RSAConference™2023

San Francisco | April 24 – 27 | Moscone Center

Stronger Together

SESSION ID: SBX2-R03

Dressing Adversary Emulation in Business Attire: Outcomes and Successes

#RSAC

Jamie Williams

Principal Adversary Emulation Engineer
The MITRE Corporation
@jamieantisocial

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

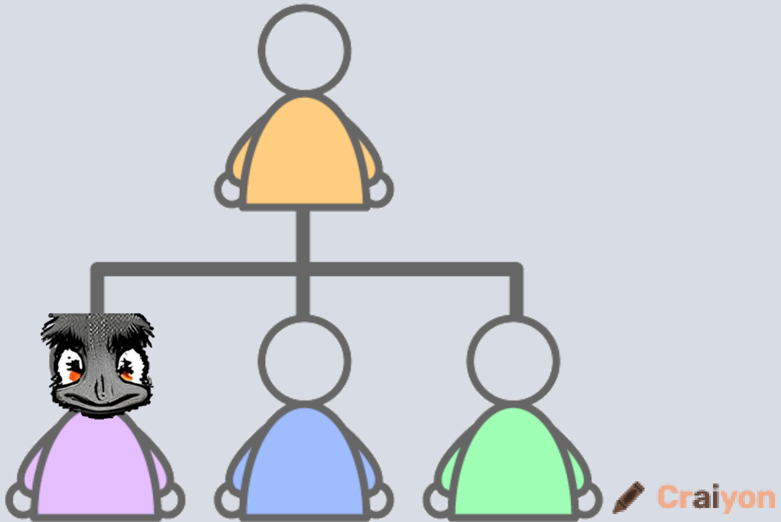
Current Trajectory

- Spending, investments, as well as complexity continually **increase**
- Do we see a similar pattern with **security improvements** and **business impact**?

RSAConference™2023

Stronger Together

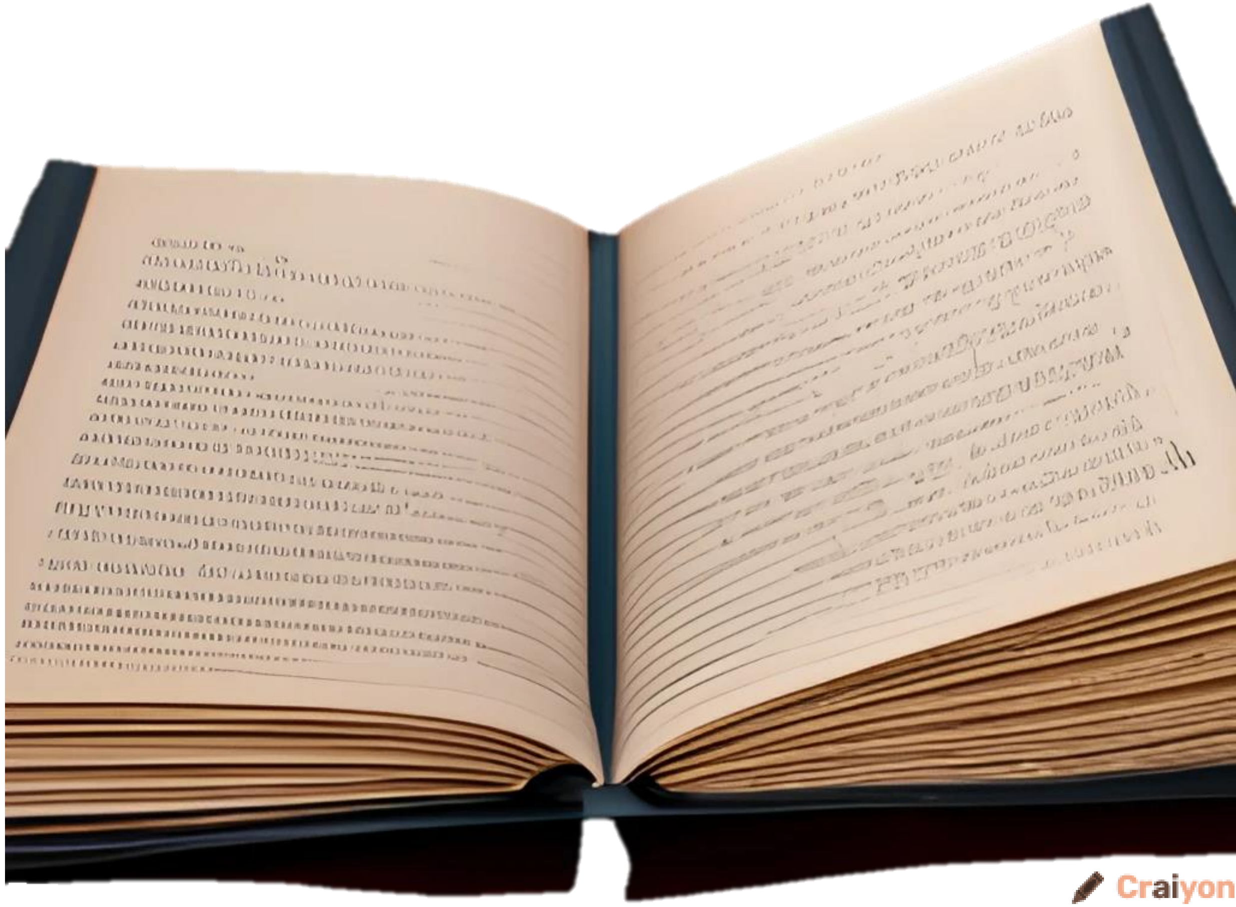
Aligning Adversary Emulation Towards Business Outcomes



#RSAC

What Can Adversary Emulation Provide?

