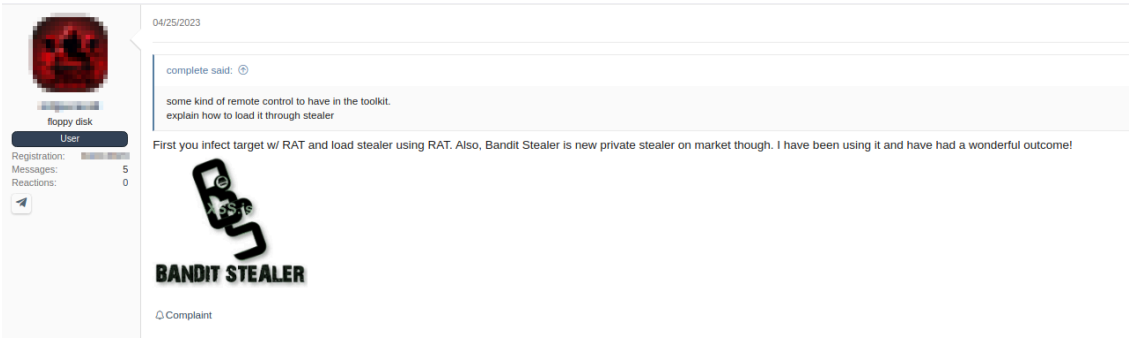
Breaking into the Bandit Stealer Malware Infrastructure

By Bablu Kumar

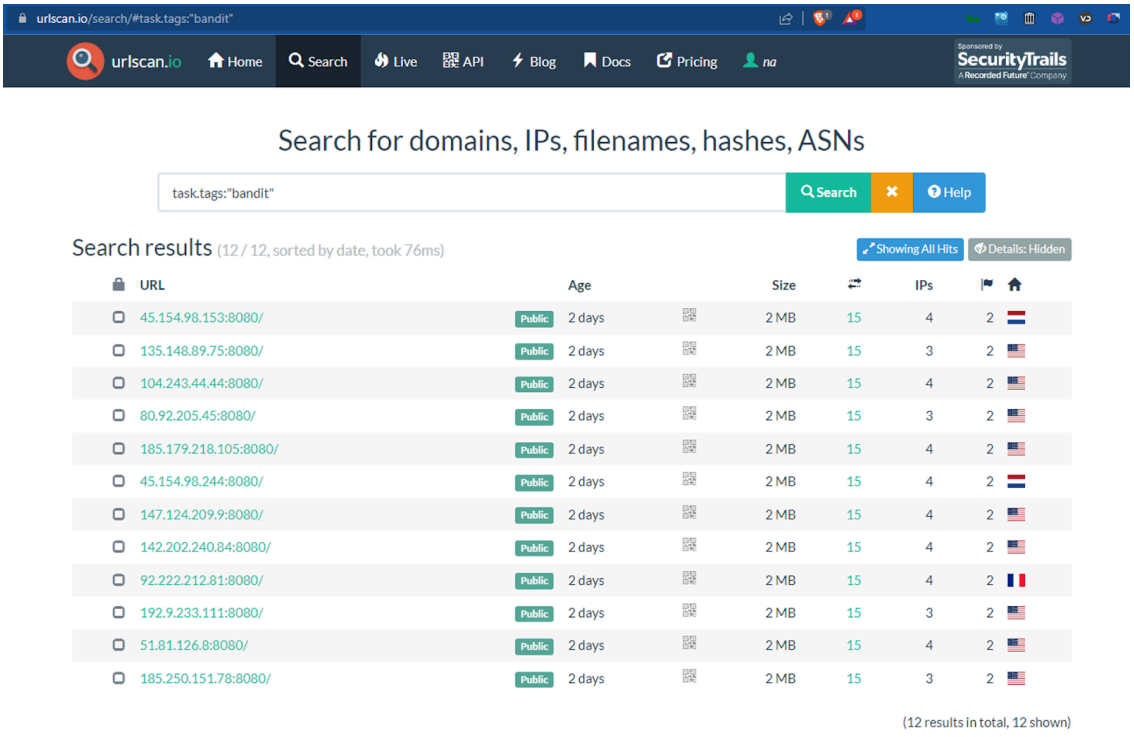
Published: 2025-08-21 · Archived: 2026-04-05 18:52:45 UTC

Analysis and Attribution

CloudSEK's contextual AI digital risk platform XVigil has discovered a post mentioning Bandit Stealer malware on a Russian-speaking underground forum where a threat actor vouched for it.



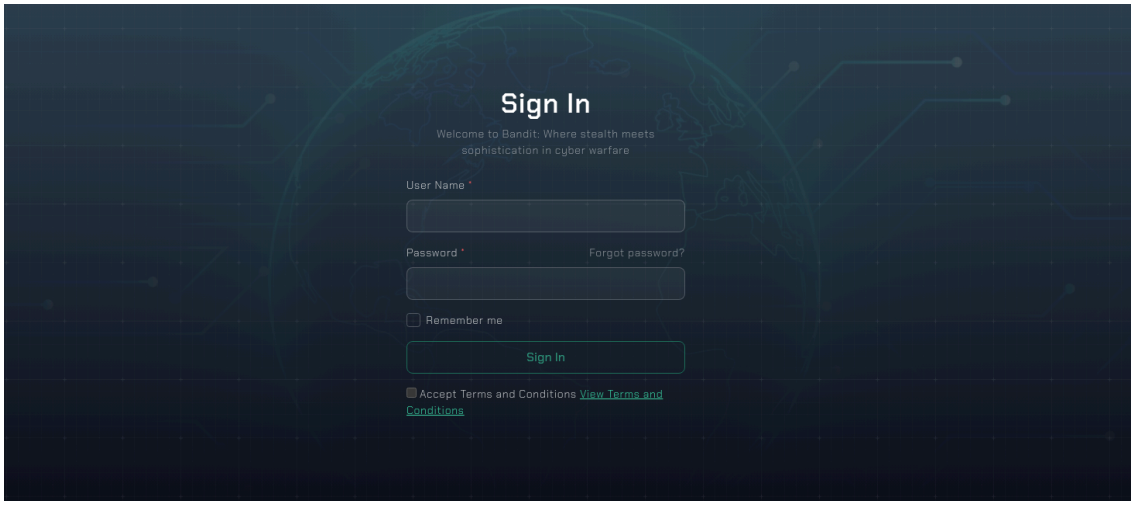
CloudSEK researchers recently discovered at least 14 IP addresses serving the Bandit Stealer web panel, most of which went down in a span of 24 hours. All of these IP addresses were running on port **8080**.



