malware-cfg/ToxicEyeRAT at main · albertzsigovits/malware-cfg

By albertzsigovits

Archived: 2026-04-05 22:58:03 UTC

ToxicEyeRAT malware configuration extraction

Script

```
# Potential improvements
# Instead of hardcoded anchor-strings, use entrypoint +offsets for finding config

import os
import sys
import re
import pefile
from pathlib import Path

def is_pe_file(file_path):
    try:
        pefile.PE(file_path)
        return True
    except:
        return False

def extract_wide_strings(file_path, min_length=4):
    with open(file_path, 'rb') as f:
        data = f.read()

    strings = []
    current_string = ''
    i = 0
    while i < len(data) - 1:
        if data[i+1] == 0 and 32 <= data[i] <= 126:
            current_string += chr(data[i])
            i += 2
        else:
            if len(current_string) >= min_length:
                strings.append(current_string)
            current_string = ''
            i += 1

    if len(current_string) >= min_length:
```

```
        strings.append(current_string)
    #print(strings)
    return strings

def find_config(strings):
    cfg_info = {}
    for i, s in enumerate(strings):
        if ".json" in s:
                cfg_info['Bitcoin'] = strings[i + 1]
                cfg_info['Etherium'] = strings[i + 2]
                cfg_info['Monero'] = strings[i + 3]
        if "JSON Parse: Quotation marks seems to be messed up." in s:
                cfg_info['InstallPath'] = strings[i + 1]
                cfg_info['AutorunName'] = strings[i + 2]
        if "Number is greater than connected displays." in s:
                cfg_info['BotID'] = strings[i + 1]
                cfg_info['ChatID'] = strings[i + 2]
    return cfg_info

def process_folder(folder_path):
    for root, _, files in os.walk(folder_path):
        for file in files:
            file_path = Path(root) / file
            if is_pe_file(file_path):
                print(f"PE file found: {file_path}")
                strings = extract_wide_strings(file_path)
                config = find_config(strings)
                if config:
                    for key, value in config.items():
                        print(f"  {key.capitalize()}: {value}")
                else:
                    print("No CFG Information found")

if __name__ == "__main__":
    if len(sys.argv) != 2:
        print("Usage: python script.py ")
        sys.exit(1)

    folder_path = sys.argv[1]
    if not os.path.isdir(folder_path):
        print(f"Error: {folder_path} is not a valid directory")
        sys.exit(1)

    process_folder(folder_path)
```

