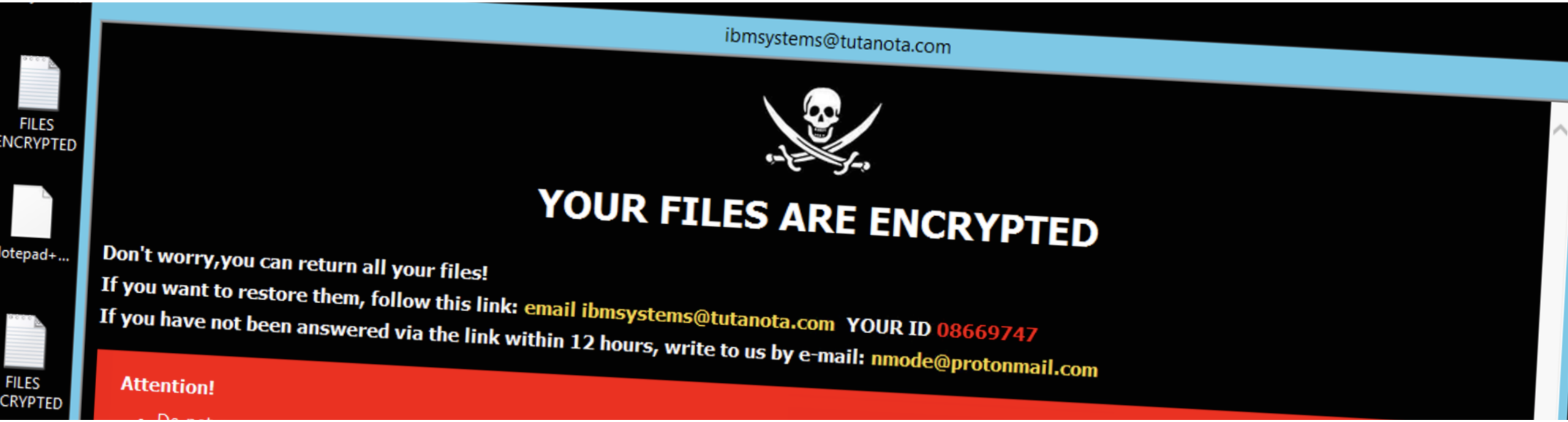
berndorf

BEE ITSECURITY



WAS WIR VON UNSEREM RDP HONEYPOT GELERNT HABEN …

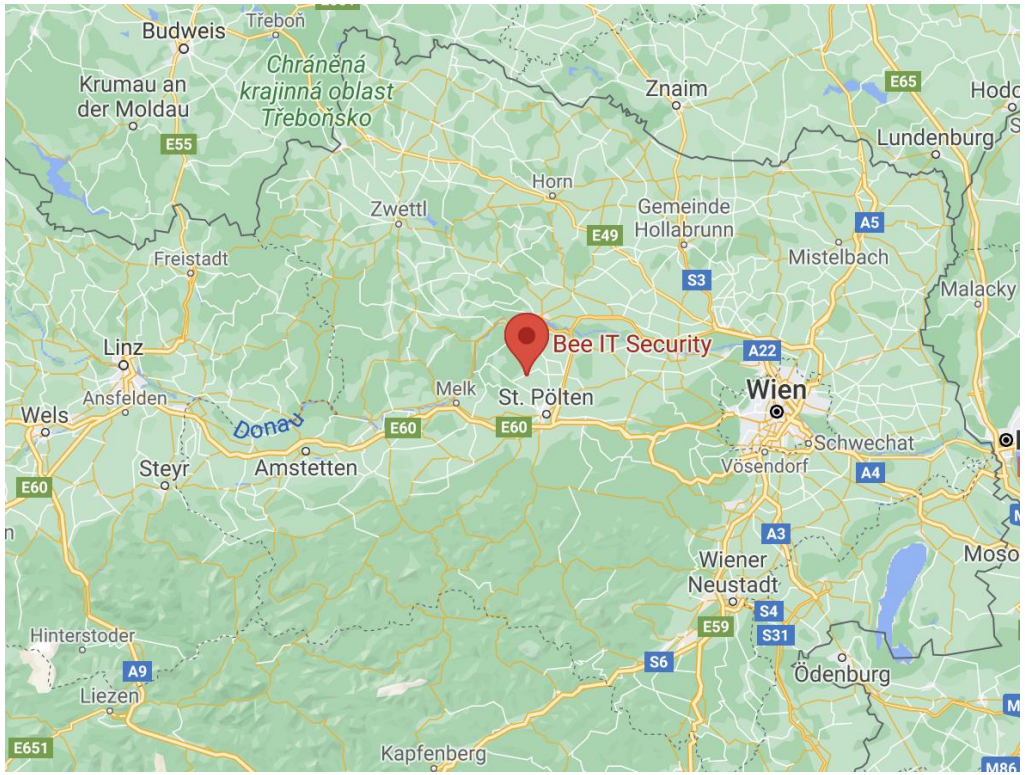
… und warum auch ich Bitcoin Besitzer werden hätte können.

#whoami

Florian Bogner

CEO der Bee IT Security
aka “Professioneller Hacker”
Speaker und Trainer
Lektor für IT / IT Security

> *Wir machen IT Security **verständlich**, so dass Sie die **richtigen Entscheidungen** treffen können!*



PS: WE ARE HIRHING!

BEE ITSECURITY

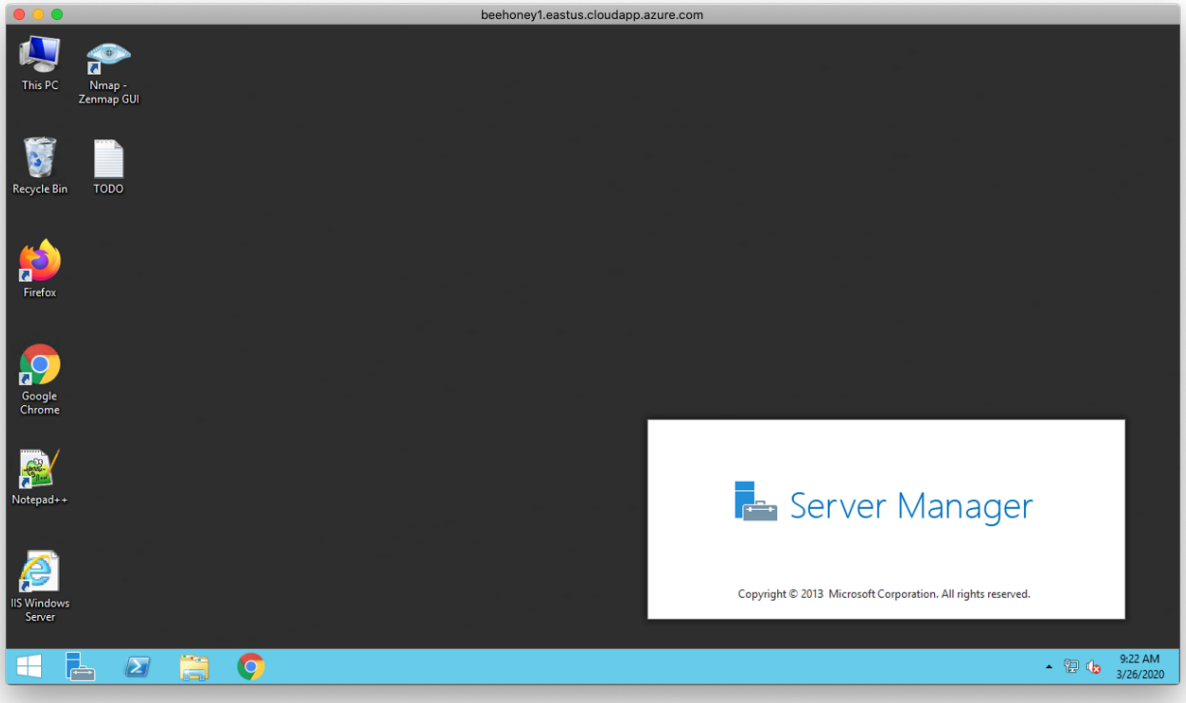
Wir wollen einen Honeypot betreiben…

Als Honigtopf, Honigtöpfchen oder auch englisch ***honeypot*** *wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind* ***vom eigentlichen Ziel ablenken*** *soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte — z. B. in Form eines* ***Scheinzieles****.*

https://de.wikipedia.org/wiki/Honeypot

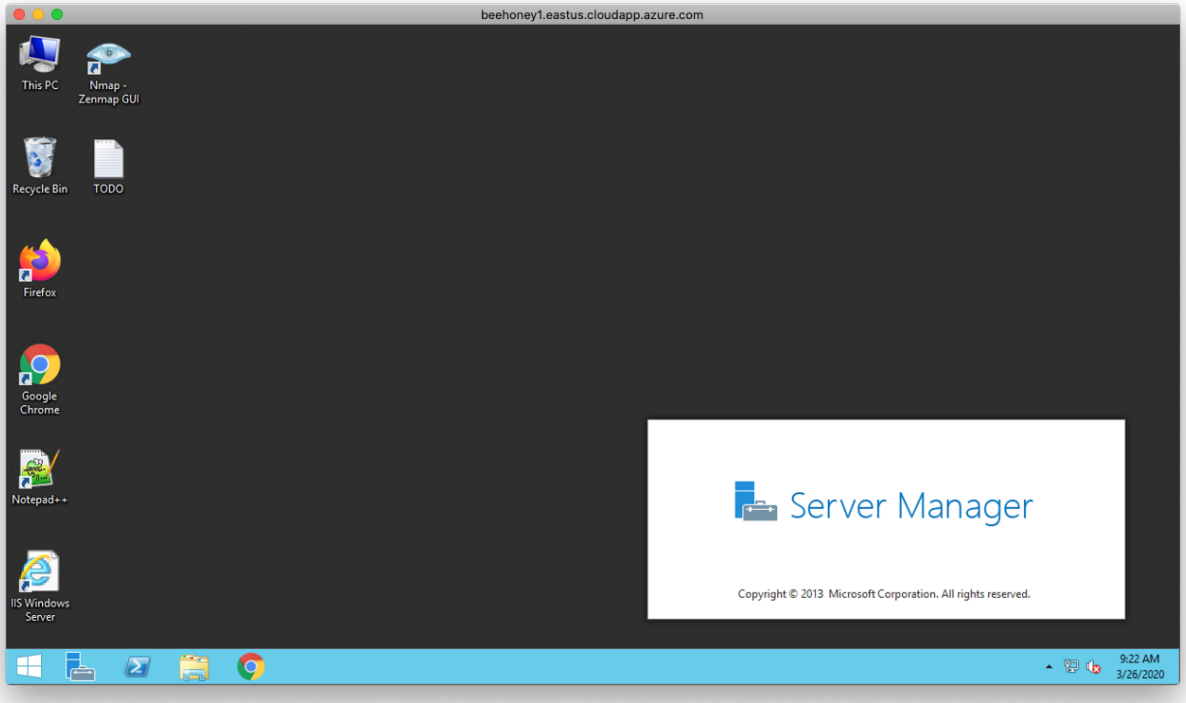
Unser Honigtopf: “MXB System”

sysmon



Unser Honigtopf: “MXB System”

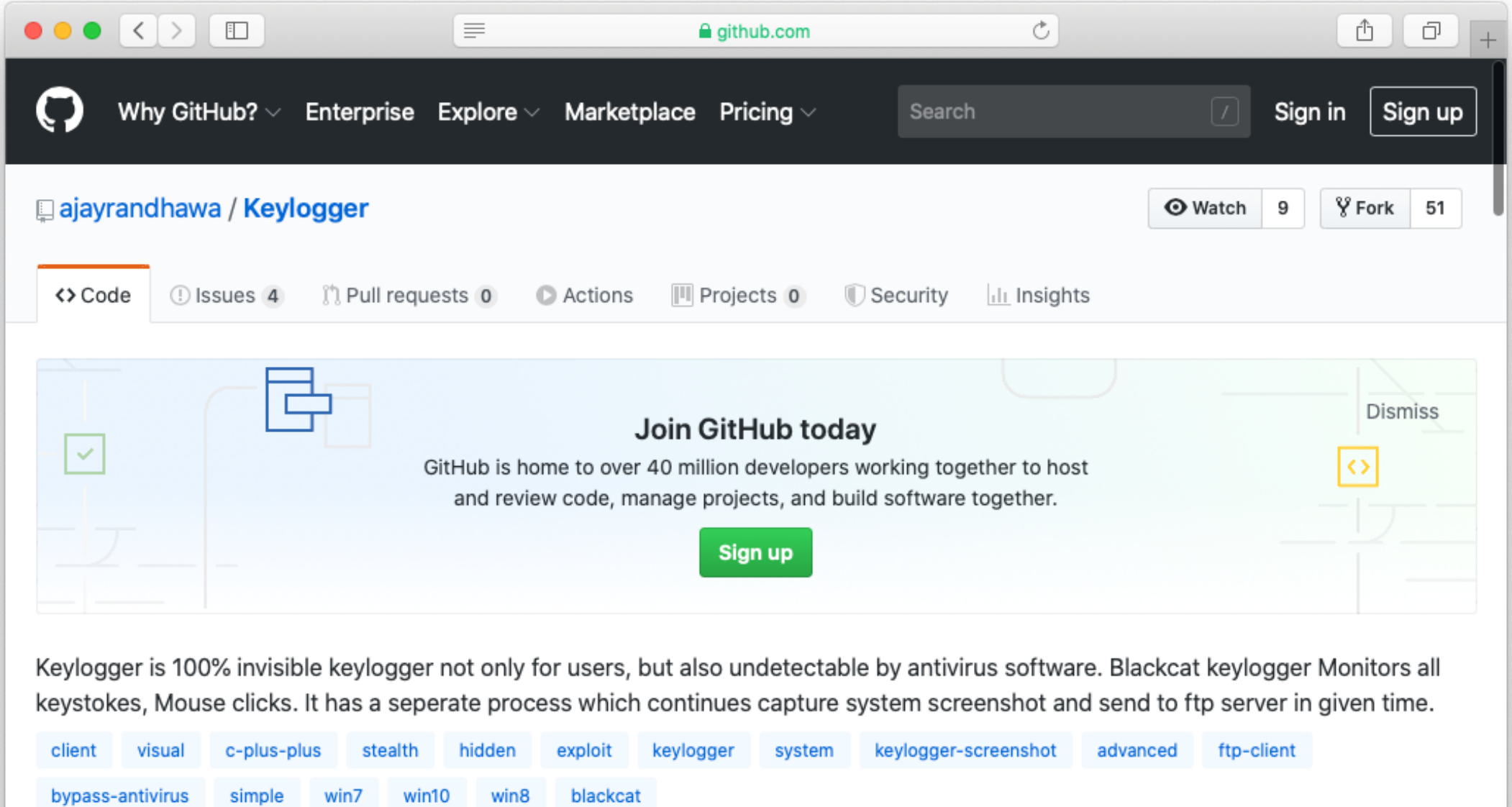
sysmon



Blackcat Keylogger

BEE ITSECURITY

Key Logger

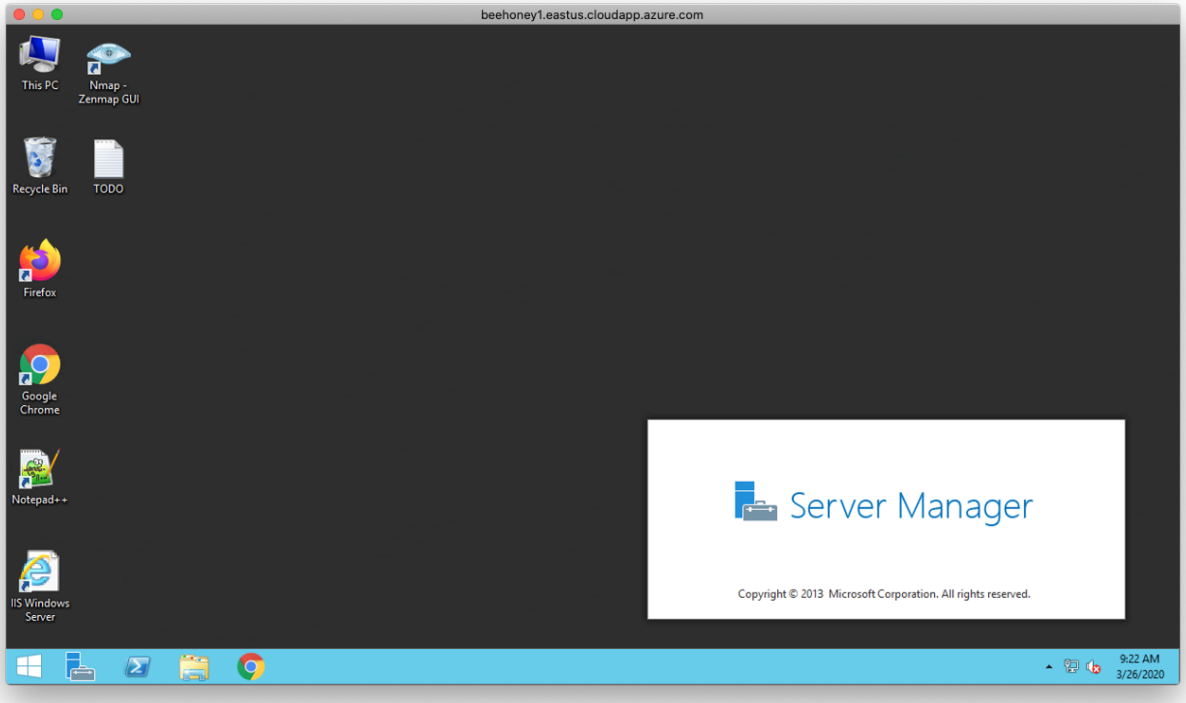


BEE ITSECURITY

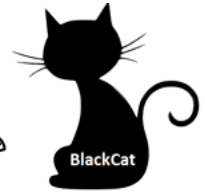
Unser Honigtopf: “MXB System”

sysmon

PS Logging



Blackcat Keylogger

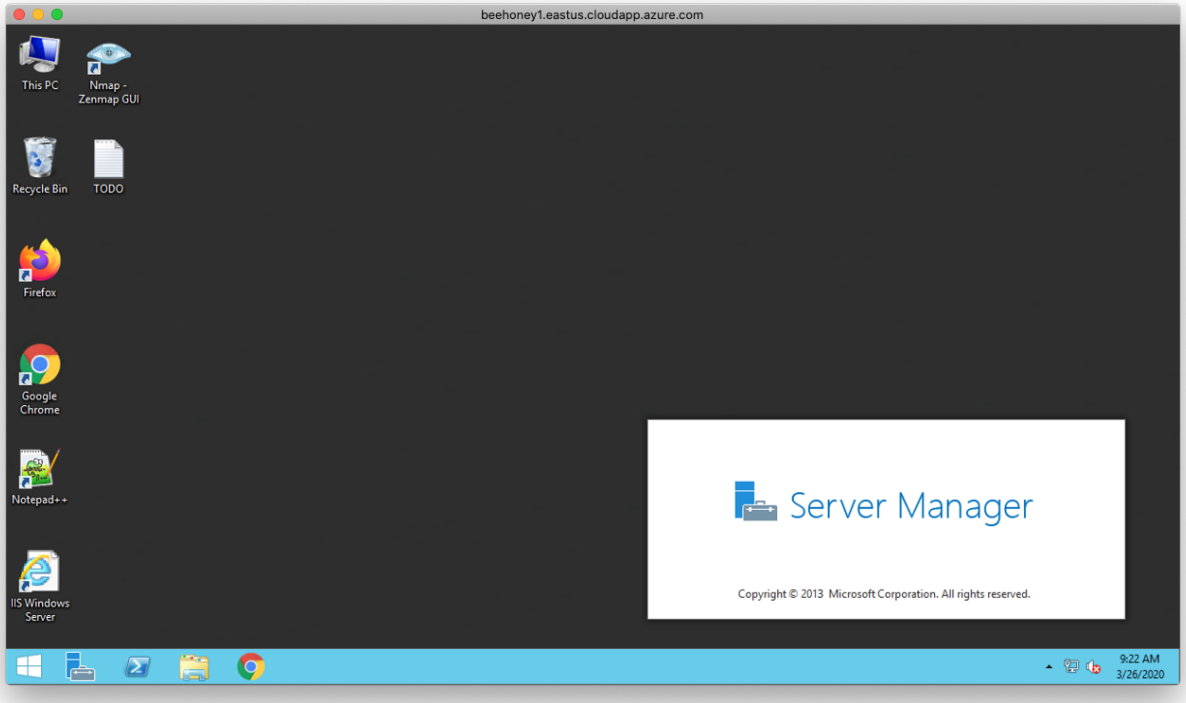


BEE ITSECURITY

Unser Honigtopf: “MXB System”

sysmon

PS Logging



Blackcat Keylogger

Teams Notifications

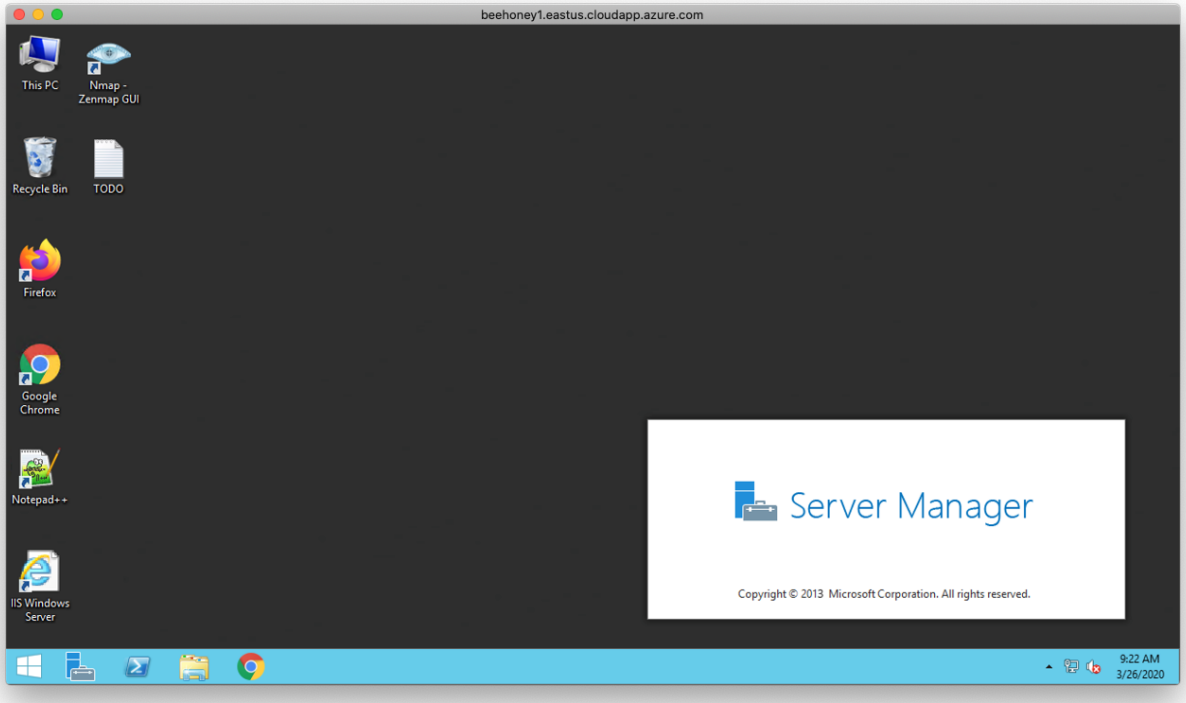
BEE ITSECURITY

Unser Honigtopf: “MXB System”

