THREATDOWN™

Ransomware Prevention Guide

Ransomware never sleeps

Introduction

Between July 2024 and June 2025, the number of known ransomware attacks increased 25%, 42 countries experienced their first ever ransomware event[1], and the average ransom payment exceeded $1 million for the first time.[2]

Ransomware gangs also continued to evolve their tactics, with ever more emphasis on speed and stealth. Attackers routinely use Living Off the Land (LOTL) techniques to stay hidden, and exploit blind spots, such as unprotected computers, to stage attacks. To ensure the slowest possible response to security alerts from IT and security staff, ransomware groups are active at night, over weekends, and during holidays.

Threat actors know that the best time to move laterally, perform reconnaissance, steal data and encrypt files is when offices are closed, staff are dispersed, and nobody is watching security consoles.

To stay secure, businesses must patch early and often, eradicate blind spots, and be as watchful at 1 AM on a Saturday as they are at 1 PM on a Monday.

Thankfully, forethought and preparation go a long way, so ThreatDown has compiled a six-point checklist for organizations that want to protect against ransomware no matter when an attack comes.

Anatomy of a Ransomware Attack

Ransomware does not target individual computers—it targets entire organizations. The aim of a ransomware attack is to stop the target organization from being able to function.

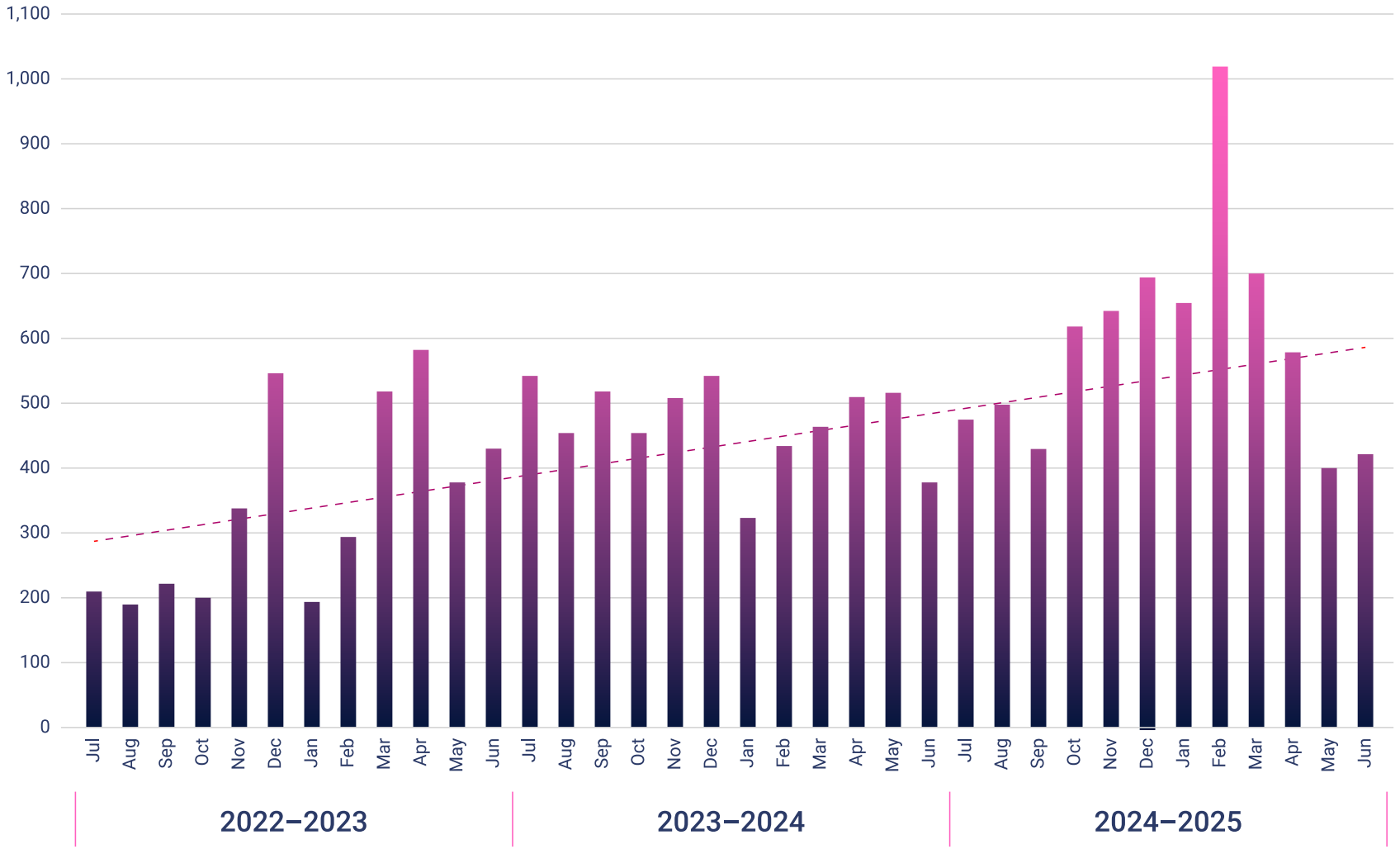
In a typical attack, threat actors will break into a company network, establish backdoors, make themselves domain administrators, explore the network, steal important company data, and use encryption to make files unusable. This approach allows them to demand payment for a decryption key or for not leaking or selling the stolen data.

