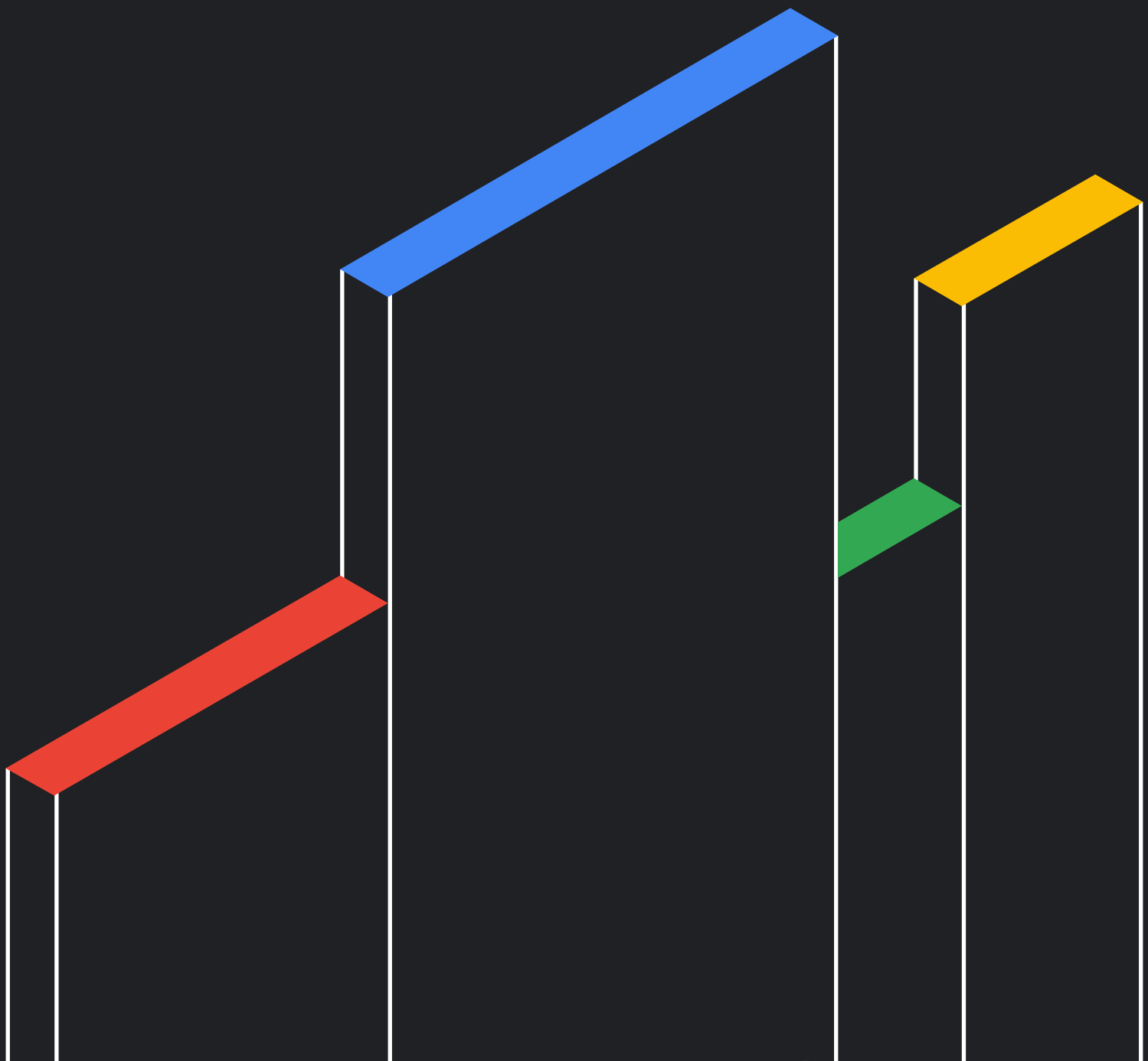
Mandiant

Google Cloud Security

M-Trends

2025 Report

Public Sector Edition



Introduction

Mandiant consultants are routinely deployed on the front lines of cyber incidents affecting public sector entities, where they conduct thorough investigations into the latest threat activities. This firsthand experience allows for a nuanced understanding of the changing threat landscape and the most effective defense strategies for protecting government and critical infrastructure systems.

Using frontline intelligence, Mandiant proactively evaluates the cybersecurity posture of public sector organizations by comparing their defenses to current adversary tactics, techniques, and procedures (TTPs). Additionally, we offer strategic support for remediation efforts, security architecture modernization, and customized cybersecurity training tailored to the specific operational and regulatory needs of public institutions.

Our commitment to public sector resilience is reinforced through the annual M-Trends report, which summarizes key findings from real-world incidents and events. By transparently sharing these insights, we enable federal, state, and local agencies with actionable intelligence to enhance national cybersecurity readiness.

U.S. Threat Numbers

Mandiant assesses with high confidence that the United States continues to face a persistent and multifaceted cyber threat environment, marked by aggressive financial, espionage, and influence-based operations. Public sector entities, including federal, state, and local governments, remain primary targets for both disruption and strategic intelligence collection.

