# McAfee Labs Threat Advisory

## Ransomware-Sodinokibi

April 3, 2020

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that can be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware & Threat Advisories" at the following URL: https://www.mcafee.com/enterprise/en-us/sns/preferences/sns-form.html.

### Summary

REvil/Sodinokibi ransomware encrypts files on a system using cryptographic algorithms. This ransomware not only encrypts the files, but also steals the information from the system and threatens the user to pay the ransom.

Detailed information about the threat, its propagation, characteristics and mitigation are in the following sections:



### Infection and Propagation Vectors

Most ransomware campaigns typically spread through Exploit Kits and Mal-spam campaigns instrumented using various botnets. However, Ransomware-Sodinokibi is suspected to be distributed using highly targeted attacks such as brute forcing of RDP connections on unprotected systems in an organization's network. When the attackers have access to the organization's network, the ransomware is deployed to business-critical systems to cause maximum disruption of services and in-turn warrant a considerable ransom.

### Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

Refer the following Knowledge Base articles to configure Access Protection rules in VirusScan Enterprise:

- KB81095: How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
- KB54812: How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

### Additional End User Recommendations

- **Do NOT open Office document file attachments unless specifically requested from the sender**. View the email header or send a separate email to validate the sender before opening attachments.

- **Disable Macro in Microsoft Office applications**. Macros can run in Office applications only if Macro Settings are set to "Enable all macros" or if the user manually enables a macro. By default, it will be in a disabled state. The recommended setting is to select the option "Disable all macros with notification" in "Macro Settings."

- **End users should back up business data to the organization's shared folders**. Data residing on user devices might be permanently lost in the event of a ransomware infection.

- **Report suspect email to the organization's Security Operations Center**. Remind your employees how and where to submit suspicious email safely.

**Endpoint Security**
Mitigation methods for assorted malware is available in the product guide below. Any specific mitigation steps, if necessary, are described later in this advisory.
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

**ePolicy Orchestrator**
- To block the access to USB drives through the ePO DLP policy, refer to this tutorial.

**VirusScan Enterprise**
- Refer to KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

**Host Intrusion Prevention**
- Refer to KB71329 to blacklist applications using a Host Intrusion Prevention custom signature.
- Refer to KB71794 to create an application blocking rules policies to prevent the binary from running, and to create an application blocking rules policies that prevents a specific executable from hooking any other executable.

**McAfee Ransomware Interceptor**
- To download and install McAfee Ransomware Interceptor, refer to McAfee Free Tools.

**Other**
- To disable the Autorun feature on Windows remotely using Windows Group Policies, refer this article from Microsoft.

## Characteristics and Symptoms

Upon execution, this malware decrypts a JSON config file stored in a binary using a hardcoded key and XOR decryption.

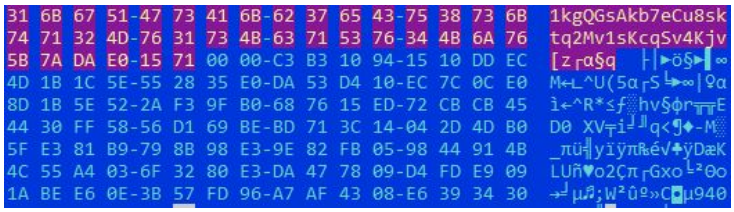


**Fig.1 Decryption key and encrypted JSON content**

```
74 5C           je 3777f3e092f2208c6670c01816562a7d.412D78
53              push ebx
8B 5D 14        mov ebx,dword ptr ss:[ebp+14]
29 5D 0C        sub dword ptr ss:[ebp+C],ebx
8B 55 08        mov edx,dword ptr ss:[ebp+8]
40              inc eax
0F B6 C8        movzx ecx,al
8B 45 08        mov eax,dword ptr ss:[ebp+8]
89 4D 10        mov dword ptr ss:[ebp+10],ecx
8B 5D 10        mov ebx,dword ptr ss:[ebp+10]
8A 0C 01        mov cl,byte ptr ds:[ecx+eax]
0F B6 C1        movzx eax,cl
03 C6           add eax,esi
0F B6 F0        movzx esi,al
8B 45 08        mov eax,dword ptr ss:[ebp+8]
8A 04 06        mov al,byte ptr ds:[esi+eax]
88 04 13        mov byte ptr ds:[ebx+edx],al
8B C2           mov eax,edx
8B D3           mov edx,ebx
8B 5D 14        mov ebx,dword ptr ss:[ebp+14]
88 0C 06        mov byte ptr ds:[esi+eax],cl
0F B6 04 02     movzx eax,byte ptr ds:[edx+eax]
8B 55 0C        mov edx,dword ptr ss:[ebp+C]
0F B6 C9        movzx ecx,cl
03 C8           add ecx,eax
0F B6 C1        movzx eax,cl
8B 4D 08        mov ecx,dword ptr ss:[ebp+8]
8A 04 08        mov al,byte ptr ds:[eax+ecx]
32 04 1A        xor al,byte ptr ds:[edx+ebx]
88 03           mov byte ptr ds:[ebx],al
43              inc ebx
8B 45 10        mov eax,dword ptr ss:[ebp+10]
89 5D 14        mov dword ptr ss:[ebp+14],ebx
83 EF 01        sub edi,1
75 AC           jne 3777f3e092f2208c6670c01816562a7d.412D23
```