Results from URLScan.io

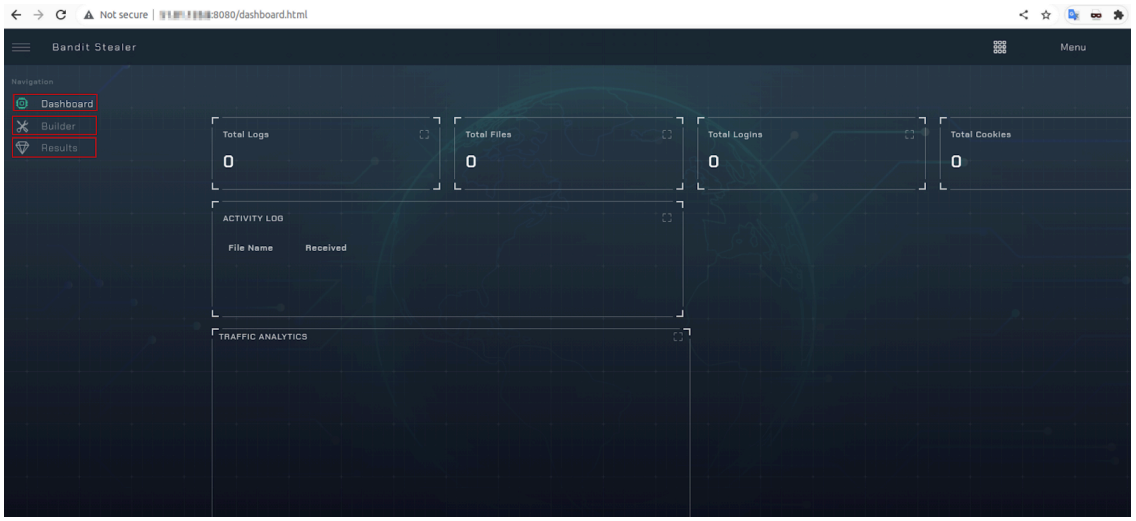
Bandit Web Panel Analysis

Our source identified a few website endpoints that allowed access to the website's internal system without entering the credentials due to a misconfiguration on the website.



Login page of Bandit Stealer web panel

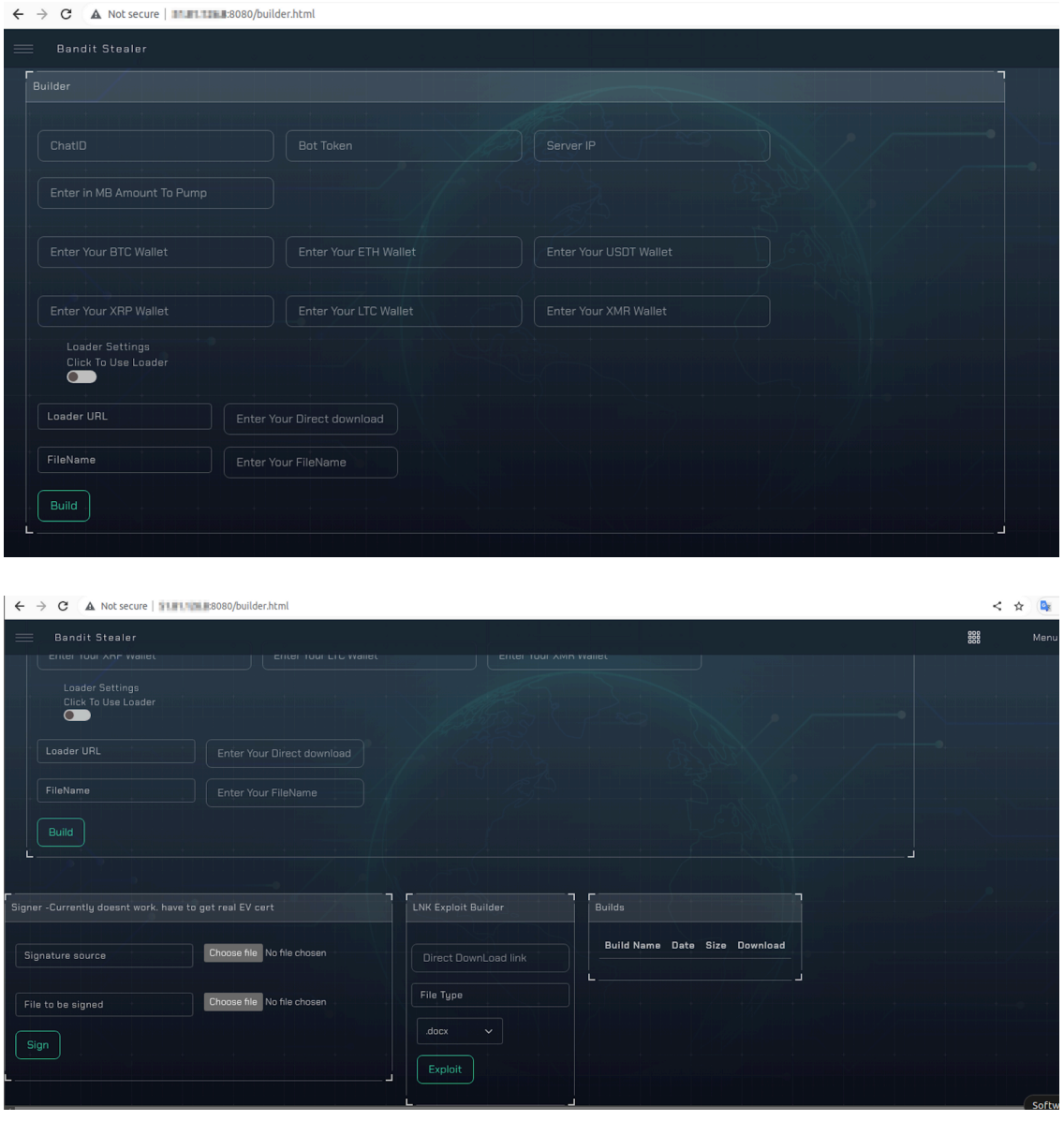
Nothing particularly significant can be noted on the dashboard except a menu for options such as **Builder** and **Results**.



