Bookworm to Stately Taurus Using the Unit 42 Attribution Framework

Kyle Wilhoit ⋮ ⋮ 9/24/2025

Executive Summary

In the complex landscape of threat intelligence and research, understanding the tools used by threat actors is just as critical as identifying the actors themselves. How do we link specific malware to its operators? We present a case study that demonstrates the process using the Unit 42 Attribution Framework to analyze well-known malware and its ties to a formally named threat group.

We examine Bookworm, a notable malware family used by Stately Taurus, a Chinese advanced persistent threat (APT) group active since at least 2012. This group conducts cyberespionage campaigns targeting government and commercial entities across Europe and Asia.

The case study illustrates how the Unit 42 Attribution Framework helps us dissect and confirm the operational link between this specific malware and its consistent usage by Stately Taurus. We provide a transparent look into the analytical process, illustrating how we moved from analyzing the malware's code to understanding the adversary's broader operations.

We explore the methodologies we use to analyze Bookworm's characteristics and examine its use in Stately Taurus campaigns. We finally demonstrate how our structured framework enhances the precision and confidence in attributing not just activity, but the actor's tradecraft. This deep dive highlights the iterative nature of attribution and how confirming malware family associations strengthens our overall intelligence picture.

Palo Alto Networks customers are better protected from Bookworm malware through the following products:

- Cortex XDR and XSIAM
- Cloud-Delivered Security Services for the Next-Generation Firewall, including Advanced WildFire, Advanced Threat Prevention, Advanced URL Filtering and Advanced DNS Security

If you think you might have been compromised or have an urgent matter, contact the Unit 42 Incident Response team.

Related Unit 42 Topics **Stately Taurus**, Bookworm

A Quick Look Back: The Unit 42 Attribution Framework

Before we dive into the specifics of Bookworm and Stately Taurus, it's beneficial to briefly revisit the core tenets of the Unit 42 Attribution Framework. We developed this framework to introduce a systematic, evidence-based approach to the often-complex world of threat actor attribution. It moves beyond subjective assessments, providing a rigorous methodology to connect observed malicious activity to specific groups or individuals.

For the purpose of this case study, it's important to remember that our framework evaluates multiple dimensions of threat data including:

- Analyzing tactics, techniques and procedures (TTPs)
- Examining tooling and malware characteristics
- Examining operational security (OPSEC) practices
- Mapping network infrastructure
- Analyzing victimology
- Meticulously analyzing timelines

We then assess each piece of evidence using the Admiralty System, which assigns scores for reliability and credibility, ensuring that we build our conclusions on a robust foundation. We track and store all this information and data in our attribution table, which helps calculate a cumulative score to determine attribution confidence.

Additionally, the framework integrates the Diamond Model of Intrusion Analysis as a critical tool for mapping and correlating activities, particularly when building confidence to move from initial observations to definitive attribution claims. The model helps analysts organize raw data about an attack into four key categories:

- Adversary: The attacker
- Capability: The tools and techniques they used (like malware)
- Infrastructure: The systems they used to launch the attack (like servers or IP addresses)
- Victim: The target of the attack

In essence, the framework allows us to accumulate and weigh diverse intelligence data, leading to high-confidence attribution and a deeper understanding of adversary operations — precisely what we'll demonstrate with Bookworm.

Understanding Bookworm: A Brief Profile

To fully appreciate the links between the Bookworm malware family and Stately Taurus, it's essential to first establish a basic understanding of the Bookworm malware family itself. First observed in 2015, Bookworm functions primarily as an advanced remote access Trojan (RAT), granting its operators extensive control over compromised systems.

Its capabilities typically include:

- Executing arbitrary commands
- Manipulating files (upload/download)
- Exfiltrating data
- Establishing persistent access

Bookworm is known for its unique modular architecture, allowing its core functionality to be expanded by loading additional modules directly from its command-and-control (C2) server. This modularity makes static analysis more challenging, as the Leader module relies on other DLLs to provide specific functionality.

What makes many of our analyzed Bookworm samples particularly noteworthy from an attribution standpoint are some of their distinct technical characteristics and observed operational patterns. For instance, our analysis has frequently uncovered specific program database (PDB) paths embedded within Bookworm samples. A notable example includes the path:

- C:\Users\hack\Documents\WhiteFile\LTDIS13n\Release\LTDIS13n.pdb

Developers often inadvertently leave in these paths during compilation. They serve as attribution indicators, acting as unique fingerprints that can potentially link different malware variants or even different malware families developed by the same actor. We identified this specific PDB path in samples of ToneShell, another custom tool that has been associated with Stately Taurus.

