Icon

Description automatically generated

Practical Malware Analysis & Triage

Malware Analysis Report

## Malware.Unknown.Exe

Sep 2024 | Ata Erdemir| v1.0

# Table of Contents

[**Table of Contents 2**](#_heading=h.gjdgxs)

[**Executive Summary 3**](#_heading=h.30j0zll)

[**High-Level Technical Summary 4**](#_heading=h.1fob9te)

[**Malware Composition 5**](#_heading=h.3znysh7)

[srvupdate.exe 5](#_heading=h.2et92p0)

[crt1.crt: 5](#_heading=h.tyjcwt)

[**Basic Static Analysis 6**](#_heading=h.3dy6vkm)

[**Basic Dynamic Analysis 7**](#_heading=h.1t3h5sf)

[**Advanced Static Analysis 8**](#_heading=h.4d34og8)

[**Advanced Dynamic Analysis 9**](#_heading=h.2s8eyo1)

[**Indicators of Compromise 10**](#_heading=h.17dp8vu)

[Network Indicators 10](#_heading=h.3rdcrjn)

[Host-based Indicators 11](#_heading=h.26in1rg)

[**Rules & Signatures 13**](#_heading=h.lnxbz9)

[**Appendices 14**](#_heading=h.35nkun2)

[A.](#_heading=h.1ksv4uv) Yara Rules 14

[B.](#_heading=h.44sinio) Callback URLs 14

[C.](#_heading=h.2jxsxqh) Decompiled Code Snippets 15

# Executive Summary

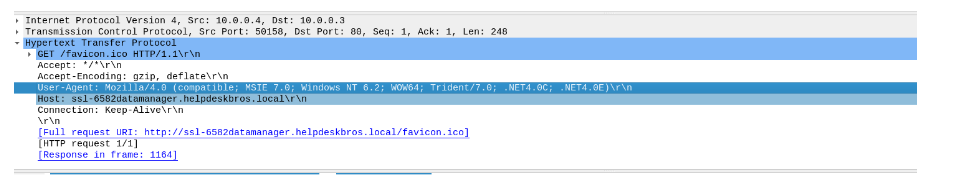
| SHA256 hash | A6AA84358130078F9455773AF1E9EF2C7710934F72DF8514C9A62ABEB83D2E81 |
| --- | --- |

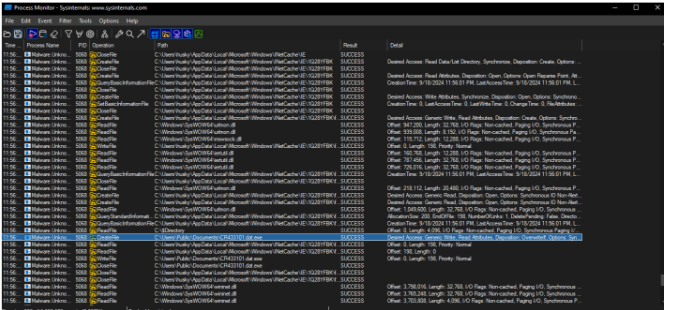
The malware.Unknown.Exe malware sample was first identified on 2021-09-04 at 11:11:12 UTC. It is a C++/C# dropper that runs on the x32 Windows operating system.

YARA signature rules are attached in Appendix A. Malware samples and hashes have been submitted to VirusTotal for further examination.

