THREAT RESEARCH

Myanmar Cyber Threat Landscape, 2016–2026: A Public-Source Review

A source-qualified review of selected cyberespionage, data exposure, cyber-enabled fraud, and targeted malware reporting connected to Myanmar from 2016 to 2026.

By Malware INFO Team September 1, 2026 20 min read

Skip to content

Executive summary

Myanmar's digital environment changed sharply between 2016 and 2026. Public reporting from researchers, incident-response organizations, newsrooms, international bodies, and affected organizations describes a varied record: malware hosted on trusted government infrastructure, website defacement, access-control failures, exposed institutional records, targeted cyberespionage, credential and document theft, and a regional online-fraud economy tied to severe human harm.

These events should not be collapsed into one trend line or one actor story. Cyberespionage is not the same phenomenon as hacktivism. A reported data leak does not establish the same facts as an analyst-observed malware chain. Organized online fraud has different incentives, victims, and evidence from a government-focused intrusion. This review therefore separates event category, affected sector, technique, and evidence class.

Research cutoff: September 1, 2026. The record below is a **selected public-source record**, not a national incident count or national incident prevalence. It cannot show how many

Skip to content

ver detected, never disclosed, or were reported only to private parties. It also cannot establish the intent behind every observed tool or infrastructure relationship.

Three conclusions are nevertheless defensible:

1. Trusted channels matter. Official websites, downloadable archives, document-like containers, and legitimate loading behavior repeatedly appear in the public record.
2. Identity and information are recurring targets. Documents, browser credentials, session cookies, webmail, personnel records, registration data, and application records all appear across different cases.
3. Evidence quality varies. Technical observation, official acknowledgement, secondary reporting, and analytical assessment answer different questions and must remain visibly distinct.

Timeline of fourteen selected public-source Myanmar cyber records from 2016 through 2026, labeled by category, sector, and evidence class

Skip to content

chart-eligible records in this review. Multiple records in one year do not imply higher national prevalence; the figure reflects the selected source set and its publication

history.

Scope and method

This paper began with themes suggested by a presentation supplied for editorial planning, but the presentation is not cited as evidence. Every retained claim was checked against an accessible public source. Unsupported specificity was removed. For example, a narrow sector claim associated with a 2019 campaign was not present in the verified source and does not appear here.

Sources were selected when they provided a clear Myanmar relationship, a usable date, an identifiable publisher, and wording that could be bounded. Priority was given to original technical research, official advisories, organizational acknowledgements, and official policy material. Contemporary news reporting was retained where it documented an important event unavailable in a stronger public source, but its limitations remain attached.

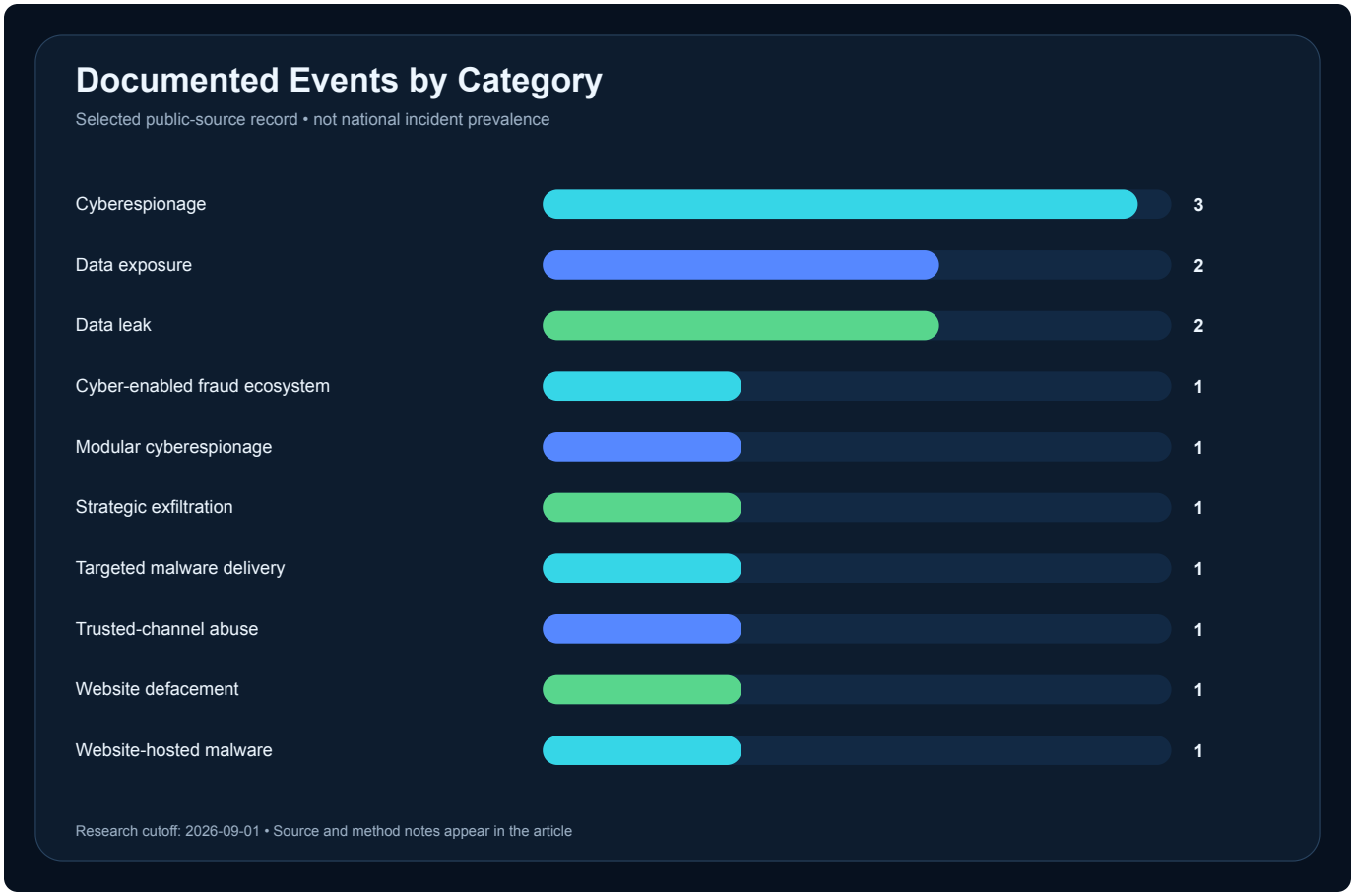
The evidence labels used in this review are deliberate:

