

Sign in


OTRF / detection-hackathon-apt29 Public Notifications Fork 41 Star 132

<> Code Issues 49 Pull requests Actions Projects Security Insights

7.A) Screen Capture, Clipboard Data, Input Capture #16

New issue


Open Cyb3rWard0g opened this issue on May 2, 2020 · 6 comments



Cyb3rWard0g commented on May 2, 2020 Contributor ...

Description

The attacker collects screenshots (T1113), data from the user's clipboard (T1115), and keystrokes (T1056).



Cyb3rWard0g commented on May 11, 2020 Contributor Author ...

7.A.1 Screen Capture

Detection Category (Telemetry)

Procedure: Captured and saved screenshots using PowerShell
Criteria: powershell.exe executing the CopyFromScreen function from System.Drawing.dll

```
systemdrawingdll = spark.sql(  
    ...  
    SELECT Image, OriginalFileName
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant



```
FROM apt29Table
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
AND EventID = 7 AND LOWER(ImageLoaded) LIKE "%drawing%"
      ''')
systemdrawingdll.show(100,truncate = False, vertical = F
```



Cyb3rWard0g commented
on May 11, 2020

Contributor

Author



From PS Logs

```
systemdrawingdll = spark.sql(
    ''')
SELECT EventID
FROM apt29Table
WHERE Channel != "Microsoft-Windows-Sysmon/Operational"
AND LOWER(Message) LIKE "%copyfromscreen%"
      ''')
systemdrawingdll.show(100,truncate = False, vertical = F
```



Cyb3rWard0g commented
on May 14, 2020

Contributor

Author



Telemetry showed powershell.exe executing CopyFromScreen from System.Drawing.dll. The event was correlated to a parent alert for Bypass User Account Control of control.exe spawning powershell.exe.

Sysmon

```
SELECT Payload
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessId, d.ParentProcessId
    FROM apt29Host d
    INNER JOIN (
        SELECT a.ProcessGuid, a.ParentProcessGuid
        FROM apt29Host a
        INNER JOIN (
            SELECT ProcessGuid
            FROM apt29Host
```



```
WHERE Channel = "Microsoft-Windows-Sysmon/Operat
AND EventID = 1
AND LOWER(Image) LIKE "%control.exe"
AND LOWER(ParentImage) LIKE "%sdclt.exe"
) b
ON a.ParentProcessGuid = b.ProcessGuid
WHERE a.Channel = "Microsoft-Windows-Sysmon/Operat
AND a.EventID = 1
AND a.IntegrityLevel = "High"
) c
ON d.ParentProcessGuid= c.ProcessGuid
WHERE d.Channel = "Microsoft-Windows-Sysmon/Operatic
AND d.EventID = 1
AND d.Image LIKE '%powershell.exe'
) e
ON f.ExecutionProcessID = e.ProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatic
AND f.EventID = 4103
AND LOWER(f.Payload) LIKE "%copyfromscreen%"
```

Results

```
CommandInvocation(Start-Job): "Start-Job"
ParameterBinding(Start-Job): name="Name"; value="Screen
ParameterBinding(Start-Job): name="ScriptBlock"; value="
Write-Host "`nJobPID`n-----`n$PID"
while($true){
    $RandomFileName = [System.IO.Path]::GetRandom
    $Filepath="$env:USERPROFILE\Downloads\$Random
    Add-Type -AssemblyName System.Windows.Forms;
    Add-type -AssemblyName System.Drawing;
    $Screen = [System.Windows.Forms.SystemInform
    $Width = $Screen.Width;
    $Height = $Screen.Height;
    $Left = $Screen.Left;
    $Top = $Screen.Top;
    $bitmap = New-Object System.Drawing.Bitmap $
    $graphic = [System.Drawing.Graphics]::FromIm
    $graphic.CopyFromScreen($Left, $Top, 0, 0, $
    $bitmap.Save($Filepath);
    Start-Sleep -Seconds
```



Cyb3rWard0g commented
on May 14, 2020

Contributor

Author

...

Security Logs + PowerShell Logs

```
SELECT Payload
FROM apt29Host f
INNER JOIN (
    SELECT split(d.NewProcessId, '0x')[1] as NewProcessId
    FROM apt29Host d
    INNER JOIN(
        SELECT a.ProcessId, a.NewProcessId
        FROM apt29Host a
        INNER JOIN (
            SELECT NewProcessId
            FROM apt29Host
            WHERE LOWER(Channel) = "security"
            AND EventID = 4688
            AND LOWER(NewProcessName) LIKE "%control.exe"
            AND LOWER(ParentProcessName) LIKE "%sdclt.ex"
        ) b
        ON a.ProcessId = b.NewProcessId
        WHERE LOWER(a.Channel) = "security"
        AND a.EventID = 4688
        AND a.MandatoryLabel = "S-1-16-12288"
        AND a.TokenElevationType = "%1937"
    ) c
    ON d.ProcessId = c.NewProcessId
    WHERE LOWER(d.Channel) = "security"
    AND d.EventID = 4688
    AND d.NewProcessName LIKE '%powershell.exe'
) e
ON LOWER(hex(f.ExecutionProcessID)) = e.NewProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatic
AND f.EventID = 4103
AND LOWER(f.Payload) LIKE "%copyfromscreen%"
```



Cyb3rWard0g commented

on May 14, 2020

Contributor

Author



7.A.2 Clipboard Data

Procedure: Captured clipboard contents using PowerShell

Criteria: powershell.exe executing Get-Clipboard

Sysmon + PowerShell Logs

