The Rebranded Crypter: ScrubCrypt

perception-point.io/blog/the-rebranded-crypter-scrubcrypt/

January 10, 2023

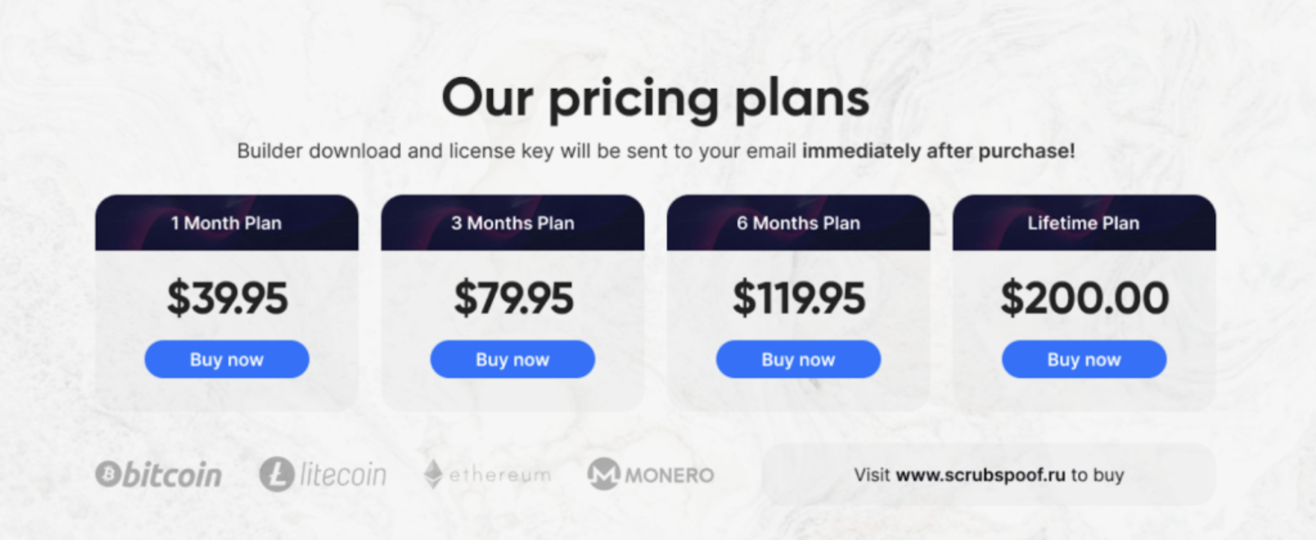
Over the past few weeks, Perception Point's IR team has been investigating a Crypter, spread wildly via phishing emails that ultimately deliver RAT (Remote Access Trojan) malware from the Xworm family.

A Crypter is a type of software used to encrypt, or hide, files or data so that they can be protected from unauthorized access. It uses strong encryption algorithms to ensure the data remains secure from attackers. However, it can also be used to encrypt, obfuscate, or manipulate malware to make it harder for AV's to detect. In this blog we review the ScrubCrypter and its origin, where threat actors can easily buy the Crypter, and how attackers use phishing campaigns to distribute the Crypter and its accompanying malware.

What is ScrubCrypt?

ScrubCrypt is a Crypter currently sold on HackForums, a hacking forum in the clear web, that anyone can access from their device.

The price of the Crypter is 40 USD for a monthly subscription and goes up to 200 USD for a lifetime subscription.



Our pricing plans

Builder download and license key will be sent to your email **immediately after purchase!**

