Jul 26 2023

NETMANAGEIT

Intelligence Report

Akira Ransomware

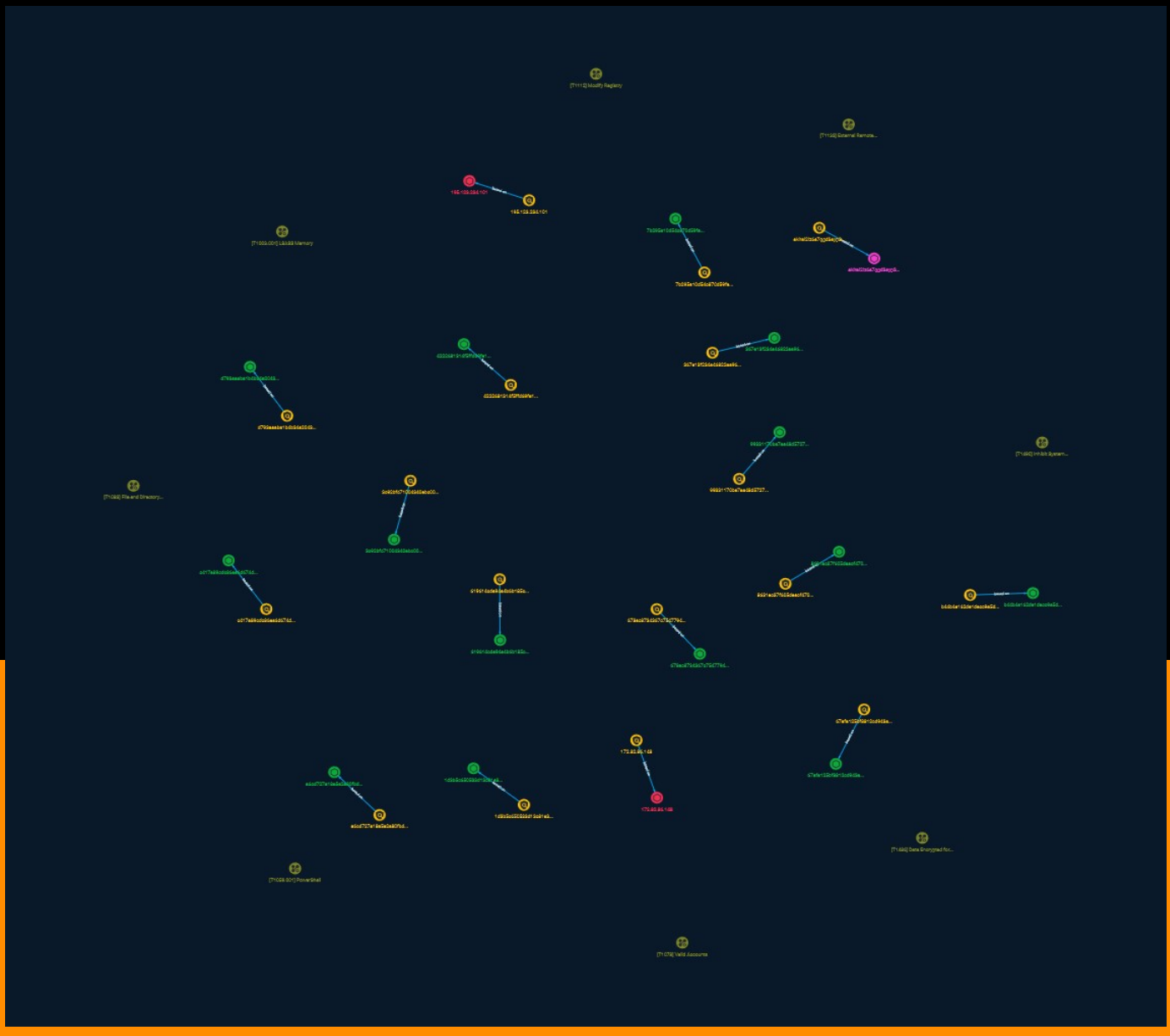

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Akira ransomware, similar to other types of ransomware, spreads within a corporate network and targets multiple devices once it gains access. However, before encrypting files, the ransomware avoids certain folders, including Recycle Bin, System Volume Information, Boot, ProgramData, and Windows, as well as specific Windows system files with .exe, .lnk, .dll, .msi, and .sys extensions.

