A real-world ransomware scenario and what would have stopped it

Agenda

- Introduction
- Overview
- Impact of Ransomware
- Methods
- Distribution of Attacks
- Attacks to Industry
- Common Ransomware Payloads
- Proof of Concept
- Fixes
- References

A real-world ransomware scenario and what would have stopped it

GTCONSULT
enabling productivity

GTconsult provides outsourced managed services by nurturing and growing talent in niche IT technologies for businesses around the world.

A Team
PROTECTION

We hack you before you get hacked. Using real world attack methodologies we identify risk and present our findings with mitigations. Our A Team clients are monitored proactively and notified of any new threats or vulnerabilities.

Hack Van

GET HACKED
www.gtconsult.com
SCAN ME

GET HACKED
www.gtconsult.com
"We hack you
B4
the bad guys do"
SCAN ME
NU 136-931

A real-world ransomware scenario and what would have stopped it

Introduction

Bradley Geldenhuys
Founder and Chairman of GTconsult
Father, Husband,
Entrepreneur & Certified Hacker

A real-world ransomware scenario and what would have stopped it

Introduction

Kyle Farr
Security Analyst and Pentest at GTconsult
Certified Hacker

A real-world ransomware scenario and what would have stopped it

200 Thousand $ Average Ransom in 2020

80 Percent Suffered another attack soon after payment

42 Percent With insurance where not fully covered for damages

29 Percent of companies had to remove jobs following an attack

2100 Healthcare data breaches since 2009

100 Percent Increase against universities

62 Percent of all records leaked in 2019 were from financial institutions

EVERY 11 SECONDS

RANSOMWARE

Is a type of malware that encrypts data and can only be unlocked with a payment in order to obtain a key to decrypt the data.

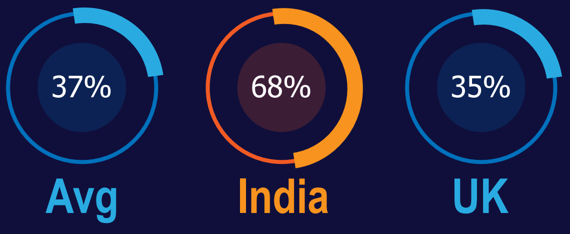
Over the years this process has not changed much but has become extremely sophisticated and now boasts support models and affiliate programs.

As the world moves more and more into an online space, this type of crime will increase as payments are large and deployment can be very simple.

Companies with employees of over 100 are targeted more and these attacks are laser focused.

Organizations hit by ransomware attacks 2021

On average, 37 percent of organizations worldwide were victims of a ransomware attack, according to a survey carried out between January and February 2021. India saw the highest rate, with over two-thirds of organizations saying they experienced a ransomware attack in the last year. In Poland, just 13 percent of responding organizations were victims of such cyber crime.



90000

Android phones were hit by ScarePackage ransomware in just 30 days

8000

mobile banking ransomware Trojan installations were detected in 2018

A real-world ransomware scenario and what would have stopped it

Impact of Ransomware

- Business Disruption
- Brand Reputation
- Financial Costs
- Post Traumatic Stress
- Fines
- Global Crisis

A real-world ransomware scenario and what would have stopped it

Impact of Ransomware

COLONIAL PIPELINE
PELHAM JUNCTION AND TANK FARM
WARNING: NO TRESPASSING
NOTICE
ALL VEHICLES AND PERSONNEL ENTERING OR LEAVING THE PREMISES SUBJECT TO SEARCH
DANGER
NO SMOKING NO FLAMES NO SPARKS
NOTICE
MINIMUM 8 CAL AR/FR PPE BEYOND THIS POINT
NOTICE
SAFETY GLASSES, SAFETY SHOES & HARD HATS ARE REQUIRED BEYOND THIS POINT
SPEED LIMIT 10
WARNING
Recorded VIDEO SURVEILLANCE
Grabación de VIDEO vigilancia
WARNING ABOVE GROUND PIPING
ALL VISITORS OR CONTRACTORS MUST SIGN IN AT BLDG
NOTICE
AUTHORIZED PERSONNEL ONLY
POLICE