Key Threat Categories

Category	Frequency	Impact
Financially Motivated (FIN)	5.0	4.5
State-Sponsored (STATE)	5.0	4.0
Information Operations / Hacktivism (IO/HACK)	4.5	3.5

The overall U.S. Cyber Threat Score for Q1 2025 is 8.1, underscoring sustained high-volume and high-impact adversary activity across critical domains of government and civil infrastructure.

Public Sector-Focused Threat Trends

Cyber Espionage

Nation-state actors—especially from Chinese Advanced Persistent Threat groups (APT40, APT31), Russia unclassified group (UNC2165), Iran, and North Korea—continued to pursue access to U.S. public sector networks. Targets include defense contractors, election infrastructure, municipal systems, and federal agencies. These actors leverage supply chain compromise, USB-based infections, and zero-day exploitation to evade detection and sustain long-term access.

Cyber Crime Targeting Government Services

Financially motivated groups increasingly exploit municipal services, public healthcare systems, and state agency networks. Tactics include the deployment of ransomware, business email compromise (BEC), and exploit-based lateral movement. Groups such as UNC5537 and UNC5055 have shown sustained interest in U.S. public digital services and payment systems.

Information Operations and Hacktivism

U.S. federal and state governments were targeted by foreign-linked disinformation campaigns, particularly during the 2024 election cycle. These efforts involved the use of falsified media, synthetic personas, and AI-generated content, which was amplified through social media. Threat actors sought to erode public trust in democratic institutions and sow societal division.

Strategic Threat Vectors

Vulnerability Exploitation

Public-facing infrastructure, including VPN appliances, authentication portals, and content management systems, was frequently targeted via known common vulnerability exploits (CVEs). Recent exploits affecting Ivanti, Fortinet, and SharePoint were used in campaigns against government entities.

Toolset Observations

Public sector compromises often involve BEACON, FAKEUPDATES, and CLEANBOOST malware families, along with credential theft tools and living-off-the-land techniques to bypass detection.

Infrastructure Challenges

U.S.-based cloud and hosting providers were exploited for command-and-control operations, allowing adversaries to blend malicious activity with legitimate traffic, thereby complicating attribution and mitigation.

Four Nation-States Targeting U.S. Public Sector

China

China continues to pose the most significant nation-state cyber threat to the U.S. public sector, with a wide array of campaigns focused on long-term espionage, infrastructure access, and credential theft:

- **Sustained Targeting of Government and Critical Sectors:** Chinese APT groups such as APT40 and APT31 remain active in campaigns against U.S. government agencies, contractors, and public institutions involved in defense, semiconductor manufacturing, and diplomacy.
- **Use of Zero-Days and USB-Based Vectors:** Chinese operations frequently incorporate advanced initial access techniques, including exploitation of zero-day vulnerabilities and the deployment of USB-based malware to gain footholds in air-gapped or sensitive systems.
- **Credential Harvesting and Identity Theft:** Threat actors linked to China are responsible for campaigns using infostealer-derived credentials, sometimes purchased from marketplaces, to access public sector environments indirectly. These credentials have been used to compromise third-party platforms relied upon by U.S. government entities.
- **Cloud and Supply Chain Exploitation:** Mandiant observed Chinese actors using both public cloud platforms and supply chain relationships as pivot points into U.S. systems. These efforts often aim to bypass direct defenses and maintain stealthy, long-term access.

China's cyber operations against the U.S. public sector are characterized by their persistence, technical sophistication, and alignment with strategic national goals, including technological acquisition and geopolitical influence. The threat is broad-based and ongoing, requiring sustained defensive investment.

Russia

Russia continues to be a major cyber adversary to the U.S. public sector, with its activity characterized by intelligence gathering, operational disruption, and gray zone influence tactics:

- **Espionage Campaigns:** Russian threat actors, including UNC2165 and groups associated with the SVR and GRU, conduct intrusions into U.S. federal agencies and state-level institutions to collect strategic intelligence, particularly around foreign policy, defense, and critical infrastructure.
- **Credential Theft and Cloud Abuse:** Mandiant tracked Russian-linked actors using infostealers to collect credentials, which were then leveraged to access cloud platforms used by public sector organizations. This allows for persistent access and indirect compromise of sensitive data.
- **Hacktivist Fronts and IO Blending:** Groups like CyberArmyofRussia_Reborn (CARR) blend information operations with real or exaggerated cyber intrusions. These efforts target municipal utilities, government websites, and public service platforms to generate headlines and instill fear, especially during periods of geopolitical tension.
- **Toolset Consistency:** Russian cyber operators frequently deploy known malware families, such as BEACON, CLEANBOOST, and REDBIKE, in their campaigns, often coupled with open-source tools and living-off-the-land binaries to evade detection and maintain access.

Overall, Russian cyber activity against the U.S. public sector remains strategically driven, frequently merging technical access with narrative shaping, particularly in the context of conflicts such as the war in Ukraine.

