Technical Analysis of Bandit Stealer

zscaler.com/blogs/security-research/technical-analysis-bandit-stealer

Key Points

- *Bandit* is a new information stealer that harvests stored credentials from web browsers, FTP clients, email clients, and targets cryptocurrency wallet applications.
- The malware sends stolen information to a command and control server via Telegram.
- Bandit implements numerous methods to detect and evade virtual machines and malware sandboxes.
- Bandit has been marketed and sold as a service on underground criminal forums since April 2023.
- The malware is written using the Go programming language, which has become increasingly popular with malware developers.

Zscaler ThreatLabz has been tracking a new information stealer called Bandit Stealer that emerged in April 2023. Bandit collects sensitive information from victims' machines including cookies, saved login data, and credit card information from more than a dozen web browsers. The stealer also performs credential theft for popular FTP clients and email clients. Lastly, Bandit targets desktop cryptocurrency wallet applications. All of the stolen information is then exfiltrated back to a command and control (C2) server via Telegram. The malware is written in the Go (a.k.a. Golang) programming language and is especially notable with the large number of attempts to evade virtual environments and automated malware analysis platforms.

Bandit Stealer is marketed and sold as a service in underground cybercriminal forums as shown in Figure 1.

Figure 1: Advertisement for Bandit Stealer on an underground forum

Technical Analysis

Anti-Virtual Machine & Sandbox Identification

Bandit stealer employs a number of anti-analysis techniques to thwart automated and manual analysis. The malware uses the *procfs* Golang library to read information about running processes and checks for the following process names shown below:

- Xen
- Vmware
- VirtualBox
- KVM
- Sandbox
- QEMU
- jail

If a running process matches any of these names, Bandit will terminate execution.

The most recent Bandit samples also check for the presence of a debugger using the Windows API by calling *IsDebuggerPresent* and *CheckRemoteDebuggerPresent*. Bandit attempts to elevate permission using the *runas* command with the username set to Administrator as shown below:

```
C:\Windows\system32\runas.exe runas /user:Administrator
C:\Users\saturn\Desktop\Bandit.exe
```

Bandit also executes the Windows Management Interface command-line (WMIC) utility to obtain the Universally Unique Identifier (UUID) of the victim machine and the screen dimensions using the following commands, respectively:

```
wmic csproduct get uuid
```

```
wmic desktopmonitor get screenheight, screenwidth
```

This information may help threat actors further identify analysis environments. In addition, Bandit uses an extensive list of IP addresses, MAC addresses, computer names, user names, process names to identify virtual environments and associate the environment with security vendors, and therefore avoid exhibiting any malicious behavior. The blacklist information is very similar to that of other prevalent open source stealers including Luna-Grabber, Kyoku-Cookie-Token-Stealer and Creal Stealer.

Bandit obtains the system's external IP address from api.ipify.org and compares it with a list of blacklisted IP addresses shown in the Appendix. Some of these IP addresses belong to antivirus companies, which may be used to block signature updates.

Bandit stealer also retrieves the MAC address of the victim machine using the *GetAdaptersAddresses* Windows API and compares it with a blacklist shown in the Appendix. If there is a match, Bandit exits. Some of these MAC addresses are associated with virtualization software, so the purpose of the blacklist may be to evade malware sandboxes. Bandit Stealer also checks if the victim's username and computer name are present in additional blacklists, which are obtained using " cmd /c net session".

The *CreateToolhelp32Snapshot* Windows API is used to capture the snapshot and traverse along the running process and matches with a list of blacklisted process names and terminates if any process is found executing in the memory shown in the Appendix.

Information Stealing Behavior

Bandit steals web browser data including saved login information, cookies, history, and credit card information stored in the browser's user profile. Bandit targets a long list of browsers as shown in Table 1.

