Gartner

Licensed for Distribution

How to Prepare for Ransomware Attacks

Published 16 November 2020 - ID G00735746 - 13 min read

By Mark Harris, Brad LaPorte, **and 1 more**

Ransomware attacks continue to increase, using techniques that are growing more and more sophisticated and targeted. Security and risk management leaders need to look beyond just the endpoints to help protect the organization from ransomware.

Overview

Key Challenges

- Remote desktop protocol, bring your own PC, and virtual private network vulnerabilities and misconfiguration are becoming the most common entry point for attackers. This has been exacerbated by the growth in remote work resulting from the pandemic.
- Ransomware is increasingly being operated by humans, rather than being delivered as spam by technology resources.
- The cost of recovery and the resulting downtime in the aftermath of a ransomware attack, as well as the reputational damage, can be 10 to 15 times more than the ransom.

Recommendations

Security and risk management leaders responsible for endpoint and network security must focus on all three stages of a ransomware attack:

- Get ready for ransomware attacks by constructing a preincident preparation strategy, that includes backup, asset management and the restriction of user privileges. Determine whether the organization is ultimately prepared to pay a ransom or not.
- Implement detection measures by deploying behavioral-anomaly-based detection technologies to identify ransomware attacks.
- Build postincident response procedures by training staff and scheduling regular drills.

Introduction

Ransomware continues to pose a significant risk to organizations. Recent attacks have evolved from the autospreading attacks, such as Wannacry and NotPetya, to more targeted examples, [1,2] which attack an organization, rather than individual endpoints. The impact these attacks have on organizations has increased to the point where some organizations have gone out of business, [3] and, in the case of healthcare, lives have been put at risk. [4] Security and risk management (SRM) leaders need to adapt to these changes and look beyond just endpoint security controls to protect against ransomware.

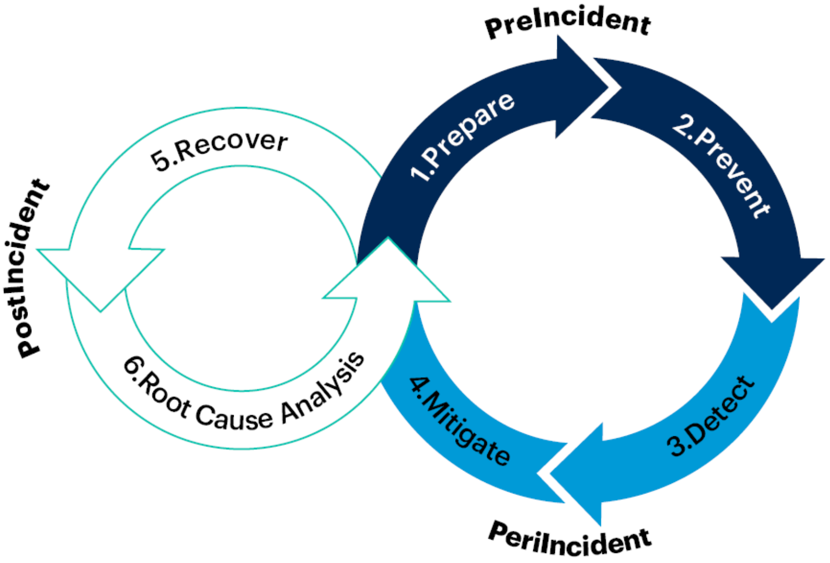
Recent ransomware campaigns, such as REvil and Ryuk, have become "human-operated ransomware," where the attack is under control of an operator, rather than spreading automatically. Such attacks often take advantage of well-known security weaknesses to gain access. For example, a number of recent ransomware incidents are thought to have started with poorly configured or vulnerable remote desktop protocol (RDP) configurations. Previously compromised credentials are also used to gain access to accounts.

Once inside, the attacker will move around in the network, identify the valuable data, and assess the security controls used, often disabling endpoint protection tools and deleting backups. Then, when the data has been identified, it can either be uploaded and later used for extortion (Doxing), or the ransomware will be launched to encrypt the data.The typical dwell time between the first evidence of malicious activity and the deployment of ransomware is three days. [5] The goal is to maximize the likelihood of the ransom being paid, often including threats to make data public if the ransom isn't paid quickly.

Protecting organizations against these attacks goes beyond endpoint protection and encompasses many different security tools and controls. Figure 1 describes the ransomware defense life cycle. It is important to examine all of these phases and to assume that an attack will be successful and plan to respond accordingly.

