

Under the Hood - LotusLite: Believe me I am MustangPanda

Published: 2026-06-09 · Archived: 2026-06-10 02:01:31 UTC

In this article, we will cover the following points:

- analysis of LotusLite 2026 (May) and links to previous versions
- affectionate messages from the malware author



Under the Hood - The new series where We share stories from our daily life as a malware hunter 🔍

We're kicking things off with a recent implant featuring **"BelievemeIamMustang-Panda"** and **"Hi,Mustang_Panda"** hardcoded in its `.data` section! A C2 over `forms.microsoft.com:443` that deliberately bypasses all TLS validation. That's unusual, and that means it's interesting!

The sample: [47e51e82229e80a387c3cb100d39d3705e6360bbf9bfa1601dbc484e8d02e653](https://www.exatrack.com/samples/47e51e82229e80a387c3cb100d39d3705e6360bbf9bfa1601dbc484e8d02e653)

Technical Analysis

INSTALLATION

To activate the dropper, the binary must be executed by calling the exported function **"AMPVIncrement"**. This function creates the directory `C:\ProgramData\SmartPrint\` and drops the executable **"SmartPrintScreen.exe"** into it, which is simply a copy of the currently running executable. Interestingly, the DLL appears to be impersonating **"AMPV.dll"**, a DLL seemingly used in "Samsung Series" software, which would be consistent with this masquerading attempt. A persistence entry is placed in the registry key

HKCU\Software\Microsoft\Windows\CurrentVersion\Run under the value DadaBank, pointing to the freshly dropped executable and using the argument `--DaDaBar`. It then displays a MessageBox reading: *“Error: The Pdf file is corrupted. Please restart your computer and try again, or contact the original author.”* The DLL is therefore likely designed to impersonate the opening of a PDF file.

This file appears to be packaged in a zip archive along with its legitimate, signed loader, and sent by email using appealing headlines. In this case, the zip filenames is “Conference_invitation” and the legitimate executable is named “Ph-china_Joint_Ministerial_Meeting.Scr”. This pattern corresponds to those described in the Acronis blog articles that we will discuss shortly.

AGENT (–DaDaBar)

On startup, the implant checks for a mutex named **“BelievemeIamMustang-Panda”** to ensure it is the first instance running. It then verifies its own execution path (as seen above) and confirms it is being run with the `--DaDaBar` argument. If both conditions are met, it fingerprints the machine and prepares a buffer as follows:

`[USERNAME]|[COMPUTERNAME]` This buffer is sent to the server using the following communication protocol: `[magic:4][cmd:4][len:4][data:...]`, where the magic is an integer: **0xB2EBCFDF**. Connections are made every 0.5 seconds, making this a fairly noisy implant.

C2 PROTOCOL

The malware establishes a connection to `103.79.77[.]181`, an IP address located in Singapore. The HTTP connection is initialized while spoofing a Microsoft domain:

```
POST https://forms.microsoft.com/info/faq/v6
Cookie: JSESSIONID=x-ms-cpim-geo
Host: forms.microsoft.com
Referer: https://www.google.com/
User-Agent: Mozilla / 5.0 (Windows NT 10.0; Win64; x64) AppleWebKit / 537.36 (KHTML, like Gecko) Chrome / 147.0.

[0xB2EBCFDF][cmd:4][len:4][data:len]
```

All TLS verification is of course disabled on the client side before the connection is initialized (otherwise, alerts would be generated).

COMMAND DISPATCHER

The magic **0xB2EBCFDF** is verified on every received frame. If absent, the loop breaks silently. The supported commands are as follows:

ID	Command
1	Write to <code>cmd.exe</code> stdin

ID	Command
3	Directory listing
6	Terminate the session
10	Create a hidden <code>cmd.exe</code> and redirect its I/O
11	Kill the <code>cmd.exe</code>
13	Change current directory
14	Write an arbitrary file

We are therefore dealing with a fairly simple yet complete toolbox!

ANTI-ANALYSIS

API resolution: All WinINet, kernel32, shell, and process APIs are resolved at runtime via a PEB walk mechanism. The only visible static import is `GetModuleHandleA("ntdll.dll")`.

