FORTRA

GUIDE *(Digital Defense)*

Beating the Business of Ransomware

Ransomware groups are even more far-reaching, powered by better organization and solid business models.

Ransomware is no longer about shady guys in a hoodie acting alone in a dark apartment. It has evolved into a corporate enterprise with products, profit sharing, subscriptions, and technical support. Ransomware is a booming business with over 1000 ransomware groups, over 100 of which are large enough and dangerous enough to be actively tracked by the FBI.

This evolved ransomware has increased the challenge for businesses and taken cyber extortion to the next level. Attackers are well funded and organized, which has allowed them to develop more devastating attacks and operate more efficiently. Fortunately, organizations can gain the upper hand by understanding the new face of ransomware and its attack vectors. This article will explore how ransomware groups are changing and how organizations can beat them in this new game.

How Ransomware is Growing as a Business

Ransomware's more organized business model was the next logical step in its evolution. After all, it takes more than a single person to manage the workload of fully-featured attack platforms that widely propagate to numerous endpoints. These criminals have formed syndicates -- some call them gangs --and contributed various skill sets to make their products harder to detect and decrypt without paying up. By operating as an enterprise and bringing together combined cybercrime services and expertise, the scourge of ransomware can scale, attacking a wider variety of targets at a much faster pace. This effectively puts all businesses in the crosshairs and increases the pressure on security teams large and small to protect their organizations.

Mass-Produced Malware

As ransomware gangs have profited from attacks, they have re-invested some of their ill-gotten gains into developing new ransomware strains. This development capability led to automated mutation technology that can mass-produce new variations. It is so effective that researchers discovered over 168 million new strains in 2021 alone. These new strains do not automatically appear on signature-based antivirus (AV) detection methods, even though they might be variations on known or existing versions. They require behavioral-based detection to catch dangerous activity and block it.

"2 out of 3 Ransomware attacks are facilitated by the RaaS." [1]

Ransomware as a Service (RaaS)

Ransomware as a service (RaaS) is one of the latest developments by ransomware groups for monetizing ransomware. As with most "as a service" offerings, criminal RaaS offers many of the expected business support capabilities such as installation and distribution guidance and technical support when things go wrong.

Gangs selling RaaS no longer have to launch attacks themselves. Instead, they offer the ransomware platforms developed for rent to other criminals. This allows less technical cybercriminals to use more advanced malware platforms as their own for a share of the profits. Some RaaS platforms have recently added backdoors, allowing the original group to step in and steal ransoms from the other criminals paying them for the service.

Despite the risks associated with utilizing RaaS, they still have customers that want to use the service. It is an easy way for criminals to get their hands into a very lucrative market without having to invest in the development of novel attack vectors. The RaaS model is designed to be turnkey where the clients leverage the technology of services of ransomware operators.

This model decreases the overall risk for the creators of ransomware and eliminates a lot of the heavy lifting of running the attacks themselves. Instead, the customer handles choosing the targets, running the attack, and negotiating the payouts. This leaves the seller free to collect the profits and if they choose, re-invest them into creating malware that is harder to detect and mitigate.

Data Theft and Double Extortion

Ransomware has also evolved beyond simply locking up endpoints to include added layers of extortion as part of the attack chain. Once ransomware has infected the endpoint, it can automatically search for valuable data. It can also open up backdoors to allow cybercriminals to search manually. The information they find is exfiltrated off-site to be ransomed off separately. Any financial information about the organization found in this process is used by criminals to more accurately price ransom demands for what they think the company can afford to pay.

Even if organizations decide not to pay the ransom to unlock endpoints, the criminals still have an avenue of profiting. Using the stolen data, they demand payment to not disclose it publicly. Of course, being criminals, there is no guarantee they will stop at one demand or even two. If the company pays this first extortion attempt, the cybercriminals can easily return with additional demands. This can lead to double, and triple extortion attacks, where the malicious actors reach out to customers, instead of the company, demanding a ransom payment, or they will share or sell the customer's personal information publicly.

Legal Avoidance

To help evade legal repercussions, many of these ransomware organizations operate in areas where enforcement is less likely or the laws of the targeted countries will not apply to them. Many of these countries have non-extradition treaties with the countries that will be attacked, or they do not have their own laws that cover cybercrime. This enables the attackers to operate legally in the country while having protection against being arrested and sent away to face charges.

This does not mean that cybercriminals are entirely above the law. With recent arrests of REVIL ransomware gang members in Russia, there is still potential for legal repercussions. Unfortunately for most ransomware targets, even if the criminals can be located, the potential to seek justice or be compensated for losses is extremely low. Even when the US knows enough information about overseas attackers to bring up charges against them, the likely outcome is that they will never actually be arrested or go to trial. Bolstered by legal loopholes and growing business prowess, ransomware is doubling the pressure on organizations to mobilize strategic defenses and protect their vital assets.

Organizational Defense

With this new face of ransomware, it has gotten more complicated for organizations to protect themselves. Doing this requires a more holistic, proactive security approach combined with the agility to adapt as quickly as attackers do.

"Knowing the most prevalent attack vectors –phishing, software vulnerabilities, and remote desktop (RDP) exploitation –organizations can develop targeted strategies for prevention."

