



ZEROFOX[®]

Your Intelligence Digest

**It's a Digital World.
Engage Securely.**

New Automated Shop Provides Threat Actors With Remote Access To Target Networks

Untested threat actor “omgo” announced a new automated shop, dubbed “Omgo”, providing threat actors with remote access to unspecified target networks on the predominantly Russian language Deep Web forum “XSS”. The shop provides access to networks via compromised Windows machines, web servers, and administrator panels. The shop has various instances available, including:

- Remote desktop (RDP)
- Secure shell (SSH)
- Web shell
- cPanel

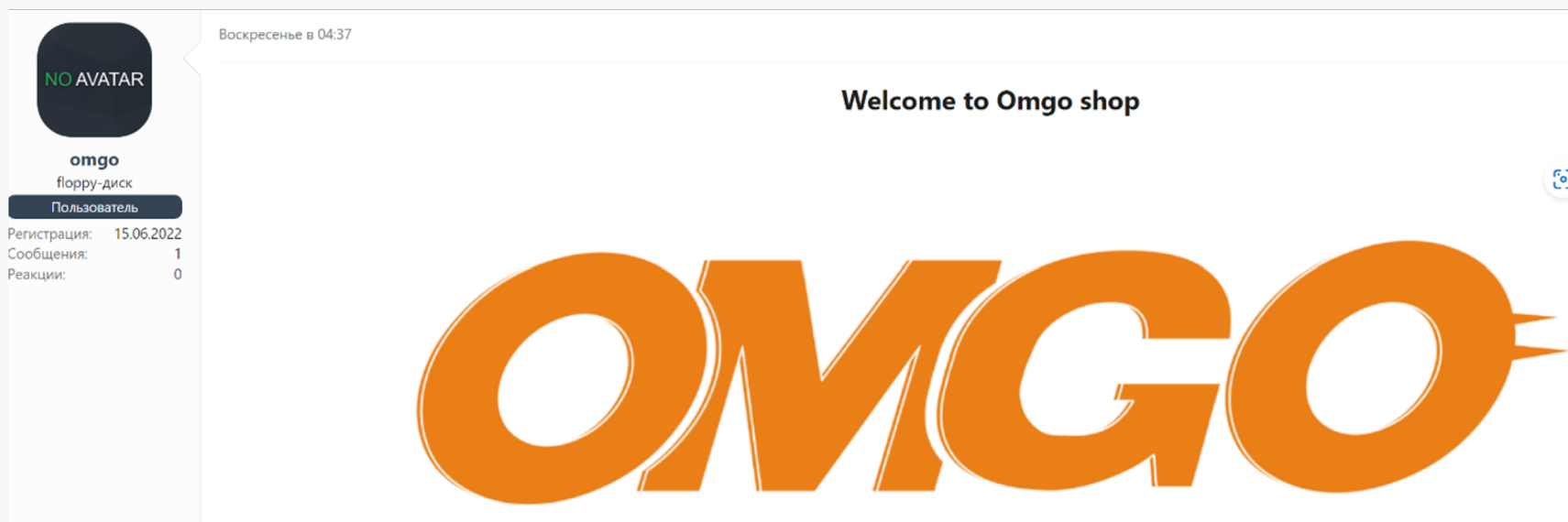
Additionally, the shop has standard items found across most Deep and Dark Web stores, including:

- Accounts (both self-registered and compromised)
- Payment cards
- Email addresses (AKA leads)
- Website traffic
- Compromised account credentials

ZeroFox researchers assess this new shop is likely to fill an emerging need in the underground economy because currently there are a limited number of reliable stores selling this type of access at affordable prices.

Original post from threat actor "omgo" announcing a new automated shop, dubbed "Omgo", providing threat actors with remote access to unspecified target networks

New Automated Shop Provides Remote Access (Cont.)



Actor Shares Method To Defraud Hurricane Ian Relief Efforts

Well-regarded and established threat actor “Crd_The_Wrld” shared a method to defraud disaster relief efforts for victims of Hurricane Ian in the U.S. on the predominantly Russian language Deep Web forum “CrdClub”. The method involves using the stolen personally identifiable information (PII) of Florida residents to fraudulently apply for loans at [fema\[.\]gov](https://fema.gov) or [disasterassistance\[.\]gov](https://disasterassistance.gov). The straightforward nature of this method indicates the program likely lacks the proper security controls to prevent fraud.

ZeroFox researchers assess the exploitation of Hurricane Ian relief efforts is likely widespread, since threat actors are now sharing their methods to defraud the program for free instead of selling them for profit.

FLORIDA DISASTER BENEFIT

👤 Crd_The_Wrld · 🕒 Yesterday at 1:08 AM



Crd_The_Wrld

VIP MEMBER

Joined:	16.01.22
Messages:	95
Reaction score:	55
Points:	18

Yesterday at 1:08 AM

1. Go to <https://fema.gov> or <https://disasterassistance.gov>
2. Go to Find Assistance.
3. Choose all of them (mark all the boxes)
4. Choose (Rent,Yes,Relocating)
5. Choose (No,Yes,No) then with number (9), choose Florida
6. Click on Apply Now.
7. You will be asked to put word there and click on Submit.