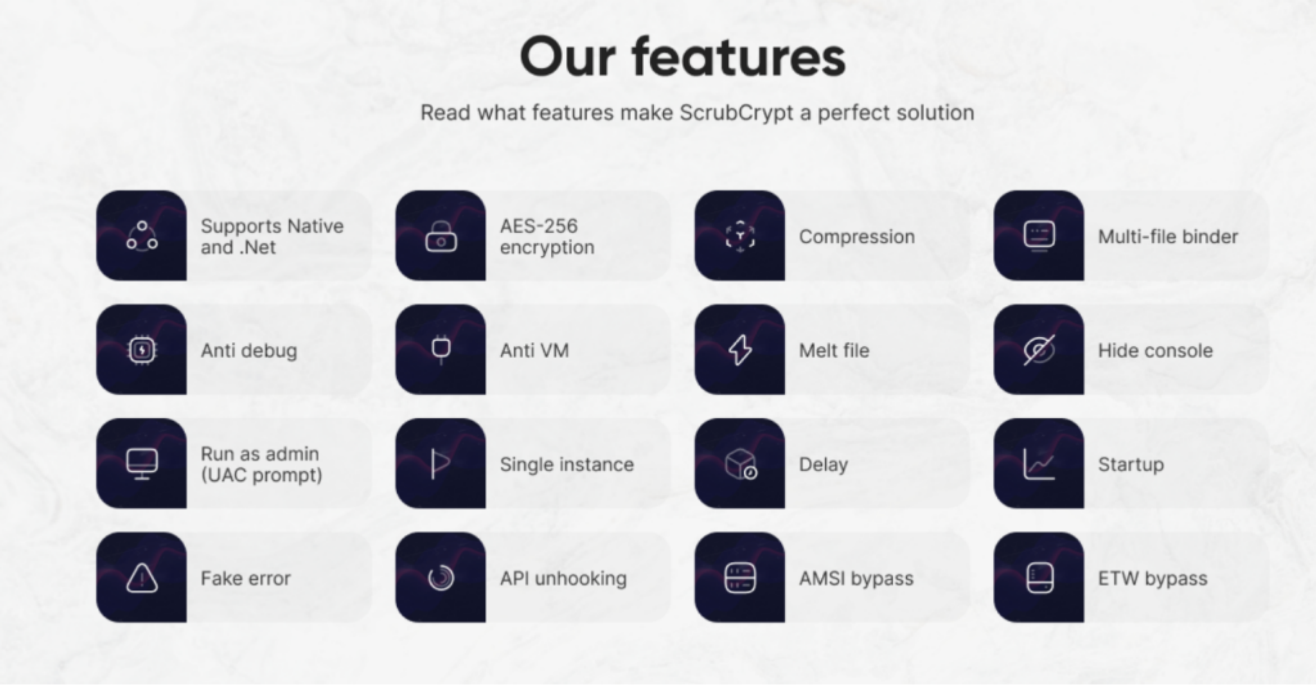
1 Month Plan	3 Months Plan	6 Months Plan	Lifetime Plan
$39.95	$79.95	$119.95	$200.00
Buy now	Buy now	Buy now	Buy now

Visit **www.scrubspoof.ru** to buy

Figure 1: ScrubCrypt pricing plan

The seller of the Crypter “Scrubspoof” provides a list of Crypter features, which include:

