DevFest

GDG Open - Lima

Anatomía de un Ransomware

Mauricio J.

Google Developer Groups

Agenda

1. ¿Quién soy?
2. ¿Qué es un Ransomware?
3. ¿Cómo funciona?
4. Ransomware en el mundo real
5. Conclusiones

Mauricio J.

- Security Researcher
  Ethical Hacker
  Red Teamer

- CRTO / CEH / EWPT

- Peruhack
  Ekoparty - Red Team Space
  Bsides

Google Developer Groups

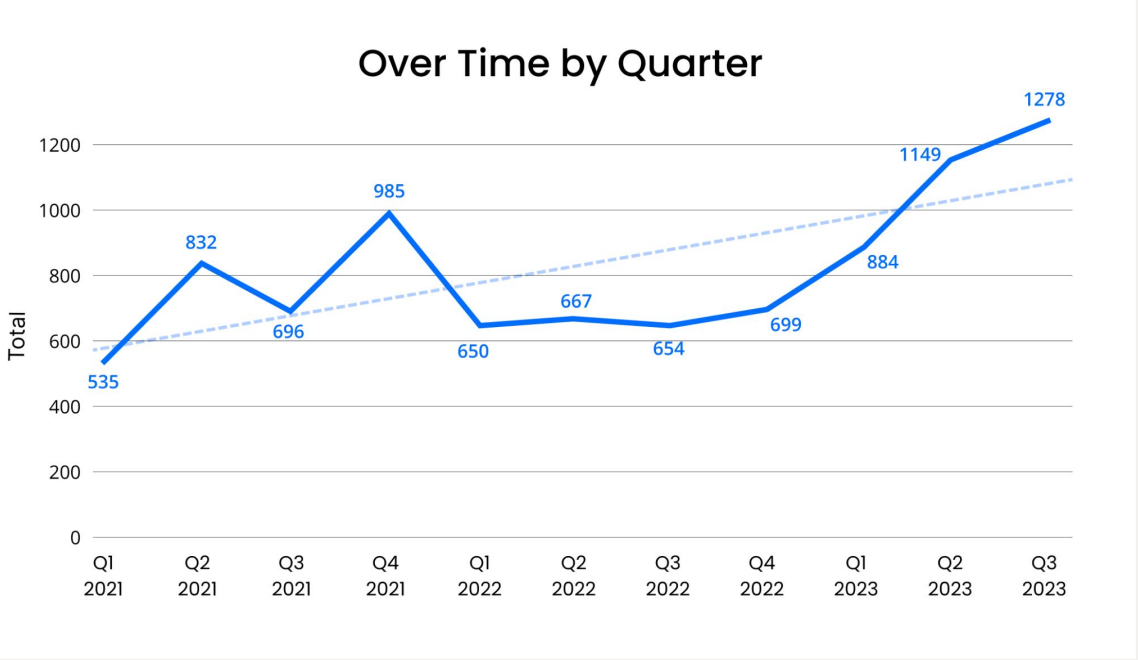
DevFest

GDG Open - Lima

¿Qué es un Ransomware?

Google Developer Groups

Google Developer Groups



Fuente: https://www.corvusinsurance.com/blog/q3-ransomware-report

DevFest

GDG Open - Lima

Google Developer Groups

LockBit extorted billions of dollars from victims, fresh leaks suggest

Investigating LockBit's finances has blown previous estimates of the operation's wealth out of the water

RANSOMWARE

US Organizations Paid $91 Million to LockBit Ransomware Gang

LockBit ransomware operators launched 1,700 attacks in the US and received roughly $91 million in ransom payments.

17 Feb

Conti Ransomware Attacks Reap in $180 Million in 2021 as Average Ransomware Payments Rise by 34%

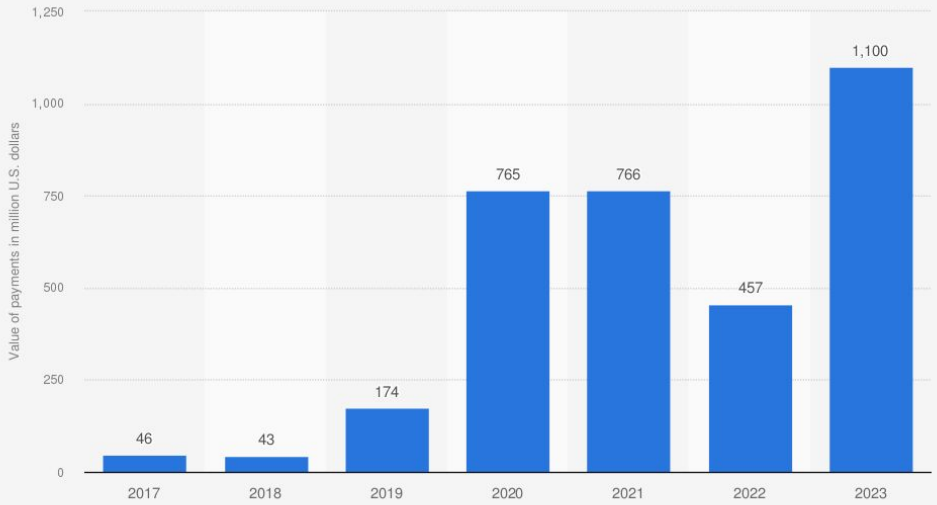
Stu Sjouwerman

Google Developer Groups

DevFest

GDG Open - Lima

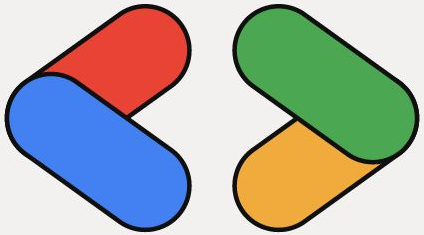
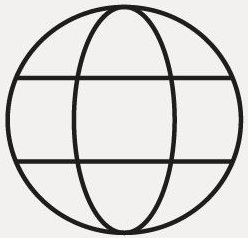
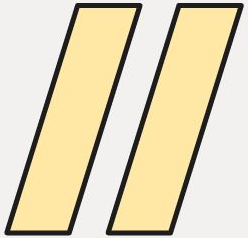
Total annual amount of money received by ransomware actors worldwide from 2017 to 2023 (in million U.S. dollars)



Sources
Malwarebytes; Chainalysis
© Statista 2024

Additional Information:
Worldwide; Chainalysis; 2017 to 2023; data is based on an analysis of the cryptocurrency addresses known to be controlle
wider industry metrics may vary

