

selectively diverting update traffic for a narrow set of targets, organizations and individuals whose positions, access, or technical roles made them strategically valuable. Taken together, the operational choices, tooling, and victim profile support attribution, with moderate to high confidence, to the China-aligned espionage actor commonly tracked as [Lotus Blossom \(G0030\)](#) in concurrence with other organizations assessment.

What most clearly distinguishes this campaign is its precision. The malicious updates were tailored, the delivery carefully gated, and the operational noise deliberately kept low. There is no evidence of ransomware, financial theft, destructive activity, or influence operations. That absence is itself a signal. Everything about the intrusion, from the limited number of victims to the patient dwell time, points to an intelligence-gathering mission oriented toward quietly acquiring insight rather than extracting immediate material gain. The inferred objectives align closely with state intelligence priorities, encompassing political decision-making, economic and financial visibility, and access to telecommunications and technical environments.

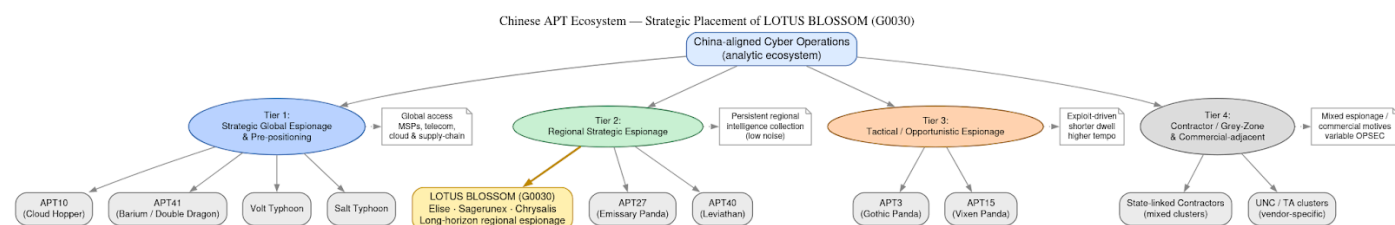
Viewed in a broader historical context, the Notepad++ compromise represents a *clear evolution in Lotus Blossom's tradecraft*. Earlier campaigns relied heavily on spear-phishing and bespoke backdoors delivered directly to victims. Rather than compromising end-user systems through conventional infrastructure attacks, such as opportunistic abuse of widely trusted software updates, the actors shifted the locus of trust toward the developer ecosystem itself. By abusing a legitimate update mechanism relied upon specifically by developers and administrators, they transformed routine maintenance into a covert entry point for high-value access. Yet despite this technical evolution, the strategic logic remains consistent. The campaign reflects continuity in purpose, a sustained focus on regional strategic intelligence, executed with more sophisticated, more subtle, and harder-to-detect methods than in prior iterations.

Actor Overview: Lotus Blossom (G0030)

Lotus Blossom is best understood as one of the more durable and methodical Chinese cyber-espionage clusters, with activity traced by multiple vendors and government-linked research groups back to at least 2009–2010. Over more than a decade of operations, the group has appeared under a shifting set of aliases, reflecting differences in vendor telemetry and analytic frameworks, but those naming inconsistencies mask a striking continuity beneath the surface. Across campaigns separated by years, Lotus Blossom exhibits the same core patterns: recurring malware families, stable operational rhythms, and a highly consistent choice of targets. This continuity is one of the strongest indicators that analysts are observing a single, long-lived espionage program rather than a loose collection of short-term intrusion efforts.

At its core, Lotus Blossom is a mission-driven intelligence actor, not a financially motivated threat group. There is no credible reporting tying the cluster to ransomware, extortion, cryptomining, or large-scale fraud. Instead, its operations consistently prioritize access, visibility, and persistence. In multiple documented campaigns, compromised environments remained under observation for months or even years, with operators carefully enumerating systems, staging data locally, and

maintaining footholds through understated persistence mechanisms. The absence of monetization artifacts, such as payment infrastructure, monetization tooling, or public-facing impact, strongly reinforces the assessment that Lotus Blossom’s mandate is intelligence collection rather than profit.



Geographically, the group’s center of gravity has long been Southeast Asia, a region that aligns closely with Chinese strategic, diplomatic, and security interests. Vietnam, the Philippines, Hong Kong, Taiwan, and neighboring states recur repeatedly in public reporting. Over time, however, there is clear evidence of measured expansion beyond this core theater. More recent campaigns, including the Notepad++ supply-chain operation, show activity extending into Central America and Oceania, suggesting either broadened tasking or an adaptive response to evolving intelligence priorities. Importantly, this expansion has not come with a change in tempo or style; the group applies the same low-noise tradecraft regardless of geography.

One of Lotus Blossom’s defining traits is its tolerance for long dwell times and multi-year campaigns. Unlike vulnerability-driven actors that move rapidly from exploitation to exit, Lotus Blossom appears comfortable maintaining access with minimal interaction, sometimes returning to environments long after initial compromise. This patience is reflected in how the group manages infrastructure and malware lifecycles. Tooling is not rapidly discarded after exposure; instead, families are iterated and refined over years, with new variants introduced only when necessary. This approach reduces operational risk and supports sustained intelligence collection.

Operationally, the group shows a strong preference for quiet persistence over disruption. Techniques documented across campaigns emphasize blending in rather than standing out: registry-based persistence, Windows services, DLL sideloading, and the use of legitimate administrative utilities. Command-and-control traffic is frequently disguised as normal web or API activity, and in some cases tunneled through legitimate platforms. This tradecraft minimizes alerts and allows the actor to remain embedded in sensitive networks without triggering incident response thresholds.

A key throughline across Lotus Blossom’s history is its reliance on custom backdoors that evolve but remain recognizably related. Early campaigns made use of backdoors such as *Elise*, followed by the long-running *Sagerunex* family, which has been observed in multiple variants since at least 2016 and is widely regarded as uniquely associated with the group. The emergence of *Chrysalis* in the Notepad++ supply-chain campaign represents the latest iteration of this lineage: a bespoke

implant designed for stealth, flexibility, and long-term access. The persistence of these families across years underscores both development continuity and institutional knowledge within the operator set.

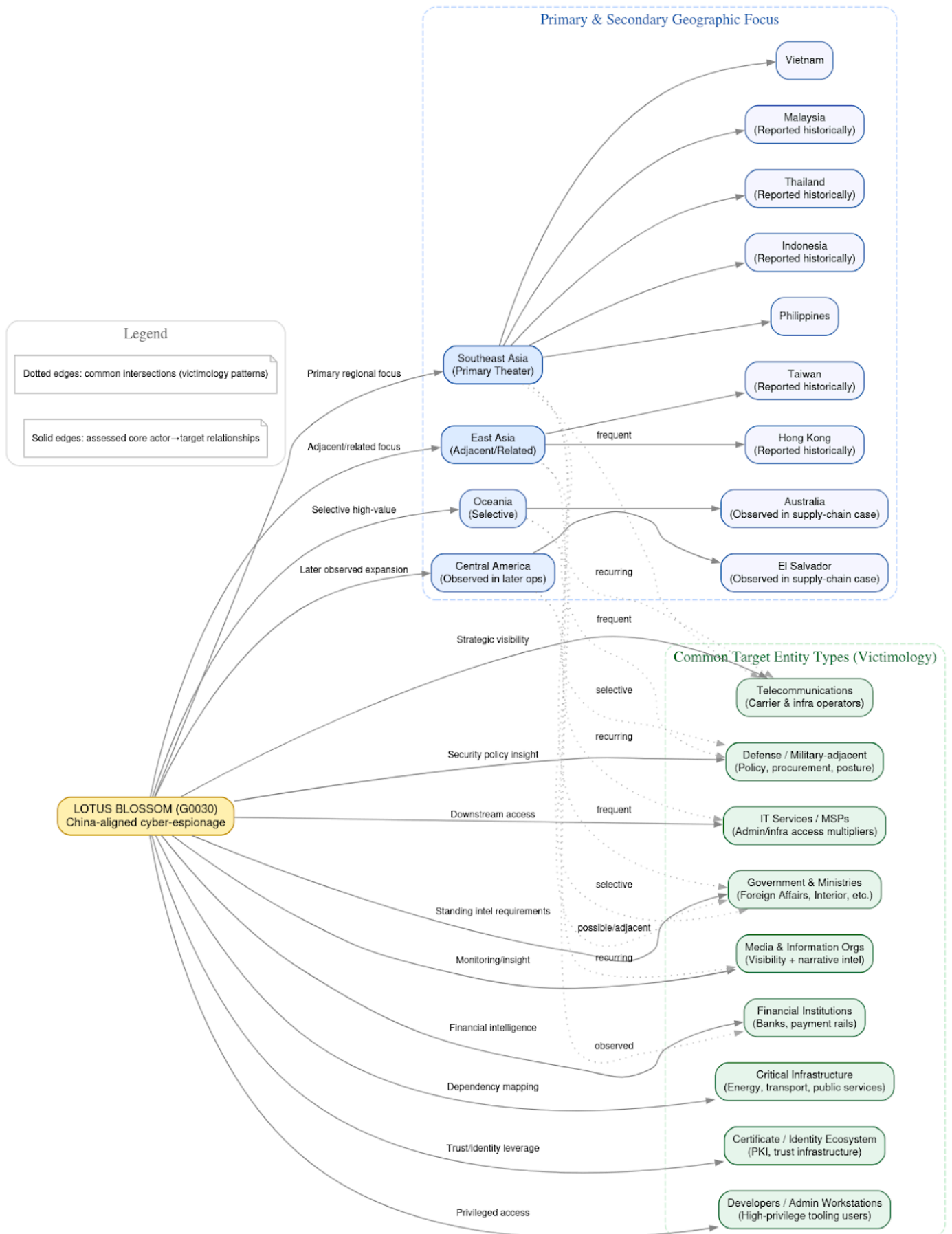
Within the broader Chinese APT ecosystem, Lotus Blossom occupies a regional strategic espionage tier. It is less globally expansive than groups such as APT10 or APT41, which have conducted large-scale, worldwide operations against managed service providers, supply chains, and intellectual property targets. At the same time, Lotus Blossom is markedly more disciplined and persistent than opportunistic or vulnerability-driven clusters that surge around new exploits and then fade. Its niche is sustained regional intelligence collection: quieter, narrower in scope, but exceptionally durable. That combination – longevity, patience, and restraint – has made Lotus Blossom one of the more consistently effective, and correspondingly harder to uproot, espionage actors operating in the Chinese cyber landscape.