Colonial Pipeline

A real-world ransomware scenario and what would have stopped it

Impact of Ransomware

Solarwinds

A real-world ransomware scenario and what would have stopped it

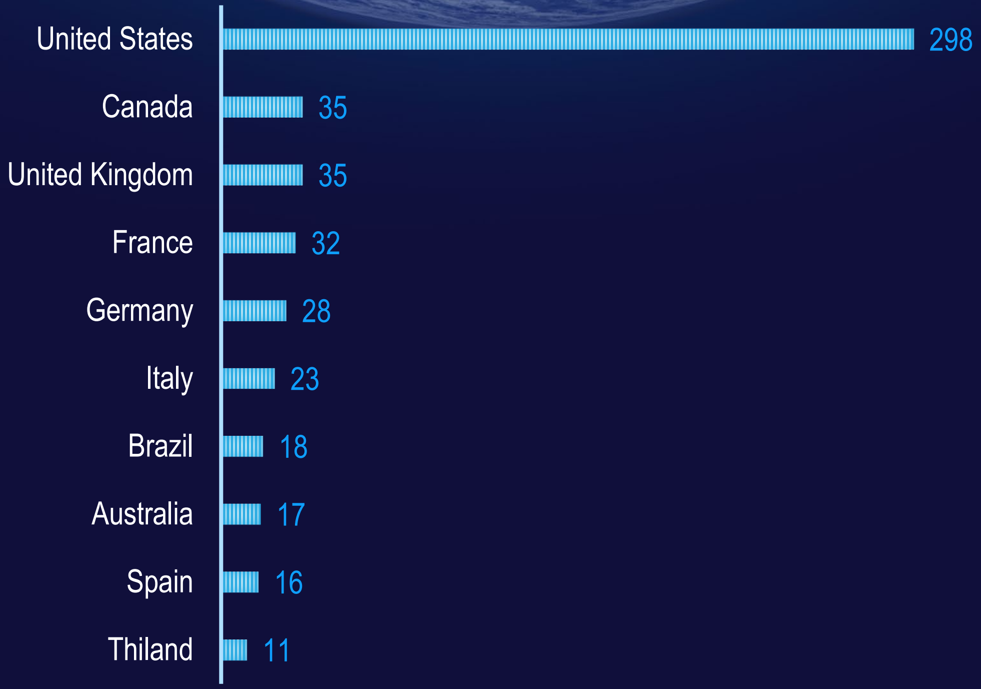
Impact of Ransomware

Pulse Secure

Methods

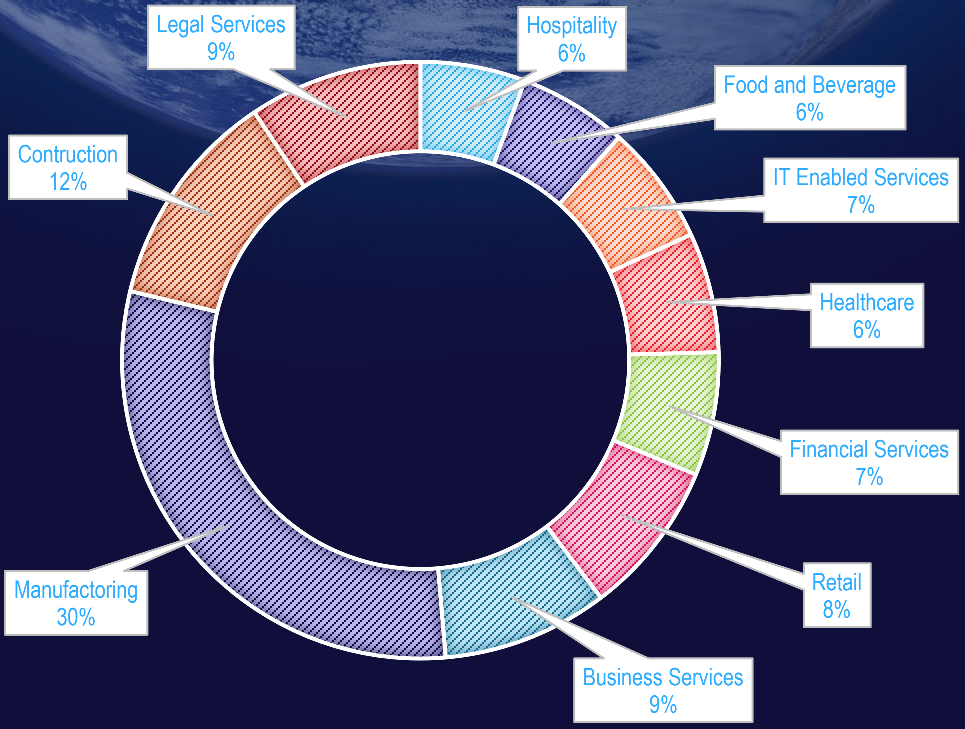
- Phishing
- Malware
- Stolen credentials
- Malicious Update
- Zero-day vulnerability
- Ransomware as a Service

