CHECK POINT™

YOU DESERVE THE BEST SECURITY

RANSOMWARE-AS-A-SERVICE:
EXPOSING THE UNDERGROUND ECONOMY AND HOW TO PROTECT YOURSELF

Smart hackers pay other hackers to do their dirty work.

That's exactly what happened when the Colonial Pipeline ransomware attack made headlines across the world — an attack that compromised critical pipeline operations, cutting almost half of the entire fuel supply consumed on the East Coast of the US.

Who was responsible? No, it wasn't a mysterious group of mastermind hackers. Instead, affiliates of DarkSide, a Ransomware-as-a-Service (RaaS) network, were ultimately responsible for perpetrating the attack.

> In the past couple years, nearly 60% of ransomware attacks were perpetrated by RaaS groups.

The growth of the RaaS model illustrates a shocking trend: the availability of cheap and ready-to-use attack tools has vastly lowered the barrier to entry for cyber criminals to launch devastating attacks.

With more threat actors in play, companies are becoming more frequent targets of cyber attacks.

Thus, it's critical for your organization to have a solid anti-ransomware strategy in place. But first, let's delve into how the RaaS model works, which is largely responsible for the recent rise in ransomware attacks.

The Ransomware-as-a-Service (RaaS) model explained

What is Ransomware-as-a-Service (RaaS)?

Here is how Microsoft describes the RaaS model: "In the same way our traditional economy has shifted toward gig workers for efficiency, criminals are learning that there's less work and less risk involved by renting or selling their tools for a portion of the profits than performing the attacks themselves. This industrialization of the cybercrime economy has made it easier for attackers to use ready-made penetration testing and other tools to perform their attacks."

In the past, each ransomware campaign had a tight relationship between the initial development of threat tools and launching of the attack. However, it's not efficient to do everything in-house. Then came along the RaaS affiliate model.

By bringing in cyber criminals as affiliates, hackers didn't have to have technical expertise to deploy or launch ransomware payloads. And ransomware developers could focus most of their energy on research and development. Ransomware has effectively become a gig economy.

In the RaaS model, there are two main players: the operator and the affiliate.

The RaaS operators are responsible for the technical backbone of the ransomware operations, which includes the developers that produce the software code and payment portals for communicating with victims. Operators provide leak sites that host portions of data extracted from the breached victims, allowing threat actors to prove that the breach is real in order to facilitate a payment. RaaS programs also provide a whole suite of extortion support, ransom notes, ransom key negotiation, and crypto transaction services.

The affiliate, who is responsible for launching the attack, purchases the ransomware software and the decryptor from the operator.

However, there's a third player in the ransomware ecosystem: access brokers. These individuals sell access to systems to other threat actors. Access brokers can infect systems with malware and sell them as a "load." Those who purchase a load can then install ransomware or other malware of their own. Brokers also compromise Remote Desktop Protocol (RDP) systems and sell access to them for a profit. Ads on the darknet often promote the sale of access into a system that has a highly privileged account such as a Domain Administrator and isn't managed by endpoint detection and response (EDR).

Figure 1. What the RaaS affiliate model looks like.[1]

In many ransomware attacks, affiliates choose to purchase access of compromised systems via an access broker—bypassing the need to compromise the system themselves. This allows affiliates to easily categorize offerings from access brokers and target industries that have high monetization potential.

To motivate their victims to pay, ransomware attackers rely on double-extortion techniques. In this method, hackers not only disables access to critical systems but also threaten to leak the data if the ransom isn't paid. Thus, relying on backups as the main defense against ransomware isn't enough. You must introduce comprehensive security to prevent a network from ever getting breached in the first place.

1 "Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself." Microsoft, 2022, https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/

The most common security weaknesses

According to Microsoft, the most common security weaknesses that allow hackers to breach and then steal valuable data are poor credential hygiene, legacy configurations and misconfigurations.

Many of the techniques used in RaaS campaigns haven't changed much from ransomware campaigns of the past.

Reports show that threat actors commonly exploit security misconfigurations to execute a successful breach.

Therefore, it would be wise to implement critical security protocols that prevent these attacks from having a wider impact on your network. If hackers can't access highly privileged accounts, then they can't spread ransomware widely, move laterally, exfiltrate data, or impact security settings.

According to AV-Comparatives, Harmony Endpoint can detect and respond to privilege escalation tactics—preventing lateral movement and data extraction.

How to stop ransomware in its tracks

When it comes to ransomware, it's wiser to rely on preventative measures rather than treating the aftermath of an attack.

Ransomware attacks frequently begin at the endpoint. Therefore, it's imperative that you have a robust endpoint protection, detection, and response solution in place.

If you're interested in an endpoint security solution, here are the most important features it must have:

- **Runtime protection across endpoints—even in offline mode.** The solution ensures on-device runtime protection against ransomware attacks, while ensuring automated recovery and safe restoration of ransomware-encrypted files.
- **Behavioral detection** that collects indicators from endpoint devices and correlates them with behavioral heuristics, rules, and machine learning models.
- **Automatic quarantining of infected machines.** This will prevent the attack from spreading via lateral movement across the rest of the corporate network.
- **Automatic remediation** and sterilization of the entire cyber kill chain, so you can restore the device to the last clean point.
- **Recovery of ransomware-encrypted files.** It must automatically sterilize and provides fully recovered even to ransomware-encrypted files.
- **Ensured full visibility into the actions taken with auto-generated forensics report.** The report also gives the ability to initiate proactive threat hunting. Forensics data supplies hunt leads to enable security professionals to query the historical data and uncover attack residue across the environment.
- **AI-driven Protection.** To address emerging and zero-day threats, your solution needs to be enriched with all kinds of AI and traditional engines, facilitating the real-time data analysis.

What anti-ransomware solution should your business implement?

Harmony Endpoint includes all of the features listed on the previous page. The latest MITRE ATT&CK® Evaluations results also confirmed that Harmony Endpoint has the highest level of detection accuracy and contextualized visibility into real-world cyber threats, all while providing autonomous detection and response capabilities.

The statistics below highlight Harmony Endpoint's most powerful benefits:

- Check Point Harmony Endpoint proved its ability to provide **full context and end-to-end threat visibility** to detect threats and act quickly, reducing the attack surface.
- Check Point Harmony Endpoint successfully **detected 100% of the unique techniques** used during the test.
- For 96% (44 out of 46) of the unique techniques, Check Point Harmony Endpoint had the **highest technique detection level**.
- **All in all, Harmony Endpoint had top-tier performance across multiple data points, including telemetry and analytic coverage**.

Click here for more information on how Harmony Endpoint can safeguard your business from ransomware attacks.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com