IT ISAC

CELEBRATING 25 YEARS OF THREAT INTELLIGENCE SHARING

STATE OF THE THREAT

IT Sector Cyber Trends

AUGUST 2026

OVERVIEW

The first half of 2026 has confirmed what defenders across the IT sector have long suspected: the threat landscape isn't just growing, it's accelerating. The IT-ISAC tracks over 330 adversaries through ongoing threat intelligence work, member collaboration, and reporting from partners across the security community. Based on this, five trends have emerged:

- **AI Acceleration:** Defenders and attackers have both been integrating AI into their daily operations. However, AI has made attackers more efficient across the board — helping them discover vulnerabilities faster, build malware faster, and adapt social engineering lures faster than defenders can keep up.

- **Ransomware Attack Volumes:** Ransomware is on pace to reach nearly 8,700 attacks in 2026, the highest since our tracking began, with no sign of slowing.

- **Nation-State Actors:** These actors are broadening their targets beyond traditional espionage, planting themselves inside critical infrastructure and slipping onto companies' payrolls.

- **Hacktivism:** Hacktivist groups are shifting, too, moving past website defacements and denial-of-service campaigns toward destructive attacks designed to cause real damage, not just make a statement.

- **ClickFix Attacks:** This type of attack is widely deployed across all threat actor groups. This attack tricks users into pasting and running malicious commands under the guise of fixing a fake error message and has become one of the fastest-growing ways for attackers to gain an initial foothold.

Taken together, these trends underscore a rapidly evolving landscape that requires constant, near-real-time adaptations and adjustments by network defenders.

AI: THE GOOD, THE BAD, AND THE BACKLOG

No trend has moved faster in 2026 than the adoption of AI on both sides of the fight. What used to be a multi-year technology adoption curve has compressed into months. While AI has become a genuine advantage for defenders, it's had the same effect for attackers.

For IT sector security teams stretched thin by a persistent talent shortage, AI is helping close the gap by triaging alerts, correlating signals, and flagging anomalies that rule-based tools would miss, such as unusual data downloads or a service account accessing new systems. AI has become an essential capability that helps understaffed teams keep pace with alert volume and reduce the time between detection and response.

On the other side, attackers have adopted AI just as aggressively, without the constraints of organizational governance, testing, or human review. Threat actors are using it to generate malware that rewrites its own code on every execution to evade signature-based detection, personalize phishing and social engineering lures at scale, and dramatically shorten the vulnerability-to-exploit timeline. Exploits now follow disclosure within hours, sometimes less. Increasingly, exploitation begins before a vulnerability is even publicly disclosed. That speed is breaking vulnerability disclosure and patch management as we know it. IT organizations feel it first as they're the ones patching the software everyone else depends on. AI is finding vulnerabilities faster than defenders can triage them, while simultaneously giving attackers a faster path to exploit them.

For example, CVE disclosures are on pace to hit 66,000 in 2026, running 46.3% ahead of projections, with AI-assisted discovery driving the surge. In 2025, of the roughly 48,000 CVEs disclosed, only about 1% were actually exploited. Whether that gap between disclosure and exploitation will hold in 2026 and beyond remains to be seen. However, these two trends, the increasing number of vulnerabilities being discovered, and the low percentage of vulnerabilities being exploited, indicate that network defenders should not treat every new CVE as equally urgent.

How to Prioritize Vulnerabilities

CVSS scores are useful, but they don't predict which vulnerabilities attackers will actually use. These two free resources can help prioritize more effectively:

CISA BOD 26-04
CISA's Binding Operational Directive 26-04 provides a structured framework for prioritizing security updates based on real-world risk factors including public exposure, presence on the Known Exploited Vulnerabilities (KEV) catalog, and technical impact.