Distribution of Attacks



A real-world ransomware scenario and what would have stopped it

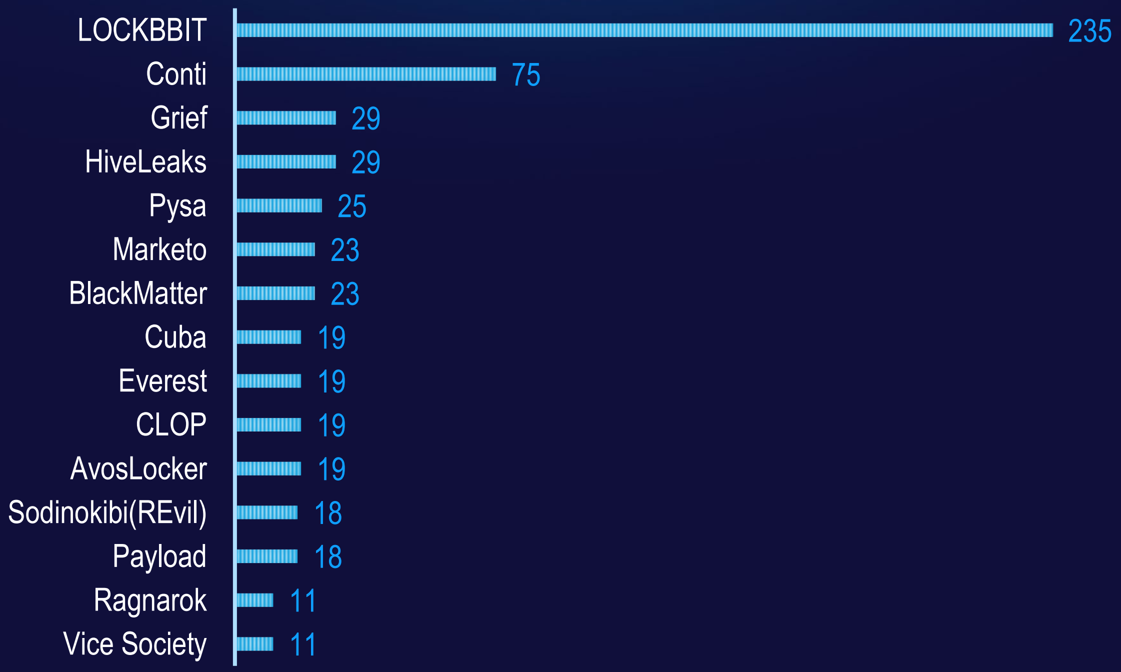
Attacks to Industry



Q3 2021

A real-world ransomware scenario and what would have stopped it

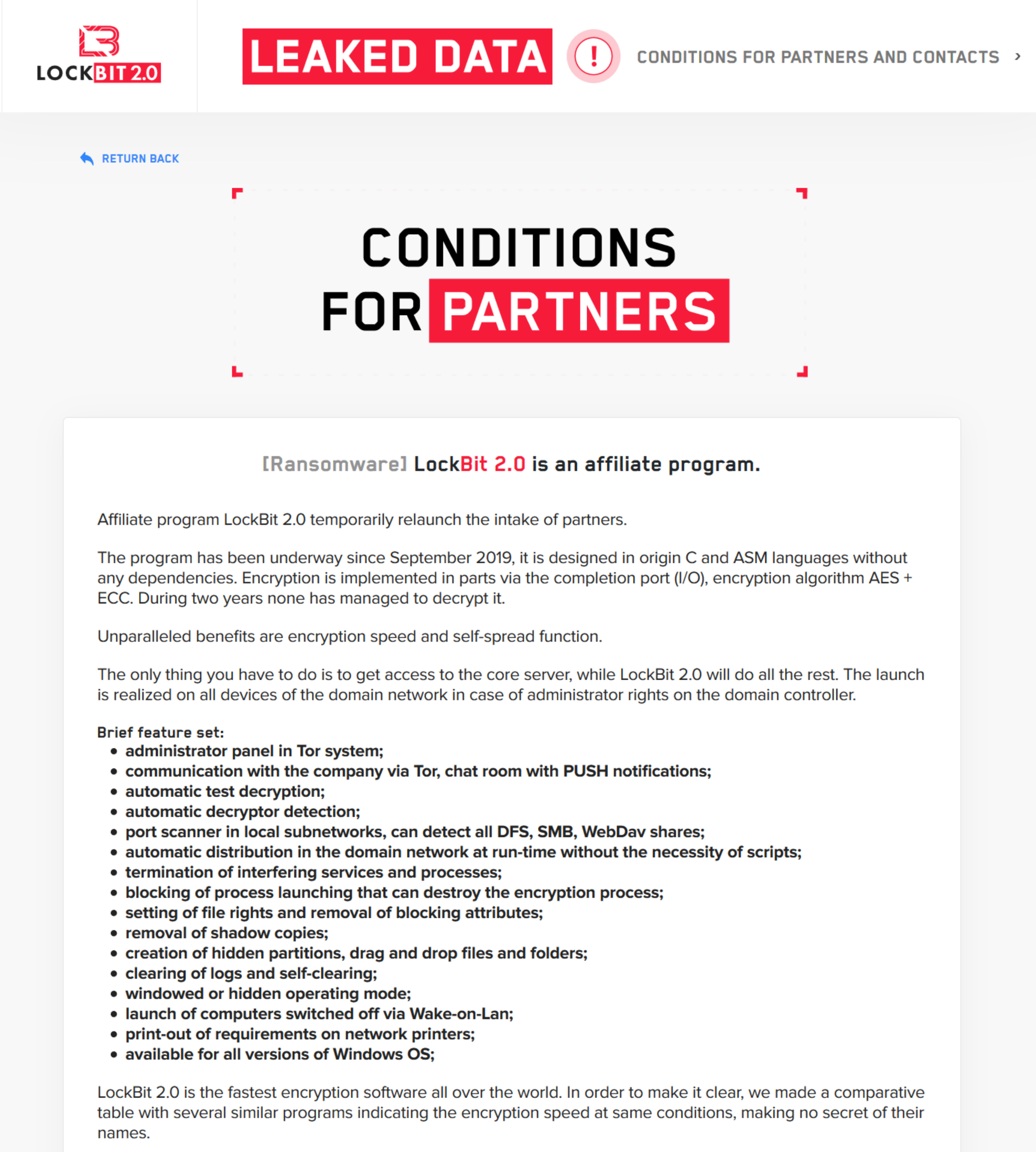