Bookworm samples exhibit various methods for C2 communication, often leveraging legitimate-looking domains or compromised infrastructure to blend in with network traffic. A technique observed in recent Bookworm variants, mirroring ToneShell, involves packaging shellcode as universally unique identifier (UUID) strings. The malware then decodes these ASCII or Base64-encoded UUIDs into binary data and executes via legitimate API functions.

Initial Bookworm analysis from 2015 primarily noted DLL sideloading for payload execution. However, newer variants have adopted this UUID technique. While the source code for this UUID method is publicly available, its consistent application across Bookworm and ToneShell payloads offers another technical commonality that is important to pay attention to.

Understanding these technical characteristics of Bookworm provides the baseline for the attribution analysis that follows, where we will directly link these features to the activities of Stately Taurus.

The Link: Bookworm and Stately Taurus through the Framework's Lenses

Having established Bookworm's technical blueprint, we can apply the Unit 42 Attribution Framework to demonstrate the operational ties between the malware family and Stately Taurus. Broadly speaking, we are performing attribution based on the following:

- Threat actor TTPs, tooling and capabilities
- OPSEC consistency
- Network infrastructure overlaps
- Victimology and targeting
- Activity time frames

We will examine each in greater detail in the following sections.

Tactics, Techniques and Procedures (Diamond Model Alignment: Capability)

Tracking threat actor TTPs is an important aspect of attribution. In this case, the modus operandi observed in Bookworm usage frequently aligns with Stately Taurus's well-documented TTPs. For instance, initial access often involves highly tailored spear-phishing campaigns using enticing decoy documents, a hallmark of Stately Taurus's approach.

Post-compromise, Bookworm exhibits behaviors consistent with Stately Taurus's broader playbook, including establishing persistence as well as collecting and exfiltrating sensitive information. The group's focus on covert data collection and espionage is reflected directly in Bookworm's design and usage, particularly as seen in prior attack campaigns against a Southeast Asian government using Bookworm.

Mapping this activity to MITRE ATT&CK techniques is a useful mechanism for tracking over time and can also be used during the attribution process. For example, attackers have delivered both Bookworm and ToneShell via spear phishing (T0865) and executed it via DLL sideloading (T1574.001). These techniques should be considered during attribution with a very low weight due to the likelihood of multiple different actors using the same techniques.

Tooling and Capabilities (Diamond Model Alignment: Capability)

Beyond Bookworm itself, the presence of other distinct tools within compromised environments reinforces the Stately Taurus link. ToneShell is a tool that Unit 42 and other researchers have observed Stately Taurus exclusively using (the Capability (Tools) entry in the attribution table below). We've also observed the use of publicly available tools like Impacket in Bookworm-related incidents. This mirrors Stately Taurus's known tendency to incorporate legitimate or open-source tools into their attack chains for lateral movement and reconnaissance (The Capability (Tools) entry in the attribution table).

Operational Security (OPSEC) Consistency (Diamond Model Alignment: Adversary)

Stately Taurus is advanced but exhibits certain OPSEC patterns that prove valuable for attribution. The previously shared PDB path (C:\Users\hack\Documents\WhiteFile\LTDIS13n\Release\LTDIS13n.pdb) found in both Bookworm and ToneShell samples is a prime example of an OPSEC consistency (the Malware Artifact (unique) entry in the attribution table) finding that could be valuable for attribution.

The discovery of these samples being compiled just eight weeks apart (ToneShell on Sep. 1, 2022, and Bookworm on Oct. 26, 2022) strongly suggests the involvement of the same developer. Such unique build artifacts and close

compile times provide an internal fingerprint of the Stately Taurus development environment.

ToneShell and Bookworm are both custom tools that share specific shellcode loading techniques, such as the aforementioned UUID method, which is another indicator of a shared development methodology.

Network Infrastructure (Diamond Model Alignment: Infrastructure)

One of the most robust elements of attribution lies in shared infrastructure. It's crucial to recognize that different types of infrastructure carry varying analytical weight. For instance, while an IPv4 address can provide a temporary link, its attributional value is generally lower compared to a typically more persistent URL or domain.

IP addresses are commonly rotated quickly as part of an actor's operational security. This makes them more transient indicators from an attribution perspective.

Domains, especially those consistently used, often require greater investment and planning. This makes them stronger, more stable markers for attribution purposes.

