When Threat Actors Fly Under the Radar: Vatet, PyXie and Defray777

unit42.paloaltonetworks.com/vatet-pyxie-defray777/5/

Ryan Tracey, Drew Schmitt November 7, 2020

By Ryan Tracey and Drew Schmitt

November 6, 2020 at 6:15 PM

Category: Malware, Ransomware, Unit 42

Tags: Defray777, PyXie, Vatet

This post is also available in: 日本語 (Japanese)

Indicators of Compromise

Cobalt Strike C2

192.169.7[.]160

51.79.42[.]156

5.135.230[.]132

162.216.240[.]7

172.245.21[.]224

192.169.6[.]180

cloud[.]falconoasisdubai[.]com

syvansoft[.]com

gue[.]life

m33[.]bar

j3qq4[.]club

PyXie C2

sarymar[.]com

benreat[.]com

planlamaison[.]com

teamchuan[.]com

tedxns[.]com

mustome[.]com

hekutn[.]com

safealyzer[.]com

bookrah[.]com

c1oudflare[.]com

Defray777 SHA256

4cae449450c07b7aa74314173c7b00d409eabfe22b86859f3b3acedd66010458

Defray777 Linux SHA256

78147d3be7dc8cf7f631de59ab7797679aba167f82655bcae2c1b70f1fafc13d

cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849

PyXie Lite SHA256

5d26300ad2fc008fe278f17f98f173236c8bd7eeb6382062d677d1d6fd37c5b5

82a2149aa09b2b59ee7c97e05d7200d4ccbcd8444182aca2f8c4913f1f59a42c

0ad10472f7aedfd241ecb65a53d5cafdeb94672d92883d161cb37f769e60f013

61b9b7e1329eb540dd751d1db6c00cc45d91b6f58db75ab0212976d4ec4c848e

84428ece8efcb6298435b15d3c4ea281592accf0990cc840ef3a7a0644191061

4d0176e2d6e30e31352f420a4dec79d26cb00f1e6c789b31e84cd05eb4d50956

5e90a331bafd98e41bcf36419c44bd7ff8296ac18cce652e944ae22db15a5366

fe564fb38a99dbb94cc8a66d8955b0b7f8e67bf0a5eb820c4a5d0c3efb96c1e5

b2b3a199291c3651b1d7413c7dba92566a893010a50e770e1802f173f1c2c7a4

5736e167e234e06b33e8d8d6bb80e13b1bacca8d7cd3271695220cdec2e4a79e

a7affc0d93e27165ce44c55ae28189e8b55967443f9e464232f230ab4ba175ca

b3c6f365819864340a8a8fe3076fb326c1debfdbbc826384cb2978aea82edc48

c7ddbc24a57d1353d73533c47a65e5e3a74e3b666c1fed685fc90de1f089c72b

510cf6e1c55a190490e93d222ea606ed888d222ecedda18bfb2f32bb73f33cab

f80bcc60e79b387f63edfe0f1fc66492af4ff201ad5eb8080b1249ca43f6f30f

6485bec374f255831b7ddbfed9925e988dcd7e893f610842809dd7cd1988cffc

c58f5b3f7300a13fd9a0a61757e20399fc5e86544befdafae15e8809a02c2db0

9847cea40cec394c947de06010ad1f3033316903b5c822ba16f9574acb30f0cd

PyXie Lite Command Line Argument

-q -s {{**<GUID>**}} -p **<NUMBER>**

Pyxie Lite Exfil Staging Paths

%temp%\tmp**<Random>**\wifi_info.txt

%temp%\tmp**<Random>**\software.txt

%temp%\tmp**<Random>**\screen.jpg

%temp%\tmp**<Random>**\pwds.txt

%temp%\tmp**<Random>**\general.txt

%temp%\tmp**<Random>**\disks_info.txt

%temp%\tmp**<Random>**\desk_files.txt

%temp%\tmp**<Random>**\cpu_ram.txt

%temp%\tmp**<Random>**\arp_a.txt

%temp%\tmp**<Random>**\cmdkey_list.txt

