Fiji – Suspicious Activities Report July 2021

Contents

Findings 3

Actions taken by Trustwave.. 5

Analysis.. 5

Persistence.. 5

Carbon Black Process Analysis 6

Affected hosts 10

Findings

As more Carbon Black agents were progressively deployed within Fiji environment, further malicious activities have been detected by Carbon Black on 72 Windows machines (as of 19th of July 2021).

Several internal Windows devices were found to connect to the following public IP addresses:

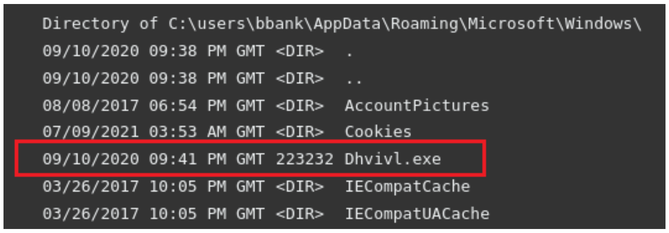
- 146.112.61.105 - api1.wipmania.com.wipmsc[.]ru
- 212.83.168.196 - api.wipmania[.]com
- 208.100.26.242 - s.yfsamwekj[.]com
- 35.205.61.67 - s.mebtmnicu[.]com

Malicious activities were attributed to a binary file that was found using different names in the following locations:

- c:\users\{username}\appdata\roaming\microsoft\windows\{6_random_characters}.exe
- c:\users\{username}\appdata\roaming\c731200

The malware is related to the Dorkbot malware family which was first discovered in 2015. It is an IRC botnet malware with various capabilities including backdoor and password stealing.

Artefacts collected on infected machines indicate that the malware has been present in the environment as far as 10 September 2020.

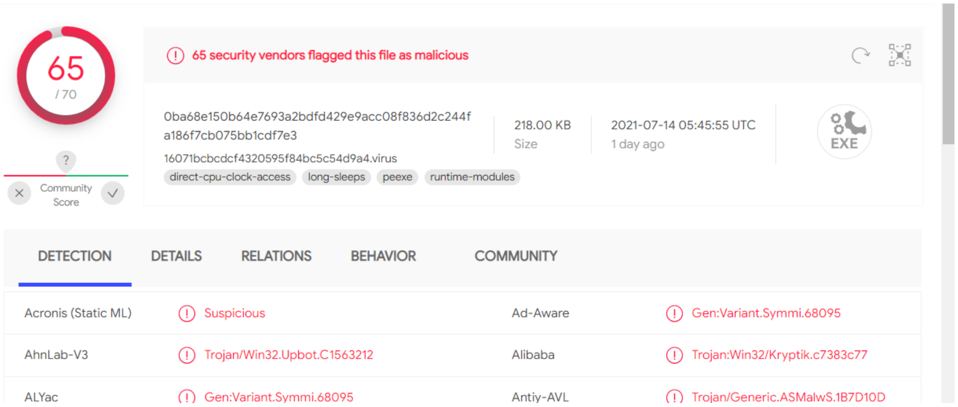


```
Directory of C:\users\bbank\AppData\Roaming\Microsoft\Windows\
09/10/2020 09:38 PM GMT <DIR>  .
09/10/2020 09:38 PM GMT <DIR>  ..
08/08/2017 06:54 PM GMT <DIR>  AccountPictures
07/09/2021 03:53 AM GMT <DIR>  Cookies
09/10/2020 09:41 PM GMT 223232 Dhvivl.exe
03/26/2017 10:05 PM GMT <DIR>  IECompatCache
03/26/2017 10:05 PM GMT <DIR>  IECompatUACache
```

Not all affected hosts have been analysed thus it is possible that the malware was present in the environment earlier than the date indicated in this finding.