Yandex Browser
Iridium Browser
7Star Browser
Vivaldi Browser
Google Chrome
Orbitum

Sputnik
uCozMedia
Microsoft Edge
Torch Web Browser
Kometa Browser
CentBrowser
BraveSoftware
Amigo Browser
Epic Privacy Browser
SeaMonkey browser
QupZilla

Table 1: Web browsers targeted by Bandit Stealer

The SQLite3 library is used to fetch data and the *CryptUnprotectData* API is used to decrypt cookies and credentials. Credit card information is also stolen, which includes the name, expiration month, year and card number.

Bandit also targets desktop cryptocurrency wallets like Electrum, Exodus, MetaMask, Guarda, Binance, Ethereum as shown in Table 2.

Coinbase wallet extension	Saturn Wallet extension
Binance chain wallet extension	Coin98 Wallet
TronLink Wallet	multibit Bitcoin

Terra Station	Electron Cash
Guildwallet extension	Electrum-btcp
MetaMask extension	Bither Bitcoin wallet
ronin wallet extension	multidoge coin
Kardiachain wallet extension	LiteCoin
Jaxx liberty Wallet	Dash Wallet
Math Wallet extension	Ethereum
Bitpay wallet extension	Exodus
Nifty Wallet extension	Atomic
Armory	Bytecoin Wallet
Coinomi wallet	Monero wallet
dogecoin	

Table 2: Cryptocurrency wallets targeted by Bandit Stealer

Bandit also has the capability to harvest keystrokes and steal clipboard data.

Recent samples of Bandit also target credentials in the following File Transfer Protocol Client (FTP) applications shown in Table 3.

BlazeFTP
NovaFTP
Staff-FTP

EasyFTP
DeluxeFTP
ALFTP
GoFTP
32BitFtp

Table 3: FTP client applications targeted by Bandit

Bandit also targets login information for the email clients shown in Table 4.

MailSpring
Mailbird
Opera Mail
Pocomail

Table 4: Email client applications targeted by Bandit

Stolen data is saved in various files inside a sub-folder in the *%appdata%\local* directory as shown in Figure 2. The sub-folder name is based on the country code and the IP address in the format [country_code][ip_address].

Figure 2: Example information collected by Bandit Stealer

The content of the USERINFO.txt contains a Bandit Stealer header followed by system information as shown in Figure 3.

Figure 3: Example content in the Bandit USERINFO.txt file

Network Communication

Bandit uses the cURL utility which is installed by default since Windows 10 v1803 to transfer data using HTTP, FTP, SMTP and more. Bandit stealer abuses pastebin.com for downloading the blacklist configuration information from a hardcoded URL as shown in Figure 4.

Figure 4: Bandit Stealer blacklist configuration downloaded from Pastebin

After Bandit finishes data collection, this information is sent to the threat actor via Telegram as shown in Figure 5.

Figure 5: Data stolen by Bandit sent to a Telegram channel

The Bandit threat actor has automated the parsing and extraction of the data and responds back with a JSON encoded structure as shown in Figure 6.

Figure 6: Example Bandit C2 response

Conclusion

Bandit Stealer is continuously updated with new features to enhance its data collection functionality. Most recently, Bandit has added support to steal FTP and email credentials. Bandit is also capable of expanding its anti-analysis features with a dynamic configuration downloaded from Pastebin. The abuse of Telegram as a C2 server has also become an increasingly popular technique to evade network-based signatures and make takedown efforts more difficult. All of these factors set up Bandit Stealer to be a potential threat for the foreseeable future.

Zscaler Coverage

Zscaler has ensured coverage for the payloads seen in these attacks via advanced threat signatures as well as Zscaler’s advanced cloud sandbox.