Numerous strings are decrypted on the fly, making generic identification of the implant significantly more difficult.

GO DEEPER - CTI

This malware is particularly interesting given its properties. Beyond its capabilities, the code is peppered with references to China, such as:

- BankChina
- BankofChina
- Bankofchinaunionpaycard

But also to pandas:

- BelieveMeIamMustang-Panda (the mutex)
- Hi, Mustang_Panda

The binary shares numerous similarities with the analysis published on May 13, 2026, at <https://0x30bad.github.io/posts/lotuslite-backdoor-writeup/>, titled “**MustangPanda New Backdoor LotusLite**”.

We can list the following overlaps:

- The same IP address
- The same HTTP headers
- The same magic value
- The same dropper directory
- The same command list, with the same command IDs

- The API version has been updated (`/info/faq/v5` -> `/info/faq/v6`)

Even earlier, on January 15, 2026, Acronis published on previous implant

<https://www.acronis.com/en/tru/posts/lotuslite-targeted-espionage-leveraging-geopolitical-themes/> which appears to be a second version but with a different versioning format (`/api/v2/updates`). Then, on April 21, 2026, Acronis published <https://www.acronis.com/en/tru/posts/same-packet-different-magic-mustang-panda-hits-indias-banking-sector-and-korea-geopolitics/>, this time with a v1 in the expected `/info/faq/v1` format.

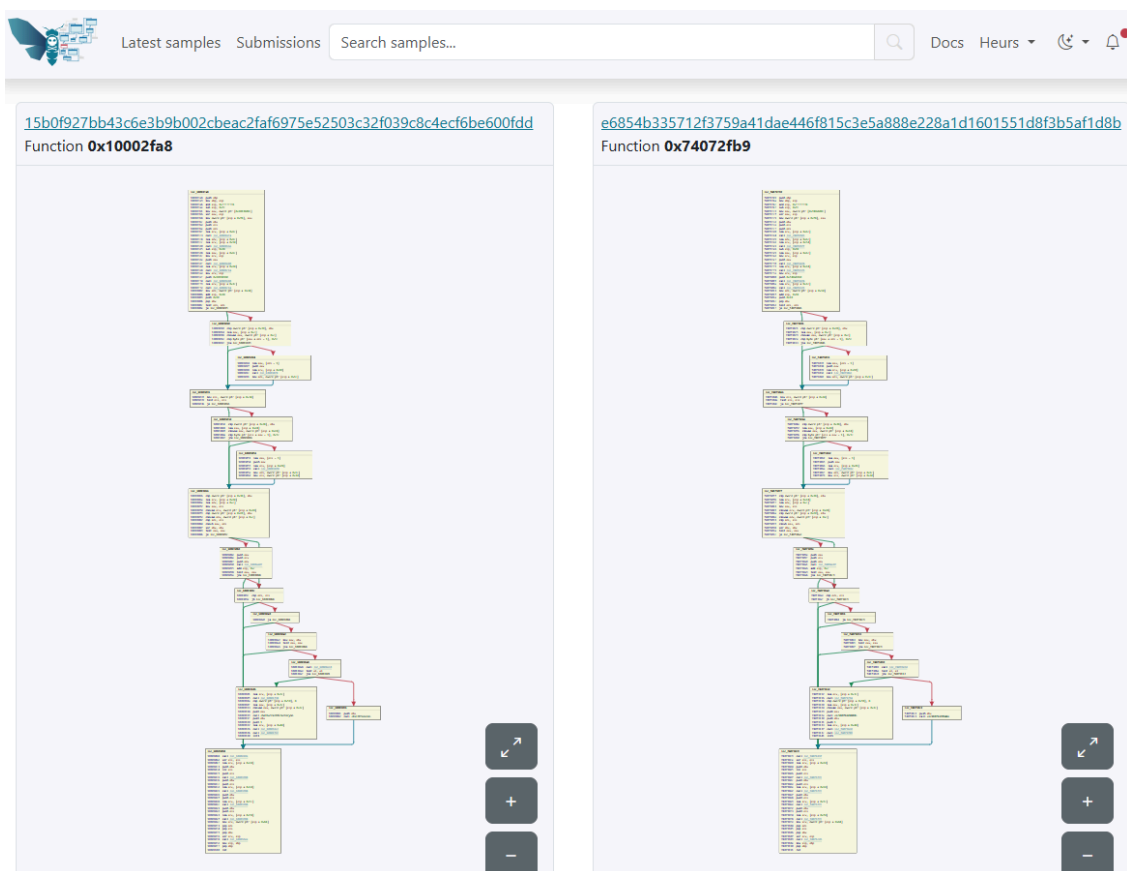
Under normal circumstances we would say everything points to MustangPanda, BUT two things genuinely complicate that assessment. First, the unabashed announcement of MustangPanda within the new version itself, which would be surprising if this were actually that threat actor. Second, we found no code overlap on Exalyze between v5 and v6, which would imply deep-reaching changes across all major functions. The binaries have also shrunk from 350KB to 260KB - it is quite unusual for an update to result in a size reduction - whereas previous versions did show code overlap with one another.

