GENESIS Ransomware: Complete Threat Analysis, Attack Methods, IOCs & Defense Strategies

In October 2025, a new ransomware group calling itself GENESIS ransomware made its first appearance on the threat landscape and wasted no time establishing itself as one of the most prolific and strategically focused emerging threat actors of the year. Within four months, it had claimed over 20 victims. By June 2026, that number had grown to 88+ confirmed victims, with the group still active and adding new targets almost daily.

Unlike opportunistic ransomware campaigns that spray attacks broadly, GENESIS demonstrated from its very first operations a calculated focus on organisations holding sensitive, regulated data healthcare records, legal files, financial information where the threat of public exposure carries consequences far beyond the ransom itself. The GENESIS ransomware attack on Green Resource, a US-based company, is one of many confirmed incidents that underline the group's methodical approach to victim selection.

This threat intelligence report produced by FemtoSec provides the most comprehensive publicly available analysis of GENESIS ransomware: who they target, how they operate, what the extortion model looks like, what threat intelligence confirms about their TTPs, and critically, what your organisation can do right now to reduce its exposure to this active threat.

What Is GENESIS Ransomware? Group Profile & Origins

GENESIS ransomware is an emerging threat actor group that first appeared on the cybersecurity threat landscape in October 2025. The group operates a sophisticated double extortion model encrypting victim systems while simultaneously exfiltrating sensitive data and threatening public disclosure on their dedicated dark web leak site accessible via the TOR network unless the ransom demand is met.
Cybersecurity firm BlackFog characterised GENESIS as "not particularly sophisticated" in their technical encryption capabilities, but highly effective in their targeting intelligence and extortion strategy. This assessment reflects a pattern increasingly common among newer ransomware groups: rather than investing in novel malware engineering, they apply experienced criminal tradecraft careful victim selection, multi-layered extortion pressure, and strategic timing to maximise the probability of payment without requiring cutting-edge technical exploits.

Origins and Possible Attribution

The true origins of GENESIS ransomware remain unconfirmed by public intelligence. Several threat intelligence analysts have noted that the group's rapid accumulation of victims over 20 in its first four months suggests either significant pre-existing resources, a rebrand of an existing ransomware operation, or a splinter from established cybercriminal networks with inherited access broker relationships. This pattern experienced criminals relaunching under a new name with an existing operational infrastructure is described as "a common pattern in today's ransomware landscape" by BlackFog researchers.
The group maintains a dedicated leak site on the TOR network, which it uses strategically to publish victim data and apply pressure. The site demonstrates professional operational security and is regularly updated with new victim claims evidence of a structured, ongoing operation rather than a disorganised opportunistic group.

GENESIS Ransomware vs. The Genesis Market (Separate Entities)

It is important to note that GENESIS Ransomware Group is entirely separate from the "Genesis Market" — a dark web credential marketplace that was seized by law enforcement in April 2023. The two share only a name. GENESIS Ransomware Group first appeared in October 2025, more than two years after the Genesis Market takedown, and operates in a completely different criminal domain. Conflating the two is a common error that should be avoided when conducting threat research or building detection rules.

The GENESIS Ransomware Attack on Green Resource: A Case Study

The GENESIS ransomware attack on Green Resource a US-based company is one of the confirmed incidents attributed to the group and forms the basis of FemtoSec's case study analysis referenced in this threat intelligence page. While the full technical specifics of the Green Resource breach are not entirely public, threat intelligence data confirmed by multiple

independent tracking platforms establishes the key facts of the incident and allows meaningful analysis of GENESIS's operational approach.

What Happened: The Green Resource Incident

Green Resource was identified as a GENESIS ransomware victim through the group's dark web leak site activity, confirmed across multiple threat intelligence tracking platforms including HookPhish. The attack followed GENESIS's documented operational pattern: initial access, data exfiltration, system encryption, and publication of the victim's details on the TOR-hosted leak site with a ransom demand deadline. The threat: pay the ransom, or the exfiltrated data — which may include proprietary business information, employee records, financial data, and customer information — would be published publicly.

