

Bitdefender Threat Debrief | March 2026

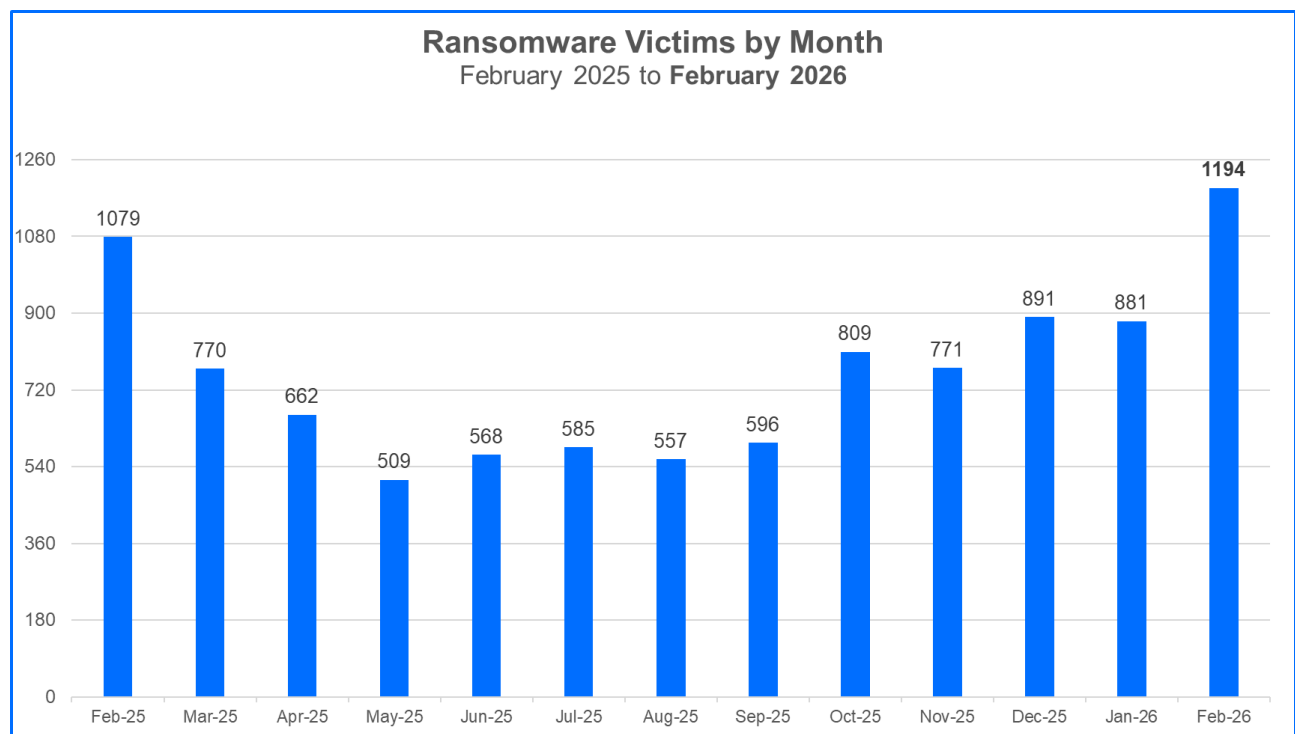
By Jade Brown

Published: 2026-03-11 · Archived: 2026-09-13 02:00:25 UTC

Ransomware Group AtomSilo Returns After 5 Year Absence

This edition of the Bitdefender Threat Debrief covers several developments in the threat landscape, including the reemergence of AtomSilo, a surge in OAPT’s claimed attacks, a threat emerging as tensions in the Iran war escalate, and more.

As ransomware continues to evolve, our goal with this monthly Bitdefender Threat Debrief is to help you stay ahead of the curve. To do this, we combine information from openly available sources (OSINT) - things like news reports and research – with data we gather by analyzing Data Leak Sites (DLSs), websites where ransomware groups post details about their victims. It is important to remember that we can't independently verify all of these claims but are confident in the trends we see over time.