- AES Encryption
- Anti VM/Debug
- Persistence mechanism



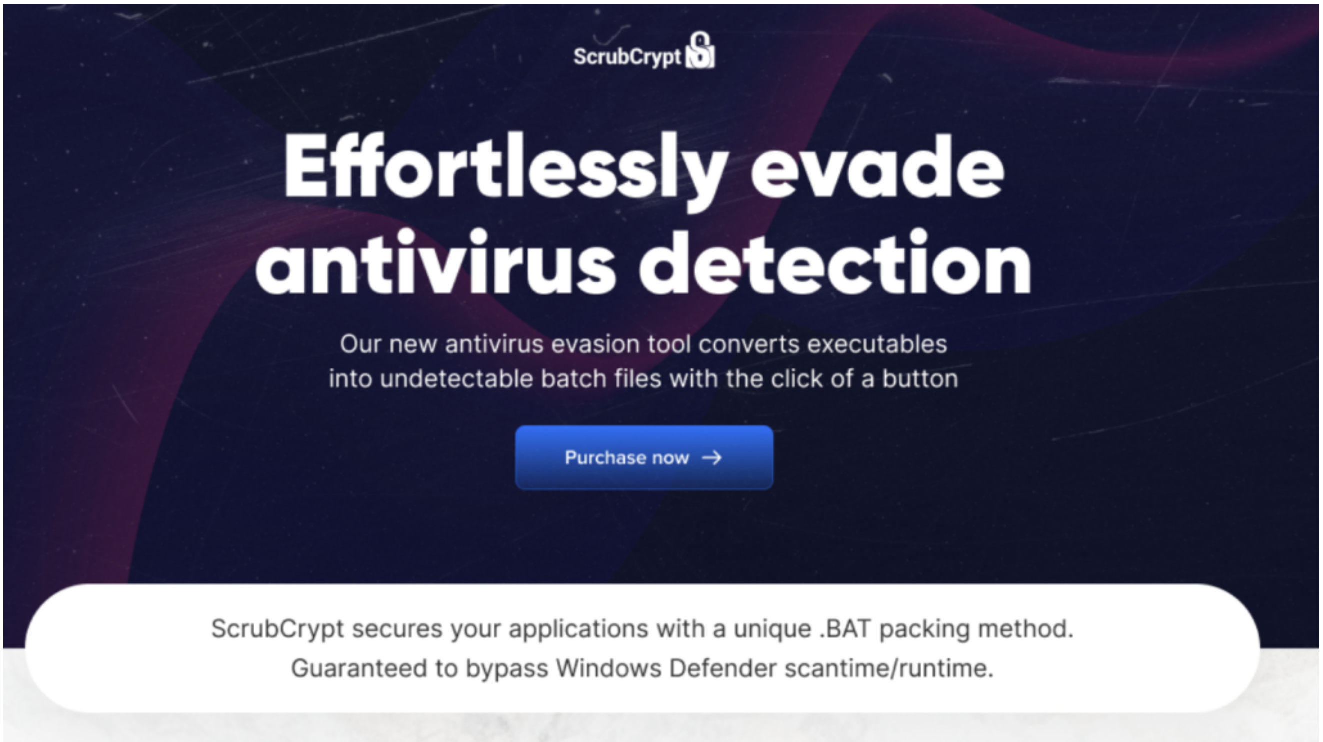
Our features

Read what features make ScrubCrypt a perfect solution

Supports Native and .Net	AES-256 encryption	Compression	Multi-file binder
Anti debug	Anti VM	Melt file	Hide console
Run as admin (UAC prompt)	Single instance	Delay	Startup
Fake error	API unhooking	AMSI bypass	ETW bypass

Figure 2: ScrubCrypt feature list

The seller describes the Crypter as an “antivirus evasion tool [that] converts executables into undetectable batch files”.



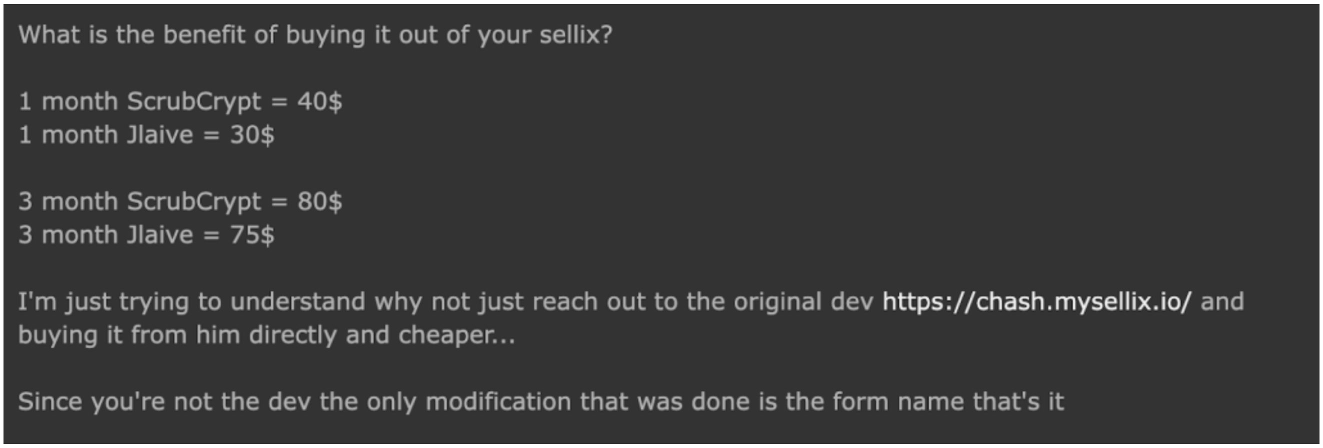
Effortlessly evade antivirus detection

Our new antivirus evasion tool converts executables into undetectable batch files with the click of a button

ScrubCrypt secures your applications with a unique .BAT packing method. Guaranteed to bypass Windows Defender scantime/runtime.