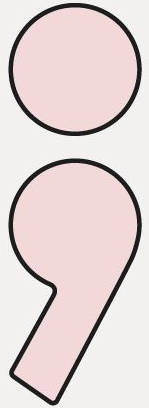
Google Developer Groups

DevFest

GDG Open - Lima

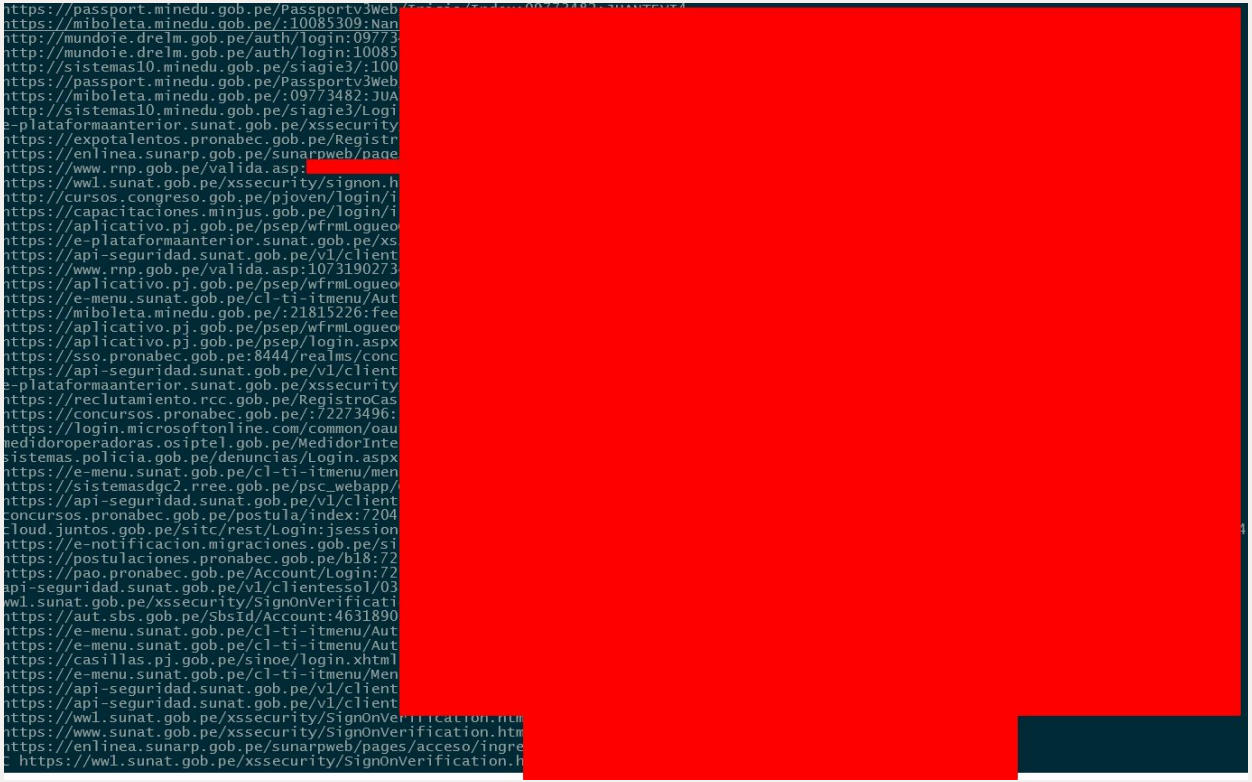
¿Cómo funciona un Ransomware?



