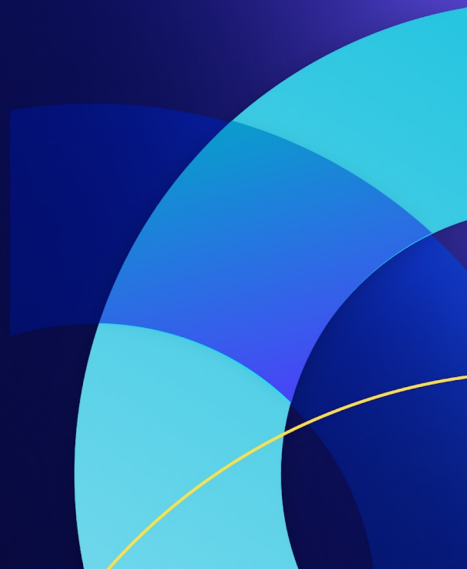
Do This, Not That

Lessons from 7 Headline Grabbing Security Breaches

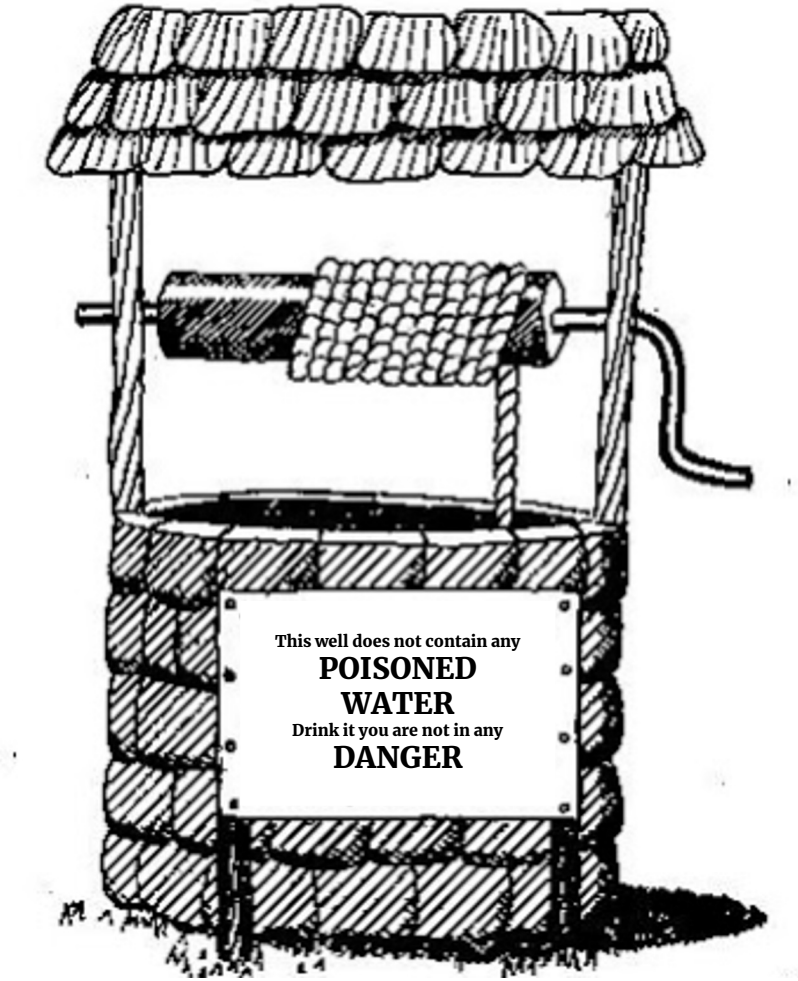
Maya Levine,
Product Manager



sysdig

Cloud vs On Premise Threats and Breaches

sysdig


This well does not contain any
POISONED
WATER
Drink it you are not in any
DANGER

Supply Chain Compromise via Malicious Image Distribution

awsmarketplace

AMI

EC2

Windows Server 2008

sysdig

Supply Chain Compromise via Malicious Image Distribution

WHY

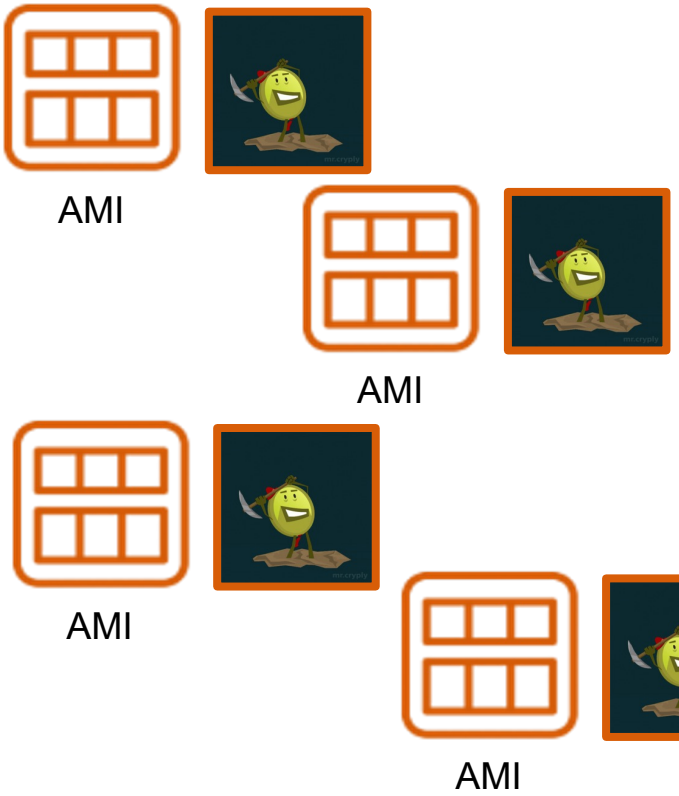
Supply Chain Compromise via Malicious Image Distribution

