
OMU
HACKERS

Announcements

- CTF Club is back on Wednesdays 1pm @ Soar Point
- Hoodies… coming soon (waiting on SU)
- If you're new & don't have a membership card, please see one of us!

SIGINT pwnEd CTF

- 3rd & 4th February (next weekend)
- Teams are being decided on
- If you want to compete, **please let us know** ASAP if you haven't already!


hackers.dmu
@dmuhackers
DMU
HACKERS
Malware

Don't do illegal shit

Introduction To Malware

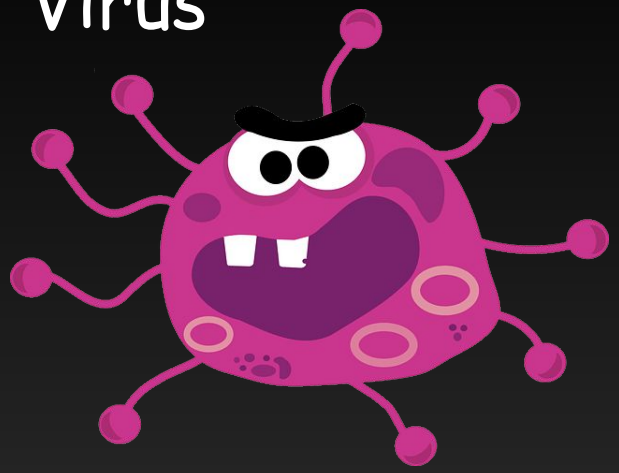
What is Malware?

- Malware is malicious software designed to
  - → compromise,
  - → damage,
  - → or gain unauthorized access to

  any computer system

Types of Malware

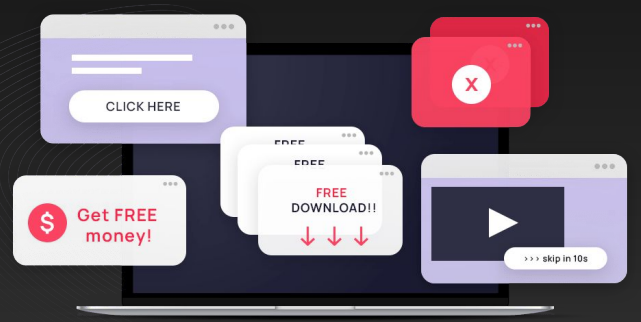
Virus



Worm

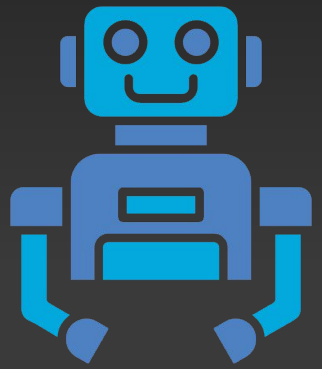
Trojan

Spyware

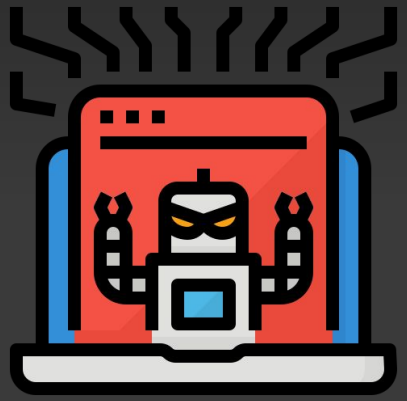


Adware

Ransomware



Botnet



Rootkit

Keylogger

Why use Malware?

- Financial Gain
- Data Theft
- System Disruption
- Botnets
- Espionage (corporate or nation-state)

Who uses malware?

- Cybercriminals
- Nation-States
- Hacktivists
- Security Researchers
- Hackers & Script Kiddies

How malware spreads?

Email Attachments

Removable Media

Phishing Emails

Software Vulnerabilities

Infected Websites

Insecure Networks

The Evolution of Malware

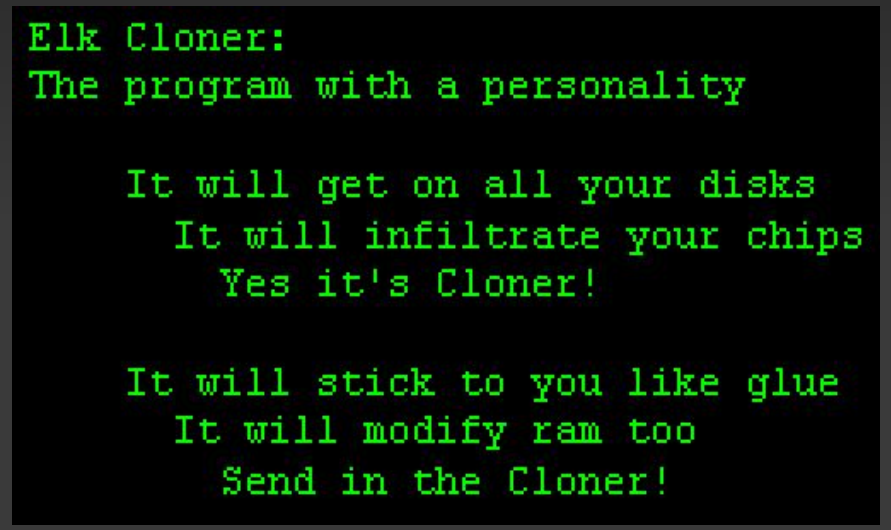
A Quick Timeline

1971 Creeper

Often regarded as the first virus. Designed as a security test to see if a self-replicating program was possible.

1982 Elk Cloner

First self-replicating program known to have spread in the wild on a large scale on the Apple II OS.



1986 Brain

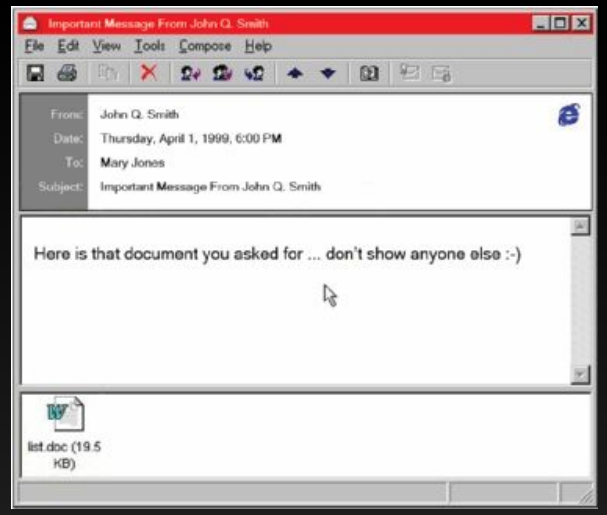
Considered to be the first virus for the IBM Personal Computer.

1989 AIDS

A trojan which counts when the computer is booted. Once it is booted 90 times, files are encrypted and a payment is asked for.

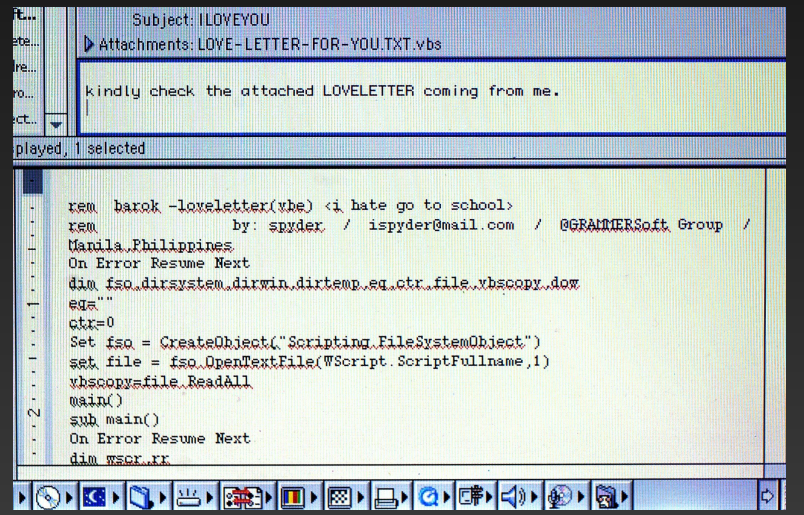
1999 Melissa

Mass-mailing virus targeting Word and Outlook systems. Email attachment contains a list of poronographic sites and accompanying logins for each.



2000 ILOVEYOU

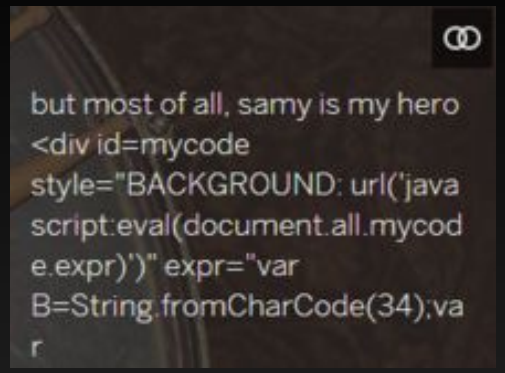
A computer worm spread to over 10 million Windows machines. Opening the attached file executes a VB script damaging the system.



