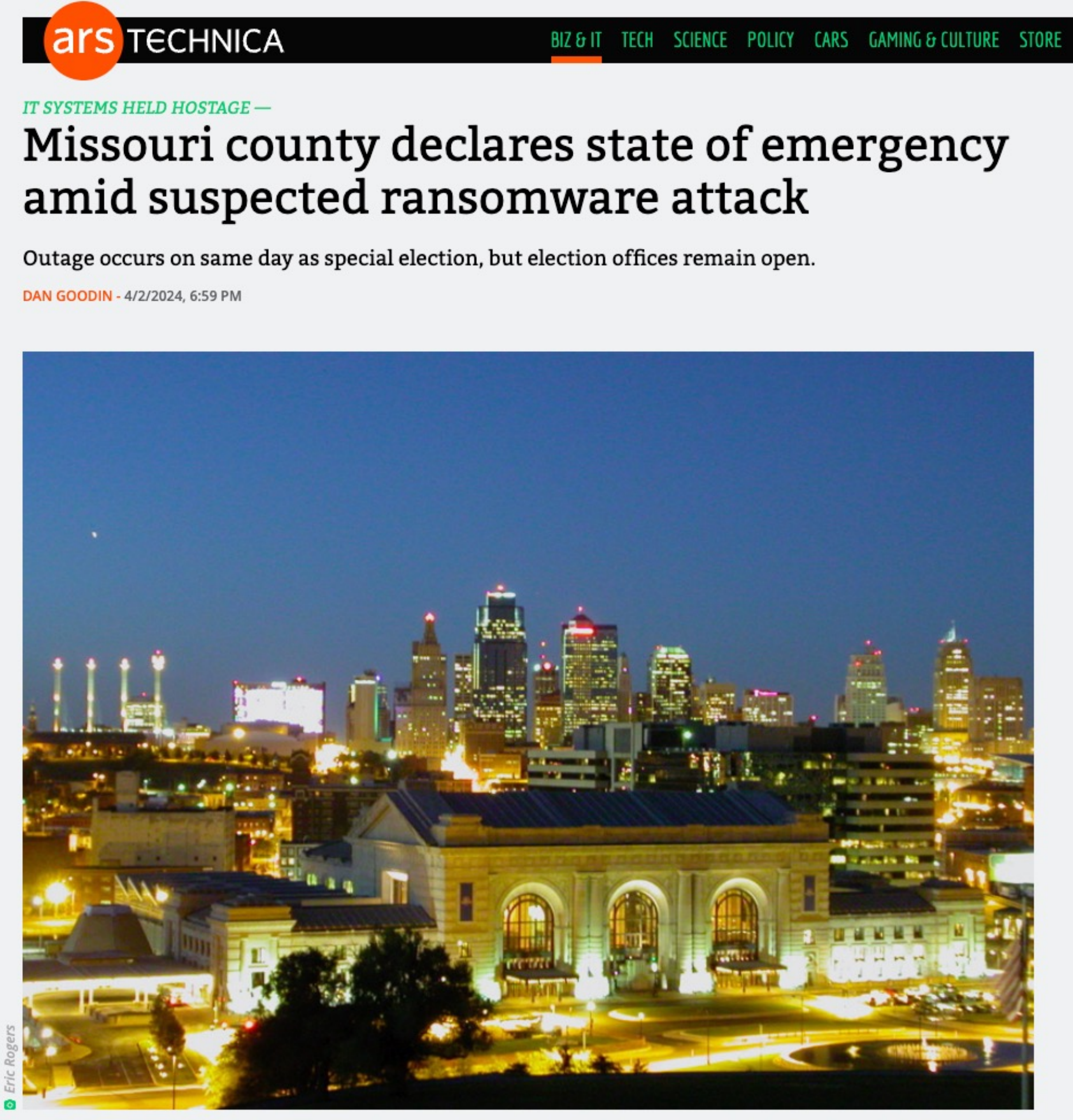
Defeating Ransomware

How a small university beat defeated a ransomware gang

Aaron Weissenfluh
Tenfold Security

aaron@tenfoldsecurity.com

Current Events



IT SYSTEMS HELD HOSTAGE —

Missouri county declares state of emergency amid suspected ransomware attack

Outage occurs on same day as special election, but election offices remain open.

DAN GOODIN - 4/2/2024, 6:59 PM

Agenda

- Timeline of events
- Challenges
- Winning moves
- Today

University of Education

You Really Want to be Here

Disclaimers

- Simple solutions
- Condensed
- Redacted

Roster

University Staff

- 1 Senior systems administrator
- 1 Systems administrator (vacation)
- 2 Helpdesk
- *1 Junior helpdesk
- 1 Database administrator – remote (4-6 hour drive)
- 1 Director of IT

Friday
5 August 2022

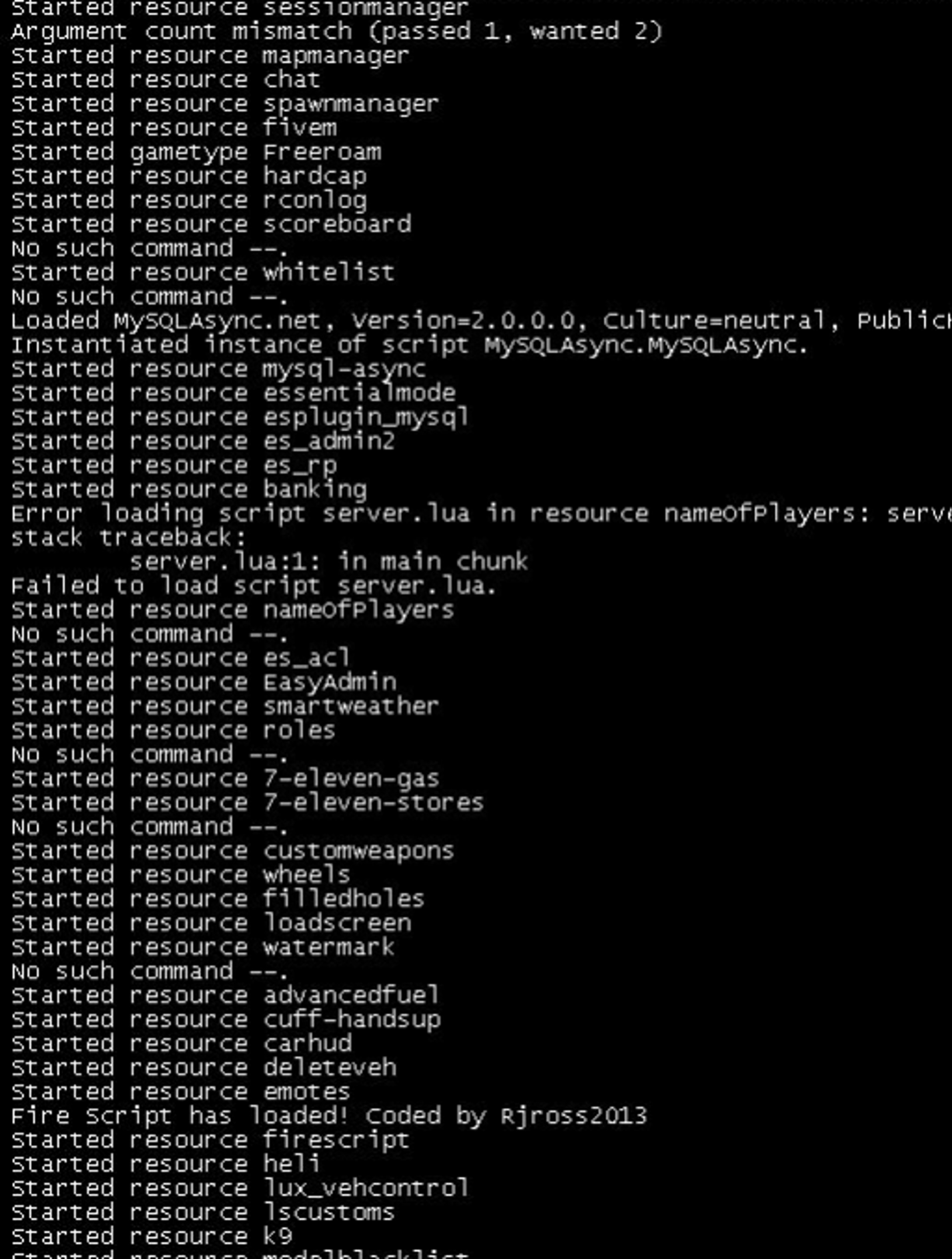
Students arrive in 10 days

Monday
8 August 2022

Students arrive in 7 days

Monday Morning

- Server issues
- Firewall logs
- Fileserver CPUs maxed
- Helpdesk tickets

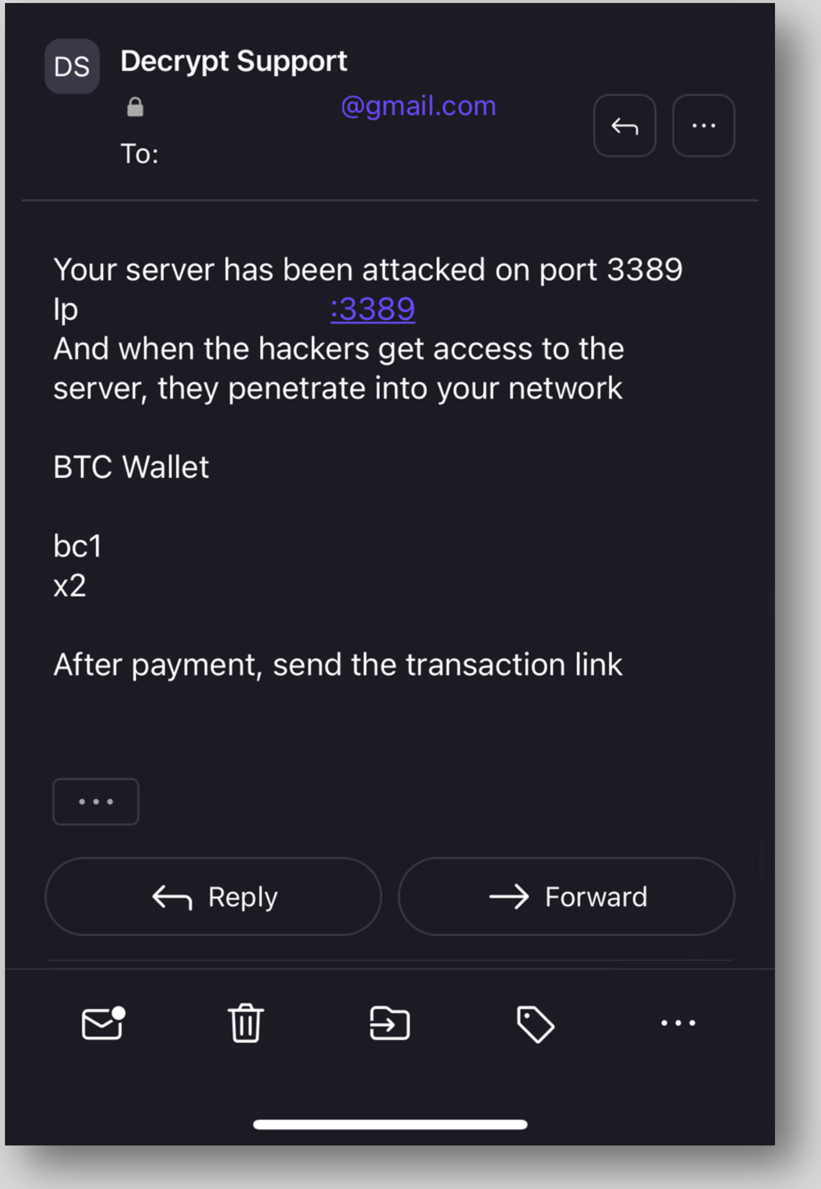


```
Started resource sessionmanager
Argument count mismatch (passed 1, wanted 2)
Started resource mapmanager
Started resource chat
Started resource spawnmanager
Started resource fivem
Started gametype Freeroam
Started resource hardcap
Started resource rconlog
Started resource scoreboard
No such command --.
Started resource whitelist
No such command --.
Loaded MySQLAsync.net, Version=2.0.0.0, Culture=neutral, PublicK
Instantiated instance of script MySQLAsync.MySQLAsync.
Started resource mysql-async
Started resource essentialmode
Started resource esplugin_mysql
Started resource es_admin2
Started resource es_rp
Started resource banking
Error loading script server.lua in resource nameofPlayers: serve
stack traceback:
        server.lua:1: in main chunk
Failed to load script server.lua.
Started resource nameofPlayers
No such command --.
Started resource es_acl
Started resource EasyAdmin
Started resource smartweather
Started resource roles
No such command --.
Started resource 7-eleven-gas
Started resource 7-eleven-stores
No such command --.
Started resource customweapons
Started resource wheels
Started resource filledholes
Started resource loadscreen
Started resource watermark
No such command --.
Started resource advancedfuel
Started resource cuff-handsup
Started resource carhud
Started resource deleteveh
Started resource emotes
Fire Script has loaded! Coded by Rjross2013
Started resource firescript
Started resource heli
Started resource lux_vehcontrol
Started resource lscustoms
Started resource k9
Started resource modelblacklist
```