sysmon

PS Logging

Fake Content

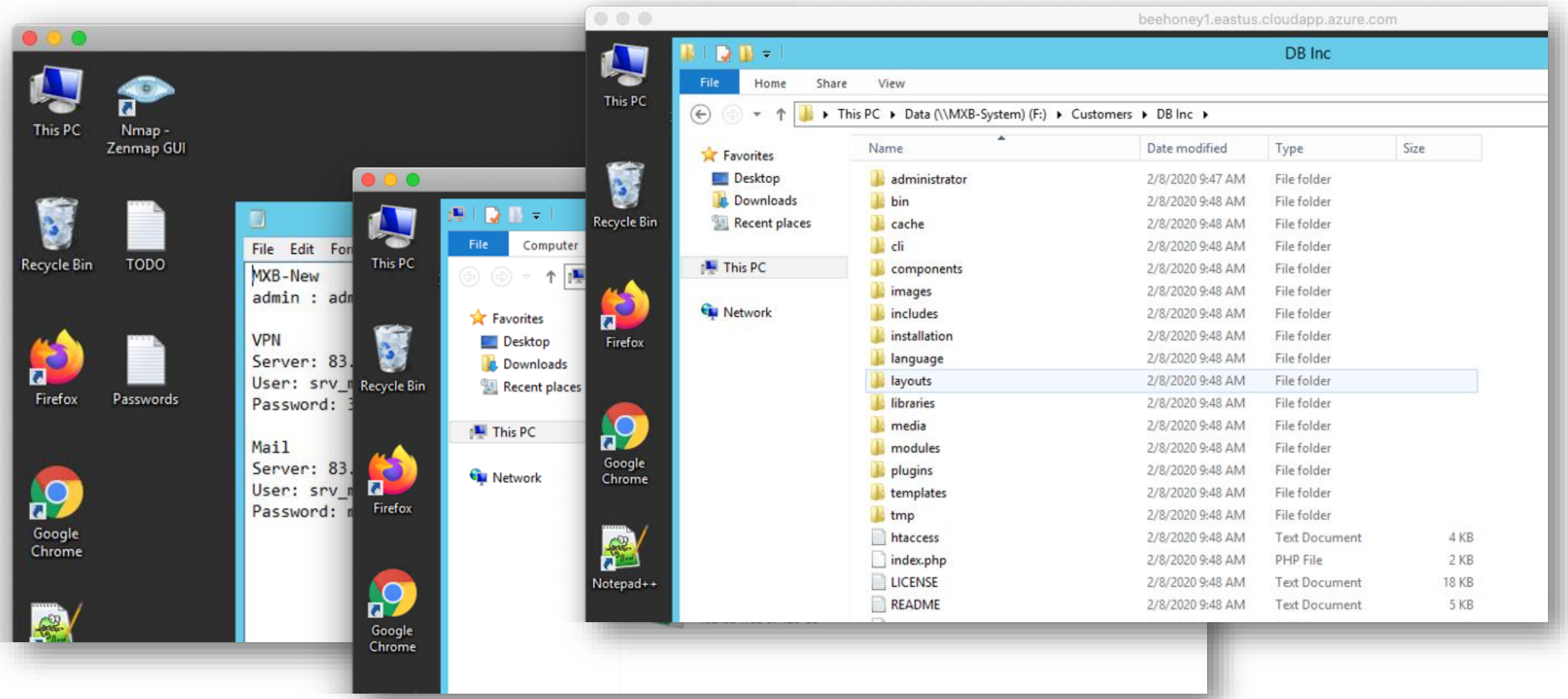


Blackcat Keylogger

Teams Notifications

BEE ITSECURITY

Fake Content



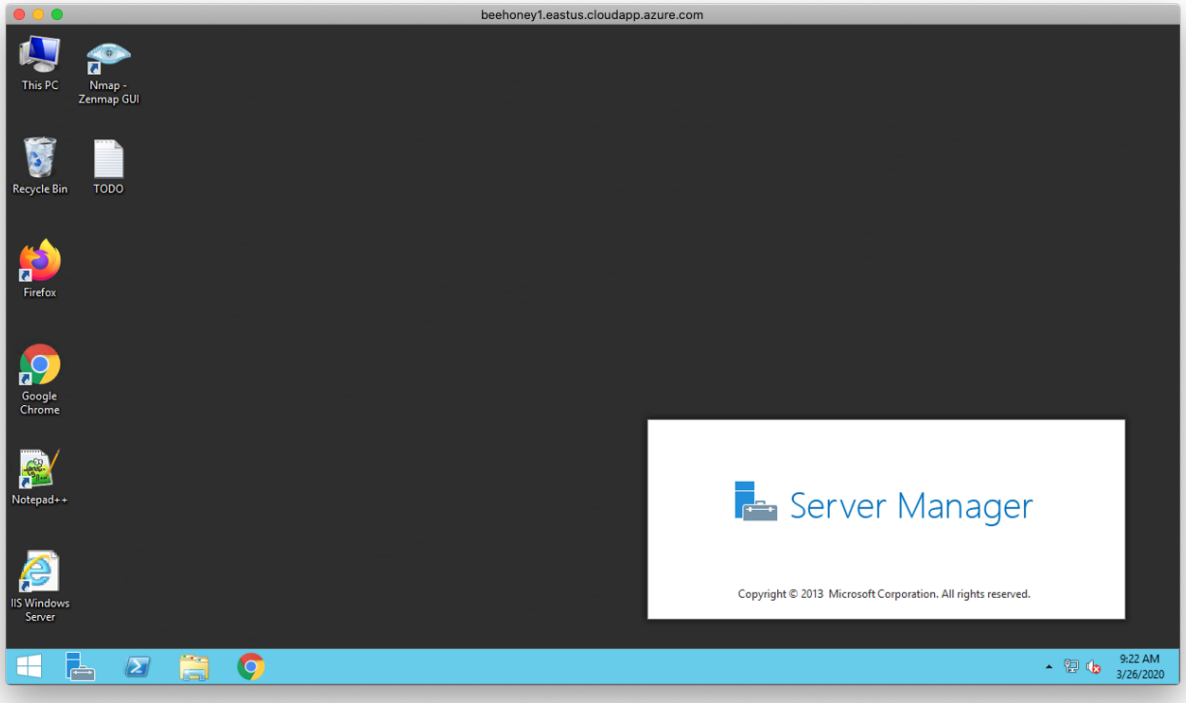
BEE ITSECURITY

Unser Honigtopf: “MXB System”

sysmon

PS Logging

Fake Content



Blackcat Keylogger

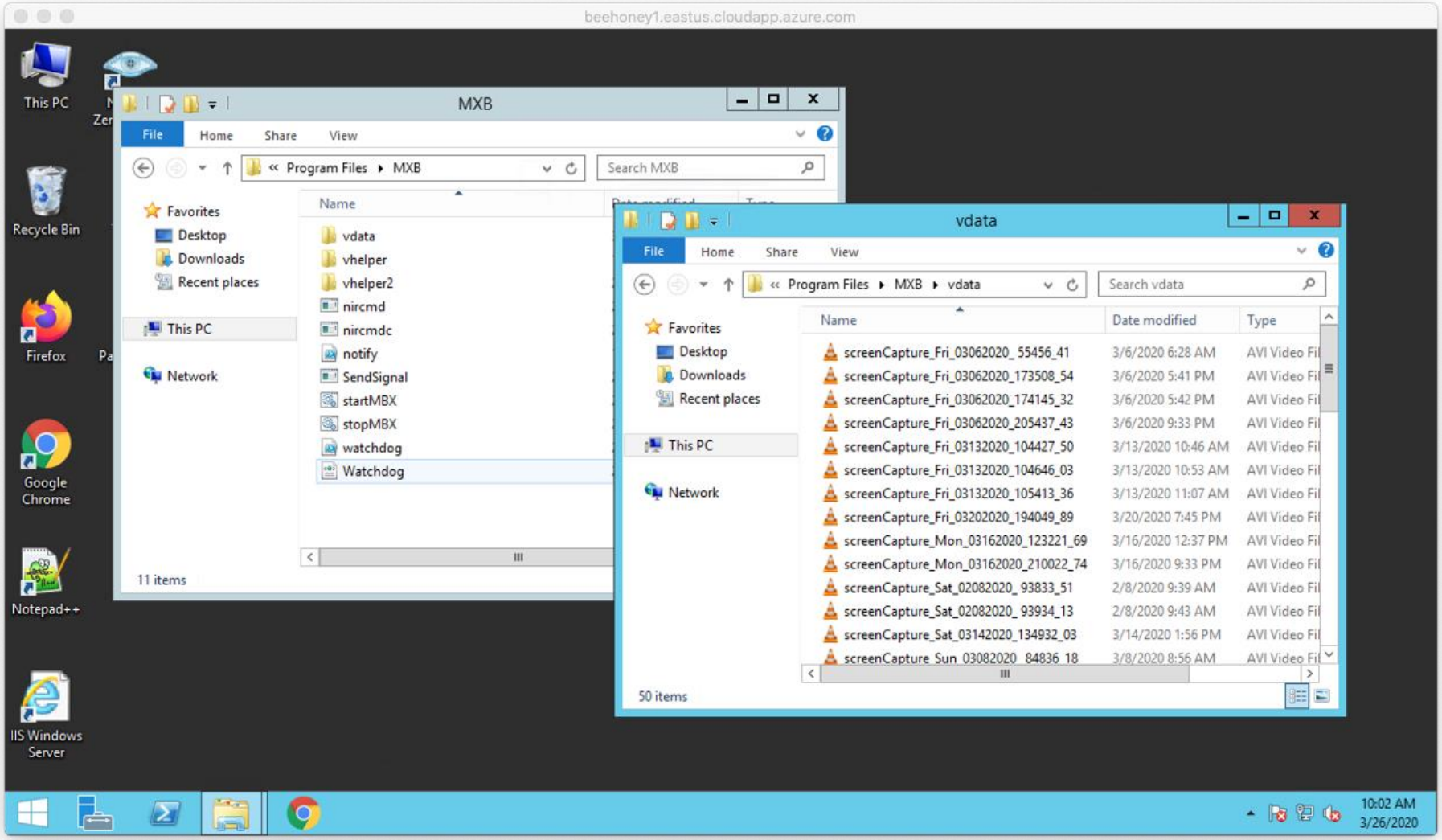
Teams Notifications

FFmpeg

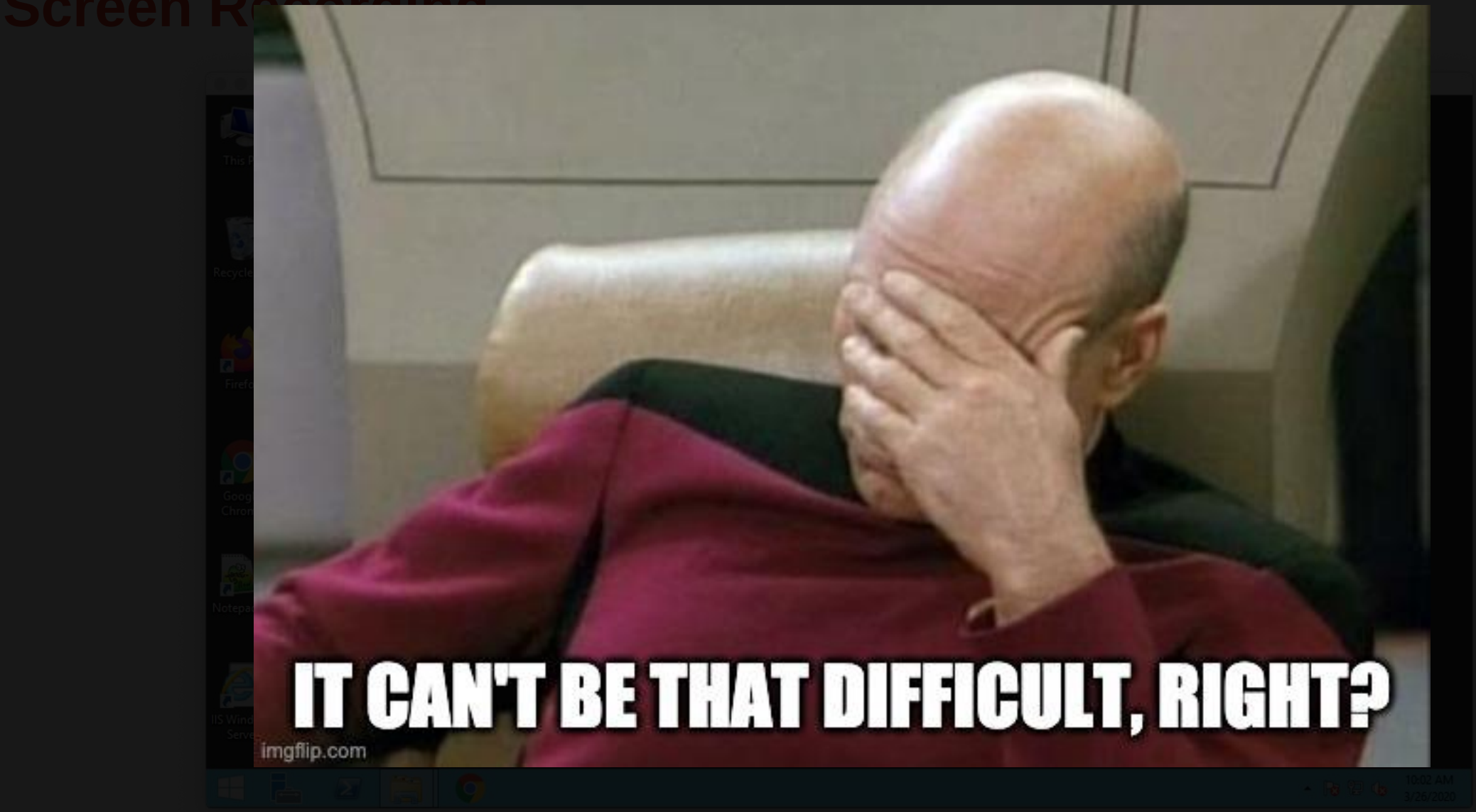
Screen Recording

BEE ITSECURITY

Screen Recording



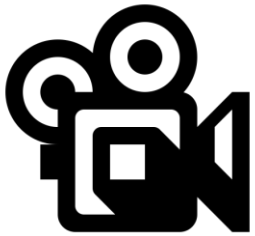
Screen Recording



Screen Recording

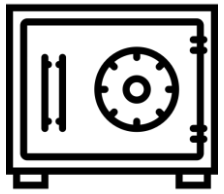
Problem #1: Login != Login

Ein RDP Login ist kein “lokaler Login“. Ein RDP Reconnect ist überhaupt etwas GGGAAAANNNZZZ anderes…



Problem #2: Kaputte Videofiles…

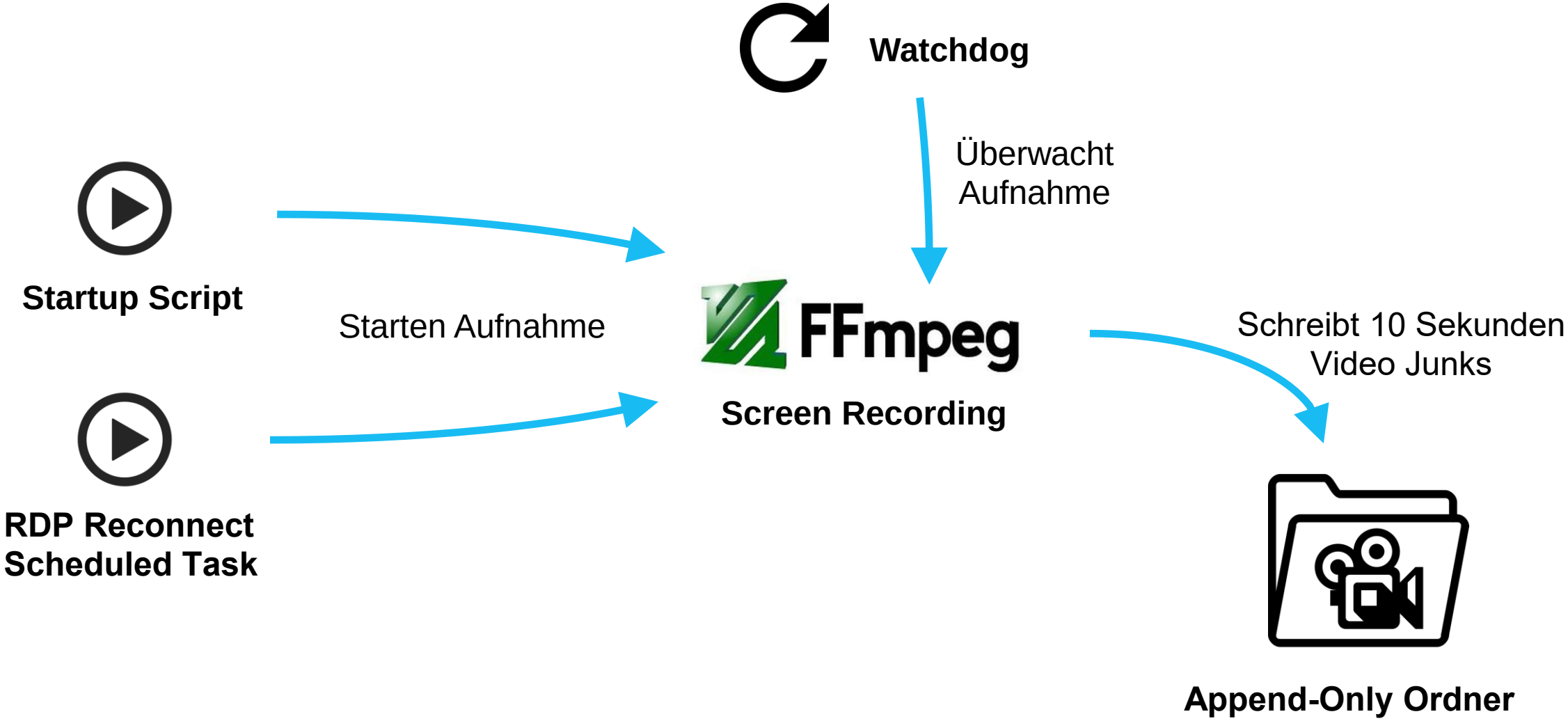
Manchmal wird der Aufnahmeprozess nicht richtig beendet. Dies führt dazu, dass die Videodateien nicht mehr abgespielt werden können.



Problem #3: Cryptolocker zerstört unsere Videos

Wir wollen wissen wie die Kriminellen arbeiten -> Leider verschlüsselt der Cryptolocker aber dann auch unsere Videodateien.

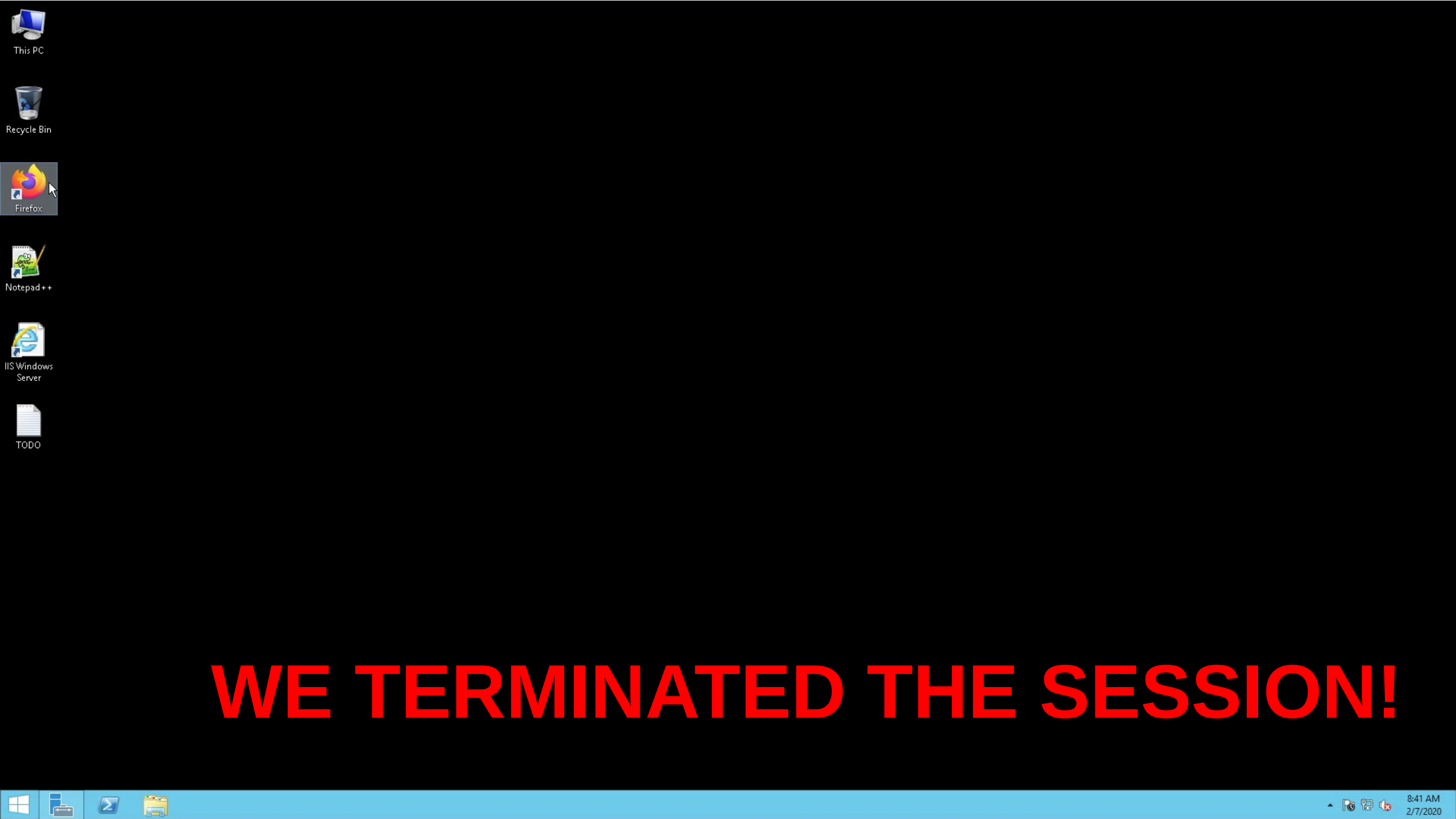
BeeHoney Screen Recording



BEE ITSECURITY

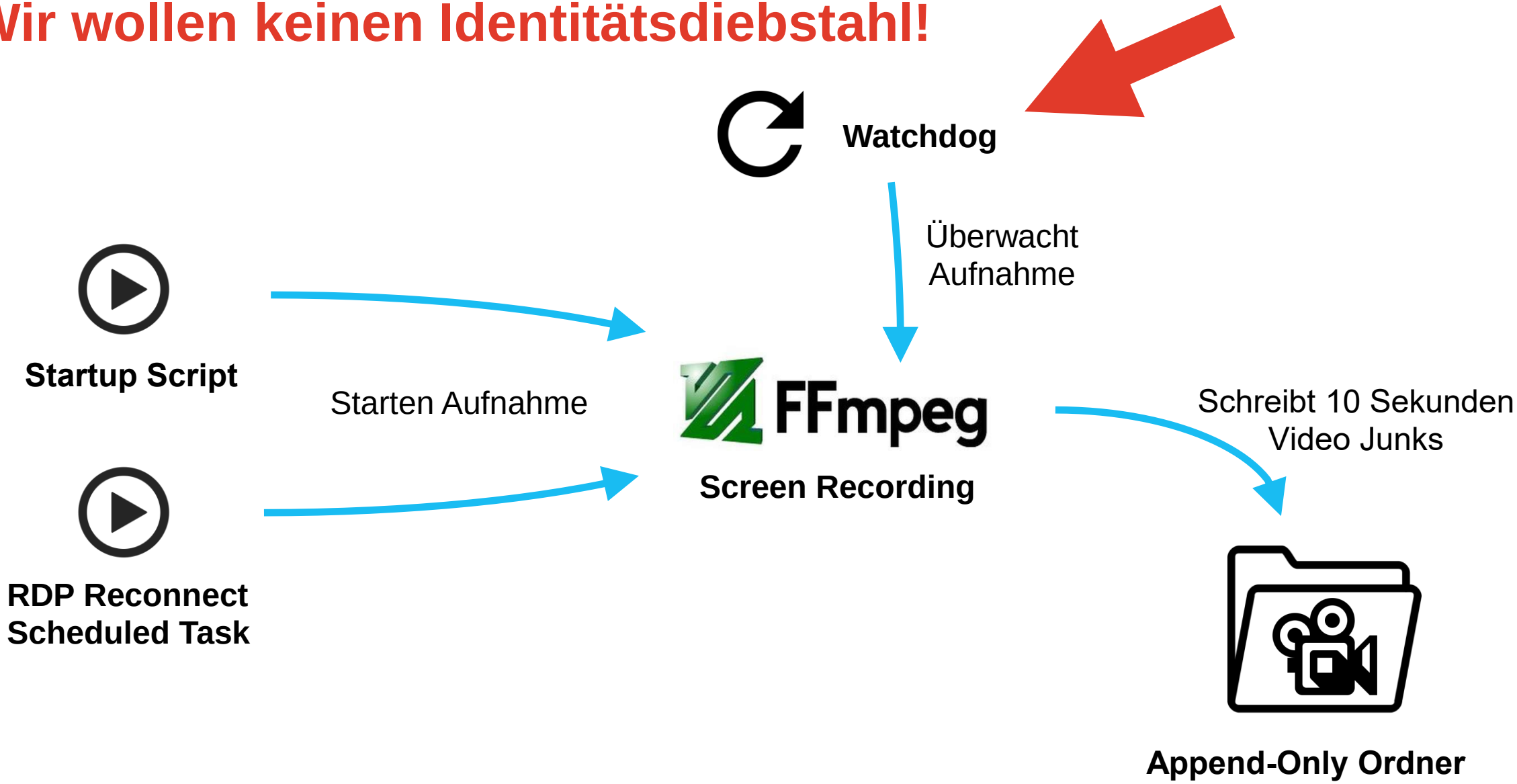
Erster Akt:
Credential Abuse

★ ★ ★ ★ ★


This PC
Recycle Bin
Firefox
Notepad++
IIS Windows Server
TODO
WE TERMINATED THE SESSION!
8:41 AM
2/7/2020

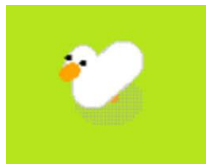
BEE ITSECURITY

Wir wollen keinen Identitätsdiebstahl!