WHY

sysdig

Supply Chain Compromise via Malicious Image Distribution

IMPACT



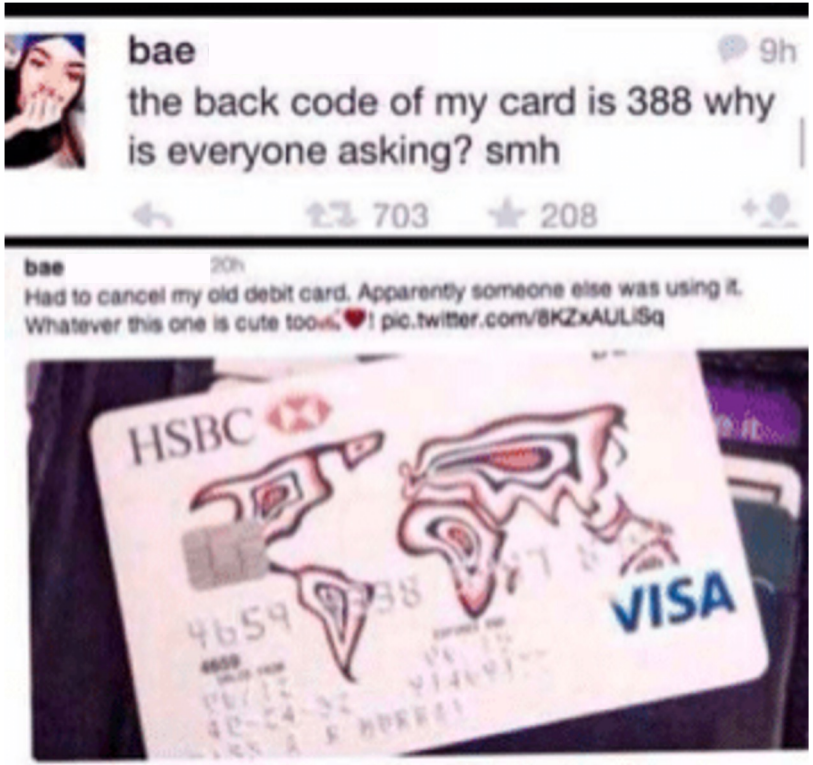
sysdig

Supply Chain Compromise via Malicious Image Distribution

TAKEAWAY

- Trusted Sources Only
- Static and Runtime Security Tools


bae
9h
Finally got my debit card! Love the blue .
4060 6860 1171 21
4060
03/17
DEBIT
VISA
ALYSSA R ALCANTAR
753
228


bae
9h
the back code of my card is 388 why is everyone asking? smh
703
208
bae
20h
Had to cancel my old debit card. Apparently someone else was using it. Whatever this one is cute too! pic.twitter.com/8KZxAULiSq
HSBC
4659
VISA

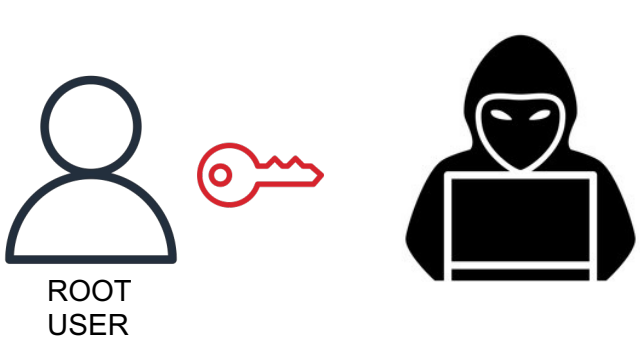
sysdig

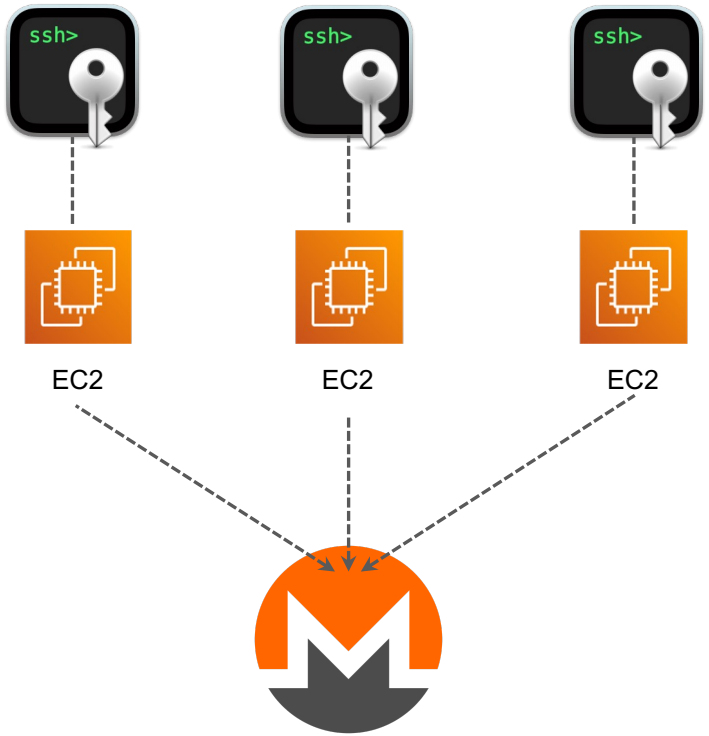
Fred 1 Dec

My new credit card came in yay! And the security code is just like my birthday 527 #RichB pic.twitter.com/d5lW0NZ9OP

Retweeted by Debit Card

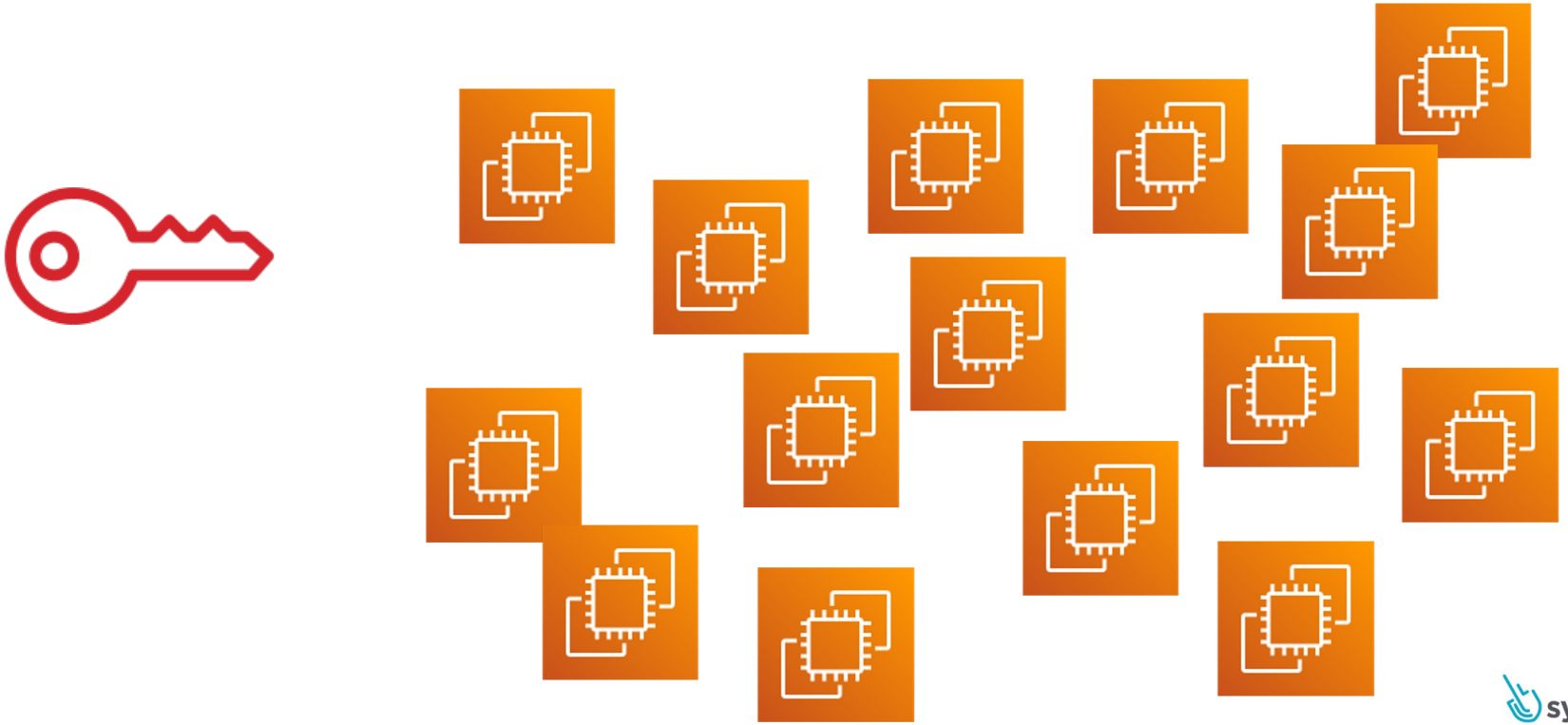
Cryptojacking via Compromised Credentials





