






Sign in


 SigmaHQ / sigma Public


 Notifications


 Fork 2.2k


 Star 8.3k


 Code


 Issues 11


 Pull requests 35

 Discussions

 Actions

 Wiki

 Security

 In progress

ScreenConnect rules #4467

New issue


Merged


nasbench merged 11 commits into SigmaHQ:master from alwashali:ScreenConnect\_Rules on Oct 5, 2023

 Conversation 24

 Commits 11

 Checks 10

 Files changed

 alwashali commented on Oct 1, 2023 • edited by nasbench Contributor

### Summary of the Pull Request

Rules to detect ScreenConnect RMM tools activity

### Changelog


new: Remote Access Tool - ScreenConnect Command Execution  
new: Remote Access Tool - ScreenConnect File Transfer  
new: Remote Access Tool - ScreenConnect Temporary File  
new: Remote Access Tool - ScreenConnect Remote Command Execution


### Example Log Event

- Process Creation


```
Process Create:  
RuleName: -  
UtcTime: 2023-10-01 09:47:05.429  
ProcessGuid: {43199d79-4019-6519-cd21-000000001400}  
ProcessId: 11456  
Image: C:\Windows\System32\whoami.exe  
FileVersion: 10.0.17763.1 (WinBuild.160101.0800)
```

#### Reviewers

 nasbench ✓

 phantinuss ✓

#### Assignees

 nasbench

#### Labels

Rules Windows

#### Projects

None yet

#### Milestone

No milestone

#### Development

Successfully merging this pull request may close these issues.

```
Description: whoami - displays logged on user information
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: whoami.exe
CommandLine: whoami
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {43199d79-f8e8-6507-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=47D7864D26FC67E0D60391CBF170D33DA518C322,MD
ParentProcessGuid: {43199d79-4019-6519-cc21-000000001400}
ParentProcessId: 1588
ParentImage: C:\Windows\System32\cmd.exe
ParentCommandLine: "cmd.exe" /c "C:\Windows\TEMP\ScreenC
ParentUser: NT AUTHORITY\SYSTEM
```

4 participants



#### Process Create:



```
RuleName: -
UtcTime: 2023-10-01 09:47:05.375
ProcessGuid: {43199d79-4019-6519-cc21-000000001400}
ProcessId: 1588
Image: C:\Windows\System32\cmd.exe
FileVersion: 10.0.17763.1697 (WinBuild.160101.0800)
Description: Windows Command Processor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: Cmd.Exe
CommandLine: "cmd.exe" /c "C:\Windows\TEMP\ScreenConnect
CurrentDirectory: C:\Windows\system32\
User: NT AUTHORITY\SYSTEM
LogonGuid: {43199d79-f8e8-6507-e703-000000000000}
LogonId: 0x3E7
TerminalSessionId: 0
IntegrityLevel: System
Hashes: SHA1=DED8FD7F36417F66EB6ADA10E0C0D7C0022986E9,MD
ParentProcessGuid: {43199d79-3eb3-6519-5821-000000001400}
ParentProcessId: 2868
ParentImage: C:\Program Files (x86)\ScreenConnect Client
ParentCommandLine: "C:\Program Files (x86)\ScreenConnect
ParentUser: NT AUTHORITY\SYSTEM
```

