Penetrum, LLC 

Analysis of malware dubbed “NewPass”

09/17/2020

contact@penetrum.com

Executive Summary;

- Penetrum threat intelligence identified a complex malicious malware publically dubbed as “NewPass” that we suspect to have Russian origins. The malware appears to use Imgur as an exfiltration and configuration system and uses HTTP/S as the command and control.
- NewPass appears to attempt to hide itself by masquerading as an Adobe update and most likely has targeted financial services in Cyprus.
- The activity seems to represent a significant threat to financial services in European Union (EU) member states and possibly expands to other countries to serve for Russian national interests.

Details of Threat;

Penetrum threat intelligence identified a complex backdoor publically referred to as NewPass. This malware most likely uses an image sharing website (Imgur) for exfiltration and configuration updates. Malware samples (available on https://penetrum.com/research) related to the NewPass dropper share similar compilation dates from mid-2020. At least one sample presents strings that indicate the malware masquerades as an Adobe update. There is limited indication that a financial entity in Cyprus was targeted using the NewPass malware, however, the infection vector of the attack is not known to Penetrum at this time of writing.

- The malware (NewPass) is a complex backdoor that potentially uploads and downloads images to and from Imgur (an image sharing site). The images may store AES-encrypted data containing the data and information that was gathered by NewPass. There also seems to be indication that the same concept applies for configuration updates. NewPass appears to contain sophisticated code that generates unique titles, descriptions, and comments for images uploaded to Imgur.

- NewPass appears to masquerade as Adobe updates identified in dropped file strings. The malware seems to remain persistent as a service named “Adobe Update Module”.
- The original dropper and launcher were uploaded in early June to an online malware repository by an individual who is believed to be associated with a financial entity in Cyprus.
- The C&C of NewPass has been identified as newshealthsport.com

Files in C&C Open Directory;

The C&C newshealthsport.com was found to be an open directory. Inside of the C&C there are a few interesting files. Such as;

- Data_7294_oem_ee.dat
  - SHA-1: 36a3573f976863376e1cd319d2ba739beb18ac0f
  - Compile time: 2020-06-08 11:32
  - Contents: File appears to only contain this hashsum: FFFFFFFFn7CqOvW5w3hI08D85BB384EC5EDE59CD00000030
- check_descriptions.dat
  - SHA-1: a738864e59129bf0ac1edeb61f15a799c9174544
  - Compile time: 2020-06-08 09:48
  - Contents: File appears to contain encrypted data.

Outlook and Implications;

Penetrum threat intelligence currently tracks NewPass activity as a potential Russian originating unnamed cluster. While it appears that the malware has been linked to Turla given open sources, Penetrum has been unable to with 100% confidence tie the malware to Turla at the time of writing, although the suspected EU member state targeting has consistency with Turla’s past activities. The stealth of the malware along with the use of the photo-sharing site

is notable and is most likely indication of an advanced tactic to circumvent network detections.

Technical Analysis;

Penetrum was able to perform full dynamic analysis on all three samples (launcher, dropper, and backdoor) and was able to determine all of the indicators of compromise. Along with this Penetrum was able to determine the following;

- Highly configurable backdoor written in C++
- Uploads, downloads, and executes files consistent with remote administration tool activity
- Surveys and collects system information
- Remotely reconfigures itself dependent on the machine
- Communicates with it's C&C server over the HTTPS protocol
- Most likely uses Imgur using encrypted data inside of images for exfiltration and configuration updates

SHA-1	Description	Compile Date	Upload Date
69f9df8ff03c949bd89b44954dfc7f2b9874b217 NewPass.bin	Dropper	2020-05-15	2020-06-03
642927729cf6e6f4ca02561401923d4d0e7676a6 NewPass_launcher.bin	Launcher	2020-06-02	2020-06-04
ddd66fc3f7c45e6486c29d4d36ea4c1113ea13fe NewPass_backdoor.bin	Backdoor	2020-05-15	2020-07-07

- Domains/Subdomains
    - 199.188.200.201 - newshealthsport.com
    - 199.188.200.201 - autodiscover.newshealthsport.com
    - 199.188.200.201 - autoconfig.newshealthsport.com
    - 199.188.200.201 - cpanel.newshealthsport.com

    - 199.188.200.201 - ftp.newshealthsport.com
    - 199.188.200.201 - imap.newshealthsport.com
    - 199.188.200.201 - mail.newshealthsport.com
    - 199.188.200.201 - pop3.newshealthsport.com
    - 199.188.200.201 - smtp.newshealthsport.com
    - 199.188.200.201 - webdisk.newshealthsport.com
    - 199.188.200.201 - webmail.newshealthsport.com
    - 199.188.200.201 - whm.newshealthsport.com
    - 199.188.200.201 - www.newshealthsport.com
- Overall entropy:
    - Dropper: 7.351358117096034
    - Backdoor: 6.151287426247101
    - Launcher: 6.258938737362491
- Checks for browsers:
    - C:\Program Files (x86)\Mozilla Firefox
- Registry keys open (due to amount only interesting ones are specified here, you can find all of them at https://penetrum.com/research):
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\shell\open\(Default)
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\iexplore.exe\shell\open
    - HKEY_CLASSES_ROOT\Applications\faxcover.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmplayer.exe\(Default)
    - HKEY_CLASSES_ROOT\Applications\cag.exe
    - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\App Paths\ehshell.exe
    - HKEY_CLASSES_ROOT\Applications\wab.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\isoburn.exe\shell
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmplayer.exe\shell\Play
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\mspaint.exe\shell
    - HKEY_CLASSES_ROOT\Applications\explorer.exe