Figure 1: Ransomware Defense Life Cycle

Ransomware Defense Life Cycle



The defense life cycle is a continuous process of **Preparation, Prevention, Detection and Mitigating Attacks**. When a ransomware attack is successful, the **Recovery** and **Root Cause Analysis** phases are triggered.

Source: Gartner
735746_C

Gartner

Analysis

Construct a Preincident Preparation Strategy

SRM leaders should work with the principle that a ransomware attack will be successful, and ensure that the organization is prepared to detect as early as possible and recover as quickly as possible.

The first and most common question is, “Should the ransom be paid?” Ultimately, this has to be a business decision. It needs to be made at a board level, with legal advice. Law enforcement agencies recommend not paying, because it encourages continued criminal activity. In some cases, paying the ransom could be seen as illegal, [6] because it provides funding for criminal activity. Even if the ransom is paid, the encrypted files are often unrecoverable.

However, if an organization wants to be ready to pay, it is important to establish a governance and legal process that includes the CEO, the board and key operational staff. Setting up a cryptocurrency wallet can take time, so, if payment is a possibility, then making the necessary preparations will speed up the time to recover. (See How to Prevent or Mitigate Ransomware Attacks That Demand Payment in Blockchain Cryptocurrency.)

A good backup process and strategy is the primary line of defense against ransomware. Ensure that the backup solution is resistant to ransomware attacks, and continuously monitor the status and integrity of backups (see Magic Quadrant for Data Center Backup and Recovery Solutions). In particular, most backup vendors provide a mechanism to create immutable second copies of backups or immutable snapshots.

Recovery goes beyond restoring the data. Ransomware will effectively lock a machine with the ransomware note and restoring machines to a known good state can be more complex than restoring the data. Having the tools and processes in place to restore endpoints to a golden image can speed up the recovery time. Some organizations resort to USB devices for remote and overseas locations. Gartner occasionally sees clients not even attempt to clean or restore a machine. Instead the ransomware event is a reason to refresh its hardware. Whatever, the process, this should be regularly simulated to uncover deficiencies.

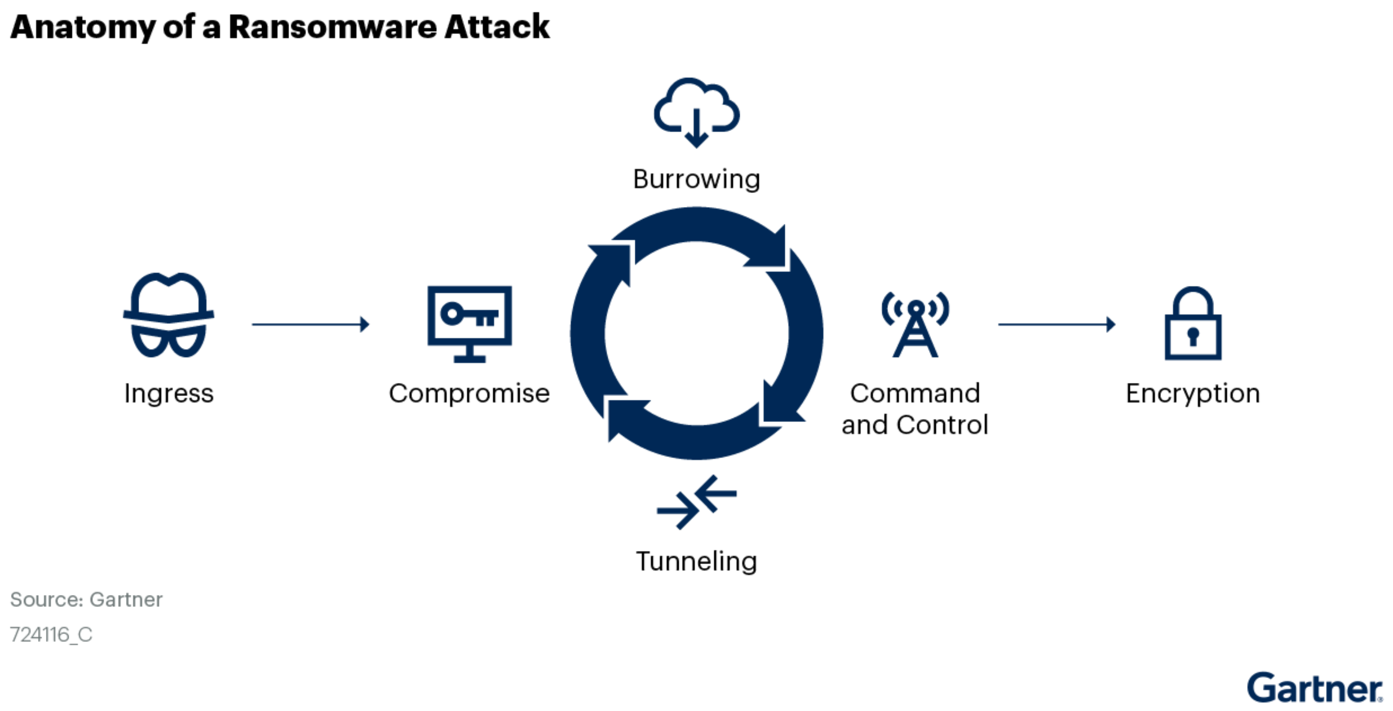
Security awareness for users is also important. Constantly educate users on the types of attacks being seen with regular alerts and security "newsletters" to reinforce the education. Create a simple set of security messages that are repeated regularly. An alert user will not only be less likely to fall for social engineering, but can act as an early warning. Ensure users are regularly trained on how to identify malicious emails, in particular. Provide an easy mechanism for reporting suspicious emails and reinforce it with confirmation that the user has done the right thing. Consider email-focused security orchestration automation and response (SOAR) tools, such as M-SOAR, to automate and improve the response to email attacks (see Market Guide for Email Security).