Dashboard interface of the malware panel

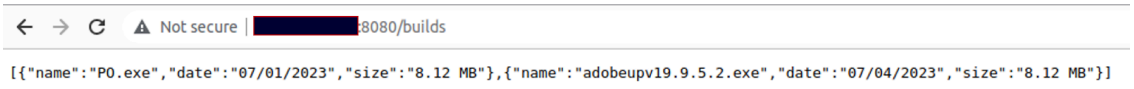
The Builder page shows the options for building a customized version of Bandit Stealer malware. And, in the stealer operation, threat actors utilize key elements to carry out their activities:

- **Communication Channel:** ChatID, Bot Token, and Server IP are utilized to establish a secure connection with Telegram. This connection enables the threat actors to receive exfiltrated data from infected users, such as compromised credentials and screenshots.
- **Cryptocurrency Wallet Addresses:** Various cryptocurrency wallet addresses are employed to transfer cryptocurrency amounts to the threat actor's wallet.
- **Loader URL:** The Loader URL serves as a mechanism for distributing the malware. For instance, in malvertising campaigns, a hidden JavaScript code operates in the background and is responsible for dropping the executable malware file onto the victim's system. This URL is a crucial component in the initial infection process.
- **FileName:** The FileName refers to the name assigned to the executable malware file. This file contains the malicious code responsible for the intended actions, such as data theft and exfiltration.



Malware builder panel used for generating executable

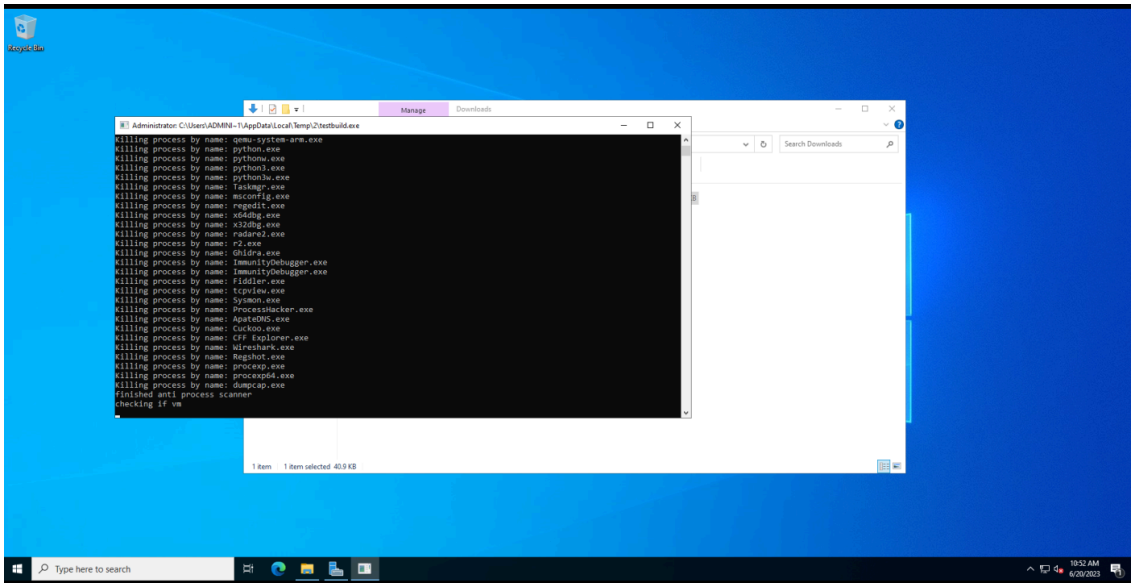
One of the discovered endpoints was **/builds** that had all the Bandit Stealer builder that had been generated so far by this particular panel. Our source was able to acquire them for further analysis.



Next, another identified endpoint was **/clients** with multiple instances of likely exfiltrated data from multiple IP addresses in JSON. In the JSON, the file name consists of the target's **Country Code + Public IP address**, followed by **size** and the exfiltration **date and time**. While our analysis confirms the data to be sent to the Telegram bot, but we assume the malware likely also keeps a copy of the exfiltrated data in its web panel.