sysdig

Cryptojacking via Compromised Credentials
WHY or IMPACT



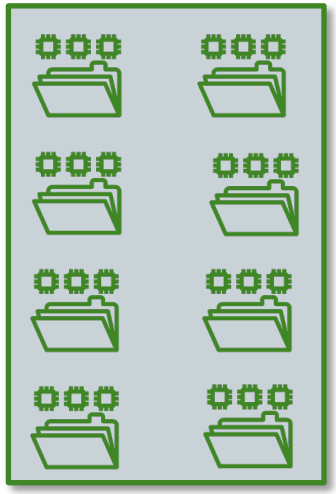
sysdig

Cryptojacking via Compromised Credentials
TAKEAWAY

- Secrets Management
- **Real Time** Monitoring

sysdig

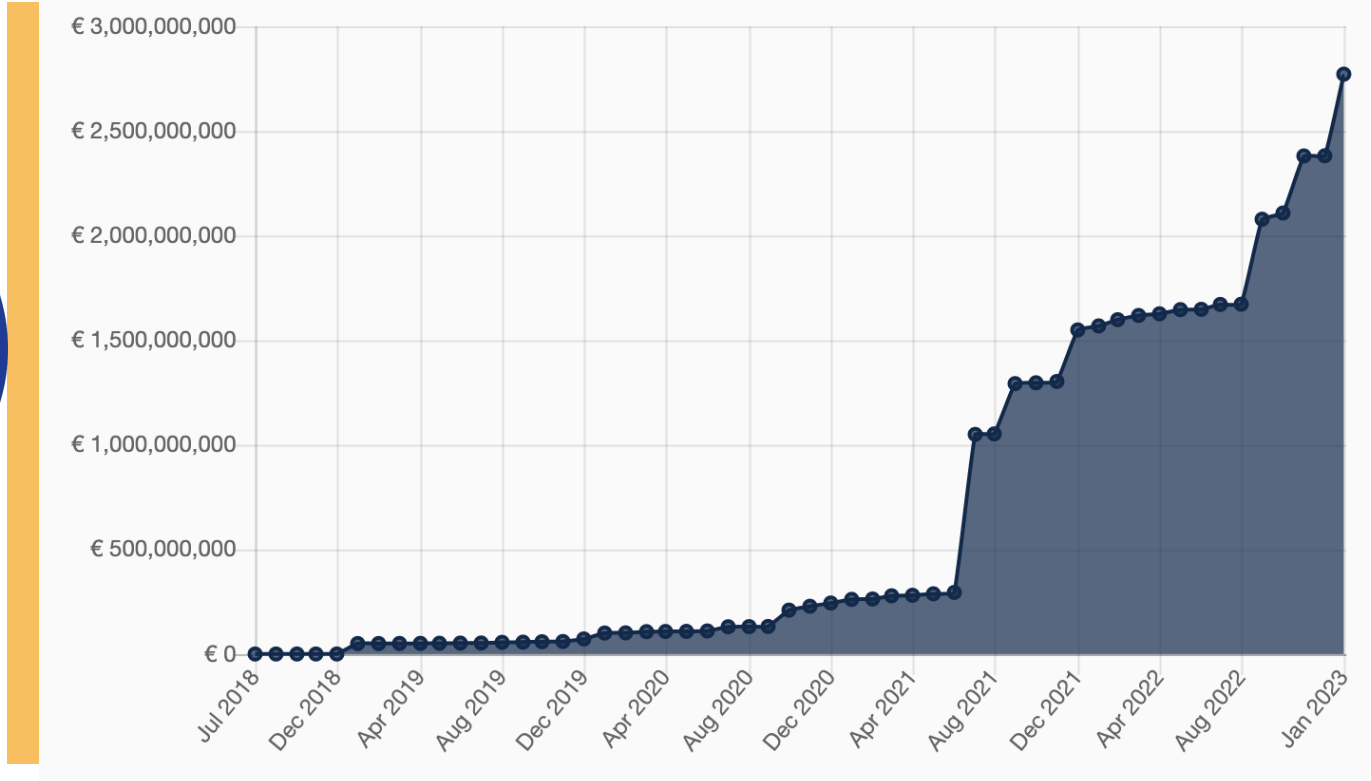
Cloud Ransomware Extortion



Cloud Ransomware Extortion
WHY

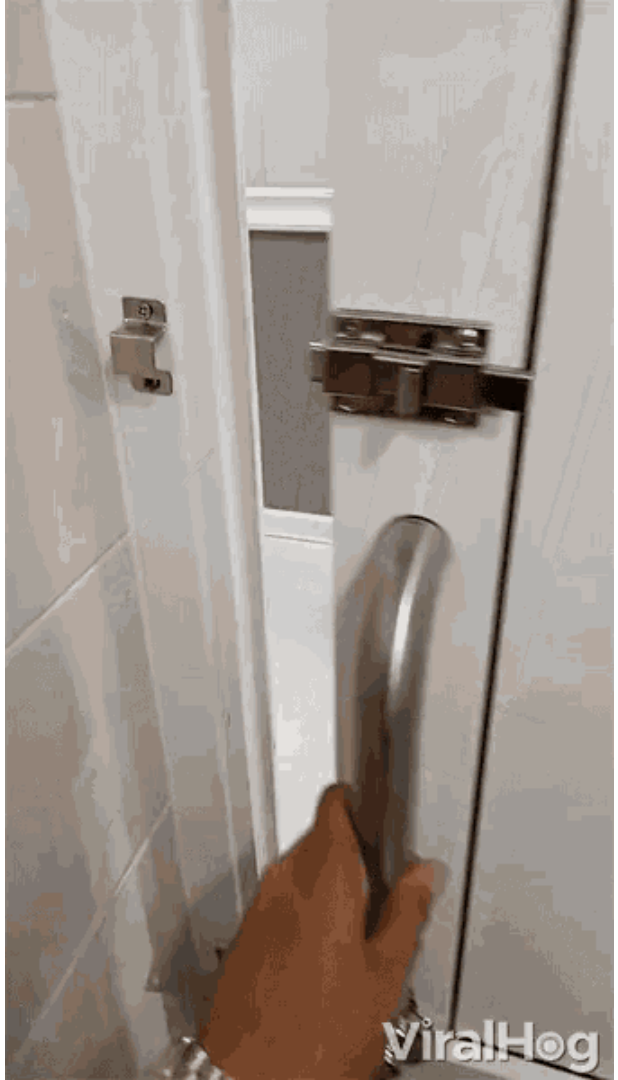
"Action": "s3:*"

Cloud Ransomware Extortion
IMPACT



Cloud Ransomware Extortion
TAKEAWAY

- Proper Vulnerability Management
- Waiting for Patch? Mitigating Controls
- Overly Permissive is a Boon to Attackers



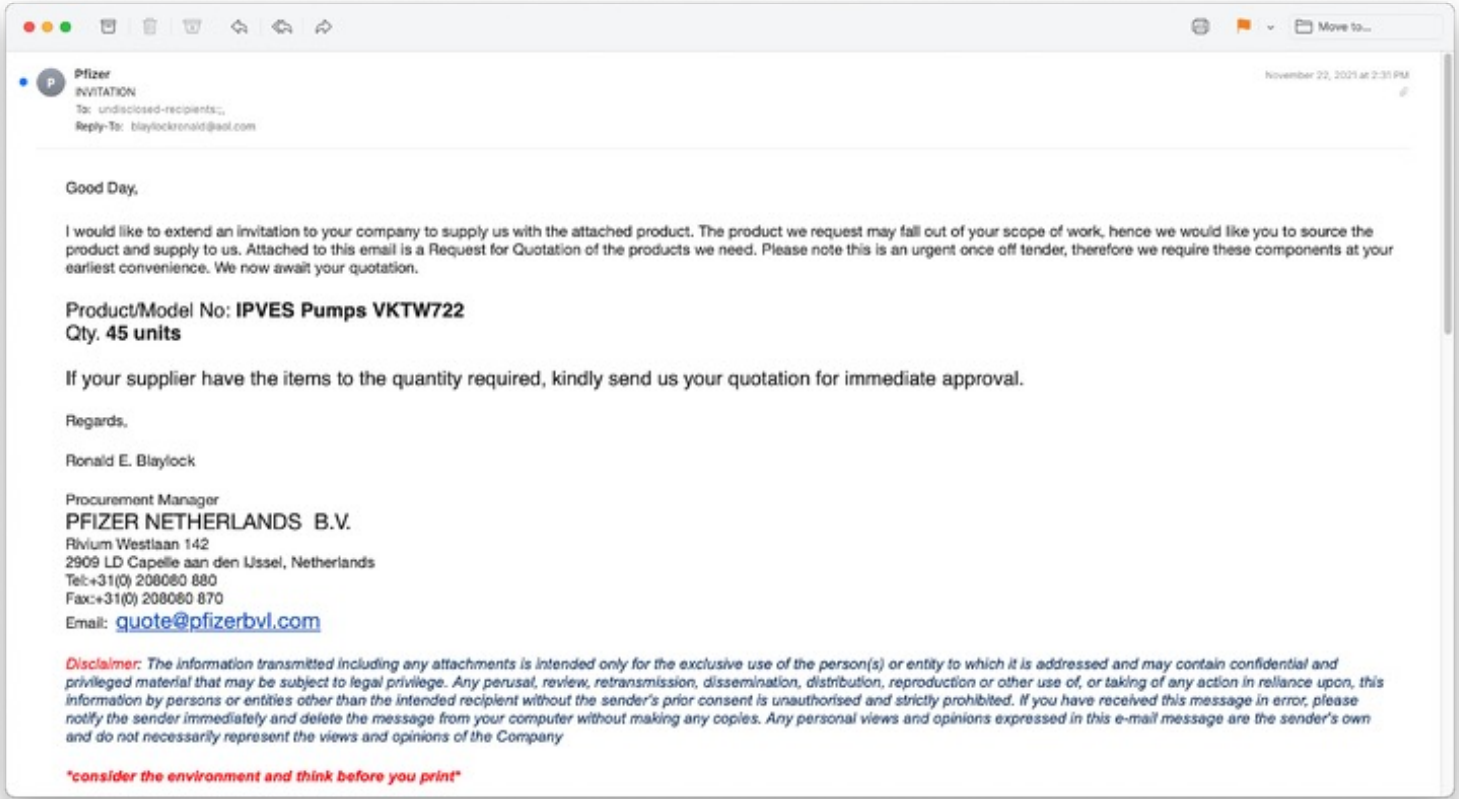
sysdig

Data Leak via Misconfigured Object Storage

Reporter Name & Contact (Reporter is the individual reporting the event, not the person completing this form) **NOTE: If reporter information is available to vendor/sub-vendor but not able to be shared please note 'IN CONFIDENCE' in Name field**	**Patient Date of Birth:** **Name:** [redacted] **Address** (minimum information required is the Country of Reporter): [redacted] **Valley Forge, PA, 19446, USA** **Email: xxx** **Telephone No: +17**[redacted]	Did reporter consent to further follow-up? **Unknown**
