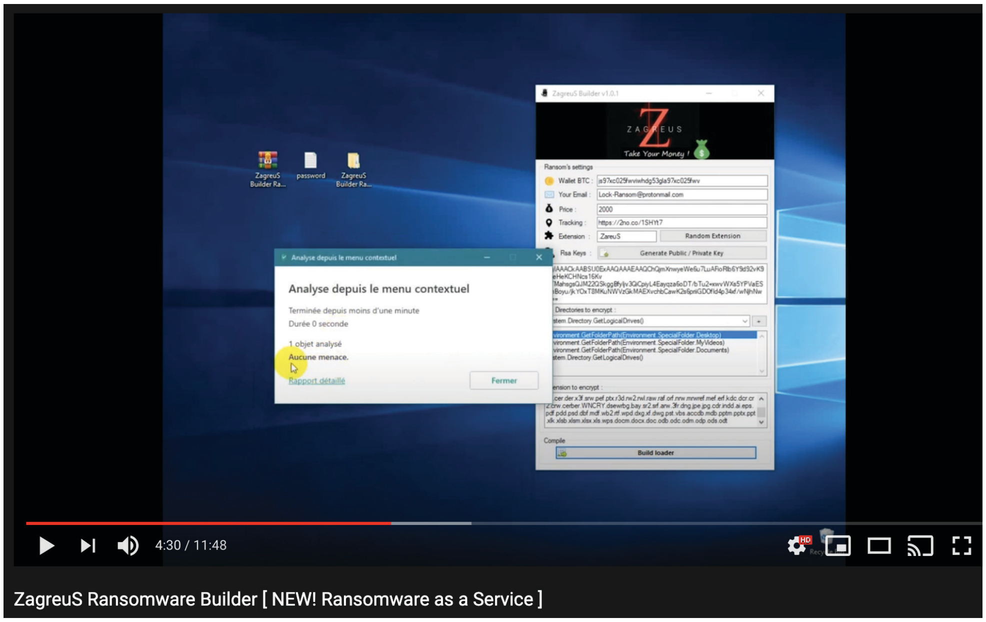
Pulse Report:
Ransomware-as-a-Service Becomes Increasingly Accessible via Social Media and Open Sources

Hackers need not search the dark web for access to their very own ransomware platforms these days. Cybercriminals are continually finding new ways to promote their underground businesses and gain the attention of new customers and novice hackers. Several threat actors have recently taken to popular social media and open sources like YouTube, Vimeo, and Sellix to advertise and demonstrate their discount-priced $40 ransomware-as-a-service (RaaS) builder called ZagreuS.



Wallet BTC : js97xc025fwviwhdg53gla97xc025fwv
Your Email : Lock-Ransom@protonmail.com
Price : 2000
Tracking : https://2no.co/1SHYt7
Extension : .ZareuS
Rsa Keys :

```
lAAACkAABSU0ExAAQAAAEAAQChQjmXnwyeWe6u7LuAFioRlb6Y9d92vK9
eHeKCHNcs16Kv
TMahsgsQJM22QSkggBfyljv3QiCpiyL4Eayqza6oDT/bTu2+xwvWXs5YPVaES
Boyu/jkYOxT8MKuNWVzGkMAEXvchbCawK2s6pniGDOfld4p34xf/wNjhNw
==
```

```
stem.Directory.GetLogicalDrives()
vironment.GetFolderPath(Environment.SpecialFolder.Desktop)
vironment.GetFolderPath(Environment.SpecialFolder.MyVideos)
vironment.GetFolderPath(Environment.SpecialFolder.Documents)
stem.Directory.GetLogicalDrives()
```

```
.cer.der.x3f.srw.pef.ptx.r3d.rw2.rwl.raw.raf.orf.nrw.mrwref.mef.erf.kdc.dcr.cr
2.crw.cerber.WNCRY.dsewrbg.bay.sr2.srf.arw.3fr.dng.jpe.jpg.cdr.indd.ai.eps.
pdf.pdd.psd.dbf.mdf.wb2.rtf.wpd.dxg.xf.dwg.pst.vbs.accdb.mdb.pptm.pptx.ppt
.xlk.xlsb.xlsm.xlsx.xls.wps.docm.docx.doc.odb.odc.odm.odp.ods.odt
```

