February 2026

Threat report

The Managed XDR Global Threat Report

How attackers target organizations and security gaps

Barracuda®
Your business, secured.

Contents

Introduction

Barracuda Managed XDR's advanced tools and experts monitor and protect customer networks 24 hours a day, 365 days a year. Every minute, the solution detects and responds to a security warning. Every 15 minutes, it sends an alert to a customer, and every 60 minutes, it automatically blocks a high-severity threat such as a compromised device or an unfolding ransomware incident.

If left unresolved, a single red flag can quickly escalate into a widespread incident that disrupts operations, reduces productivity, compromises sensitive data, and damages financial stability and brand reputation. No organization is immune; attackers target businesses of every size, across all industries and geographies.

What makes targets vulnerable can be many things — security gaps, rogue devices, unpatched systems, oversights, misconfigurations — and a lack of time and resources to spot the intrusion, remove the attackers and lock the door firmly behind them.

The purpose of this report is to help IT and security professionals in resource-constrained organizations better understand how attackers target potential victims and the security weak spots they will try to exploit. We provide examples of real-world incidents and recommendations on how to stay safe and cyber resilient.

In a world of increasingly complex and evasive cyberthreats, organizations are not facing the challenge alone. Your security provider has the tools and insight to help you address the issues identified in this report — and we are with you every step of the way.

The underpinning data

The findings detailed in this report are based on Barracuda Managed XDR's unique dataset of more than two trillion IT events collected during 2025, nearly 600,000 security alerts and more than 300,000 protected endpoints, firewalls, servers, cloud assets, and more. Around 53,000 high-severity threats were triaged by Barracuda Managed XDR's security orchestration and automated response (SOAR) platform.

Key findings

100%

of security incidents involved at least one unprotected or rogue endpoint

96%

of incidents involving lateral movement ended with the release of ransomware

66%

of incidents involved the supply chain or a third party (up from 45% in 2024)

3 hours

the fastest ransomware attack, from breach to encryption

90%

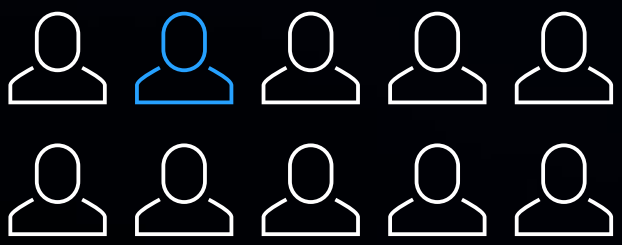
of ransomware incidents exploited firewalls

13 years

the most detected vulnerability is a 2013 bug in obsolete encryption

1 in 10

detected vulnerabilities have a known exploit



How attackers target organizations

Effective extended detection and response (XDR) solutions are designed to intercept inbound threats at the earliest stage of the attack chain — the point of initial compromise and access. Barracuda Managed XDR is no exception. It also provides additional visibility across later attack phases, including lateral movement and impact. This broad capability is reflected in the content of this report.

Leading the list of the most detected threats against organizations in the last 12 months are attacks targeting identities and identity security.

This includes unusual or unexpected logins to a user account. These are connections that do not correspond to the user's typical behavior pattern in terms of device, location or time. Such detections are a strong indicator of credential theft and account compromise. Other red flags are attempts to connect from a blocked geolocation and the 'impossible travel' rule, where a user logs in from a second location they could never have reached in the time between logins.