Tuesday
9 August 2022

Students arrive in 6 days

Initial Email



Your server has been attacked on port 3389
Ip :3389
And when the hackers get access to the server, they penetrate into your network

BTC Wallet

bc1
x2

After payment, send the transaction link

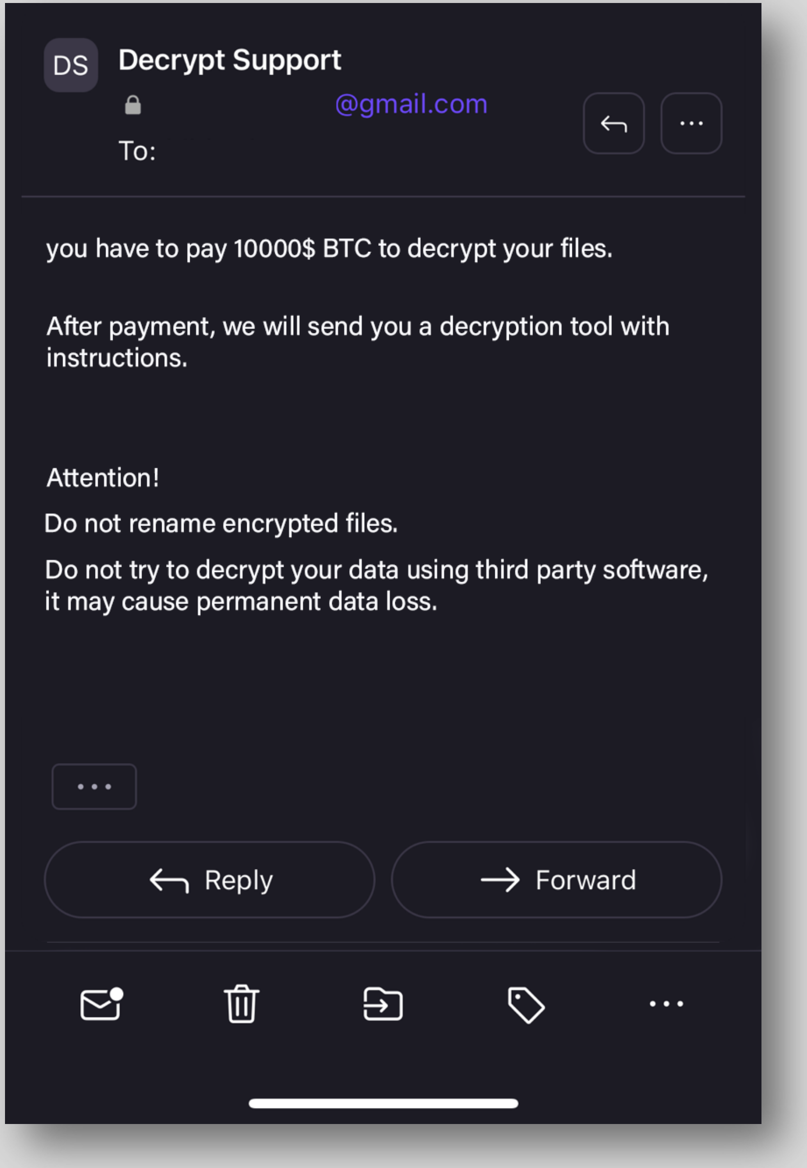
Wednesday
10 August 2022

Students arrive in 5 days

The Beginning

- The demand
- Network crawling
- Systems going offline

**Redacted to protect the adversary's identity*



you have to pay 10000$ BTC to decrypt your files.

After payment, we will send you a decryption tool with instructions.

Attention!

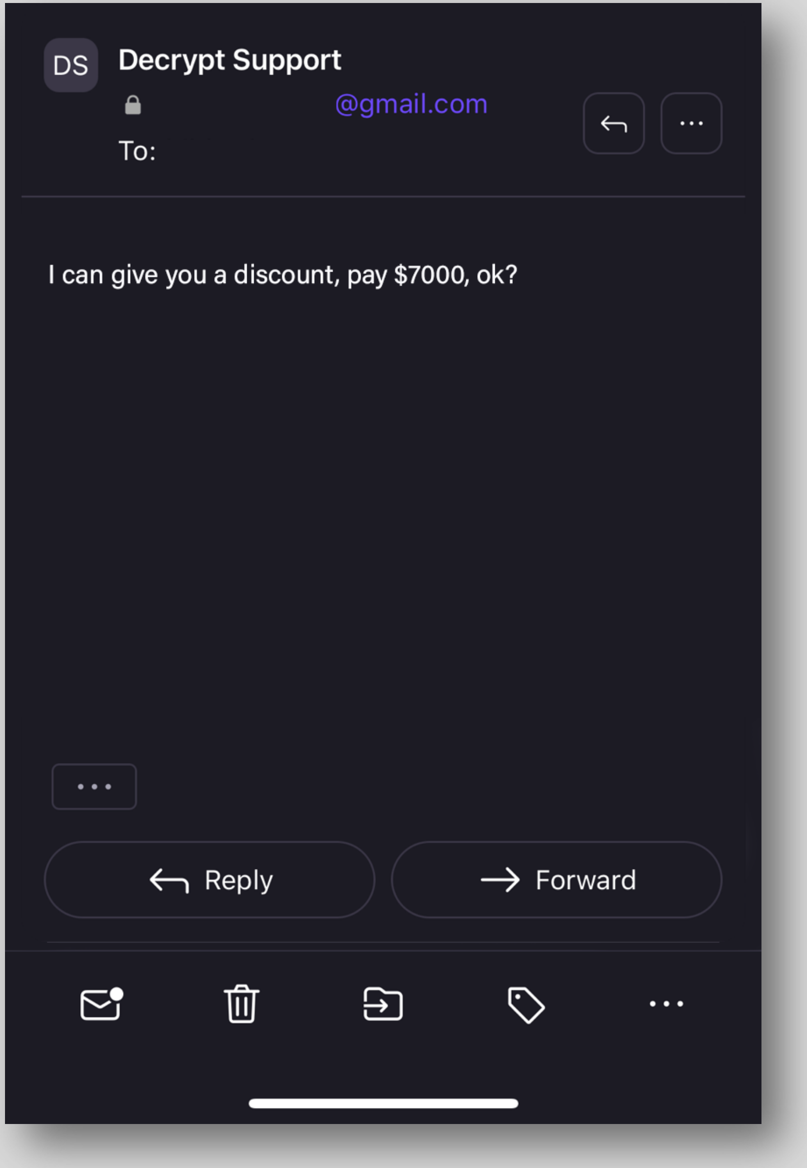
Do not rename encrypted files.

Do not try to decrypt your data using third party software, it may cause permanent data loss.

Meanwhile...

Negotiations Begin

**Redacted to protect the adversary's stupidity/inexperience*

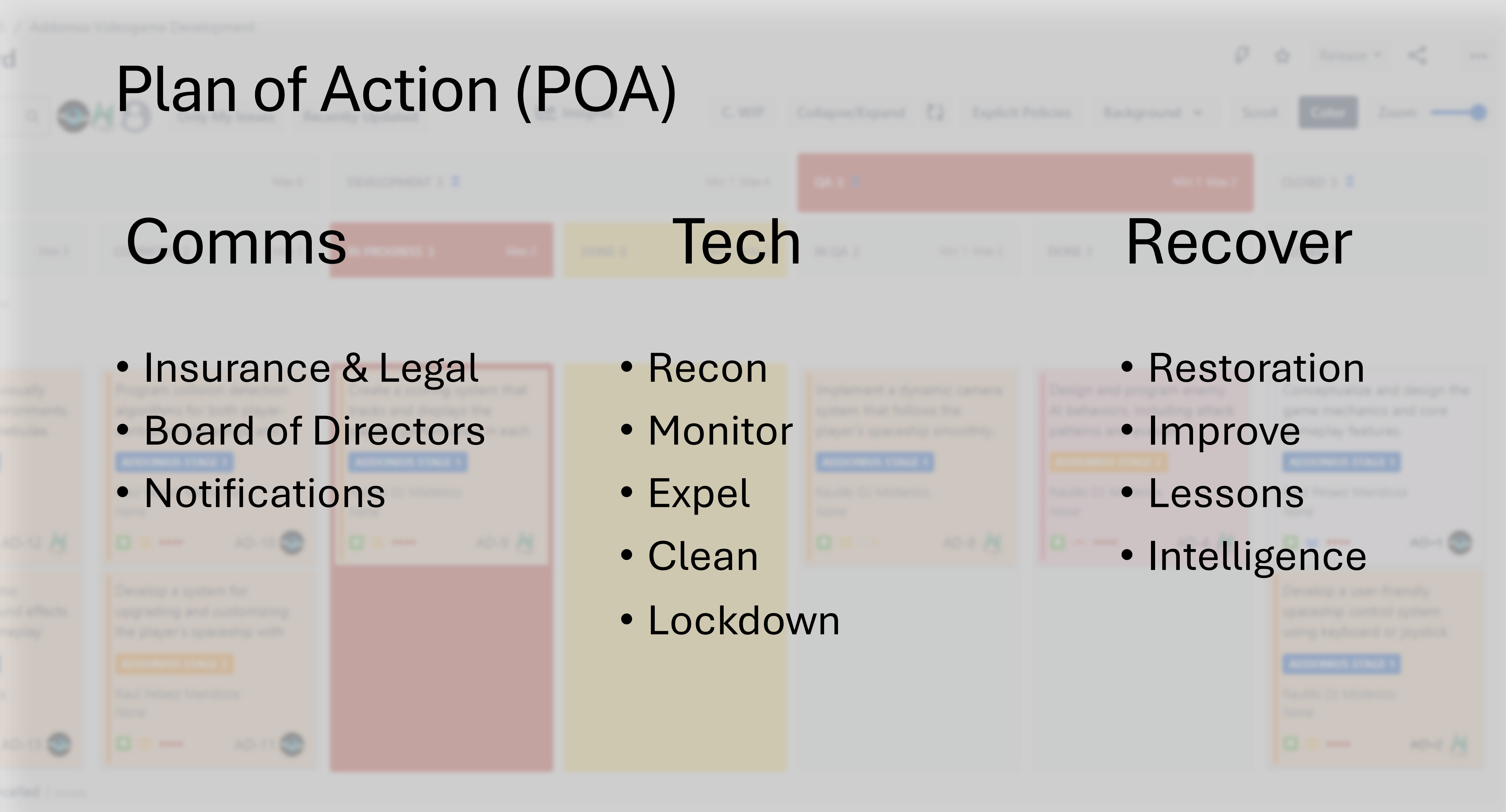


DS Decrypt Support

@gmail.com

To:

I can give you a discount, pay $7000, ok?