Verbatim and Event Description (Describe the adverse experience (AE)/beneficial effect/at risk including all pertinent information **If death is reported please inquire about the cause of death and note on this report**	**Provide clear narrative description, as provided by the reporter, of the sequence of event(s), diagnosis, treatment, (including dates), and any other relevant details. Include any laboratory tests and/or results provided by the reporter.** IVR: Automated message. IVR: After the beep, please say your complete mailing address including your house or apartment number, street name, city, state, and zip code. Please spell any difficult words. Go ahead. <beep> Caller: (Misplaced comments) [redacted], [redacted], Valley Forge, Pennsylvania, 19446 and I gave money to somebody to buy one of the Advil 10 tablets like a travelling size, I cannot get the lid off. I have worked and worked then I used one of those. IVR: Automated message.	

sysdig

Data Leak via Misconfigured Object Storage
IMPACT



Pfizer
INVITATION
To: undisclosed-recipients:;
Reply-To: blaylockronald@aol.com

November 22, 2021 at 2:31 PM

Good Day,

I would like to extend an invitation to your company to supply us with the attached product. The product we request may fall out of your scope of work, hence we would like you to source the product and supply to us. Attached to this email is a Request for Quotation of the products we need. Please note this is an urgent once off tender, therefore we require these components at your earliest convenience. We now await your quotation.