File details and Indicators of Compromise (IOC):

- MD5 hash: 16071bcbcdcf4320595f84bc5c54d9a4
- SHA1: 94c2bef0ecb7416f259cfed9cd4d634efc17707b
- SHA256: 0ba68e150b64e7693a2bdfd429e9acc08f836d2c244fa186f7cb075bb1cdf7e3
- Size: 223,232 bytes
- Type: PE32
- VirusTotal analysis: https://www.virustotal.com/gui/file/0ba68e150b64e7693a2bdfd429e9acc08f836d2c244fa186f7cb075bb1cdf7e3/detection



65 security vendors flagged this file as malicious

0ba68e150b64e7693a2bdfd429e9acc08f836d2c244fa186f7cb075bb1cdf7e3
16071bcbcdcf4320595f84bc5c54d9a4.virus
direct-cpu-clock-access long-sleeps peexe runtime-modules

218.00 KB
Size

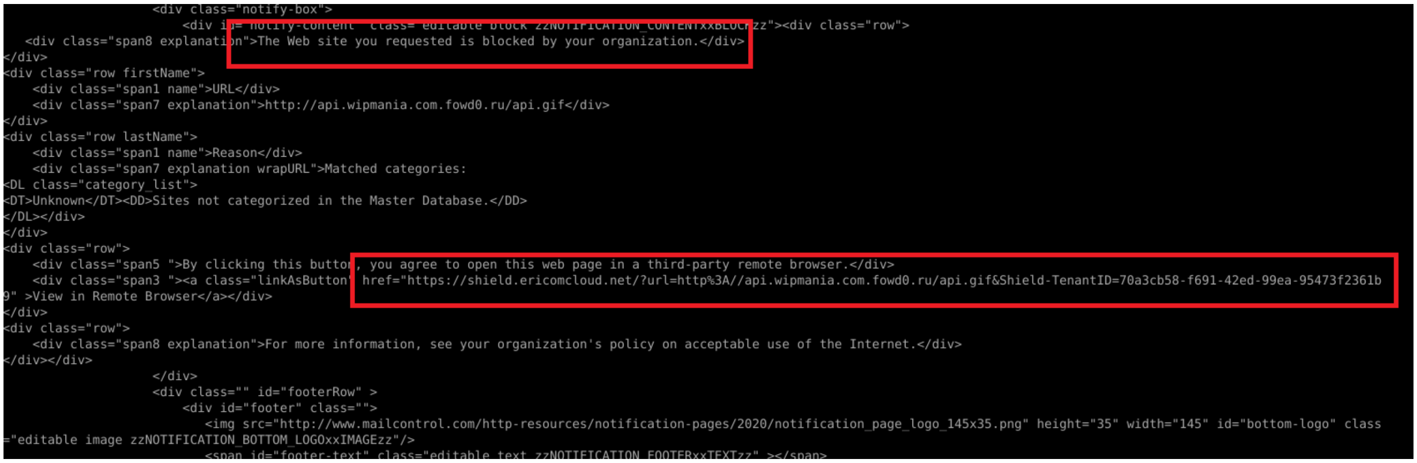
2021-07-14 05:45:55 UTC
1 day ago

Acronis (Static ML)	Suspicious	Ad-Aware	Gen:Variant.Symmi.68095
AhnLab-V3	Trojan/Win32.Upbot.C1563212	Alibaba	Trojan:Win32/Kryptik.c7383c77
ALYac	Gen:Variant.Symmi.68095	Antiy-AVL	Trojan/Generic.ASMalwS.1B7D10D

Actions taken by Trustwave

- Requested network communications with identified C2 IP addresses to be blocked at firewall/proxy level.
- Added SHA256 hash of the malicious file to CB banned list.
- Acquisition of artefacts from various hosts for analysis by Trustwave DFIR.
- Recommended affected hosts to be re-imaged.
- Recommended to review anti-virus status on all systems and to ensure it is up-to-date and running.

