Sign in

vadim-hunter / **Detection-Ideas-Rules**
Public

Notifications
Fork 28
Star 178

Code
Issues
Pull requests
Actions
Projects
Security
Insights

Detection-Ideas-Rules / Threat Intelligence / The DFIR Report
/ 20210329_Sodinokibi_(aka_REvil)_Ransomware.yaml

652 lines (650 loc) · 42.5 KB

Code
Blame
Raw

```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 to execute
```

```
    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.exe" OR Proce
            AND CreatorProcessName:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
          - Channel:Sysmon AND EventID:1 AND (Image:"\\wbem\\WMIC.exe" OR CommandLine:"*wmic *" OR Or
            AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
        ideas: >
          - monitor WMI "Win32_Process::Create" command execution by Office applications processes.
            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.exe" OR "\\
        ideas: >
          - Excel called wmic to finally proxy execute regsvr32 with the payload. An attacker wanted
            But we have command-line in the event which allow us to "restore" this suspicous parent-c
            Monitor process creation with "wmic process call create" and LOLBins in command-line with
            Note: add more LOLBins 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.exe" OR Proce
            AND ProcessCommandLine:(*regsvr32* OR *rundll32* OR *msiexec* OR *mshta* OR *verclsid*) A
          - Channel:Sysmon AND EventID:1 AND (Image:"\\wbem\\WMIC.exe" OR CommandLine:"*wmic *" OR Or
            AND CommandLine:*process* AND CommandLine:*call* AND CommandLine:*create* AND CommandLine
            AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
        ideas: >
          - monitor LOLBins process creations by Office applications.
```

```
            Note: add more LOLBins and 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:("\\regsvr32.exe" OR "\\rund
            AND CreatorProcessName:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
          - Channel:Sysmon AND EventID:1 AND Image:("\\regsvr32.exe" OR "\\rundll32.exe" OR "\\msiexe
            AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
        ideas: >
          - monitor LOLBins process creations with Wmiprvse parent process.
            Note: add more LOLBins to the rules logic of your choice. FPs are possible here, but some
        telemetry:
          process_create:
            - Windows EID 4688
            - Sysmon EID 1
            - EDR (PsSetCreateProcessNotifyRoutine/Ex)
        rules: >
          - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\regsvr32.exe" OR "\\rund
            AND CreatorProcessName:("\\wbem\\WmiPrvSE.exe")
          - Channel:Sysmon AND EventID:1 AND Image:("\\regsvr32.exe" OR "\\rundll32.exe" OR "\\msiexe
            AND ParentImage:("\\wbem\\WmiPrvSE.exe")
        ideas: >
          - monitor executable and script files creation by Office applications, use files extensions
            Note: add more files extensions/magic bytes to the rules logic of your choice.
        telemetry:
          file_create:
            - Sysmon EID 11
            - EDR (minifilter)
          file_rename:
            - EDR (minifilter)
        rules: >
          - Channel:Sysmon AND EventID:11 AND Image:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.
            AND TargetFilename:(*.exe OR *.dll OR *.ocx OR *.com OR *.ps1 OR *.vbs OR *.sys OR *.bat
          - Channel:EDR AND EventType:(FileCreate OR FileRename) AND Image:("\\winword.exe" OR "\\exc
            AND (Filename:(*.exe OR *.dll OR *.ocx OR *.com OR *.ps1 OR *.vbs OR *.sys OR *.bat OR *.
    quote: >
      - "This (MS Excel) then made a network request to download a file from this URL"
    mitre_attack:
      defense_evasion:
        - T1218.010 - Signed Binary Proxy Execution - Regsvr32
      detection:
        ideas: >
          - MS Excel process initiated an external network connection, if we try to monitor such acti
```

```
          MS Excel process initiated an external network connection, if we try to monitor such acti
          instead monitor outbound network connections initiated by Regsvr32.exe (not directly rela
          Note: you may also check hypothesis for local-to-local connections and add other LOLBins 
```

```
    - EDR (minifilter)
   file_rename:
    - EDR (minifilter)
   file_delete:
    - EDR (minifilter)
  rules: >
   - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\rclone.exe" OR ProcessCo
   - Channel:Sysmon AND EventID:1 AND (OriginalFileName:"rclone.exe" OR Company:""*rclone\.org
   - Channel:EDR AND EventType:(FileCreate OR FileRename OR FileDelete) AND (OriginalFileName:
    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" OR ProcessCo
    AND ProcessCommandLine.keyword:/.*\\\\.*\\(ADMIN|IPC|C)\$.*/ AND ProcessCommandLine:(*htt
   - Channel:Sysmon AND EventID:1 AND (Image:"\\rclone.exe" OR CommandLine:"*rclone *" OR Orig
    AND CommandLine.keyword:/.*\\\\.*\\(ADMIN|IPC|C)\$.*/ AND CommandLine:(*http* OR *ftp*)
  ideas: >
   - monitor system processes execution from untypical paths. Add more executables of your cho
  telemetry:
   process_create:
    - Windows EID 4688
    - Sysmon EID 1
    - EDR (PsSetCreateProcessNotifyRoutine/Ex)
  rules: >
   - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\svchost.exe" OR "\\gpupd
    AND NOT NewProcessName:("C\:\\Windows\\System32\\" OR "C\:\\Windows\\SysWOW64\\")
   - Channel:Sysmon AND EventID:1 AND Image:("\\svchost.exe" OR "\\gpupdate.exe" OR "\\taskhos
    AND NOT Image:("C\:\\Windows\\System32\\" OR "C\:\\Windows\\SysWOW64\\")
quote: >
 - "For the final actions, the threat actors dropped a ransomware executable on the domain contr
detection:
 - https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/main/TTPs/Defense%20Evasion/T1197%
quote: >
 - "The -smode flag was used with the ransomware executable to set the system to reboot into Saf
 - "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 REG_SZ /d "bc
    mitre_attack:
      defense_evasion:
        - T1562.001 - Impair Defenses - Disable or Modify Tools
      detection:
        ideas: >
          - monitor bootcfg/bcdedit tools execution with "safeboot" option. Multiple alerts of this r
          - monitor writing bootcfg/bcdedit executables to Windows registry run keys. Add more regist
      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" OR "\\bootcf
        - Channel:Sysmon AND EventID:1 AND (Image:("\\bcdedit.exe" OR "\\bootcfg.exe") OR CommandLine
          OR Description:("Boot Configuration Data Editor" OR "BootCfg*")) AND CommandLine:*safeboot*
        - Channel:Windows-Security AND EventID:4657 AND ObjectName:"*\\Windows\\CurrentVersion\\Run*"
        - Channel:Sysmon AND EventID:13 AND TargetObject:"*\\Windows\\CurrentVersion\\Run*" AND Detai
        - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:("\\powershell.exe" OR "\\pws
          AND ProcessCommandLine:("*Set-ItemProperty*" OR "* sp *" OR "*add*") AND ProcessCommandLine
        - Channel:Sysmon AND EventID:1 AND (Image:("\\powershell.exe" OR "\\pwsh.exe" OR "\\reg.exe")
          OR Description:("Windows PowerShell" OR "Registry Console Tool")) AND CommandLine:("*Set-It
        - Channel:Windows-Powershell AND EventID:400 AND HostApplication:("*powershell *" OR "*pwsh *
          AND HostApplication:"*\\Windows\\CurrentVersion\\Run*" AND HostApplication:("*bcdedit *" OR


```