



Insights Report

1H 2022

Table of Contents

Page 3

Introduction

Page 4

Ransomware Highlights

Emerging Variants

Ransomware

Pages 5-7

Implementation Matters: Misconfigured Critical Controls

Scope of Coverage – Trust but verify

Configuration & Monitoring

Case Study

Pages 8-11

A Step Ahead: Evolving ransomware tactics demand proactive planning

Protect both the “front door” and the “back door”
when it comes to backups

Re-encryption

Encryption speed – a double-edged sword

Peeling multiple encryption onions

Pages 12-14

Cloud Backups: Resilient, but not a panacea

Immutability is key

Cold Storage

Restoration traffic jam

Legacy Systems’ Hidden Costs

Page 15

Recommendations

Contributors

Jim Aldridge, Thomas Aneiro,
John Beers, Jeff Chan, Sean Duffy,
Claire Geiser, Michael Rogers,
ReseAnne Sims, Mike Wager.

Welcome to MOXFIVE Insights

The first half of 2022 marked a notable deviation from prior trends: the number of ransomware assaults that targeted victims in the US significantly dropped when compared to the preceding three years. Even so, the organizations that MOXFIVE has helped respond to intrusions this year would find that trend to be cold comfort. Businesses are still being disrupted by extortion attacks driven by data theft, Advanced Persistent Threat (APT) attacks driven by espionage, and business email compromises (BECs).



Reflecting on the first half of 2022, four observations stand out:

- Implementation matters - simply checking the box with critical controls, such as EDR and MFA – leaves organizations open to unexpected risk and came back to haunt many clients.
- Certain tactics employed by ransomware threat operators have increased business interruption and can be countered with proactive planning.
- Cloud-based infrastructures are a boon to resilience, but sometimes there is no substitute for cold, offline storage.
- End-of-life software and legacy systems can complicate recovery and increase costs in unexpected ways.

The Insights shared within this report are derived from relevant engagement-related data collected from providing response, recovery and resilience services through our incident management platform. MOXFIVE Insights provides context around themes that impact cybersecurity risk to help organizations make better, more informed decisions.

Forensics. Recovery. Resilience. One Platform.

MOXFIVE minimizes the business impact of cyber-attacks by coupling the 'in the trenches' experience of our Technical Advisors with the capabilities of our Partner Ecosystem. The MOXFIVE Platform streamlines the incident response process with its ability to quickly scale to meet the demand for incident response services and efficiently deliver the expanded expertise, technologies, and resources clients need in the wake of a cyber-attack. At MOXFIVE we strive to provide the clarity and peace of mind needed for attack victims during the incident response process and to help them build a more resilient environment.