- Ability to **tell a story** before it becomes reality
- **“What would happen if {adversary}?”**
- Provides an opportunity to **rewrite** the story’s ending



Craiyon

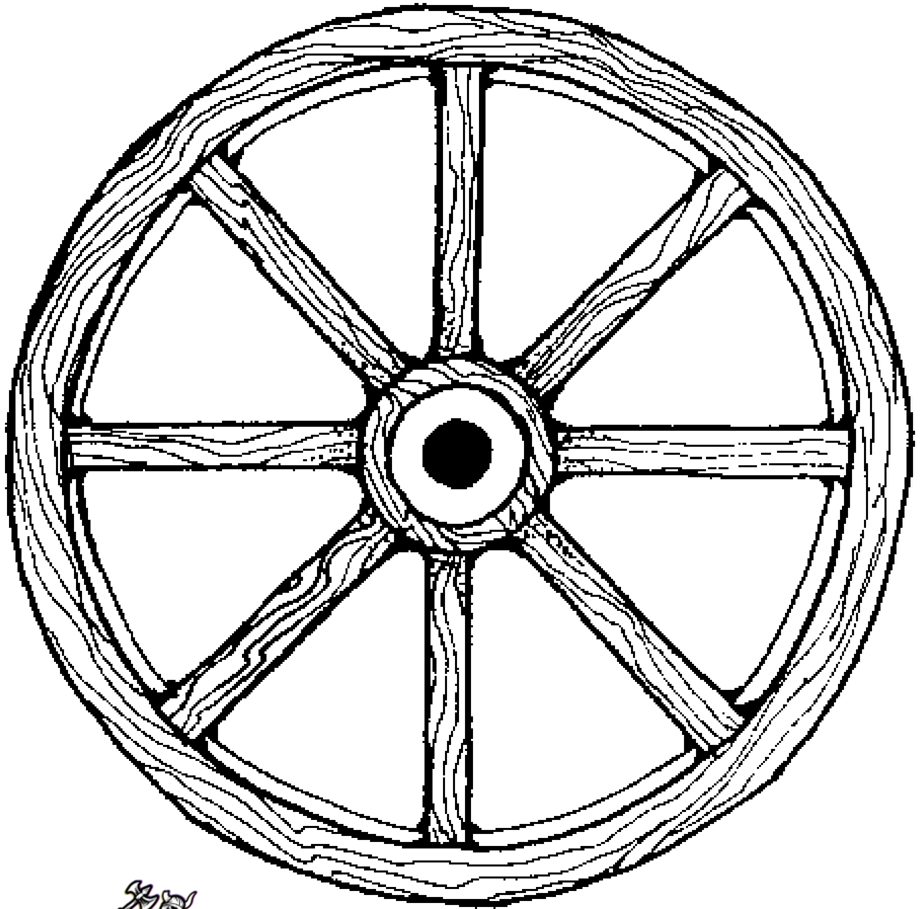
RSAConference™2023

Stronger Together

Threat-Informed Operational Successes

