FORTRA

Dissecting Ransomware: Understanding Types, Stages, and Prevention

While many new threats and emerging attack methods could significantly impact your organization, the more likely scenario is attackers will apply tried and tested methods they already know to be effective. Attackers favor low-effort, high-value tactics – like ransomware – because they are easy to pull off and profitable.

According to Verizon Research, no matter how many other threats are out there, ransomware continues to dominate as three of the top four incident attack vectors. It's no wonder ransomware is a staple, as attackers get approximately **$170k per ransom** on average. Considering how easy it is to spread via phishing, email, and infected websites, ransomware is the very definition of low effort and high reward.

Preventing ransomware infections takes more than an antivirus (AV), as AV solutions are not perfect, and one failure can have significant consequences. Organizations need a combination of awareness, prevention, and a cohesive strategy to combat this threat, building in layers of protection.

The Types and Stages of Ransomware

To determine an effective strategy, it helps to understand the different types and stages of ransomware. With this information, you can select appropriate controls to stop ransomware before a full-blown infection runs its course.

Ransomware Types

The most common types of ransomware used by attackers are listed below. Encryptors and lockers lead the pack as the most used among them.

- **Crypto ransomware or encryptors** - Encrypts files so organizations cannot access them.
- **Lockers** - Locks organizations out of their systems.
- **Scareware** - Disguised as a solution and mimics legitimate security tools.
- **Doxware or leakware** - Threatens to publish personal information or impersonates law enforcement demanding fines.
- **Ransomware as a Service (RaaS)**- Malicious actors lease ransomware strains and initial access to compromised networks for a share the profits.

Within these types exist different groups or families of ransomware. For example, Darkside is the group that uses a RaaS model and is known for the attack on the Colonial Pipeline in 2020.

- **LockBit** - Extremely active but prefers low-profile attacks. Encrypts and exfiltrates files.
- **Black Basta** - Deploys DDoS attacks. Known to rely on double extortion tactics.
- **Hive** - Targets industrial and education targets, encrypting data.
- **ALPHV/BlackCat** - A RaaS model, it launches DDoS attacks.

Ransomware Stages

While there are more than 130 different ransomware families detected since 2020, most ransomware attacks follow the same general process and are broken up into five major stages:

1. **Delivery** - The start of the attack where the malware makes an appearance via a phishing email, use of an exploit, or accessing an infected external host. At this stage, the malware hasn't taken root, but something or someone has been exposed.
2. **Command and Control** - Once the malware has found a place to run, it reaches back to its origin for further instructions. Usually, the initial installation is nothing more than the groundwork to get embedded in a device. The later stages' more complicated instructions, encryption keys, and code are downloaded here.
3. **Credential Access** - As the malware is already installed and running on a device, it starts investigating for stored credentials or saved access. The goal is to spread to different accounts and devices across the network, so anything discovered here will lead to more damage across the organization. This is where backdoors may be open to allow attackers direct access to the network.
4. **Canvasing** - The malware looks for valuable files, especially those containing personal information, financial data, or research. Before these files are encrypted, they get sent back to the source for later attacks. In this stage, the malware stretches its tendrils out to other shared storage and devices to infect them and repeat the process.
5. **Extortion** - This step is the culmination of the attack. Data has already been stolen and the device is fully encrypted. Attackers demand payment from victims to regain access to their data. If payment is made, the attackers might provide a decryption key, but there are no guarantees.

Stopping the cycle early is crucial for defending the business. Blocking ransomware in the earlier stages diminishes the overall impact on the organization including data loss and effort required to remediate.

Post-attack Extortion

Despite ransomware having a direct cost of holding data hostage, there is a secondary target in stealing the data. Once an attacker has an endpoint infected, it is more efficient and profitable to steal data simultaneously. This leads to double and triple extortion attacks that multiply beyond the initial cost of unlocking of the data with threats to release or sell the data.

With double extortion, attackers will extort the company itself not to have the data released or sold. The triple extortion attack has the attackers go a step further to contact those who have had their data stolen (customers or partners of the target business) and individually request ransom from them. At this point, the breach becomes very public and much harder to contain.

Ransomware Data Theft

Even for those who pay the additional extortion requests, it is still likely that the attacker will sell the data on the dark web. Sensitive information such as social security numbers (SSNs), credit cards, bank accounts, driver's licenses, and other personal data is valuable. Reselling this information is easy, and it is challenging for law enforcement to track down the sellers, making the risk to criminals extremely low.

Data theft results in a breach for organizations, which has direct consequences if a legal or regulatory compliance framework controls the information. Not only must the organization report the breach in these cases, but in many cases, the company is liable for the breach. This can result in direct fines, corrective action plans, or lawsuits from affected customers. Beyond this is the residual reputational damage that will plague the company, decreasing the trust existing and future customers have in their security, resulting in lost business down the road.

Building Barriers to Ransomware

To remain safe, organizations need several security layers to prevent malware from ever getting to the point where it starts to run. Targeted malware circumvents specific types of controls, making it harder to detect and block. Multiple layers of controls ensure that protection remains even if one is bypassed, maintaining your security.

Antivirus Isn't Enough

Antivirus solutions alone are insufficient to protect against every strain of malware. Zero-day and unique permutations keep ahead of many signature-based detections. By the time an AV has detected ransomware, it has already passed through numerous lines of defense. While not as susceptible to the lag in detection as signature-based detection, behavior-based virus detection may not be enough either. By the time AV observes risky behavior, the damage has already been done, or data is irrevocably lost.

