

NETMANAGEIT

Intelligence Report

Decrypted: DoNex

Ransomware and its Predecessors

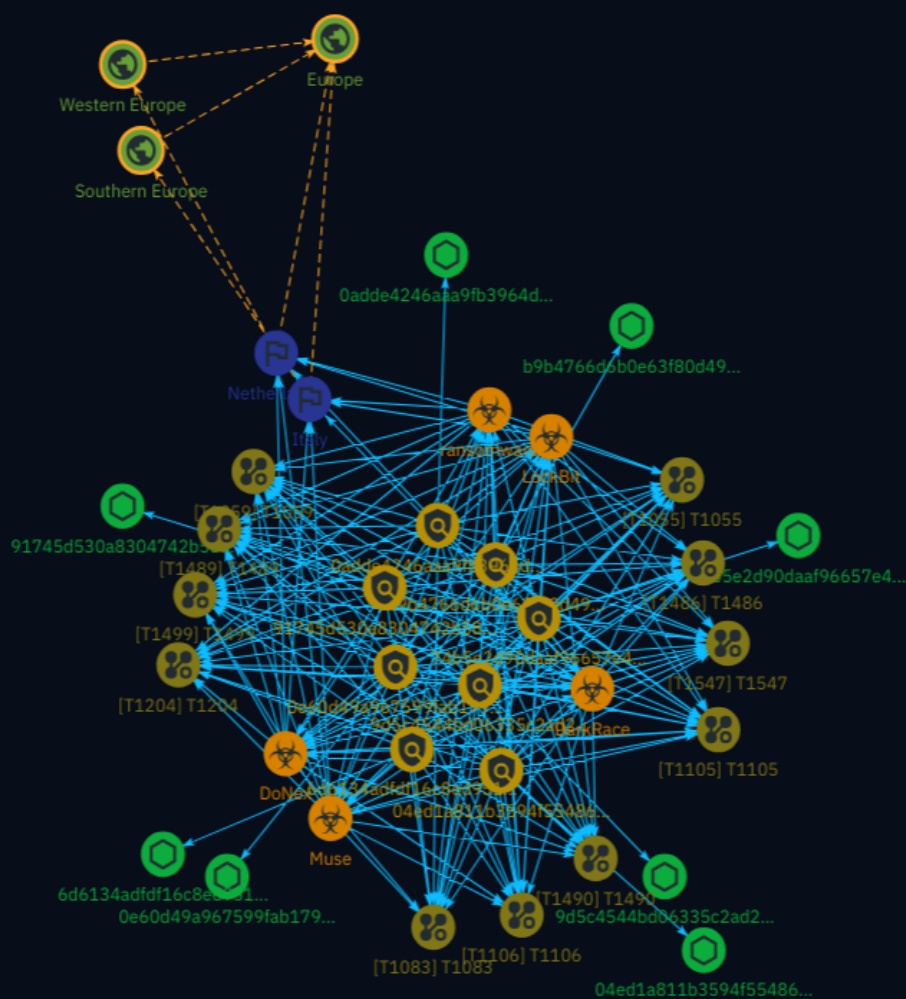


Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Attack-Pattern	6
● Indicator	16
● Region	20
● Country	21
● Malware	22
● uses	23
● indicates	25
● located-at	29
● targets	30
● based-on	31

Observables

- StixFile 32

External References

- External References 33

Overview

Description

Researchers have uncovered a cryptographic flaw in the DoNex ransomware and its previous iterations, allowing for the creation of a decryptor tool. Initially discovered in March 2024, this cryptographic weakness was made public at Recon 2024. The ransomware, which has undergone several rebrands since its inception as Muse in April 2022, utilizes targeted attacks primarily focused on the US, Italy, and the Netherlands. Its encryption process involves generating a key through `CryptGenRandom()`, initializing ChaCha20 symmetric encryption, and appending the RSA-4096 encrypted symmetric file key to each file. Configuration data, including whitelisted extensions and processes, is stored in an encrypted XML format within the malware samples.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Attack-Pattern

Name

T1547

ID

T1547

Description

Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.