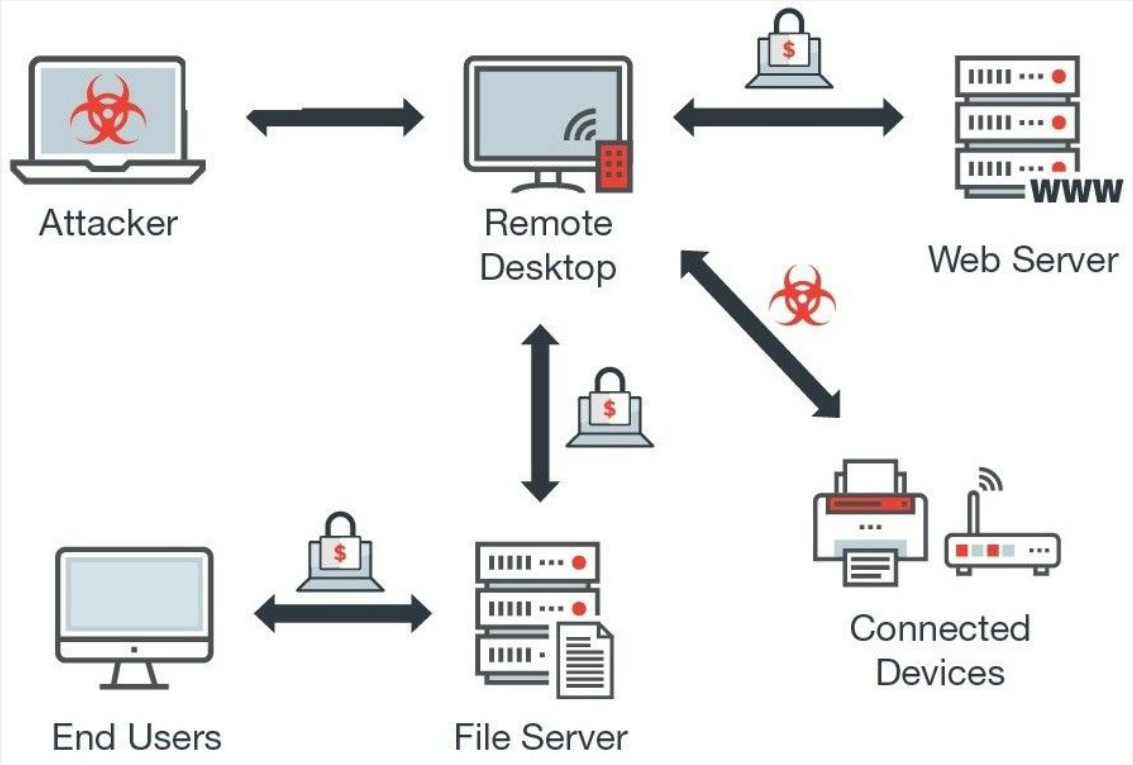
Google Developer Groups

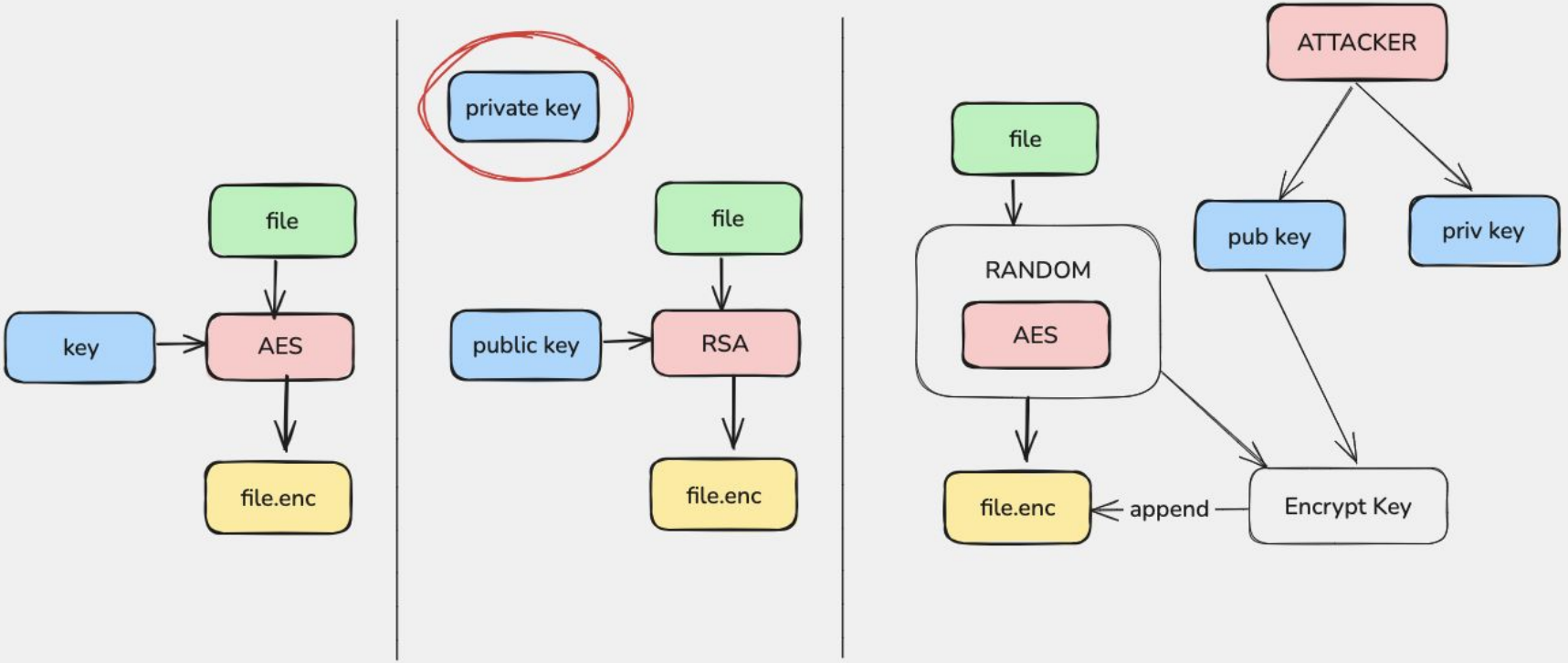
Acceso Inicial	Compromiso	Exfiltración	Encriptación
Phishing	Persistencia	Contraseñas	Claves únicas
Documentos	Movimiento Lateral	Información sensible	Nota con el detalle de la encriptación
Cracks	Extracción de credenciales	Extorsión	Negociaciones
Stealers		Demanda de dinero	

