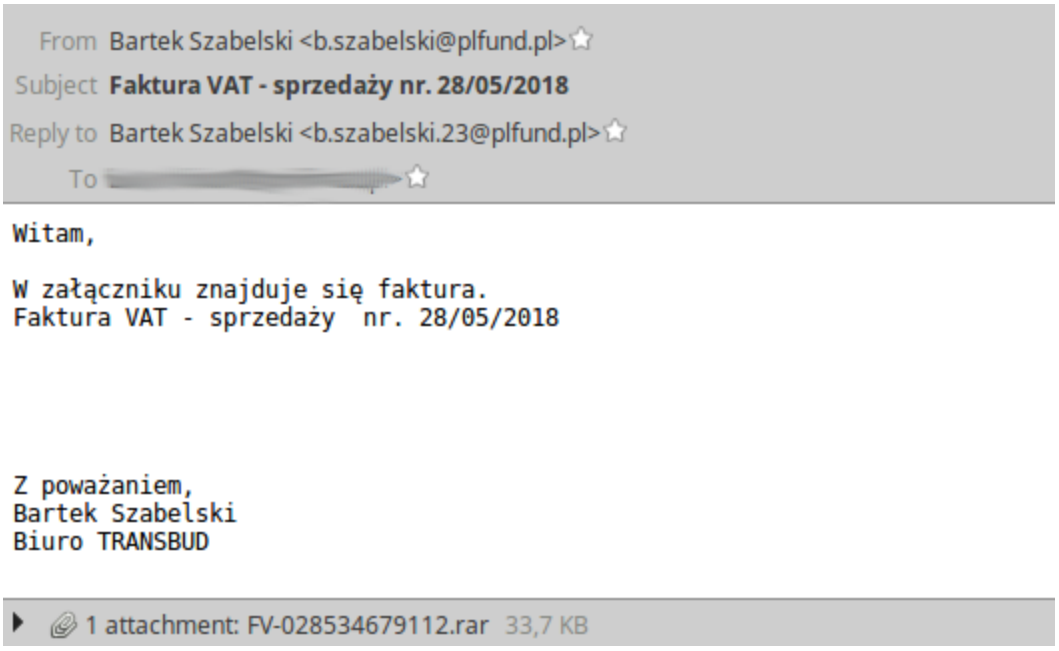
Dropper evolves to botnet (2017)

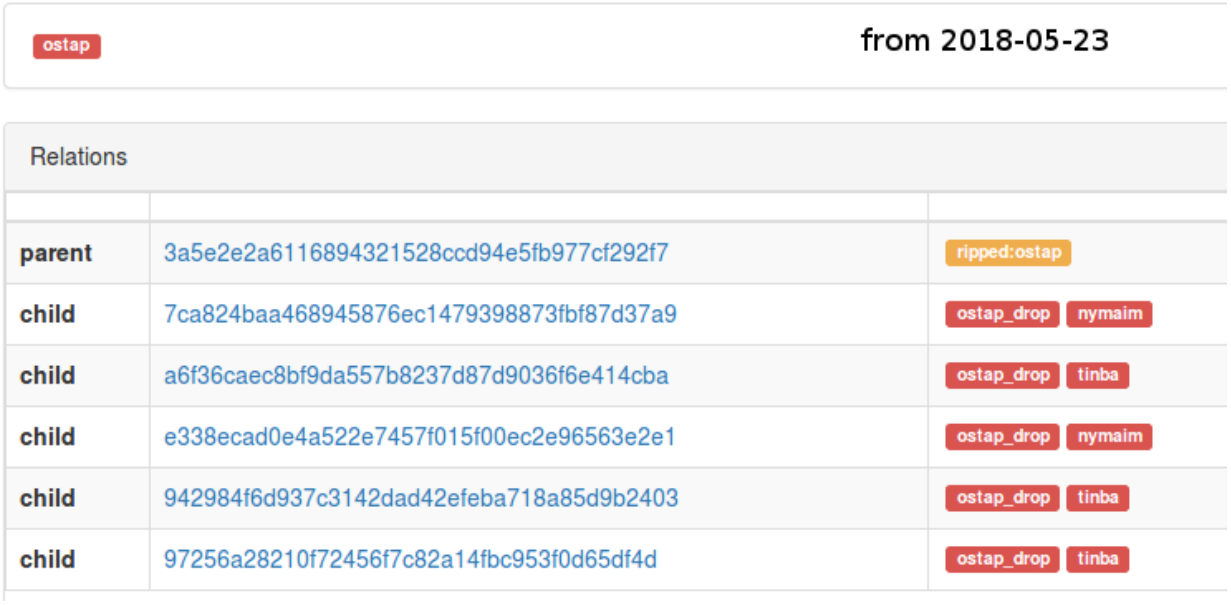
cert.pl/en/news/single/ostap-malware-analysis-backswap-dropper/