Iran

Iran-nexus cyber activity in 2024 demonstrated a marked increase in both volume and capability, posing a growing threat to U.S. public sector entities. Iranian actors, some affiliated with the Islamic Revolutionary Guard Corps (IRGC), focused on espionage, disruption, and influence operations. Notably:

- Over 45 new malware families were attributed to Iranian actors, representing a 35% increase from 2023.
- Campaigns targeted Israeli entities primarily, but methods such as wiper malware, cloud service abuse, and advanced social engineering apply to U.S. government and critical infrastructure networks.
- Public cloud infrastructure and remote monitoring tools were leveraged to obfuscate operations.
- Graphical user interfaces (GUIs) were embedded in malware to mask malicious payloads, increasing the likelihood of success against government personnel.

The TTPs and tools observed in Iranian operations suggest a heightened ability to bypass detection and potentially impact U.S. public systems, notably where defenses lag behind cloud-focused and social engineering threats.

North Korea

North Korea (Democratic People's Republic of Korea (DPRK) poses a distinctive and evolving cyber threat to the U.S. public sector, primarily through espionage and revenue-generating operations that indirectly support state objectives:

- **Insider Access through Fraudulent Employment:** North Korea deploys IT workers abroad, many under false identities, to infiltrate Western organizations, including U.S. firms. These individuals use remote access tools and VPNs (notably Astrill VPN) to mask their location and mimic legitimate employee behavior.
- **Espionage and Extortion Risk:** Although direct malicious activity by these insiders has been limited, their access enables potential espionage, credential theft, and extortion. Mandiant has observed initial cases of extortion, indicating that this tactic may be expanding.
- **Use of U.S. Infrastructure:** North Korean threat actors have abused U.S.-based cloud platforms and hosting services to facilitate command-and-control and phishing infrastructure, complicating attribution and takedown efforts.
- **Credential Theft via Infostealers:** North Korean-linked groups, such as UNC5537, have leveraged credentials stolen through infostealer malware to access third-party systems, including cloud databases used by U.S. public and private sector entities.

Overall, the DPRK threat combines covert workforce infiltration, sophisticated credential harvesting, and infrastructure abuse, making it a low-volume but high-consequence concern for public sector organizations that manage sensitive data or critical operations.

Volt and Salt Typhoon

Google assesses with high confidence that UNC3236 (a.k.a. Volt Typhoon) and UNC5807 (a.k.a. Salt Typhoon), two PRC-affiliated cyber espionage groups, pose a critical and ongoing threat to U.S. public sector networks, particularly within telecommunications, defense, and government operations.

Actor	Target	Tactics	Strategic Implications
Volt Typhoon	U.S. critical infrastructure	Living-off-the-land, native admin tools, hands-on-key-board intrusions	Prepositioning for potential disruption or sabotage
Salt Typhoon	Federal agencies and telecom providers	Exploitation of lawful intercept tools, long-dwell espionage	Enables persistent surveillance of sensitive communications

Specific Concerns for the U.S. Public Sector

National Security Risk

Both groups exhibit deep operational access across public networks and infrastructure, not limited to espionage, but potentially preparatory for broader conflict scenarios.

Detection Evasion

These actors avoid malware and instead manipulate legitimate administrative tools and credentials, evading traditional endpoint detection systems used by public sector agencies.

Systemic Weaknesses

Google highlights that legacy procurement models and underinvestment in AI-driven defense have left federal networks vulnerable to stealthy post-exploitation techniques, such as those seen in Volt Typhoon's attacks on routers and Salt Typhoon's access to telecom metadata.

Threat Implications for the U.S. Public Sector

Stealthy Persistence in Strategic Networks

The exploitation of widely used VPN appliances enables adversaries to establish long-term access effortlessly, bypassing regular detection through minimal reliance on custom malware.

Lateral Propagation into Sensitive Domains

Once VPNs are compromised, adversaries can maneuver laterally using legitimate credentials and tools, thereby putting federal and critical infrastructure systems at direct risk.

Pre-positioning for Disruption or Espionage

Compromises in energy, healthcare, academic, and defense ecosystems—identified by both Mandiant and NSA Cybersecurity Collaboration Center—suggest an adversary preparing for broader operations beyond pure data theft.

Google's Strategic Recommendations for Public Sector Organizations

Adopt cloud-native security controls and AI-driven detection to counter stealthy actors exploiting lateral movement and credential misuse.

Accelerate zero trust implementation across public sector networks.

Expand information sharing through interagency and industry partnerships to expose TTPs faster.

Secure legacy infrastructure (VPNs, routers) targeted by PRC-nexus groups for persistent access.

Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation

What do I need to know?