Ransomware Highlights

Emerging Variants

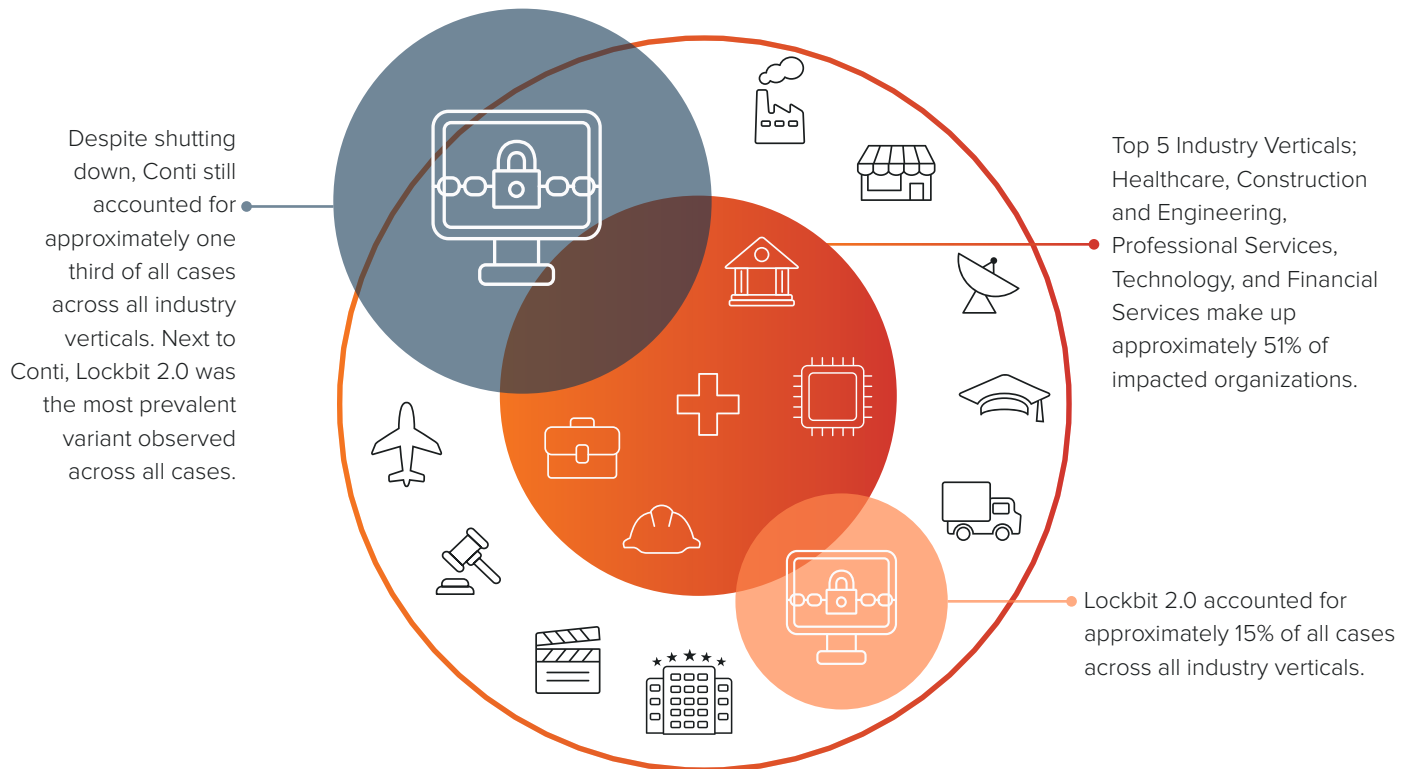
With Conti ceasing operations, new groups, some of which first appeared in 2021, became more prevalent. Threat Actors are operating in nontraditional ways such as powering off VMs before encryption, leaking data earlier in the negotiations cycle, and executing with greater speed (reduced dwell time) to include partial file encryption only. Ransomware-as-a-Service (RaaS) and Affiliate vulnerability sharing are increasingly observed.

JANUARY 2022

- Black Basta
- BlackByte
- BlackCat
- Daixin
- Lockbit 3.0
- Quantum

JULY 2022

By the numbers





Implementation Matters: Misconfigured Critical Controls



In the first half of 2022, most MOXFIVE clients lacked fully deployed and effectively configured endpoint detection and response (EDR) tooling at the time of the incident. Statistics for multifactor authentication (MFA) deployment at the outset of incidents were similar.

These technologies make it significantly more difficult for attackers to use stolen passwords or malware to gain entry into a network, and to remain undetected should they find a way in. They are critical controls that reduce the risk of many types of threat actors ranging from malicious insiders to state-sponsored actors, and extortionists to ransomware operators. Simply installing them is a step in the right direction but is ultimately insufficient.

When it comes to cybersecurity insurance, this topic is top-of-mind for carriers. In July 2022, Travelers [filed a lawsuit](#) to rescind a policy based on alleged misrepresentations related to the deployment of MFA by their insured. We can expect increased scrutiny of insureds' assertions related to key controls that mitigate insurance carriers' risk. On August 26, 2022, the lawsuit was dismissed, with judgment entered in favor of Travelers, after ICS agreed to allow the court to [issue a judgment](#) rescinding the policy.

Scope of coverage – trust but verify

From a risk management perspective, it is important to understand the extent to which these key technologies have been deployed. For EDR, it is crucial that the software is installed on every supported system – including servers (virtual or physical, on-premises or cloud), and workstations. It may sound obvious, but remember that the technology can only protect systems on which it is installed: a disciplined asset management program helps validate full deployment.