Evidence found on affected hosts that the malware cannot communicate with the C2 server since traffic is blocked by the ForcePoint proxy, as indicated by a file recovered from an infected machine:



```
                    <div class="notify-box">
                        <div id="notify-content" class="editable block zzNOTIFICATION_CONTENTxxBLOCKzz"><div class="row">
   <div class="span8 explanation">The Web site you requested is blocked by your organization.</div>
</div>
<div class="row firstName">
    <div class="span1 name">URL</div>
    <div class="span7 explanation">http://api.wipmania.com.fowd0.ru/api.gif</div>
</div>
<div class="row lastName">
    <div class="span1 name">Reason</div>
    <div class="span7 explanation wrapURL">Matched categories:
<DL class="category_list">
<DT>Unknown</DT><DD>Sites not categorized in the Master Database.</DD>
</DL></div>
</div>
<div class="row">
    <div class="span5 ">By clicking this button, you agree to open this web page in a third-party remote browser.</div>
    <div class="span3 "><a class="linkAsButton" href="https://shield.ericomcloud.net/?url=http%3A//api.wipmania.com.fowd0.ru/api.gif&Shield-TenantID=70a3cb58-f691-42ed-99ea-95473f2361b
9" >View in Remote Browser</a></div>
</div>
<div class="row">
    <div class="span8 explanation">For more information, see your organization's policy on acceptable use of the Internet.</div>
</div></div>
                    </div>
                    <div class="" id="footerRow" >
                        <div id="footer" class="">
                           <img src="http://www.mailcontrol.com/http-resources/notification-pages/2020/notification_page_logo_145x35.png" height="35" width="145" id="bottom-logo" class
="editable image zzNOTIFICATION_BOTTOM_LOGOxxIMAGEzz"/>
                           <span id="footer-text" class="editable text zzNOTIFICATION_FOOTERxxTEXTzz" ></span>
```

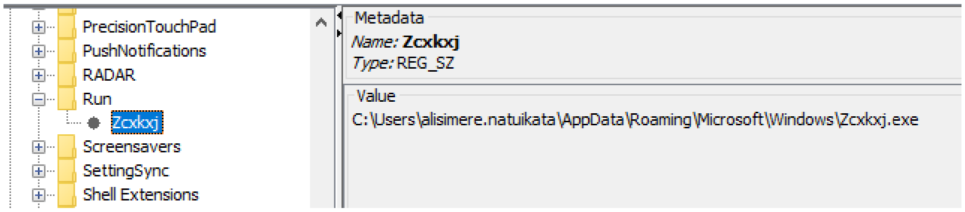
Analysis

Persistence

The malware maintains persistence through the use of the "Run" key located in the user's NTUSER.DAT registry:

- Registry: c:\users\{username}\NTUSER.DAT
- Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Run
- Value: c:\users\{username}\appdata\roaming\microsoft\windows\{6_alphabetic_char}.exe

Example of the "Run" key value:



Metadata
Name: **Zcxkxj**
Type: REG_SZ

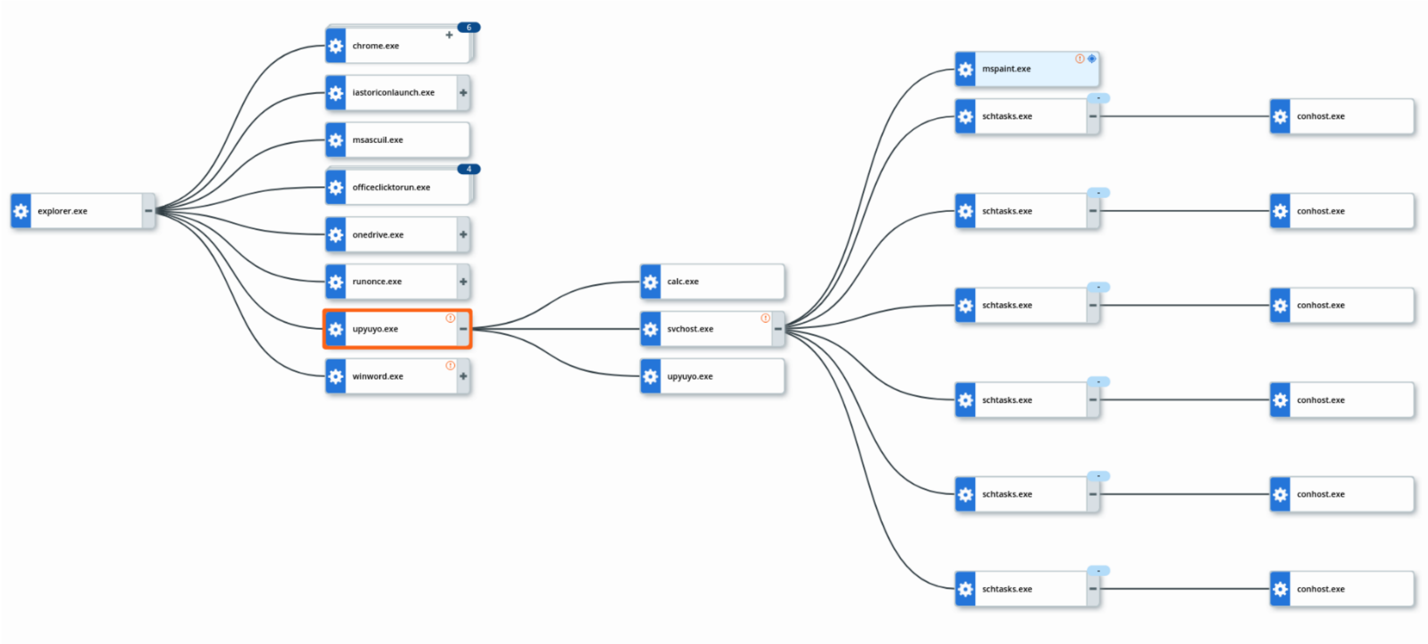
Value
C:\Users\alisimere.natuikata\AppData\Roaming\Microsoft\Windows\Zcxkxj.exe