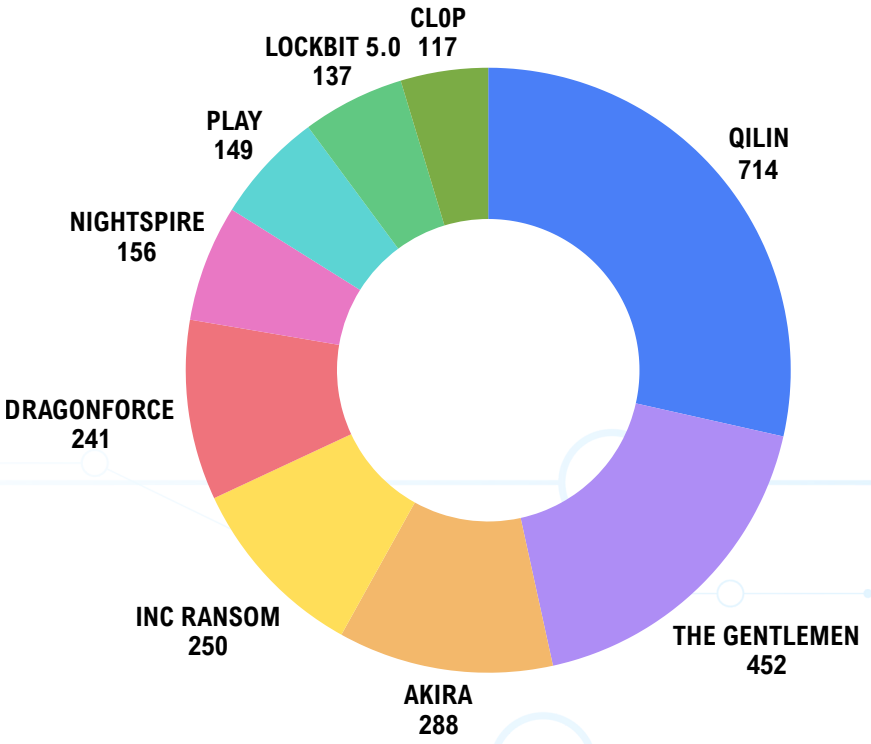
Exploit Prediction Scoring System (EPSS)
Developed by FIRST, EPSS uses machine learning to identify patterns between vulnerability characteristics and observed exploitation activity, offering a substantially better predictor of real-world exploitation than CVSS thresholds alone.

RANSOMWARE ACTIVITY

Ransomware remains the most consistent and costly threat organizations face, and 2026 is on pace to be one of the most active ransomware years on record. Between January and July 2026, IT-ISAC tracked 4,272 attacks across 108 unique threat groups. This is up 22.7% from the same period in 2025 and 219.5% from the same period in 2024.

The top ten most active ransomware groups accounted for the majority (59%) of the attacks tracked through July. Qilin, known for its double-extortion tactics, custom Rust-based malware, and ransomware-as-a-Service (RaaS) model, took the number-one spot with 714 observed attacks.

TOP 10 ACTIVE RANSOMWARE GROUPS
January - July 2026



For additional context, IT-ISAC tracked 6,635 incidents throughout 2025. For 2026, they are on pace to reach nearly 8,700 observed incidents by year's end. This would be a roughly 31% year-over-year increase. The IT sector alone ranked third among all sectors targeted, absorbing 512 attacks, or roughly 12% of everything tracked through July.

NATION-STATE ACTIVITY

Nation-state activity has intensified in 2026, with state-sponsored actors expanding their playbook well beyond traditional espionage. This year's activity spans everything from increased, quiet pre-positioning inside critical infrastructure to brazen workforce fraud schemes. Threats from nation-states show no signs of slowing down. In IT-ISAC's most recent threat report, nation-state actors accounted for the largest share of adversaries targeting the IT sector.

China isn't hiding what it's after — cyberspace dominance is a stated pillar of its national strategy. What it doesn't publicize, though, is how: U.S. and allied intelligence agencies assess that Chinese operators are pre-positioning inside U.S. critical infrastructure, laying the groundwork for disruption if a conflict ever calls for it. Salt Typhoon is one example, having sustained a targeted espionage campaign for years. China is also working to sow societal friction; in June 2026, an OpenAI threat intelligence team identified what they believe are China-linked account clusters using ChatGPT to generate content that stokes anger around AI and data centers.

Russia, meanwhile, is looking for doors people forgot to close: CISA advisory AA26-194A warns that Russian state-sponsored actors continue exploiting poorly configured and vulnerable networking devices worldwide, scanning for exposed routers to gain access and exfiltrate sensitive configuration data. Targeting spans critical infrastructure globally and has a particular focus on communications, the defense industrial base, energy, financial services, government facilities, and healthcare and public health. It is worth noting that Russian actors have in the past launched disruptive attacks against critical infrastructure.

In March 2026, members from the National Council of ISACs (NCI) issued a joint advisory warning of the potential for Iran to launch cyber attacks as a result of the conflict with the United States. Unfortunately, this warning played out in real time in late July 2026, when cyberattacks hit water and wastewater utilities across at least seven U.S. states, with Minnesota bearing the brunt. The FBI, EPA, and CISA confirmed attackers were exploiting internet-exposed programmable logic controllers (PLCs), in some cases changing passwords and altering IP addresses to lock operators out of their own systems. Formal attribution is still pending, but federal officials have pointed to tradecraft consistent with prior Iranian operations, following a documented pattern of Iranian-linked attacks on U.S. water and energy infrastructure since the war began. Beyond these attacks focused on the water sector, Iranian-affiliated actors continue targeting internet-facing operational technology (OT) more broadly, alongside espionage against aerospace, defense, telecommunications, and aviation targets.

