

Twitter Thread by Dumfounded ■ #TrumpConcedeNowMF



Dumfounded ■ #TrumpConcedeNowMF

@j2dumfounded



Time for a little thread on SolarWinds \$SWI which has been hacked by Russia's FSB, APT P29, commonly known as Cozy Bear.

The hackers embedded code that allows access to databases of the many clients SolarWinds sells to, including USG & 425 of the Fortune 500.



Sunday, Arapaho was kind enough to tag me in on the breaking development.

I'll share her great thread, then dive into some breaking news, then wrap with a bit of info from investor analysts.

<https://t.co/fmqwQQ6s4W>

More on this. h/t @yotesrhungry cc: @clearing_fog @j2dumfounded @ThomasS4217

1/ "Treasury, Commerce, FireEye--were breached through an IT Management System called \U0001f449Solar Winds\U0001f448" (more...)<https://t.co/mepsAc0mqi>

— Arapaho415 (@arapaho415) December 14, 2020

Long story short, this is a ■ **DISASTER OF EPIC PROPORTIONS** ■.

General McCaffrey is not a word mincer.

He's directly calling out Trump here. ■ <https://t.co/lrNmriwckH>

Russian hack of US government agencies and commercial ventures is a major disaster for US national security. . Not discovered for a month or longer. An intelligence collection mission not disruption... yet. TRUMP HAS MADE NO RESPONSE. <https://t.co/XuNCJHZ6Ex>

— Barry R McCaffrey (@mccaffreyr3) December 16, 2020

Over at AP News, Frank Bajak is not mincing words, either. <https://t.co/UIRVftZJda>

What 2019s seems clear is that this campaign 2014 which cybersecurity experts says exhibits the tactics and techniques of Russia's SVR foreign intelligence agency 2014 will rank among the most prolific in the annals of cyberespionage. 2019 <https://t.co/KJGWwlhjrp>

— @youmustchange (@youmustchange) December 16, 2020

Went to check in on my fave datasec guy and it turns out Chris Vickery is on Zev's show tonight. It's an hour long so I'll post it now and screen it later if I can stay awake that long. ■ <https://t.co/vjs4AG54QZ>

Watch! Fascinating show about how exposed we are as a country and in our homes to cyber intrusion. Hack of the Century. @ideagov Alan Silberberg and Chris @VickerySec @narativ live <https://t.co/bXzikWn5pv>

— Zev Shalev (@ZevShalev) December 16, 2020

Brian Krebs is reporting 18,000 customers may have been impacted by the malware! <https://t.co/aPiltn7gXo>

The SolarWinds breach may have pushed malware to ~18,000 customers, the company said Monday. Meanwhile, Microsoft should have some idea which/how many SolarWinds customers were hit, as it recently took over a key domain used to control infected systems. <https://t.co/etOSw8mCDQ>

— briankrebs (@briankrebs) December 15, 2020

This from the Wall Street Journal, "The Cybersecurity and Infrastructure Security Agency issued an emergency alert Sunday night urging federal agencies to disconnect from the affected SolarWinds product."

<https://t.co/bmJw1Xn4qe>

The shock waves could extend elsewhere across the public and private sectors. The Cybersecurity and Infrastructure Security Agency issued an emergency alert Sunday night urging federal agencies to disconnect from the affected SolarWinds product. The Electricity Subsector Coordinating Council, an executive roundtable for the electric sector, said in a statement Monday that it “conducted a situational awareness call” to discuss the threat and coordinate an industry wide response.

Local governments are also on high alert because of the SolarWinds breach, said Mike Hamilton, co-founder of the cybersecurity firm Critical Informatics Inc. Mr. Hamilton said SolarWinds “is ubiquitous” among local governments, which make up a large portion of his firm’s customers. In recent days, they have scrambled to update the software in question and monitor systems for other suspicious activity.

“Everybody is worried about being extorted,” said Mr. Hamilton, formerly the chief information security officer for the City of Seattle. He cited local governments’ fears of criminal groups affiliated with the attackers “dropping the ransomware bomb and lighting the fuse.”

