Files

02bcbfc

Go to file

KB
TTPs
Threat Intelligence
MSTIC
The DFIR Report
20210329_Sodinokibi_(aka_RE...
Tools
README.md


```yaml
source_type: "Threat Intelligence Report"
report:
  title: "Sodinokibi (aka REvil) Ransomware"
  vendor: "The DFIR Report"
  published: "29.03.2021"
  link:
    - https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
  analyzed_by: Vadim Khrykov (@BlackMatter23)
  threat:
    name:
      - REvil
    aliases:
      - Sodinokibi
      - GOLD SOUTHFIELD
      - G0115
    attribution:
      - Worldwide
    tools:
      - IceID (Bokbot)
      - Cobalt Strike
      - Bloodhound
analysis:
  quote: >
    - "Initial execution of the document writes a file to... The Excel file called wmic
  mitre_attack:
    execution:
      - T1204.002 - User Execution - Malicious File
      - T1047 - Windows Management Instrumentation
    defense_evasion:
      - T1218.010 - Signed Binary Proxy Execution - Regsvr32
detection:
  ideas: >
    - monitor Office applications spawning WMI command-line (WMIC.exe) utility.
      Note: add more office applications to the rules logic of your choice.
  telemetry:
    process_create:
      - Windows EID 4688
      - Sysmon EID 1
      - EDR (PsSetCreateProcessNotifyRoutine/Ex)
  rules: >
    - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\wbem\\WMIC.e
      AND CreatorProcessName:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
    - Channel:Sysmon AND EventID:1 AND (Image:"\\wbem\\WMIC.exe" OR CommandLine:"*w
      AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
  ideas: >
    - monitor WMI "Win32_Process::Create" command execution by Office applications
      Note: add more office applications to the rule logic of your choice.
  telemetry:
    wmi_execution:
      - EDR (Microsoft-Windows-WMI-Activity ETW)
  rules: >
    - Channel:EDR AND EventType:WMIExecution AND Image:("\\winword.exe" OR "\\excel
  ideas: >
    - Excel called wmic to finally proxy execute regsvr32 with the payload. An atta
      But we have command-line in the event which allow us to "restore" this suspic
      Monitor process creation with "wmic process call create" and LOLBins in comma
```

```
56              Monitor process creation with "wmic process call create" and LOLBins in comma
57              Note: add more LOLBins to the rules logic of your choice.
58          telemetry:
59            process_create:
60              - Windows EID 4688
61              - Sysmon EID 1
62              - EDR (PsSetCreateProcessNotifyRoutine/Ex)
63          rules: >
64            - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\wbem\\WMIC.e
65              AND ProcessCommandLine:(*regsvr32* OR *rundll32* OR *msiexec* OR *mshta* OR *
66            - Channel:Sysmon AND EventID:1 AND (Image:"\\wbem\\WMIC.exe" OR CommandLine:"*w
67              AND CommandLine:*process* AND CommandLine:*call* AND CommandLine:*create* AND
68              AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
69          ideas: >
70            - monitor LOLBins process creations by Office applications.
71              Note: add more LOLBins and Office applications to the rules logic of your cho
72          telemetry:
73            process_create:
74              - Windows EID 4688
75              - Sysmon EID 1
76              - EDR (PsSetCreateProcessNotifyRoutine/Ex)
77          rules: >
78            - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\regsvr32.exe
79              AND CreatorProcessName:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
80            - Channel:Sysmon AND EventID:1 AND Image:("\\regsvr32.exe" OR "\\rundll32.exe"
81              AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
82          ideas: >
83            - monitor LOLBins process creations with Wmiprvse parent process.
84              Note: add more LOLBins to the rules logic of your choice. FPs are possible he
85          telemetry:
86            process_create:
87              - Windows EID 4688
88              - Sysmon EID 1
89              - EDR (PsSetCreateProcessNotifyRoutine/Ex)
90          rules: >
91            - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\regsvr32.exe
92              AND CreatorProcessName:("\\wbem\\WmiPrvSE.exe")
93            - Channel:Sysmon AND EventID:1 AND Image:("\\regsvr32.exe" OR "\\rundll32.exe"
94              AND ParentImage:("\\wbem\\WmiPrvSE.exe")
95          ideas: >
96            - monitor executable and script files creation by Office applications, use file
97              Note: add more files extensions/magic bytes to the rules logic of your choice
98          telemetry:
99            file_create:
100             - Sysmon EID 11
101             - EDR (minifilter)
102           file_rename:
103             - EDR (minifilter)
104         rules: >
