Ransomware: Improving Readiness, Resilience, and Response.

An Industry Guide

VMware Security

vmware

This VMware Industry Guide provides an overview of the class of cyber attack known as *"ransomware"*.

> *Ransomware is an attack whereby a victim's data and often systems are made unavailable to them generally through the use of encryption. The attacker will demand payment (the ransom) within a set time period in order for them to provide the means to decrypt the systems and data they have attacked. Attackers also often steal copies of data and threaten to sell or release the stolen copies as a further means to demand ransom payment.*

Readers of this guide can expect to learn:

- A general overview of the techniques used by the perpetrators of ransomware attacks;
- The challenges facing IT and cyber (security) defenders;
- Recommendations to uplift an organization's readiness, increase its resilience, and enable it to more rapidly and effectively respond should an attack occur.

This document is intended for readers from a business background and does not require highly technical Information Technology or Cyber Security skills and knowledge.

By design this Industry Guide does not recommend specific VMware Inc. technology or services and readers should refer to other documentation and to VMware experts for details on how to best architect and configure VMware Inc. solutions to minimize the risk of ransomware and other cyber attacks. Please see *"Additional Resources"* in this guide for a list of recommended documentation and information assets.

Table of Contents

Introduction

Ransomware – how did we get here?

Users who fell victim to what is regarded as the first example of ransomware, the AIDS Trojan, were handed a payment less get-out-of-cyber-jail card courtesy of restoration and recovery utilities made available by early computer virus researchers. Since that initial 1989 introduction ransomware has exploded, growing in sophistication, breadth of technique, overall volume, size of payment demanded, and velocity of attack spread.

Meanwhile the rise of crypto currency has provided a means to not only collect payment easily, but to do so with a degree of anonymity and immunity from prosecution. The closing months of the 1980's may have seen the introduction of the computer virus ransom, but here in the 2020s we are firmly entrenched in the age of ransomware. More recently; in the first six months of 2022 ransomware type attacks have also been used as a weapon of international intimidation, with destructive attacks launch against Ukrainian organizations at high frequency.

Ransomware payments today top $600 Million [1], with the total damages attributed to ransomware hitting $20 Billion in lost productivity, downtime, brand damage, and additional ongoing costs [2]. Attacks like WannaCry [3] demonstrate that ransomware attacks are also now weapons leveraged by nation state affiliated adversaries seeking to bypass international sanctions, or to further their geopolitical goals. Meanwhile less sophisticated adversaries rent out ransomware-as-a-service (RaaS) platforms. As a result coding skills are now optional, and a loose moral code of conduct is the only characteristic necessary in the pursuit of a quick dollar.

The continued evolution in techniques and sophistication of modern ransomware groups now mean that a multi-layered and more sophisticated approach is required to reduce the risk of falling victim to an attack, and to increase the business' resilience should ransomware gain an initial foothold.

Those early victims of the AIDS Trojan may have been saved through recovery utilities, and many victims since have either paid up from their own or their insurer's pocket or turned to data and system backups to avoid ransom payment. Now defenders must balance people skills, planned processes, and a range of technology tools to remain resilient against ransomware.

RaaS

Ransomware-as-a-Service

The tools and infrastructure for an attacker to conduct an end-to-end ransomware based attack are available in an 'as-a-service' model.

RaaS was first reported in 2014/2015 and VMware's research now finds that RaaS based attacks now comprise circa 14% of all ransomware type attacks.

RaaS offerings include:
- Malware and non-malware methods that will allow an attacker to gain initial entry into an organization's network and systems. Non-malware based methods include details of previously stolen credentials (usernames & passwords)
- Malware that may be used to perform data and system encryption
- Customizable templates that may be used to demand ransom payment and communicate with the victim organization at various stages of the attack
- Payment platforms that may be used for deposit and processing of the paid ransom
- Details that may assist in selection of target organizations

The more sophisticated RaaS platforms also offer help desks and forums to their customers (the attacker).

