

Cracking the Chaos Ransomware family

Alexander Andersson



malware

Chaos Ransomware Builder

  Jun 9, 2021

1 2 3 ... 6 Next ▶

Watch



Пользователь

Joined: Jun 8, 2021
Messages: 26
Reaction score: 17






Jun 9, 2021

  #1

Я занимался разработкой ransomware и я хотел бы поделиться с вами, ребята. Поделитесь, пожалуйста, своим мнением по этому поводу. Какую функцию вы бы хотели видеть в этом ransomware?

Ссылка для скачивания: [https://github.com/\[redacted\]nyuk-ransomware](https://github.com/[redacted]nyuk-ransomware)
попробуйте только на виртуальной машине

 Report

 Like +  Quote  Reply




   and 11 others



main 1 branch 0 tags

Go to file

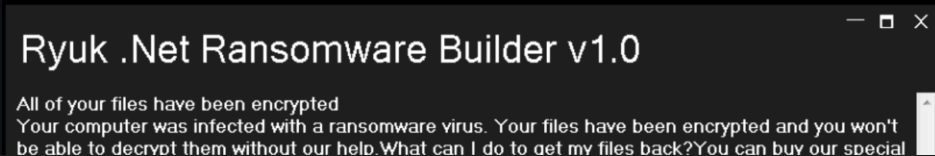
Code

	Update README.md	6fd1557 8 hours ago	9 commits
	README.md	Update README.md	8 hours ago
	Ryuk .Net Ransomware Builder.zip	Add files via upload	yesterday

README.md

ryuk-ransomware

TRY ON VM ONLY. Ryuk .Net Ransomware overwrites all files on the computer (It means nobody can ever return files back) and makes it at least 2 times faster than other ransoms. It drops read_it.txt for startup folder and all folders which files has been encrypted. This project depends on your donation. Please donate if you want to see next releases in the future



About

No description, website, or topics provided.

Readme


Releases

No releases published

Packages

No packages published

JUN 2021



Chaos Builder 1.0/Ryuk.NET

Overwrites every file

Need partners for ransomware

by [REDACTED]

Hi. I am programmer and also owner of [bagli ransomware](https://www.pcrisk.com/removal-guides/2...ransomware) ([https://www.pcrisk.com/removal-guides/2 ... ransomware](https://www.pcrisk.com/removal-guides/2...ransomware)) but I have a better version which I develop and maintain right now. My new version of ransomware is more modern and more user friendly ransomware. I crypt and keep payload fully undetectable. If you want to earn from ransomware help me spread it and get your 50% from that. How it is gonna work?

I will create new bitcoin address in ransomware for each my partner and when new transaction shows up in blockchain (for example [https://www.blockchain.com/btc/address/ ... 2vd2x67s8p](https://www.blockchain.com/btc/address/...2vd2x67s8p)) it means 50% of that money is yours.

Modern ransomware

[https://\[REDACTED\]W8/modern.gif](https://[REDACTED]W8/modern.gif)

[https://\[REDACTED\]nQ/Screenshot-3.png](https://[REDACTED]nQ/Screenshot-3.png)

contact [\[REDACTED\]@yandex.com](mailto:[REDACTED]@yandex.com)

JUN 2021

Bagli Wiper



Chaos Builder 1.0/Ryuk .NET

Overwrites every file

JUN 2021

Bagli Wiper



Chaos Builder 1.0/Ryuk .NET

Overwrites every file

Chaos Builder 2.0

Renamed to Chaos, UAC, Shadow copies, etc

Hidden Tear



Chaos Builder 3.0

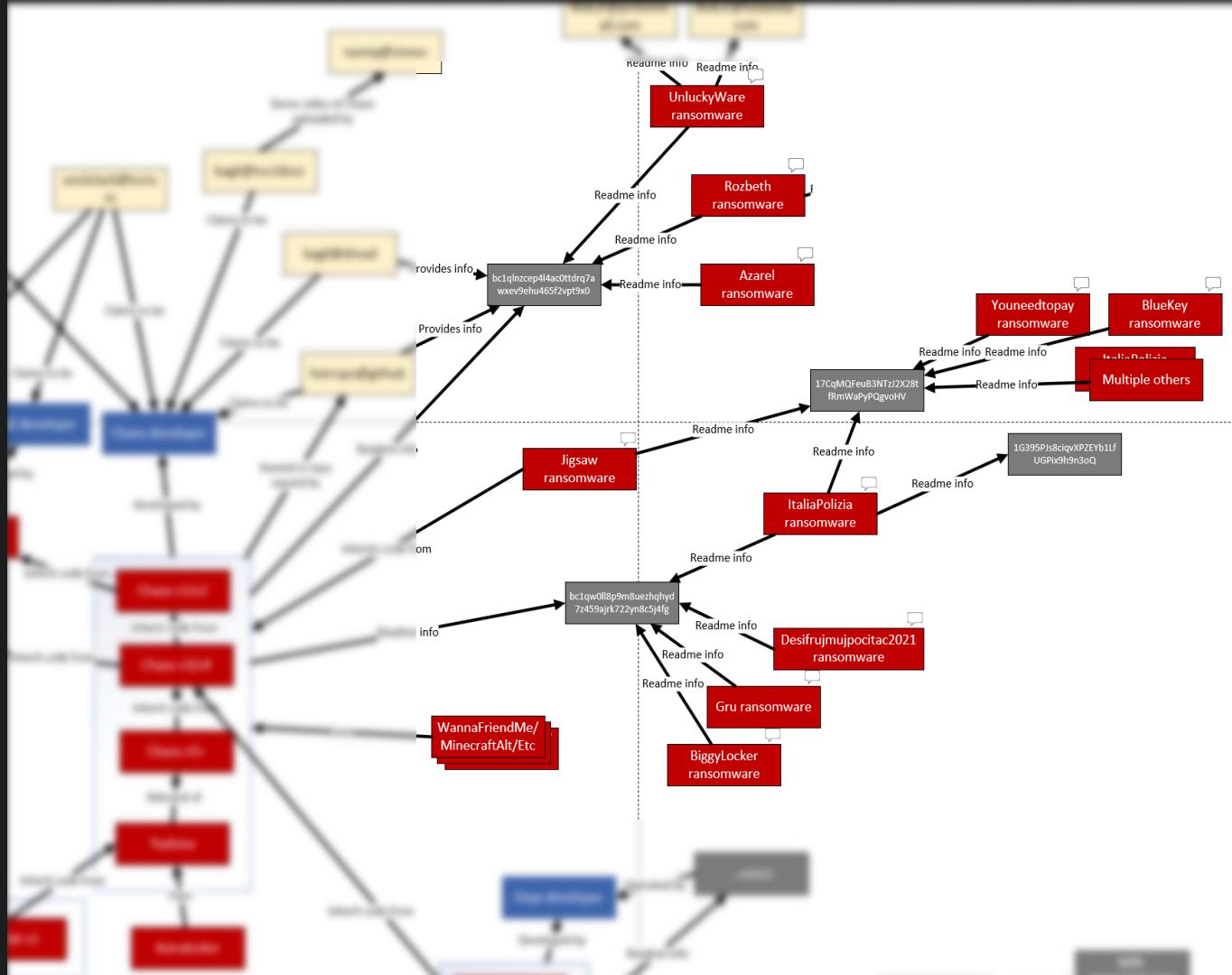
Encryption with AES/RSA, Decryptor generator. Max 1 MB.

