Icon

Description automatically generated

Practical Malware Analysis & Triage

Malware Analysis Report

Conti-Ransomware

Set 2022 | theNerdInTheHighCastle | v1.0

# Table of Contents

[Table of Contents 2](#_Toc85207993)

[Executive Summary 3](#_Toc85207994)

[High-Level Technical Summary 4](#_Toc85207995)

[Malware Composition 5](#_Toc85207996)

conti[.exe 5](#_Toc85207997)

[Basic Static Analysis 6](#_Toc85207999)

[Basic Dynamic Analysis 7](#_Toc85208000)

[Advanced Static Analysis 8](#_Toc85208001)

[Advanced Dynamic Analysis 9](#_Toc85208002)

[Indicators of Compromise 10](#_Toc85208003)

[Network Indicators 10](#_Toc85208004)

[Host-based Indicators 11](#_Toc85208005)

[Rules & Signatures 13](#_Toc85208006)

[Appendices 14](#_Toc85208007)

[A. Yara Rules 14](#_Toc85208008)

[B. Callback URLs 14](#_Toc85208009)

# Executive Summary

|  |  |
| --- | --- |
| SHA256 hash | 004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf |

Conti is a ransomware malware sample first identified in late 2019. It is a C-compiled ransomware that runs on the x64 and x32 Windows operating system. It consists of one payload that is executed following a successful spearphishing attempt. Symptoms of infection include the encryption of all the user files with the addition of the .CONTI extension. Possibly the malware could try to propagate itself due to the some network discover capabilities. n.

YARA signature rules are attached in Appendix A. The malware sample was downloaded with study and practicing scope from https://www.vx-underground.org/.

# Malware Composition

Conti consists of the following components:

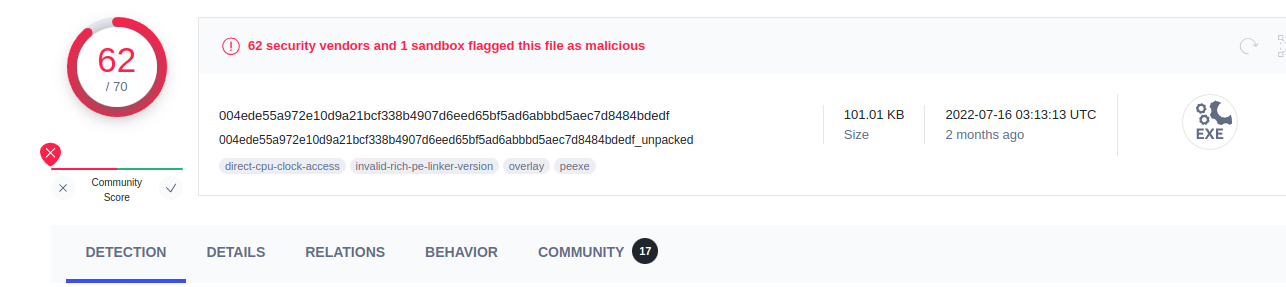
|  |  |
| --- | --- |
| File Name | SHA256 Hash |
| **conti.exe** | 004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf |
|  |  |

## conti.exe

The initial executable that runs after a successful in case of a successful vector attack, such as phishing or social engineering.

# Basic Static Analysis

{Screenshots and description about basic static artifacts and methods}

- Community score on [VirusTotal](https://www.virustotal.com/gui/file/004ede55a972e10d9a21bcf338b4907d6eed65bf5ad6abbbd5aec7d8484bdedf);

- **Floss.exe** string analysis:

|  |
| --- |
| LoadLibraryA  GetProcAddress  GetCommandLineW  CreateMutexA  ReleaseMutex  MultiByteToWideChar  CloseHandle  lstrcmpiW  lstrcpyA  KERNEL32.dll  CommandLineToArgvW  SHELL32.dll  The network is LOCKED. Do not try to use other software. For decryption KEY write HERE:  **flapalinta1950@protonmail.com**  **xersami@protonmail.com**HOW\_TO\_DECRYPTPAnullnull<?xml version='1.0' encoding='UTF-8' standalone='yes'?> |

- **PEStudio and PEView** results:

|  |  |
| --- | --- |
| M Z .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. .. @ .. .. .. .. .. .. .. .. | First byte signature, which describes a Windows Executable |
| 32bit | Architecture |
| Windows Server | os-version |
| shlwapi.dll  kernel32.dll  shell32.dll | Shell Light-weight Utility Library  Windows NT BASE API Client DLL  Windows Shell Common Dll |
| StrStrIA  GetCommandLineW  lstrcpyA  LoadLibraryA  GetProcAddress  lstrcmpiW  CreateMutexA  ReleaseMutex  MultiByteToWideChar  CloseHandle  CommandLineToArgvW | shlwapi.dll  kernel32.dll  kernel32.dll  kernel32.dll  kernel32.dll  kernel32.dll  kernel32.dll  kernel32.dll  kernel32.dll  kernel32.dll  shell32.dll |

