Ako Ransomware: Another Day, Another Infection Attacking Businesses

By **Lawrence Abrams** January 10, 2020 06:00 AM **0**

Like moths to a flame, new ransomware targeting businesses keep appearing every day as they are enticed by the prospects of million-dollar ransom payments. An example of this is a new ransomware called Ako that is targeting the entire network rather than just individual workstations.

Ako was discovered yesterday when a victim posted in the BleepingComputer support forums about a new ransomware that had encrypted both their Windows 10 desktop and their Windows SBS 2011 server.

Forum Post about Ako

After looking at the ransom note and the Tor payment site, it quickly became apparent that this was not a ransomware infection we had seen before.

Looking on VirusTotal, I was able to find an older sample of the ransomware and shared it with SentinelLab's Vitali Kremez who offered to help analyze it. Soon after, newer samples [1, 2] were found that allowed us to see a broader picture of how this ransomware works.

According to Kremez, who performed the analysis of the ransomware, Ako shares some similarities to MedusaLocker that has led people to call it MedusaReborn.

"This is the new ransomware-as-a-service offering under development with the version 0.5 that seems to be inspired by the Medusa Locker behavior including its anti-Windows behavior and registry mapped drive disable targeting and isolating specific machines for encryption," Kremez told BleepingComputer.

The ransomware operators confirmed this by telling BleepingComputer via email that the Ako ransomware is their own program.

> "We see news about us. But that is wrong. About MedusaReborn. We have nothing to do with Medusa or anything else. This is our own product - Ako Ransomware, well, this is if you are of course interested."

To make matters worse, when we asked the ransomware operators if they are stealing data before encrypting, they told us "Yes, it's our job."

How Ako Ransomware encrypts a device

When started, Ako will first execute the following commands to delete shadow volume copies, clear recent backups, and disable the Windows recovery environment.

```
vssadmin.exe Delete Shadows /All /Quiet
bcdedit.exe /set {default} recoveryenabled No
bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
wbadmin DELETE SYSTEMSTATEBACKUP
wbadmin DELETE SYSTEMSTATEBACKUP -deleteOldest
wmic.exe SHADOWCOPY /nointeractive
```

It will also create the Registry value **EnableLinkedConnections** under the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** registry key and set it to **1**. This is done to make sure mapped drives are accessible even in a UAC launched process.

The ransomware will now begin to encrypt files on the device.

When encrypting files, Ako will encrypt all files that do not match the ".exe,. dll, .sys, .ini, .lnk, .key, .rdp" extensions and whose paths do not contain the following strings:

```
Folder Blacklist:
$,AppData
Program Files
Program Files (x86)
AppData
boot
PerfLogs
ProgramData
Google
Intel
Microsoft
Application Data
Tor Browser
Windows
```

When a file is encrypted, it will be renamed to and a randomly generated extension will be appended to the file name. For example, 1.doc would be encrypted and renamed to 1.doc.Ci3Qn3 as shown below.

Encrypted Files

Appended to the contents of each file will also be a **CECAEFBE** file marker that can be used to identify that this file was encrypted by Ako. This file marker can be seen in the hex editor of an encrypted file below.

CECAEFBE File Marker

During the encryption process, Ako will use the GetAdaptersInfo function to get a list of network adapters and their associated IP addresses.

The ransom will then perform a ping scan of any local networks using the IcmpSendEcho function to create a list of responding machines.

Any machines that respond, will be checked for network shares to encrypt as well.

When the ransomware is finished, the encryption key used to encrypt the victim's files will itself be encrypted and stored in a file named **id.key** on the victim's Windows desktop.

Encrypted encryption key

Also on the desktop will be a ransom note named **ako-readme.txt**. This note contains a URL to access the Ako Tor payment site in order to get payment instructions. This site is located
at http://kwvhrdibgmmpkhkidrby4mccwqpds5za6uo2thcw5gz75qncv7rbhyad.onion.

Ako Ransom Note

Note how the ransom note states that "Your network have been locked" to indicate they are targeting networks and not individual devices. When we asked the ransomware developers whether they target both both networks and individual workstations, they told BleepingComputer that they are "Only working on network."

Included in the ransom note is a 'Personal ID' that when decoded becomes a JSON formatted object containing the extension, encrypted key, network configuration setting, a subid most likely used for affiliates, and the ransomware's version. The version is currently at .5.

Decoded Personal ID

When a victim accesses the Tor site they will need to enter their personal ID to see the ransom demand and instructions.

Tor Payment Site

This Tor payment site also includes a chat service and the ability to decrypt 1 file, which is a bit low as most ransomware infections allow the decryption of at least three files.

Unfortunately, in a brief analysis by ID-Ransomware owner Michael Gillespie, the encryption method used by Ako appears to be secure.

If a weakness is discovered, we will be sure to post more information. For now, if you wish to discuss this ransomware or need help, you can use our Ako Ransomware Support & Help topic.

Furthermore, it is not known how this ransomware is distributed but is most likely through hacked Remote Desktop services. If you are affected by this ransomware, we would be interested in learning how your network became infected.

Related Articles:

Nemty Ransomware to Start Leaking Non-Paying Victim's Data

Sodinokibi Ransomware Hits New York Airport Systems

Sodinokibi Ransomware Publishes Stolen Data for the First Time

The Week in Ransomware - January 10th 2020 - Now Data Breaches

Maze Ransomware Publishes 14GB of Stolen Southwire Files

IOCs

Hashes:

```
389747789dfab2142873617585e342575792d8c1c85f4b51b36539a16c461b5a
a6ba509923864b65a437047e8a53d249c68025f4e29eb3efe0ebe16761d28667
```

Associated file names:

```
ako-readme.txt
id.key
```

Associated Registry keys:

```
HKEY_CURRENT_USER\Software\akocfg
```

AKO **MEDUSALOCKER** **RANSOMWARE**

LAWRENCE ABRAMS

Lawrence Abrams is the creator and owner of BleepingComputer.com. Lawrence's area of expertise includes malware removal and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

PREVIOUS ARTICLE

NEXT ARTICLE

Post a Comment

Community Rules

You need to login in order to post a comment

Login

Not a member yet? Register Now

You may also like:

POPULAR STORIES

Windows 7 Reminder: Get a Free Windows 10 Upgrade While You Can

Sodinokibi Ransomware Publishes Stolen Data for the First Time

Follow us:

MAIN SECTIONS

News

Downloads

Virus Removal Guides

Tutorials

Startup Database

Uninstall Database

File Database

Glossary

COMMUNITY

Forums

Forum Rules

Chat

USEFUL RESOURCES

Welcome Guide

Sitemap

COMPANY

About BleepingComputer

Contact Us

Send us a Tip!

Advertising

Write for BleepingComputer

Social & Feeds

Changelog