RaaS operators monetize their offerings through up-front payment and a percentage of the ransom payment.

[1] https://therecord.media/ransomware-victims-paid-more-than-600-million-to-cybercriminals-in-2021/

[2] https://www.cloudwards.net/ransomware-statistics/

[3] WannaCry was a highly destructive ransomware attack that occurred in 2017 and impacted organisations globally. The attack is estimated to have impacted over 200,000 machines across 150 countries. See also: https://blogs.vmware.com/networkvirtualization/2017/05/use-zero-trust-protects-against-wannacry.html/

What's the risk?

Early example of ransomware involved the attacker introducing malware (malicious software) into a victim's environment through a vector such as phishing, with the malware then rapidly spreading from machine to machine while encrypting data and otherwise locking up the system's function. Victims of ransomware generally knew fairly quickly they had fallen victim, and ransom demands generally just followed the "pay me this and I will unlock that" format.

An increasing percentage of all ransomware attacks today involve double-extortion whereby attackers, once they gain initial entry to an organization's systems, will stealthily move from system to system (lateral movement) on the hunt for valuable data that they will steal and stage in the cloud, and along the way set themselves up multiple methods of return in preparation for the event that defenders detect the attack and attempt to shut down the attack [4]. When the data is eventually encrypted and the ransom demanded, the attackers leverage the stolen data as an additional hostage, and as an additional "double dip" method to monetize their crime.

Such double extortion techniques mean that relying on backups as a method to avoid ransom payment is flawed. The attackers can sell, or at the minimum threaten to sell or expose the stolen data regardless. Furthermore, the stealthy early stages of the attack provide the means for the attacker to establish multiple ways to return, steal more sensitive secrets, corrupt systems, and use one company's computers and networks as a launching point to the customers and business partners of the initial victim.

Defenders against ransomware must now consider the following risks:

1. Denial of access to core workload and end user systems through data encryption;
2. Destruction of core workload and end user systems through firmware and OS corruption;
3. Damage to physical Operational Technology (OT) connected systems through corruption of control systems and/or data encryption [5];
4. Theft, sale and/or public disclosure of sensitive corporate data;
5. Theft and sale of sensitive security data (user credentials and system information) to other criminals;
6. An elevated likelihood of additional attacks that leverage established return access paths, and living off the land techniques;
7. That any data backups may themselves be unreliable if the attackers already had a footprint in the environment during the time that the backups were taken. Unless stored as immutable copies, or otherwise protected, backups may be encrypted by ransomware as it spreads;
8. That attackers may use trusted tools rather than what may be thought of a "computer virus" [6].

[4] https://securityintelligence.com/articles/ransomware-double-extortion/
[5] OT systems are those that interface directly with, measure the state of, and often control, physical processes. An example of OT would be a set of lightweight computers that measure the speed of a set of industrial centrifuges and are also used to control the speed of rotation.
[6] VMware's Threat Analysis Unit (TAU) documented such an attack that leverages only Windows Powershell: https://community.carbonblack.com/t5/Threat-Research-Docs/TAU-TIN-BlackSun-Ransomware/ta-p/110588

The Challenges in Effective Defense

Ransomware continues to be a significant threat to organizations of all sizes and relative levels of security program sophistication. As previously noted, this is due to the fact that sophisticated ransomware toolsets are now available as-a-service, lowering the technical bar for entry to those who simply have the means and the willingness to pay for service. Adversaries have also adapted their techniques and procedures, leveraging double-extortion to increase the leverage of their threats while potentially increasing monetary yields.

Meanwhile two significant other arenas of challenge exist; firstly the Defender Challenge, and secondly the Ecosystem Challenge. We will examine each in turn.

The Defender Challenge

Effective security programs require a balancing of People, Processes, and Technology. All three legs of this tripod can present challenges to effective ransomware defense.