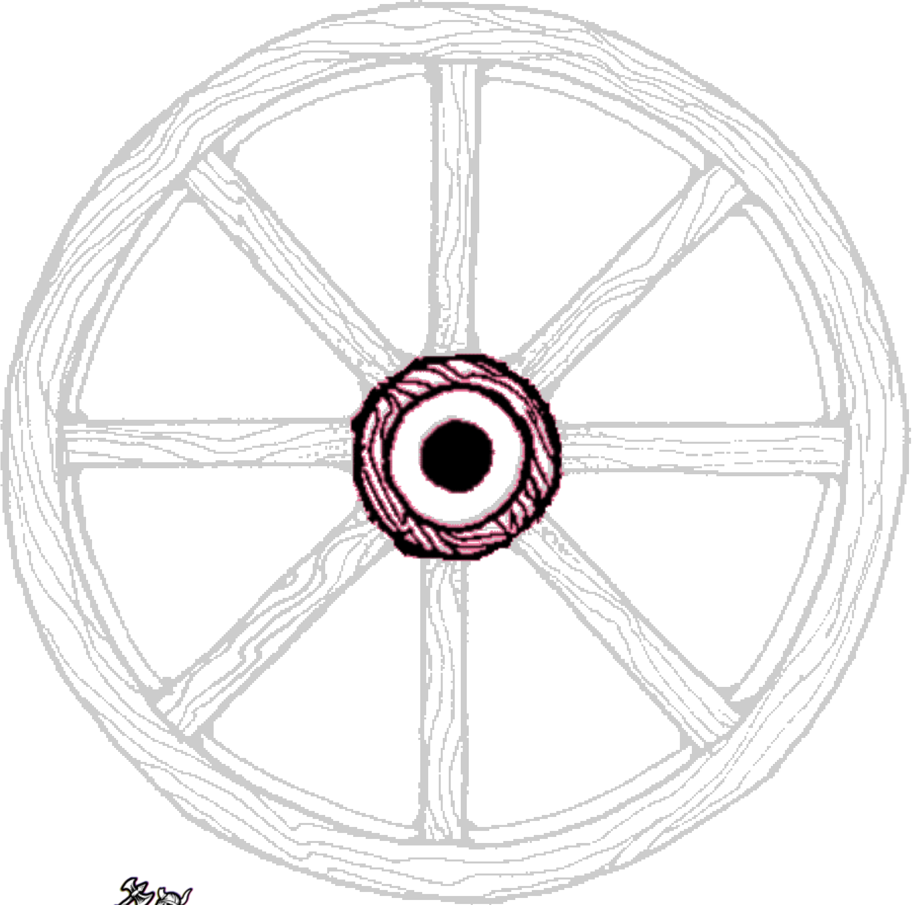
#RSAC

Threat-Informed Mindset

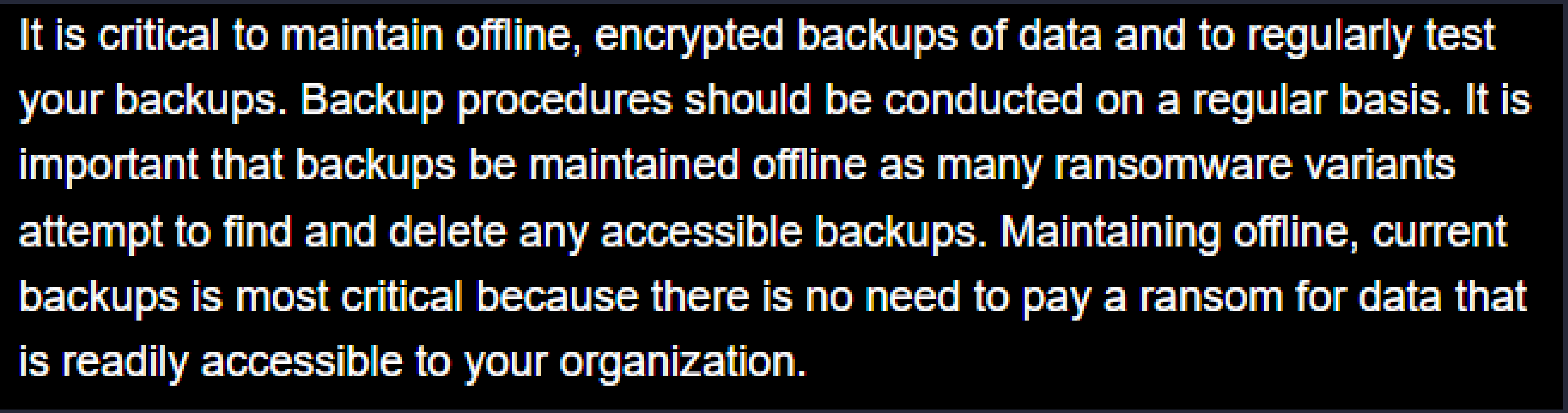


- Assess and implement **security decisions** using **perspective of our adversaries**
- Takes **different forms**, but applies to strategic down to tactical levels