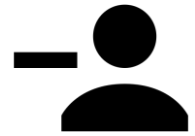


BEE ITSECURITY

Wir wollen keinen Identitätsdiebstahl!



Watchdog



Überwacht
Aufnahme

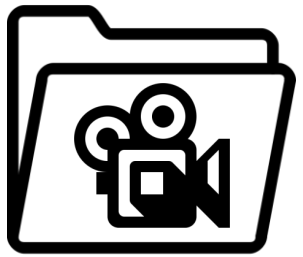
Startup Script

RDP Reconnect
Scheduled Task

Starten Aufnahme

Screen Recording

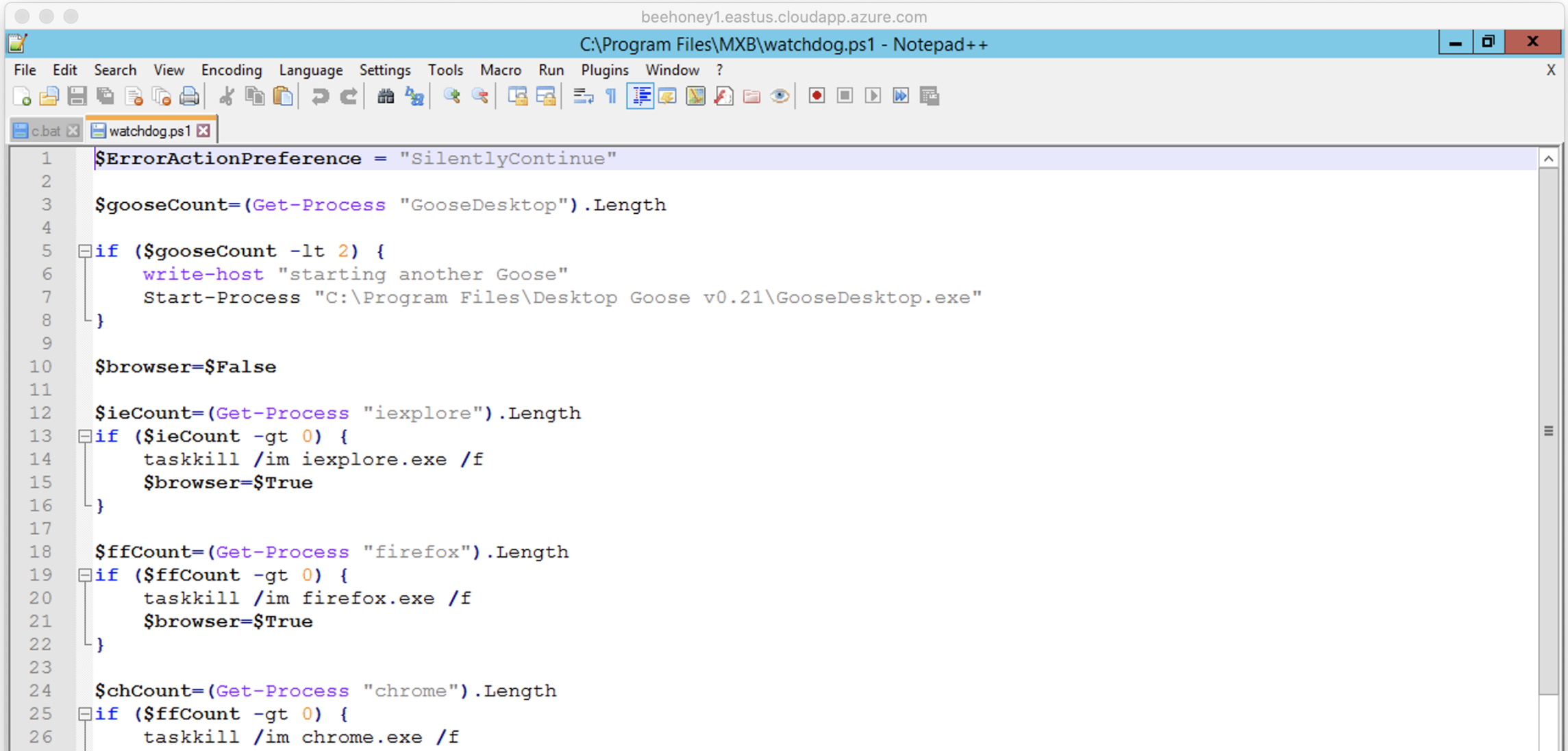
Schreibt 10 Sekunden
Video Junks



Append-Only Ordner

BEE ITSECURITY

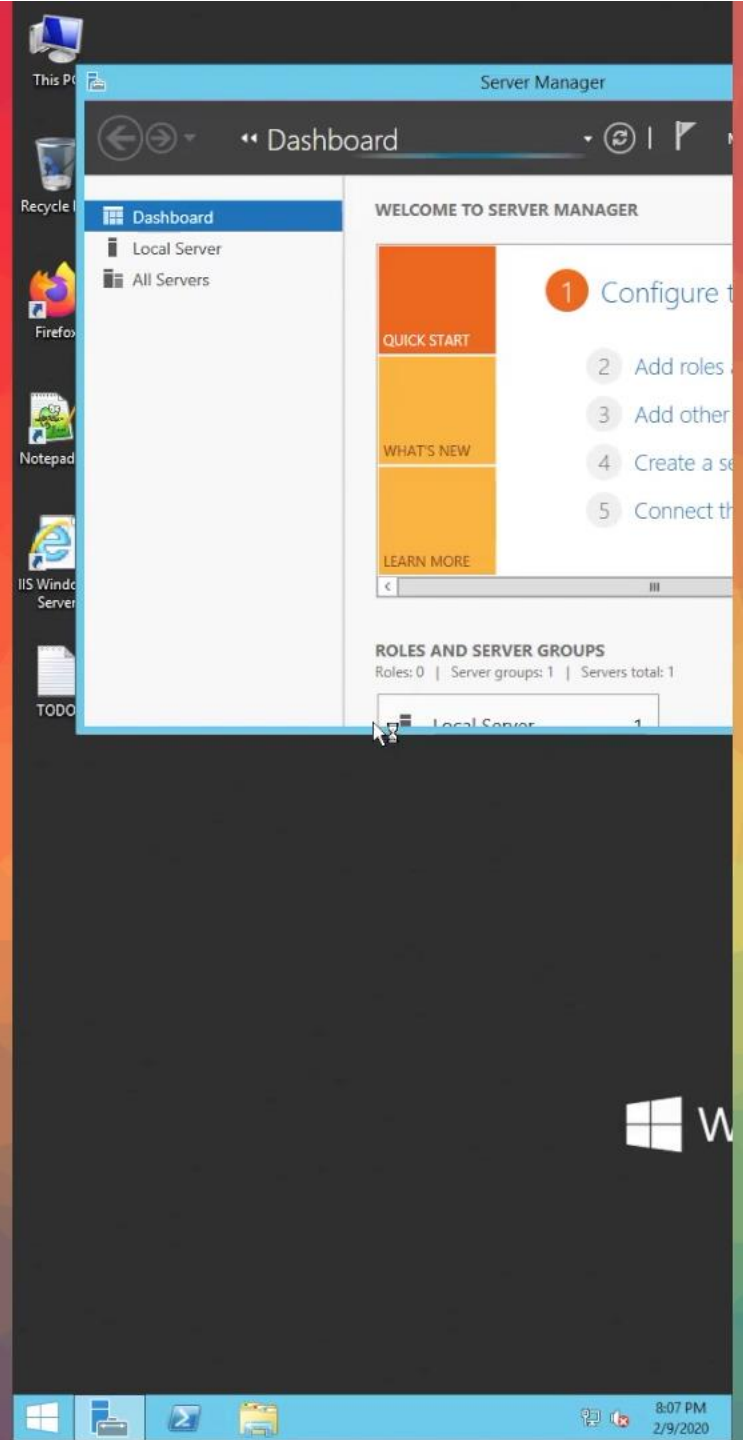
Watchdog



BEE ITSECURITY

Zweiter Akt:
“Picasso”

★ ★ ★ ★ ★


Server Manager
Dashboard
Dashboard
Local Server
All Servers
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure t
2 Add roles
3 Add other
4 Create a se
5 Connect th
ROLES AND SERVER GROUPS
Roles: 0 | Server groups: 1 | Servers total: 1
8:07 PM
2/9/2020

