



ZEROFOX®

Your Intelligence Digest

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

Zero-Day Exploit Targets RCE Vulnerability In SonicWall SSL VPN

New and positively trending threat actor “eliotto” advertised what they alleged to be a zero-day exploit for an RCE vulnerability in SonicWall SSL VPN, on the Russian language Dark Web forum “RAMP”. According to the actor, the exploit allows an unauthenticated user to remotely execute malicious code on any SSL VPN-compatible SonicWall device. The actor is asking \$100,000 USD for the exploit.

The same actor gained positive feedback on the forum after listing their first zero-day exploit for Quantum storage devices in January 2022, indicating expertise in this area and a potentially functioning exploit for SonicWall SSL VPN.

ZeroFox researchers note that this is the second SonicWall zero-day exploit advertised in the month of February. The first observation was on February 5, 2022 when untested threat actor “0x_0day” advertised their SonicWall SSL VPN exploit on the Dark Web Russian language forum Exploit. This threat actor charged \$15,000 for the exploit, but did not provide further details.

Dell SonicWALL SSLVPN Pre-Auth root RCE

eliotto · Thursday at 9:54 PM

Forums > Market \ 市场 > Malware \ 恶意软件



eliotto

Dec 20, 2021

Messages	25
Reaction score	4
Points	3

Thursday at 9:54 PM

Привет, продаю Dell SonicWALL SSLVPN Pre-Auth root RCE
Уязвимые модели - все. Все пружфы - пм или контакты
Прайс: 100k\$

Report

New Malware Loader Service Compromises Android Devices Via Google Play

Well-regarded threat actor, and known ransomware operator, “gustavedore” advertised their service to compromise Android devices via malicious applications hosted on Google Play, on the Russian language Dark Web forum “RAMP”. Unlike similar services offering malicious applications, the actor claims to provide fully functional infrastructure, including:

- Domains
- Servers
- SSL certificates

The actor also claims to create Google Play Developer accounts to manage and publish malicious applications. Another tactic the actor claims to utilize is seeking out and purchasing pre-existing mobile applications on Google Play to later weaponize.

The malware is controlled from a web panel, where threat actors are provided with different payloads to choose from, including banking trojans and botnet stealers. The panel logs any instances where malware is successfully downloaded or installed to a target Android device.

The actor charged approximately \$2,800 USD for their service.

Original post from
threat actor
"gustavedore"
advertising their
malware loader service

New Malware Loader Service Via Google Play Cont.

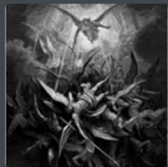
Android Loader on Google Play

gustavedore · Friday at 10:03 PM

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

Jump to new Watch

Reply



gustavedore

Nov 4, 2021

Messages	16
Reaction score	13
Points	3

Friday at 10:03 PM

Android Loader on Google Play

Вашему вниманию предоставляется сервис по разработки лоадеров под ключ! Лоадеры работают как часы, имеют конверт около 20-35%, а так же очень конфигурируемы за счет панели управления, а так же умного сервиса на устройстве.

Веб панель:

Правила

New

< > #1

More Threat Actors Migrating To ‘J-Shop’ To Buy Stolen Payment Card Data

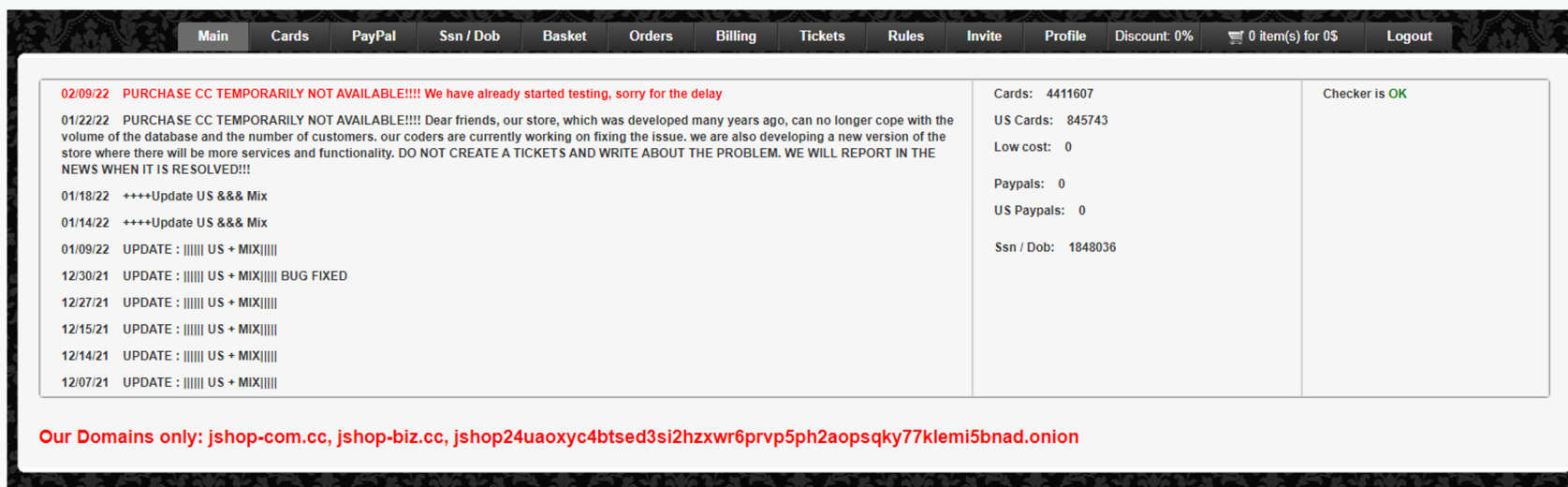
ZeroFox is observing a large migration of threat actors to the carding shop “J-Shop”. The shop is one of the oldest and most trusted marketplaces to buy stolen payment card data in the underground. ZeroFox researchers note that this new surge in activity comes one-year after the shutdown of “Joker’s Stash”, which left a void in the carding world that has yet to be filled by a single marketplace.