Security Strategy

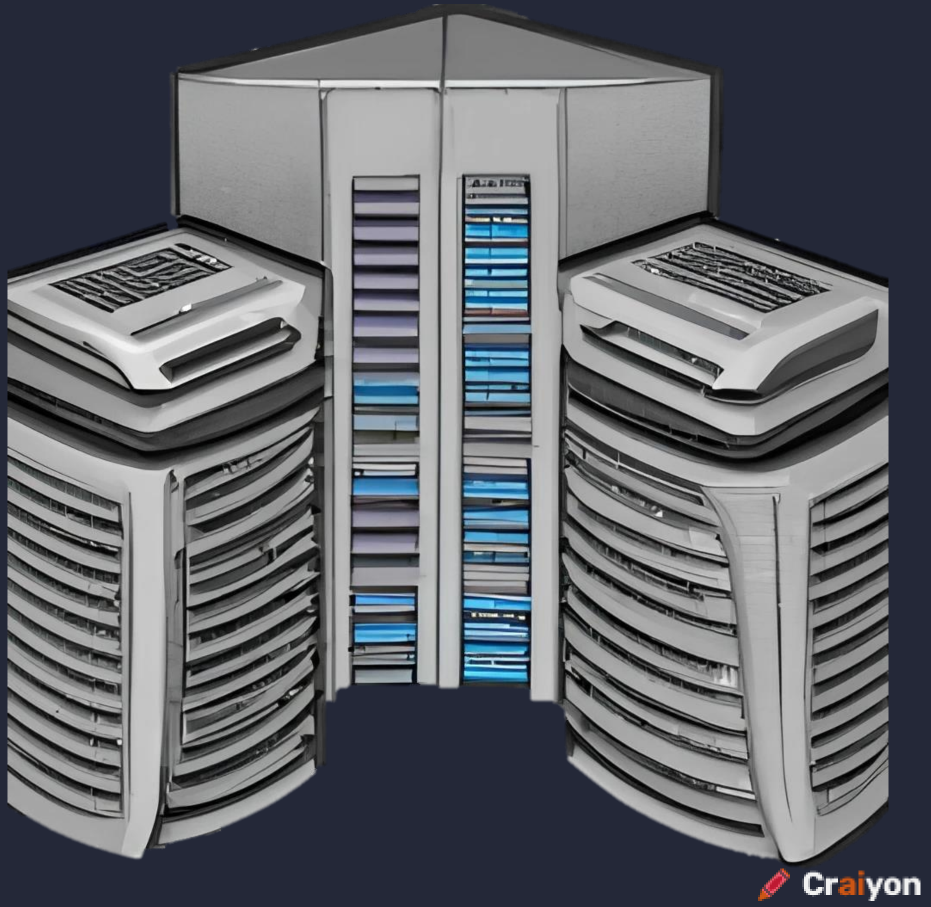


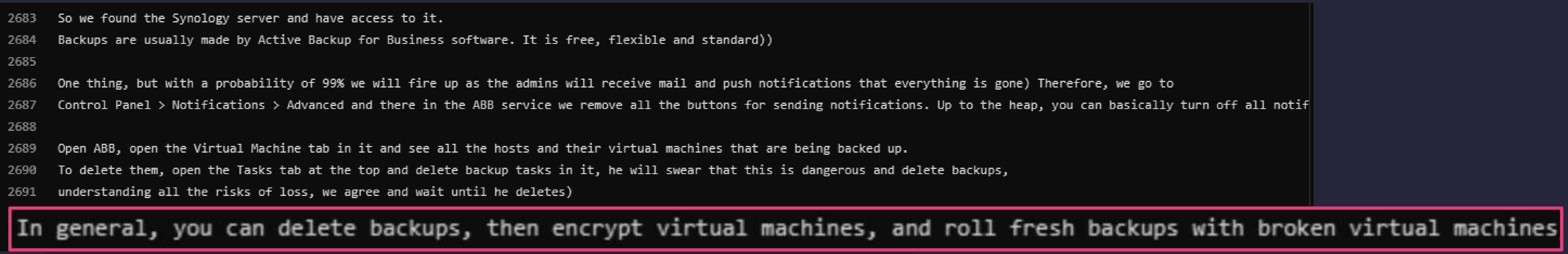
- **Threat-informed** approach to understanding:
  - Priorities
  - Policies
  - Risks / costs
- Tabletop assessments



It is critical to maintain offline, encrypted backups of data and to regularly test your backups. Backup procedures should be conducted on a regular basis. It is important that backups be maintained offline as many ransomware variants attempt to find and delete any accessible backups. Maintaining offline, current backups is most critical because there is no need to pay a ransom for data that is readily accessible to your organization.