Google Developer Groups

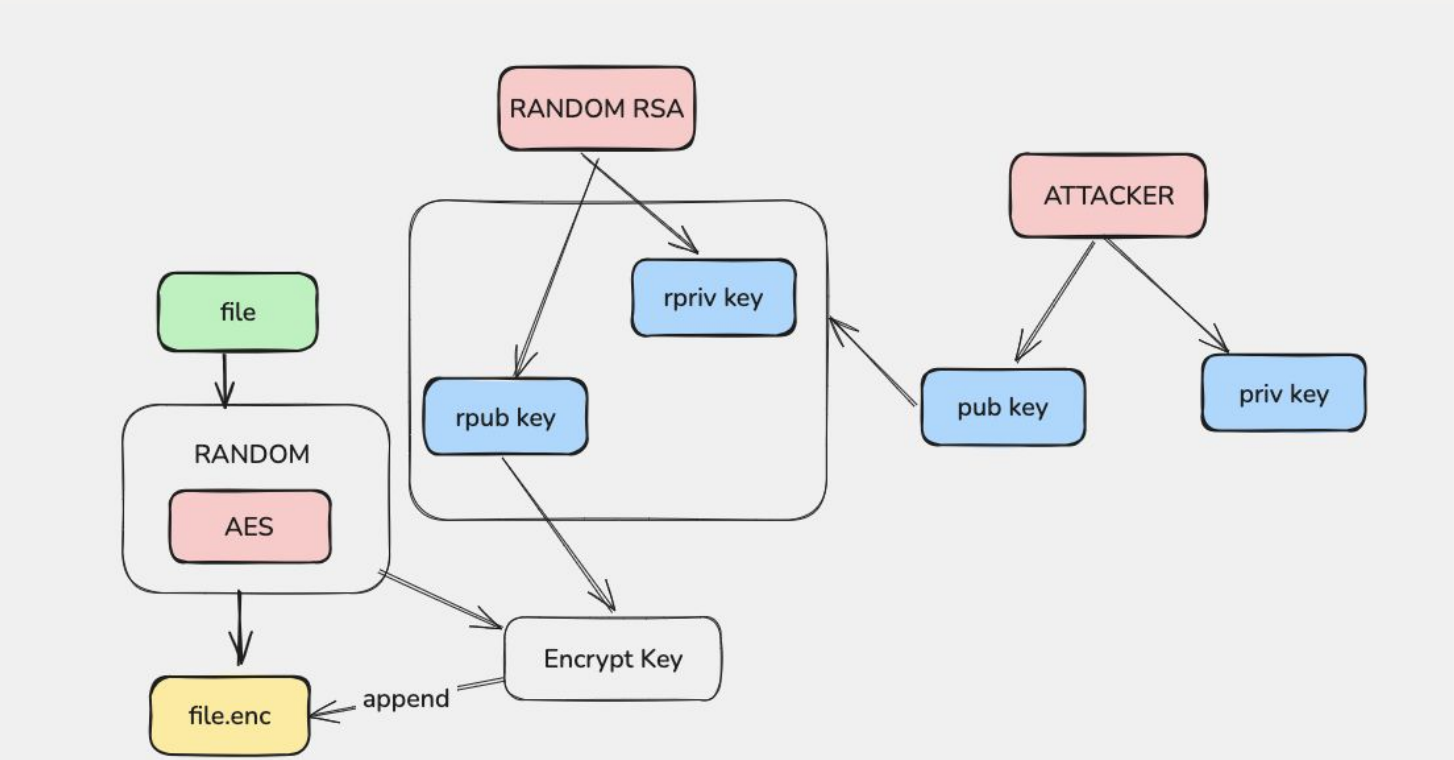


Google Developer Groups

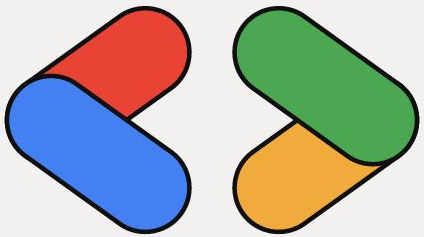
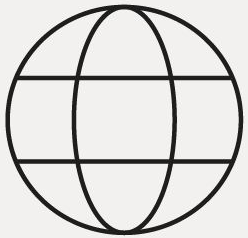
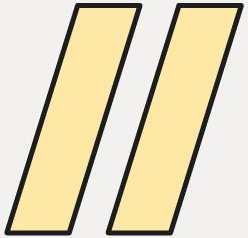

Attacker
Remote Desktop
Web Server
www
End Users
File Server
Connected Devices



Google Developer Groups



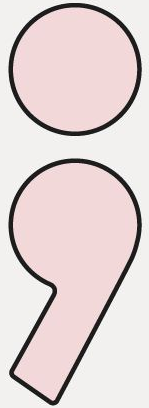
Google Developer Groups

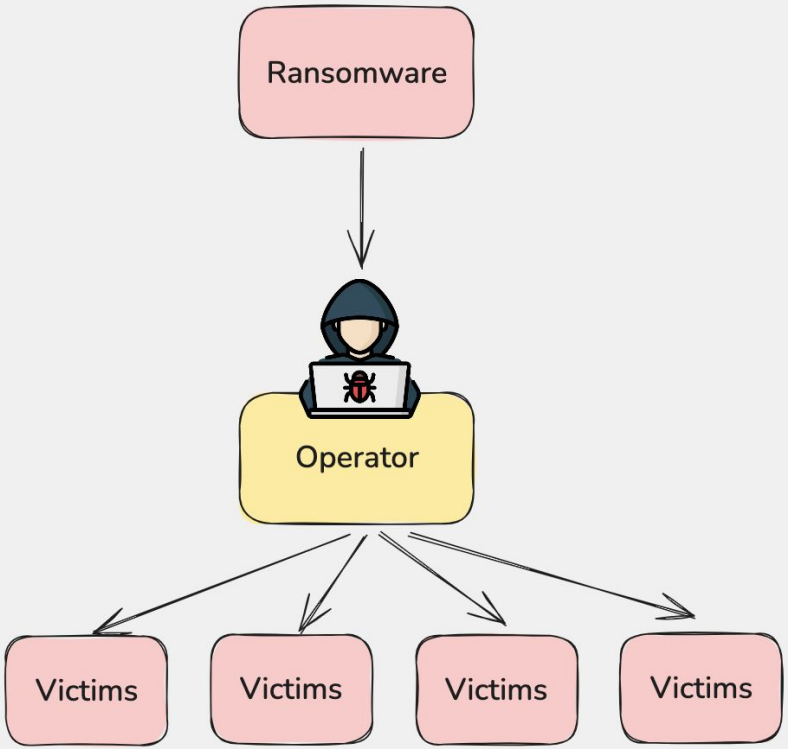
DevFest

GDG Open - Lima

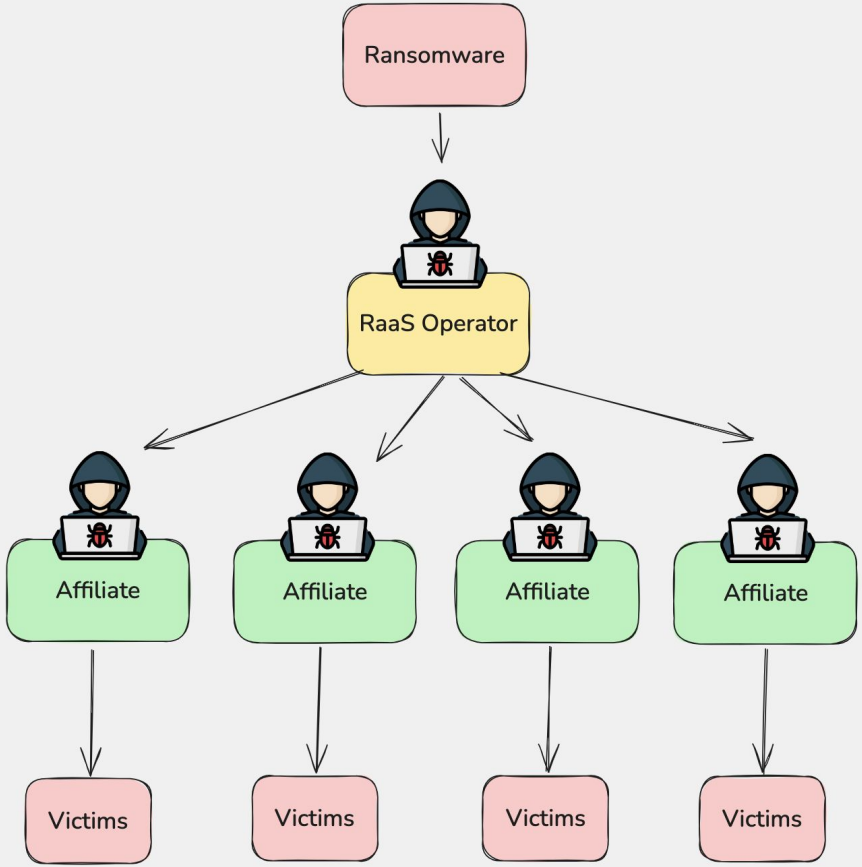
¿Qué es un RaaS?



