Mustang Panda PlugX - Reused Mutex and Folder Found in the Extracted Config

blog.xorhex.com/blog/mustangpandaplugx-2/

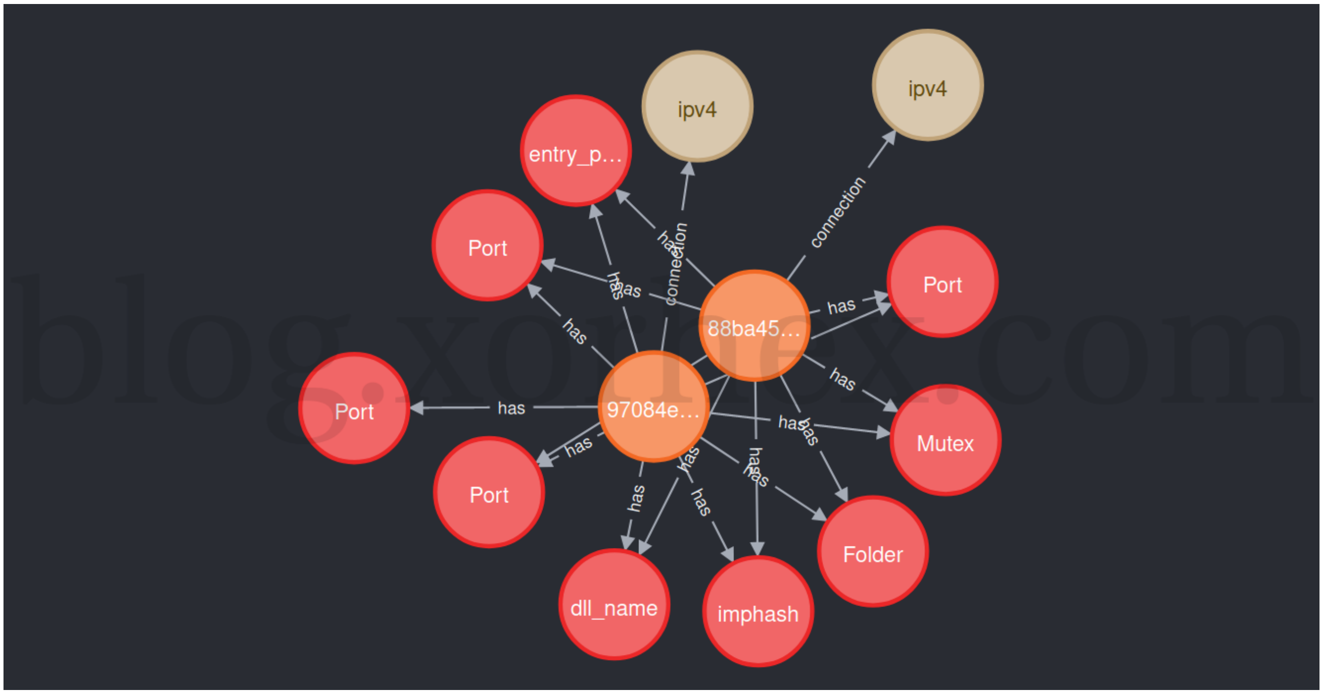
xorhex

Focus on Threat Research through malware reverse engineering

New Mustang Panda PlugX sample containing overlapping properties uploaded to VirusTotal.

May 27, 2021
xorhex

3-Minute Read



Family	PlugX - Variant: XXXXXXXX Config Check
Threat Actor	Mustang Panda / Red Delta

Encrypted	de0f65a421ce8ee4a927f4f9228f29ff12be69ac71edecb18c35cb5101e4c3cf
Decrypted	2bfd100498f70938dedef42116af09af2db77ef1315edcea0ffd62c93015ddf5
XOR Decyption Key	0x4b, 0x73, 0x51, 0x4f, 0x74, 0x6d, 0x49, 0x68, 0x63, 0x43
XOR Decryption Key Length	10

Summary

On 2021-05-26 another encrypted Mustang Panda PlugX binary was uploaded to VirusTotal.

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

```
{
    "config": {
        "cncs": [
            {
                "num": 1,
                "host": "103.192.226.100",
                "port": 80
            },
            {
                "num": 1,
                "host": "103.192.226.100",
                "port": 110
            },
            {
                "num": 1,
                "host": "103.192.226.100",
                "port": 8080
            },
            {
                "num": 1,
                "host": "103.192.226.100",
                "port": 5938
            }
        ],
        "mutex": "MvyShgFjKjaJsMinCCgJ",
        "sleep": 1000,
        "folder": "AvastSvcZEg"
    },
    "extracted_from_sha256":
"2bfd100498f70938dedef42116af09af2db77ef1315edcea0ffd62c93015ddf5"
}
```

Related Samples

This sample reuses both the Folder name and Mutex which were also found in the prior identified sample: e4981316b5fc251a5cea5d941303046dad13a9b993006ec07ff7727b17e0e17b.

Config Pivot

Content Loading..

Click a Node to Load Details Below