Plan of Action (POA)

Comms

- Insurance & Legal
- Board of Directors
- Notifications

Tech

- Recon
- Monitor
- Expel
- Clean
- Lockdown

Recover

- Restoration
- Improve
- Lessons
- Intelligence

Wednesday 10 August 2022

- External domain
- Out of band communication
- Updates every hour
- Leave tech people alone
- IR plan activated
- IT Director Lead

Checkpoint 1

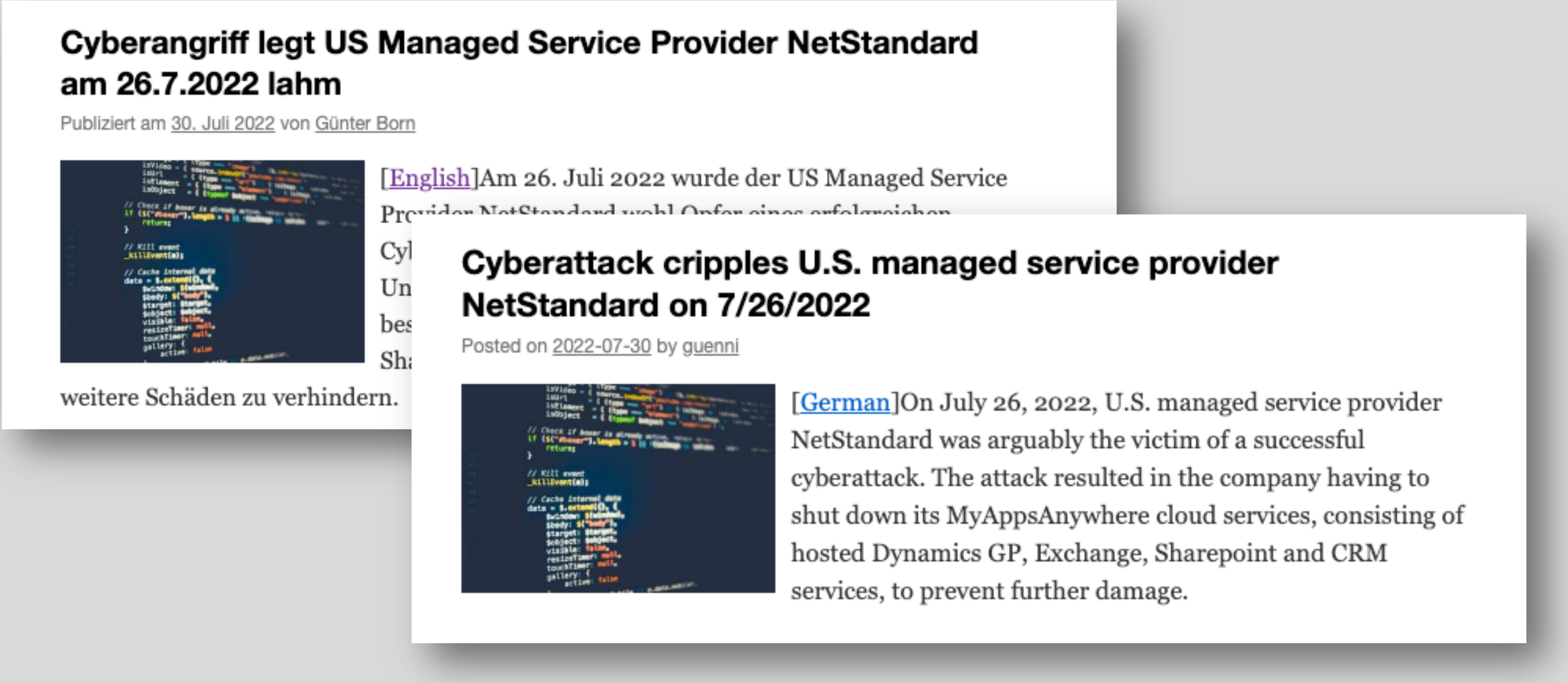
- The Good
  - Backups
  - Firewall
  - MFA
  - Some monitoring
  - Incident Response Plan

- The Bad
  - Disinformation
  - Foreign National

Background

The Intern Shines

IIG Process



Cyberangriff legt US Managed Service Provider NetStandard am 26.7.2022 lahm

Publiziert am 30. Juli 2022 von Günter Born

[English]Am 26. Juli 2022 wurde der US Managed Service Provider NetStandard wohl Opfer eines erfolgreichen

Cy

Un

bes

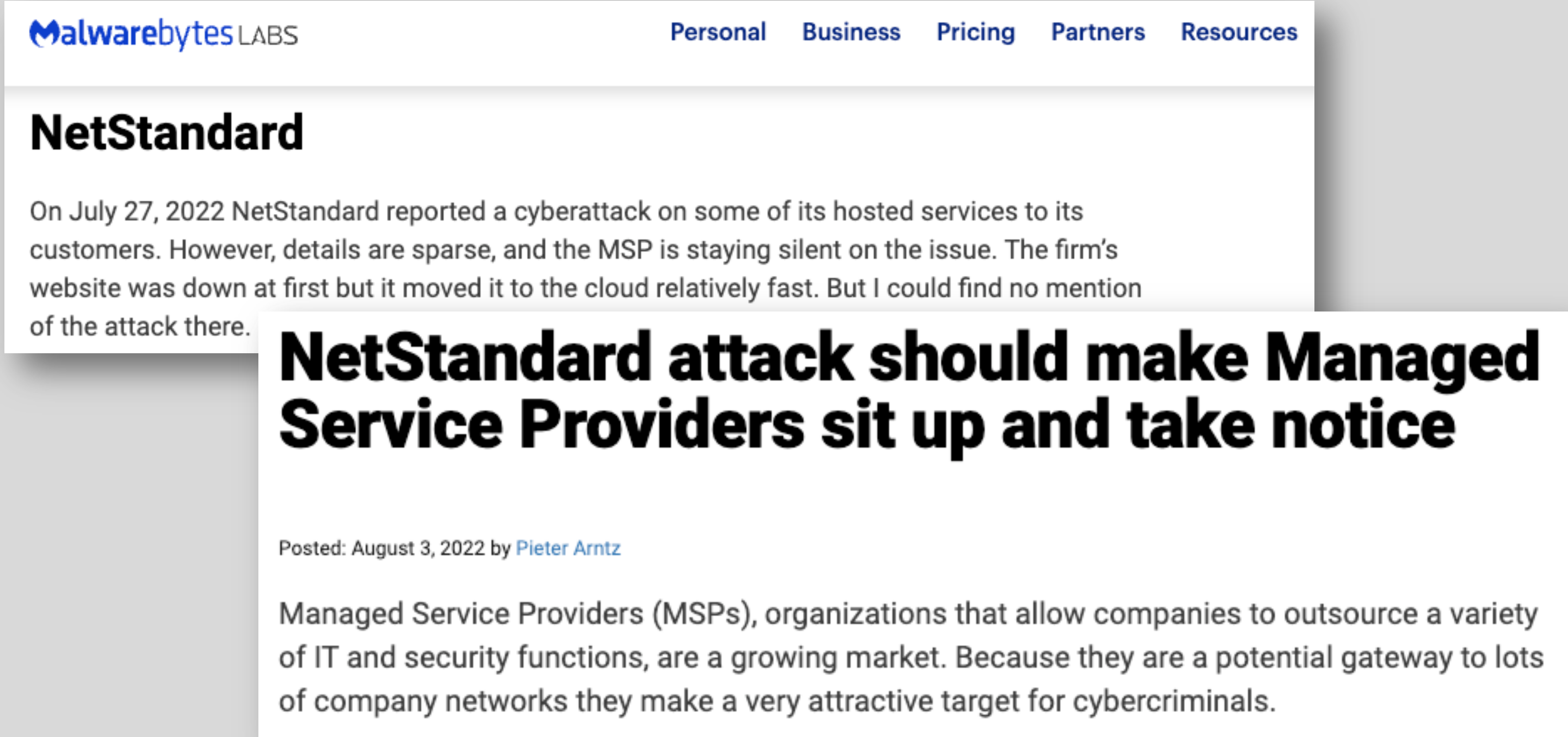
Sha

weitere Schäden zu verhindern.

Cyberattack cripples U.S. managed service provider NetStandard on 7/26/2022

Posted on 2022-07-30 by guenni

[German]On July 26, 2022, U.S. managed service provider NetStandard was arguably the victim of a successful cyberattack. The attack resulted in the company having to shut down its MyAppsAnywhere cloud services, consisting of hosted Dynamics GP, Exchange, Sharepoint and CRM services, to prevent further damage.



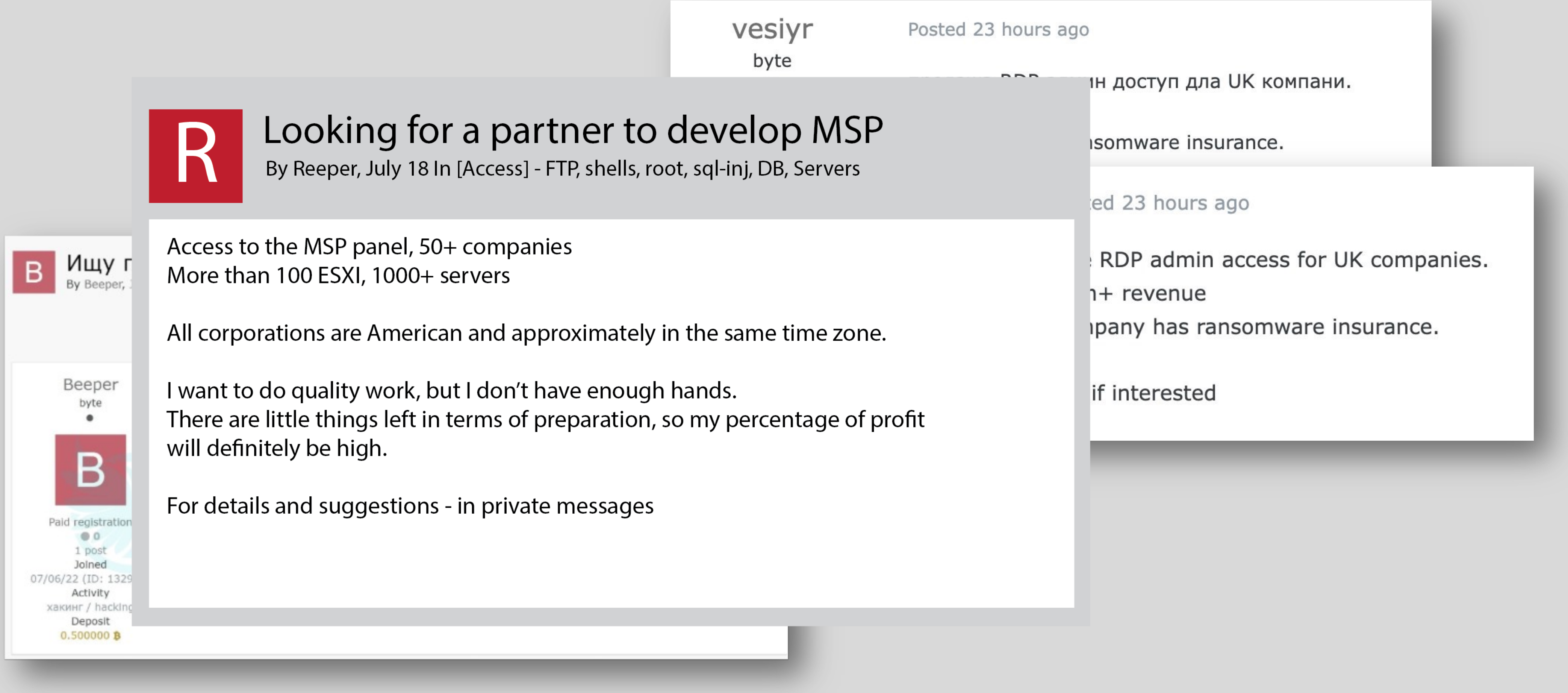
NetStandard

On July 27, 2022 NetStandard reported a cyberattack on some of its hosted services to its customers. However, details are sparse, and the MSP is staying silent on the issue. The firm’s website was down at first but it moved it to the cloud relatively fast. But I could find no mention of the attack there.

NetStandard attack should make Managed Service Providers sit up and take notice

Posted: August 3, 2022 by Pieter Arntz

Managed Service Providers (MSPs), organizations that allow companies to outsource a variety of IT and security functions, are a growing market. Because they are a potential gateway to lots of company networks they make a very attractive target for cybercriminals.



R

Looking for a partner to develop MSP

By Reeper, July 18 In [Access] - FTP, shells, root, sql-inj, DB, Servers

Access to the MSP panel, 50+ companies
More than 100 ESXI, 1000+ servers

All corporations are American and approximately in the same time zone.