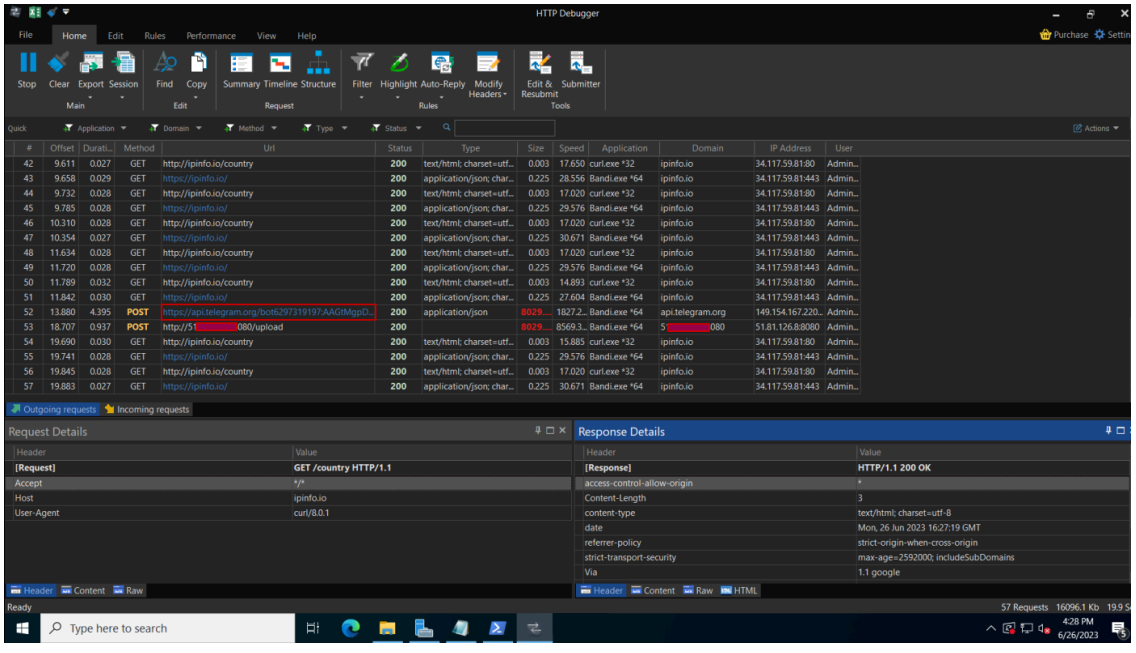
Analysis of Stealer Logs

Our source was able to exfiltrate the stealer logs from their web panel for Analysis. One of the log files was from the test machine with lots of screenshots which they might have used for testing the malware. The screenshot shows the process of anti-reversing tools being killed using Command Prompt. The other screenshot shows the same process using PowerShell. As the malware has screen capture capabilities, it is assumed that the malware have captured these screenshots during the infection (likely on the test machine).



The process of killing anti-reversing tools

Another screenshot reveals the usages of a Telegram bot in the stealer malware as the C2 communication channel.



Using Telegram bot for C2 servers

Malware Delivery Mechanism

The malware is being distributed through YouTube videos which is a commonly seen malware delivery mechanism among threat actors. In our previous report, we highlighted that since November 2022, there has been a 200-300% month-on-month increase in Youtube videos containing links to stealer malware such as Vidar, RedLine, and Raccoon in their descriptions.

video_title	video_link	url	views	published_at	channel	subscribe
ADOBE AFTER EFFECTS CRACK 2023…	https://www.youtube.com/watch?v=mUp…	bit.ly/3JlrfM6	1976	2023-07-02T21:16:0…	JAKA GL	134

Technical Analysis

Bandit Stealer, a newly discovered form of information stealer malware, showcases advanced capabilities and evasive techniques. Written in the Go language, it employs various methods to circumvent detection by debugging tools and virtual machine environments, ensuring its covert operations remain undetected.

To avoid analysis and hinder reverse engineering efforts, Bandit Stealer employs clever tactics. It actively checks for the presence of debuggers using techniques like **IsDebuggerPresent** and **CheckRemoteDebuggerPresent**. Furthermore, it possesses the ability to detect sandbox environments, swiftly shutting itself down if such environments are detected, thereby eluding analysis attempts. The malware even terminates reverse engineering tools that could potentially interfere with its functionality.

Notably, Bandit Stealer has been observed spreading through YouTube videos to reach mass users.

In order to establish persistence on infected systems, the malware creates an autorun registry entry, named "Bandit Stealer." By doing so, it ensures that the malicious code runs each time the machine is booted up.

Collected PC, User, and IP Information

The stealer is designed to obtain valuable information from PCs and users. It discreetly collects data such as PC and user details, screenshots, geolocation and IP information, webcam images, and data from popular browsers, FTP applications, and digital wallets. The stolen data is then sent to a secure Telegram bot, packaged in a ZIP file for easy transfer.

The Stealer employs a curated blacklist obtained from an external URL, in some instances a Pastebin URL, and stores it in **C:\Users\USERNAME\AppData\Roaming\blacklist.txt** and the file gets deleted once the stealer finishes execution. This blacklist serves a crucial role in determining whether the Stealer is running within a sandbox/virtual environment or on an actual system. Additionally, it aids in identifying specific processes and reversing tools that the Stealer aims to terminate in order to thwart any potential analysis or reverse engineering attempts.