2004 Mydoom

A worm consisting of an email that spread to at least 500,000 computers. An attached file spreads the email when opened.

2005 Samy

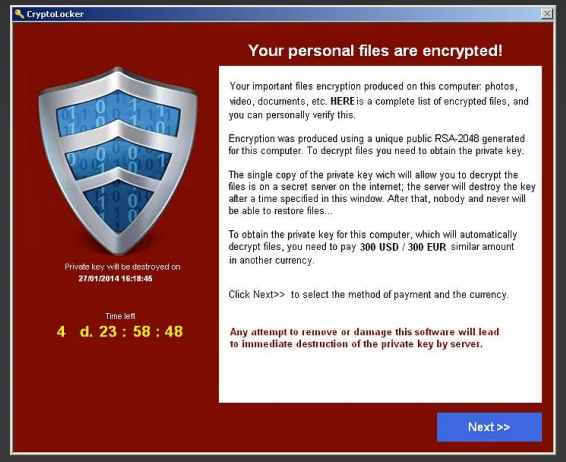


A XSS worm designed to propagate across MySpace. Carried a payload that would display "but most of all, samy is my hero" on the user's profile page.

2010 Stuxnet

A worm targeting SCADA systems and was believed to cause substantial damage to Iran's nuclear program. (Cyber Warfare??)

2013 CryptLocker

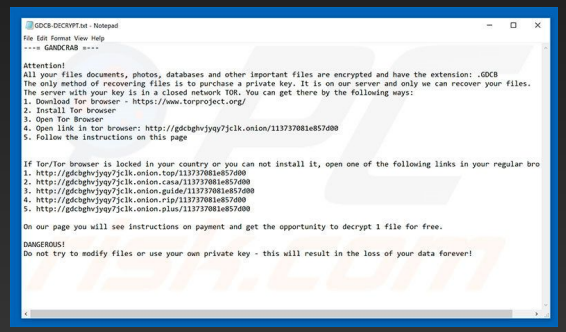


Ransomware targeting Windows computers. Encrypts files until a ransom is paid in cryptocurrency.

2017 WannaCry

A Windows ransomware responsible for the biggest attack against the NHS. Had a kill switch that involved registering a domain name.

2019 GandCrab



Another Windows ransomware demanding payment in order to train their data.

2022 LockBit 3.0

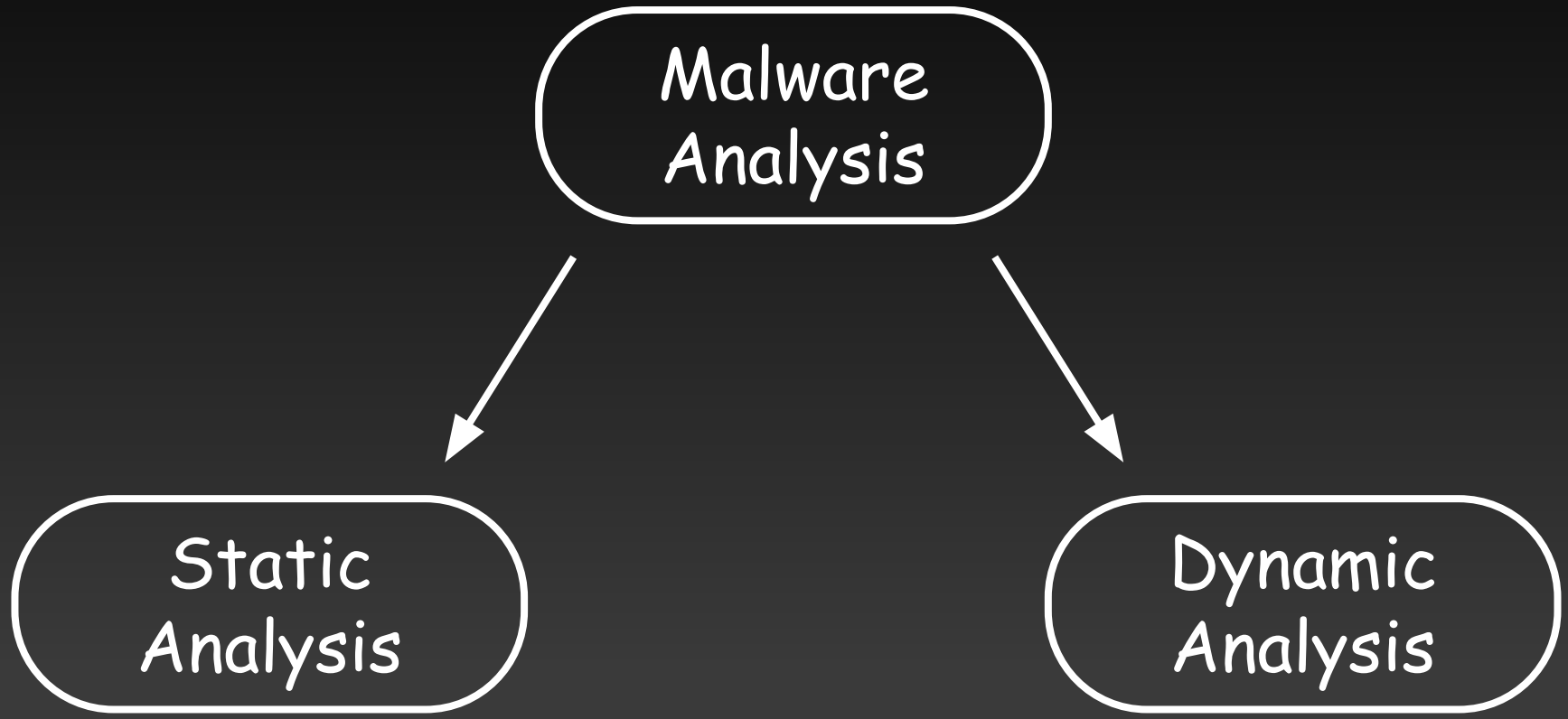
A ransomware as a service (RaaS) cyber criminal group selling the use of the ransomware to fellow criminals. Responsible for a big attack on Royal Mail in 2023.

Other Honorable Mentions

- qBot - A banking trojan first observed in 2007
- Clop - Ransomware targeting entire networks
- Zeus Gameover - Disguised as legitimate software to steal banking information
- Petya - Another Windows ransomware but infects the master boot record, completely preventing Windows from booting