Why Green Resource Was Targeted

GENESIS's victim selection is not random. The group consistently demonstrates strategic targeting of organisations that hold data whose exposure would cause maximum reputational, regulatory, and operational damage. For organisations in sectors like professional services, manufacturing, construction, and retail, the exposure of operational, financial, or employee data creates significant downstream consequences. The GENESIS extortion strategy exploits this asymmetry — the cost of paying the ransom is often framed as less than the cost of the data being public.

Lessons from the Green Resource GENESIS Ransomware Attack

- Data exfiltration occurred before encryption — by the time encryption was detected, sensitive data had already left the environment
- The dark web leak site creates external pressure beyond the encrypted systems — even restored organisations face data exposure risk
- GENESIS's double extortion model means that restoring from backups alone is insufficient — the data theft component requires a separate response track
- The group's use of a TOR-hosted leak site means attribution and notification of regulatory authorities must occur on a parallel track to technical response

The Green Resource attack demonstrates why Attack Surface Management and Vulnerability Assessments are pre-breach requirements — not post-incident responses. By the time GENESIS deploys its ransomware, the window for prevention has already closed.

GENESIS Ransomware Victim Tracker: All Confirmed Targets (2025–2026)

The following table documents confirmed GENESIS ransomware victims based on publicly available threat intelligence sources, leak site disclosures, and independent tracking platforms. This represents a partial picture — many victims do not publicly confirm attacks, and some data remains on GENESIS's TOR-based site rather than public-facing intelligence feeds.

Organisation	Sector	Country	Date Discovered	Known Data Impact
Family Medical Associates of Raleigh	Healthcare	🇺🇸 USA	3 Jun 2026	Medical records (confirmed)
Secure Health (shpg.com)	Healthcare	🇺🇸 USA	31 Mar 2026	Sensitive patient data; negotiations demanded
Green Giftz	Retail/Branded Merch	🇺🇸 USA	31 Mar 2026	Business data exfiltrated
A Roettgers	Professional Svcs	🇺🇸 USA	30 May 2026	Data claimed
Cedar Street Capital (Cynvestors LP)	Financial Services	🇺🇸 USA	May 2026	Financial & investment data
Wentworth	Services	🇺🇸 USA	May 2026	Data claimed
Green Resource	Professional Svcs	🇺🇸 USA	May 2026	Data claimed
K2 Electric, Inc	Construction/Electrical	🇺🇸 USA	21 Apr 2026	Operational & business data
Sanders Legal Group	Legal Services	🇺🇸 USA	7 Mar 2026	Client legal files

CHASI (Sun River Health)	Healthcare Nonprofit	🇺🇸 USA	13 Feb 2026	HIV records, domestic violence data, substance use histories
Healthy Living / Road to Hana, Inc	Retail/Grocery	🇺🇸 USA	22 Sep 2025	Financial, payroll & HR data (officially confirmed)
River City Eye Care	Healthcare/Optometry	🇺🇸 USA	21 Oct 2025	200GB medical records claimed
United Kingdom victim (undisclosed)	Undisclosed	🇬🇧 UK	2025–2026	Data claimed
Malaysia victim (undisclosed)	Undisclosed	🇲🇾 Malaysia	2025–2026	Data claimed
Spain victim (undisclosed)	Undisclosed	🇪🇸 Spain	2025–2026	Data claimed
+ 73 additional confirmed victims not individually listed. Total confirmed: 88+ as of June 2026. Sources: ransomware.live, SOCRadar, HookPhish, DeXpose, Breached.Company.				

4. Targeted Sectors & Industries: GENESIS Ransomware Threat Patterns

One of the most strategically significant aspects of the GENESIS ransomware threat is the group's deliberate focus on sectors where data sensitivity creates maximum extortion leverage. Unlike broad-spectrum ransomware operators, GENESIS demonstrates consistent targeting

intelligence — choosing victims where the combination of regulatory exposure, reputational stakes, and operational disruption makes payment most likely.