For this month's report, we analyzed data from February 1 to February 28 and recorded a total of 1,194 claimed ransomware victims. Overall, the number of claimed attacks surged 43% compared to last month. This surge primarily reflects increased reports of OAPT victims that may not exist.

OAPT claimed 458 victims in February, a significant leap from the 91 victims they claimed in January. However, their claims, as reported in the [January Threat Debrief](#), are likely false and inflated due to a combination of factors: poor telemetry, filtering, and likely a “fake it until you make it” mentality. These numbers should not be

considered accurate representations of the legitimate number of ransomware victims. Therefore, we do not believe that the total number of victims claimed in February 2026 (1,194) is a record. Instead, February 2025 remains ransomware's biggest all-time month, with 1,079 legitimate victims (chart, above).

Featured Story: Ransomware Group AtomSilo Returns After 5 Year Absence

What Happened?

The AtomSilo ransomware group went dormant in 2021 and suddenly reappeared in February 2026. But is this revitalized iteration of AtomSilo connected to its 2021 predecessor?

AtomSilo Background

Before AtomSilo went dormant, we learned several things about the group. For one thing, its pattern of activity was linked to another state-sponsored adversary affiliated with China. The adversary, [Cinnamon Tempest](#) (or Bronze Starlight), was also active in 2021 and was known for exploiting CVEs to gain access to vulnerable systems, execute malware, and conduct espionage.

It's likely AtomSilo descended from Cinnamon Tempest, and both threat actors were known to deploy ransomware and increase their profits via extortion. Their motives also align with nation-state APT motives, with attacks focused on reconnaissance and counterintelligence efforts.

AtomSilo's re-emergence after five years is rare compared with other ransomware groups. It is far more common for ransomware groups to dissolve or rebrand within one to two years. As examples, consider former groups like Hive and Royal.

The Hive ransomware group emerged in early 2021 and rebranded to Hunter's International in 2023 following the FBI's [seizure of their infrastructure](#). Less than a year and a half later, Hunter's International rebranded to World Leaks, prioritizing data theft and data extortion over the use of encryptors to lock down systems.

Royal originally appeared under the moniker Zeon in early 2022. The group officially rebranded to Royal later that year. Then, in the second half of 2023, a group known as BlackSuit ransomware became active. More than a year later, Royal and BlackSuit ransomware were confirmed as variants within the same ransomware family, with some operators from the former Royal group sticking around for BlackSuit's operations. In July 2025, a joint law enforcement investigation known as Operation Checkmate, culminated in the seizure of the BlackSuit site. However, this was not a long-term deterrent for BlackSuit, who rebranded under the name Chaos with some of their operations already in play prior to the 2025 law enforcement takedown.

Why do most ransomware groups re-invent themselves more quickly than AtomSilo did? It's because a ransomware group's long-term success often depends on affiliate relationships. Most affiliates or connected partners will not wait two or three years (or more) to regroup. Instead, they will jump ship to other leading groups.

There is also the issue of a ransomware group's staff. Most groups that vanish for five years would face difficult challenges in rebuilding their brand and securing new staff. However, it's worth noting that state-sponsored or affiliated groups are far more likely to receive help and resources to restart the business and grow their ranks, regardless of the group's year-in, year-out profits.

What's Next?

Groups in a position like AtomSilo face some heavy burdens. They reenter the ransomware ecosystem, where they face intense competition and typically must evolve their tactics. At the time of this release, AtomSilo has claimed a couple of victims based in Brazil and one victim based in Japan.

There is also an anomaly that raises more questions about AtomSilo's motives and capabilities. The group recently claimed a victim named *A large bank in Asia*. This tactic of refusing to name their victim directly could be a decision made to negotiate a ransom payment, or the claim could be fake. At this time, additional information on AtomSilo's current tactics remains limited. However, given the group's history and affiliation as a state-sponsored threat, AtomSilo's activity could experience significant developments as they organize targeted espionage campaigns under the guise of a ransomware operation.