Blacklisted IP Addresses:

```
blackListedIPS = ['88.132.231.71', '78.139.8.50', '20.99.160.173', '88.153.199.169', '84.147.62.12', '194.154.78.160',
                  '92.211.109.160', '195.74.76.222', '188.105.91.116', '34.105.183.68', '92.211.55.199',
                  '79.104.209.33', '95.25.204.90', '34.145.89.174', '109.74.154.90', '109.145.173.169',
                  '34.141.146.114', '212.119.227.151', '195.239.51.59', '192.40.57.234', '64.124.12.162',
                  '34.142.74.220', '188.105.91.173', '109.74.154.91', '34.105.72.241', '109.74.154.92', '213.33.142.50',
                  '109.74.154.91', '93.216.75.209',
                  '192.87.28.103', '88.132.226.203', '195.181.175.105', '88.132.225.100', '92.211.192.144',
                  '34.83.46.130', '188.105.91.143', '34.85.243.241', '34.141.245.25', '178.239.165.70', '84.147.54.113',
                  '193.128.114.45', '95.25.81.24', '92.211.52.62', '88.132.227.238', '35.199.6.13', '80.211.0.97',
                  '34.85.253.170', '23.128.248.46', '35.229.69.227', '34.138.96.23', '192.211.110.74', '35.237.47.12',
                  '87.166.50.213', '34.253.248.228', '212.119.227.167', '193.225.193.201', '34.145.195.58',
                  '34.105.0.27', '195.239.51.3', '35.192.93.107']
```

Blacklisted Mac Addresses:

```
blackListedMacs = ['00:15:5d:00:07:34', '00:e0:4c:b8:7a:58', '00:0c:29:2c:c1:21', '00:25:90:65:39:e4',
                   'c8:9f:1d:b6:58:e4', '00:25:90:36:65:0c', '00:15:5d:00:00:f3', '2e:b8:24:4d:f7:de',
                   '00:15:5d:13:6d:0c', '00:50:56:a0:dd:00', '00:15:5d:13:66:ca', '56:e8:92:2e:76:0d',
                   'ac:1f:6b:d0:48:fe', '00:e0:4c:94:1f:20', '00:15:5d:00:05:d5', '00:e0:4c:4b:4a:40',
                   '42:01:0a:8a:00:22', '00:1b:21:13:15:20', '00:15:5d:00:06:43', '00:15:5d:1e:01:c8',
                   '00:50:56:b3:38:68', '60:02:92:3d:f1:69', '00:e0:4c:7b:7b:86', '00:e0:4c:46:cf:01',
                   '42:85:07:f4:83:d0', '56:b0:6f:ca:0a:e7', '12:1b:9e:3c:a6:2c', '00:15:5d:00:1c:9a',
                   '00:15:5d:00:1a:b9', 'b6:ed:9d:27:f4:fa', '00:15:5d:00:01:81', '4e:79:c0:d9:af:c3',
                   '00:15:5d:b6:e0:cc', '00:15:5d:00:02:26', '00:50:56:b3:05:b4', '1c:99:57:1c:ad:e4',
                   '08:00:27:3a:28:73', '00:15:5d:00:00:c3', '00:50:56:a0:45:03', '12:8a:5c:2a:65:d1',
                   '00:25:90:36:f0:3b', '00:1b:21:13:21:26', '42:01:0a:8a:00:22', '00:1b:21:13:32:51',
                   'a6:24:aa:ae:e6:12', '08:00:27:45:13:10', '00:1b:21:13:26:44', '3c:ec:ef:43:fe:de',
                   'd4:81:d7:ed:25:54', '00:25:90:36:65:38', '00:03:47:63:8b:de', '00:15:5d:00:05:8d',
                   '00:0c:29:52:52:50', '00:50:56:b3:42:33', '3c:ec:ef:44:01:0c', '06:75:91:59:3e:02',
                   '42:01:0a:8a:00:33', 'ea:f6:f1:a2:33:76', 'ac:1f:6b:d0:4d:98', '1e:6c:34:93:68:64',
                   '00:50:56:a0:61:aa', '42:01:0a:96:00:22', '00:50:56:b3:21:29', '00:15:5d:00:00:b3',
                   '96:2b:e9:43:96:76', 'b4:a9:5a:b1:c6:fd', 'd4:81:d7:87:05:ab', 'ac:1f:6b:d0:49:86',
                   '52:54:00:8b:a6:08', '00:0c:29:05:d8:6e', '00:23:cd:ff:94:f0', '00:e0:4c:d6:86:77',
                   '3c:ec:ef:44:01:aa', '00:15:5d:23:4c:a3', '00:1b:21:13:33:55', '00:15:5d:00:00:a4',
                   '16:ef:22:04:af:76', '00:15:5d:23:4c:ad', '1a:6c:62:60:3b:f4', '00:15:5d:00:00:1d',
                   '00:50:56:a0:cd:a8', '00:50:56:b3:fa:23', '52:54:00:a0:41:92', '00:50:56:b3:f6:57',
                   '00:e0:4c:56:42:97', 'ca:4d:4b:ca:18:cc', 'f6:a5:41:31:b2:78', 'd6:03:e4:ab:77:8e',
                   '00:50:56:ae:b2:b0', '00:50:56:b3:94:cb', '42:01:0a:8e:00:22', '00:50:56:b3:4c:bf',
                   '00:50:56:b3:09:9e', '00:50:56:b3:38:88', '00:50:56:a0:d0:fa', '00:50:56:b3:91:c8',
                   '3e:c1:fd:f1:bf:71', '00:50:56:a0:6d:86', '00:50:56:a0:af:75', '00:50:56:b3:dd:03',
                   'c2:ee:af:fd:29:21', '00:50:56:b3:ee:e1', '00:50:56:a0:84:88', '00:1b:21:13:32:20',
                   '3c:ec:ef:44:00:d0', '00:50:56:ae:e5:d5', '00:50:56:97:f6:c8', '52:54:00:ab:de:59',
                   '00:50:56:b3:9e:9e', '00:50:56:a0:39:18', '32:11:4d:d0:4a:9e', '00:50:56:b3:d0:a7',
                   '94:de:80:de:1a:35', '00:50:56:ae:5d:ea', '00:50:56:b3:14:59', 'ea:02:75:3c:90:9f',
                   '00:e0:4c:44:76:54', 'ac:1f:6b:d0:4d:e4', '52:54:00:3b:78:24', '00:50:56:b3:50:de',
                   '7e:05:a3:62:9c:4d', '52:54:00:b3:e4:71', '90:48:9a:9d:d5:24', '00:50:56:b3:3b:a6',
                   '92:4c:a8:23:fc:2e', '5a:e2:a6:a4:44:db', '00:50:56:ae:6f:54', '42:01:0a:96:00:33',
                   '00:50:56:97:a1:f8', '5e:86:e4:3d:0d:f6', '00:50:56:b3:ea:ee', '3e:53:81:b7:01:13',
                   '00:50:56:97:ec:f2', '00:e0:4c:b3:5a:2a', '12:f8:87:ab:13:ec', '00:50:56:a0:38:06',
                   '2e:62:e8:47:14:49', '00:0d:3a:d2:4f:1f', '60:02:92:66:10:79', '', '00:50:56:a0:d7:38',
                   'be:00:e5:c5:0c:e5', '00:50:56:a0:59:10', '00:50:56:a0:06:8d', '00:e0:4c:cb:62:08',
                   '4e:81:81:8e:22:4e']
```

