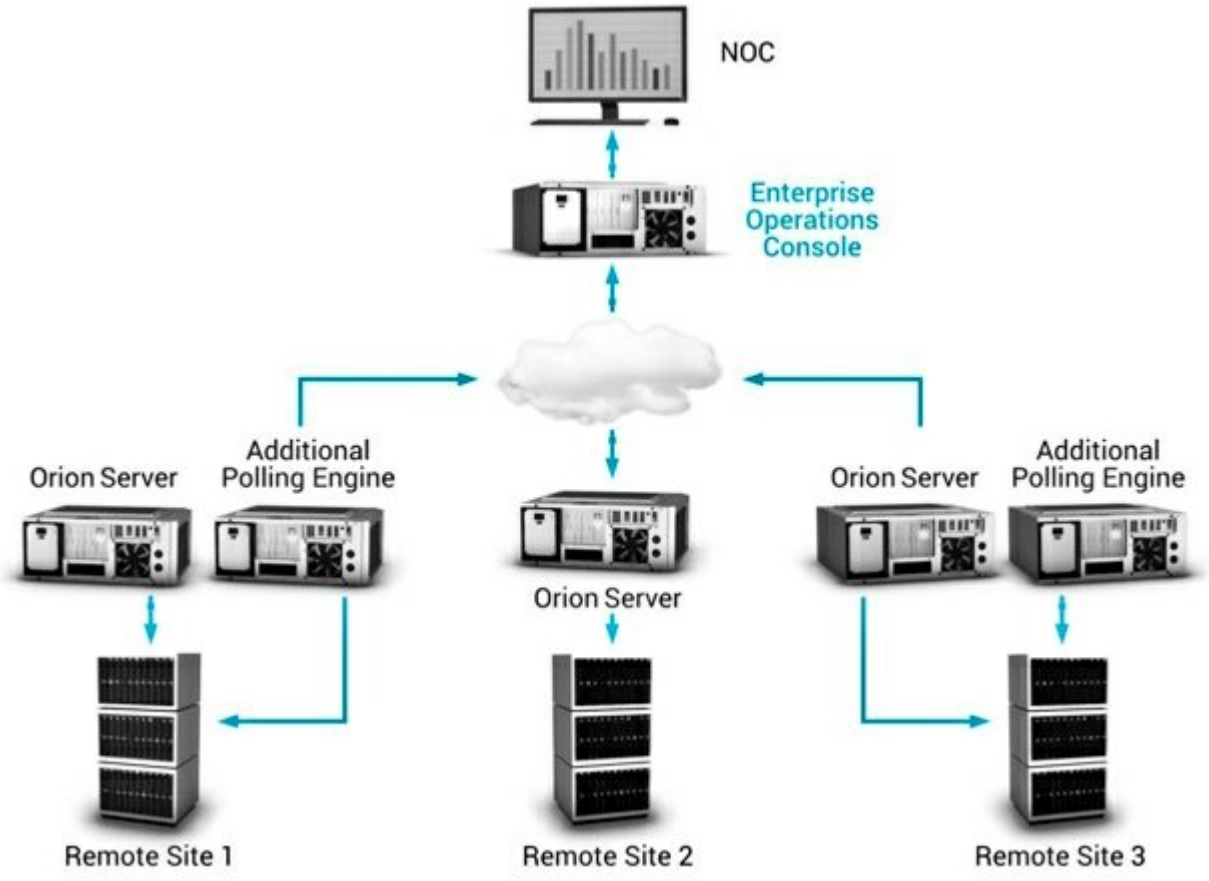
Twitter Thread by John Basham ■■

John Basham ■■
@JohnBasham

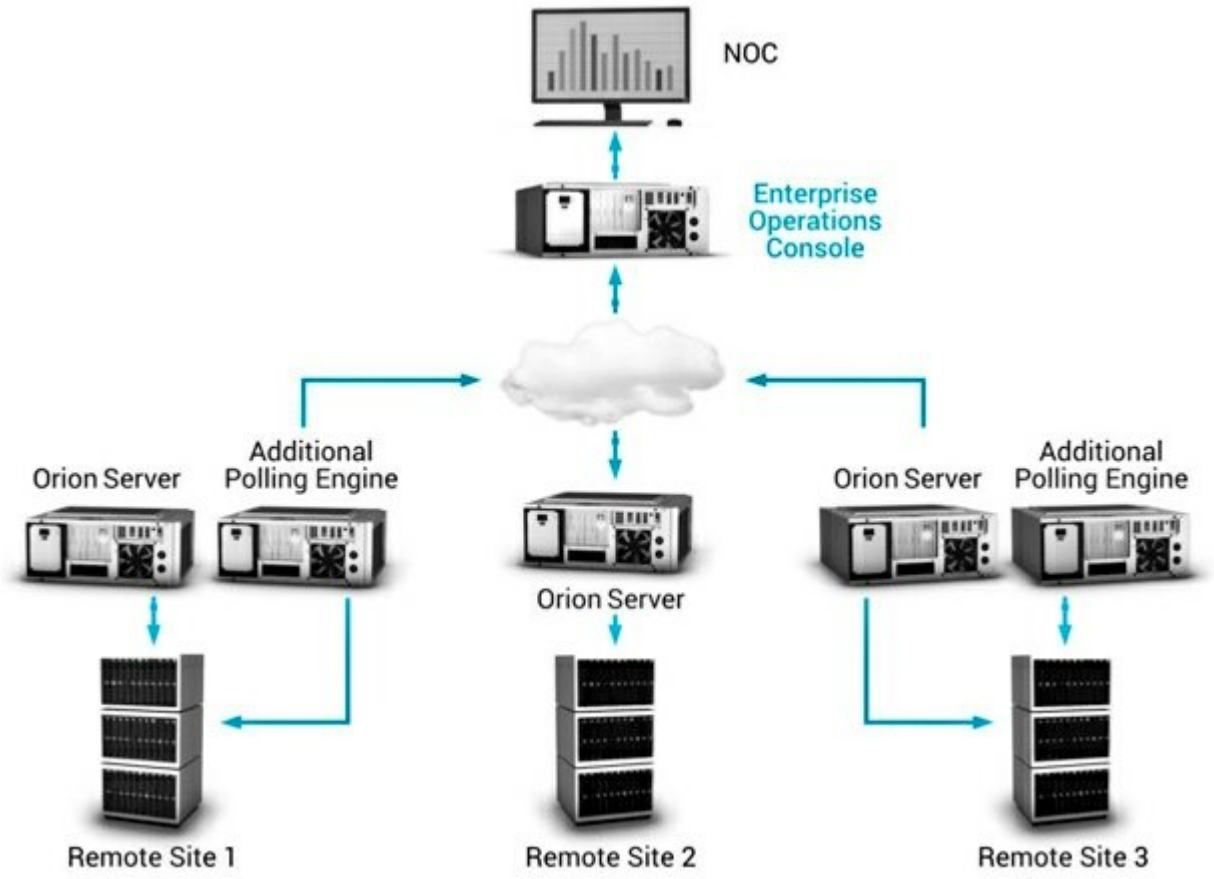
FLASH: "Emergency Directive 21-01 calls on all federal civilian agencies to review their networks for indicators of compromise and disconnect or power down SolarWinds Orion products immediately."-@CISAgov Read more:

CONTD: @CISAgov is responding to an exploit of Federally operated @solarwinds Orion products by malicious actors. They Issued an Emergency Directive to federal civilian agencies to review networks & DISCONNECT OR POWER DOWN ALL SOLARWINDS ORION PRODUCTS NOW!



CONTD: @FireEye discovered an attack trojanizing @solarwinds Orion biz software distributing malware named #SUNBURST.
The attacker's use multiple techniques to evade detection/obscure activity. The campaign is widespread affecting public &

private organizations around the world.