When the user logs in to the machine, the value of the Run key is read and executed, launching the malicious file.

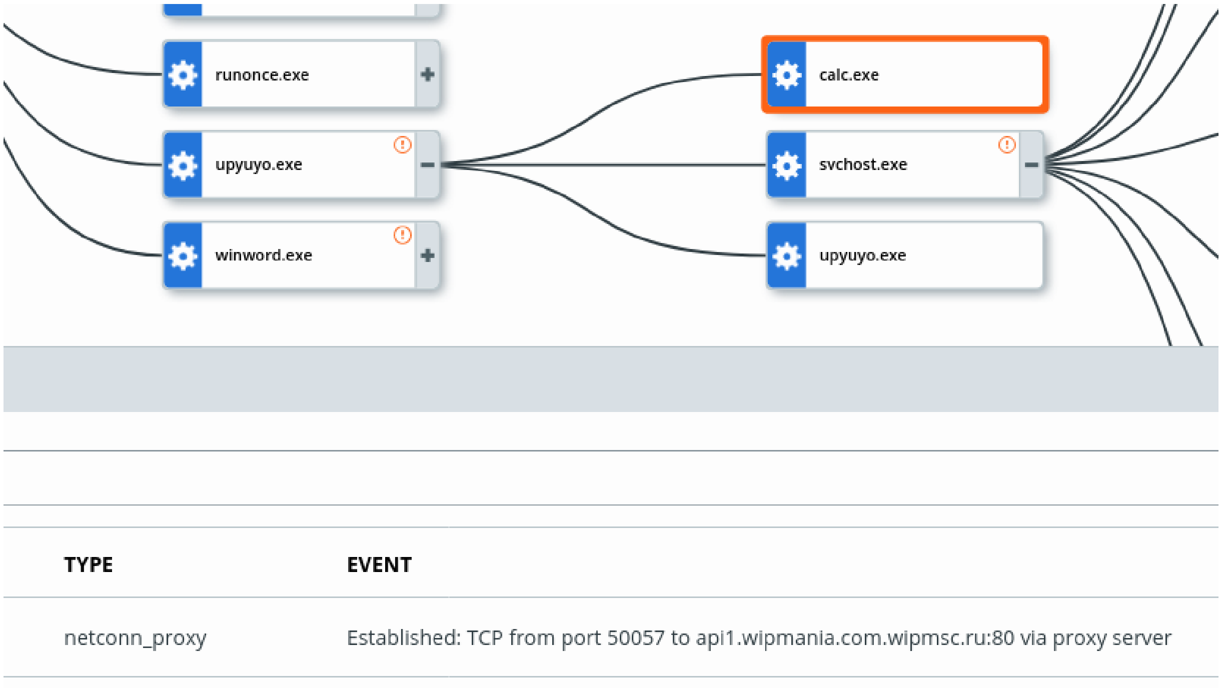
Carbon Black Process Analysis

Process analysis of the malicious file was conducted using Carbon Back to identify and visualise parent and child processes, and to determine system operations and network activities performed by the malware.

