



ZEROFOX[®]

Your Intelligence Digest

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

Threat Actor Selling 'Qyick' Ransomware

Untested threat actor “lucrostm” advertised a ransomware variant dubbed “Qyick”, on the English language Dark Web forum “CryptBB.” According to the actor, this variant follows the growing trend of ransomware gangs utilizing intermittent encryption for their projects. This technique allows operators to encrypt a victim’s files faster than traditional methods and avoid detection by most antivirus products by only encrypting a portion of the targeted files’ content during an attack. Additional features of the ransomware include:

- Written in Go
- Prevents Event Tracing for Windows (ETW) from logging system events
- Malware executes on all target machines on network at the same time
- Obfuscates malicious C2 communications

The actor specified that the current ransomware version does not support an automated method for data exfiltration. However, the actor plans to add this functionality in the future.

If legitimate, ZeroFox researchers assess that a deal involving the sale of “Qyick” ransomware would very likely lead to the proliferation of new ransomware gangs, since most established, Russian-speaking ransomware groups typically offer affiliate programs instead of selling their projects outright.

Original post from threat actor "lucrostm" advertising a ransomware variant dubbed "Qyick"

Threat Actor Selling 'Qyick' Ransomware (Cont.)

Qyick ransomware ~ FUD ~ Private customization ~ 0 tax UPDATED 1.02



lucrostm •
Junior
Member

Posts: 7
Joined: Mar 2022
Reputation: 3

#1

08-30-2022, 09:46 PM

Wrote in Golang from scratch, it's "simple" yet very high quality, making it highly versatile and useful.

It uses many cutting-edge evasion techniques including proprietary methods.

Notably Qyick features intermittent encryption which is what the cool kids are using as you read this. Combined with the fact that is written in go, the speed is unmatched.

Each build is unique.

It is fully undetected and has been battle-tested, profiting millions in the right hands, 100x-ing the investment.

Verified Financial Services Accounts For Sale

New and untested threat actor “Stealthway” advertised verified accounts for different financial services, and their corresponding PII, on the predominantly Russian language Deep Web forum “Exploit.” Capable threat actors could almost certainly leverage these accounts to cash out stolen funds or commit other fraud, since the accounts are verified using real, compromised data. The shop, also known as “Stealthway,” has various accounts available, including:

- PayPal
- Apple Pay
- Venmo
- Coinbase
- Binance
- BlackCatCard
- Revolut

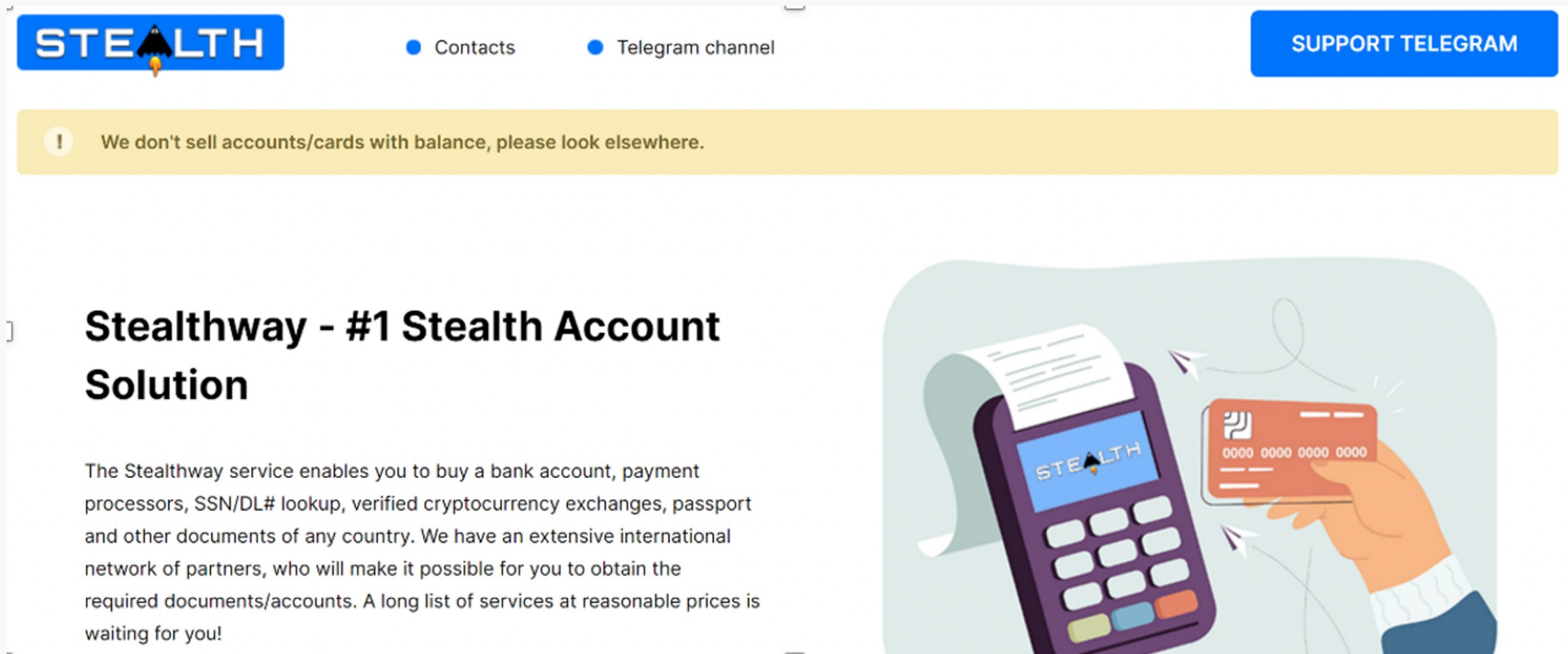
After purchase, the actor claims that buyers will also receive a copy of the stolen PII that was used to verify the accounts.