Google Developer Groups



Google Developer Groups



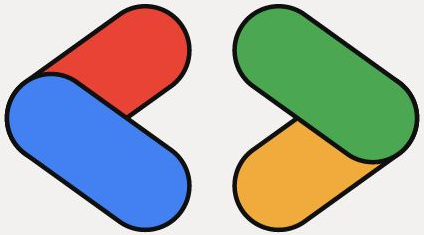
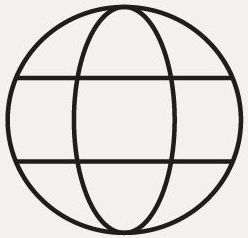
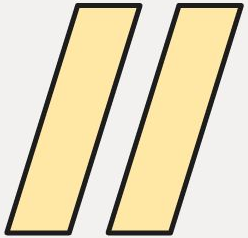
Google Developer Groups

DevFest

GDG Open - Lima

Fuente: https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/

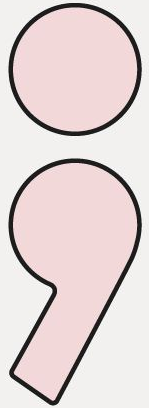
Google Developer Groups

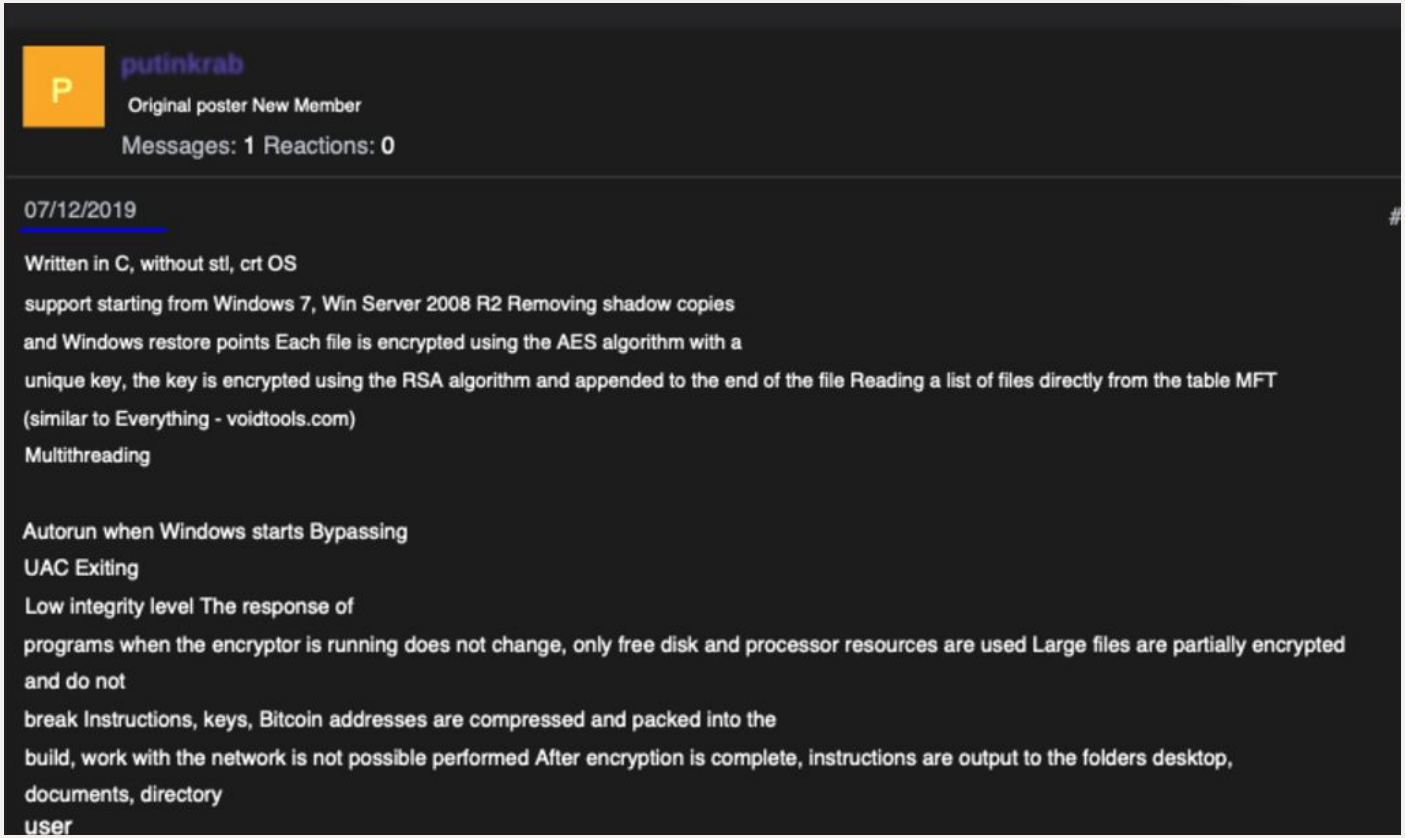
DevFest

GDG Open - Lima

Ransomware en el mundo real



Google Developer Groups


P
putinkrab
Original poster New Member
Messages: 1 Reactions: 0
07/12/2019
Written in C, without stl, crt OS
support starting from Windows 7, Win Server 2008 R2 Removing shadow copies
and Windows restore points Each file is encrypted using the AES algorithm with a
unique key, the key is encrypted using the RSA algorithm and appended to the end of the file Reading a list of files directly from the table MFT
(similar to Everything - voidtools.com)
Multithreading
Autorun when Windows starts Bypassing
UAC Exiting
Low integrity level The response of
programs when the encryptor is running does not change, only free disk and processor resources are used Large files are partially encrypted
and do not
break Instructions, keys, Bitcoin addresses are compressed and packed into the
build, work with the network is not possible performed After encryption is complete, instructions are output to the folders desktop,
documents, directory
user

NO AVATAR

Lockbi

Premium

Premium

registration: 01/17/2020
Messages: 6
Reactions: 4
Points: 3

01/17/2020 Topic Author #1

Hello friends!

Lokbit development has been underway since September 2019; they could not decrypt; there have been attempts.