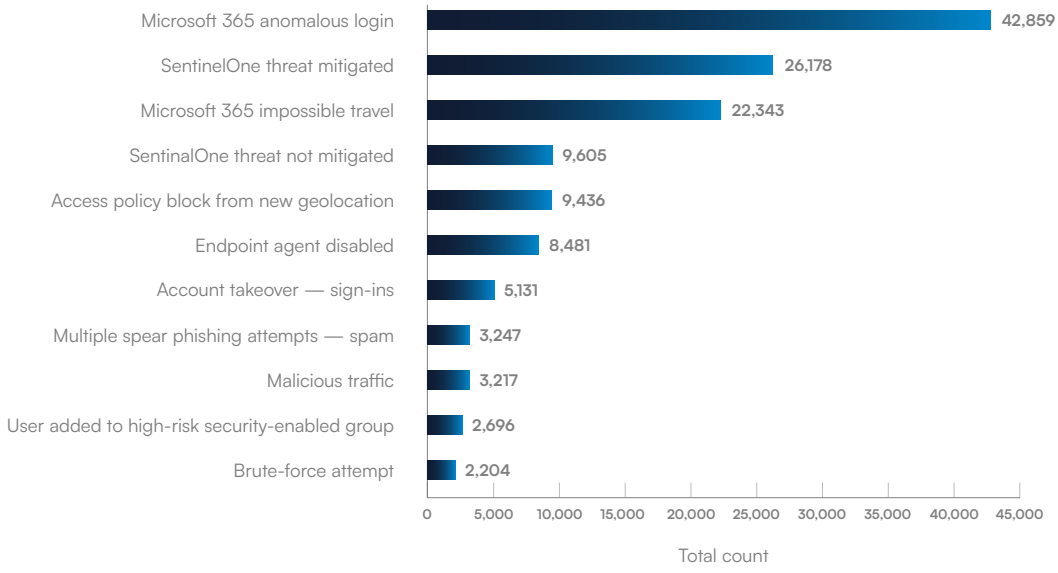


FIGURE 1

Top attack detections against organizations

The list of top detections also includes activities that could mean an account has been compromised and the attackers are in the network. Security teams need to investigate such detections immediately. They include signs that suggest someone has tried to bypass or disable endpoint protection and notifications that a user has been added to a security-sensitive group, which could be an attacker trying to escalate their privileges.

How attackers tamper with privilege rights once inside the system

Privilege escalation is crucial for attackers because it turns limited access into full administrative control, enabling them to disable defenses, move laterally across systems and access sensitive data. The result can be large-scale compromise and the release of ransomware.

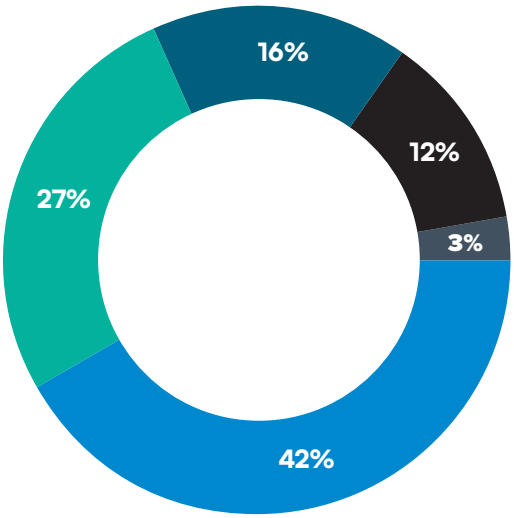


FIGURE 2

How attackers tamper with privilege rights

- Windows — Added a user to a group with high-risk security rights
- Windows — Removed a user from a group with high-risk security rights
- Microsoft 365 — Added a user as a global administrator
- Microsoft 365 — Removed a user as a global administrator
- FortiGate Firewall — Added a user as an administrator

Barracuda Managed XDR's firewall, Windows and Microsoft 365 security tools detected the following behaviors that point to attempted privilege escalation:

Windows — added a user to a group with high-risk security rights (accounting for 42% of suspicious privilege escalations)

- **What this means:** A user was added to a group with powerful permissions (e.g., domain administrators).
- **Attackers can use it to:** Move laterally, deploy malware or exfiltrate data.
- **How to stay safe:** Monitor group changes and manage the allocation of all privileged access rights.

Windows — removed a user from a group with high-risk security rights (27%)

- **What this means:** A user was taken out of a high-privilege group.
- **Attackers can use it to:** Cover their tracks after privilege escalation.
- **How to stay safe:** Investigate why removal occurred and check for any misuse that took place before removal.

Microsoft 365 — added a user as a global administrator (16%)

- **What this means:** Someone was given the highest level of access in Microsoft 365.
- **Attackers can use it to:** Create new accounts, steal data or disable security.
- **How to stay safe:** Review administrator role changes, enforce multifactor authentication (MFA) and introduce proper review and approval processes.

Microsoft 365 — removed a user as a global administrator (12%)

- **What this means:** Someone lost their global administrator rights.
- **Attackers can use it to:** Avoid detection by removing their added accounts.
- **How to stay safe:** Check whether the change was authorized, and review audit logs for suspicious activity or misuse.

FortiGate Firewall — added a user as an administrator for the firewall (3%)

- **What this means**: A new administrator account was created on the firewall.
- **Attackers can use it to**: Disable protections and open backdoors.
- **How to stay safe**: Confirm account legitimacy and enforce strong administrator controls.

Incident Report — The malicious attachment that led to a RAT

A remote access Trojan (RAT) was found on a client's systems after an employee inadvertently downloaded a malicious executable file. The file immediately tried to establish persistence: It asked to register as a Windows' service, which would allow it to start automatically, run in the background and operate with system-level access so it could control the system remotely without support. It also tried to install the trusted remote management tool ScreenConnect via PowerShell.

Hiding in plain sight

Adding and removing users from privileged access groups is a legitimate IT activity. Attackers' ability to hide malicious behavior among normal everyday tasks and tools is one of the biggest challenges facing security teams today.

This approach of living off the land (LOTL) is on the rise, with threat actors leveraging legitimate software tools and techniques to evade detection. Fortunately, AI is helping advanced security systems detect subtle anomalies in seemingly benign activity that can be investigated and mitigated.

Incident Report — Akira ransomware turns victim's remote management tool on itself

The attackers gained access to the domain controller (DC) and installed the Datto RMM. Their activity closely mirrored what a backup agent might legitimately do during scheduled jobs, which made everything look like regular IT activity.

