



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



```
1  source_type: "Threat Intelligence Report"
2  report:
3    title: "Sodinokibi (aka REvil) Ransomware"
4    vendor: "The DFIR Report"
5    published: "29.03.2021"
6    link:
7      - https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/
8  analyzed_by: Vadim Khrykov (@BlackMatter23)
9  threat:
10    name:
11      - REvil
12    aliases:
13      - Sodinokibi
14      - GOLD SOUTHFIELD
15      - G0115
16    attribution:
17      - Worldwide
18    tools:
19      - IceID (Bokbot)
20      - Cobalt Strike
21      - Bloodhound
22  analysis:
23    quote: >
24      - "Initial execution of the document writes a file to... The Excel file called wmic to execute
```

```
25     mitre_attack:
26     execution:
27         - T1204.002 - User Execution - Malicious File
28         - T1047 - Windows Management Instrumentation
29     defense_evasion:
30         - T1218.010 - Signed Binary Proxy Execution - Regsvr32
31     detection:
32         ideas: >
33             - monitor Office applications spawning WMI command-line (WMIC.exe) utility.
34             Note: add more office applications to the rules logic of your choice.
35     telemetry:
36         process_create:
37             - Windows EID 4688
38             - Sysmon EID 1
39             - EDR (PsSetCreateProcessNotifyRoutine/Ex)
40     rules: >
41         - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\wbem\\WMIC.exe" OR ProcessName:"\\wbem\\WMIC.exe"
42           AND CreatorProcessName:"\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
43         - Channel:Sysmon AND EventID:1 AND (Image:"\\wbem\\WMIC.exe" OR CommandLine:"*wmic *" OR ProcessName:"\\wbem\\WMIC.exe"
44           AND ParentImage:"\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
45     ideas: >
46         - monitor WMI "Win32_Process::Create" command execution by Office applications processes.
47         Note: add more office applications to the rule logic of your choice.
48     telemetry:
49         wmi_execution:
50             - EDR (Microsoft-Windows-WMI-Activity ETW)
51     rules: >
52         - Channel:EDR AND EventType:WMIExecution AND Image:"\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe"
53     ideas: >
54         - Excel called wmic to finally proxy execute regsvr32 with the payload. An attacker wanted to execute regsvr32 but we have
55           But we have command-line in the event which allow us to "restore" this suspicious parent-process.
56           Monitor process creation with "wmic process call create" and LOLBins in command-line with "process call create"
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.exe" OR ProcessName:"\\wbem\\WMIC.exe"
65           AND ProcessCommandLine:(*regsvr32* OR *rundll32* OR *msiexec* OR *mshta* OR *verclsid*) AND ParentProcessName:"\\winword.exe"
66           OR "\\excel.exe" OR "\\powerpnt.exe")
67         - Channel:Sysmon AND EventID:1 AND (Image:"\\wbem\\WMIC.exe" OR CommandLine:"*wmic *" OR ProcessName:"\\wbem\\WMIC.exe"
68           AND CommandLine:*process* AND CommandLine:*call* AND CommandLine:*create* AND ParentImage:"\\winword.exe" OR "\\excel.exe"
69           OR "\\powerpnt.exe")
70     ideas: >
71         - monitor LOLBins process creations by Office applications.
```

```

701 Note: add more LOLBins and Office applications to the rules logic of your choice.
702 telemetry:
703     process_create:
704         - Windows EID 4688
705         - Sysmon EID 1
706         - EDR (PsSetCreateProcessNotifyRoutine/Ex)
707 rules: >
708     - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\regsvr32.exe" OR "\\rundll32.exe" OR "\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
709     AND CreatorProcessName:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
710     - Channel:Sysmon AND EventID:1 AND Image:("\\regsvr32.exe" OR "\\rundll32.exe" OR "\\msiexec.exe" OR "\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
711     AND ParentImage:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe")
712 ideas: >
713     - monitor LOLBins process creations with Wmiprvse parent process.