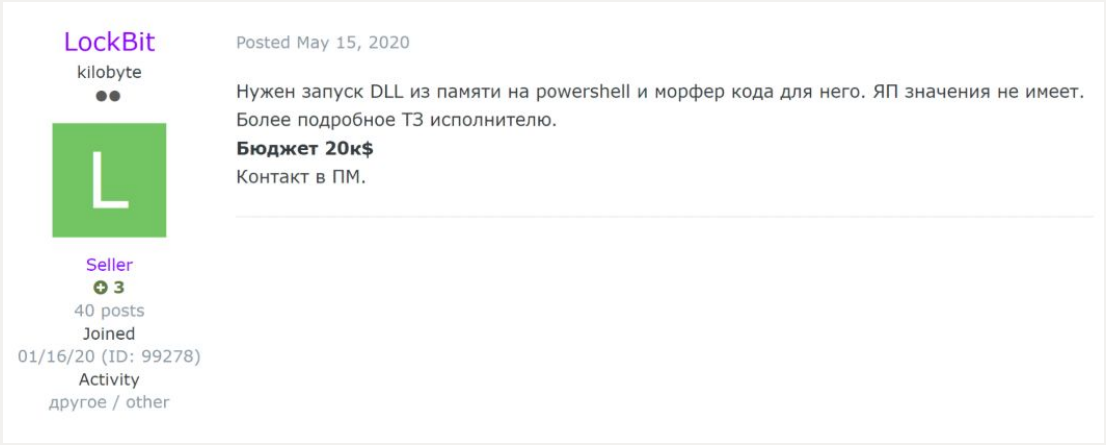
There are no school emails, multithreading, which, in fact, loads the system more than encrypts, is not here.

The software is written in C and Asembler, encryption through the IO completion port, port scanner on local subnets, finds all DFS, SMB, WebDav balls, admin in the torus, automatic test decryption, descriptor output, chat with PUSH notifications, Jabber bot forwarding correspondence , termination of services / processes according to the list and preventing the opening of the file in the moment. Setting file permissions and removing blocking attributes, deleting shadow copies, cleaning logs, mounting hidden partitions, drag'n'drop files and folders, console / hidden mode of operation. Encrypts files in chunks in different places, the larger the file size, the more chunks. Algorithm AES + RSA.
The amount of the ransom is set by you after talking with the patient, you receive payment in your wallets, in a convenient currency.
Jabber-bot completely replaces the admin panel, ban, decrypt, chat - all this without leaving the jabber.