1. Global view of malicious file “upyuyo.exe” execution tree:

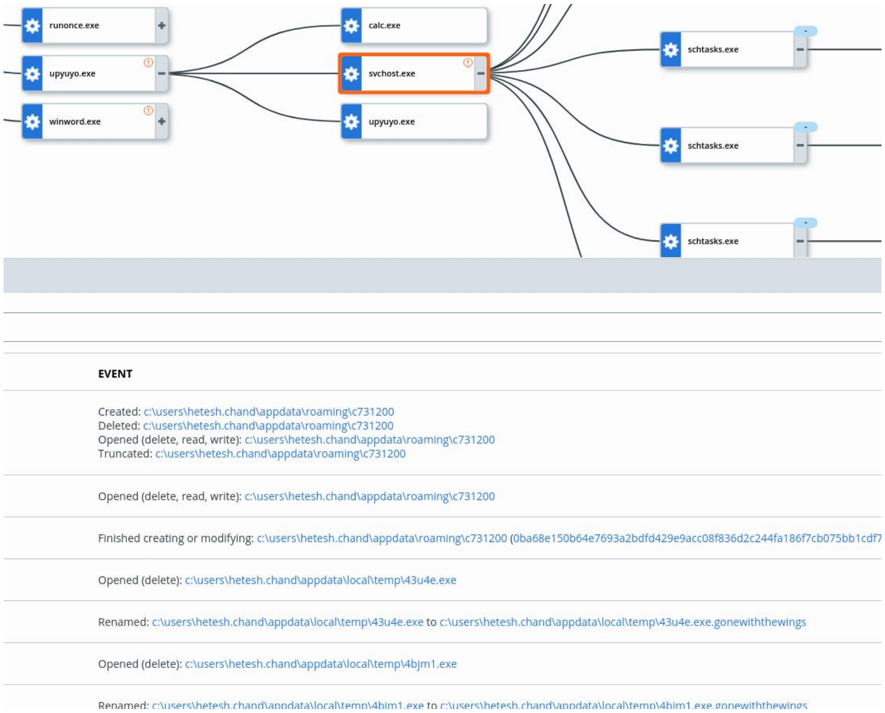


2. Process "upyuyo.exe" spawned "calc.exe" process, which established a connection to api1.wipmania.com.wipmsc[.]ru on port 80 via proxy server:



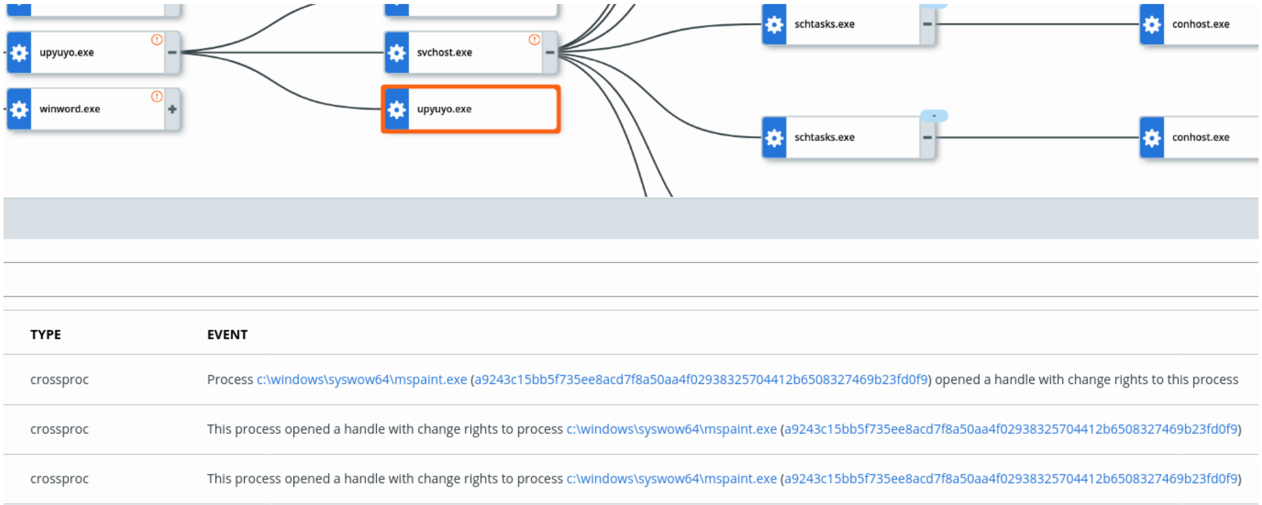
TYPE	EVENT
netconn_proxy	Established: TCP from port 50057 to api1.wipmania.com.wipmsc.ru:80 via proxy server

