Shining the light on SUNBURST:

IRONNET BEHAVIORAL ANALYTICS + COLLECTIVE DEFENSE

Perhaps the **biggest cybersecurity news of 2020** was the **SolarWinds/SUNBURST breach**.

WHO?
Presumably nation-state adversaries of Russian origin

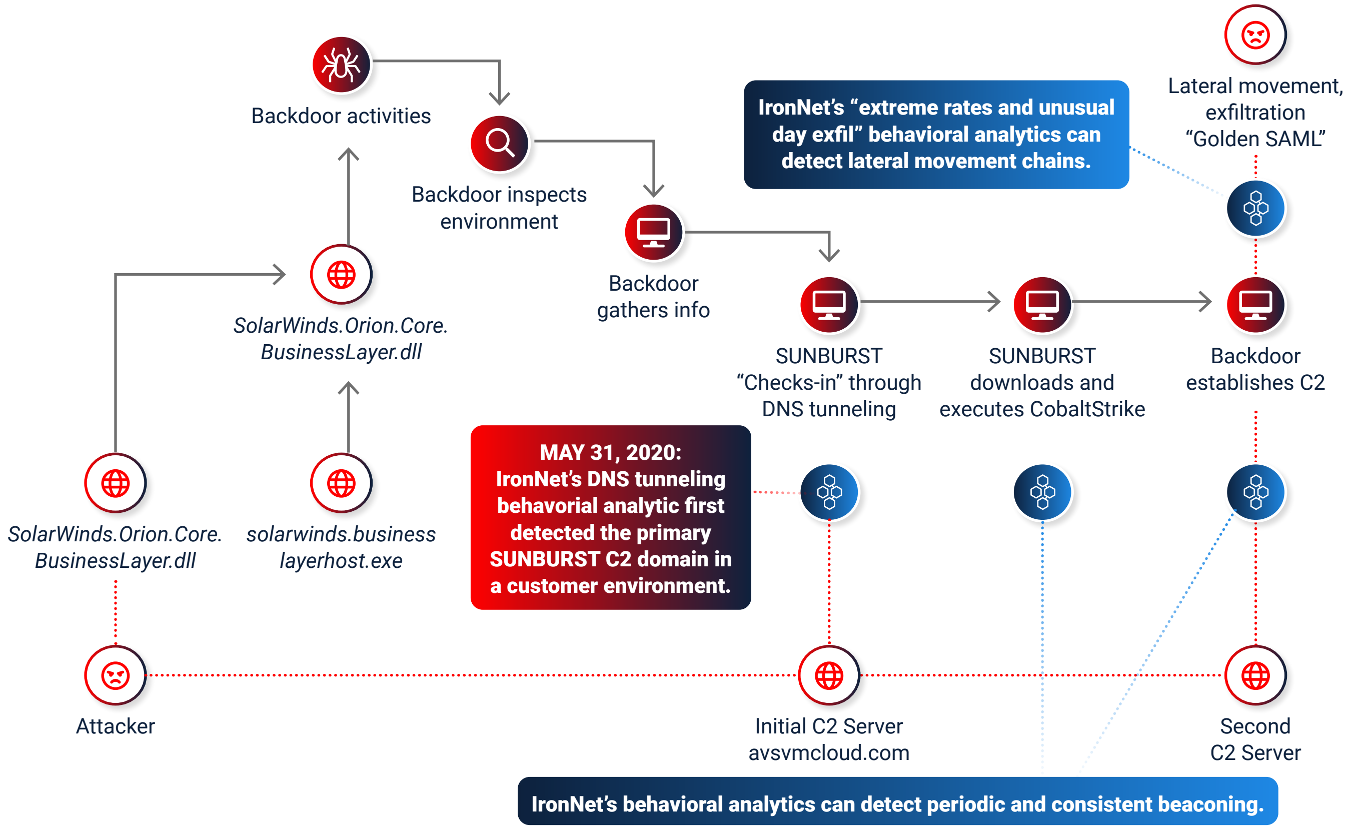
WHAT?
A malware attack that used an IT management software update as a "backdoor" to a vast supply chain

WHERE?
Globally exposed 18,000 customers of SolarWinds IT management software

WHY?
Presumably to piggyback on a supply chain backdoor to access federal government networks in the U.S.

HOW?
By using sophisticated techniques to hide command and control traffic, such as mimicking SolarWinds Orion traffic and leveraging cloud providers to masquerade as trusted geolocated environments

WHICH IRONNET BEHAVIORIAL ANALYTICS CAN DETECT SUNBURST TECHNIQUES?


Backdoor activities
Backdoor inspects environment
Backdoor gathers info
Lateral movement, exfiltration "Golden SAML"
SolarWinds.Orion.Core. BusinessLayer.dll
SUNBURST "Checks-in" through DNS tunneling
SUNBURST downloads and executes CobaltStrike
Backdoor establishes C2
SolarWinds.Orion.Core. BusinessLayer.dll
solarwinds.business layerhost.exe
Attacker
Initial C2 Server avsvmcloud.com
Second C2 Server

IronNet's "extreme rates and unusual day exfil" behavioral analytics can detect lateral movement chains.

MAY 31, 2020: IronNet's DNS tunneling behavorial analytic first detected the primary SUNBURST C2 domain in a customer environment.

IronNet's behavioral analytics can detect periodic and consistent beaconing.

IronNet aided customer response to SUNBURST by supporting investigations, collaborating with customers, and using alerting to help provide context.

IronNet™

Visit IronNet.com to schedule a live demo

> *"IronNet is a partner, not a vendor. You are the first call I make when I need support and a second set of eyes to help determine "what's next."*
>
> — LARGE ENERGY UTILITY COMPANY, IN RESPONSE TO IRONNET'S SUNBURST SUPPORT