Critical zero-day in Ivanti Connect Secure (ICS)
On April 3, 2025, Ivanti disclosed CVE-2025-22457, a stack-based buffer overflow affecting ICS versions up to 22.7R2.5—later confirmed exploitable for unauthenticated remote code execution (RCE)—scoring 9.0 (Critical) under CVSS v3.1

Threat actor URGENCY and attribution
Exploitation began as early as mid-March 2025 by UNC5221, a suspected China-nexus espionage group known for targeting edge devices. The group reportedly reverse-engineered Ivanti's patch (22.7R2.6, released February 11, 2025) to tailor the exploit for unpatched 22.7R2.5 and earlier systems

TTPs
The exploit workflow typically involves version-probing HTTP requests, buffer overflow payload delivery, and post-compromise deployment of in-memory droppers (TRAILBLAZE), passive backdoors (BUSHFIRE/BUSHWALK), and cache-dump mechanisms (, masked .css archives of VPN session data)

Operational impact in the public sector
ICS appliances, often internet-exposed for remote access, are attractive targets. NHS Digital and others reported active exploitation of CVE-2025-0282/CVE-2025-0283, concurrent vulnerabilities, underscoring the compound threat on public infrastructure

Stealth and anti-forensics
Exploits disable SELinux, alter firewall rules to block syslog forwarding, remove debug logs, embed web shells in legitimate CGI handlers, suppress kernel messages, and introduce fake upgrade routines to persist post-patch and conceal detection

Data theft), credential harvesting, and lateral movement
Once inside, UNC5221 exfiltrates session/NAT/cache databases via web-served artifacts, deploys DRYHOOK Python credential stealer, abuses LDAP to enumerate internal AD environments, and uses built-in utilities (nmap, dig) for internal reconnaissance.

What do we need to do?

Patch/Upgrade
Immediately update Ivanti ICS to 22.7R2.6 or later; also patch Policy Secure and ZTA Gateway appliances as updates become available.

Factory reset prior to patch
As advised by Ivanti perform a factory reset before applying patches to eliminate embedded persistence mechanisms.

Use Integrity Checker Tool (ICT)
Run Ivanti's ICT before and after patching to detect any compromise, including stealth backdoors.

Hunt and monitor
Audit logs for version-probing HTTP requests and syslog suppression tactics.

Monitor Lightweight Directory Access Protocol (LDAP) queries
Monitor ICS appliances and suspicious login patterns. Use network IDS/IPS to flag anomalies (outbound HTTPS traffic or tunneled data transfers masked as CSS/JS files).

Credential revocation and rotation
Reset all local admin accounts, LDAP credentials, session cookies, API keys, and client certificates if ICS compromise is detected.

Network segmentation

Isolate VPN appliances from internal AD, file shares, or sensitive resources. Restrict outgoing connectivity to only Ivanti update servers and authorized logs.

Deploy advanced detection

Implement file integrity monitoring and memory inspection tools on appliances to surface in-memory implant activity (TRAILBLAZE); use YARA rules and IOCs published by Mandiant and CISA.

Continuous validation

Use Breach and Attack Simulation (BAS) to emulate known TTPs (TRAILBLAZE, BUSHFIRE, LDAP abuse) and evaluate detection posture.

Threat intel integration

Ingest Indicators of Compromise (IoCs), TTPs, and YARA signatures from Mandiant, CISA KEV catalog, and third-party advisories into SIEM/XDR platforms.

Prepared recovery plan

Assume compromise if unpatched ICS appliances were exposed. Conduct incident response: isolate, forensic image, revoke credentials, redeploy clean appliances, restore segmented access, and report to applicable public sector cybersecurity centers as required.

Healthcare Ransomware

What do I need to know?

Healthcare continues to be a consistent ransomware target

In 2024, healthcare organizations accounted for approximately 7% of victims listed on monitored data leak sites (DLS), a slight increase from the historical average of 6%. However, the number of hospital subsector victims increased notably, indicating higher interest in institutions with critical care services.

Underground actor sentiment varies

Actor stances on healthcare targeting fall into three broad categories:

- **Prohibited:** Some actors (PLAYCRYPT, BlackSuit) restrict attacks on healthcare to avoid attention.
- **Limited Scope:** Others permit attacks on non-critical care facilities (, plastic surgery clinics, pharmaceutical companies).
- **Unrestricted:** Groups like INC and Qilin (AGENDA ransomware) impose few if any restrictions.

Notable 2024 incidents

- **Saint Anthony Hospital (LockBit):** A $800,000 ransom demand was made following a data theft.
- **Romania hospitals (Phobos):** Over 100 healthcare facilities impacted across 25 targets.
- **Change Healthcare:** A sequential compromise by ALPHV and RansomHub resulted in the theft of 4 TB of sensitive data.
- **Octapharma Plasma (BlackSuit):** Disruption to over 150 U.S. donation centers.
- **Synnovis Labs (UK):** Ransomware attack disrupted blood test operations at seven London hospitals.

Actor tactics and tooling

- Threat clusters such as UNC2165, UNC3786, and UNC5348 leveraged methods ranging from fake software updates (FAKEUPDATES) to credential theft and multi-vector intrusions.
- Frequently observed tools included Mimikatz, BEACON, Ligolo, PowerView, and exfiltration mechanisms like Rclone and MEGASync.

Ransomware families

Mandiant observed widespread use of ALPHV, LOCKBIT, RANSOMHUB, REDBIKE (Akira), INC, RHYSIDA, and AGENDA[.]RUST across 2024 incidents involving healthcare victims. Most strains utilized strong encryption (ChaCha20, AES), lateral movement capabilities (IMPACKET), and data wiping or volume shadow deletion for impact maximization.