- **Technical observation** means a research team described artifacts, infrastructure, tools, or a delivery chain it examined.
- **Official acknowledgement** means an affected organization reportedly described an incident or scope.
- **Reported breach or leak** means a publication documented claims or observed effects without giving this research independent access to the underlying incident evidence.
- **Analytical assessment** means a research or policy source combined observations into a broader judgment.
- **Suspected or linked attribution** preserves explicit uncertainty about an actor or campaign relationship.

One publication can contain several technical details, but those details do not become independent corroboration simply because they are numerous. Likewise, an advisory that repeats a named operation can provide valuable defensive guidance without independently

Skip to content ntity.

No leaked dataset, personal record, customer evidence, malware binary, or credential collection was downloaded or inspected for this paper. The research uses descriptions available on public pages and documents. Links lead to the publishers, not to leaked material or executable samples.



Bar chart grouping the selected Myanmar cyber records by event category, with a warning that counts reflect source selection rather than national frequency

Figure 2. Categories help prevent unlike events from being treated as one measurement. Counts describe this review's selected records only.

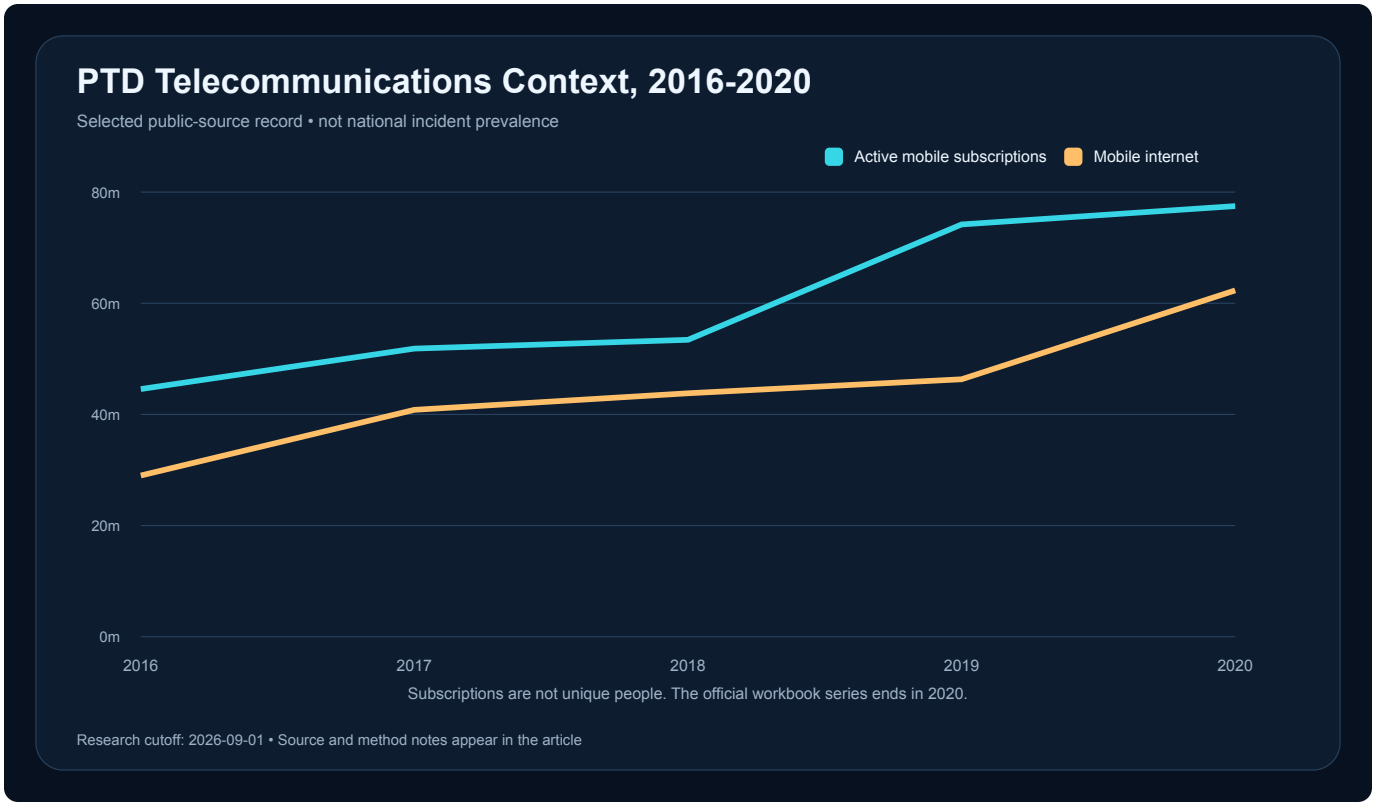
Telecommunications context: expanding connectivity, not a risk score

