WHAT IS RANSOMWARE AS A SERVICE? RAAS EXPLAINED

Software is shifting away from locally-installed apps to Software as a Service web applications that run in the cloud. Criminals are cashing in on this trend, which has led to the creation of Ransomware as a Service (RaaS), a growing threat to business.

RaaS refers to various online malware exploits that bad actors can use to attack the IT assets of businesses and individuals. These attack programs are created by criminal entrepreneurs who sell their services to other criminals. The people who buy these programs then extort or blackmail their victims by holding computer systems to ransom.

It's painfully clear that the popularity of these ransomware platforms will continue to grow, so you must be prepared.

How ransomware as a service works

Most models for RaaS follow a similar approach:

1. Experienced hackers and cybercriminals (code creators) write ransomware code.
2. Code creators rent or sell the code or "exploit kit" to other criminals (attackers) who want to exploit computer systems.
3. Code creators provide guidance to attackers on using the code to penetrate the target's defenses.
4. Attackers launch the ransomware code onto the target and exploit vulnerabilities.
5. Ransomware code typically encrypts, locks up, or threatens to delete the victim's systems and

files.
6. Victims have to pay a ransom to have systems and files restored.
7. Criminals split the ransoms between the code creators, attackers, and anyone else involved.

Why criminals use ransomware as a service

RaaS is available over the dark web, a hidden, "underground" internet where criminals trade in identity theft, data breaches, malware, and other activities. RaaS is becoming more popular because it allows attackers without coding experience to partner with ransomware creators who may not want to initiate attacks themselves. Creators earn money for writing and adapting code, while attackers can rent attack software.

Most ransomware attacks use well-understood attack methods, exploiting known vulnerabilities, phishing, email malware payloads, and various other techniques.

The impact of ransomware

If you're the victim of a ransomware attack, you have three options if your files and services are encrypted or locked:

1. Roll back your data and systems to a backup taken before you were attacked.
2. Attempt to delete the ransomware application and decrypt the files yourself.
3. Pay the ransom and hope the attacker provides a decryption key.

Practically speaking, if you don't have a snapshot data backup, option one won't be possible. Option two will be extremely difficult due to the level of encryption used. For option three, you have no guarantee the attacker will decrypt your systems.

How to better prevent ransomware

Back up and take snapshots of your data

You never want to be the victim of a ransomware attack, but if you are, the best solution is to wipe your data and systems and restore to a good backup. Setup incremental, complete, and snapshot image backups of all your systems and information. There must be a "gap" between your live and backup systems so that any ransomware infection is not copied over to your backup data.

Create a Disaster Recovery and Business Continuity Plan

Just backing up your data is not enough. Write a disaster recovery and business continuity plan that formalizes the process you will follow after identifying an attack. It should guide you through how you will protect your backups, wipe your systems, and reinstall them, all while minimizing the impact on your business and employees. Once you have a plan in place, test it on a regular basis to ensure readiness.

Use a proven, robust security suite

The right security suite will detect and prevent the majority of ransomware attacks. In addition to standard antivirus and firewall measures, implement intrusion detection, vulnerability assessment, runtime malware identification, proper authentication, and software that uses industry-standard best practices. TrueSight Vulnerability Management will scan, report on, track, and fix vulnerabilities across all your IT environments: data centers, hosted, local, public, private, and hybrid clouds.

Train employees to identify suspicious links, software, and other issues

Phishing and social engineering are the two main ways that ransomware gets into your organization's systems. Both exploit the most vulnerable part of your IT defenses: your employees. Train them to recognize potential security threats and provide policies and processes for how to deal with anything suspicious.

Frequently patch software vulnerabilities and update systems

Ransomware often takes advantage of newly-identified or known vulnerabilities. Patch all systems and software as soon possible. Maintenance and software updates should be applied quickly after they're released and tested.

Identify and Resolve Exploits with BMC

TrueSight Vulnerability Management helps security and IT operations teams prioritize and remediate risks based on potential impact to the business.

- Powerful dashboards show vulnerability data, performance trends, and SLA compliance for simple prioritization of remediation tasks
- Streamlined workflows match vulnerability scan information with remediation tasks
- Blind spot awareness allows you to discover areas of your infrastructure which aren't being monitored
- Rapid import lets you quickly consume vulnerability scanning reports
- Data export helps create custom reports to help satisfy audit requirements and enhance process improvements

Learn more about TrueSight Vulnerability Management now.