RedACTinsights

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

PHISHING CAMPAIGNS AGAINST UNIVERSITY OF PISA
ALPHV/BLACKCAT AND BEYOND

AUGUST 2025

@SIGNORINA37

real data. real threats. ***ransomNews****.*

/about_insights

Red**ACT** *insights* is the strategic analysis line of ransomNews.
Built as an extension of the monthly Red**ACT** report, it delivers in-depth coverage of ransomware trends, threat actors, tactics, and sector-specific risks.

Each piece is **grounded in verified data**, manual intelligence workflows, and OSINT/SOCMINT methodologies - developed through extensive research and a deep passion for threat analysis.

Tailored for decision-makers, analysts, incident responders, and cybersecurity professionals, Red**ACT** *insights* offers focused, actionable content drawn from real-world threat dynamics.

RedACTinsights

/follow_us

ransomnews.online
bsky.app/profile/**ransomnews.online**
linkedin.com/company/**ransomnews**
github.com/**ransomnews**
x.com/**ransomnews**
desk@ransomews.online

/use_conditions

The full or partial reproduction of Red**ACT** *insights* is allowed and permitted for **non-commercial use**, provided that the source is cited in accordance with the **Creative Commons Attribution • CC BY-NC** license.

Sophisticated phishing campaigns against University of Pisa
ALPHV/BlackCat and beyond

HIGHLIGHTS

- **A targeted phishing campaign** against the University of Pisa, involving cloned login portals designed to steal institutional credentials, may represent a renewed phase in an ongoing threat pattern first exploited during the 2022 **ALPHV/BlackCat** ransomware attack. While the group has since gone silent, the tactics observed in the recent phishing attempts align closely with ALPHV's typical initial access methods, suggesting that **affiliates or copycats** could be pursuing a similar compromise strategy.

- These phishing operations are not isolated events but **part of a broader trend** of persistent reconnaissance and access harvesting in the education sector. Institutions like the University of Pisa, which have previously faced high-profile breaches, remain attractive targets for follow-up campaigns. The continued targeting of student and staff credentials indicates a long-game strategy: gather access quietly, infiltrate slowly, and strike opportunistically.

RedACTinsights

Strategic Analysis
Recent Italian CERT-AGID alert: spear-phishing towards UniPI

CERT-AGID (Italy's national CyberSecurity Incident Response Team) recently reported targeted phishing campaigns aimed at University of Pisa personnel and students.

Attackers deployed **highly convincing login pages** impersonating the university's authentication portal. The objective is to capture cleartext institutional credentials (email and password) for unauthorized access to internal systems. The campaigns exhibit a degree of tailoring and specificity consistent with spear-phishing rather than mass phishing.

The phishing sites were designed to bypass user skepticism, **mimicking legitimate SSO portals**, including SPID access gateways. This represents a sophisticated initial access tactic, consistent with those seen in enterprise-grade ransomware campaigns.

The 2022 ALPHV/BlackCat ransomware Incident

In June 2022, the University of Pisa was among the **confirmed victims** of the ALPHV/BlackCat ransomware group. The attackers reportedly **demanded a ransom of around $4.5 million**.

Threat actor often **gained initial access** via stolen credentials, whether acquired through phishing, access brokers, or brute-force techniques.
While the full details of initial compromise in the 2022 attack were **not disclosed**, ALPHV's historical reliance on credential-based entry supports the hypothesis that similar phishing tactics were used, either directly or indirectly, to facilitate the breach.

Possible correlation: tactical echoes or strategic continuity?

Although ALPHV/BlackCat's infrastructure has **largely gone dark since late 2023** and US authorities dismantled part of its operational network, its TTPs (tactics, techniques, and procedures) remain widely emulated.