Output

```
PE file found: samples/2e53a6710f04dd84cfd3ac1874a2a61e690568405f192e7cbf8a4df12da334c4
  Installpath: C:\Users\ToxicEye\rat.exe
  Autorunname: Chrome Update
  Bitcoin: 1DJ5VetDBuQnmDZjRHRgEiCwYwvc6PSwu8
  Etherium: 0x357C0541F19a7755AFbF1CCD824EE06059404238
  Monero: 42Pwy6Xe4mPTz3mLap7AB5Jjd9NBt1MWjiqyvEFx3Fn8Fo9cRw9aJUHE1iTXEpUbQacMNiSxYejBKFE7UdGnyEncEE
  Botid: 5981399083:AAEHnXdvbepNaf6NW5inPfw0j_A5k_d0F-o
  Chatid: 5564760978
PE file found: samples/4ea7e73f2854efa48c46ec1d99b647c0bbd274b32d183beaec0d5e8774e5005f
  Installpath: C:\Users\autoupdate\update.exe
  Autorunname: Chrome Update
  Bitcoin: bc1qgsw0j06uy72euer9calppr4mtlu9826ugkzyel
  Etherium: 0xCB3Fe4B92f74A16592576bE186B8b39C10a0811F
  Monero: GBYAVJXEOMMUEF3G6F7XJOBD5LYWO47R7Z7FV6RHPKXGOGH7IHKJD2EE
  Botid: 5498387673:AAF0PqxFYWRu0ioPVaK-ZP5umyKlFVXVajM
  Chatid: 637293597
PE file found: samples/294e5efb8db8a8e1112e2890a6ea945e7920e3d4f83c4c81c9ace8cec6306020
  Installpath: C:\Windows\System32\Sub302\svchost.exe
  Autorunname: Java Update
  Bitcoin: 1DJ5VetDBuQnmDZjRHRgEiCwYwvc6PSwu8
  Etherium: 0x357C0541F19a7755AFbF1CCD824EE06059404238
  Monero: 42Pwy6Xe4mPTz3mLap7AB5Jjd9NBt1MWjiqyvEFx3Fn8Fo9cRw9aJUHE1iTXEpUbQacMNiSxYejBKFE7UdGnyEncEE
  Botid: 5245693641:AAF7eZrRjdXCkx-zaq0R9OGO7Zy2XnOizLQ
  Chatid: 874740096
PE file found: samples/c08017c476f4aae9085ed1dfe00c72ca260cddc276ef391716e62afc53e97663
  Installpath: C:\Users\ToxicEye\rat.exe
  Autorunname: Chrome Update
  Bitcoin: 1DJ5VetDBuQnmDZjRHRgEiCwYwvc6PSwu8
  Etherium: 0x357C0541F19a7755AFbF1CCD824EE06059404238
  Monero: 42Pwy6Xe4mPTz3mLap7AB5Jjd9NBt1MWjiqyvEFx3Fn8Fo9cRw9aJUHE1iTXEpUbQacMNiSxYejBKFE7UdGnyEncEE
  Botid: 1827852599:AAFwI-lniXiikR620kaPKw-aBcjPkkUlrLY
  Chatid: 1853695902
PE file found: samples/728c4e3a68f1f55cbafffc315ace09d2dc21857964cc60389f1382fabecec70a
  Installpath: C:\Users\BIBIL\Desktop\TelegramRAT\TelegramRAT\bin\Release\rat.exe
  Autorunname: Chrome Update
  Bitcoin: 1DJ5VetDBuQnmDZjRHRgEiCwYwvc6PSwu8
  Etherium: 0x357C0541F19a7755AFbF1CCD824EE06059404238
  Monero: 42Pwy6Xe4mPTz3mLap7AB5Jjd9NBt1MWjiqyvEFx3Fn8Fo9cRw9aJUHE1iTXEpUbQacMNiSxYejBKFE7UdGnyEncEE
  Botid: 1783902025:AAHm9dm4RX-LOHSfENpqgBpDfscY7wMp7cs
  Chatid: 1114717555
```

YARA (IL)

```
rule RAT_ToxicEye_IL : malware rat toxiceye {
    meta:
```

```
        author = "albertzsigovits"
        sha256 = "2e53a6710f04dd84cfd3ac1874a2a61e690568405f192e7cbf8a4df12da334c4"
        reference = "https://github.com/albertzsigovits/malware-cfg/tree/main/ToxicEyeRAT"
        reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.toxiceye"
        reference = "https://bazaar.abuse.ch/browse/signature/toxiceye/"

    strings:
        $ = {
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::ClipperEnabled
            72 [4]                      // ldstr    a1dj5vetdbuqnmd // "1DJ5VetDBuQnmDZjRHRgEiCwYw
            80 ?? 00 00 04              // stsfld   string TelegramRAT.config::bitcoin_address
            72 [4]                      // ldstr    a0x357c0541f19a // "0x357C0541F19a7755AFbF1CCD
            80 ?? 00 00 04              // stsfld   string TelegramRAT.config::etherium_address
            72 [4]                      // ldstr    a42pwy6xe4mptz3 // "42Pwy6Xe4mPTz3mLap7AB5Jjd9
            80 ?? 00 00 04              // stsfld   string TelegramRAT.config::monero_address
            2?                          // ret
        }

        $ = {
            80 ?? 00 00 04              // stsfld   string[] TelegramRAT.config::EncryptionFileTyp
            20 [4]                      // ldc.i4   0x600000
            ??                          // conv.i8
            80 ?? 00 00 04              // stsfld   int64 TelegramRAT.config::GrabFileSize
            1F ??                       // ldc.i4.s 0x15
            8D [4]                      // newarr   [mscorlib]System.String
            2?                          // dup
        }

        $ = {
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::MeltFileAfterStart
            72 [4]                      // ldstr    aCUsersToxiceye // "C:\\Users\\ToxicEye\\rat.e
            80 ?? 00 00 04              // stsfld   string TelegramRAT.config::InstallPath
            1?                          // ldc.i4.1
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::AutorunEnabled
            72 [4]                      // ldstr    aChromeUpdate  // "Chrome Update"
            80 ?? 00 00 04              // stsfld   string TelegramRAT.config::AutorunName
            1?                          // ldc.i4.1
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::ProcessBSODProtection
            1?                          // ldc.i4.1
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::HideConsoleWindow
            1?                          // ldc.i4.1
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::PreventStartOnVirtual
            1?                          // ldc.i4.0
            80 ?? 00 00 04              // stsfld   int32 TelegramRAT.config::StartDelay
            1?                          // ldc.i4.1
            80 ?? 00 00 04              // stsfld   bool TelegramRAT.config::BlockNetworkActivityW
            1F ??                       // ldc.i4.s 9
```

```
            8D [4]                          // newarr   [mscorlib]System.String
            2?                              // dup
        }

    condition:
        all of them
}
```

