Protezione da Flash? Se lo propone Facebook per Edge non serve

Feb 21, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Il browser Microsoft contiene una whitelist che permette l'avvio automatico dei contenuti in Flash del social network di Zuckerberg. Alla faccia della sicurezza…

Sono anni che tutti i ricercatori di sicurezza lanciano anatemi contro **Flash**. Il formato sviluppato da **Adobe**, infatti, è uno dei più vulnerabili ad attacchi ed è considerato **una sorta di "buco nero" per la sicurezza**.

Negli ultimi tempi anche i produttori di software sembrano aver capito l'antifona e hanno introdotto limitazioni al suo utilizzo, prevedendo, per esempio, che **Flash non venga attivato automaticamente nelle pagine Web ma solo con un "consapevole" clic dell'utente**.

A quanto pare, però, **Microsoft** ha deciso di prevedere qualche eccezione. **Ivan Fratric**, un ricercatore del **Project Zero di Google** si è accorto che **Edge** integra una whitelist nascosta che contiene alcuni siti Internet ai quali sarebbe concesso di eseguire automaticamente Flash.

La lista è nascosta in un file ben poco rintracciabile (C:\Windows\system32\edgehtmlpluginpolicy.bin) e comprendeva, fino allo scorso novembre, **58 domini Internet** (curiosamente c'è anche un sito italiano, quello di La7) che Microsoft considerava "sicuri". Tra questi c'è, accanto a siti di

qualsiasi genere, anche **Facebook.**

Hash	Dominio in chiaro
01d004ae59fe9d0902b0e4526999432118199654f78b0384e4eb983e986d562d	www.pogo.com
0309388894379c1e0d01081f6f4d5d4412a82dc5b9bd66476de2270b361cecfd	www.wasu.cn
0ae9eeba3229fa449ff5fcf42692cad2305e14933a6102187e94c48346ab8c9d	www.tvnow.de
0bc8e61a5970eb325f02148c05b79d60a9a0462efc18a6a60b7f8cd2dc84ccbc	chushou.tv
0bfc80d67c9b57f3f1bb978344c8d8d6ac19786e261f98c1c9735f6ba5ec344c	more2.starfall.com
1136593de37540f6f5396fdbbf93aa070c2b1c844d2d3d06de5373831a9df3bf	loa.gtarcade.com
12055be963e0f2c7786d1283d343afbaac921513a985a21f5f83b6a82b9582e9	nseindia.com
12c3d9b1a0a1f33a7d7ab1b4ccb53c1163210ee527ad5336175eb40ff1fcfe45	N/A
2135e9b55346dd4146bbfae6f0cc896a39688d3287a952f63ae222837e5de152	www.wgt.com
22af4cad3e57873a50693fe36d6385795ae6c56e4d0d759530f263db571a6b2c	netgauge.unitel.ao
2df0e6efc506a72a4c9e91ebebe70cf8252f1ffbd8b483043b1a856b75d13ce9	www.icourses.cn
2f87a652a9d2880a3ad580ec4a91bde3f4d2d32ac8f792d4258518d46330870f	www.la7.it
2f9f879f017ebe4d6f71a0755eee3b08a5f757c0d011112ded94e6b337b3b520	www.dgestilistas.es
348374ff89afe5693015c3d38758c83867c180a8010372a564c8f5eeaf9b5d0b	www.zxxk.com
3c23924f2f71c05d3b484fbaaa6e4ab4319d5bb3f0a002688132aa0f8434fd3b	weathernews.jp
46bdf3a01ab608d1a5e68923532e610ff7725a68d4bb063c96c8dedd4617404a	bigfarm.goodgamestudios.com
4740f56f40ed20eddb576ae29fdf0c507dd06681e949bda8be5611eaf3ad9d3d	www.facebook.com
4779eb7f42cc6736ca2b1e52449799705214f2542fa4cf952e741d8dd5efad31	www.deezer.com
4f5db25a3bd2f1abf3dd1a509b2e1a6d81b9ba4428f333454c29d93e794150bc	N/A
515563682e9bfc44b6fed4459149f83ba7f207bf53f6a0208156ac7c46e59d92	yahoo-mbga.jp
51bfa3e340a5ff7dfa37ad7ad409e5a214caadd0f82fc1fef82d38b766c2f088	ok.ru
563d53ee90b355ebd7558c2d9f3bee94489d406c565f9ed5741fb59bbc734544	seer.61.com
5b13e0a388860a0f136eefdd36d2f57fb81f46588ca85e7d93a4fd24cf6462f8	empire.goodgamestudios.com
5e7fc524d10f21da23bc43f24de00967094d69d6f4ccda277fff7042024c3ce5	www.friv.com
5f832e1442b497050d79cd18b32de807e4201a3181929ade823112defa6c1079	video.baomihua.com
64e2991629e5e208874400bc1ea0161fb064f1c2397b1cedc3bb282ea3f4ee3b	hiztesti.turktelekom.com.tr
6793b64c0ccc547a01b8b6982318e25ae3dc0b91dfc09366c7f1f1b3a7fa127e	www.scholastic.com
68fc10e638f0bb2e25149d2ef8d3d87cf318bbf2de7c9aa74131d53e926fe79e	www.viz.com
881bcca2199248b7c82ed14cb1dbd6e87ac9ea899d1f9f02d13d29e837487782	www.dilidili.wang
89ac7d2d82b6a2ef952e3d627853180fb250167ed56b893647814e8374d4f5cd	games.aarp.org
900da7ee51cf43450699d9cd11e3cf6ba8d2d04d9d836cd359281d7791e328af	www.douyu.com
9adea347b4e793529c9a5e1a35e2aa7c88772b7e2a086d2d24a4f8ccbb20e3ac	rc.qzone.qq.com
9c97a59b30e879d3245139795adea4380f62e4e14149025f12f69eb3b532e518	www.nicovideo.jp
a2cf2fe6a8822459d81d15b1327b5bac601bafc460fafa716bc2dcc21e9ab50e	www.mynet.com
a77de76633b0717c62034512fb5c3fbb50633ad9b5ebef7a8acf180e455a3025	www.hotstar.com
ad973e7d68dd2c1a8e9f04886e34db40021e1e76eff3bbc53e7ab8934688a4ed	www.4399.com
b61f47eb2fc64b2ad7ee4ae780ea0ac1a886b4f02f1ec8da77db13f920b4874b	www.bilibili.com
ba33c2367ea9f0c66b5b3f345be68a0287a96ca797654c0bf9b2e584d2809ccb	www.msn.com
ba3bc78ec1f427cba6e22cbd63dae305814ca0f0740c0dbd494f804fcaef671a	zone.msn.com
c2fda282c3b5875eaeb6d27ecf62b995684d5739ba1e4082d265dd28dd98ef70	www.worldsurfleague.com