Telegram Channel Regularly Leaks Unique Datasets To Subscribers

ZeroFox researchers identified a Telegram channel, dubbed “A r e s”, that regularly leaks unique datasets to subscribers for a subscription fee. The channel shares the personally identifiable information (PII) and sensitive documents of victims from all over the world, including:

- U.S. citizens
- Iranian citizens
- Russian military
- Indonesian Consulate General in Guangzhou, China

The channel also provides samples of less valuable datasets and previously leaked data for free.

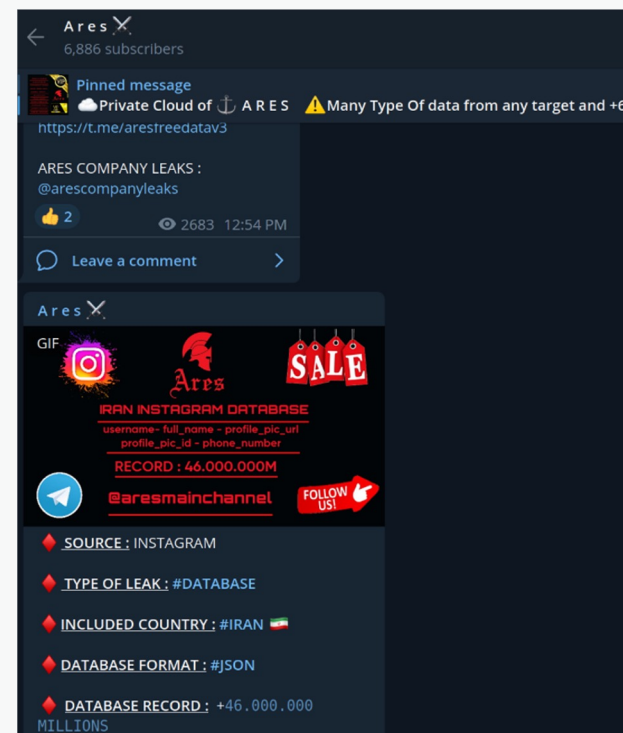
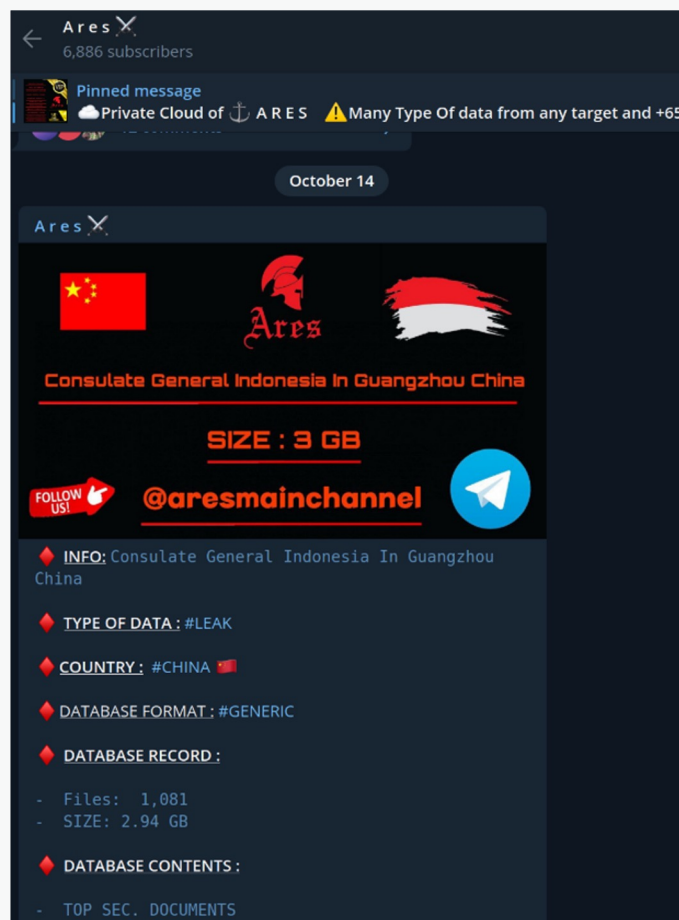
Prices to subscribe to the channel vary depending on the length of the license, including:

- \$400 USD for one-month
- \$800 USD for three-months
- \$1,500 USD for six-months
- \$5,000 USD for life

ZeroFox researchers assess the growth of this channel will likely lead to an increase in fraudulent operations, since many threat actors require stolen PII for phishing or spam campaigns, account takeovers, and credential stuffing attacks.

Screenshots of two leaked databases available on the Telegram channel "Ares"

Telegram Channel Leaks Datasets To Subscribers (Cont.)



Automated Service Steals OTP SMS Codes

New and untested threat actor “bototp” advertised an automated service to steal one-time password (OTP) SMS codes on the predominantly Russian language Deep Web forum “Club2Crd”. This service would likely increase a threat actor’s chances of successfully compromising accounts with multi-factor authentication enabled. In addition to stealing OTP codes, the service can:

- Send spam text messages
- Spoof phone numbers
- Decode the keys victims press by analyzing tones
- Make robocalls with threat actor’s preferred script

Threat actors can operate the service from a web panel or mobile application.

ZeroFox researchers assess the actor is likely credible because multiple peers have already vouched for the service, including the moderately credible threat actor “choco10”.