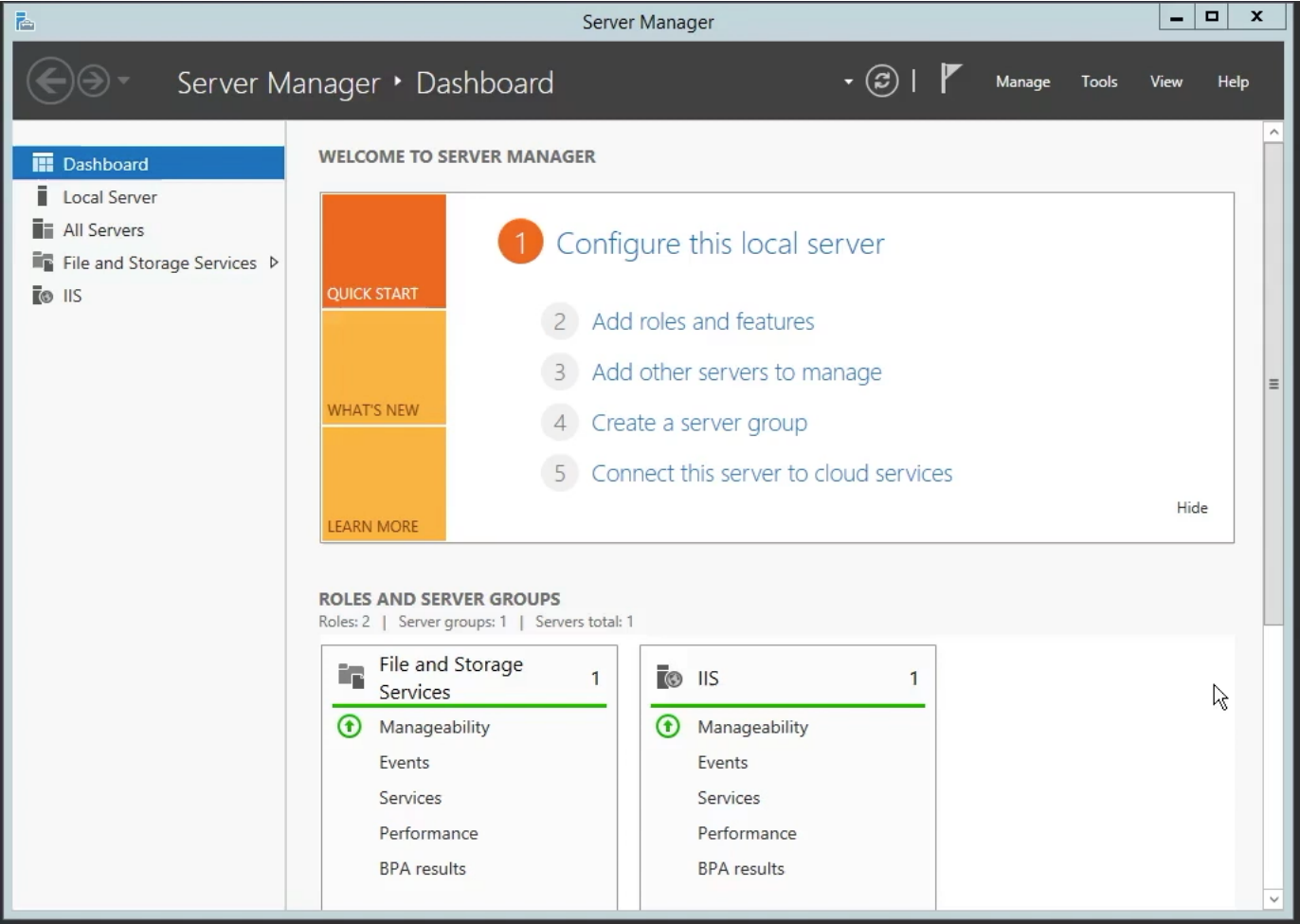

I am too


I am too

BEE ITSECURITY

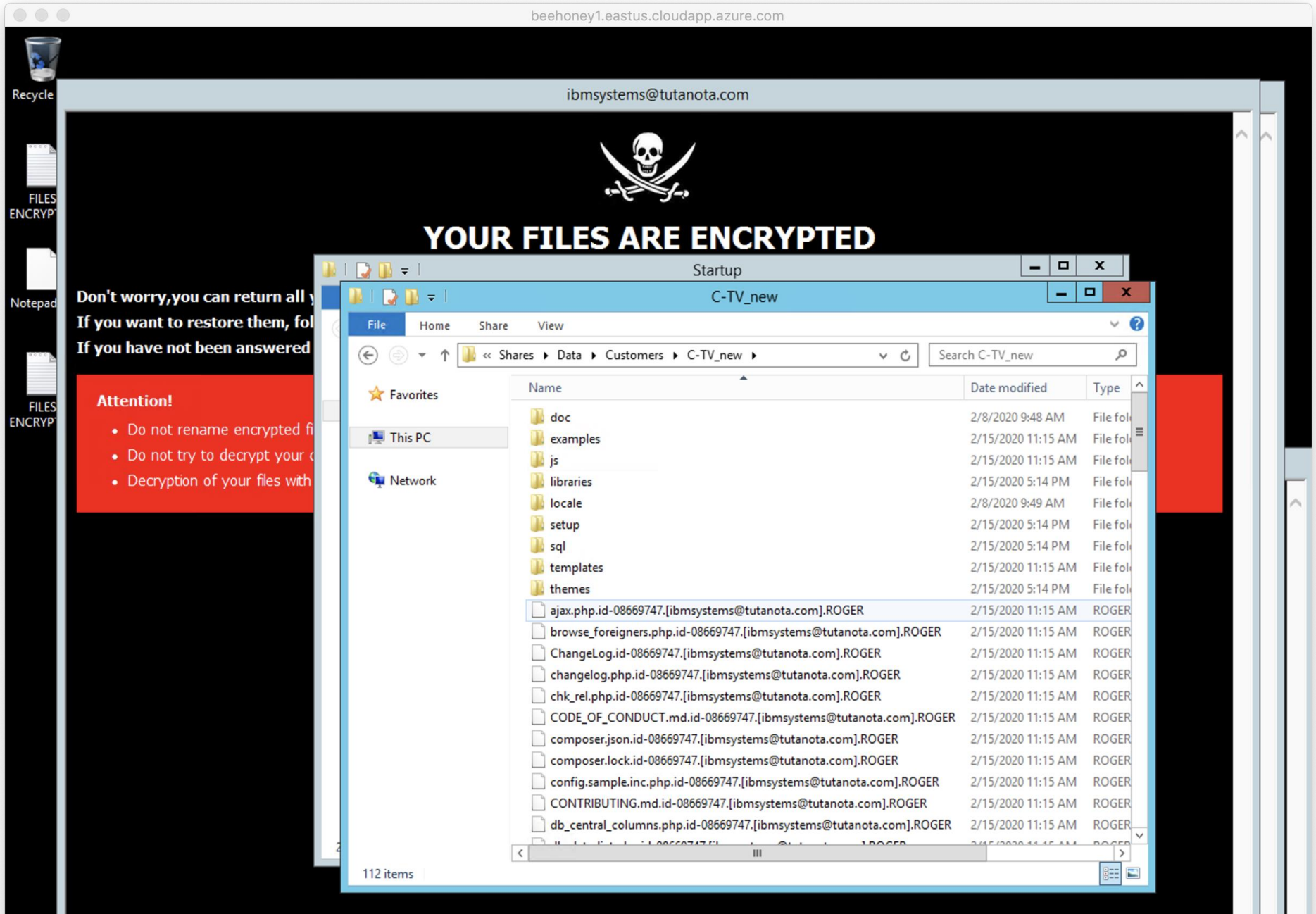
Dritter Akt:
Cryptolocker

★ ★ ★ ★ ★

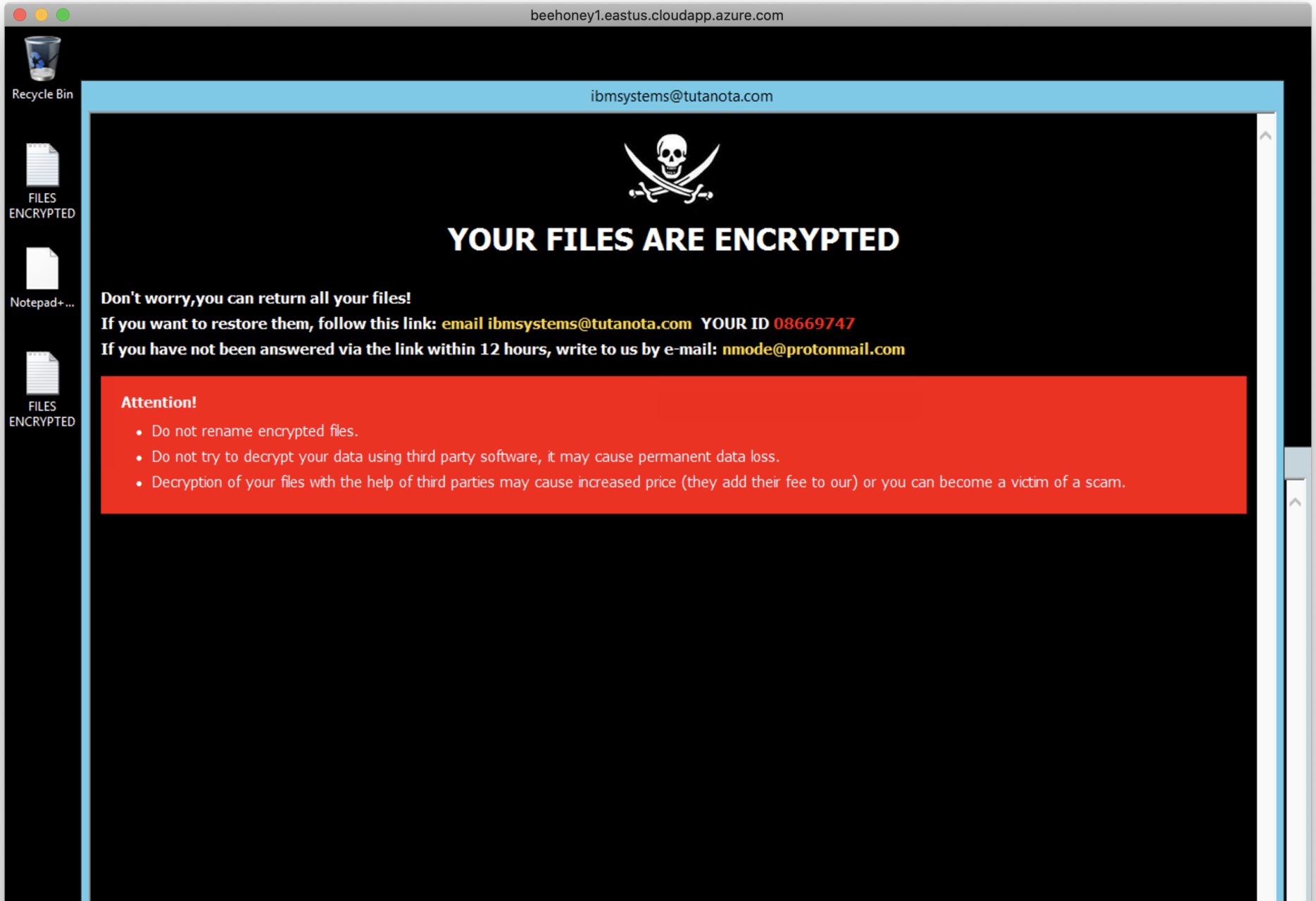


Windows Server 2012 R2

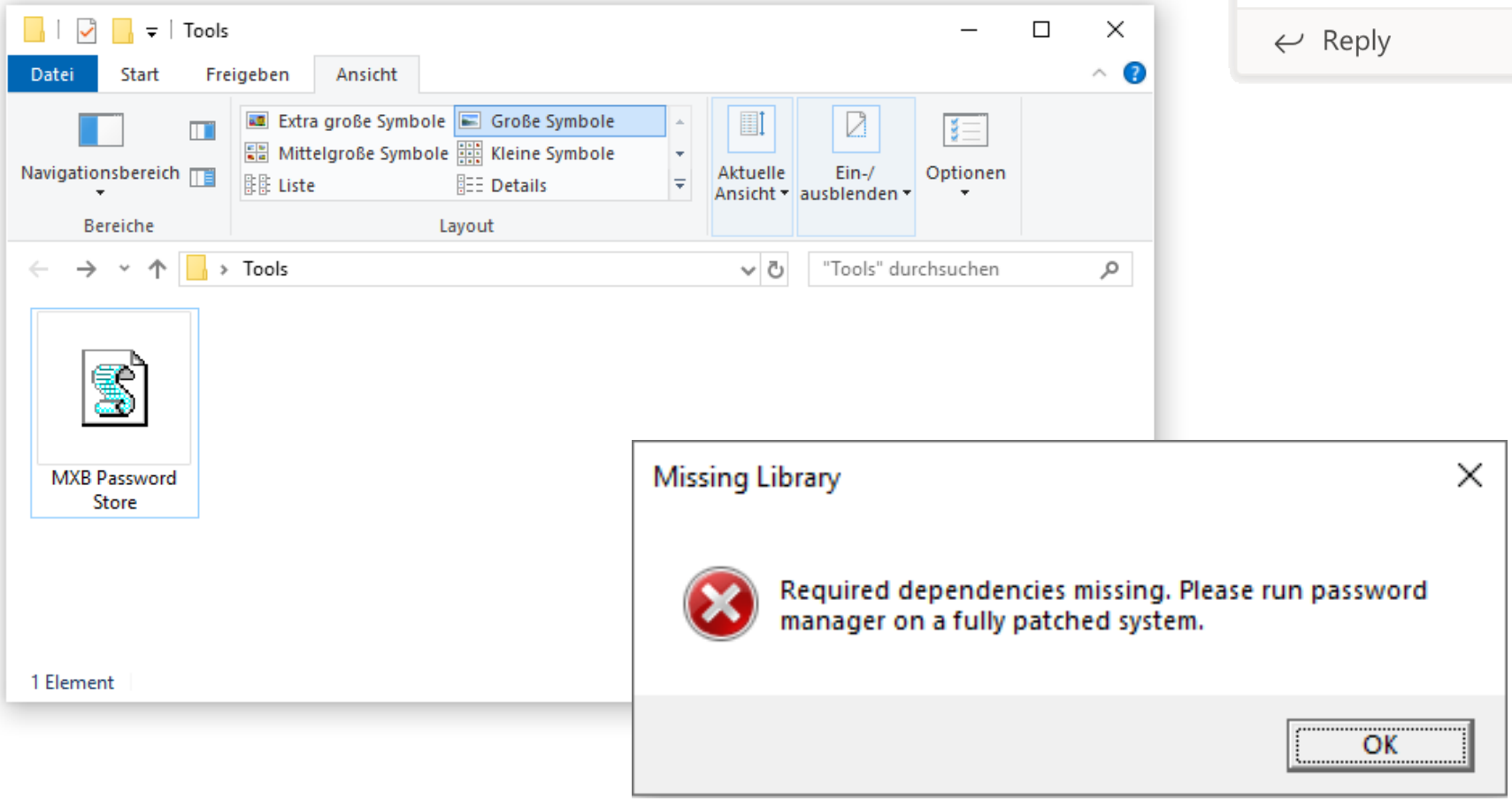
11:09 AM
2/15/2020


beehoney1.eastus.cloudapp.azure.com
Recycle
FILES ENCRYP
Notepad
FILES ENCRYP
ibmsystems@tutanota.com
YOUR FILES ARE ENCRYPTED
Don't worry,you can return all y
If you want to restore them, fol
If you have not been answered
Attention!
Do not rename encrypted fi
Do not try to decrypt your
Decryption of your files with
Startup
C-TV_new
File
Home
Share
View
Shares ▸ Data ▸ Customers ▸ C-TV_new
Search C-TV_new
Favorites
This PC
Network
Name
Date modified
Type
doc 2/8/2020 9:48 AM File fol
examples 2/15/2020 11:15 AM File fol
js 2/15/2020 11:15 AM File fol
libraries 2/15/2020 5:14 PM File fol
locale 2/8/2020 9:49 AM File fol
setup 2/15/2020 5:14 PM File fol
sql 2/15/2020 5:14 PM File fol
templates 2/15/2020 11:15 AM File fol
themes 2/15/2020 5:14 PM File fol
ajax.php.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
browse_foreigners.php.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
ChangeLog.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
changelog.php.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
chk_rel.php.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
CODE_OF_CONDUCT.md.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
composer.json.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
composer.lock.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
config.sample.inc.php.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
CONTRIBUTING.md.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
db_central_columns.php.id-08669747.[ibmsystems@tutanota.com].ROGER 2/15/2020 11:15 AM ROGER
112 items

BEE ITSECURITY



One More Thing…



BeeShell

New BeeShell client connected!

↩ Reply

BEE ITSECURITY

BeeShell C&C Interface

beeshell.eastus.cloudapp.azure.com/beeshell/admin/ui/

BEE SHELL

OS: Windows 10 Pro

WIN-MVVVR3ATJ11\Administrator@WIN-MVVVR3ATJ11
State: Online
Last pingback: 1 second(s)
OS: Windows Server 2012 R2 Standard

-PC\Administrator@-PC
State: Offline
Last pingback: 10 day(s)
OS: Windows Server 2012 R2 Standard

DESKTOP-66O0ACF\Olph@DESKTOP-66O0ACF
State: Offline
Last pingback: 41 day(s)
OS: Windows 10 Enterprise

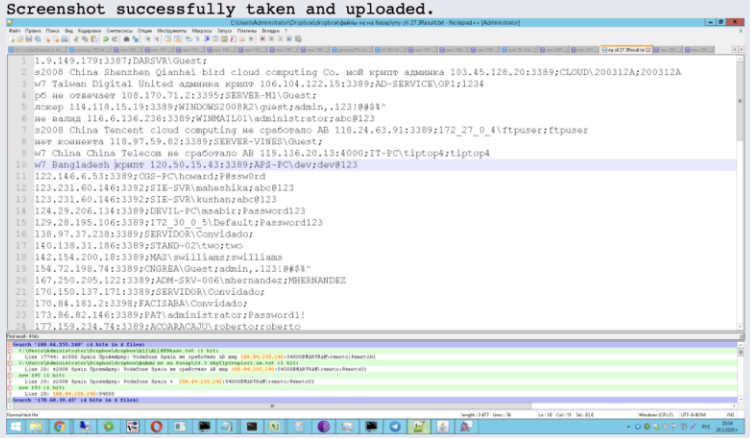
DESKTOP-R9MDTS2\Florian Bogner@DESKTOP-R9MDTS2
State: Offline
Last pingback: 26 day(s)
OS: Windows 10 Enterprise

RTHRQB-PC\rtHRQb@RTHRQB-PC
State: Offline
Last pingback: 24 day(s)
OS: Windows 10 Pro

SUNAND\admin@WIN-GH48A4O5RSJ
State: Offline
Last pingback: 24 day(s)
OS: Windows Server 2012 R2 Standard

DOUCHBAGS\Fred@CL14
State: Offline
Last pingback: 113 day(s)

```
C:\Users\Administrator\Desktop> Get-Screenshot-And-Upload
Screenshot successfully taken and uploated.
```



```
C:\Users\Administrator\Desktop> ls
Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime     Length Name
----                 -------------     ------ ----
d----          8.1.2020 r.      0:03            1nstrument
d----         25.3.2020 r.     19:55            data to sell
d----         30.10.2019 r.    11:54            gmer
d----         22.12.2019 r.    18:29            KPortScan3
da---         19.11.2019 r.     0:02            Masscan GUI
da---          12.3.2020 r.    12:15            masscan GUI2020
d----         26.10.2019 r.    21:14            mimikatz
d----          14.8.2019 r.     2:42            mimikatz-2.2.0-20190813
d----         29.12.2019 r.    21:15            New folder
d----          12.2.2020 r.    10:28            nl
d----         15.11.2019 r.    15:36            nl - Copy
d----         30.10.2019 r.    11:41            PCHunter_free
d----         24.10.2019 r.    11:59            ProxAllium
d----         24.10.2019 r.    11:46            RDP Brute
d----         21.11.2019 r.    12:23            RDP Brute - Copy
d----          28.2.2020 r.    18:12            RDP Brute - Copy (2)
d----         24.10.2019 r.    11:36            RDP FORCER 1.4
```

C:\Users\Administrator\Desktop>

Shortcodes

The following list allows you to run complex commands with a single click

One Click Launcher
Create a one click launcher for the client

Screenshot
Takes a screenshot of the target system

IEX WebClient Runner
Downloads PS code from and url an runs it

Install LNK Persistence
Persists the client by placing a LNK file in the StartUp folder

Remove LNK Persistence
Removes the LNK file from the startup folder

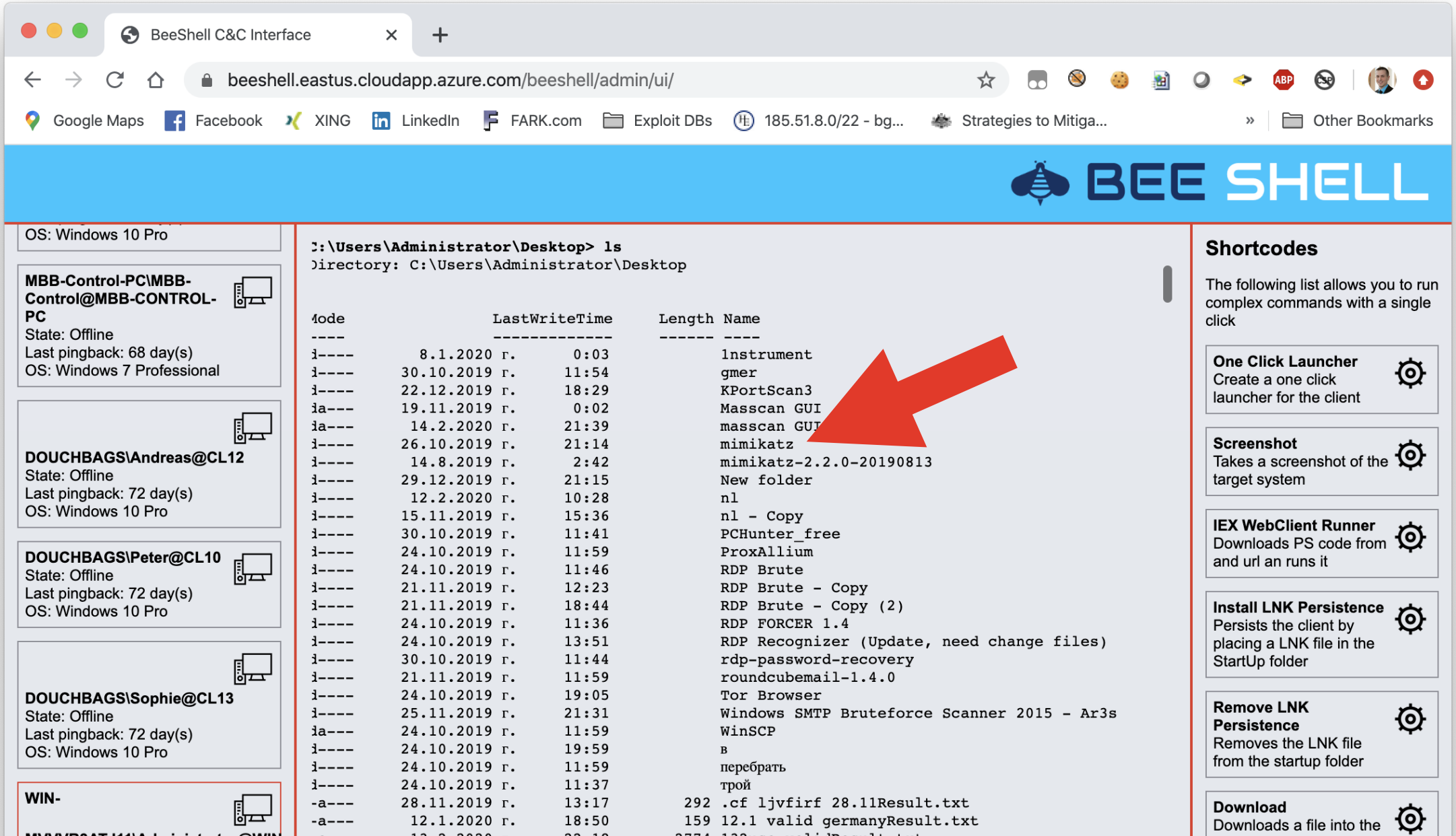
Download
Downloads a file into the current directory

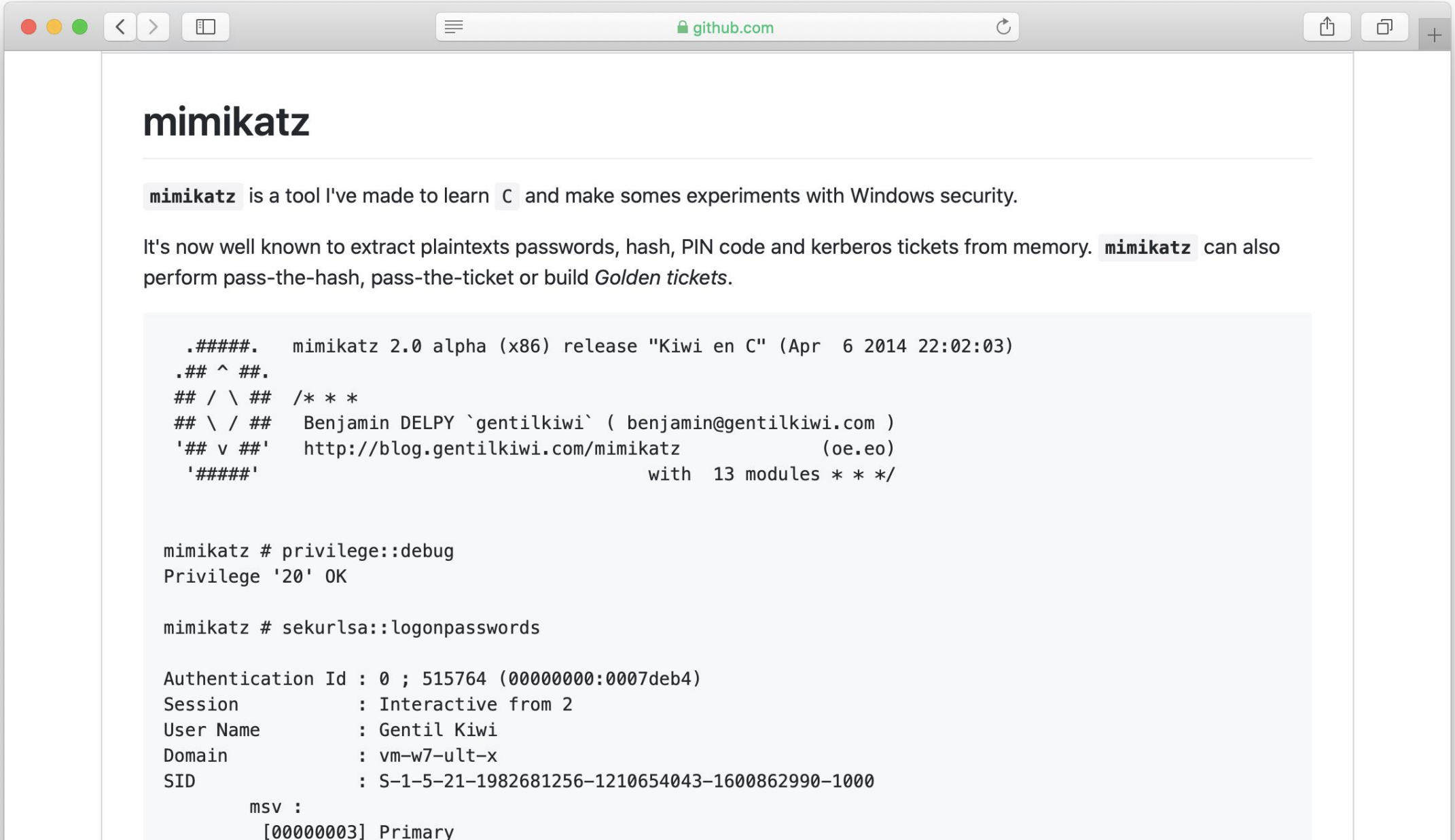
Upload
Uploads a file from the client to the C&C server

Show Uploads
Shows all the uploaded file for a client

Show Command Queue
Shows the command queue of the current system

BEE ITSECURITY





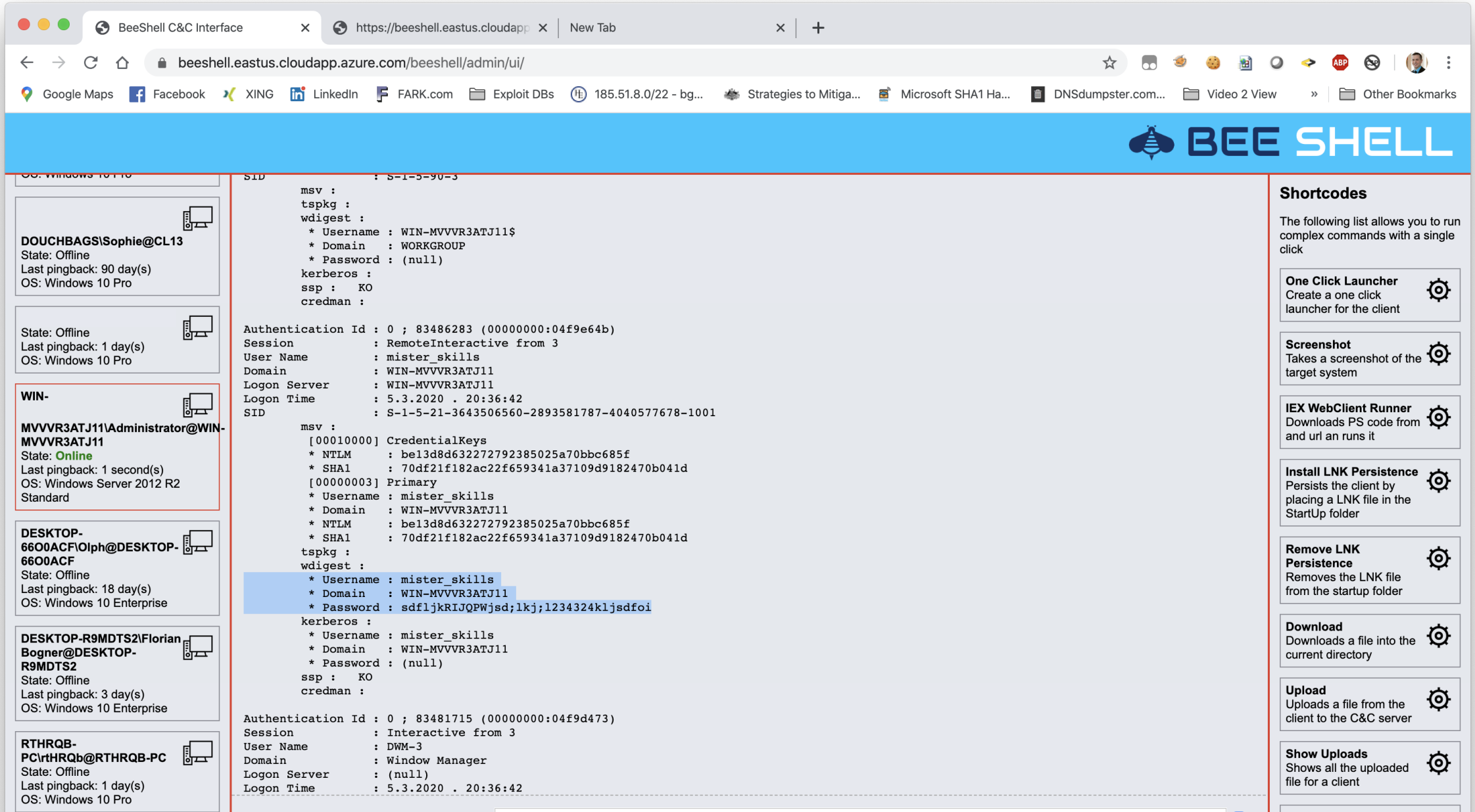
mimikatz

mimikatz is a tool I've made to learn C and make somes experiments with Windows security.

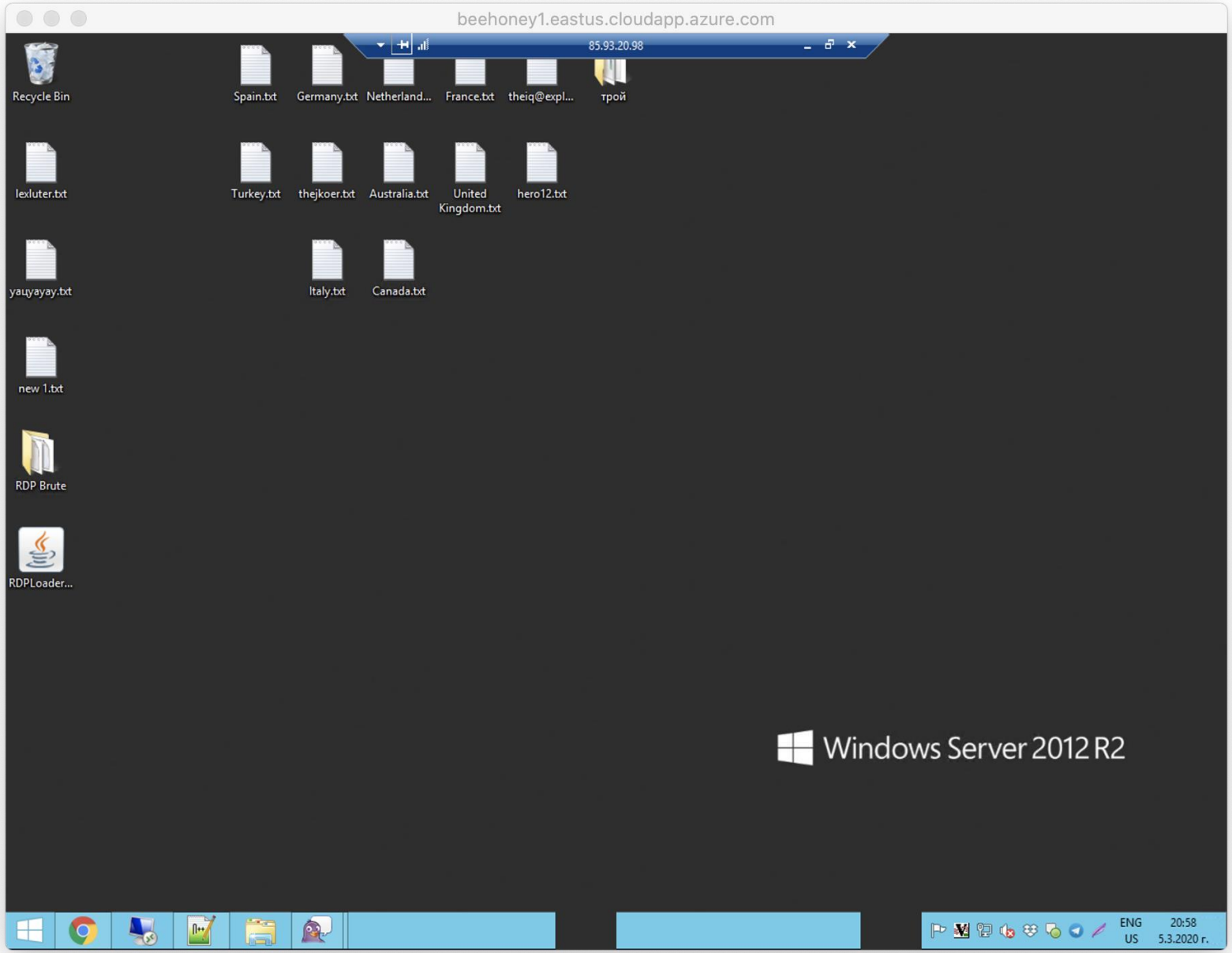
It's now well known to extract plaintexts passwords, hash, PIN code and kerberos tickets from memory. **mimikatz** can also perform pass-the-hash, pass-the-ticket or build *Golden tickets*.

```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with  13 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
```

BEE ITSECURITY

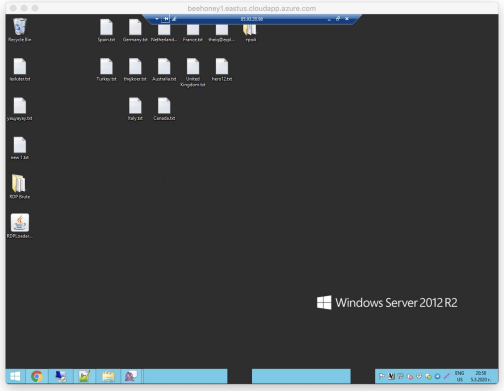


BEE ITSECURITY



BEE ITSECURITY

Ein paar Zahlen



Über drei Monate beobachtet

Über diesen Zeitraum konnten wir die Aktionen der Kriminellen beobachten.

