SolarStorm Privacy & Security Forum

John Martineau – Principal Consultant

May 2021

Agenda

1. Introductions
2. In the beginning...
3. SolarStorm Timeline
4. SolarStorm Attack Lifecycle
5. The Story Continues...

Introductions

John Martineau – Principal Consultant
Pittsburgh, PA

- Champlain Grad
- Many letters (GASF, GREM, GCFA, ENCE)
- Love DFIR puzzles

Our Story Begins on December 8th...

FireEye reported a breach and data exfiltration of red team tools.

Dec. 8, 2020

...And Then the Plot Thickened

FireEye reported a breach and data exfiltration of red team tools.

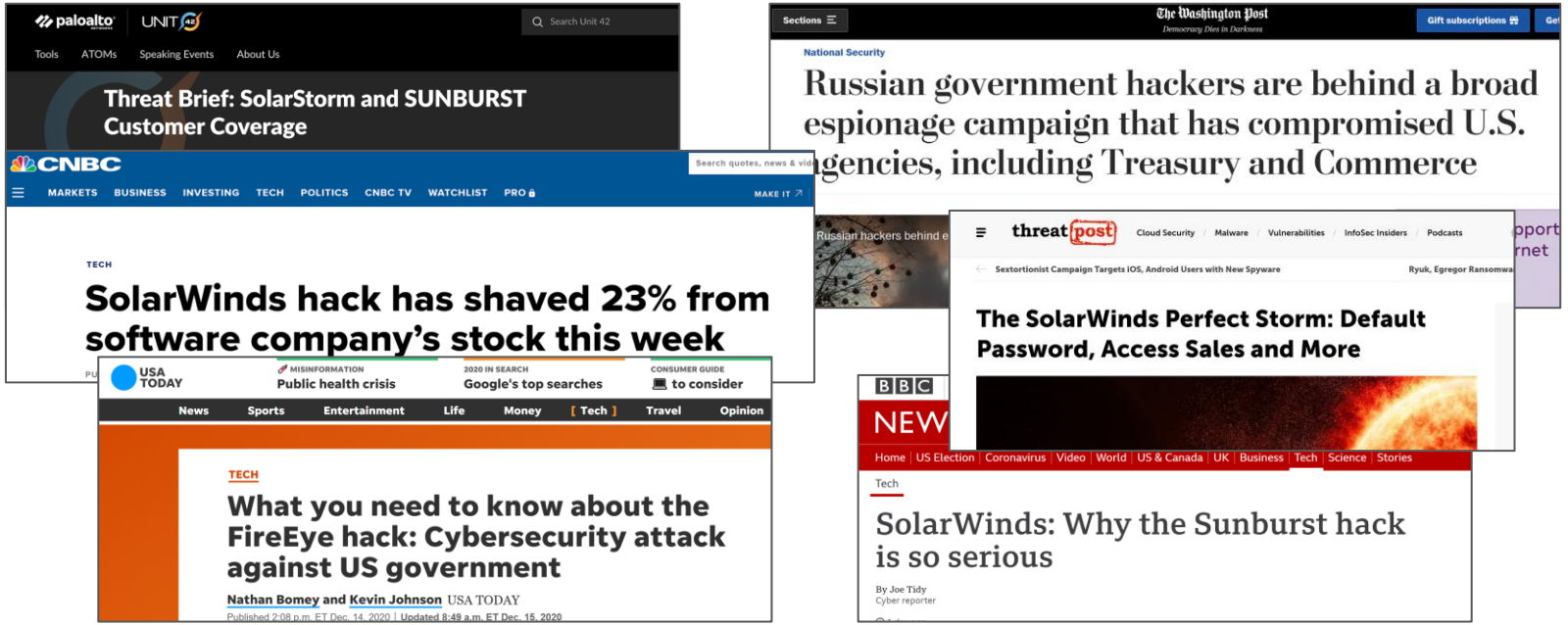
Dec. 8, 2020

FireEye shared information related to the breach, disclosing that the breach is a part of a widespread campaign, carried out by a group we refer to as **SolarStorm**.