Figure 3: ScrubCrypt value proposition

Customers can leave a review about the Crypter in the HackForum post thread. One interesting comment we stumbled upon was as follows:



What is the benefit of buying it out of your sellix?

1 month ScrubCrypt = 40$
1 month Jlaive = 30$

3 month ScrubCrypt = 80$
3 month Jlaive = 75$

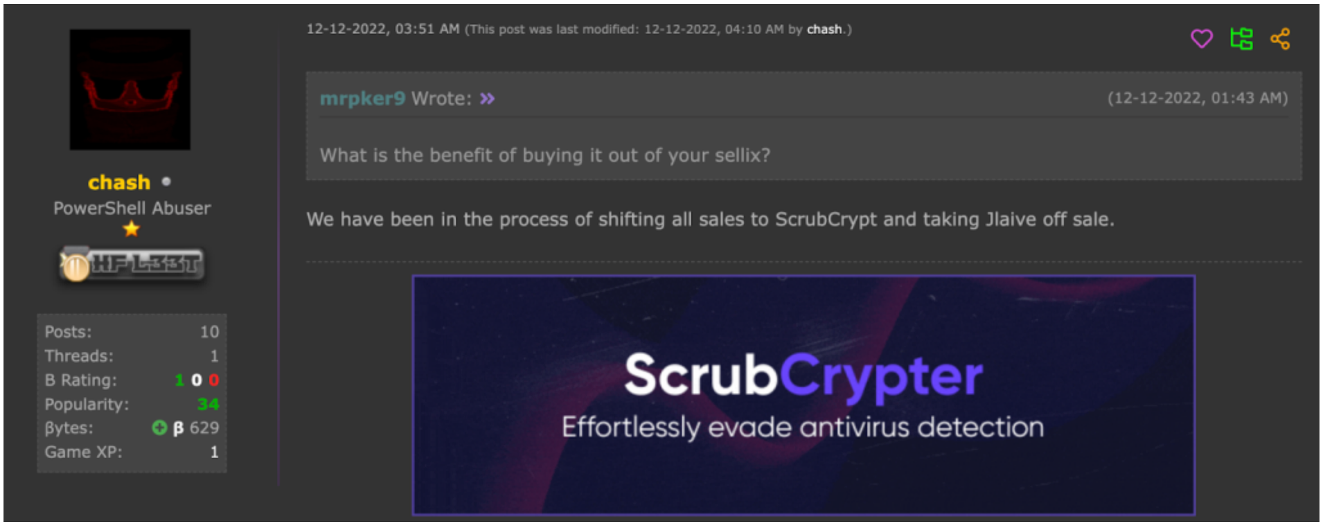
I'm just trying to understand why not just reach out to the original dev https://chash.mysellix.io/ and buying it from him directly and cheaper...

Since you're not the dev the only modification that was done is the form name that's it

Figure 4: Prospective customer comment

This comment was made by a confused potential customer that managed to identify the similarity between ScrubCrypter and the well known Jlaive Crypter. The Jlaive Crypter has been used for a long time by many threat actors as their main Crypter of choice.

Eventually, the main developer of the Jlaive Crypter replied to the user:



chash
PowerShell Abuser

Posts:	10
Threads:	1
B Rating:	1 0 0
Popularity:	34
βytes:	β 629
Game XP:	1

12-12-2022, 03:51 AM (This post was last modified: 12-12-2022, 04:10 AM by chash.)

> mrpker9 Wrote: » (12-12-2022, 01:43 AM)
>
> What is the benefit of buying it out of your sellix?

We have been in the process of shifting all sales to ScrubCrypt and taking Jlaive off sale.

