



ZEROFOX[®]

Your Intelligence Digest

It's a Digital World.
Engage Securely.

New Ransomware Project Open To Affiliates

New and untested threat actor “mysteryghost” announced a new ransomware-as-a-service (RaaS) project on the Russian language Dark Web forum “RAMP”. This is the first time since November 2021 that ZeroFox researchers have observed a ransomware group open an affiliate program to the public. The actor dubbed the new program “Luna”, which is said to target machines running different operating systems and hypervisors, including:

- Windows
- Unix
- ESXI

Additional features of the ransomware include:

- Written in Rust
- Encrypts files using Advanced Encryption Standard (AES)
- Most antivirus products do not detect it as malicious

The actor claims that project developers will also provide affiliates with the necessary infrastructure to carry out ransomware attacks, including cryptocurrency wallets, email addresses, and communication channels.

The actor specified that they are only willing to work with Russian-speaking threat actors. Profits from any successful ransom payments will be split 85/15 in favor of project developers. ZeroFox researchers note this is a drastic shift, as other RaaS affiliates typically earn a larger share of the spoils.

Original post from threat actor "mysteryghost" announcing a new ransomware-as-a-service (RaaS) project dubbed "Luna".

New Ransomware Project Open To Affiliates (Cont.)

RaaS Luna 85/15 Rust

mysteryghost · Friday at 8:56 PM

Forums > Market \ 市场 > Partners Program \ RaaS \ 合作伙伴计划

[Jump to new](#) [Watch](#)



mysteryghost
Jan 13, 2022

Messages	1
Reaction score	0
Points	1

Friday at 8:56 PM

rust aes + x25519
85/15
win/*nix/esxi
только почты, только русскоязычные пользователи.
почты ваши, кошельки ваши, общение ваше.
поддержка локера от детектов (03.06 все топовые ав пропускают локер)

2792FFB9D8329374D8FE9D604F76E5C45F35CF3BB33423FE0669EAB97E6C753DD1DF1C535688

[Report](#)

[New](#) [←](#) [🔖](#) [#1](#)

[Like](#) [Reply](#)

New SMS Spamming Service Announced

New and untested threat actor “BetaGateway” announced a new SMS spamming service, named “Beta Route”, on the Russian language Deep Web forum exploit[.]in. The service features a web-based GUI where users can easily launch spam campaigns by sending SMS messages to mobile phones in various countries, including:

- U.S.
- U.K.
- Germany
- Australia

Additional features of the service include:

- Automatically refills account’s balance
- Sends fake alerts from financial institutions
- Test routes for fastest delivery rate
- Specify routes to prioritize messages

The actor also claims to have leads, or lists containing victim PII, that users can leverage to target specific individuals based on their mobile carrier or geographic region.

ZeroFox researchers assess that this new service is likely to be successful since it streamlines the spamming process, lowering the barrier for entry to threat actors.

Original post from
threat actor
"BetaGateway"
announcing their new
SMS spamming service
dubbed "Beta Route".

New SMS Spamming Service Announced (Cont.)

B SMS Gateway - ALL CONTENT - Automatic route selection - Automatic Deposit
By BetaGateway, Saturday at 02:10 PM in [Spam] - mailings, databases, responses, mail-dumps, software

Follow 2

Start new topic

Reply to this topic

BetaGateway

byte

B

Paid registration

1 post

Joined

06/04/22 (ID: 131433)

Activity

cnam / spam

Posted Saturday at 02:10 PM (edited)

Beta Route

NEW SPAM GATEWAY!

We are proud to finally announce the launch of our new SMS gateway! Below you'll find some key features of our new gateway that will ensure you have the most powerful SMS tools at your fingertips. This gateway allows all content that you want to send, without restrictions! You'll be able to fire away all your campaigns with high DLR (Delivery rate) **at cheap prices!**

Key features:

- Bank Senders Supported
- Automatic top-up system
- Auto-Test routes
- Select routes yourself
- Over 44+ countries supported

Want to get started right away? Register below to get started!

<https://beta.smsroute.to/register>

With us you are in safe hands! We ensure you'll be met with a professional team if you ever need help or if issues would ever occur. We support a lot of countries, here is a list of current **supported countries:**

Australia, Brazil, China, **Germany**, Spain, France, **United Kingdom**, Ireland, India, Italy, Korea, Netherlands, Poland, Portugal, **United States**, Belgium, New Zealand, Norway, Chile, Canada, Sweden, Greece, Philippine, United Arab Emirates, Finland, Lithuania, Thailand, Taiwan, Israel, Bahrain, Denmark, Singapore, Turkey, Hong Kong, Estonia, Switzerland, Czech Republic, Mexico, Malaysia, Ukraine, Austria

We always strive to add new countries once we've found routes. If you want to get a country added that isn't on the list, contact the team!

We also have **leads**, we have Carrier MIX Leads (First and Last name), GEO Dedicated Leads filtered by Gender, Age and City, **Business Owner Leads**, **Business Leads**, **High income Leads**, **Dedicated Bank Leads!**

Contact us today to get a quote on the leads!