In the past year, there have also been increasing instances of ransomware groups modeling Advanced Persistent Threat or APT-like behavior by using techniques that differ from the common ransomware playbook. Extending the time they dwell within a victim's environment is one example. This is not the only trend that has resurfaced; in the past year, some ransomware groups and syndicates have coordinated attacks with resources from nation-state APTs, with the most notable instances being ShinyHunters' operations in August 2025 and [Qilin's Korean Leaks campaign](#) supported by a North Korean threat actor.

While ransomware groups across the board tend to be financially motivated and have a pattern of attack that differs from APT's, it's important for organizations to recognize that a blending of these entities and their attacks may also occur. As a result, we recommend staying informed about ransomware and APT threat actors.

Proactive measures that may be taken to limit the likelihood of a successful attack, from either threat, include regularly collecting and reviewing threat intelligence on threat actor TTPs, [reducing your attack surface](#), and monitoring network traffic for unusual activity. Furthermore, logging and retaining a wide range of security events to investigate an intrusion is critical alongside maintaining a [rapid response capability](#) equipped to isolate compromised assets and block malicious activities.

Other Notable Ransomware News

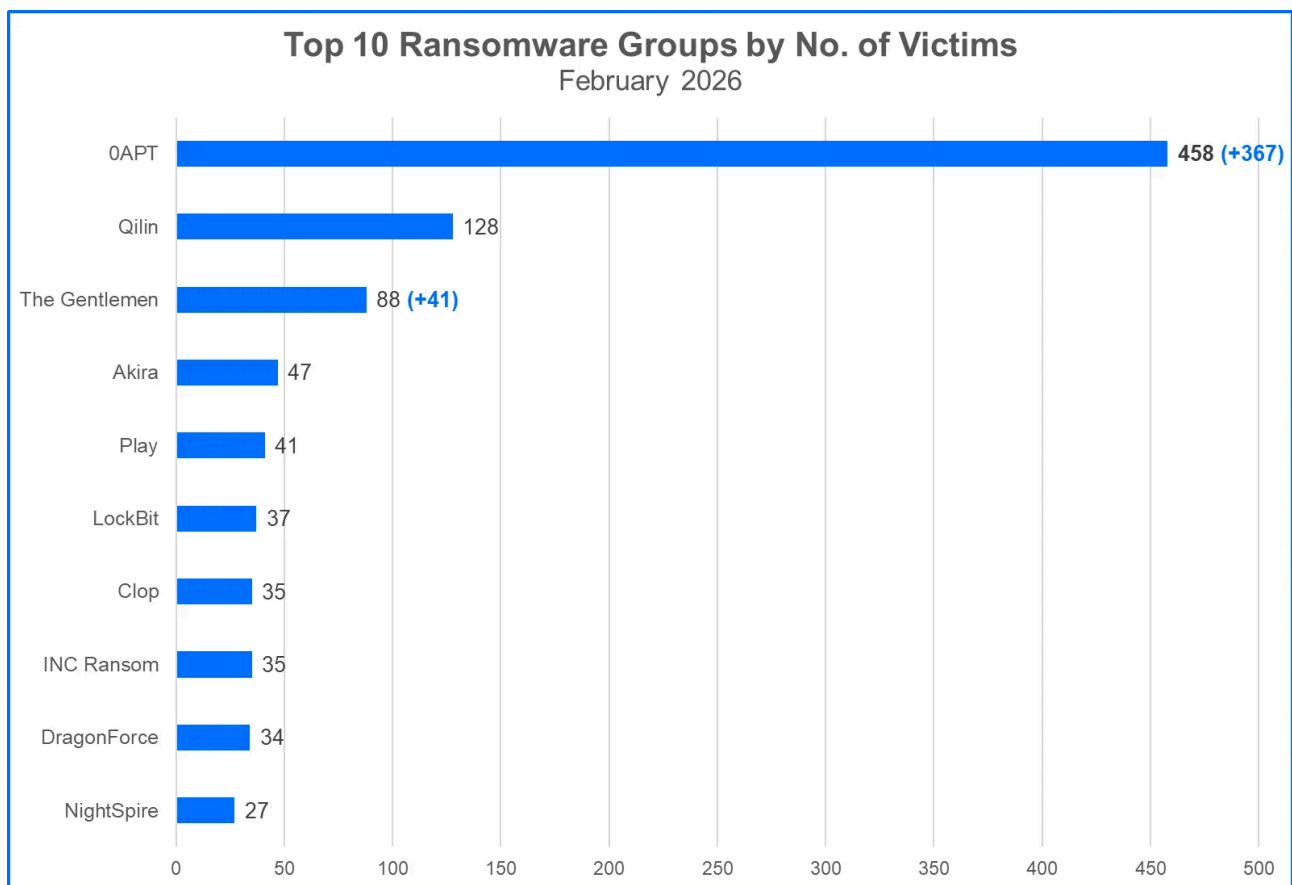
Now, let's explore the notable news and findings since the [last Threat Debrief](#).