Despite these nuances, our investigations revealed direct and significant overlaps in C2 infrastructure between Bookworm and ToneShell. For example, we observed specific IP addresses such as 103.27.202[.]68 and 103.27.202[.]87 resolving C2 domains for *both* Bookworm (e.g., update.fjke5oe[.]com, www.hbsanews[.]com) and ToneShell (e.g., www.uvfr4ep[.]com) (the Infrastructure (IPv4) entries in the attribution table). This shared infrastructure, particularly when involving custom tools known to be exclusive to Stately Taurus like ToneShell, demonstrates compelling evidence of a unified operational control.

Also, we observed certain URL paths (e.g., /v11/2/windowsupdate/redir/v6-winsp1-wuredir) used by PUBLOAD samples (another Stately Taurus-associated malware) in Bookworm-related campaigns, indicating cross-tool infrastructure reuse (the Infrastructure (URL) entries in the attribution table). It’s important to note that the URL path was meant to mimic a legitimate Windows Update URL, but they misspelled it, increasing its weight in infrastructure overlaps.

Victimology and Targeting (Diamond Model Alignment: Victim)

The victimology associated with Bookworm strongly aligns with Stately Taurus's targeting objectives. Our telemetry indicates that Bookworm has impacted governments in Southeast Asia and multiple organizations globally. This aligns with previous Stately Taurus campaigns, which have a well-documented history of focusing on government entities and critical infrastructure across Southeast Asia.

Based on the overlaps observed in recent activity, we have now confidently associated previously unattributed attacks on governments and organizations in Southeast Asia to Stately Taurus, as far back as nine years ago.

Timeline Analysis (Diamond Model Alignment: Adversary)

The operational timelines of Bookworm campaigns fit within the known activity periods of Stately Taurus activity. We first observed Bookworm attacking targets in a Southeast Asian government in July 2015. The malware's evolution, including changes in how its shellcode loads additional modules, has allowed attackers to package it in different form factors, with variants observed from 2015-2021 and 2022.

This deployment and adaptation of Bookworm, running in parallel with other Stately Taurus operations, showcases its long-term role in the actor's arsenal. It also points to a sustained, long-term commitment to its development and use by the group.

Evidence Scoring and Confidence Level in the Attribution Table

The collection and analysis of evidence, as detailed in the previous sections, forms the backbone of the Unit 42 Attribution Framework. However, merely listing evidence is insufficient. Its true value is unlocked through a structured assessment of its reliability and credibility through our attribution table, which is shown in Figure 1 below.

This is precisely where the Admiralty System, as discussed in our previous article, demonstrates a core component of the Unit 42 Attribution Framework. It provides a standardized method for evaluating each piece of data, allowing us to build a comprehensive picture of confidence.

As a reminder, the Admiralty System assigns a two-character code to each evidentiary item: a letter (A-F) for **source reliability** and a number (1-6) for **information credibility**.

- **Source reliability (A-F):** This assesses the trustworthiness of the source itself. An A denotes a completely reliable source with a proven history, while an F indicates an unreliable or unjudged source. Internal telemetry from Palo Alto Networks (PANW), for instance, typically starts with a high reliability score (e.g., A) due to its direct and controlled nature. Public research, depending on the reputation of the reporting entity and the depth of their analysis, might receive a C or B. This can be analyst adjusted based on preference.
- **Information credibility (1-6):** This evaluates the truthfulness and consistency of the information provided. A 1 means the information is confirmed by other independent sources and is logical, whereas a 6 means its truth cannot be judged.

Let's look at how the scores from our attribution table are interpreted when applying the Admiralty System to the analysis pertaining to Stately Taurus. Figure 1 below shows an example attribution table.

