

# 2021-09-17 (FRIDAY) - SQUIRRELWAFFLE LOADER WITH COBALT STRIKE

[malware-traffic-analysis.net/2021/09/17/index.html](https://malware-traffic-analysis.net/2021/09/17/index.html)

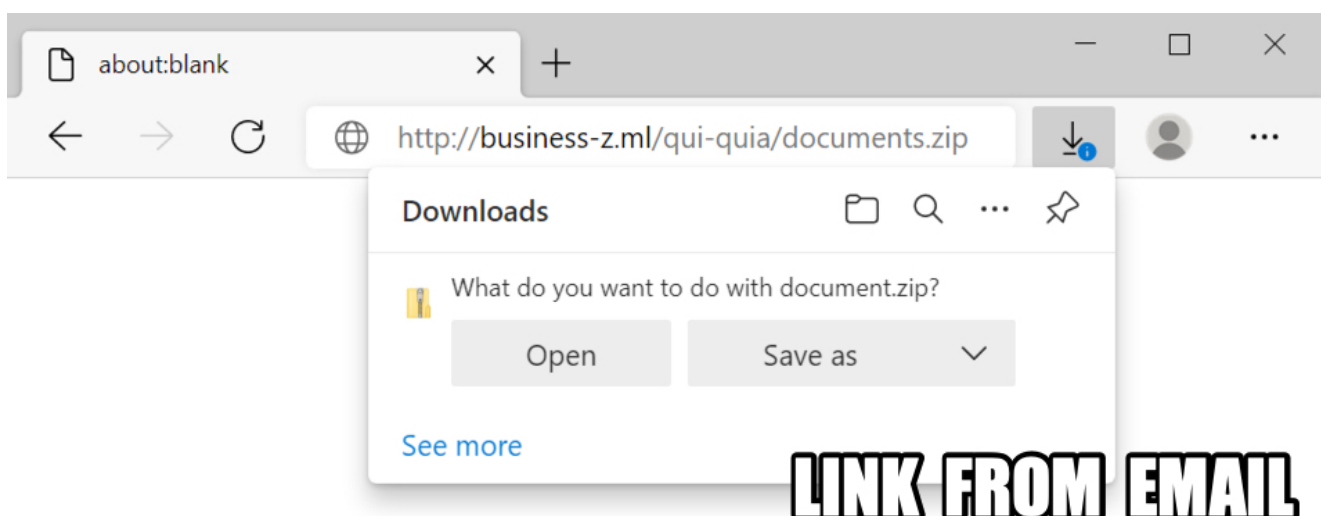
## ASSOCIATED FILES:

- [2021-09-17-IOCs-for-Squirrelwaffle-loader-with-Cobalt-Strike.txt.zip](#) &nbsp; 3.6 kB &nbsp; (3,563 bytes)
- [2021-09-17-Word-docs-for-Squirrelwaffle-Loader-10-examples.zip](#) &nbsp; 1.3 MB &nbsp; (1,347,448 bytes)
- [2021-09-17-Squirrelwaffle-loader-with-Cobalt-Strike.pcap.zip](#) &nbsp; 7.0 MB &nbsp; (7,008,533 bytes)
- [2021-09-17-Squirrelwaffle-and-Cobalt-Strike-malware-and-artifacts.zip](#) &nbsp; 558 kB &nbsp; (558,102 bytes)