Malware Analysis

Malware Analysis

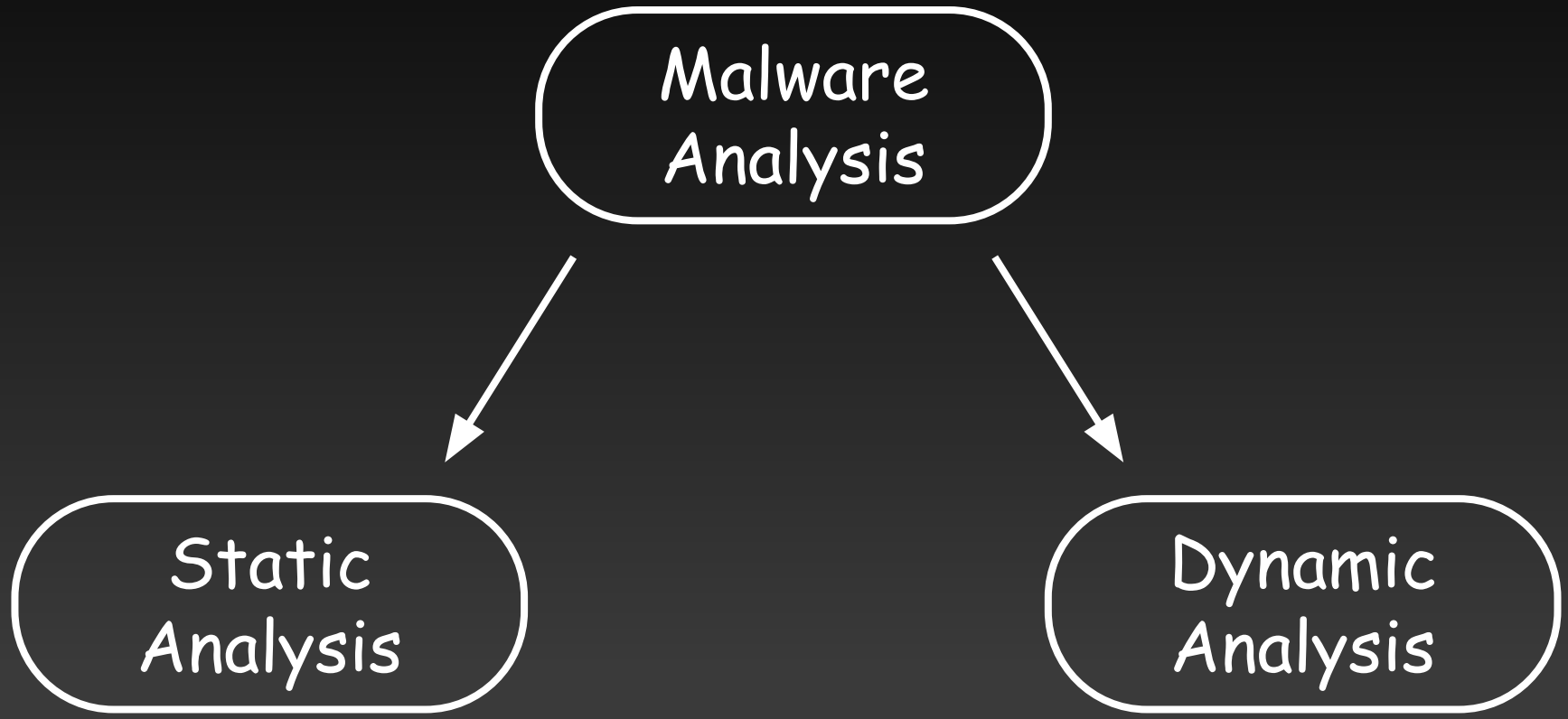


Static Analysis

- Analyse malware code and characteristics without executing the malicious program

- Code Review (disassembly)
- String Analysis
- Pattern Matching
- Dependency Analysis
- API Call Analysis
- Metadata Analysis
- Executable Analysis
- Binary Analysis
- Machine Learning Analysis

Malware Analysis



Dynamic Analysis

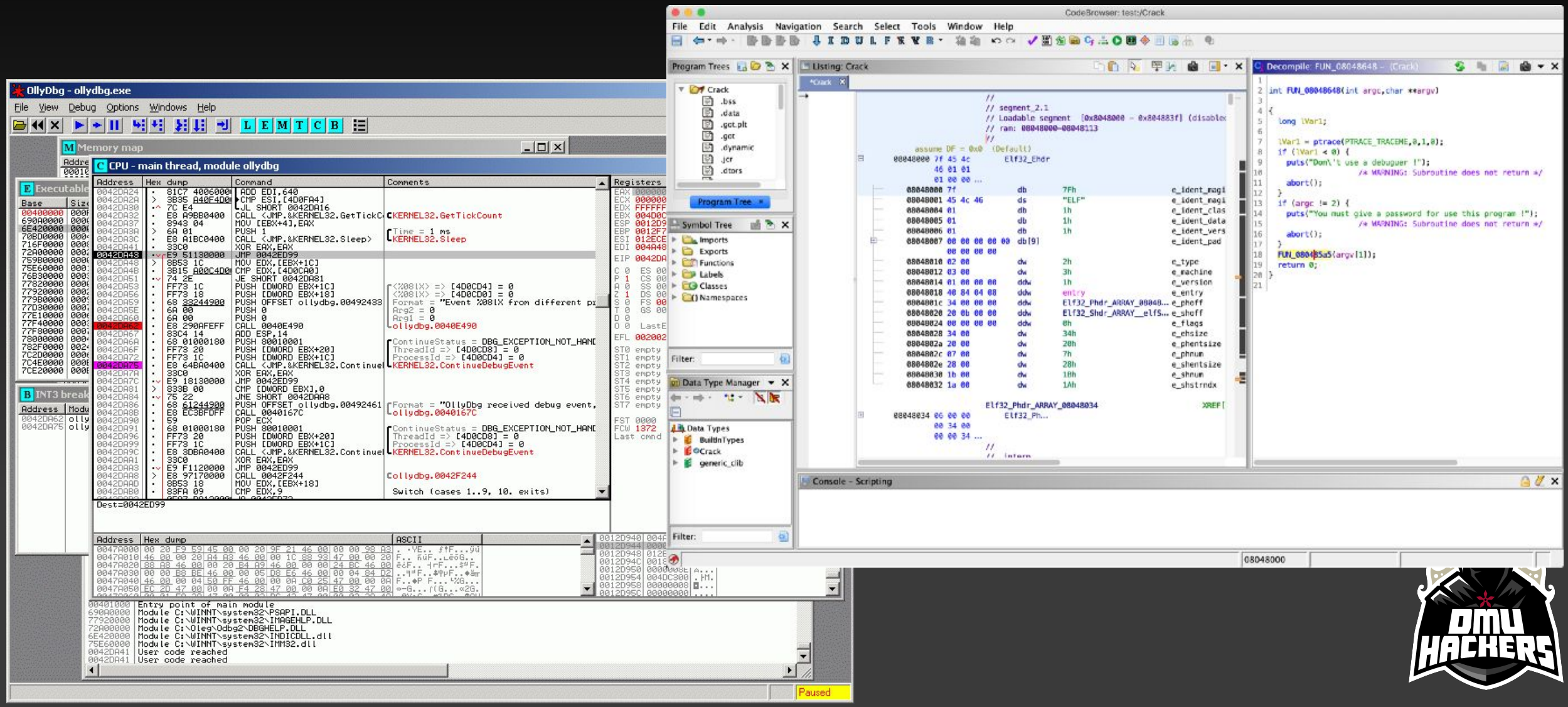
- Analyse malware code and characteristics by executing the malicious program

- Sandboxing
- Dynamic Code Analysis
- Behaviour Analysis
- API Monitoring
- Network Traffic Analysis
- Memory Analysis
- Resource Usage Monitoring
- Syscall Analysis
- Dynamic Malware Signature Analysis

Reverse Engineering

- Reverse engineering is a method of malware analysis where the executable is decompiled and the assembly code is analysed
- Some reverse engineering tools do their best to convert this to C, but are not always successful
- Disassemblers (like ghidra, IDA & Radare2) can do this
- Debuggers (like OllyDbg) can allow you to step through this assembly code

Reverse Engineering



Case Study

A Look Into LockBit - RaaS

- Upcoming groups are now using a Ransomware as a Service model.
- LockBit allow 'Affiliates' to use their ransomware, leak site, and other tools to conduct attacks.
- Affiliates can join the program for a deposit of $10,000.
- They must give LockBit 20% of the ransom money for using their tools.

1. Affiliate Program

CONDITIONS FOR PARTNERS

[Ransomware] LockBit 2.0 is an affiliate program.

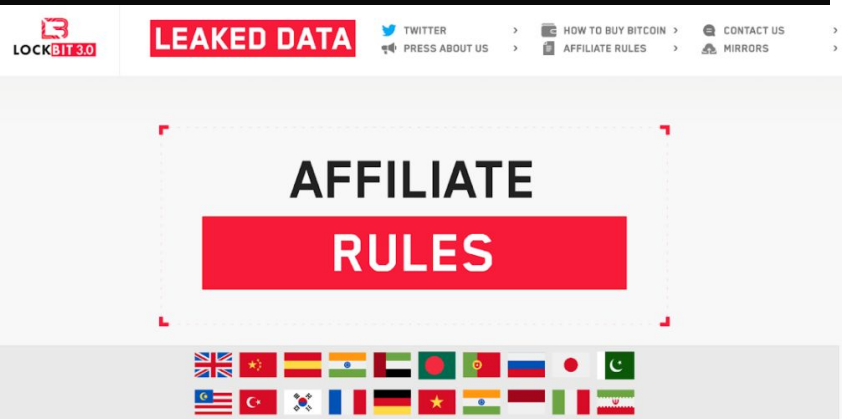
Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

1. Affiliate Program



The oldest international [Ransomware] LockBit affiliate program welcomes you.

We are located in the Netherlands, completely apolitical and only interested in money.
We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.
First and foremost, we're looking for cohesive and experienced teams of pentestors.
In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process - you can control the communication with the victim. In case when the company was encrypted and has not paid, you will see the stolen data in the blog.
We also work with those who don't encrypt networks, but just want to sell the stolen data, posting it on the largest blog on the planet.