Malicious scripts, distributed via spam e-mails, have been getting more complex for some time. Usually, if you got an e-mail with .js attachment, you could safely assume it's just a simple dropper, which is limited to downloading and executing malware. Unfortunately, there is a growing number of campaigns these days, where script doesn't exit after downloading sample. Instead of ending its life – it remains active, waiting for additional commands or more samples to fetch. Some of the examples are: vjw0rm used in Vortex ransomware campaigns and **Ostap** – the main protagonist of our story.

This article is an introduction to Backswap malware analysis, which is a second-stage malware downloaded by Ostap. Our analysis of Backswap malware will be published soon!

Ostap has became a very popular malware worldwide, but the most interesting campaigns observed by CERT.pl occured in Poland. It is mostly used for banking malware distribution. Currently it distributes two banker families simultaneously: Nymaim and **Backswap**, which is actually slightly modified Tinba. Because both malware families are dropped at the same time, there is specific correlation between them – noticed by ESET in their Backswap analysis. Analysis of both banker families can be also found on our webpage.





Script is delivered as a compressed attachment (fake invoice). It has an .rar extension, but don't be fooled – actually it's an ACE archive. This is a very usual technique, used to mislead some automatic analyzers, which identify a file type by its extension. Despite that, WinRAR is able to recognize the real archive format, so victims don't have any problems to execute the Ostap script using that software.

The archive contains a JSE file, which is an encoded JScript. Because of the obfuscation method used (characteristic for this malware), file is rather large, and can exceed several hundred kilobytes in size.

First Ostap campaigns (2016)

First campaigns were observed by CERT.pl in May 2016. In the first versions, Ostap was just a simple dropper, which uninstalls itself after completing its mission. The characteristic part was the obfuscation method mentioned before – strings were completed char-by-char using complex expressions evaluated by JScript interpreter.

After deobfuscation:

During execution – script was performing few actions:

- Shows message The document is corrupted and cannot be opened
- Adds itself to the Startup folder oShell['NameSpace'](7), which ensured automatic execution on logon (in case the file was not available immediately)
- Tries to download and execute EXE file from URL https://217.28.218.217/YOP634EFARRR/q64.php?add=gtyhbncdfewpnjm9oklmnfdrtqdczdfgrt&<random number>. In case of failure – it tries again every 80 seconds.
- After successful download and instalation – removes itself from Startup and deletes downloaded file, ending its existence on compromised host.

So, at first, Ostap was just simple dropper, but pretty characteristic (e.g. because of add= argument containing campaign identifier, obfuscation, URL format). Samples downloaded by Ostap weren't usually available immediately after the beginning of the campaign and they were distributed only for a short period of time. Downloaded malware samples were usually bankers: KBot and Gozi ISFB

A month later – in June 2016, we found next version of Ostap, sending additional information about victim environment.

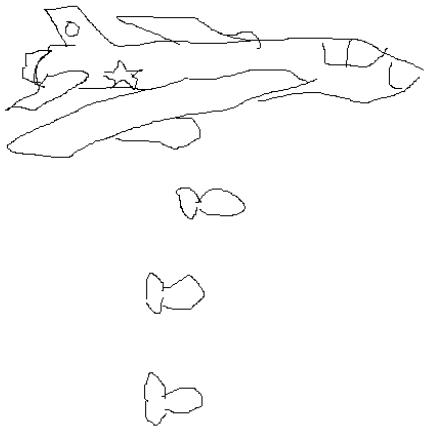
C&C address was slightly different and contained more fields:

Meaning of each field is described below:

- hash from the Startup path and computer name (uid)
- operating system version (based on Users substring existence in %HOMEPATH%) – ver
- additional request was sent after successful download (out=1)

C&C was delivering malware encoded in Base64. Ostap was perfoming some decoding using the built-in certutil command. Also, new version contained some fail-safe methods of malware execution:

Criminals were showing their (kind of) creativity, sometimes adding a bitmap file to ACE archives.



A few months later, script started to deliver various types of banking malware such as Tinba, Ramnit or ISFB. Since then, Ostap (named after ostap.php script name) was slowly becoming serious piece of malware.

