Twitter Thread by George Webb - Investigative Journalist

George Webb - Investigative Journalist
@GeorgeW63613375

1. SolarWinds - an IT monitoring company with the NSA, all five military branches of the Pentagon, and several major civilian agencies, had their software hacked by the Russian hacker group Cozy Bear yesterday, the same group responsible for the 2016 DNC hack.

TECHNOLOGY NEWS DECEMBER 13, 2020 / 1:51 PM / UPDATED 3 HOURS AGO

Suspected Russian hackers spied on U.S. Treasury emails - sources

By Christopher Bing 5 MIN READ

WASHINGTON (Reuters) -Hackers believed to be working for Russia have been monitoring internal email traffic at the U.S. Treasury and Commerce departments, according to people familiar with the matter, adding they feared the hacks uncovered so far may be the tip of the iceberg.



2. SolarWinds uses a protocol called Orion Improvement Protocol (I believe this is a wrapper for RMON and SNMP calls), and this protocol was hacked at Treasury and NTIA, the National Telecommunication advisor agency.

FIREEYE™ Products Mandiant Solutions Customers Par

Threat Research

Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor

December 13, 2020 | by FireEye

FIREEYE EVASION SUPPLY CHAIN

Executive Summary

- We have discovered a global intrusion campaign. We are tracking the actors behind this campaign as UNC2452.
- FireEye discovered a supply chain attack trojanizing SolarWinds Orion business software updates in order to distribute malware we call SUNBURST.
- The attacker's post compromise activity leverages multiple techniques to evade detection and obscure their activity, but these efforts also offer some opportunities for detection.
- The campaign is widespread, affecting public and private organizations around the world.
- FireEye is releasing signatures to detect this threat actor and supply chain attack in the wild. These are found on our public GitHub page. FireEye products and services can help customers detect and block this attack.

Summary

FireEye has uncovered a widespread campaign, that we are tracking as UNC2452. The actors behind this campaign gained access to numerous public and private organizations around the world. They gained access to

3. As a veteran of hacking forensics, I always look at modus operandi by malicious groups and at human factor compromises as the first investigative avenues to pursue. My research partner Jen Moore discovered Pavel Yershov lead the 2016 attack for GRU also worked for Microsoft.



Task Force Find Cozy Bears (Nataliia Sova) To Fancy Bears Link (Yershov)

4. Interesting that Warren Flood also works for Microsoft Pro Services, and he was intimately involved in the 2016 DNC Microsoft GRU "Hack". Flood and his wife were instrumental in the Dominion Voting Machine purchases in Wayne County, Michigan and the State of Georgia,



5. Even more interesting that Warren Flood has worked for a long time for Joe Biden as has his wife.



Warren Flood

Microsoft Corporate Affairs for Detroit.

President

Bright Blue Data

Nov 2010 – Dec 2018 · 8 yrs 2 mos

Washington D.C. Metro Area

Analytics Special Projects Director

Obama for America

Oct 2011 – Nov 2012 · 1 yr 2 mos

Greater Chicago Area

6. We have also tracked two GRU hackers, Krylova and Bogacheva, to a safe house in Novi, Michigan, and Ypsilanti through a Kelly Service handler named Paul Whelan, a man convicted of espionage in Russia.

WORLD

Former US Marine Paul Whelan, convicted of espionage charges in Russia, gets 16-year prison sentence

Kim Hjelmgaard and Deirdre Shesgreen USA TODAY

Published 4:29 a.m. ET Jun. 15, 2020 | **Updated 2:31 p.m. ET Jun. 15, 2020**



7. A Ukrainian Hacker named Nataliia Sova was also involved in the Washington, DC area providing safe houses for Eastern European hackers in 2012, and she was married to a member of the Awan Spy Ring on Capitol Hill for the 2016 DNC "Hack".