The phishing activity observed by CERT-AGID **shares significant overlap** with ALPHV's **typical intrusion path**:

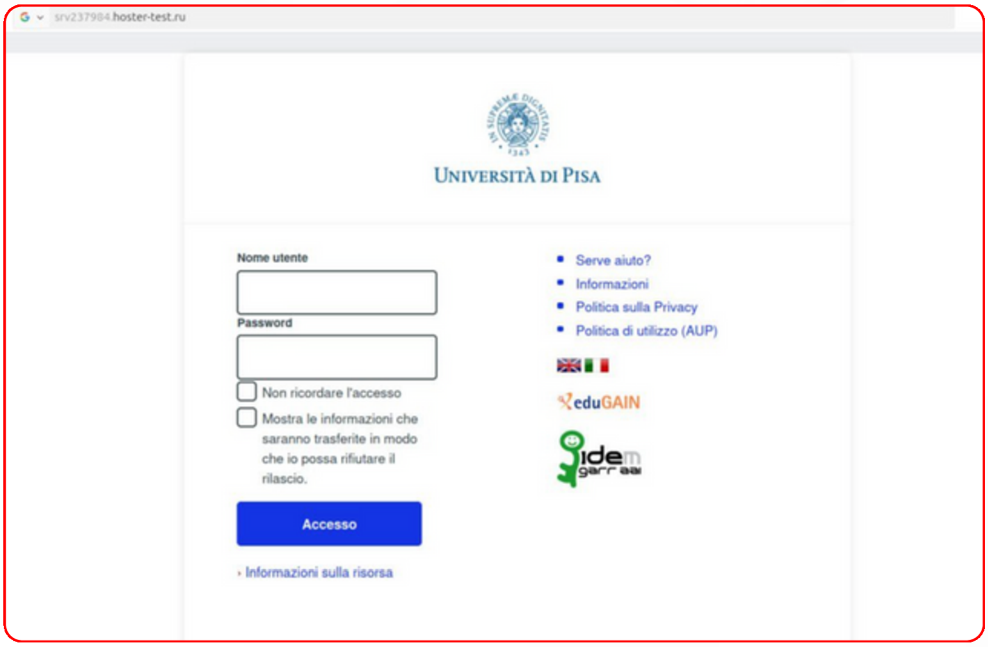
credential harvesting

stealthy accesses

data storaging

encryption extortion

RedACTinsights



srv237984.hoster-test.ru

UNIVERSITÀ DI PISA

Nome utente

Password

□ Non ricordare l'accesso

□ Mostra le informazioni che saranno trasferite in modo che io possa rifiutare il rilascio.

Accesso

› Informazioni sulla risorsa

- Serve aiuto?
- Informazioni
- Politica sulla Privacy
- Politica di utilizzo (AUP)

eduGAIN

idem garr aai

image courtesy AGID-CERT

It is highly plausible that the current phishing campaigns are either:

- a **reconnaissance phase** of a new ransomware campaign by former ALPHV affiliates now operating independently
- an effort by **access brokers harvesting valid credentials** to sell to ransomware operators
- or **part of a long-term persistence strategy**, aimed at silently regaining entry to previously compromised institutions

Alternative scenario: individualized extortion strategies

While the prevailing analysis **links phishing campaigns** to institutional compromise (just like credential harvesting as an entry point for broader ransomware operations), a second-layer implication is emerging: the **targeting of individuals for personalized extortion**.

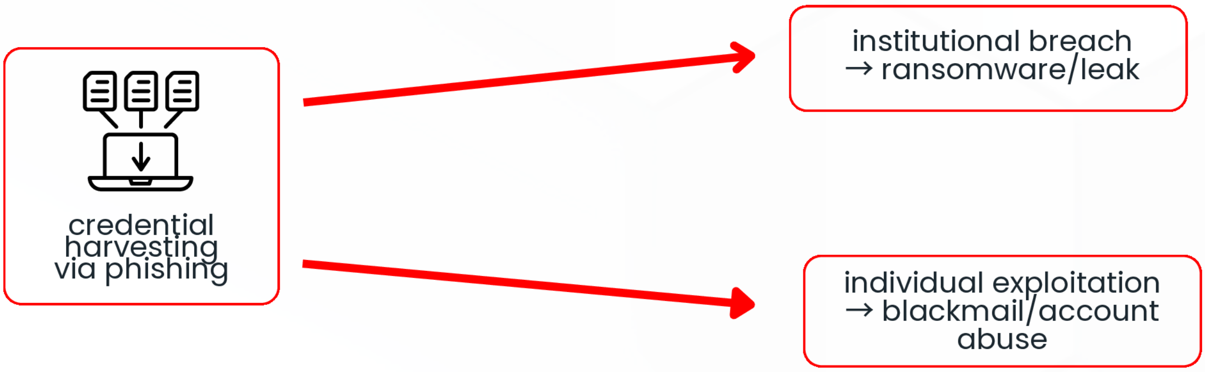
Once credentials are harvested from students, faculty, or administrative staff, attackers may not always aim for lateral movement into the institution. Instead, they might **leverage compromised accounts**, email inboxes, or document repositories to build psychological pressure directly on the individual.