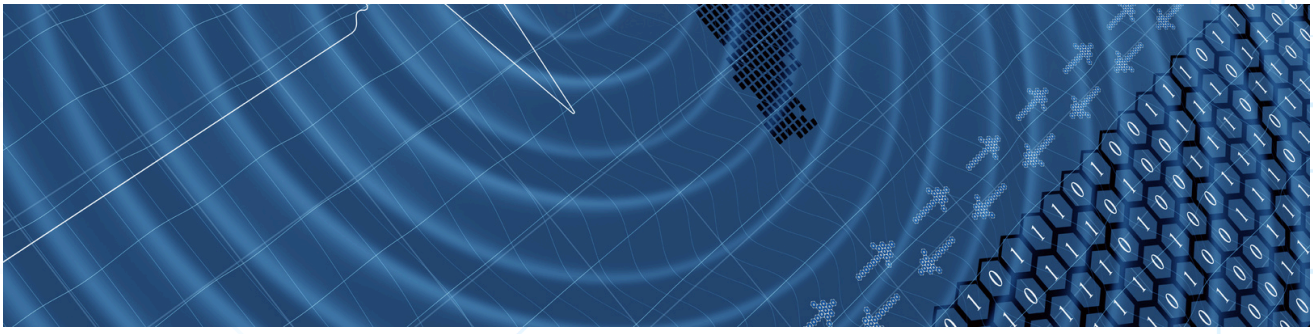
North Korea (DPRK) has taken a different approach entirely, dispatching thousands of skilled IT workers to pose as freelancers or full-time remote employees at U.S. firms including tech and finance. They use stolen identities, laptop farms to fake a U.S. location, and crypto payment chains to launder their wages back to the regime. Although it primarily started as a salary-collection scheme, this approach has evolved into something riskier: data theft, source code exfiltration, extortion, and insider access sold to other threat actors.

Learn more about DPRK workers and signs to watch for here.

HACTIVISIM

Hacktivism is not always as clear-cut as it looks on the surface. The line between state-sponsored activity and independent hacktivist activity in support of a country's foreign policy objectives is often blurry. For example, Iran has a documented history of running state operations through hacktivist fronts, which makes attribution murky and the activity more dangerous than it first appears. Following Operation Epic Fury, Rescana tracked 149 distributed denial-of-service (DDoS) claims against 110 organizations across 16 countries. The activity showed a heavy concentration against supervisory control and data acquisition (SCADA) systems, the software that runs industrial and critical infrastructure equipment.

The activity isn't staying confined to disruption, either. In March 2026, a Stryker wiper attack widely attributed to another Iranian-aligned group destroyed data outright instead of holding it for ransom, which is a shift from the usual goal of making a statement.



CLICKFIX ATTACKS

ClickFix has gone from a niche technique to one of the fastest-growing initial access methods in the threat landscape. What makes ClickFix worth calling out as a genuine trend, rather than a single clever gimmick, is who has adopted it and how fast it keeps evolving. Nation-state groups including Russia's APT28, North Korea's Kimsuky, and Iran's MuddyWater have folded it into espionage operations. Ransomware operators also use it as a reliable way to get a foothold before deploying ransomware or selling access to someone who will.

This type of attack tricks users into "fixing" a fake problem, such as a broken video player, a failed CAPTCHA, or an error message, by copying and pasting attacker-supplied commands into PowerShell or a terminal. ESET recorded a 517% jump in ClickFix attacks from late 2024 through the first half of 2025, and detections rose another 108% in the first half of 2026.

CLOSING

The IT sector sits on the front lines of the digital battlespace. Adversaries aren't just using advanced tools to find and exploit vulnerabilities in products the sector builds. The IT companies themselves are under direct attack. AI is reshaping both defense and offense, and the accelerating pace of vulnerability discovery and exploitation is straining product security and network security teams alike. Ransomware keeps climbing, and the IT sector itself ranks among the top three sectors targeted. Nation-states are treating IT infrastructure, edge devices, telecom networks, and remote hiring pipelines as a direct path into the systems that matter. Hacktivists are growing more sophisticated, more closely aligned with state actors, and more willing to inflict permanent damage. ClickFix has emerged as one of the most common and effective methods across nearly every category of attacker. There are no signs of a slowdown.

Attackers share with each other, and defenders need to do the same. Indicators are short-lived, but trusted partnerships are long-lasting. A dependable community sees more than any single organization can piece together on its own. In a time when security resources are constrained, collaboration with trusted peers is a cost-effective force multiplier, and one of the best ways to keep pace with a rapidly changing threat landscape that isn't slowing down for anyone.

Information Technology - Information Sharing and Analysis Center (IT-ISAC)

Founded in 2000, the IT-ISAC is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

Learn more at IT-ISAC.org or email us at membership@it-isac.org.