Sep 13 2023

NETMANAGEIT

Intelligence Report

3AM: New Ransomware Family Used As Fallback in Failed LockBit Attack

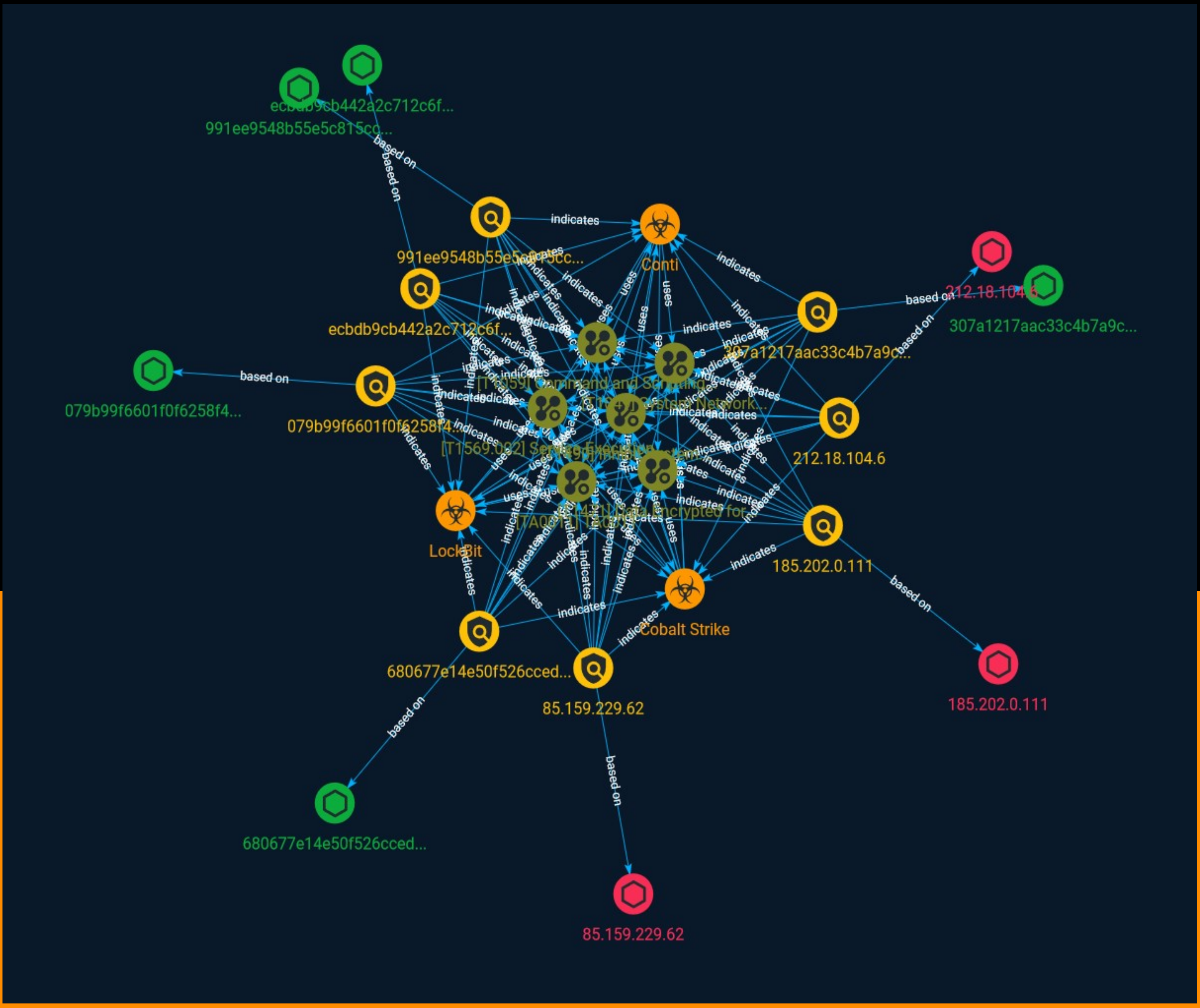

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A new ransomware family calling 3AM has been used as a fallback in a recent LockBit attack, according to security firm Symantec. the company's Threat Hunter Team and its researchers.

Confidence

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

15 / 100

Attack-Pattern

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

TA0011

ID

TA0011

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

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

Service Execution

ID

T1569.002

Description

Adversaries may abuse the Windows service control manager to execute malicious commands or payloads. The Windows service control manager (`services.exe`) is an interface to manage and manipulate services.(Citation: Microsoft Service Control Manager) The service control manager is accessible to users via GUI components as well as system utilities such as `sc.exe` and [Net](https://attack.mitre.org/software/S0039). [PsExec](https://attack.mitre.org/software/S0029) can also be used to execute commands or payloads via a temporary Windows service created through the service control manager API.(Citation: Russinovich Sysinternals) Tools such as [PsExec](https://attack.mitre.org/software/S0029) and `sc.exe` can accept remote servers as arguments and may be used to conduct remote execution. Adversaries may leverage these mechanisms to execute malicious content. This can be done by either executing a new or modified service. This technique is the execution used in conjunction with [Windows Service](https://attack.mitre.org/techniques/T1543/003) during service persistence or privilege escalation.