Historical Operations and Tradecraft Evolution

Lotus Blossom's operational history can be understood as a gradual but deliberate evolution, marked by clear phases in tooling, targeting, and delivery mechanisms, each building on lessons learned from the last.

campaigns increasingly encompassed telecommunications providers, media organizations, and manufacturing or industrial firms. This broader victimology suggests an intelligence remit that had widened to include information flows, public narratives, supply chains, and industrial capacity.

LOTUS BLOSSOM (G0030) — Historical Targeting Map (Geography + Entity Types)



Technically, this era is notable for Lotus Blossom's growing reliance on legitimate third-party services as covert command-and-control channels. By tunneling communications through cloud platforms, webmail, and other widely used services, the group was able to blend malicious traffic into normal enterprise activity, significantly reducing detection risk. At the same time, operators invested in improved operational security and persistence mechanisms, favoring low-visibility techniques such as Windows services, registry modifications, and careful privilege management. These choices enabled long dwell times and multi-year access to sensitive environments, reinforcing the group's reputation for patience and discipline.

The modern era, beginning in 2025 and extending into 2026, represents the most pronounced shift in Lotus Blossom's tradecraft. In this phase, the group adopted supply-chain compromise as a primary delivery vector, moving upstream to exploit trusted software distribution mechanisms rather than targeting victims directly. This approach dramatically reduced reliance on social engineering and increased the likelihood of execution in privileged, trusted contexts. Central to this period was the development and deployment of *Chrysalis*, a previously undocumented backdoor that fits within the group's established lineage but reflects contemporary defensive realities, emphasizing stealth, flexibility, and survivability.

Operational focus in this era also shifted toward developer and administrator tooling, applications and environments used by individuals with elevated privileges and deep visibility into organizational systems. Even when positioned to affect a broad population, Lotus Blossom demonstrated highly selective victim delivery, carefully gating malicious updates to a narrow set of high-value targets. This restraint underscores the intelligence-driven nature of the activity and the group's continued aversion to unnecessary exposure.

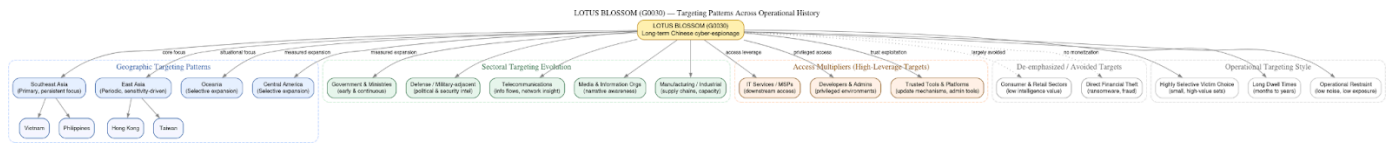
Viewed end to end, the Notepad++ supply-chain campaign stands as the clearest and most mature expression of this evolution. It combines the group's longstanding strategic focus on regional intelligence with a modern delivery mechanism that exploits trust itself, integrating bespoke tooling, blended command-and-control, and disciplined selectivity into a single, tightly executed operation.

Targeting Patterns Across Lotus Blossom's Operational History

Across more than a decade of observed activity, Lotus Blossom's targeting patterns reveal a high degree of consistency in strategic intent, even as the specific sectors and access methods have evolved. Rather than pursuing breadth or opportunistic exploitation, the group has repeatedly demonstrated a preference for narrow, high-value target sets aligned with enduring state intelligence requirements.

Geographically, Lotus Blossom's center of gravity has remained firmly anchored in Southeast Asia since its earliest documented campaigns. Countries such as Vietnam and the Philippines recur across multiple reporting periods, reflecting their geopolitical relevance, proximity to contested maritime regions, and the importance of regional security dynamics. Over time, the group's

targeting expanded outward in a measured fashion rather than a sudden global surge. East Asian entities, particularly in Hong Kong and Taiwan, appear during periods of heightened political sensitivity, while more recent operations show selective activity in Oceania and Central America. This pattern suggests deliberate tasking tied to evolving diplomatic, security, and economic priorities rather than indiscriminate global reach.



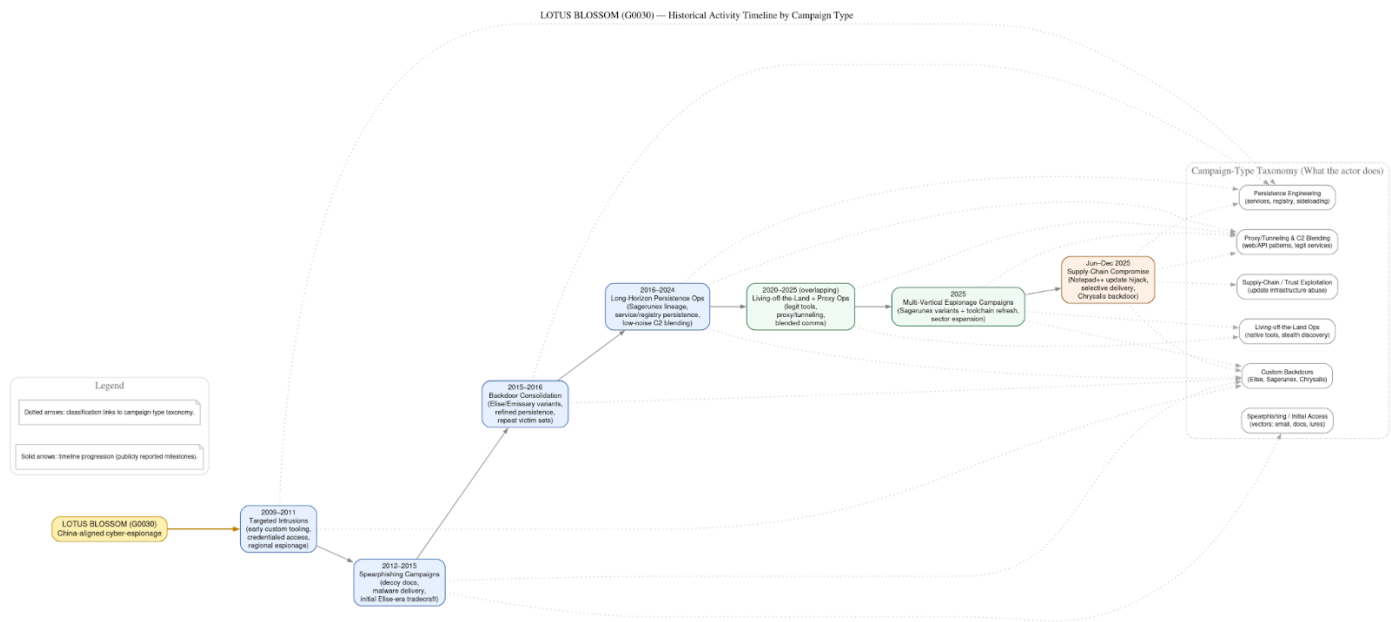
Sectorally, Lotus Blossom’s targeting history shows a clear progression from core state institutions toward broader strategic enablers. In its early years, the group focused heavily on government ministries and military or defense-adjacent organizations, consistent with a mandate centered on political and defense intelligence. As the group matured, it expanded into telecommunications providers, a shift that provided insight into information flows, network dependencies, and potential downstream access. Subsequent targeting of media organizations indicates an interest in narrative awareness and public messaging, while incursions into manufacturing and industrial sectors point to intelligence collection related to supply chains, industrial capacity, and economic resilience.