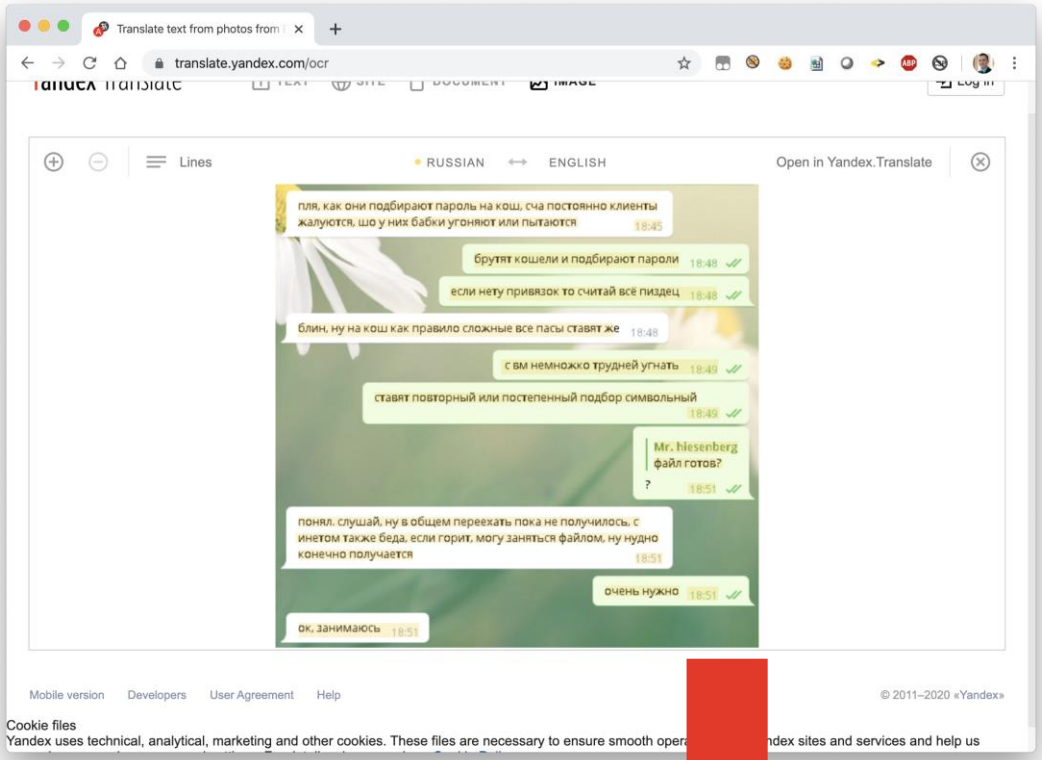
Mehr als 4GB analyisiert

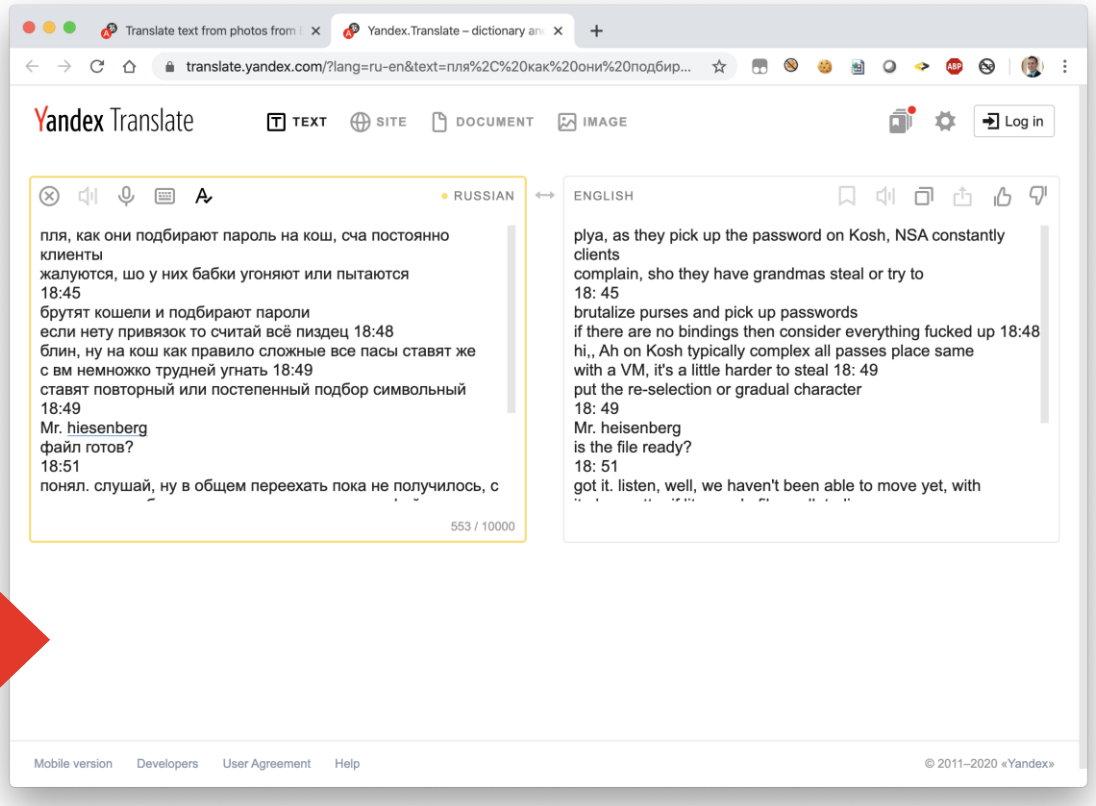
Um die Abläufe zu verstehen, wurden mehr als 4GB an Daten durchforstet.

Jenseits von 2.000 Screenshots

Für einen interaktiven Einblick wurden über zweitausende Screenshots erzeugt.

Mein Russisch ist richtig schlecht: Yandex Image Translate



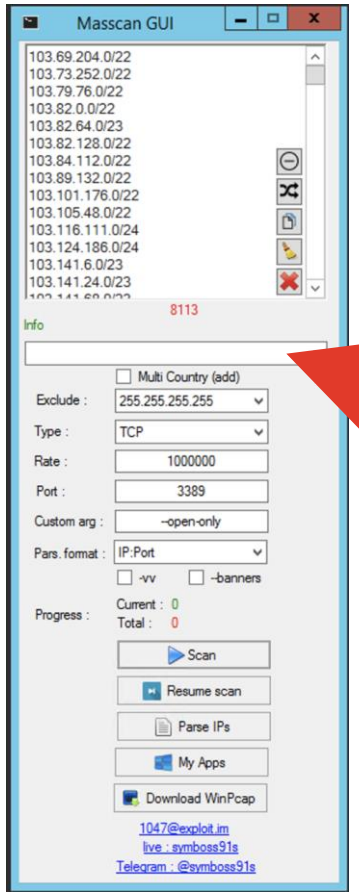


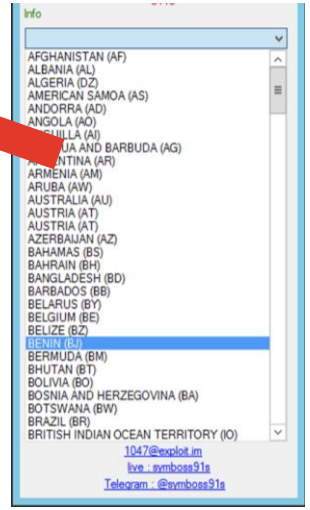
BEE ITSECURITY

Wie bricht man in RDP Server ein?

1 Masscan

Findet öffentliche RDP Server

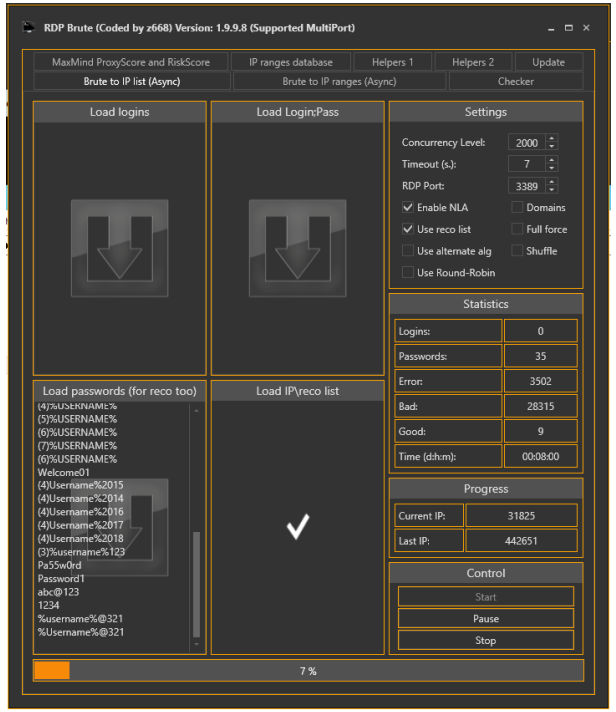




Länder IP Ranges inklusive

2 RDP Brute

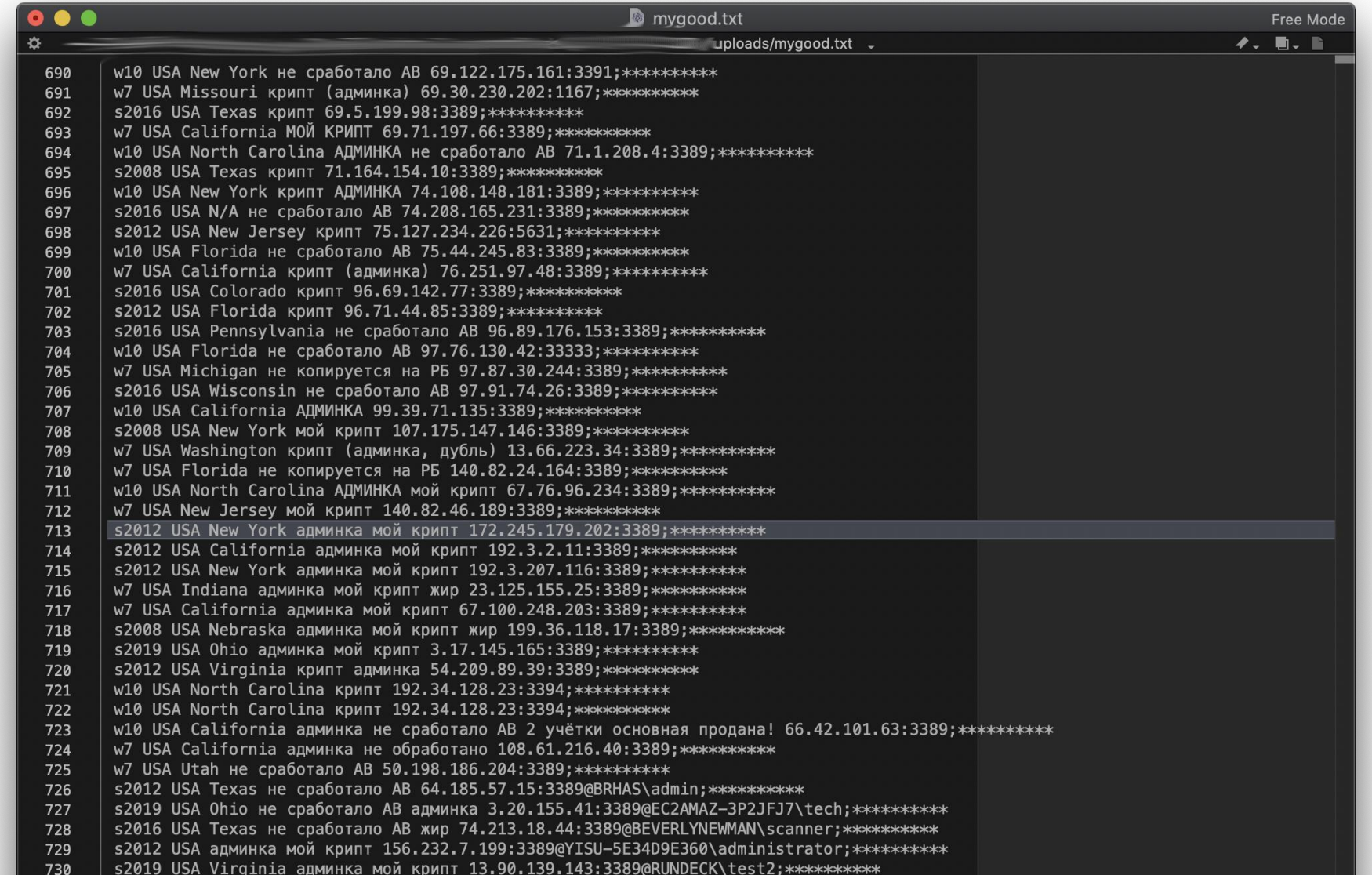
RDP Bruteforce / Dictionary Attack Tool



RDP Brute beinhaltet auch einen „Checker“ um einmal gefundene Logins zu testen

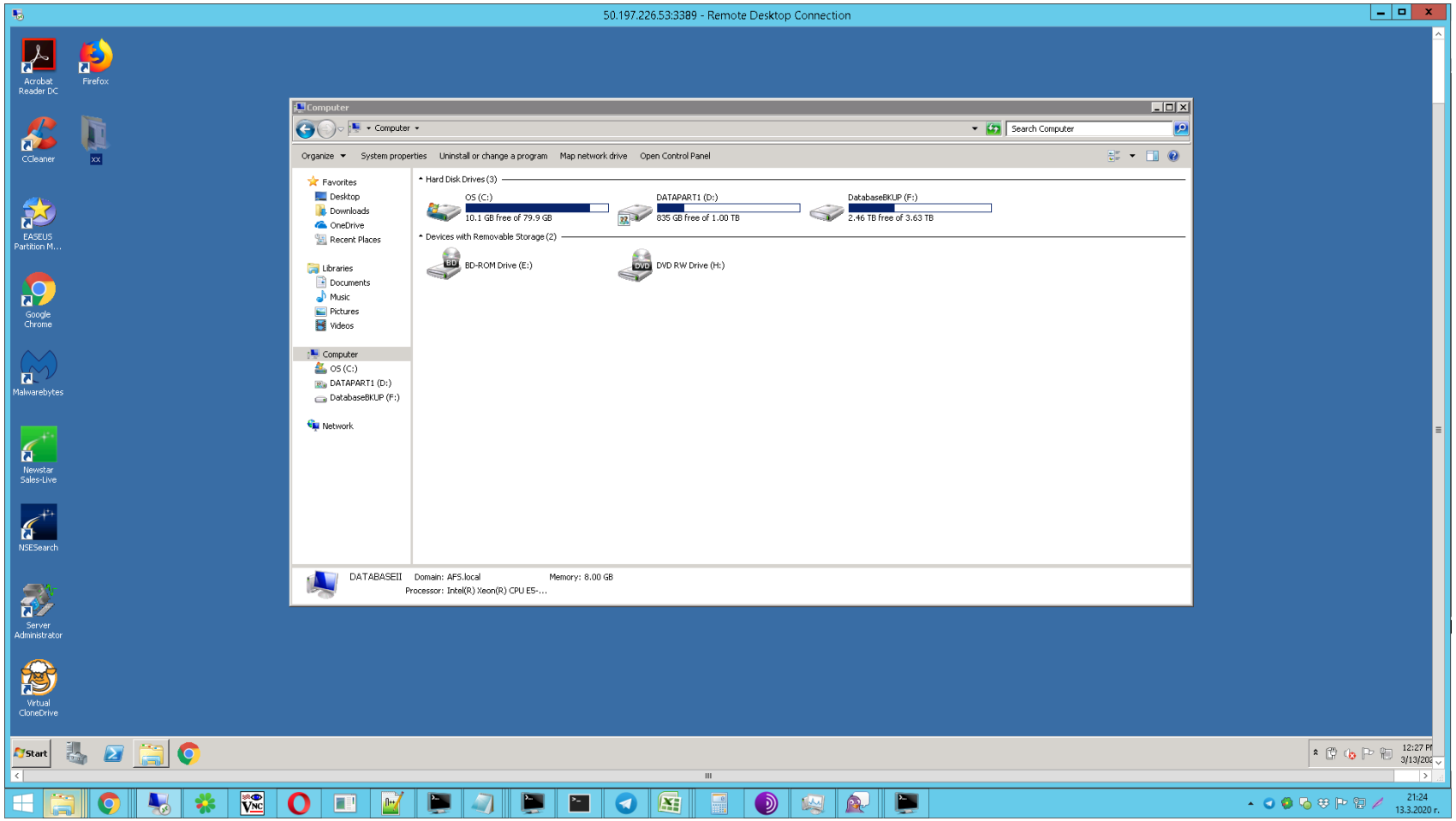
BEE ITSECURITY

Wie bricht man in RDP Server ein?



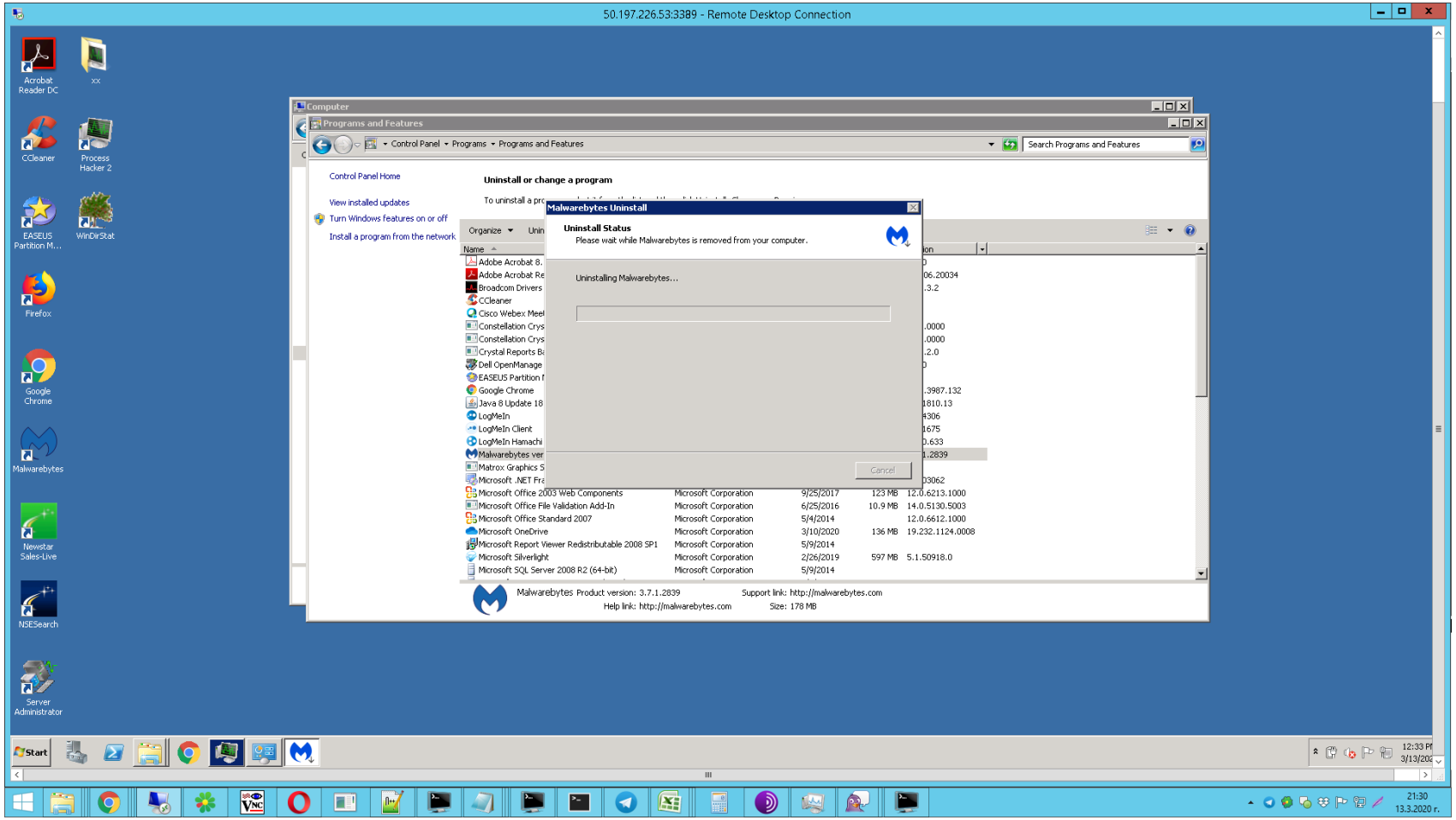
Nächster Schritt: manuelle Analyse

Der Angreifer verbindet sich per mstsc.exe auf eines der gehakten Systeme



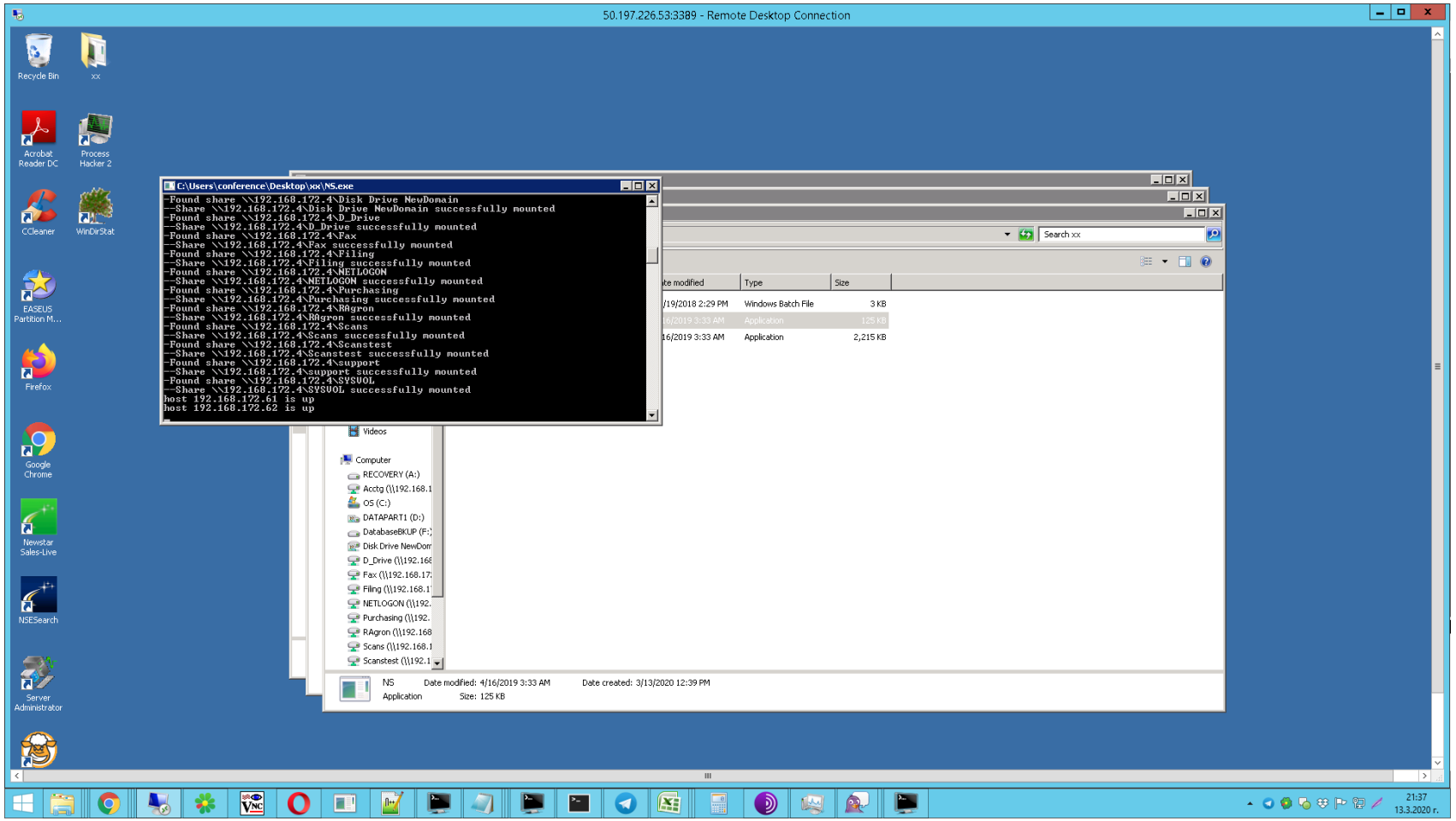
Nächster Schritt: manuelle Analyse

Installierte Anti Viren Lösungen werden per Systemsteuerung oder IObit Uninstaller entfernt