This could include:

- **threats** to release academic or medical records
- **fabricated accusations** based on email content (cheating, harassment, ideological stances)
- **blackmail** based on private messages or stored files

This **micro extortion logic** mirrors trends seen in sextortion, infostealer monetization, and data leak marketplaces, and **represents a shift** from institutional to personal exploitation.

For threat actors, **this model is low-cost**, lower-risk, and potentially lucrative, especially when institutions enforce rapid lockdown protocols that make full network compromise harder to achieve.
Also, by attacking people instead of systems, criminals bypass hardened perimeters and **exploit the emotional and social vulnerabilities** of individuals, a tactic particularly effective in academic environments where reputational pressure is high.



credential harvesting via phishing

institutional breach → ransomware/leak

individual exploitation → blackmail/account abuse

RedACTinsights

Implications for Academia and other critical sectors

The reuse of phishing, especially tailored against prior victims, suggests that threat actors expect institutions to have incomplete recovery post-breach, including insufficient MFA enforcement, poor credential hygiene, or dormant user accounts.

Such campaigns reinforce the need for:

> - continuous threat hunting across authentication logs
> - mandatory multi-factor authentication across all internal and federated services
> - aggressive phishing simulation training tailored to the latest impersonation methods
> - zero-trust posture toward internal network movement, even with valid credentials.

Sectors such as healthcare and universities are a crucial target for threat actors. Since January 2022 we were able to track, among all, these claims:

- **ASL Napoli 3 Sud**, claimed by Sabbath (January 2022)
- **ASP Messina**, claimed by LockBit2 (April 2022)
- **Ospedale Macedonio Melloni**, claimed by ViceSociety (June 2022)
- **Azienda Ospedaliera di Alessandria**, claimed by Ragnarlocker (December 2022)
- **ASL 1 Avezzano, Sulmona, L'Aquila**, claimed by MONTI (May 2023)
- **Università di Salerno**, claimed by Rhysida (July 2023)
- **Ordine degli Psicologi della Lombardia**, claimed by NoEscape (October 2023)
- **Ospedale Centro Ortopedico di Quadrante**, claimed by LockBit3 (November 2023)
- **Azienda Ospedaliera Universitaria di Verona**, claimed by Rhysida (November 2023)
- **Azienda USL di Modena**, claimed by Hunters (December 2023)
- **ASP Basilicata, ASM Matera, IRCCS CROB**, claimed by Rhysida (February 2024)
- **Università di Siena**, claimed by LockBit3 (May 2024)
- **ASST Rhodense**, claimed by Cicada3301 (June 2024)
- **Comune di Pisa**, claimed by Nova (May 2025)

The social engineering terrain: the exploitable fatigue of change

Beyond technical vectors, a less visible yet highly exploitable factor is at play: remediation fatigue.

It is reasonable to assume that University of Pisa users (both staff and students) have been subjected to repeated credential renewal requests, password reset instructions, migrations to new authentication systems, and evolving portal access procedures in the wake of past incidents.

This creates a perfect cognitive landscape for phishing. The constant flux of legitimate security communications, when spread over months or years, dulls the user's sensitivity to unusual requests.