A notable and recurring theme is Lotus Blossom’s focus on access multipliers, entities or roles that provide visibility beyond their immediate organizational boundaries. Telecommunications operators, IT service providers, and managed service environments appear repeatedly because they offer the potential to observe or pivot into multiple downstream networks. This logic is further reinforced in the group’s most recent campaigns, which emphasize developer and administrator environments. By targeting the tools and systems used by highly privileged technical staff, Lotus Blossom maximizes intelligence yield while minimizing the number of compromises required.

Equally important is what the group does not target. There is little evidence of sustained activity against consumer sectors, retail organizations, or entities primarily associated with direct financial gain. Even when financial institutions appear in victimology, the surrounding indicators point toward financial intelligence and relationship mapping, not theft or fraud. This restraint reinforces the assessment that Lotus Blossom’s targeting is governed by intelligence value rather than monetization potential.

Finally, Lotus Blossom’s targeting is characterized by selectivity and patience. Campaigns routinely involve small numbers of victims, long dwell times, and repeated engagement with the same regions or sectors over many years. The Notepad++ supply-chain campaign exemplifies this approach: despite access to a potentially massive user base, the group limited malicious delivery to a tightly controlled subset of targets. This pattern is consistent with an actor that values sustained insight and low exposure over rapid or dramatic effects.

Taken together, Lotus Blossom’s targeting history reflects a disciplined, intelligence-driven model. Geography, sector, and individual victim selection all serve a coherent strategic purpose, supporting the conclusion that the group functions as a long-term regional intelligence collector rather than a broad-spectrum or opportunistic threat actor.

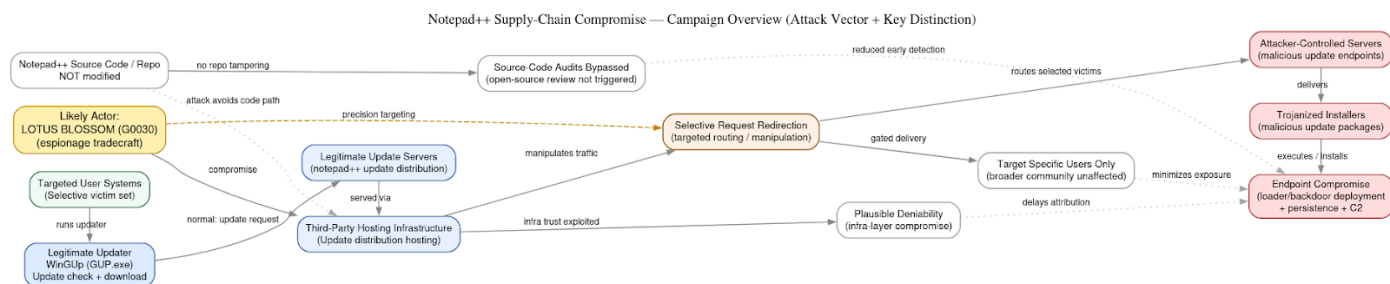


Campaign Overview: Notepad++ Supply-Chain Compromise

Campaign Overview: Notepad++ Supply-Chain Compromise

The Notepad++ campaign represents a deliberate and technically mature supply-chain operation built around the exploitation of trust, rather than the compromise of software code itself. Instead of tampering with the Notepad++ application or its publicly available source, the attackers targeted third-party hosting infrastructure responsible for distributing software updates. By positioning themselves within this upstream delivery path, they were able to influence what end users received without altering the integrity of the project’s codebase or repositories.

Central to the operation was the abuse of WinGUp (GUP.exe), the legitimate updater mechanism used by Notepad++. Under normal conditions, GUP.exe is responsible for periodically checking for updates and retrieving them from trusted servers. The attackers subverted this process by selectively redirecting update requests from chosen systems to attacker-controlled servers. To the end user, and to most security controls, the process appeared indistinguishable from a routine update transaction.



A critical distinguishing feature of this campaign is that the Notepad++ source code was never modified. This choice conferred several operational advantages. By avoiding source-level tampering, the attackers bypassed source-code reviews, integrity checks, and the scrutiny of the open-source community. The malicious payloads were delivered in the form of trojanized installers, injected only at the point of distribution, allowing the operation to remain invisible to developers and maintainers focused on the code itself.

This approach also enabled a high degree of plausible deniability. Because the compromise occurred within hosting and delivery infrastructure rather than the project's repositories, attribution was obscured and initial investigations could plausibly attribute anomalies to misconfiguration or transient infrastructure issues. Most importantly, the attackers exercised tight control over victim selection. Update redirection was applied only to specific targets, ensuring that malicious installers were delivered to a narrow, high-value subset of users while the vast majority of the Notepad++ user base continued to receive legitimate updates without incident.

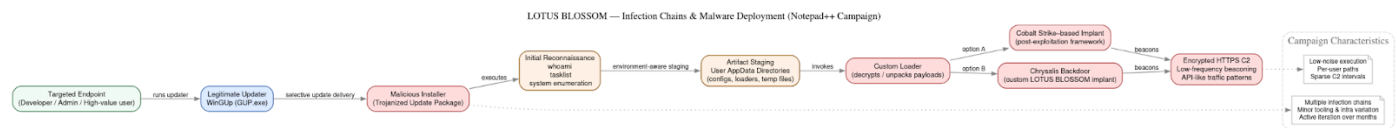
Taken together, these elements reflect a campaign characterized by advanced planning, privileged access, and operational restraint. The selective nature of delivery, the avoidance of unnecessary exposure, and the exploitation of infrastructure trust rather than code vulnerabilities are all hallmarks of Lotus Blossom's established tradecraft. The Notepad++ supply-chain compromise stands as a clear example of how the group has adapted its methods to modern software ecosystems while remaining true to its long-standing emphasis on stealthy, intelligence-driven operations.

Infection Chains and Malware Deployment

Analysis of the Notepad++ supply-chain incident reveals that the operation was not built around a single, static infection pathway, but rather multiple distinct infection chains deployed over the course of several months. Each chain showed minor variations in tooling, payload composition, and supporting infrastructure, suggesting active management and iteration by the operators. This modularity allowed Lotus Blossom to adapt to changing conditions, rotate infrastructure, and selectively tailor implants to different victims, all while preserving a consistent operational framework.

Despite these variations, the infection chains shared a set of core behavioral elements that define the campaign's execution. In every observed case, the process began with a legitimate Notepad++ update request, handled by the WinGUp (GUP.exe) updater. For selected targets, this

trusted process was subverted to launch a malicious installer delivered from attacker-controlled infrastructure. From the perspective of the operating system and the user, the execution chain appeared routine, inheriting the trust and execution context of a normal software update.



Once execution was achieved, the malware performed initial reconnaissance to situate itself within the environment. Commands such as `whoami` and `tasklist`, along with broader system enumeration routines, were used to identify the current user context, running processes, and basic system characteristics. This early situational awareness informed subsequent decisions, including which payloads to deploy and how aggressively to establish persistence.

The next phase involved the staging of artifacts within user application data directories, a deliberate choice that balanced accessibility and stealth. By operating within per-user paths rather than system-wide locations, the malware reduced the likelihood of triggering security controls tied to protected directories, while still maintaining reliable execution and storage. These directories served as temporary holding areas for loaders, configuration files, and auxiliary components.

From this staging environment, the operation progressed to the deployment of a custom loader, responsible for orchestrating the remainder of the infection chain. The loader acted as a pivot point, handling decryption, unpacking, and execution of the final payloads. Depending on the target and the specific chain in use, this culminated in the installation of either Cobalt Strike—based implants or the *Chrysalis* backdoor. The presence of both options indicates a flexible approach: Cobalt Strike offered a mature, feature-rich post-exploitation framework, while *Chrysalis* provided a bespoke, lower-profile alternative aligned with Lotus Blossom’s preference for custom tooling.