A word about remote access and management (RMM) tools

Remote access tools are a growing target for attackers. Successfully compromising an RMM tool gives attackers a significant amount of power while reducing the risk of being detected because RMMs are widely used by organizations.

Over the last 12 months, Barracuda Managed XDR mitigated incidents involving the abuse of, among others, SonicWall SSL-VPN, (a popular virtual private network) ScreenConnect, RDP (the Remote Desktop Protocol), PsExec (a command line tool for running programs and commands on remote computers), AnyDesk, and other firewall VPNs.

To reduce risk, security teams need to deploy detection systems that specifically look for RMM abuse. For example, Barracuda Managed XDR has developed a detection rule that uses telemetry from endpoints to identify requests sent from ScreenConnect to suspicious top-level domains (TLDs).

Red flag combinations

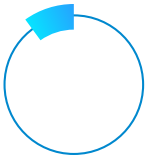
Suspicious activity can also be identified by looking at the bigger picture. An analysis of real-world incidents involving Barracuda Managed XDR in the last 12 months identified the following common combinations of tools/techniques and behaviors:

66%

of cases involving fileless malware used PowerShell as the primary execution method. PowerShell is a platform-agnostic tool used for automating tasks and managing configurations.

44%

of firewall-related incidents involved password-spraying — where attackers try out lots of common passwords against stolen usernames.



10%

of server security breaches involved the clearing of activity logs to cover attackers' tracks.

96%

of cases involving lateral movement resulted in ransomware deployment.

90%

of ransomware incidents exploited firewalls through a CVE (a classified software vulnerability) or vulnerable account.

34%

of incidents involved social engineering that tricked users into downloading potentially malicious files.

For attacks to succeed, attackers need to find and take advantage of gaps in their intended victims' security. Barracuda Managed XDR's detection data and incident insight shines a light on some of the potential weak spots that left targets vulnerable to cyberthreats over the last year.

How organizations leave themselves exposed

Top network security vulnerabilities

Inadequate or outdated encryption methods that don't protect sensitive traffic, as well as the lack of proper validation — or certification — of network activity can be used by attackers to further their attacks.

Barracuda Managed XDR has identified the following network security risks over the last year:

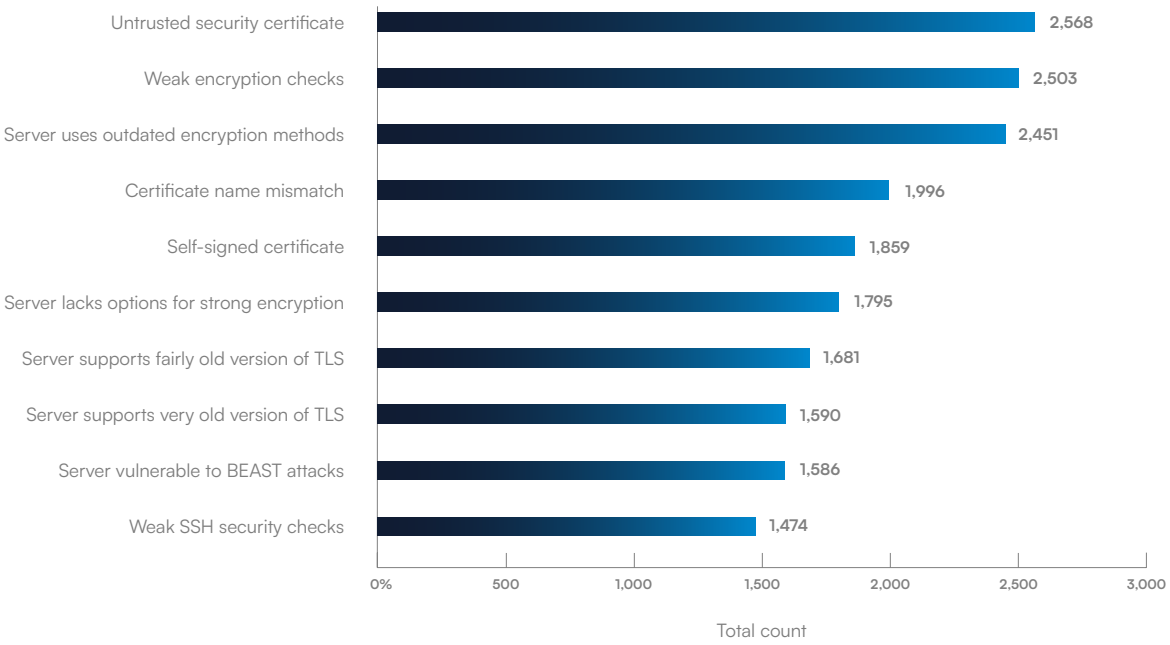


FIGURE 3

Top network security vulnerabilities

Untrusted security certificate

What this means:

The certificate presented by the server is not issued by a trusted Certificate Authority (CA).