Security hygiene is critical to protect against "human-operated" ransomware, and a holistic view of the whole organization is required. SRM leaders should include the following as part of their strategy to protect against ransomware:

- Build a reliable asset management process to identify what needs to be protected and who is responsible. Particular attention should be paid to legacy systems (see Magic Quadrant for Enterprise Asset Management Software).
- Implement a risk-based vulnerability management process that includes threat intelligence (TI). Ransomware often relies on unpatched systems to allow lateral movement. This should be a continuous process. The risk associated with vulnerabilities changes as vulnerabilities are exploited by attackers (see The Essential Elements of Effective Vulnerability Management).
- Remove users' local administrative privileges on endpoints and limit access to the most sensitive business applications, including email to prevent account compromise (see Magic Quadrant for Privileged Access Management).
- Implement compliance scanning for misconfigured and noncompliant systems, as well as penetration testing and breach attack simulation (BAS) tools.
- Implement strong authentication for privileged users, such as database and infrastructure administrators, and service accounts. Log the activity. Bad actors will often use known, detected malware to gain access to higher-privileged account credentials.

Ransomware attacks typically follow the attack pattern shown in Figure 2.

Figure 2: Anatomy of a Ransomware Attack



Anatomy of a Ransomware Attack

Source: Gartner
724116_C

SRM leaders should align their security strategies to the patterns and techniques used by the attackers. The MITRE ATT&CK framework can be used to assess and score an organization's protection against each phase. MITRE also provides SHIELD, which is an active defense knowledge base that maps attack techniques to defense techniques, as well as a cyber TI repository listing the postcompromise techniques and tactics used.

The attack starts with ingress, i.e., the initial point of attack. This often takes the form of a compromised website delivered through a phishing or targeted attack. Secure email gateways (SEGs) and secure web gateways (SWGs) can help provide protection. Technologies such as web isolation can also limit the impact. As discussed earlier, another common method of attack is through vulnerable RDP ports. Penetration testing can be effective at finding holes in defenses.

Once compromised, endpoint protection platforms (EPPs), endpoint detection and response (EDR), and mobile threat defense (MTD) solutions should be used as part of the defense. If internal teams don't have the necessary skill set or bandwidth, supplement EDR with managed services (see Market Guide for Managed Detection and Response Services). EDR tools are designed to detect the encryption activity and prevent it from continuing.

Compromised machines receive instructions through command and control channels. DNS security, SWGs, and other network detection and response (NDR) solutions can detect and block these channels. Further tunneling or lateral movement occurs as the attacker tries to move around the organization. Endpoint firewalls and segmentation of networks, as well as strong vulnerability and patch management, limit what the attacker is able to achieve.

Implement Detection Measures to Identify Ransomware Attacks

Inevitably, ransomware may get past your defenses and the protections put in place. Then it becomes a matter of how quickly you are able to detect the incident. Many of the tools described for protection will also provide the data and telemetry for detection. In particular, EDR tools collect indicators of compromise (IOCs) and events that may not be enough to specifically identify and prevent an attack, but can show that there "may" be an attack underway. EDR can also help identify "burrowing," where the attack remains quiet, while further compromised accounts and privileges are gathered.

The understanding, interpreting and investigating of these IOCs and events tend to require a higher level of expertise. Increasingly this is being purchased as part of an EDR solution or as a wider MDR or managed solution. Using these services can be beneficial to organizations without the staff or skill sets to have their own security operations centers (SOCs).

