



ZEROFOX[®]

Your Intelligence Digest

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

New Ransomware Variant Targets Systems Running Windows 11

New and untested threat actor “Cod_Fish” announced one of the first new ransomware variants that ZeroFox researchers have observed targeting Windows 11 on the Russian language Dark Web forum “RAMP”. The actor shared various articles, indicating this is likely a new version of Thanos ransomware. Features include:

- Works with systems that run Windows XP through Windows 11
- Erases backup copies of files and Recycle Bin
- Terminates database-related processes to prevent accessing backups
- Automatically enables network discovery and file sharing
- Spreads to remote systems connected to same network
- Mimics explorer.exe process
- Contains anti-sniffer to detect systems monitoring network traffic for sensitive data

The actor also claimed that their service includes obfuscation of the payload. However, the actor specified that the ransomware is not native and has .NET 4 software dependencies.

Pricing varies, depending on the length of the license:

- \$4,000 USD for six-months
- \$8,000 USD for one-year
- \$12,000 USD for a lifetime

ZeroFox researchers highlight this finding to demonstrate recent ransomware activity in the underground. Although this post seems more credible than the Groove ransomware announced on RAMP (a hoax by threat actors) researchers cannot rule out the possibility that this is also a hoax.

Translated post from threat actor "Cod_Fish" announcing new ransomware variant.

New Ransomware Variant Targets Windows 11 Cont.



Cod_Fish
Jan 20, 2022
Messages 1
Reaction score 0
Points 1

Friday at 12:59 PM

Application for pentesting, confidential data securing and transporting employing insecure means.
Never had a single bad review or arbitration opened.

Features:

- Works in the form of a builder to create an small worker application that performs all the job.
- OS compatible from Windows XP to Windows 11. Server from Server 2008 and up.
- Not possible to decrypt algorithm (RSA 4096).
- You can create any number of new encryption keys and old ones are always saved.
- Shadow copies and recycle bin erased.
- Databases processes terminated as well as optional generic memory cleaner available.
- Two main modes of operation (many more available). Static for decoding many PC's with a single decryptor or dynamic to decode each PC individually.
- Can work in user or elevated mode.
- UAC bypass.
- Files to be secured can be selected by size, extension or you can simply encode all files (automatically bypassing important OS files).
- NAS, QNAP, Synology, Hyper-V.
- Webdav, DFS, local homegroup, local shares.
- Files uploader which can select files by extension and size.
- Automatic enabling of Network discovery, file sharing, SMB1 enabling, Linked connections.
- Multi-threading and IOCP which assures fast data processing.
- Entire LAN securing is possible by detecting remote resources and tool self-replication to all PC's in the LAN if remote execution is allowed.
- Fast files cataloging by means of master file table direct access.
- Processing files in memory and not as temporary files is optional.
- Multiple tools for debugging results, which include: process log, debug log, real time console report.
- Recovery note is fully customizable (file name, content, location to drop) with relevant data both in text as well as in html format, at windows logon or at boot time. Even windows logon password can be changed.
- Enhanced notifications. Includes, taskbar icon notification of process finished, Windows logon recovery note shown.
- Encoding in safe mode possible for non UEFI OS.

New Shop Selling Access To Bots To Distribute Malware

Threat actor “GreatSupport” is advertising a new shop selling access to malware infected gaming computers (AKA bots) on a Dark Web forum. Threat actors may purchase access to compromised machines to infect with additional malware.

The actor claimed that malware can be loaded onto 200-300 gaming computers per day. The actor specified that most of their bots were located in the U.S. or EU countries. Unlike similar services, a threat actor who purchased a bot from this shop would obtain exclusive access to it and not have to share the access with other threat actors who purchased the same resource.

Even though the actor claims access to negate the User Account Control (UAC) on the infected gaming computers, they specified that buyers would still need to obfuscate their own payloads to avoid being detected as malicious by most antivirus products.

The actor had a minimum order of 100 downloads for \$50 USD.

Original post from
threat actor
"GreatSupport"
advertising their new
shop selling access to
bots that can be used
to distribute malware

New Shop Selling Access To Bots To Distribute Malware Cont.

Bot Shop | Selling REAL un-shared Downloads | Gaming Traffic | Not Installs



GreatSupport •
Junior
Member
••

Posts: 12
Joined: Aug 2021
Reputation: 

Yesterday, 11:27 AM #1

Welcome to GreatSupport's Bot Shop.

As everyone here probably knows, most installs that you find on various forums are shared between up to 10 customers, which is pointless in my eyes and not suitable for every operation.

I am here to offer you REAL Downloads coming from gaming traffic, with an execution rate of up to 80%. This means that no one has access to your bots except yourself, as those bots are not coming from a stream, but from gaming traffic.

Each bot downloads your payload and executes it by themselves, execution rate is up to 80%. Those bots do not come from a loader and you are their real owner, as if you were spreading yourself. Bots execute through UAC no problem. SmartScreen / Chrome is no problem, as your file is distributed in a passworded archive.

Statistics Link is given to you through RapidShare or other services which count downloads.

Bots come from gaming traffic and therefore mostly have gaming PC's, mostly coming from USA and EU. No Indian shit.

- about 50-60% have 6GB+ GPU
- 15-20% 4GB+ GPU
Rest is CPU.

Currently, I can offer 200-300 downloads daily.