The list of blacklisted HWIDs:

```
blacklisted_hwids = ['7AB5C494-39F5-4941-9163-47F54D6D5016', '03DE0294-0480-05DE-1A06-350700080009',
                     '11111111-2222-3333-4444-555555555555', '6F3CA5EC-BEC9-4A4D-8274-11168F640058',
                     'ADEEEE9E-EF0A-6B84-B14B-B83A54AFC548', '4C4C4544-0050-3710-8058-CAC04F59344A',
                     '00000000-0000-0000-0000-AC1F6BD04972', '00000000-0000-0000-0000-000000000000',
                     '5BD24D56-789F-8468-7CDC-CAA7222CC121', '49434D53-0200-9065-2500-65902500E439',
                     '49434D53-0200-9036-2500-36902500F022', '777D84B3-88D1-451C-93E4-D235177420A7',
                     '49434D53-0200-9036-2500-369025000C65', 'B1112042-52E8-E25B-3655-6A4F54155DBF',
                     '00000000-0000-0000-0000-AC1F6BD048FE', 'EB16924B-FB6D-4FA1-8666-17B91F62FB37',
                     'A15A930C-8251-9645-AF63-E45AD728C20C', '67E595EB-54AC-4FF0-B5E3-3DA7C7B547E3',
                     'C7D23342-A5D4-68A1-59AC-CF40F735B363', '63203342-0EB0-AA1A-4DF5-3FB37DBB0670',
                     '44B94D56-65AB-DC02-86A0-98143A7423BF', '6608003F-ECE4-494E-B07E-1C4615D1D93C',
                     'D9142042-8F51-5EFF-D5F8-EE9AE3D1602A', '49434D53-0200-9036-2500-369025003AF0',
                     '8B4E8278-525C-7343-B825-280AEBCD3BCB', '4D4DDC94-E06C-44F4-95FE-33A1ADA5AC27',
                     '79AF5279-16CF-4094-9758-F88A616D81B4', 'FF577B79-782E-0A4D-8568-B35A9B7EB76B',
                     '08C1E400-3C56-11EA-8000-3CECEF43FEDE', '6ECEAF72-3548-476C-BD8D-73134A9182C8',
                     '49434D53-0200-9036-2500-369025003865', '119602E8-92F9-BD4B-8979-DA682276D385',
                     '12204D56-28C0-AB03-51B7-44A8B7525250', '63FA3342-31C7-4E8E-8089-DAFF6CE5E967',
                     '365B4000-3B25-11EA-8000-3CECEF44010C', 'D8C30328-1B06-4611-8E3C-E433F4F9794E',
                     '00000000-0000-0000-0000-50E5493391EF', '00000000-0000-0000-0000-AC1F6BD04D98',
                     '4CB82042-BA8F-1748-C941-363C391CA7F3', 'B6464A2B-92C7-4B95-A2D0-E5410081B812',
                     'BB233342-2E01-718F-D4A1-E7F69D026428', '9921DE3A-5C1A-DF11-9078-563412000026',
                     'CC5B3F62-2A04-4D2E-A46C-AA41B7050712', '00000000-0000-0000-0000-AC1F6BD04986',
                     'C249957A-AA08-4B21-933F-9271BEC63C85', 'BE784D56-81F5-2C8D-9D4B-5AB56F05D86E',
                     'ACA69200-3C4C-11EA-8000-3CECEF4401AA', '3F284CA4-8BDF-489B-A273-41B44D668F6D',
                     'BB64E044-87BA-C847-BC0A-C797D1A16A50', '2E6FB594-9D55-4424-8E74-CE25A25E36B0',
                     '42A82042-3F13-512F-5E3D-6BF4FFFD8518', '38AB3342-66B0-7175-0B23-F390B3728B78',
                     '48941AE9-D52F-11DF-BBDA-503734826431', '032E02B4-0499-05C3-0806-3C0700080009',
                     'DD9C3342-FB80-9A31-EB04-5794E5AE2B4C', 'E08DE9AA-C704-4261-B32D-57B2A3993518',
                     '07E42E42-F43D-3E1C-1C6B-9C7AC120F3B9', '88DC3342-12E6-7D62-B0AE-C80E578E7B07',
                     '5E3E7FE0-2636-4CB7-84F5-8D2650FFEC0E', '96BB3342-6335-0FA8-BA29-E1BA5D8FEFBE',
                     '0934E336-72E4-4E6A-B3E5-383BD8E938C3', '12EE3342-87A2-32DE-A390-4C2DA4D512E9',
                     '38813342-D7D0-DFC8-C56F-7FC9DFE5C972', '8DA62042-8B59-B4E3-D232-38B29A10964A',
                     '3A9F3342-D1F2-DF37-68AE-C10F60BFB462', 'F5744000-3C78-11EA-8000-3CECEF43FEFE',
                     'FA8C2042-205D-13B0-FCB5-C5CC55577A35', 'C6B32042-4EC3-6FDF-C725-6F63914DA7C7',
                     'FCE23342-91F1-EAFC-BA97-5AAE4509E173', 'CF1BE00F-4AAF-455E-8DCD-B5B09B6BFA8F',
                     '050C3342-FADD-AEDF-EF24-C6454E1A73C9', '4DC32042-E601-F329-21C1-03F27564FD6C',
                     'DEAEB8CE-A573-9F48-BD40-62ED6C223F20', '05790C00-3B21-11EA-8000-3CECEF4400D0',
                     '5EBD2E42-1DB8-78A6-0EC3-031B661D5C57', '9C6D1742-046D-BC94-ED09-C36F70CC9A91',
                     '907A2A79-7116-4CB6-9FA5-E5A58C4587CD', 'A9C83342-4800-0578-1EE8-BA26D2A678D2',
                     'D7382042-00A0-A6F0-1E51-FD1BBF06CD71', '1D4D3342-D6C4-710C-98A3-9CC6571234D5',
                     'CE352E42-9339-8484-293A-BD50CDC639A5', '60C83342-0A97-928D-7316-5F1080A78E72',
                     '02AD9898-FA37-11EB-AC55-1D0C0A67EA8A', 'DBCC3514-FA57-477D-9D1F-1CAF4CC92D0F',
                     'FED63342-E0D6-C669-D53F-253D696D74DA', '2DD1B176-C043-49A4-830F-C623FFB88F3C',
                     '4729AEB0-FC07-11E3-9673-CE39E79C8A00', '84FE3342-6C67-5FC6-5639-9B3CA3D775A1',
                     'DBC22E42-59F7-1329-D9F2-E78A2EE5BD0D', 'CEFC836C-8CB1-45A6-ADD7-209085EE2A57',
                     'A7721742-BE24-8A1C-B859-D7F8251A83D3', '3F3C58D1-B4F2-4019-B2A2-2A500E96AF2E',
                     'D2DC3342-396C-6737-A8F6-0C6673C1DE08', 'EADD1742-4807-00A0-F92E-CCD933E9D8C1',
                     'AF1B2042-4B90-0000-A4E4-632A1C8C7EB1', 'FE455D1A-BE27-4BA4-96C8-967A6D3A9661',
                     '921E2042-70D3-F9F1-8CBD-B398A21F89C6']
```