Debbie Wasserman Schultz's IT Staffer Was Liquidating Multiple Properties Upon His Arrest

By Joseph A. Wulfsohn | Jul 30th, 2017, 10:01 pm

595 comments

Tweet reddit



8. Also, Peter Strzok's favorite Russian spy handler, Patrick Byrne, arranged meetings between Russian femme fatale Maria Butina and Stanley Fisher, a high-level official at the hacked agency. FBI LURES can use extracting thumb drives to steal passwords from top exec laptops.

Exclusive: Alleged Russian agent Butina met with U.S. Treasury, Fed officials

By Sarah N. Lynch

7 MIN READ

(An earlier version of this article corrected the date of Simes's trip to February 2015 instead of 2016)

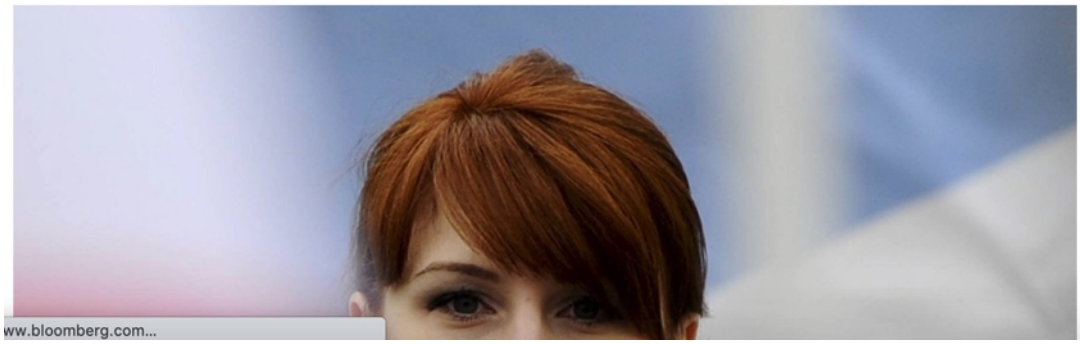


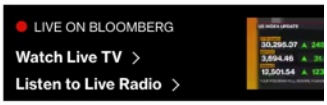
9. Would it not make sense to see which known GRU agents have hacked before, and to study their DNC connections. Physical access is usually the most difficult part of hacking. Butina "met" with John Rockefeller IV and Hank Greenberg also in DC, both known to maintain DC spy nets

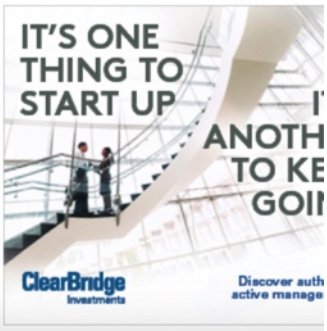
Butina Sought a Secret Kremlin Line to the U.S. A Rockefeller May Have Helped

By Polly Mosendz, Greg Farrell, and Ilya Arkhipov
July 26, 2018, 1:48 PM EDT *Updated on July 27, 2018, 1:18 PM EDT*

- O'Neill hosted 2017 dinner for prayer-breakfast delegates
- A Russian-language guide to Rohrabacher and other guests







10. And Butina transferred over 12 Terabytes to Moscow for a Treasury transactions to her Russian Central Bank Exec Alex Torshin. Sound like a hack to you? And Patrick Byrne, her handler, specializes in encrypted, blockchain financial transactions.

the government has substantial discovery they are ready to turn over right away.

Right now we already have about 4 to 6 terabytes of data, the equivalent of over 1-1/2 million files, that we're ready to turn over just as fast as it can be loaded onto a portable hard drive. There's another batch of data, approximately 4 to 6 terabytes --

THE COURT: Let me stop you. With regard to that first batch, how long do you think that will take to transfer?

MR. SAUNDERS: Barring the issue of a protective order, which I'll get to in a moment, it shouldn't take more than a couple of days.

THE COURT: All right. Okay.

11. Is Strzok moping up his 2016 hacks now with a covering hack in 2020. Same Cozy Bears. Same IP addresses. Same DNC operatives. Same safe houses. Same handlers. You Decide. Just a continuation of a four-year Russian Hoax?