# High-Level Technical Summary

This malware is a RAT. After downloading to the computer it goes to a malicious website via favicon.ico

****

****

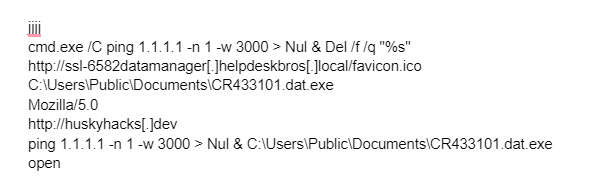
# Malware Composition

DemoWare consists of the following components:

| File Name | SHA256 Hash |
| --- | --- |
| dat.exe | 92730427321a1c4ccfc0d0580834daef98121efa9bb8963da332bfd6cf1fda8a |

## dat.exe

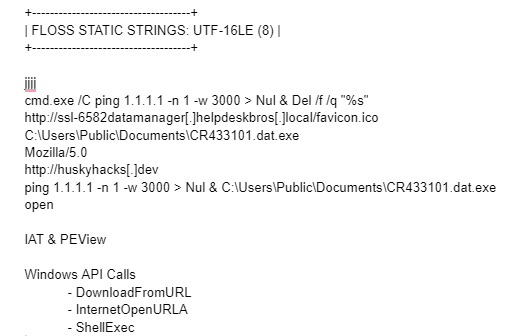
The initial executable that runs after malware downloads this via favioc



*Fig 1: Base64 encoded cert of the stage 1 payload.*

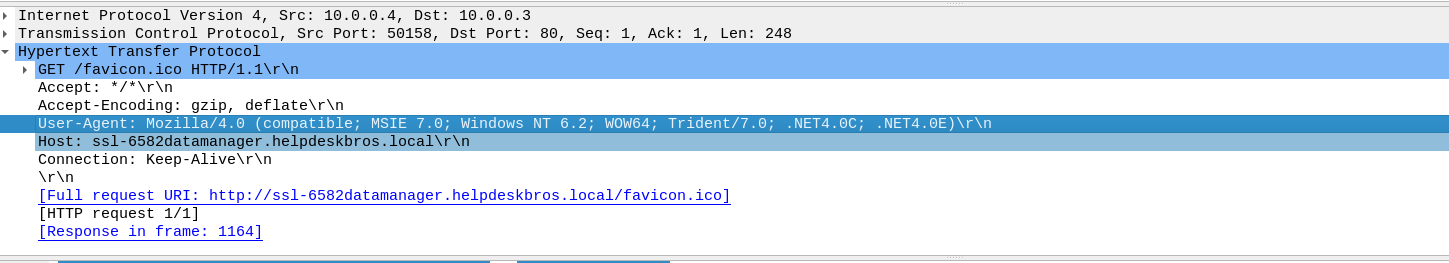
# Basic Static Analysis

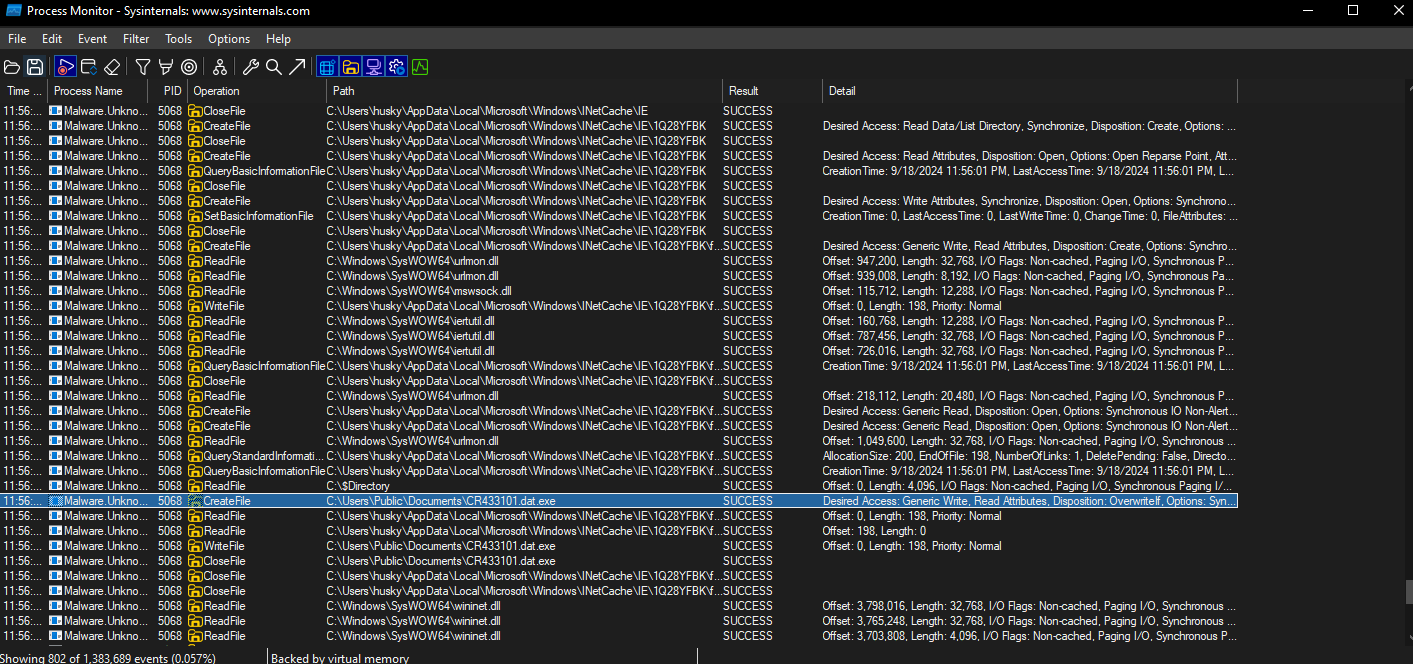
{Screenshots and description about basic static artifacts and methods}