%temp%\tmp**<Random>**\cpu_ram.txt

%temp%\tmp**<Random>**\disks_info.txt

%temp%\tmp**<Random>**\files.txt

%temp%\tmp**<Random>**\general.txt

%temp%\tmp**<Random>**\gpresult_z.txt

%temp%\tmp**<Random>**\ipconfig_all.txt

%temp%\tmp**<Random>**\ipconfig_displaydns.txt

%temp%\tmp**<Random>**\mimi.txt

%temp%\tmp**<Random>**\net_config_workstation.txt

%temp%\tmp**<Random>**\net_group_domain_admins_domain.txt

%temp%\tmp**<Random>**\net_group_domain_admins.txt

%temp%\tmp**<Random>**\net_group_enterprise_admins.txt

%temp%\tmp**<Random>**\net_localgroup_administrators.txt

%temp%\tmp**<Random>**\net_localgroup.txt

%temp%\tmp**<Random>**\net_share.txt

%temp%\tmp**<Random>**\net_use.txt

%temp%\tmp**<Random>**\net_user.txt

%temp%\tmp**<Random>**\net_view_all_domain.txt

%temp%\tmp**<Random>**\net_view_all.txt

%temp%\tmp**<Random>**\netstat_an.txt

%temp%\tmp**<Random>**\nslookup_typeany_userdnsdomain.txt

%temp%\tmp**<Random>**\portscan.txt

%temp%\tmp**<Random>**\pwds.txt

%temp%\tmp**<Random>**\route_print.txt

%temp%\tmp**<Random>**\soft.txt

%temp%\tmp**<Random>**\software.txt

%temp%\tmp**<Random>**\systeminfo.txt

%temp%\tmp**<Random>**\tasklist_v.txt

%temp%\tmp**<Random>**\wmic_process.txt

PyXie SHA256

70dfa6b21f5eea28ccb77ddac876cf6eac58b2ac55ab7b9ee52d79b1b5f3734d

8d2b3b0cbb32618b86ec362acd142177f5890917ae384cb58bd64f61255e9c7f

260be87cd75f304272094d3bef02eff6ef6b605f01ffe2983361e6e2f6116769

09bb81e5a6c716f14c625ff36beb3b184d0089ed29252af10635b604b69f22ef

70dfa6b21f5eea28ccb77ddac876cf6eac58b2ac55ab7b9ee52d79b1b5f3734d

744d0c4b89e1b2ddd70d614b4dc009afa8f3a528c821c371cf72e60cc3367f19

37268f0ade3050fa2008b546920c4f2052732c092de04a6e108257f5de22ff48

80bd15267756343f028cbe77afe810068b0e6a36ce32f52be63f620ef5b5ed89

e2d4aa8662b3db2f3857dbacada1ff0da0ceaf75bbba579bc5ef1a555c065206

aed5b487e13e920835b0ba5ca964e25a815f8a10011d8e1eb29278ae254771d9

f9da4d61344457c3d68ef0525139c2cf6ee28d3f09220168ba2be601b5c54d6f

e03680e0af40a6fa1a12bed2f701c6137335d28b3d222579552658e951cbd13c

e2faf6586f8ac70cd98e4ec648f79435bfabaf84d440044aedce0c5c59b662e8

814357417aa8a57e43d50cb3347c9d287b99955b0b8aee4e53e12b463f7441a0

de44656b4a3dde6e0acdc6f59f73114ce6bb6342bec0dcd45da8676d78b0042e

78471db16d7bd484932c8eb72f7001db510f4643b3449d71d637567911ca363b

e0f22863c84ee634b2650b322e6def6e5bb74460952f72556715272c6c18fe8e

563dd5a95f439bc2b4170a74c8be565a1af076e6cbebd1d018b2809a1e8bc908

411eb20988f57317c177ea64c8bb4c059cc39da6e91eb1e7b9b8da96775d93d5

ed675db1e7c93526141d40ba969bdc5bbdfd013932aaf1e644c66db66ff008e0

f9290cd938d134a480b41d99ac2c5513a964de001602ed34c6383dfeb577b8f7

d271569d5557087aecc340bb570179b73265b29bed2e774d9a2403546c7dd5ff