#### • File Create

#### File created:

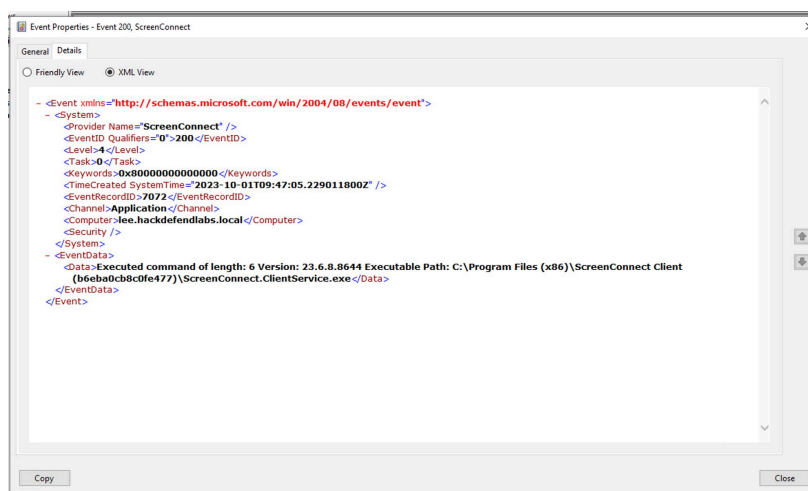


```
RuleName: -
UtcTime: 2023-10-01 09:59:00.206
ProcessGuid: {43199d79-3eb4-6519-5921-000000001400}
```

```
ProcessId: 7684
Image: C:\Program Files (x86)\ScreenConnect Client (b6eb
TargetFilename: C:\Users\sam\Documents\ConnectWiseContro
CreationUtcTime: 2023-10-01 09:59:00.206
User: HACKDEFENDLABS\sam

Process Create:
RuleName: -
UtcTime: 2023-10-01 09:59:00.635
ProcessGuid: {43199d79-42e4-6519-f721-000000001400}
ProcessId: 8588
Image: C:\Users\sam\Documents\ConnectWiseControl\Temp\Ms
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: "C:\Users\sam\Documents\ConnectWiseControl\
CurrentDirectory: C:\Users\sam\Documents\ConnectWiseCont
User: HACKDEFENDLABS\sam
LogonGuid: {43199d79-fa62-6507-a9d7-270000000000}
LogonId: 0x27D7A9
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA1=BFCFCE9CEBB56C9850171DFF03B73588D0B07FB8,MD
ParentProcessGuid: {43199d79-42e4-6519-f621-000000001400
ParentProcessId: 9868
ParentImage: C:\Program Files (x86)\ScreenConnect Client
ParentCommandLine: "C:\Program Files (x86)\ScreenConnect
ParentUser: HACKDEFENDLABS\sam
```