# Basic Dynamic Analysis

{Screenshots and description about basic dynamic artifacts and methods}

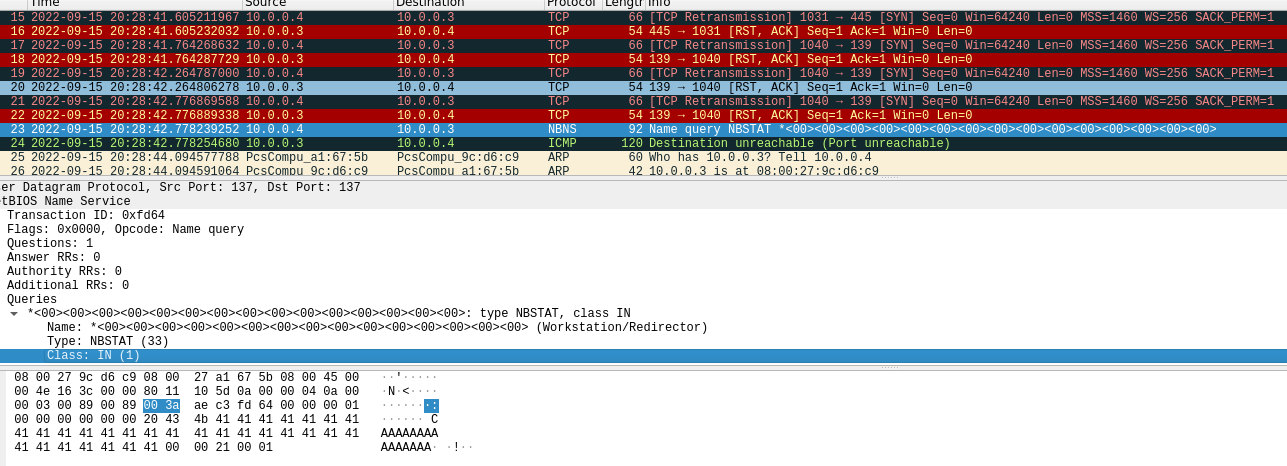
- Detonation of the Malware:

|  |
| --- |
|  |
|  |

After the detonation, on the Desktop it appears this scary message in a txt file. The detonation happens also with an Internet Simulation running (inetsim). Every file is also encrypted and no longer accessible and it is changed with a new extension .CONTI.

The use of **ProcessMonitor** shows the creation of different suspicious files after detonation which represents an ongoing encryption process.

- **Wireshark network analysis**:



The use of Wireshark shows that after detonation the malware triggers some TCP handshake connection and a UDP connection to a not reachable host.

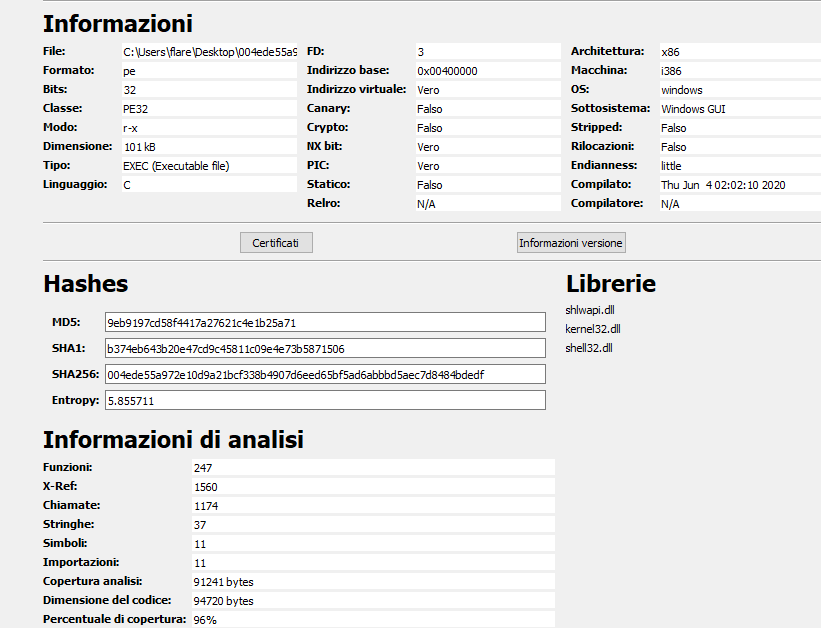
The execution of Simple Service Discovery Protocol to http://239[.]255.255.250:1900\* it may be used by the malware to perform Network discovery capabilities.

Later on the malware continues with NetBios name service querying.

# Advanced Static Analysis

{Screenshots and description about findings during advanced static analysis}

- **Cutter**:

The above image is the initial dashboard from Cutter.

From graph view there is an entry0 e no main section. Entry0 after a few variables declaration calls a function fcn.00401000 which corresponds to section text and it is loaded into EDI registry memory. The initial stage moves to ESI registry and loads libraries:

|  |
| --- |
|  |

# Advanced Dynamic Analysis

{Screenshots and description about advanced dynamic artifacts and methods}

The use of **x32dbg** leads to different interesting entry points:

|  |
| --- |
|  |

**From what it is available after reviewing different entry points it seems there is no killswitch.**

# Indicators of Compromise

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

## Network Indicators

{Description of network indicators}

|  |
| --- |
|  |

*Fig 3: WireShark Packet Capture of initial beacon check-in*

|  |
| --- |
|  |

*Fig 4: WireShark Packet Capture of first NetBios Name Service query to unreachable host.*

|  |
| --- |
|  |

*Fig 4: WireShark Packet Capture of further NetBios Name Service queries.*

## Host-based Indicators

{Description of host-based indicators}

|  |
| --- |
|  |

*Fig 5: ProcessMonitor SysInternal Suite monitoring of creation of IOCs during the encryption process*

# Rules & Signatures

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

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

The Conti.yara rule is aimed at carving out from the malware interesting signature such as MZ related to Windows Executable and strings regarding library exploited by the malware.

# Appendices

## Yara Rules

Full Yara repository located at: https://github.com/theNerdInTheHighCastle/yaraRules

|  |
| --- |
|  |

## Callback URLs

|  |  |
| --- | --- |
| **Domain** | **Port** |
| **//** |  |
|  |  |
|  |  |