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
IT Security Expert
Speaker und Trainer
Lektor für IT / IT Security

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

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

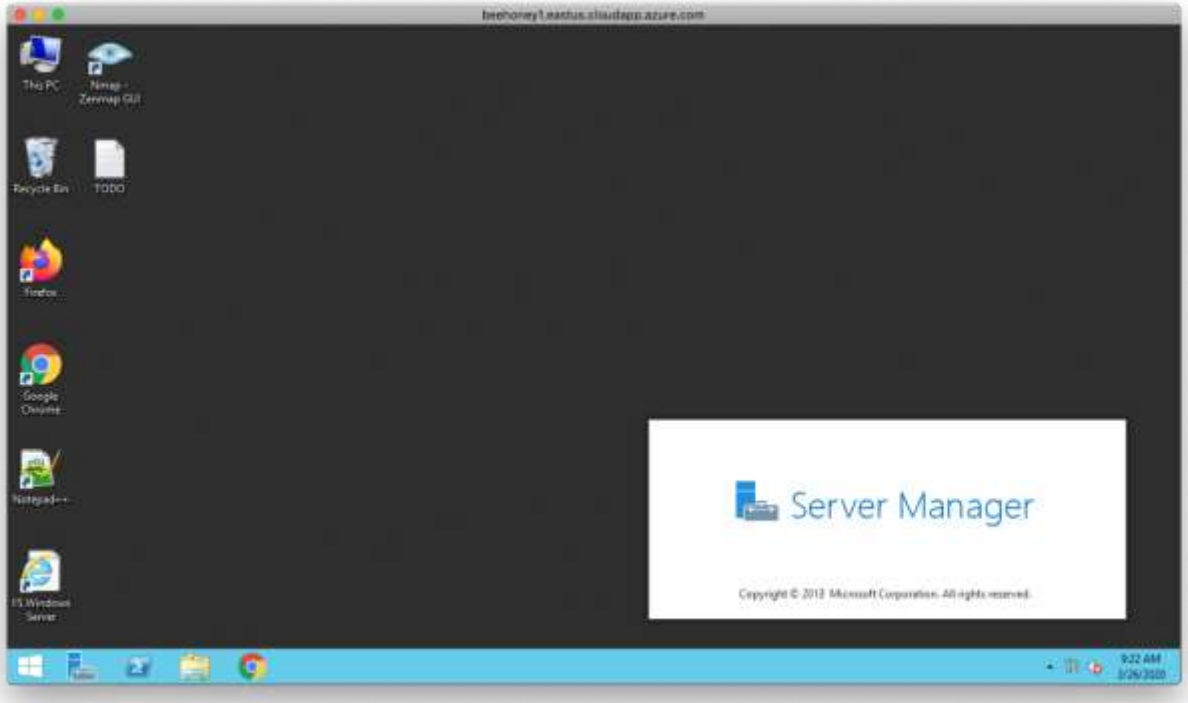
BEE ITSECURITY

Unser Honigtopf: “MXB System”