Name

T1489

ID

T1489

Description

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster) Adversaries may accomplish this by disabling individual services of high importance to an organization, such as `MSEExchangeIS`, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](https://attack.mitre.org/techniques/T1485) or [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

Name

T1055

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

T1490

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](<https://attack.mitre.org/techniques/T1485>) and [Data Encrypted for Impact](<https://attack.mitre.org/techniques/T1486>). (Citation: Talos Olympic Destroyer 2018) (Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](<https://attack.mitre.org/techniques/T1047>) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system * `diskshadow.exe` can be used to delete all volume shadow copies on a system - `diskshadow delete shadows all` (Citation: Diskshadow) (Citation: Crytox Ransomware) On network devices, adversaries may leverage [Disk Wipe](<https://attack.mitre.org/techniques/T1561>) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack) (Citation: Rhino Security Labs AWS S3 Ransomware)

Name

T1204

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary; running malicious JavaScript in their browser, allowing adversaries to [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)s; or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). (Citation: Talos Roblox Scam 2023)(Citation: Krebs Discord Bookmarks 2023) For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219). (Citation: Telephone Attack Delivery)

Name

T1486

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [System Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](<https://attack.mitre.org/techniques/T1078>), [OS Credential Dumping](<https://attack.mitre.org/techniques/T1003>), and [SMB/Windows Admin Shares](<https://attack.mitre.org/techniques/T1021/002>).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](<https://attack.mitre.org/techniques/T1491/001>), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1106

ID

T1106

Description

Adversaries may interact with the native OS application programming interface (API) to execute behaviors. Native APIs provide a controlled means of calling low-level OS services within the kernel, such as those involving hardware/devices, memory, and processes. (Citation: NT API Windows)(Citation: Linux Kernel API) These native APIs are leveraged by the OS during system boot (when other system components are not yet initialized) as well as carrying out tasks and requests during routine operations. Adversaries may abuse these OS API functions as a means of executing behaviors. Similar to [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059), the native API and its hierarchy of interfaces provide mechanisms to interact with and utilize various components of a victimized system. Native API functions (such as `NtCreateProcess`) may be directed invoked via system calls / syscalls, but these features are also often exposed to user-mode applications via interfaces and libraries.(Citation: OutFlank System Calls)(Citation: CyberBit System Calls)(Citation: MDSec System Calls) For example, functions such as the Windows API `CreateProcess()` or GNU `fork()` will allow programs and scripts to start other processes.(Citation: Microsoft CreateProcess)(Citation: GNU Fork) This may allow API callers to execute a binary, run a CLI command, load modules, etc. as thousands of similar API functions exist for various system operations.(Citation: Microsoft Win32)(Citation: LIBC) (Citation: GLIBC) Higher level software frameworks, such as Microsoft .NET and macOS Cocoa, are also available to interact with native APIs. These frameworks typically provide language wrappers/abstractions to API functionalities and are designed for ease-of-use/ portability of code.(Citation: Microsoft NET)(Citation: Apple Core Services)(Citation: MACOS Cocoa)(Citation: macOS Foundation) Adversaries may use assembly to directly or indirectly invoke syscalls in an attempt to subvert defensive sensors and detection signatures such as user mode API-hooks.(Citation: Redops Syscalls) Adversaries may also attempt to tamper with sensors and defensive tools associated with API monitoring, such as unhooking monitored functions via [Disable or Modify Tools](https://attack.mitre.org/techniques/T1562/001).

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](<https://attack.mitre.org/software/S0095>). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](<https://attack.mitre.org/techniques/T1570>)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](<https://attack.mitre.org/software/S0160>), and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>) commands such as `EX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Adversaries have also abused file application features, such as the Windows `search-ms` protocol handler, to deliver malicious files to victims through remote file searches invoked by [User Execution](<https://attack.mitre.org/techniques/T1204>) (typically after interacting with [Phishing](<https://attack.mitre.org/techniques/T1566>) lures). (Citation: T1105: Trellix_search-ms) Files can also be transferred using various [Web Service](<https://attack.mitre.org/techniques/T1102>)s as well as native or otherwise present tools on the victim system. (Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine. (Citation: Dropbox Malware Sync)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](<https://attack.mitre.org/>

techniques/T1059/004) while Windows installations include the [Windows Command Shell] (<https://attack.mitre.org/techniques/T1059/003>) and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>). There are also cross-platform interpreters such as [Python] (<https://attack.mitre.org/techniques/T1059/006>), as well as those commonly associated with client applications such as [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) and [Visual Basic](<https://attack.mitre.org/techniques/T1059/005>). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](<https://attack.mitre.org/tactics/TA0001>) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1499