- **The Gentlemen Surpasses Akira in the Top 10 Groups:** In February, the ransomware group The Gentlemen claimed 88 victims, which was a stark increase from the 41 victims they claimed in January. The group targets numerous industries; however, many of their victims from February were in the manufacturing, transportation, technology, and construction industries. The Gentlemen also claimed half of Thailand's ransomware victims in February. Taking an aggressive approach to stealth, the group employs Bring Your Own Vulnerable Driver (BYOVD) tactics, including the use of the [legitimate driver ThrottleStop.sys](#) to kill EDR and anti-virus processes. Understanding how similar [BYOVD attacks work](#) is crucial to determining [how to protect](#) vulnerable systems. The Gentlemen has also implemented a strategic approach to purging artifacts, removing select data from [Windows Defender logs](#), RDP logs, and Prefetch files.
- **The Iranian Conflict Galvanizes a Ransomware Group with Hacktivist Aims:** The ransomware group BQTLock, also known as BaqiyatLock, is building their presence in the RaaS (ransomware as a service)

ecosystem. At the end of January, the group posted an offer to provide their RaaS platform for free to hackers interested in contributing to their cause. BQTLock's political attitude leans towards an ideology that supports Iranian and Palestinian interests. The group has attacked organizations in the United States and the United Arab Emirates, claiming victims in the technology and government sectors. This type of victimology indicates that they're not primarily concerned with profits but instead are focused on executing campaigns designed to disrupt the US government ecosystem, and take down organizations based in the United Arab Emirates and other opposing regions like Israel.