Confidence

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

15 / 100

Indicator

Name
67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4']
Name
367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9']
Name

akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion

Pattern Type

stix

Pattern

[domain-name:value = 'akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion']

Name

4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda']

Name

d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee']

Name
195.123.234.101
Description
CC=US ASN=AS204957 Green Floid LLC
Pattern Type
stix
Pattern
[ipv4-addr:value = '195.123.234.101']
Name
a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce']
Name
619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b
Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b']

Name

b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa']

Name

c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598']

Name

172.82.86.148

Description

CC=NL ASN=AS26383 ASNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.82.86.148']

Name

99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba']

Name

678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33

Description

stack_string SHA256 of d25890a2e967a17ff3dad8a70bfdd832

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33']

Name

7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488

Description

stack_string

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488']

Name

8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50

Description

stack_string SHA256 of e44eb48c7f72ffac5af3c7a37bf80587

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50']

Name

3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c

Description

stack_string SHA256 of 923161f345ed3566707f9f878cc311bc6a0c5268

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c']

Name

1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296

Description

is__elf SHA256 of 9180ea8ba0cdfe0a769089977ed8396a68761b40

Pattern Type

stix

Pattern
[file:hashes.'SHA-256' = '1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296']

Attack-Pattern

Name

External Remote Services

ID

T1133

Description

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop) Access to [Valid Accounts](https://attack.mitre.org/techniques/T1078) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging) Access to remote services may be used as a redundant or persistent access mechanism during an operation. Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Name

Valid Accounts

ID

T1078

Description

Adversaries may obtain and abuse credentials of existing accounts as a means of gaining Initial Access, Persistence, Privilege Escalation, or Defense Evasion. Compromised credentials may be used to bypass access controls placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, network devices, and remote desktop.(Citation: volexity_0day_sophos_FW) Compromised credentials may also grant an adversary increased privilege to specific systems or access to restricted areas of the network. Adversaries may choose not to use malware or tools in conjunction with the legitimate access those credentials provide to make it harder to detect their presence. In some cases, adversaries may abuse inactive accounts: for example, those belonging to individuals who are no longer part of an organization. Using these accounts may allow the adversary to evade detection, as the original account user will not be present to identify any anomalous activity taking place on their account.(Citation: CISA MFA PrintNightmare) The overlap of permissions for local, domain, and cloud accounts across a network of systems is of concern because the adversary may be able to pivot across accounts and systems to reach a high level of access (i.e., domain or enterprise administrator) to bypass access controls set within the enterprise.(Citation: TechNet Credential Theft)

Name

LSASS Memory

ID

T1003.001

Description

Adversaries may attempt to access credential material stored in the process memory of the Local Security Authority Subsystem Service (LSASS). After a user logs on, the system generates and stores a variety of credential materials in LSASS process memory. These credential materials can be harvested by an administrative user or SYSTEM and used to conduct [Lateral Movement](https://attack.mitre.org/tactics/TA0008) using [Use Alternate

Authentication Material](https://attack.mitre.org/techniques/T1550). As well as in-memory techniques, the LSASS process memory can be dumped from the target host and analyzed on a local system. For example, on the target host use procdump: * `procdump -ma lsass.exe lsass_dump` Locally, mimikatz can be run using: * `sekurlsa::Minidump lsassdump.dmp` * `sekurlsa::logonPasswords` Built-in Windows tools such as comsvcs.dll can also be used: * `rundll32.exe C:\Windows\System32\comsvcs.dll MiniDump PID lsass.dmp full`(Citation: Volexity Exchange Marauder March 2021)(Citation: Symantec Attacks Against Government Sector) Windows Security Support Provider (SSP) DLLs are loaded into LSASS process at system start. Once loaded into the LSA, SSP DLLs have access to encrypted and plaintext passwords that are stored in Windows, such as any logged-on user's Domain password or smart card PINs. The SSP configuration is stored in two Registry keys: `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` and `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`. An adversary may modify these Registry keys to add new SSPs, which will be loaded the next time the system boots, or when the AddSecurityPackage Windows API function is called.(Citation: Graeber 2014) The following SSPs can be used to access credentials: * Msv: Interactive logons, batch logons, and service logons are done through the MSV authentication package. * Wdigest: The Digest Authentication protocol is designed for use with Hypertext Transfer Protocol (HTTP) and Simple Authentication Security Layer (SASL) exchanges. (Citation: TechNet Blogs Credential Protection) * Kerberos: Preferred for mutual client-server domain authentication in Windows 2000 and later. * CredSSP: Provides SSO and Network Level Authentication for Remote Desktop Services.(Citation: TechNet Blogs Credential Protection)