3. Process "upyuyo.exe" spawned "svchost.exe" process, which performed several file operations on the disk such as creating temporary files:



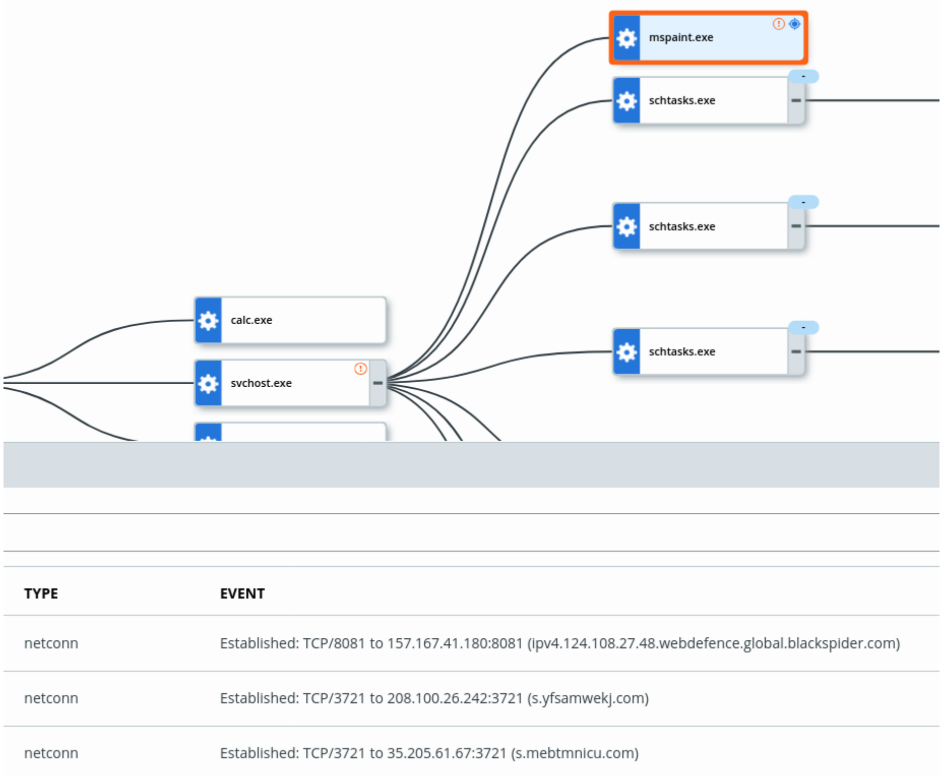
EVENT
Created: c:\users\hetesh.chand\appdata\roaming\c731200 Deleted: c:\users\hetesh.chand\appdata\roaming\c731200 Opened (delete, read, write): c:\users\hetesh.chand\appdata\roaming\c731200 Truncated: c:\users\hetesh.chand\appdata\roaming\c731200
Opened (delete, read, write): c:\users\hetesh.chand\appdata\roaming\c731200
Finished creating or modifying: c:\users\hetesh.chand\appdata\roaming\c731200 (0ba68e150b64e7693a2bdfd429e9acc08f836d2c244fa186f7cb075bb1cdf7
Opened (delete): c:\users\hetesh.chand\appdata\local\temp\43u4e.exe
Renamed: c:\users\hetesh.chand\appdata\local\temp\43u4e.exe to c:\users\hetesh.chand\appdata\local\temp\43u4e.exe.gonewiththewings
Opened (delete): c:\users\hetesh.chand\appdata\local\temp\4bjm1.exe
Renamed: c:\users\hetesh.chand\appdata\local\temp\4bjm1.exe to c:\users\hetesh.chand\appdata\local\temp\4bjm1.exe.gonewiththewings