3a47e59c37dce42304b345a16ba6a3d78fc44b21c4d0e3a0332eee21f1d13845

92a8b74cafa5eda3851cc494f26db70e5ef0259bc7926133902013e5d73fd285

ea27862bd01ee8882817067f19df1e61edca7364ce649ae4d09e1a1cae14f7cc

c3b3f46a5c850971e1269d09870db755391dcbe575dc7976f90ccb1f3812d5ea

edd1480fe3d83dc4dc59992fc8436bc1f33bc065504dccf4b14670e9e2c57a89

3aa746bb94acee94c86a34cb0b355317de8404c91de3f00b40e8257b80c64741

1d970f2e7af9962ae6786c35fcd6bc48bb860e2c8ca74d3b81899c0d3a978b2b

56e96ce15ebd90c197a1638a91e8634dbc5b0b4d8ef28891dcf470ca28d08078

5937746fc1a511d9a8404294b0caa2aedae2f86b5b5be8159385b6c7a4d6fb40

0da9e149ba324f20a390140e9d7913b13ababa07f5b65e4d25e3555c1119e768

a765df03fffa343aa7a420a0a57d4b5c64366392ab6162c3561ff9f7b0ad5623

7330fa1ca4e40cdfea9492134636ef06cd999efb71f510074d185840ac16675d

c9400b2fff71c401fe752aba967fa8e7009b64114c9c431e9e91ac39e8f79497

PyXie Command Line Argument

%SYSTEMROOT%\system32\worker.exe

Vatet SHA256

bacc02fd23c4f95da0fbc5c490b1278d327fea0878734ea9a55f108ef9f4312e

5e0062def3e1d2ac206aa43854a60e23b0d1158fa982e99e0ba8190e77290dbf

4421720e0321ac8b3820f8178eb8a5ff684388438b62c85f93df9743a1d9fdb9

915e660ec51abea9ffd5716fb2c9b8593643adc5e9ea0834a88d8ea4016899f0

0b42bf15b77cfe9f9e693f2776691647e78a91be27f5bdb8d1a366be510a773f

57eea67e3eebde707c3fb3473a858e7f895ae12aad37cc664f9c0512c0382e6a

2f149a79f721bb78eb956f70183b531fb6a1b233ceb4a3d6385759a0b0c16fd3

6ac07424e5c9b87d76645aa041772ac8af12e30dc670be8adf1cf9f48e32944b

382d9bf5da142d44de5fda544de4fffe2915a3ffc67964b993f3c051aa8c2989

ef7e21d874a387f07a9f74f01f2779a280ff06dff3dae0d41906d21e02f9c975

e5ce1c1b69bd12640c604971be311f9544adb3797df15199bd754d3aefe0a955

37e8d3ae4c34441b30098d7711df8ef0bcc12c395f265106b825221744b956bc

10c4067908181cebb72202d92ff7a054b19ef3aada939bf76178e35be9506525

b159fadb829a206c9a59ec547aa9e2a3ee83e8a3cc1441de04f58fd02a43c760

6c1b17c8d8eca38b9926b40637cb793d0997a6183156d9e6353b53d7b3955f20

375afe90771e63dbec77de439625267d723dc6bbb37cc5e94cf4d281d16c2ca8

4d39782ccdb902e8e5348b8b3ce92f0834c713c565cca82be67a0a8eb6468df6

6497d14f6dd14c39c037cb7da24b51d90b7040af64c245aaab6c6cc80cde7f3b

95e5e83b10df32f06080bd6f8428592d81febbf55e72ec5f843dd6188bef25da

01a2404fcf56027be610c65bbfb0f2dda9cfaf67385cb7f93f0b586e3aa6803a

b7fbbbdf7e8795022a41f4e6a94be1de432ae1911e49625f73555e01a5fdc719

d7bcb52f027f66c988e595dc29a343e27af7599e3659901f85a92c26440a5e1f

d353eeb623e96b32c086a9b64991dfedbc8d31254aec2c3cda51042ceb07ee82

66c2038c6d86333cbc51726bc54d3b8a00162493b2c92ca7f839b50435eaa314

47d6cc0a05218d0c1078dabf8d0ca7b7b424cdd73eaf3bf6261fa1b42f92fe0b

5dc7f70a0d20f97c30c25bd927235deec713cde5d1c41916e23dd0c3431ffacd