I want to do quality work, but I don’t have enough hands.
There are little things left in terms of preparation, so my percentage of profit will definitely be high.

For details and suggestions - in private messages

B Ищу г
By Beeper,

Beeper
byte
●
B
Paid registration
● 0
1 post
Joined
07/06/22 (ID: 1329
Activity
хакинг / hacking
Deposit
0.500000 ฿

vesiyr
byte

Posted 23 hours ago

н доступ дла UK компани.

ısomware insurance.

ted 23 hours ago

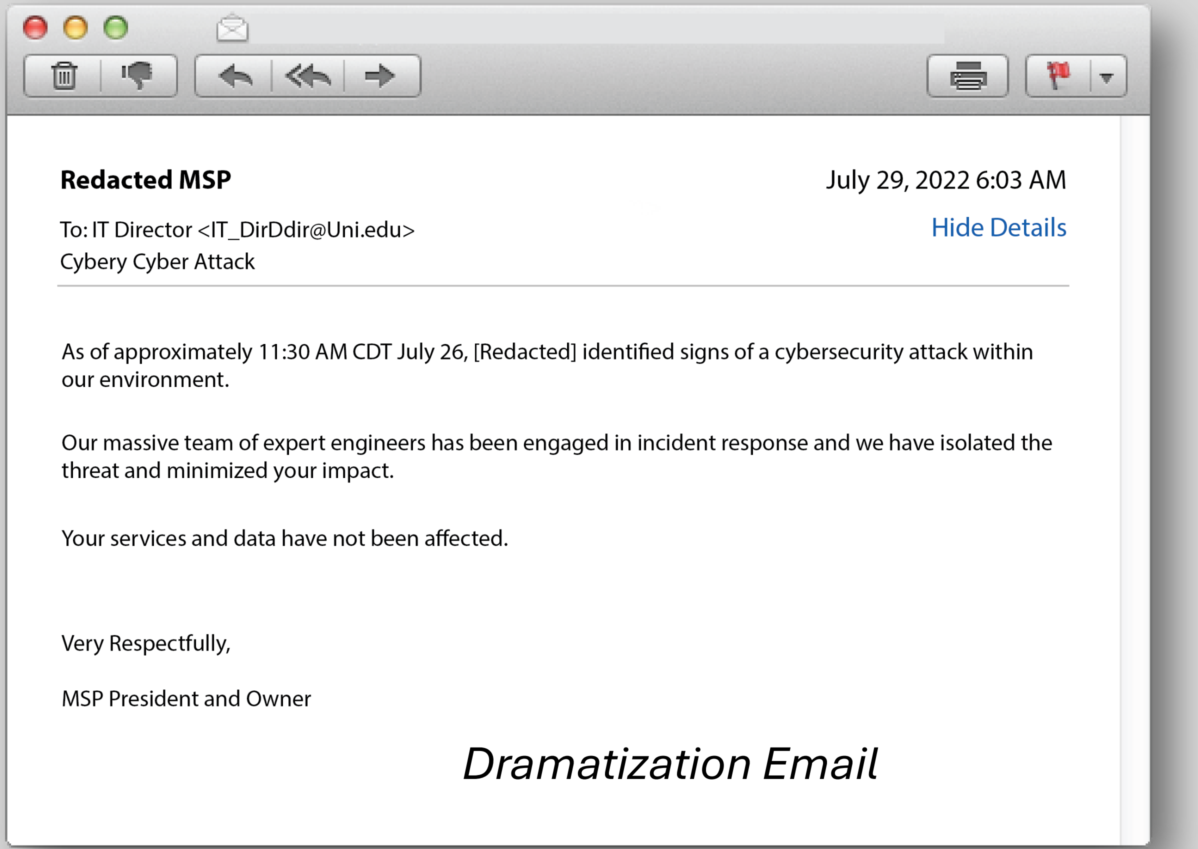
RDP admin access for UK companies.
ı+ revenue
ıpany has ransomware insurance.

if interested

Vendor Notification

Not actual email

**Recreated for dramatic effect*



Redacted MSP

July 29, 2022 6:03 AM

To: IT Director <IT_DirDdir@Uni.edu>

Hide Details

Cybery Cyber Attack

As of approximately 11:30 AM CDT July 26, [Redacted] identified signs of a cybersecurity attack within our environment.

Our massive team of expert engineers has been engaged in incident response and we have isolated the threat and minimized your impact.

Your services and data have not been affected.

Very Respectfully,

MSP President and Owner

Dramatization Email

Wednesday
Mid-morning

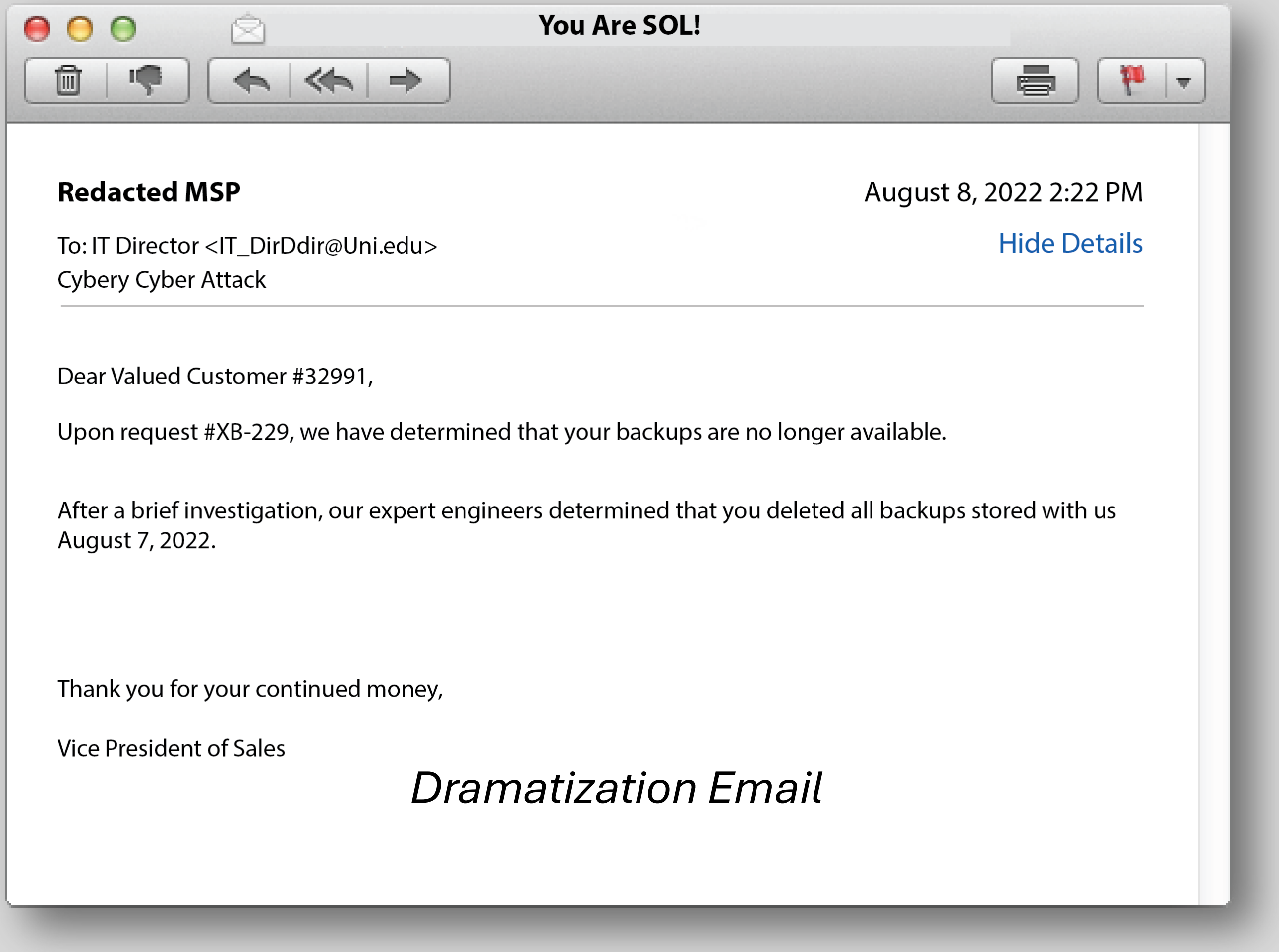
Students arrive in 4.75 days

“Seek first to understand...” – Stephen Covey

Q&A - Backups

Not actual email:

**Recreated for dramatic effect*



Redacted MSP August 8, 2022 2:22 PM

To: IT Director <IT_DirDdir@Uni.edu>

Hide Details

Cybery Cyber Attack

Dear Valued Customer #32991,

Upon request #XB-229, we have determined that your backups are no longer available.

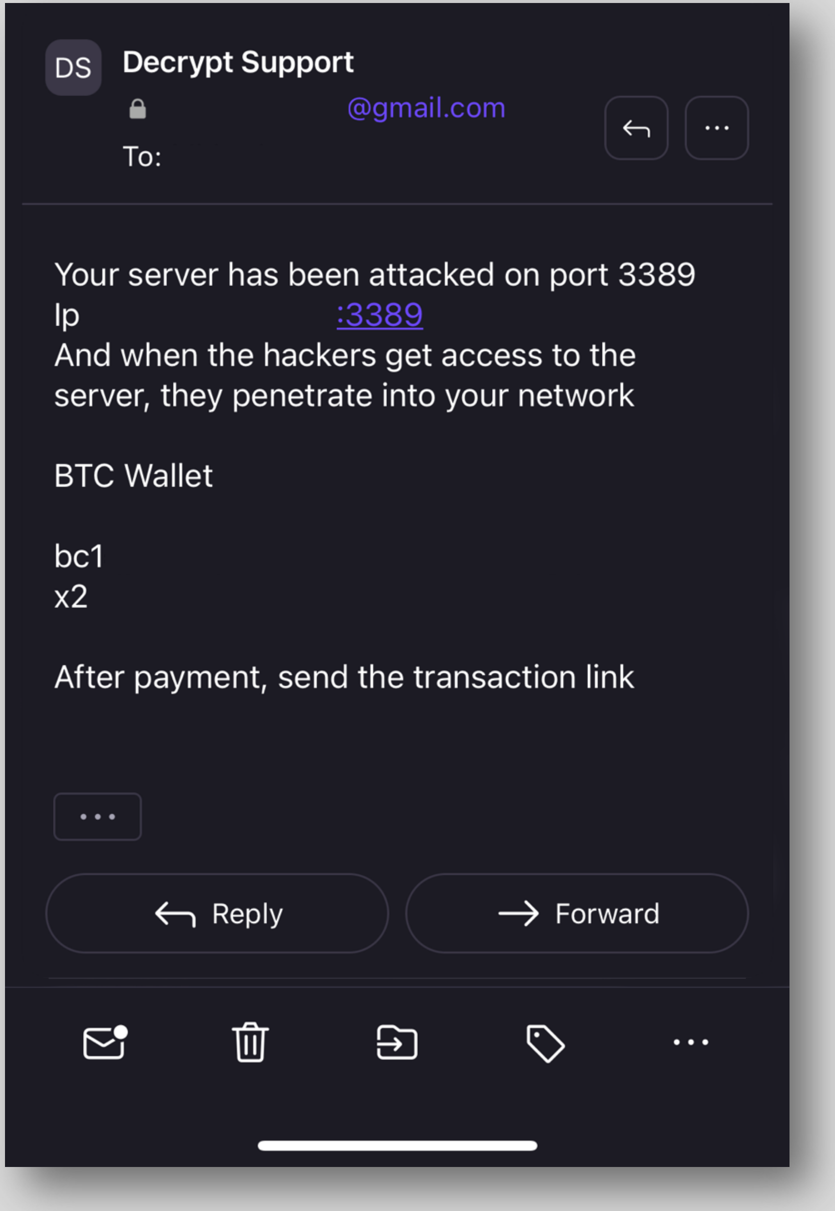
After a brief investigation, our expert engineers determined that you deleted all backups stored with us August 7, 2022.