People

- The security industry is suffering from a gap between the demand for, and the availability of skilled security professionals of all types; architects, implementors, operators and analysts, and forensic and incident responders. Those on the frontline of defending their environments report high stress levels and burnout from the workload. This skills shortfall also leads to a high cost and potential rapid turnover of skilled staff.
- The changing techniques and procedures of ransomware adversaries requires a new type of skill; the ability to conduct proactive threat hunting [7]. Organizations may lack the means or resources to hold these skills in-house or may have failed to provision them from a third-party provider under an established service contract.
- The failure to empower key stakeholders to make decisions in a timely manner in the event an attack occurs. Ransomware (and other cyber attacks) can unfold and escalate rapidly and stakeholders, both from the technical and business sides of an organization must be free to make informed and decisive action quickly. Remember too that the various stakeholder teams may have differing agendas, for example the Security team may want to take the time to fully understand the root cause and scope of the attack while the Business Resilience team may prioritize system restoration. Delays risk worsening the scope of damage to system and the overall impact to the smooth running of the business. Furthermore, ransom demands are time limited ("Pay $X in YY days or else!") and delays in decision making eat into that time.

[7] Hunting systems and networks for metaphorical breadcrumbs that may indicate early signs of potential intrusion, in the absence of an obvious alert (for example a firewall alert logged in a SIEM).

Processes

- Ransomware (and other cyber attacks) are too often seen as purely an IT problem rather than as a business problem. This contributes to decision making that does not effectively consider or balance business needs related to reputational risk, legal obligations, and cost issues as business stakeholders will (initially) be absent during key decision making. *Refer also to previous point*.

- Lack of planning for an eventual attack. Defenders may assume that their preventative security controls will always protect them from successful attack and may fail to plan adequately for effective Incident Response (IR) [8]. Similarly, too many organizations don't have comprehensive Disaster Recovery (DR) plans, don't test them frequently, and may not have considered the criticality of disaster recovery in a ransomware protection scenario.

- Lack of testing of the plan. When an IR and DR plan does exist, there may be a failure to adequately and regularly test the continued effectiveness of the plans. Without these practice runs the effectiveness of the plans in a real scenario may not be known. Furthermore, decision making can be delayed, be more likely to be error-prone, and the plan may rapidly become out of date as adversaries continue to evolve, the systems being defended are updated, and the overall state and risk appetite of the business changes.

- Lack of sophistication in the IR plan. An IR plan may also have been formed on the basis of incorrect assumptions regarding the sophistication and nature of modern adversaries; for example, adversaries often establish multiple return paths back in to an environment. If the IR plan fails to consider this fact defender actions may fall short of effective response and remediation, leading to follow on attacks that may be more destructive in nature.

- Lack of iteration of the IR plan. The only certainty in cyber security is that threats and attacks will constantly evolve. A static IR plan is one that will become outdated and less useful in a short period of time.

[8] A cyber security "control" refers to a technology or procedure that is intended to mitigate against a specific type of threat. Controls may be *preventative* or *detective* in nature. Preventative controls seek to block (prevent) a type of attack, whereby detective controls provide information to inform of an attack. A useful analogy is to be found in physical security: a door and a lock are preventative controls while CCTV cameras and motion detectors are detective controls.

Tools

- Defenders can no longer assume that preventative controls will protect against all attacks always. Nor can defenders assume that preventative controls will generate an alert. Preventative controls must be balanced with a range of detective controls that enable proactive threat hunting, and the gathering of forensic information. These detective controls must span the user device (endpoint), workload, and network layers whether on-prem or in the public cloud.

- Backups will generally be targeted by attackers. Defenders must ensure that backup data is effectively protected from attack by adversaries (in effect, separated from the backed-up environment by an air-gap). The frequency of the backups and the duration they are maintained must also align with the cadence the organization can effectively hunt for threats; there is no point in having a backup regime whereby the longest storage period for backup data is 3 months if an organization only hunts for threats once a year as a you cannot guarantee that the stored backup is trustworthy; attackers may already have been in the environment undetected and have corrupted backups in subtle yet critical ways.