7ad92c9d63bd9ed305acbe217c40f9945deb98ed5ecced8b92b93332dc27d3c6

d46f72b8598ff80de5661205f6cac0b47831778f70b5edd7525e23418706cc1a

ccc162d3a3d6136a9c472d7d2d07acbae47f88a9a7d9b2c9b97b331e7ab7605d

3cd581621d9a16ebe724e9ba7445aa82162307ff6b2a31be572e87dbce2aa8ad

e1653fe62e8d90153557324ffe4470d9c9262fe3bddad2bf555680b6078cf66a

75728bc96c934c1521ae08e03ec916e20628e000b056c55b6ee04ccc18c602f6

a50a25a312adb9103e52e94018013ebdb6dbfe792a34122cacd53cfa3bbb26ac

87210d6f1773473d28b51de21ed55ecfb6a9bd34f56d2d37f483ed05a1d7efd8

d7d28af8af5be22ecca267bdc7e142667f584550cf8a3bbebdb1368725bb6469

d7641089fd5d0474b835a633d6d852028b3481c18b3574023b021bfa1e3c1cc1

5aec2fa9e954473d9c6b5233512f833e63541965e2d2e4af2419a457676c440d

fcdd72fd2e03badfac13eed5e2d17054bbdcea7c1743179095ce109bf40a7f0f

350926c6bb7419330e55e687c9f00520a560c41f6013528cbb9ea42faeeb3201

8eef012c2eecb7f8a776464f52e12f62c466cfc85adf4eef0d2bc270e7a19212

3928bd8f2fd2db4891b320fa85b37c2598706d27283818ad33a0eeac16d59192

8373be56ddab97188a8606eb5f529187bfb819f5cb5a50c56f6a7878c94c7f86

a098b5455fd1e9d0dea067405cd891b94cc42a0067cbd21d385f9c1254c21fdd

2b13dae3c35eb3958253dbf945f6609e59978c2aedbd163608f03920d7d3623b

01011bb45dec3b520ea09e5d9d3c9fb4acce74de72261f68ff1011f9ea6ccebb

80c9d6cf4e8119dc2d0e263f3f4d5c3bf4221715117505d9d6a02e3671337bf8

bec5a3cfd7332241e3a7463d951b8f9a9e771d4f436d7776a426074a82d19a7d

c7f96f8b15c324bd6bf1aa16f6697d6d407f91ad2d7628a14d70f146334d34be

c5ca45581da0bbb3e4d0c6e51d602512fa52833cd16eebed351397a9a0326518

6f1e8f91773609087a417cb34887f292a0be5c246dab667195854f979a45349a

e07dd37c92d24ac20b94a183e1f0a22a4eec0f950f441761c065faf0afd2abdd

0d14a1b5574dc12f6286d37d0a624232fb63079416b98c2e1cb5c61f8c2b66ff

e5fede5eb43732c7f098acf7b68b1350c6524962215b476de571819b6e5a71fc

ecf3f4ba8dd16551908488cfbf2afd18a55584dbf81c28623026a29b9fa4a62d

edecfdd2a26b4579ecacf453b9dff073233fb66d53c498632464bca8b3084dc5

1309b052618c6301901ec75cf552e7b49f93d66fb47d4de59b82d37d6ac39039

2ceb5de547ad250140c7eb3c3d73e4331c94cf5a472e2806f93bf0d9df09d886

3259dd0efed1d28a149d4e8c4f980a19199d9bead951ee1231e3a26521185f2f

3a3b7b198769de3e5d81a92aa166f783b611a39a7fcea1b5ec762b54295dbc8d

56934547dcf0d7ecf61868ae2f620f60e94c094dbd5c3b5aaf3d3a904d20a693

608f34a79e5566593b284ef0d24f48ea89bc007e5654ae0969e6d9f92ec87d32

625c22b21277c8a7e1b701da9c1c21b64bfa02baef5d7a530a38f6d70a7a16d0

73609f8ebd14c6970d9162ec8d7786f5264e910573dff73881f85b03163bd40e

840985b782648d57de302936257ba3d537d21616cb81f9dce000eaf1f76a56c8

88565b4c707230eac34d4528205056264cd70d797b6b4eb7d891821b00187a69

91c62841844bde653e0357193a881a42c0bc9fcc798a69f451511c6e4c46fd18