**Fig. 2 XOR decryption**


```
{
        "pk":"YO9E7ouT83RseZgGnLR2DxiFRbXiteYQirOJcZOjplo=",
        "pid":"$2a$10$7qQ70syLvX5aslSuSa9AWurg843zRR.433XEtfk2rGURjN9e.xNz6",
        "sub":"3195",
        "dbg":false,
        "et":1,
        "wipe":false,
        "wht":{
                "fld":["programdata","perflogs","application data","appdata","$windo
                "fls":["boot.ini","ntuser.dat","iconcache.db","autorun.inf","bootse
                "ext":["msp","rom","rtp","shs","mod","cur","msc","nomedia","deskthe
              },
        "wfld":["backup"],
        "prc":["w3wp","thunderbird","mydesktopqos","powerpnt","outlook","srv","info
        "dmn":"sweering.fr;shiresresidential.com;bogdanpeptine.ro;ruralarcoiris.com
        "net":false,
        "svc":["memtas","crm","quickbooks","svc$","veeam","oracle","mepocs","exchan
        "nbody":"LQAtAC0APQA9AD0AIABXAGUAbABjAG8AbQBlAC4AIABBAGcAYQBpAG4ALgAgAD0APQA
        "nname":"{EXT}-readme.txt",
        "exp":false,
        "img":"QQBsAGwAIABvAGYAIAB5AG8AdQByACAAZgBpAGwAZQBzACAAYQByAGUAIABlAG4AYwBy
        "arn":false
}
```


**Fig. 3 JSON config file**

Fields and definitions in the JSON config file:

- pk: Base64-encoded attacker's public key.
- pid: Probably infection campaign identifier.
- sub: Probably infection campaign identifier.
- dbg: Key to set debug mode in development.
- et: Unknown integer.
- wipe: Switch to wipe blacklisted folders.
- wht: Contains whitelisted folder, file, and file extension.
    - fld: Array of the whitelisted folders.
    - fls: Array of the whitelisted files.
    - ext: Array of the whitelisted file extensions.
- wfld: Contains the blacklisted folder. If this key was set, this ransomware attempts to wipe this folder instead of encrypting.
- prc: Process that this ransomware tries to terminate.
- dmn: List of domains of C2 servers.
- net: Switch to exfiltrate host information and set information to C2 server.
- svc: Target servers to terminate.
- nbody: Base64-encoded ransom note.
- nname: File name of the ransom note that drop to each folder.
- exp: Switch to elevate privileges by exploiting a local privilege escalation (LPE) vulnerability.
- img: Base64-encode ransom desktop image.
- arn: Unknown value

After the config file decryption, it tries to create a mutex as shown below, using a hard-coded value as its name. This mutex can be used as an indicator to detect or prevent a Sodinokibi ransomware infection.

| | | |
|---|---|---|
| Key | HKCU\Software\Microsoft\Windows NT\CurrentVersion | 0x2f8 |
| Mutant | \BaseNamedObjects\1DE3C565-E22C-8190-7A66-494816E6C5F5 | 0x150 |
| Mutant | \Sessions\1\BaseNamedObjects\SM0:7484:168:WilStaging_02 | 0x1bc |

Fig. 4. Mutex created by Sodinokibi ransomware

If the creation of the mutex is successful, it tries to query the **"exp"** key in the JSON config file to elevate privileges using an LPE exploit if this key is enabled.