YARA (Ascii)

```
rule RAT_ToxicEye_StringsA : malware rat toxiceye {
    meta:
        author = "albertzsigovits"
        sha256 = "2e53a6710f04dd84cfd3ac1874a2a61e690568405f192e7cbf8a4df12da334c4"
        reference = "https://github.com/albertzsigovits/malware-cfg/tree/main/ToxicEyeRAT"
        reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.toxiceye"
        reference = "https://bazaar.abuse.ch/browse/signature/toxiceye/"

    strings:
        $ = "\\Users\\attationin"
        $ = "\\ToxicEye-master-myfork"
        $ = "\\ToxicEye-master"
        $ = "TelegramChatID"
        $ = "TelegramRAT"
        $ = "TelegramToken"
        $ = "TelegramGrabber"
        $ = "TelegramCommandCheckDelay"
        $ = "AutoStealer"
        $ = "Clipper"
        $ = "Ivan Medvedev"
        $ = "AttributeSystemEnabled"
        $ = "AttributeHiddenEnabled"
        $ = "ProcessBSODProtectionEnabled"
        $ = "AutorunEnabled"
        $ = "AutoStealerEnabled"
        $ = "ClipperEnabled"
        $ = "inSandboxie"
        $ = "DiscordGrabber"
        $ = "SteamGrabber"
        $ = "TelegramGrabber"
        $ = "runAntiAnalysis"
        $ = "DetectAntivirus"
        $ = "webcamScreenshot"
        $ = "desktopScreenshot"

    condition:
```

```
        15 of them
}
```