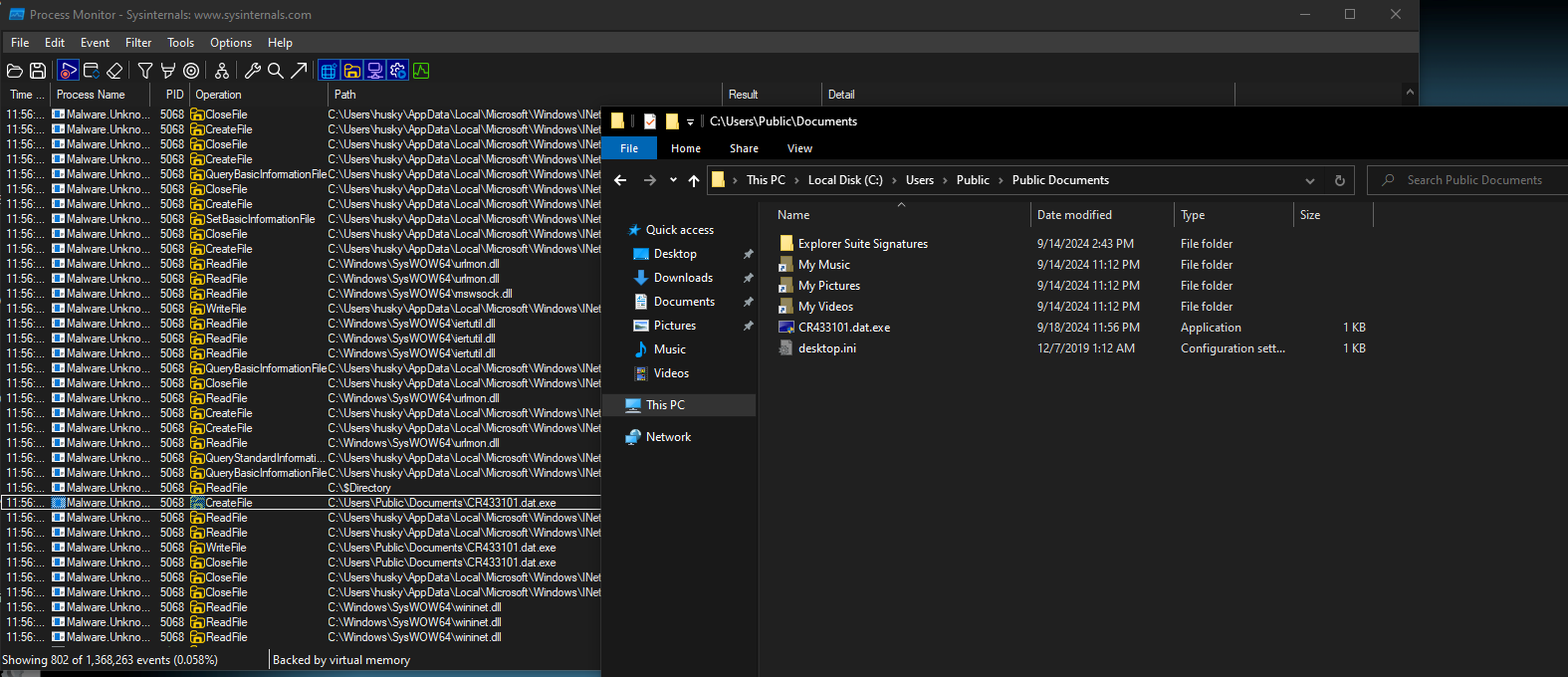


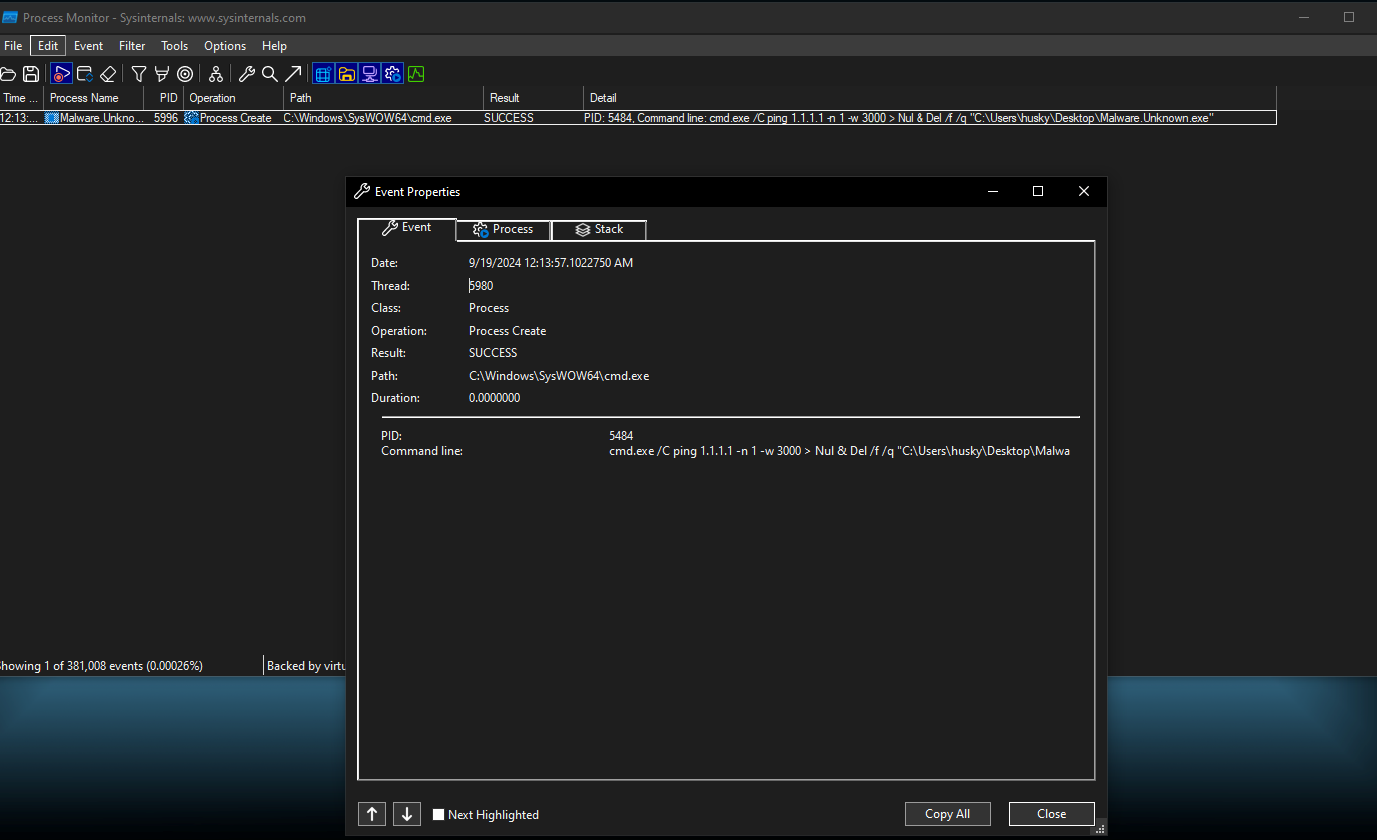
# Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}









# Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

# Advanced Dynamic Analysis

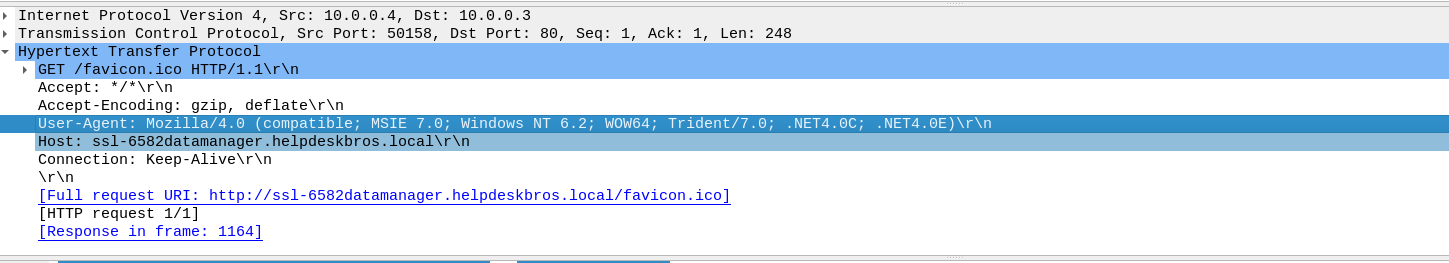
{Screenshots and description about advanced dynamic artifacts and methods}

# Indicators of Compromise

The full list of IOCs can be found in the Appendices.

