Breach Breakdown: Solarwinds

4/28/2021

Society for Cyber Security

BREACH BREAKDOWN: Solarwinds

Sep. 2019

Solarwinds is breached

Hackers break into Solarwinds and embed malicious code onto their Orion application.

Mar. - Jun.

Orion is shipped to customers

The infected network management software, Orion, is shipped to over 18,000 customers.

Jun. - Dec.

Hackers comb through victims data

Hackers make their way around victims networks.

Dec.

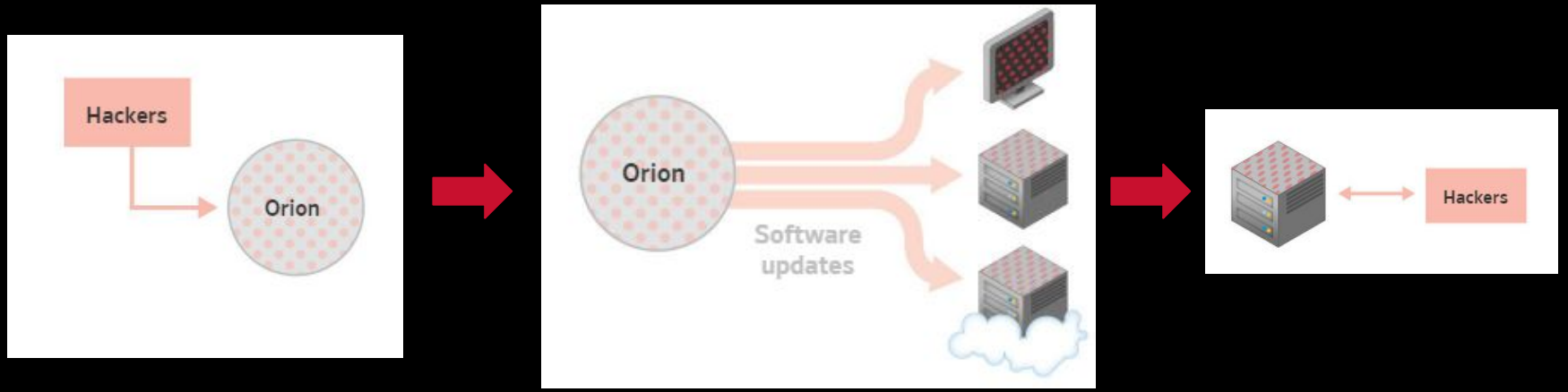
FireEye discovers malware

FireEye receives alert of a potentially compromised user and decides to investigate the incident.

Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

BREACH BREAKDOWN: Solarwinds

How did it happen?



Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

BREACH BREAKDOWN: Solarwinds

Who was affected?

FIREEYE™

intel®

Microsoft

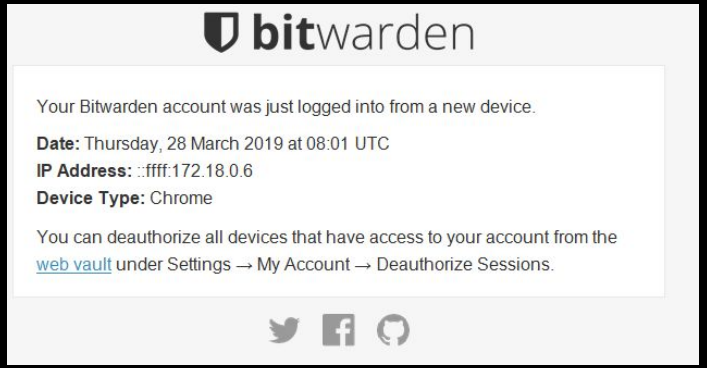
CISCO

vmware

Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

BREACH BREAKDOWN: Solarwinds

How was the malware discovered?



"We looked through 50,000 lines of source code, which we were able to determine there was a backdoor within SolarWinds," said Charles Carmakal, senior vice president and chief technical officer at Mandiant, FireEye's incident response arm.

Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

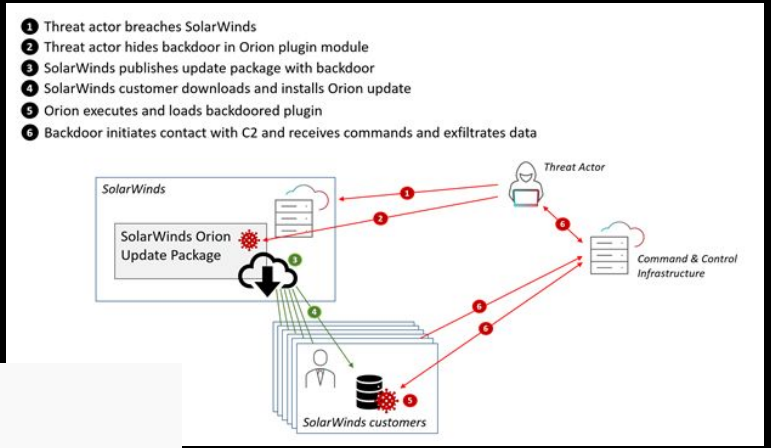
BREACH BREAKDOWN: Solarwinds

Who is behind the SUNBURST malware?

Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

BREACH BREAKDOWN: Solarwinds

What can we learn from this attack?



Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

BREACH BREAKDOWN: Solarwinds

Disclaimer: This organization for educational purpose only, and we are not condone hacking of other computers or enterprises. It is ILLEGAL to hack another computer other than your own. Please exercise ethical techniques when practicing the tools learned in this classroom.

BREACH BREAKDOWN: Solarwinds - Sources and Articles

- https://www.bloomberg.com/news/articles/2020-12-15/fireeye-stumbled-across-solarwinds-breach-while-probing-own-hack
- https://github.com/ITAYC0HEN/SUNBURST-Cracked/blob/main/OrionImprovementBusinessLayer_modified.cs
- https://www.wsj.com/articles/hack-suggests-new-scope-sophistication-for-cyberattacks-11608251360
- https://www.channele2e.com/technology/security/solarwinds-orion-breach-hacking-incident-timeline-and-updated-details/
- https://www.newsweek.com/solarwinds-orion-software-cyberattack-hack-victims-targets-list-1555840
- https://media-exp1.licdn.com/dms/document/C4D1FAQEUYT4vqLzDNw/feedshare-document-pdf-analyzed/0/1619469461234?e=1619560800&v=beta&t=vkZI_x52yHqL-num_MQYGoN4D7lL9EYs0ZCDHNs7v_I
- https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know#:~:text=How%20did%20the%20SolarWinds%20hack,to%20hack%20the%20networks%20directly.

SCS Social Media Handles

ugascs@gmail.com

https://ugascs.com

@uga.scs

@ugascs