Mustang Panda PlugX - 45.251.240.55 Pivot

blog.xorhex.com/blog/mustangpandaplugx-1/

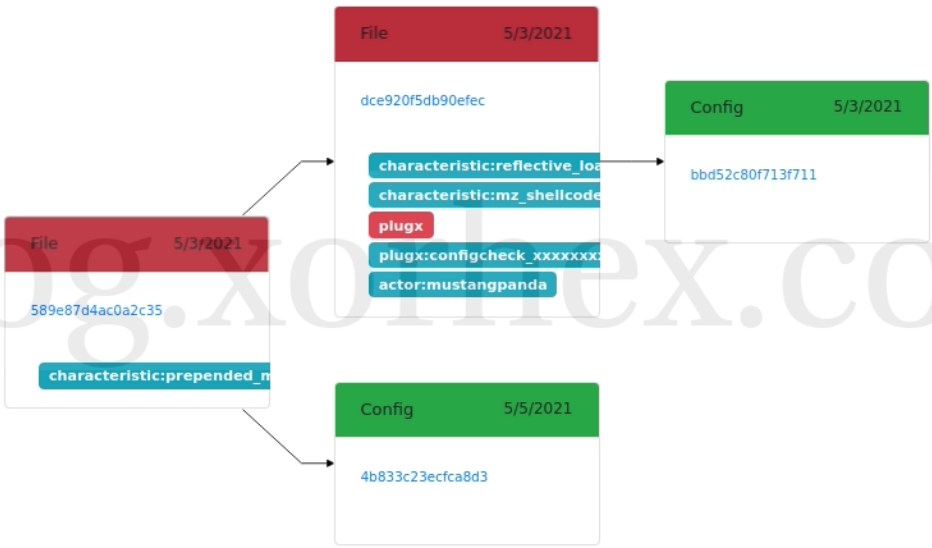
xorhex

Focus on Threat Research through malware reverse engineering

New Mustang Panda PlugX sample compared with prior Mustang Panda/RedDelta PlugX samples

May 17, 2021
xorhex

6-Minute Read



Family	PlugX
Threat Actor	Mustang Panda
Encrypted	589e87d4ac0a2c350e98642ac53f4940fcfec38226c16509da21bb551a8f8a36

Decrypted	dce920f5db90efecc7fb7a6b6399c80fc83e3f1251f160cd1295b6a4b67125d4

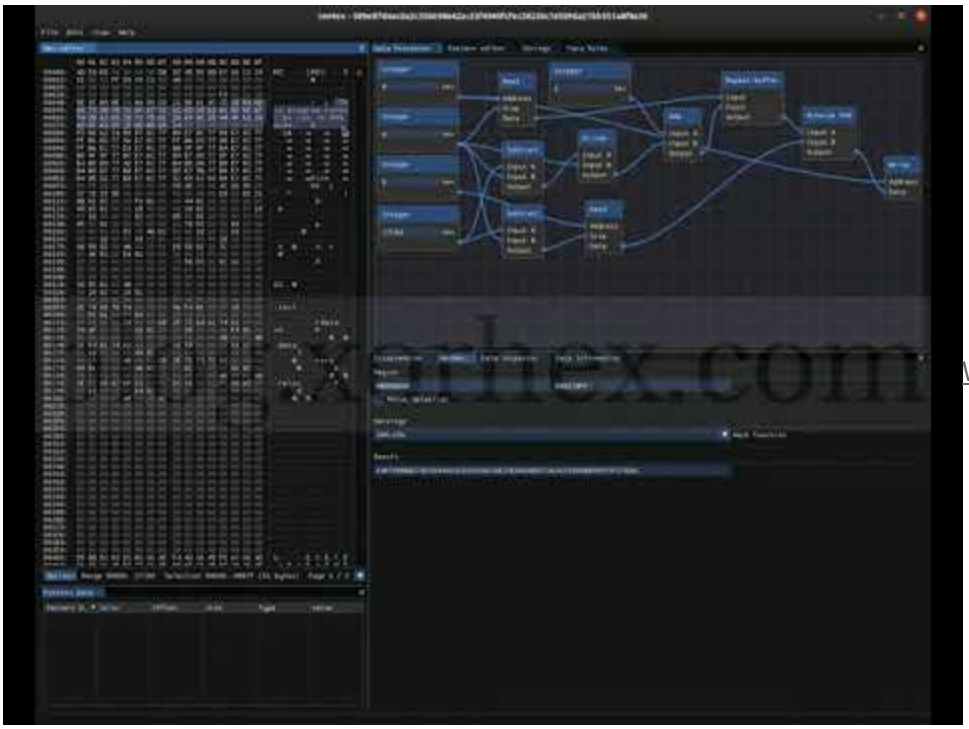
Summary

On 2021-05-01 another encrypted Mustang Panda PlugX binary was uploaded to VirusTotal.

Like the other samples, this encrypted PlugX file used a 10 byte prepended XOR key (a null byte seperates the key from the encrypted contents).

