13 יולי 2015

כ״ו תמוז תשע״ה

סימוכין : י-ס- 136

הנדון: התרעה על מתקפת דיוג במתווה פקס

תיאור

- לאחרונה הגיע לידי ה-CERT הלאומי מידע על אודות מתקפת דיוג באמצעות דוא״לים המכילים, לכאורה, סריקת פקס.
- נושא הדוא״ל מתייחס לסריקת/העברת פקס ומכיל קישורים זדוניים.

מזהים (IOC)

(Indicators Of Compromise) - מאפיינים שנצפו ברשת או במערכת ההפעלה שעשויים להעיד על חדירה או פגיעה במערכות מחשב.

להלן החתימות הידועות ושרתי ה-C&C שנצפו בתקיפות נוספות :

(יתכן וחתימות מסוימות לא יופיעו כלל עקב אי הפעלת שלב מסוים, או עקב שינוי בשמות הקבצים, יתכן אף כי גם כתובות ה IP של שרתי ה- C&C משתנות ואינן הכתובות שנצפו בתקיפות שהתגלו)

כתובות IP :

- 188.20.86.186
- 86.39.202.101
- 184.107.193.218
- 204.196.242.115
- 204.196.242.34
- 200.125.133.28
- 200.119.128.45
- 201.76.51.10
- 203.156.161.49
- 208.75.241.246
- 202.76.237.216
- 209.40.72.2
- 200.125.142.11
- 202.206.232.20
- 210.59.2.20
- 209.191.186.196
- 75.126.24.94
- 183.78.169.5
- 121.193.130.170

Domains:

- expediataap.com
- dalfon.com
- fese.eu
- ppi.net
- sanjosemaristas.com
- frontrange360.com
- bigblueroad.com
- europeanissuers.eu
- airastanapromotion.com
- F1Tool@europarl.europa.eu
- seccionpolitica.com.ar
- pivotglobalresources.com
- getiton.hants.org.uk

תיקיות וקבצים (Files):

- atiadlxx.dll
- hppscan854.pdf
- .0647exe
- .2537pdf
- .6289exe
- clinfo.exe
- atiapfxx.exe
- .5283pdf
- aticfx32.dll
- aticalrt.dll
- atiumdag.dll
- Video.zip
- .6289zip
- doc853.pdf
- atidemgy.dll
- amdhdl32.dll
- atiodcli.exe
- atisamu32.dll
- reader_sl.exe
- .0647pdf
- .5283exe
- .6289pdf
- aticalcl.dll
- .8634exe
- .2537exe
- .8634pdf
- atidxx32.dll
- atiuxpag.dll
- ovdecode.dll
- atimuixx.dll
- .3852exe
- atimpc32.dll
- aticalrt.dll
- atiumdag.dll
- hppscan854.exe
- eFAX-854.zip
- coinst_13.152.dll
- amdocl_ld32.exe
- amd_opencl32.dll
- amdh264enc32.dll
- amdmiracast.dll
- amdocl_as32.exe
- amdhdl32.dll
- atiodcli.exe
- .2537zip
- .5283zip
- doc853.exe
- aticaldd.dll
- .3852zip
- atidxx32.dll
- atiuxpag.dll

- atimuixx.dll
- Video.zip
- ovdecode.dll
- aticaldd.dll
- 3852.zip
- .2537zip
- .5283zip
- .6289zip
- atidemgy.dll
- doc853.exe
- doc853.pdf
- .3852exe
- atimpc32.dll

מזהי MD5 שנמצאו:

- BD2EE25383F95B65E39AF765FF9D8F05
- 972167F10642DB5C32DAA3B678017E98
- 19D22033BCDE42E4E4D26725D8A5C21B
- FAD89E154297772778EE3AF8D8190CB4
- 0C53A6290E505DFCE03D6662CD7B5D11
- B898D6FAFA7BE9002EFD6CF5D4DA4D98
- A3208ABFA33C5C12FEE5812D9F84E252
- DA311C2005E7580C662D1911DBEE49C0
- 56729E5170A93A4C790C707284BA05DF
- 491FD23AE9AF784114B887BEEE7465C0
- 416DB420E781C709BB71ACEE0B79282F
- 556B9ECA4A85F52E2F3176C306E18661
- 8670710BC9477431A01A576B6B5C1B2A
- 83F57F0116A3B3D69EF7B1DBE9943801
- BFE93862514887B8BE272E01CA1F4334
- E084A992DD25E7420ED98DE84094B132
- D5B10B1EEFF8E83D3480CBD05B8718CC
- 54C774CC16725868712E344D80BCEC30
- 9AD55B83F2EEC0C19873A770B0C86A2F
- AE505C295FC0F98C10AA08577FB9FE00
- 45D6515EBB7F57404B8703F1E77A461A
- 1819EFF02C4FD5B30771EB89CAC4FE69
- 95B3EC0A4E539EFAA1FAA3D4E25D51DE
- 68271DF868F462C06E24A896A9494225
- 69CAB1853DF0749D42B68BF41D78E655
- 3101D619E195F8863F272398F3B3AD92
- ACBA9C3C0C9D963AB1C80E9AC64B2D5E
- 001ABADC1F78D5A7E897B5F7A02B01CF
- 31A1E641893FFE3AE0D75B52BC02B296
- A5D6AD8AD82C266FDA96E076335A5080
- 1DDE02FF744FA4E261168E2008FD613A
- 08709EF0E3D467CE843AF4DEB77D74D5
- 5EBCE6CBEDFEC82F1428C3409E3DF0EF
- 10B852B9F669AA6EC60BC838DBEE6DE3
- F16629AD4BC9473EF4978D6A3DD551F1
- 864BB9137F6BF94E59FBAA9B21065D1E
- FD8E27F820BDBDF6CB80A46C67FD978A
- 305D9106B8BD836B4E31B390CABD0CE1
- 52474B705610245F67BBD1C86AB8BD7B
- D9703D014C5D4F55E2996F3573544476
- 93176DF76E351B3EA829E0E6C6832BDF
- 6AC90156CA39CA1457C65C1E6CB9429D

- 209A4A102A977B698544C99D8236E9CA
- 62C4CE93050E48D623569C7DCC4D0278
- 330ED7549D50BDB56497A5577132610A
- B4AE6966E65E47AFA41610B1FB554607
- B5553645FE819A93AAFE2894DA13DAE7
- 5FA3C3DABB8EDD601302D9CF02DB899D
- 181A88C911B10D0FCB4682AE552C0DE3
- FE17934587E41662EF6FBD7708023733
- FEF254D6C46FDCED294DB44ACEF8D839
- FC6772572B884A849BAF100E7FAF2E00
- 50992EEFE5DF1C85DDE85DC008B5010D
- 037B1E7798960E0420003D05BB577EE6

URL:

- http://expediataap.com/promo
- https://200.125.142.11/news.php
- http://dalfon.com/serviceplans
- http://expediataap.com/Contacts
- https://200.125.133.28/search.php
- http://diplomacy.pl/eFAX-854.ZIP
- http://bigblueroad.com/whoweare.html
- http://bigblueroad.com/index.html
- http://pivotglobalresources.com/about.html
- http://pivotglobalresources.com/bestpractic
- http://www.seccionpolitica.com.ar/galeria/in
- http://pivotglobalresources.com/services.ht
- http://www.europeanissuers.eu/fax/8634.ZI
- http://airastanapromotion.com/about.html
- http://www.tafex-trade.eu/eFAX/5463.ZIP
- http://airastanapromotion.com/seats.html
- http://airastanapromotion.com/terms.html
- http://bigblueroad.com/ourprojects.html
- https://200.119.128.45/mobile.php
- http://dalfon.com/about
- http://expediataap.com/about

כתובות דוא"ל:

- noreply.mfp742@gmail.com
- noreply.mfp3035@ppi.net

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר.
לכל מידע נוסף ניתן לפנות אלינו.

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,

CERT-IL

טל: 03-7450801

team@cert.gov.il