RedACTinsights

What should be a **red flag**, such as a new login page or credential prompt, becomes normalized. The novelty factor, often key in detecting phishing attempts, loses its effectiveness in an environment already saturated with change.

Social engineering thrives where users are overwhelmed by legitimate security noise.

This is not a user failure, but an operational and communications challenge for security teams: defending against advanced phishing requires not only technology, but also strategic alignment of change management, UX design, and **user trust calibration**.

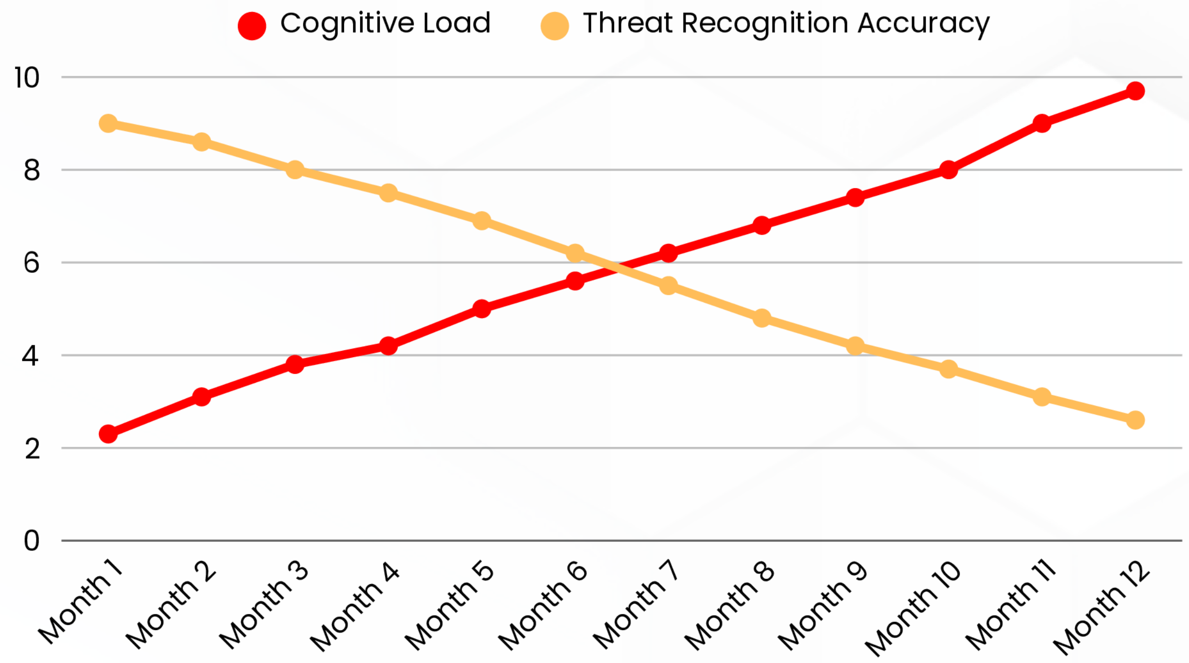
Security change fatigue versus User vigilance

A subtle yet critical behavioral trend in cybersecurity emerges strong: as **security related changes accumulate** over time (such as password resets, MFA rollouts, or portal migrations) **user cognitive load increases**.

This growing burden, though often necessary from an operational standpoint, has a psychological side effect: **a gradual decline in the user's ability to detect malicious cues**, particularly in phishing attempts.

The inverse correlation shown in the graph highlights how **overexposure to legitimate security communications** can inadvertently create fertile ground for social engineering. In environments where every week brings a new login interface or credential update, users begin to normalize unexpected requests, precisely the behavior attackers do count on.

RedACTinsights



RedACTinsights

RANSOMNEWS DISCLOSURE & ACTIVITY TRACKING

PHISHING CAMPAIGNS AGAINST UNIVERSITY OF PISA

ALPHV/BLACKCAT AND BEYOND

AUGUST 2025

@SIGNORINA37

real data. real threats. ***ransomNews.***