Figure 7: The Zscaler Cloud Sandbox successfully detected the malware

Zscaler's multilayered cloud security platform detects indicators at various levels, as shown below:

Win64_PWS_Bandit

Indicators of Compromise (IOCs)

MD5 Hash Values	Description
17c697da407acacadcaa8fb5c4885179	Bandit Stealer
fdb111c9e0c6b1a94e2bf22131e4266d	Bandit Stealer
700e57847516d1f3e4ebf02e015e9f8d	Bandit Stealer
329562ce914d3d5998ac071333e43c1c	Bandit Stealer
4ab55868b65dc8f16d9d62edfd1893fa	Bandit Stealer
34323d65b744664567c06f8c6076a6b1	Bandit Stealer
2207a896e3e2ac5dae04643e56767dcd	Bandit Stealer
caf4884072724f1d75a6288f27e8e8fe	Bandit Stealer

Appendix

IP addresses blacklisted by Bandit Stealer

88.132.231.71	95.25.204.90	34.105.72.241	193.128.114.45
78.139.8.50	34.145.89.174	109.74.154.92	95.25.81.24
20.99.160.173	109.74.154.90	213.33.142.50	92.211.52.62

88.153.199.169	109.145.173.169	109.74.154.91	88.132.227.238
84.147.62.12	34.141.146.114	93.216.75.209	35.199.6.13
194.154.78.160	212.119.227.151	192.87.28.103	80.211.0.97
92.211.109.160	195.239.51.59	88.132.226.203	34.85.253.170
195.74.76.222	192.40.57.234	195.181.175.105	23.128.248.46
188.105.91.116	64.124.12.162	88.132.225.100	35.229.69.227
34.105.183.68	34.142.74.220	92.211.192.144	34.138.96.23
92.211.55.199	188.105.91.173	34.83.46.130	192.211.110.74
79.104.209.33	109.74.154.91	188.105.91.143	35.237.47.12
178.239.165.70	34.141.245.25	34.85.243.241	87.166.50.213
34.105.0.27	34.145.195.58	193.225.193.201	34.253.248.228
35.192.93.107	195.239.51.3	84.147.54.113	212.119.227.167

MAC addresses blacklisted by Bandit Stealer

00:15:5d:00:07:34	00:50:56:b3:14:59	16:ef:22:04:af:76	42:01:0a:8a:00:22
00:e0:4c:b8:7a:58	ea:02:75:3c:90:9f	00:15:5d:23:4c:ad	00:1b:21:13:32:51
00:0c:29:2c:c1:21	00:e0:4c:44:76:54	1a:6c:62:60:3b:f4	a6:24:aa:ae:e6:12

00:25:90:65:39:e4	ac:1f:6b:d0:4d:e4	00:15:5d:00:00:1d	08:00:27:45:13:10
c8:9f:1d:b6:58:e4	52:54:00:3b:78:24	00:50:56:a0:cd:a8	00:1b:21:13:26:44
00:25:90:36:65:0c	00:50:56:b3:50:de	00:50:56:b3:fa:23	3c:ec:ef:43:fe:de
00:15:5d:00:00:f3	7e:05:a3:62:9c:4d	52:54:00:a0:41:92	d4:81:d7:ed:25:54
2e:b8:24:4d:f7:de	52:54:00:b3:e4:71	00:50:56:b3:f6:57	00:25:90:36:65:38
00:15:5d:13:6d:0c	90:48:9a:9d:d5:24	00:e0:4c:56:42:97	00:03:47:63:8b:de
00:50:56:a0:dd:00	00:50:56:b3:3b:a6	ca:4d:4b:ca:18:cc	00:15:5d:00:05:8d
00:15:5d:13:66:ca	92:4c:a8:23:fc:2e	f6:a5:41:31:b2:78	00:0c:29:52:52:50
56:e8:92:2e:76:0d	5a:e2:a6:a4:44:db	d6:03:e4:ab:77:8e	00:50:56:b3:42:33
ac:1f:6b:d0:48:fe	00:50:56:ae:6f:54	00:50:56:ae:b2:b0	3c:ec:ef:44:01:0c
00:e0:4c:94:1f:20	42:01:0a:96:00:33	00:50:56:b3:94:cb	06:75:91:59:3e:02
00:15:5d:00:05:d5	00:50:56:97:a1:f8	42:01:0a:8e:00:22	42:01:0a:8a:00:33
00:e0:4c:4b:4a:40	5e:86:e4:3d:0d:f6	00:50:56:b3:4c:bf	ea:f6:f1:a2:33:76
42:01:0a:8a:00:22	00:50:56:b3:ea:ee	00:50:56:b3:09:9e	ac:1f:6b:d0:4d:98
00:1b:21:13:15:20	3e:53:81:b7:01:13	00:50:56:b3:38:88	1e:6c:34:93:68:64
00:15:5d:00:06:43	00:50:56:97:ec:f2	00:50:56:a0:d0:fa	00:50:56:a0:61:aa
00:15:5d:1e:01:c8	00:e0:4c:b3:5a:2a	00:50:56:b3:91:c8	42:01:0a:96:00:22
00:50:56:b3:38:68	12:f8:87:ab:13:ec	3e:c1:fd:f1:bf:71	00:50:56:b3:21:29