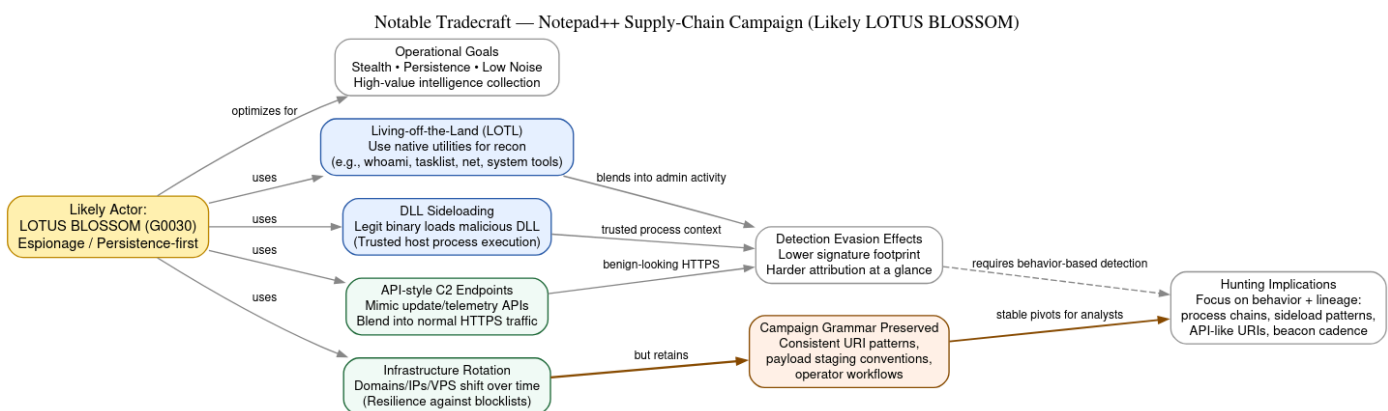
In all observed chains, post-compromise communications were conducted using encrypted, low-frequency outbound connections over HTTPS. Beaconing intervals were deliberately sparse, and traffic was structured to resemble legitimate web or API interactions, minimizing anomalies in network telemetry. This communications model prioritized stealth and survivability over responsiveness, reinforcing the broader pattern of restraint and long-term access that characterizes Lotus Blossom’s operations.

Collectively, these infection chains demonstrate a disciplined, repeatable deployment model that balances adaptability with consistency. The variations across chains reflect active operational oversight, while the shared elements underscore a well-established playbook optimized for covert, intelligence-driven access rather than rapid exploitation or overt impact.

Tradecraft Observed in the Notepad++ Supply-Chain Operation

In analyzing the Notepad++ supply-chain compromise and correlating it with broader reporting on Lotus Blossom operations, a consistent theme emerges. The group relies on stealthy, evasive techniques that blend malicious activity into normal system behavior rather than overt exploitation that would draw defensive attention. This section explains the key tradecraft elements that enabled the campaign's success and situates them within broader patterns observed in similar Chinese state-aligned espionage activity.

A foundational aspect of Lotus Blossom's technique set is the frequent use of living-off-the-land (LOTL) utilities, trusted, legitimate system tools that are co-opted to execute malicious logic under the guise of normal administrative or maintenance tasks. In LOTL attacks, adversaries leverage binaries that are already present on the target system (such as command interpreters or native utilities) to perform reconnaissance, lateral movement, or privilege escalation. Because these tools are part of the standard operating environment, their invocation often escapes traditional signature-based defenses and is not flagged by endpoint security as anomalous behavior. This approach is deliberately evasive, allowing an attacker to achieve foothold and persistence while minimizing the generation of new, suspicious artifacts. ([Kiteworks](#) | [Your Private Data Network](#))



Another sophisticated tactic documented in the Notepad++ intrusion was the abuse of DLL sideloading, an established evasion technique that enables malicious code to be loaded by a legitimate host process. In the Notepad++ case, researchers found that a renamed legitimate utility (the Bitdefender Submission Wizard) was used as the initial execution context. A malicious companion DLL, placed in the same directory with the same name expected by the host process, was then loaded in place of the legitimate library. This technique allows the adversary to inject custom payloads without directly executing an executable they control, further blending with normal system activity and reducing the footprint seen by defensive tools. ([Security Affairs](#))

Once executed, many of the campaign's implants communicated with remote infrastructure using API-style command-and-control (C2) endpoints designed to resemble benign web traffic. These endpoints often expose paths that mimic legitimate update, telemetry, or cloud service APIs rather than raw sockets or obvious HTTP beaconing. By shaping communications in this way and by hosting them behind domains or services that appear innocuous, operators improve the chances

that their traffic will traverse restrictive egress filters and escape detection by network intrusion detection systems. This API-like pattern of C2 infrastructure has been observed not only in the Notepad++ campaign but also in prior Lotus Blossom activity where third-party services (e.g., Dropbox, Twitter, or webmail) were repurposed as covert tunnels for beaconing and data exfiltration. ([Cisco Talos Blog](#))

Finally, Lotus Blossom's infrastructure usage patterns demonstrate rotation and redundancy without abandoning operational grammar. Rather than hard-coding a static set of servers or domains, the group periodically shifts hosting providers, domain names, and IP space while maintaining consistent behavioral identifiers in their implants and C2 protocols. This approach complicates blunt IP-blocklist defenses while preserving the recognizable telemetry that seasoned defenders use to attribute activity over time. The result is an operational posture that is resilient to takedown and resistant to simple detection heuristics, yet still exhibits an identifiable signature across campaigns and years of activity.

Collectively, these tradecraft elements illustrate a highly disciplined adversary that prioritizes stealth, persistence, and low noise. By blending malicious activity into the fabric of normal system and network behavior, Lotus Blossom not only evaded detection during the Notepad++ campaign but also reaffirmed the group's long-standing preference for covert intelligence collection over disruptive or noisy exploitation.

Victimology and Target Base

The victimology observed in the Notepad++ supply-chain campaign reinforces the assessment that this operation was tightly scoped and intelligence-driven, rather than opportunistic or indiscriminate. Public reporting and forensic analysis identify a small, carefully selected set of confirmed or strongly suspected victims, each of which aligns with Lotus Blossom's historical targeting logic.

Among the confirmed or observed targets were a government organization in the Philippines, a financial institution in El Salvador, and an IT service provider in Vietnam. In addition, individual technical users were identified in Vietnam, Australia, and El Salvador. While the total number of victims was limited, the diversity of roles and sectors represented is significant. Each victim category provides a disproportionate intelligence return relative to the number of compromises required.

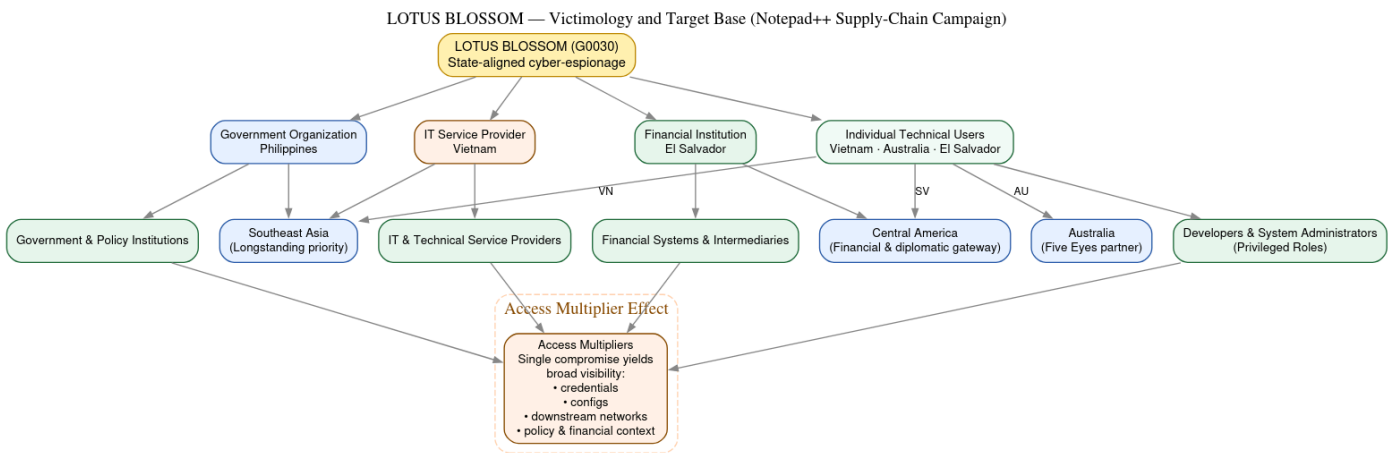
Geographic Pattern

The geographic distribution of victims is coherent and strategically consistent, rather than random. Southeast Asia remains the clear center of gravity, with Vietnam and the Philippines reflecting long-standing intelligence priorities for China. These countries sit at the intersection of contested maritime regions, regional security cooperation, and shifting diplomatic alignments, making them enduring targets for political, military, and economic intelligence collection.