Attackers can use it to:

Impersonate a legitimate site using a fake certificate, enabling attackers to insert themselves into legitimate communications to steal data, bypass security, inject malicious content, and more.

How to stay safe:

Use certificates from reputable CAs.

For more technical teams: Implement proper certificate validation and enable 'certificate pinning' (where the application only trusts a specific certificate when connecting to a server). It is also important to check whether an application's certificate has been revoked (using tools such as CRL and OCSP) to avoid trusting compromised certificates. See: OWASP Certificate Validation.

Weak encryption checks

What this means:

The server uses weak algorithms or insufficient key lengths for encryption.

Attackers can use it to:

Brute-force or exploit weaknesses to decrypt sensitive data such as passwords and financial information. Brute-forcing involves trying many different username/password combinations to see if one works.

How to stay safe:

Enforce strong encryption standards such as AES-256, RSA-2048+.

For more technical teams: Disable weak ciphers and regularly audit configurations. Consider implementing elliptic curve cryptography (ECC), such as ECDSA or ECDHE, for better security and performance (See: NIST ECC Recommendations). Use Perfect Forward Secrecy (PFS) cipher suites to protect past sessions if keys are compromised.

Server uses outdated encryption methods

What this means:

The server relies on retired algorithms such as MD5, SHA-1 or RC4.

Attackers can use it to:

Exploit known vulnerabilities to break encryption or forge signatures, leading to data breaches.

How to stay safe:

Upgrade to modern algorithms such as SHA-256 or AES, and follow industry best practices (e.g., the NIST guidelines above).

For more technical teams: Remove support for deprecated algorithms (MD5, SHA-1, RC4) from all configurations. Test with tools like SSL Labs to verify no outdated algorithms are enabled. See: SSL Labs Test.

Certificate name mismatch

What this means:

The domain name does not match the certificate's Common Name (CN) or Subject Alternative Name (SAN).

Attackers can use it to:

Launch interception attacks by redirecting traffic to a malicious server.

How to stay safe:

Ensure certificates match all domains/subdomains in use.

For more technical teams: Use SAN fields for multi-domain certificates. Automate certificate management to avoid mismatches during renewals.

Self-signed certificate

What this means:

The certificate is signed by the same entity that owns it, not a trusted CA.

Attackers can use it to:

Make it easier to impersonate servers since anyone can create self-signed certificates.

How to stay safe:

Use CA-issued certificates for public-facing services and restrict self-signed certificates to internal systems.

For more technical teams: Maintain a private CA for internal use and distribute its root certificate securely. Monitor for unauthorized self-signed certificates on your network.

Server lacks strong encryption options

What this means:

The server does not offer modern, secure cipher suites.

Attackers can use it to:

Force a downgrade to weaker encryption.

How to stay safe:

Configure servers to support strong cipher suites, such as Transport Layer Security (TLS) 1.2/1.3 with AES-GCM.

For more technical teams: Disable support for weak or insecure TLS cipher options such as NULL or EXPORT, so that only strong, encrypted and authenticated connections are allowed. Regularly update server software to support the latest protocols and cipher suites.

Server supports older versions of TLS

What this means:

The version of TLS used is outdated and vulnerable to attacks.

Attackers can use it to:

Exploit protocol weaknesses for interception or downgrade attacks that trick the system into using an older, weaker security protocol.

How to stay safe:

Update the version of TLS used.

For more technical teams: Disable TLS 1.0 and 1.1. Only support TLS 1.2 and 1.3. See: Mozilla TLS Recommendations.

Server supports very old version of TLS

What this means:

The version of TLS in use is obsolete and insecure.

Attackers can use it to:

Exploit known vulnerabilities.

How to stay safe:

Update the version of TLS used.

For more technical teams: Remove SSLv2, SSLv3 and early TLS versions entirely. Use automated tools to scan for legacy protocol support.

Server vulnerable to BEAST attack

What this means:

BEAST (Browser Exploit Against SSL/TLS) attacks target older versions of TLS that have weakness in their block-based encryption.

Attackers can use it to:

Decrypt HTTPS (Hypertext Transfer Protocol Secure — a secure version of the basic web communication protocol) traffic and expose confidential data.

How to stay safe:

Update to the latest version of TLS and use secure cipher suites.

For more technical teams: Consider TLS 1.2+ with AES-GCM or ChaCha20-Poly1305 cipher suites. Disable CBC-mode ciphers on older TLS versions.

Weak SSH security checks

What this means:

The SSH configuration uses weak algorithms or outdated protocols. SSH (Secure Shell) is a secure network protocol used to remotely access and control computers over an unsecured network, such as the internet.

Attackers can use it to:

Brute-force credentials or exploit weak keys to gain unauthorized access.

How to stay safe:

Enforce strong key exchange algorithms, disable weak SSH protocols, use key-based authentication and deploy specialist intrusion-prevention tools that protect servers from brute forcing, such as Fail2Ban or similar.