a50b58e24eb261157c4f85d02412d80911abe8501b011493c7b393c1905fc234

b1f54b88c9b7680877981f6bebde6aea9effbc38a0a8b27a565fb35331094680

bd7da341a28a19618b53e649a27740dfeac13444ce0e0d505704b56335cc55bd

cb2619b7aab52d612012386d88a0d983c270d9346169b75d2a55010564efc55c

ce0936366976f07ea24e86733888e97e421393829ecfd0fde66bd943d4b992ab

d50f28cf5012e1ffde1cd28655e07519dadcf94218b15c701c526ab0f6acb915

d612144c1f6d4a063530ba5bfae7ef4e4ae134bc55dcf067439471934b841b00

ddf83c02effea8ae9ec2c833bf40187bed23ec33c6b828af49632ef98004ea82

e48e88542ec4cd6f1aa794abc846f336822b1104557c0dfe67cff63e5231c367

Vatet Payload SHA256

a512e5ffd33da906fdf896c536bf64adc59599ec2227f60dace4a4ef23d3d21a

56f6084d84bd6371918c3ae7b555099474cdb6665bed0d969f6b5762b8cf5cc9

2f1e047e840620460bdf7371e62e966919f25f763a53248357f890a4ff11791f

6812190b1dec8c2a4c5d2b327d1bdbe72974fc017d86d2337ea06e9d3337959e

77f2df32060e5125c6d4a3ab2a2a0c862eb44bc44614d494d23f4690a45d08a3

309af51a8d86e031e25c2c928101b9afc9bcd1dcadbf4ef27ed3c0e8d7da0c98

c2861e5626c5ba40d28ec6c7d4ac32edc972a969d2454e74dc50829d02b5de2a

8a7dc1c39321d972a21bf4fdd24f6f2ef3a03e4ea95c49f383ba03902010210c

0e7824dfb7668af175a2b887e592773517f17213555c3b9af4f98d54278621d5

d389e2fc1515b8a2d8d365d072c201a308f776c873fdb185f826a35fde6fbf2b

bde87df68407fafc3ebd95665838eb5476cb854b338fb97252d153a2250f28b8

ab432a84b05de381c2f96a000c318ec78c98e39abfa7eea3210840c85b0cbee7

Vatet Payload Path

<IP>**<EPOCHTIME>**\settings.dat

<IP>**<EPOCHTIME>**\upgrade.dat

<IP>**<EPOCHTIME>**\vodafone.dat

<IP>**<EPOCHTIME>**\winint2.sto

c:\windows\INF\Rainmeter.dat

c:\windows\INF\notepad.dat

c:\windows\INF\options.dat

c:\windows\debug\Rainmeter.dat

c:\windows\debug\config.dat

c:\windows\debug\notepad.dat

c:\windows\debug\options.dat

c:\windows\help\Rainmeter.dat

c:\windows\help\notepad.dat

c:\windows\help\options.dat

c:\windows\media\notepad.dat

c:\windows\notepad.dat

c:\windows\options.dat

c:\windows\system\options.dat

c:\windows\temp\options.dat

PDB Paths

C:\Users\1\Downloads\notepad-plus-plus-master\PowerEditor\bin\npp.pdb

C:\Users\1\Downloads\rainmeter-master\x32-Release\Obj\Library\Rainmeter.pdb

C:\Users\1\Downloads\rainmeter-master\x32-Release\Obj\Application\Rainmeter.pdb

C:\Users\1\Downloads\notepad-master\Debug\notepad.pdb

C:\Users\1\Downloads\tetris-game-master\Release\TetrisGame_zjy.pdb

Z:\coding\pyproject\compiled\cobalt_mode\cobalt_mode.pdb

Z:\coding\pyproject\compiled\ransom\ransom.pdb

PyXie Lite Config


```
{
"logs": {
"gates": [
"<REDACTED>:8443/data"
],
"aes_key": "THIS_KEY_IS_FOR_INTERNAL_USE_ONLY",
"send_attempts": 10,
"send_attempts_timeout": 5
},
"dirs_keys": ["actifio",
"aldelo",
```