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\shell\open\ddeexec
- HKEY_CLASSES_ROOT\Applications\wpnpinst.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\rundll32.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\firefox.exe\shell\open\command
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\ehshell.exe
- HKEY_CLASSES_ROOT\Applications\Ttxmpc97.exe
- HKEY_CLASSES_ROOT\Applications\depends.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmpdmc.exe\(Default)
- HKEY_CLASSES_ROOT\Applications\wmplayer.exe
- HKEY_CLASSES_ROOT\Applications\mnyimprt.exe
- HKEY_CLASSES_ROOT\Applications\CChat.exe
- HKEY_CLASSES_ROOT\Applications\grpconv.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\shell\open
- HKEY_CLASSES_ROOT\Applications\mspaint.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\iexplore.exe\shell\open\command
- HKEY_CLASSES_ROOT\Applications\wordpad.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\NTVDM.exe\shell
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\shell
- HKEY_CLASSES_ROOT\Applications\mshta.exe
- HKEY_CLASSES_ROOT\Applications\ehshell.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\notepad.exe\shell
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\isoburn.exe\(Default)

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\(Default)
- HKEY_CLASSES_ROOT\Applications\perfmon.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\mspaint.exe\(Default)
- HKEY_CLASSES_ROOT\Applications\drwatson.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmplayer.exe\shell
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\iexplore.exe\(Default)
- HKEY_CLASSES_ROOT\Applications\notepad.exe
- HKEY_CLASSES_ROOT\Applications\finder.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\firefox.exe\shell\open
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wordpad.exe\shell
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmplayer.exe\shell\play\command
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\firefox.exe\(Default)
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wordpad.exe\(Default)
- HKEY_CLASSES_ROOT\Applications\accwiz.exe
- HKEY_CLASSES_ROOT\Applications\datainst.exe
- HKEY_CLASSES_ROOT\Applications\msiexec.exe
- HKEY_CLASSES_ROOT\Applications\regedit.exe
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\App Paths\rundll32.exe
- HKEY_CLASSES_ROOT\Applications\mplayer.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ehshell.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\App Paths\rundll32.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmplayer.exe

- HKEY_CLASSES_ROOT\Applications\firefox.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\mspaint.exe\shell\edit\command
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\mspaint.exe\shell\open
- HKEY_CLASSES_ROOT\Applications\hh.exe
- HKEY_CLASSES_ROOT\Applications\WScript.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\iexplore.exe
- HKEY_CLASSES_ROOT\Applications\wltmime.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\notepad.exe\shell\open
- HKEY_CLASSES_ROOT\Applications\msimn.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\notepad.exe\(Default)
- HKEY_CLASSES_ROOT\Applications\rasphone.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wordpad.exe\shell\open
- HKEY_CLASSES_ROOT\Applications\graflink.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\iexplore.exe\shell
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\firefox.exe\shell
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\rundll32.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wordpad.exe\shell\open\command
- HKEY_CLASSES_ROOT\Applications\themes.exe
- HKEY_CLASSES_ROOT\Applications\fontview.exe
- HKEY_CLASSES_ROOT\Applications\isoburn.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\shell\open\DropTarget
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\notepad.exe\shell\open\command
- HKEY_CLASSES_ROOT\Applications\snapview.exe

    - HKEY_CLASSES_ROOT\Applications\awdvstub.exe
    - HKEY_CLASSES_ROOT\Applications\MSInfo32.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\wmpdmc.exe\shell
    - HKEY_CLASSES_ROOT\Applications\NTVDM.exe
    - HKEY_CLASSES_ROOT\Applications\wusa.exe
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\PropertySystem\PropertyHandlers\.exe
    - HKEY_CLASSES_ROOT\Applications\winhlp32.exe
    - HKEY_CLASSES_ROOT\Applications\wmpdmc.exe
    - HKEY_CLASSES_ROOT\Applications\sdclt.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\cmd.exe
    - HKEY_CLASSES_ROOT\Applications\helpctr.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\NTVDM.exe\(Default)
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\mspaint.exe\shell\edit
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\mspaint.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\firefox.exe
    - HKEY_CLASSES_ROOT\Applications\MMC.exe
    - HKEY_CLASSES_ROOT\Applications\cmd.exe
    - HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Applications\ehshell.exe\shell\open\command
    - HKEY_CLASSES_ROOT\Applications\fpidcwiz.exe
    - HKEY_CLASSES_ROOT\Applications\iexplore.exe
- Commands executed:
    - ehshell.exe
    - dmd.exe
    - lsass.exe
    - rundll32.exe
    - iexplorer.exe