The Ecosystem Challenge

Organizations have increasingly turned to cyber insurance coverage to externalize the monetary costs of both ransomware payout, as well as the costs of Incident Response and/or downtime if recovery from backups is necessary. There is in effect an ecosystem that exists that assists organizations defend themselves against and respond adequately to an attack. This ecosystem includes professional, for-hire Incident Response teams, Managed Detection Providers, and the cyber insurer marketplace.

Due to the significant increase in volume and velocity of ransomware attacks on a global basis this ecosystem is beginning to break down. Most notably cyber insurers have rapidly retreated from the market; excluding ransomware from policy coverage all together, substantially jacking up premium costs, and at a minimum requiring a substantially higher burden of proof that the insured party has a thorough and balanced cyber program [9].

[9] https://www.lifeinsuranceinternational.com/news/cyber-insurers-running-scared-ransomware-as-profitable-as-cocaine/

Developing an Effective Ransomware Strategy

Key Considerations

Consider the following questions that need to be answered in a timely manner in the event of a ransom demand:

- Do we pay the ransom or accept the business downtime and risk that will result from electing to recover from backups?
- What are our compliance risks and our legislated reporting responsibilities?
- Should we advise our customers and business partners that their data has potentially been stolen?

It should be clear that these are not questions that a company director or a company board would expect an IT professional regardless of seniority to answer on behalf of the business as a whole.

Therefore, an effective strategy to dealing with ransomware (and other cyber attacks) is to recognize the problem as being one that is primarily owned by the business. IT and Security teams are key, frontline stakeholders, but the overall ownership of risk and the responsibility for assuring effective governance must sit at the executive leadership level in any organization, and all else flows from this point.

With that consideration in mind the following must be included in an effective strategy:

People

- A clear team of decision-making stakeholders must be assembled that includes business and IT stakeholders. Consider including staff who are empowered to make decisions from the Audit & Risk, Legal, Marketing / PR, Customer Relations, Partner Management, Finance, as well as IT / Cyber Security teams. Clear lines of decision making and sign off authority must be established.
- Adequate technical staff must be available with the cyber and forensic skills necessary for them to both respond to and recover from an attack, and to proactively hunt for threats. Businesses may opt to rely on specialist, third party Managed Detection Response (MDR) teams to augment the available internal skills. Where external MDR and IR services are relied upon these must be selected and engaged under a pre-agreed term of service ahead of time.

Processes

a. A formal IR plan must be established. Businesses may elect to engage the services of an external advisory team to assist with the initial establishment of this plan, and the plan must be a living document subject to change as the nature of the threat continues to evolve.

b. The IR plan must be stored in a location (physical or electronic) where it cannot be made unavailable by virtue of the attack. There is no point having a plan if it has been encrypted by ransomware and thus made unavailable!

c. The full plan should be tested regularly. At minimum a desktop exercise that involves all stakeholders should be held once every 12 months. The IT/Cyber team should test the

technical aspects of the plan on a more regular basis, at a minimum whenever the technical environment being defended changes, or as new cyber preventative and detective controls are adopted.

d. The IR plan must be built with the assumption that the adversaries are already in the environment and have the means to both return, and to detect that their presence has been detected by defenders. These assumptions mean that the IR plan must emphasize thorough analysis and understanding of what the attacker has done in order to identify all potential return paths prior to attempting to remove them from the environment. Furthermore, all intra-IR team communications must use out of channel methods; for example, no reply on corporate email or SLACK channels as the adversary may be monitoring these channels. Instead consider using WhatsApp or Signal messaging apps.

e. Do we have a comprehensive ransomware recovery plan to regain access to our data and avoid paying the ransom? How quickly can critical information be restored? How quickly can less mission critical information be restored (keeping in mind that the information loss from a ransomware attack may be widespread in scope)? What are system dependencies to running the restore processes (keeping in mind that systems used to initiate and manage the restore process may be rendered unusable by the ransomware attack)?

f. Backup retention period (the duration that backups are maintained) must be balanced with the ability for an organization to detect and respond to an attack. Backups must be available for use for a period of time that exceeds the maximum length of time it will take an organization to detect, analyze, respond to and recover from an attack. It must also be possible ensure that the backup media itself cannot be compromised. Lastly, the IR effort must include focus on establishing the timing of the initial compromise such that the appropriate restoration point can be determined.