"altaro",

"avamar",

"avs",

"back-up",

"backup",

"bank",

"bitmessage",

"client",

"cobaltstrike",

"coin",

"diebold",

"filemaker",

"htape",

"magtek",

"ncr",

"passw",

"payment",

"rapid7",

"replication",

"screenconnect",

"swift",

"tivoli",

"unitrends",

"vault",

"veeam",

"vranger",

"wallet",

"wincor"],

"shell_cmds": ["arp -a",

"cmdkey /list",

"dclist",

"gpresult /z",

"ipconfig /all",

"ipconfig /displaydns",

"klist",

"manage-bde -status",

"net config workstation",

"net group \"domain admins\" /domain",

"net group \"Domain Admins\"",

"net group \"Enterprise Admins\"",

"net localgroup \"administrators\"",

"net localgroup",

"net share",

"net use",

"net user",

"net view /all /domain",

"net view /all",

"netstat -an",

"nltest /domain_trusts /all_trusts",

"nltest /domain_trusts",

"nslookup -type=any %userdnsdomain%",

"qwinsta",

"route print",

"systeminfo",

"tasklist /V",

"vssadmin List Shadows",

"wmic process",

"wmic qfe list"],

"dirs": ["%ALLDRIVESROOTS%\\Alliance",

"%APPDATA%\\Agama",

"%APPDATA%\\Armory",

"%APPDATA%\\B3-CoinV2",

"%APPDATA%\\BeerMoney",

"%APPDATA%\\Bitcloud",

"%APPDATA%\\Bitcoin",

"%APPDATA%\\BitcoinZ",

"%APPDATA%\\bitconnect",

"%APPDATA%\\Bither",

"%APPDATA%\\bitmonero",

"%APPDATA%\\BlocknetDX",

"%APPDATA%\\Cybroscoin",

"%APPDATA%\\Daedalus",

"%APPDATA%\\DashCore",

"%APPDATA%\\DeepOnion",

"%APPDATA%\\DigiByte",

"%APPDATA%\\Dogecoin",

"%APPDATA%\\ElectronCash",

"%APPDATA%\\Electrum",

"%APPDATA%\\Electrum-LTC",

"%APPDATA%\\Ember",

"%APPDATA%\\EmeraldWallet",

"%APPDATA%\\Ethereum Wallet",

"%APPDATA%\\Exodus",

"%APPDATA%\\FairCoin",

"%APPDATA%\\faircoin2",

"%APPDATA%\\Florincoin",

"%APPDATA%\\FORT",

"%APPDATA%\\GambitCoin",

"%APPDATA%\\GeyserCoin",

"%APPDATA%\\GreenCoinV2",

"%APPDATA%\\GridcoinResearch",

"%APPDATA%\\Gulden",

"%APPDATA%\\Hush",

"%APPDATA%\\IOTA Wallet",

"%APPDATA%\\Komodo",

"%APPDATA%\\Learncoin",

"%APPDATA%\\lisk-nano",

"%APPDATA%\\Litecoin",

"%APPDATA%\\Minexcoin",

"%APPDATA%\\mSIGNA_Bitcoin",

"%APPDATA%\\MultiBitHD",

"%APPDATA%\\MultiDoge",

"%APPDATA%\\Neon",

"%APPDATA%\\NXT",

"%APPDATA%\\Parity",

"%APPDATA%\\Particl",

"%APPDATA%\\Peercoin",

"%APPDATA%\\pink2",

"%APPDATA%\\PPCoin",

"%APPDATA%\\Qtum",

"%APPDATA%\\RainbowGoldCoin",

"%APPDATA%\\RoboForm",

"%APPDATA%\\StartCOIN-v2",

"%APPDATA%\\straks",

"%APPDATA%\\Stratis",

"%APPDATA%\\StratisNode",

"%APPDATA%\\TREZOR Bridge",

"%APPDATA%\\TrumpCoinV2",

"%APPDATA%\\VeriCoin",

"%APPDATA%\\Verium",

"%APPDATA%\\Viacoin",

"%APPDATA%\\VivoCore",

"%APPDATA%\\Xeth",

"%APPDATA%\\Zcash",

"%APPDATA%\\ZcashParams",

"%APPDATA%\\Zetacoin",

"%LOCALAPPDATA%\\bisq",

"%LOCALAPPDATA%\\copay",

"%LOCALAPPDATA%\\programs\\zap-desktop",

"%LOCALAPPDATA%\\RippleAdminConsole",

"%LOCALAPPDATA%\\StellarWallet",

"%PROGRAMDATA%\\bitmonero",

"%PROGRAMDATA%\\electroneum",

"%PROGRAMDATA%\\Tiger Technology",

"%PROGRAMDATA%\\tivoli"],

"file_find": {

"enabled": 1,

"patterns": ["10-q",

"10-sb",

"access",

"avamar",

"admin",

"attack",

"aws",

"amazon",

"backup",

"balance",

"bitcoin",

"bitlocker",

"bribery",

"cardholder",

"censored",

"checking",

"clandestine",

"compromate",

"concealed",

"confidential",

"contraband",

"convict",

"credent",

"cyber",

"disclosure",

"engineering",

"esxi",

"ethereum",

"explosive",

"finance",

"fraud",

"hidden",

"illegal",

"infrastruct",

"instruction",

"investigation",

"logins",

"marketwired",

"military",

"n-csr",

"nasdaq",

"nda",

"newswire",

"operation",

"passport",

"passw",

"personal",

"privacy",

"private",

"restricted",

"routing",

"saving",

"secret",

"security",

"spy",

"statement",

"storage",

"submarine",

"suspect",

"tactical",

"treason",

"username",

"vault",

"victim",

"vsphere",

"wallet",

"wasabi",

"wire"

