

RANSOMWARE.

Malware that **encrypts data and holds it hostage** for payment. Modern campaigns steal data before they encrypt it — turning a single intrusion into extortion, business disruption, and reputational damage.

- MITRE ATT&CK
- DOUBLE EXTORTION
- RAAS
- CISA #STOPRANSOMWARE

01 THE MECHANISM

Initial access & foothold
Attackers land through **phishing, exposed RDP/VPN, purchased credentials**, or an unpatched public-facing vulnerability. A single foothold is enough to begin the intrusion.

Lateral movement & staging
Once inside, actors **escalate privileges, map the network, and disable backups, shadow copies, and EDR agents** before deploying anything destructive.

Encryption & extortion
Files across endpoints and servers are encrypted with **hybrid AES/RSA cryptography**. A ransom note demands cryptocurrency payment, often with a leak-site countdown.

02 THE FLOW

The Intrusion DAYS TO WEEKS BEFORE DETONATION

1

Initial access via phishing, credential stuffing, or a **foothold purchased from an initial access broker**.

2

The attacker escalates privileges, **disables logging and backups**, and moves laterally across the domain.

3

Sensitive data is quietly **exfiltrated to attacker-controlled infrastructure** before a single file is touched.

The Detonation MINUTES, ACROSS THE ENVIRONMENT

1

The ransomware binary deploys simultaneously across endpoints and servers, **encrypting files with a hybrid AES/RSA scheme**.

2

A ransom note appears on every machine, demanding **cryptocurrency payment against a countdown**.

3

Double extortion: non-payment triggers publication of the stolen data on a dark-web leak site.

03 COMMON ENTRY VECTORS

VECTOR	WHY IT WORKS
Phishing email	Exploits human trust in a message or attachment, bypassing perimeter controls entirely.
Exposed RDP / VPN	Directly reachable from the internet and routinely brute-forced or credential-stuffed.
Unpatched public vulnerability	Known CVEs are weaponized into working exploits within days of disclosure.
Purchased access (IAB)	Turnkey footholds are bought and sold ready-made on criminal marketplaces.
Compromised software supply chain	Malicious code inherits the trust users already place in a legitimate vendor update.

04 HOW OPERATING MODELS COMPARE

MODEL	DATA STOLEN	PAYMENT PRESSURE	TYPICAL TARGET
Encryption-only	No	Ransom for a decryption key	Opportunistic, low-value
Double extortion	Yes	Ransom + leak-site threat	Mid-to-large enterprises
Triple extortion	Yes	Ransom + leak + DDoS / customer contact	High-value, high-profile
Ransomware-as-a-Service	Varies	Affiliate revenue share	Any sector, at scale

RANSOMWARE.

OPERATE · GOVERN · COMMUNICATE

05

RECOVERY & RESPONSE

Containment first.

Isolate affected segments immediately — network isolation outranks investigation speed in the first hour.

Immutable backups are the recovery path.

Follow a 3-2-1-1-0 strategy with at least one copy offline or immutable, unreachable by domain credentials.

Don't trust decryptors blindly.

Test free tools from vetted sources like No More Ransom against a known family before running them at scale.

Eradicate before you restore.

Rotate all credentials and rebuild from known-good images to confirm attacker access is fully removed first.

06

CONTROL MAPPING

NIST CSF 2.0

Maps resilience across **Identify, Protect, Detect, Respond, and Recover**, with Recover formalized as a first-class function.

CISA #STOPRANSOMWARE

Cross-sector baseline of prevention, detection, and response practices maintained with the **FBI and MS-ISAC**.

MITRE ATT&CK

Frames activity as chained techniques, e.g. **T1486** Data Encrypted for Impact and **T1490** Inhibit System Recovery.

PCI DSS V4.0 / SOC 2

Ties directly to **backup integrity, incident response planning**, and access-control requirements auditors already test.

07

WHAT CONTROLS DO NOT SOLVE

Zero-day exploitation

Unknown vulnerabilities bypass patch-based defenses entirely. **Assume compromise**, not just prevention.

Insider & credential abuse

Legitimate, authorized access can still detonate ransomware. **MFA doesn't stop a trusted account gone rogue**.

Backup targeting

Affiliates actively hunt for and delete backups first. **Only isolated, immutable copies survive**.

Reputational fallout

Recovery restores systems, not customer trust or **breach-notification obligations** already triggered.

08

MYTHS VS. REALITY

MYTH	REALITY
"Paying the ransom guarantees you get your data back."	There is no enforcement behind a criminal promise — a meaningful share of payers never get a working decryptor, and payment itself can carry sanctions exposure.
MYTH	REALITY
"Antivirus alone will stop ransomware."	Affiliates use living-off-the-land techniques and disable endpoint tools before detonation. Defense requires layered detection and response.
MYTH	REALITY
"Having backups guarantees recovery."	Attackers actively search for and destroy backups before encrypting. Only offline or immutable copies reliably survive.
MYTH	REALITY
"Small organizations aren't worth targeting."	RaaS affiliates automate targeting at scale . Small and mid-sized organizations make up a majority of reported victims.
MYTH	REALITY
"It's purely an IT problem."	A ransomware event is a business continuity crisis requiring legal, communications, and executive leadership from the first hour.

09

SPEAK THE THREAT — KEY TERMS

RAAS

Ransomware-as-a-Service — developers **lease ransomware tooling** to affiliates for a share of the profits.

DOUBLE EXTORTION

Combining encryption with a **threat to publish stolen data** if the ransom is not paid.

INITIAL ACCESS BROKER

A criminal seller of **already-compromised footholds** into a target network.

LEAK SITE

A dark-web page operators use to **publish or auction stolen data** as pressure.

LIVING OFF THE LAND

Using an environment's **own admin tools** to operate while evading detection.

IMMUTABLE BACKUP

A backup that **cannot be altered or deleted**, even with compromised admin credentials.