Common Ransomware Payloads



Q3 2021

A real-world ransomware scenario and what would have stopped it

Proof of Concept



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.

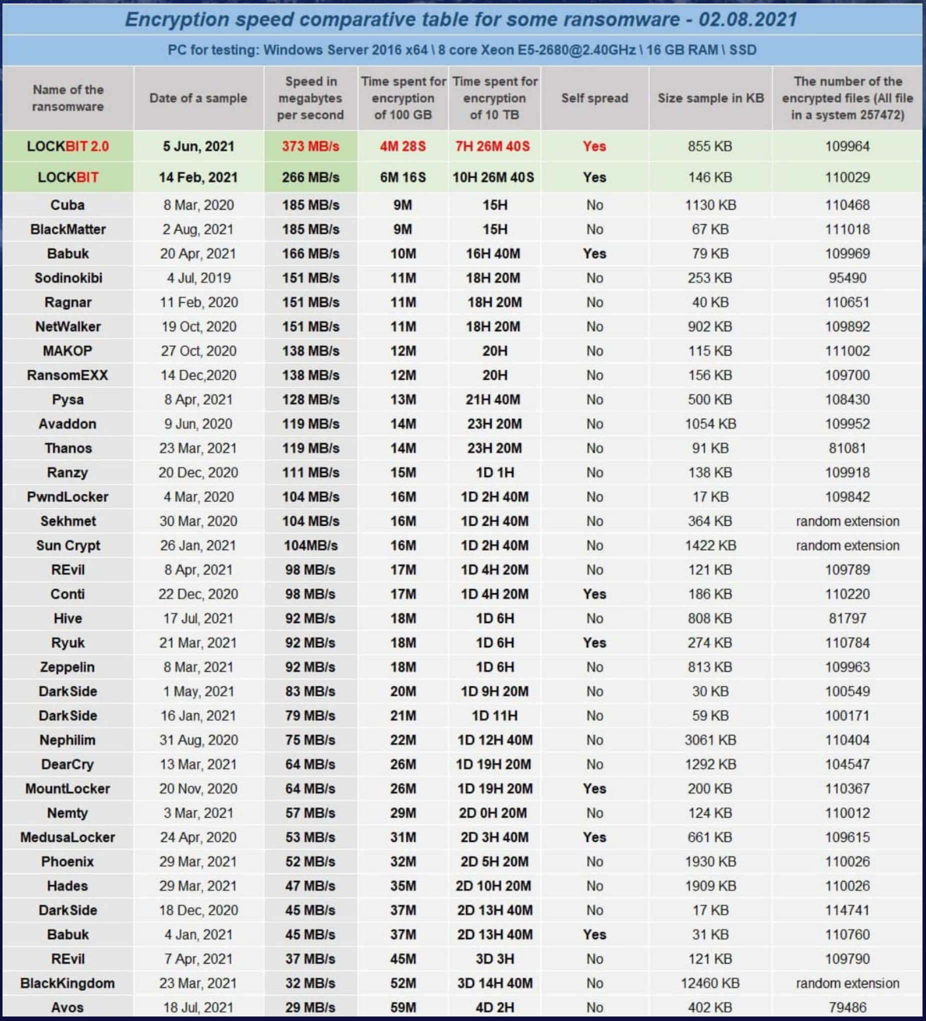
Brief feature set:

- **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.

A real-world ransomware scenario and what would have stopped it

Proof of Concept



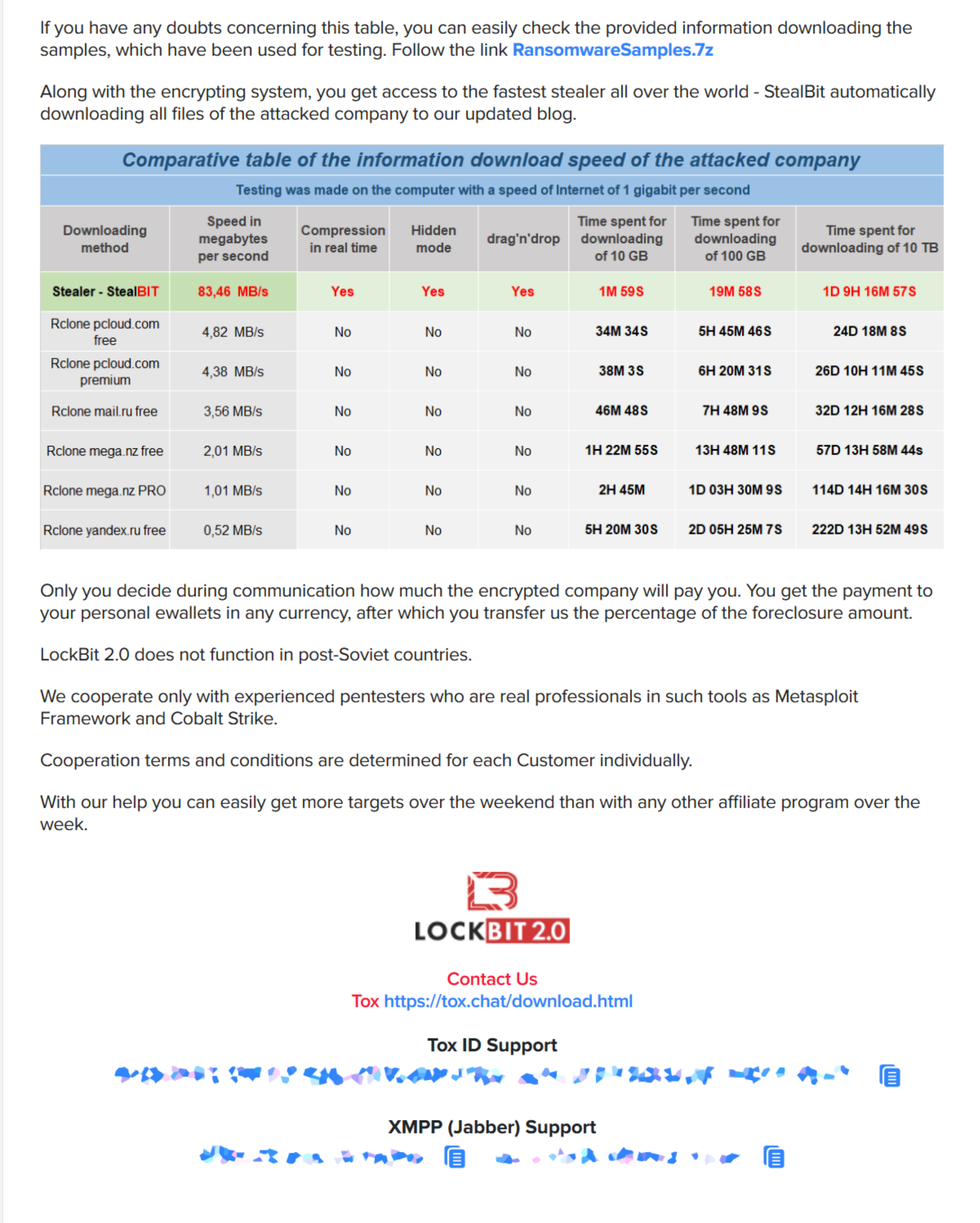
Encryption speed comparative table for some ransomware - 02.08.2021