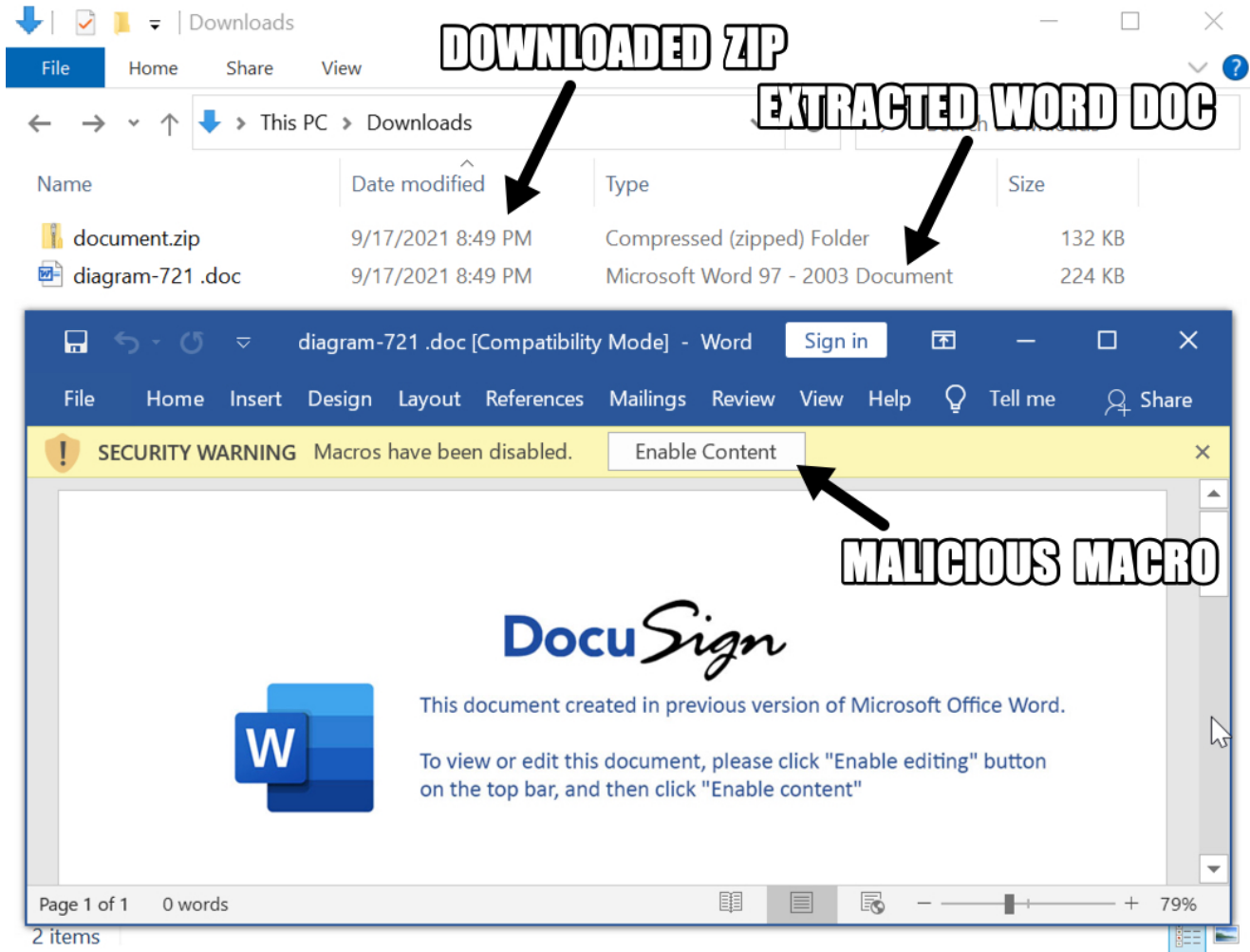
## NOTES:

- See [2021-09-17-IOCs-for-Squirrelwaffle-loader-with-Cobalt-Strike.txt.zip](#) for more info on Squirrelwaffle Loader and this specific infection.
- All zip archives on this site are password-protected. If you don't know the password, see the "about" page of this website.

