

# Indicators of Compromise

## Domains

voipasst[.]com  
voipreq12[.]com  
telecomwl[.]com  
crm-domain[.]net  
leads-management[.]net  
fxmt4x[.]com  
xlmfx[.]com  
telefx[.]net  
voipssupport[.]com  
trquotesys[.]com  
extrasectr[.]com  
veritechx[.]com  
quotingtrx[.]com  
vvxtech[.]net  
corpstech[.]com

## IP addresses

193.56.28[.]201  
185.236.230[.]25  
5.206.227[.]81  
176.107.188[.]175

## LNK

db5d09edc2e9676a41f26f5f4310df9d13abdae8011b1d37af7139008362d5f1  
3b7cd07e87902deae4b482e987dea9e25a93a55ec783884e8b466dc55c346bce  
c7cf5c62ecfade27338acb2cc91a06c2615dbb97711f2558a9379ee8a5306720  
f5f79e2169db3bbe7b7ae3ff4a0f40659d11051e69ee784f5469659a708e829e  
cff5ed4de201256678c7c068c1dbda5c47f4b322b618981693b1fd07a0ea7e68  
83c375dcdadb8467955f5e124cf4e8d6eac78c51c03fb7393dc810a243ba1a90

## 0.js / media.js

4ce0954ca7173bd696afe8f44bf48027b3d4d630c0cce414b95d6715e662b5fb  
0d7dc074be83f1096f39ba95bfc4e1a17c411dbed0e5eeeb48e88a12d79b541c  
4e396586fd6dfcc24686aae73ba5c336939ee7a7aa9ffb76a1f78867926c6e4b  
5aa1109d057e830d6f3faf4b6ff6f69075d158dadb5f46794b3e07685922d09d

## ddpp.exe

25c119a7ee5b53212b5992992907a7772610b491ce2992c860dc206d0f3f844d  
e678ec3dbccfbd5cf0f303d2841e726ac7628044de5297bf9ebe791d66270a2f  
a81f152a31c03b45dbcf29439050bbe080b1f6308b032aebc0205886d1f41e5d  
6136309a207b89ccd423f8c087a9cdd633d8f5e78b8ebd576b7750b49274c532

### **fplayer.exe**

0c920e7dfdd0028d9d15344c2e9c64ae57c2c9417dc7b22b865fdfe0cc0b8b1f  
79e21ff9142821b2e3d6e3dc8d812e86da231dbbd1217415b4add748a4c1ce3c  
c4b90fdec0848ad68abe18a42889ec0e5e45b7678afb0353fedf53915b76275  
79e21ff9142821b2e3d6e3dc8d812e86da231dbbd1217415b4add748a4c1ce3c  
4574239efb728913fd379cc914039b1d7fa8c3ac8d6e3503d6f5bc73de504c96

### **devAHJE.tmp**

79b032dbb8ade21b97be5dcaa63c974b6cddb3c6f32b4abf2872288ae43ea4a6  
1a3f39dc604dbca691aefef1d5a372fbca3650003d4145671525a2960e1239e  
bdc20527d5afc4f13fa45c9182c8f58eb88cb4edc76aa38be83d95fd3365ce0a

### **Dropped PDF**

048388c04738763c0ec57124e3a88fc82a545639636fb5ed6cd397881dd6ced9  
11d9a87b144c0eaf71e8dea1b08117d464ed7f24a6e716e935e0c7f3a7e03edc  
0b95c8c70d2dad47baef15d0299cd7e273e8a59ae0420921632b21789a80aef0

### **PyVil py2exe executable**

f388a2ebbb6a7e577e8aa6205e87d5b2975e7c08464123cc36e8e3d437e9a523  
130e0536cdb4e9f7cfb273dbabc9ee196a51d1217cd4b981847af6314f46b052  
d6343a07357e5443d6a59f10e16a06796c46bec3cbe5968ac04b0f082d6fcec

### **PyVil first obfuscation layer**

568ec03a27740f8babc3513948a44ce1a2944d05f3d454ce345e67a0634a4a73

### **PyVil second obfuscation layer**

63a4b6ef72e0a3a0886364a5ebcc0009c6da8c27d93cf9d6c8107b6f025fed34

### **PyVil python libraries**

1aa9ecb83acbebc64b23f7192e763cf4bd278f10df2223512087b87230e411b4  
9dfb040dab1fd05fbccf69ff3461295815edc463a61a6304af18a72f82bce534  
8dfb2f5c74f38ff39bfc17bf6a62d5822c458215619c1b2ec2eb345f21d1265  
3f3738e4606ea85a382319269405ee72a928a8a761273914c52342b116cbddfc  
a787ecc380021b3b7115c97242ba06706a0a1e41efe1b734552d74384bae22ec  
062ed9f40ca330f0fed63cbdd401521deb23f93b5527038fc88f70ed9acadf39