For more technical teams: Use SSH protocol version 2 only. Enforce minimum key lengths (e.g., RSA 4096, Ed25519). Disable password authentication if possible and use key-based authentication. Restrict SSH access by IP and use firewall rules. Regularly update SSH server software. See: SSH Security Best Practices.

The top detected CVE software vulnerabilities

Out-of-date and unpatched software is a magnet for cyberthreats. According to Barracuda Managed Vulnerability Security, these are the key software vulnerabilities identified in customer networks over the last year:

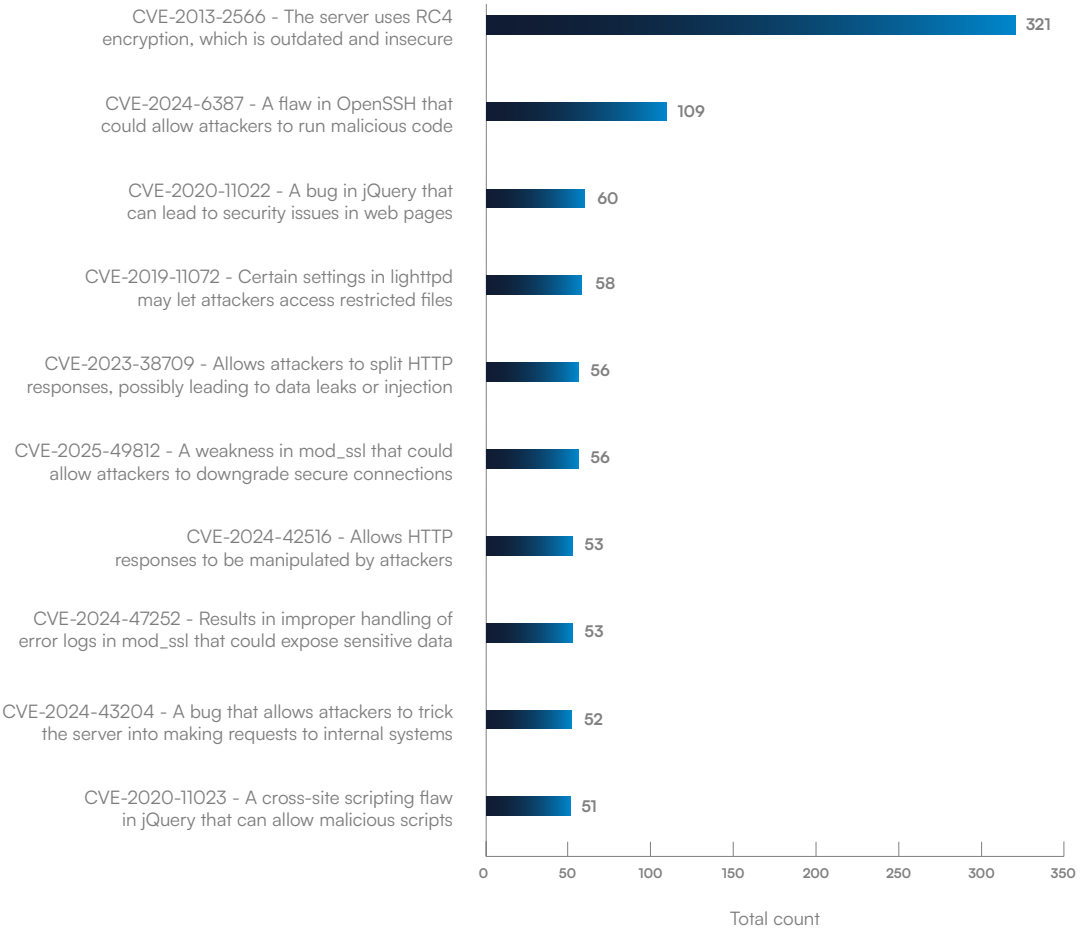


FIGURE 4

Top vulnerabilities with a designated CVE found in organizations

The most widely detected vulnerability is also the oldest. CVE-2013-2566 has been around for almost 13 years and can still be found in legacy systems such as old servers, embedded devices or applications.

These systems can be in active use, but they are often inactive and forgotten. The prevalence of this vulnerability is a stark warning about the risk of dormant exposure. The sooner a vulnerability is patched, the less chance there is of it being overlooked.

Only one CVE on the list has a critical severity rating, but five are designated high severity. The average severity score of all the vulnerabilities detected in the last 12 months was 5.9.

CVE-2013-2566 — The server relies on vulnerable and outdated RC4 encryption

Severity: **MEDIUM**

Attackers can use it to:

Exploit weak encryption to decrypt sensitive data into plain text. RC4 is a type of encryption cipher.

How to stay safe:

Disable RC4 in TLS (see above) configurations and use modern ciphers such as AES, TLS 1.2+.

CVE-2024-6387 — A flaw in OpenSSH that could allow attackers to run malicious code

Severity: **CRITICAL**

Attackers can use it to:

Gain full control of affected systems remotely. SSH is Secure Shell, a protocol used to securely connect to remote systems over an unsecured network like the internet, and OpenSSH is a free, open-source version.