60:02:92:3d:f1:69	00:50:56:a0:38:06	00:50:56:a0:6d:86	00:15:5d:00:00:b3
00:e0:4c:7b:7b:86	2e:62:e8:47:14:49	00:50:56:a0:af:75	96:2b:e9:43:96:76
00:e0:4c:46:cf:01	00:0d:3a:d2:4f:1f	00:50:56:b3:dd:03	b4:a9:5a:b1:c6:fd
42:85:07:f4:83:d0	60:02:92:66:10:79	c2:ee:af:fd:29:21	d4:81:d7:87:05:ab
56:b0:6f:ca:0a:e7	00:50:56:a0:d7:38	00:50:56:b3:ee:e1	ac:1f:6b:d0:49:86
12:1b:9e:3c:a6:2c	be:00:e5:c5:0c:e5	00:50:56:a0:84:88	52:54:00:8b:a6:08
00:15:5d:00:1c:9a	00:50:56:a0:59:10	00:1b:21:13:32:20	00:0c:29:05:d8:6e
00:15:5d:00:1a:b9	00:50:56:a0:06:8d	3c:ec:ef:44:00:d0	00:23:cd:ff:94:f0
b6:ed:9d:27:f4:fa	00:e0:4c:cb:62:08	00:50:56:ae:e5:d5	00:e0:4c:d6:86:77
00:15:5d:00:01:81	4e:81:81:8e:22:4e	00:50:56:97:f6:c8	3c:ec:ef:44:01:aa
4e:79:c0:d9:af:c3	08:00:27:3a:28:73	52:54:00:ab:de:59	00:15:5d:23:4c:a3
00:15:5d:b6:e0:cc	00:15:5d:00:00:c3	00:50:56:b3:9e:9e	00:1b:21:13:33:55
00:15:5d:00:02:26	00:50:56:a0:45:03	00:50:56:a0:39:18	00:15:5d:00:00:a4
00:50:56:b3:05:b4	12:8a:5c:2a:65:d1	32:11:4d:d0:4a:9e	00:50:56:ae:5d:ea
1c:99:57:1c:ad:e4	00:25:90:36:f0:3b	00:50:56:b3:d0:a7	94:de:80:de:1a:35
00:1b:21:13:21:26			