The Posts and Telecommunications Department (PTD) provides an official Statistical

Skip to content and linked workbook. Its consistently labeled annual series records active

mobile subscriptions rising from 44.56 million in 2016 to 77.48 million in 2020, while mobile-internet subscriptions rise from 29.00 million to 62.31 million over the same period.

Those values provide infrastructure context: more subscriptions and more connected services create a larger environment in which digital identity, availability, and institutional trust matter. They do **not** measure attacks, unique people, national cybersecurity maturity, or causation. One person can hold multiple subscriptions, and the official series used here ends in 2020. Other workbook fields with formatting anomalies were excluded rather than normalized speculatively.



Line chart of PTD active mobile and mobile-internet subscriptions in millions from 2016 to 2020, noting that subscriptions are not unique people

Figure 3. Official PTD connectivity context. The two lines are not incident-volume or security-maturity measures.

2016–2019: trusted websites, public disruption, and

Skip to content **trusion**

2016: malware on election-related web infrastructure

Citizen Lab's April 2016 investigation documented malware samples hosted on infrastructure associated with Myanmar's Union Election Commission. The report connected material to its UP007 investigation and discussed a Trochilus-linked sample described by ASERT. The defensible observation is that trusted public web infrastructure was used to host suspicious material. Hosting alone does not reveal every victim, the complete compromise path, or a fully proven objective.

The case established an early theme for the decade: users may assign trust to an official domain, but domain ownership does not guarantee that every hosted file is trustworthy. Defenders need independent file identity, reputation, signing, and behavior evidence even when content originates from a familiar website.

2017: website defacement and crisis-linked hacktivism

Democratic Voice of Burma reported in September 2017 that several Myanmar government websites were targeted and displayed altered content. This is a public-trust and availability event, not automatically an espionage case. The contemporary report did not provide an independently verified intrusion path or a complete inventory of affected sites, so attribution should remain at the level stated by the source.

Defacement is sometimes dismissed because it can be visually obvious and operationally short-lived. That is a mistake. It demonstrates loss of control over a public communication channel and can create misinformation, reputational harm, or a path to further compromise. But it should not be counted as equivalent to credential theft or covert document collection.

2019: Myanmar in wider APT reporting

Kaspersky's 2019 APT review described HoneyMyte targeting governments including Myanmar and separately noted a Myanmar bank compromised by BlueNoroff. This places Myanmar organizations within the vendor's campaign assessment, but the review spans multiple actors, targets, and countries. It is not evidence that every described tool affected Myanmar, or that the selected cases represent nationwide activity.

Skip to content

The practical lesson is to preserve campaign context without importing unsupported detail. Vendor attribution can be useful for comparing tooling and infrastructure, yet local defenders still need endpoint, identity, network, and server evidence from the affected environment before deciding what happened there.

2020–2022: access control, trusted delivery, and strategic collection

2020: COVID-19 QR-pass exposure

KrASIA reported in October 2020 that changing digits in a URL could allow users to view or alter other records in a Yangon COVID-19 QR-pass system. The reported weakness concerns object-level access control: an application must verify that the current user is authorized for the specific record requested, not merely that a record identifier exists.

This research did not reproduce the weakness or access affected records. The case is retained because it illustrates that cyber risk is not limited to malware. A simple authorization failure in a high-demand public service can expose identity and travel-related data while undermining confidence in an emergency system.

