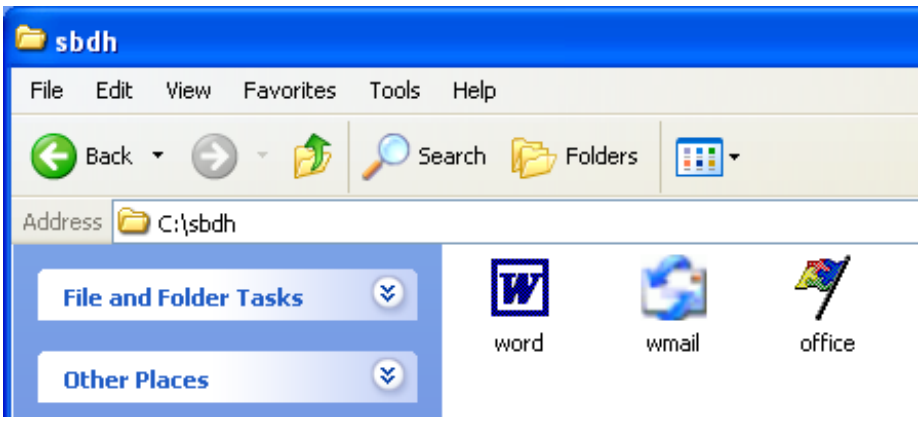
Espionage toolkit targeting Central and Eastern Europe uncovered

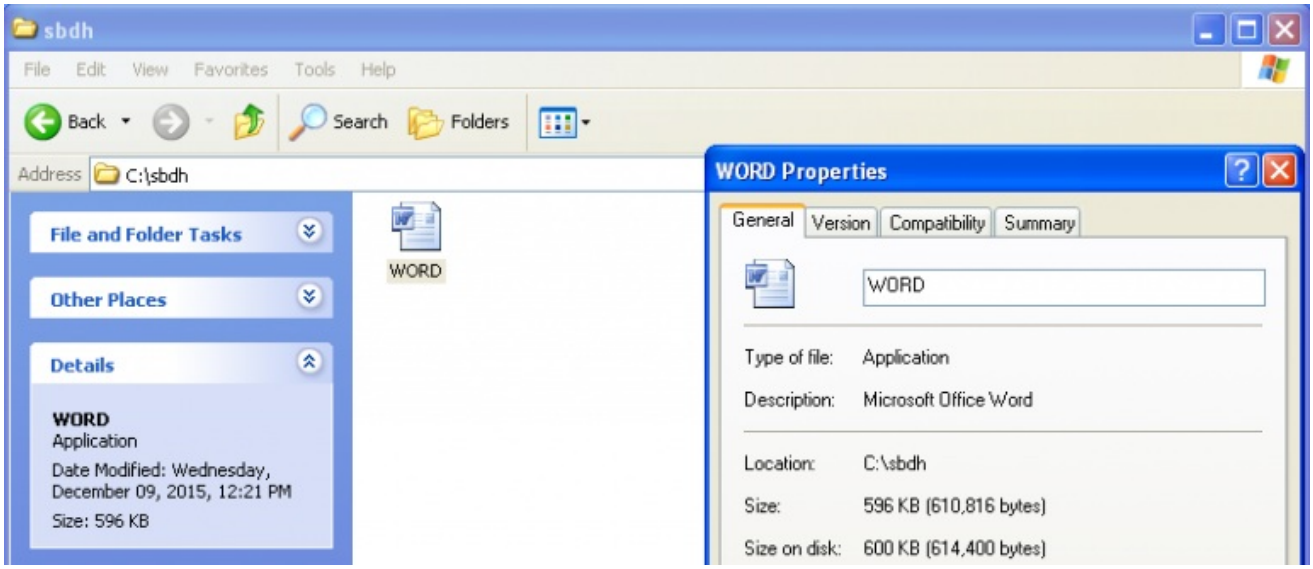
welivesecurity.com/2016/07/01/espionage-toolkit-targeting-central-eastern-europe-uncovered/

By Tomáš Gardoň

Over the course of the last year, ESET has detected and analyzed several instances of malware used for targeted espionage – dubbed **SBDH toolkit**. Using powerful filters, various methods of communication with its operators and an interesting persistence technique, it aims to exfiltrate selected files from governmental and public institutions, which are mostly focused on economic growth and cooperation in Central and Eastern Europe. ESET's SBDH findings were presented during the Copenhagen Cybercrime Conference 2016 by researchers Tomáš Gardoň and Robert Lipovský.

This toolkit – actually only its initial part – was spreading as an executable with a double extension attached to a phishing email (counting on Windows' default behavior of hiding an extension). To further increase its chances of being run by the receiver, it uses legitimate looking icons of several Microsoft applications or a Word document.