Blacklisted PC User and Names:

```
blacklisted_users = ['WDAGUtilityAccount', 'Abby', 'hmarc', 'patex', 'RDhJ0CNFevzX', 'kEecfMwgj', 'Frank',
                     '8Nl0ColNQ5bq', 'Lisa', 'John', 'george', 'PxmdUOpVyx', '8VizSM', 'w0fjuOVmCcP5A',
                     'lmVwjj9b', 'PqONjHVwexsS', '3u2v9m8', 'Julia', 'HEUeRzl', 'fred', 'server', 'BvJChRPnsxn',
                     'Harry Johnson', 'SqgFOf3G', 'Lucas', 'mike', 'PateX', 'h7dk1xPr', 'Louise', 'User01', 'test',
                     'RGzcBUyrznReg']

blackListedPCNames = ['BEE7370C-8C0C-4', 'DESKTOP-NAKFFMT', 'WIN-5E07COS9ALR', 'B30F0242-1C6A-4', 'DESKTOP-VRSQLAG',
                      'Q9IATRKPRH', 'XC64ZB', 'DESKTOP-D019GDM', 'DESKTOP-WI8CLET', 'SERVER1', 'LISA-PC', 'JOHN-PC',
                      'DESKTOP-B0T93D6', 'DESKTOP-1PYKP29', 'DESKTOP-1Y2433R', 'WILEYPC', 'WORK', '6C4E733F-C2D9-4',
                      'RALPHS-PC', 'DESKTOP-WG3MYJS', 'DESKTOP-7XC6GEZ', 'DESKTOP-5OV9S0O',
                      'QarZhrdBpj', 'ORELEEPC', 'ARCHIBALDPC', 'JULIA-PC', 'd1bnJkfV1H', 'NETTYPC', 'DESKTOP-BUGIO',
                      'DESKTOP-CBGPFEE', 'SERVER-PC', 'TIQIYLA9TW5M', 'DESKTOP-KALVINO', 'COMPNAME_4047',
                      'DESKTOP-19OLLTD', 'DESKTOP-DE369SE', 'EA8C2E2A-D017-4', 'AIDANPC', 'LUCAS-PC', 'MARCI-PC',
```

Information Stealing & C2 Server Communication

Bandit steals web browser data that includes the theft of saved login information, crucial cookies, browsing history and sensitive credit card details stored within the browser's user profile.