Other security tools also come into play during the detection phase. Intrusion prevention systems (IPSs), as well as NDR and network traffic analysis (NTA) solutions, can help provide early detection (see Market Guide for Network Detection and Response). Deception tools can also be effective. This can be as simple as setting up fake "administration" accounts that are never actually used, so that, if an attempt is made to use it, an alert can be sent. Other types of lures, such as deception platforms and honeypots, can also be deployed as part of a ransomware defense strategy (see Improve Your Threat Detection Function With Deception Technologies).

In addition to the IOCs and alerts coming from security tools, it's also important to look at what is "not happening." If backup schedules are changed or stopped, backup volume or change rates increase unexpectedly. Shadow copies disabled on certain machines, as well as security tools no longer running on machines, could indicate that an attacker is inside the organization.

Once a ransomware attack has been detected, minimizing the impact is essential. The most common technique used is isolation. There are a variety of isolation techniques, and many EDR tools provide on-device isolation functionality to enable incident responders to isolate machines from the rest of the network, while allowing remote access for remediation to be carried out.

Network-based isolation is more of a blunt instrument and requires banning suspected devices based on the hardware-level MAC address (hence the importance of mature asset management). This is applied to on-premises network switches, virtual private networks (VPNs), network access control (NAC) and the organization's Wi-Fi access points. Often this becomes frantically pulling out network cables. However, this can slow the recovery phases, because it requires physical access to devices for remediation.

Many organizations will need assistance to help mitigate and recover from an attack. Specialist incident response teams can play an important role, and having an incident response retainer in place can reduce the cost and speed of the response (see Every Organization Should Assess the Value of an Incident Response Retainer).

The tactical recovery steps will vary, depending on the organization and the extent of the ransomware, but will involve:

- Recovery of data from backups, including verifying the integrity of those backups and understanding what data, if any, has been lost.
- Once compromised, EPPs and EDR, as well as MTD solutions, should be used as part of the remediation response to remove the threat and roll back any changes. As noted earlier, recovery goes beyond recovering the data; infected machines may be "locked" and may require physical access. During the preparation phase, it's important to understand and plan for how this would be achieved.
- Validation of the integrity of a device before it is allowed back onto the network.
- Updating or removing compromised credentials; without this, the attacker will be able to gain entry again.
- Perform a thorough root cause analysis of how and what happened, including any data that has been exfiltrated (doxing). Doxing occurs when bad actors threaten to release stolen information. This is increasingly becoming a secondary method of extortion if a victim decides not to pay the ransom.

Infrastructure as a service (IaaS) and platform as a service (PaaS) environments are equally susceptible to ransomware attacks. Conceptually, these should be addressed the same way. What changes is the tactical activities that are needed to execute to isolate affected devices/network segments.

Build Postincident Response Procedures by Training Staff and Scheduling Drills

SRM leaders must ultimately be prepared for a ransomware attack to be successful and have plans, processes and procedures in place. These plans need to include the IT aspects, as well as communication plans to both internal staff and partners\suppliers (see How to Prepare for and Respond to Business Disruptions After Aggressive Cyberattacks). It is important to recovery that SRM leaders quickly and clearly communicate the issue. Provide regular updates on status and when systems will be recovered to the point where systems are usable. Several cyber crisis simulation tools can help identify gaps in procedures, roles and responsibilities.

These plans will vary, based on the extent and success of a ransomware attack. It may only be a small part of an organization, and the impact could be minimal. For larger attacks, the impact may go beyond the organization to customers and partners. As part of the preparation, running regular fire drills or table-top exercises to rehearse a response can be beneficial (see Toolkit: Tabletop Exercise for Cyberattack Preparation and Response).

Once recovery is in progress, collect enough information to understand the root cause of the attack and understand what controls failed or weren't in place. Again, specialist digital forensics and incident response services play an important role in this analysis. Once systems are recovered, it is critical to implement the lessons learned and feed them back into the preparation phase.

Evidence

[1] Major Hospital System Hit With Cyberattack, Potentially Largest in U.S. History, NBC News.

[2] They Come in the Night: Ransomware Deployment Trends

[3] Company Shuts Down Because of Ransomware, Leaves 300 Without Jobs Just Before Holidays, ZDNet.

[4] German Hospital Hacked, Patient Taken to Another City Dies, SecurityWeek.

[5] They Come in the Night: Ransomware Deployment Trends, FireEye.

[6] Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, U.S. Department of the Treasury.

Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment

advice and its research should not be construed or used as such. Your access and use of this publication are governed by Gartner’s Usage Policy. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "Guiding Principles on Independence and Objectivity."