sysmon

PS Logging

Fake Content



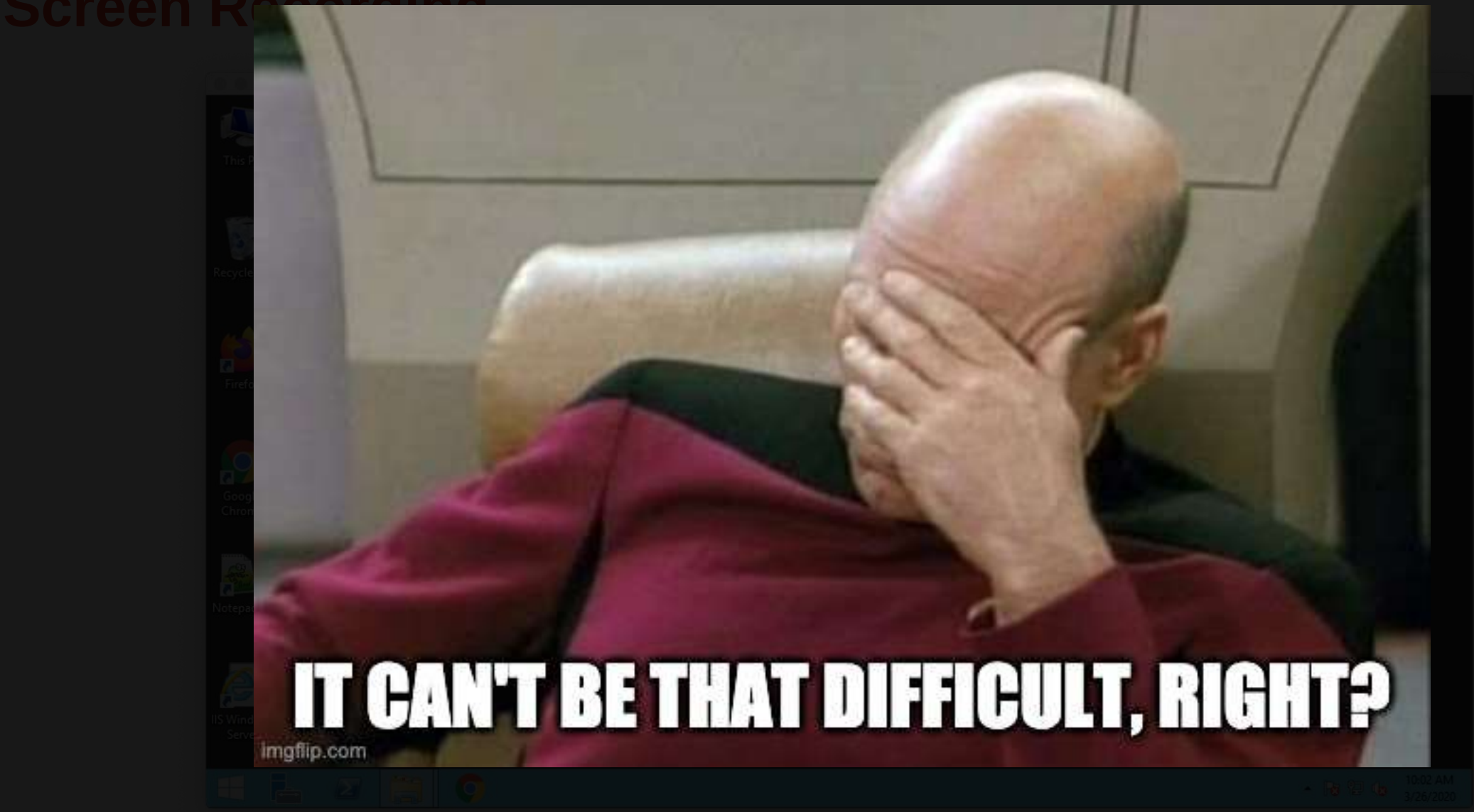
Blackcat Keylogger

Teams Notifications

FFmpeg

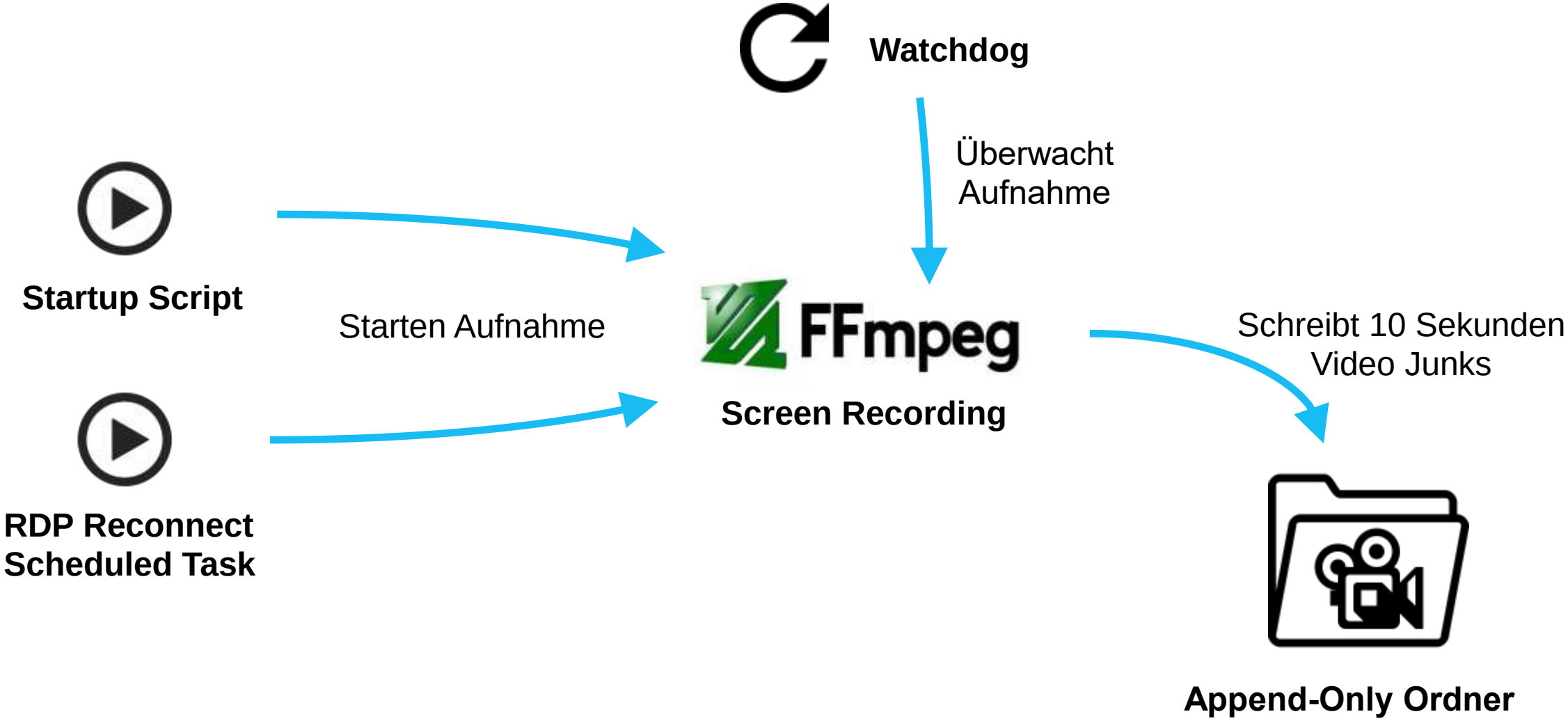
Screen Recording

Screen Recording