Hardware IDs blacklisted by Bandit Stealer

7AB5C494-39F5-4941-9163-47F54D6D5016	050C3342-FADD-AEDF-EF24-C6454E1A73C9	BB233342-2E01-718F-D4A1-E7F69D026428	79AF5279-16CF-4094-9758-F88A616D81B4
03DE0294-0480-05DE-1A06-350700080009	4DC32042-E601-F329-21C1-03F27564FD6C	9921DE3A-5C1A-DF11-9078-563412000026	FF577B79-782E-0A4D-8568-B35A9B7EB76B
11111111-2222-3333-4444-555555555555	DEAEB8CE-A573-9F48-BD40-62ED6C223F20	CC5B3F62-2A04-4D2E-A46C-AA41B7050712	08C1E400-3C56-11EA-8000-3CECEF43FEDE
6F3CA5EC-BEC9-4A4D-8274-11168F640058	05790C00-3B21-11EA-8000-3CECEF4400D0	00000000-0000-0000-0000-AC1F6BD04986	6ECEAF72-3548-476C-BD8D-73134A9182C8
ADEEEE9E-EF0A-6B84-B14B-B83A54AFC548	5EBD2E42-1DB8-78A6-0EC3-031B661D5C57	C249957A-AA08-4B21-933F-9271BEC63C85	49434D53-0200-9036-2500-369025003865
4C4C4544-0050-3710-8058-CAC04F59344A	9C6D1742-046D-BC94-ED09-C36F70CC9A91	BE784D56-81F5-2C8D-9D4B-5AB56F05D86E	119602E8-92F9-BD4B-8979-DA682276D385
00000000-0000-0000-0000-AC1F6BD04972	907A2A79-7116-4CB6-9FA5-E5A58C4587CD	ACA69200-3C4C-11EA-8000-3CECEF4401AA	12204D56-28C0-AB03-51B7-44A8B7525250
00000000-0000-0000-0000-000000000000	A9C83342-4800-0578-1EE8-BA26D2A678D2	3F284CA4-8BDF-489B-A273-41B44D668F6D	921E2042-70D3-F9F1-8CBD-B398A21F89C6
5BD24D56-789F-8468-7CDC-CAA7222CC121	D7382042-00A0-A6F0-1E51-FD1BBF06CD71	BB64E044-87BA-C847-BC0A-C797D1A16A50	D8C30328-1B06-4611-8E3C-E433F4F9794E
49434D53-0200-9065-2500-65902500E439	1D4D3342-D6C4-710C-98A3-9CC6571234D5	2E6FB594-9D55-4424-8E74-CE25A25E36B0	00000000-0000-0000-0000-50E5493391EF

49434D53-0200-9036-2500-36902500F022	CE352E42-9339-8484-293A-BD50CDC639A5	42A82042-3F13-512F-5E3D-6BF4FFFD8518	00000000-0000-0000-0000-AC1F6BD04D98
777D84B3-88D1-451C-93E4-D235177420A7	60C83342-0A97-928D-7316-5F1080A78E72	38AB3342-66B0-7175-0B23-F390B3728B78	4CB82042-BA8F-1748-C941-363C391CA7F3
49434D53-0200-9036-2500-369025000C65	02AD9898-FA37-11EB-AC55-1D0C0A67EA8A	48941AE9-D52F-11DF-BBDA-503734826431	B6464A2B-92C7-4B95-A2D0-E5410081B812
B1112042-52E8-E25B-3655-6A4F54155DBF	DBCC3514-FA57-477D-9D1F-1CAF4CC92D0F	032E02B4-0499-05C3-0806-3C0700080009	FA8C2042-205D-13B0-FCB5-C5CC55577A35
00000000-0000-0000-0000-AC1F6BD048FE	FED63342-E0D6-C669-D53F-253D696D74DA	DD9C3342-FB80-9A31-EB04-5794E5AE2B4C	C6B32042-4EC3-6FDF-C725-6F63914DA7C7
EB16924B-FB6D-4FA1-8666-17B91F62FB37	2DD1B176-C043-49A4-830F-C623FFB88F3C	E08DE9AA-C704-4261-B32D-57B2A3993518	FCE23342-91F1-EAFC-BA97-5AAE4509E173
A15A930C-8251-9645-AF63-E45AD728C20C	4729AEB0-FC07-11E3-9673-CE39E79C8A00	07E42E42-F43D-3E1C-1C6B-9C7AC120F3B9	CF1BE00F-4AAF-455E-8DCD-B5B09B6BFA8F
67E595EB-54AC-4FF0-B5E3-3DA7C7B547E3	84FE3342-6C67-5FC6-5639-9B3CA3D775A1	88DC3342-12E6-7D62-B0AE-C80E578E7B07	365B4000-3B25-11EA-8000-3CECEF44010C
C7D23342-A5D4-68A1-59AC-CF40F735B363	DBC22E42-59F7-1329-D9F2-E78A2EE5BD0D	5E3E7FE0-2636-4CB7-84F5-8D2650FFEC0E	63FA3342-31C7-4E8E-8089-DAFF6CE5E967
63203342-0EB0-AA1A-4DF5-3FB37DBB0670	CEFC836C-8CB1-45A6-ADD7-209085EE2A57	96BB3342-6335-0FA8-BA29-E1BA5D8FEFBE	8DA62042-8B59-B4E3-D232-38B29A10964A