AUG 2021

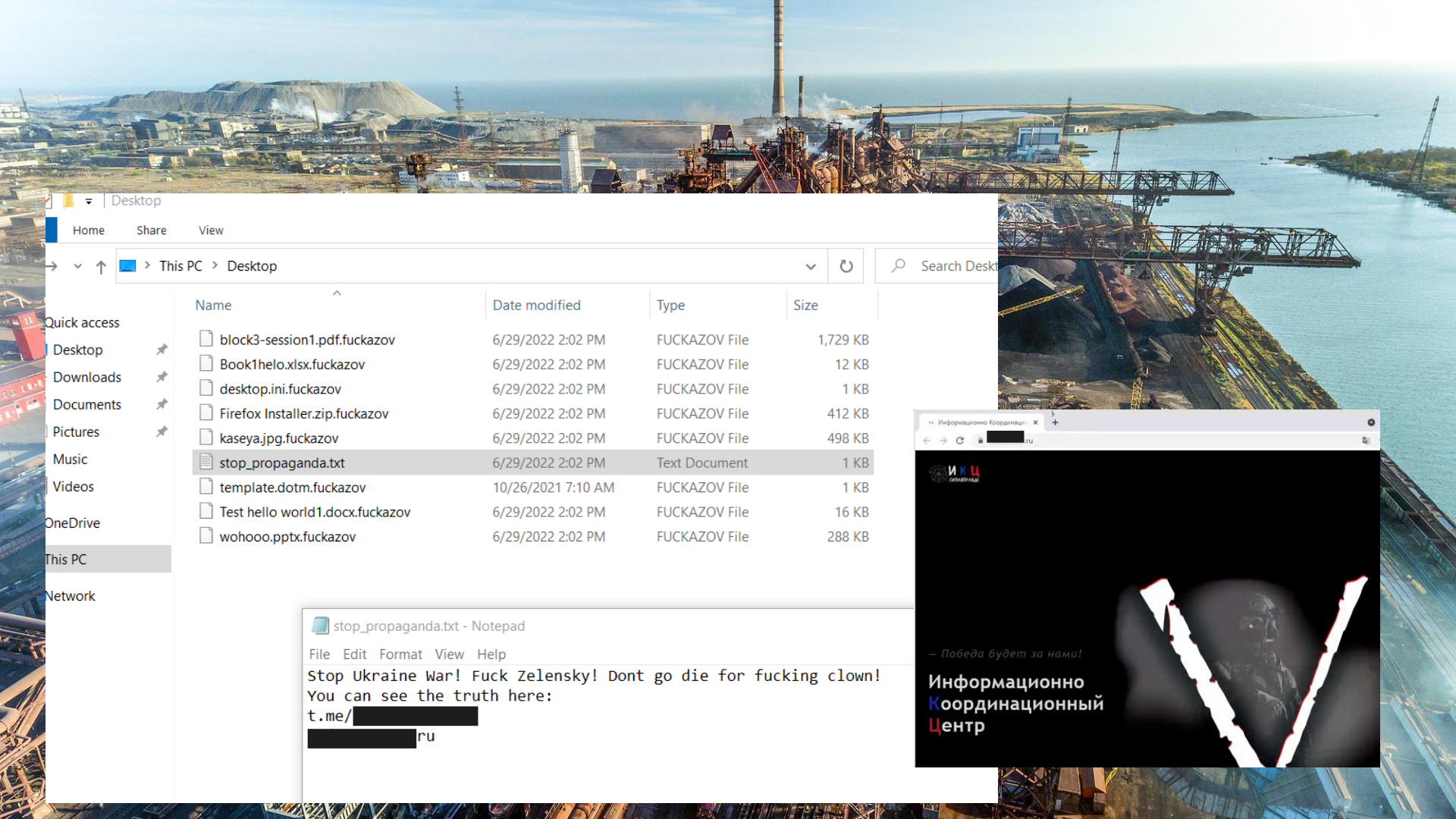
Chaos Builder 4.0

Max 2 MB









Desktop

Home Share View

→ < > This PC > Desktop

Name	Date modified	Type	Size
block3-session1.pdf.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	1,729 KB
Book1helo.xlsx.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	12 KB
desktop.ini.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	1 KB
Firefox Installer.zip.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	412 KB
kaseya.jpg.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	498 KB
stop_propaganda.txt	6/29/2022 2:02 PM	Text Document	1 KB
template.dotm.fuckazov	10/26/2021 7:10 AM	FUCKAZOV File	1 KB
Test hello world1.docx.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	16 KB
wohooo.pptx.fuckazov	6/29/2022 2:02 PM	FUCKAZOV File	288 KB

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Music
- Videos
- OneDrive
- This PC
- Network

stop_propaganda.txt - Notepad


File Edit Format View Help

```
Stop Ukraine war! Fuck Zelensky! Dont go die for fucking clown!  
You can see the truth here:  
t.me/[REDACTED]  
[REDACTED].ru
```

Информационно Координационный Центр

— Победа будет за нами!

Информационно
Координационный
Центр

An aerial photograph of a large industrial complex, possibly a steel mill or refinery, situated along a body of water. The facility features numerous tall chimneys, complex piping, and large storage tanks. In the background, a large, flat-topped hill or mountain is visible under a clear sky. The water in the foreground is a deep blue-green color.

```
FileInfo fileInfo = new FileInfo(files[index]);
fileInfo.Attributes = FileAttributes.Normal;
if (fileInfo.Length < 2117152L)
{
    if (Program.encryptionAesRsa)
        Program.EncryptFile(files[index]);
}
else if (fileInfo.Length > 20000000L)
{
    string plainText = Encoding.UTF8.GetString(Program.random_bytes(new Random().Next(20000000, 30000000)));
    File.WriteAllText(files[index], Program.randomEncode(plainText));
    File.Move(files[index], files[index] + "." + Program.RandomStringForExtension(4));
}
else
{
    string plainText = Encoding.UTF8.GetString(Program.random_bytes(Convert.ToInt32(fileInfo.Length)));
    File.WriteAllText(files[index], Program.randomEncode(plainText));
    File.Move(files[index], files[index] + "." + Program.RandomStringForExtension(4));
}
```

Ryuk Decrypter



By 

Price **€ 1,499**

Buy

Type Pass

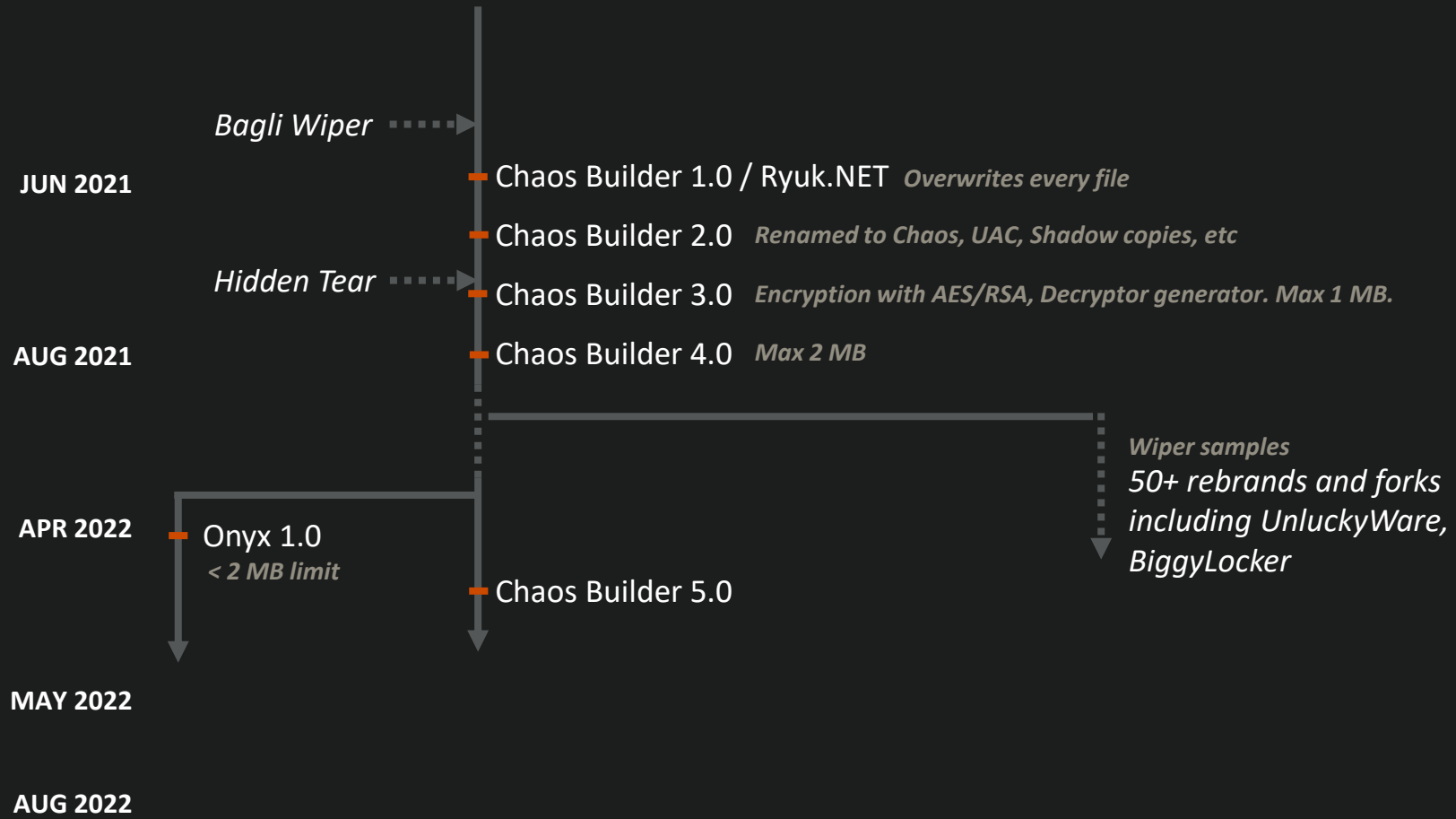
Updated Jun. 05, 2022



Use this Pass in:



Discovered by @MalwareHunterTeam



VSOP NEWS

If you are a client who declined the deal and did not find your data on website or did not find valuable files, this does not mean that we forgot about you, it only means that data was sold and only therefore it did not publish in free access!



[Redacted] .com

[Redacted] SHERIFF'S
OFFICE



Email: [Redacted]



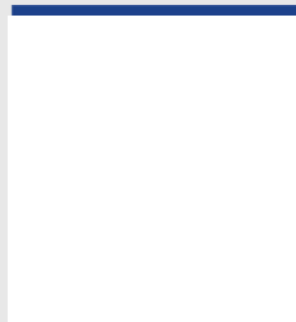
[Redacted]

ei [Redacted] m

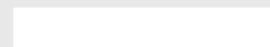
c [Redacted]

[Redacted]

[Redacted]



[Redacted] com



Recover all your files safely and easily with **SOLIDBIT**



What happened?

Many of your documents, databases, videos and other important files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

SOLIDBIT Ransomware uses AES and RSA cryptography algorithms.



How to recover my files?

We guarantee that you can recover all your files safely and easily. You can decrypt a single file for warranty - we can do it. But if you want to decrypt all your files, you need to pay.