AV should not be the only protection. Organizations must layer their security with proactive measures at the beginning of the attack continuum – before the attack.

> **"AV SOLUTIONS ARE AN EXCELLENT LAST LINE OF DEFENSE BUT FENDING OFF RANSOMWARE EARLIER IN THE ATTACK CYCLE MINIMIZES IMPACT"**

Code Vulnerability Discovery

Vulnerabilities exist not just in endpoints but also in the code created for software and applications. Custom applications have vulnerabilities that stem from logical errors, third-party libraries, and coding mistakes. Much like managing vulnerabilities on an endpoint, these issues need to be discovered, prioritized, and remediated using the right tools.

Endpoint vulnerability scanning tools draw from publicly available databases of known vulnerabilities. Custom applications require a combination of testing tools to evaluate the code and how it performs so they can uncover unknown vulnerabilities.

SAST - Static application security testing tools review the code looking for logical errors and mistakes made by developers.

DAST - Dynamic application security testing tools test against built software to determine exploitable paths in the software when it runs.

Fuzzing - Fuzzing tools are a form of DAST testing that tests software inputs and interfaces using malformed and random information to induce errors.

Using a combination of testing solutions during the software development lifecycle (SDLC) can determine the security posture of custom software and applications and prevent costly breaches.

Find and Fix Vulnerabilities

One of the best ways to make your organization a more challenging target for ransomware attacks is to remove accessible entrances for attackers to exploit. Attackers often start their process by scanning their target for known vulnerabilities that have not been detected or remediated. Using a known vulnerability makes the attack process less complicated and allows them an easier path to install ransomware.

Endpoint Vulnerability Scanning

Endpoints are often the target for attackers with ransomware, especially since more people are working remotely and using non-corporate devices. Malicious actors look for known exposures that they can easily compromise first, before getting more inventive. Proactive scans and testing help discover problems before attackers do.

The effectiveness of the vulnerability evaluation process depends on the quality of the vulnerability scanning solution employed. Not all scanners are made equally. They draw from different databases of known vulnerabilities, have different levels of accuracy, and scan at varying rates. Even for solutions that seem identical across these lines, not every solution is made for every platform. Some work well for on-premises resources but have no capacity for the cloud, while others are built with a cloud-first approach.

Managing Vulnerability with Limited Resources

There is more to vulnerability management than identifying and fixing what exposures exist. Organizations have limited resources, so addressing everything is impossible. An organized and standardized plan is crucial for this process. It allows organizations to reduce as much of their risk as possible without overtaxing their current staff.

Personalize Prioritization

Prioritization is the most critical step to successful vulnerability management. Some organizations believe that simply squashing all vulnerabilities that are scored high or critical by CVSS is sufficient to protect themselves, but in reality, this approach is highly inefficient and leaves them exposed.

In CVSS scores, general vulnerability exploitability is factored in, but it is not organization-specific. The way each company implements its technology can create controls that make it harder or easier for an attacker to leverage a vulnerability. Knowing this infrastructure-specific information and adjusting the scoring accordingly helps personalize prioritization for a risk-based approach that optimizes team efficiency and effectiveness.

Test and Validate

The existence of exploitable vulnerabilities can be further validated through penetration testing. Sharing vulnerability scanning results with a pen testing team or pen testing software can confirm if any of these vulnerabilities can be exploited and identify what business-critical assets and data can be accessed through that exploit.

Additionally remediation verification pen testing can validate that implemented fixes are effective for resolving the vulnerability. Penetration testers can validate that new controls not only function as expected but also that they are not easily circumvented. They do this by thinking and behaving as malicious attackers do, but without damaging or stealing your data. An example of this is their ability to chain together several vulnerabilities of lower risks to determine if, in combination, they can elevate to a more impactful exposure.

Having this functionality is not easy for every organization, as skilled testers can be costly to maintain and hard to hire. In these cases, there are alternatives to having a permanent on-site team.

Outsourcing - Using an external team or vendor allows your organization to get many benefits of penetration testing without keeping them on staff full-time. External testers can also augment existing teams with specialized skills, helping in focused testing.

Self-Service - Using specialized toolsets, organizations can accomplish some of the same testing that a penetration tester can do with less experienced individuals. Self-testing can remove some data-gathering steps in validating controls, streamlining a future pen testing engagement.

No matter how an organization wishes to approach it, the vital step is to test against the control to validate that it is functioning correctly.

Monitoring Infrastructure

Monitoring for anomalous utilization is essential for discovering ransomware's presence. Ransomware comes with telltale signs, such as dialing home to known malicious locations or network probing that can serve as early indicators of an attack. Watching for these indicators can give your organization a head start in stopping an infection from spreading.

Knowing When Attackers are Knocking

Automated threat detection tools monitor asset behavior to identify malware infection. These attacks come with known indicators such as elevations in hardware utilization, network probing, and attempts to access external resources. Monitoring this information and leveraging machine learning (ML) to determine variations from expected behavior can raise alerts early in the infection process. This approach can be tied into automated alerting and blocking access, cutting off paths for malware to propagate, and reducing the overall blast radius of infection.

Layers of Protection

Reducing your ransomware risk requires a complete toolset to create multiple layers of protection. However layered doesn't have to mean complicated. Working with organizations that offer interoperable solutions can help simplify your efforts to establish layered security. We offer high-powered security solutions that are bundled together to help reduce dashboard fatigue and prevent data silos.

Learn more about our offensive security bundles – including penetration testing, adversary simulation, and vulnerability management - and see how they can help simplify and strengthen your organization's security.

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.