2021.
[8] U.S. Department of Homeland Security, Transportation Security Administration, "Security Directive Pipeline-2021-02D," July 2023.
[9] U.S. Securities and Exchange Commission, "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," Final Rule, Release 33-11216, July 26, 2023; effective December 18, 2023.
[10] U.S. Department of the Treasury, Office of Foreign Assets Control, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," September 21, 2021 (and subsequent guidance).
[11] W. Barker, K. Scarfone, W. Fisher, and M. Souppaya, "Ransomware Risk Management: A Cybersecurity Framework Profile," NIST Interagency Report 8374, February 2022.
[12] Dragos, Inc., "Year in Review 2023: ICS/OT Cybersecurity," February 2024.
[13] U.S. Cybersecurity and Infrastructure Security Agency, "Cross-Sector Cybersecurity Performance Goals," updated March 2023.
[14] National Institute of Standards and Technology, "The NIST Cybersecurity Framework 2.0," February 26, 2024.