Write to support if you want to buy decryptor.

TRIAL DECRYPT

You can decrypt a single file for warranty - **we can do it.**

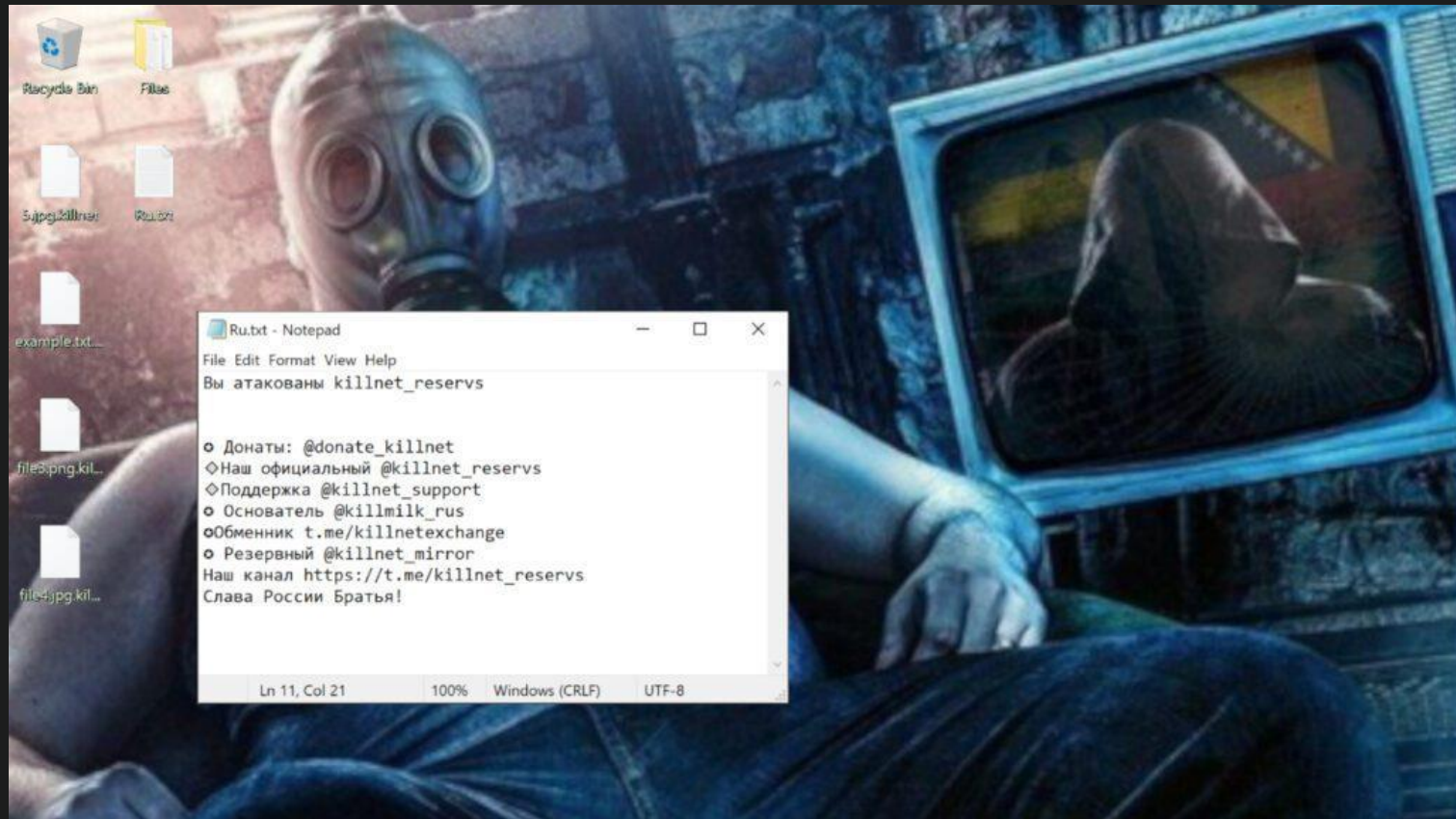
Select encrypted file

No file selected.

Max size: 1mb

CHAT WITH SUPPORT

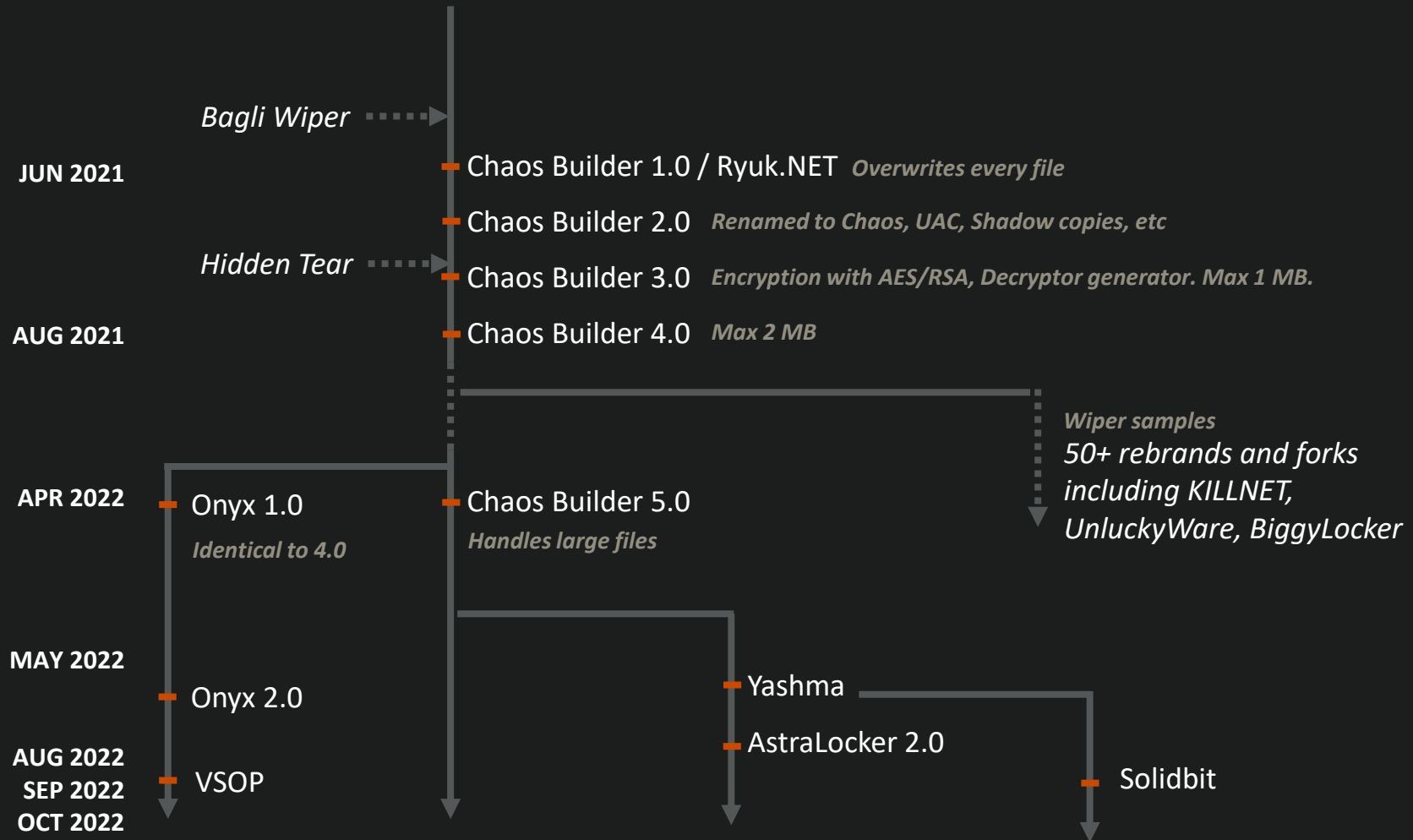
Enter your message...



