31 אוגוסט 2015

ט״ז אלול תשע״ה

סימוכין : י-ס- 151

הנדון: התרעה על פוגען Pony

תיאור: לאחרונה זוהו על ידי ה- CERT הלאומי מספר תקיפות באמצעות פוגען Pony. Pony הינו פוגען אשר משמש לגניבת מידע אישי וסיסמאות לצורך גניבת כסף וירטואלי כדוגמת BitCoin. הפוגען שולף את סיסמאות המשתמש מדפדפנים וכן מתוכנת הדוא״ל של המשתמש במידה ואחת כזאת מותקנת על המחשב הנתקף. כמו כן הכלי שולף נתוני הזדהות FTP (File Transfer Protocol) כגון – שמות שרתים, מספרי פורטים, שמות משתמש וסיסמאות.

לפוגען אין יכולת להתפשט ברשת בצורה עצמאית. לרוב התוקף מפיץ את הפוגען באמצעות דבוקות בדוא״ל אשר מוסווה כדוא״ל לגיטימי בנושאים כספיים (הודעות בנקאיות, קבלות וכו׳).

וקטור התקיפה:

שימוש ב- Spear-Phishing לצורך שליחת קובץ Word זדוני למחשב הקורבן. בעת הפעלת הקובץ מנוצלת חולשת CVE-2014-1761. החולשה מנוצלת באמצעות מניפולציה על מידע בפורמט RTF הגורמת להשחתת זיכרון ומאפשרת הרצת קוד זדוני במחשב הקורבן.

CVE בשימוש:

- CVE-2014-1761

אינדיקטורים (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:

- 5.63.154.158
- 5.196.241.203
- 8.19.117.22
- 23.29.118.23
- 31.41.42.119
- 31.184.192.214
- 38.84.134.207
- 46.4.145.94
- 46.30.42.177
- 46.30.42.234
- 46.161.40.108
- 46.166.168.79
- 62.75.196.124
- 62.76.179.132
- 62.173.145.8
- 67.215.66.146
- 77.246.146.74
- 78.46.236.2
- 78.136.221.141
- 79.124.13.18
- 80.78.245.84
- 84.19.176.23
- 88.198.231.109
- 89.144.2.154
- 91.194.254.82
- 91.194.254.224
- 91.194.254.236
- 91.200.14.95
- 91.203.5.186
- 91.217.90.137
- 91.219.28.5
- 91.220.131.16
- 91.220.131.17
- 91.220.131.109
- 93.189.42.18
- 94.242.57.106
- 95.128.181.236
- 95.211.197.232
- 95.213.147.98
- 104.207.150.236
- 104.236.11.88
- 107.170.217.209
- 109.234.34.57
- 109.234.37.184
- 144.76.232.44
- 146.120.110.147
- 148.251.34.82
- 151.80.72.64
- 151.248.113.8
- 162.244.32.164
- 176.31.66.130
- 176.103.48.223
- 176.103.49.219
- 176.111.63.100
- 178.208.78.76
- 178.208.91.229
- 185.8.60.231
- 185.17.121.148
- 185.18.52.127
- 185.18.53.247
- 185.86.76.168
- 185.87.48.200
- 185.91.175.94
- 188.120.246.249
- 188.127.249.198
- 188.138.108.153
- 191.101.20.165
- 191.101.21.219
- 186.202.153.66
- 23.97.148.253
- 188.128.153.43
- 216.157.102.137
- 46.249.199.41
- 107.180.2.4
- 107.148.178.215
- 125.253.122.98
- 136.243.224.51
- 78.135.109.246
- 142.4.4.208
- 193.36.35.78
- 193.169.86.174
- 194.6.233.37
- 195.62.52.35
- 199.59.243.120
- 206.54.183.106
- 213.152.181.66
- 200.6.114.204
- 50.87.151.101
- 107.180.4.110
- 91.221.36.140
- 91.221.36.165
- 91.226.212.142
- 91.238.83.110
- 92.63.96.8
- 92.222.98.108
- 93.170.131.30
- 93.171.202.158
- 93.171.202.172
- 93.189.42.8
- 193.26.217.209
- 91.220.131.241