- EID 200



- EID 201

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
  <Provider Name="ScreenConnect" />
  <EventID Qualifiers="0">201</EventID>
  <Level>4</Level>
  <Task>0</Task>
  <Keywords>0x8000000000000000</Keywords>
  <TimeCreated SystemTime="2023-10-01T10:03:37.5508280Z" />
  <EventRecordID>7083</EventRecordID>
  <Channel>Application</Channel>
  <Computer>lee.hackdefendlabs.local</Computer>
  <Security />
</System>
- <EventData>
  <Data>Transferred files with action 'RunSilentElevated': ScreenConnect.ClientUninstall.vbs Version:
23.6.8.8644 Executable Path: C:\Program Files (x86)\ScreenConnect Client (b6eba0cb8c0fe477)
\ScreensConnect.ClientService.exe</Data>
</EventData>
</Event>
```



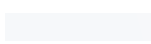


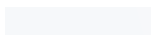


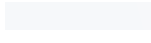
## Fixed Issues

N/A

## SigmaHQ Rule Creation Conventions

- If your PR adds new rules, please consider following and applying these [conventions](#)

 alwashali added 3 commits [last year](#)

-   Screenconnect: provider applicaiton ...  dae550d
-   ScreenConnect remote command execution ...  04a928d
-   ScreenConnect remote binary execution ...  3f44b93



frack113 commented on Oct 2, 2023

Member



Hi,

I have make a quick view.

You can use

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/application/esent/win\\_esent\\_ntdsutil\\_abuse.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/application/esent/win_esent_ntdsutil_abuse.yml) as model to upgrade your 2 "application" rules.


You have to fix the `logsource` and the selection (you write an OR list).

Mitre tags are lowercase.



1



 **frack113** added **Rules** **Work In Progress** **Windows** labels  
on Oct 2, 2023



**alwashali** added 4 commits last year



 Update  **b0cad0d**  
win\_app\_remote\_binary\_execution.yaml  
...



 Update  **57c6dac**  
win\_app\_remote\_command\_execution.yaml  
...



 Update  **993876b**  
file\_event\_win\_screenconnect\_remote\_tool\_execution.yaml



 Update  **94de111**  
proc\_creation\_win\_screenconnect\_remote\_command\_execution.yaml



**alwashali** commented on Oct 2, 2023 **Contributor** **Author** ...

Hello frack113

Thank you for checking the rules  
I have made the changes, can you check please



 chore: update positions  **06fccc2**



**nasbench** requested changes **View reviewed changes**  
on Oct 2, 2023

**nasbench** left a comment

**Member** ...

Hi [@alwashali](#) thanks for the contribution. Just have a couple of questions before we can merge these if you may :)

rules/windows/file/file\_event/file\_event\_win\_screenconnect\_remote\_tool\_execution.yaml

Outdated

Show resolved

rules/windows/process\_creation/proc\_creation\_win\_screenconnect\_remote\_command\_execution.yaml

Outdated

Show resolved

rules/windows/process\_creation/proc\_creation\_win\_screenconnect\_remote\_command\_execution.yaml

Outdated

Show resolved

rules/windows/builtin/application/screenconnect/win\_app\_remote\_command\_execution.yaml

Outdated

Show resolved

rules/windows/builtin/application/screenconnect/win\_app\_remote\_binary\_execution.yaml

Outdated

Show resolved



**nasbench** self-assigned this on Oct 2, 2023



**alwashali** requested a review from **nasbench** last year



**nasbench** commented on Oct 4, 2023

Member



**@alwashali** for the rules using the application logs. Can you post the log or screenshot of the details view. The General view has text that is often generated and not part of the log itself.





**nasbench** added 2 commits [last year](#)





chore: rename

6f217c0

  chore: update metadata 4eb16ab


  **nasbench** added **2nd Review Needed** and removed **Work In Progress** labels on Oct 4, 2023

  **nasbench** requested a review from **phantinuss** last year

  **nasbench** approved these changes [View reviewed changes](#)  
on Oct 4, 2023


  **alwashali** commented on Oct 4, 2023 [View reviewed changes](#)

```
...ultin/application/screenconnect/win_app_remote_access_tools_screenconnect_file_transfer.yml
```

 [Show resolved](#)


  **phantinuss** reviewed on Oct 5, 2023 [View reviewed changes](#)

```
...ultin/application/screenconnect/win_app_remote_access_tools_screenconnect_file_transfer.yml
```

**Outdated**  [Show resolved](#)

  **phantinuss** reviewed on Oct 5, 2023 [View reviewed changes](#)

```
...ultin/application/screenconnect/win_app_remote_access_tools_screenconnect_file_transfer.yml
```

**Outdated**  [Show resolved](#)

  **phantinuss** reviewed on Oct 5, 2023 [View reviewed changes](#)

```
...windows/process_creation/proc_creation_win_remote_access_tools_screenconnect_remote_exec.yml
```

Outdated

Show resolved



phantinuss reviewed on Oct 5, 2023

[View reviewed changes](#)

```
rules/windows/file/file_event/file_event_win_remote_access_tools_screenconnect_remote_file.yml
```

Outdated

Show resolved



phantinuss reviewed on Oct 5, 2023

[View reviewed changes](#)

```
...uiltin/application/screenconnect/win_app_remote_access_tools_screenconnect_file_transfer.yml
```

Outdated

Show resolved



phantinuss reviewed on Oct 5, 2023

[View reviewed changes](#)

```
...builtin/application/screenconnect/win_app_remote_access_tools_screenconnect_command_exec.yml
```

Outdated

Show resolved



fix: wording

b47e515



phantinuss approved these changes on Oct 5, 2023

[View reviewed changes](#)



nasbench removed the **2nd Review Needed** label on Oct 5, 2023





**nasbench** merged commit **6075db0** into

**SigmaHQ:master** on Oct 5, 2023

10 checks passed

[View details](#)

**Sign up for free**

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact](#)

[Manage cookies](#)

[Do not share my personal information](#)



© 2024 GitHub, Inc.