MOXFIVE has seen many environments where EDR agents were not fully installed, even though the organization’s leadership thought that the technology was fully deployed. For example, one client had a small overseas office where they had difficulty getting the agents deployed. At the time of the attack, that office did not have EDR installed and was the weak point that enabled the attacker to gain an undetected foothold. The result was ransomware deployed across the entire global network.



Are you hearing that EDR is ‘deployed’? It would be wise to dig into the details.

For example, if EDR is said to be 99% deployed, how was the denominator in that percentage – the total number of systems in the environment – calculated? Does it include all branch offices or lab environments that may not be connected to the main network and systems that may not be part of Active Directory? How does the organization go about identifying systems that should have EDR installed, but do not? Use a variety of data sources, including active network discovery scan results, to ensure that the asset inventory includes all systems in the environment.

For MFA, it is most important that authentication to Internet-facing systems requires more than just a password. This could be a token generated by a smartphone application or a numeric code sent to the user’s mobile phone via text message. If limitations exist regarding the ability to deploy MFA across all applications and systems, focus on covering email, virtual private networks (VPN), and other systems that could provide entry to the network over Internet-facing applications and access to internal resources.

In a recent case, a healthcare organization thought that they had full MFA coverage for VPN. This company had a legacy VPN that they maintained for emergency purposes, in case the newer VPN, which was protected by MFA, had issues. Though this VPN was thought of as “legacy” and not a factor, it was very much accessible to the Internet – and did not require MFA for authentication. The attacker leveraged that legacy VPN with stolen credentials to gain entry to the network, ultimately encrypting nearly four hundred systems and severely disrupting their operations.

When it comes to MFA coverage, ensure that all externally accessible means of accessing the network require MFA for authentication. Question how the team is sure that those known access points in fact represent “all” such access points. Multiple methods, including external network scans of address space owned by the organization and reviewing network devices’ configurations should be used to instill confidence in the list’s completeness. Additionally, it is important to ensure that all accounts that are permitted to authenticate require MFA. MOXFIVE has seen cases where MFA was applied to all the right sources of ingress, for almost all users, but a few user accounts were exempted – and those were used by the attacker to gain entry with stolen credentials.

Configuration and monitoring

MOXFIVE has seen attacks succeed because EDR tools' blocking functionality was not enabled, despite those agents being fully deployed.

Ensure that EDR tools are configured with appropriate blocking settings to reduce the risk of both known and unknown malware execution. Include specific tests related to this scenario within general IT assessment and penetration test plans. **Protect EDR, MFA, and other key security software consoles – consider them “crown jewels” within security planning processes.** Require MFA for access to the consoles, secure underlying operating systems with the most stringent standards, and monitor console access and policy change logs. A change to blocking policies should be a red flag that generates an alert and leads to immediate intervention by administrators.

In one scenario involving a large organization in the entertainment industry, the attacker leveraged an initial foothold inside the network to gain access to the EDR tool's management console. From there, the attacker set up exclusions for the malicious tools they wanted to execute – and ultimately severely disrupted the company by deploying ransomware. Despite EDR agents being appropriately deployed and configured in blocking mode, protection of the EDR console failed with serious results.

Related, because of the substantial number of alerts that security tools can generate, **organizations should not consider their implementation complete unless they have an effective monitoring regime in place.** Take for example, a manufacturing company that deployed an effective EDR tool, but only to approximately 90% of their IT environment. It was not deployed on the system that the attacker initially gained access to. From there, alerts related to significant attacker activity inside their network began on a weekend. Unfortunately, the alerts went unnoticed until Monday morning, by which time the attacker was already well into executing the ransomware attack.

Ensure that skilled analysts monitor security tools using tested processes that have proven to be effective, especially EDR alerts. **Alert fatigue is real.** For smaller teams, leveraging an external managed service can provide a cost-effective way to benefit from specialist expertise without hiring full-time resources. Test detection processes through technical exercises that simulate attacks. Many in the industry have begun referring to such combined simulations as Purple Team exercises, which combines Red Team (offensive tests simulating an attack) with Blue Team (simulating detection and defense against attacks) elements.



Case Study



Client with \$350 million in annual revenue, 700 systems, and 400 users was impacted with BlackByte ransomware.



Endpoint Detection and Response (24/7) was operational when the threat actor gained access, however, the EDR was only in alerting mode and did not have blocking enabled.