],

"extentions": [".doc",

".docx",

".xls",

".xlsx",

".pdf",

".txt",

".rtf"],

"gold_masks": ["*.rdp",

"*.kdbx",

"*.vnc",

"*.cpp",

"*.c",

"*.sln",

"*.vcproj",

"*.h",

"*.asm",

"*cobaltstrike*",

"*.ovpn",

"*.pcf",

"*.conf"],

"black_files": ["Default.rdp",

"Microsoft June",

"Release_Note",

"Release Note",

"desktop.ini",

"Microsoft Silverlight",

"localhost_access_log",

"dd_clwireg.txt"],

"black_dirs": ["\\microsoft\\windows",

"\\gfi\\languard",

"\\microsoft\\windows\\cookies",

"\\vmware\\vcenterserver",

"\\autoupdate\\cache",

"\\microsoft office\\root"],

"max_size": 5242880

},

"software": [" OPOS",

"Aldelo",

"Actifio",

"Alliance WebStation",

"Alliance Workstation",

"Altaro",

"Back-up",

"Rapid7",

"Backup",

"Bank",

"Blockchain",

"Boot Camp",

"Box Sync",

"BridgeHead",

"CAM Commerce Solutions",

"Card Processing",

"Cash",

"Cisco",

"Citrix",

"Cloud",

"Coin",

"Dashlane",

"Diskeeper",

"Double-Take",

"Dropbox",

"Elcomsoft",

"FileZilla Server",

"FortiClient",

"Fund",

"iDrive",

"Ledger",

"LexisNexis",

"LogMeIn",

"M262x",

"Microsoft Dynamics RMS Store Operations",

"Microsoft POS",

"vRanger",

"Money",

"mRemoteNG",

"MSR",

"Password",

"Payment",

"Private",

"Protect",

"PuTTY",

"QuickBooks",

"Replication",

"ScreenConnect",

"Shadow",

"SII RP-D10",

"Storage",

"SWIFT",

"TeamViewer",

"Token",

"Trade",

"Treasury",

"Trezor",

"Vault",

"Unitrends",

"VIP Access",

"VMware",

"Vnc",

"VPN",

"Wallet",

"Withdraw"],

"registry": ["SOFTWARE\\Ammyy",

"SOFTWARE\\Cppcheck",

"SOFTWARE\\DASH",

"SOFTWARE\\Dash",

"SOFTWARE\\DeterministicNetworks",

"SOFTWARE\\GitForWindows",

"SOFTWARE\\GlavSoft LLC.",

"SOFTWARE\\GnuPG",

"SOFTWARE\\Hex-Rays",

"SOFTWARE\\Hex-Rays SA",

"SOFTWARE\\HexaD",

"SOFTWARE\\ITarian",

"SOFTWARE\\LogMeIn Ignition",

"SOFTWARE\\LogMeIn",

"SOFTWARE\\MetaQuotes Software",

"SOFTWARE\\Microsoft\\ResKit\\Robocopy",

"SOFTWARE\\Nmap",

"SOFTWARE\\Pulse Secure",

"SOFTWARE\\PyBitmessage",

"SOFTWARE\\PyBitmessage",

"SOFTWARE\\S.W.I.F.T.",

"SOFTWARE\\ShrewSoft",

"SOFTWARE\\SimonTatham",

"SOFTWARE\\SonicWall",

"SOFTWARE\\TortoiseSVN",

"SOFTWARE\\Veeam",

"SOFTWARE\\VisualSVN",

"SOFTWARE\\Whole Tomato",

"SOFTWARE\\WinLicense"],

"portscan": {"Bitcoin": [8332,8333],

"DNS": [53],

"Elasticsearch": [9200,9300],

"FTP": [21],