Proactive Cyber Defense

Organizations cannot stand idly by and wait until cybercriminals penetrate their defenses and ransomware has already taken hold. As resources are never infinite, they need to prioritize their strategy implementation. Taking a defense-in-depth approach to security that closes the gaps and allows rapid detection is vital to the process of ransomware prevention. Optimal solutions will help close the most gaps for the least expensive money and time investment.

One of the most cost-effective methods of doing this is identifying and mitigating software vulnerabilities. As vulnerabilities are often publicly published, they serve as easy targets for bad actors who can quickly scan systems to detect them. Organizations can take advantage of this and use the same approach to identify gaps with vulnerability scanning before attackers get the opportunity. Vulnerabilities can be prioritized by risk using this information to get the most efficient return on remediation.

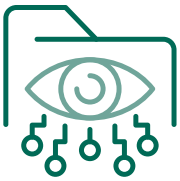
Vulnerability Management

Closing the vulnerability gap is crucial for stopping malware, Malware often exploits existing vulnerabilities to gain escalated privileges to install and take control of an endpoint. With fewer vulnerabilities in an organization, the attack surface is decreased, narrowing the options for criminals to trick your systems into running their malware.

Vulnerability scanning and assessment come in many different varieties and are used together to create a complete vulnerability management program. There is the internal vulnerability scanning of endpoints that focuses on infrastructure and investigates endpoints for exposures such as misconfigurations or software with exploits.

These assessments utilize either a built-in agent or credentials to see beyond what is exposed on the network but the actual configuration and software installed on the endpoint. This information allows organizations to gain highly targeted data about what vulnerabilities might exist, even if they are not apparent to an external attacker. Using this information, businesses can take a proactive approach to remediation and close potential gaps, before attackers can discover and exploit them.

Assessing application security vulnerabilities is the other crucial component of managing organizational vulnerabilities. Almost all applications have defects, with 76% of applications produced having one or more known flaws. These flaws may originate with the in-house programming team or imported libraries and must be identified and evaluated to determine how much risk they bring to the organization. Using application security testing such as Static Application Security Testing (SAST), or Dynamic Application Security Testing (DAST), businesses can detect these application security vulnerabilities, determine how dangerous they are, and prioritize them for remediation. DAST and SAST tools are optimized through cybersecurity automation to ensure they are baked into the build process guaranteeing that they are run every build reducing the probability of vulnerabilities making it into production code.



Increasing Visibility

Effective ransomware protection requires exceptional visibility. Much like on a battlefield, the visibility of your assets enables early detection and response to any actions taken against you. This data comes from a combination of network traffic, endpoints, and software messaging both on-premises and in the cloud.
It is crucial to not confuse the collection of data and analytics with true visibility. Just because large sums of data are collected, does not mean that this information is useful or actionable. To turn the collected data into functional analytics and alerts, it needs to be centrally managed. Centralized management in a cybersecurity dashboard allows for consolidated visibility in one location rather than forcing staff to access and monitor multiple locations. Doing this eases the labor requirements and helps to create more in-depth insights on the data collected.

Threat Detection

When organizations consolidate their organizational visibility, they can leverage technology to deliver faster and more accurate alerting. Modern threat detection utilizes a combination of artificial intelligence (AI) and machine learning (ML) in the analysis of large volumes of data. This analysis creates baselines of behavior for all aspects of the IT ecosystem. With these baselines, the threat detection software can alert on anomalies that may indicate malware infections.

Early detection is vital to threat management allowing teams to rapidly respond to anomalies and determine whether the anomaly is caused by ransomware, an attacker, or something else. Rapidly responding to potential attacks decreases the ability of the ransomware to spread throughout the organization. When infected machines are detected, they can be isolated and rebuilt. If detected early enough, the encryption and exfiltration may not have been completed, allowing data to be recovered and limiting the impact of the attack.

Combat Ransomware with Defense-in-Depth Strategy

Don't let your company fall victim to Ransomware tactics. With the proper defensive layers, you can prevent, detect, and proactively stop attackers from holding your organization hostage. Using vulnerability management as a foundational component of your stack allows you to scan, assess, analyze and manage threats to your network so you can effectively prioritize remediation. Additionally, be sure you have the application security tools needed to secure apps – dynamic application testing (DAST) and Black Box Fuzzing preemptively test applications before they launch to help detect security holes, while static application security testing (SAST) checks for insecurities at the time of development so there aren't costly fixes afterward the code is released. Lastly, it's a security best practice to conduct regular penetration testing to ensure your infrastructure doesn't have exploitable vulnerabilities. Combining these tools to create a defense-in-depth approach will pave the way to securing your organization against ransomware and other attacks by malicious actors.

SECURITY LAYERS

DEFENSE IN-DEPTH

1 NETWORK LAYER SECURITY
Firewalls, IDS/IPS, DMZ, Port Scanners, Network Sniffers, Patching, Vulnerability Scanners

2 PLATFORM LAYER SECURITY
Antivirus Programs, Patching, Security Specs for Systems, Access Mgmt, & Port Scanning

3 APPLICATION LAYER SECURITY
Secure Coding Practices, Web Application Firewalls, Secure Web Gateway Services

4 DATA LAYER SECURITY
Encryption, User access and Identity Management, Update Systems

5 RESPONSE LAYER MECHANISM
Security Monitoring, Intrusion detection, Recovery

[1] https://www.zdnet.com/article/ransomware-as-a-service-is-the-new-big-problem-for-business/

FORTRA

Fortra.com

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.