Product/Model No: **IPVES Pumps VKTW722**
Qty. **45 units**

If your supplier have the items to the quantity required, kindly send us your quotation for immediate approval.

Regards,

Ronald E. Blaylock

Procurement Manager
PFIZER NETHERLANDS B.V.
Rivium Westlaan 142
2909 LD Capelle aan den IJssel, Netherlands
Tel:+31(0) 208080 880
Fax:+31(0) 208080 870
Email: quote@pfizerbvl.com

Disclaimer: The information transmitted including any attachments is intended only for the exclusive use of the person(s) or entity to which it is addressed and may contain confidential and privileged material that may be subject to legal privilege. Any perusal, review, retransmission, dissemination, distribution, reproduction or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient without the sender's prior consent is unauthorised and strictly prohibited. If you have received this message in error, please notify the sender immediately and delete the message from your computer without making any copies. Any personal views and opinions expressed in this e-mail message are the sender's own and do not necessarily represent the views and opinions of the Company

consider the environment and think before you print

sysdig

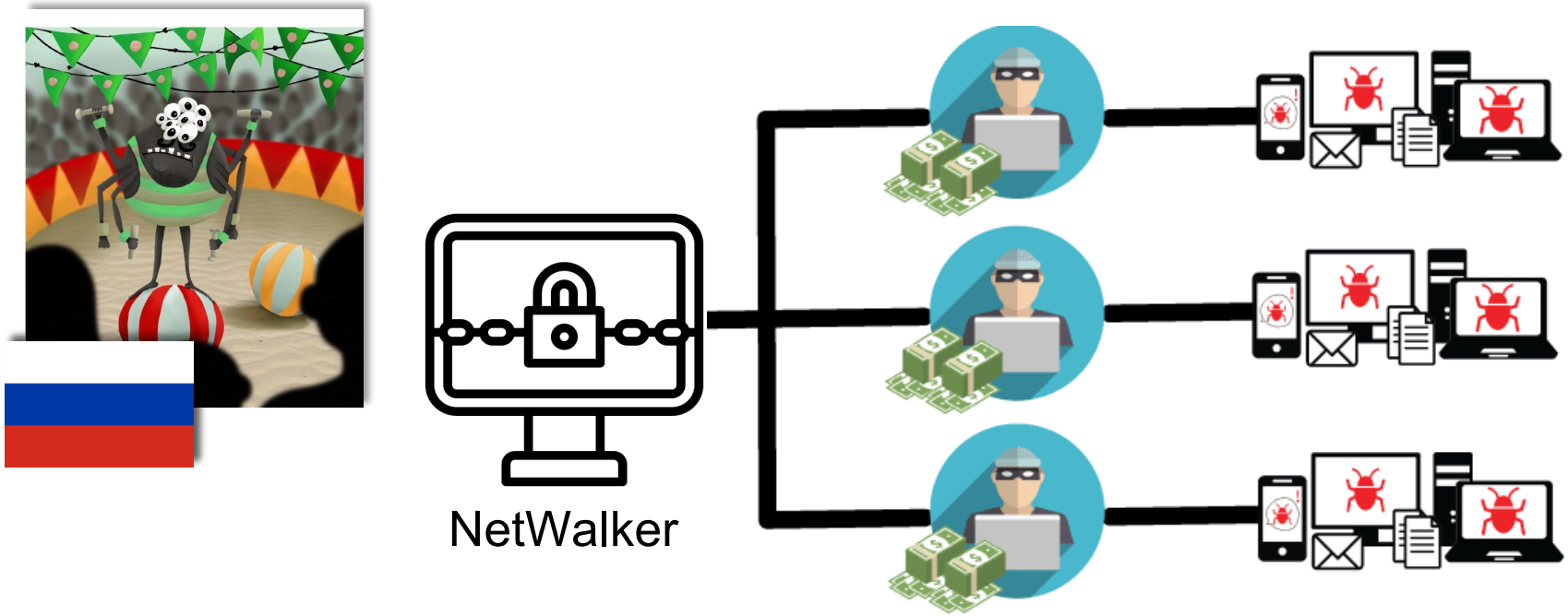
Data Leak via Misconfigured Object Storage
TAKEAWAY

- Make buckets private and add authentication protocols
- Refrain from logging sensitive customer data if possible