Due to limited network visibility of portions of the environment and the lack of blocking, the threat actor was able to steal a large amount of data and encrypt a significant portion of the environment before the teams were able to act.



MOXFIVE's analysis helped soften the financial impact of the attack; by highlighting the limited nature of the data exposed, they were able to negotiate a reduction in the attacker's extortion demand by over 90%.

A Step Ahead:

Evolving ransomware tactics demand proactive planning

Protect both the “front door” and the “back door” when it comes to backups

Some organizations learn the hard way that when it comes to the security of system backups, there are effectively both a “front door” and a “back door” to consider. The “front door” is the interface into the backup software – the control panels that administrators use to configure it, and the behind-the-scenes connections that seamlessly function to ensure that data is archived. The “back door” is the direct route into the system that actually stores the archived data.

Even when the backup system is configured appropriately, in some architectures, there is a risk that the attacker may gain direct access to the systems where the backup data is stored. By using stolen administrators’ passwords or exploiting other vulnerabilities to gain access to this “back door,” the attacker is then in a position to encrypt or delete data in a manner that cannot be recovered. Ransomware operators actively try to do this, prior to encrypting the environment, to increase the victim’s motivation to pay the demand.

Having a backup system that advertises immutability is not enough. Ensure that backups systems are not only configured appropriately, but that any underlying infrastructure that stores backup data is protected at the operating system level. Verify through having experts review the architectures and technical configurations, and through simulating attacks against backup systems with “insider access” specifically as part of penetration testing.



85% of domain joined backup solutions are partially or fully impacted during ransomware incidents

Re-encryption

Picture the following scenario. The response to a ransomware attack has entered its second week, and the team is beginning to feel cautiously optimistic. Backups were found viable and relatively recent, the core business functions are now operational, and systems are being restored. Then, suddenly, the ransomware begins spreading again, setting back the recovery effort and forcing the victim organization's hand toward paying the ransom demand.

The ransomware operators use a variety of basic, but effective, means of deploying ransomware across the environment. To maximize their chances of forcing payment from the victim, these can often be triggered by actions such as booting or logging into a system – and the mechanisms may be left behind even though the attackers no longer have access into the environment at will.

To fully resolve any cyber-attack, the attacker must be expelled from the environment. For ransomware attacks this includes identifying all the means by which the ransomware was deployed and ensuring that those are systematically mitigated.

Though a lengthy forensics report is not always necessary, it is important that forensics experts conduct enough of an investigation to understand these key elements: do not skip the investigation. Ensure that the tools analysts need to perform their investigation are fully deployed and appropriately configured. Based on their analysis, build checks into the work instructions used by the engineers restoring systems to check for and remove known malicious tools prior to placing systems onto the main network.



Encryption speed – a double-edged sword

Some ransomware variants only encrypt parts of files to improve the speed of encryption, which gives defenders less time to react once the encryption process begins. A recent [study](#) by Splunk found that the median time that it took a sample of ransomware encryptors to encrypt a set of files in a lab environment was 42 minutes and 52 seconds. Researcher Antonio Cocomazzi [attributed](#) the speed of LockBit and Babuk, in particular, to those variants only encrypting parts of files.

While this tactic makes the ransomware operator's attack more difficult to defend against, it can also open the possibility to recover certain types of encrypted files without purchasing the decryption key. For example, in some cases MOXFIVE has been able to salvage parts of structured data files, such as databases. This was made possible because the ransomware variants employed only encrypted, for example, the first 1 KB of the file, rendering most of the data unencrypted.

Remember that such recovery techniques, while sometimes possible, typically take a significant level of effort to execute. When considering a data recovery approach, assess the costs and likelihood of success between this and other options to balance cost versus business interruption.



When hit with ransomware, having viable and current backups is crucial to avoid having to work through encryption-related considerations.

Facing downtime, victim organizations should work with their forensic experts to understand the nature of the ransomware encryptor used in their environment to determine if there may be options to recover certain files through specialized data recovery techniques.



42
minutes &
52 seconds

MEDIAN TIME FOR A SAMPLE OF RANSOMWARE ENCRYPTORS TO ENCRYPT A SET OF FILES IN A LAB ENVIRONMENT

Peeling multiple encryption onions

Within the ransomware ecosystem, initial access brokers gain entry into victim organizations and then sell that capability to others who leverage the access to steal files and deploy ransomware. It is common for multiple threat actors to have access to the same environment.