Brief description of functionality:
- admin panel on the Tor network;
- communication with companies on the Tor network, chat with notifications and file transfer;
- the ability to create private chats for secret communication with companies;
- automatic decryption of test files;
- automatic decrypter output, by pressing the button in the panel;
- possibility of maximum protection of the decrypter, in this case the decrypter is stored on the flash drive;
- StealBit stealer, searchable by file name and extension;
- automatic data uploading to the blog, by you personally without our participation;
- Possibility to specify any Internet port in StealBit for downloading, for example 22 or 3389, to bypass network security policies;
- The ability to upload pictures to the blog;
- Ability to post the history of correspondence with the attacked company to the blog;
- ability to generate builds with different settings, but with one encryption key for one corporate network;
- 2 different encryption lockers for Windows in one panel, written by different programmers, allowing to encrypt the network twice, if time allows, it will be useful for paranoiacs who doubt the reliability and implementation of the cryptographic algorithm and believe in free decryption;
- ability to edit the list to kill processes and services;
- ability to edit the list of exceptions - computer name, names and file extensions that do not need to be encrypted;
- the fastest and most efficient cleanup (without the possibility of recovery) of free space after encryption;
- file name encryption, helps to avoid even partial recovery of a piece of information from the desired file;
- killing and removing Windows Defender;
- impersonation to automatically elevate permissions on local computers;
- SafeMode operation for bypassing anti-viruses and stronger encryption;
- port scanner in local subnets, can detect all shared DFS, SMB, WebDav resources;
- automatic distribution in the domain network at runtime without the need for scripts, GPO or psexec methods;
- safely delete the shadow copies;
- delete artifacts from system journals. It necessary to protect from forensics examination;
- shutting down the computer after finishing work, to make it impossible to remove the dump from RAM;
- printing claims on network printers in infinite numbers;
- work on all versions of Windows, with very flexible settings (exe, dll, ReflectiveDll, ps1);
- running on all versions of ESXi (except 4.0), with very flexible settings;
- work on multiple Linux versions (14 architectures for NAS encryption, RedHat, KVM and others);

All this and much more awaits you, if you join our team. If you do not find one of your favorite features, please inform us, maybe we will add it especially for you.

[Ransomware] LockBit 2.0 is an affiliate program.

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:
- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**
- **launch of computers switched off via Wake-on-Lan;**
- **print-out of requirements on network printers;**
- **available for all versions of Windows OS;**

LockBit 2.0 is the fastest encryption software all over the world. In order to make it clear, we made a comparative table with several similar programs indicating the encryption speed at same conditions, making no secret of their names.

1. Affiliate Program

Percentage rate of affiliate program is 20% of the ransom, if you think that this is too much and because of this you are working with another affiliate program or using your personal software, then you should not deny yourself the pleasure of working with us, just increase the amount of ransom by 20% and be happy.
You receive payments from companies to your personal wallets in any convenient currency and only then transfer the share to our affiliate program. However, for ransom amounts over $500 thousand, you give the attacked company 2 wallets for payment - one is yours, to which the company will transfer 80%, and the second is ours for 20%, thus we will be protected from scam on your part.

You personally communicate with the attacked companies and decide yourself how much money to take for your invaluable pentest work, which should surely be generously paid.

If you have any questions, doubts or complaints, you do not like something, please tell it to TOX support. If you are very shy, you can do it anonymously by creating a new one-time TOX. It is very important for us to know about all our strengths and weaknesses in order to constantly improve our service.

1. Affiliate Program

Rules of the affiliate program:

You must be active to work with our software package.

It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.

It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.

It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.

It is not forbidden to work with competitors, but be sure to report it and explain why and what you like from your competitors, we will implement any of your worthy wishes, we care very much about progress and constant development.

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

1. Affiliate Program

Rules of the affiliate program:

You must be active to work with our software package.

It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.

It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.

It is [illegible] to down[illegible]

It is [illegible] your worthy wishes, we care very much about progress and constant development.

Strictly forbidden to give access to the panel to other people… …your partner may turn out to be a mole or be arrested by the police at any moment

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

1. Affiliate Program

Rules of the affiliate program:

You must be active to work with our software package.

It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.

It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.

It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.

It is

wort

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants and other similar organisations. Allowed to steal data without encryption.

Cate

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

1. Affiliate Program

Rules of the affiliate program:

You must be active to work with our software package.

It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.

It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.

It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.

It is not forbidden to work with competitors, but be sure to report it and explain why and what you like from your competitors, we will implement any of your worthy wishes, we care very much about progress and constant development.

Categories of targets to attack:

It is forbidden to attack the post-soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lituania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

1. Affiliate Program

Rules of the affiliate program:

You must be active to work with our software package.

It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.

It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.

It is imperative to download va… …bility to download the information, ther…

It is not forbidden to work with… …y of your worthy wishes, we care very mu…

Categories of targets to atta…

It is illegal to encrypt files in cri… organizations. Allowed to steal … The oil and gas industry, such a… …ypted. It is allowed to steal data without… It is forbidden to attack the pos… …istan, Turkmenistan, Uzbekistan, Ukra… …Union, the former largest country in th…

- **Allowed to attack educational institutions as long as they are private**
- **Allowed to attack non-profit organisations**
- **Allowed to carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex**
- **Forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centres… …maternity hospitals.**
- **It is allowed to steal data from any medical facilities without encryption**
- **It is very commendable to attack police stations and any other law enforcement agencies**
- **It is allowed to attack government organisations only with revenue**

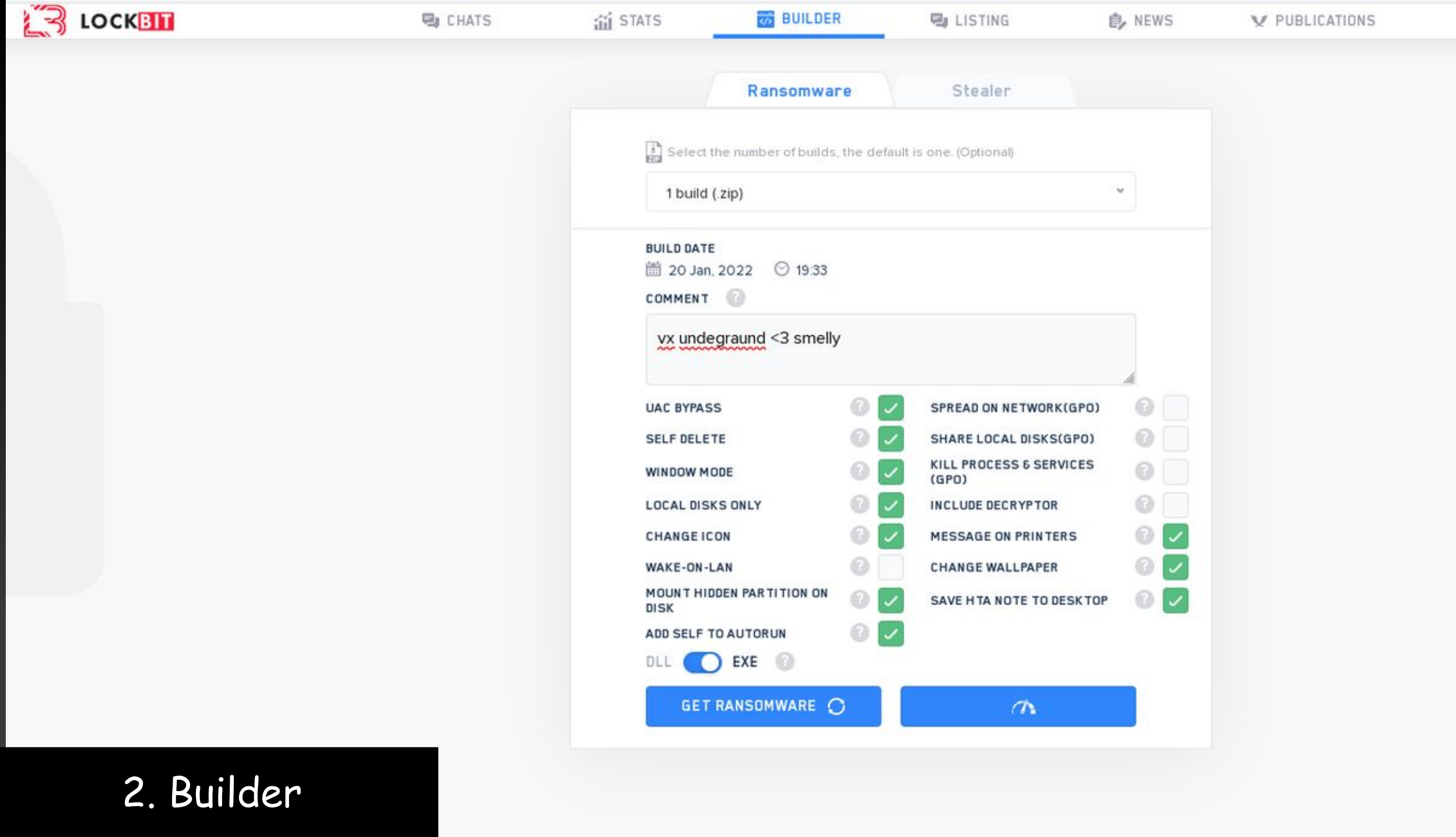
It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