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 KB	109964
LOCKBIT	14 Feb, 2021	266 MB/s	6M 16S	10H 26M 40S	Yes	146 KB	110029
Cuba	8 Mar, 2020	185 MB/s	9M	15H	No	1130 KB	110468
BlackMatter	2 Aug, 2021	185 MB/s	9M	15H	No	67 KB	111018
Babuk	20 Apr, 2021	166 MB/s	10M	16H 40M	Yes	79 KB	109969
Sodinokibi	4 Jul, 2019	151 MB/s	11M	18H 20M	No	253 KB	95490
Ragnar	11 Feb, 2020	151 MB/s	11M	18H 20M	No	40 KB	110651
NetWalker	19 Oct, 2020	151 MB/s	11M	18H 20M	No	902 KB	109892
MAKOP	27 Oct, 2020	138 MB/s	12M	20H	No	115 KB	111002
RansomEXX	14 Dec,2020	138 MB/s	12M	20H	No	156 KB	109700
Pysa	8 Apr, 2021	128 MB/s	13M	21H 40M	No	500 KB	108430
Avaddon	9 Jun, 2020	119 MB/s	14M	23H 20M	No	1054 KB	109952
Thanos	23 Mar, 2021	119 MB/s	14M	23H 20M	No	91 KB	81081
Ranzy	20 Dec, 2020	111 MB/s	15M	1D 1H	No	138 KB	109918
PwndLocker	4 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	17 KB	109842
Sekhmet	30 Mar, 2020	104 MB/s	16M	1D 2H 40M	No	364 KB	random extension
Sun Crypt	26 Jan, 2021	104MB/s	16M	1D 2H 40M	No	1422 KB	random extension
REvil	8 Apr, 2021	98 MB/s	17M	1D 4H 20M	No	121 KB	109789
Conti	22 Dec, 2020	98 MB/s	17M	1D 4H 20M	Yes	186 KB	110220
Hive	17 Jul, 2021	92 MB/s	18M	1D 6H	No	808 KB	81797
Ryuk	21 Mar, 2021	92 MB/s	18M	1D 6H	Yes	274 KB	110784
Zeppelin	8 Mar, 2021	92 MB/s	18M	1D 6H	No	813 KB	109963
DarkSide	1 May, 2021	83 MB/s	20M	1D 9H 20M	No	30 KB	100549
DarkSide	16 Jan, 2021	79 MB/s	21M	1D 11H	No	59 KB	100171
Nephilim	31 Aug, 2020	75 MB/s	22M	1D 12H 40M	No	3061 KB	110404
DearCry	13 Mar, 2021	64 MB/s	26M	1D 19H 20M	No	1292 KB	104547
MountLocker	20 Nov, 2020	64 MB/s	26M	1D 19H 20M	Yes	200 KB	110367
Nemty	3 Mar, 2021	57 MB/s	29M	2D 0H 20M	No	124 KB	110012
MedusaLocker	24 Apr, 2020	53 MB/s	31M	2D 3H 40M	Yes	661 KB	109615
Phoenix	29 Mar, 2021	52 MB/s	32M	2D 5H 20M	No	1930 KB	110026
Hades	29 Mar, 2021	47 MB/s	35M	2D 10H 20M	No	1909 KB	110026
DarkSide	18 Dec, 2020	45 MB/s	37M	2D 13H 40M	No	17 KB	114741
Babuk	4 Jan, 2021	45 MB/s	37M	2D 13H 40M	Yes	31 KB	110760
REvil	7 Apr, 2021	37 MB/s	45M	3D 3H	No	121 KB	109790
BlackKingdom	23 Mar, 2021	32 MB/s	52M	3D 14H 40M	No	12460 KB	random extension
Avos	18 Jul, 2021	29 MB/s	59M	4D 2H	No	402 KB	79486

A real-world ransomware scenario and what would have stopped it

Proof of Concept



If you have any doubts concerning this table, you can easily check the provided information downloading the samples, which have been used for testing. Follow the link RansomwareSamples.7z

Along with the encrypting system, you get access to the fastest stealer all over the world - StealBit automatically downloading all files of the attacked company to our updated blog.