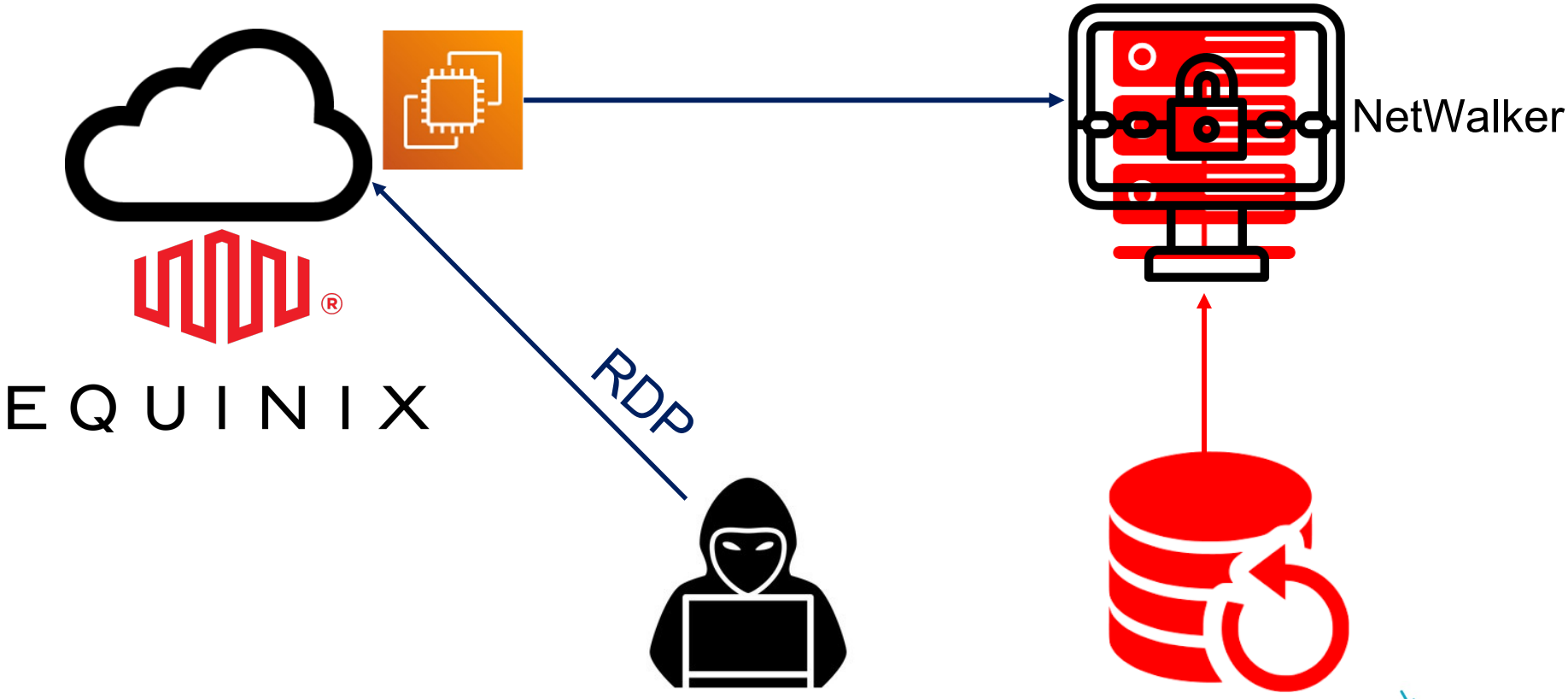
If not…encrypt!


HBOmax
PIVOT!

On Premise Ransomware via Pivot from Cloud



On Premise Ransomware via Pivot from Cloud

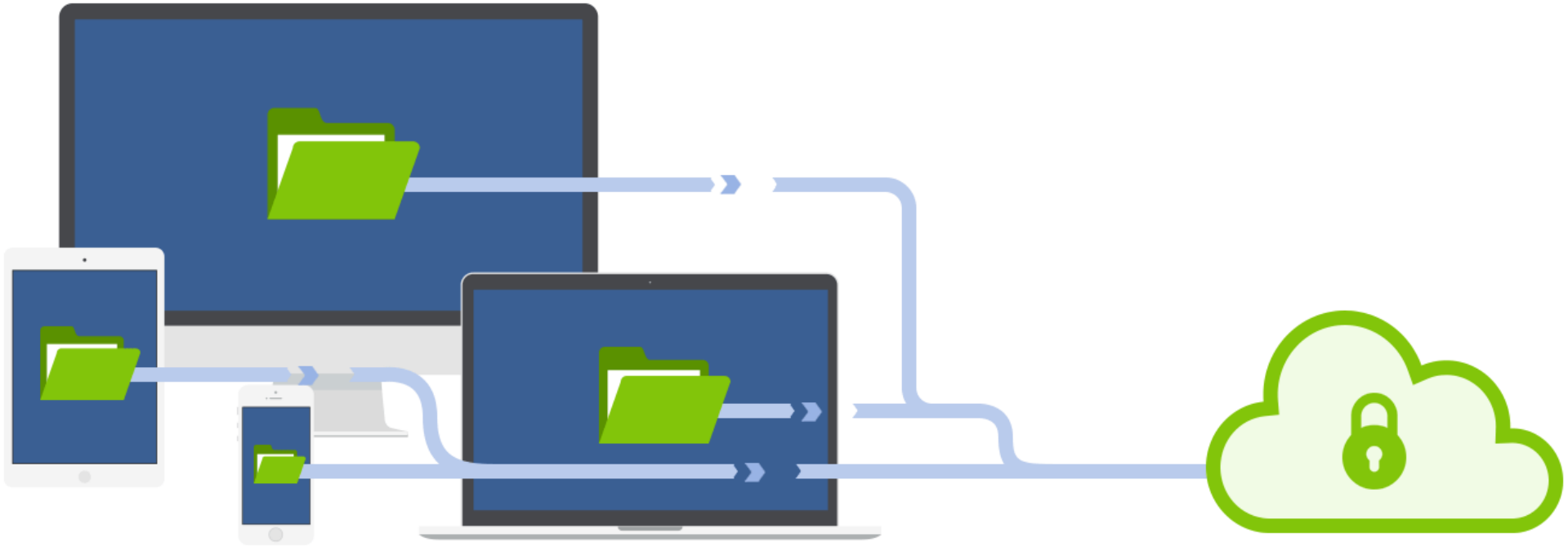


sysdig

On Premise Ransomware via Pivot from Cloud
WHY

sysdig

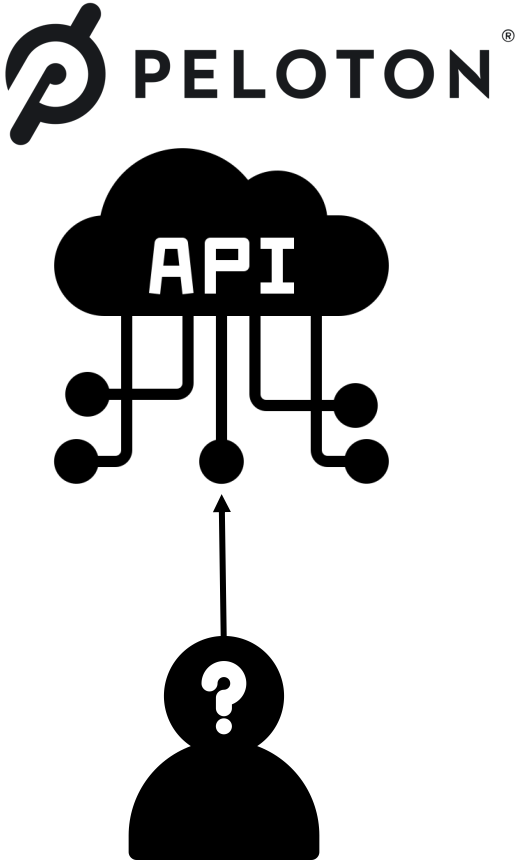
On Premise Ransomware via Pivot from Cloud
IMPACT



On Premise Ransomware via Pivot from Cloud
TAKEAWAY

- Inventory of Cloud Assets
- Security Policies Applied to all Systems
- Backup (So You Don’t Pay Up)