Our landing page can be found here:

<https://beta.smsroute.to/>

Threat Actors Warn Against Using Telegram For Fraudulent Operations

In early May 2022, ZeroFox researchers observed two new and untested threat actors, “swift_” and “Silverman”, share a news article on the Deep Web forums “Exploit” and “KickAss”, respectively, indicating that Telegram had recently shared user data with federal authorities in Germany.

Based on the traction these threads have gained from reputable members of both forums, ZeroFox researchers assess that some threat actors may begin to move away from using Telegram for their fraudulent operations in favor of other secure messaging services, such as Jabber or TOX.

ZeroFox first observed the threat actor “Swift_” warn “Exploit” users against using Telegram for fraudulent operations, opting instead to use Jabber servers hosted in countries allegedly outside of U.S. jurisdiction. These include:

- China
- Vietnam
- Ukraine
- Switzerland

Threat actor “Silverman” mentioned the previous thread on “KickAss”, echoing the same sentiment against using Telegram for business. The well-regarded threat actor and administrator of the forum, “NSA”, later replied to this thread, claiming that they have always opposed Telegram.

Original posts from threat actors "swift_" and "Silverman" warning threat actors against using Telegram for fraudulent operations.

Threat Actors Warn Against Using Telegram (Cont.)



Telegram shares user data with police - Use XMPP!

By swift_, Saturday at 07:57 AM in Software

swift_
byte



Paid registration

2

14 posts

Joined

05/13/22 (ID: 130415)

Activity

кардинг / carding

Posted Saturday at 07:57 AM

I never trust Telegram. I say this for a long time. Do not conduct business on Telegram. Now here is proof:

Telegram has released user data to the Federal Criminal Police Office of Germany in several cases:
<https://www.spiegel.de/netzwelt/apps/telegram-gibt-nutzerdaten-an-das-bundeskriminalamt-a-0e4d3fcb-8081-4b87-b062-db412bbc294b>

[XMPP / Jabber for private, security communications](#)

Here are some of my favorite servers which I know are secure and also outside of U.S. law (can not be sized by the U.S. government).

xmpp.cn - host in China
xmpp.vn - host in Vietnam
jabber.ua - Host in Ukraine
darknet.im- they have many domains and host in Switzerland

and of course, exploit.im !

I hope this article reminds you to stop using telegram for your business!

Do NOT use Telegram. They share with police.



Silverman

Junior Member

Progress: 33%

Posts: 13

Threads: 7

Reputation: 0

This should be obvious by now. Telegram = major OPSEC fail. Everyone always asks me for my Telegram account. Why???

When did people become too lazy to use XMPP?

I found this article on Exploit:

Telegram has released user data to the Federal Criminal Police Office of Germany in several cases:
<https://www.spiegel.de/netzwelt/apps/telegram-gibt-nutzerdaten-an-das-bundeskriminalamt-a-0e4d3fcb-8081-4b87-b062-db412bbc294b>

OP also gives some good XMPP servers to use that can not be seized by U.S. government.

xmpp.cn - hosted in China
xmpp.vn - Vietnam
jabber.ua - Host in Ukraine
darknet.im - Switzerland

Database Containing The PII Of 19 Million U.S. Voters Advertised

The well-regarded and established threat actor “Malbar” advertised a database allegedly containing the PII of 19 million U.S. voters, on the Russian language Deep Web forum “XSS”. The actor claimed to have 60 GB of sensitive data compiled from different, unspecified elections that took place between February 2013 and February 2022. The alleged data includes:

- Full name
- Gender
- Ethnicity
- Date of birth
- Physical Address
- Email address
- Phone number
- Voter ID
- Election ID
- Voting precinct
- Voting method
- Date and time ballot cast
- Party affiliation

The actor did not specify a price for the database, stating they are open to negotiations. The actor also agreed to use an escrow service, indicating they likely possess said data.

Original post from threat actor "Malbar" advertising a database that allegedly contains the PII of 19 million U.S. voters.

Database Containing The PII Of 19 Million U.S. Voters (Cont.)

USA voters, elections 19kk lines +

Malbar · Friday at 08:51 · phone+mail+name+full_address+dob usa voters

IN THIS THEME YOU CAN USE AN AUTOMATIC GUARANTOR!

[+ New deal](#)



Malbar
Premium

Sign up: 12.07.2020
Messages: 555
Reaction: 332
Guarantor of the transaction: 3

Today at 09:36

Welcome Sell
database you are a company for organizing district elections, conducting surveys, advertising, campaigning, analysis, etc. by conducting companies in social networks, SMS mailing, ringing.
Data on 60 GB (csv)
Database consists of 25 tables as follows:
voter_district_profiles 436.9 kk rows

id	voter_id	district_id	created_at	updated_at
503269065	20098206	77655486	7/7/2017 05:02:55	7/7/2017 05:02:55
503269066	20098207	77655486	7/7/2017 05:02:55	7/7/2017 05:02:55