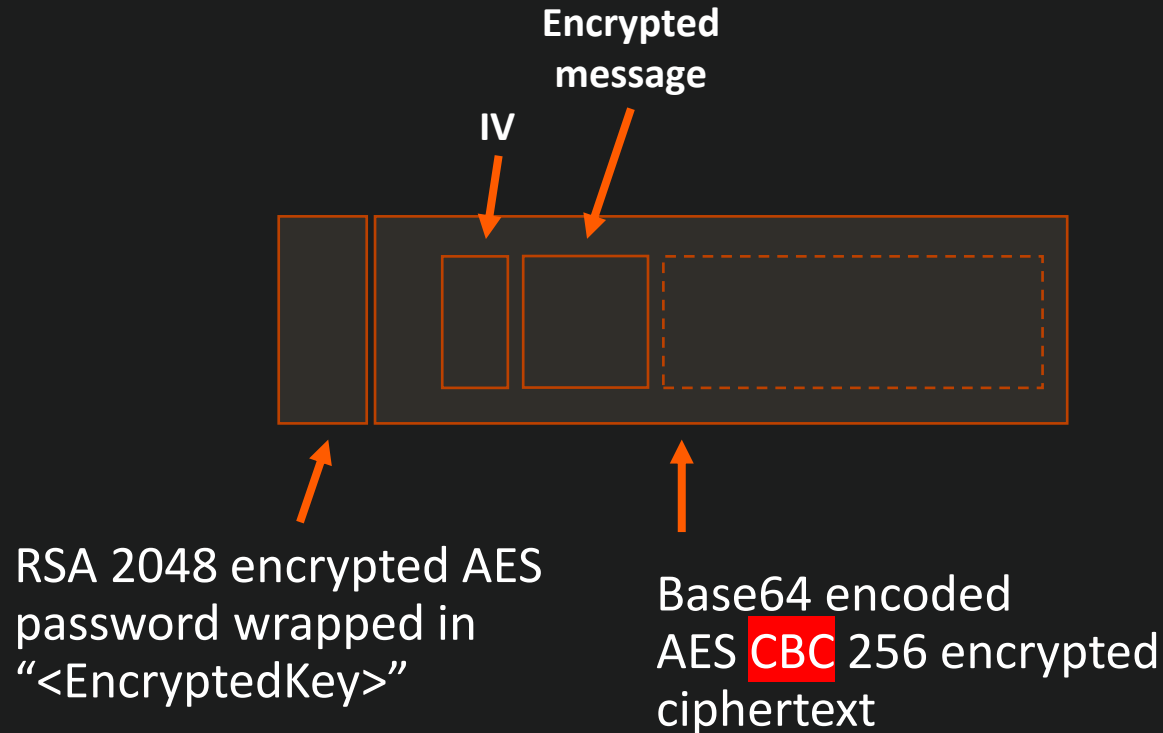
```
Ru.txt - Notepad
File Edit Format View Help
Вы атакованы killnet_reservs

o Донаты: @donate_killnet
o Наш официальный @killnet_reservs
o Поддержка @killnet_support
o Основатель @killmilk_rus
o Обменник t.me/killnetexchange
o Резервный @killnet_mirror
Наш канал https://t.me/killnet_reservs
Слава России Братья!
```

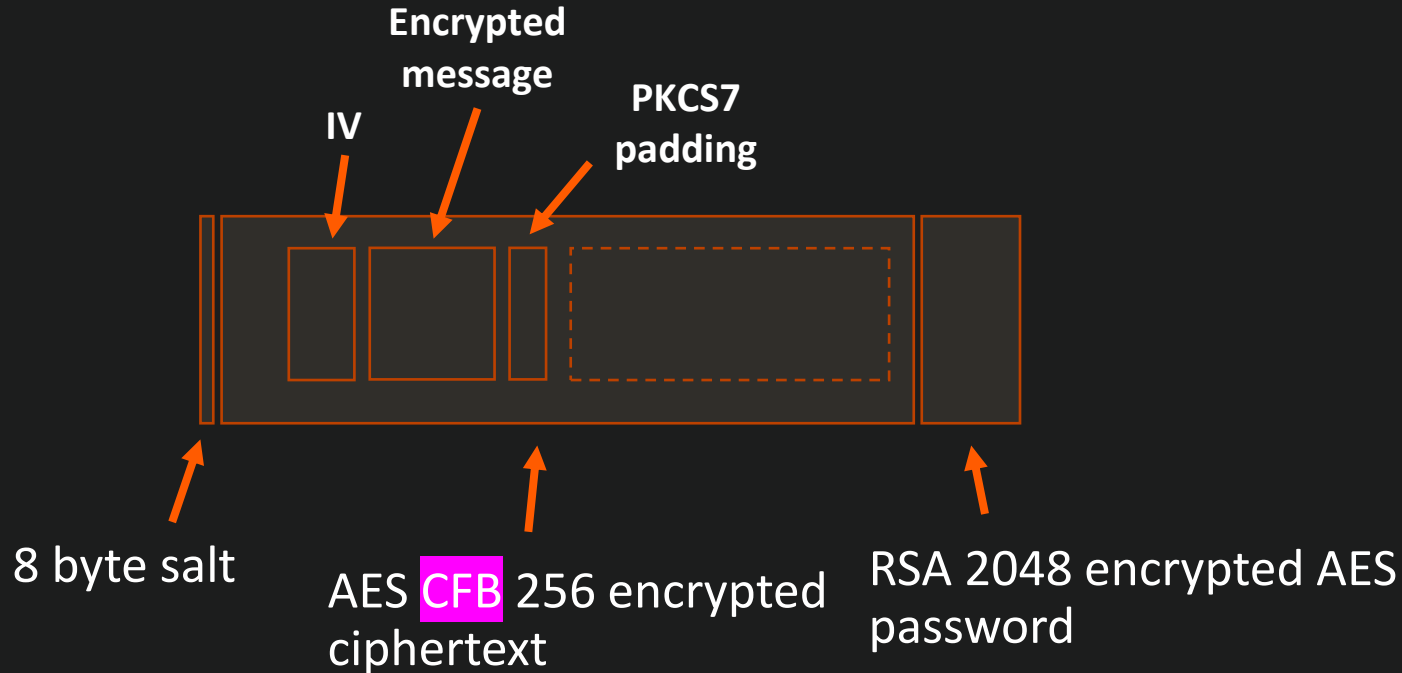
Ln 11, Col 21 100% Windows (CRLF) UTF-8



Encrypted File Format (Chaos)



Encrypted File Format (Onyx/VSOP)



File size limit had changed

```
480     string password = Program.CreatePassword(40);
481     if (fileInfo.Length < 1368709120L)
482     {
483         if (Program.checkDirContains(files[index]))
484         {
485             string keyRSA = Program.RSA_Encrypt(password, Program.rsaKey());
486             Program.AES_Encrypt(files[index], password, keyRSA);
487         }
488     }
489     else
490     Program.AES_Encrypt_Large(files[index], password, fileInfo.Length);
```

Figure: Decompiled Onyx/Chaos Ransomware Source Code

Key Generation

```
568 public static string CreatePassword(int length)
569 {
570     StringBuilder stringBuilder = new StringBuilder();
571     Random random = new Random();
572     while (0 < length--)
573         stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*! =&?&/"[random.Next
574             ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*! =&?&/" .Length)]);
575     return stringBuilder.ToString();
576 }
```

Figure: Decompiled Onyx/Chaos Ransomware Source Code

Encryption

```
580     byte[] numArray = new byte[8]
581     {
582         (byte) 1,
583         (byte) 2,
584         (byte) 3,
585         (byte) 4,
586         (byte) 5,
587         (byte) 6,
588         (byte) 7,
589         (byte) 8
590     };
591     FileStream fileStream1 = new FileStream(path, FileMode.Create);
592     byte[] bytes = Encoding.UTF8.GetBytes(password);
593     RijndaelManaged rijndaelManaged = new RijndaelManaged();
594     rijndaelManaged.KeySize = 256;
595     rijndaelManaged.BlockSize = 128;
596     rijndaelManaged.Padding = PaddingMode.PKCS7;
597     Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(bytes, numArray, 1);
598     rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
599     rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
600     rijndaelManaged.Mode = CipherMode.CFB;
601     fileStream1.Write(numArray, 0, numArray.Length);
```

Figure: Decompiled Onyx Ransomware Source Code

Let's look at that again...

```
568 public static string CreatePassword(int length)
569 {
570     StringBuilder stringBuilder = new StringBuilder();
571     Random random = new Random();
572     while (0 < length--)
573     {
574         stringBuilder.Append("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
                    ("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890*! =&?&/")
                    return stringBuilder.ToString();
```

Figure: Decompiled Onyx/Chaos Ransomware Source Code

Key Generation

os://docs.microsoft.com/en-us/dotnet/api/system.random?view=net-6.0

Pseudo-random numbers are chosen with equal probability from a finite set of numbers. The chosen numbers are not completely random because a mathematical algorithm is used to select them, but they are sufficiently random for practical purposes. The current implementation of the `Random` class is based on a modified version of Donald E. Knuth's subtractive random number generator algorithm. For more information, see D. E. Knuth. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley, Reading, MA, third edition, 1997.

To generate a cryptographically secure random number, such as one that's suitable for creating a random password, use the `RNGCryptoServiceProvider` class or derive a class from `System.Security.Cryptography.RandomNumberGenerator`.

In this topic:

[Instantiating the random number generator](#)

Let's call Carl



Let's call Carl

Is that `System.Random`
thing just theoretical?



Let's call Carl

Is that `System.Random` thing just theoretical?



I got a PoC on my github

So, how would this work?



1



33457863753639394...

2



48437873978577437...

3



93533974859249925...