Thank you for your continued money,

Vice President of Sales

Dramatization Email

Q&A - Firewall



Decrypt Support

@gmail.com

To:

Your server has been attacked on port 3389
Ip :3389
And when the hackers get access to the server, they penetrate into your network

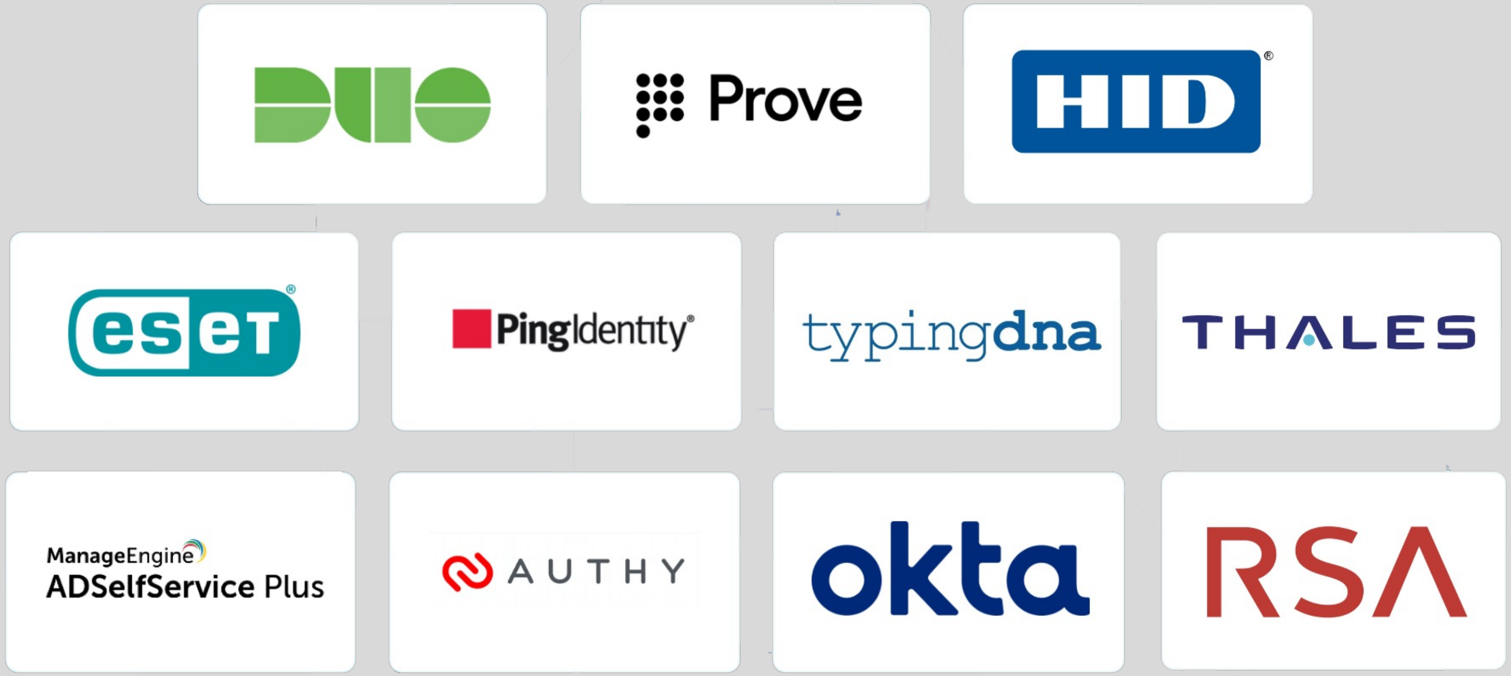
BTC Wallet

bc1
x2

After payment, send the transaction link

Redacted Email

Q&A – MFA (2FA)


DUO
Prove
HID
eset
PingIdentity
typingdna
THALES
ManageEngine ADSelfService Plus
AUTHY
okta
RSA

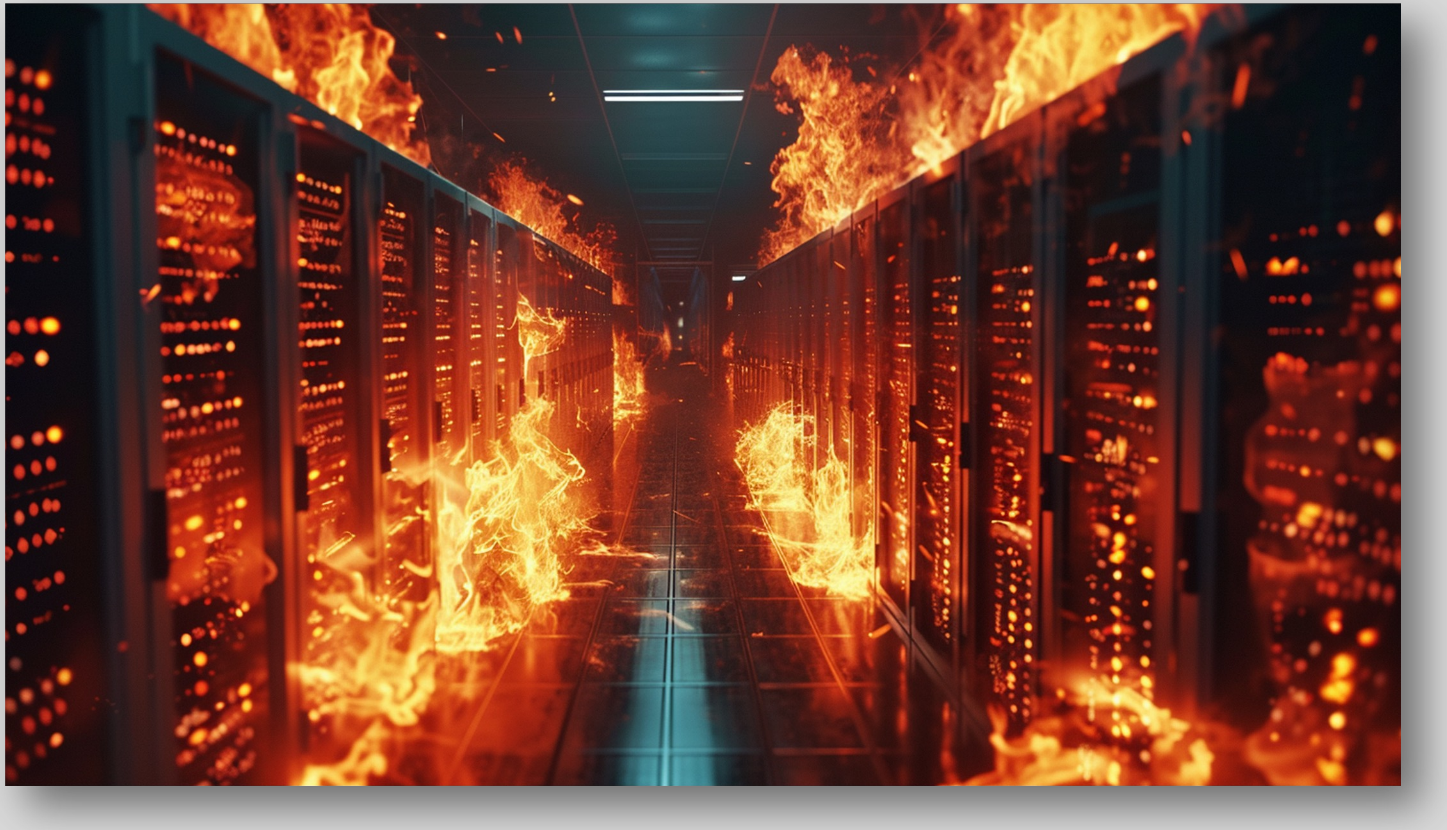
Checkpoint 2

- The Good
  - ~~Backups~~
  - ~~Firewall~~
  - ~~MFA~~
  - Monitoring
  - Incident Response Plan

- The Bad
  - ~~Disinformation~~
  - ~~Foreign National~~
  - Backups
  - Firewall
  - MFA

Offline

- Most Servers
- Most PCs
- Remote access
- IP phones
- Wireless

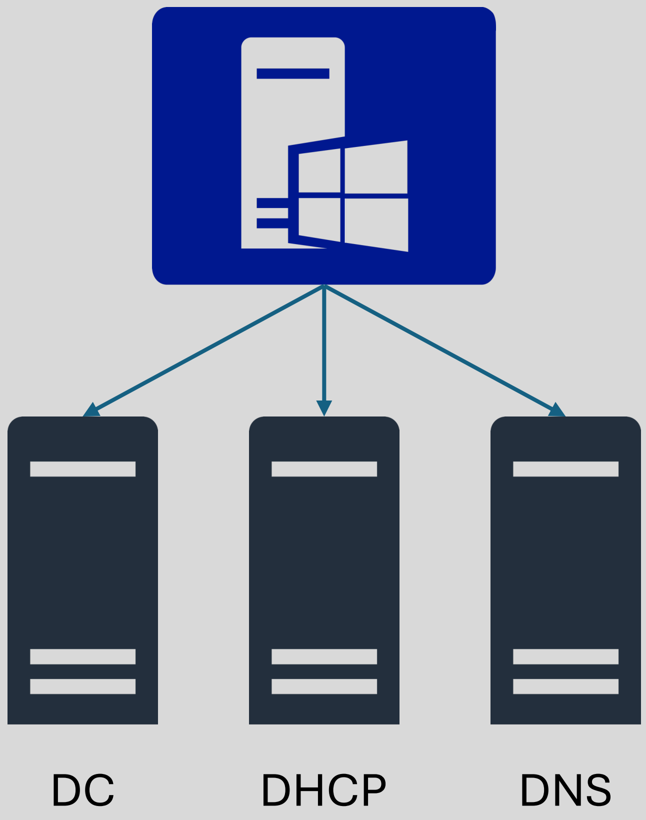


Roadblocks

- Sr. Admin AWOL
- Passwd gatekeeper
- Admin vacation
- Insurance & legal

Inadvertent Success

- Domain controller
- DHCP lease time
- Most pcs lost connectivity
- No lateral movement
- NAS in process of upgrade