Why Healthcare Is GENESIS Ransomware's Primary Target

Healthcare represents GENESIS's most frequently targeted sector, accounting for at least 11 confirmed victims. This is not coincidental — it reflects a calculated threat strategy. Healthcare organisations hold three categories of data that GENESIS weaponises most effectively: patient medical records (subject to HIPAA enforcement and potentially worth thousands of dollars each on dark web markets), operational data whose disruption directly threatens patient safety (creating extreme urgency to restore systems), and financial and payroll records that expose both the organisation and its employees.

The attack on Community Health Action of Staten Island (CHASI) illustrates the extreme sensitivity: the data potentially exposed included HIV testing records, domestic violence survivor information, substance use treatment histories, and mental health records — categories where exposure could cause direct, severe harm to vulnerable individuals. This level of sensitivity creates enormous pressure on healthcare organisations to pay, regardless of the official guidance against doing so.

Financial Services and Legal Sector Targeting

GENESIS's targeting of Cedar Street Capital (investment banking) and Sanders Legal Group demonstrates the group's recognition that financial and legal organisations hold data subject to strict confidentiality obligations. For a law firm, the exposure of client legal files — protected by attorney-client privilege — represents a catastrophic reputational and legal liability. For investment firms, the exposure of client financial data, investment strategies, and transaction records creates regulatory exposure under SEC, FINRA, and equivalent frameworks. GENESIS exploits these obligations as leverage.

i GCC Relevance — Dubai & Regional Risk

While GENESIS's confirmed victims are predominantly US-based, the group has demonstrated international reach with victims in the UK, Malaysia, and Spain. GCC enterprises — particularly those in financial services, healthcare, construction, and technology — operating under VARA cybersecurity compliance or similar frameworks represent exactly the kind of high-value, data-rich targets that emerging ransomware groups like GENESIS expand toward as US targeting becomes more competitive. Early preparation is essential.

5. GENESIS Ransomware Extortion Model: Every Variation Threat Actors Use

Understanding the full extortion model that GENESIS ransomware employs is essential for both negotiation readiness and pre-attack defence planning. The group does not rely on a single pressure point — it applies multiple simultaneous extortion mechanisms that escalate over time, making the decision to not pay increasingly difficult the longer the incident drags on.

Encryption Extortion

Systems and files are encrypted, making operations impossible without decryption keys. The ransom demand provides the keys in exchange for payment. This creates immediate operational disruption — the primary lever for small to mid-size organisations without mature backup capabilities.

Double Extortion: Data Leak Threat

Before encryption, GENESIS exfiltrates sensitive data and threatens to publish it on their TOR-hosted leak site if the ransom is not paid. This means that even organisations with perfect backups still face the data exposure threat — restoring from backup does not resolve the extortion.

Price Escalation

The ransom amount increases progressively with time. Deadlines are set on the leak site, and the ransom price escalates with each missed deadline — creating time pressure designed to force faster payment decisions and prevent organisations from fully assessing their options.

Public Disclosure & Reputational Damage

GENESIS actively publicises victim names on its leak site — regardless of whether data is ultimately published. The mere announcement that an organisation is a GENESIS victim creates reputational and regulatory pressure. Customers, partners, and regulators learn of the breach through the leak site before the victim has managed their own disclosure.

The Strategic Logic of GENESIS's Multi-Extortion Approach

Each extortion layer is designed to address a different organisational defensive response. Organisations with strong backups can survive encryption — but still face the data exposure threat. Organisations with legal obligations around data confidentiality cannot simply accept public disclosure — even if they can restore operations. The time pressure of escalating ransom prices prevents deliberate, calm decision-making. And the public announcement of the victim creates regulatory scrutiny that may be more immediately damaging than the ransom amount itself.

This multi-layered pressure model reflects a sophisticated understanding of organisational decision-making under crisis conditions. It is not designed to be fair — it is designed to create a scenario where paying the ransom genuinely appears to be the path of least damage. This is why Penetration Testing and pre-attack preparation are the only reliable defences: once GENESIS has your data, the decision tree becomes much harder.