714     Note: add more LOLBins to the rules logic of your choice. FPs are possible here, but some are not.
715 telemetry:
716     process_create:
717         - Windows EID 4688
718         - Sysmon EID 1
719         - EDR (PsSetCreateProcessNotifyRoutine/Ex)
720 rules: >
721     - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\regsvr32.exe" OR "\\rundll32.exe" OR "\\wbem\\WmiPrvSE.exe")
722     AND CreatorProcessName:("\\wbem\\WmiPrvSE.exe")
723     - Channel:Sysmon AND EventID:1 AND Image:("\\regsvr32.exe" OR "\\rundll32.exe" OR "\\msiexec.exe" OR "\\wbem\\WmiPrvSE.exe")
724     AND ParentImage:("\\wbem\\WmiPrvSE.exe")
725 ideas: >
726     - monitor executable and script files creation by Office applications, use files extensions
727     Note: add more files extensions/magic bytes to the rules logic of your choice.
728 telemetry:
729     file_create:
730         - Sysmon EID 11
731         - EDR (minifilter)
732     file_rename:
733         - EDR (minifilter)
734 rules: >
735     - Channel:Sysmon AND EventID:11 AND Image:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe" OR "\\msiexec.exe" OR "\\cmd.exe" OR "\\powershell.exe")
736     AND TargetFilename: (*.exe OR *.dll OR *.ocx OR *.com OR *.ps1 OR *.vbs OR *.sys OR *.bat OR *.cmd OR *.psm1 OR *.psd1 OR *.psd2 OR *.psd3 OR *.psd4 OR *.psd5 OR *.psd6 OR *.psd7 OR *.psd8 OR *.psd9 OR *.psd10 OR *.psd11 OR *.psd12 OR *.psd13 OR *.psd14 OR *.psd15 OR *.psd16 OR *.psd17 OR *.psd18 OR *.psd19 OR *.psd20 OR *.psd21 OR *.psd22 OR *.psd23 OR *.psd24 OR *.psd25 OR *.psd26 OR *.psd27 OR *.psd28 OR *.psd29 OR *.psd30 OR *.psd31 OR *.psd32 OR *.psd33 OR *.psd34 OR *.psd35 OR *.psd36 OR *.psd37 OR *.psd38 OR *.psd39 OR *.psd40 OR *.psd41 OR *.psd42 OR *.psd43 OR *.psd44 OR *.psd45 OR *.psd46 OR *.psd47 OR *.psd48 OR *.psd49 OR *.psd50 OR *.psd51 OR *.psd52 OR *.psd53 OR *.psd54 OR *.psd55 OR *.psd56 OR *.psd57 OR *.psd58 OR *.psd59 OR *.psd60 OR *.psd61 OR *.psd62 OR *.psd63 OR *.psd64 OR *.psd65 OR *.psd66 OR *.psd67 OR *.psd68 OR *.psd69 OR *.psd70 OR *.psd71 OR *.psd72 OR *.psd73 OR *.psd74 OR *.psd75 OR *.psd76 OR *.psd77 OR *.psd78 OR *.psd79 OR *.psd80 OR *.psd81 OR *.psd82 OR *.psd83 OR *.psd84 OR *.psd85 OR *.psd86 OR *.psd87 OR *.psd88 OR *.psd89 OR *.psd90 OR *.psd91 OR *.psd92 OR *.psd93 OR *.psd94 OR *.psd95 OR *.psd96 OR *.psd97 OR *.psd98 OR *.psd99 OR *.psd100)
737     - Channel:EDR AND EventType:(FileCreate OR FileRename) AND Image:("\\winword.exe" OR "\\excel.exe" OR "\\powerpnt.exe" OR "\\msiexec.exe" OR "\\cmd.exe" OR "\\powershell.exe")
738     AND (Filename: (*.exe OR *.dll OR *.ocx OR *.com OR *.ps1 OR *.vbs OR *.sys OR *.bat OR *.cmd OR *.psm1 OR *.psd1 OR *.psd2 OR *.psd3 OR *.psd4 OR *.psd5 OR *.psd6 OR *.psd7 OR *.psd8 OR *.psd9 OR *.psd10 OR *.psd11 OR *.psd12 OR *.psd13 OR *.psd14 OR *.psd15 OR *.psd16 OR *.psd17 OR *.psd18 OR *.psd19 OR *.psd20 OR *.psd21 OR *.psd22 OR *.psd23 OR *.psd24 OR *.psd25 OR *.psd26 OR *.psd27 OR *.psd28 OR *.psd29 OR *.psd30 OR *.psd31 OR *.psd32 OR *.psd33 OR *.psd34 OR *.psd35 OR *.psd36 OR *.psd37 OR *.psd38 OR *.psd39 OR *.psd40 OR *.psd41 OR *.psd42 OR *.psd43 OR *.psd44 OR *.psd45 OR *.psd46 OR *.psd47 OR *.psd48 OR *.psd49 OR *.psd50 OR *.psd51 OR *.psd52 OR *.psd53 OR *.psd54 OR *.psd55 OR *.psd56 OR *.psd57 OR *.psd58 OR *.psd59 OR *.psd60 OR *.psd61 OR *.psd62 OR *.psd63 OR *.psd64 OR *.psd65 OR *.psd66 OR *.psd67 OR *.psd68 OR *.psd69 OR *.psd70 OR *.psd71 OR *.psd72 OR *.psd73 OR *.psd74 OR *.psd75 OR *.psd76 OR *.psd77 OR *.psd78 OR *.psd79 OR *.psd80 OR *.psd81 OR *.psd82 OR *.psd83 OR *.psd84 OR *.psd85 OR *.psd86 OR *.psd87 OR *.psd88 OR *.psd89 OR *.psd90 OR *.psd91 OR *.psd92 OR *.psd93 OR *.psd94 OR *.psd95 OR *.psd96 OR *.psd97 OR *.psd98 OR *.psd99 OR *.psd100)