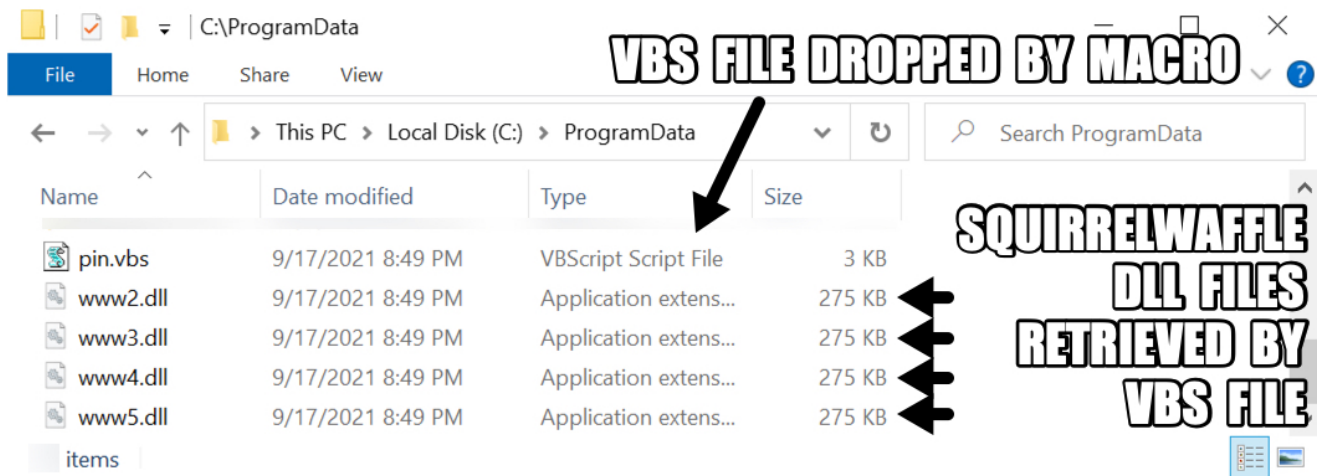
## IMAGES



Shown above: Link for malicious zip archive from an email pushing Squirrelwaffle loader.



Shown above: Word doc extracted from downloaded zip archive.



Shown above: Squirrelwaffle artifacts from an infected Windows host.