Sometimes this is because an access broker has sold credentials to multiple actors, other times it occurs because the vulnerability that provided initial access (e.g. unpatched Exchange) remains accessible over time for multiple threat actors to discover. This can lead to multiple ransoms – either occurring back-to-back or simultaneously – as well as encryption challenges. We have seen up to three ransoms demanded within a one-month window from the same victim.

Common complications include the ransomware executable being written poorly or executed ineptly causing files to be encrypted over and over (with the same encryptor).

We have also observed multiple independent threat actors gain access and run their respective ransomware encryptors against the same systems. This results in files being encrypted multiple times, each time with a different encryptor – meaning that to recover the files, one would first need to decrypt using the decryption tool associated with the last ransomware to run, followed by a separate tool for the next to last ransomware, and so on. In addition to this as mentioned previously the tools will inherently be bug prone and come with their own challenges and may require back and forth discussions with the threat actor.

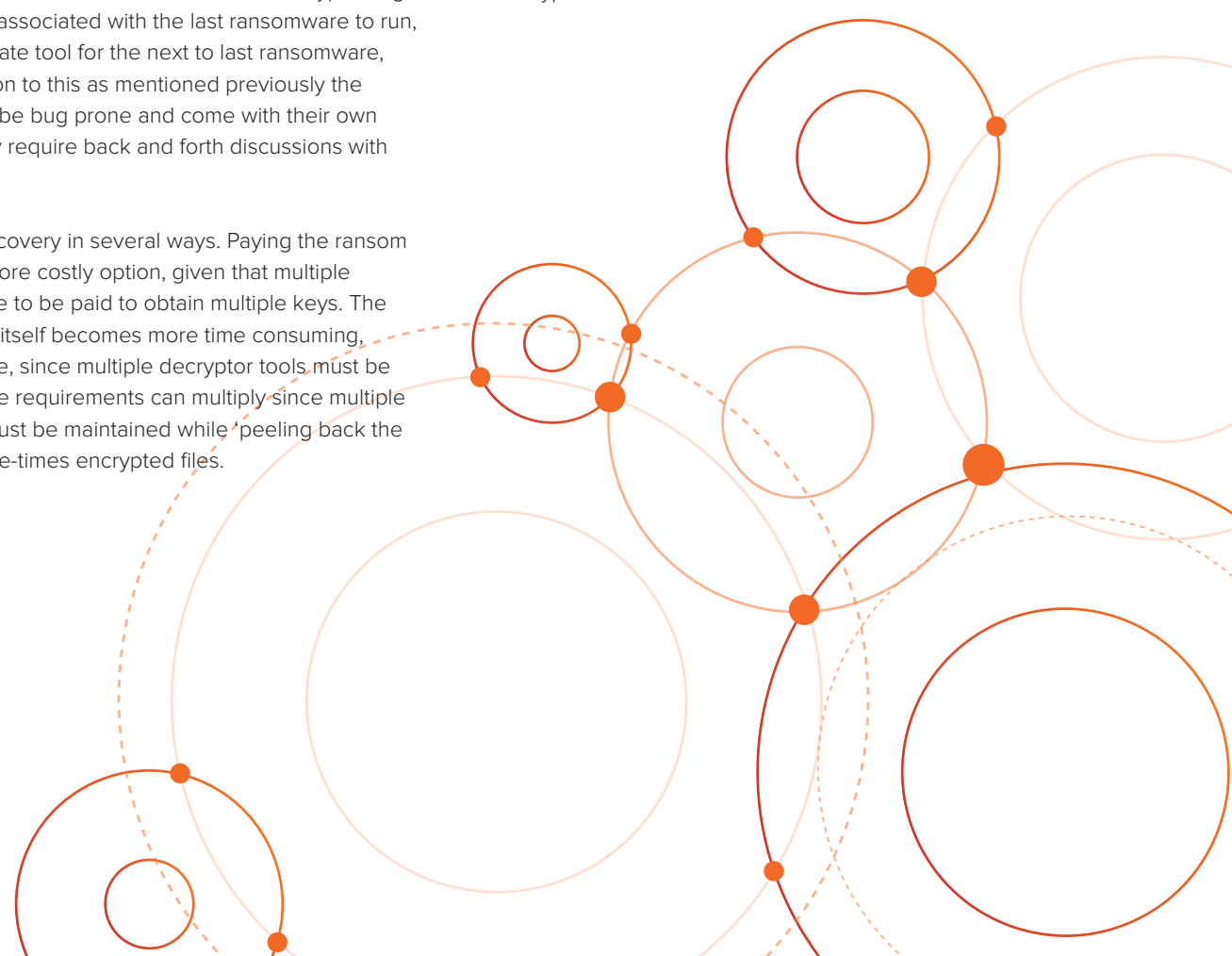
This complicates recovery in several ways. Paying the ransom becomes a much more costly option, given that multiple ransoms would have to be paid to obtain multiple keys. The decryption process itself becomes more time consuming, increasing downtime, since multiple decryptor tools must be run. Working storage requirements can multiply since multiple intermediate files must be maintained while ‘peeling back the onion’ of the multiple-times encrypted files.



