CYBERSECURITY 101 · eBuilder Security

Ransomware as a Service

Ransomware is now a rental business. Criminals lease ready-made ransomware, break in and split the profits. Here is how the model works and how to blunt it.

WHAT IT IS

Ransomware as a service (RaaS) is a criminal business model. Developers build and run the ransomware, the payment portals and the leak sites, then rent the kit to affiliates who break into organisations and deploy it. The two sides split the ransom. The model removed the skill barrier, which is why ransomware attacks now come from far more criminals and hit organisations of every size.

WHY IT MATTERS

About 20%

The cut LockBit's operator kept from each ransom, leaving the rest to the affiliate

US DOJ, 2024

$500M+

Extorted by LockBit from more than 2,500 victims before it was disrupted

US DOJ, 2024

Most pervasive

Ransomware was again the top threat to US critical infrastructure in 2024

FBI IC3, 2024

WHAT HAPPENED

In January 2024 the Akira RaaS group encrypted part of a Tietoevry data centre in Sweden. The attack took down the Primula payroll platform used by more than 30 government agencies and most Swedish universities, along with retailers and a cinema chain. Tietoevry isolated the affected system to contain it. Source: Tietoevry, 2024.

RED FLAGS TO WATCH FOR

Early signs an affiliate may already be inside your network.

- Logins from unusual locations or at odd hours, or repeated failed multi-factor prompts
- Security tools, logging or backups being disabled or altered
- New admin accounts or unexpected privilege changes
- Large or unusual volumes of data leaving the network
- Mass file renaming or encryption starting on a handful of machines

THE ONE RULE THAT STOPS IT

Require multi-factor authentication on every remote-access, email and admin account, so a single stolen password is never enough to get in.

THEN BUILD THE HABIT AROUND IT

- Patch internet-facing systems fast, especially VPNs and remote-access gateways

- Keep offline, immutable backups and test that you can restore from them
- Segment the network and apply least privilege to limit lateral movement
- Run continuous detection so an intrusion is caught before encryption
- Rehearse an incident-response plan, including who to call and how to report

MYTHS AND FACTS

MYTH

If we have backups, ransomware cannot hurt us.

FACT

Double extortion means attackers also steal your data and threaten to publish it, so backups do not remove the leak threat.

MYTH

Paying is the fastest way to recover.

FACT

Payment is strongly discouraged, can breach sanctions and never guarantees a working decryptor or that stolen data is deleted.

MYTH

Taking down one group ends the threat.

FACT

After Operation Cronos disrupted LockBit in 2024, affiliates moved to other programs. The ecosystem reconstitutes.

THE LEGAL DUTY

In Sweden a significant ransomware incident must be reported under Cybersäkerhetslagen (NIS2) to CERT-SE at the National Cyber Security Centre (NCSC), part of FRA since 1 July 2026, with a 24-hour early warning, a 72-hour notification and a final report within one month. If personal data is exposed, GDPR Article 33 adds a 72-hour notification to the data protection authority IMY.

GET HELP

Talk to a Sweden-based analyst about ransomware readiness and your NIS2 reporting duties.

Read the Full Article →