Access for sale in underground forums

Underground forums frequently featured advertisements for initial access to healthcare environments, including general clinics, medical software vendors, hospitals, and dental and ophthalmic centers across the U.S., Europe, and Latin America. Some actors specifically targeted these sectors for premium operations due to the high perceived likelihood of a ransom payout.

Ethical variance does not correlate with reduced targeting

Despite some threat actors publicly disavowing attacks on hospitals, enforcement of restrictions among ransomware-as-a-service (RaaS) affiliates is inconsistent. Cases of healthcare organizations appearing on “restricted” operators’ DLS suggest rule violations or selective exceptions.

What do we need to do?

Harden external surfaces
Audit internet-facing systems (VPNs, RDP, web portals). Ensure proper segmentation between patient-facing applications and internal infrastructure to maintain security and integrity

Enhance credential protection
Enforce phishing-resistant multifactor authentication (MFA) (FIDO2), especially on VPNs and administrative systems. Monitor for credential reuse and signs of credential stuffing.

Improve third-party risk management
Vet access and software from external partners (MediSecure breach originated from a vendor). Regularly validate vendor controls, patch hygiene, and breach disclosures.

Conduct ransomware-specific tabletop exercises
Simulate scenarios involving mass disruption (lab communication breakdowns, data exfiltration, and ransom timelines). Include operational staff (nursing, lab managers) in drills.

Prioritize data backup integrity
Implement offsite, immutable backups. Regularly test recovery procedures under degraded conditions (during offline or isolated network states).

Detect lateral movement and exfiltration
Deploy endpoint detection and response/extended detection and response (EDR/XDR) with capabilities to detect common TTPs (BEACON, Ligolo tunneling, Mimikatz credential dumping). Alert on large outbound transfers to cloud services or anomalous ZIP/RAR activity.

Integrate DLS monitoring into threat intel
Monitor DLS postings to identify if your organization or related vendors appear. This can serve as an early indicator of compromise or exposure.

Deploy deception and containment controls
Use honeypots, decoy credentials, and network canaries to detect unauthorized lateral movement. Combine with microsegmentation to limit internal blast radius.

Prepare public communication protocols
Draft boilerplate statements for patient notification, operational continuity, and regulatory engagement (HIPAA, GDPR). Review in light of the 2024 incident examples.

Coordinate with H-ISAC and sector-specific CERTs
Share IOCs, threat actor TTPs, and playbooks with industry peers. Utilize sector-level collaboration to identify and respond to shared threats more effectively.

Phishing Campaigns Against Higher Education

What do I need to know?

Significant uptick since Aug 2024

Mandiant and Google Workspace Trust and Safety observed a marked rise in phishing attacks targeting U.S. universities beginning August 2024, forming part of multi-year campaigns dating back to at least October 2022

The academic calendar is weaponized

Phishing waves align with key academic events, such as semester commencements, enrollment periods, and financial aid deadlines, to exploit institutional workflows and timing vulnerabilities.

Three key campaign vectors

- Google Forms misuse —malicious forms hosted on compromised educational domains.
- Cloned login portals—replicas of university sign-in pages, often hosted on external infrastructure.
- Two-step targeting—distinct campaigns aimed separately at students and faculty/staff

Scope and scale

At least 15 U.S. universities have been targeted, with thousands of credential-harvesting attempts per month

Goal: credential theft and financial fraud

Attackers aim to harvest login credentials from students and staff, then convert access into account takeovers or facilitate fraudulent redirects of payments (tuition, grants, P-card purchases)

Threat actor diversity

While attribution is still evolving, campaigns include opportunistic cybercriminals and resonant nation-state APTs (Iran's APT42 targeting academia, Russia-aligned UNC6293 aiming at academics)

Large Language Model (LLM) driven spear-phishing emerges

Academic research shows large organizations, including universities, are now vulnerable to hyper-targeted phishing using LLM-generated content, bypassing traditional filters and achieving near-perfect F1 detection scores only with advanced machine learning (ML) based solutions.

What do we need to do?

Enhance awareness and training

Implement phishing awareness tailored to academia. Emphasize recognizing fake Google Forms and cloned login portals. Conduct regular simulated campaigns timed to coincide with key academic events.

Strengthen technical defences

Enforce DMARC, DKIM, and SPF to block domain spoofing. Deploy advanced scanning for known phishing URLs, especially Google Forms and fake university domains.

MFA adoption and enforcement

Enforce phishing-resistant MFA (FIDO2). Where unavailable, enable per-session SMS-based second factors, which block ~96% of phishing threats.

Credential compromise monitoring

Integrate account monitoring to detect anomalous access (geo-irregularity, odd login times) or brute force attempts.

Threat intel sharing

Exchange phishing indicator of attacks (IOAs), compromised domains, and TTPs via EDUCAUSE, REN-ISAC, and NSF-funded cybersecurity coalitions.