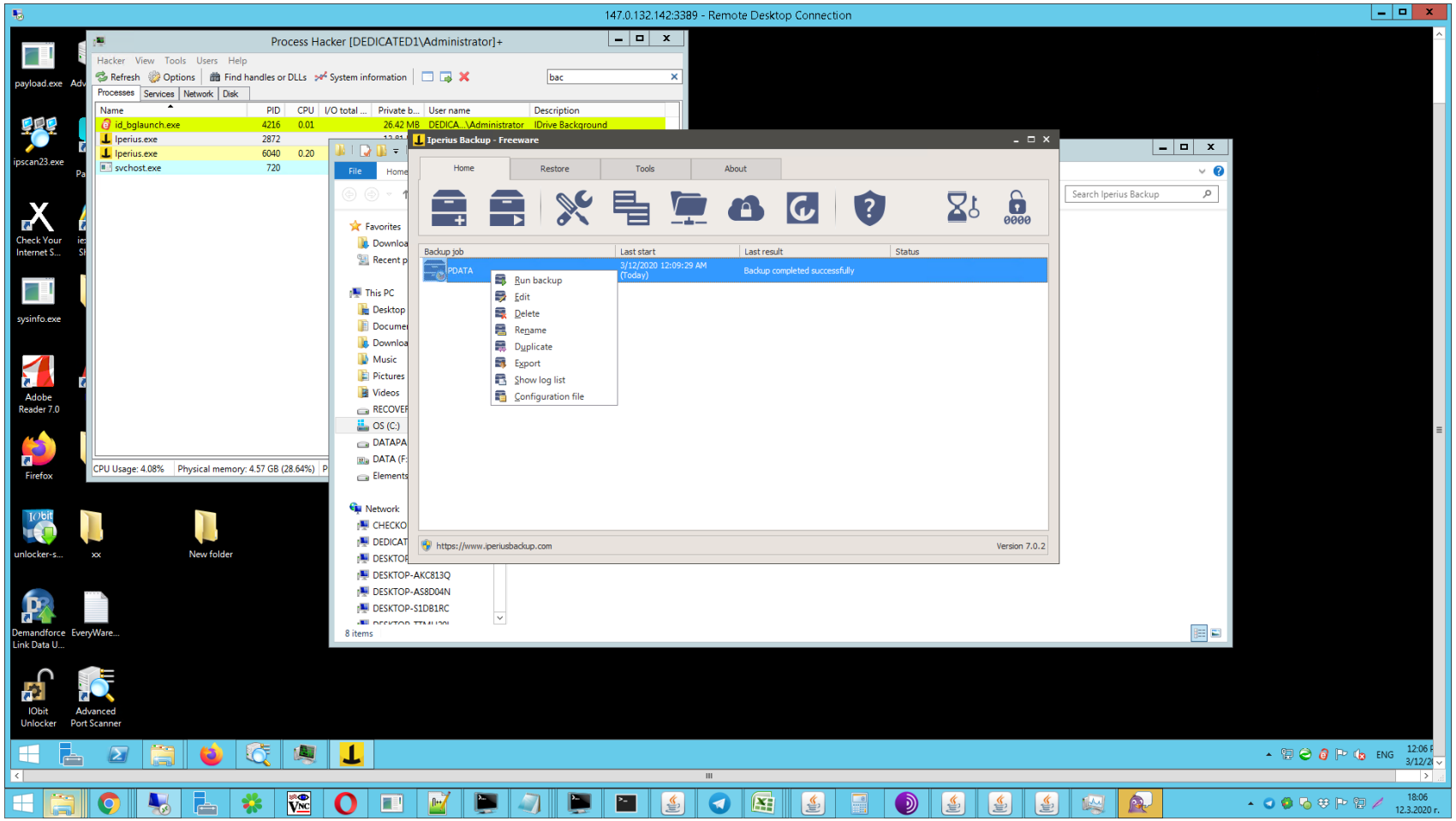
Nächster Schritt: manuelle Analyse

„NS.exe“ sucht nach verwendeten SMB Shares und sucht auch das lokale Netzwerk nach Fileservern ab



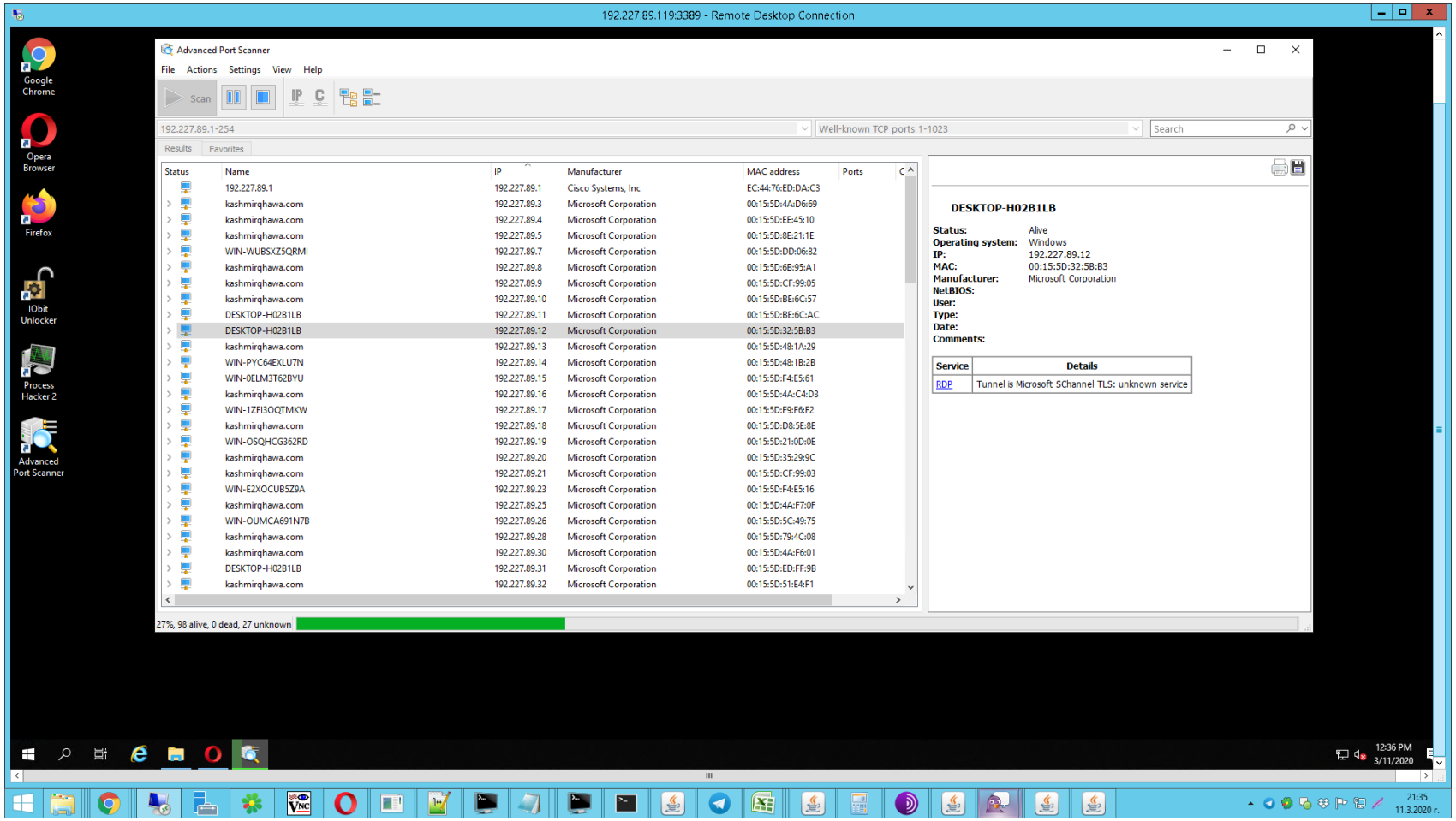
Nächster Schritt: manuelle Analyse

Vorhandene Backups werden manuell gelöscht



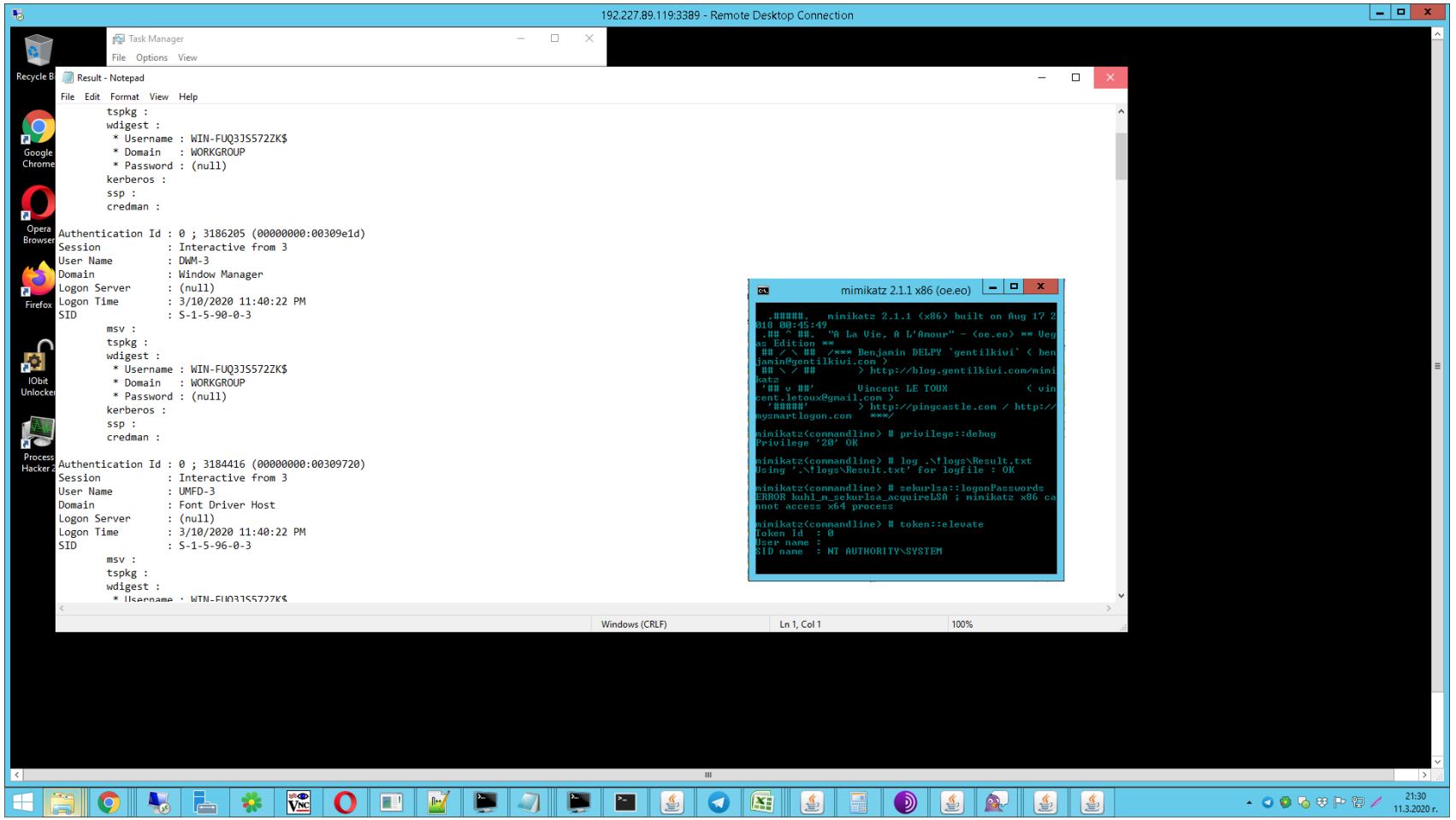
Nächster Schritt: manuelle Analyse

Mit dem Advanced Port Scanner werden mögliche Pfade zur Privilege Escalation gesucht



Nächster Schritt: manuelle Analyse

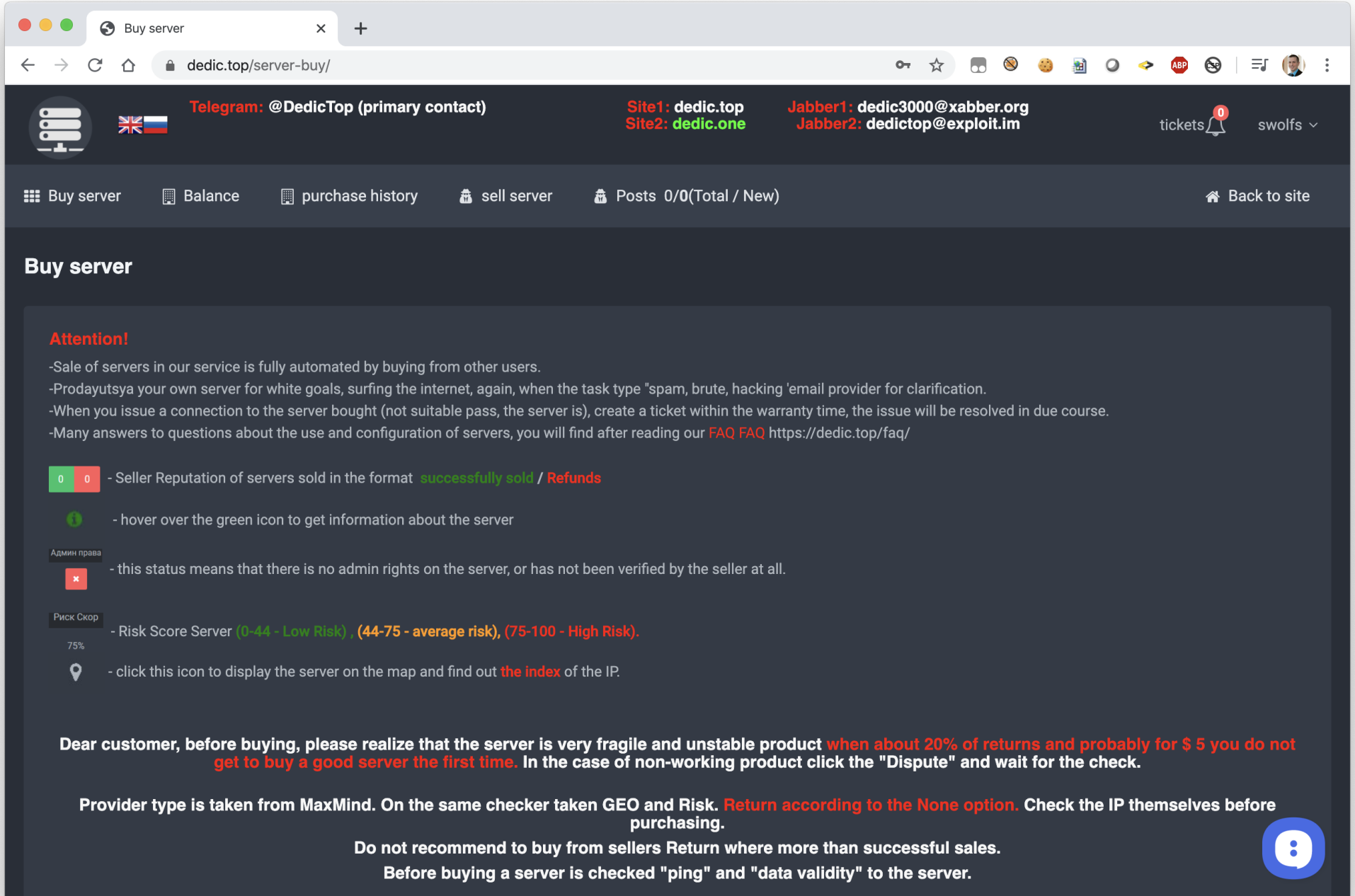
Um weitere Zugangsdaten dafür zu erhalten wird u.a. mimikatz verwendet