Diamond Model	Type	Source of Attribution	Value	Analysis	Overlaps	Suggested Score	Manual Admiralty	Suggested Score Total
Victim	Organization	Internal (PANW)	Government organizations	Prior attack campaigns using bookworm impacted	https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government	A5	A5	58.4
Capability	Malware Artifact (unique)	Internal (PANW)	C:\Users\hack\Documents\WhiteFile\LTDIS13n\Release\LTDIS13n.pdb	ToneShell and Bookworm samples have the same PDB path b382cc85eee95a620fc11370309ff76de9a3bcaefb645790434d8251a3b9fce1 (ToneShell) and fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81 and a229a2943cf8d1b073574f0c050ca06392d0525b2028f4b4b04d1e4b40110c66 (Bookworm). ToneShell is a custom tool known to be used by only Stately Taurus		A2	A2	
Infrastructure	IPv4	Internal (PANW)	103.27.202[.]68	IP address resolved Bookworm C2 update.fjke5oe[.]com and ToneShell C2 www.uvfr4ep[.]com. ToneShell is a custom tool known to be used by only Stately Taurus		A4	A4	
Infrastructure	IPv4	Internal (PANW)	103.27.202[.]87	IP address resolved Bookworm C2 www.hbsanews[.]com for a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927 and ToneShell C2 www.uvfr4ep[.]com. ToneShell is a custom tool known to be used by only Stately Taurus		A4	A4	
Infrastructure	URL	Public Research	/v11/2/windowsupdate/redir/v6-winsp1-wuredir	URL used by PUBLOAD sample associated with Mustang Panda (Stately Taurus)	https://lab52.io/blog/new-mustang-pandas-campaing-against-australia/	C3	C3	
Infrastructure	URL	Public Research	/v11/2/windowsupdate/redir/v6-winsp1-wuredir	URL used by PUBLOAD sample associated with Mustang Panda (Stately Taurus)	https://csirt-cti.net/2024/01/23/stately-taurus-targets-myanmar/	C3	C3	
Capability	Tools (Public)	Internal (PANW)	Use the publicly available source code from https://research.nccgroup.com/2021/01/23/rift-analysing-a-lazarus-shellcode-execution-method/	TONESHELL payload (ab9d8f1021f2a99c74aa66f8ddb52996ac2337da9de2676d090b87e19ce93033) uses UUID for it's payload, so has Bookworm (cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86, 5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b, fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81)		A5	A5	
Capability	Tools (Public)	Internal (PANW)	b000a0095a8fda38227103f253b6d79134b862a83df50315d7d9c5b537fd994b	Impacket sample seen in Bookworm incident	https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian-government/	A5	A5	

Figure 1. Bookworm attribution table.

- **A5 (Victim - Organization)**: For the entry on the victim organization, the score of A5 indicates an A (completely reliable) source, which is our internal Palo Alto Networks telemetry. However, the information credibility is a 5 (improbable). This might seem counterintuitive. However, it reflects that while the source is impeccable, the specific *details* of an *ongoing, singular* victim engagement might be hard to fully confirm across all facets. It might also be a general observation that is highly probable but not yet fully confirmed by multiple, independent lines of evidence at the highest level. It establishes a strong lead based on trusted internal data but acknowledges room for further corroboration.
- **A2 (Capability - Malware Artifact (unique))**: The shared PDB path (C:\Users\hack\Documents\WhiteFile\LTDIS13n\Release\LTDIS13n.pdb) between Bookworm and ToneShell receives an A2. This signifies an A (completely reliable) internal source (PANW) and 2 (probably true) information. The consistency of this unique artifact across different malware samples, especially when paired with close compile times, makes the conclusion of a shared development environment highly probable.
- **A4 (Infrastructure - IPv4):** For the IP addresses 103.27.202[.]68 and 103.27.202[.]87 resolving both Bookworm and ToneShell C2s, both receive an A4. This means an A (completely reliable) internal source (PANW), but the information is 4 (doubtfully true) in terms of its long-term persistence or exclusivity. This tells us that while internal Unit 42 data confirms the resolution, IP addresses are commonly rotated quickly as part of actor activity. Therefore, without additional corroborating evidence of their sustained or unique use, we often assign them a default credibility score of 4 (this can be changed based on valid analyst justification). It's still strong due to the reliable source but indicates a need for continued monitoring and fresh intelligence to maintain its relevance.
- **C3 (Infrastructure - URL):** The URLs used by PUBLOAD samples associated with Stately Taurus, referenced by public research, score C3. This implies a C (fairly reliable) source (public research, like lab52.io or csirt-cti.net) and 3 (possibly true) information. Public reports are generally reliable but require Unit 42 validation and cross-referencing to elevate the credibility, hence “possibly true” rather than “probably true” without additional internal corroboration.
- **A5 (Capability - Tools (Public)):** The observation that ToneShell and Bookworm payloads use UUIDs, leveraging publicly available source code, receives an A5. Again, an A (completely reliable) internal source. However, the information about the UUID *usage by these specific malware families* is 5 (improbable) to be unique or definitive enough on its own for strong attribution, as the underlying technique is public. This

highlights the framework's nuance: a tool being public doesn't diminish source reliability, but it can affect the *credibility* of that specific tool as a *unique* attribution point.
- **A5 (Capability - Tools (Public)):** Similarly, the Impacket sample seen in a Bookworm incident, also from an internal PANW source, gets an A5. While Impacket is a common tool, its consistent appearance in Stately Taurus's specific operational context is important, but its general availability makes it “improbable” as a standalone, high-credibility indicator without other corroborating evidence.