Incident playbooks for academia

Develop response playbooks for compromised student and faculty credentials, covering containment, password resets, account audits, and sanctioning of fraudulent attempts.

Secure Google Forms usage

Audit form activity. Block public or form-published links and enforce access control. Monitor domain hosts for impersonation.

Web proxy and DNS filtering

Implement filters to block access to known phishing infrastructure. Use analytics to alert on suspicious form access from campus IP ranges.

Use deception and sandboxes

Deploy honeypot forms and trap accounts. Redirect clicked phishing links through sandboxed environments to disrupt attacker workflows.

Post-incident review and adjustments

Following incidents, analyze phishing vectors, update training, improve detection rules, and share lessons learned.

Hacktivist Threats to Operational Technology (OT)

What do I need to know?

Hacktivist threats to OT remain low to moderate but evolving

Mandiant assesses with high confidence that most hacktivist campaigns targeting operational technology (OT) assets are unsophisticated and primarily seek publicity. However, groups with ties to state-sponsored threat actors—such as Iran, Russia, and Israel—have demonstrated capabilities resulting in real-world impacts.

OT access is often opportunistic and enabled by misconfigurations

The most frequent avenue of access involves internet-exposed OT assets with weak authentication or misconfigured services. Claims often include screenshots or video of manipulated human-machine interfaces (HMIs) and remote terminal units (RTUs), sometimes resulting in disruptions such as tank overflows or altered system states.

Key actors and affiliations

- **Pro-Iranian/Pro-Palestinian:** CyberAveng3rs, Handala Hack Team, Homeland Justice, Jerusalem Electronic Army—some linked to the IRGC or MOIS—target water treatment, energy, and port infrastructure.
- **Pro-Israeli:** Predatory Sparrow conducts precision OT operations, allegedly disrupting Iranian rail and energy sectors.
- **Pro-Russian:** CyberArmyofRussia_Reborn (CARR) and FRwL Team have demonstrated manipulation of OT in Western countries, including U.S. water systems and French dams.
- **Pro-Ukrainian:** Team OneFist targets Russian OT infrastructure with limited impact.
- **Other:** GhostSec has developed custom malware (GHOSTLOCKER, GHOSTSTEALER) and ICS-specific exploits, claiming attacks against Modbus and IEC-104 devices.

False-front personas and information operations (IO)

Groups like CARR and Homeland Justice operate as plausible-deniability proxies for state activity. These personas amplify unverified or overstated claims to influence perceptions, particularly during geopolitical conflict (Ukraine-Russia, Israel-Hamas).

Toolset evolution includes Industrial Control Systems (ICS) specific malware

Several groups have begun developing or adapting OT-specific modules. GhostSec, for example, claimed the first ransomware operation against an RTU in 2023. Tooling includes known ICS Metasploit modules, web console bypasses, and "Killbus" utilities against Modbus systems.

OT attacks primarily pose a nuisance, but risks are growing

Most incidents do not involve complex intrusion chains or the deployment of malware. However, as convergence between IT and OT environments continues, and as hacktivists mature their toolsets, the risk of real-world OT impact rises, especially for organizations aligned with contentious geopolitical or ideological causes.

What do we need to do?

Reduce internet exposure

Inventory and isolate all OT assets from the public internet unless explicitly required. Apply network segmentation and firewall controls to OT networks. Monitor Shodan and Censys listings for exposed devices.

Secure HMI/RTU interfaces

Disable default credentials. Apply strict access controls (VPN-only access, MFA where possible). Ensure OT-facing HMIs and dashboards are not externally routable.

Monitor for prepositioning

Collect telemetry from OT assets, including logs, failed login attempts, configuration changes, and user access anomalies. Deploy passive intrusion detection system (IDS) solutions for ICS/SCADA environments.

Deploy honeypots and deception

Use OT-specific honeypots (simulated Programmable Logic Controllers, or PLCs) to detect reconnaissance or low-sophistication access attempts. Monitor for screenshot exfiltration behaviors or access to fake dashboards.

Enhance situational awareness

Regularly review actor claims and underground chatter for targeting indicators. Correlate with geopolitical flashpoints and physical threats (water systems in conflict zones).

Test OT incident response

Update incident response (IR) playbooks to include hacktivist scenarios, such as HMI defacement, data leaks, and social media amplification. Conduct cross-disciplinary tabletops with engineering and PR teams.

Patch and harden gateway devices

Update the firmware and software of devices such as CalAmp routers, Moxa NPorts, or Berghof PLCs. Disable any unneeded services (Telnet, SSH). Lock down web consoles.

Threat hunting for exploit modules

Scan internal environments for the use of publicly known tools, such as METEOR, CHILLWIPE, or ICS-specific Metasploit payloads. Incorporate threat hunting for GhostSec and CARR TTPs.

Geo-targeted defenses

Deploy rate-limiting, geo-fencing, and access filtering for users from high-risk geographies. Use anomaly detection tuned for OT protocols (Modbus, IEC-104).

Integrate with ISAC/ISA resources

Join and contribute to Information Sharing and Analysis Centers (ISACs) such as E-ISAC, Water-ISAC, or industrial alliances. Leverage ISA/IEC 62443 standards for ICS cybersecurity governance.