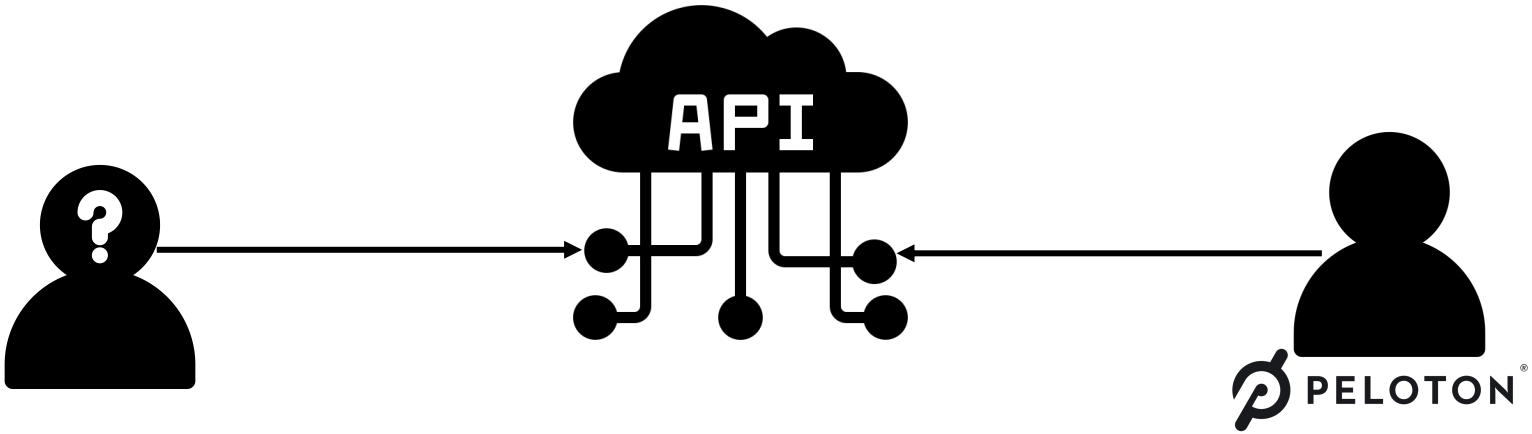
Data Exfiltration via Unauthenticated API Request




```
"ae[redacted]":{
  "age":41,
  "age_group":"40s",
  "avatar":"https://s3.amazonaws.com/peloton-profile-images/[redacted]
  "gender":"female",
  "short_gender":"F",
  "is_birthday":false,
  "is_digital":false,
  "is_profile_private":true,
  "location":"Maryland",
  "nth_workout":2,
  "start_time":1612526841,
  "user_id":"6[redacted]",
  "username":"Stj[redacted]",
  "workout_id":"ael[redacted]",
  "is_live":true,
  "bike_number":null,
  "is_studio":false,
  "peloton_id":"a6[redacted]",
  "peloton_start_time":1612525884,
  "tags_info":{
    "primary_name":"[redacted]",
    "total_joined":3
  },
  "authed_user_follows":null
```

Data Exfiltration via Unauthenticated API Request

WHY



Data Exfiltration via Unauthenticated API Request
IMPACT

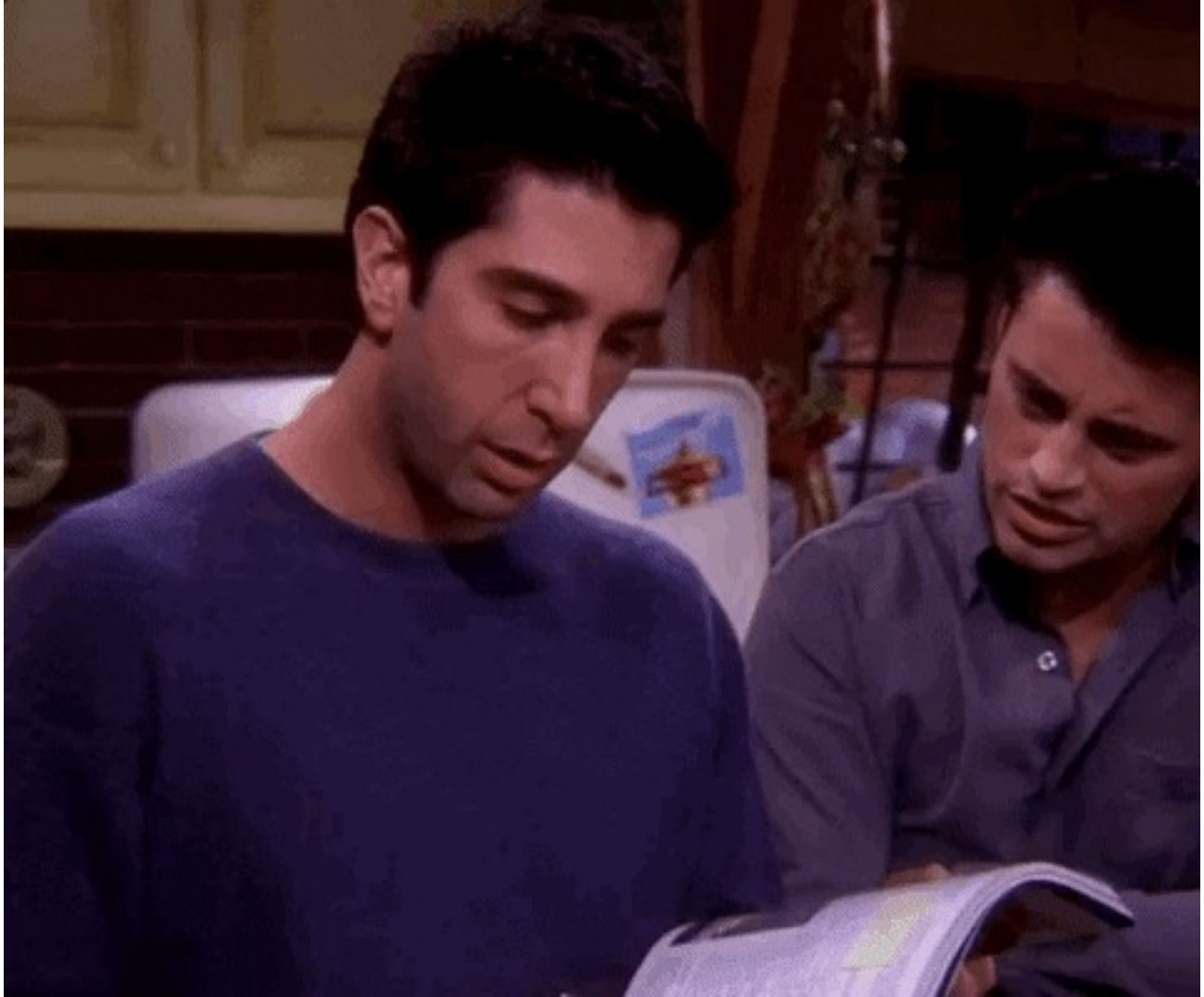
Information disclosed included:
– User IDs
– Instructor IDs
– Group Membership
– Location
– Workout stats
– Gender and age
– If they are in the studio or not