Organizations should consider adoption of the following tools, which may be deployed and managed either internally, or externally by MDR and IR professionals:

g. DETECTIVE CONTROLS THAT ENABLE THREAT HUNTING:

i. **Endpoint Detection and Response (EDR):** A technology which continuously collects data, or telemetry, from an endpoint and workload and through automated analytics identifies known and potentially risky behavior of applications that may indicate a cyber attack including ransomware;

ii. **Network Detection and Response (NDR):** A technology which continuously collects data, or telemetry, from the network and through automated analytics identifies known and potentially risky behavior of applications that may indicate a cyber attack including ransomware;

iii. **Sandbox:** A technology that provides full emulation of a machine to allow for 'detonation' (execution) of suspect code in order to assist with detection and analysis of adversary tools;

iv. **Intrusion Detection / Protection Systems (IDS/IPS):** A technology that inspects all traffic that enters the network, detecting and preventing known threats from

gaining access to the network, critical systems, and data. IDS/IPS looks for known malicious traffic patterns, to hunt for attacks in the traffic flow [10].

h. PREVENTATIVE CONTROLS THAT REDUCE THE LIKELIHOOD AND/OR SCOPE OF ATTACK

i. **Microsegmentation**: A software defined network-based technology that allows for very granular segmentation of the network such that the elements of a single application are in effect on their own network. Thus, an attack on the HR application is less likely to spread to the finance application;

ii. **Egress Firewall policy:** Policies that ensure that traffic going out of (egress) from inside the network to the internet are monitored and managed. Thus, attackers are more likely to be detected and blocked if they try to move stolen data to the cloud, and attack tools that rely on communication from an internal system to an externally hosted 'command and control' server will be prevented;

iii. **Multi-factor Authentication (MFA) / Privileged Authentication Management (PAM):** MFA is a set of technologies that replace passwords with a range of far stronger, alternate methods. An example is a random number token generating key or software app. PAM ensures the principle of 'least privilege' whereby highly privileged users within the organization such as systems administrators do not have to conduct all their tasks, all the time with a user credential that allows unrestricted 'god like' access. Such user privileges are highly sought by attackers and if gained effectively give over the keys to the kingdom;

iv. **Cloud Access Service Broker (CASB):** A technology that manages cloud service consumption. A CASB offers services such as monitoring of cloud user activity, alerting of cloud administrators of potentially risky behavior, and the enforcing of security policies related to the cloud;

v. **Airgapped backups:** Data and system backups are always important. In the context of their use as a tool to enable restoration of ransomed data it is vital that the backups themselves are isolated either physically or logically from the backed-up environment.

vi. **Data Encryption**: While it may seem counter-intuitive to consider data encryption as an element of ransomware defense, encryption of data-at-rest can help defend from dual-extortion methods modern ransomware gangs employ. Databases and critical file systems that attackers will consider worthy targets for theft, sale, and/or ransom of contents should be encrypted on disk.

[10] See https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall.pdf.

Evaluation Guidance

Use this checklist to perform a rapid, high-level evaluation of your readiness to deal effectively with a ransomware attack:

Identify:

- ❑ Have created and tested disaster recovery plans before ransomware event occurs.
- ❑ Understand and confirm what response will be taken if a ransomware event occurs (i.e., pay/not pay ransom).
- ❑ Have documented critical systems, processes, flows, and dependencies.
- ❑ Ability to identify security gaps and vulnerabilities in environment.
- ❑ Have plans and documentation critical to the execution of the IR plan stored in a location where they cannot be rendered inaccessible by a ransomware attack.