BEE ITSECURITY

BeeHoney Screen Recording



BEE ITSECURITY

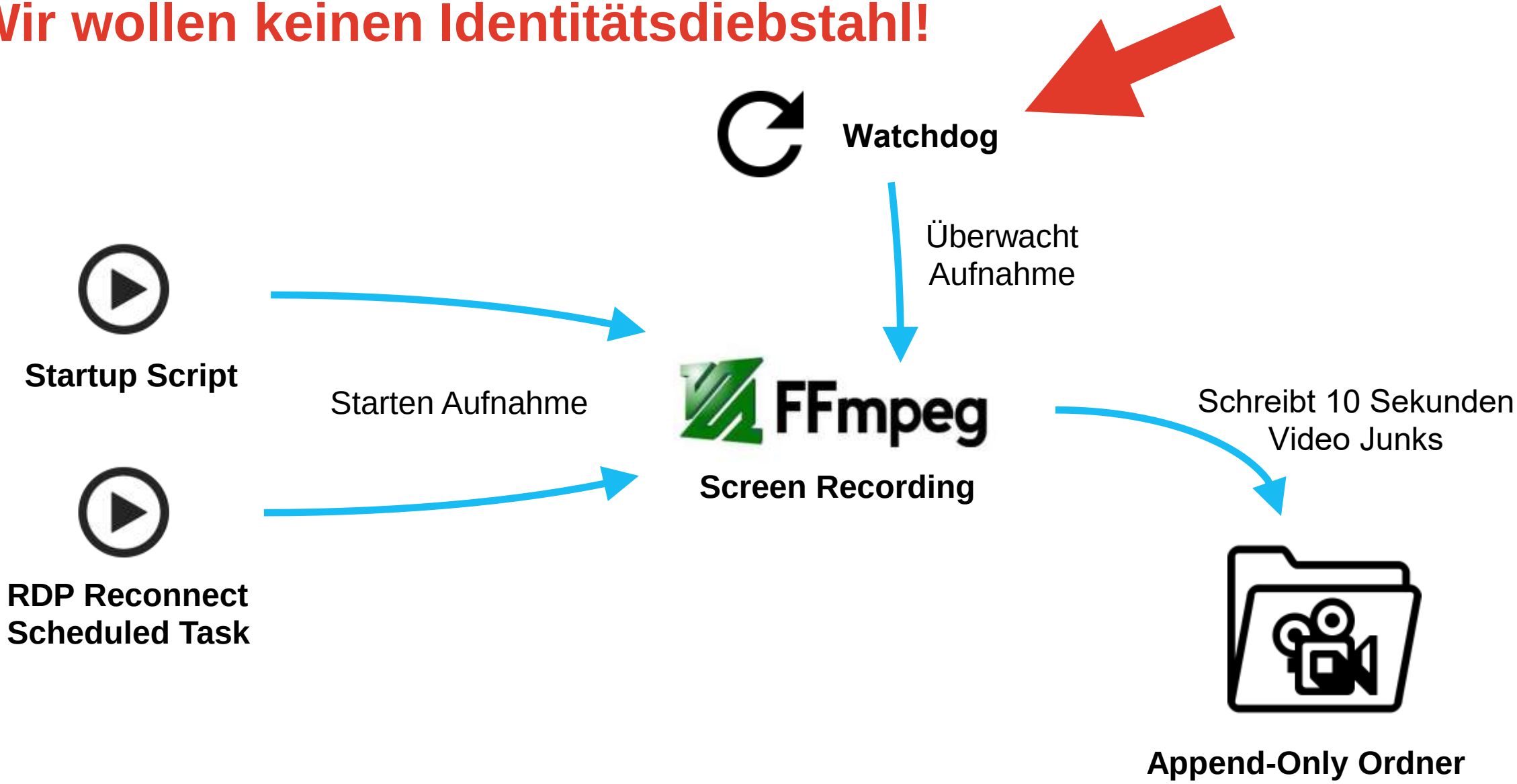
Erster Akt:
Credential Abuse

★ ★ ★ ★ ★


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