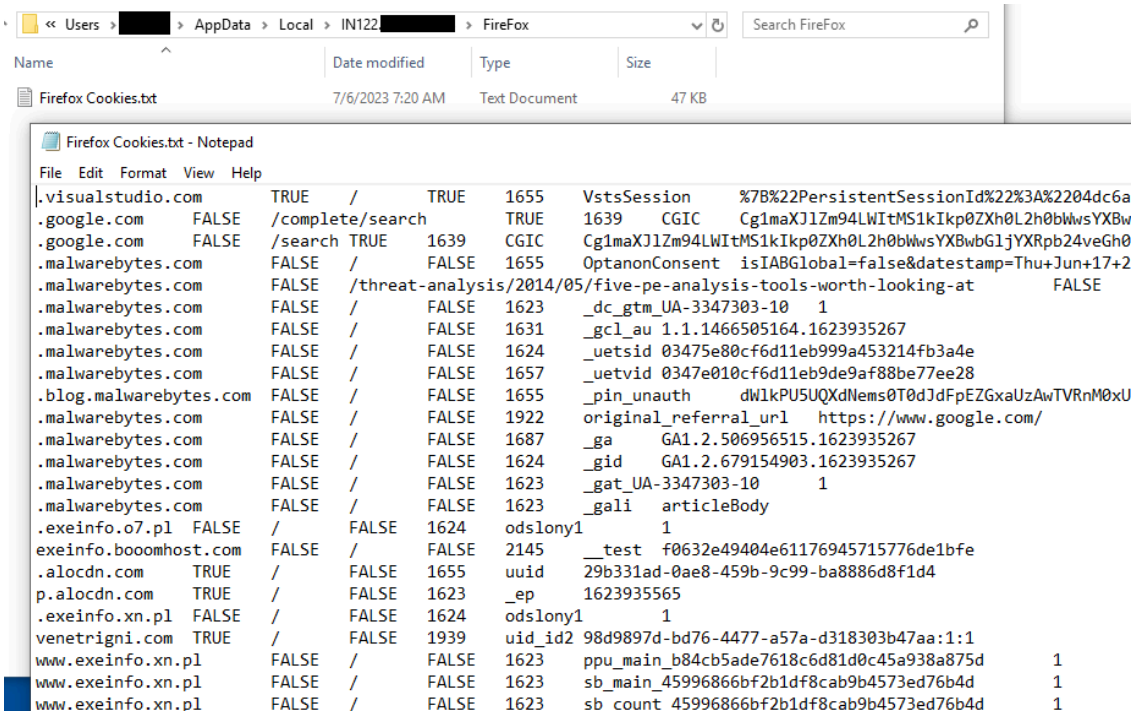
List of Target Browsers			
Chrome Browser	Iridium Browser	7Star Browser	Vivaldi Browser
Yandex Chrome	Orbitum	Orbitum	uCozMedia
Microsoft Edge	Torch Web Browser	Kometa Browser	CentBrowser
BraveSoftware	Amigo Browser	Epic Privacy Browser	SeaMonkey browser
QupZilla			

The malware also targets a large list of digital cryptocurrency wallets.

List of Cryptocurrency Wallets			
Coinbase wallet extension	Saturn Wallet extension	MetaMask extension	Bither Bitcoin wallet
Binance chain wallet extension	Coin98 Wallet	ronin wallet extension	multidoge coin
TronLink Wallet	multibit Bitcoin	Kardiachain wallet extension	LiteCoin
Terra Station	Electron Cash	Jaxx liberty Wallet	Dash Wallet
Guildwallet extension	Electrum-btcp	Math Wallet extension	Ethereum

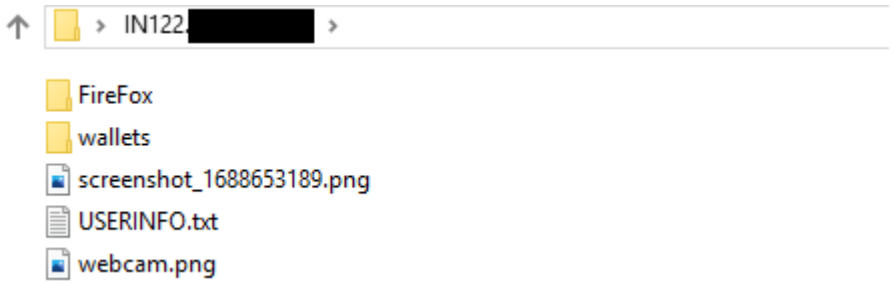
Bitpay wallet extension	Exodus	Nifty Wallet extension	Atomic
Armory	Bytecoin Wallet	Coinomi wallet	Monero wallet
dogecoin			

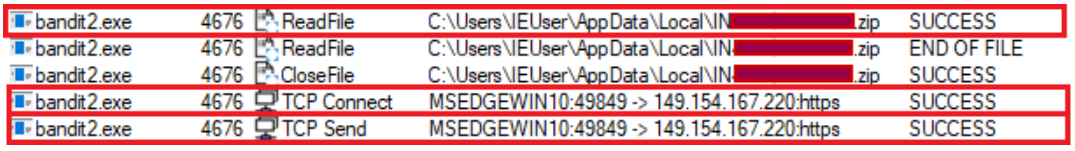
Here is an example of captured Firefox cookies by the Bandit Stealer.



Theft of browser cookies by Bandit Stealer

The collected data is then packaged up into a ZIP file and then exfiltrated to the C2 server which points to the Telegram server (**149.154.167.220**).





*Data exfiltration to the C2 server belonging to Telegram (**149.154.167.220**)*

Source: https://www.cloudsek.com/blog/breaking-into-the-bandit-stealer-malware-infrastructure