When planning recovery scenarios, consider the impact of working storage needed during the decryption process.

Avoid running the decryptor on the original encrypted file; instead, decrypt a copy in case the decryptor corrupts the file. For example, this means that for every 100GB virtual disk file being decrypted, at least 300GB of working storage is required: 100GB for the original (encrypted) file, 100GB for a copy of the encrypted file, and 100GB for the decrypted file.

From a stakeholder management standpoint during an incident, ensure that technical teams factor these types of considerations into their estimations of time to recover. Paying the ransom and receiving the decryption key is an important milestone but is just the beginning of an often painful process to actually decrypt the environment.



Cloud Backups: Resilient, but not a panacea

Immutability is key

Ensuring the immutability of backups is crucial in recovering from a ransomware attack that has impacted a network. Due to the Write Once Read Many (WORM) permissions available in cloud storage services, these storage locations were initially leveraged by IT teams for the ease-of-use. It is key to note that cloud backups still need to be configured properly, the storage itself is not inherently immutable. Enterprise grade backup solutions now provide these permissions natively and can greatly decrease the time to restore due to the data residing locally as opposed to traversing the internet during a restore.



Some may be surprised to hear that tape backups are far from dead.

Though we would not recommend shifting to tape as a strategy for a variety of reasons, the medium is by its nature is resistant to disruption by ransomware attacks. In addition to using a cloud-based backup tool – configured to prevent the intentional deletion of backups – smaller organizations should consider making a simple, periodic backup of critical data to encrypted external hard drives that will be stored in a secure location such as a safe.

“ Cold storage

It was three days into a ransomware recovery and things were not going well. The attacker had encrypted Active Directory servers, which ground business to a halt as users could not access systems or applications. Facing the need to rebuild Active Directory from scratch, one of the engineers remembered having taken a domain controller offline and literally putting it into a closet a month prior. The system had been power surged during a storm, damaging some components, but the hard disk drives were intact. With those drives, they were able to quickly restore Active Directory and resume operations.

This anecdote illustrates the value of cold storage, a fully offline last line of defense that can become invaluable when online backups and cloud backups are impacted by ransomware. MOXFIVE has seen similar scenarios where clients were saved by tape backups, or even a few hard drives with key backups rotated into a safe every few weeks.

Restoration traffic jam

While organizations have increasingly adopted cloud-based backup solutions, few organizations have tested how they would recover their environment during ransomware scenario. As a result, they are not able to forecast recovery times, which has ripple-down effects that make the incident response effort more painful than it needs to be.