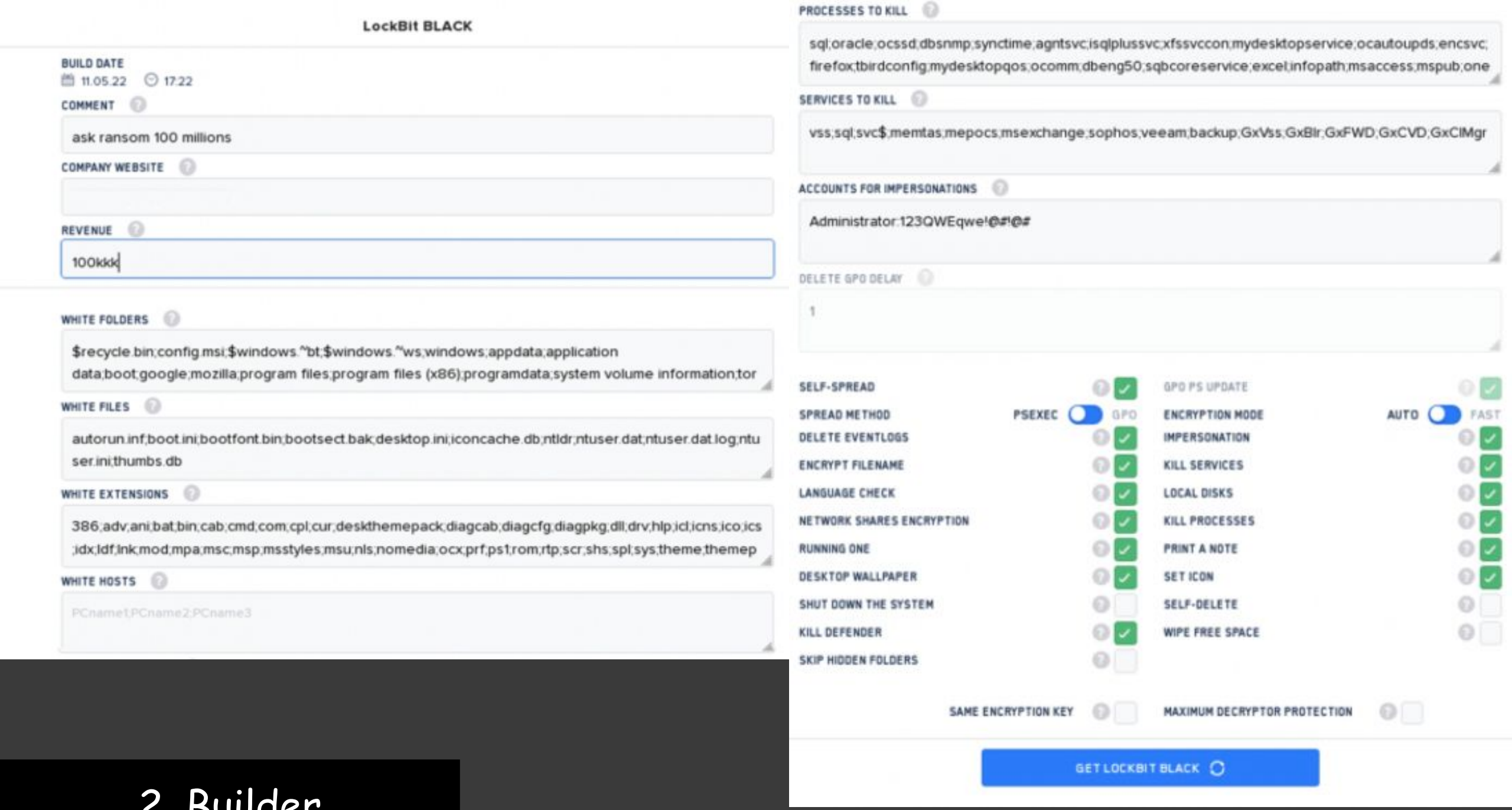
It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

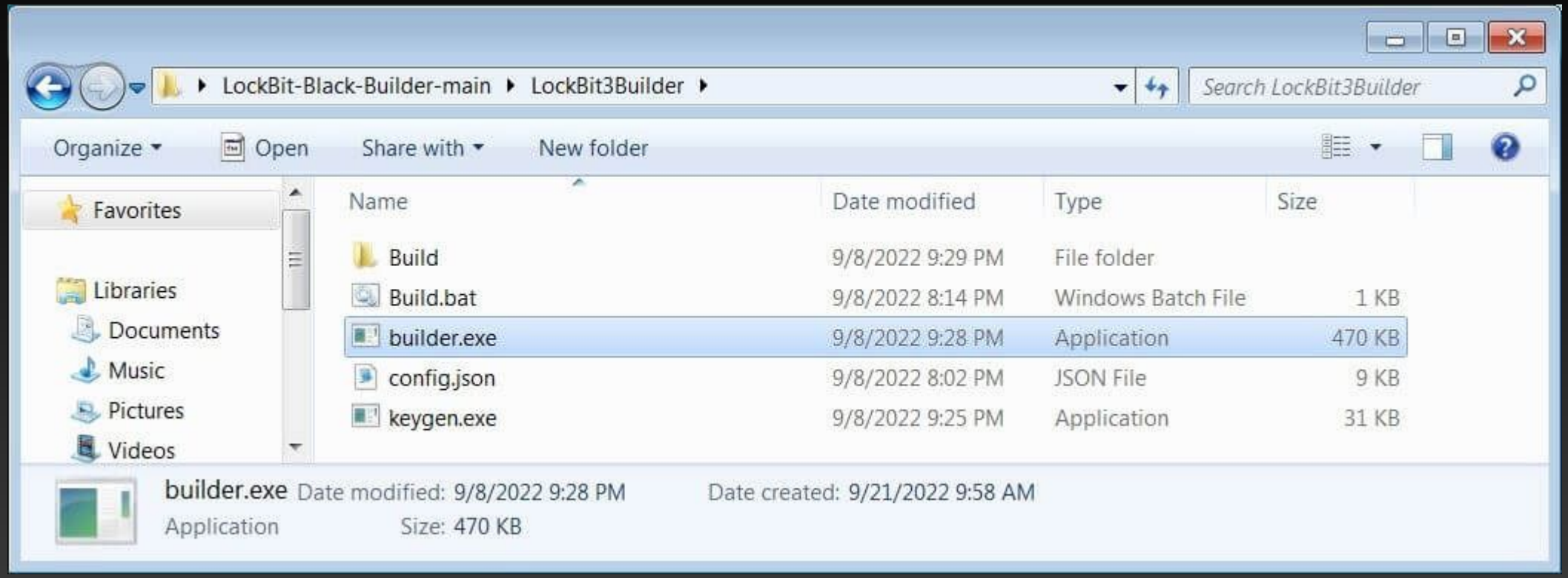
It is allowed to attack government organizations, only with revenue.


LOCKBIT
CHATS
STATS
BUILDER
LISTING
NEWS
PUBLICATIONS
Ransomware
Stealer
Select the number of builds, the default is one. (Optional)
1 build (.zip)
BUILD DATE
20 Jan, 2022
19:33
COMMENT
vx undegraund <3 smelly
UAC BYPASS
SELF DELETE
WINDOW MODE
LOCAL DISKS ONLY
CHANGE ICON
WAKE-ON-LAN
MOUNT HIDDEN PARTITION ON DISK
ADD SELF TO AUTORUN
SPREAD ON NETWORK(GPO)
SHARE LOCAL DISKS(GPO)
KILL PROCESS & SERVICES (GPO)
INCLUDE DECRYPTOR
MESSAGE ON PRINTERS
CHANGE WALLPAPER
SAVE HTA NOTE TO DESKTOP
DLL
EXE
GET RANSOMWARE