> 10 Byte XOR Key: `0x47, 0x45, 0x48, 0x47, 0x7a, 0x67, 0x5a, 0x6e, 0x75, 0x6d`

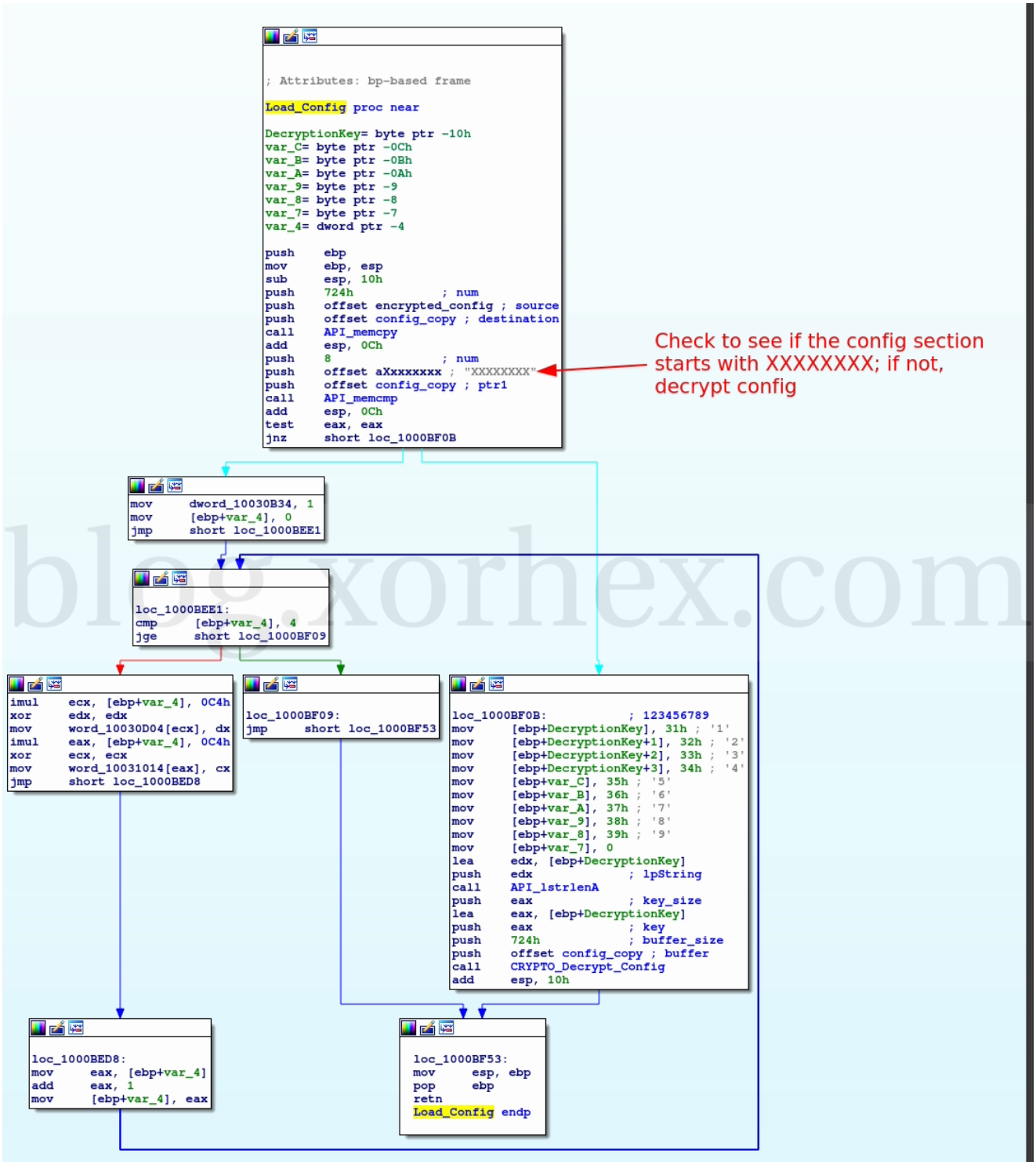
The decrypted file continues to embed shell code in the MZ header. The video below shows the decryption process and the embedded shell code at the begining of the file.



Watch Video At:

https://youtu.be/Ua82pW6439M

This instance of PlugX checks for `XXXXXXXX` at the start of the config section. The RedDelta varient uses `########` instead of 8 Xs.



The extracted config contains values seen in prior Mustang Panda PlugX files.

```
{
    "config": {
        "cncs": [
            {
                "num": 1,
                "host": "45.251.240.55",
                "port": 443
            },
            {
                "num": 1,
                "host": "45.251.240.55",
                "port": 8080
            },
            {
                "num": 1,
                "host": "45.251.240.55",
                "port": 8080
            },
            {
                "num": 1,
                "host": "45.251.240.55",
                "port": 443
            }
        ],
        "mutex": "eZlapRxpEQvscgtWBqqr",
        "sleep": 1000,
        "folder": "AAM UpdatesBif"
    },
    "extracted_from_sha256":
"dce920f5db90efecc7fb7a6b6399c80fc83e3f1251f160cd1295b6a4b67125d4"
}
```


Let's see what other sample we have that are similar.

Related Samples

Using data points extracted from our sample set, I filtered down the related samples based upon the ones with a matching IP addresses. The interactive visualization below shows the related samples and any property extracted where it was used by two or more samples.

IP Pivot

Content Loading..

Click a Node to Load Details Below

We identified 40 additional PlugX samples upon expanding our pivot to include samples that also matched on these properties. Theese samples span across both the `XXXXXXXX` and `########` varients.

Expanded IP Pivot

Content Loading..

Click a Node to Load Details Below

This actually encompasses all of the MustangPanda/RedDetla PlugX samples I've in my collection at this time.

Note: I'm still building out my collection, so overtime it will be apparent which property values are worth pivoting on and which ones are not.