sysdig

Data Exfiltration via Unauthenticated API Request
TAKEAWAY

- Secure Coding Practices in Development Process
- API Security Tools

sysdig

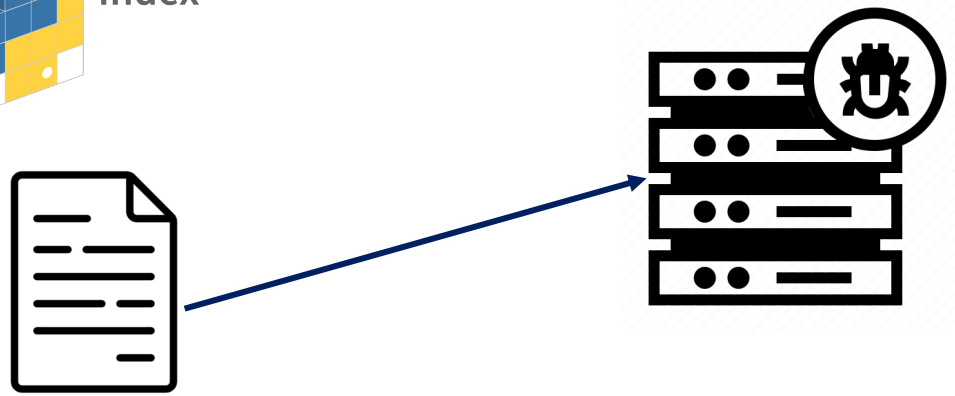


sysdig

Supply Chain Compromise of Open Source Software

PyTorch

python™ Package Index



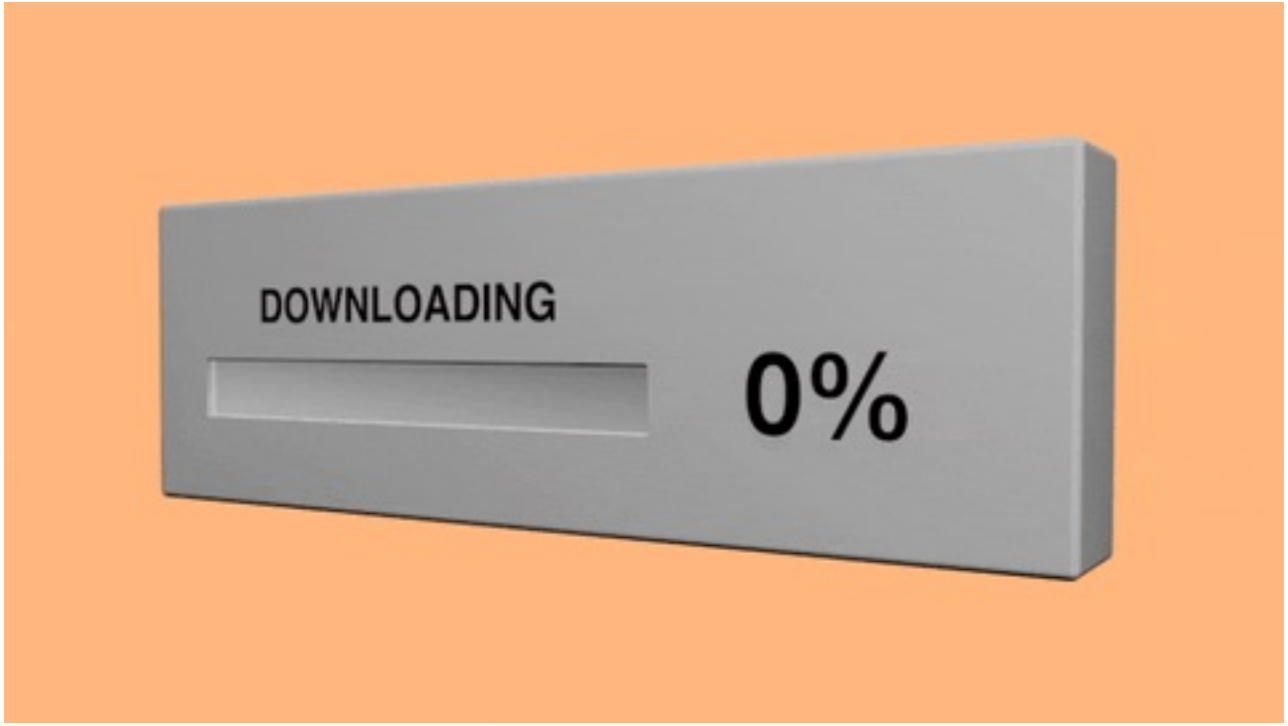
torchtriton 3.0.0

sysdig

Supply Chain Compromise of Open Source Software
WHY

sysdig

Supply Chain Compromise of Open Source Software
IMPACT



sysdig

Supply Chain Compromise of Open Source Software
TAKEAWAY

- No Blind Trust
- Trust But Verify
- Shift Left

High Level Trends in Cloud Attacks & Defenses

Cryptomining will get more popular

SCALE

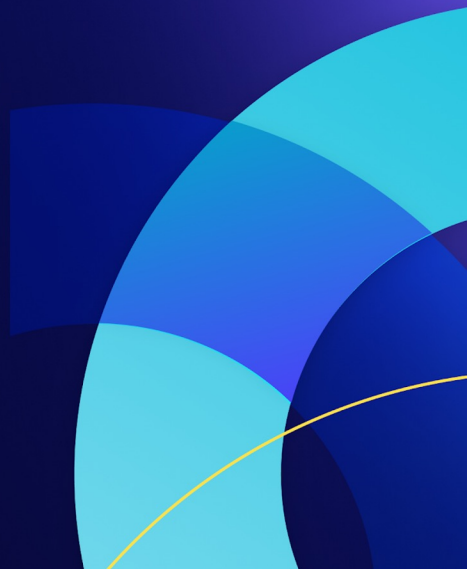
Selling of Malware on Dark Web makes advanced attacks accessible

Supply chain compromises – devastating effects

How to Cope:

- Visibility – Real Time
- Least Permissive
- Backups

Thank You!



sysdig