eBook

ThreatDown™
Powered by Malwarebytes

2025 Ransomware Prevention Guide

Because ransomware never takes a day off

Introduction

For ransomware gangs, there's no better time to steal a company's data and encrypt its computers than when its offices are closed, the staff are dispersed, and nobody's watching the security consoles. And while many organizations respond to these threats with improved security just before major holidays, the risk of a ransomware attack doesn't magically disappear once staff have returned.

Ransomware gangs like to work at night, at weekends, or during holidays—whenever security alerts are likely to go unnoticed or staff will be slower to respond.

The only viable option for businesses is to be as watchful at 1 AM on a Saturday as they are at 1 PM on a Monday.

Since 2022, ransomware attacks have escalated significantly, with the number of known attacks increasing 64% between September 2022 and September 2024.

At the same time, the average ransom payment climbed to $650,000[1] in 2023. And there is no exemption for small businesses, with 30% of attacks impacting organizations with 100 employees or less[2].

Ransomware gangs also evolved their tactics so that their attacks became faster and stealthier, making early detection even more difficult.

Anatomy of a Ransomware Attack

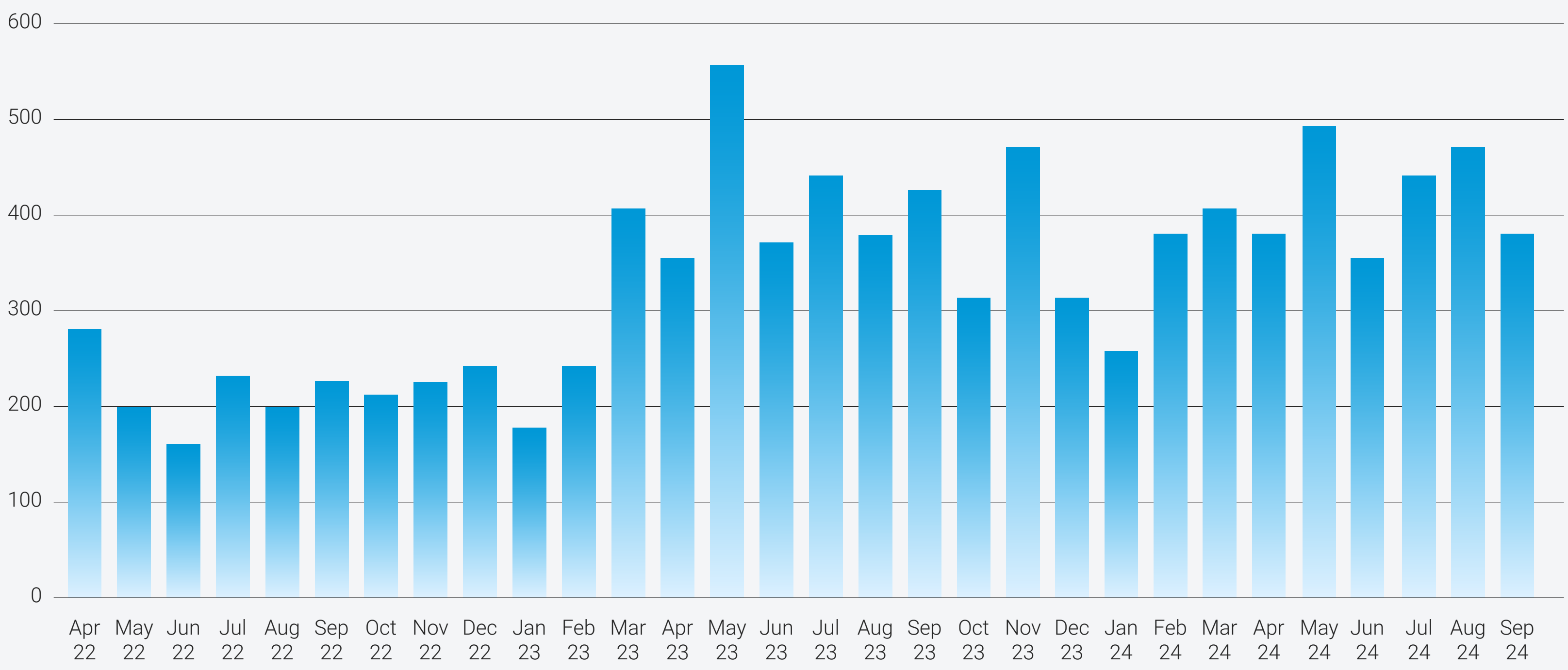
Ransomware attacks are designed to stop your business operating so you feel you have no choice but to pay an exorbitant ransom. Typically, attackers will try to steal important company data, and run malware that encrypts your computers, making them unusable. They then demand payment for a decryption key, and for not selling your data.