Checkpoint 3

- The Good
  - Monitoring
  - Incident Response Plan
  - DHCP
  - DNS
  - NAS

- The Bad
  - Admin AWOL
  - MFA
  - Firewall
  - Backups
  - Monitoring

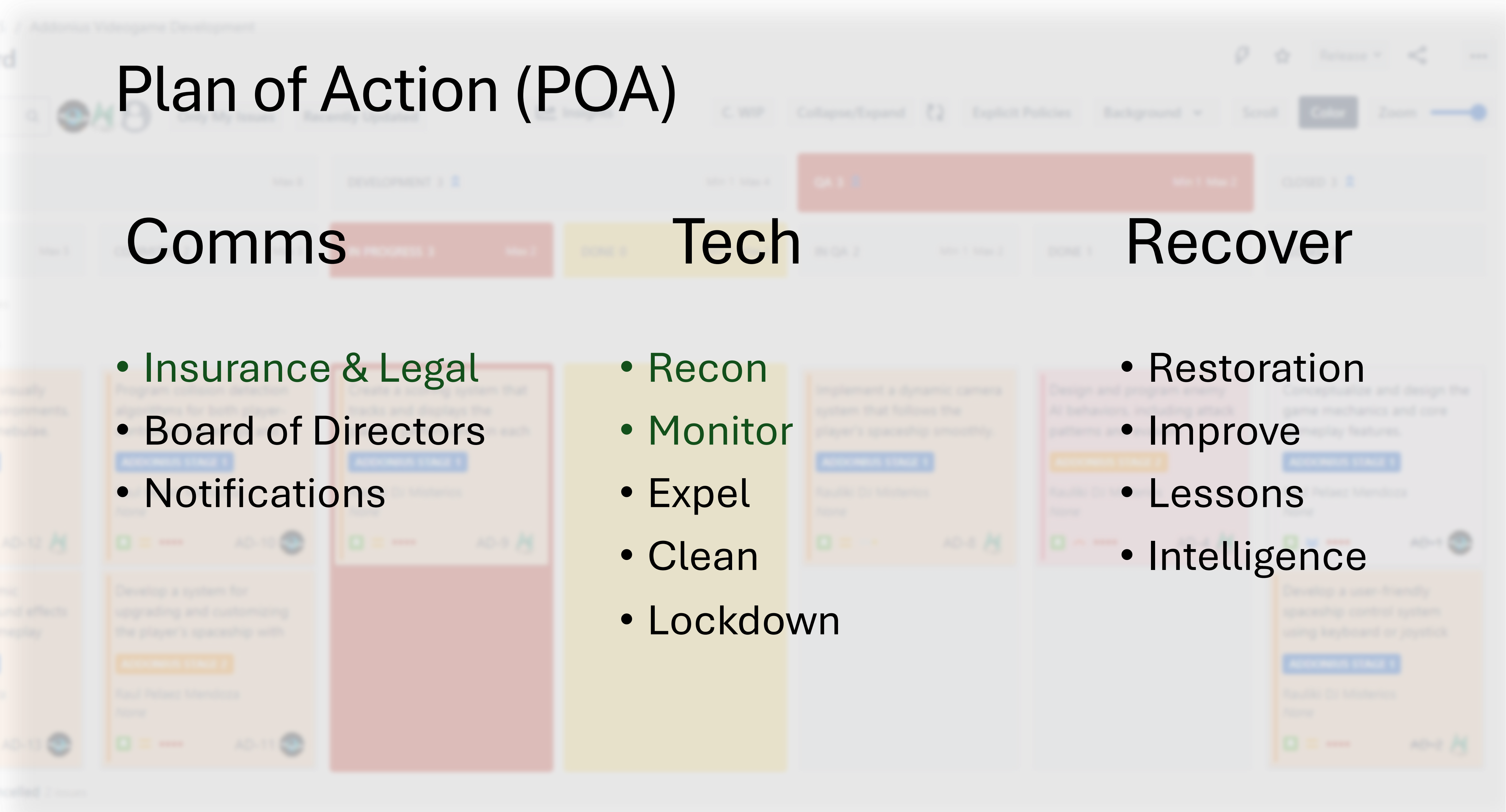
Wednesday
Afternoon

Students arrive in 4.5 days

Wednesday 10 August 2022

- Insurance, outside counsel involved
- Discussing in committee
- Triage question

Plan of Action (POA)



Comms

- Insurance & Legal
- Board of Directors
- Notifications

Tech

- Recon
- Monitor
- Expel
- Clean
- Lockdown

Recover

- Restoration
- Improve
- Lessons
- Intelligence

Vendor Contact

- Gather information on adversary

FS-ISAC

REN-ISAC

**Do not expect your vendors to assist you with anything*

Insurance Assigned/Approved

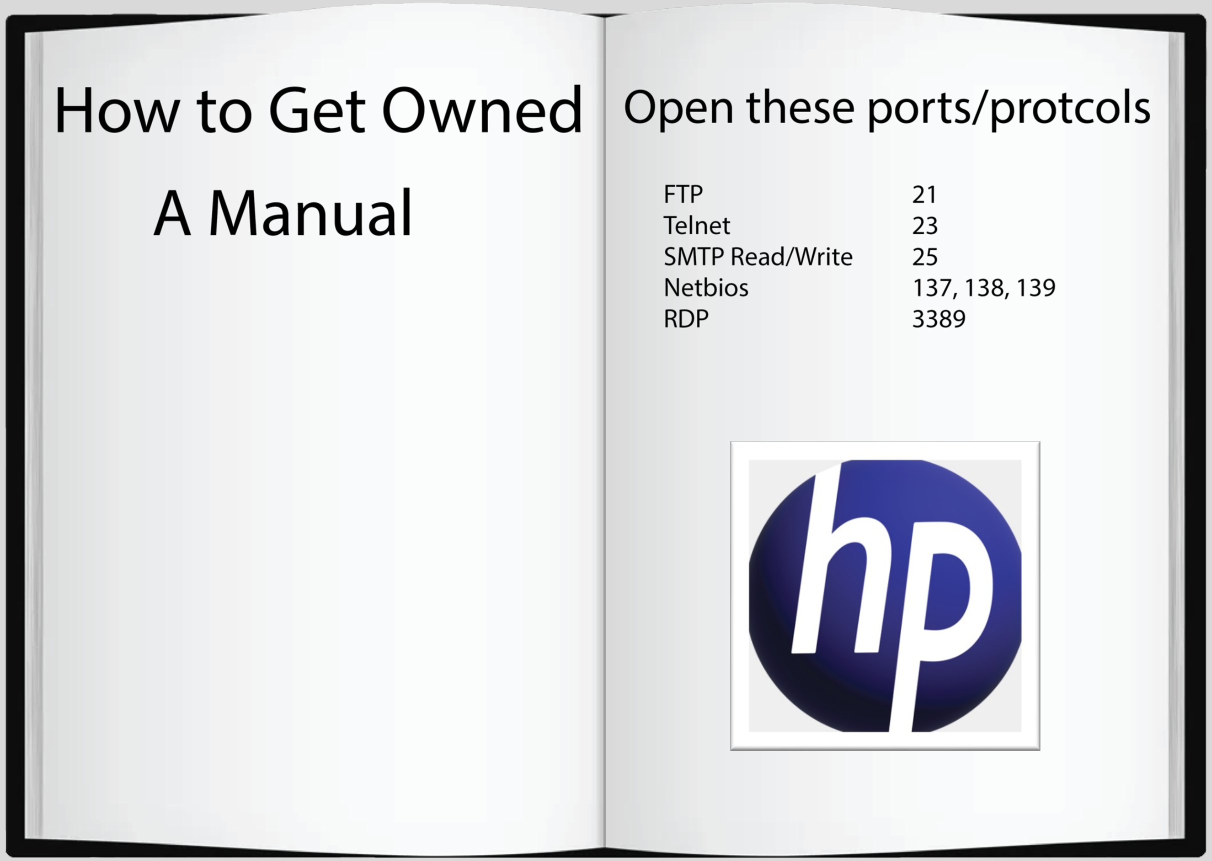
- Forensics team – remote – directing 10FS work
- 10FS team on site
- Insurance/Legal - negotiations with adversary
- Admin Found!

Information Gathering - Backups

- Investigate Jump/Staging Box (Backup Vendor)
- Has Sentinel One Installed
- Neither App or OS patched
- Alerting Off – changed alert contact, IP, etc…
- Only 3 accounts
  - vendor account
  - admin account
  - service account - hackprint

Information Gathering - Firewall

- ~320 3389
- .ru
- Hackprint Any/Any
- Backup Vendor Any/Any



How to Get Owned

A Manual

Open these ports/protcols

FTP	21
Telnet	23
SMTP Read/Write	25
Netbios	137, 138, 139
RDP	3389

Wednesday
Evening

Students arrive in 4.2 days

Communications

- Insurance & Legal
  - Contact adversary, open comms
- President & Exec Council
  - Contact Board of Directors
  - Draft notifications to staff
  - Formulate work around plan for student arrival
- Meeting Cadence Established

Information Gathering

- 10FS & University Staff
  - Install S1 & Velociraptor all systems
  - Recall all laptops

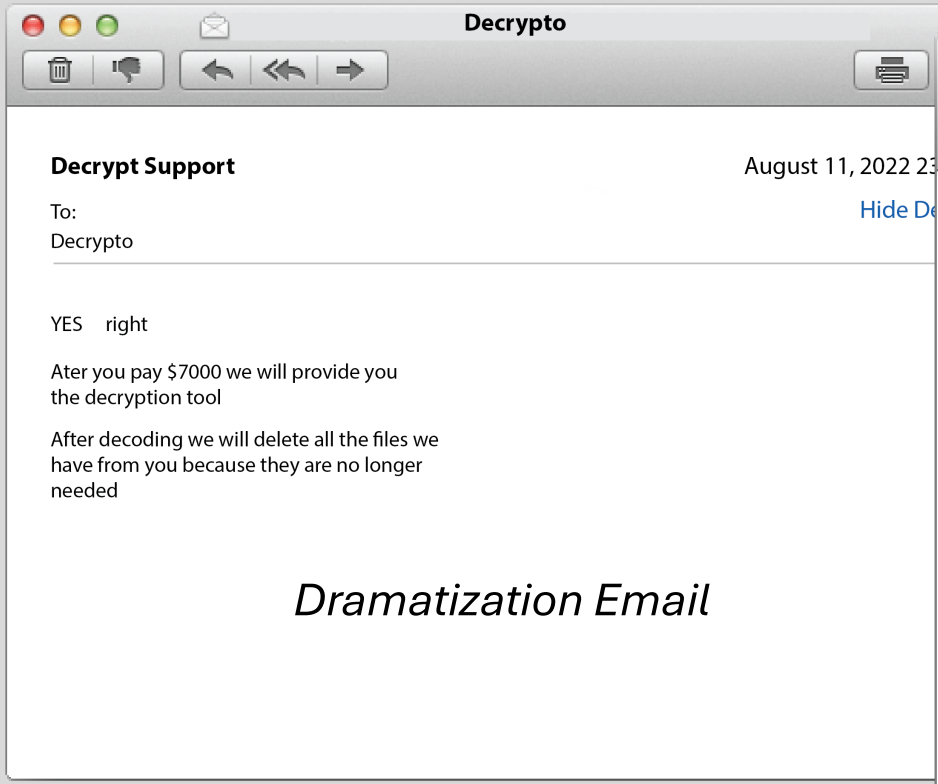
Thursday
11 August 2022

Students arrive in 4 days

Expulsion

- Cut off all access

Communications



Decrypt Support

August 11, 2022 23

To:
Decrypto

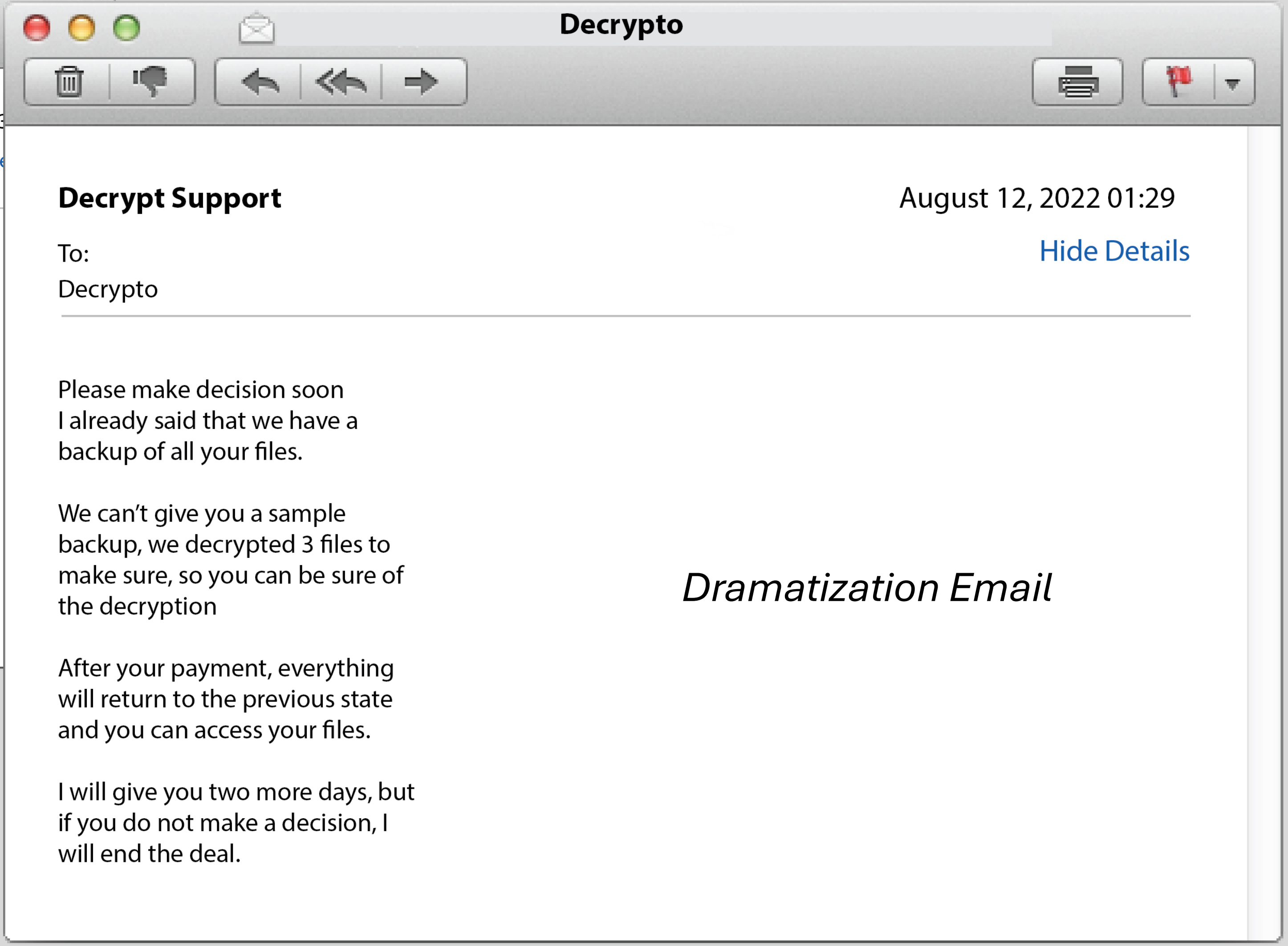
Hide De

YES   right

Ater you pay $7000 we will provide you
the decryption tool

After decoding we will delete all the files we
have from you because they are no longer
needed

Dramatization Email



Decrypt Support

August 12, 2022 01:29

To:
Decrypto

Hide Details

Please make decision soon
I already said that we have a
backup of all your files.

