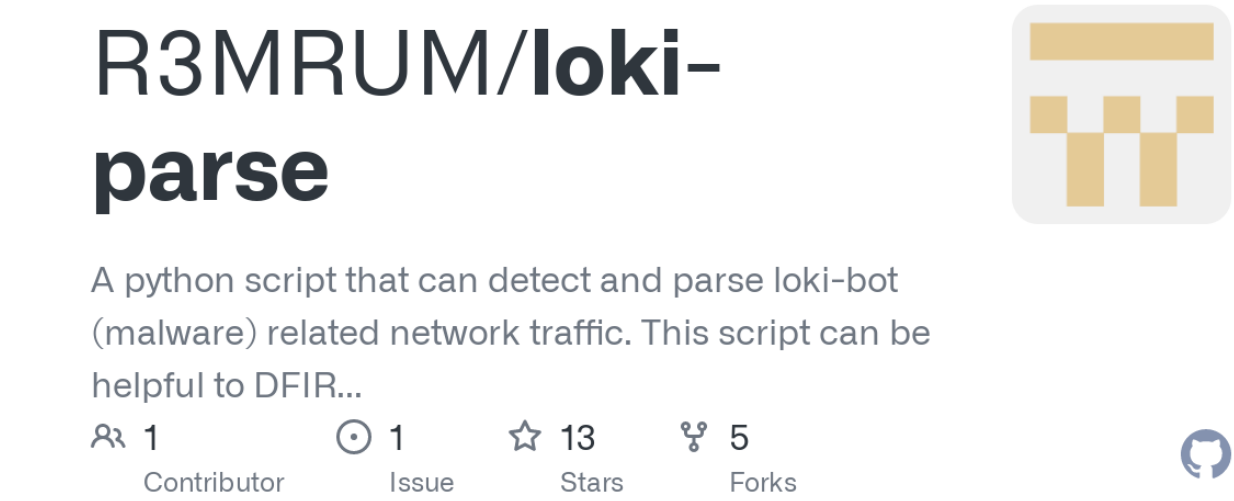
R3MRUM/loki-parse: A python script that can detect and parse loki-bot (malware) related network traffic. This script can be helpful to DFIR analysts and security researchers who want to know what data is being exfiltrated to the C2, bot tracking, etc...

github.com/R3MRUM/loki-parse

R3MRUM



loki-parse

A python script that can detect and parse loki-bot (malware) related network traffic between a compromised host and a C2 server. This script can be helpful to DFIR analysts and security researchers who want to know what data is being exfiltrated to the C2, bot tracking, etc...

This script can either sniff the wire directly (no switch) or read in a PCAP of network traffic (using --pcap $pcap_file) . When the script detects loki-bot related network traffic, it will dump out the data contained within the packets out to the screen in JSON format.

Some of the packets contain data being exfiltrated that is compressed with aPLib. The script will decompress that data and display it to your screen but know that there is additional processing that has not been incorporated into this script...YET. This being said, **it is important that you also download the aplib.py script and keep it in the same directory as loki-parse.py**. This script is required in order for loki-parse to execute successfully.

Finally, there is an issue with the code used for sniffing network traffic where the data portion of the packet can get chopped off. It appears to be related to how scapy parses the traffic. This will likely happen with larger packets that have compressed data. If this happens, the following dictionary key will be created:

Decompressed Application/Credential Data': 'ERROR: Incomplete Packet Detected

This issue does not seem to occur within saved PCAPs so, if you receive this error, try saving the network traffic into a pcap file and rerunning loki-parse on the pcap.

If the script is able to successfully decompress the data within the packet, this data is simply dumped to the screen (not in JSON format). I plan to address this in later versions.

I've provided **loki-bot_network_traffic.pcap** as an example pcap for you to play with.

Example Output

$ sudo ./loki_parse.py

Sniffing PCAPS from the wire

```
{
    "Compromised Host/User Data": {
        "Compressed Application/Credential Data Size (Bytes)": 2310,
        "Compression Type": 0,
        "Data Compressed": true,
        "Encoded": false,
        "Encoding": 0,
        "Original Application/Credential Data Size (Bytes)": 8545
    },
    "Compromised Host/User Description": {
        "64bit OS": false,
        "Built-In Admin": true,
        "Domain Hostname": "REMWorkstation",
        "Hostname": "REMWORKSTATION",
        "Local Admin": true,
        "Operating System": "Windows 8.1 Workstation",
        "Screen Resolution": "3440x1440",
        "User Name": "REM"
    },
    "Malware Artifacts/IOCs": {
        "Binary ID": "XXXXX11111",
        "Loki-Bot Version": 1.8,
        "Mutex": "B7E1C2CC98066B250DDB2123",
        "Potential Hidden File [Hash Database]": "%APPDATA%\\C98066\\6B250D.hdb",
        "Potential Hidden File [Keylogger Database]":
"%APPDATA%\\C98066\\6B250D.kdb",
        "Potential Hidden File [Lock File]": "%APPDATA%\\C98066\\6B250D.lck",
        "Potential Hidden File [Malware Exe]": "%APPDATA%\\C98066\\6B250D.exe",
        "Unique Key": "g5cy2",
        "User-Agent String": "Mozilla/4.08 (Charon; Inferno)"
    },
    "Network": {
        "Data Transmission Time": "2017-04-27T15:03:20.921806",
        "Destination Host": "185.141.27.187",
        "Destination IP": "185.141.27.187",
        "Destination Port": 80,
        "First Transmission": true,
        "HTTP Method": "POST",
        "HTTP URI": "/danielsden/ver.php",
        "Source IP": "172.16.0.130",
        "Source Port": 49344,
        "Traffic Purpose": "Exfiltrate Application/Credential Data"
    }
}
```