Cybercrime as a National Security Threat

What do I need to know?

Cybercrime dwarfs state-sponsored threats by volume

In 2024, financially motivated intrusions accounted for nearly four times more incident responses by Mandiant Consulting than state-sponsored ones. Despite lower visibility within national security circles, their volume and potential impact are comparable.

Critical infrastructure and public services are at risk

Ransomware and extortion attacks regularly target energy grids (Colonial Pipeline 2021, ARA refinery 2022, Petro-Canada 2023) and hospitals, where operational disruptions directly affect citizens' access to essential services.

Healthcare data exfiltration is accelerating

The hospital subsector's share of DLS postings has doubled over three years, while the number of leak sites grew by nearly 50% year-over-year, emphasizing sustained criminal interest in sensitive medical information.

Blurring lines with nation-state operations

Cybercriminal tools and services bolster state operations. Russian GRU-aligned APT44 and CIGAR have used crimeware tools for espionage/disruption in Ukraine, while Iran and China similarly co-opt ransomware gangs; North Korea uses cybercrime directly for regime funding.

Cumulative impact strains national readiness

High incident volume depletes cybersecurity workforce resilience, erodes readiness for state-level campaigns, and creates a systemic drag on national defenses.

Transnational and decentralized challenge

Cybercrime's agility and cross-border organization render takedowns only temporarily effective. New actors rapidly fill the voids left by disrupted groups.

What do we need to do?

Elevate cybercrime as a national security priority

Recognize the strategic threat posed by cybercrime. Allocate intelligence, incident response, and law enforcement to financially motivated attacks alongside state threats.

Strengthen cross-border cooperation

Enhance international partnerships (INFOCOM, Europol, INTERPOL) for coordinated cybercriminal takedowns, joint investigations, and evidence sharing—limited takedowns yield short-term success.

Integrate cybercrime into defense planning

Expand national and sector-level threat assessments to include financially motivated actors. Factor ransomware and DLS threats into critical infrastructure resilience planning.

Disconnect criminal services from state-aligned operations

Target the crimeware ecosystem (marketplaces, malware-as-a-service), disrupting the supply chain that enables state-aligned campaigns.

Support ecosystem resilience

Invest in public awareness, healthcare preparedness (backup systems), and energy utility continuity. Tailor training to non-digital sectors critical to public welfare.

Prioritize workforce resilience

Expand federal cybersecurity staffing, including Mandiant-like defensive surge teams. Implement measures to combat burnout and capacity shortfalls.

Enhance intelligence fusion

Centralize intel on financially motivated actors in national centers (CISA National Cybersecurity and Communications Integration Center), with real-time sharing to public-sector security operation centers (SOCs) and critical infrastructure operators.

Invest in automation and AI-assisted defense

Deploy automated detection of ransomware and DLS activity with AI tools to bolster SOC efficiency and counter the scale of criminal operations.

The Ransomware Ecosystem

What do I need to know?

Ransomware operations remain highly modular and resilient

Mandiant assesses with high confidence that the ransomware ecosystem is sustained by a decentralized supply chain: access brokers, tooling developers, infrastructure providers, and money laundering services operate as independent layers, making disruption efforts temporary and incomplete.

DLSs are central to extortion

Most major ransomware groups, whether RaaS or exclusive, operate a DLS to pressure victims. These platforms have grown in number and scope, facilitating multi-vector extortion strategies that include encryption, data theft, harassment, and reputational damage.

Affiliate-driven operations dominate

The rise of RaaS has enabled scalability. Affiliates conduct the intrusions, while core developers provide the malware and infrastructure. Prominent RaaS models include LockBit, ALPHV, and Qilin. These models often evade enforcement actions by rebranding or forming splinter groups.

Key threat actors overlap with national interests

Some groups (UNC2165, UNC5537) serve both financially motivated and state-aligned agendas. For example, North Korean and Russian-aligned actors have used ransomware to finance operations or enable strategic access.

Takedowns cause disruption but not deterrence

Law enforcement operations (ALPHV takedown) temporarily lower activity levels but are followed by adaptive behaviors—rebrands, rebuilds, or redirection to new infrastructure (, RansomHub rising after ALPHV disruption).

Victimology includes critical infrastructure and the public sector

Ransomware attacks on municipalities, healthcare systems, and education highlight the operational impact. Critical services have been disrupted even when "no-target" rules are publicly claimed by actor groups.

What do we need to do?

Disrupt the ecosystem, not just the brand

Target enablers: access brokers, bulletproof hosting, crypter services, and laundering networks, not just front-end groups like ALPHV or LockBit.

Enforce financial pressure

Expand blockchain tracing and seizure operations. Increase international cooperation to sanction mixers, laundering exchanges, and ransomware cashouts.

Harden public-facing assets

Audit for exposed services (for example, Remote Desktop Protocol (RDP), enforce patch management, and disable unnecessary protocols. Use threat intel to monitor for initial access broker listings.