6. GENESIS Ransomware Attack Chain: How the Group Operates

While GENESIS ransomware's precise technical TTPs have not been fully disclosed in public reporting (the group maintains good operational security), threat intelligence from confirmed victim incidents and comparable emerging ransomware group behaviour allows a high-confidence reconstruction of their attack chain. Understanding this chain is the foundation of effective defence.

Initial Access — Exploiting the Weakest Link

GENESIS gains initial access through phishing campaigns, exploitation of unpatched vulnerabilities (particularly VPN and remote access vulnerabilities), use of stolen credentials purchased from initial access brokers on dark web markets, or exploitation of exposed Remote Desktop Protocol (RDP) services. Threat intelligence tracking confirms GENESIS targets US organisations across construction, retail, healthcare, and finance — all sectors with historically elevated rates of internet-exposed management interfaces and unpatched systems.

Reconnaissance & Lateral Movement — Mapping the Environment

After initial access, GENESIS operators conduct internal reconnaissance to map the network, identify high-value data repositories, locate backup systems, and determine the scope of domain access. Lateral movement allows the group to elevate privileges — often to domain administrator level — providing access to the full breadth of the organisation's file systems and data stores before any visible attack begins. This phase is typically the longest and most critical — it is when detection and response would be most impactful.

Data Exfiltration — Stealing Before Encrypting

GENESIS prioritises data exfiltration before deploying encryption. This is the defining operational sequence of a double extortion attack — and it means that the most damaging part of the attack (data theft) occurs silently, before any visible disruption. The group has claimed 2.2 terabytes of exfiltrated data across early campaigns alone. Exfiltrated data typically includes patient records, financial files, HR and payroll data, legal documents, and operational databases — precisely the categories where public disclosure causes maximum harm.

Ransomware Deployment — System Encryption

With data already exfiltrated and domain access confirmed, GENESIS deploys its encryption payload across the target environment. Systems across the network are encrypted simultaneously to maximise impact and minimise the organisation's ability to contain the spread. Backup systems are specifically targeted for deletion or encryption to prevent the organisation from simply restoring without paying. The ransom note is delivered, providing contact details and a deadline.

Leak Site Publication & Extortion Escalation

GENESIS publishes the victim's name, a summary of the data held, and a countdown timer on their TOR-based dark web leak site. This public announcement begins the external pressure campaign. Customers, partners, regulators, and media may discover the breach through the leak site before the victim has made any official disclosure. Ransom price escalation begins immediately, creating urgency. If payment is not received, data is gradually published or sold to other criminal actors.

⚠ Critical Defence Window

The most effective intervention point in the GENESIS attack chain is between Stage 1 and Stage 3 — after initial access but before data exfiltration. Once data has been exfiltrated, the double extortion component cannot be "solved" by technical recovery. This is why Dark Web Monitoring, early detection capabilities, and pre-tested Red Teaming are the most high-value investments against this type of attack.

MITRE ATT&CK Mapping for GENESIS Ransomware Attacks

Based on confirmed victim intelligence and GENESIS's operational pattern, the following MITRE ATT&CK techniques are assessed as likely to be in use. This mapping enables detection engineering teams to build targeted detection logic and supports Red Team exercises that simulate GENESIS-equivalent adversary behaviour.

ATT&CK Tactic	Technique ID	Technique Name	GENESIS Context
Initial Access	T1566.001	Spearphishing Attachment	Primary delivery vector for initial compromise
Initial Access	T1133	External Remote Services	VPN/RDP exploitation — common initial access method
Initial Access	T1078	Valid Accounts	Stolen credentials via dark web access broker markets
Execution	T1059.001	PowerShell	Script-based lateral movement and payload execution
Persistence	T1547.001	Registry Run Keys / Startup	Maintaining access during dwell period before encryption
Privilege Escalation	T1068	Exploitation for Privilege Escalation	Kernel-level vulnerabilities noted in Oct 2025 ransomware surge