It then creates random file extensions, a ransom note, and a desktop image. The filename of the ransom note is created by using the key "nname" in the JSON config file. The {EXT} part is replaced with a random prefix (for example, n6986ti74t-readme.txt), and this ransom note will be dropped in each affected folder.

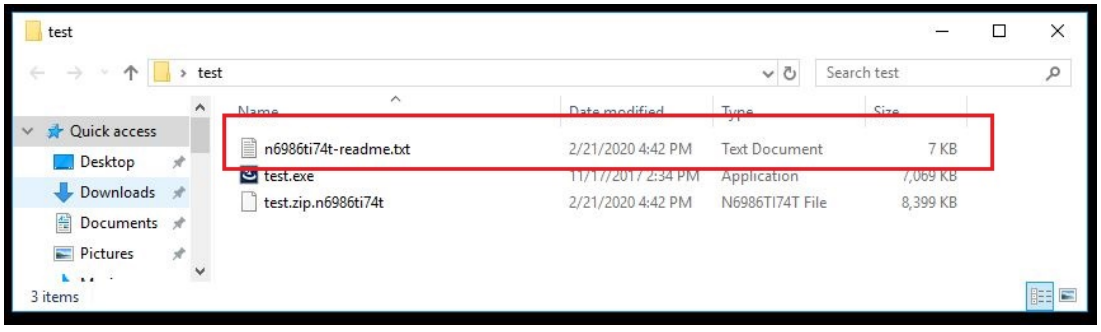


**Fig. 5. Ransom note**

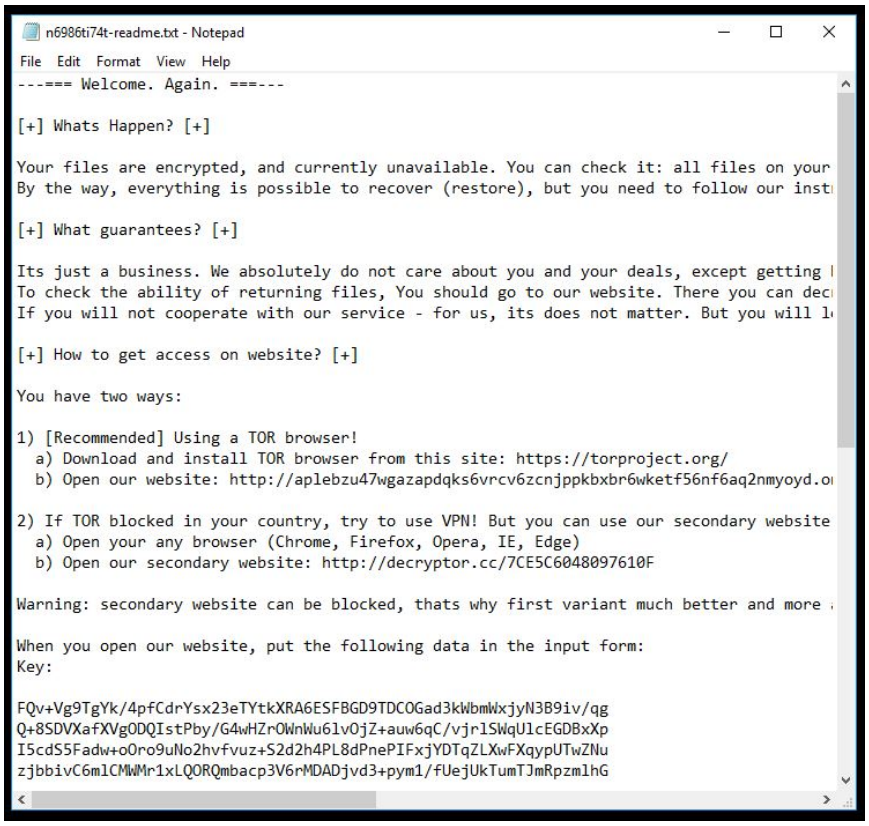


Fig. 6. Ransom note content


Fig. 7. Ransomware background image

Before it encrypts the files on the disk and in network share folders, it will enumerate all the running process, and terminate processes that contain the following strings:

- "w3wp"
- "thunderbird"
- "mydesktopqos"
- "powerpnt"
- "outlook"
- "srv"
- "infopath"
- "msaccess"
- "ocautoupds"
- "qb"
- "core"
- "mspub"
- "store"
- "ssms"
- "dbeng50"