Comparative table of the information download speed of the attacked company

Testing was made on the computer with a speed of Internet of 1 gigabit per second

Downloading method	Speed in megabytes per second	Compression in real time	Hidden mode	drag'n'drop	Time spent for downloading of 10 GB	Time spent for downloading of 100 GB	Time spent for downloading of 10 TB
Stealer - StealBIT	83,46 MB/s	Yes	Yes	Yes	1M 59S	19M 58S	1D 9H 16M 57S
Rclone pcloud.com free	4,82 MB/s	No	No	No	34M 34S	5H 45M 46S	24D 18M 8S
Rclone pcloud.com premium	4,38 MB/s	No	No	No	38M 3S	6H 20M 31S	26D 10H 11M 45S
Rclone mail.ru free	3,56 MB/s	No	No	No	46M 48S	7H 48M 9S	32D 12H 16M 28S
Rclone mega.nz free	2,01 MB/s	No	No	No	1H 22M 55S	13H 48M 11S	57D 13H 58M 44s
Rclone mega.nz PRO	1,01 MB/s	No	No	No	2H 45M	1D 03H 30M 9S	114D 14H 16M 30S
Rclone yandex.ru free	0,52 MB/s	No	No	No	5H 20M 30S	2D 05H 25M 7S	222D 13H 52M 49S

Only you decide during communication how much the encrypted company will pay you. You get the payment to your personal ewallets in any currency, after which you transfer us the percentage of the foreclosure amount.

LockBit 2.0 does not function in post-Soviet countries.

We cooperate only with experienced pentesters who are real professionals in such tools as Metasploit Framework and Cobalt Strike.

Cooperation terms and conditions are determined for each Customer individually.

With our help you can easily get more targets over the weekend than with any other affiliate program over the week.

LOCKBIT 2.0

Contact Us
Tox https://tox.chat/download.html

Tox ID Support

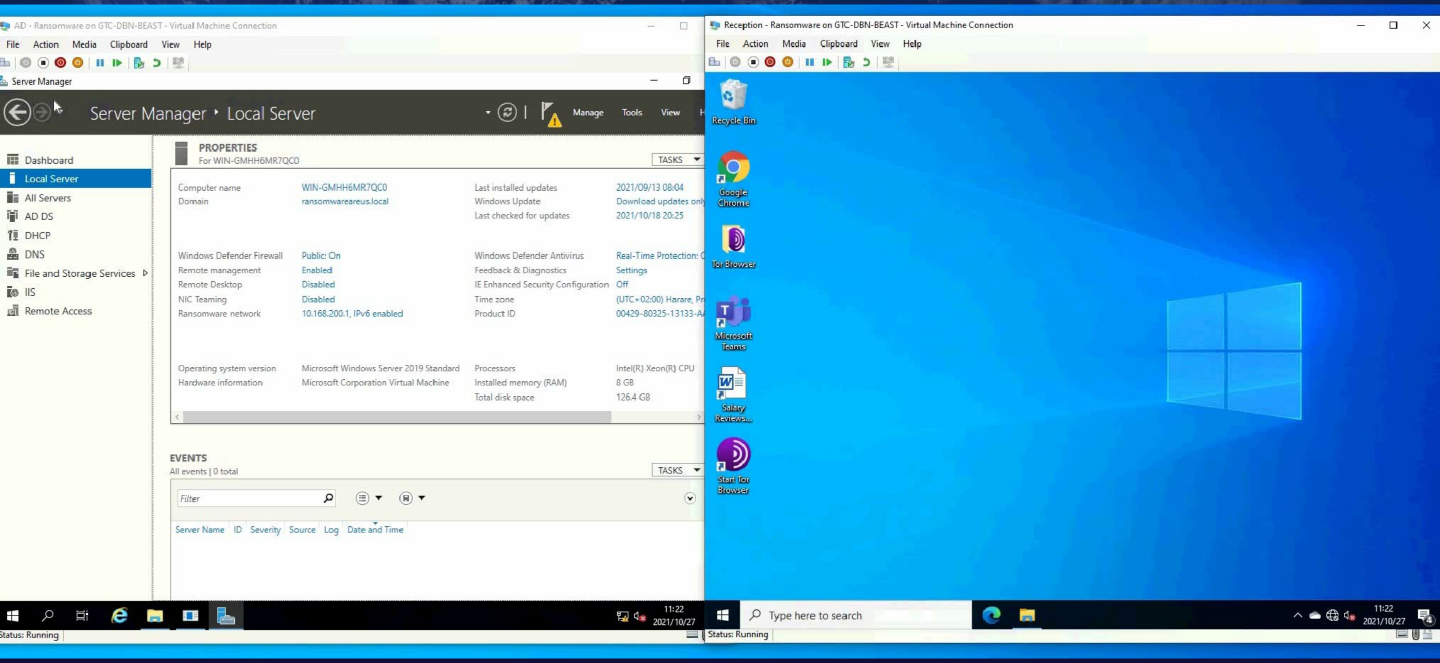
[redacted]