Name

System Network Connections Discovery

ID

T1049

Description

Adversaries may attempt to get a listing of network connections to or from the compromised system they are currently accessing or from remote systems by querying for information over the network. An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery techniques depending on the operating system, but the resulting information may include details about the networked cloud environment relevant to the adversary's goals. Cloud providers may have different ways in which their virtual networks operate.(Citation: Amazon AWS VPC Guide)(Citation: Microsoft Azure Virtual Network Overview)(Citation: Google VPC Overview) Similarly, adversaries who gain access to network devices may also perform similar discovery activities to gather information about connected systems and services. Utilities and commands that acquire this information include [netstat](https://attack.mitre.org/software/S0104), "net use," and "net session" with [Net](https://attack.mitre.org/software/S0039). In Mac and Linux, [netstat](https://attack.mitre.org/software/S0104) and `lsof` can be used to list current connections. `who -a` and `w` can be used to show which users are currently logged in, similar to "net session". Additionally, built-in features native to network devices and [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) may be used (e.g. `show ip sockets`, `show tcp brief`).(Citation: US-CERT-TA18-106A)

Indicator

Name

85.159.229.62

Description

ISP: LLC POWERNET **OS:** Ubuntu -------------------------- Hostnames: - serv11.ip-ptr.tech -------------------------- Domains: - ip-ptr.tech -------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDEA+L2rmMasvQceYAAOjARIxN6VVys7PhOuuYRIGmzO wKZ wN3ftKTPoS+O6isTRNUq07GKIAFM0/bkBREtYQzFjGuYIK27X5XGUTt2bdVlSW+rZDOnDfJHSezE FB33+a7sU5iR2kakW4SfZgcro8CmVDFXL69pii1FcGBa2YLBjGEK/I93Im/83xAeG2F0q8AIOpaR AXCk5eywCO+Th7wByjMdJFahLOkM59hnDq8DmVfmavNwUNkMfCyIjECvmtEJfiRUlk0w/n7HeuLd AjkJ7wV0K0FdJ5ZmhehCX2lr1SNcWSGMZDzYcX5WJG0zF1hzQ04Sx4ZS/+z1T7Bgz9NB Fingerprint: 6e:11:ea:25:e0:09:56:8c:d5:5c:52:fa:15:f5:4e:f6 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.159.229.62']

Name

ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc

Description

TEL:Trojan:Win32/BazaarLoader!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc']

Name

212.18.104.6

Description

ISP: GLOBAL INTERNET SOLUTIONS LLC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **445:** ``` SMB Status: Authentication: enabled SMB Version: 2 Capabilities: raw-mode ``` ------------------ **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10 (version 2004)/Windows Server (version 2004) OS Build: 10.0.19041 Target Name: DESKTOP-TCRDU4C NetBIOS Domain Name: DESKTOP-TCRDU4C NetBIOS Computer Name: DESKTOP-TCRDU4C DNS Domain Name: DESKTOP-TCRDU4C FQDN: DESKTOP-TCRDU4C ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.18.104.6']

Name

680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4']

Name

991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af']

Name

185.202.0.111

Description

ISP: Internet Technologies LLC **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **8000:** ``` \x00[\x1f@\xb9\xca\x00o ``` ------------------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.202.0.111']

Name

079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22']

Name

307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' =
'307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e']

Malware

Name
LockBit
Name
Conti
Description
[Conti](https://attack.mitre.org/software/S0575) is a Ransomware-as-a-Service (RaaS) that was first observed in December 2019. [Conti](https://attack.mitre.org/software/S0575) has been deployed via [TrickBot](https://attack.mitre.org/software/S0266) and used against major corporations and government agencies, particularly those in North America. As with other ransomware families, actors using [Conti](https://attack.mitre.org/software/S0575) steal sensitive files and information from compromised networks, and threaten to publish this data unless the ransom is paid.(Citation: Cybereason Conti Jan 2021)(Citation: CarbonBlack Conti July 2020)(Citation: Cybleinc Conti January 2020)
Name
Cobalt Strike
Description
[Cobalt Strike](https://attack.mitre.org/software/S0154) is a commercial, full-featured, remote access tool that bills itself as “adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors”. Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics,

all executed within a single, integrated system.(Citation: cobaltstrike manual) In addition to its own capabilities, [Cobalt Strike](https://attack.mitre.org/software/S0154) leverages the capabilities of other well-known tools such as Metasploit and [Mimikatz](https://attack.mitre.org/software/S0002).(Citation: cobaltstrike manual)

StixFile

Value
991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af
ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc
307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e
680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4
079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22

IPv4-Addr

Value
185.202.0.111
212.18.104.6
85.159.229.62

External References

- https://otx.alienvault.com/pulse/6501cc69cc0ead4d9032b395
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/3am-ransomware-lockbit