Figure 5: Jlaive Crypter developer response

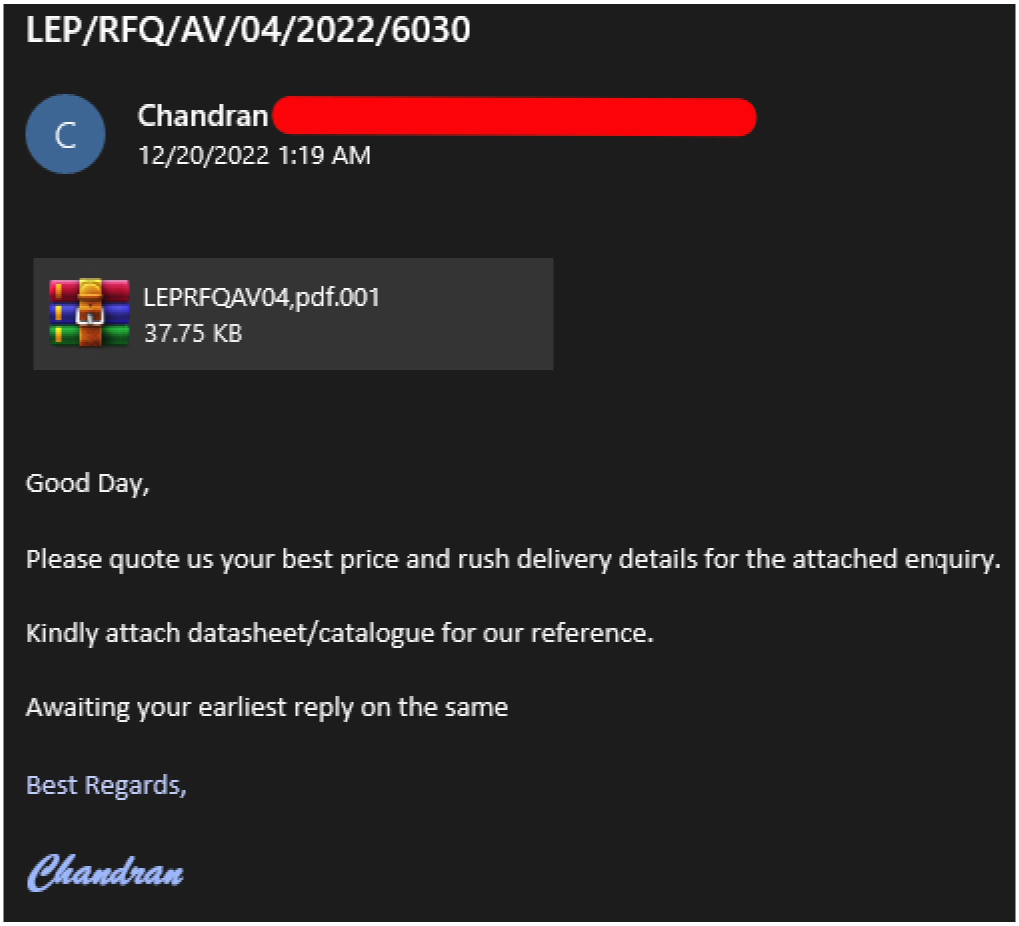
The developer's response was confirmation that ScrubCrypter is just a renamed version of the Jlaive Crypter. While other customers claim that ScrubCrypter has better performance than Jlaive, the features and functions are nearly identical. With a Crypter so easily available and accessible, any malicious actor can buy it and use it to propagate malware or the actor's attack of choice. This threatens the overall security of many organizations, as the Crypter hides the final payload, making it less detectable to even some advanced security systems.

Now that we have covered what ScrubCrypt is and how easy it is to access, let's investigate how it can be used in a real-world example.

The Crypt Goes Phish

In this example that Perception Point's advanced threat detection platform caught, a customer received a seemingly typical phishing email. However, upon further review there is more to this email than just meets the subject line.

The user receives an email with the subject: "LEP/RFQ/AV/04/2022/6030". Upon opening the message, there is a generic body with keywords often employed in social engineering campaigns. he goal of the message is to convince the user to download the attachment.



LEP/RFQ/AV/04/2022/6030

Chandran [redacted]
12/20/2022 1:19 AM

LEPRFQAV04,pdf.001
37.75 KB

Good Day,

Please quote us your best price and rush delivery details for the attached enquiry.

Kindly attach datasheet/catalogue for our reference.