4. Process “upyuyo.exe” spawned another “upyuyo.exe” process, which performed operations on local processes such as opening a handle to a process in order to inject code:



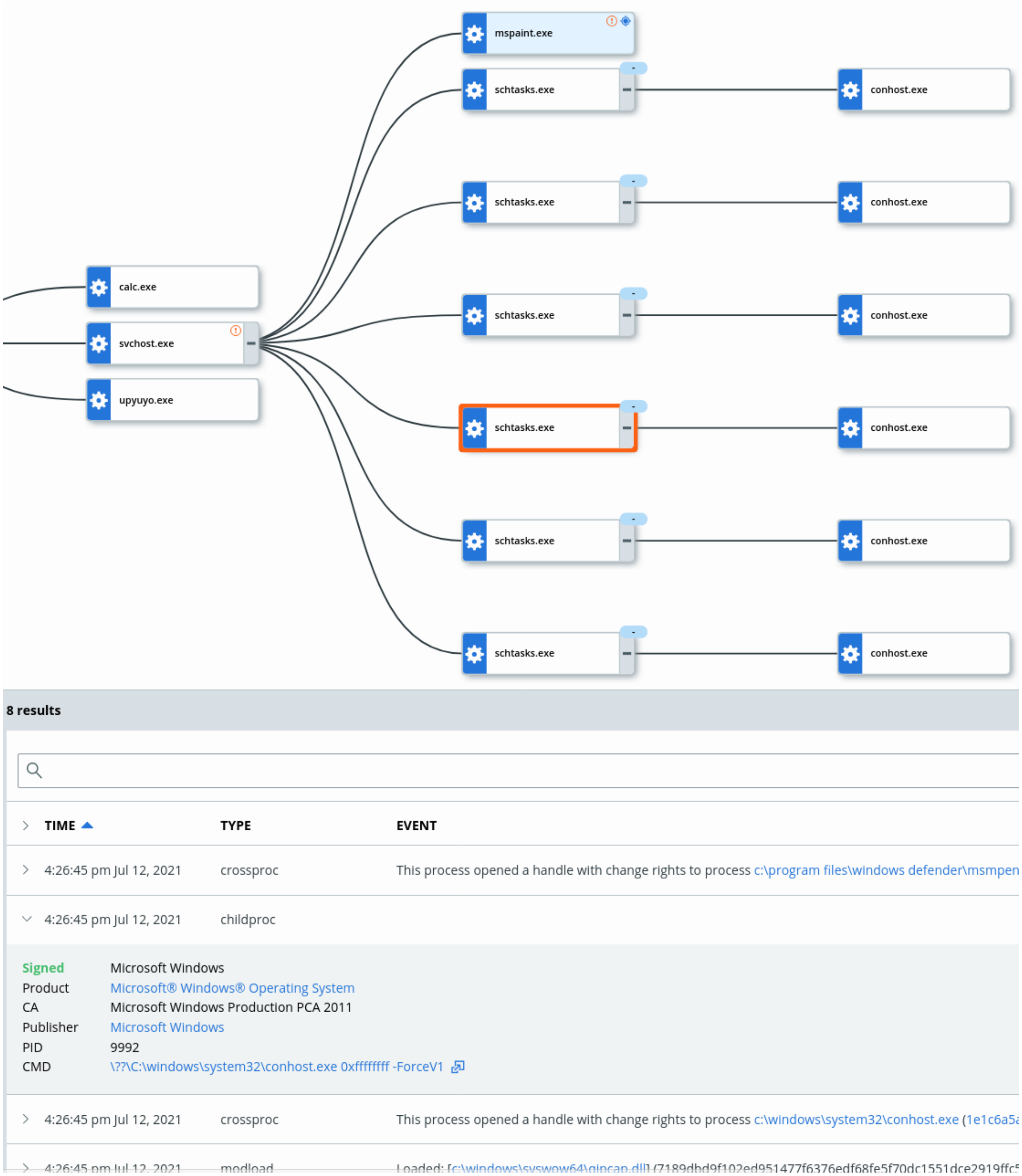
TYPE	EVENT
crossproc	Process c:\windows\syswow64\mspaint.exe (a9243c15bb5f735ee8acd7f8a50aa4f02938325704412b6508327469b23fd0f9) opened a handle with change rights to this process
crossproc	This process opened a handle with change rights to process c:\windows\syswow64\mspaint.exe (a9243c15bb5f735ee8acd7f8a50aa4f02938325704412b6508327469b23fd0f9)
crossproc	This process opened a handle with change rights to process c:\windows\syswow64\mspaint.exe (a9243c15bb5f735ee8acd7f8a50aa4f02938325704412b6508327469b23fd0f9)