Australia’s appearance in the victim set is also notable. As a Five Eyes intelligence partner, Australia represents a high-value target for insight into allied policy coordination, defense posture, and intelligence sharing frameworks. Even limited access to technical users in this environment can yield significant contextual intelligence.

The inclusion of El Salvador and, more broadly, Central America reflects a more recent but increasingly visible pattern. While not traditionally viewed as a primary cyber-espionage theater, the region functions as a financial and diplomatic intelligence gateway, offering visibility into international financial relationships, development financing, and external influence dynamics. The presence of both a financial institution and individual technical users in this geography suggests deliberate tasking rather than incidental spillover.

Sectoral Focus



Across all geographies, the sectoral composition of victims follows a consistent pattern. Targets cluster around government and policy-relevant institutions, financial systems and intermediaries, and IT and technical service providers. In the most recent phase of operations, particular emphasis is placed on developers and system administrators, individuals whose roles grant them privileged access and broad situational awareness within their organizations.

These targets function as access multipliers. A single compromised developer workstation or IT service provider can expose configuration data, credentials, network topologies, and downstream customer environments. Similarly, access to financial institutions or government agencies provides insight into policy deliberations, economic conditions, and institutional relationships that extend well beyond the compromised endpoint itself.

Taken together, the victimology of the Notepad++ campaign underscores Lotus Blossom’s disciplined targeting philosophy. The group consistently favors high-leverage roles and institutions that maximize intelligence value while minimizing operational exposure. The limited number of victims, combined with their strategic placement across regions and sectors, reinforces the conclusion that this campaign was designed to support sustained intelligence collection rather than broad access or immediate impact.

Why Notepad++?

Notepad++ occupies a uniquely advantageous position within technical environments, which helps explain its selection as a delivery vector in this campaign. The application is ubiquitous among technical users, including developers, system administrators, network engineers, and security analysts. In many organizations, it is installed by default on workstations used for infrastructure management, application development, and operational support. As a result, systems running Notepad++ often belong to users who possess elevated privileges, deep contextual knowledge of internal systems, and routine access to sensitive resources.

From an intelligence perspective, compromising such a tool offers an unusually high return on investment. Technical users commonly rely on Notepad++ to view, edit, and temporarily store credentials, configuration files, and infrastructure details in plaintext. Scripts and automation logic, used to manage servers, networks, cloud resources, and security controls, are frequently authored or reviewed within the editor. Access to these materials can reveal VPN endpoints, cloud service credentials, API keys, internal naming conventions, and operational workflows, providing insight far beyond the confines of a single endpoint. In many cases, these artifacts also reference institutional documentation, internal procedures, and architectural diagrams that are not otherwise externally visible.

Equally important is the trust relationship inherent in the software's update mechanism. The Notepad++ updater is a routine, background process that users expect to run without intervention or scrutiny. By abusing this mechanism, the attackers were able to inherit the implicit trust that users and operating systems place in legitimate updates. This eliminated the need for phishing emails, malicious attachments, or other forms of overt social engineering that might raise suspicion or trigger defensive controls. The act of updating the software, normally a security-positive behavior, became the point of compromise.

In effect, the update process itself functioned as the lure. Rather than persuading users to take risky actions, the attackers embedded themselves in a workflow that users already regarded as safe and necessary. This inversion of trust reflects a sophisticated understanding of how technical users operate and underscores why Notepad++ was such an effective and strategically chosen access vector for an intelligence-focused campaign.

Political, Economic, Financial, and Espionage Motives

Intelligence Objectives and Strategic Rationale

The intelligence objectives underlying the Notepad++ supply-chain campaign align closely with long-standing state priorities, particularly in the political, economic, and strategic domains. The operation's design and execution suggest a deliberate effort to build situational awareness rather than to achieve immediate operational effects.

Political Intelligence.

A central aim of the campaign appears to be sustained monitoring of government policy direction in Southeast Asia, a region where diplomatic alignment, security cooperation, and maritime disputes remain fluid. Access to technical users and institutions in this environment provides insight into policy deliberations, inter-agency coordination, and shifts in national posture that may not be visible through public channels. Closely related is the collection of intelligence on defense cooperation and maritime strategy, including how regional governments coordinate with one another and with external partners. The presence of targets linked to allied ecosystems further suggests an interest in alignment with U.S. and partner positions, offering indirect visibility into broader coalition dynamics and strategic intent.

Economic and Industrial Intelligence.

Beyond politics and defense, the campaign reflects a clear focus on economic and industrial intelligence. Access to financial institutions and technical service providers enables visibility into indicators of economic stability, capital flows, and institutional dependencies. Similarly, targeting entities involved in infrastructure and technology operations supports an understanding of modernization efforts, procurement cycles, and industrial capacity. Monitoring regulatory discussions and trade posture, often embedded in internal documentation, draft policies, and technical planning materials provides advanced awareness of economic decisions that can shape regional competitiveness and resilience.

Financial Intelligence (Non-Theft).

Notably, while financial institutions appear in the victim set, there is no evidence of fraud, theft, or fund diversion associated with this campaign. Instead, the activity is consistent with financial intelligence collection: mapping relationships between institutions, understanding transaction flows at a structural level, and identifying dependencies within national and regional financial systems. This distinction is important. The absence of monetization artifacts reinforces the assessment that the objective was insight, not profit, and places the activity firmly in the realm of state intelligence rather than cybercrime.

Strategic Espionage Doctrine.

Taken together, these objectives reflect a strategic espionage doctrine that prioritizes access over action, patience over disruption, and information dominance without escalation. The campaign was designed to quietly position the operator for long-term understanding, not to coerce, signal, or destabilize. By avoiding destructive activity and limiting exposure, the operation preserved freedom of action while minimizing diplomatic or political risk. In this sense, the Notepad++ supply-chain compromise represents intelligence preparation, laying the groundwork for informed decision-making rather than attempting to shape outcomes directly through cyber means.

Attribution Assessment

The totality of available [evidence](#) supports attribution of the Notepad++ supply-chain campaign, with moderate to high confidence, to Chinese actors, and [specifically Lotus Blossom \(G0030\)](#). This assessment is not based on any single indicator, but on the convergence of multiple independent factors that, taken together, form a coherent and internally consistent attribution picture.

First, the campaign aligns closely with Lotus Blossom's longstanding geographic focus on Southeast Asia. Vietnam and the Philippines, both represented among confirmed or observed victims, have appeared repeatedly in the group's historical operations over more than a decade. This persistent regional focus distinguishes Lotus Blossom from more globally oriented Chinese APT clusters and reinforces continuity with prior tasking rather than a one-off expansion by a different actor.

Second, the tooling lineage observed in this campaign is consistent with Lotus Blossom's established development patterns. The deployment of *Chrysalis*, a previously undocumented backdoor, fits cleanly within the group's historical reliance on bespoke implants such as *Elise* and *Sagerunex*. The design philosophy, custom code, low noise, and flexibility for long-term access, mirrors earlier Lotus Blossom tooling rather than the commodity frameworks or mixed criminal-espionage toolsets associated with other Chinese clusters.

Third, the selective nature of targeting and low infection counts strongly support this attribution. Despite access to an update mechanism capable of affecting a massive global user base, the attackers constrained delivery to a narrow set of high-value victims. This restraint is characteristic of Lotus Blossom's operational model, which consistently favors precision and intelligence yield over scale. It contrasts sharply with campaigns conducted by other Chinese APTs that have demonstrated a willingness to pursue broad, high-volume access when aligned with their objectives.

Fourth, the campaign demonstrates mature operational security and infrastructure discipline. The use of infrastructure-level compromise, API-style command-and-control endpoints, low-frequency encrypted communications, and careful infrastructure rotation without abandoning recognizable campaign grammar reflects a level of planning and tradecraft that Lotus Blossom has exhibited repeatedly in past operations. These elements point to an actor experienced in sustaining access over long periods while minimizing detection and attribution risk.

Finally, the victimology aligns closely with historical Lotus Blossom target sets. Government entities, financial institutions used for intelligence rather than theft, IT service providers, and privileged technical users all fall squarely within the group's established targeting preferences. This continuity in "who" is targeted is as significant as the technical "how," reinforcing the conclusion that the campaign represents an evolution of an existing program rather than the work of a different group adopting similar techniques.