105           - Channel:Sysmon AND EventID:11 AND Image:("\\winword.exe" OR "\\excel.exe" OR
106             AND TargetFilename:(*.exe OR *.dll OR *.ocx OR *.com OR *.ps1 OR *.vbs OR *.s
107           - Channel:EDR AND EventType:(FileCreate OR FileRename) AND Image:("\\winword.ex
108             AND (Filename:(*.exe OR *.dll OR *.ocx OR *.com OR *.ps1 OR *.vbs OR *.sys OR
109     quote: >
110       - "This (MS Excel) then made a network request to download a file from this URL"
111     mitre_attack:
112       defense_evasion:
113         - T1218.010 - Signed Binary Proxy Execution - Regsvr32
114       detection:
115         ideas: >
116           - MS Excel process initiated an external network connection, if we try to monit
117             instead monitor outbound network connections initiated by Regsvr32.exe (not d
118             Note: you may also check hypothesis for local-to-local connections and add ot
```

```
            - EDR (minifilter)
          file_rename:
            - EDR (minifilter)
          file_delete:
            - EDR (minifilter)
        rules: >
          - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\rclone.exe"
          - Channel:Sysmon AND EventID:1 AND (OriginalFileName:"rclone.exe" OR Company:""
          - Channel:EDR AND EventType:(FileCreate OR FileRename OR FileDelete) AND (Origi
            AND NOT FilePath:"\\rclone.exe"
        ideas: >
          - monitor Rclone tool execution with suspicious command-lines.
        telemetry:
          process_create:
            - Windows EID 4688
            - Sysmon EID 1
            - EDR (PsSetCreateProcessNotifyRoutine/Ex)
        rules: >
          - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\rclone.exe"
            AND ProcessCommandLine.keyword:/.*\\\\.*\\(ADMIN|IPC|C)\$.*/ AND ProcessComma
          - Channel:Sysmon AND EventID:1 AND (Image:"\\rclone.exe" OR CommandLine:"*rclon
            AND CommandLine.keyword:/.*\\\\.*\\(ADMIN|IPC|C)\$.*/ AND CommandLine:(*http*
        ideas: >
          - monitor system processes execution from untypical paths. Add more executables
        telemetry:
          process_create:
            - Windows EID 4688
            - Sysmon EID 1
            - EDR (PsSetCreateProcessNotifyRoutine/Ex)
        rules: >
          - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\svchost.exe"
            AND NOT NewProcessName:("C\:\\Windows\\System32\\" OR "C\:\\Windows\\SysWOW64
          - Channel:Sysmon AND EventID:1 AND Image:("\\svchost.exe" OR "\\gpupdate.exe" O
            AND NOT Image:("C\:\\Windows\\System32\\" OR "C\:\\Windows\\SysWOW64\\")
      quote: >
        - "For the final actions, the threat actors dropped a ransomware executable on the
      detection:
        - https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/main/TTPs/Defense%20Ev
      quote: >
        - "The -smode flag was used with the ransomware executable to set the system to reb
        - "bootcfg /raw /a /safeboot:network /id 1 (pre-Vista)"
        - "bcdedit /set {current} safeboot network" (Vista+)"
        - "bcdedit /deletevalue {current} safeboot"
        - "REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /v "*UndoSB" /t R
      mitre_attack:
        defense_evasion:
          - T1562.001 - Impair Defenses - Disable or Modify Tools
        detection:
          ideas: >
            - monitor bootcfg/bcdedit tools execution with "safeboot" option. Multiple aler
            - monitor writing bootcfg/bcdedit executables to Windows registry run keys. Add
        telemetry:
          process_create:
            - Windows EID 4688
            - Sysmon EID 1
            - EDR (PsSetCreateProcessNotifyRoutine/Ex)
          registry_value_set:
            - Windows EID 4657 (SACL)
            - Sysmon EID 13
            - EDR (CmRegisterCallback/Ex, Registry API)
        rules: >
          - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:("\\bcdedit.exe"
          - Channel:Sysmon AND EventID:1 AND (Image:("\\bcdedit.exe" OR "\\bootcfg.exe") OR
            OR Description:("Boot Configuration Data Editor" OR "BootCfg*")) AND CommandLin
          - Channel:Windows-Security AND EventID:4657 AND ObjectName:"*\\Windows\\CurrentVe
          - Channel:Sysmon AND EventID:13 AND TargetObject:"*\\Windows\\CurrentVersion\\Run
          - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:("\\powershell.ex
            AND ProcessCommandLine:("*Set-ItemProperty*" OR "* sp *" OR "*add*") AND Proces
          - Channel:Sysmon AND EventID:1 AND (Image:("\\powershell.exe" OR "\\pwsh.exe" OR
            OR Description:("Windows PowerShell" OR "Registry Console Tool")) AND CommandLi
          - Channel:Windows-Powershell AND EventID:400 AND HostApplication:("*powershell *"
            AND HostApplication:"*\\Windows\\CurrentVersion\\Run*" AND HostApplication:("*b
```