Upon successful execution, the malware contacts a remote location in order to download two other main components of the toolkit: a backdoor and a data stealer. The combination of these modules provides the attacker not only with full remote control of the compromised computer, but also with an advanced method of data exfiltration.

Thanks to powerful filters the operator can specify in great detail which data should be exfiltrated, using conditions such as file extension, date of creation, file size and others. These can be modified via the malware configuration files.

```
K1TU4ckBn.dec                    ↓FRO ========                    0000002A|Hiew 8.10 (c)SEN
[main]
folder=c:\Program Files (x86)\Windows Live\Mail\
runkey=Windows Live Mail
reload_ini=1
sleep=300
fullog=0

[zip]
maxsize=19000000
minfree=500000000

[send]
enabled=1
server=5.1.81.150
waitfromstart=60
method=post
max_size=520000
maxsizeofthezip=100000000
olderthan=4000
biggerthan=5000000
sleep=22

[recent documents]
enabled=1
ext=.ini;.conf;.txt;.rtf;.doc;.docx;.pdf;.csv;.xls;.xlsx;.pps;.ppt;.pptx;.wpd;.wpf;.odt;.ott;.odm;.
oth;.ods;.ots;.odp;.otp;.sxf;.stw;.sxd;.htm;.html;.mht;.tif;.tiff;.eml;.msg;.zip;.gz;.rar;.tar;.7z
sleep=1800
fron=2014.08.28

[docs]
enabled=1
drives=d:\Mail [redacted]\inbox;d:\Mail [redacted]\sent items
ext=.eml
sleep=1800
fron=2014.08.28
cmd=

[usb]
enabled=1
ext=.ini;.conf;.txt;.rtf;.doc;.docx;.pdf;.csv;.xls;.xlsx;.pps;.ppt;.pptx;.wpd;.wpf;.odt;.ott;.odm;.
oth;.ods;.ots;.odp;.otp;.sxf;.stw;.sxd;.htm;.html;.mht;.tif;.tiff;.eml;.msg;.zip;.gz;.rar;.tar;.7z
fron=2014.08.28
waitfromstart=10
sleep=600

[outlook]
enabled=0
sleep=3600
1Help 2Unwrap 3      4Mode 5Goto 6LnFeed 7Search 8Table 9Files 10Quit 11Hem 12
```

Because all of the components of this espionage toolkit require connection to the C&C server, the malware depends heavily on handling network communication.

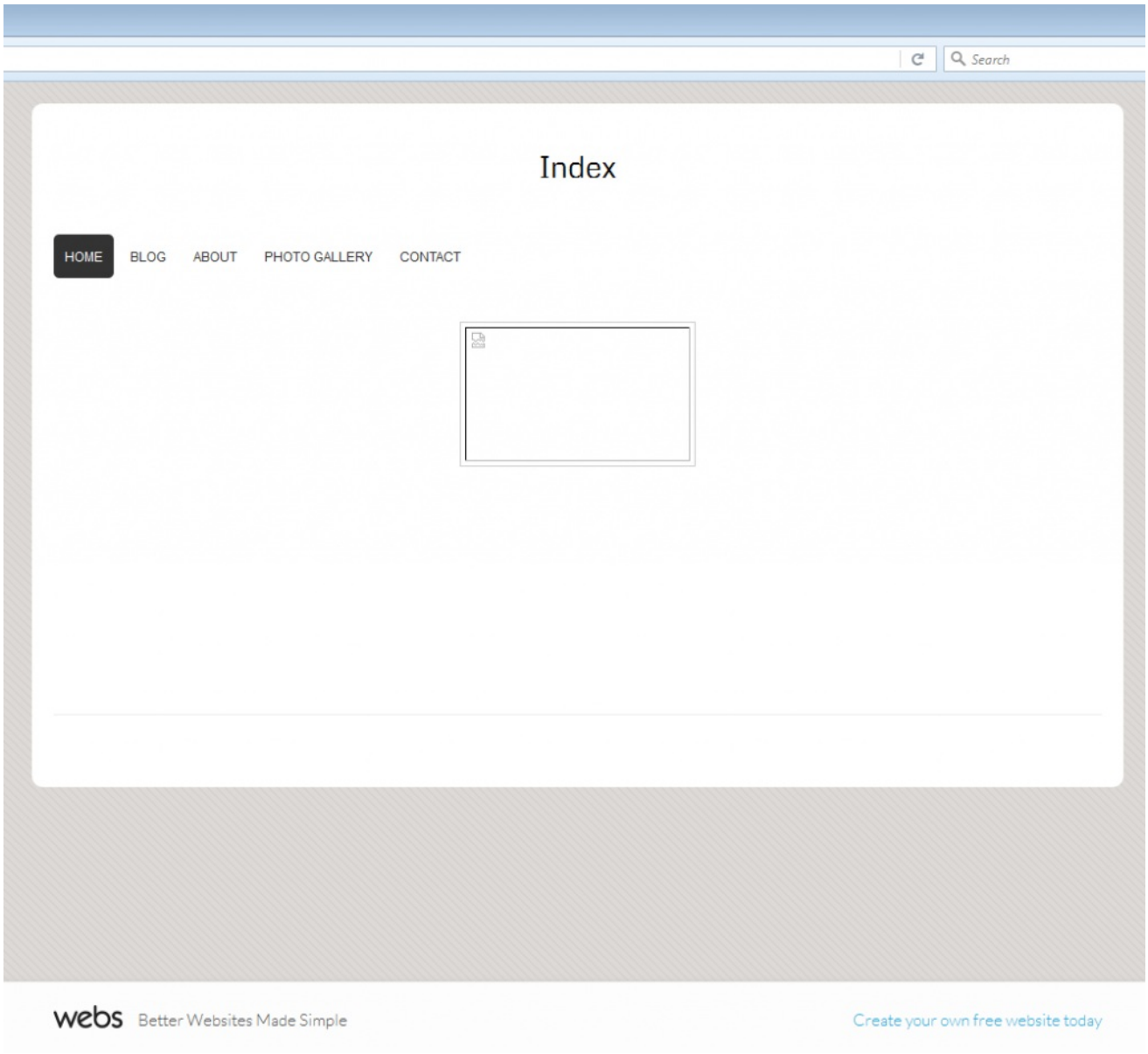
To increase its chances, it uses multiple methods for connection. First it attempts to use HTTP protocol. If that fails, the SBDH malware opts for a second method and tries to communicate via SMTP protocol using a free external gateway.