739 quote: >
740     - "This (MS Excel) then made a network request to download a file from this URL"
741 mitre_attack:
742     defense_evasion:
743         - T1218.010 - Signed Binary Proxy Execution - Regsvr32
744 detection:
745     ideas: >
746         - MS Excel process initiated an external network connection if we try to monitor such activity

```

```
116         if EXCEL process initiated an external network connection, if we try to monitor such connections
117         instead monitor outbound network connections initiated by Regsvr32.exe (not directly related to EXCEL)
118         Note: you may also check hypothesis for local-to-local connections and add other LOLBins
```



```

579         - EDR (minifilter)
580     file_rename:
581         - EDR (minifilter)
582     file_delete:
583         - EDR (minifilter)
584 rules: >
585     - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\rclone.exe" OR ProcessCo
586     - Channel:Sysmon AND EventID:1 AND (OriginalFileName:"rclone.exe" OR Company:""*rclone\org
587     - Channel:EDR AND EventType:(FileCreate OR FileRename OR FileDelete) AND (OriginalFileName:
588         AND NOT FilePath:"\\rclone.exe"
589 ideas: >
590     - monitor Rclone tool execution with suspicious command-lines.
591 telemetry:
592     process_create:
593         - Windows EID 4688
594         - Sysmon EID 1
595         - EDR (PsSetCreateProcessNotifyRoutine/Ex)
596 rules: >
597     - Channel:Windows-Security AND EventID:4688 AND (NewProcessName:"\\rclone.exe" OR ProcessCo
598         AND ProcessCommandLine.keyword:/.*\*\*\.*\\(ADMIN|IPC|C)\$.*/ AND ProcessCommandLine:(*htt
599     - Channel:Sysmon AND EventID:1 AND (Image:"\\rclone.exe" OR CommandLine:"*rclone *" OR Orig
600         AND CommandLine.keyword:/.*\*\*\.*\\(ADMIN|IPC|C)\$.*/ AND CommandLine:(*http* OR *ftp*)
601 ideas: >
602     - monitor system processes execution from untypical paths. Add more executables of your cho
603 telemetry:
604     process_create:
605         - Windows EID 4688
606         - Sysmon EID 1
607         - EDR (PsSetCreateProcessNotifyRoutine/Ex)
608 rules: >
609     - Channel:Windows-Security AND EventID:4688 AND NewProcessName:("\\svchost.exe" OR "\\gpupc
610         AND NOT NewProcessName:("C:\\Windows\\System32\\" OR "C:\\Windows\\SysWOW64\\")
611     - Channel:Sysmon AND EventID:1 AND Image:("\\svchost.exe" OR "\\gpupdate.exe" OR "\\taskhos
612         AND NOT Image:("C:\\Windows\\System32\\" OR "C:\\Windows\\SysWOW64\\")
613 quote: >
614     - "For the final actions, the threat actors dropped a ransomware executable on the domain contr
615 detection:
616     - https://github.com/vadim-hunter/Detection-Ideas-Rules/blob/main/TTPs/Defense%20Evasion/T1197%20Evil-Winlogon%20Abuse%20for%20Ransomware%20Deployment
617 quote: >
618     - "The -smode flag was used with the ransomware executable to set the system to reboot into Saf
619     - "bootcfg /raw /a /safeboot:network /id 1 (pre-Vista)"
620     - "bootcfg /raw /a /safeboot:network /id 1 (pre-Vista)"

```