2021: a trusted download channel reportedly delivers a loader

The Record reported in June 2021, citing ESET analysis, that a Myanmar Unicode font archive offered through the president's office website had been modified to include an `Acrobat.dll` Cobalt Strike loader. The public report supports the trusted-channel-abuse observation; it does not let this paper independently reconstruct the server compromise, determine how many users executed the archive, or strengthen the source's qualified attribution.

For defenders, official distribution paths need the same release controls expected from software repositories: controlled build provenance, hashes, signing where appropriate, change monitoring, least-privileged publishing, and rapid revocation. For investigators, a familiar filename or official referrer is context—not proof that the payload is benign.

Skip to content

2021: company-registration data reportedly released

KrASIA also reported a claimed 330.5 GB collection associated with roughly 120,000 companies in DICA/MyCO systems. The article described company and officer records and attributed collection claims to an activist group and scraper. This review did not obtain or validate the released material, so the volume, method, and completeness remain source-reported.

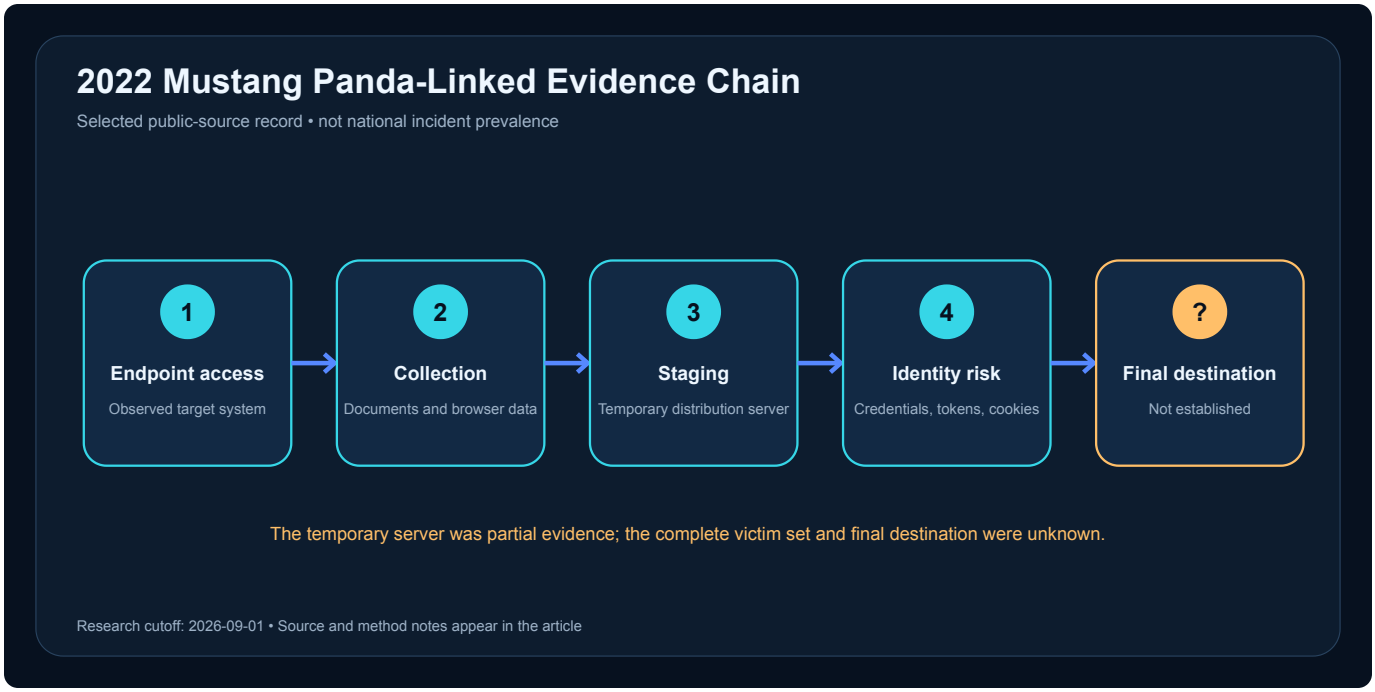
The event highlights an important distinction between public availability and safe reuse. Records may contain information that was individually accessible or intended for limited administrative use, yet bulk aggregation changes the risk. Searchability, linkage, persistence, and scale can increase exposure for directors, officers, organizations, and public institutions.

2022: temporary infrastructure exposes a larger collection chain

Avast Threat Research, now published by Gen Digital, described a temporary distribution and storage server linked by the researchers to Mustang Panda. Their observation included Myanmar-related government, diplomatic, military, activist, and identity material, with daily gigabyte-scale staging. Reported content included documents, recordings, webmail dumps, passport scans, stored browser credentials, tokens, and cookie sessions.

This is one of the strongest technical observations in the selected record, but it still has a boundary. A temporary server is a window into part of an operation. It does not necessarily reveal the complete victim set, every collection method, the duration of access, or the final destination of the data.