Work speed clearly

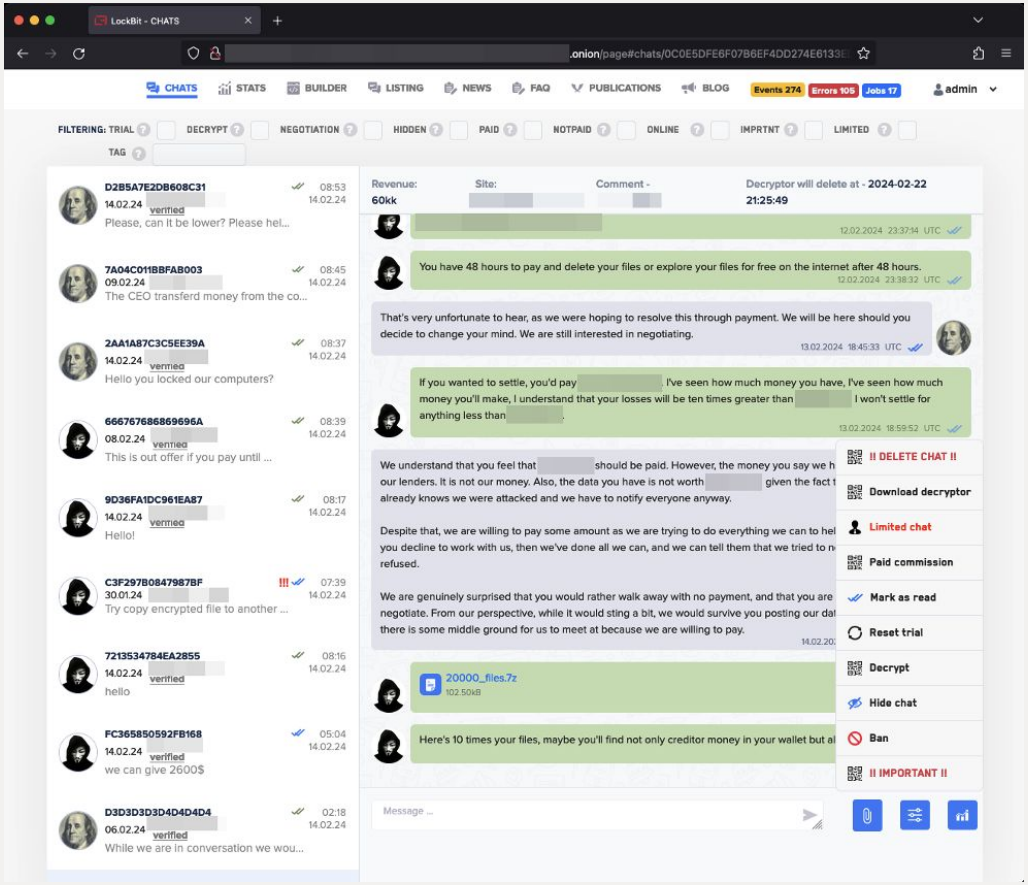
Local NVMe SSD M.2

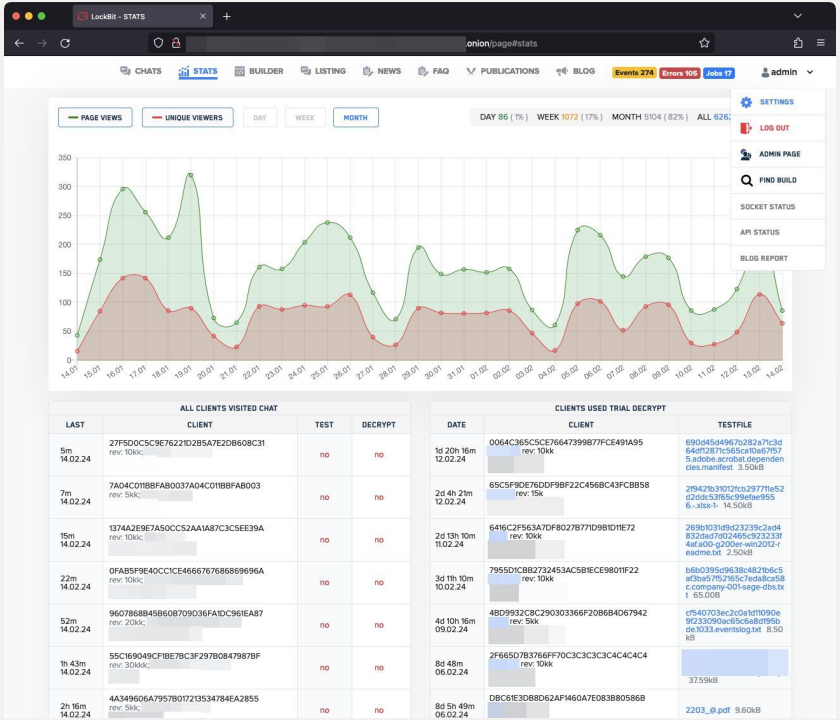
Google Developer Groups


LockBit
kilobyte
L
Seller
3
40 posts
Joined
01/16/20 (ID: 99278)
Activity
другое / other
Posted May 15, 2020
Нужен запуск DLL из памяти на powershell и морфер кода для него. ЯП значения не имеет.
Более подробное ТЗ исполнителю.
Бюджет 20к$
Контакт в ПМ.

LockBit
kilobytes
L
Posted September 16, 2020
Looking for a specialist.
We need automation of one task for the entire domain. Active Directory Group Policies.
The price starts from $5k. Contact in PM.
+
Quote

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
[redacted]
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[redacted]
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
[redacted]





Google Developer Groups

TechRadar

LockBit ransomware attack stole data on millions of Infosys McCamish users

When LockBit ransomware affiliates struck Infosys McCamish Systems (IMS) in late 2023, they did not steal sensitive information on some...

The Record from Recorded Future News

Industrial and Commercial Bank of China dealing with LockBit ransomware attack

One of the world's largest banks is dealing with a ransomware attack, according to media reports on Thursday.

SC Media UK

LockBit Ransomware Operators Demanded $80M from Royal Mail

The operators of LockBit demanded an $80 million ransom payment, according to TechCrunch. The ransomware gang threatened to publish all stolen data from the...

BankInfoSecurity

LockBit Leaks 1.5TB of Data Stolen From Indonesia's BSI Bank

The LockBit ransomware group on Tuesday published 1.5 terabytes of personal and financial information the group said it stole from Bank Syariah Indonesia.