Segment and backup critical assets

Implement segmented backups, offline recovery, and immutable storage. Assume compromise and prioritize recovery planning alongside prevention.

Improve DLS visibility

Integrate DLS feeds into SOC workflows. Monitor for third-party compromise (vendors, affiliates) to detect supply chain exposure.

Degrade affiliate scalability

Focus on disrupting affiliate onboarding, credential harvesting, and command/control delivery. Use Yet Another Recursive Acronym (YARA) rules and sandboxing to detect affiliate-used variants.

Coordinate national response

Establish response frameworks across government, law enforcement, and healthcare/public sector entities. Create ransomware-specific contingency plans with cross-sector applicability.

Support long-term resilience

Fund proactive cyber hygiene initiatives (endpoint hardening, MFA adoption), especially in under-resourced municipal and healthcare environments.

Integrate ransomware threat intel: Feed IOCs, TTPs, and DLS data into centralized platforms (CISA's Joint Cyber Defense Collaborative) for shared visibility and rapid incident correlation.

Drive-By Compromises

What do I need to know?

Drive-by compromise techniques are escalating in scope and sophistication

Threat actors are increasingly using search engine optimization (SEO) poisoning, malvertising, and compromised websites to deliver malware through drive-by methods. These techniques target users during routine web activity, exploiting common browsing behaviors and abusing trusted brand imagery.

Multiple distribution vectors are often combined

Campaigns now frequently blend phishing emails, SMS, social media lures, and voice phishing (vishing) with drive-by compromise, thereby increasing success rates. This multi-vector approach reflects the adversary's adaptation to improved enterprise defenses.

Social engineering is central to initial access

Actors consistently exploit human trust to bypass controls. Examples include impersonating IT help desks, using fake error messages (ClickFix), and deploying deepfake media to convincingly spoof senior executives or trusted services.

Public sector and critical services are key targets

Municipalities, NGOs, and defense-related sectors have been victimized by campaigns leveraging deceptive content related to elections, military conflicts (Russia-Ukraine, Israel-Hamas), and public service brands. APT groups, including APT42 and UNC1549, actively use these themes in high-impact spear-phishing operations.

AI-enabled social engineering is gaining traction

Threat actors are beginning to use generative AI for creating phishing lures and deepfake voice/video content. Some criminal operations now offer deepfake tools to impersonate executives for fraud or lateral movement within victim networks.

What do we need to do?

Detect and block drive-by delivery vectors

Monitor for SEO manipulation, malvertising redirection chains, and abuse of common CMS platforms (WordPress). Integrate browser telemetry with threat detection systems.

Strengthen IT help desk verification processes

Implement call-back verification and enforce multifactor resets only via internal secured systems. Train staff to flag impersonation attempts.

Combat lure credibility

Regularly update users on current phishing themes (tax season, job offers, conflict-related decoys). Emphasize critical evaluation of inbound content, even from seemingly legitimate sources.

Deploy anti-deepfake controls

Integrate speaker verification and visual verification layers into high-risk workflows. Monitor for signs of audio/video manipulation in high-value communication.

Red team and simulate layered social engineering

Test user responses to multi-channel attacks (email followed by chat or phone). Include ClickFix-style payload simulations in tabletop exercises.

Secure web interactions

Use browser isolation for high-risk categories (technical manuals, software downloads). Deploy inline web content inspection and disable unnecessary script execution.

Limit exposure in digital ecosystems

Monitor for unauthorized use of branding on social platforms, phishing kits mimicking agency login pages, or impersonation in SEO results.

Enhance phishing-resistant MFA adoption

Prioritize FIDO2/WebAuthn deployment. Monitor for misuse of legacy MFA methods that are susceptible to fatigue or token theft.

Track threat actor innovations

Subscribe to threat intel feeds with tagging for drive-by, malvertising, and social engineering operations. Monitor adoption of new TTPs like ClickFix or AI-generated lures across adversary clusters.

Bibliography

Public Facing

M-Trends 2025

https://cloud.google.com/blog/topics/threat-intelligence/phishing-targeting-higher-education?e=48754805

https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day

https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai

https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger

https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat

https://cloud.google.com/blog/topics/threat-intelligence/chinese-espionage-tactics?e=0

https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers?e =48754805

https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement?e=48754805

Non-Public Facing

Russia-Linked 'Hacktivist' Group Cyber Army of Russia Reborn Claims Manipulation of Texas Water Facilities' OT.pdf

Overview of Hacktivist Threats to OT.pdf

Country Snapshot: The United States (Q1 2025).pdf

Healthcare Remains a Prime Target for Ransomware Attacks in 2024.pdf

The Ransomware Ecosystem Recalibrates: 2004 Ransomware Tactics, Techniques, and Procedures.pdf

It's a Trap! Social Engineering Trends for 2024 and Outlook for 2025.pdf

If your organization suspects a cyber incident, or you are experiencing a security breach, please contact Mandiant for Incident Response Assistance.

A special thank you to these contributors

Meegan Arpino Jamie Parker Jeremy Rosado Jose Valerio

Google Cloud

For more information, visit **cloud.google.com**.