Skip to content



Five-stage diagram of the 2022 observed incident chain from endpoint access through collection, browser identity theft, temporary staging, and an unknown final destination

Figure 4. An evidence-bounded interpretation of the 2022 observation. The unknown final destination is part of the finding, not a gap to fill with speculation.

The case also shows why browser artifacts deserve incident-response priority. A stolen password may be reset; a live session cookie or token can sometimes provide continued access until revoked. Response should therefore consider session invalidation, token rotation, mailbox rules, identity-provider logs, trusted-device enrollment, and evidence-preserving endpoint collection—not password changes alone.

2023–2026: regional cyber-enabled crime and continuing targeted campaigns

2023: cyber-enabled fraud as a human-security problem

The United Nations Office on Drugs and Crime documented Myanmar within a Southeast Asian ecosystem of casinos, online scams, financial fraud, and trafficking in persons for forced criminality. The report is qualitative and explicitly notes limited statistical data. It should not be

Skip to content

precise Myanmar incident count.

This category must remain separate from state-linked espionage reporting. The actors, economics, operational models, and victim harms differ. At the same time, enterprise defenses still intersect with the ecosystem: impersonation, deceptive recruitment, social engineering, account takeover, payment abuse, and identity misuse can reach employees and customers across borders.

2024: suspected government targeting remains qualified

CERT-EU's February 2024 brief summarized reporting that Myanmar's ministries of Defence and Foreign Affairs were suspected targets between November 2023 and January 2024. The brief used qualified language: Mustang Panda was suspected and backdoor deployment was described as likely. This paper preserves those qualifiers because the source is a CERT summary rather than direct incident evidence from the ministries.

Analysts should resist turning repeated campaign names into certainty. Attribution can carry several levels: shared malware, shared infrastructure, behavioral resemblance, a vendor assessment, government assessment, or direct operational evidence. Public reporting often exposes only part of that ladder.

2025: a modular toolset, but a narrow starting sample

In a two-part April 2025 investigation, Zscaler ThreatLabz documented ToneShell and StarProxy and PAKLOG, CorKLOG, and SplatCloak. The investigation began with two machines at an organization in Myanmar and described DLL side-loading, remote-access and proxy capabilities, keylogging, and attempts to impair security telemetry.

The detail is valuable for detection engineering, but two starting machines do not establish prevalence across a country. Nor does a campaign tool catalog prove that every component executed on every target. Defenders should convert the report into testable hypotheses—specific file relationships, loading behavior, persistence, network destinations, and telemetry gaps—then confirm or reject them using local evidence.

Also in 2025, Burma News International reported exposure of civil-service personnel information including names, positions, departments, and home addresses, followed by tighter

Skip to content

ministry security measures. No raw records were obtained for this review, and the technical path, exact volume, and responsible actor remain unverified.

2026: continuing government-sector targeting

Kaspersky reported in January 2026 new HoneyMyte campaigns that included Myanmar government-sector targeting. The publication described CoolClient variants, browser-login data stealers, DLL side-loading, backdoors, and reconnaissance scripts across several countries and campaigns. It does not show that every component applied to every Myanmar target.

In June, The Star reported an AYA Bank acknowledgement: limited non-financial data from a legacy application portal was reportedly affected, while core banking systems were said to be unaffected. Both scope statements remain attributed to that reported acknowledgement because this paper did not obtain the original incident record or establish a technical intrusion path.