The shop also has scanned copies of documents containing sensitive data of victims from all over the world that threat actors are highly likely to use for identity theft, including:

- SSNs
- Driver’s licenses
- Passports
- Photos of victims holding IDs
- Credit scores
- Background checks

Screenshot from
"Stealthway" shop
selling verified
accounts for different
financial services and
PII

Verified Financial Services Accounts For Sale (Cont.)



The screenshot shows the Stealthway website interface. At the top, there is a blue header with the "STEALTH" logo (a penguin icon) on the left, navigation links for "Contacts" and "Telegram channel" in the center, and a blue button labeled "SUPPORT TELEGRAM" on the right. Below the header is a yellow banner with an information icon and the text: "We don't sell accounts/cards with balance, please look elsewhere." The main content area features the heading "Stealthway - #1 Stealth Account Solution" followed by a paragraph: "The Stealthway service enables you to buy a bank account, payment processors, SSN/DL# lookup, verified cryptocurrency exchanges, passport and other documents of any country. We have an extensive international network of partners, who will make it possible for you to obtain the required documents/accounts. A long list of services at reasonable prices is waiting for you!" To the right of the text is an illustration of a purple calculator with the "STEALTH" logo on its screen, a receipt coming out of the top, and a hand holding a red credit card with the number "0000 0000 0000 0000".

STEALTH ● Contacts ● Telegram channel **SUPPORT TELEGRAM**

! We don't sell accounts/cards with balance, please look elsewhere.

Stealthway - #1 Stealth Account Solution

The Stealthway service enables you to buy a bank account, payment processors, SSN/DL# lookup, verified cryptocurrency exchanges, passport and other documents of any country. We have an extensive international network of partners, who will make it possible for you to obtain the required documents/accounts. A long list of services at reasonable prices is waiting for you!

Custom Fraud Bots Service Advertised

New and untested threat actor “ATOM INC” advertised a service to develop custom bots for fraudulent operations, on the predominantly Russian language Deep Web forum “WWH-Club.” ZeroFox researchers are observing an uptick in more threat actors automating their operations on secure messaging applications, like Telegram or Discord, as these platforms are free to use and offer more security and flexibility than traditional Deep or Dark Web marketplaces.

The actor claims that they can build custom Telegram bots with obfuscated code, offering better security to bad actors, including attempts to reverse engineer the source code to reveal the true identities of both buyers and sellers. The actor also claims to develop custom bots for VK and Discord.

If legitimate, ZeroFox researchers assess this service is likely to expand, with the growing interest in automation, and because the actor is allegedly recruiting for an affiliate program.

VIP

ATOM INC | Reverse / Software development, Telegram bots, WEB-sites

ATOM INC

Saturday at 22:14

TC



ATOM INC

Platinum Member

Project participant

Sign up:

13 Aug 2022

Messages:

3

Reaction:

0

General Sales:

\$0

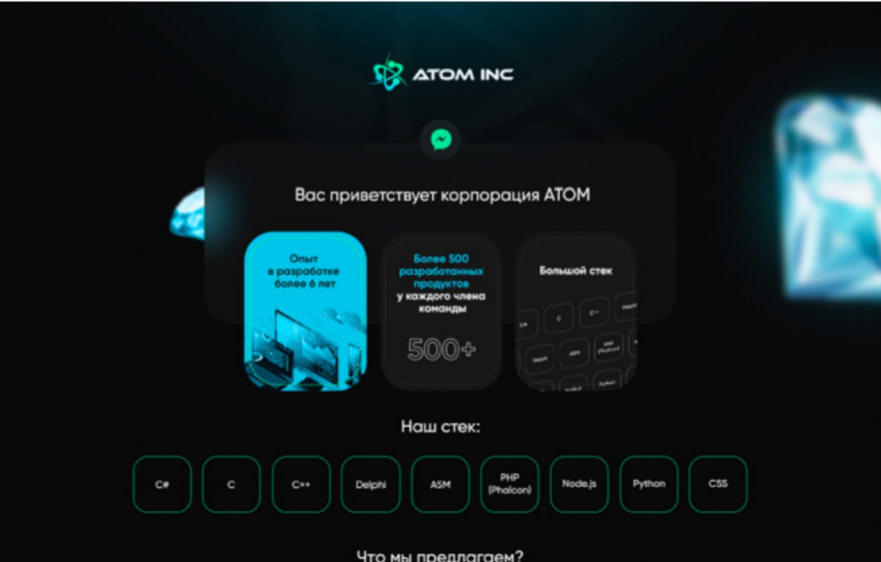
General Purchases:

\$5,409

Donated:

\$0

Saturday at 22:14



Threat Actor Offering Spamming & Phishing Infrastructure Setup

Moderately credible threat actor “Anunnaki” advertised a service to install the infrastructure needed to perform spamming and phishing campaigns at scale, on the predominantly Russian language Deep Web forum “XSS.” The actor claims to utilize a setup to ensure that a high volume of spam messages will be successfully delivered to the inboxes of the intended victims.

Despite the actor’s lack of credibility on the forum, ZeroFox researchers assess this service is likely to facilitate successful spam and phishing campaigns, as the actor agreed to use an escrow service, requiring them to make a deposit before brokering a deal.

ZeroFox researchers note that the actor is likely offering this service in response to automated competitors, since similar tools leveraging automation cannot adapt to changes in anti-spam policies or other fraud management tools as quickly as competitors that rely more on manual functionality.