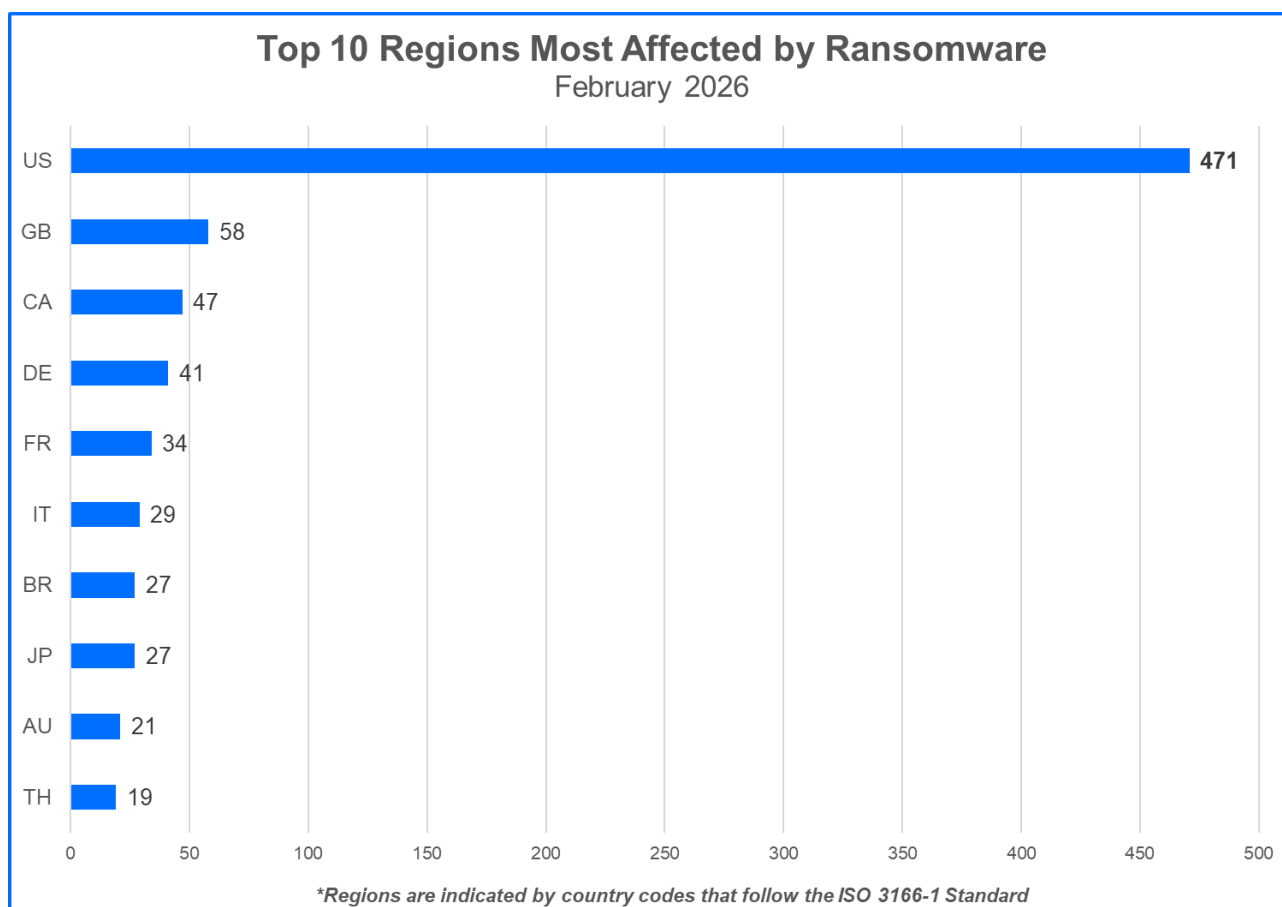
- **ShadowByt3\$ Twists the Narrative for the Ransomware Business Model:** ShadowByt3\$ emerged at the beginning of the year and is now reaching out for new recruits with penetration testing experience. The group describes themselves as a Wiper as a Service (WaaS) operation that does not execute ransomware. Based on their comments, it's instead understood that the group operates by infiltrating an organization, stealing data, and then wiping or threatening to wipe it if the victim does not submit payment. This sabotage strategy underscores the importance of maintaining regular backups, kept isolated from critical environments. While other groups, such as Anubis and NightSpire, have incorporated malware with wiping modules into their campaigns, this designation of a threat as a WaaS group is unique.
- **Europol Announces the Takedown of the Stronghold LeakBase:** LeakBase, a highly popular dark web forum dedicated to [sharing info stealers](#), leaked databases, and other sensitive data, was taken down in a joint effort led by Europol, the FBI and other law enforcement agencies. The fall of LeakBase, which had [more than 140,000 users](#), is a pivotal moment in the fight against cybercrime that occurred just after another landmark event: the [seizure of RAMP](#). Both takedowns leave a rift in the criminal ecosystem, with some cybercriminals moving to other reputable platforms with a rich history and strong userbase for ransomware and hacking groups such as XSS. More ransomware groups are also flocking to Telegram and Signal communities.
- **Ransomware Groups Exploit a Critical BeyondTrust Vulnerability:** [CVE-2026-1731](#) is a vulnerability that allows unauthenticated attackers to perform remote code execution. The vulnerability affects [Remote Support \(RS\)](#) versions 25.3.1 and older and [Privileged Remote Access \(PRS\)](#) versions 24.3.4 and older. Organizations using BeyondTrust to facilitate remote support and other privileged remote access activities are advised to apply the RS patch BT26-02-RS and the PRS patch BT26-02-PRA and ensure that both products are current.
- **Scammer Masquerading as Russian intelligence Officer Outwits Conti:** A report from a Russian news outlet revealed an interesting reversal of roles. During September 2022, Ruslan Satuchin, a Russian nationalist, posed as a Federal Security Service (FSB) officer. Satuchin was able to acquire contacts in the aftermath of the Conti Leaks matter, where an insider leaked Conti chats and identities. He then [contacted Conti staff](#) and offered them protection from the Russian government he said was investigating them, in exchange for money. Satuchin was detained by Russian law enforcement in October 2025. He was recently charged and is waiting for a trial date. Satuchin faces a [prison sentence of ten years](#) for impersonating an FSB officer; a \$13,000 fine is also associated with his offense.