2. Builder


LockBit BLACK
BUILD DATE
11.05.22
17:22
COMMENT
ask ransom 100 millions
COMPANY WEBSITE
REVENUE
100kkk
WHITE FOLDERS
$recycle.bin;config.msi;$windows.~bt;$windows.~ws;windows;appdata;application data;boot;google;mozilla;program files;program files (x86);programdata;system volume information;tor
WHITE FILES
autorun.inf;boot.ini;bootfont.bin;bootsect.bak;desktop.ini;iconcache.db;ntldr;ntuser.dat;ntuser.dat.log;ntuser.ini;thumbs.db
WHITE EXTENSIONS
386;adv;ani;bat;bin;cab;cmd;com;cpl;cur;deskthemepack;diagcab;diagcfg;diagpkg;dll;drv;hlp;icl;icns;ico;ics;idx;ldf;lnk;mod;mpa;msc;msp;msstyles;msu;nls;nomedia;ocx;prf;ps1;rom;rtp;scr;shs;spl;sys;theme;themep
WHITE HOSTS
PCname1;PCname2;PCname3
PROCESSES TO KILL
sql;oracle;ocssd;dbsnmp;synctime;agntsvc;isqlplussvc;xfssvccon;mydesktopservice;ocautoupds;encsvc;firefox;tbirdconfig;mydesktopqos;ocomm;dbeng50;sqbcoreservice;excel;infopath;msaccess;mspub;one
SERVICES TO KILL
vss;sql;svc$;memtas;mepocs;msexchange;sophos;veeam;backup;GxVss;GxBlr;GxFWD;GxCVD;GxCIMgr
ACCOUNTS FOR IMPERSONATIONS
Administrator:123QWEqwe!@#!@#
DELETE GPO DELAY
1
SELF-SPREAD
SPREAD METHOD
PSEXEC
GPO
DELETE EVENTLOGS
ENCRYPT FILENAME
LANGUAGE CHECK
NETWORK SHARES ENCRYPTION
RUNNING ONE
DESKTOP WALLPAPER
SHUT DOWN THE SYSTEM
KILL DEFENDER
SKIP HIDDEN FOLDERS
GPO PS UPDATE
ENCRYPTION MODE
AUTO
FAST
IMPERSONATION
KILL SERVICES
LOCAL DISKS
KILL PROCESSES
PRINT A NOTE
SET ICON
SELF-DELETE
WIPE FREE SPACE
SAME ENCRYPTION KEY
MAXIMUM DECRYPTOR PROTECTION
GET LOCKBIT BLACK

2. Builder


LockBit-Black-Builder-main ▸ LockBit3Builder ▸
Search LockBit3Builder
Organize
Open
Share with
New folder
Favorites
Libraries
Documents
Music
Pictures
Videos
Name
Date modified
Type
Size
Build 9/8/2022 9:29 PM File folder
Build.bat 9/8/2022 8:14 PM Windows Batch File 1 KB
builder.exe 9/8/2022 9:28 PM Application 470 KB
config.json 9/8/2022 8:02 PM JSON File 9 KB
keygen.exe 9/8/2022 9:25 PM Application 31 KB
builder.exe Date modified: 9/8/2022 9:28 PM Date created: 9/21/2022 9:58 AM
Application Size: 470 KB