Snort Rule;

alert tcp $HOME_NET any -> any $HTTP_PORTS (msg:"NewPass"; flow:established,to_server; content:"POST"; depth:4; content:"|0d0a0d0a|newpass="; distance:0; content:"&server_page="; distance:0; content:"&passdb="; distance:0; content:"&targetlogin="; distance:0; content:"&table_data="; distance:0; sid:1000000;)

Yara Rules;

```
rule NewPass_bin
{

        meta:
        author = "Generated by Malcore on 09-17-2020 (contact@penetrum.com)"
        ref = "https://penetrum.com"
        copyright = "Penetrum, LLC"

        strings:
        $specific1 = ",,,,$$$$,,,,TTTTLLLLDDDDLLLLTTTT,,,,$$$$,,,,"
        $matchable1 = "            </security>"
        $matchable10 = "  '&GEO"
        $matchable11 = "  'n"
        $matchable12 = "  /."
        $matchable13 = "  /.$,+*"
        $matchable14 = "  /.M(*"
        $matchable15 = "  /.mp)"
        $matchable16 = "  04+"
        $matchable17 = "  </trustInfo>"
        $matchable18 = "  = hr13<<=&r% "
        $matchable19 = "  ?>-<;:"
        $matchable2 = "            <security>"
        $matchable20 = "  ?>:<;:"
        $matchable21 = "  s(!"
        $matchable22 = " ! j"
        $matchable23 = " ! o"
        $matchable24 = " !##"
        $matchable25 = " !&'"
        $matchable26 = " !&'$%"
        $matchable3 = "  #-%$'j"
        $matchable4 = "  #g"
        $matchable5 = "  '&"
        $matchable6 = "  '&!X+*)(/."
```

```
        $matchable7 = "  '&#$+*"
        $matchable8 = "  '&%$"
        $matchable9 = "  '&+$+*q(/.,,"

        condition:
        1 of ($specific*) and 13 of ($matchable*)
}


rule NewPass_backdoor_bin
{

        meta:
        author = "Generated by Malcore on 09-17-2020 (contact@penetrum.com)"
        ref = "https://penetrum.com"
        copyright = "Penetrum, LLC"

        strings:
        $matchable1 = "            H"
        $matchable10 = " A_A]A\\^["
        $matchable11 = " A_A^A\\"
        $matchable12 = " A_A^A\\_^"
        $matchable13 = " A_A^A]"
        $matchable14 = " A_A^A]A\\_"
        $matchable15 = " A_A^A]A\\_^]"
        $matchable16 = " A_A^^"
        $matchable17 = " A_A^_"
        $matchable18 = " Base Class Array'"
        $matchable19 = " Complete Object Locator'"
        $matchable2 = " !.350:"
        $matchable20 = " L9A"
        $matchable21 = " Type Descriptor'"
        $matchable22 = " delete"
        $matchable23 = " delete[]"
        $matchable24 = " new"
        $matchable25 = " new[]"
        $matchable26 = " r>p1v!t,z8x-~8|?b,`"
        $matchable3 = " #?%lu"
        $matchable4 = " &(6'"
        $matchable5 = " (e/=>cP"
        $matchable6 = " 2>59:"
        $matchable7 = " A^]["
        $matchable8 = " A^^]"
        $matchable9 = " A^_^"
```

```
        condition:
        13 of ($matchable*)
}


rule NewPass_launcher_bin
{

        meta:
        author = "Generated by Malcore on 09-17-2020 (contact@penetrum.com)"
        ref = "https://penetrum.com"
        copyright = "Penetrum, LLC"

        strings:
        $matchable1 = "            H"
        $matchable10 = " (l93;-"
        $matchable11 = " )55!+2"
        $matchable12 = " 3,f"
        $matchable13 = " 41%31"
        $matchable14 = " 4;92r"
        $matchable15 = " =5x~m|"
        $matchable16 = " A^]["
        $matchable17 = " A^^]"
        $matchable18 = " A^_^"
        $matchable19 = " A^_^]["
        $matchable2 = "            </security>"
        $matchable20 = " A_A\\^]["
        $matchable21 = " A_A^A\\"
        $matchable22 = " A_A^A\\_^"
        $matchable23 = " A_A^A\\_^]["
        $matchable24 = " A_A^A]"
        $matchable25 = " A_A^A]A\\_"
        $matchable26 = " A_A^A]A\\_^]"
        $matchable3 = "            <security>"
        $matchable4 = "  ** 2i,%&"
        $matchable5 = "  </trustInfo>"
        $matchable6 = " !HG"
        $matchable7 = " &!22+="
        $matchable8 = " &(8((&,-9"
        $matchable9 = " &0$.C%3< >M"

        condition:
        13 of ($matchable*)
}
```