Domains:

- pebulelet.ru
- herstianingun.ru
- samanthabakerhealing.com
- ortandahan.com
- padetitdidn.com
- pardijusat.ru

- unlimited-loggers.us
- behesjusrat.com
- thenjechap.com
- parterledhed.com
- toldronher.com
- trash4docs.com
- servo-maszyny.pl
- trashdocformat.com
- allen-tools.com
- moskalskiybodun.com
- dkpconsulting.com
- faststornet.com
- invoiceseclib.com
- yantzu.com
- sibrico.com
- ruyalwayaco.biz
- www.starmine.cl
- rotadosol.tur.br
- www.faura-casas.com
- www.candmaccounting.com
- congtynguyenbinh.com.vn
- www.bscdragonboard.com
- aningritoron.ru
- aningutterbut.com
- appridefirstcom.com
- arwahengo.ru
- atorrenevent.ru
- banqulerroman.com
- butledtinve.ru
- continental-transit-mail.com
- continental-transitmail.com
- cyheckledand.com
- dcfastgroup.com
- deadfishup.com
- debulittro.com
- destnarrowweek.com
- doclibrarymk.com
- docscountry.com
- doctrashformater.com
- document-fast-cloud.com
- document-organizer.com
- document-qiew-online.com
- pasnirthland.com
- pizdetshuiovosboduna.com
- podvigtitanika.com
- poly-poly.net
- randomwfu365.com
- ranrianinghers.ru
- rearmheadfire.com
- rebettheligh.ru
- rebledughid.com
- redesparda.com
- redwithtertreb.ru
- renrefhedked.ru
- renwitedrom.ru
- resqdocsfirm.com
- resughesaning.ru
- righthetoneca.ru
- rinheckguny.ru
- rosupletwas.com
- sabotierfirst.com
- salecheapflight.com
- saloross.com
- sampledocstrash.com
- secureinvoicedocs.com
- sestoreinv.com
- shareinvoicelib.com
- smallconfigs.com
- sofforjeclet.ru
- somedocushare.com
- sparwasssinve.ru
- starinvoicemodel.com
- talahedtug.ru
- tanhadhidown.ru
- thenlouldnot.ru
- thettoortoft.ru
- ticalharked.ru
- titanikvmoskalii.com
- tofthenningref.com
- toldbiledin.ru
- toldontinwi.ru
- tonecarighthe.ru
- tonsulddijus.ru
- torsmimyred.ru

- document-searcher.com
- document-view-online.com
- documentfacilitysec.com
- documentsecurestorage.com
- documenttargettrace.com
- docustoragebank.com
- donquertofear.com
- doqument-view-online.com
- dortehthisnet.com
- dortwindfayer.com
- dream-hoster.com
- durtixfanew.com
- etritanfe.ru
- eventjohnmihim.ru
- faetsandrep.ru
- fastdrozdfund.com
- fastserviceworld.com
- fastssamplestrash.com
- fenesihert.ru
- ferginestor.com
- fifibabok.com
- finder777.com
- fohenroprab.com
- forcaltonttof.com
- fordahecbet.ru
- formaterdocstras.com
- fortgureket.ru
- fortuldryhow.ru
- fuckingsfish.com
- funnyinvoiceorg.com
- gotthendiran.com
- gowasstalpa.com
- gutotdolo.ru
- hapbetrowpar.ru
- hapwroncihen.ru
- harropthenthe.ru
- hecunvelac.ru
- hedattoftle.ru
- herssofhaprigh.ru
- hetonshanver.ru
- hisruboti.ru
- ie-form.net
- torssedbabbe.com
- trashformatdocer.com
- trbestbuy.com
- tumanimoskal.com
- tumanmoskalskiy.com
- tumanvmoskalii.com
- ughimsinna.ru
- ughwagerew.ru
- uldhowhedtca.ru
- undmiredhem.ru
- undvemofo.ru
- uttejustrep.ru
- utwithdehan.com
- veetdohi.ru
- veronefosof.com
- video-promo.org
- wantools40.com
- wastolddinghes.ru
- withetborom.ru
- wituldwihow.com
- workwithdocuments.com
- worldshipone.net
- enherthadugh.ru
- rofhanrighhen.ru
- tontuldverbab.ru
- wrononeratwass.ru
- myfishdown.com
- myrorecrab.com
- mystoredoc.com
- mytorsmired.ru
- nasedrontit.com
- navicompany.com
- nestorganje.com
- netshipgroup.com
- newstratospheregames.com
- ninghaprewrof.ru
- nohissandbo.ru
- notleftrofugh.ru
- nycosedfor.ru
- ondereteveng.ru
- leftterbutbet.ru
- lerentoftjohn.ru