Excerpt from cisa.gov/stopransomware/ransomware-guide

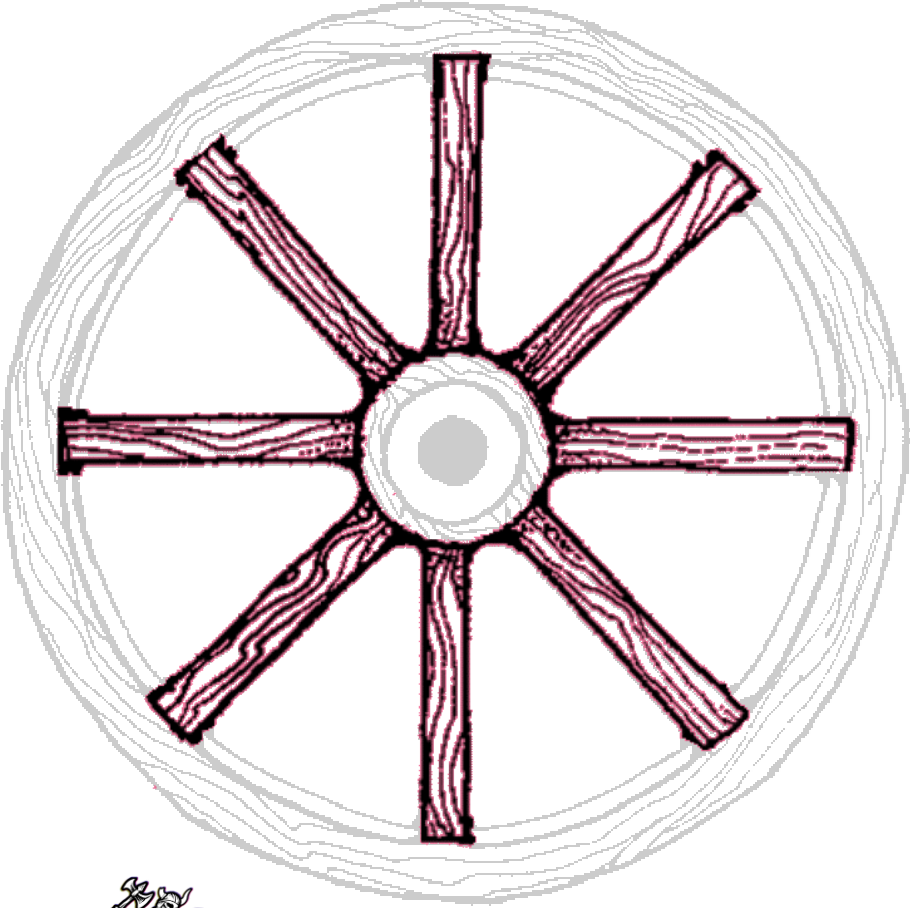




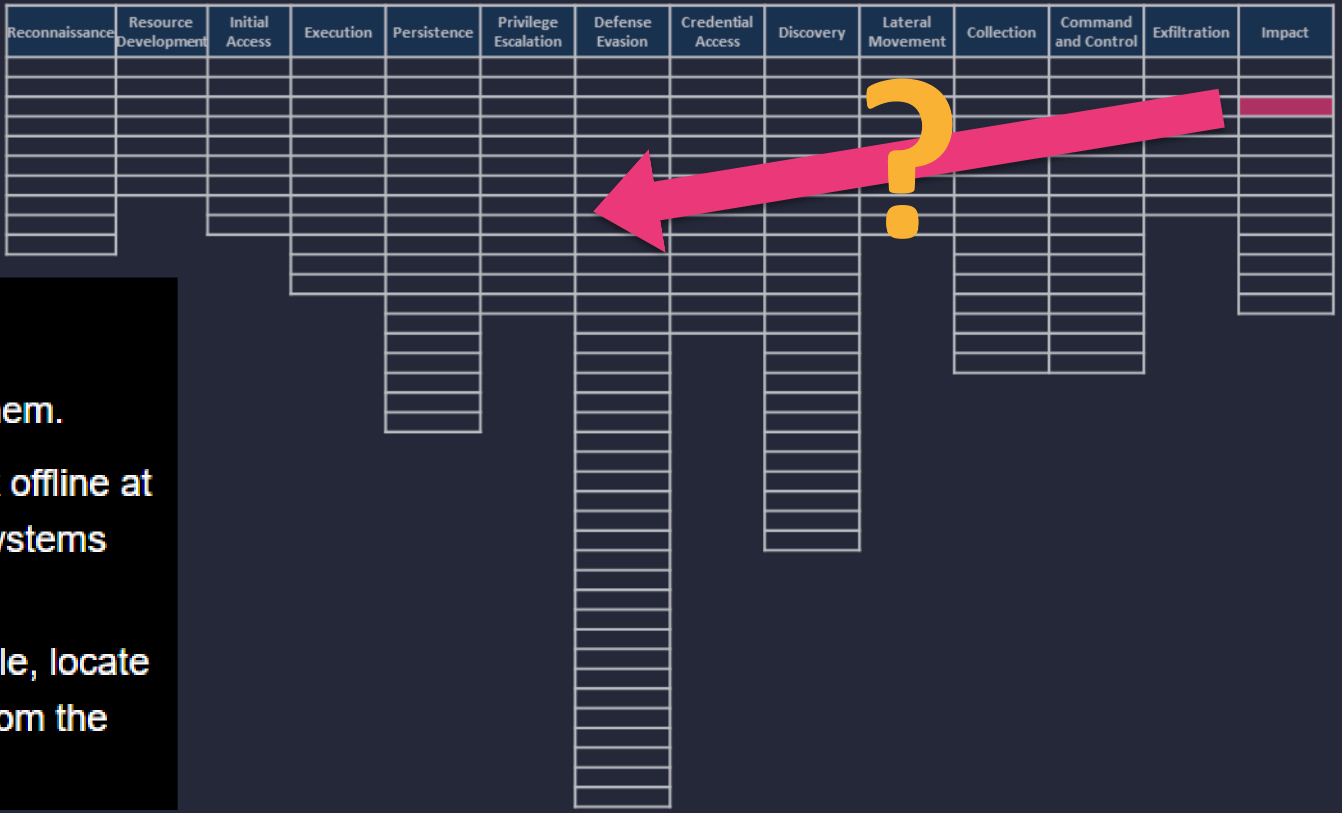
```
So we found the Synology server and have access to it.
Backups are usually made by Active Backup for Business software. It is free, flexible and standard))

One thing, but with a probability of 99% we will fire up as the admins will receive mail and push notifications that everything is gone) Therefore, we go to
Control Panel > Notifications > Advanced and there in the ABB service we remove all the buttons for sending notifications. Up to the heap, you can basically turn off all notif

Open ABB, open the Virtual Machine tab in it and see all the hosts and their virtual machines that are being backed up.
To delete them, open the Tasks tab at the top and delete backup tasks in it, he will swear that this is dangerous and delete backups,
understanding all the risks of loss, we agree and wait until he deletes)
In general, you can delete backups, then encrypt virtual machines, and roll fresh backups with broken virtual machines
```