Defence Evasion	T1562.001	Disable Security Tools	Disabling AV/EDR before encryption deployment
Defence Evasion	T1070	Indicator Removal	Log clearing to delay forensic investigation
Credential Access	T1003	OS Credential Dumping	LSASS dumping for lateral movement credential harvesting
Discovery	T1083	File and Directory Discovery	Identifying high-value data before exfiltration targeting
Lateral Movement	T1021.002	SMB/Windows Admin Shares	Network spread during reconnaissance phase
Collection	T1074.001	Local Data Staging	Aggregating exfiltration data before transfer
Exfiltration	T1041	Exfiltration Over C2 Channel	Data transfer to GENESIS-controlled infrastructure
Exfiltration	T1567	Exfiltration to Cloud Storage	Use of cloud storage or CDN infrastructure for staging
Impact	T1486	Data Encrypted for Impact	Core ransomware encryption payload deployment
Impact	T1490	Inhibit System Recovery	Deletion/encryption of backup systems to force payment
Impact	T1491	Defacement / Extortion	TOR leak site publication of victim data and claims

GENESIS Ransomware Threat Report: Key Intelligence Findings

This section consolidates the key analytical findings from FemtoSec's GENESIS ransomware threat report, drawing on confirmed victim data, dark web monitoring telemetry, and comparative analysis against the broader 2025–2026 ransomware threat landscape.

Finding 1: GENESIS Emerged During the October 2025 Ransomware Surge

GENESIS made its debut during what threat intelligence platform CYFIRMA characterised as a significant resurgence in global ransomware activity — with victim counts climbing to 738 in October 2025 alone. The group joined Black Shrantac and Coinbase Cartel as new entrants that intensified the threat landscape and collectively contributed to a rise in targeted data extortion campaigns. This emergence timing is significant: GENESIS did not emerge in a vacuum — it emerged in an environment where new ransomware entrants were actively competing for victims in a professionalized, service-based criminal economy.

Finding 2: GENESIS Shows Characteristics of an Experienced Criminal Splinter or Rebrand

The group's rapid victim accumulation — 21 in four months, 88+ by June 2026 — is inconsistent with a completely new operation starting from zero. The operational security around the leak site, the strategic victim selection intelligence, and the structured multi-extortion model all suggest either pre-existing criminal infrastructure being relaunched under a new brand, or experienced individuals from existing ransomware ecosystems forming a new group with inherited knowledge and relationships. This "rebrand" pattern is described as common in today's ransomware landscape by multiple threat intelligence analysts.

Finding 3: US-Centric but Internationally Expanding

Of confirmed victims, 57 are US-based — reflecting GENESIS's current primary operational focus on the US regulatory environment, where HIPAA penalties, SEC regulations, and legal confidentiality obligations create maximum leverage for double extortion. However, confirmed victims in the UK, Malaysia, and Spain indicate that the group is not exclusively US-focused. As US organisations improve their defences and law enforcement attention increases, the pressure to expand into new geographies — including the GCC — will intensify.