When weighed collectively, these factors form a strong attribution case. While other Chinese APT clusters share individual characteristics, such as supply-chain access, custom tooling, or regional interest, no other known group fits the full combination of geography, tradecraft, restraint, tooling lineage, and victimology as closely as Lotus Blossom.

Defensive and Strategic Implications

The Notepad++ supply-chain compromise carries implications that extend well beyond this single incident, both for network defenders and for policymakers concerned with national and economic security. The campaign highlights structural weaknesses in how trust is established, maintained, and defended in modern software ecosystems.

Implications for Defenders.

First, the operation underscores that open-source software is not inherently low risk. Transparency of code does not automatically translate into security when the distribution and update mechanisms sit outside the codebase itself. In this case, the source remained intact while the delivery path was subverted, demonstrating that trust can be undermined upstream of any code review or integrity check. Defenders should treat open-source tools with the same rigor applied to proprietary software, particularly where update mechanisms rely on third-party infrastructure.

Second, the campaign highlights updating infrastructure as a critical attack surface. Software updaters are privileged by design, frequently allowed through endpoint and network controls, and trusted to execute code without user scrutiny. When compromised, they provide an attacker with a reliable and stealthy execution path. Securing update pipelines through stronger integrity validation, monitoring of anomalous update behavior, and defense-in-depth around hosting and distribution, is therefore as important as securing the software itself.

Third, the targeting logic reinforces that developer and administrator workstations are among the highest-value espionage targets in modern environments. These systems often aggregate credentials, scripts, configuration files, and architectural knowledge that can expose entire networks or multiple downstream organizations. Traditional security models that focus primarily on servers or perimeter assets risk overlooking these high-leverage endpoints.

Finally, the campaign demonstrates the limits of indicator-driven defense. Behavioral detection and contextual analysis are more reliable than static IOCs against a patient, low-noise adversary. Infrastructure rotation, bespoke tooling, and selective targeting render simple blocklists and hash-based detection insufficient. Defenders are better served by focusing on anomalous process chains, unexpected updater behavior, unusual DLL loading patterns, and deviations in network communication profiles such as perimeter DNS or packet inspection, even when individual indicators appear benign in isolation.

Implications for Policy and National Security.

At a strategic level, the campaign illustrates that supply-chain compromise has become a primary vector for state-level espionage. As articulated in the work of Jian Tan on software supply-chain trust, capable actors increasingly avoid the cost of penetrating targets individually and instead position themselves inside trusted ecosystems that provide scalable, repeatable access to high-value users. This shift complicates deterrence and response, as such compromises can persist undetected for extended periods and propagate across multiple sectors simultaneously through a single poisoned trust relationship.

The victimology also highlights that smaller and mid-sized states are frequently targeted as intelligence gateways. Access to institutions in these countries can yield disproportionate insight into regional dynamics, allied relationships, and international financial or diplomatic flows. This reality challenges assumptions that only major powers or headline geopolitical rivals face sustained cyber-espionage pressure.

Finally, the incident reinforces that trust relationships within software ecosystems are now contested terrain. Developers, maintainers, hosting providers, and users all participate in chains of trust that adversaries actively seek to exploit. Protecting these ecosystems is both a technical and strategic challenge, requiring coordination between private industry, open-source communities, and governments to harden shared infrastructure without undermining the openness and collaboration that make these ecosystems valuable in the first place.

Taken together, these implications point to a future in which defending against espionage is less about patching individual vulnerabilities and more about protecting trust itself, in software, in infrastructure, and in the relationships that bind modern digital systems together.

Outlook and Forward Assessment

Looking ahead, the patterns observed in the Notepad++ campaign and in Lotus Blossom's historical operations provide a useful basis for anticipating how this actor is likely to operate in the near to medium term. The group's evolution has been incremental rather than abrupt, suggesting continuity of mission and tradecraft rather than experimentation for its own sake.

Likely Future Activity

Lotus Blossom is likely to continue targeting developer and administrator tooling, particularly applications and platforms that are widely deployed in technical environments and implicitly trusted by their users. These tools offer consistent access to privileged contexts and aggregate high-value information such as credentials, automation scripts, configuration data, and architectural documentation. As long as developers and administrators remain central to modern infrastructure operations, they will remain attractive espionage targets.

Geographically, future activity is expected to involve measured expansion into adjacent regions with strategic relevance, rather than a dramatic shift toward global saturation. Southeast Asia will almost certainly remain the core theater, but selective operations in regions that function as diplomatic, economic, or intelligence gateways, similar to the activity observed in Oceania and Central America, are likely to continue. Such expansion reflects evolving intelligence requirements rather than a change in operational philosophy.

From a delivery perspective, the group's demonstrated success with the Notepad++ compromise strongly suggests an ongoing preference for supply-chain and trust-based access. Compromising distribution infrastructure, update mechanisms, or widely trusted platforms reduces reliance on social engineering and increases the likelihood of execution in high-trust environments. This model is efficient, stealthy, and well aligned with Lotus Blossom's emphasis on low-noise, long-term access.

Warning Indicators

Defenders should be alert to a set of warning indicators that are subtle in isolation but meaningful in combination. Selective update anomalies, where only a small subset of systems receive unexpected update behavior, may indicate upstream manipulation rather than benign error. Similarly, low-volume, API-style beaconing that blends into normal HTTPS traffic can signal command-and-control activity designed to evade traditional network detection.

Another important indicator is the compromise of "boring but trusted" tools: utilities that are widely used, rarely scrutinized, and considered operationally mundane. These applications often sit outside the focus of security monitoring precisely because they are perceived as low risk, making them ideal vehicles for trust exploitation. Finally, defenders should treat long dwell times without overt impact as a potential red flag rather than a sign of benign activity. In Lotus Blossom's operating model, the absence of disruption is often an intentional feature, not an accident.

Taken together, these indicators point to an adversary that values patience, precision, and invisibility. Future campaigns are likely to look unremarkable at first glance, blending into routine operational noise. Recognizing and responding to them will depend less on spotting dramatic events and more on detecting subtle deviations in how trusted systems behave over time.

Bottom-Line Judgment

The Notepad++ supply-chain campaign is a textbook example of modern Chinese state-aligned cyber-espionage, optimized for discretion, persistence, and strategic intelligence collection.

Lotus Blossom remains one of China's most quietly effective APTs, less visible than headline actors, but deeply embedded in regional intelligence operations.

Confidence Ratings

- APT involvement: **High**
- Espionage motive: **High**
- Lotus Blossom attribution: **Moderate–High**

Appendix A: Indicators of Compromise (IOCs)

Actor: Lotus Blossom (G0030)

Campaign: Notepad++ Supply-Chain Compromise (2025–2026)

Analyst note: This appendix consolidates publicly reported and analytically derived IOCs associated with Lotus Blossom and the Notepad++ supply-chain campaign. The list is intended for threat hunting and contextual correlation, not as a stand-alone blocklist. The actor demonstrates frequent infrastructure rotation, selective delivery, and low-noise operations; therefore, behavioral correlation remains essential.

A.1 Campaign-Specific Network IOCs (Notepad++ Supply-Chain)

Command-and-Control Domains (observed in reporting):

- cdncheck[.]it[.]com
- wiresguard[.]com
- Skycloudcenter[.]com

cdncheck.it.com

- This domain has been observed as a command-and-control endpoint used by malicious payloads delivered in the Notepad++ supply-chain campaign; Cobalt Strike Beacons were configured to communicate with it, and attackers used paths like /api/update/v1 and /api/FileUpload/submit for C2 traffic.
- It is deployed in multiple infection chains as a C2 domain, not a legitimate service; security analysts note its inclusion in IoCs tied to the Notepad++ compromise.
- There is no public indication that cdncheck.it.com is associated with any legitimate “cdncheck” project such as the ProjectDiscovery tool named cdncheck (which is an open-source asset scanning tool). The similarity in names appears coincidental.

Summary: Used as attacker-controlled infrastructure; no publicly known legitimate service.

2. wiresguard.com (referred to in C2 contexts)

- The domain api.wiresguard.com appears in Notepad++ campaign IoCs collected by security researchers—Beacons and API paths like /update/v1, /api/FileUpload/submit, and /api/getInfo/v1 were observed being used by Cobalt Strike implants and other payloads.

- There is no evidence from public OSINT that the domain is linked to the WireGuard VPN project (the legitimate technology is spelled *WireGuard*). It is widely assessed to be an attacker-controlled domain imitating a plausible service name to blend into developer traffic.
- Analysts treat this domain as part of malicious infrastructure rather than a trusted service provider.

Summary: Likely malicious C2 domain mimicking a benign service name; no legitimate affiliation found in open OSINT.