The true strength of the Admiralty System, however, lies not in any single score, but in its cumulative effect and associated calculations in the attribution table. Individual pieces of evidence or data may carry varying levels of certainty. But it’s the volume and consistent pattern of high-scoring evidence across multiple categories (i.e., TTPs, tooling, OPSEC, infrastructure, victimology) that allow us to confidently attribute Bookworm's usage to Stately Taurus.

Using a proprietary formula in the attribution table that aggregates the weighted Admiralty scores from the attribution table, we calculate an overall confidence score for the attribution claim. This helps us create estimative language that is accurate and based on technical facts.

Our confidence ranges are defined as follows:

- **Low confidence:** 0-8
- **Moderate confidence:** 8-32
- **High confidence:** 32 +

For this specific case study, the evidence presented in our attribution table yields a score of 58.4. This definitively places the attribution of Bookworm's operations to Stately Taurus within the high-confidence range. The presence of multiple A2, A4 and A5 scores, particularly when cross-referenced and corroborated by external C3 scores, builds a sufficient body of evidence. This systematic scoring process ensures transparency, reduces bias and provides a clear audit trail for our attribution conclusions, moving us beyond mere conjecture.

Conclusion

This case study on Bookworm and Stately Taurus demonstrates the power and precision of the Unit 42 Attribution Framework. We've traced how a systematic, evidence-based approach allowed us to move beyond mere observations to definitively link the Bookworm malware family to the operations of Stately Taurus.

Through the analysis of:

- Shared PDB paths
- Consistent tooling (like ToneShell)
- Overlapping infrastructure
- Historical victimology in Southeast Asia
- Synchronized timelines

Each piece of evidence, scored with the Admiralty System, contributed to a high-confidence attribution of 58.4.

This level of detailed and confirmed attribution is not merely an academic exercise. It carries profound implications for the broader cybersecurity research and threat intelligence community.

By openly sharing our methodology and its practical application, we aim to:

- **Improve collaboration and consistency:** Providing a common language and framework for analysts across different organizations, fostering more consistent and less ambiguous threat reporting.
- **Enhance analytical rigor:** Offering a model for thorough, evidence-based analysis, elevating the overall quality and defensibility of attribution claims.
- **Facilitate proactive research:** Enabling fellow researchers to build upon established links, focusing their efforts on deeper dives into actor capabilities, evolving TTPs, and emerging campaigns.
- **Strengthen collective intelligence:** Contributing to a more accurate, unified and actionable global understanding of threat actor operations, benefiting all defenders.

The enduring activity of Stately Taurus, coupled with the continued evolution of malware like Bookworm, underscores the necessity of continuous monitoring and a systematic attribution methodology. As adversaries adapt, so too must our intelligence gathering and analysis, and crucially, our ability to communicate these findings with clarity and confidence.

Palo Alto Networks Protection and Mitigation

Palo Alto Networks customers are better protected from Bookworm malware through the following products:

- Advanced WildFire cloud-delivered malware analysis service accurately identifies the known samples as malicious.
- Advanced URL Filtering and Advanced DNS Security identify known URLs and domains associated with Bookworm activity as malicious
- The Next-Generation Firewall with the Advanced Threat Prevention security subscription can help block the attacks with best practices. Advanced Threat Prevention has an inbuilt machine learning-based detection that can detect exploits in real time.
- Cortex XDR and XSIAM are designed to prevent the execution of known malware, and also prevent the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.

If you think you may have been compromised or have an urgent matter, get in touch with the Unit 42 Incident Response team or call:

- North America: Toll Free: +1 (866) 486-4842 (866.4.UNIT42)
- UK: +44.20.3743.3660
- Europe and Middle East: +31.20.299.3130
- Asia: +65.6983.8730
- Japan: +81.50.1790.0200
- Australia: +61.2.4062.7950
- India: 000 800 050 45107

Palo Alto Networks has shared these findings with our fellow Cyber Threat Alliance (CTA) members. CTA members use this intelligence to rapidly deploy protections to their customers and to systematically disrupt malicious cyber actors. Learn more about the Cyber Threat Alliance.

Additional Resources

- Introducing Unit 42's Attribution Framework – Unit 42, Palo Alto Networks