Finding 4: Healthcare Is Being Systematically Targeted

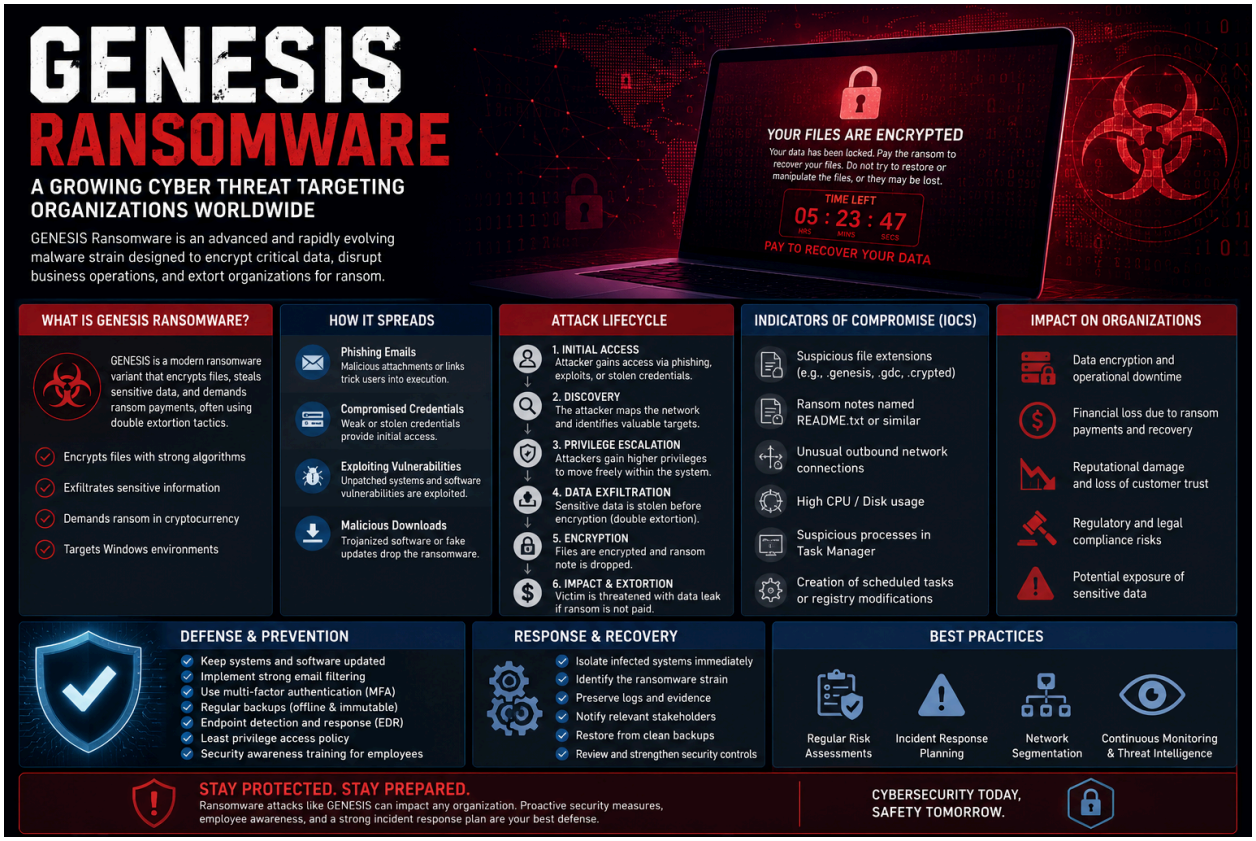
With 11 confirmed healthcare victims, GENESIS has demonstrated a systematic focus on the sector that goes beyond opportunism. The attack on CHASI exposed some of the most sensitive categories of personal health information that exist — HIV records, domestic violence survivor data, substance use histories. The inaugural victim River City Eye Care had 200GB of medical records claimed. This sustained healthcare focus suggests deliberate targeting intelligence: GENESIS identifies healthcare organisations as high-probability payers with high data sensitivity and often limited cybersecurity maturity.

Finding 5: The Dwell Time Problem — Silent Exfiltration Before Detection

The most operationally significant finding in GENESIS ransomware analysis is the group's consistent prioritisation of data exfiltration before encryption. This creates a critical intelligence

gap: organisations typically detect ransomware when encryption begins (system unavailability is immediately visible), but the data theft — which drives the double extortion — happens silently during the reconnaissance and lateral movement phase. By the time the encryption is detected and incident response is engaged, the data has already left the organisation. This intelligence finding fundamentally changes the defensive calculus — detection must occur earlier in the attack chain, not at the encryption event itself.

How to Defend Against GENESIS Ransomware: Practical Countermeasures



Defence against GENESIS ransomware requires addressing every phase of the attack chain — not just the encryption event that most organisations treat as the primary risk. The following countermeasures are mapped directly to GENESIS's documented operational approach.