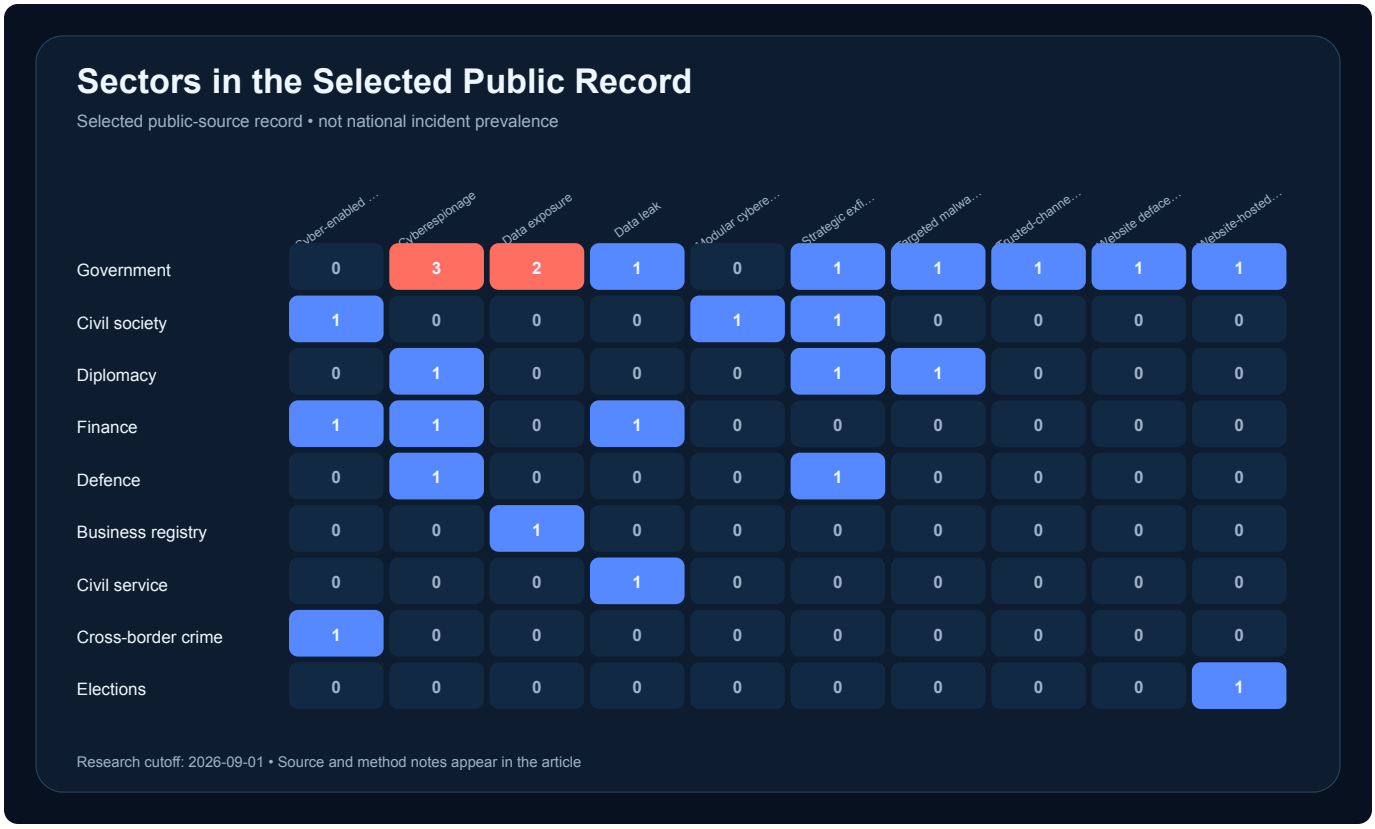
In August, Seqrite Labs documented Operation QUICSILVER, a targeted delivery chain aimed at Myanmar diplomatic interests. The report described a VHD container, LNK execution, split-payload reconstruction, and a Go backdoor. Seqrite used the qualified term “China-nexus”; this review does not rewrite it as confirmed national attribution.

Myanmar's national cyber emergency response team later published MM-CERT defensive guidance for the operation. That official alert is operationally important for local defenders. It is not, by itself, independent proof of a named actor, a national victim count, or every technical detail in the original research.

Which sectors and trust relationships recur?

Government and government-adjacent organizations appear frequently in the selected record, followed by finance, diplomacy, civil society, health, elections, and business-registration contexts. The distribution partly reflects what researchers and newsrooms can observe and choose to publish. It should not be interpreted as a ranking of every sector's real-world risk.

Skip to content



Matrix showing selected event categories across government, finance, diplomacy, civil society, health, elections, and business-registry sectors

Figure 5. Sector/category intersections in the selected public record. A blank cell means no retained record in this dataset, not that the sector experienced no incidents.

Across sectors, several trust relationships recur:

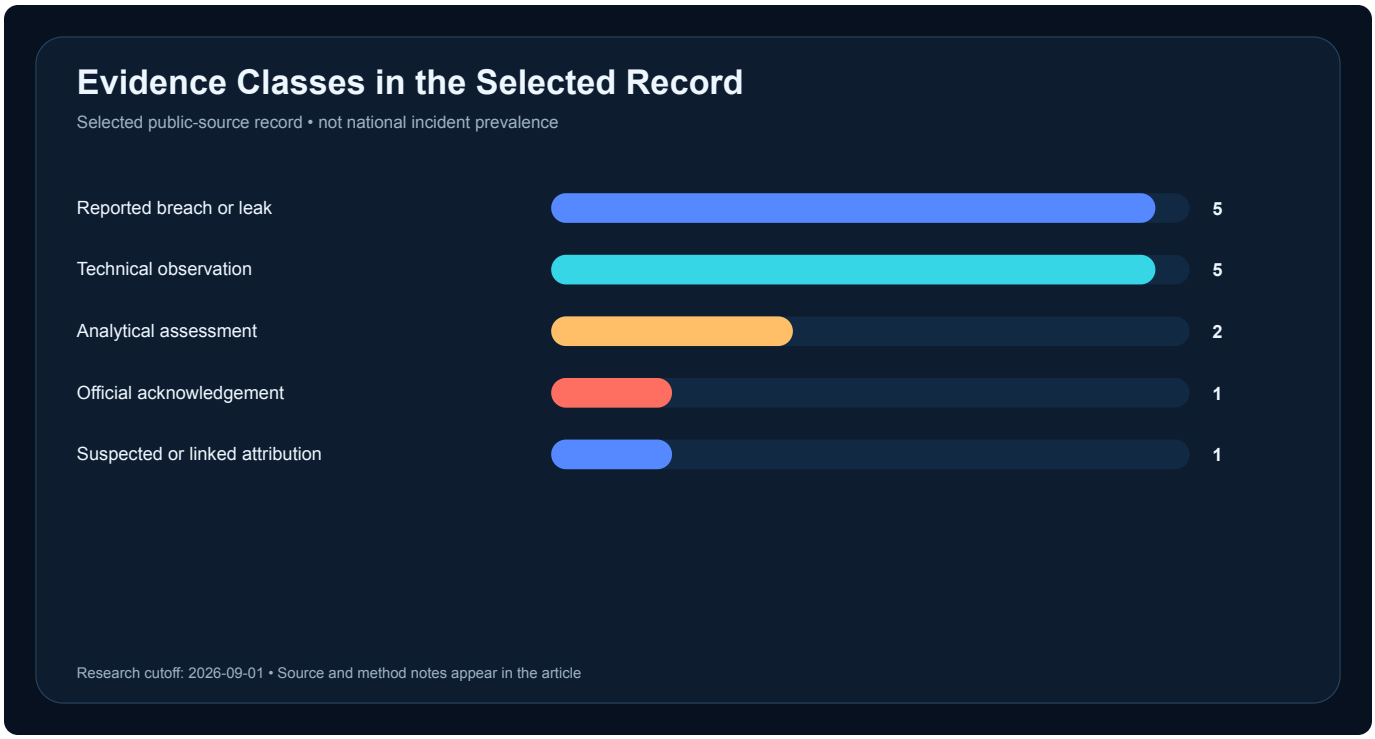
- **Official-channel trust:** government sites and downloadable packages can be abused.
- **Identity trust:** credentials, session tokens, cookies, personnel data, and identity documents can enable access or harm beyond the first affected system.
- **Application authorization:** a valid session is insufficient when record-level access checks are weak.
- **Software-loading trust:** DLL side-loading and document-like delivery can make malicious execution appear adjacent to legitimate software or user activity.
- **Public-information trust:** defacement and data release can damage confidence even when the event is not covert espionage.

Skip to content

These patterns support controls that cross product boundaries: asset ownership, secure publishing, identity logging, token revocation, application authorization testing, endpoint visibility, egress monitoring, resilient backups, and a response process that preserves evidence before remediation destroys it.

Evidence class changes what a claim can prove

The chart below is not a confidence score. A technical report may contain high-quality artifact evidence yet still leave actor identity uncertain. An official acknowledgement may accurately describe business impact while omitting technical detail. Secondary reporting can document a socially significant event without providing forensic access.



Bar chart counting technical observations, reported breaches or leaks, analytical assessments, suspected attribution, and official acknowledgement in the selected record

Figure 6. Evidence-class counts for the selected records. The classes describe source basis; they are not Malware INFO verdicts and do not rank publisher credibility.

A practical reading discipline is to ask four questions for each claim:

Skip to content

1. **What was directly observed?** Examples include a file, server, delivery chain, altered web page, or application behavior.
2. **Who observed it?** An affected organization, technical research team, public agency, journalist, or third party may have different access.
3. **What remains inferred?** Campaign ownership, intent, victim scope, and final data destination are often assessments rather than direct observations.
4. **What is unavailable?** Private telemetry, incident timelines, forensic images, disclosure constraints, and unreported events can materially change the picture.

Defensive implications for Myanmar organizations

The decade does not support one universal detection rule. It supports a layered operating model.

Protect trusted publishing paths. Inventory who can change public websites, software packages, fonts, documents, and download archives. Monitor changes, preserve version history, and publish verifiable hashes or signatures where practical. Treat an unexpected server-side file change as an incident requiring scope analysis.

Harden identity beyond passwords. Use phishing-resistant multifactor authentication where feasible, restrict legacy authentication, monitor abnormal sessions, and make token/session revocation part of playbooks. Browser credential stores and active sessions are evidence targets, not merely user conveniences.

Test authorization at the object level. Public-service portals should verify entitlement for every requested record and action. Rate limits and unpredictable identifiers can help, but neither replaces authorization. Testing must avoid accessing real users' records without authority.

Monitor legitimate execution relationships. DLL side-loading and trusted-binary abuse require visibility into which process loaded which module, from which path, with what signer and hash, and what happened next. A tool name or export name alone does not establish

Skip to content ır; correlate file, process, memory, registry, and network evidence.

Plan for evidence preservation. Decide in advance which logs, memory captures, endpoint packages, cloud audit records, and network records can be collected lawfully. Evidence can contain credentials, personal data, and sensitive organizational content; access, retention, transfer, and disclosure require controls.

Report and coordinate. MM-CERT publishes alerts, advisories, activities, and an incident-reporting route. Organizations should align escalation with legal obligations, sector rules, contracts, and the sensitivity of affected data. A public alert can improve readiness, but public disclosure should not precede containment or expose victims unnecessarily.