Int32 is 4 bytes



-2^{31} to 2^{31}

$2^{31} = 2,147,483,647$

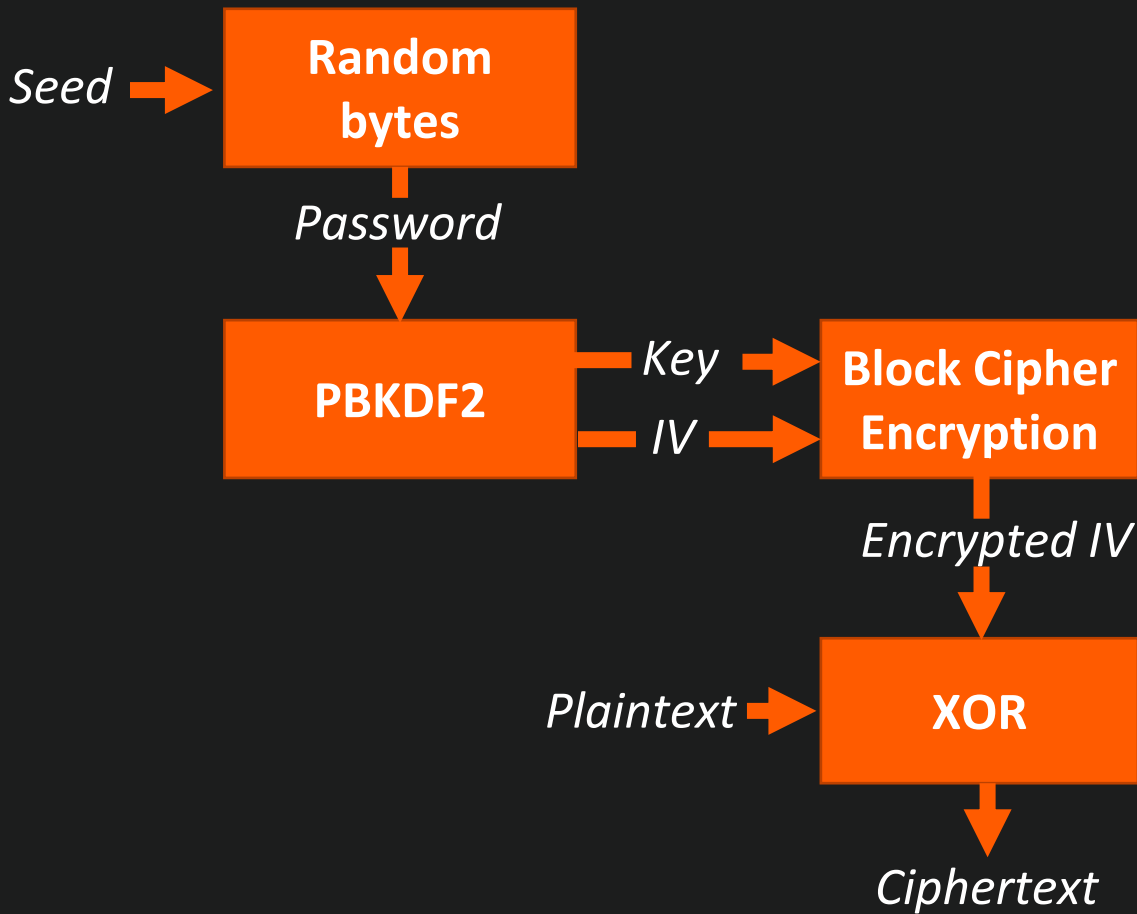


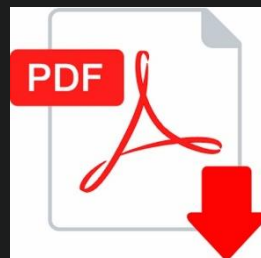
~2 billion possible seeds

Encryption (Onyx)

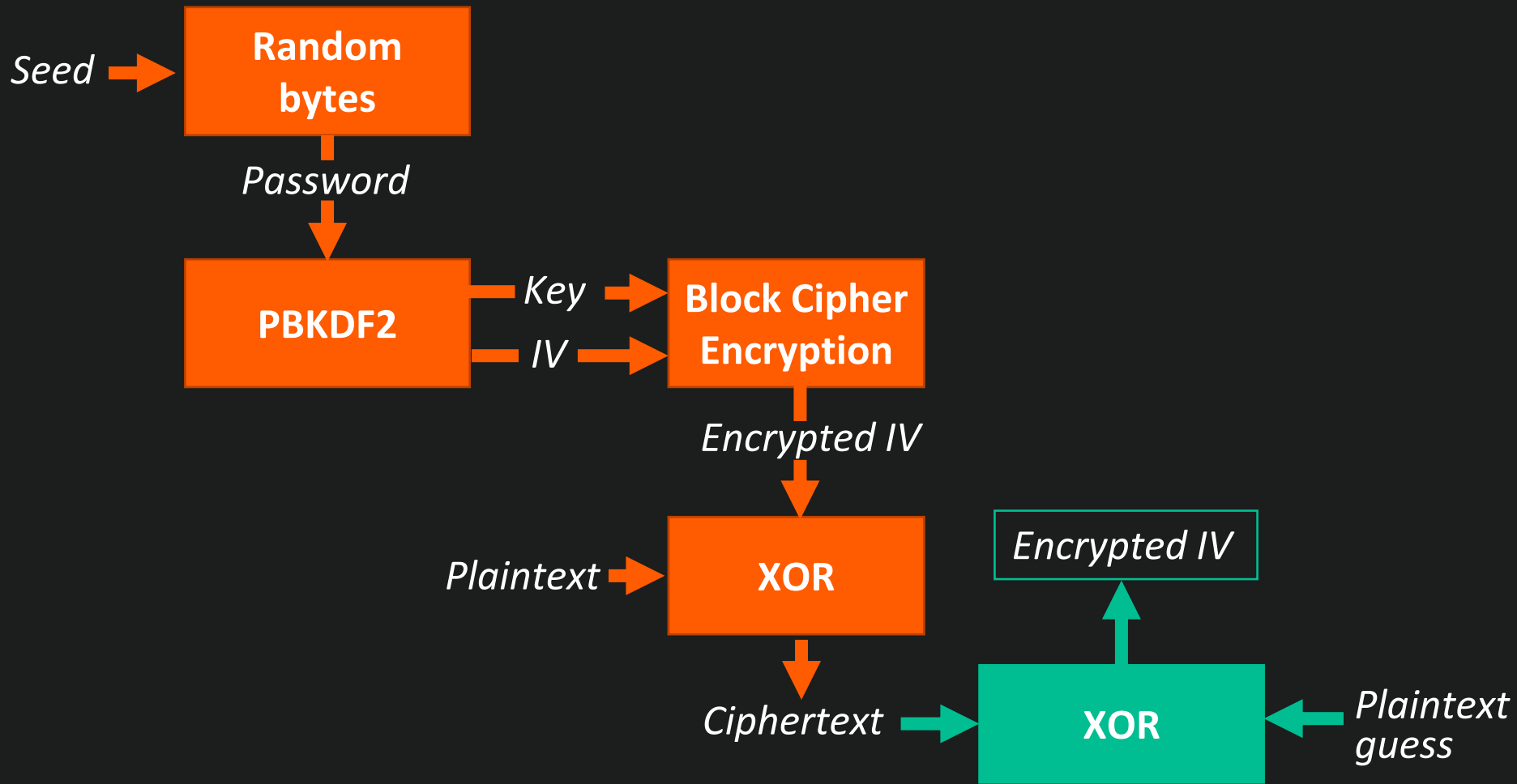
```
FileStream fileStream1 = new FileStream(path, FileMode.Create);
byte[] bytes = Encoding.UTF8.GetBytes(password);
RijndaelManaged rijndaelManaged = new RijndaelManaged();
rijndaelManaged.KeySize = 256;
rijndaelManaged.BlockSize = 128;
rijndaelManaged.Padding = PaddingMode.PKCS7;
Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(bytes, numArray, 1);
rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);
rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);
rijndaelManaged.Mode = CipherMode.CFB;
```

Figure: Decompiled Onyx Ransomware Source Code





Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	25	50	44	46	2D	31	2E	37	0A	0A	34	20	30	20	6F	62	%PDF-1.7..4 0 ob
00000010	6A	0A	28	49	64	65	6E	74	69	74	79	29	0A	65	6E	64	j.(Identity).end
00000020	6F	62	6A	0A	35	20	30	20	6F	62	6A	0A	28	41	64	6F	obj.5 0 obj.(Ado
00000030	62	65	29	0A	65	6E	64	6F	62	6A	0A	38	20	30	20	6F	be).endobj.8 0 o
00000040	62	6A	0A	3C	3C	0A	2F	46	69	6C	74	65	72	20	2F	46	bj.<<./Filter /F
00000050	6C	61	74	65	44	65	63	6F	64	65	0A	2F	4C	65	6E	67	lateDecode./Leng
00000060	74	68	20	33	34	30	36	37	0A	2F	4C	65	6E	67	74	68	th 34067./Length



Seed

Encrypted IV

0



8B 12 44 A3

1



EF C2 44 AB

2



C0 BB AF 00

3



C0 FF EE EE

...



... ..