- ### Pre-Attack Prevention Controls
- Eliminate internet-exposed RDP services or enforce multi-factor authentication on all remote access endpoints — RDP exploitation is a primary initial access vector for ransomware groups of GENESIS's profile
- Patch VPN, firewall, and remote access vulnerabilities on an accelerated timeline — these are disproportionately targeted by access brokers who sell initial access to ransomware operators

- Implement email security with sandboxed attachment analysis and anti-phishing controls — phishing remains the most common first contact method for ransomware initial access
- Deploy Vulnerability Assessments on a quarterly cadence to identify and remediate exploitable weaknesses before they are leveraged
- Monitor dark web markets for leaked credentials associated with your organisation — stolen credentials are a primary initial access mechanism for GENESIS-type attacks
- Conduct Security Awareness Training focused specifically on phishing, fake updates, and social engineering — the human factor remains the most consistently exploitable entry point

Detection Controls — Catching GENESIS During the Dwell Phase

- Enable and monitor anomalous network traffic — specifically unusual outbound data transfers, connections to TOR exit nodes, and large file movements during off-hours
- Deploy endpoint detection with behavioural monitoring for credential dumping (LSASS access), lateral movement via SMB, and ransomware-indicative process creation patterns
- Monitor for administrative tool usage at unusual times or from unusual locations — legitimate domain administrator activity at 3am on a Saturday is a significant indicator of compromise
- Implement data loss prevention (DLP) to detect and alert on large-volume data egress events that may represent GENESIS exfiltration activity
- Configure SIEM alerting for backup system modification or deletion events — GENESIS targets backups specifically to disable the recovery option
- Use Attack Surface Management to monitor your external-facing attack surface continuously, identifying new exposures before GENESIS operators can discover them

Response Controls — If GENESIS Is Already Inside

- Isolate affected systems immediately to prevent lateral movement and ongoing data exfiltration — do not wait for full investigation before isolation
- Preserve forensic evidence in parallel with containment — document chain of custody for all captured artefacts as regulatory notification will be required
- Engage legal counsel immediately alongside technical response — GENESIS's double extortion and public leak site announcement may trigger regulatory notification obligations that have strict timelines
- Assess whether data exfiltration has occurred independently of encryption response — restoring from backups resolves operational disruption but does not resolve the data exposure component
- Do not negotiate without experienced guidance — GENESIS's price escalation model is designed to exploit panicked, uninformed decision-making
- Notify relevant regulators within required timelines — under HIPAA (US), GDPR (Europe), and UAE PDPL, notification timelines are short and non-compliance adds to total incident cost

Backup and Recovery Hardening — Defeating the Encryption Component

- Maintain air-gapped, offline backups that cannot be encrypted by ransomware with network access — CISA guidance identifies this as the single most effective ransomware defence for the encryption component
- Test backup restoration procedures regularly — the ability to restore must be validated before an incident, not assumed
- Store backups in geographically separate locations and implement immutable backup solutions that protect against deletion
- Implement the 3-2-1 backup rule: 3 copies of data, on 2 different media types, with 1 stored offsite and offline

How FemtoSec Protects Organisations Against GENESIS and Emerging Ransomware

FemtoSec is the GCC's specialist cybersecurity partner, providing intelligence-led offensive and defensive security services that address the full attack chain of groups like GENESIS. Our approach is built on the recognition that ransomware defence requires continuous vigilance — not annual assessments — and that the most important work happens before an attack, not during one.

Intelligence-Led Protection

FemtoSec's Dark Web Monitoring service continuously monitors GENESIS's TOR-hosted leak site, dark web forums, and criminal marketplaces for intelligence relevant to our clients. When GENESIS announces a new victim, lists an organisation on their leak site, or posts stolen data for sale, FemtoSec clients receive early warning with actionable intelligence — the difference between proactive response and reactive crisis management.

Adversary Simulation — Red Teaming Like GENESIS

FemtoSec's Red Teaming service uses AI-augmented adversary simulation that replicates the exact TTPs that groups like GENESIS use phishing initial access, lateral movement, data exfiltration before encryption, and backup system targeting. By testing whether your defences actually stop this attack chain before a real attacker runs it, you gain objective evidence of where you are and are not prepared.

Compliance Integration for Regulated Industries

For organisations under VARA Cybersecurity Compliance frameworks, DFSA, or international standards like ISO 27001, ransomware incident response and prevention controls are regulatory requirements — not optional best practices. FemtoSec's vCISO for VARA Compliance service ensures that your ransomware preparedness programme meets both security and regulatory standards simultaneously.