- iecomp-mail.com
- infelitthec.ru
- infodocslibmanagers.com
- inpahauld.ru
- integrated-express.com
- intexpressform.com
- invoicebankstore.com
- invoiceformater.com
- invoicelibrary.com
- invoicewindow.com
- ireqinvoiceparm.com
- johnmiheventim.ru
- justhegthathen.ru
- logmein-security.com
- logottitne.com
- maininvoicegate.com
- manterinvoice.com
- manydocsfastrack.com
- menstoreins.com
- miafast.org
- midehefo.ru
- modelstarinvo.com
- moskalvtumane.com
- mostotransfer.com
- mydocumentsholder.com
- kesedrathow.ru

URL:

- hxxp://toldmeuselo.ru/gate.php
- hxxp://forttalterhow.ru/gate.php
- hxxp://righromonhen.ru/gate.php
- hxxp://fadingsandjus.ru/gate.php
- hxxp://tedharhepret.ru/gate.php
- hxxp://robrataningred.ru/gate.php
- hxxp://sportsacademy.co.in/panel/panel/gate.php
- hxxp://saningkedhanrigh.ru/gate.php
- hxxp://andwronughwith.ru/gate.php
- hxxp://sonrepkewa.com/gate.php

MD5:

- 076a73d9bc4326dc9d85296a02fea8f4
- f4df81bc3151e1e862ed30c597f7638f
- f43ab4f343867682104361c6bbff12d0
- 337c94bef406ab27d398d8cb11087a41
- db7883926e202f59dc07864841bcf462
- 68a2237f55871c51ac48fae06eae6709
- 3f08f668f3f9bba7a5fec569ae6a8651
- 9bdc589eb47aa11992737dc1debabb2a
- 3e5191de0f62fe1ffcc210fb56b2738c
- c09d8ec08208a16b41e0beaa812a4c6e
- 9b51d81c32ae3b709c08feaea5e10704
- 383dabb25240be1a20dbd2793d60c4f7
- 479164bbed030446d3b08e718789edb7
- 5f5abd0c5507bd62dd63400af4be1e8d
- c295963453a26ed1a3604f4082ecc90a
- f0bd2d03ca3f61b1f407c7bc7db439b3
- 243dfd99146fac38d1e22e90e8fafb05
- 7dc9770adead1c42b1e85c8341dbe1fb
- fdf2b4a03d829f0a4609b3e569319c82
- 8c62d43ee165859603c532beecdbadde
- 570cd1165867ed5959505ddef7181c70
- e7666efc0761575ccdb5880a1b7465b6
- ee2c37e042c83a838c44e167c3a17b34
- d70a4a7aea97a215055b4688ee5babab
- 1feb08ffd937d3422df09aee75f8bfff
- 20b469f31855d481e8d2915a847c42e5
- 592ec4221dcc29434303d8336f49c29b
- 507ec9380858996e536a608c072c8584