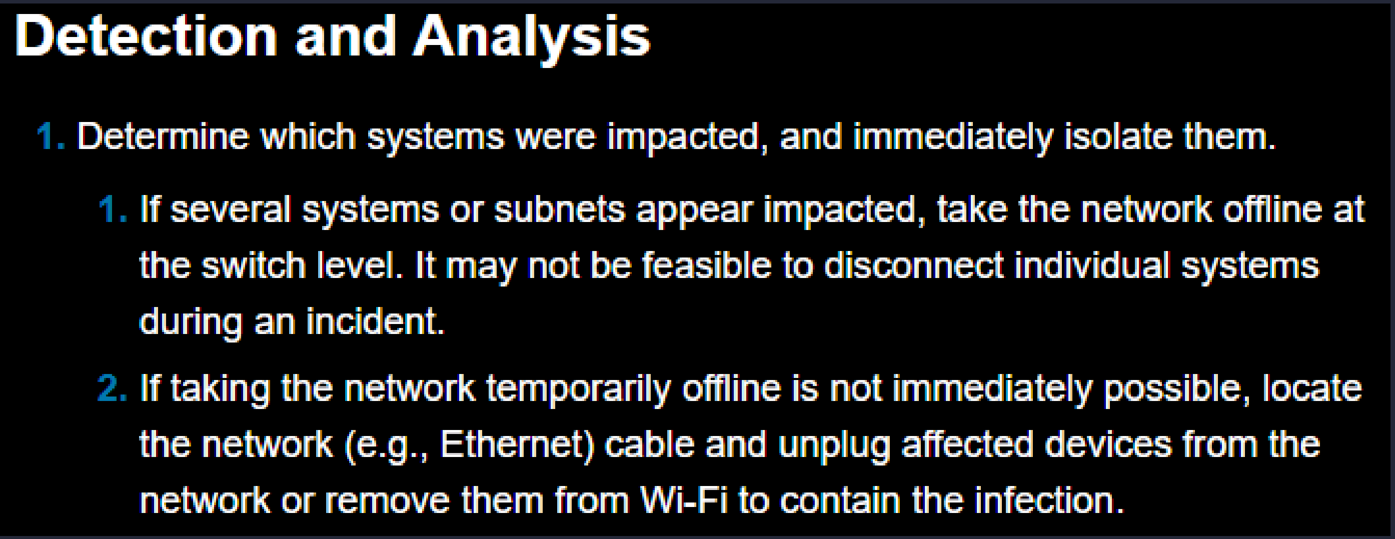
Excerpt from github.com/tsale/translated_conti_leaked_comms

Security Operations



- **Threat-informed** approach to understanding how strategy is implemented through:
  - Detection
  - Response
  - Remediation
- Scenario-based assessments

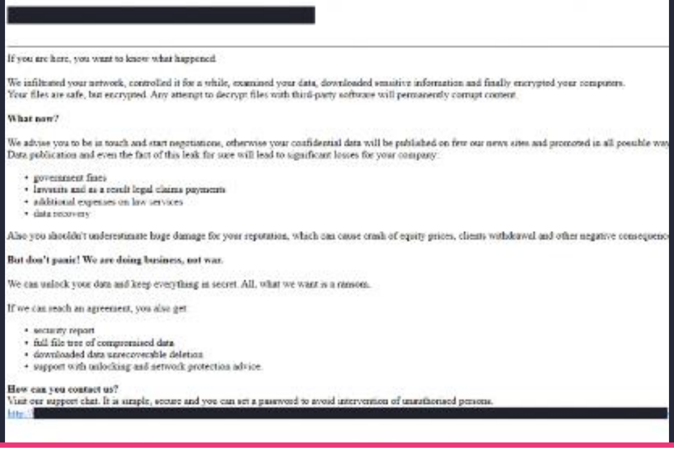




Detection and Analysis

1. Determine which systems were impacted, and immediately isolate them.
   1. If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
   2. If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.

Excerpt from cisa.gov/stopransomware/ransomware-guide



[redacted]

If you are here, you want to know what happened.

We infiltrated your network, controlled it for a while, examined your data, downloaded sensitive information and finally encrypted your computers.
Your files are safe, but encrypted. Any attempt to decrypt files with third-party software will permanently corrupt content.

What now?

We advise you to be in touch and start negotiations, otherwise your confidential data will be published on few our news sites and promoted in all possible way
Data publication and even the fact of this leak for sure will lead to significant losses for your company:

- government fines
- lawsuits and as a result legal claims payments
- additional expenses on law services
- data recovery

Also you shouldn't underestimate huge damage for your reputation, which can cause crash of equity prices, clients withdrawal and other negative consequenc

But don't panic! We are doing business, not war.

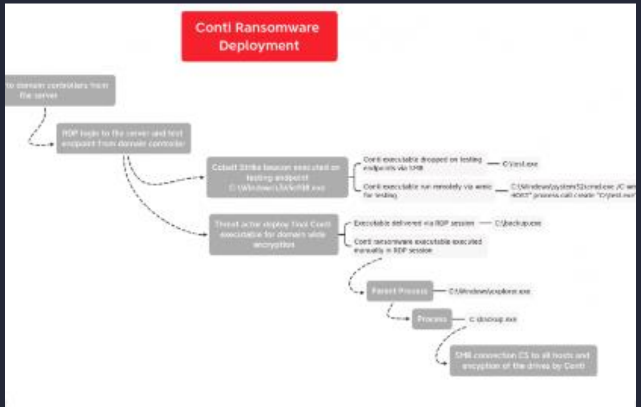
We can unlock your data and keep everything in secret. All, what we want is a ransom.