How to stay safe:

Apply the latest OpenSSH patches immediately and restrict SSH access.

CVE-2020-11022 — A bug in jQuery that can lead to security issues in web pages

Severity: **MEDIUM**

Attackers can use it to:

Inject malicious scripts into web pages and steal sessions and data. jQuery is a JavaScript library that makes coding easier for developers.

How to stay safe:

Upgrade to the latest version of jQuery and clean data before your system uses it.

CVE-2019-11072 — Certain settings in the lighttpd web server may let attackers access restricted files

Severity: **HIGH**

Attackers can use it to:

Access restricted files on the server including sensitive configurations or data. A lighttpd server is an open-source web server designed for speed-critical environments.

How to stay safe:

Update the lighttpd web server to the latest version and make sure any file locations provided by users are checked and cleaned to prevent misuse.

CVE-2023-38709 — Allows attackers to split HTTP responses in vulnerable Apache web servers, possibly leading to data leaks or injection

Severity: **HIGH**

Attackers can use it to:

Add fake instructions to web responses, trick systems into storing harmful data or inject malicious code into web pages, compromising data integrity and user security.

How to stay safe:

Update the Apache web server and ensure all browser-to-server instructions or header data are properly checked and cleaned.

CVE-2025-49812 — A weakness in mod_ssl that could allow attackers to downgrade secure connections

Severity: **HIGH**

Attackers can use it to:

Downgrade the level of encryption or intercept traffic and expose sensitive data. mod_ssl is an Apache HTTP server module that adds support for encryption.

How to stay safe:

Apply the latest Apache patches and enforce strong TLS encryption configurations.

CVE-2024-42516 — A security flaw that lets attackers manipulate HTTP web responses sent to users

Severity: **HIGH**

Attackers can use it to:

Exploit weakness in how a system receives, checks and processes data to inject harmful content or redirects that can lead to phishing, malware delivery or stolen user sessions.

How to stay safe:

Apply vendor patches promptly and enforce strong security headers.

CVE-2024-47252 — Results in improper handling of error logs in mod_ssl that could expose sensitive data

Severity: **MEDIUM**

Attackers can use it to:

Inject malicious content into logs that can poison logs and potentially escalate privileges.

How to stay safe:

Update Apache and restrict log access.

CVE-2024-43204 — A bug that allows attackers to trick the server into making requests to internal systems

Severity: **HIGH**

Attackers can use it to:

Force a server to make requests to internal systems, exposing the internal network.

How to stay safe:

Patch Apache and validate header configurations.

CVE-2020-11023 — A cross-site scripting flaw in jQuery that can allow malicious scripts

Severity: **MEDIUM**

Attackers can use it to:

Inject malicious scripts.

How to stay safe:

Upgrade jQuery, clean user inputs and use tools to block harmful code.

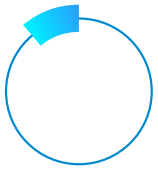
Additional findings from Barracuda Managed Vulnerability Security

4,146

Total number of critical vulnerabilities detected.

2,525

Total number of unique vulnerabilities identified.



11%

Proportion of vulnerabilities that have a known exploit.

Incident Report — Unpatched firewall used in RansomHub attempt

The attackers exploited unpatched vulnerabilities in a Fortinet firewall. They launched brute-force activity against a customer's network but were blocked. A month later, they tried a remote (SSL VPN) login but were blocked again. Two days later, they made a third attempt. Barracuda Managed XDR detected PsExec (remote command) activity and found malicious software on the primary domain controller and backup server.

Misconfiguration: Incidents that involve accidental or intentionally disabled security tools

Security tools that have not been properly configured are a major security risk. The danger can be heightened by the false sense of safety that comes from having the tool installed in the first place. Over the last 12 months, Barracuda Managed XDR identified disabled features that included endpoint protection agents (accounting for 94% of disabled security detections), MFA (3.62%), safe link (1.4%), and safe attachment rules (0.6%).

Studies show that most organizations are trying to manage too many security tools. When resources are stretched, configuration errors can easily creep in. The best protection is an integrated security platform with full visibility over settings and configurations that can quickly and automatically flag gaps that need fixing.