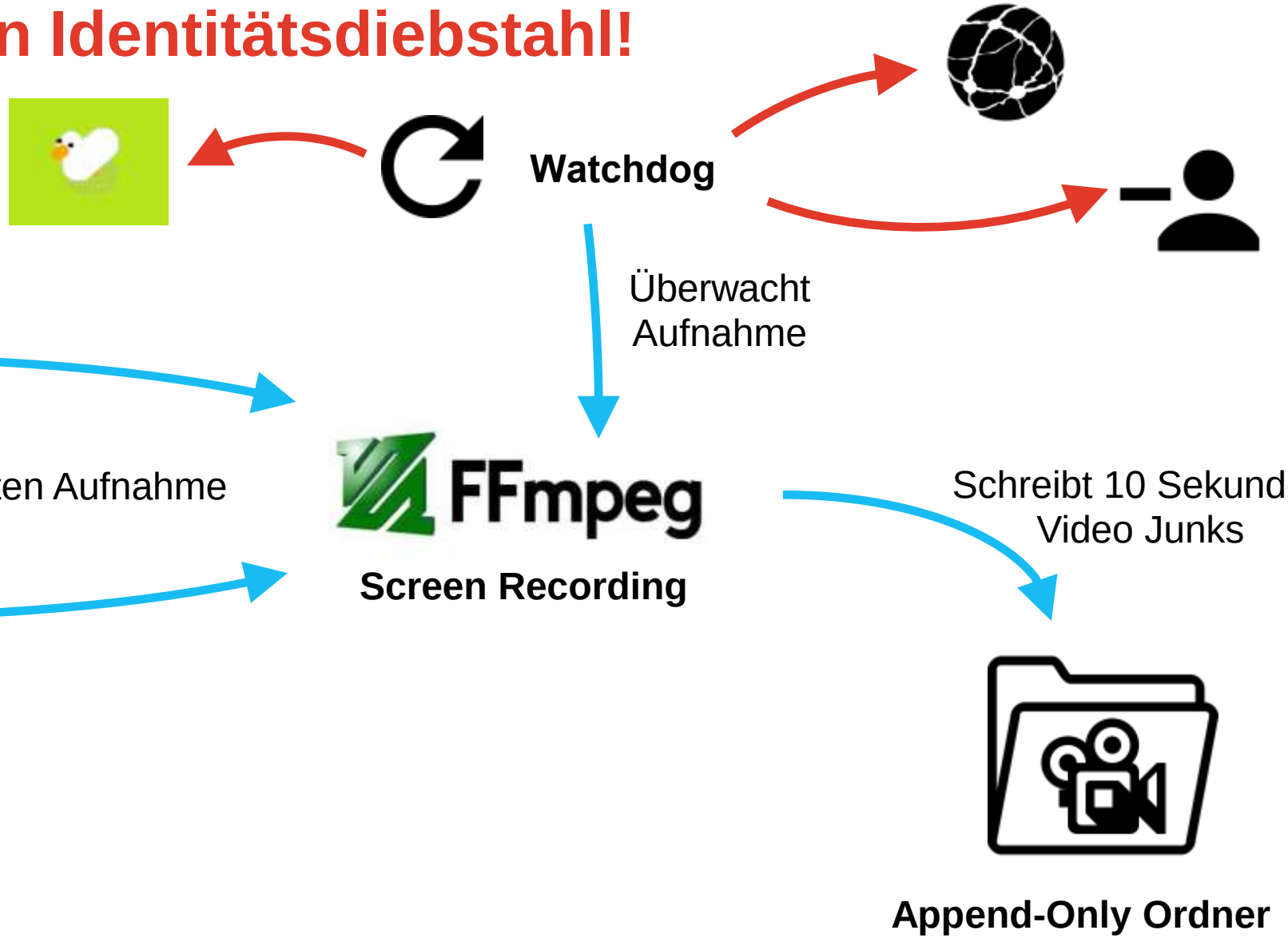
BEE ITSECURITY

Wir wollen keinen Identitätsdiebstahl!



BEE ITSECURITY

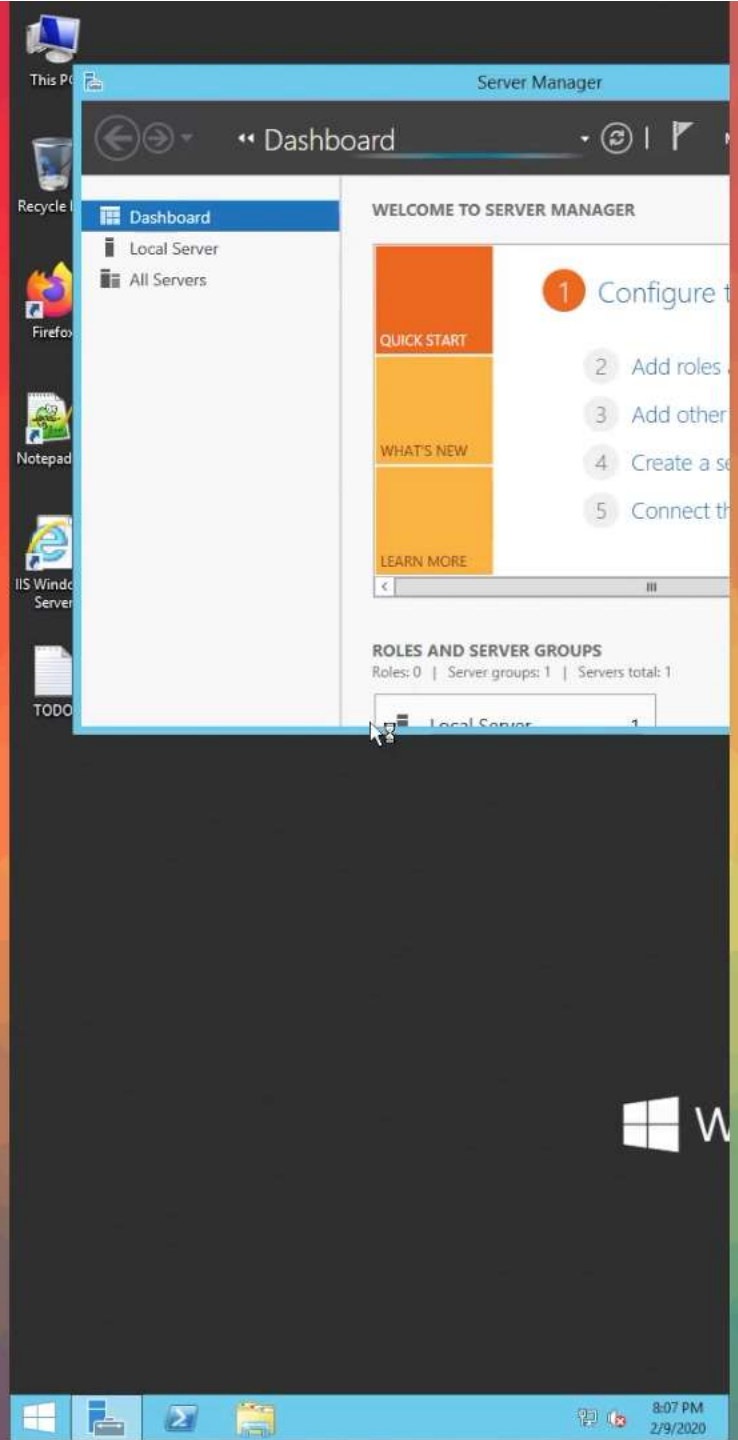
Wir wollen keinen Identitätsdiebstahl!



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 s
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”

★ ★ ★ ★ ★

Zweiter Akt:
„Cryptolocker“

TOO BE CONTINUED…

★ ★ ★ ★ ★