Name

Inhibit System Recovery

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 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

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

Modify Registry

ID

T1112

Description

Adversaries may interact with the Windows Registry to hide configuration information within Registry keys, remove information as part of cleaning up, or as part of other techniques to aid in persistence and execution. Access to specific areas of the Registry depends on account permissions, some requiring administrator-level access. The built-in Windows command-line utility [Reg](https://attack.mitre.org/software/S0075) may be used for local or remote Registry modification. (Citation: Microsoft Reg) Other tools may also be used, such as a remote access tool, which may contain functionality to interact with the Registry through the Windows API. Registry modifications may also include actions to hide keys, such as prepending key names with a null character, which will cause an error and/or be ignored when read via [Reg](https://attack.mitre.org/software/S0075) or other utilities using the Win32 API. (Citation: Microsoft Reghide NOV 2006) Adversaries may abuse these pseudo-hidden keys to conceal payloads/commands used to maintain persistence. (Citation: TrendMicro POWELIKS AUG 2014) (Citation: SpectorOps Hiding Reg Jul 2017) The Registry of a remote system may be modified to aid in execution of files as part of lateral movement. It requires the remote Registry service to be running on the target system. (Citation: Microsoft Remote) Often [Valid Accounts](https://attack.mitre.org/techniques/T1078) are required, along with access to the remote system's [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) for RPC communication.

Name

Data Encrypted for Impact

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

File and Directory Discovery

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)

Domain-Name

Value
akiral2iz6a7qgd3ayp3l6yub7xx2uep76idk3u2kollpj5z3z636bad.onion

StixFile

Value
c417a89cdc86ea6d674d2dc629ae1872b4054ac43e948e8ed60d3f3f47178598
367e13f234a46822aa9655690f18000319123ad07a62e56bcf8bebbfbb0de7b9
619614cda94a4b6b185c0c122d11ef2b8b0b3e7fc94a1a5c2ff1ac49233df54b
4222681314f5ffd69fe17ab2ae4b9aaa60866571fe2b53afc10f87e3738cedda
b44b4e162de1decc9a5d3c61a045eb4776c55fccd33c9eced5b9f622faee19fa
a6cd727a18e5e2a80fbd8a51c299a2030bd5e68e4bbf136e07eb9d0b3f3bb8ce
99331170be7aa48d572728f68e52ac8d3eb3c8307cb8050ce504ef9f4624a4ba
67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
d793aaaba1b4b34a20432b86505b851d838def0cd722b8cbdd1d08e19a08b6ee
8631ac37f605daacf47095955837ec5abbd5e98c540ffd58bb9bf873b1685a50
3c92bfc71004340ebc00146ced294bc94f49f6a5e212016ac05e7d10fcb3312c
7b295a10d54c870d59fab3a83a8b983282f6250a0be9df581334eb93d53f3488
678ec8734367c7547794a604cc65e74a0f42320d85a6dce20c214e3b4536bb33

1d3b5c650533d13c81e325972a912e3ff8776e36e18bca966dae50735f8ab296

IPv4-Addr

Value
172.82.86.148
195.123.234.101

External References

- https://otx.alienvault.com/pulse/64c11b20713f2ef9c8dbb9b8
- https://www.cert-in.org.in/
- https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVA01&VACODE=CIVA-2023-2113