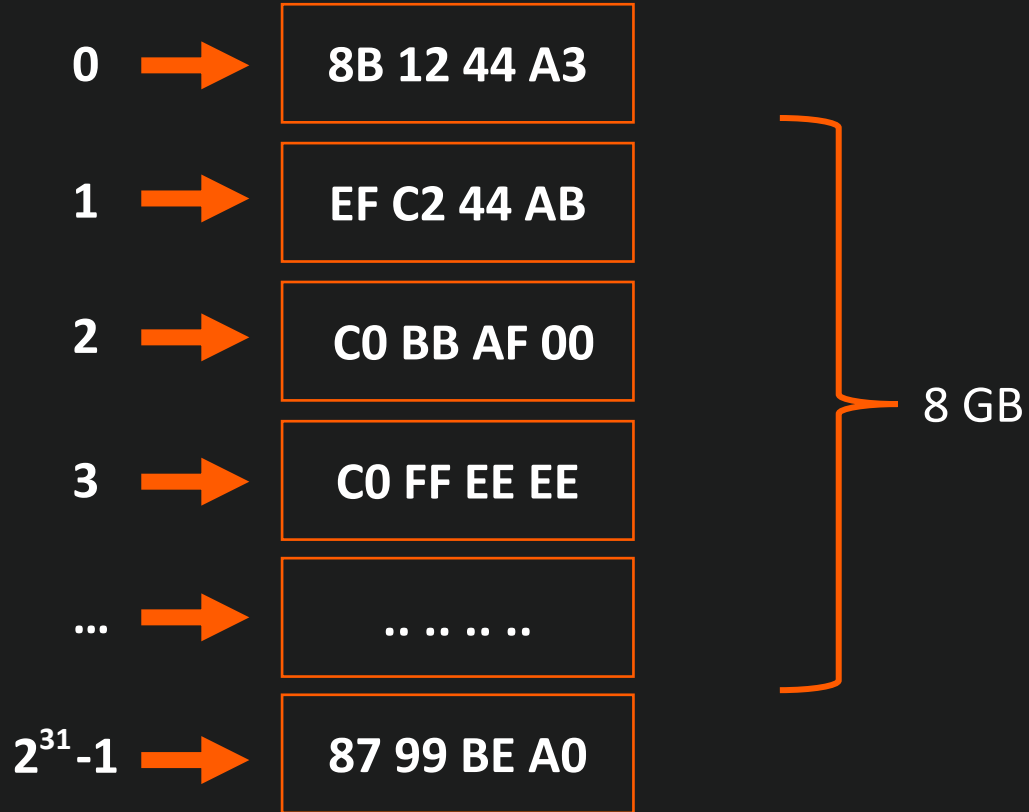
$2^{31}-1$



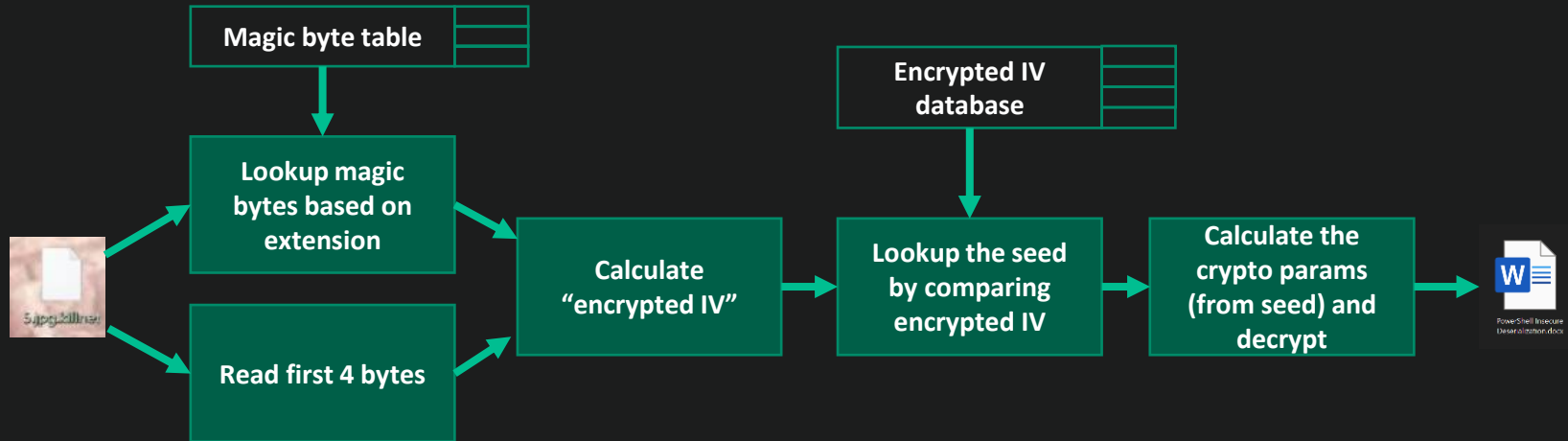
87 99 BE A0

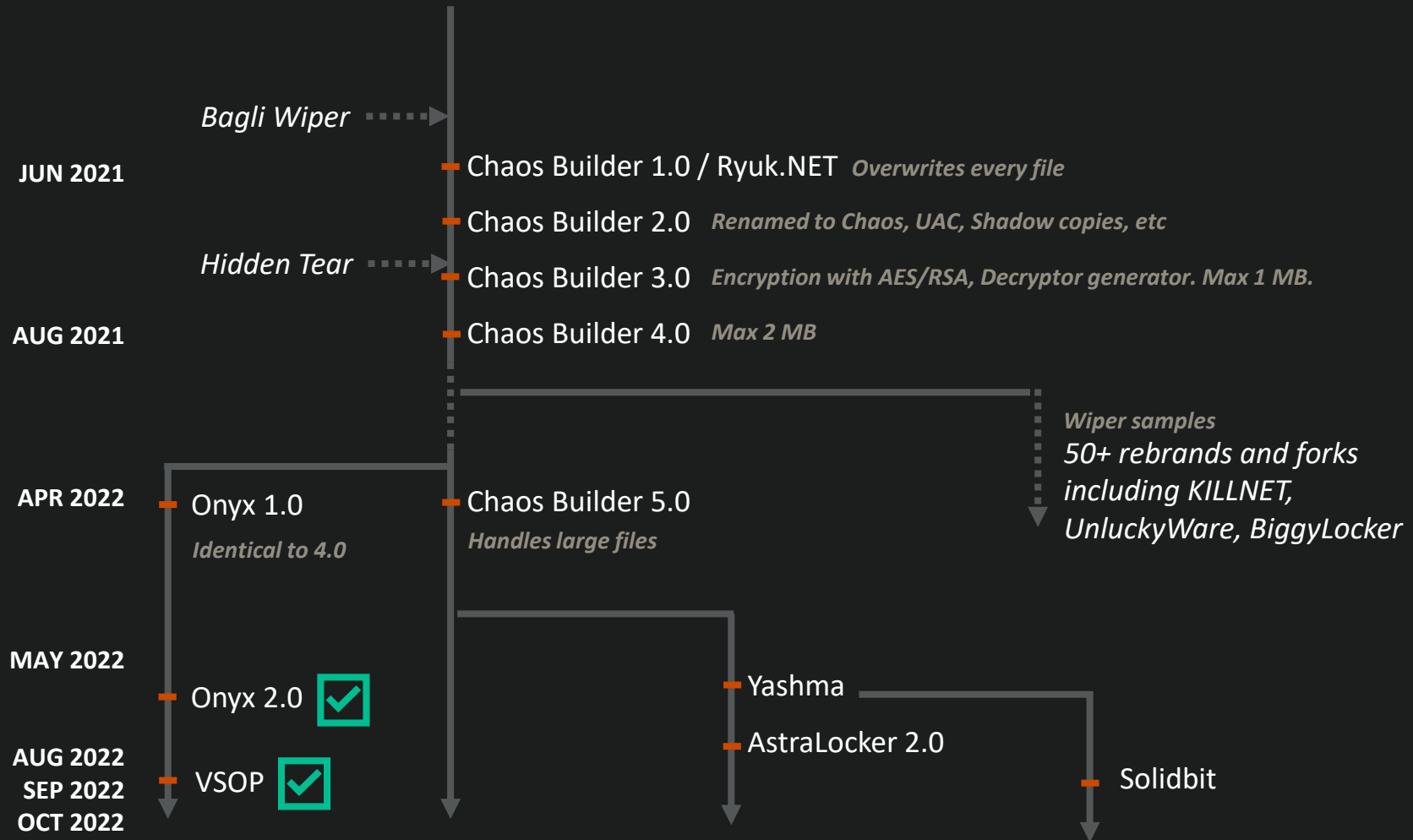
Seed

Encrypted IV



Let's implement a decryptor



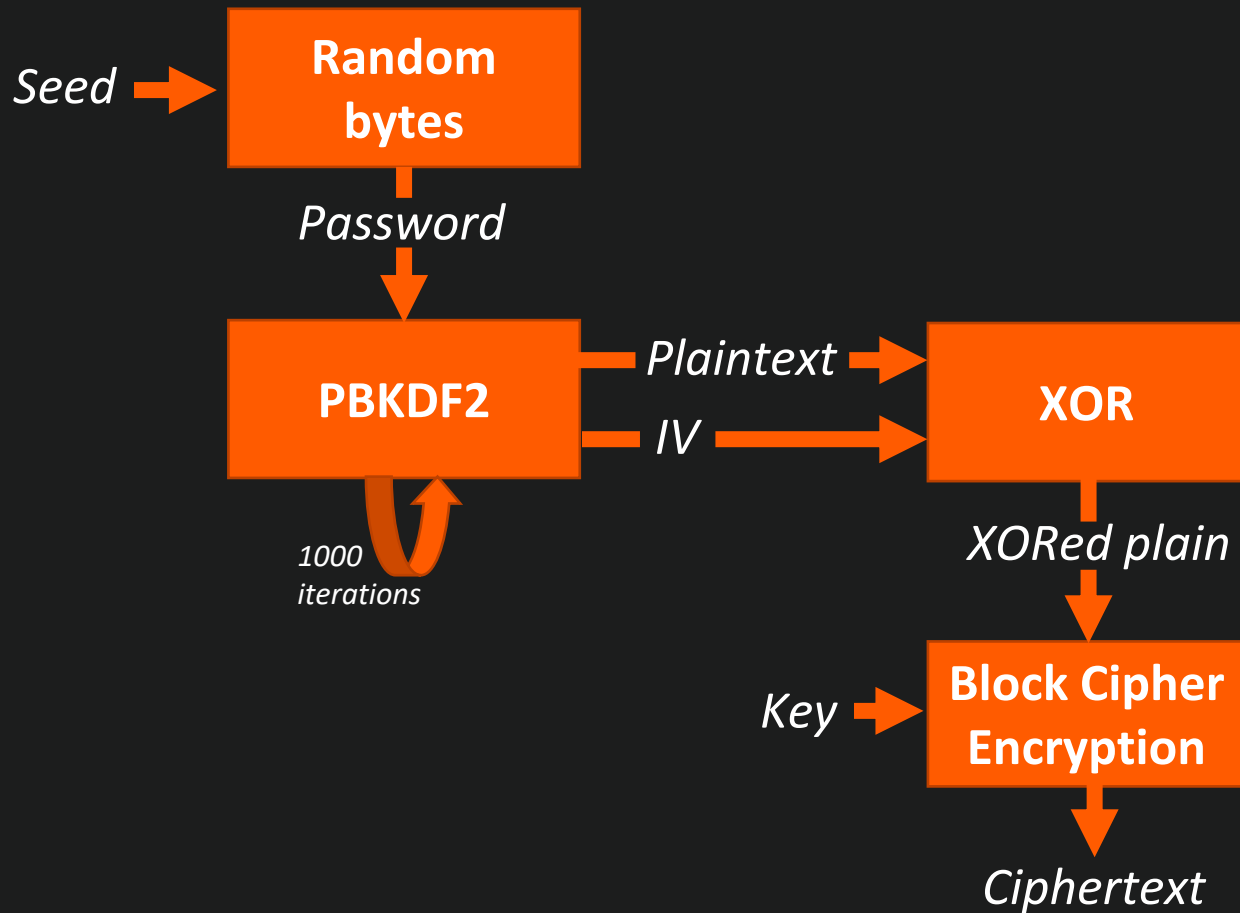


*Can we crack the entire
family?*

Generalizing to the entire family

```
rijndaelManaged.KeySize = 256;  
rijndaelManaged.BlockSize = 128;  
Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(passwordBytes, salt, 1000);  
rijndaelManaged.Key = rfc2898DeriveBytes.GetBytes(rijndaelManaged.KeySize / 8);  
rijndaelManaged.IV = rfc2898DeriveBytes.GetBytes(rijndaelManaged.BlockSize / 8);  
rijndaelManaged.Mode = CipherMode.CBC;
```

Figure: Decompiled Chaos Ransomware Source Code



Seed

Password + IV

0



8B 12

1



FF C6

2



AA 4B

3



C0 FF

...



... ..

$2^{31}-1$



E2 91

Seed

Password + IV

0



8B 12

1



FF C6

2



AA 4B

3



C0 FF

...



... ..

$2^{31}-1$



E2 91



103 GB

Seed

Password + IV

0



8B 12

1



FF C6

2



AA 4B

3



C0 FF

...



... ..