XMPP (Jabber) Support

[redacted] [redacted]

A real-world ransomware scenario and what would have stopped it

Proof of Concept


AD - Ransomware on GTC-DBN-BEAST - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
Server Manager ‣ Local Server
Manage Tools View
Dashboard
Local Server
All Servers
AD DS
DHCP
DNS
File and Storage Services
IIS
Remote Access
TASKS
EVENTS
All events | 0 total
TASKS
Filter
Server Name ID Severity Source Log Date and Time
11:22
2021/10/27
Status: Running
Reception - Ransomware on GTC-DBN-BEAST - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Google Chrome
Tor Browser
Microsoft Teams
Salary Reviews...
Start Tor Browser
Type here to search
11:22
2021/10/27
Status: Running

PROPERTIES
For WIN-GMHH6MR7QC0

Computer name: WIN-GMHH6MR7QC0
Domain: ransomwareareus.local
Last installed updates: 2021/09/13 08:04
Windows Update: Download updates only
Last checked for updates: 2021/10/18 20:25

Windows Defender Firewall: Public: On
Remote management: Enabled
Remote Desktop: Disabled
NIC Teaming: Disabled
Ransomware network: 10.168.200.1, IPv6 enabled
Windows Defender Antivirus: Real-Time Protection: O
Feedback & Diagnostics: Settings
IE Enhanced Security Configuration: Off
Time zone: (UTC+02:00) Harare, Pr
Product ID: 00429-80325-13133-AA

Operating system version: Microsoft Windows Server 2019 Standard
Hardware information: Microsoft Corporation Virtual Machine
Processors: Intel(R) Xeon(R) CPU
Installed memory (RAM): 8 GB
Total disk space: 126.4 GB

Ransomware through
CVE-2021-40444

Fixes

- User training
- Strong passwords with MFA
- Password Managers
- Regular backup and recover practised procedures
- Cloud-based storage with history
- Vulnerability Assessments
- Anti-virus and End Point Protection
- Email Protection
- Regular tested software updates
- Enable smart rules for logins and suspect activity
- Implement a Zero Trust Security Model

References

- https://www.vox.com/recode/22428774/ransomeware-pipeline-colonial-darkside-gas-prices
- https://www.varonis.com/blog/ransomware-statistics-2021/
- 7 real and famous cases of ransomware attacks - Gatefy
- Ransomware Attacks and Types | How do Locky, Petya and other ransomware differ? | Kaspersky
- 7 Examples of Ransomware Attacks - Updated 2021 - Tessian
- 10 Examples of Recent and Impactful Ransomware Attacks (securityscorecard.com)
- https://blog.cyble.com/2021/08/04/a-deep-dive-analysis-of-venomous-ransomware/
- https://blog.cyble.com/2021/08/24/a-deep-dive-analysis-of-karma-ransomware/
- https://www.varonis.com/blog/ransomware-statistics-2021/
- LockBit 2.0 Ransomware Becomes LockFile Ransomware with a Never-Before-Seen Encryption Method (deepinstinct.com)
- https://www.statista.com/statistics/1246438/ransomware-attacks-by-country/
- https://github.com/klezVirus/CVE-2021-40444