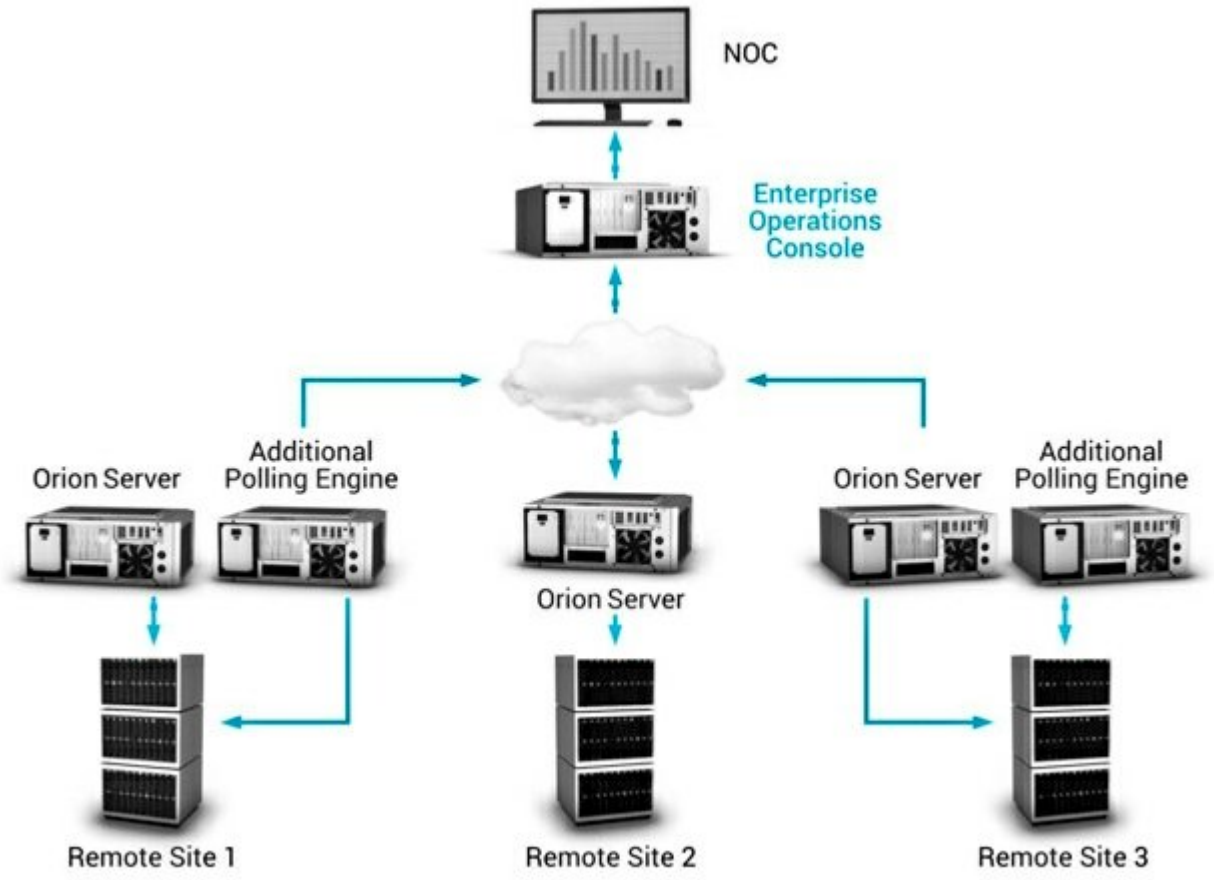


CONTD: The trojan version of a @SolarWinds Orion plug-in codename #SUNBURST. After a dormant period of up to 2 weeks, it retrieves & executes commands including transfering files, executing files, profile the system, reboot, & disable system services.... more

CONTD: #SUNBURST hides network traffic & stores recon within legitimate plugin configuration files allowing it to blend in with legitimate activity. The backdoor uses obfuscated blocklists to i.d. forensic & anti-virus tools running as processes, services, & drivers.... more

CONTD: Worldwide Victims With #SUNBURST Distributed March thru May 2020. @FireEye has detected this malware in government, consulting, tech, telecom & extractive entities in North America, Europe, Asia & the Middle East & anticipate there are additional victims.... more

CONTD: After #SUNBURST gains access the attacker group disguise their operations moving laterally in the compromised network. The attacker maintains a light malware footprint, instead preferring legitimate credentials & remote access for access through the victim’s environment.



CONTD: If @SolarWinds infrastructure is not isolated:
-Restrict scope of connectivity to endpoints from SolarWinds servers!
-Restrict the scope of accounts that have local administrator privileged on SolarWinds servers!
.... more

CONTD: If @solarwinds infrastructure is not isolated:
-Block Internet egress from servers or other endpoints with SolarWinds software.
-At MINIMUM changing passwords for accounts that have access to SolarWinds servers / infrastructure.
....more

CONTD: If @solarwinds manages networking infrastructure:
-Review network device configurations for unexpected / unauthorized modifications. This is a proactive measure due to the scope of SolarWinds functionality.

CONTD: @SolarWinds' Customers;
-425+ of US Fortune 500 co's
-All of top 10 US telecom co's
-All 5 branches US Military
-Pentagon
-State Department
-NASA
-NSA
-USPS
-NOAA

-DOJ
-Office of POTUS
-Top 5 US accounting firms
-100's universities/colleges
List: https://t.co/N202UZdyjC