//adamnet.works

CASE STUDY

Case Study: Orion Solar Winds Breach
adam:ONE® vs Solarigate

- Trojanized software update March - June 2020.
- Threat actors from Russia. APT: UNC2452 Nobelium.
- Discovered By FireEye only 9 months later.
- 30% of attacks were on companies with no direct link to Solar Winds by gaining access to affected cloud services. .
- All defenses of the world's top security systems failed due to failure of detection.

adam:ONE®

- **All of the managed adam:ONE® users in ZTc configuration were immune to the attack from day 0** without any of us knowing that the attack existed. All exfiltration channels as well as command and control was blocked by default by adam:ONE®.
- Once news broke of the threat discovered by FireEye, we were able to go back and see in logs that **all attempted connections were neutralized (along with all other unverified or unknown DNS or IP connection requests)**. Our clients' immunity against this attack verifies the statement released by CISA that *proper egress control could have successfully mitigated the attack.*

18,000 Victims WERE BREACHED USING THE BEST-IN-CLASS STATUS QUO SECURITY STACKS. Including:

- US Treasury Department,
- Cybersecurity and Infrastructure Agency (CISA)
- The Department of Homeland Security (DHS)
- US Department of State
- US Department of Energy (DOE)
- US cybersecurity firm FireEye (Now Mandiant, acquired by Google)
- The US Department of Commerce NTIA
- The Department of Health's National Institute of Health (NIH)
- Fortune 500 companies

Outcomes:

- ADAM technology has proven to be **immune to APT attacks** such as the **Solar Winds breach** and **Pegasus.**
- Our users were **protected BEFORE the threats became known** and did not require detection from any Next-Gen system or endpoint software still safely in operation behind ZTc.

Protecting the people and systems you care about. ™

contact@adamnet.works

See adam:ONE® in action:
adamnet.io/C2begone

For a more detailed case description: adamnet.io/IR