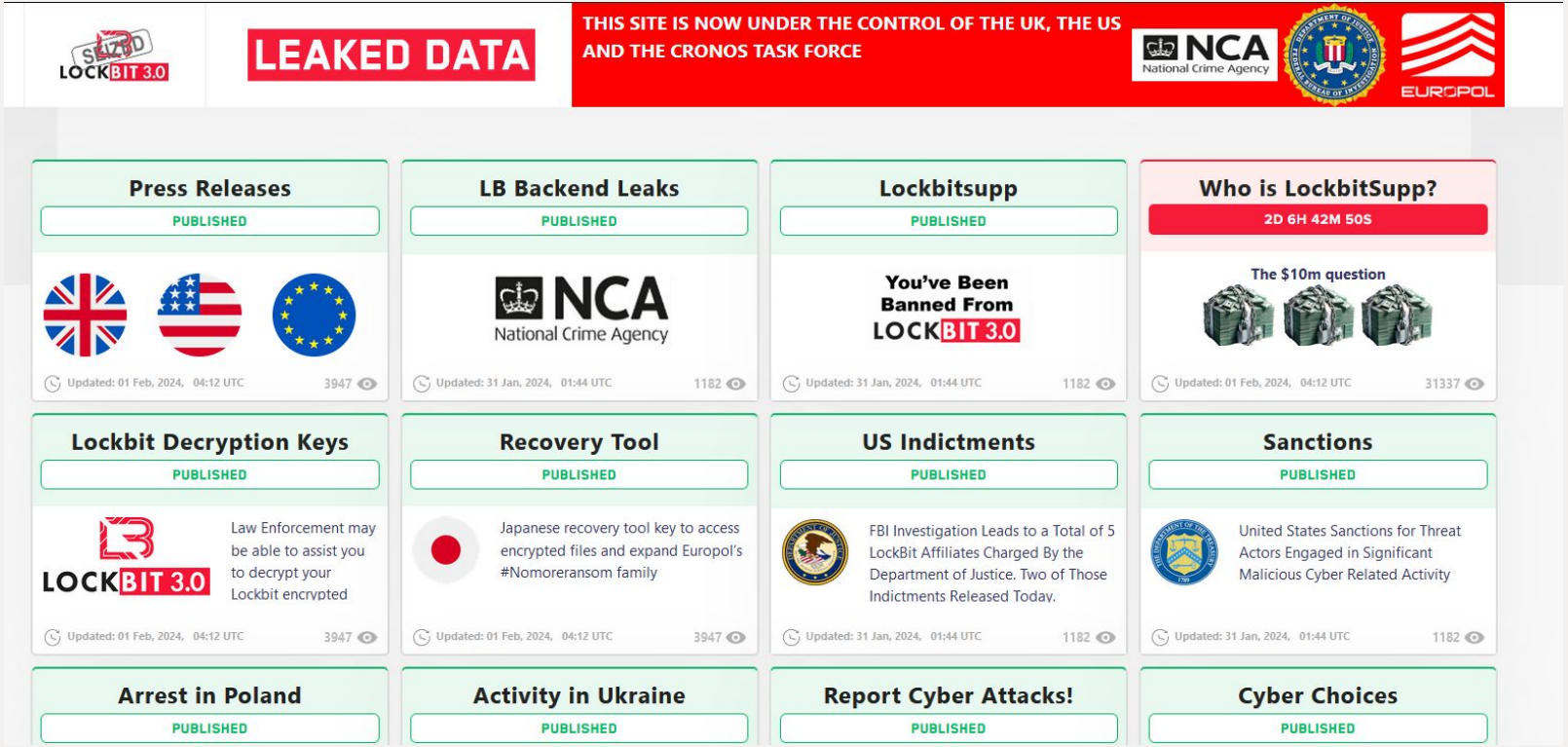
Google Developer Groups

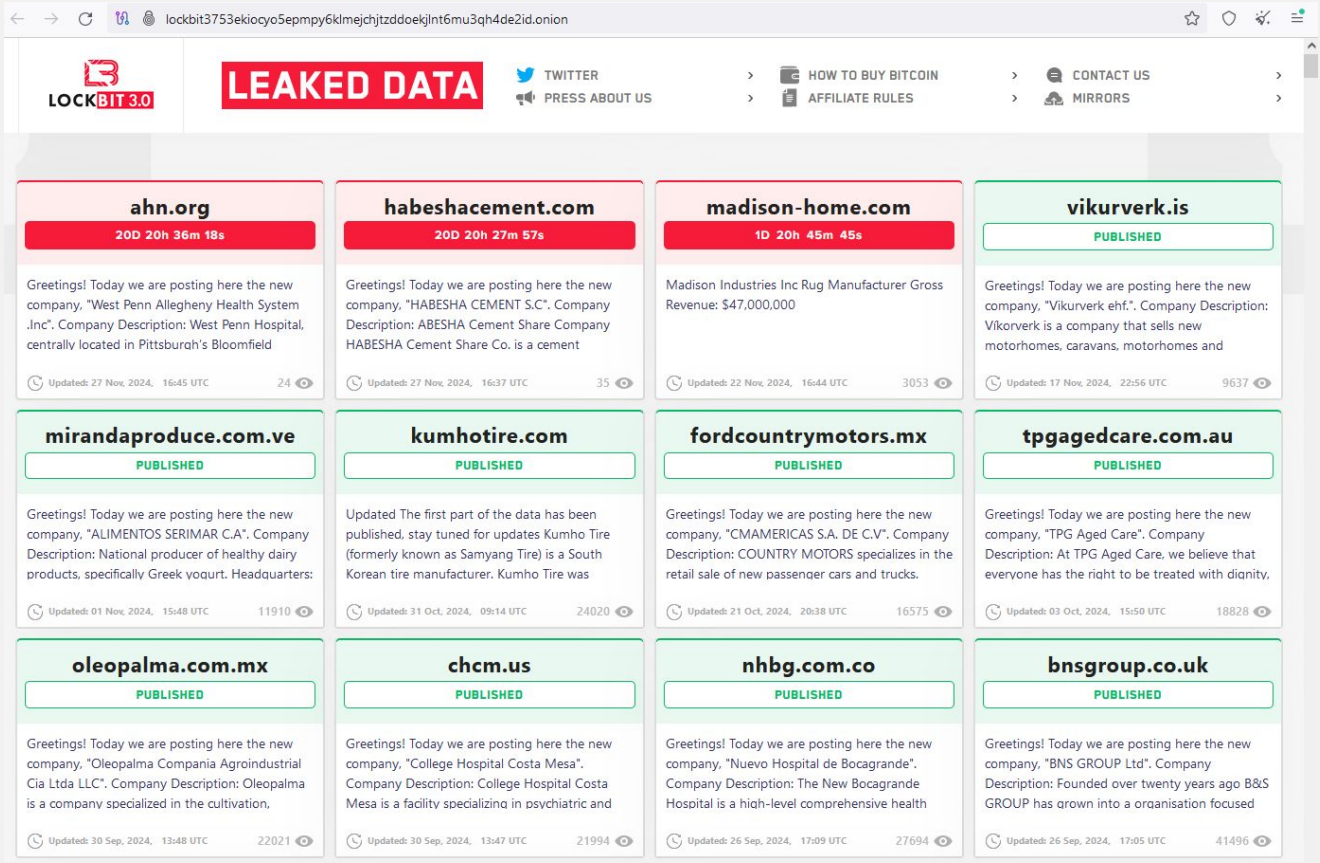
Encryption speed comparative table for some ransomware							
PC for testing: Windows Server 2016 x64 \ 8 core Xeon E5-2680@2.40GHz \ 16 GB RAM \ SSD							
Name of the ransomware	Date of a sample	Speed in megabytes per second	Time spent for encryption of 100 GB	Time spent for encryption of 10 TB	Self spread	Size sample in KB	The number of the encrypted files (All file in a system 257472)
LOCKBIT 2.0	5 Jun, 2021	373 MB/s	4M 28S	7H 26M 40S	Yes	855	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130	110468
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186	110220
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274	110784

Fuente:
https://www.splunk.com/en_us/blog/security/gone-in-52-seconds-and-42-minutes-a-comparative-analysis-of-ransomware-encryption-speed.html

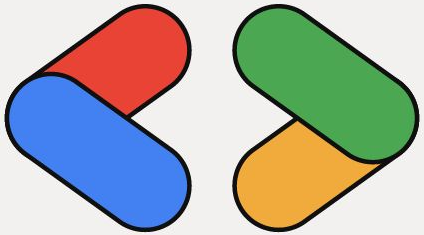
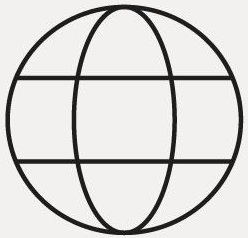
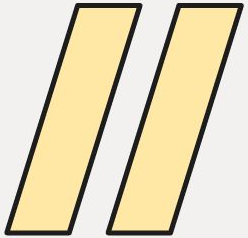
```php
<?php
$phar = new Phar('malicious.phar');
$phar->startBuffering();
$phar->addFromString(str_repeat('A', PHP_MAXPATHLEN - 1).'B', 'This is the content of the file.');
$phar->stopBuffering();
?>
```

Google Developer Groups


SEIZED
LOCKBIT 3.0
LEAKED DATA
THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE
NCA
National Crime Agency
EUROPOL
Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC
3947
LB Backend Leaks
PUBLISHED
NCA
National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC
1182
Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC
1182
Who is LockbitSupp?
2D 6H 42M 50S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC
31337
Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to decrypt your Lockbit encrypted
Updated: 01 Feb, 2024, 04:12 UTC
3947
Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
Updated: 01 Feb, 2024, 04:12 UTC
3947
US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.
Updated: 31 Jan, 2024, 01:44 UTC
1182
Sanctions
PUBLISHED
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC
1182
Arrest in Poland
PUBLISHED
Activity in Ukraine
PUBLISHED
Report Cyber Attacks!
PUBLISHED
Cyber Choices
PUBLISHED



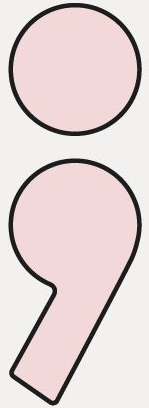
Google Developer Groups

DevFest

GDG Open - Lima

GRACIAS 😎



Google
Developer
Groups