Limitations

This paper is constrained by public availability, publisher access, language, archive stability, and disclosure practices. The absence of a public report is not evidence that an incident did not occur. Publication dates may differ from incident dates, and a year with more retained records may simply have better reporting.

The event categories are editorial groupings, not a universal taxonomy. Sector labels can overlap. Campaign and actor names are reproduced only at the confidence level used by their sources. No attempt was made to identify private victims, reproduce vulnerabilities against live systems, obtain leaked records, execute malware, or contact suspected infrastructure.

The PTD chart ends in 2020 and measures subscriptions rather than unique people. The UNODC report uses a qualitative regional methodology. Several breach and leak entries rely on secondary reporting rather than primary forensic material. These limitations make the review suitable for defensible orientation and research planning—not for calculating a national incident rate, assigning liability, or declaring attacker intent.

Conclusion

From 2016 through the September 2026 cutoff, Myanmar-linked public reporting shows repeated pressure on institutional trust: trusted websites and archives, government and

Skip to content ints, browser identities, public-service applications, business and personnel

records, and financial portals. It also shows that cyber harm extends beyond malware to application design, bulk data exposure, account abuse, public disruption, and organized online fraud.

The strongest analytical habit is separation. Separate observation from attribution. Separate an exposed server from a complete operation. Separate subscriptions from people and connectivity from incident volume. Separate a reported leak from independently examined evidence. When those boundaries remain visible, public-source research becomes more useful to defenders—and less likely to manufacture certainty that the evidence cannot support.

References

- Citizen Lab, Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaigns, April 18, 2016.
- Democratic Voice of Burma, Hackers target govt websites in cyber spillover from Arakan crisis, September 5, 2017.
- Kaspersky Securelist, APT review: what the world's threat actors got up to in 2019, December 4, 2019.
- KrASIA, Cyberattacks hobble Myanmar's COVID-19 QR pass system, expose massive security flaws, October 1, 2020.
- KrASIA, Massive data trove from 120,000 Myanmar companies surface online in Wikileaks-style release, February 22, 2021.
- The Record, Backdoor malware found on the Myanmar president's website, again, June 3, 2021.
- Gen Digital / Avast Threat Research Team, Hitching a ride with Mustang Panda, December 2, 2022.
- UNODC, Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia, September 2023.
- Skip to content er Security Brief 24-03 — February 2024, February 2024.

- Zscaler ThreatLabz, Mustang Panda: ToneShell and StarProxy and PAKLOG, CorKLOG, and SplatCloak, April 16, 2025.
- Burma News International, Myanmar junta tightens data security after massive leak of non-CDM staff records, September 8, 2025.
- Kaspersky, Kaspersky reveals new HoneyMyte APT campaigns and toolset, January 27, 2026.
- The Star, Old AYA Bank application portal suffers limited data leak in Myanmar; core banking systems unaffected, June 26, 2026.
- Seqrite Labs, Operation QUICSILVER: China-Nexus Actor Targets Myanmar Diplomats via VHD-Delivered Go Backdoor, August 17, 2026.
- MM-CERT, Operation QUICSILVER defensive guidance, August 28, 2026.
- Posts and Telecommunications Department, Statistical Information, workbook accessed September 1, 2026.

Myanmar | Cyber Threat Intelligence | Public-Source Research | APT | Data Exposure | Cybercrime

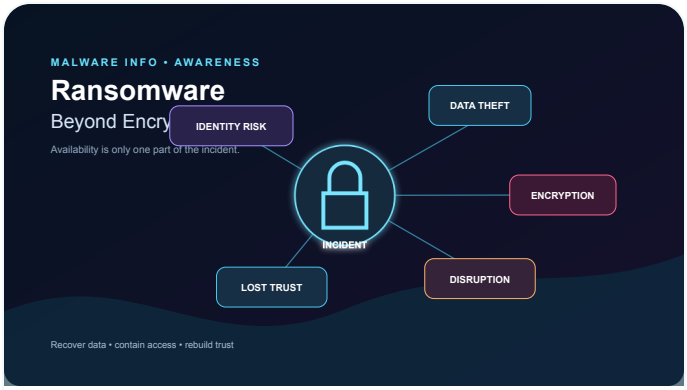
← Back to all posts

CONTINUE READING

Related posts

Skip to content

THREAT RESEARCH



CYBERSECURITY AWARENESS

From a Pension-Themed Spear-Phishing Email to a GitHub-Backed Implant: Investigating a SideWinder Connection

An evidence-led investigation traces a Myanmar pension lure from an encrypted Word attachment to an embedded implant and evaluates its overlap with regional SideWinder reporting.

September 10, 2026 35 min read

Ransomware: Beyond Encrypted Files

A source-based guide to ransomware history, hidden data theft, variant-specific recovery opportunities, evidence preservation, and resilient preparation.

September 7, 2026 31 min read