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

By Ryan Tracey, Drew Schmitt

Published: 2020-11-07 · Archived: 2026-04-05 22:49:56 UTC

{

"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]

}

}

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)
```

---