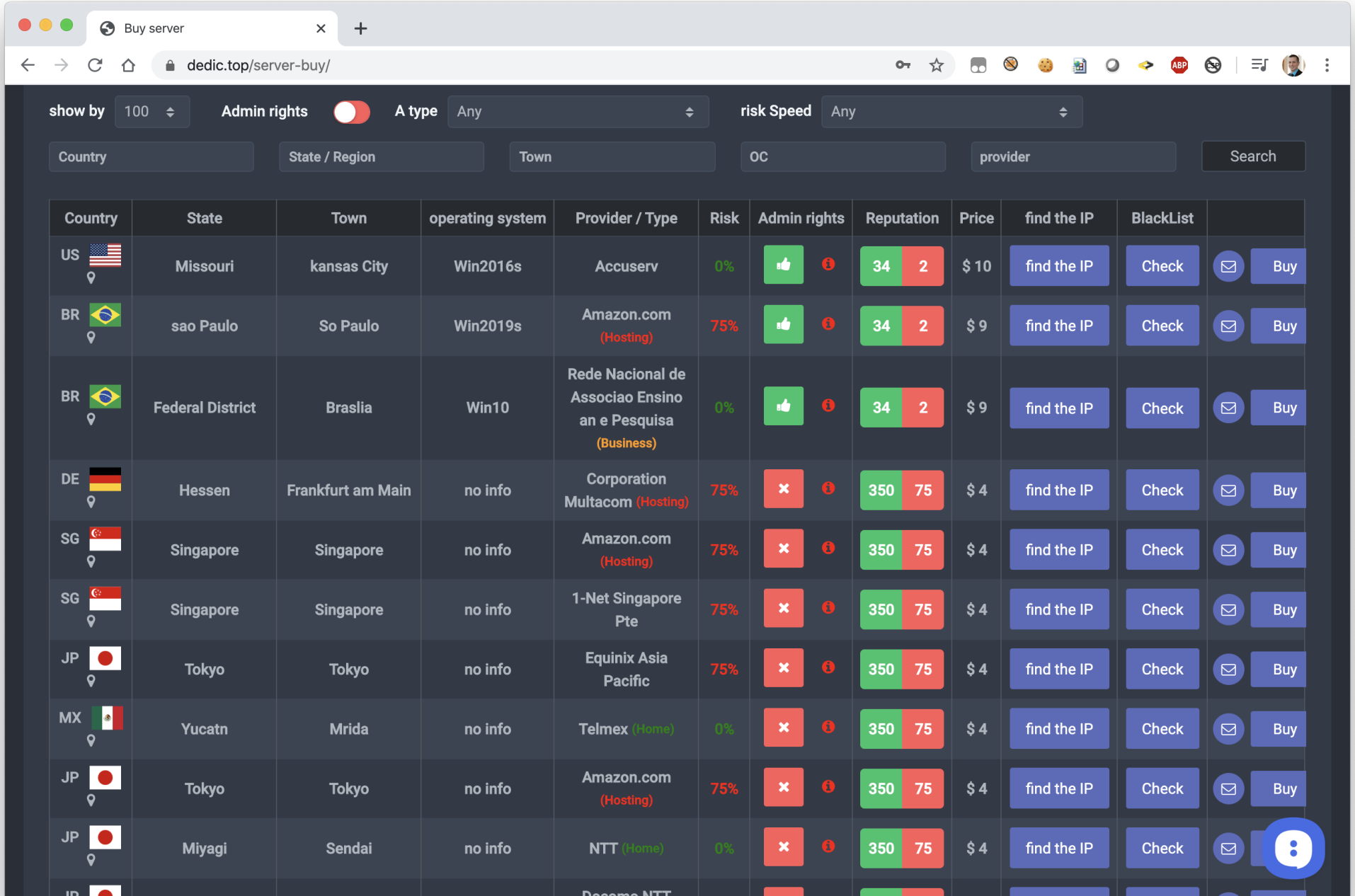
Das Finale: Cash-out

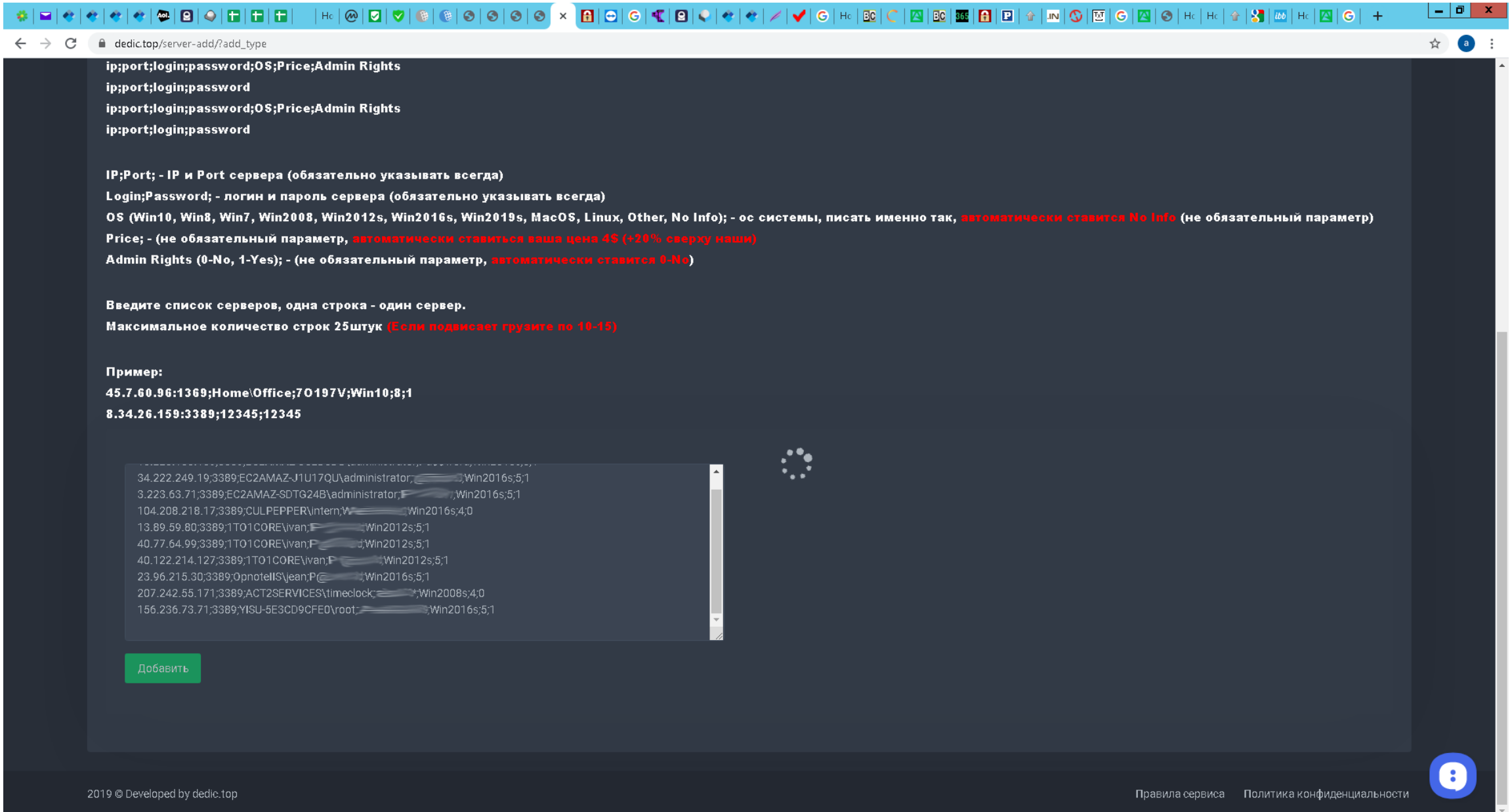
Verkauf

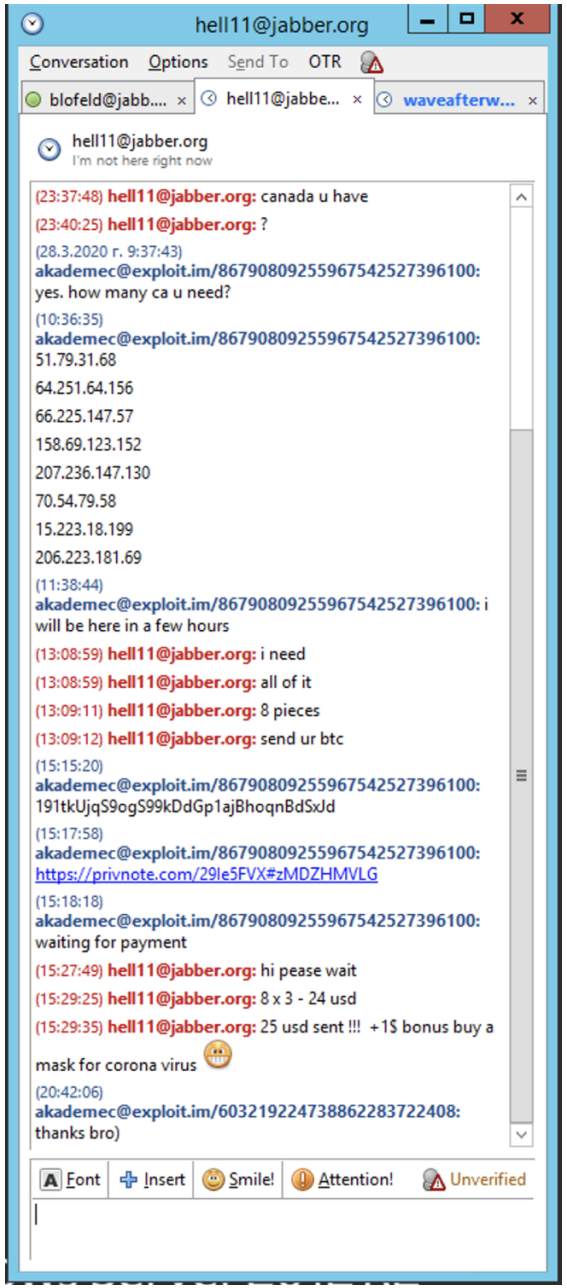
- Wenige Dateien: Verkauf für Identitätsdiebstahl
- Viele Dateien: Verkauf für weitere Analysen (u.a. Datendiebstahl)

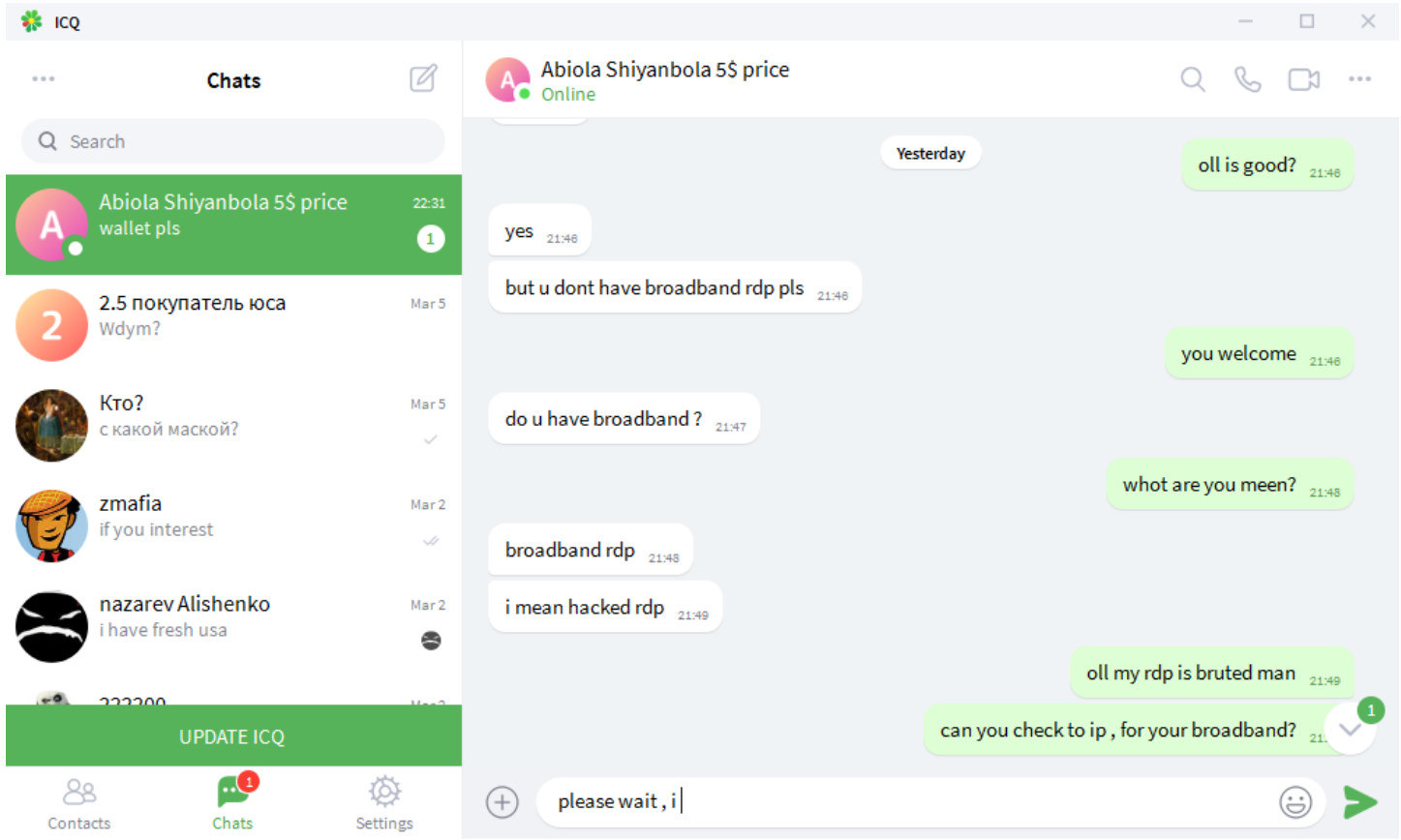

Buy server
dedic.top/server-buy/
Telegram: @DedicTop (primary contact)
Site1: dedic.top
Site2: dedic.one
Jabber1: dedic3000@xabber.org
Jabber2: dedictop@exploit.im
tickets
swolfs
Buy server
Balance
purchase history
sell server
Posts 0/0(Total / New)
Back to site
Buy server
Attention!
-Sale of servers in our service is fully automated by buying from other users.
-Prodayutsya your own server for white goals, surfing the internet, again, when the task type "spam, brute, hacking 'email provider for clarification.
-When you issue a connection to the server bought (not suitable pass, the server is), create a ticket within the warranty time, the issue will be resolved in due course.
-Many answers to questions about the use and configuration of servers, you will find after reading our FAQ FAQ https://dedic.top/faq/
0 0 - Seller Reputation of servers sold in the format successfully sold / Refunds
- hover over the green icon to get information about the server
Админ права
- this status means that there is no admin rights on the server, or has not been verified by the seller at all.
Риск Скор
75%
- Risk Score Server (0-44 - Low Risk) , (44-75 - average risk), (75-100 - High Risk).
- click this icon to display the server on the map and find out the index of the IP.
Dear customer, before buying, please realize that the server is very fragile and unstable product when about 20% of returns and probably for $ 5 you do not get to buy a good server the first time. In the case of non-working product click the "Dispute" and wait for the check.
Provider type is taken from MaxMind. On the same checker taken GEO and Risk. Return according to the None option. Check the IP themselves before purchasing.
Do not recommend to buy from sellers Return where more than successful sales.
Before buying a server is checked "ping" and "data validity" to the server.

BEE ITSECURITY




dedic.top/server-add/?add_type
ip;port;login;password;OS;Price;Admin Rights
ip;port;login;password
ip:port;login;password;OS;Price;Admin Rights
ip:port;login;password
IP;Port; - IP и Port сервера (обязательно указывать всегда)
Login;Password; - логин и пароль сервера (обязательно указывать всегда)
OS (Win10, Win8, Win7, Win2008, Win2012s, Win2016s, Win2019s, MacOS, Linux, Other, No Info); - ос системы, писать именно так, автоматически ставится No Info (не обязательный параметр)
Price; - (не обязательный параметр, автоматически ставиться ваша цена 4$ (+20% сверху наши)
Admin Rights (0-No, 1-Yes); - (не обязательный параметр, автоматически ставится 0-No)
Введите список серверов, одна строка - один сервер.
Максимальное количество строк 25штук (Если подвисает грузите по 10-15)
Пример:
45.7.60.96:1369;Home\Office;7O197V;Win10;8;1
8.34.26.159:3389;12345;12345
34.222.249.19;3389;EC2AMAZ-J1U17QU\administrator;[redacted];Win2016s;5;1
3.223.63.71;3389;EC2AMAZ-SDTG24B\administrator;[redacted];Win2016s;5;1
104.208.218.17;3389;CULPEPPER\intern;[redacted]Win2016s;4;0
13.89.59.80;3389;1TO1CORE\ivan;[redacted];Win2012s;5;1
40.77.64.99;3389;1TO1CORE\ivan;[redacted];Win2012s;5;1
40.122.214.127;3389;1TO1CORE\ivan;[redacted];Win2012s;5;1
23.96.215.30;3389;OpnotelIS\jean;[redacted];Win2016s;5;1
207.242.55.171;3389;ACT2SERVICES\timeclock;[redacted];Win2008s;4;0
156.236.73.71;3389;YISU-5E3CD9CFE0\root;[redacted];Win2016s;5;1
Добавить
2019 © Developed by dedic.top
Правила сервиса
Политика конфиденциальности


hell11@jabber.org
Conversation Options Send To OTR
blofeld@jabb.... hell11@jabbe... waveafterw...
hell11@jabber.org
I'm not here right now
(23:37:48) hell11@jabber.org: canada u have
(23:40:25) hell11@jabber.org: ?
(28.3.2020 г. 9:37:43)
akademec@exploit.im/867908092559675425273961000:
yes. how many ca u need?
(10:36:35)
akademec@exploit.im/867908092559675425273961000:
51.79.31.68
64.251.64.156
66.225.147.57
158.69.123.152
207.236.147.130
70.54.79.58
15.223.18.199
206.223.181.69
(11:38:44)
akademec@exploit.im/867908092559675425273961000: i will be here in a few hours
(13:08:59) hell11@jabber.org: i need
(13:08:59) hell11@jabber.org: all of it
(13:09:11) hell11@jabber.org: 8 pieces
(13:09:12) hell11@jabber.org: send ur btc
(15:15:20)
akademec@exploit.im/867908092559675425273961000:
191tkUjqS9ogS99kDdGp1ajBhoqnBdSxJd
(15:17:58)
akademec@exploit.im/867908092559675425273961000:
https://privnote.com/29le5FVX#zMDZHMVLG
(15:18:18)
akademec@exploit.im/867908092559675425273961000:
waiting for payment
(15:27:49) hell11@jabber.org: hi pease wait
(15:29:25) hell11@jabber.org: 8 x 3 - 24 usd
(15:29:35) hell11@jabber.org: 25 usd sent !!! +1$ bonus buy a mask for corona virus
(20:42:06)
akademec@exploit.im/603219224738862283722408:
thanks bro)
Font Insert Smile! Attention! Unverified


ICQ
Chats
Search
Abiola Shiyanbola 5$ price
wallet pls
22:31
2.5 покупатель юса
Wdym?
Mar 5
Кто?
с какой маской?
Mar 5
zmafia
if you interest
Mar 2
nazarev Alishenko
i have fresh usa
Mar 2
UPDATE ICQ
Contacts
Chats
Settings
Abiola Shiyanbola 5$ price
Online
Yesterday
oll is good? 21:46
yes 21:46
but u dont have broadband rdp pls 21:46
you welcome 21:46
do u have broadband ? 21:47
whot are you meen? 21:48
broadband rdp 21:48
i mean hacked rdp 21:49
oll my rdp is bruted man 21:49
can you check to ip , for your broadband?
please wait , i

Das Finale: Cash-out

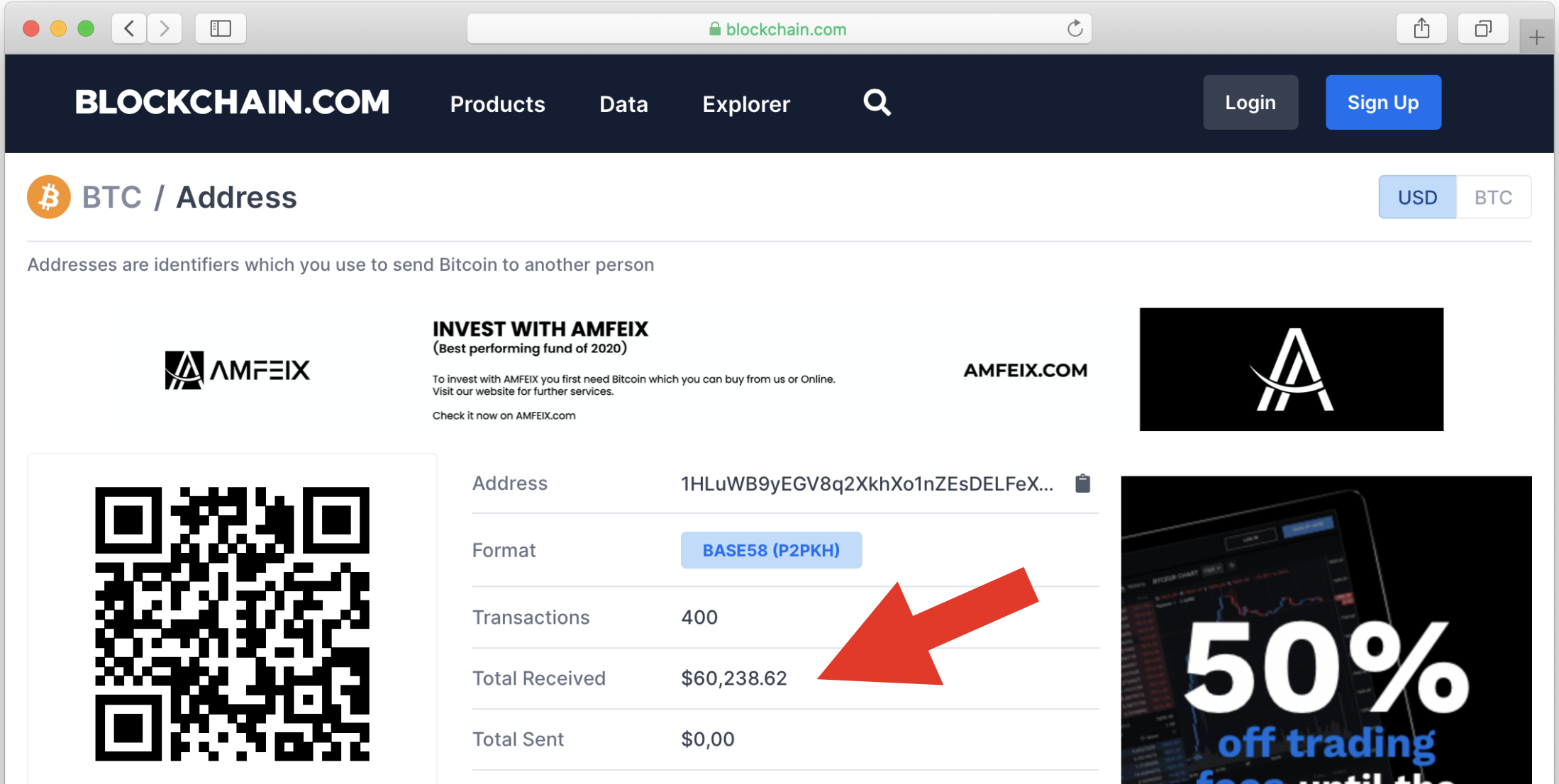
Verkauf

- Wenige Dateien: Verkauf für Identitätsdiebstahl
- Viele Dateien: Verkauf für weitere Analysen (u.a. Datendiebstahl)

Cryptolocker

- Verschlüsselung von einem / mehreren Systemen
- Wie in unserem Fall
- Forderung: zuerst 3k, dann 5k

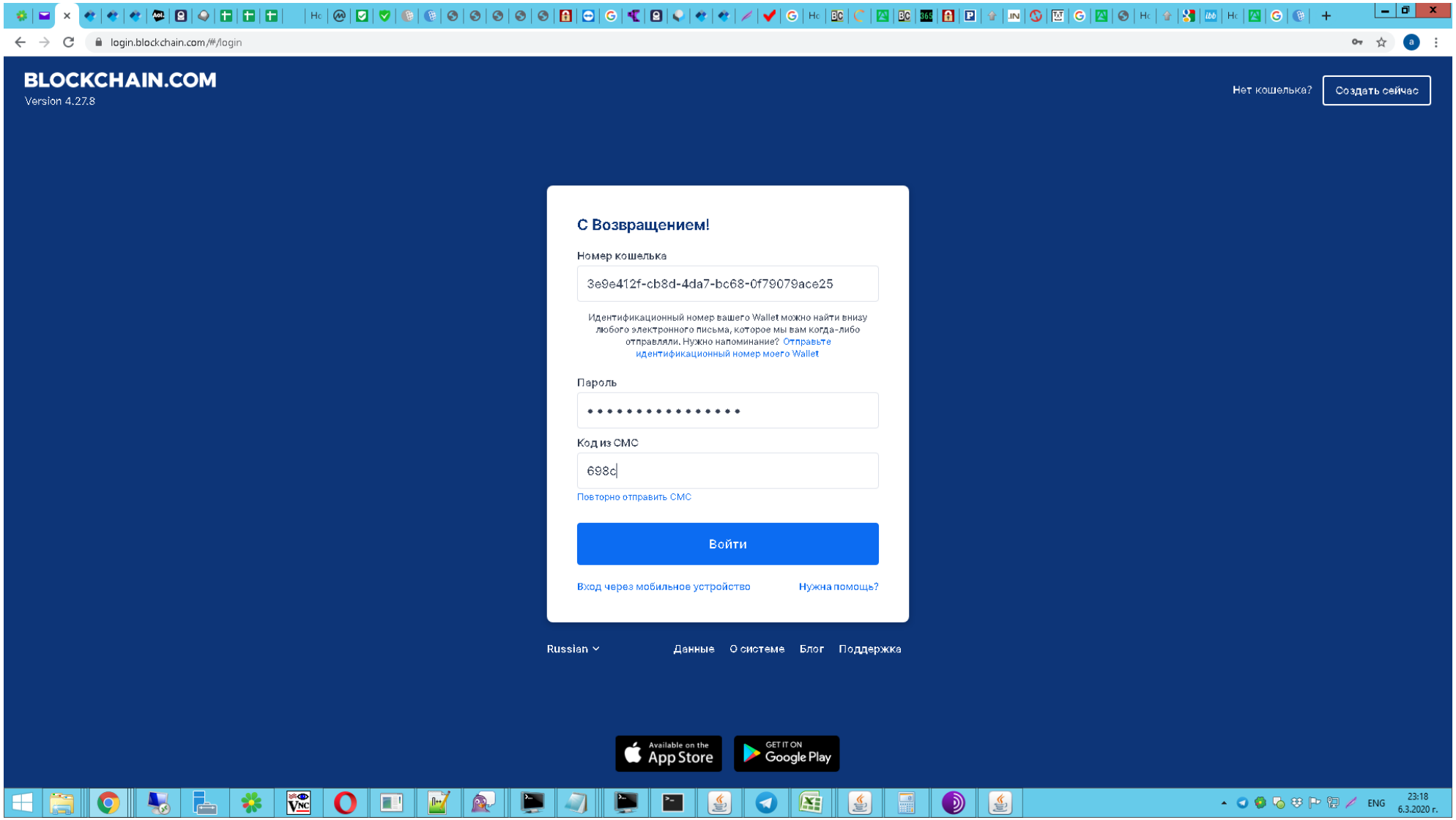
Der Verdienst ist durchaus verlockend




NUR EINMAL ANGENOMMEN:
WÜRDEN WIR VIELLEICHT AUF DIE BITCOIN WALLET ZUGRIFF BEKOMMEN?