As a last resort, it has the capability to communicate by injecting specially crafted emails into Microsoft Outlook Express. This way, injected emails were sent under the account of the currently logged user, allowing the malware to bypass security measures (assuming the user had rights to send and receive emails). These malicious messages created by the malware were then placed directly in a victim's outbox, to avoid their attention.

In cases of incoming communication, the malware searched the victim's inbox in order to identify emails received with a specific subject. If the toolkit found such emails, they were parsed and checked for malware commands. Finally, the subjects of these emails were changed to prevent any further examination by the malware.

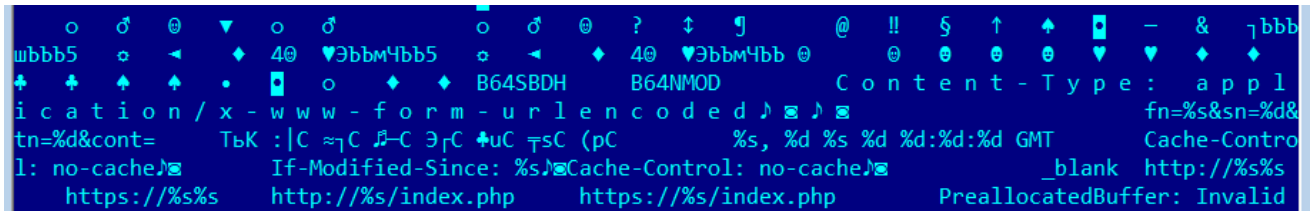
However, this last option was only used up until 2006, when Outlook Express was replaced by the newer Windows Mail application. Since then, the developers of this toolkit have increasingly focused on improving the HTTP communication method and started camouflaging communications with the C&C server by using fake image files (.JPG, .GIF) to carry the data.

In case of the C&C server's unavailability, the backdoor component had yet another "backup solution" – a hard-coded URL pointing to a fake image (hosted on a free blog webpage) that contained the address of an alternative C&C server.



Some of the analyzed samples of this component implemented an interesting persistence method; the malware was replacing the handler for Word documents. It means, whenever the infected system tries to open/edit a Word document, the malware gets executed.

Last but not least, if you are asking yourself where the name of the toolkit comes from, the “SBDH” string found in compilation paths of its downloader and – more interestingly – the string “B64SBDH”, acts as a trigger to download its remaining components from a remote server.



Using similar techniques as the malware in Operation Buhtrap, the SBDH espionage toolkit proves that even advanced threats are still being spread via simple vectors, such as malicious email attachments. Yet, such risks can be spotted by properly trained staff in organizations and further mitigated by implementing a reliable multi-layered security solution.

Hashes

1345B6189441CD1ED9036EF098ADF12746ECF7CB
15B956FEEE0FA42F89C67CA568A182C348E20EAD
F2A1E4B58C9449776BD69F62A8F2BA7A72580DA2
7F32CAE8D6821FD50DE571C40A8342ACAF858541
5DDBDD3CF632F7325D6C261BCC516627D772381A
4B94E8A10C5BCA43797283ECD24DF24421E411D2
D2E9EB26F3212D96E341E4CBA7483EF46DF8A1BE
09C56B14DB3785033C8FDEC41F7EA9497350EDAE