Ransomware gangs hide their activity by using standard computer administration tools and hijacked administrator accounts and may be working quietly inside your network for days or even weeks. Data encryption is carried out when you're least able to respond: At night, over a weekend, or during the holidays.

[1] Coveware, "Ransom Monetization Rates Fall to Record Low Despite Jump In Average Ransom Payments", 2023, https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

[2] Ibid

Known Ransomware Attacks per Month, April 2022-September 2024



How Ransomware Stays Hidden

Ransomware gangs have made themselves harder to detect with three tactics.

Nighttime attacks

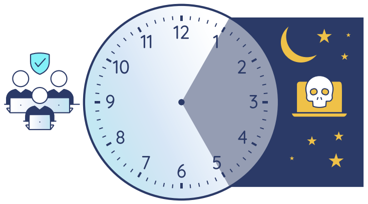
In the past year, ransomware gangs have become more reliant on attacking companies on weekends and in the early hours of the morning—when IT staff are least likely to be watching. Most of the ransomware attacks handled by the ThreatDown MRS team in the last 12 months have occurred between 1 AM and 5 AM.

Faster attacks

Ransomware gangs are taking less and less time to encrypt and steal data. The time taken for the entire ransomware attack chain—from initial access to lateral movement, to data exfiltration and then encryption—has decreased from weeks to hours, according to ThreatDown Incident Response (IR) data.

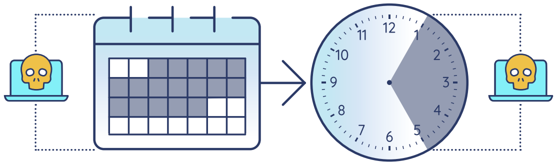
Stealthier attacks

Ransomware gangs are increasingly using Living off the Land (LOTL) techniques in their attacks, using legitimate software and administration tools that don't look out of place on their targets' networks instead of malware. Most of the modern ransomware attack chain is now composed of LOTL techniques.



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.

Six-point Checklist

□ **Make a contact list.** If ransomware strikes, you'll need all hands on deck, and you'll have better things to do than wasting time trying to remember people's names and numbers. Make an up-to-date list of names and contact numbers and share it in a way that won't fail if your network is struck with ransomware.

□ **Assign roles and access.** People can be made unavailable at any moment for vacations, illnesses, family emergencies, and more. Make a note of who does what and when they can be reached (add it to your contact list). If critical IT or security positions will be vacant for a scheduled amount of time, make sure those positions are covered by at least one other person, and that the people providing cover have the knowledge, documentation, access, and equipment they need.

□ **Turn off what you can.** The most secure configuration for a computer is "off". The fewer computers that are on, and the less software you have running, the harder it will be for ransomware gangs to break into your organization, to move around inside it, or to find your critical data.

□ **Install security updates.** Patching is arguably the single most impactful security task you can do. On a regular, scheduled basis, make sure the software in your environment has had all the latest security updates. If you can't get to everything in the first attempt, prioritize Internet-facing software and actively exploited vulnerabilities.

□ **Test your backups.** Your last line of defense against encrypting ransomware is your backups, but backups are only useful if they work. Ransomware gangs will try to delete them, so make sure you have an offline backup of your data that can't be reached from your network and test it's working by trying to restore critical data from it.

□ **Watch your alerts.** A lot of cybercriminals are noisy enough to trigger security alerts as they build up to their attack, but they get away with it because the alerts go unnoticed by staff busy with other things. Make sure your alerts are working and assign somebody to look at them regularly. Better yet, use a Managed Detection and Response service, like ThreatDown MDR, for 24 x 7 x 365 threat monitoring.

Managed Detection & Response

The best of both technology innovations and human experience

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

ThreatDown™
Powered by Malwarebytes

Copyright © 2024, Malwarebytes. All rights reserved. Malwarebytes, the Malwarebytes logo, ThreatDown, and the ThreatDown logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind. 12/24