Dec 27 2023

NETMANAGEIT

Intelligence Report

Akira, again: The ransomware that keeps on taking

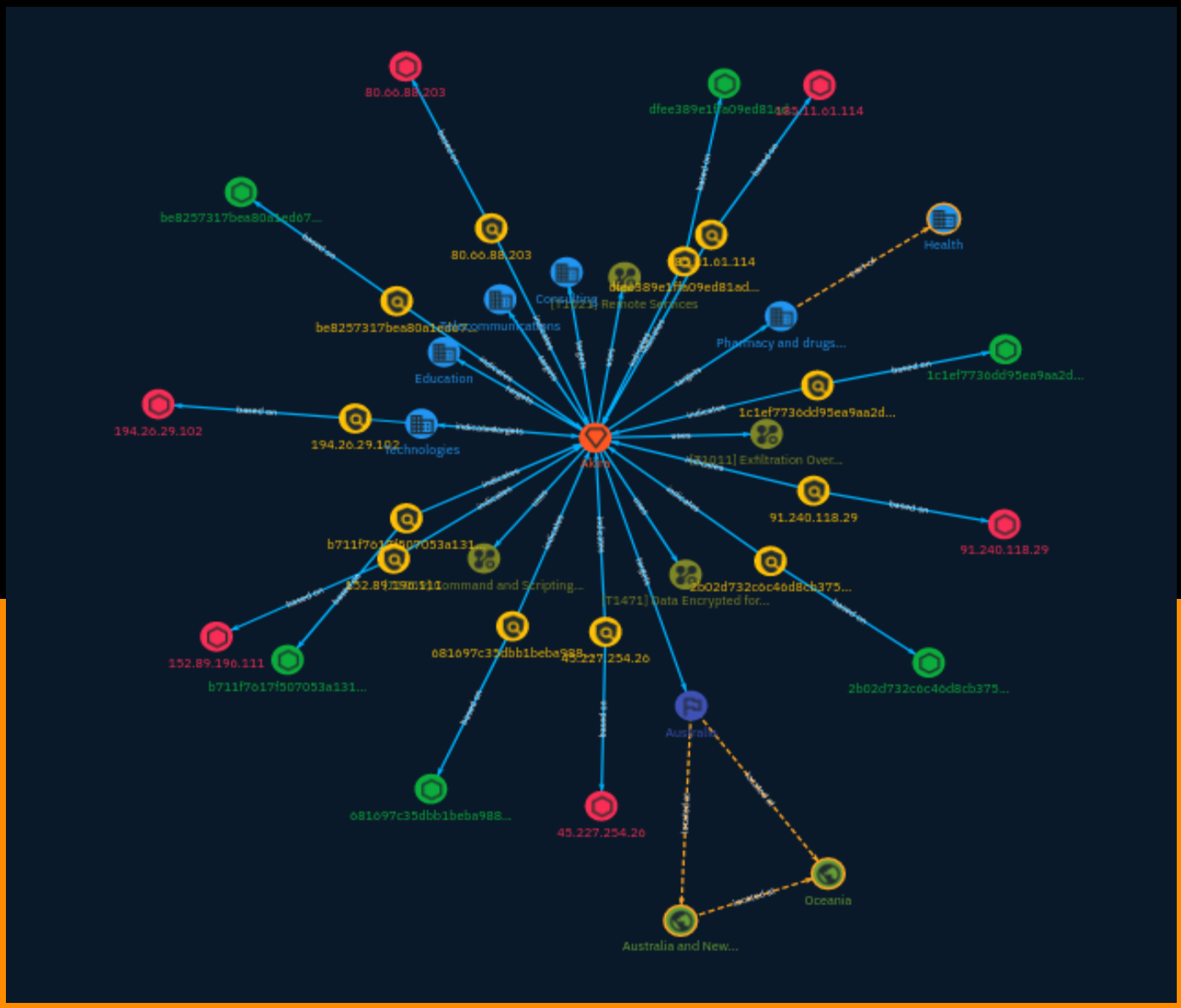

Table of contents

Overview

Entities

Observables

External References

Overview

Description

The Sophos MDR Threat Intelligence team previously published the blog Akira Ransomware is “bringin’ 1988 back” in May 2023, roughly two months after the group was reported to have begun operations.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

Command and Scripting Interpreter

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

Remote Services

ID

T1021

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user. In an enterprise environment, servers and workstations can be organized into domains. Domains provide centralized identity management, allowing users to login using one set of credentials across the entire network. If an adversary is able to obtain a set of valid domain credentials, they could login to many different machines using remote access protocols such as secure shell (SSH) or remote desktop protocol (RDP).(Citation: SSH Secure Shell)(Citation: TechNet Remote Desktop Services) They could also login to accessible SaaS or IaaS services, such as those that federate their identities to the domain. Legitimate applications (such as [Software

