Infocyte

If they try it, we'll stop it.

HUNTING FOR SUNBURST COMPROMISES

The recently discovered SolarWinds Orion compromise is looking like it might be the most extensive hack in history. Every organization using SolarWinds Orion versions 1029.4 through 2020.2.1 (per the Homeland Security advisory linked here) for server monitoring is advised to assume that their servers and networks are compromised by the actors responsible. Initial estimates are that 18,000+ entities including most Fortune 500 companies and many sensitive government entities are users of the software. As the situation continues to evolve, Infocyte is working to help those that need it in any way we can.

Infocyte proactively began hunting and notifying our customers who may be affected by the malware. As a result of this effort, we have tested and published an official Infocyte extension which scans servers for all reported Sunburst host-based indicators of compromise related to this compromise or vulnerability. Users and partners are advised to run this on your servers in addition to our standard memory scans that will pick up the secondary payloads (like Cobalt Strike) which are injected by the SolarWinds embedded malware.

WITH INFOCYTE, ORGANIZATIONS CAN:

- Deploy in minutes with our **agentless** option
- Find any potential vulnerabilities quickly and with precision
- Hunt and detect potential exploits or compromises from such vulnerabilities based on **live memory and forensic analysis**
- Respond immediately across your entire network via our cloud console
- You have the option to have our certified experts or partners provide third party validation that the assessment is successful and compromises are eradicated

When it comes to unprecedented incidents of this magnitude, Infocyte has the benefit of technology that truly delivers on swift, effective endpoint detection and response as well as incident response.

Learn more: infocyte.com/sunburst

ADDITIONAL RECOMMENDATIONS:

If you are unsure which machines have the SolarWinds Orion Application installed on, you can use Infocyte to view all applications that were found in the last 90 days under the ***Analyze*** tab.

1. CISA and FireEye have recommended blocking all traffic to and from hosts that have SolarWinds Orion installed and monitor your network traffic for anomalies.
2. CISA recommends organizations"**Forensically image** system memory and/or host operating systems hosting all instances of SolarWinds Orion versions 2019.4 through 2020.2.1. Analyze for new user or service accounts, privileged or otherwise." A quick version of these actions can be performed via the Infocyte platform.
3. Use Infocyte to scan your entire server environment for secondary memory-only remote access tools (RATs) like Cobalt Strike.
4. Check Orion management servers for .net web shells (SUPERNOVA)
5. Ensure you are conducting host-based behavior monitoring via enabling real-time monitoring in Infocyte. Look for powershell activity and one-to-many administrative connections coming from Orion servers or servers in their local subnet.

Remember, having Orion isn't confirmation that your data and network were totally lost. It means the actors had opportunity but with tens of thousands of targets, it's likely they triaged those networks for the best targets first.

No one should go through a breach alone. If there is anything we can help with, please reach out to us. Existing customers and partners have direct access to our team via the chat interface in the Infocyte app.

PHONE: 844.463.6298

EMAIL: sales@infocyte.com

ABOUT INFOCYTE

Founded by the leaders of the United States Air Force Cyber Incident Response Team (AFCIRT), Infocyte is the globally trusted leader in proactive threat detection and incident response. The world's leading security and incident response companies use Infocyte's platform to proactively detect and respond to vulnerabilities and threats within their customers' endpoints, data centers, and cloud environments. Infocyte's team and partner ecosystem help organizations maintain compliance, stop ransomware and account takeover, reduce risk, optimize security operations, and scale security teams. Infocyte is the faster, simpler, smarter way to detect and orchestrate response to sophisticated threats. Learn more at infocyte.com or follow us on Twitter: @InfocyteInc.