ca6efef88504373a9406ed9a31b430d6df8bb60ea630ac698b0d7c4dab0faf7a	www.stupidvideos.com
d833be74b7f95eb0ac133c5aa06c71b7792b5051b1a369740694e78525a4d872	entitlement.auth.adobe.com
dd0f56a6b1a1f2908f4ff45438ffa5e05679375ed0aade8e3ab36bf4c0bd40f4	video.fc2.com
dd2ab62df5da52e66844171efc4415a087cc1a8c432312d814a62da582f40e2d	www.ontvtime.ru
ddf38cb97def571ec55f58d372db15fe6ee01578adc85b1087823d239d758af8	apps.facebook.com
e2f07d2fb0e6beac78d55962dda9ebcedba6c3ba30bf83b0880fae69d29537bf	www.totaljerkface.com
e35635613116ae9266c41348d2f4978f093c2fe75ae91f010ad23c1be31b833c	www.hungamatv.com
e39ce3cd42a88216ff9060e8b136bdc153f52322f259321a5925e629659684f8	edu.glogster.com
e4003a967100eb3a92e9148a51e7cd302e6ca4bcc34566c671378a4b0756ef66	v.pptv.com
e4dcd660eae7eeb1ea42050b6dcb108a9bedf1a66e3791438c6abe1efc907e1b	life.pigg.ameba.jp
e57c8c0083d4ea6fb4b390682d8ad3dffaeda2d37d1c11b9d29418b4a318e1a9	www.panda.tv
e7bce4b54da6dda25cabbe9da2359fe2833c94ec1ce3edd67077a089ed76ef31	www.vudu.com
e9ce06c9a6a05878802f64fac17399cc0a8452c652403445995a90dc9b19401d	www.nseindia.com
ef7f6be560fb99cff749ac35415beeed4aa86f40e10138858289dde1284661c9	music.microsoft.com
f2313491b771d1180f9c4e9cf979820e276a7833859555976dbf4a529cb2189f	en.ikariam.gameforge.com
f4f46a8b3a55ffb3e3784e6743266ed8d7cd2fdd21f494a82e2772fc68590d1b	www.deraktionaer.tv
fcb0eec77983791a7eeb971a2320f38cdbac2ca16cf3f418f83a00a4338eafd4	www.a1.net
fee3af1754656ed83ba706b46c6fa570b020ff79ad84b5adee4882fbf6adaf0e	www.poptropica.com

Nel suo report, Fratric spiega che il rischio di attacchi che sfruttino questa peculiare (e insensata) policy di Edge è elevatissimo, visto che basterebbe una qualsiasi falla che consenta un attacco **XSS (Cross-Site Scripting)** per aprire la strada ai pirati informatici.

La vulnerabilità sarebbe stata mitigata con l'ultimo aggiornamento di Windows, ma non risolta completamente. Microsoft avrebbe infatti introdotto il requisito della **connessione HTTPS** per consentire l'avvio automatico di Flash e avrebbe ridotto il numero di siti compresi nella lista.

Tra questi, però, c'è ancora Facebook. Una scelta discutibile, visto e considerato che il social network di **Mark Zuckerberg**, oltre ad aver dimostrato nel tempo di non essere precisamente "inattaccabile", rappresenta un calderone in cui chiunque può facilmente pubblicare ciò che preferisce.

Please follow and like us:

Follow

Falla in WinRAR vecchia di 19 anni mette a rischio 500 milioni di utenti

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/02/21/protezione-da-flash-se-lo-propone-facebook-per-edge-va-bene/