- "ax32"
- "sql"
- "exchange"
- "onenote"
- "ocssd"
- "sage"
- "pos"
- "word"
- "java"
- "sophos"
- "xfssvccon"
- "visio"
- "synctime"
- "oracle"
- "crm"
- "excel"
- "dbs"
- "ocomm"
- "svc$"

It will also terminate services that contain the following strings:

- "memtas"
- "crm"
- "quickbooks"
- "svc$"
- "veeam"
- "oracle"
- "mepocs"
- "exchange"
- "pos"
- "vss"
- "sql"
- "backup"
- "qb"
- "sophos"
- "sage"

To ensure that the compromised system is unable to restore from backup, it will launch a new process to execute a PowerShell script to delete the shadow volume.

```
Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

**Fig. 8. PowerShell script to delete shadow volume**

Sodinokibi will wipe the file inside blacklisted folders if the wipe key is set to true. In testing, the wipe key of this variant is set to “false” and the blacklisted folder is set to “backup.”

During its encryption routine, the ransomware will avoid infecting certain folders, files, and even files with certain extensions.

**Whitelisted folder:**

- "programdata"
- "perflogs"
- "application data"
- "appdata"
- "$windows.~bt"
- "system volume information"
- "windows"
- "tor browser"
- "google"
- "msocache"

- "boot"
- "windows.old"
- "$windows.~ws"
- "mozilla"
- "intel"

**Whitelisted file:**
- "boot.ini"
- "ntuser.dat"
- "iconcache.db"
- "autorun.inf"
- "bootsect.bak"
- "desktop.ini"
- "thumbs.db"
- "ntuser.ini"
- "ntuser.dat.log"
- "ntldr"
- "bootfont.bin"

**Whitelisted extension:**
- "msp"
- "rom"
- "rtp"
- "shs"
- "mod"
- "cur"
- "msc"
- "nomedia"
- "deskthemepack"
- "diagcab"
- "diagcfg"
- "msstyles"
- "scr"
- "hta"
- "idx"
- "ics"
- "lock"
- "diagpkg"
- "icns"
- "msi"
- "themepack"
- "key"
- "bin"
- "theme"
- "bat"
- "cab"
- "nls"
- "spl"
- "icl"
- "sys"
- "drv"
- "lnk"
- "cmd"
- "adv"
- "cpl"
- "ico"
- "com"
- "exe"
- "ocx"
- "dll"
- "hlp"
- "mpa"
- "prf"
- "wpx"
- "ani"

- "msu"
- "ps1"
- "386"

Sodinokibi uses AES and Salsa20 algorithms to encrypt files. AES is used to encrypt session keys and data that is sent to the control server, and files are encrypted using Salsa20 encryption. So, it's impossible to recover the file without the attacker's private key. The encrypted file was renamed with random prefix and its original value, as shown below:

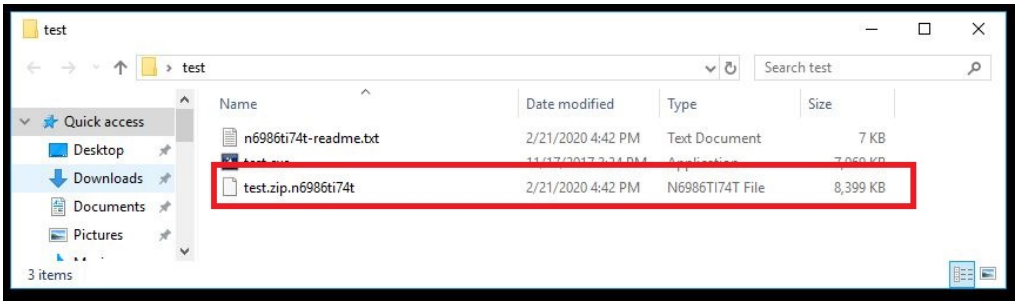


Fig. 9. File encrypted by Sodinokibi

Once the encryption process is done, Sodinokibi will query the "net" key in JSON file to determine if C2 communication should take place. If the key is set to true, it will iterate all of the C2 domains listed in the JSON config file and use the designed pattern to build the URL. In the testing sample, "net" key is set to false, so no network activity was observed.

## Restart Mechanism

Once the machine is encrypted, there are no signs of any restart mechanism for this malware on the system.

## Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risks and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://www.mcafee.com/enterprise/en-us/services/foundstone-services.html

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.