For this to work, your file has to bypass Windows Defender, as else its pointless and you won't get results that you aim for. Bypassing other AV's is a good plus too.

Minimum Order: 100 Downloads
Price per Download: 0,50\$ BTC / XMR.

Contact: PM / XMPP [OTR] on Profile

Internal Network Access To Unnamed U.S. Financial Services Company For Sale

Threat actor “vespa” (AKA “wasp” in English) is selling internal network access to compromised systems of an unnamed U.S. financial services company on the Russian language Deep Web forum exploit[.]in. This is significant as U.S. targets have fallen off most public network access listings since the DarkSide ransomware gang was accused of attacking the Colonial Pipeline last year, shutting down the largest gas pipeline in the U.S. for several days in May 2021. The actor claimed to have administrator access to various databases and customer relationship management (CRM) systems containing the PII of more than 22,000 clients and 6,400 payment cards.

The actor shared scanned copies of sensitive documents as proof, including:

- Social Security cards
- Passports
- Driver’s licenses

Additionally, the actor claimed to have access to client email and password combinations for Equifax and two other CRM portals.

The actor is auctioning this access, with an initial bid of \$20,000 USD, a minimum bid of \$1,000 USD, and an instant purchase price of \$30,000 USD.

Since network access deals of this price are typically only exploitable by more experienced threat actor groups, ZeroFox researchers assess this deal is intended for existing, successful ransomware operators.

Original post from threat actor "vespa"(AKA "wasp" in English), who is selling internal network access to compromised systems owned by an unnamed U.S. financial services company

Access To Unnamed U.S. Financial Services Company For Sale Cont.

 **USA CRM Финансы**
By vespa, 5 hours ago in Auctions

wasp
byte

User
1
10 posts
Joined
02/09/18 (ID: 85422)
Activity
другое

Posted 5 hours ago (edited)

I will sell access to the office that deals with fin. Services. country
USA Type of access: web-shell,phpmyadmin(root),crm admin access

In the database of 22k clients for each full info. ssn+dob+ almost every dock, as well as in the database 6.4k ss almost all without cvv(But for new ones you can do to write cvv

code) Also customers have a login and password to access equifax and two similar offices Every month ~ 180 clients are added

Start:20k

Step:1k

Blitz:30k

<https://www.sendspace.com/file/ezww1v>

<https://www.sendspace.com/file/opq8fo>



The screenshot shows a web application interface. On the left, there is a table with columns 'Title', 'Folder Name', and 'As'. The table contains four rows: 'front of file', 'Front of File', 'SS', and 'ID/PP'. To the right of the table is a large image of a Social Security card. The card displays the text 'SOCIAL SECURITY', 'THIS NUMBER HAS BEEN ESTABLISHED FOR', '04-9524', 'RECEIVED', 'AMERICAN', 'SIGNATURE', and '09/05/2017'. On the right side of the interface, there is a sidebar with a list of links: 'Client Summary', 'Client Details', 'Comments', 'Updates', 'Activities', 'Emails', 'Tickets', 'Documents', and 'Invoice'. The 'Documents' link is highlighted in red.

Actor Seeks Partner To Provide Ransomware To Their Team Of Insiders

New and untested threat actor “EricJapier”, on the Russian language Deep Web forum exploit[.]in, is seeking a partner to help them carry out ransomware attacks against various companies in France, where they claim to have insiders working. The actor claims that their insiders span different industries, including:

- Banking
- Insurance
- Real estate
- Automotive

The actor offered to split any funds they earned 50-50 with a partner who could provide them with ransomware. They specified that they would pass the malware along to their insiders, who the actor claims are willing to infect machines within the target companies by walking up to their boss’ computers and plugging in USB drives armed with malware.

Depending on the outcome of their first job together, the actor states that they would be open to a long-term partnership. If successful, the actor indicated that they would turn their attention to companies in Spain and Switzerland.



Original post from threat actor "EricJapier" seeking partner to provide their team of insiders with ransomware

Actor Seeks Partner To Provide Ransomware To Insiders Cont.

E

FRANCE: HAVE PEOPLE IN IMPORTANT COMPAGNIES TO INFECT THEM / ПОСТАВЬТЕ ЛЮДЯМ В ВАЖНЫХ КОМПАНИЯХ, ЧТОБЫ ЗАРАЗИТЬ ИХ

By EricJapier, Yesterday at 09:10 AM in [Job] - search, execution of work

Follow 1

Start new topic

Reply to this topic

EricJapier

byte

•

E

Paid registration

@ 0

2 posts

Joined

01/30/22 (ID: 124919)

Activity

вирусология / malware

Posted yesterday at 09:10 AM

Hello. I know some people that are working in important compaignies. For exemple : banks , insurance, real estate , car concessionary.

I'm looking for a partner that provide some programs to infect / ransom the compaignies. I propose 50 %-50% deal (payment of the people that will help us inside included).

There is some in important job , some in less important job but that has no fear to go at the boss's computer and plug an USB stick. Because I'm handling most of those person by making believe to them it is not risked. If our first jobs go well. Then I hope to find partner for a long time.

Every compaignies are in France. I our jobs are success I can find some in Switzerland and Spain.

Thanks for you read. I'll now use google traduction to put this message in Russian. Sorry if there is some language mistake !

Fell free to send me a PM or add my telegram @thief75 or my icq : @thief75