



jaapbrasser.com/about







State of PowerShell

Demo Mimikatz & PowerShell Logging

## Demo Summary

- Setup PowerShell logging
- Dump credentials
- Reconfigure logging
- Follow bread crumbs
- Determined what ran



Demo
Obfuscation &
Detection

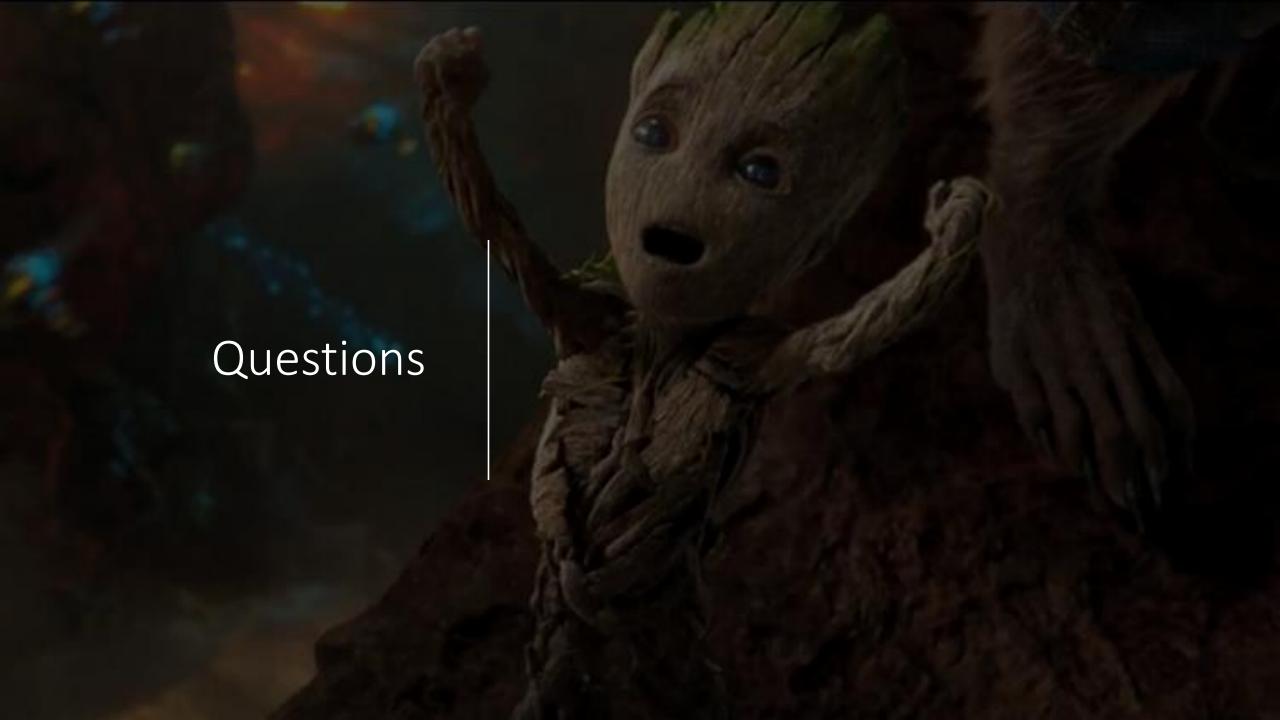


## Demo Summary

- Determined character frequency
- Used Vector Frequency
- Encoded existing scripts
- Looked at different methods of obfuscation



Defensive PowerShell



## References

- github.com/jaapbrasser/Events/tree/master/BSidesAms2017
- www.bsidesams.nl
- jaapbrasser.com