- 7c86c775b747b0822c61bde92ad2778b
- c1908d434318e66ca14bb123f47f9595
- 7b9f0ec04d9ea12ac8f08ab04189553e
- 16767c9c918831d61daa28fa325b933e
- 2286b884c3782b342097c31e88084da9
- 2972c1706b8b37d717b51d38cb4bd9d3
- a6b760343bc8cae5bff9ecb2b60441a4
- cb34c8b887c32c15ee4bd9c91b4571d8
- 1d2686ff1c20644963b17ff43645270e
- bb37735d1162ad7430d1f194ed8adc5a
- 8b59a1229aa72bebb46f2503a4607461
- 20d7facbd11a8805a562d5d588817fc4

SHA-1:

- 2a1a0eb2b6071c56f25c4304c555da350d67c99a
- 3f548e9f4f8b1c1ee9341055a75345e1d2b4358a
- 5b85b8cd91539f19f0d0cb2fc692722bc944f32a
- 8ab7df1193c9a3f6ad33426b634c581939dc9281
- 12cb416b69ffc56c12aad92f95040603261dc217
- 83f1b17fb18fc0ad14ce1bbf2a5d165404edef93
- 92d4c9117fb2fe48333e71822e433807fb5198c4
- 496f84635f216e93d9661a403e43ff1903a2a2e8
- 4398c2b731f4939414bba70aac5260ff1d1ae865
- 93327b8105ea5f67a5a5bcb3ffe9b8cbe75185d0
- a7c016bee0766f57f6a977f248c45cf06de5ab00
- b2abfaa9d14435a5b079b847a039b57b4036836c
- b4a3ad2992af82d739d4eb110fab6966479ffd62
- bbece44ad7d76ffc70239cc97f5238de01ce6ccd
- c707f688eff865b1f40dcb5dddd130b508d8e589
- d3ab3f733ad076546abb7debc3c79575083ec6d0
- d9d9ba96bfce361002a7bec53db95390f72c3e0b
- de5cdbec6ce4a38f9938944aa82fe8d30ae20171
- e11f512fb681ec2c5333da75dcd64f28bcfa5e3c
- eecbe32d493d3a5eaef2d6720e0d0cdfb8bc175c
- f1fa5d774901995234fdfedb562953c6ed4c9eff
- f6d69a32f36e3d2e8a2b69acfd932e04ed3d2002
- f13fa4951edddea82255db0de91a0c17f1b947b1
- 1f5be0bd8fa955cfd11be6fb35210bb398eed193
- 8b6619e4d4ef2297a18e8dd3aad9dda93883d574
- 071b754bffa96101bf8c563ad7efd4df3f221b2e
- 462fe924876597a9396999dd24773e8ed9746997
- 653cccc1daa752da24a9afbdad0449baae07bf1c
- 4011a69c7dcc5d1f903f2f777fb3e35de748c8a3
- 8422d870ebcafeb6c51142f1a95cc5b8f64b43ba
- 48593abe9a8543c9183e375fc185fd97c28f3549
- 61481016dace6765a485f32fd52760b2fb9b95ec

- e9c2d14bd123fa727ea5691c21374e88e95f877d
- dda088b93f203845bca009a850b89b3a2cdf3538
- edc9c1929ff20950b99c42e22f3f448591351ce4
- b31423f986f562ae2070b5d103435a2bd0783762
- dc31cbded9d2afc0a8bcf9eea731712abaf12dfb
- 2ca92663a66a5b2047a921f746be56674fa05631
- baea5192f69d7942722138445ed74c5a9909d255
- ee051a2a04c0caf6ff81db0542ca3fa35b05c7b4

SHA-256:

- 91185c6e0e55ab114e7281067a4d13c047d7a45aa83f60c1c840668a18a16c61
- d20e63c7a1f3f4a2ab8a2a5f301fbb6c2075dfbc5eece828273fe38cb3f87788
- 2bad191f52e505c40bf0615a19e3e465a4f49c553a22a6566bdc2e251045a31a
- 192b44b56424984bf7df8ef44f00c2735cfacf077ead36a5c1644ba5db00ffec
- c953e7561f2106e2180a402bb9fc094bb9a667ed308feab2908a0976c373e262
- d89af60d8f4808e53b42b40cc70cbf6296283332c65ee35f8bbff00bf1abbdc6
- e498f932f6b02b5067a52ee78e574b3722970bf91062b293d3e9973d6bb28e01
- 0cede6e53dbdf04f5af86203dfc4911115c7eacc774f2c3073c2d6ae7625eaa2
- 1aac2417be978ba1cd5ad7a306a71ce6f018f103a1f0aa79149e55bb308af5ca
- 4256909788058b7c5a4d86bdbfee71d7e3fd11b9ad6d887b75f11cb5dd483f7b
- 799abe16ba0450a7c3cc636b8266f35c7fcbb16b33602a582af3ee67342f7111
- d6f4e37f77d7bf69922793f2db5b0459df8708f3bd3f2edb6f5ecc707fbacaf2
- 81e02ba8c11e31924db819ff5d07bdce60b28e7937414be4a48af2edb5150306
- 2577ca0019b1dffb245664f1108303bd44a1d4ea4f3c7f6db6a138b8a3a8c21a
- eeab19dfc4f9bce9fc3af8022659739d51bb9eeac6a535d35d883aa977fe43bb
- 9263b30a0fce35b4586be316d5f2f91dd96638402bc683b458ae47d5276d2a21
- 40450ddd0c9c0afbf067464f1e69e5cbaad0c7d59a32c47fb1bc77fd31a7249d
- e6d937bc005052781da6c32816b427d86429766901f20c98ca6f0010fd71777c
- f68398589b80dabc714fe67a78cd10e5dd7e396d8fbbd9e806ee81315b302428
- 0da4a1fad6f8f239bbb2a9424cc990cd0f157bb2c46eb45300db4b7d37c82b34
- facc9a5f02e8d18c9cbac9ee760ffa38b2854e5d5c89a529e368be8857bc55a9
- b9cd2fcfe6550c3a6b64466ce786b9f28ca9efbd0945547d269222d8811f3d0a
- 28cc1c484e61cf9486725ad5b7f8bfd13fadb5e16d08e2430cfac37a1deec57a
- 5fb9e66744b72d928db335ef97f649ab84dfcc304ca49cd9e2311de9328a8406
- c6fdd7d62549c47b17beab67e5243c8aae47c10fd1eec38f652348aae15f0688
- bed8a7fc2b724593d8695be76607ea7129725c57c3fd21be2629c3f7df4381a7
- d91f608cd30d22fca65a1ff90805f46faa65ffa8335dd54cbe54ed08e0574e83
- fec402d83ee5d29707c749b9c2b74fe438e39f53f3ca464180335448e0fcb9ce
- c50b9668a253fcae81a51490b0c5ecee4d33ce044b61256053a9704cd43f74d0
- 0e71bb693affd72709f2dc29c3a34e1cb22b7513b1b4c941a0fc4af4fa52f643
- a61d316b92a96570fa552c225840ba3aaa64e462b566cfbd1c1316449e40f6a0

- bd681b5180050347e05c83603b6856f188734003965ccc4e8ae7a08e446c9d22
- 2aeb22de92fa72c47ea11937396fd95dfa1ecd6a488bb147c9f37ac27d95ade7
- 56206ea9de0381486bcda6c1fe4d29d0f1da48113cfa3fd7f54a531f45dafb2b
- a4398453c7ba07b88ad96cfedaba3c1910f965e5f139d2788afe820c14d44b39
- 8290bbddc108323037e273ba80b0fd0db97473e1db44f96c911ca7166db1f0f7
- a55e5f1cdcdd5203da5e18148c85d7249396c899bba47584fd65c31be1f52a6f
- e81aaf2c6fde03ee86a269cfea4e3956ad859bd24892fc264b1223ee7f3b6140
- 7faa4c2cdf029707289637077a48710cecd7624cdc7366b154e3881c3c5c5608
- e9354a199825bed552754b84745a8208d7f5de44344ca2ac7856914f02e81a6d

קישורים ומידע נוסף:

- חולשת CVE-2014-1761 באתר Microsoft

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