3. skycloudcenter.com

- The subdomain api.skycloudcenter.com is identified in multiple IoC lists from incident analysis—it appears in URLs such as /a/chat/s/{GUID} used by the *Chrysalis* backdoor for encrypted communications.
- Reporting notes that this domain is part of the API-style command-and-control infrastructure rather than a known cloud provider or mainstream SaaS platform.
- There is no clear legitimate service tied to this domain in publicly indexed OSINT; its naming seems intended to resemble a cloud service but lacks authoritative footprint (no major product, published service, or corporate identity in searchable records).

Summary: Appears exclusively as attacker infrastructure used for backdoor C2; no confirmed legitimate service.

Associated IP Addresses (observed during campaign window):

- 45.77.31[.]210
- 59.110.7[.]32:8880
- 124.222.137[.]114:9999

45.77.31[.]210 (HTTPS)

Role in campaign: Hosted second-stage Cobalt Strike Beacon shellcode and exposed API-style C2 endpoints used by the Beacon (GET/POST patterns). ([Securelist](#))

Observed paths / IOCs:

- [https://45.77.31\[.\]210/users/admin](https://45.77.31[.]210/users/admin) (Beacon shellcode retrieval) ([Securelist](#))
- [https://45.77.31\[.\]210/api/update/v1](https://45.77.31[.]210/api/update/v1) (Beacon HTTP-GET) ([Securelist](#))
- [https://45.77.31\[.\]210/api/FileUpload/submit](https://45.77.31[.]210/api/FileUpload/submit) (Beacon HTTP-POST) ([Securelist](#))

Hosting / network ownership (OSINT):

- rDNS indicates **Vultr**-hosted infrastructure (e.g., 45.77.31.210.vultrusercontent.com). ([IPinfo](#))
- Vultr's public ASN is **AS20473 (The Constant Company)**. ([IPinfo](#))

Analytic note: Securelist describes a later shift where the same “grammar” (paths, updater chain) persists while delivery/C2 pivots toward domains (e.g., cdncheck[.]it[.]com)—classic “rotate infra, keep protocol shape” tradecraft. ([Securelist](#))

59.110.7[.]32:8880 (HTTP)

Role in campaign: Hosted a Cobalt Strike Beacon and implemented API-like endpoints for GET/POST comms (directly referenced as part of the Notepad++ supply-chain operation telemetry set). ([Securelist](#))

Observed paths / IOCs:

- [http://59.110.7\[.\]32:8880/uffhxpSy](http://59.110.7[.]32:8880/uffhxpSy) (Beacon staging/hosting URL) ([Rapid7](#))
- [http://59.110.7\[.\]32:8880/api/getBasicInfo/v1](http://59.110.7[.]32:8880/api/getBasicInfo/v1) (Beacon HTTP-GET) ([Rapid7](#))
- [http://59.110.7\[.\]32:8880/api/Metadata/submit](http://59.110.7[.]32:8880/api/Metadata/submit) (Beacon HTTP-POST) ([Rapid7](#))

Hosting / network ownership (OSINT):

- Mapped to AS37963 (Hangzhou Alibaba Advertising Co., Ltd.), i.e., Alibaba Cloud–linked hosting. ([IPinfo](#))
- Also appears in Abuse.ch ecosystem tracking as malicious-host infrastructure (additional corroboration signal, not attribution by itself). (urlhaus.abuse.ch)

124.222.137[.]114:9999 (HTTP)

Role in campaign: Hosted a Cobalt Strike Beacon with the same “API façade” pattern (update/status/info submission), and is listed by both Securelist (campaign IOC list) and Rapid7 (Chrysalis/related tooling context). ([Securelist](#))

Observed paths / IOCs:

- [http://124.222.137\[.\]114:9999/3yZR31VK](http://124.222.137[.]114:9999/3yZR31VK) (Beacon staging/hosting URL) ([Rapid7](#))
- [http://124.222.137\[.\]114:9999/api/updateStatus/v1](http://124.222.137[.]114:9999/api/updateStatus/v1) (Beacon HTTP-GET) ([Rapid7](#))
- [http://124.222.137\[.\]114:9999/api/Info/submit](http://124.222.137[.]114:9999/api/Info/submit) (Beacon HTTP-POST) ([Rapid7](#))

Hosting / network ownership (OSINT):

The [124.222.137.0/24](#) netblock is shown as AS45090 (Shenzhen Tencent Computer Systems Company Limited), i.e., Tencent Cloud–linked hosting. ([IPinfo](#))

What these three IPs imply (campaign-level assessment)

- All three are consistent with the campaign’s **low-volume, high-control delivery** model: they’re not mass-distribution nodes; they’re **purpose-built staging/C2** with “**benign enterprise API**” URL shapes (/api/* /v1, /submit, etc.). ([Securelist](#))

- The hosting mix (**Vultr + Alibaba Cloud + Tencent Cloud**) is consistent with **infrastructure agility** and **cost-effective rotation** without changing the operational “grammar” (paths, beacon profile style). ([Securelist](#))

C2 Characteristics:

- HTTPS-based communication
- API-style URI paths (update/telemetry-like)
- Low-frequency beaconing
- Small request/response payloads
- Consistent URI grammar across rotating domains

Appendix A.2 (Expanded): Malware & Tooling IOCs

Actor: Lotus Blossom (G0030)

Campaign: Notepad++ Supply-Chain Compromise (2025–2026)

A.2.1 Custom Backdoors / Implants

1. Chrysalis – Custom Backdoor (Campaign-specific)

- **Description:** A previously undocumented custom backdoor deployed via malicious Notepad++ updates. It’s feature-rich, implements structured C2, and uses advanced loader obfuscation and API hashing techniques. It was delivered after DLL sideloading via renamed Bitdefender binaries and NSIS installer abuse.
- **Observed in:** Multiple security reports on the Notepad++ supply-chain compromise confirm Chrysalis as the primary bespoke implant in the most recent execution chain. Chrysalis replaces or augments Cobalt Strike payloads in some infection conduits. ([Rapid7](#))

Sample Name or Artifact	Type	Observed Role	Notes / Citation
update.exe	NSIS installer	Initial dropper for backdoor	Rapid7 analysis discussed multiple NSIS bundles delivering Chrysalis components. (Rapid7)
BluetoothService.exe	Legitimate loader renamed	DLL sideload host	Rapid7 cites the renamed Bitdefender utility abused for sideloading log.dll. (Help Net Security)
log.dll	Loader DLL	Decrypts/executes the backdoor	Rapid7 notes that log.dll loads and decrypts Chrysalis. (Help Net Security)

Sample Hash Indicators:

(These are candidate hashes observed in threat-hunting discussions associated with Chrysalis-type activity; use with contextual correlation)

- 8ea8b83645fba6e23d48075a3f3fd23eba515b4536710cda4f1f232718f53e
- [a511be5164dc1122fb5a7daa3eef9467e43d8458425b15a640235796006590c9](#)
- [77bfea78def679aa1117f569a35e8fd1542df21f7e00e27f192c907e61d63a2e](#)

(These hashes have appeared in threat-hunting context lists tied to Notepad++ indicators.)
([Reddit](#))

Notes: Chrysalis is associated with multi-stage loading and encrypted communications and is explicitly tied to the Notepad++ compromise in Rapid7 technical analysis. ([Rapid7](#))

2. Sagerunex – Historical Lotus Blossom Backdoor Family

- **Description:** A long-standing backdoor family consistently linked with Lotus Blossom operations in Southeast Asia prior to the Notepad++ incident. Sagerunex appears in multiple variants over years and is part of the group's standard espionage toolkit. ([Picus Security](#))
- **Behavior:** Often installed as a Windows service or registry persistence component; connects to C2 via encrypted or tunneled channels; used for long-term access and data exfiltration. ([Picus Security](#))

Sample Hash Indicators:

(Historical Sagerunex variants are well documented in vendor telemetry but specific public hashes for this campaign have not been widely published. The below hashes are examples drawn from public threat intelligence discussions tied to earlier variants.)

- [2da00de67720f5f13b17e9d985fe70f10f153da60c9ab1086fe58f069a156924](#) *(sample linked in community hunting lists)*
- [3bdc4c0637591533f1d4198a72a33426c01f69bd2e15ceee547866f65e26b7ad](#) *(community-listed indicator)*
- 9276594e73cda1c69b7d265b3f08dc8fa84bf2d6599086b9acc0bb3745146600 *(contextual IOC conversation)*
- [f4d829739f2d6ba7e3ede83dad428a0ced1a703ec582fc73a4eee3df3704629a](#) *(contextual IOC conversation)*

(These have been shared in public Reddit-based or tool-hunt contexts and should be correlated carefully with metadata.) ([Reddit](#))

Notes: Sagerunex's variants may not be directly linked to the Notepad++ campaign but represent the broader Lotus Blossom backdoor lineage. ([Picus Security](#))

3. Elise – Early Custom Backdoor (Historic, Pre-Campaign)

- **Description:** An older custom backdoor associated with early Lotus Blossom campaigns (circa 2012–2015), widely referenced in historic vendor analysis. ([Picus Security](#))
- **Behavior:** Provided persistence and remote access, often delivered via spear-phishing lures targeting government and defense institutions.