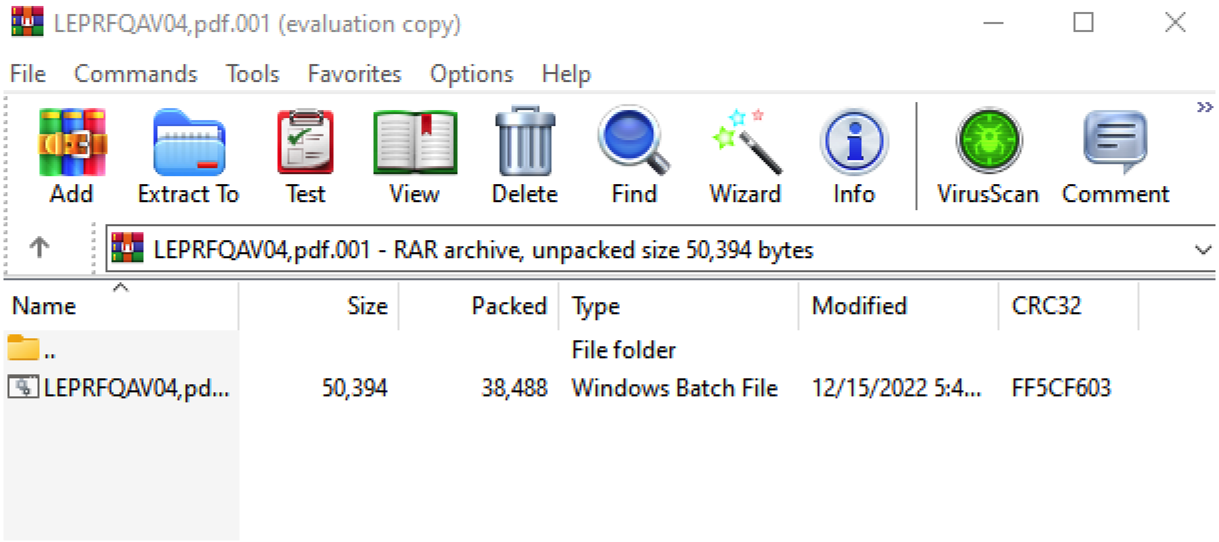
Awaiting your earliest reply on the same

Best Regards,

Chandran

Figure 6: The phishing email

When the user downloads the attached file, it leads to a .bat file (batch script), which, once executed by the user, leads to a multi-stage execution chain.



LEPRFQAV04,pdf.001 - RAR archive, unpacked size 50,394 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
LEPRFQAV04,pd...	50,394	38,488	Windows Batch File	12/15/2022 5:4...	FF5CF603

Figure 7: .bat File

This eventually unleashes the Xworm RAT. Xworm RAT is a brand new Remote Access Trojan written in .NET language. Like any other RAT, it begins by stealing the user's basic information like their country, IP address, operating system, etc. From there, it connects to the C2 server, allowing the threat actor to employ a variety of commands like keylogging, remote control of the user's mouse, and downloading ransomware.

By using the Crypter to send this attachment, it makes it more difficult for security systems to detect. The Crypter adds a layer of protection to the malicious file, supposedly ensuring that the attacker will gain access to the user's system or network.

Perception Point's advanced threat detection platform flagged this message as malicious. The platform was able to recognize the sender's low reputation and lack of a known connection to the user. In addition, the platform identified that the attachment was an archive file, which contained an executable that prompted an automatic download on the user's operating system.

Summary

Attackers using a Crypter to hide malicious files poses a major security concern for all organizations, regardless of industry. The accessibility and availability of this specific ScrubCrypt makes it all the more dangerous, as attackers can easily purchase it and use it to conduct widespread attack campaigns. Without the necessary security features, an individual could open a ScrubCrypt file and unknowingly impact their entire organization, thus leading to irreparable damages.

In this blog we outlined the origins and uses of a Crypter. In subsequent blogs we will explore and expand upon the Crypter itself and the attack chain of Xworm RAT malware.

IOCs

- LEPRFQAV04,pdf.001 – 28d6b3140a1935cd939e8a07266c43c0482e1fea80c65b7a49cf54356dcb58bc (Sha256)
- LEPRFQAV04,pdf.bat – 04ce543c01a4bace549f6be2d77eb62567c7b65edbbaebc0d00d760425dcd578 (Sha256)

All IOCs found by PerceptionPoint can be found on MalwareBazzar