Deployment Tools](https://attack.mitre.org/techniques/T1072) and other administrative programs) may utilize [Remote Services](https://attack.mitre.org/techniques/T1021) to access remote hosts. For example, Apple Remote Desktop (ARD) on macOS is native software used for remote management. ARD leverages a blend of protocols, including [VNC](https://attack.mitre.org/techniques/T1021/005) to send the screen and control buffers and [SSH](https://attack.mitre.org/techniques/T1021/004) for secure file transfer. (Citation: Remote Management MDM macOS)(Citation: Kickstart Apple Remote Desktop commands)(Citation: Apple Remote Desktop Admin Guide 3.3) Adversaries can abuse applications such as ARD to gain remote code execution and perform lateral movement. In versions of macOS prior to 10.14, an adversary can escalate an SSH session to an ARD session which enables an adversary to accept TCC (Transparency, Consent, and Control) prompts without user interaction and gain access to data.(Citation: FireEye 2019 Apple Remote Desktop)(Citation: Lockboxx ARD 2019)(Citation: Kickstart Apple Remote Desktop commands)

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.

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
Pharmacy and drugs manufacturing
Description
Public and private entities involved in producing and selling medicinal products and drugs.
Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.

Name
Telecommunications
Description
Private and public entities involved in the production, transport and dissemination of information and communication signals.
Name
Consulting
Description
Private entities providing expert advice in a specific field to external entities.
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
1c1ef7736dd95ea9aa2dc5784dc51977a1d890c92159e16315ef15546556bcdf
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1c1ef7736dd95ea9aa2dc5784dc51977a1d890c92159e16315ef15546556bcdf']
Name
681697c35dbb1beba9886f5c44882ccca32dd7e9e483a381e981e7409a0e35cb
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '681697c35dbb1beba9886f5c44882ccca32dd7e9e483a381e981e7409a0e35cb']
Name

80.66.88.203

Description

CC=NL ASN=AS208091 Xhost Internet Solutions Lp

Pattern Type

stix

Pattern

[ipv4-addr:value = '80.66.88.203']

Name

dfee389e1ffa09ed81adcf0d0f165d859e0c045ad7d90f6edcf3f96dfcceba2b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dfee389e1ffa09ed81adcf0d0f165d859e0c045ad7d90f6edcf3f96dfcceba2b']

Name

194.26.29.102

Description

CC=RU ASN=AS206728 Media Land LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.26.29.102']

Name

185.11.61.114

Description

CC=RU ASN=AS57523 Chang Way Technologies Co. Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.11.61.114']

Name

152.89.196.111

Description

CC=RU

Pattern Type

stix

Pattern

[ipv4-addr:value = '152.89.196.111']

Name

be8257317bea80a1ed670d70eb4f21bba246c266a59724185b366c2dcfb2b8ea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'be8257317bea80a1ed670d70eb4f21bba246c266a59724185b366c2dcfb2b8ea']

Name

91.240.118.29

Description

Agressive IP known malicious on AbuseIPDB - countryCode: RU - abuseConfidenceScore: 100 - lastReportedAt: 2023-11-28T13:55:03+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.240.118.29']

Name

45.227.254.26

Description

Agressive IP known malicious on AbuseIPDB - countryCode: BZ - abuseConfidenceScore: 100 - lastReportedAt: 2023-12-25T14:14:40+00:00

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.227.254.26']

Name

b711f7617f507053a131a75b0971409f76663b404aa1c51bfbe2cd32f2ac8fb8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b711f7617f507053a131a75b0971409f76663b404aa1c51bfbe2cd32f2ac8fb8']

Name

2b02d732c6c46d8cb3758851c9e79a52761956109f55407c1a5d693a8a1af1f3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2b02d732c6c46d8cb3758851c9e79a52761956109f55407c1a5d693a8a1af1f3']

Intrusion-Set

Name
Akira

Country

Name
Australia

Region

Name
Oceania

Name
Australia and New Zealand

StixFile

Value
dfee389e1ffa09ed81adcf0d0f165d859e0c045ad7d90f6edcf3f96dfcceba2b
1c1ef7736dd95ea9aa2dc5784dc51977a1d890c92159e16315ef15546556bcdf
681697c35dbb1beba9886f5c44882ccca32dd7e9e483a381e981e7409a0e35cb
be8257317bea80a1ed670d70eb4f21bba246c266a59724185b366c2dcfb2b8ea
b711f7617f507053a131a75b0971409f76663b404aa1c51bfbe2cd32f2ac8fb8
2b02d732c6c46d8cb3758851c9e79a52761956109f55407c1a5d693a8a1af1f3

IPv4-Addr

Value
91.240.118.29
152.89.196.111
80.66.88.203
45.227.254.26
194.26.29.102
185.11.61.114

External References

- https://otx.alienvault.com/pulse/658c45ad9b174d9cf1b26ce0