Public Hashes:

There are *no widely published hashes specifically tied to Elise in the context of the Notepad++ campaign*. Historical Elise variants appear in older vendor IOC sets but are not directly cited in current Notepad++ analyses.

Notes: Elise remains part of the Lotus Blossom malware ecosystem but is not directly observed in the Notepad++ supply-chain campaign in available public reporting. ([Picus Security](#))

A.2.2 Ancillary / Supporting Artifacts

Loaders / Execution Components Observed:

- NSIS installer artifacts (e.g., update.exe) — utilized to bootstrap malicious payload delivery. ([Rapid7](#))
- Renamed legitimate utilities (e.g., Bitdefender Submission Wizard / BluetoothService.exe) — used for DLL sideloading of malicious components. ([Help Net Security](#))

Note on Hash Interpretation:

Several hashes circulating in public hunting forums are included above for Chrysalis and Sagerunex, but these should be used only in conjunction with behavioral and contextual evidence (e.g., execution lineage, process ancestry, file paths, registry persistence) due to the non-global nature of the Notepad++ campaign.

A.2.3 Confidence Levels

Malware/Tool	Campaign-Relevant	Hash Availability
Chrysalis Backdoor	High	Partial public hunting hashes available
Sagerunex Backdoor	Moderate (historical)	Yes (historical lists)
Elise Backdoor	Low (historical)	Limited public hashes

Post-Exploitation Frameworks:

Cobalt Strike–based implants (selective deployment)

Execution & Loading Techniques:

- DLL sideloading via legitimate executables
- Custom loaders responsible for decrypting/unpacking final payloads

A.3 File System Artifacts

Observed / Common Staging Locations:

- %APPDATA%\ProShow\load
- %APPDATA%\Adobe\Scripts\alien.ini
- %APPDATA%\Bluetooth\BluetoothService\

General Patterns:

- Use of user-writable directories
- Non-descriptive filenames
- Configuration files masquerading as benign application data
- Loader and payload separation

A.4 Process & Execution Indicators

Suspicious Parent/Child Relationships:

- GUP.exe (WinGUP updater) spawning non-standard installer binaries
- Legitimate signed executables loading unsigned or anomalous DLLs

Reconnaissance Commands Observed:

- whoami
- tasklist
- System and environment enumeration commands
- Network configuration discovery

A.5 Persistence Indicators

Persistence Techniques (Observed Historically):

- Windows services created for backdoor execution
- Registry modification for auto-start
- DLL search-order hijacking
- Loader-based persistence chained from user context

A.6 Infrastructure & Operational Patterns (Campaign Grammar)

These are higher-order IOCs useful for hunting beyond static indicators:

- API-like C2 endpoints mimicking update or cloud services

- Infrastructure rotation without change in URI structure
- Selective delivery (only a subset of update requests redirected)
- Long dwell times with no visible disruption
- Absence of ransomware, cryptomining, or fraud tooling

A.7 Historical Lotus Blossom Targeting Context (Non-Exhaustive)

Geographies Recurrently Associated with Activity:

- Southeast Asia (Vietnam, Philippines, Indonesia)
- East Asia (Hong Kong, Taiwan)
- Oceania (Australia)
- Central America (El Salvador)

Target Entity Types:

- Government ministries and agencies
- Defense-adjacent organizations
- Telecommunications providers
- Financial institutions (intelligence, not theft)
- IT service providers / MSPs
- Developers and system administrators

A.8 Defensive Guidance for IOC Use

- Do not rely solely on blocklists. Many IOCs are short-lived.
- Correlate with behavioral indicators:
 - Unexpected updater behavior
 - DLL sideloading chains
 - API-like HTTPS beaconing
 - Long-term low-noise persistence
- Treat developer and admin endpoints as high-priority hunt targets.
- Monitor update infrastructure and third-party hosting dependencies.

A.9 Confidence Statement

The IOCs listed above align with public vendor reporting and multi-source analysis of Lotus Blossom activity. While individual indicators may overlap with other actors or benign infrastructure, the combined presence of these IOCs with Lotus Blossom tradecraft patterns provides a strong basis for attribution and threat-hunting.

Appendix B: Sources and Citations

This appendix consolidates all primary reporting, technical analyses, and authoritative reference material used to support the assessments, attribution, and narrative in this report. Sources are grouped by function (technical analysis, media reporting, and reference frameworks) to allow readers to distinguish between direct forensic evidence, journalistic corroboration, and contextual intelligence baselines.

B.1 Primary Technical Analysis and Vendor Research

These sources form the core evidentiary basis for the campaign analysis, infection chains, victimology, and tradecraft assessment.

1. Kaspersky Securelist
“Notepad++ supply-chain attack”
Comprehensive technical analysis detailing infection chains, infrastructure abuse, victim categories, and malware behavior.
<https://securelist.com/notepad-supply-chain-attack/118708/>
2. Kaspersky Press and Research Materials
Supplemental summaries and clarifications derived from Securelist reporting and telemetry.
<https://www.kaspersky.com/about/press-releases>
3. MITRE ATT&CK – Lotus Blossom (G0030)
Authoritative reference for historical tooling, targeting patterns, and known techniques associated with Lotus Blossom.
<https://attack.mitre.org/groups/G0030/>

B.2 Media and Independent Reporting

These sources provide external corroboration, contextual framing, and confirmation of selectivity, attribution hypotheses, and geopolitical relevance.

4. Ars Technica
“Notepad++ updater was compromised for 6 months in supply-chain attack”
Reporting on duration, infrastructure compromise, and selective delivery.
<https://arstechnica.com/security/2026/02/notepad-updater-was-compromised-for-6-months-in-supply-chain-attack/>
5. Reuters
“Popular open-source coding application targeted in Chinese-linked supply-chain attack”
Independent confirmation of selective targeting, suspected Chinese state linkage, and expert commentary.
<https://www.reuters.com/technology/popular-open-source-coding-application-targeted-chinese-linked-supply-chain-2026-02-02/>

6. Tom's Hardware

"Notepad++ update server hijacked in targeted attacks"

Coverage of update infrastructure compromise and threat actor speculation.

<https://www.tomshardware.com/tech-industry/cyber-security/notepad-update-server-hijacked-in-targeted-attacks>

7. TechRadar Pro

"Notepad++ hit by suspected Chinese state-sponsored hackers – what we know so far"

Summary reporting and confirmation of supply-chain vector and victim selectivity.

<https://www.techradar.com/pro/security/notepad-hit-by-suspected-chinese-state-sponsored-hackers-heres-what-we-know-so-far>

B.3 Tradecraft, Techniques, and Supporting Intelligence

These sources provide background validation for techniques observed in the campaign and historical Lotus Blossom operations.

8. Cisco Talos Intelligence

"Lotus Blossom espionage group"

Historical overview of Lotus Blossom tooling, C2 behavior, and targeting.

<https://blog.talosintelligence.com/lotus-blossom-espionage-group/>

9. Security Affairs

Coverage of DLL sideloading, infrastructure compromise, and China-linked APT analysis relevant to the Notepad++ campaign.

<https://securityaffairs.com/>

10. Living-off-the-Land (LOTL) Reference

Background on LOTL techniques leveraged by advanced threat actors.

<https://www.kiteworks.com/risk-compliance-glossary/living-off-the-land-attacks/>

B.4 Attribution and Analytical Confidence Notes

- Attribution to Lotus Blossom (G0030) is based on multi-factor correlation, including:
 - Geographic and sectoral victimology
 - Custom malware lineage (Elise → Sagerunex → Chrysalis)
 - Operational selectivity and restraint
 - Infrastructure and C2 grammar continuity
- No single source alone asserts attribution with certainty; confidence derives from convergent analysis across multiple independent sources.

B.5 Citation Handling Notes

- No specific victim organizations are named in publicly available technical reporting; all victim references are sector- and country-level, consistent with source disclosures.

- Indicators of Compromise (Appendix A) are drawn from public reporting and are time-bound and perishable.
- This appendix reflects sources available as of February 2026; subsequent disclosures may refine or expand attribution and victimology.