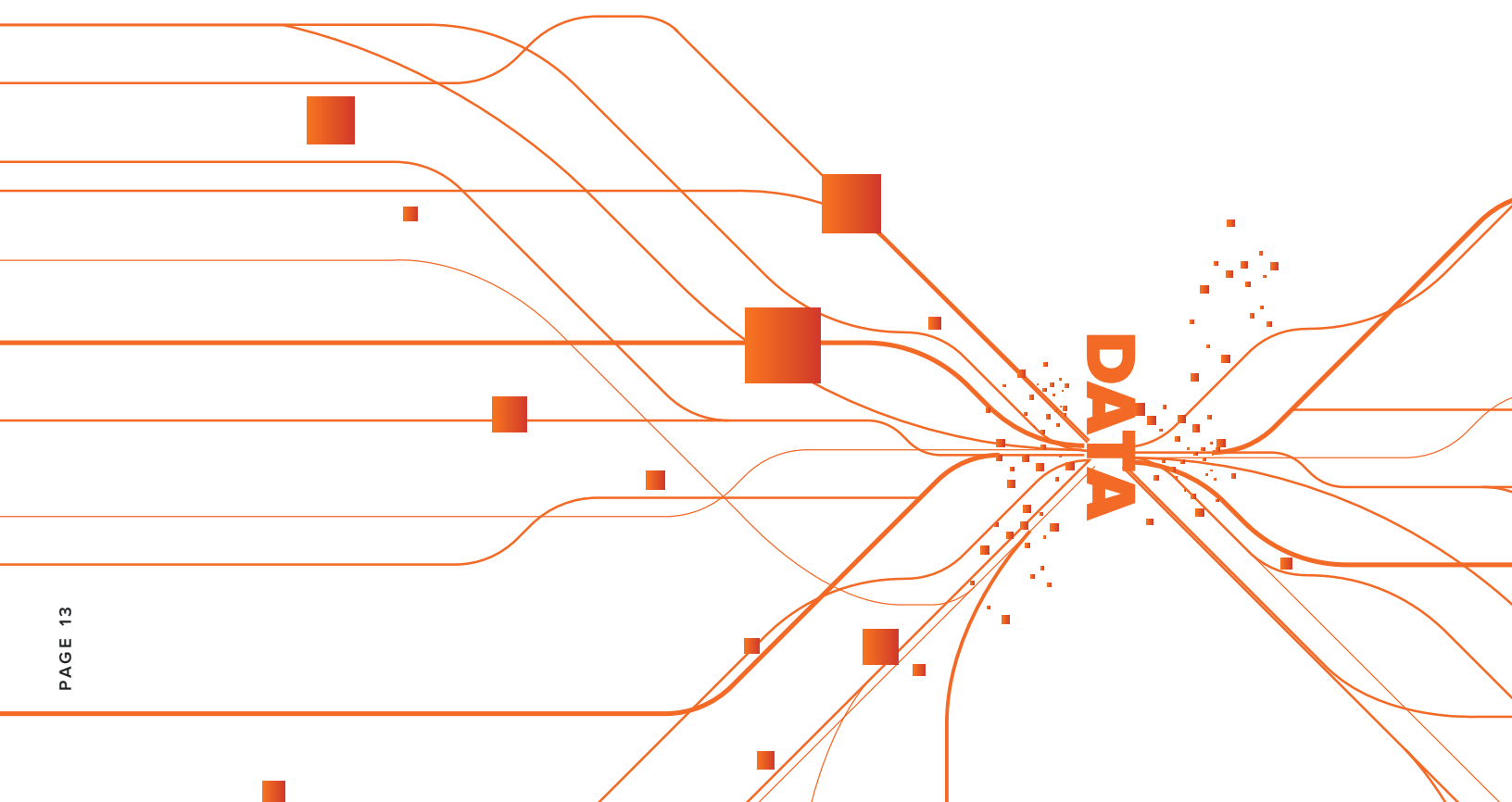
MOXFIVE has seen variations on the following scenario following numerous ransomware attacks. The first few days are tense, with the business severely interrupted, and the extent of the damage and path to recovery unclear. Then viable backups are identified. This is a moment when everyone breathes a small sigh of relief – there is a path to recovery outside of paying the criminal the ransom they demanded. Leadership asks for an estimate on recovery times for key business functions because they need that information to manage stakeholders that include the board of directors, key clients, upstream and downstream partners, and potentially regulators.

The IT team has confirmed the effectiveness of restorations from the cloud backup system, but only at a small scale. As the team starts to restore hundreds of archived virtual server images from the cloud, it dawns on them that system and

network bandwidth limitations at the relevant sites combine to limit simultaneous downloads to, for example, three server images every five hours. Timelines then begin to stretch out, and the team must scramble to find alternative means of restoration.