```
SELECT Message
FROM apt29Host f
```



```
INNER JOIN (
  SELECT d.ProcessId, d.ParentProcessId
  FROM apt29Host d
  INNER JOIN (
    SELECT a.ProcessGuid, a.ParentProcessGuid
    FROM apt29Host a
    INNER JOIN (
      SELECT ProcessGuid
      FROM apt29Host
      WHERE Channel = "Microsoft-Windows-Sysmon/Operat
        AND EventID = 1
        AND LOWER(Image) LIKE "%control.exe"
        AND LOWER(ParentImage) LIKE "%sdclt.exe"
    ) b
    ON a.ParentProcessGuid = b.ProcessGuid
    WHERE a.Channel = "Microsoft-Windows-Sysmon/Operat
      AND a.EventID = 1
      AND a.IntegrityLevel = "High"
    ) c
    ON d.ParentProcessGuid= c.ProcessGuid
    WHERE d.Channel = "Microsoft-Windows-Sysmon/Operatio
      AND d.EventID = 1
      AND d.Image LIKE '%powershell.exe'
    ) e
    ON f.ExecutionProcessID = e.ProcessId
    WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatio
      AND f.EventID = 4103
      AND LOWER(f.Payload) LIKE "%get-clipboard%"
```

Results

CommandInvocation(Get-Clipboard): "Get-Clipboard" 

Context:

```
Severity = Informational
Host Name = ConsoleHost
Host Version = 5.1.18362.628
Host ID = b802b425-c255-486e-81a2-6d10f7563af8
Host Application = powershell.exe
Engine Version = 5.1.18362.628
Runspace ID = f703f141-62e0-4a88-967c-42505edb0c
Pipeline ID = 21
Command Name = Get-Clipboard
Command Type = Cmdlet
Script Name =
Command Path =
Sequence Number = 62
User = DMEVALS\pbeesly
Connected User =
Shell ID = Microsoft.PowerShell
```

Security + PowerShell Logs

```
SELECT Message
FROM apt29Host f
INNER JOIN (
  SELECT split(d.NewProcessId, '0x')[1] as NewProcessId
  FROM apt29Host d
  INNER JOIN(
    SELECT a.ProcessId, a.NewProcessId
    FROM apt29Host a
    INNER JOIN (
      SELECT NewProcessId
      FROM apt29Host
      WHERE LOWER(Channel) = "security"
        AND EventID = 4688
        AND LOWER(NewProcessName) LIKE "%control.exe"
        AND LOWER(ParentProcessName) LIKE "%sdclt.exe"
    ) b
    ON a.ProcessId = b.NewProcessId
    WHERE LOWER(a.Channel) = "security"
      AND a.EventID = 4688
      AND a.MandatoryLabel = "S-1-16-12288"
      AND a.TokenElevationType = "%%1937"
    ) c
    ON d.ProcessId = c.NewProcessId
    WHERE LOWER(d.Channel) = "security"
      AND d.EventID = 4688
      AND d.NewProcessName LIKE '%powershell.exe'
    ) e
  ON LOWER(hex(f.ExecutionProcessID)) = e.NewProcessId
  WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatic
  AND f.EventID = 4103
  AND LOWER(f.Payload) LIKE "%get-clipboard%"
```

Results

```
CommandInvocation(Get-Clipboard): "Get-Clipboard"
Context:
  Severity = Informational
  Host Name = ConsoleHost
  Host Version = 5.1.18362.628
  Host ID = b802b425-c255-486e-81a2-6d10f7563af8
  Host Application = powershell.exe
  Engine Version = 5.1.18362.628
  Runspace ID = f703f141-62e0-4a88-967c-42505edb0c
  Pipeline ID = 21
  Command Name = Get-Clipboard
  Command Type = Cmdlet
  Script Name =
  Command Path =
```

```
Sequence Number = 62
User = DMEVALS\pbeesly
Connected User =
Shell ID = Microsoft.PowerShell
```



Cyb3rWard0g commented
on May 14, 2020

Contributor

Author

...

7.A.3 Input Capture

Procedure: Captured user keystrokes using the GetAsyncKeyState API

Criteria: powershell.exe executing the GetAsyncKeyState API

[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.