Since December 2021, ZeroFox researchers have observed at least eight new batches of stolen payment cards uploaded to “J-Shop”. During this time, administrators have briefly halted purchasing on the shop several times so developers could make the necessary changes on the backend to accommodate the influx of new customers.

In addition to stolen payment cards, “J-Shop” sells the PII of victims from the U.S. The marketplace also features a tool that threat actors can leverage to determine if stolen payment card numbers are valid or not.

A screenshot highlighting some of the most recent activity on “J-Shop”

More Threat Actors Migrating To ‘J-Shop’ Cont.



The screenshot shows the J-Shop website interface. At the top is a navigation bar with links: Main, Cards, PayPal, Ssn / Dob, Basket, Orders, Billing, Tickets, Rules, Invite, Profile, Discount: 0%, 0 item(s) for 0\$, and Logout. The main content area is divided into two columns. The left column contains a list of updates, with the most recent one dated 02/09/22 stating that credit card purchases are temporarily unavailable due to database issues. The right column displays account information, including the card number 4411607, US Cards count of 845743, and a status of 'Checker is OK'. At the bottom, a red banner displays the website's domains.

Date	Update
02/09/22	PURCHASE CC TEMPORARILY NOT AVAILABLE!!!! We have already started testing, sorry for the delay
01/22/22	PURCHASE CC TEMPORARILY NOT AVAILABLE!!!! Dear friends, our store, which was developed many years ago, can no longer cope with the volume of the database and the number of customers. our coders are currently working on fixing the issue. we are also developing a new version of the store where there will be more services and functionality. DO NOT CREATE A TICKETS AND WRITE ABOUT THE PROBLEM. WE WILL REPORT IN THE NEWS WHEN IT IS RESOLVED!!!
01/18/22	++++Update US &&& Mix
01/14/22	++++Update US &&& Mix
01/09/22	UPDATE : US + MIX
12/30/21	UPDATE : US + MIX BUG FIXED
12/27/21	UPDATE : US + MIX
12/15/21	UPDATE : US + MIX
12/14/21	UPDATE : US + MIX
12/07/21	UPDATE : US + MIX

Our Domains only: jshop-com.cc, jshop-biz.cc, jshop24uaoxyc4btsed3si2hzxwr6prvp5ph2aopsqky77klemi5bnad.onion

Threat Actors Take Notice Of Tax Season

More threat actors are harvesting and selling the personal information of victims from the U.S., as the deadline for filing federal tax returns approaches. ZeroFox researchers have observed at least two high-profile cases so far in 2022, including the moderately credible threat actor “AK-74M”, advertising a database that they claim contains the sensitive tax documents of U.S. victims, on the Russian language forum xss[.]is. Compromised data includes:

- SSNs
- Dates of birth
- Bank account numbers
- Driver’s license numbers
- Credit reports

The actor is asking \$8,000 USD for the database.

Additionally, ZeroFox identified untested threat actor “ciisco”, who is selling administrator access to the internal network of an unspecified U.S. tax company, on the Russian language Deep Web forum club2crd[.]cc. Like “AK-74M”, the actor also claims to have access to sensitive tax documents and victim PII.

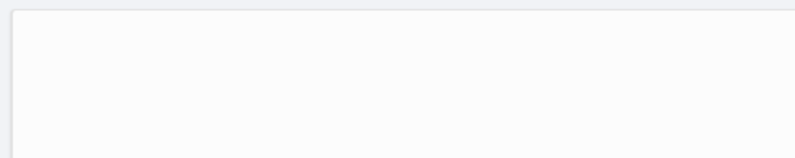
The actor is asking \$5,000 USD for access to the network. They also required escrow to facilitate payment, indicating that they are more likely to have a foothold in the network.

Original posts from threat actors “AK-74M” and “ciisco” advertising sensitive tax documents (left) and access to the internal network of an unspecified U.S. tax company (right)

Threat Actors Take Notice Of Tax Season Cont.

USA Tax Return database + access (W2 , W-9 , 1099, W-4)

AK-74M · 10.01.2022 · fulls ssn database tax tax return





AK-74M
Премиум

Регистрация: 07.11.2021
Сообщения: 37
Реакции: 3

15.01.2022

Website Database with Documents for Tax Returns. W2. W-9.

Price: \$8k
More info and communication in PM.

Код:

- SSN - DOB
- W-2
- W-4
- W-9
- 1099
- Bank Acc #s
- Drivers Lic
- SSA
- Credit Reports
- Other Data

16-01-2022, 10:12

ciisco
Senior Member



Price : 0.12BTC / \$5000

Admin Level Access to Tax Company in USA.
|W2 |W9 |1099 |DL |SSN |Credit Reports etc

Screenshots and Proof in private.

strictly through guarantor.

PM for contact.

Join Date: May 2017

Location: $x^3+y^3+z^3=k$

Posts: 197

Reputation: 1 [+/-]

Balance: 0.00\$