Analyse depuis le menu contextuel

Analyse depuis le menu contextuel

Terminée depuis moins d'une minute
Durée 0 seconde

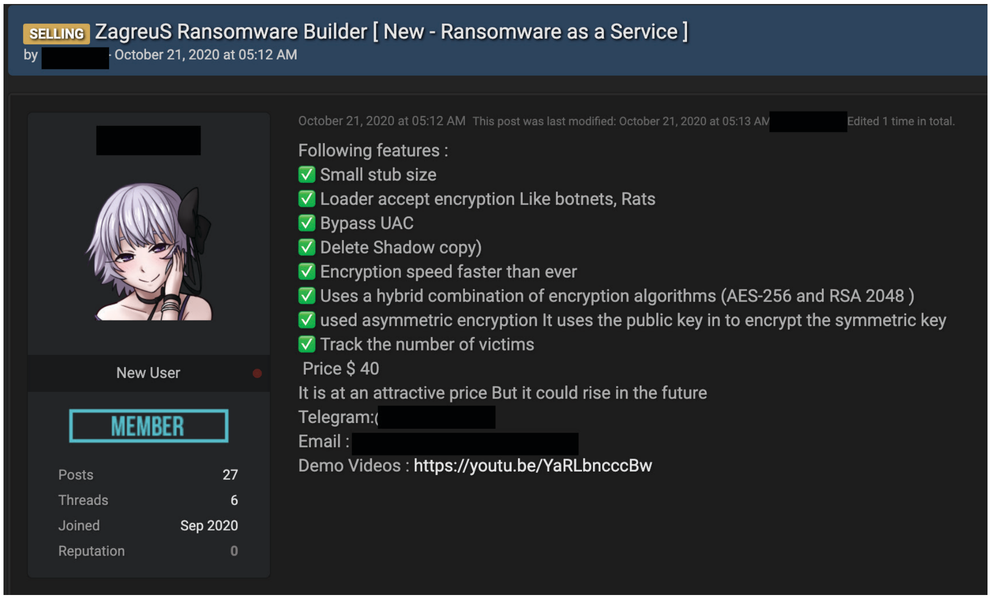
1 objet analysé
Aucune menace.

ZagreuS Ransomware Builder [NEW! Ransomware as a Service]

YouTube video demonstration of the ZagreuS ransomware builder. (Source: Recorded Future)

The ZagreuS ransomware offers several attractive and easy-to-use features that make it accessible and manageable for low-level beginner hackers. According to the sellers, the ransomware features include:

- Asymmetric encryption. Uses a hybrid combination of AES-256 and RSA-2048 algorithms to lock files on the target machine.
- It deletes shadow copies and is claimed to encrypt files at a very high speed.
- Claims to bypass UAC.
- Built-in loader that can be customized to drop additional payloads such as RATs (remote-access trojans).
- The attacker can monitor the number of victims infected with the ransomware.
- Easy personalization. Enter your contact information and bitcoin address for fast payment.



SELLING ZagreuS Ransomware Builder [New - Ransomware as a Service]
by [redacted] October 21, 2020 at 05:12 AM

[redacted]

New User

MEMBER

Posts	27
Threads	6
Joined	Sep 2020
Reputation	0

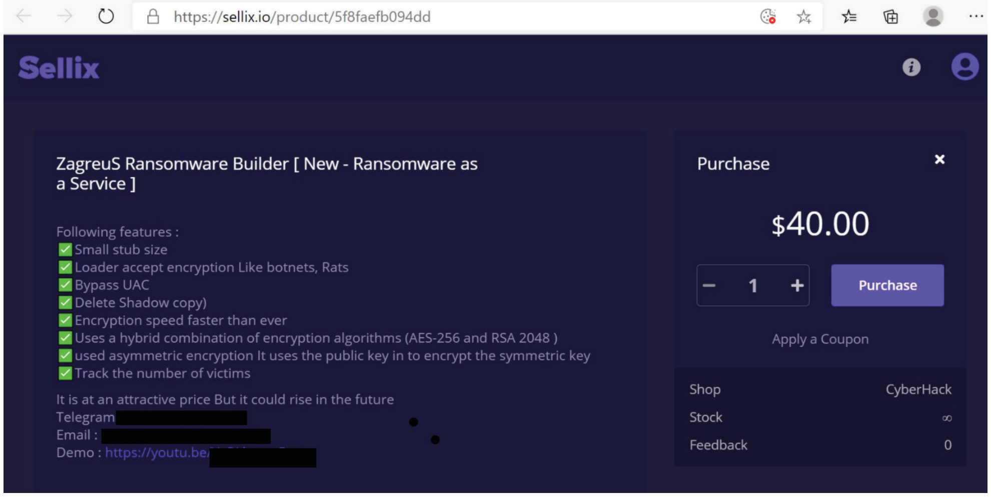
October 21, 2020 at 05:12 AM This post was last modified: October 21, 2020 at 05:13 AM [redacted] Edited 1 time in total.