Because of the variety of samples and number of parallel campaigns, we began to suspect that Ostap is used as distribution service and delivered software is not associated with single actor. From 2016, Ostap was getting more and more active.

From the half of 2017, Ostap became more powerful. The first thing developed in 2017 version were several anti-analysis techniques.

Gathering information about execution environment

Before Ostap launches – malware executes WMI query, requesting for active processes list, user name, domain name, version of operating system etc.

Output from sysInfo and procInfo is then concatenated:

Then, Ostap looks for occurences of several names characteristic for analysis tools and sandbox environments:

If a characteristic name is found, Ostap calls document.alert method. Object document doesn't exist in Windows Script Host context (it is seen only in web browsers) which raises an unhandled exception, stopping the execution.

After gathering information from WMI – script copies itself to Startup and goes to the main part.

Communication with C&C (downloading malicious samples)

URL pattern used by Ostap from 2017 was very similar. However, few communication aspects changed from the 2016 version.

- Request method changed from GET to POST
- Ostap sends fetched sysInfo+procInfo as request body
- Argument names were shortened (uid becomes u)

C&C server sends additional information about blob format and method of sample execution:

- File could be sent raw or Base64-encoded (Content-Transfer-Encoding was set to binary or base64)
- There were few methods of execution, based on you_god_damn_right HTTP response header value (actual name differs depending on the malware version)

Yup, Ostap is full of "Breaking bad" quotes.

Possible values of you_god_damn_right are:

- 0 – file is an update (replace the original script and execute, closing itself)
- 1 – run DLL file (with secretFunction as entrypoint)
- 2 – install software silently with Administrator privileges (MSI installer)

By default, fetched file was run using cmd /c start <file path>

After successful installation – script removes all files from TEMP folder which were potentially associated with fetched sample (*.exe,* .gop – base64 encoded, *.txt,* .log, *.jse – update)

Destructive propagation on removable media and network shares

If creation of file after download was unsuccessful (file still doesn't exist under expected location) – Ostap becomes more nasty than usual.

At the beginning, script was preparing a list of files with specified extensions, which are located on removable media and mounted network shares. List of files found was written to temporary file saymyname.txt.

Then, based on that list – all files were deleted and replaced by Ostap copy (with preserved name and added .jse extension). The purpose was probably to "punish" incautious analysts, which can accidentally trigger that code by script modifications.

Persistence

Starting from 2017, Ostap doesn't erase itself after successful download anymore. Using self-update capabilities, malware persists on infected machine, serving banking malware from various families. The victim becomes a part of distribution botnet.

Current version (2018)

Currently, Ostap is one of the most active families targeting the online banking customers in Poland. Malware code is being constantly developed and improved.

Version from 2018 has added few more methods of sandbox detection:

- Malware doesn't execute on Windows XP
- Ostap verifies length of process list (>1500 characters is needed, which was efective against emulation using tools like box-js)

- Few strings were added to blacklist:

If a sandbox substring was detected:

- Malware executes ploha['show']('No more half-measures.'); which triggers undefined variable exception (ploha doesn't exist in the code)
- If exception is not raised (or handled externally) – Ostap tries to terminate script using WScript.Quit()
- If script is still working – "destructive propagation" is activated

Destructive propagation has additional condition now – if file creation was unsuccessful and sandbox was detected without script termination, malware starts removing files.

The URL address was also slightly changed:

Now, the add parameter isn't the campaign identifier – that role is taken over by DeretghrttLolookest75=awsedrftgyhujiko, which changes depending on the sample.

In latest version – HTTP execution method header is also different: We_are_done_when_I_say_we_are_done, as well as message displayed after executing script first time, which changed to PDF Error: The document could not be printed..

Summary

Ostap shows how simple dropper script can evolve into real botnet malware. In summary, here is the listing of characteristic elements for Ostap malware:

- Distribution via large-sized JSE files, delivered as ACE archives with .rar extension

- Message showed after first execution of script (PDF Error: The document could not be printed.)
- Characteristic script obfuscation method
- Persistence (self-update capabilities, adding itself to Startup folder)
- Unusual URL pattern https://<ip[:port]>/<path>.php?<campaign_id1>=<campaign_id2>&add=james&(arguments…)

Additional information

Example samples:

Samples after deobfuscation:

- 2016-q64
- 2016-ostap
- 2017
- 2018

Ostap was mentioned frequently in various articles (as “interesting dropper” or “JS/Nemucod”):