Top 10 Ransomware Families



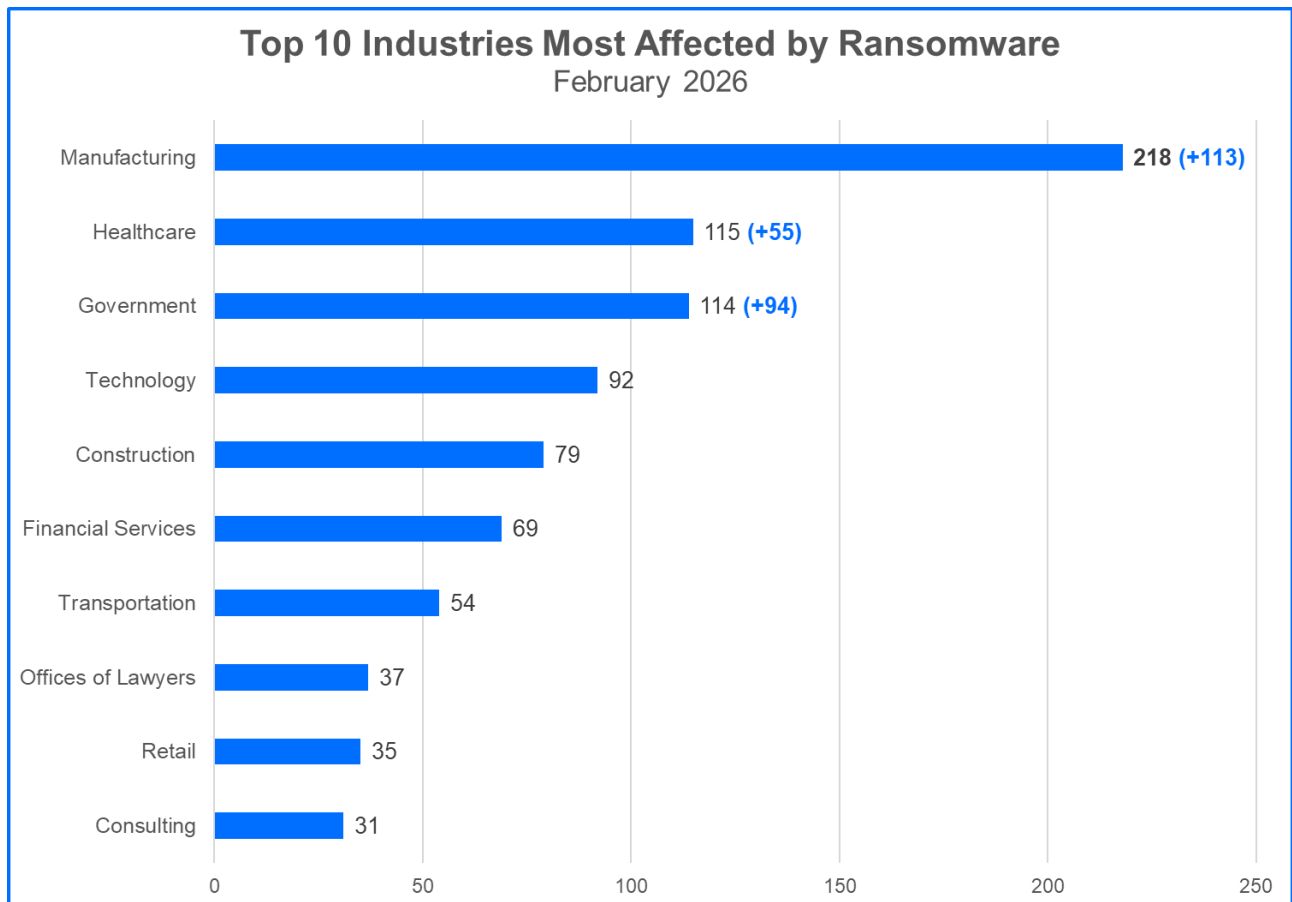
Bitdefender's Threat Debrief analyzes data from ransomware data leak sites, where groups publicize their claimed number of compromised organizations. This approach provides valuable insights into the overall activity of the RaaS market. However, there is a trade-off: while it reflects attackers' self-proclaimed success, the information comes directly from criminals and may be unreliable. Additionally, this method captures the number of victims claimed, not the actual financial impact of these attacks. Here are the Top 10 ransomware groups.