"Horizon Agent": [22443,4172,9427,32111],

"HTTP": [80,5000,9043],

"HTTPS": [443,8443,1311,5001,8200],

"JAVA-RMI": [34571,1099,1090,1098,1099,4444,11099,47001,47002,10999],

"MongoDB": [27017],

"MSSQL": [1433],

"MySQL": [3306],

"neo4j": [7687],

"NetBackup": [5637],

"NETBIOS": [139],

"Oracle": [1521],

"POP3": [110],

"POP3s": [995],

"PostgreSQL": [5432],

"PPTP": [1723],

"RADMIN": [4899],

"RDP": [3389],

"SMTP": [25],

"SonicWall-VPN": [4433],

"SSH": [22],

"Telnet": [23],

"Tivoli": [1500,1581],

"TOR": [9050],

"AcronixBackup": [9877],

"vCenter": [22024,902,903,10080,10443],

"Veeam": [9392,9393,9394,9397,9398,9399],

"VNC": [5900, 5800],

"WinRM": [5985,5986],

"Zabbix": [10050,10051],

"JDWP": [45000,45001],

"JMX": [8686,9012,50500],

"jBoss": [11111,4444,4445],

"Cisco Smart Install": [4786],

"HP Data Protector": [5555,5556],

"GlassFish": [4848]

}

}

PyXie Lite Remapped Opcodes

def_op('PRINT_ITEM', 78)
def_op('PRINT_NEWLINE', 63)

def_op('POP_TOP', 85)

def_op('RETURN_VALUE', 88)

def_op('ROT_TWO', 29)

def_op('ROT_THREE', 9)

def_op('STORE_MAP', 55)

def_op('INPLACE_ADD', 28)

def_op('ROT_FOUR', 72)

def_op('UNARY_POSITIVE', 12)

def_op('UNARY_NEGATIVE', 64)

def_op('UNARY_NOT', 66)

def_op('UNARY_CONVERT', 20)

```
def_op('UNARY_INVERT', 65)
def_op('GET_ITER', 83)
def_op('BINARY_MULTIPLY', 80)
def_op('BINARY_POWER', 79)
def_op('BINARY_DIVIDE', 15)
def_op('BINARY_MODULO', 76)
def_op('BINARY_ADD', 84)
def_op('BINARY_SUBTRACT', 89)
def_op('BINARY_SUBSCR', 57)
def_op('BINARY_FLOOR_DIVIDE', 68)
def_op('INPLACE_FLOOR_DIVIDE', 24)
def_op('INPLACE_DIVIDE', 82)
def_op('INPLACE_SUBTRACT', 22)
def_op('INPLACE_MULTIPLY', 13)
def_op('INPLACE_MODULO', 70)
def_op('STORE_SUBSCR', 54)
def_op('DELETE_SUBSCR', 77)
def_op('BINARY_LSHIFT', 60)
def_op('BINARY_RSHIFT', 21)
def_op('BINARY_AND', 3)
def_op('BINARY_XOR', 73)
def_op('BINARY_OR', 56)
def_op('INPLACE_POWER', 23)
def_op('POP_BLOCK', 2)
def_op('DUP_TOP', 75)
def_op('PRINT_ITEM_TO', 5)
def_op('PRINT_NEWLINE_TO', 11)
def_op('INPLACE_LSHIFT', 59)
```

```
def_op('INPLACE_RSHIFT', 74)
def_op('INPLACE_AND', 61)
def_op('INPLACE_XOR', 27)
def_op('INPLACE_OR', 71)
def_op('BREAK_LOOP', 58)
def_op('WITH_CLEANUP', 19)
def_op('END_FINALLY', 4)
def_op('BUILD_CLASS', 87)
def_op('EXEC_STMT', 10)
def_op('LOAD_LOCALS', 67)
def_op('IMPORT_STAR', 26)
def_op('YIELD_VALUE', 25)
```