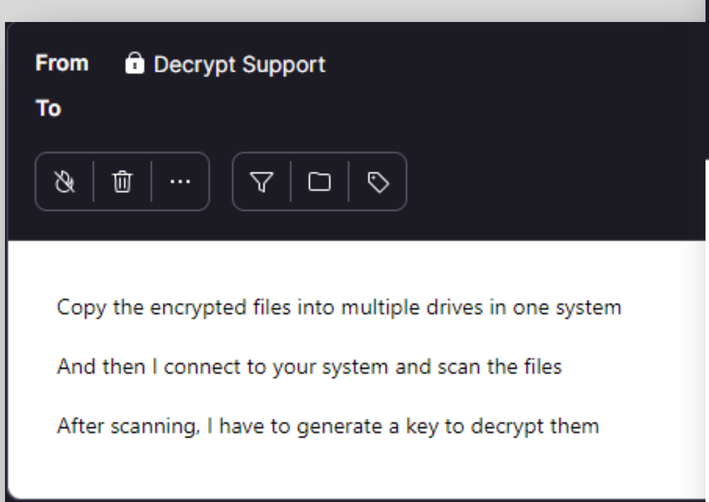
We can't give you a sample
backup, we decrypted 3 files to
make sure, so you can be sure of
the decryption

After your payment, everything
will return to the previous state
and you can access your files.

I will give you two more days, but
if you do not make a decision, I
will end the deal.

Dramatization Email

Instructions



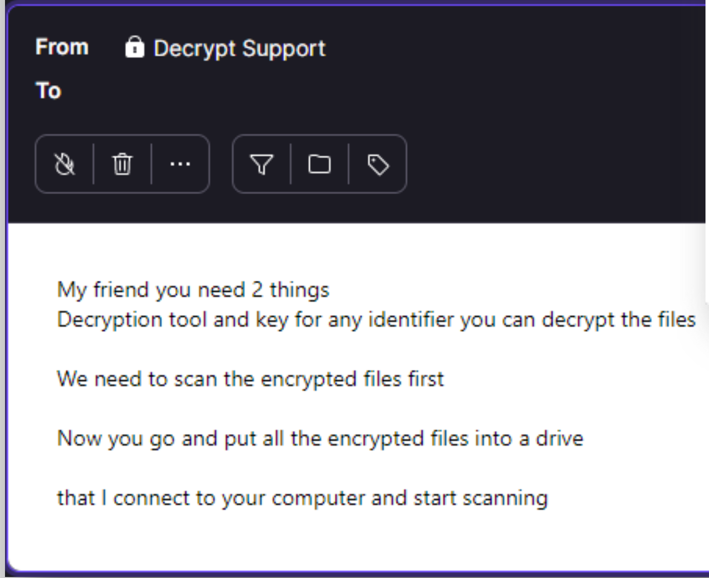
From 🔒 Decrypt Support

To

Copy the encrypted files into multiple drives in one system

And then I connect to your system and scan the files

After scanning, I have to generate a key to decrypt them



From 🔒 Decrypt Support

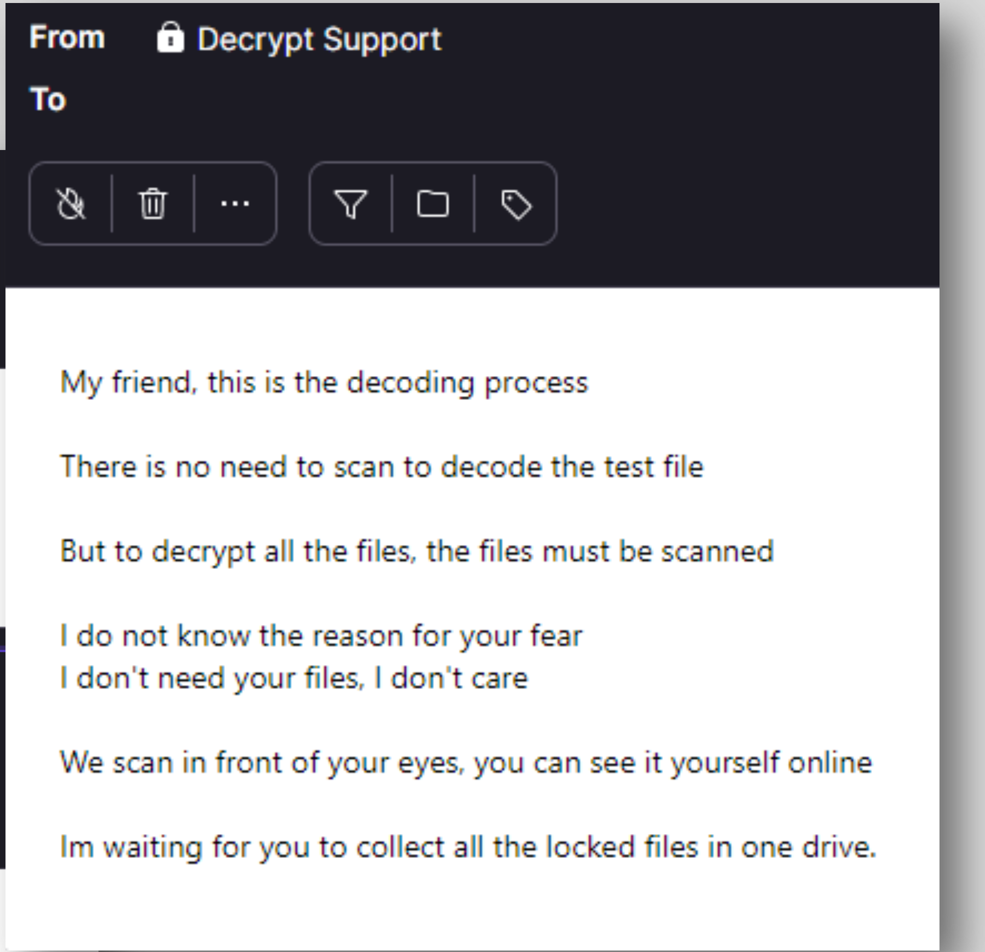
To

My friend you need 2 things
Decryption tool and key for any identifier you can decrypt the files

We need to scan the encrypted files first

Now you go and put all the encrypted files into a drive

that I connect to your computer and start scanning



From 🔒 Decrypt Support

To

My friend, this is the decoding process

There is no need to scan to decode the test file

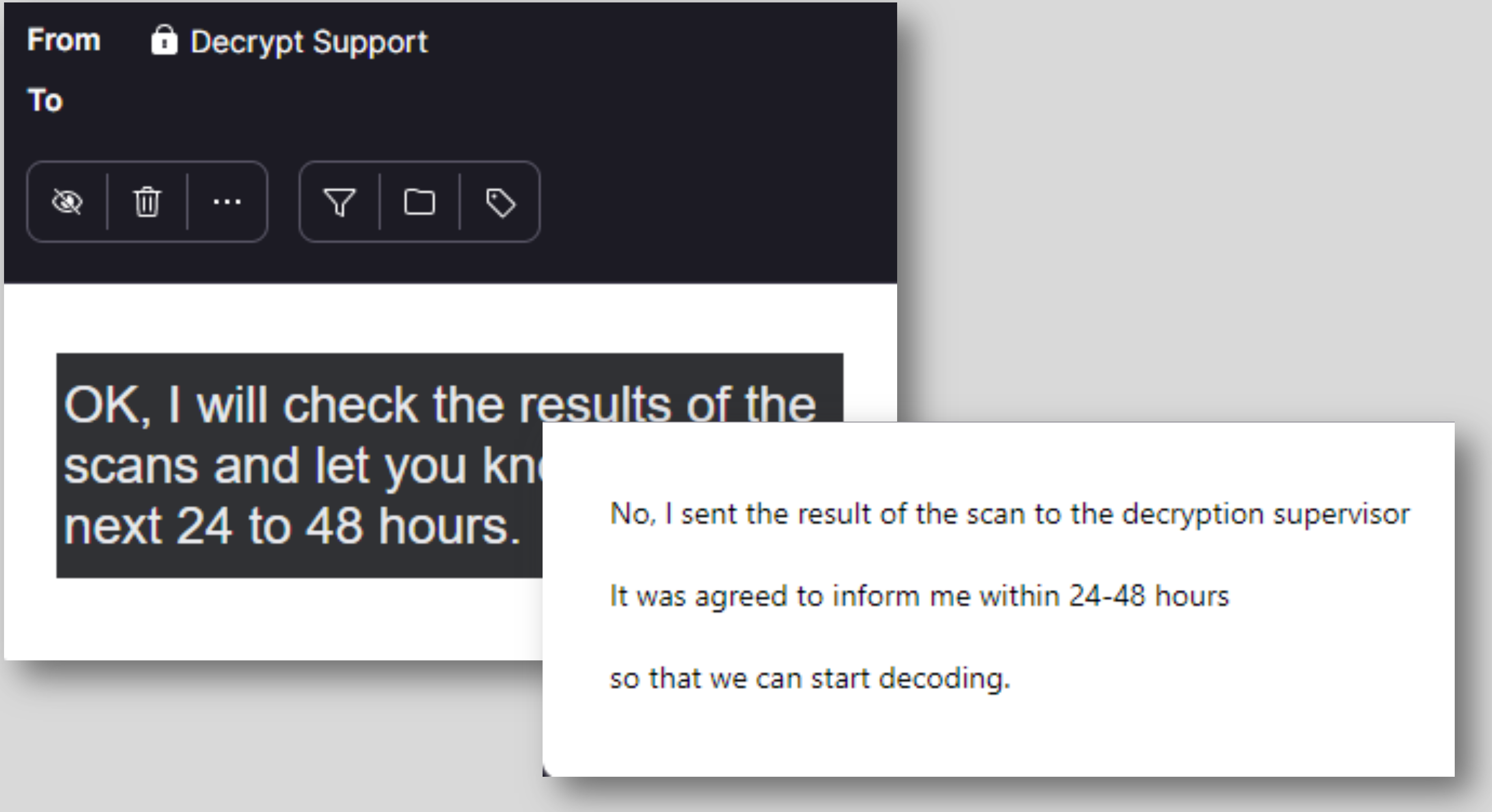
But to decrypt all the files, the files must be scanned

I do not know the reason for your fear
I don't need your files, I don't care

We scan in front of your eyes, you can see it yourself online

Im waiting for you to collect all the locked files in one drive.