Ransomware gangs hide their activity by using legitimate software, system administration tools, hijacked accounts, and unprotected computers. Although some attacks only last a few hours, threat actors can sometimes work quietly inside a network for days or even weeks.

[1] ThreatDown (2025), 2025 State of Ransomware, https://www.threatdown.com/dl-state-of-ransomware-2025/
[2] Coveware (2025), Targeted social engineering is en vogue as ransom payment sizes increase, https://www.coveware.com/blog/2025/7/21/targeted-social-engineering-is-en-vogue-as-ransom-payment-sizes-increase

THREATDOWN™

Known Ransomware Attacks per Month



THREATDOWN™

How Ransomware Stays Hidden

Ransomware gangs have made themselves harder to detect using four tactics.

Working at night

Ransomware gangs work at night, on weekends, and during holidays, when IT staff are least likely to be watching security consoles. This gives attackers time to work, even if their actions trigger endpoint detection and response (EDR) alerts for suspicious activity.

Living Off the Land

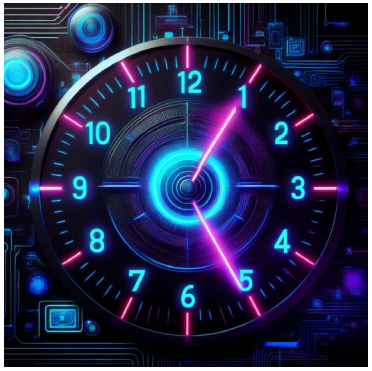
Attackers routinely use legitimate software and administration tools instead of malware, a technique known as Living Off the Land. This makes cyber-defense a matter of investigating suspicious behavior instead of detecting malicious software.

Staging From Blind Spots

After breaking into a network, attackers will try to identify computers that do not have security protection installed. These blind spots allow criminals to prepare and stage attacks, away from EDR sensors and countermeasures.

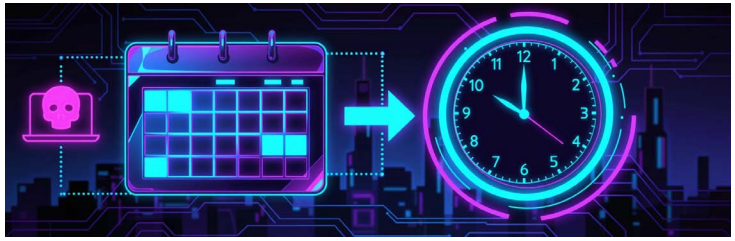
Faster attacks

The time that ransomware gangs are active on a target network is decreasing. Multi-stage attacks that include initial access, privilege escalation, lateral movement, data exfiltration and encryption can now be completed in hours instead of days or weeks.



Most ransomware attacks happen between 1 AM and 5 AM.

What used to take weeks...



...now only takes hours.

Ransomware gangs hide their activity by using admin tools.

THREATDOWN™

Six-point Checklist

Prevention

- ☐ **Patch early, patch often.** In the past 12 months, ransomware gangs have made extensive use of software vulnerabilities in firewalls to penetrate networks. Organizations should prioritize actively exploited and critical vulnerabilities, and ensure that internet-facing systems are patched with security updates on a regular, scheduled basis.
- ☐ **Monitor EDR 24x7.** Ransomware groups know that they are likely to trigger EDR alerts as they prepare an attack, so they work at night when alerts may not be noticed. Organizations should ensure their EDR is monitored 24x7, using in-house security staff, a managed service provider (MSP), or a service like ThreatDown's Managed Detection and Response.
- ☐ **Remove blind spots.** Attackers will seek out blind spots on a network, such as devices that do not have EDR installed, or devices where the EDR has overly permissive exclusions. Organizations should shut down "shadow IT" devices, ensure that all servers and endpoints are protected by EDR, and audit their security policies regularly to eliminate unnecessary exclusions.

Mitigation

- ☐ **Test backups.** Ransomware gangs know that an organization's last line of defense against encrypting ransomware is its backups, so attackers will try to delete them. Organizations should maintain offline backups that can't be reached if the network is compromised and test backups regularly by attempting to restore critical systems from them.
- ☐ **Assign roles and access.** Staff are often unavailable or hard to reach over weekends and holidays, when attacks are likely to occur. Organizations should maintain a contact list of names, phone numbers and roles that can still be accessed if its computer systems are compromised, and ensure that people providing cover for others have the documentation and access they need.
- ☐ **Make a disaster recovery plan.** A well-practiced disaster recovery plan can be the difference between hours of disruption and weeks of downtime. Organizations should document step-by-step procedures for responding to an attack, rehearse them through tabletop exercises, and ensure the plan is accessible even if critical systems are unavailable.

Managed Detection & Response

The best of both technology innovations and human experience

- 24x7x365 threat monitoring by ThreatDown security experts.
- Proactive threat hunting to limit future threats and exposure.
- Rapid response to expedite recovery and reduce downtime.

Get a quote

THREATDOWN™ | threatdown.com | sales@threatdown.com