## Network Indicators

{Description of network indicators}

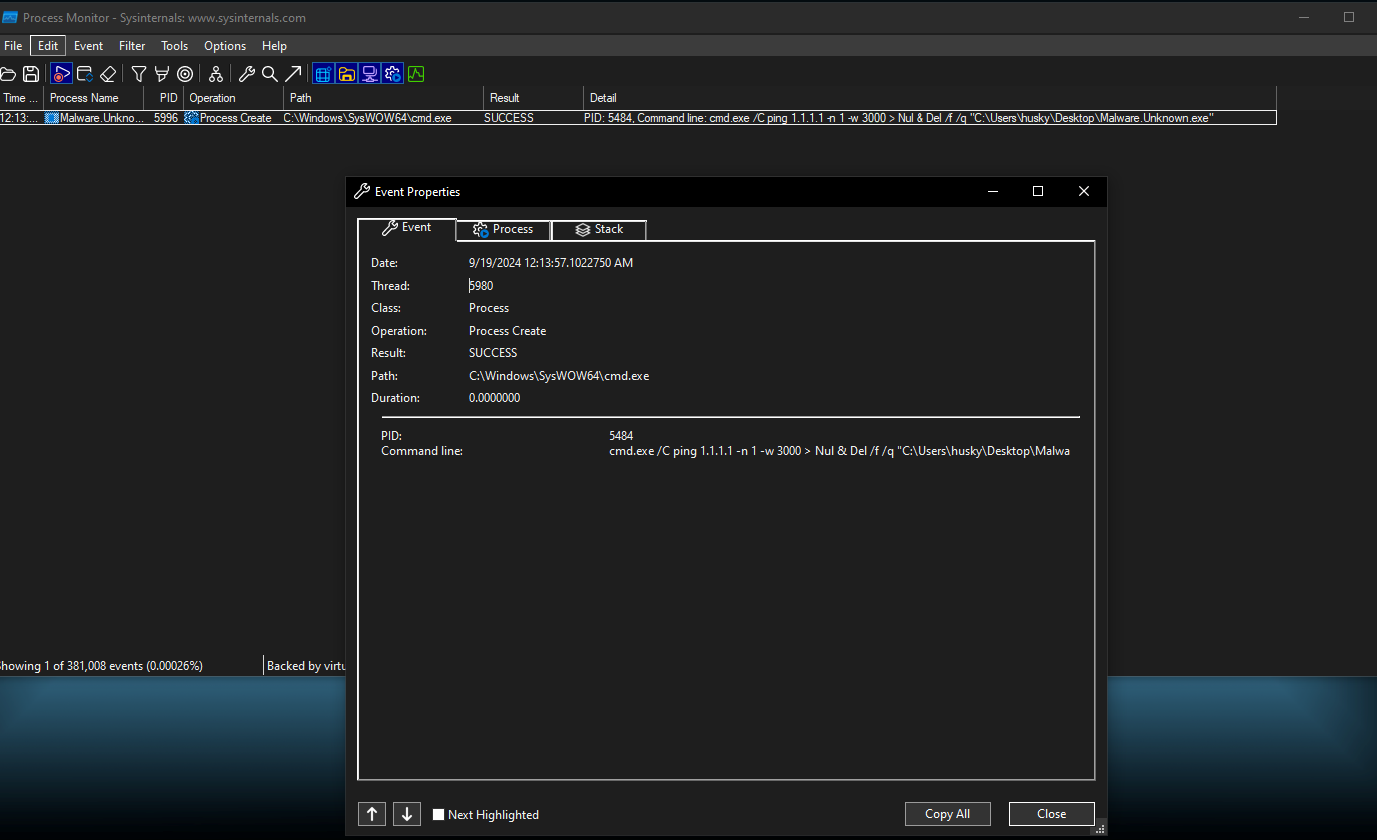


A picture containing table

Description automatically generated

*Fig 4: WireShark Packet Capture of stage 2 executable download.*

## Host-based Indicators



# Rules & Signatures

A full set of YARA rules is included in Appendix A.

{Information on specific signatures, i.e. strings, URLs, etc}

# Appendices

## Yara Rules

Full Yara repository located at: http://github.com/HuskyHacks/PMAT-lab

rule Yara\_Example {

    meta:

        last\_updated = "2021-10-15"

        author = "PMAT"

        description = "A sample Yara rule for PMAT"

    strings:

        // Fill out identifying strings and other criteria

*$string1* = "YOURETHEMANNOWDOG" ascii

*$string2* = "nim"

*$PE\_magic\_byte* = "MZ"

*$sus\_hex\_string* = { FF E4 ?? 00 FF }

    condition:

        // Fill out the conditions that must be met to identify the binary

*$PE\_magic\_byte* at 0 and

        (*$string1* and *$string2*) or

*$sus\_hex\_string*

}

## Callback URLs

| Domain | Port |
| --- | --- |
| http://ssl-6582datamanager[.]helpdeskbros[.]local/favicon.ico | 443 |

## Decompiled Code Snippets

Text

Description automatically generated

*Fig 5: Process Injection Routine in Cutter*