Jan 16 2024

NETMANAGEIT

Intelligence Report

Medusa Ransomware Turning Your Files into Stone

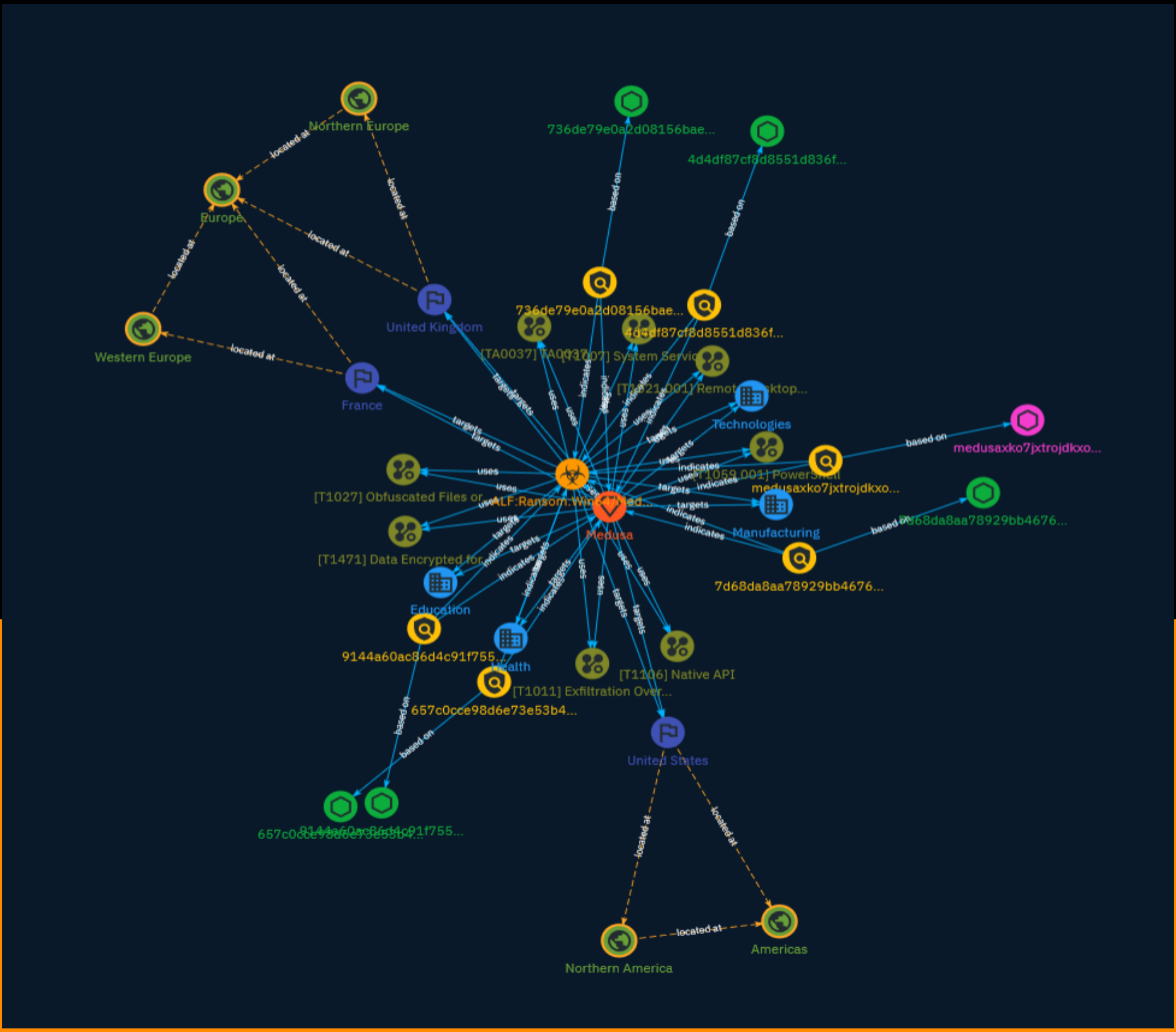

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Unit 42 Threat Intelligence analysts have noticed an escalation in Medusa ransomware activities and a shift in tactics toward extortion, characterized by the introduction in early 2023 of their dedicated leak site called the Medusa Blog. Medusa threat actors use this site to disclose sensitive data from victims unwilling to comply with their ransom demands.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

PowerShell

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

Native API

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 in-directly 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

TA0037

ID

TA0037

Name

Exfiltration Over Other Network Medium

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection.

Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

System Service Discovery

ID

T1007

Description

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Name

Data Encrypted for Impact

ID
T1471

Description
An adversary may encrypt files stored on a mobile device to prevent the user from accessing them. 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.

Name
Remote Desktop Protocol

ID
T1021.001

Description
Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

Sector

Name

Education

Description

Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.

Name

Manufacturing

Description

Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.

Name

Health

Description

Public and private entities involved in research, services and manufacturing activities related to public health.

Name
Technologies

Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name

4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6

Description

SUSP_XORed_URL_in_EXE

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6']

Name

657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980

Description

SUSP_XORed_URL_in_EXE

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980']

Name

736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270

Description

Win32:RansomX-gen\ [Ransom]

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270']

Name

7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95']

Name

9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669']

Name

medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion']

Intrusion-Set

Name
Medusa

Region

Name
Europe

Name
Northern Europe

Name
Northern America

Name
Western Europe

Name
Americas

Country

Name
United Kingdom

Name
France

Name
United States

Malware

Name
ALF:Ransom:Win64/MedusaLocker

Domain-Name

Value
medusaxko7jxtrojdkxo66j7ck4q5tgktf7uqsqyfry4ebnxlcbkccyd.onion

StixFile

Value
9144a60ac86d4c91f7553768d9bef848acd3bd9fe3e599b7ea2024a8a3115669
4d4df87cf8d8551d836f67fbde4337863bac3ff6b5cb324675054ea023b12ab6
7d68da8aa78929bb467682ddb080e750ed07cd21b1ee7a9f38cf2810eeb9cb95
657c0cce98d6e73e53b4001eeea51ed91fdcf3d47a18712b6ba9c66d59677980
736de79e0a2d08156bae608b2a3e63336829d59d38d61907642149a566ebd270

External References

- https://otx.alienvault.com/pulse/65a07afb559173d01a6eb537
- https://unit42.paloaltonetworks.com/medusa-ransomware-escalation-new-leak-site/