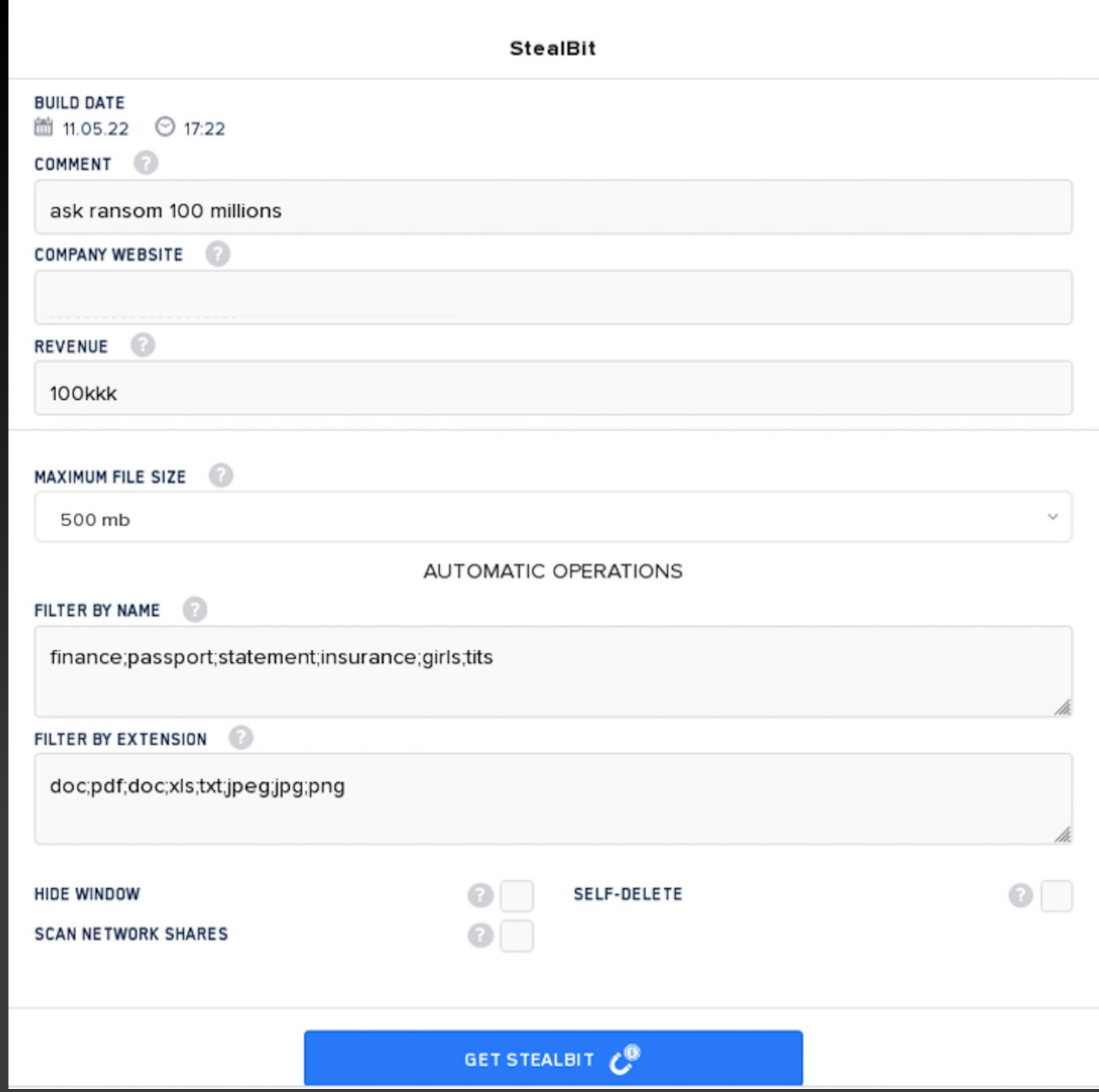
2. Builder

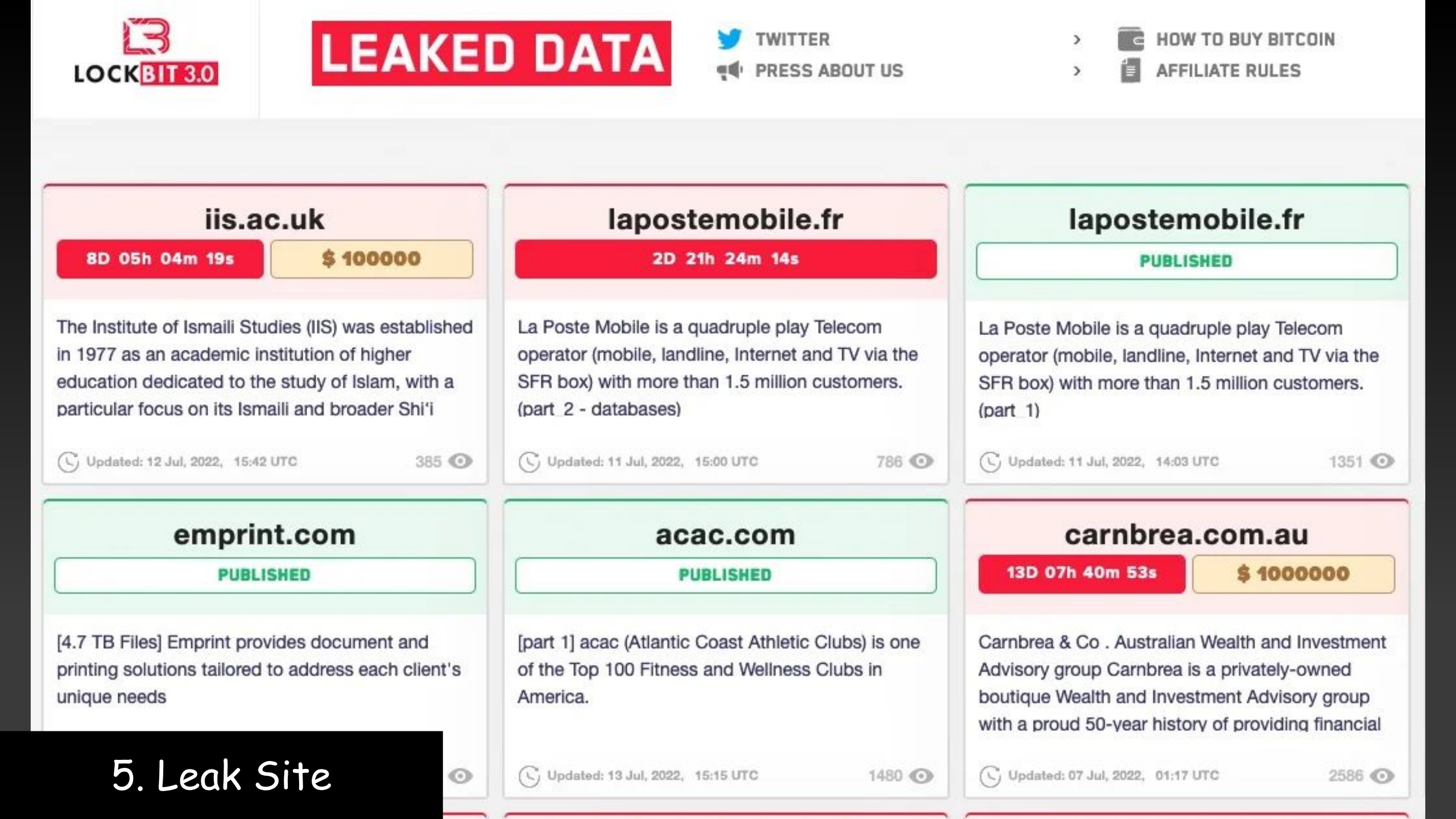
3. Infection


LOCKBIT 2.0
ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!
All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.
Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
3085B89A0C515D2FB124D645906F5D3DA5CB97CE8EA975959AE4F95302A04E1D709C3C4AE9B7
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
http://lockbitapt6vx57t3eeqjofwgcglmutr3a35nygvokja5uuccip4ykyd.onion

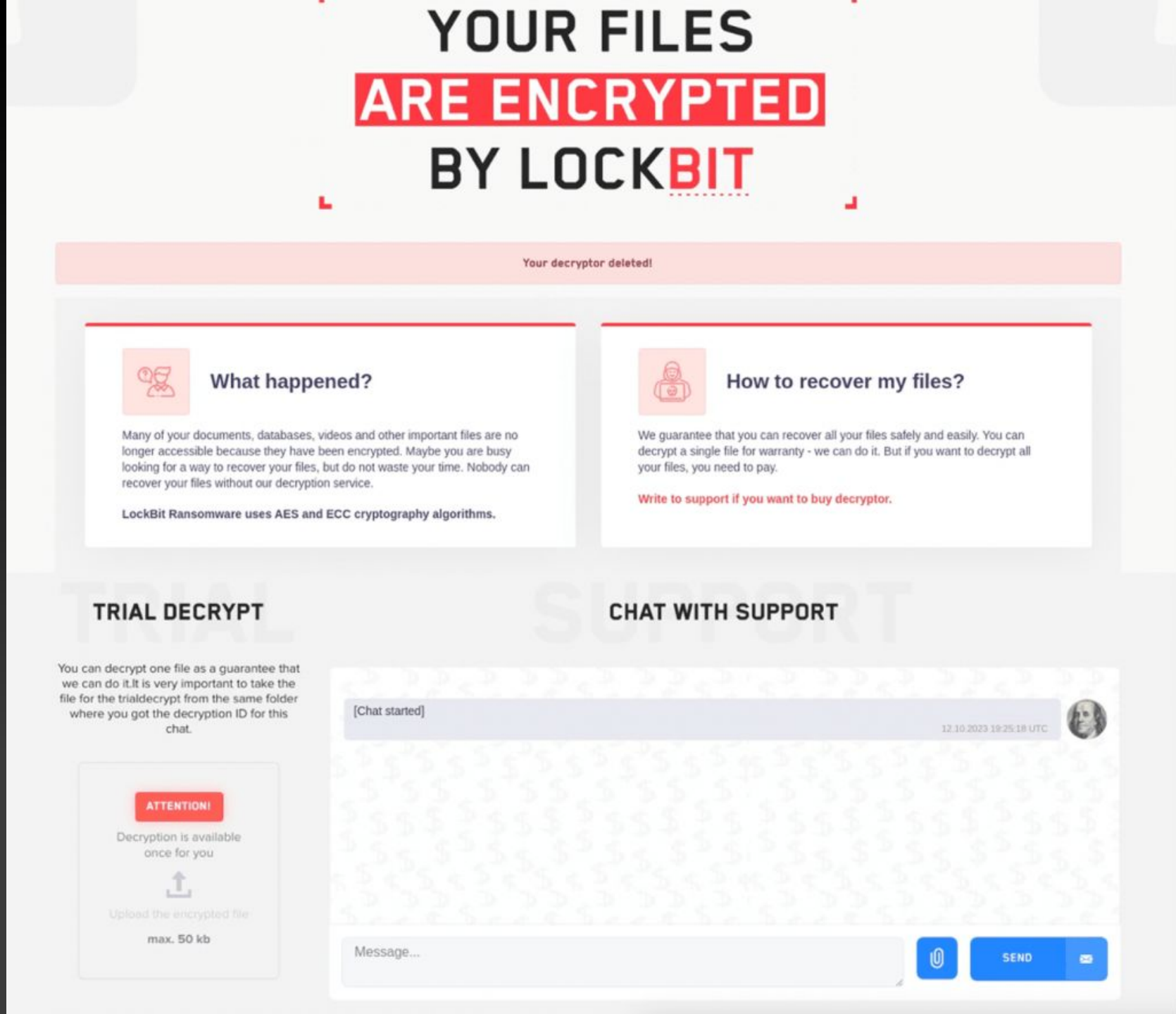
4. Exfiltration

- LockBit have developed a tool called StealBit, which their affiliates can use to exfiltrate data from their victims computers.