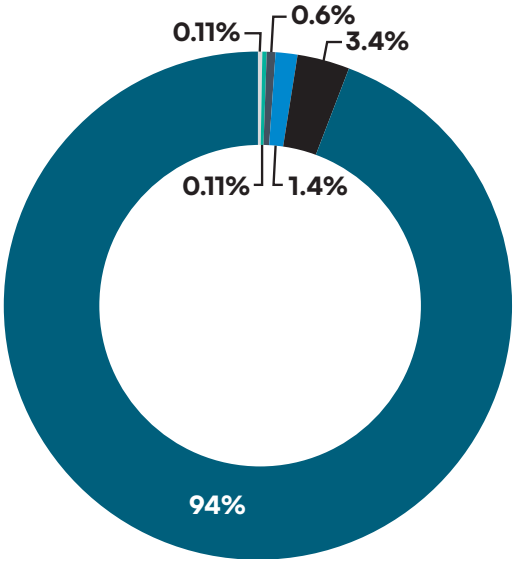


FIGURE 5

Most commonly disabled security features

- SentinelOne Endpoint agent disabled
- Microsoft 365 MFA disabled
- Microsoft 365 ATP 'safe links' rule disabled
- Microsoft Office ATP 'safe attachment' rule disabled
- Microsoft Azure MFA disabled
- Google Workspace MFA disabled

100%

Proportion of incidents that Barracuda Managed XDR responded to that involved at least one unprotected or rogue endpoint

66%

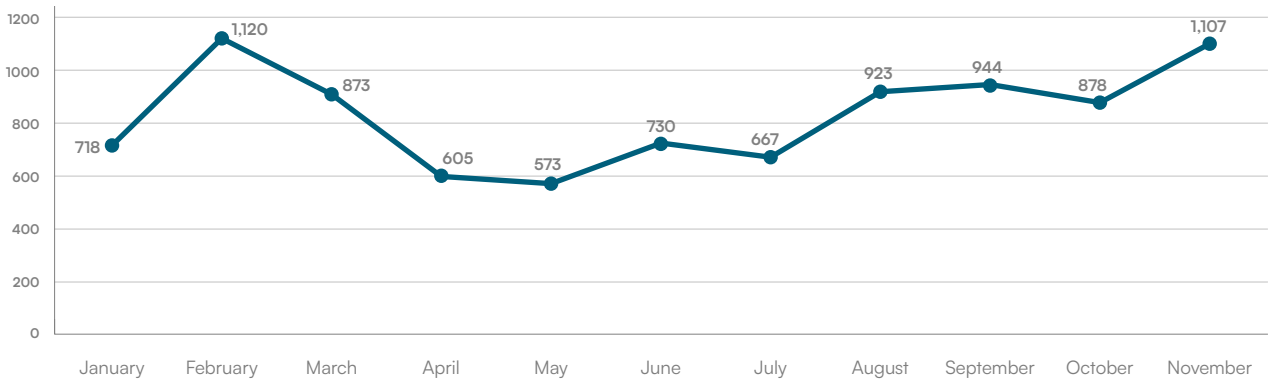
Proportion of incidents that Barracuda Managed XDR responded to that involved the supply chain or a third party (up from 45% in 2024)

The enduring threat of ransomware

Over the last 12 months, Barracuda Managed XDR identified 13,514 indicators that a ransomware attack was in progress, including tools, techniques and behaviors. Unlike previous years, there are no longer any sharp peaks or troughs, but a steady high level of incidents all year round.

FIGURE 6

2025 ransomware-related incidents



1.5% to 5.6%

Proportion of all organizations impacted by ransomware each month in 2024

5.1% to 10.9%

Proportion of all organizations impacted by ransomware each month in 2025

Top ransomware families encountered in 2025

Akira

- Akira is a relatively new ransomware group known for targeting organizations with sophisticated attacks. It often employs double extortion tactics, encrypting data and threatening to release sensitive information unless a ransom is paid.
- **Tactics**: Use of advanced malware, targeted attacks and data theft.

Qilin

- Qilin is a ransomware group that has gained attention for its targeted attacks on critical infrastructure and enterprise organizations.
- **Tactics**: Double extortion, exploiting vulnerabilities and leveraging malware to encrypt data.

RansomHub

- RansomHub is a ransomware operation that operates as ransomware-as-a-service (RaaS), allowing affiliates to deploy ransomware under their branding.
- **Tactics**: Ransomware-as-a-Service (RaaS) model, data theft and extortion.

Cactus

- Cactus is a ransomware group that has been involved in targeted attacks, often demanding high ransoms.
- **Tactics**: Data encryption, double extortion and exploiting vulnerabilities.

Incident Report — Multiple security gaps expose target to Cactus

Targets were tricked into downloading malicious files through Teams calls. The attackers set up channels to issue commands remotely, move laterally and maintain persistence. Malicious scheduled tasks, registry edits and DLL sideloading (when a program is tricked into loading a fake, harmful shared code file so the attacker's code runs instead of the real one) helped attackers escalate privileges and evade detection. The Barracuda Managed XDR team found rogue devices and more than 1,600 unprotected devices on the network, lax Microsoft Teams permissions, vulnerable deployments of remote desktop protocol (RDP) and secure shell, unsigned files and a lack of employee awareness.