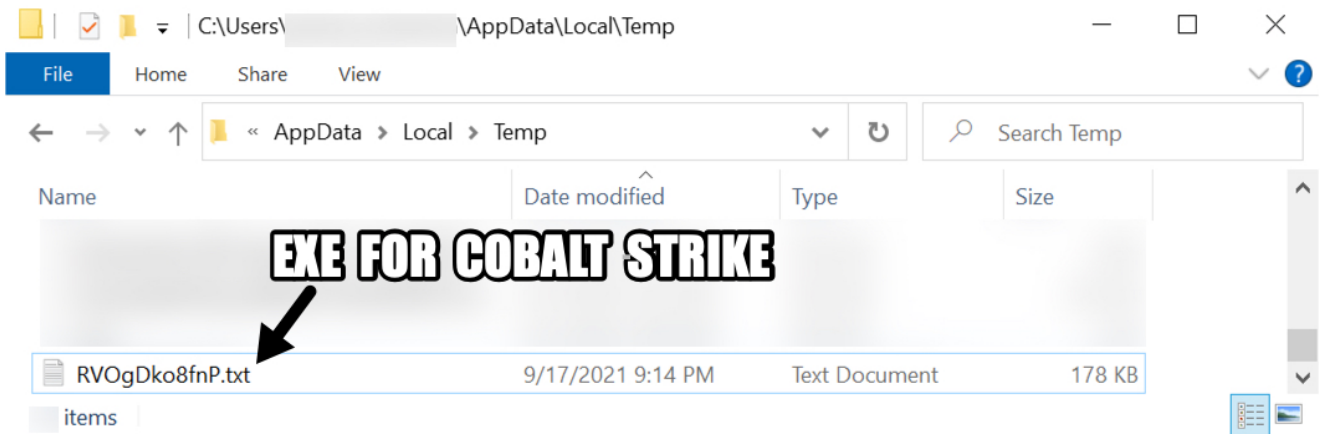
**RETURNS ZIP CONTAINING WORD DOC**

Time	Dst	port	Host	Info
2021-09-17 20:49...	192.185.52.124	80	bussiness-z.ml	GET /qui-quia/documents.zip HTTP/1.1
2021-09-17 20:49...	192.185.52.124	443	bussiness-z.ml	Client Hello
2021-09-17 20:49...	162.222.226.77	443	perfectdemos.com	Client Hello
2021-09-17 20:49...	204.11.58.87	443	priyacareers.com	Client Hello
2021-09-17 20:49...	108.167.172.125	443	cablingpoint.com	Client Hello
2021-09-17 20:49...	162.241.85.65	443	bonus.corporatebusinessmachines.co.in	Client Hello
2021-09-17 20:50...	192.185.115.199	80	bonusvulkanvegas.srdm.in	POST /U7o0xmI1m/0QsaDixzHTgtfjMcGypGen
2021-09-17 20:50...	192.185.115.199	80	bonusvulkanvegas.srdm.in	POST /U7o0xmI1m/0QsaDixzHTgtfjMcGypGen
2021-09-17 20:50...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/ASK5Kx0SPR8lJJE5eTg9G
2021-09-17 20:50...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/ASK5Kx0SPR8lJJE5eTg9G
2021-09-17 20:51...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/fxMKNg0nKzN/DA15DggBI
2021-09-17 20:51...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/fxMKNg0nKzN/DA15DggBI
2021-09-17 20:51...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/eDkAA0bInx9Rnp9eWJ+f
2021-09-17 20:51...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/eDkAA0bInx9Rnp9eWJ+f
2021-09-17 20:52...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/LjI+JSoqJQ4lBiywAhr7K
2021-09-17 20:52...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/LjI+JSoqJQ4lBiywAhr7K

**HTTPS TO DOWNLOAD DLL FILES**

**SQUIRRELWAFFLE C2**

Shown above: Traffic from a Squirrelwaffle loader infection filtered in Wireshark.



Shown above: Windows EXE for Cobalt Strike seen as follow-up malware.

Time	Dst	port	Host	Info
2021-09-17 21:14...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/AD0jNh4yPXMuNjMDDTsAGiWzChY
2021-09-17 21:14...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/AD0jNh4yPXMuNjMDDTsAGiWzChY
2021-09-17 21:14...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/MQN8fQJCe3x+YXp8Zx1henhz HT
2021-09-17 21:14...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/MQN8fQJCe3x+YXp8Zx1henhz HT
2021-09-17 21:14...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:14...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:14...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/HQusCCQkQ3p7fWV7fWJ+Zxt5dA=
2021-09-17 21:14...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/Jys7KDkzJh4/DQN4cg8iQnt8fmF
2021-09-17 21:15...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/LSQbFSMq0i86Nycf0A4HexMIIXw
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/BBgSjYk5IBkWCy89fQAs0xJ4fyp
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/EQ4v00Z6fXlfn1kemJ+eXI= HT
2021-09-17 21:15...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/PiskOBudCh41JnIjR80IQgaJkZ
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:15...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:16...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:16...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/B0N6e31le31ifmV7eXQ= HTTP/1
2021-09-17 21:16...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:16...	95.214.132.17	80	test.dirigu.ro	POST /dxF4cS4GPL/JRAYDypzJBSdByU60xY+P35+ejc
2021-09-17 21:16...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:16...	213.227.154.92	8080	systemmentorsec.com	Client Hello
2021-09-17 21:16...	213.227.154.92	8080	systemmentorsec.com	Client Hello

**HTTPS TRAFFIC FOR COBALT STRIKE ON 213.217.154.92 OVER TCP PORT 8080**

Shown above: Traffic filtered in Wireshark showing when Cobalt Strike activity started.

[Click here](#) to return to the main page.