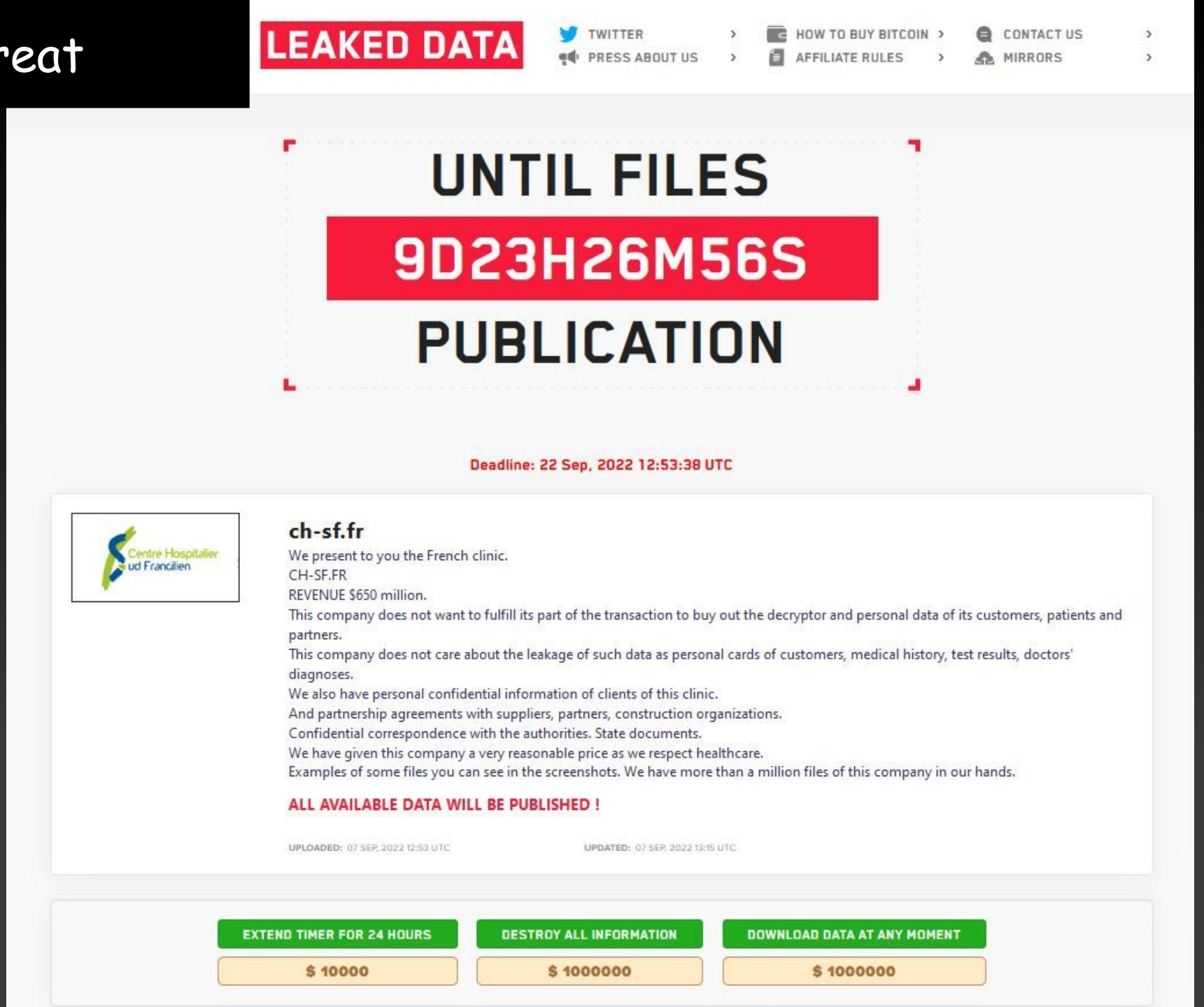

LOCKBIT 3.0
LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
iis.ac.uk
8D 05h 04m 19s
$ 100000
The Institute of Ismaili Studies (IIS) was established in 1977 as an academic institution of higher education dedicated to the study of Islam, with a particular focus on its Ismaili and broader Shi'i
Updated: 12 Jul, 2022, 15:42 UTC
385
lapostemobile.fr
2D 21h 24m 14s
La Poste Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part_2 - databases)
Updated: 11 Jul, 2022, 15:00 UTC
786
lapostemobile.fr
PUBLISHED
La Poste Mobile is a quadruple play Telecom operator (mobile, landline, Internet and TV via the SFR box) with more than 1.5 million customers. (part_1)
Updated: 11 Jul, 2022, 14:03 UTC
1351
emprint.com
PUBLISHED
[4.7 TB Files] Emprint provides document and printing solutions tailored to address each client's unique needs
acac.com
PUBLISHED
[part 1] acac (Atlantic Coast Athletic Clubs) is one of the Top 100 Fitness and Wellness Clubs in America.
Updated: 13 Jul, 2022, 15:15 UTC
1480
carnbrea.com.au
13D 07h 40m 53s
$ 1000000
Carnbrea & Co . Australian Wealth and Investment Advisory group Carnbrea is a privately-owned boutique Wealth and Investment Advisory group with a proud 50-year history of providing financial
Updated: 07 Jul, 2022, 01:17 UTC
2586

5. Leak Site



6. Victim Page

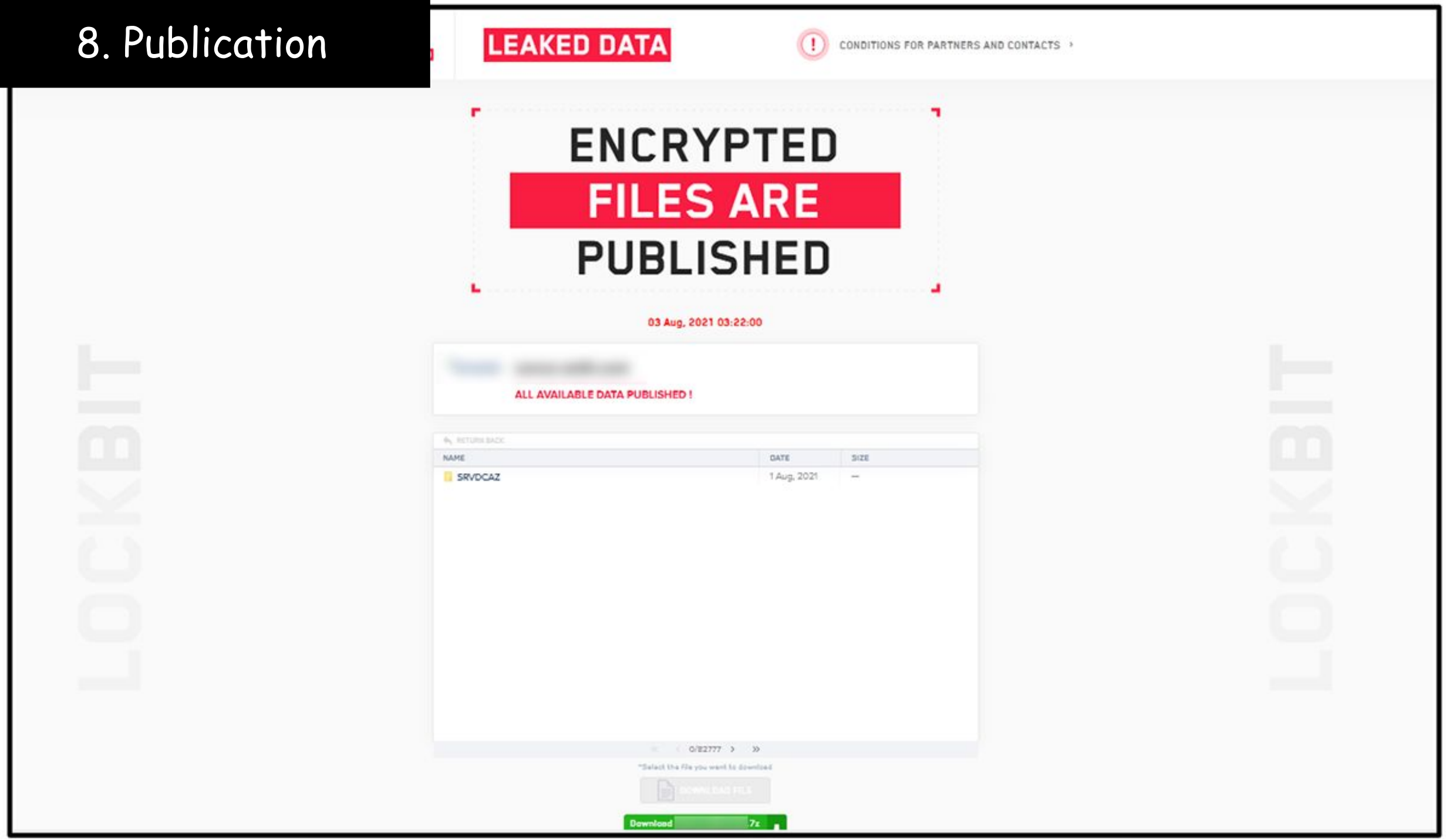
7. Threat


LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS
UNTIL FILES
9D23H26M56S
PUBLICATION
Deadline: 22 Sep, 2022 12:53:38 UTC
Centre Hospitalier ud Francilien
ch-sf.fr
We present to you the French clinic.
CH-SF.FR
REVENUE $650 million.
This company does not want to fulfill its part of the transaction to buy out the decryptor and personal data of its customers, patients and partners.
This company does not care about the leakage of such data as personal cards of customers, medical history, test results, doctors' diagnoses.
We also have personal confidential information of clients of this clinic.
And partnership agreements with suppliers, partners, construction organizations.
Confidential correspondence with the authorities. State documents.
We have given this company a very reasonable price as we respect healthcare.
Examples of some files you can see in the screenshots. We have more than a million files of this company in our hands.
ALL AVAILABLE DATA WILL BE PUBLISHED !
UPLOADED: 07 SEP, 2022 12:53 UTC
UPDATED: 07 SEP, 2022 13:15 UTC
EXTEND TIMER FOR 24 HOURS
$ 10000
DESTROY ALL INFORMATION
$ 1000000
DOWNLOAD DATA AT ANY MOMENT
$ 1000000

7. Threat


EXTEND TIMER FOR 24 HOURS
$ 10000
DESTROY ALL INFORMATION
$ 1000000
DOWNLOAD DATA AT ANY MOMENT
$ 1000000

8. Publication



Why RaaS is so Dangerous?

- Double extortion (or sometimes triple).
- Any attacker with the experience (and money) can use a highly complex malware program.
- Every time a build is generated, it's different. Signature detection is hard.
- It's new. This is just the start.

Demonstration

Demo - LockBit

1. Configure our own LockBit sample
2. Use the builder to create our malware
3. Take a look at our generated build
4. Infect our system
5. Decrypt our files


OMU
HACKERS

Today's Task...

Basic Malware Analysis

1. Go to the DMU Hackers GitHub in the week 17 folder.
2. Download the malware sample.
3. Complete the tasks.
4. Use the hints if needed!
1. Solutions will be uploaded after the session.

http://tinyurl.com/dmuhackers-malware

Resources & Further Reading

- https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/
- https://www.ncsc.gov.uk/section/keep-up-to-date/malware-analysis-reports
- https://tryhackme.com/module/malware-analysis
- https://www.sans.org/blog/how-you-can-start-learning-malware-analysis/
- https://www.amazon.co.uk/Practical-Malware-Analysis-Hands-Dissecting/dp/1593272901


SALOON
Dr. Squatch
It's time to hydrate


Dr. Squatch
It's time to hydrate