Communications



From 🔒 Decrypt Support

To

OK, I will check the results of the scans and let you kn

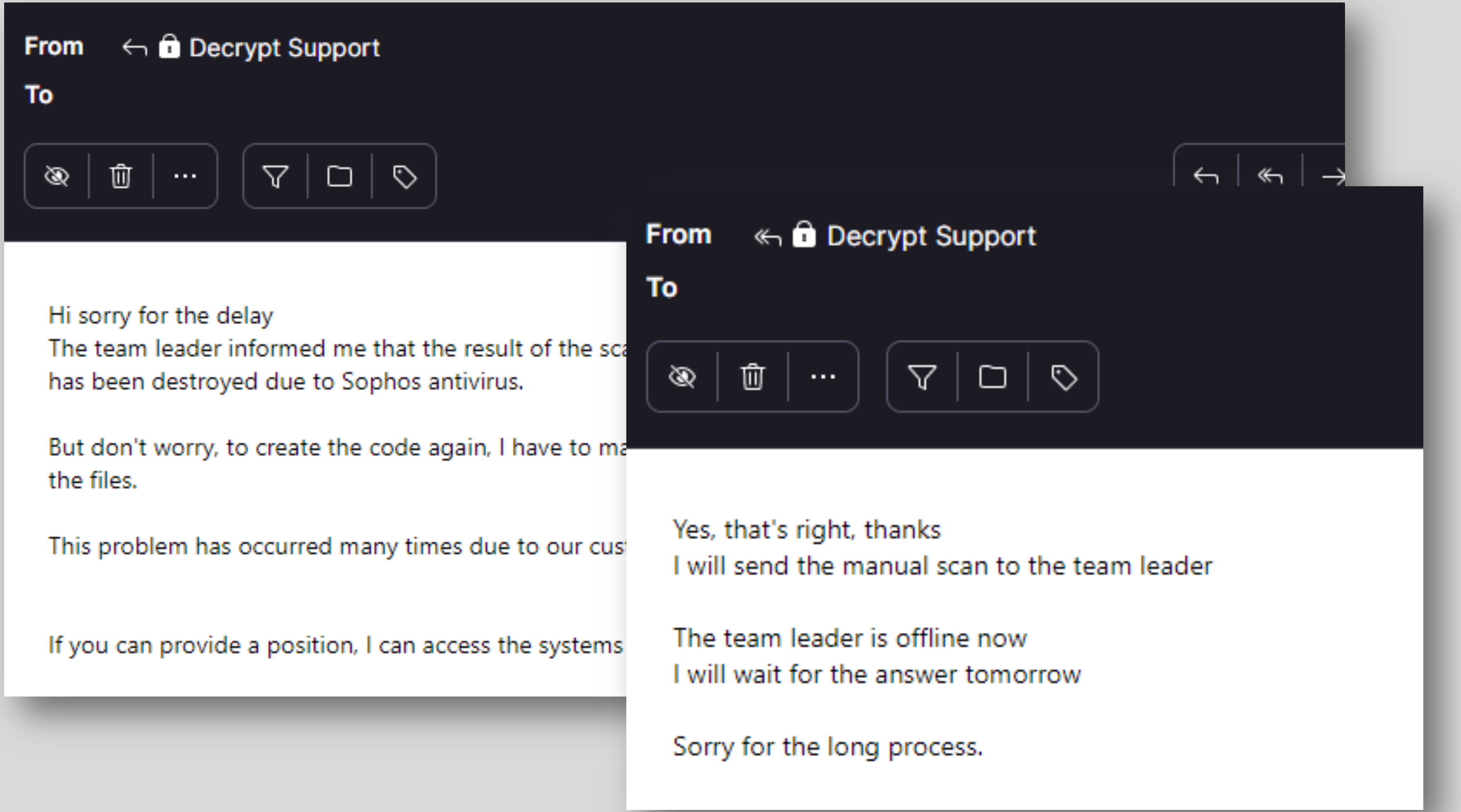
next 24 to 48 hours.

No, I sent the result of the scan to the decryption supervisor

It was agreed to inform me within 24-48 hours

so that we can start decoding.

Team Leader



From ↩ 🔒 Decrypt Support
To

Hi sorry for the delay
The team leader informed me that the result of the sca
has been destroyed due to Sophos antivirus.

But don't worry, to create the code again, I have to ma
the files.

This problem has occurred many times due to our cus

If you can provide a position, I can access the systems

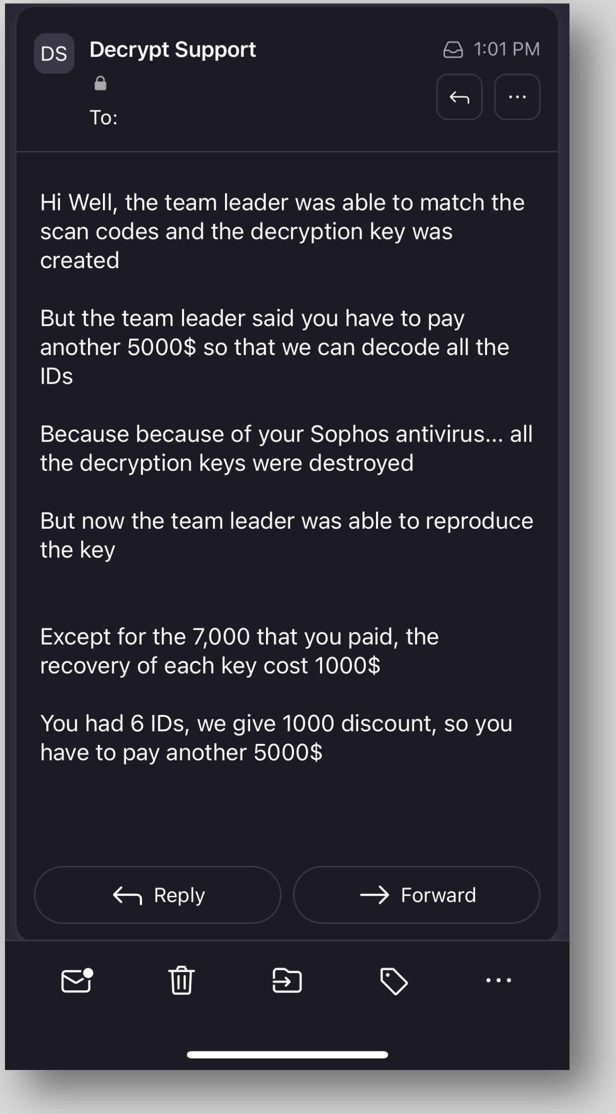
From 🔒 Decrypt Support
To

Yes, that's right, thanks
I will send the manual scan to the team leader

The team leader is offline now
I will wait for the answer tomorrow

Sorry for the long process.

Nickle & Dime



Hi Well, the team leader was able to match the scan codes and the decryption key was created

But the team leader said you have to pay another 5000$ so that we can decode all the IDs

Because because of your Sophos antivirus... all the decryption keys were destroyed

But now the team leader was able to reproduce the key

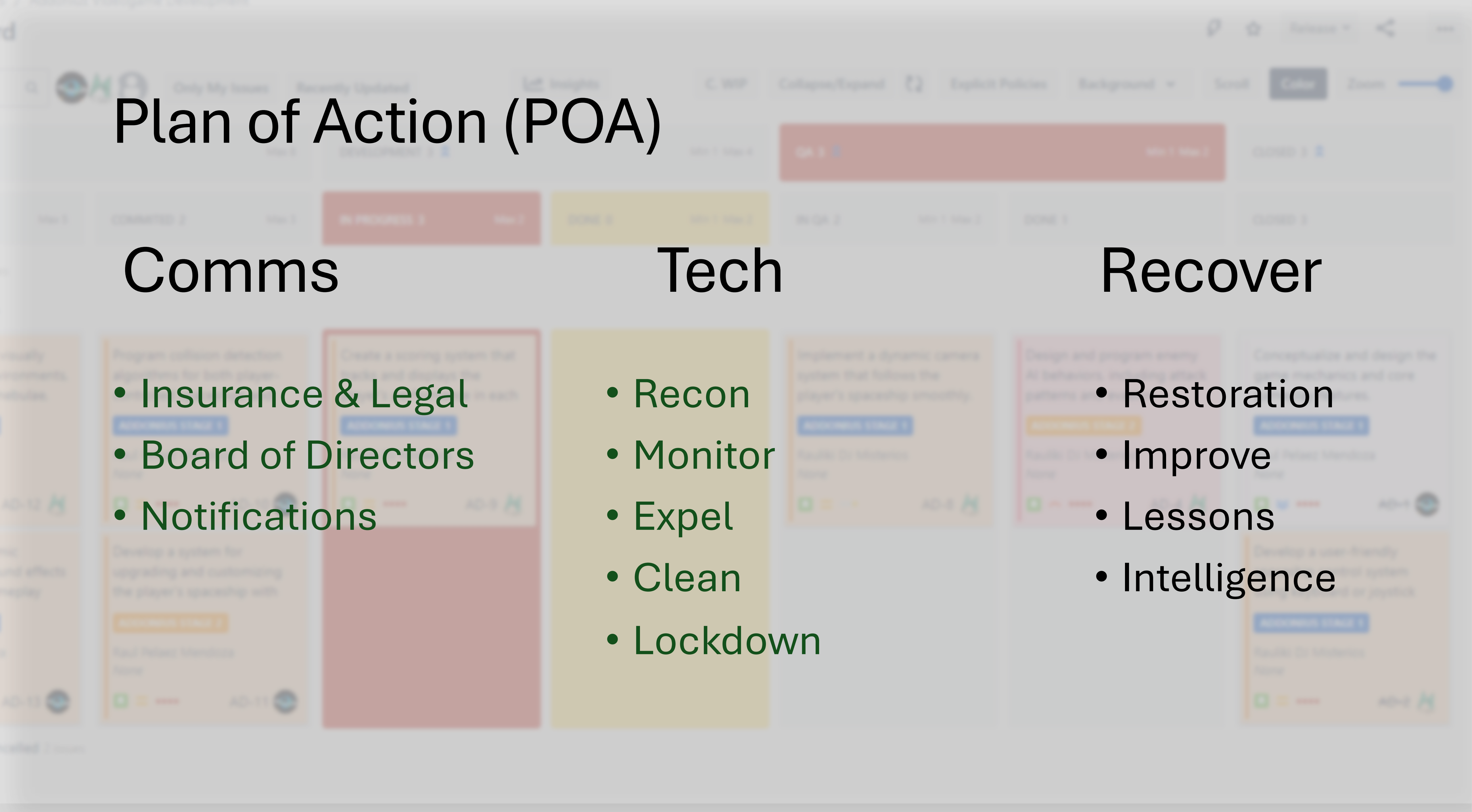
Except for the 7,000 that you paid, the recovery of each key cost 1000$

You had 6 IDs, we give 1000 discount, so you have to pay another 5000$

Thursday

- Recall Effort
- Phased Network Recovery

Plan of Action (POA)



Comms

- Insurance & Legal
- Board of Directors
- Notifications

Tech

- Recon
- Monitor
- Expel
- Clean
- Lockdown

Recover

- Restoration
- Improve
- Lessons
- Intelligence

Friday
12 August 2022

Students arrive in 3 days

Recovery

- Rebuild all servers
- Clean, test, recover partial data
- Firewalls upgraded
- Additional rules & filters
- S1 – communicate with forensics team

Saturday
13 August 2022

Students arrive in 2 days

Sunday
14 August 2022

Students arrive in 1 day

Monday
15 August 2022

Students arrive

We Win

- All students on campus
- No interruption to classes

- Just the beginning
- Work progressed for months

Today

- Cloud backups
- Weekly testing
- Offline truly offline
- Upgraded NAS
- Upgraded firewalls
- 3 disparate paths

- Full SIEM (managed & onsite)
- Full functioning SOC
- MFA ALL ACCOUNTS
- Active Penetration Testing
- Intelligence gathering
- Threat Hunting
- Account monitoring

Today

- Incident Response Upgraded & Regular Testing
- Implemented NIST/ISO/GLBA/CIS governance
- Vendor management
- Change control
- Trained entire staff (ongoing)
- Hired 2 additional staff

Cybersecurity Program

- National Center of Excellence
- Full classes
- Internships guaranteed
- Industry leading instructors
- Sponsorship by great companies

Lessons Learned

Prevention > Reaction

Lessons Learned – Top 3

- Awareness
- Communication
- Prepare & Prevent

Aaron Weissenfluh
Tenfold Security

aaron@tenfoldsecurity.com

Questions

TENFOLD
ARTISAN SPICE BLEND
LITTLE HEAT
LITTLE SWEET
LITTLE SMOKE
HOT

HOTSOS

Defeating Ransomware

How a small university beat defeated a ransomware gang