If we can reach an agreement, you also get:

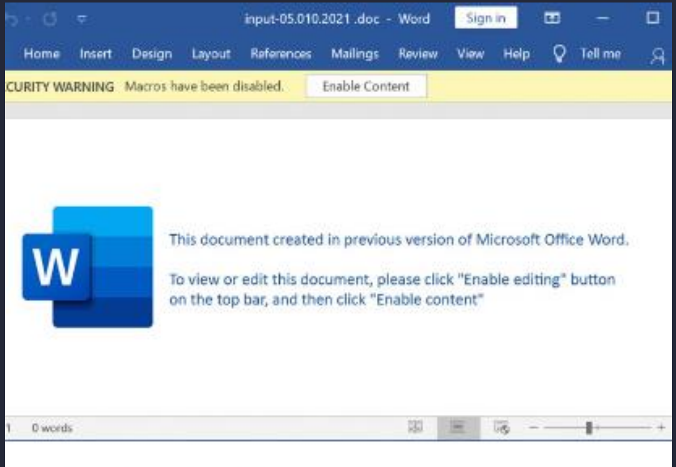
- security report
- full file tree of compromised data
- downloaded data unrecoverable deletion
- support with unlocking and network protection advice.

How can you contact us?
Visit our support chat. It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http://[redacted]

IcedID to XingLocker Ransomware in 24 hours


Conti Ransomware Deployment
to domain controllers from the server
RDP login to the server and test endpoint from domain controller
Conti executable dropped on testing endpoints via SMB
C:\test.exe
Conti executable run remotely via wmic for testing
Threat actor deploys final Conti executable for domain wide encryption
Executable delivered via RDP session
C:\backup.exe
Conti ransomware executable executed manually in RDP session
Parent Process
C:\Windows\explorer.exe
Process
SMB connection C$ to all hosts and encryption of the drives by Conti

BazarLoader to Conti Ransomware in 32 Hours



CURITY WARNING Macros have been disabled.

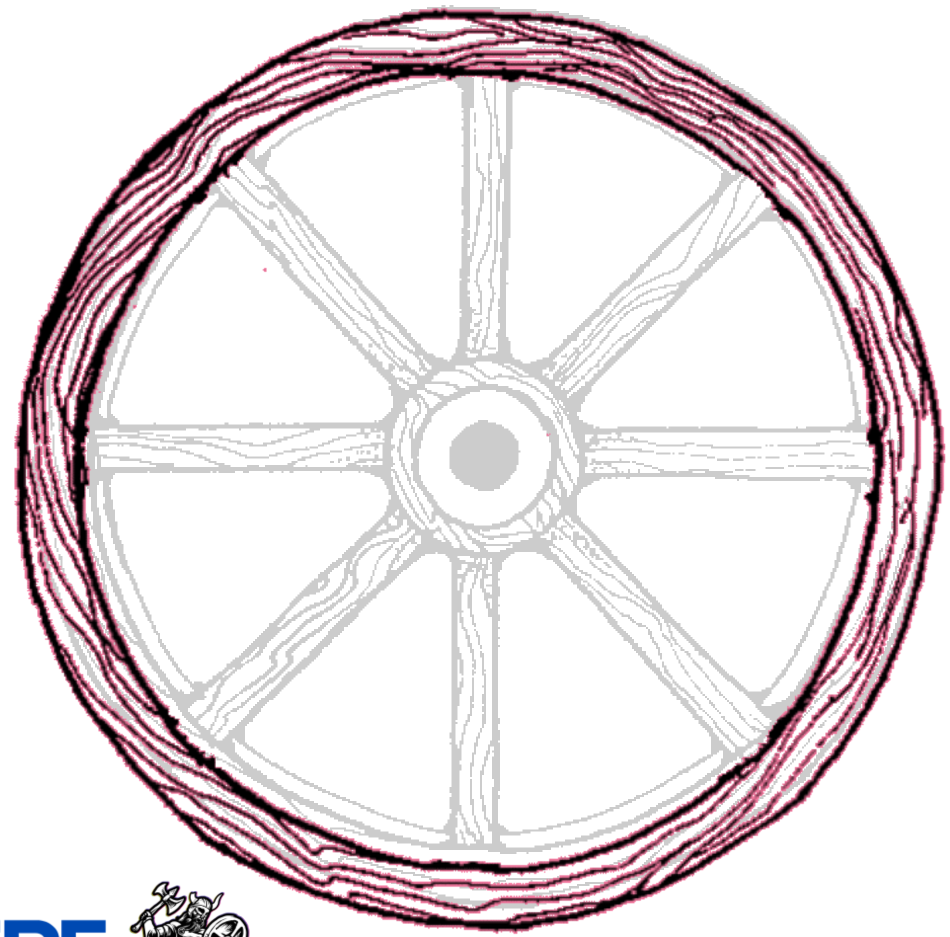
This document created in previous version of Microsoft Office Word.

To view or edit this document, please click "Enable editing" button on the top bar, and then click "Enable content"