Top 10 Most Attacked Regions



Ransomware gangs prioritize targets where they can potentially squeeze the most money out of their victims. In many cases, this means focusing on developed countries with higher projected growth rates. Threat actors may also execute strategic attacks that unfold during geopolitical conflicts or periods of social unrest. Let's see the top 10 regions that took the biggest hit from ransomware attacks.

Top 10 Most Attacked Industries



Ransomware gangs may target organizations in critical infrastructure sectors, select other organizations that offer services tailored to consumers, or attack organizations that fall into both categories. Understanding the trends and ramifications of specific industries, and how specialized services and clientele are affected, is crucial for assessing risk. Here are the Top 10 industries affected by ransomware attacks.

Note: The Top 10 Industries Most Affected by Ransomware graphic (above) includes significant increases, highlighted in February, that show changes in several industries impacted by ransomware. These increases are most apparent, particularly in the manufacturing, healthcare, and government industries. It's important to note that the OAPT ransomware group accounted for these increases.

Data on targeted industries must be assessed with great scrutiny as a result. While the manufacturing industry would persist as a top industry affected by ransomware, regardless of the victims claimed by OAPT, it's likely that the government sector ranked below the top 10. It typically ranks 12 or 13 on the list of most attacked industries, however, the OAPT group has skewed these results.

MDR Threat Insights

Threat trends shift quickly, and the Bitdefender MDR (managed detection and response) team sees them in real time. The following insights consolidate key findings captured from real-world incidents.

In February 2026, our MDR teams found that hallmarks of threat actor activity included:

- A focus on identity-first compromise, including the theft of VPN credentials

- Remote registry hive access
- The use and installation of legitimate RMM tools for persistence
- Firewall and RDP enablement modifications
- Fileless attacks and in-memory code execution

The MDR team also raised an important point this month: an increasing number of incidents do not involve malware. Attackers are increasingly leveraging legitimate admin tools and operating quietly.

The Bitdefender MDR + EDR technology:

- Detects and interrupts domain-level compromise before it becomes an outage
- Detects the malicious use of trusted tools

Explore the power of [MDR](#) and read the Bitdefender Ransomware [white paper](#) (frequently updated) for more information on protecting against ransomware.

About Bitdefender Threat Debrief

The Bitdefender Threat Debrief (BDTD) is a monthly series analyzing threat news, trends, and research from the previous month. Don't miss the next BDTD release, subscribe to the [Business Insights](#) blog, and [follow us on Twitter](#). You can find all previous debriefs [here](#).

Bitdefender provides cybersecurity solutions and advanced threat protection to hundreds of millions of endpoints worldwide. More than 200 technology brands license Bitdefender technology as part of their product or service offerings. This vast [OEM ecosystem](#) complements the telemetry data already collected from Bitdefender business and consumer solutions. Overall, Bitdefender Labs discovers more than 1,000 new cyberthreats each minute and validates 50 billion threat queries each day. This gives us one of the industry's most extensive real-time views of the threat landscape.

We would like to thank Bitdefenders Stefan Hanu, Mihai Leonte, Gabriel Macovei, Andrei Mogage, and Nikki Salas for their help with putting this report together.

Source: <https://www.bitdefender.com/en-us/blog/businessinsights/bitdefender-threat-debrief-march-2026>