A May 28 update - [15b0f927bb43c6e3b9b002cbeac2faf6975e52503c32f039c8c4ecf6be600fdd](#) - provides further information (the binary had started getting detected fairly well, hitting 15 detections on VirusTotal, so the author updated it and dropped back down to 1):

- New strings, such as **“Fu-ck-China-because-China-Sucks”**
- Code overlap with the version we analyzed
- An updated API version: `/info/faq/v7`

We also have features shared between version 6 and version 7, but not 5, as you can see in the Exalyze screenshot:

Matching functions	8	Matched samples
0x10001241	2	Function 0x10002fb9 Sample 47e51e82229e80a387c3cb100d39d3705e6360bbf9bfa1601dbc484e8d02e653 Capabilities
0x100018b4	1	
0x10001da3	1	
0x10002b6e	2	Function 0x74072fb9 Sample e6854b335712f3759a41dae446f815c3e5a888e228a1d1601551d8f3b5af1d8b Capabilities
0x10002ec0	1	
0x10002fa8	2	
0x1000428b	2	



The diffing is [here](#).

We therefore suspect that this malicious actor has either made considerable efforts to reproduce LotusLite, or updated its code following the public disclosure of its implant, and used these phrases as a “FalseFlag” (a bit direct), or has taken it very badly to be associated with MustangPanda.

Indicators of Compromise (IOCs)

SHA256	Version
15b0f927bb43c6e3b9b002cbeac2faf6975e52503c32f039c8c4ecf6be600fdd	v7
47e51e82229e80a387c3cb100d39d3705e6360bbf9bfa1601dbc484e8d02e653	v6
e6854b335712f3759a41dae446f815c3e5a888e228a1d1601551d8f3b5af1d8b	v6
8dd7d6472771db5b82cfc87adcb03b303fcd8f16462700ce6ff63f3d935348d9	v5
0312e58fec7c03fdaad929333743be36d77fcea394ebb42a3110ff0269a9448	v5
c5c667c3e74cd063043e444bd9d9239adac4d31ac047361122267b77043c3581	v5
6cd52ea299e99e3cf4a175b83a35b5a2516ce44a2c3c43b9d7a152753258998c	v1
2c34b47ee7d271326cfff9701377277b05ec4654753b31c89be622e80d225250	(previous) v2

SHA256	Version
2c69daf837b446ab8ea41d0aba93ad027003cc51f7e5e630a159fd9ee25cf81e	Dropper

Yara rule detecting LotusLite:

```
rule NotMustangPanda_LotusLite {
  meta:
    description = "Lotuslite implant"
    sha256      = "47e51e82229e80a387c3cb100d39d3705e6360bbf9bfa1601dbc484e8d02e653"
    date        = "2026-06-03"
    author      = "Heurs"
  strings:
    $pattern_1 = { DF CF EB B2 }
    $pattern_2 = /\info\faq\v[1-9]/ wide
    $pattern_3 = "x-ms-cpim-geo" wide
    $pattern_4 = "Bankofchinaunionpaycard" ascii
  condition:
    uint16(0) == 0x5A4D and (2 of ($pattern_*))
}
```

Source: https://blog.exatrack.com/UnderTheHood_Believe_me_I_am_MustangPanda/