ID

T1499

Description

Adversaries may perform Endpoint Denial of Service (DoS) attacks to degrade or block the availability of services to users. Endpoint DoS can be performed by exhausting the system resources those services are hosted on or exploiting the system to cause a persistent crash condition. Example services include websites, email services, DNS, and web-based applications. Adversaries have been observed conducting DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion.(Citation: Symantec DDoS October 2014) An Endpoint DoS denies the availability of a service without saturating the network used to provide access to the service. Adversaries can target various layers of the application stack that is hosted on the system used to provide the service. These layers include the Operating Systems (OS), server applications such as web servers, DNS servers, databases, and the (typically web-based) applications that sit on top of them. Attacking each layer requires different techniques that take advantage of bottlenecks that are unique to the respective components. A DoS attack may be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To

perform DoS attacks against endpoint resources, several aspects apply to multiple methods, including IP address spoofing and botnets. Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. Botnets are commonly used to conduct DDoS attacks against networks and services. Large botnets can generate a significant amount of traffic from systems spread across the global internet. Adversaries may have the resources to build out and control their own botnet infrastructure or may rent time on an existing botnet to conduct an attack. In some of the worst cases for DDoS, so many systems are used to generate requests that each one only needs to send out a small amount of traffic to produce enough volume to exhaust the target's resources. In such circumstances, distinguishing DDoS traffic from legitimate clients becomes exceedingly difficult. Botnets have been used in some of the most high-profile DDoS attacks, such as the 2012 series of incidents that targeted major US banks.(Citation: USNYAG IranianBotnet March 2016) In cases where traffic manipulation is used, there may be points in the global network (such as high traffic gateway routers) where packets can be altered and cause legitimate clients to execute code that directs network packets toward a target in high volume. This type of capability was previously used for the purposes of web censorship where client HTTP traffic was modified to include a reference to JavaScript that generated the DDoS code to overwhelm target web servers.(Citation: ArsTechnica Great Firewall of China) For attacks attempting to saturate the providing network, see [Network Denial of Service](<https://attack.mitre.org/techniques/T1498>).

Name

T1083

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](<https://attack.mitre.org/techniques/T1083>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include ``dir``, ``tree``, ``ls``, ``find``,

and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](<https://attack.mitre.org/techniques/T1106>). Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A) Some files and directories may require elevated or specific user permissions to access.

Indicator

Name

04ed1a811b3594f55486a52ab81227089c178f5c73944a3a9665d7052c3b7df9

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'04ed1a811b3594f55486a52ab81227089c178f5c73944a3a9665d7052c3b7df9']

Name

0e60d49a967599fab179f8c885d91db25016be996d66a4e00cbb197e5085efa4

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'0e60d49a967599fab179f8c885d91db25016be996d66a4e00cbb197e5085efa4']

Name

b9b4766d6b0e63f80d49e969fbd63ae90b0d1e487ef008b55c096bf46395d32e

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'b9b4766d6b0e63f80d49e969fbd63ae90b0d1e487ef008b55c096bf46395d32e']

Name

91745d530a8304742b58890e798448de9fbe4ea0bc057f30ab0beb522b4bb688

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'91745d530a8304742b58890e798448de9fbe4ea0bc057f30ab0beb522b4bb688']

Name

6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40']

Name

9d5c4544bd06335c2ad2545b0d177218f84b77dd1834b22bf6a4cfe7e1de91fb

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'9d5c4544bd06335c2ad2545b0d177218f84b77dd1834b22bf6a4cfe7e1de91fb']

Name

74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3']

Name

0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca']

Region

Name

Europe

Name

Southern Europe

Name

Western Europe

Country

Name

Netherlands

Name

Italy

Malware

Name

LockBit

Name

DoNex

Name

DarkRace

Name

ransomware

Name

Muse

uses

Name
Name
Name
Name
Name
Name
Name
Name

Name

Name

Name

Name

Name

Name

Name

Name

indicates

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

Name

located-at

Name

Name

Description

Country Netherlands is located in Western Europe

targets

Name
Name
Name
Name

based-on

Name

StixFile

Value

6d6134adfdf16c8ed9513aba40845b15bd314e085ef1d6bd20040afd42e36e40

91745d530a8304742b58890e798448de9fbe4ea0bc057f30ab0beb522b4bb688

9d5c4544bd06335c2ad2545b0d177218f84b77dd1834b22bf6a4cfe7e1de91fb

04ed1a811b3594f55486a52ab81227089c178f5c73944a3a9665d7052c3b7df9

b9b4766d6b0e63f80d49e969fbd63ae90b0d1e487ef008b55c096bf46395d32e

0e60d49a967599fab179f8c885d91db25016be996d66a4e00cbb197e5085efa4

0adde4246aaa9fb3964d1d6cf3c29b1b13074015b250eb8e5591339f92e1e3ca

74b5e2d90daaf96657e4d3d800bb20bf189bb2cf487479ea0facaf6182e0d1d3

External References

-
- <https://decoded.avast.io/threatresearch/decrypted-donex-ransomware-and-its-predecessors/>
-
- <https://otx.alienvault.com/pulse/668e5587adc16587a94465bd>