5. Process “svchost.exe”, which is a child process of “upyuyo.exe”, spawned “mspaint.exe” process via process injection, and performed several operations, including registry modifications, opening handle to processes and connecting to two URLs “s.yfsamwekj[.]com” and “s.mebtmnicu[.]com”



TYPE	EVENT
netconn	Established: TCP/8081 to 157.167.41.180:8081 (ipv4.124.108.27.48.webdefence.global.blackspider.com)
netconn	Established: TCP/3721 to 208.100.26.242:3721 (s.yfsamwekj.com)
netconn	Established: TCP/3721 to 35.205.61.67:3721 (s.mebtmnicu.com)

6. Process “svchost.exe”, which is a child process of “upyuyo.exe”, spawns 6 “schtasks.exe” processes and associated “conhost.exe” processes. These processes are indication of execution of the Windows task scheduler command line tool, which is used to create, delete, update run tasks.



8 results

TIME	TYPE	EVENT
4:26:45 pm Jul 12, 2021	crossproc	This process opened a handle with change rights to process c:\program files\windows defender\msmpen
4:26:45 pm Jul 12, 2021	childproc	

Signed Microsoft Windows
Product Microsoft® Windows® Operating System
CA Microsoft Windows Production PCA 2011
Publisher Microsoft Windows
PID 9992
CMD \??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1

TIME	TYPE	EVENT
4:26:45 pm Jul 12, 2021	crossproc	This process opened a handle with change rights to process c:\windows\system32\conhost.exe (1e1c6a5a
4:26:45 pm Jul 12, 2021	modload	Loaded: [c:\windows\syswow64\gipcap.dll] (7189dbd9f102ed951477f6376edf68fe5f70dc1551dce2919ffc5

Affected hosts

commsuvapc002
edusuvanb084
edusuvapc599
fjafsuvapc023
forsilpc005
hlthbapc010
hlthbapc014
hlthcwmpc018
hlthcwmpc024
hlthcwmpc060
hlthcwmpc153
hlthcwmpc166
hlthcwmpc168
hlthcwmpc212
hlthcwmpc226
hlthcwmpc270
hlthcwmpc296
hlthlmlmpc002
hlthltkpc031
hlthltkpc044
hlthltkpc064
hlthltkpc083
hlthltkpc104
hlthltkpc114
hlthltkpc147
hlthltkpc158
hlthnadpc006
hlthnaupc007
hlthrakpc006
hlthsigpc008
hlthsigpc016
hlthsuvapc053
hlthsuvapc066
hlthsuvapc094
hlthtavpc003
hlthtavpc005
hlthtavpc006
hlthtmvpc120
hlthwdmpc019
homesuvapc040
judltkpc101
labbapc001
labnadipc013
labsuvapc064
labsuvapc377
labsuvapc379
moitsuvapc007
moitsuvapc222
moitsuvapc255
moitsuvapc258
parlsuvanb021
pwdsuvapc007
pwdsuvapc021
pwdsuvapc262
regdnsrpc014
rfmfsuvapc328
socwelbapc008
socwelkorvpc001
socwelrapc001
socwelsuvapc160
socweltkpc003
tabbapc001
tabbapc003
tabbapc004
tabbapc008
tabltkpc002
tabnadipc010
tabrewapc005
tabsuvanb005
tabsuvapc061
tabsuvapc081
youthsuvapc173