YARA (Wide)

```
rule RAT_ToxicEye_StringsW : malware rat toxiceye {
    meta:
        author = "albertzsigovits"
        sha256 = "2e53a6710f04dd84cfd3ac1874a2a61e690568405f192e7cbf8a4df12da334c4"
        reference = "https://github.com/albertzsigovits/malware-cfg/tree/main/ToxicEyeRAT"
        reference = "https://malpedia.caad.fkie.fraunhofer.de/details/win.toxiceye"
        reference = "https://bazaar.abuse.ch/browse/signature/toxiceye/"

    strings:
        $str01 = "ToxicEye" wide
        $str02 = "Coded by LimerBoy, attationin, Apasniy Suren" wide
        $str03 = "Do not spread among people, this was developed against mamonts only!" wide
        $str04 = "Preparing blue screen of death..." wide
        $str05 = "Warning! System will be destroyed! Run command /OverwriteBootSector_CONFIRM to con
        $str06 = "Trying overwrite boot sector..." wide
        $str07 = "Found blocked process" wide
        $str08 = "This is some text in the file." wide
        $str09 = "Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System" wide
        $str10 = "DisableTaskMgr" wide
        $str11 = "\\root\\SecurityCenter2" wide
        $str12 = "Select * from AntivirusProduct" wide
        $str13 = "Starting autostealer..." wide
        $str14 = "Stopping autostealer..." wide
        $str15 = "autosteal.lock" wide
        $str16 = ".crypted" wide
        $str17 = "STEALER:" wide

        $status01 = "[!] Failed load libraries, not connected to internet!" wide
        $status02 = "[!] Stopping command listener thread" wide
        $status03 = "[!] Retrying connect to api.telegram.org" wide
        $status04 = "[!] Retrying connect to internet..." wide
        $status05 = "[!] Shutdown signal received.." wide
        $status06 = "[+] Process checker started" wide
        $status07 = "[+] Restarting command listener thread" wide
        $status08 = "[+] Set process critical" wide
        $status09 = "[+] Set process not critical" wide
        $status10 = "[+] Hiding console window" wide
        $status11 = "[+] Copying to system..." wide
        $status12 = "[+] Uninstalling from system..." wide
        $status13 = "[+] Installing to autorun..." wide
        $status14 = "[+] Uninstalling from autorun..." wide
```

```
$status15 = "[+] Clipper is starting..." wide
$status16 = "[?] Already running 1 copy of the program" wide
$status17 = "[?] Sleeping {0}" wide
$status18 = "[~] Trying elevate previleges to administrator..." wide

$cnc01 = "https://api.mylnikov.org/geolocation/wifi?bssid" wide
$cnc02 = "http://ip-api.com/json/" wide
$cnc03 = "https://api.telegram.org/" wide
$cnc04 = "https://api.telegram.org/file/" wide

$txt01 = "keylogs.txt" wide
$txt02 = "MyTest.txt" wide
$txt03 = "bookmarks.txt" wide
$txt04 = "cookies.txt" wide
$txt05 = "credit_cards.txt" wide
$txt06 = "filezilla.txt" wide
$txt07 = "history.txt" wide
$txt08 = "passwords.txt" wide

$zip01 = "desktop.zip" wide
$zip02 = "steam.zip" wide
$zip03 = "audio.zip" wide
$zip04 = "fmedia.zip" wide

$debug01 = "Trying to kill Defender..." wide
$debug02 = "Uninstalling malware from device..." wide
$debug03 = "Preparing ForkBomb..." wide
$debug04 = "Preparing blue screen of death..." wide
$debug05 = "Trying overwrite boot sector..." wide
$debug06 = "Starting autostealer..." wide
$debug07 = "Stopping autostealer..." wide
$debug08 = "Archiving desktop files..." wide
$debug09 = "Telegram session found by process. Please wait..." wide
$debug10 = "Telegram session found in default path. Please wait..." wide
$debug11 = "Uploading file..." wide
$debug12 = "Uploading directory..." wide
$debug13 = "Downloading CommandCam..." wide
$debug14 = "Downloading FMedia..." wide
$debug15 = "Please wait..." wide
$debug16 = "Target turns off the power on the device..." wide

$exfil01 = "[BOOKMARKS]" wide
$exfil02 = "[COOKIES]" wide
$exfil03 = "[CREDIT CARDS]" wide
$exfil04 = "[FILEZILLA SERVERS]" wide
$exfil05 = "[HISTORY]" wide
$exfil06 = "[PASSWORDS]" wide
```

```
    condition:
        10 of ($str*)
        or 10 of ($status*)
        or all of ($cnc*)
        or 7 of ($txt*)
        or all of ($zip*)
        or 10 of ($debug*)
        or all of ($exfil*)
        or ( 1 of ($str*) and 1 of ($status*) and 1 of ($cnc*) and 1 of ($txt*) and 1 of ($zip*) and
}
```

Source: https://github.com/albertzsigovits/malware-cfg/tree/main/ToxicEyeRAT