The SolarWinds Incident

Frank Appunn

Professor, Researcher, & Consultant

All content sourced from public sources

Maine InfraGard Members Alliance
A Partnership for Protection

THOMAS

SolarWinds Part 2

7. Why SolarWinds?
8. Government Agencies
9. Russian Involvement
10. Private Companies
11. Who is at Risk in the Future?
12. My Protection

Why SolarWinds

- Trusted supply chain source
- Their products connect to many things
- The products run at escalated security levels
- Manipulated inclusion of bad code into an update
- Attacks
- Global
- Microsoft: “the largest and most sophisticated attack the world has ever seen.”

Government Agencies

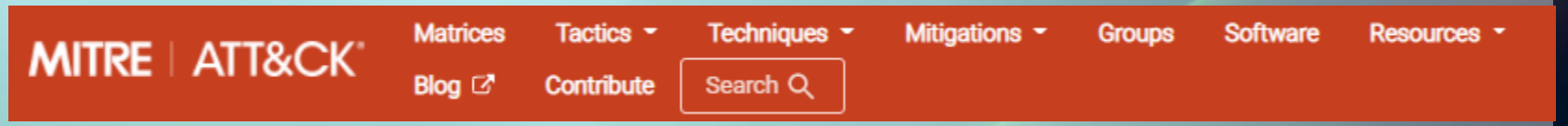
- Numbers are fuzzy. Estimates over 10 000 instances
- Yielded the fifth emergency directive since 2015

- Targets reported: Treasury, DHS, State Department, DOJ, NSA, Los Alamos Labs (nuclear), NASA, CDC.

- Expectation was a shutdown, forensic copy and blocks

Russian Involvement

- Attribution is difficult
- Russia is fashionable
- Russia is plausible
- UNC2452 Mandiant (FireEye)
- MITRE ATT&CK and Groups
  - 2019 think tank
  - Mailbox user discovery
  - Transport
  - Manual activity to compromise – Cobalt Strike, Raindrop, Sunburst



Private Companies

- Microsoft – source code
- FireEye – source code
- But it becomes cloudy
  - AWS
- Affected or attacked?
- Mimecast, Ford, Ernst & Young, Blue Cross, Cisco, PWC, Lockheed Martin, AT&T, New York times …and many more.
- But, were there losses?

Who is at Risk in the Future?

- It is the concept that should scare you.

- Everyone is at risk
- Passive defense?

- There are new ideas and tools on earth

My Protection

- Least Privilege
- Zero Trust
- People and products
- Least privilege, by design.