$2^{31}-1$



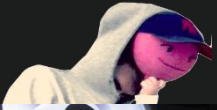
E2 91



103 GB

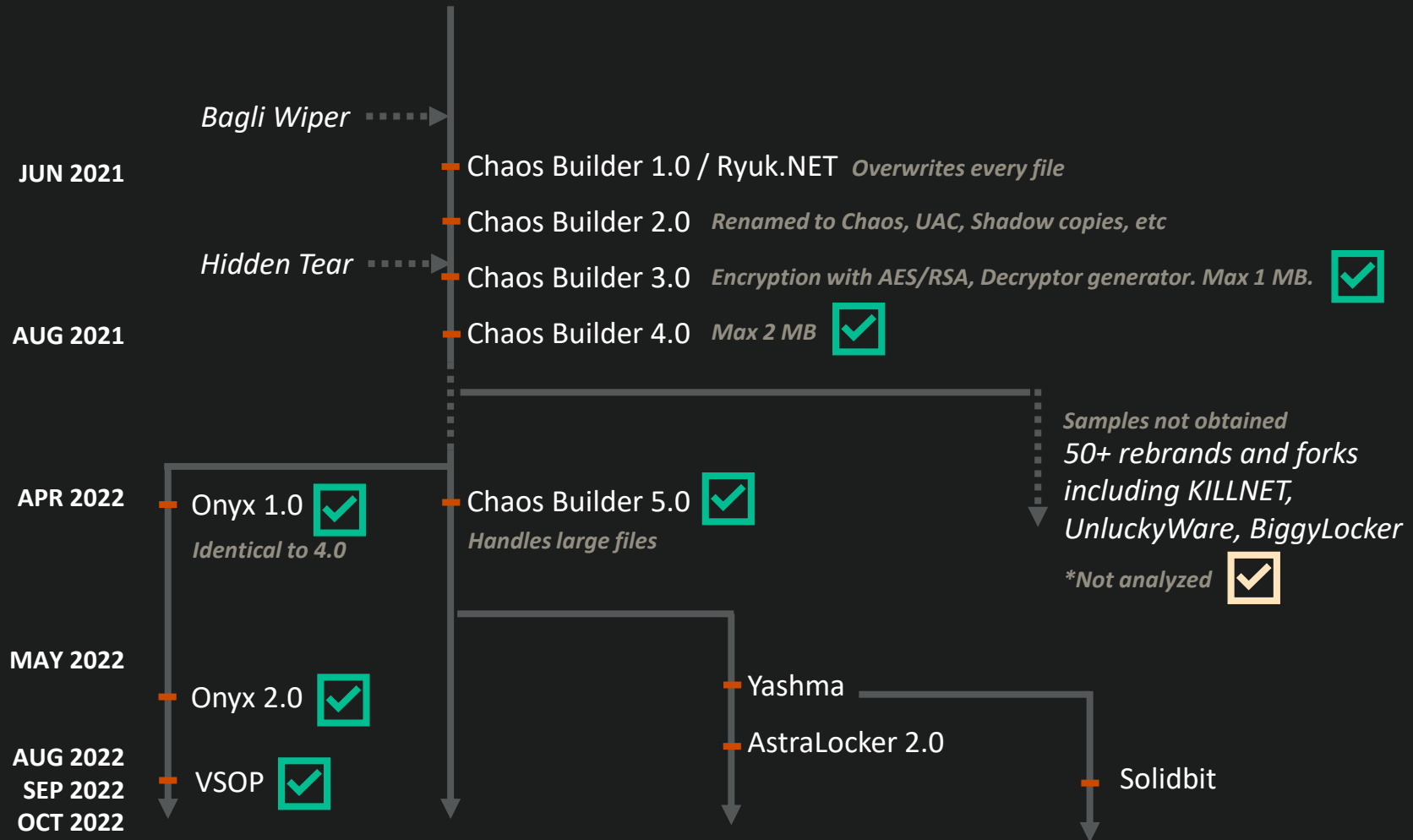


203 days on CPU

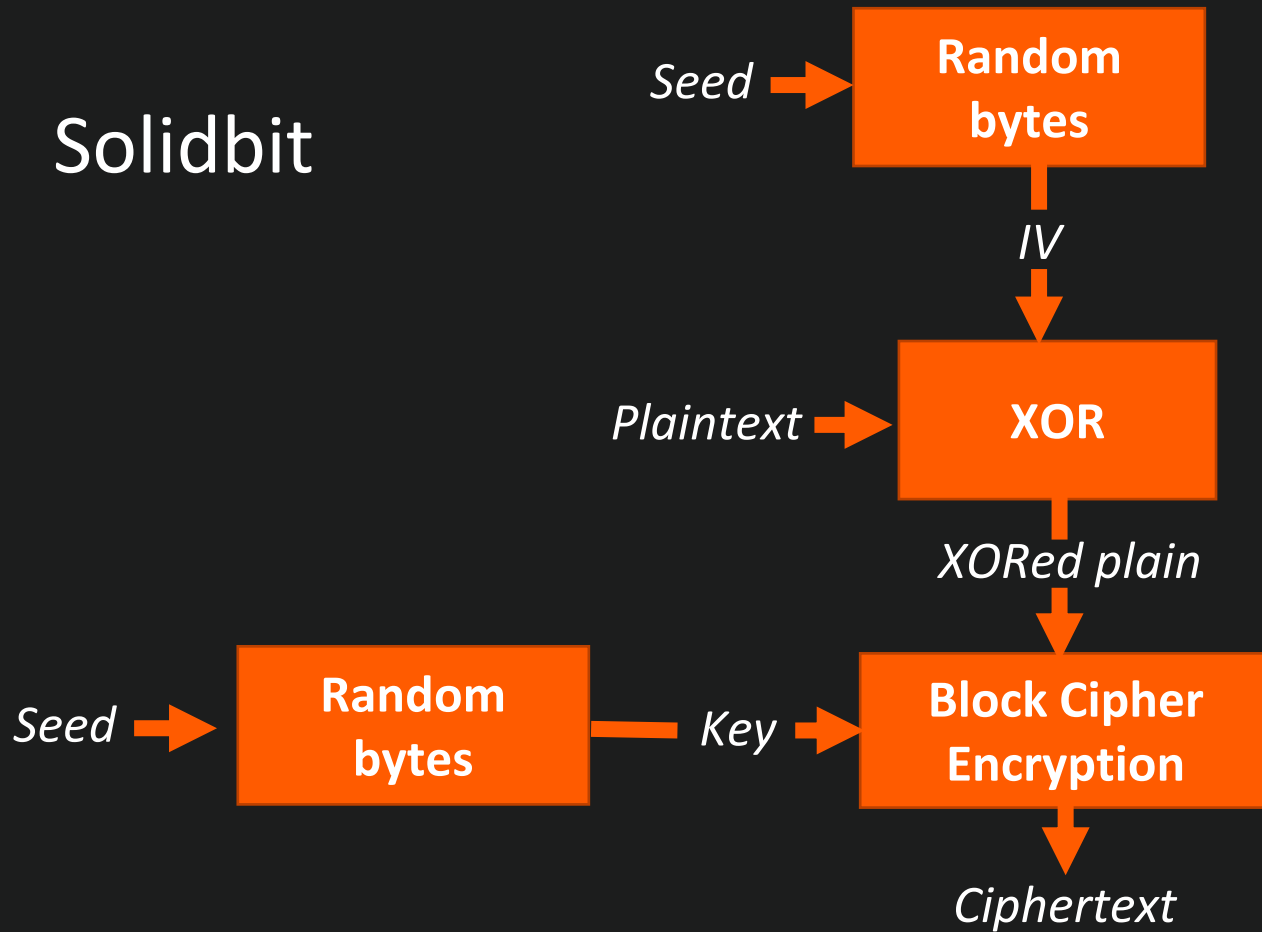


=> around a minute



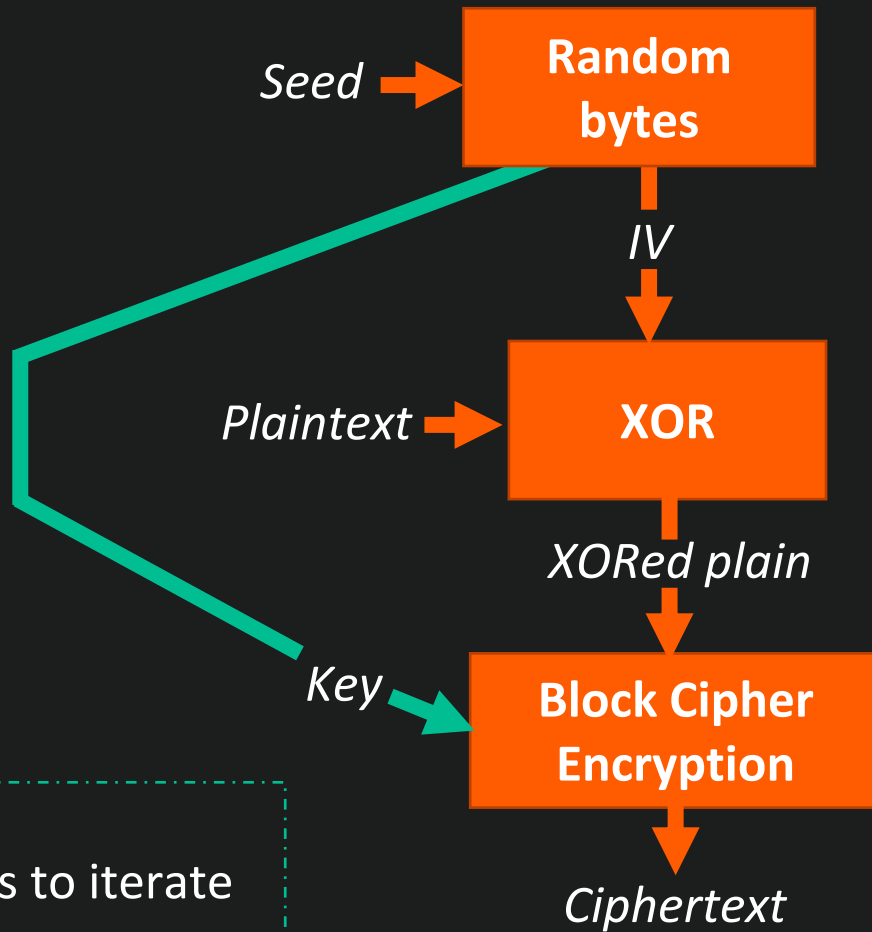


Solidbit



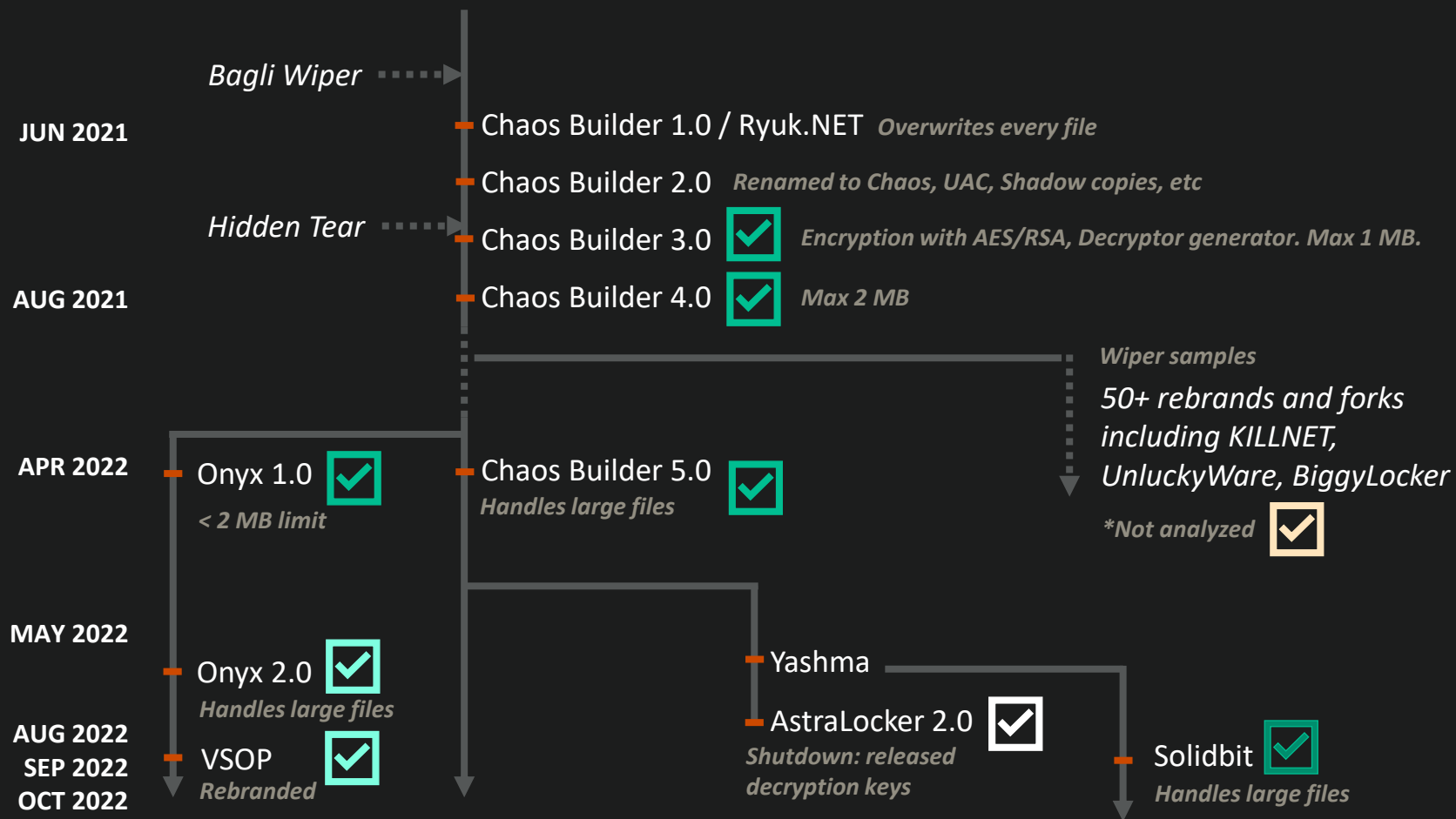
What is the seed, really?

Solidbit



Only 2^{31} values to iterate

Let's get our files back!



EUROPOL

<🔒/>
**NO MORE
RANSOM**

NEED HELP
unlocking your
digital life with-
out paying your
attackers*?

YES

NO

Partners

About the Project

English

Home

Crypto Sheriff

Ransomware: Q&A

Prevention Advice

Decryption Tools

Report a Crime



Ransomware is malware that locks your computer and mobile devices or encrypts your electronic files. When this happens, you can't get to the data unless you pay a ransom.

However this is not guaranteed and you should never pay!

DECRYPTED

The battle is over for these ransomware threats. If you have been infected with one of these types of ransomware click on the link under its name and it will lead you to a decryption tool.

[VIEW ALL](#)



SOLIDBIT



ONYX2



CHAOS



LOCKERGOGA



LOOCIPHER



HIVE (V1 TO V4)



ASTRALOCKER



DAIVOL
RANSOMWARE



TARGETCOMPANY



HERMETICRANSOM



NOWAY



MAZE /
SEKHMET /
EGREGOR

[TO TOP](#)

NO MORE CHAOS

Free open source (GPLv3) decryptor for the Chaos ransomware family, by Truesec.

- nomoreransom.org
- github.com/Truesec/TSDecryptors