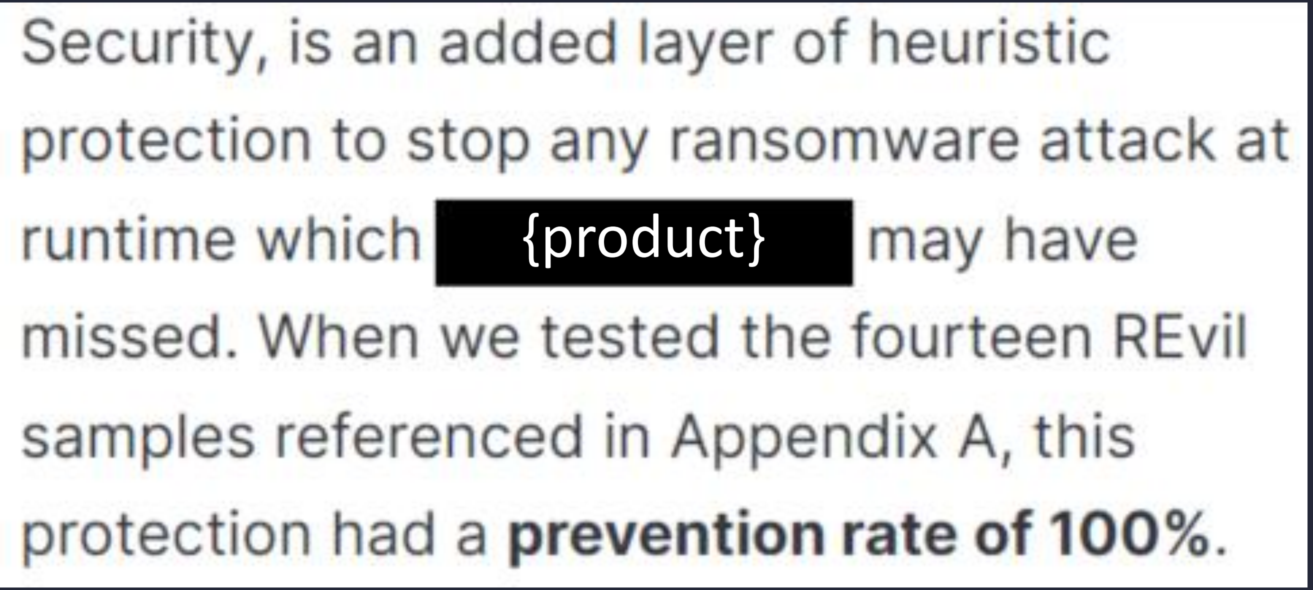
From Word to Lateral Movement in 1 Hour

Excerpts from thedfirreport.com

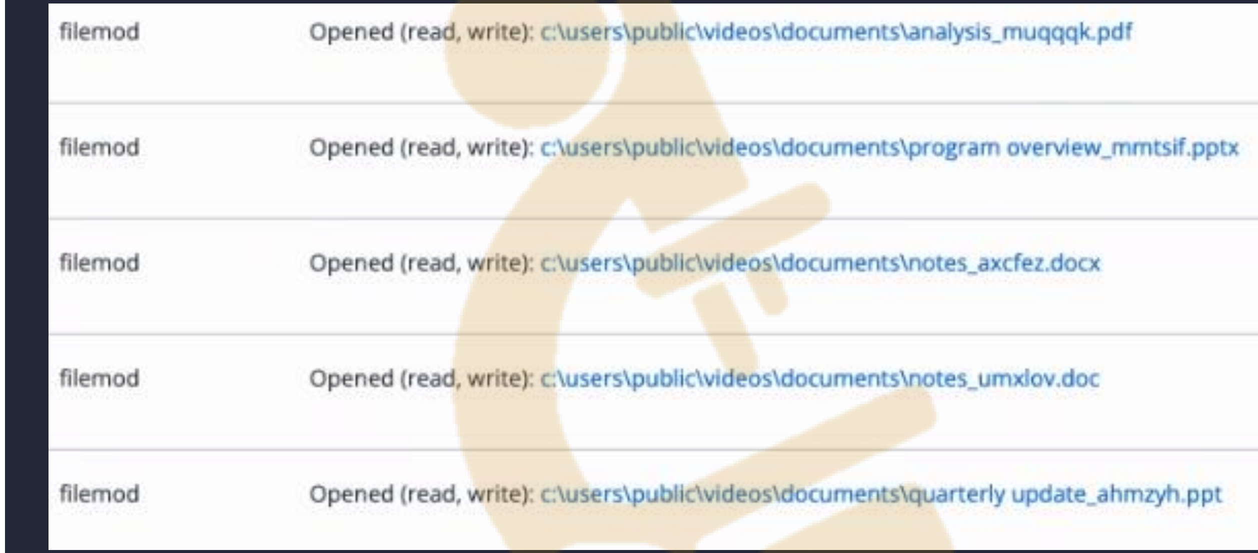
Security Tooling & Infrastructure



- **Threat-informed** approach to enabling operations through tooling:
  - Selection
  - Configuration
  - Evolution
- Product assessments



Security, is an added layer of heuristic protection to stop any ransomware attack at runtime which {product} may have missed. When we tested the fourteen REvil samples referenced in Appendix A, this protection had a **prevention rate of 100%**.



```
filemod    Opened (read, write): c:\users\public\videos\documents\analysis_muqqqk.pdf
filemod    Opened (read, write): c:\users\public\videos\documents\program overview_mmtsif.pptx
filemod    Opened (read, write): c:\users\public\videos\documents\notes_axcfez.docx
filemod    Opened (read, write): c:\users\public\videos\documents\notes_umxlov.doc
filemod    Opened (read, write): c:\users\public\videos\documents\quarterly update_ahmzyh.ppt
```

Bringing It All Back Together

Strategy

Operations

Tooling & Infrastructure

RSAConference™2023

Stronger Together

Wrapping Up

#RSAC

Summary

Adversary emulation can help **contextualize** various levels of **security-decisions** towards providing real **impact to the business**

Thank you for your time and attention!