When performing disaster recovery simulations, calculate recovery times that consider the need to restore large amounts of data at one time.

Have secondary options available, for example, a surge in network bandwidth capability with the internet service provider (ISP) or a pre-determined ability to have a physical storage device shipped. If your organization does not perform such simulations, it should start.





Legacy systems' hidden costs

It is easy for an IT auditor to point out that end-of-life operating systems should be upgraded and that legacy systems should be migrated to platforms with modern security capabilities. In the real world, IT engineers often face the reality that certain business-critical applications or systems cannot easily be upgraded. The software vendor may no longer be in business, newer operating systems may not support running it, and yet it may be responsible for a critical process such as running machinery that directly supports generating revenue.

Legacy systems often throw a wrench into recovery plans, both from a technical perspective and from an insurance coverage perspective once the insurance carrier processes the cyber insurance claim (if applicable). For example, consider a ten-year-old application that controls a robot arm on a production line running on an operating system and hardware of the same vintage. If that system is encrypted by ransomware and viable backups are not available, it will need to be rebuilt.

When engineers plan the rebuild, they first realize they do not have the installation media for the original version of the software. Fortunately, they can get a newer version. But that newer version does not function on the vintage operating system, so they need to upgrade the server operating system. But that modern operating system exceeds the hardware's capabilities, so they upgrade the hardware. After running into delays at each step of the process, culminating in a delay getting the new hardware because of supply chain shortages, the application is up and running.

Months later when the insurance carrier reviews the claim, it is very possible they will classify many of the costs involved in that process as not covered by the cyber insurance policy because they appear to be unnecessary upgrades and enhancements over and above recovering the system that was affected by ransomware.

Migrating away from legacy applications will help to avoid an array of complications and hidden costs not limited to those mentioned here.

In the interim, legacy systems can be segregated from the general population to limit their exposure to attacks in the first place. While it may not be feasible for many organizations to highly segment their networks, isolating a few systems that are used for limited purposes, often by a limited population of users that need to interact with the system, is far easier. Consider leveraging software-based microsegmentation tools to further ease the level of effort. MOXFIVE has applied such tools during ransomware recoveries to segment critical, legacy systems and bring their business-critical functions back online more quickly.

Recommendations

1

Endpoint Detection and Response

Ensure all servers and end-user systems have EDR installed and blocking capabilities activated. This capability often represents the difference between a minor intrusion that can be contained within minutes and a full-blown ransomware attack that materially impacts business.

Backup Plan

Design a resilient backup plan with intentional attacks in mind. Ensure your backup solutions are being patched rapidly and have the required immutability features enabled. We increasingly see threat actors intentionally corrupting or erasing backups to increase their impact and improve odds of a ransom being paid by a victim.

2

3

Multifactor Authentication

Protect Internet-facing systems including email and VPN with Multifactor Authentication. Stolen credentials and password guessing are continuing to be common initial access methods and are made easy without MFA enabled. Focus on covering all systems that could provide entry to the network and others that are accessible outside of your network.

Management Tools

Ensure every system can be managed with system, patch, and vulnerability management tools. Having this basic capability is crucial to recovering from incidents and has a multitude of other benefits that reduce risk. Install tooling so that IT administrators can take control of any organization-managed system regardless of location.

4


5

Privileged Access Management

Implement a Privileged Access Management (PAM) system to properly manage credentials throughout your environment. In the average enterprise, privileged accounts are often sprawled across the environment that threat actors can quickly take advantage of. PAM solutions can ensure MFA is required for privileged accounts and allow for stronger policies such as immediate password rotation to be enabled. Features may differ but most enterprise grade PAM solutions contain reporting and alerting mechanisms that allow better insight for security teams to review how credentials and policies are being utilized.

MOXFIVE is a specialized technical advisory firm founded to help minimize the business impact of cyber attacks. Over the last decade, our team of experts has helped thousands of businesses respond to major incidents and saw firsthand that there needed to be a better way for organizations to get the technical expertise they need when they need it most. With deep roots in incident response and corporate IT, MOXFIVE Technical Advisors strive to be the go-to technical resource for our clients - helping organizations of all types solve their most challenging technology-related problems and provide technical expertise at scale.

 www.moxfive.com

 (833) 568-6695

 info@moxfive.com