44B94D56-65AB-DC02-86A0-98143A7423BF	A7721742-BE24-8A1C-B859-D7F8251A83D3	0934E336-72E4-4E6A-B3E5-383BD8E938C3	3A9F3342-D1F2-DF37-68AE-C10F60BFB462
6608003F-ECE4-494E-B07E-1C4615D1D93C	3F3C58D1-B4F2-4019-B2A2-2A500E96AF2E	12EE3342-87A2-32DE-A390-4C2DA4D512E9	F5744000-3C78-11EA-8000-3CECEF43FEFE
D9142042-8F51-5EFF-D5F8-EE9AE3D1602A	D2DC3342-396C-6737-A8F6-0C6673C1DE08	38813342-D7D0-DFC8-C56F-7FC9DFE5C972	AF1B2042-4B90-0000-A4E4-632A1C8C7EB1
49434D53-0200-9036-2500-369025003AF0	EADD1742-4807-00A0-F92E-CCD933E9D8C1	FE455D1A-BE27-4BA4-96C8-967A6D3A9661	4D4DDC94-E06C-44F4-95FE-33A1ADA5AC27
8B4E8278-525C-7343-B825-280AEBCD3BCB			

Usernames blacklisted by Bandit Stealer

WDAGUtilityAccount	server	8VizSM
Abby	BvJChRPnsxn	w0fjuOVmCcP5A
hmarc	Harry Johnson	lmVwjj9b
patex	SqgFOf3G	PqONjHVwexsS
RDhJ0CNFevzX	Lucas	3u2v9m8
kEecfMwgj	mike	Julia
Frank	PateX	HEUeRzl

8Nl0ColNQ5bq	h7dk1xPr	fred
Lisa	Louise	RGzcBUyrznReg
John	User01	PxmdUOpVyx
george	test	

Computer names blacklisted by Bandit Stealer

BEE7370C-8C0C-4	WILEYPC	DESKTOP-CBGPFEE
DESKTOP-NAKFFMT	WORK	SERVER-PC
WIN-5E07COS9ALR	6C4E733F-C2D9-4	TIQIYLA9TW5M
B30F0242-1C6A-4	RALPHS-PC	DESKTOP-KALVINO
DESKTOP-VRSQLAG	DESKTOP-WG3MYJS	COMPNAME_4047
Q9IATRKPRH	DESKTOP-7XC6GEZ	DESKTOP-19OLLTD
XC64ZB	DESKTOP-5OV9S0O	DESKTOP-DE369SE
DESKTOP-D019GDM	QarZhrdBpj	EA8C2E2A-D017-4
DESKTOP-WI8CLET	ORELEEPC	AIDANPC
SERVER1	ARCHIBALDPC	LUCAS-PC
LISA-PC	JULIA-PC	MARCI-PC
JOHN-PC	d1bnJkfVlH	DESKTOP-1PYKP29
DESKTOP-B0T93D6	NETTYPC	DESKTOP-1Y2433R

DESKTOP-BUGIO

Process names blacklisted by Bandit Stealer

httpdebuggerui	vmwareuser
wireshark	vgauthservice
fiddler	vmacthlp
regedit	x96dbg
cmd	vmsrvc
taskmgr	x32dbg
vboxservice	vmusrvc
df5serv	prl_cc
processhacker	prl_tools
vboxtray	xenservice
vmtoolsd	qemu-ga
vmwaretray	joeboxcontrol
ida64	ksdumperclient
ollydbg	ksdumper
pestudio	joeboxserver