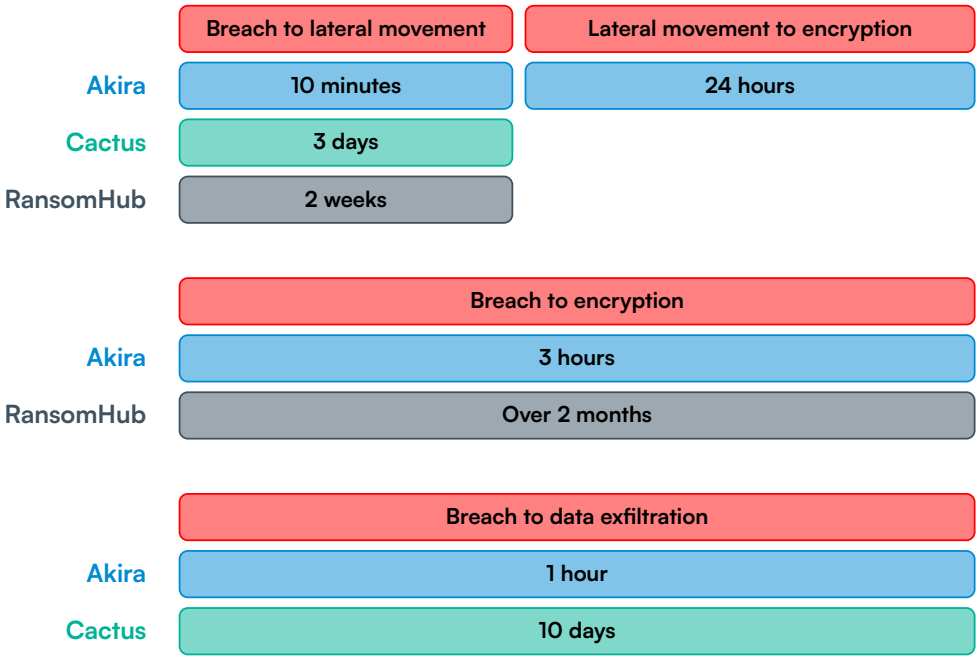
Ransomware moves at different speeds

According to Barracuda Managed XDR's detection and incident data, the fastest ransomware attacks in 2025 took just hours end-to-end, while the longest took months.

Lengthy intrusions allow for maximum damage as attackers have time for reconnaissance, data exfiltration, sabotage, and more. Incidents that move at lightning speed can be harder to catch and contain before they've been executed and the damage is done.

Organizations need to be ready for both types of attacks — and have security tools in place that are always on the lookout.

The speed of ransomware — 3 actors



Times estimated from real-world incidents

Incident Report — XDR catches Akira ransomware exploiting 'ghost' account and unprotected server

The attackers breached the network through an account that was created for a third-party vendor and not deactivated when they left. The attackers tried to move laterally and disable endpoint security but were blocked. They shifted to an unprotected server, escalated their privileges and launched the ransomware. All impacted devices were neutralized. Other risks found on the target network included unprotected devices, an open VPN channel in their firewall and inconsistent MFA.

Conclusion: How to stay safe in a world of complex threats

Security teams face mounting challenges. With limited resources, they must safeguard an ever-expanding landscape of devices, applications, critical vulnerabilities, and fragmented security tools, often without the unified visibility needed to stay ahead of threats.

Everything is about to become even harder as attackers start to leverage agentic AI.

Agentic AI systems will automate the early and repetitive stages of an attack, scan environments nonstop, identify weak configurations, and launch targeted exploits in minutes. Threat actors leveraging AI agents will be able to make decisions, adjust strategies and correct or rewrite malicious code when something fails or they encounter an obstacle. This shift will dramatically increase the speed, scale and consistency of attacks.

Organizations need a unified security strategy that integrates advanced, AI-powered detection technologies with a fully autonomous SOC, complemented by user education, automated threat response and a resilient security culture.

There are quick wins, such as those described throughout this report. They include consistent multifactor authentication and access controls, a robust approach to patch management and data protection, and regular cybersecurity awareness training for employees.

This should be underpinned by a comprehensive, managed security platform and 24/7 managed XDR solution that integrates network, endpoint, server, cloud, and email security — providing full end-to-end visibility and management control supported by a fully autonomous SOC.

Long-term security lies in cyber resilience. Detection and prevention are the cornerstones of any security strategy, but in the face of increasingly complex and evasive threats, being able to respond to and recover from attacks quickly and with minimal impact is key.

The findings in this report are based on detection data from Barracuda Managed XDR, an extended visibility, detection and response (XDR) platform, backed by a security operations center (SOC) that provides customers with around-the-clock human and AI-led threat detection, analysis, incident response, and mitigation services.

Barracuda Managed XDR is part of BarracudaONE, an AI-powered platform that secures email, data, applications, and networks with innovative solutions and a centralized dashboard to maximize protection and strengthen cyber resilience.

About Barracuda

Barracuda is a leading global cybersecurity company providing complete protection against complex threats for all size business. Our AI-powered BarracudaONE platform secures email, data, applications, and networks with innovative solutions, managed XDR and a centralized dashboard to maximize protection and strengthen cyber resilience. Trusted by hundreds of thousands of IT professionals and managed service providers worldwide, Barracuda delivers powerful defenses that are easy to buy, deploy and use.