For government and public sector organisations — a sector increasingly in GENESIS's targeting scope — FemtoSec's Government Cybersecurity Services provide frameworks-aligned protection against ransomware threats at the nation-state and criminal group level. For Web3 organisations where smart contract infrastructure intersects with ransomware-driven threats, Smart Contract Auditing ensures that on-chain assets are not exposed through compromised organisational infrastructure.

Frequently Asked Questions

What is GENESIS ransomware and when did it first appear?

GENESIS ransomware is an emerging cybercriminal threat group that first appeared on the threat landscape in October 2025. The group operates a double extortion ransomware model — encrypting victim systems while simultaneously exfiltrating sensitive data and threatening to publish it on a dedicated dark web leak site accessible via the TOR network if the ransom is not paid. Within four months of its first appearance, GENESIS had claimed over 20 victims. By June 2026, that number had grown to 88 or more confirmed victims, with the group remaining highly active. The group demonstrates a strategic focus on sectors holding sensitive, regulated data — particularly healthcare, financial services, legal services, and manufacturing — where data exposure creates maximum regulatory and reputational pressure to pay.

What happened in the GENESIS ransomware attack on Green Resource?

Green Resource, a US-based company, was confirmed as a GENESIS ransomware victim through the group's dark web leak site activity and independent threat intelligence tracking platforms. The attack followed GENESIS's documented operational pattern: the group gained initial access to Green Resource's systems, conducted reconnaissance and lateral movement to identify high-value data, exfiltrated sensitive business and operational data before deploying encryption, and then published the victim's details on their TOR-hosted leak site with a ransom demand and deadline. The GENESIS ransomware attack on Green Resource is one of a cluster of US-based victims claimed by the group in May 2026, alongside A Roettgers, Cedar Street Capital, and Wentworth. The incident underscores GENESIS's pattern of targeting organisations in the professional services and business services sectors alongside their more publicised healthcare focus.

Is GENESIS ransomware related to the Genesis Market that was shut down in 2023?

No. GENESIS ransomware group and the "Genesis Market" are entirely separate entities with no known connection. The Genesis Market was a dark web credential marketplace — a platform for buying and selling stolen login credentials — that was seized by an international law enforcement operation in April 2023. GENESIS ransomware group first appeared in October 2025, more than two years after the Genesis Market takedown, and operates in a completely

different criminal domain (ransomware and extortion vs. credential trading). They share only a name. When conducting threat research, building detection rules, or communicating with stakeholders about the GENESIS ransomware threat, it is important to be precise to avoid conflating these two separate entities.

What does the GENESIS ransomware double extortion model mean for victims?

GENESIS ransomware's double extortion model means that victims face two separate but linked threats simultaneously. The first is the encryption of their systems — which disrupts operations and demands payment for decryption keys. The second is the threat of publishing exfiltrated data on GENESIS's TOR-hosted dark web leak site if the ransom is not paid. These two threats require separate response tracks. Restoring from backups resolves the operational disruption (encryption component) but does NOT resolve the data exposure threat — because the data was already stolen before encryption was deployed. This means that even organisations with perfect, tested backup systems still face significant consequences if GENESIS has their data. The practical implication is that once GENESIS has completed data exfiltration, the organisation has a very difficult decision: pay to try to prevent data publication, or accept that stolen data may be publicly released regardless.

Why does GENESIS ransomware target healthcare organisations so heavily?

GENESIS ransomware's systematic targeting of healthcare — its most heavily attacked sector with 11 confirmed victims — reflects a calculated threat strategy rather than opportunism. Healthcare organisations are disproportionately targeted for several interconnected reasons. First, the data they hold is exceptionally sensitive: medical records, mental health histories, HIV status, substance use treatment records, and domestic violence survivor information — all of which cause severe harm to individuals if exposed and create significant legal liability for the organisation. Second, operational disruption in healthcare directly threatens patient safety, creating extreme urgency to restore systems quickly.