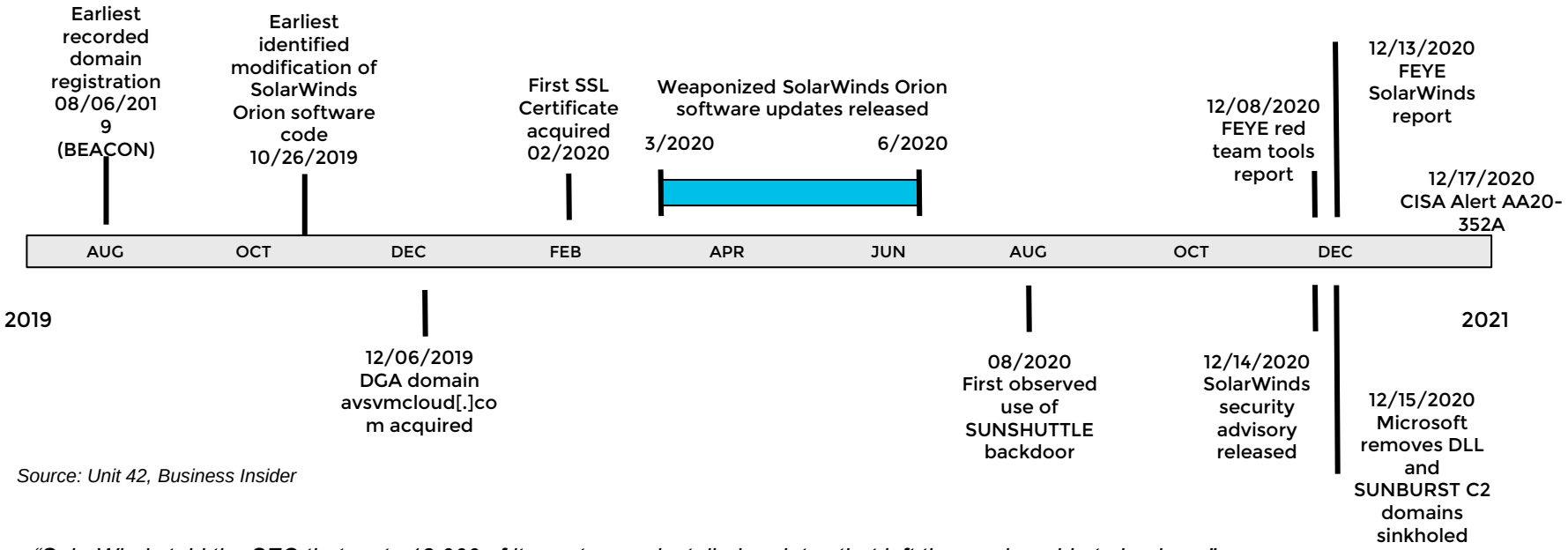
Dec. 13, 2020

The SolarStorm Group Executed a SolarWinds Supply Chain Attack

- ~18,000 SolarWinds customers were potentially infected with a malicious DLL file
- Once installed, attackers could steal credentials, move laterally and exfiltrate data



“SolarStorm” – SolarWinds Zero Day



Source: Unit 42, Business Insider

“SolarWinds told the SEC that up to 18,000 of its customers installed updates that left them vulnerable to hackers.”

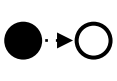
SolarStorm Attack Lifecycle

1. SolarWinds Orion downloads malicious update DLL file (SUNBURST)

2. Malicious update file downloads DLL file with CobaltStrike (TEARDROP and RAINDROP)

3. CobaltStrike attempts to beacon to C2

4. Lateral Movement \ Persistence \ Reconnaissance



5. Exfiltration

The Story Continues…

- March 2021 –
  - Microsoft and FireEye publish about new malware (SUNSHUTTLE) potentially tied to the threat actors behind the SolarWinds supply chain attack
- April 2021 –
  - White House ties activity to SVR (Russia)
  - RiskIQ released 77 domains, IP addresses, and SSL certificates potentially associated with the TA
- May 2021 –
  - SolarWinds reports the earliest sign of compromise within their environment was January 2019
  - Actual post SUNBURST exploitation customer numbers according to SolarWinds were “fewer than 100”
  - CISA releases Fact Sheet on Russian SVR activities related to SolarWinds compromise

