קשר דייגים – IOCs **מניתוח** **ראשוני**

**כתובות :IP**

על מנת להשלים את תהליך ההצפנה הפוגען מנסה לתקשר עם אחת או יותר מהכתובות הבאות:

* 82.94.251.203
* 76.73.17.194
* 208.83.223.34
* 171.25.193.9
* 212.112.245.170
* 193.23.244.244
* 194.109.206.212
* 154.35.32.5
* 86.59.21.38

**קבצים**:

* 68120519.exe
* 958189.od
* 59637965.od
* 60380576.od
* CVR9EED.tmp.cvr
* CVR55A0.tmp.cvr
* CVRCD.tmp.cvr
* Default.linkapp
* Temp\_cab\_67811310.cab
* Twain001.Mtx
* TWAIN.LOG
* Twunk001.MTX
* oeqoycd.exe
* %temp%\CVRF25F.cvr
* %temp%\ytauxki.exe
* Decrypt All Files pwcvceg.txt
* Decrypt All Files pwcvceg.bmp

**גיבוב Md5:**

* 624eea98cd6fc090cf5ab6d8b353a95c
* c2af192a3d441478abfb7a22a1e85a77
* e6b9e1596af5632fc6102e7a9f75e9fd
* 44d8d9d30ea0d696134dee3f76d70122
* 38044f2f95cabc4e1e3d0ce46afd0d69
* c2af192a3d441478abfb7a22a1e85a77
* cf9d1bad9aec70dbb2dc864b38f10e22
* d1d356d9c9e4a417ce3d6871dc1781de
* 2c40005e51b86c263bfe30db0f647991
* a1ca06a3cbe3bef689db71c754235e6a
* cd65f83852eb6d739e8d74fdc42f6761
* 9cff5af851a145f78b1bf9f87debe8cd
* e60eea4b624c0f7a28ce6cad89da8f6e
* 4ece68d0ac97c8c313f04877fee82b31
* d41d8cd98f00b204e9800998ecf8427e
* ae1e6f12a7b8193f3bc2cdfe42b20645
* deeb642a21cbfc4ce1ae230ec7483784