Following features :
✅ Small stub size
✅ Loader accept encryption Like botnets, Rats
✅ Bypass UAC
✅ Delete Shadow copy)
✅ Encryption speed faster than ever
✅ Uses a hybrid combination of encryption algorithms (AES-256 and RSA 2048)
✅ used asymmetric encryption It uses the public key in to encrypt the symmetric key
✅ Track the number of victims
Price $ 40
It is at an attractive price But it could rise in the future
Telegram:([redacted]
Email : [redacted]
Demo Videos : https://youtu.be/YaRLbncccBw

A new user advertised the ZagreuS features on a deep web hacking forum. (Source: Recorded Future)

According to the original seller, ZagreuS is designed for attacking larger networks of companies, enterprises, and hospitals. The 11-minute demo video posted on YouTube describes that the seller will receive a 30 percent commission for each ransom collected, while the remaining 70 percent is kept by the operator/buyer. The ransomware builder is currently trending at a low price of $40 USD, paid in cryptocurrency to the sellers wallet.

Several interested buyers left comments on the sale posts on underground forums inquiring if anyone had tested the ZagreuS builder, and expressed interest in trying it out. Typically, in these instances, the low price of the builder is an indication that the seller is lacking experience or that the tool is not very valuable. Insikt Group has found that most often, the tool does not function well, can be easily decrypted, and it can be very difficult for the "affiliates" criminals to make a profit off of their victims.



https://sellix.io/product/5f8faefb094dd

Sellix

ZagreuS Ransomware Builder [New - Ransomware as a Service]

Following features :
✅ Small stub size
✅ Loader accept encryption Like botnets, Rats
✅ Bypass UAC
✅ Delete Shadow copy)
✅ Encryption speed faster than ever
✅ Uses a hybrid combination of encryption algorithms (AES-256 and RSA 2048)
✅ used asymmetric encryption It uses the public key in to encrypt the symmetric key
✅ Track the number of victims

It is at an attractive price But it could rise in the future
Telegram [redacted]
Email : [redacted]
Demo : https://youtu.be/ [redacted]

Purchase ×

$40.00

− 1 + Purchase

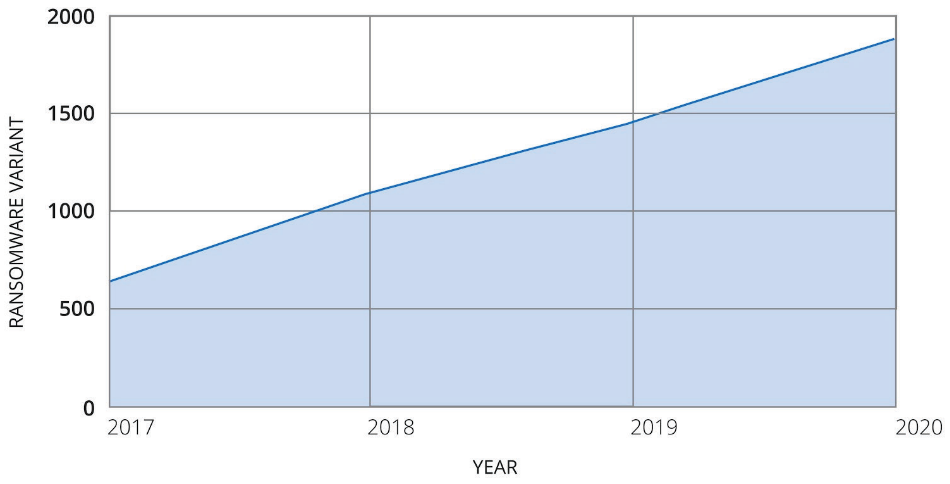
Apply a Coupon

Shop	CyberHack
Stock	∞
Feedback	0

This threat actor cross-posted their advertisement for ZagreuS ransomware builder on YouTube and Sellix.io

Many online platforms and social media applications are aware of these advertisements and work to have them removed. When this particular demo video was removed from the original YouTube channel, the threat actor quickly uploaded it again under a different link and pivoted to other platforms for clear web and deep web marketing, including sellix.io, RAID forums, hackforums, and Github.

Ransomware Variant Coverage by Year



(Source: Recorded Future)

Ransomware has stolen the cybercrime stage in the past year, quickly becoming one of the most damaging and prevalent forms of cyber attacks. Industries such as state and local government, healthcare, and finance have taken an especially hard hit from ransomware attacks in the past year, and it does not appear to be slowing down. There are currently over 1,800 variants of ransomware, with the top 45 variants bringing in the most ransom money.

Although the barrier of entry for threat actors to get into ransomware has been lower than ever, very few criminals make a profit off of these low-cost, simple RaaS tools. However, those that are successful have taken advantage of the situation and have increased ransom demands. Some are even practicing double exploitation of their victims -- demanding a ransom, and still releasing the victims' personal data for sale on underground forums after they have paid.

For more information on security intelligence to defend against ransomware threats, visit www.recordedfuture.com.

Recorded Future®

www.recordedfuture.com

@RecordedFuture

About Recorded Future

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams by informing decisions in real time with contextual, actionable intelligence. By analyzing data from open, dark, and proprietary sources, Recorded Future offers a singular, integration-ready view of threat information, risks to digital brand, vulnerabilities, third-party risk, geopolitical risk, and more.