Protect:

- ❑ Can implement security policies to prevent malicious behaviors and applications.
- ❑ Continually perform dynamic analysis of unknown binaries for malicious/suspicious behaviors.
- ❑ Have tested ability to back up to and recover data from a secure, clean, disaster recovery environment.

Detect:

- ❑ Have ability to find initial compromise time, location, and vector through investigation.
- ❑ Have ability, either via internal staffing or via contract with a third party, to proactively threat hunt and detect earlier attack stages (ex: initial access, lateral movement, persistence, etc.)
- ❑ Can correlate signals to identify attack campaigns and spread.

Respond:

- ❑ Have ability to take immediate action even if the affected system, or the IR team personnel are remote.
- ❑ Ability to prevent lateral movement when malicious activity is detected [11].

[11] Lateral Movement refers to the actions an attacker takes, once they have achieved initial compromise, to move from one system to another within the same network.

Recover:

- In the case of compromise can recover data and endpoints to clean state based on investigative data.
- Ability to audit recovered data and systems to ensure accuracy and also that they are free of any potential residual threats that the ransomware attack may have left installed.

Summary and Additional Resources

The nature of modern ransomware attacks has evolved tremendously over the last few years, and we find that globally ransomware is reported as being in the top three types of cyber threats (country and industry sector dependent). The criminals behind these ransomware attacks have significantly altered and expanded the range of techniques they use throughout the execution of their campaigns. We also find that ransomware attacks are launched against organizations of all sizes, and that they are both specifically targeted against chosen organizations as well as conducted on a widespread "spray and pray" approach that may affect many. The technical entry-barrier to running a sophisticated ransomware campaign has also lowered, with all of the infrastructure necessary to conduct such a campaign available for rent in the form of Ransomware-as-a-Service.

Due to this changing landscape, and the fact that the business imperative to innovate is rapidly driving up the reliance on IT systems organizations must prepare for an inevitable ransomware attack. To not do so is to unnecessarily increase business risk.

Much as we may wish for it, there is no single, silver bullet solution that addresses all aspects of a sophisticated ransomware attack. Technology vendors who purport to offer a single boxed solution that claims to do so are today's Snake Oil Salesmen.

With these factors in mind, the only effective approach to mitigation of this class of cyber threat is one that is led by business and supported by a series of cross functional teams. Ransomware, which by the very nature of its execution is an attack against information technology, must of course also be countered by a range of information technology initiatives. These include efforts by the Cyber (or Information Security) team to prevent, detect, and respond to ransomware attacks, as well as those efforts made by the Infrastructure and Network teams to build resilient and recoverable systems.

This VMware Inc. Industry Guide has provided an introduction to the modern state of ransomware, and provided an overview of the recommended strategic approach to minimizing the risk that this threat poses to your organization. For more information, including details of technical solutions VMware offers please refer to "Additional Resources".

Ransomware, like other types of cyber attacks will continue to evolve over time. We will therefore continue to update this Industry Guide over time as we identify significant changes to ransomware attack types and the techniques the attackers utilize that require material changes to our recommended best practices.

Additional Resources

- https://www.vmware.com/topics/glossary/content/ransomware.html
- https://core.vmware.com/ransomware
- https://www.vmware.com/products/cloud-disaster-recovery/ransomware.html
- https://www.vmware.com/solutions/ransomware-protection.html
- https://www.youtube.com/watch?v=Fg0p1Ccxf7E (Detection and rollback of ransomware with VMware Carbon Black Cloud)
- https://www.youtube.com/watch?v=ovWr52KDoQs (vSphere LIVE: Ransomware & Security)
- https://blogs.vmware.com/security/2020/09/stop-ransomware-nsx-network-detection-and-response.html

Changelog

The following updates were made to this guide:

Date	Description of Changes
3 June 2022	• Initial publication.

Feedback

Your feedback is valuable.

To comment on this paper, contact VMware Carbon Black Technical Marketing techzone-sbu@vmware.com.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.