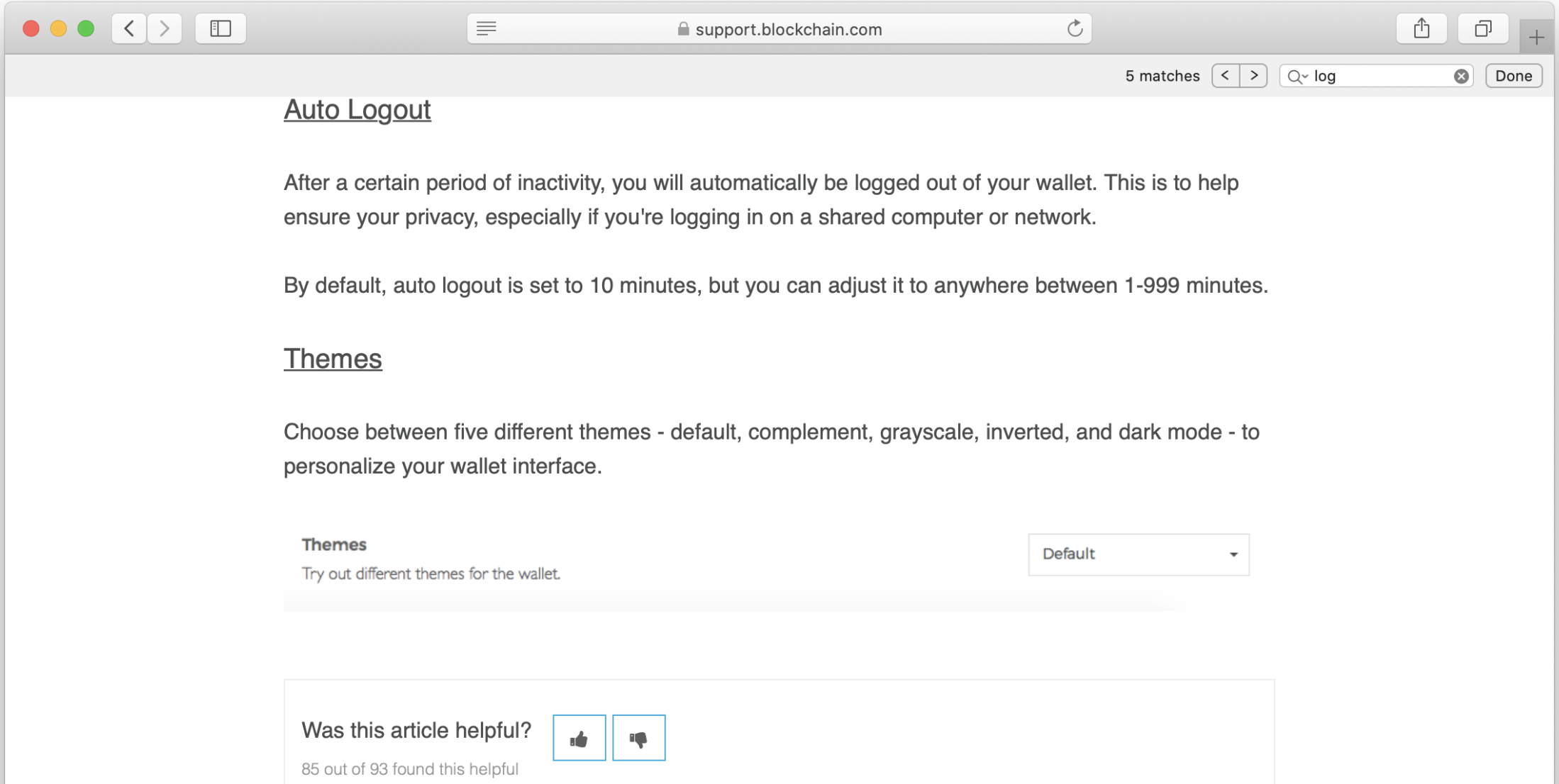
BEE ITSECURITY

MFA ist dein ~~Freund~~ Feind



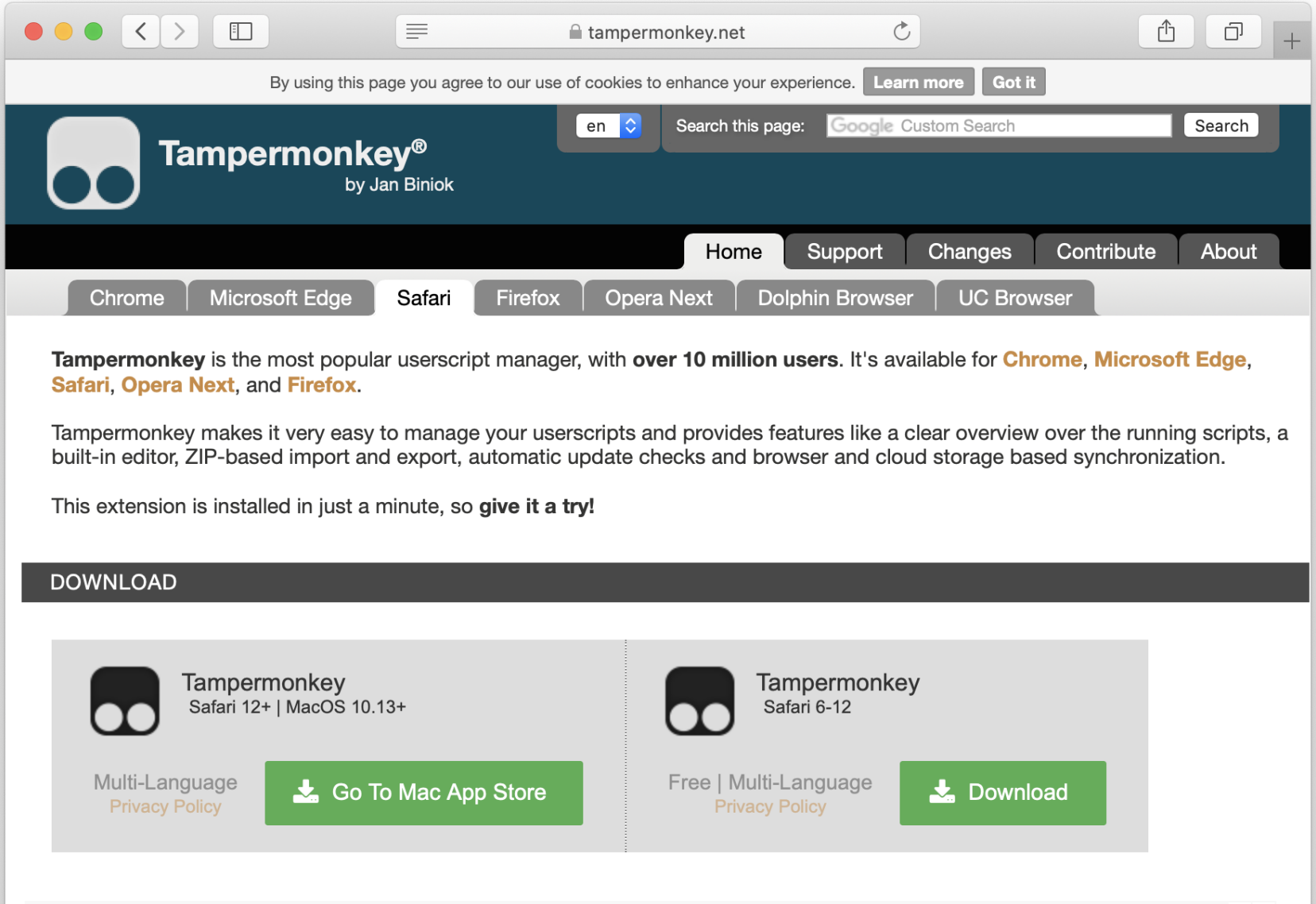
BEE ITSECURITY

Auto Logout ist dein ~~Freund~~ Feind



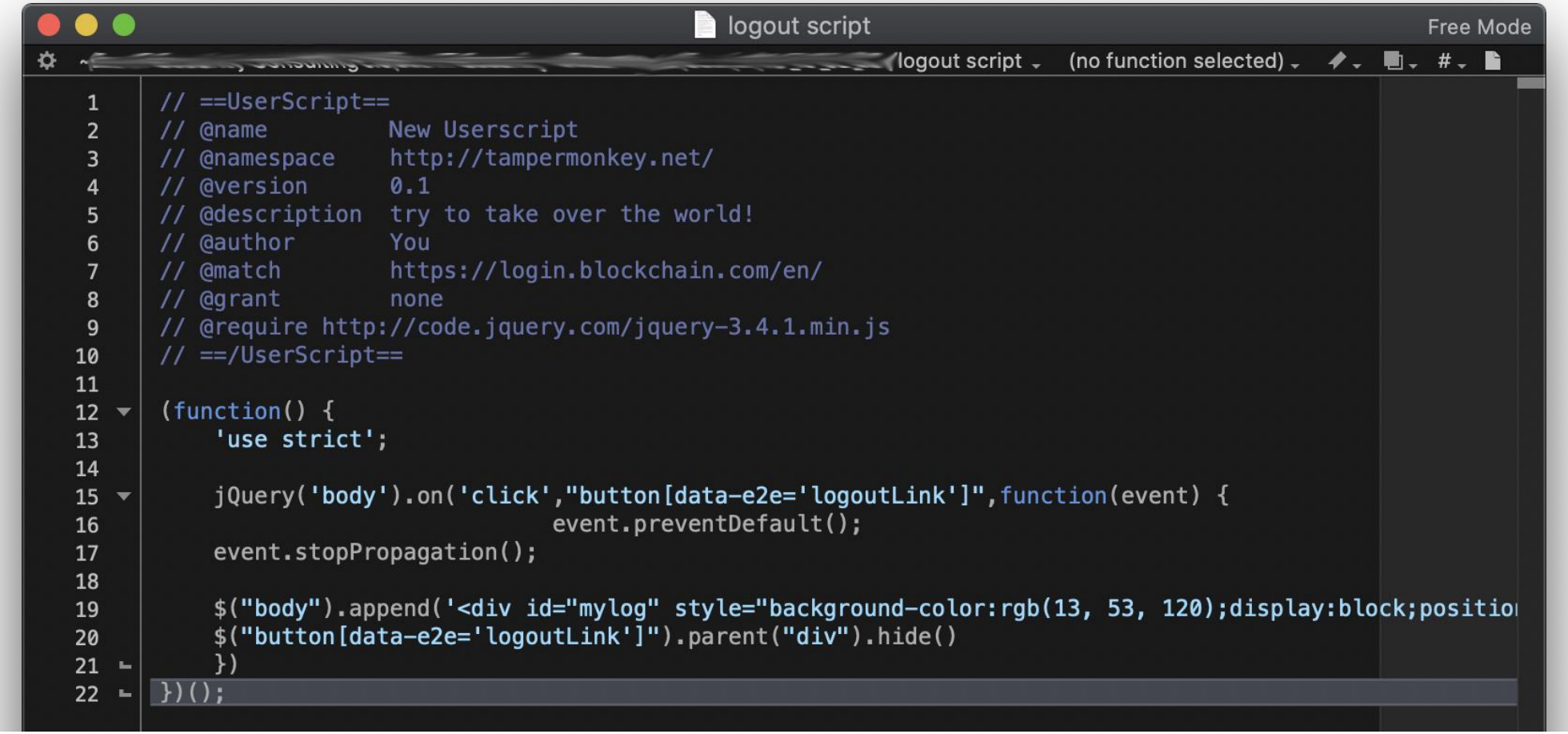
BEE ITSECURITY

Tampermonkey To The Rescue



BEE ITSECURITY

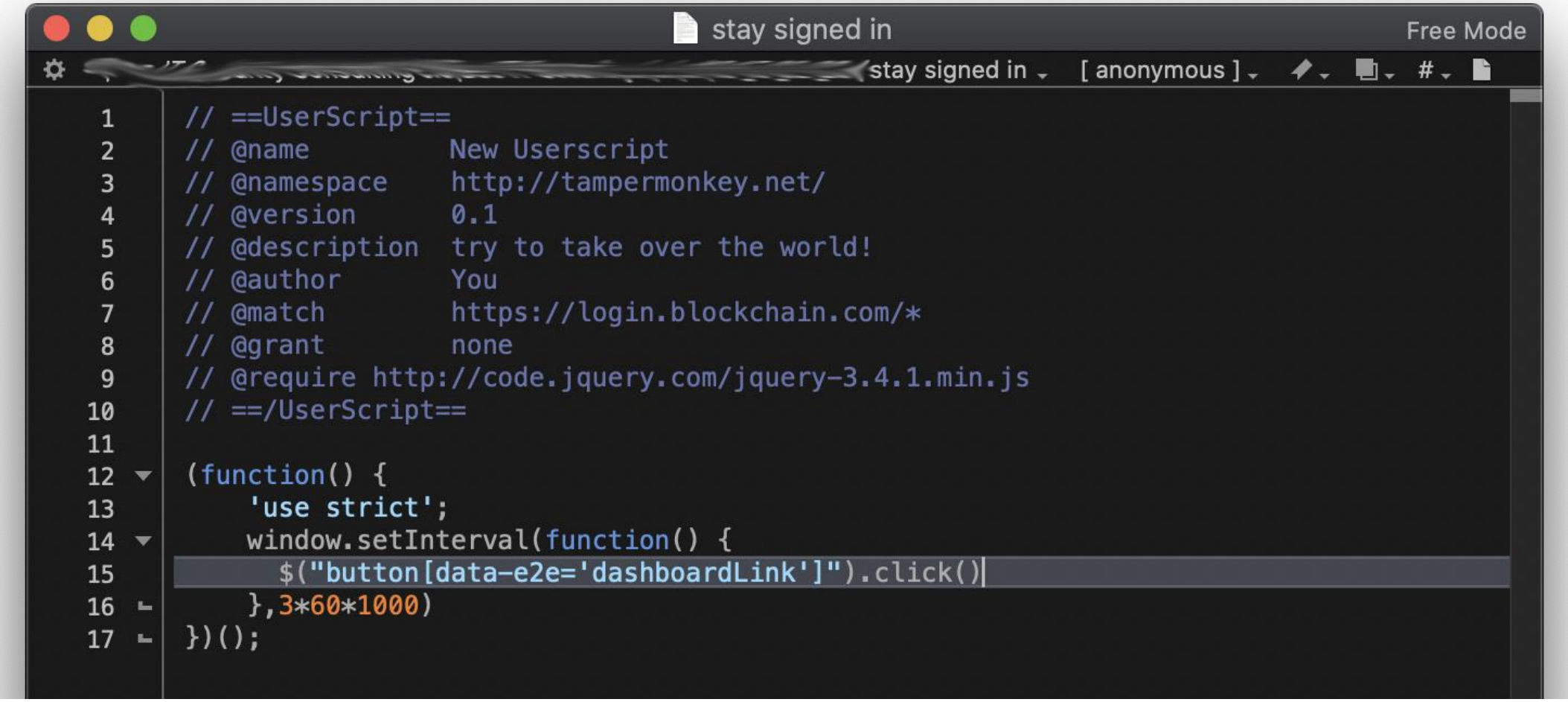
Tampermonkey To The Rescue



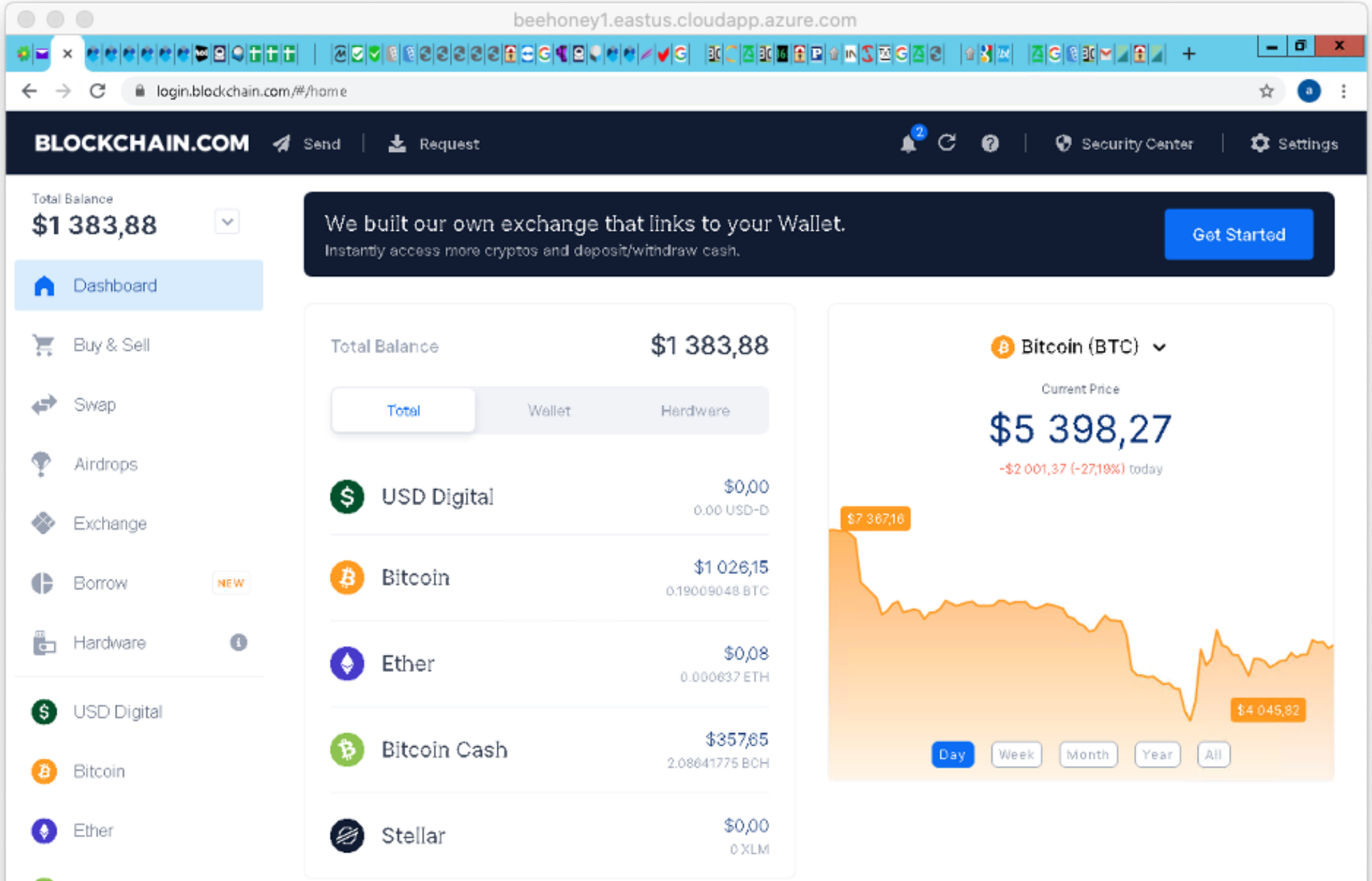
Logout Button deaktivieren

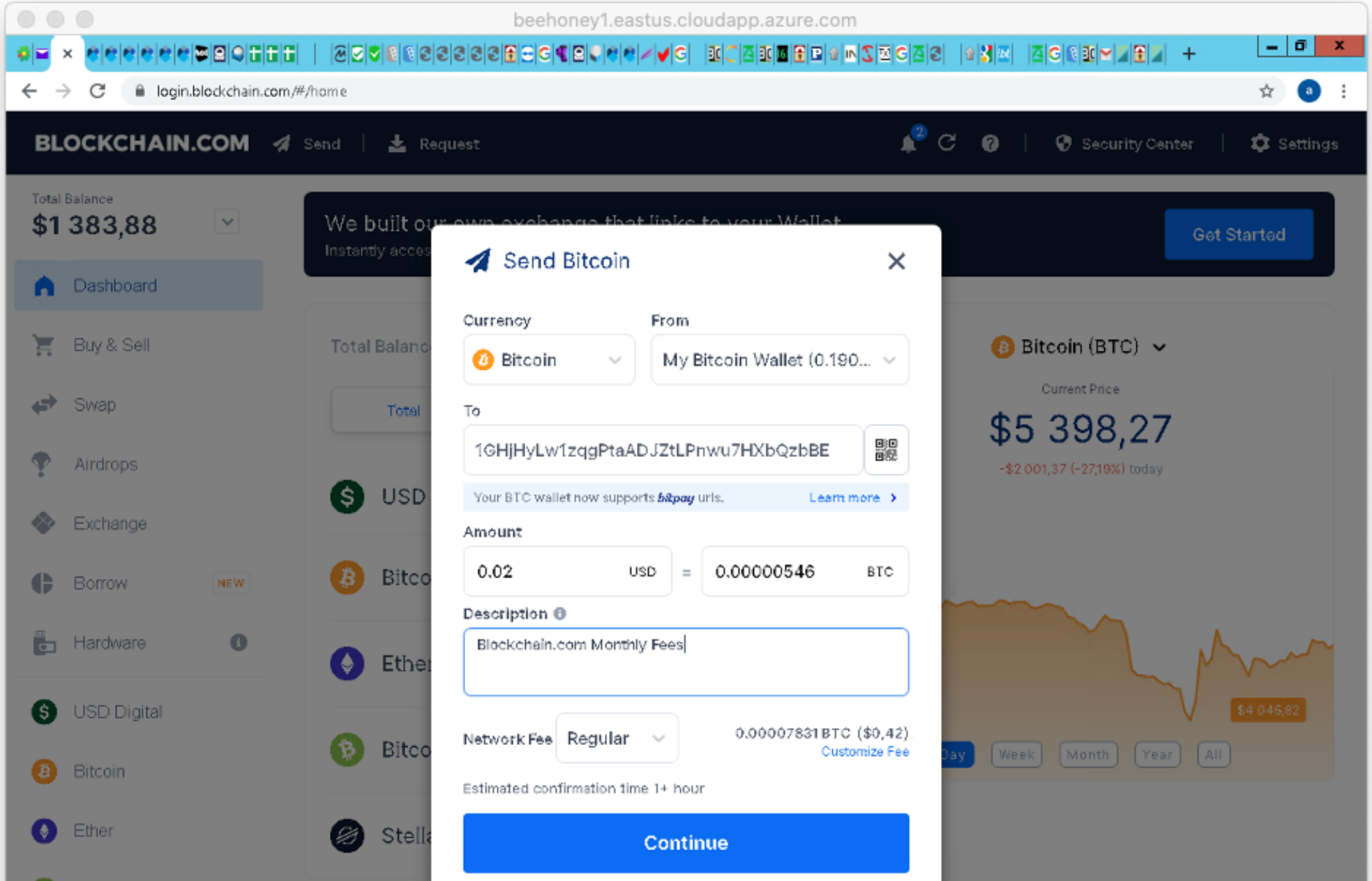
BEE ITSECURITY

Tampermonkey To The Rescue



Auto Logout deaktivieren


beehoney1.eastus.cloudapp.azure.com
login.blockchain.com/#/home
BLOCKCHAIN.COM
Send
Request
Security Center
Settings
Total Balance
$1 383,88
Dashboard
Buy & Sell
Swap
Airdrops
Exchange
Borrow
NEW
Hardware
USD Digital
Bitcoin
Ether
We built our own exchange that links to your Wallet.
Instantly access more cryptos and deposit/withdraw cash.
Get Started
Total Balance
$1 383,88
Total
Wallet
Hardware
USD Digital
$0,00
0.00 USD-D
Bitcoin
$1 026,15
0.19009048 BTC
Ether
$0,08
0.000637 ETH
Bitcoin Cash
$357,65
2.08641775 BCH
Stellar
$0,00
0 XLM
Bitcoin (BTC)
Current Price
$5 398,27
-$2 001,37 (-27,19%) today
$7 367,16
$4 045,82
Day
Week
Month
Year
All


beehoney1.eastus.cloudapp.azure.com
login.blockchain.com/#/home
BLOCKCHAIN.COM
Send
Request
Security Center
Settings
Total Balance
$1 383,88
Dashboard
Buy & Sell
Swap
Airdrops
Exchange
Borrow
NEW
Hardware
USD Digital
Bitcoin
Ether
Get Started
Send Bitcoin
Currency
Bitcoin
From
My Bitcoin Wallet (0.190...
To
1GHjHyLw1zqgPtaADJZtLPnwu7HXbQzbBE
Your BTC wallet now supports bitpay urls.
Learn more
Amount
0.02
USD
=
0.00000546
BTC
Description
Blockchain.com Monthly Fees
Network Fee
Regular
0.00007831 BTC ($0,42)
Customize Fee
Estimated confirmation time 1+ hour
Continue
Bitcoin (BTC)
Current Price
$5 398,27
-$2 001,37 (-27,19%) today
$4 045,82
Week
Month
Year
All


I'M SO RICH
BILL GATES DOES MY LAUNDRY
memegenerator.net

Wie können wir uns schützen?

Multi Faktor Authentifizierung verwenden

Benutzername und Passwort reicht heute nicht mehr aus um unsere Konten abzusichern!

RDP gehört nicht ins Internet

Es sollte immer eine entsprechende Gateway Lösung oder ein VPN vorgeschalten werden.

Unbedingt Lockout Policies einsetzen

Mit „Smart Lockouts“ bietet ADFS hier eine gute Lösung für externe Portale.

Mitarbeiter schulen

Durch Awareness Trainings lernen die Mitarbeiter wie wichtig sichere Passwörter sind

IT Systeme härten (Empfehlung: Purple Teaming)

Gefährliche Datentypen deaktivieren; Powershell einschränken, …


I am too

BEE ITSECURITY

Bee IT Security Consulting GmbH
Nibelungenstraße 37, A-3123 Schweinern

Florian Bogner
Information Security Expert

+43 660 123 9 454
florian@bee-itsecurity.at
https://www.bee-itsecurity.at