Russia’s foreign-intelligence service is thought to be behind the attack but the Russian Embassy in Washington [has denied those claims](#), The Wall Street Journal reported Sunday. The incident is tied to a breach the cybersecurity firm [FireEye Inc.](#) [disclosed last week](#).

As I like to say about the Kremlin, it’s not official until the official denial.

“Russia’s foreign-intelligence service is thought to be behind the attack but the Russian Embassy in Washington has denied

those claims.”

Full #LavrovLaffOff. ■■

wsj.com

“Everybody is worried about being extorted,” said Mr. Hamilton, formerly the chief information security officer for the City of Seattle. He cited local governments’ fears of criminal groups affiliated with the attackers “dropping the ransomware bomb and lighting the fuse.”

Russia’s foreign-intelligence service is thought to be behind the attack but the Russian Embassy in Washington [has denied those claims](#), The Wall Street Journal reported Sunday. The incident is tied to a breach the cybersecurity firm [FireEye](#) Inc. [disclosed last week](#).

OK time for a nice compilation of \$SWI analysis from the (free) app Seeking Alpha.

Trading Places Research call the SolarWinds breach potentially the ■ most consequential hack of all time ■

The SolarWinds Hack Has A Long List Of Potential Victims

Dec. 14, 2020 11:11 PM ET | **SolarWinds Corporation (SWI)** | CHTR, DOW, FEYE... |

44 Comments | 23 Likes



Trading Places Research

4.70K Followers

Follow

Summary

- From what little we know, the SolarWinds hack has the potential to be the most consequential hack of all time.
- They have a giant customer list, all corporations and government agencies with massive, complex systems filled with important data. The hackers had access to any of this they wanted.
- We only know of 3 victims right now - the Departments of Commerce and Treasury, and FireEye. Should that list grow, SolarWinds' liability is open-ended.
- But should the damage be limited, their customers may look at their choices and stick with SolarWinds.
- I am going to keep an eye on it and maybe take a small taste soon.

This is simply a partial list of the over 18,000 customers who could find the cozy Russian bear has come through their back door and emptied out the larder of all its goodies. Nom, nom. Cozy Bear is hangry.

SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom	General Dynamics	Sabre
Ameritrade	Gillette Deutschland GmbH	Saks
AT&T	GTE	San Francisco Intl. Airport
Bellsouth Telecommunications	H&R Block	Siemens
Best Western Intl.	Harvard University	Smart City Networks
Blue Cross Blue Shield	Hertz Corporation	Smith Barney
Booz Allen Hamilton	ING Direct	Smithsonian Institute
Boston Consulting	IntelSat	Sparkasse Hagen
Cable & Wireless	J.D. Byrider	Sprint
Cablecom Media AG	Johns Hopkins University	St. John's University
Cablevision	Kennedy Space Center	Staples
CBS	Kodak	Subaru
Charter Communications	Korea Telecom	Supervalu
Cisco	Leggett and Platt	Swisscom AG
CitiFinancial	Level 3 Communications	Symantec
City of Nashville	Liz Claiborne	Telecom Italia
City of Tampa	Lockheed Martin	Telenor
Clemson University	Lucent	Texaco
Comcast Cable	MasterCard	The CDC
Credit Suisse	McDonald's Restaurants	The Economist
Dow Chemical	Microsoft	Time Warner Cable
EMC Corporation	National Park Service	U.S. Air Force
Ericsson	NCR	University of Alaska
Ernst and Young	NEC	University of Kansas
Faurecia	Nestle	University of Oklahoma
Federal Express	New York Power Authority	US Dept. Of Defense
Federal Reserve Bank	New York Times	US Postal Service
Fibercloud	Nielsen Media Research	US Secret Service
Fiserv	Nortel	Visa USA
Ford Motor Company	Perot Systems Japan	Volvo
Foundstone	Phillips Petroleum	Williams Communications
Gartner	Pricewaterhouse Coopers	Yahoo
Gates Foundation	Procter & Gamble	

Every one of these organizations is at risk and has been since March. SolarWinds website screenshot. Moments after I took that screenshot on Monday morning, the company took it down and the page is [404](#)

And Cozy Bear has found the pantry well stocked with all sorts of delectable data. Pretty much the proverbial keys to the kingdom. We're so fucked.

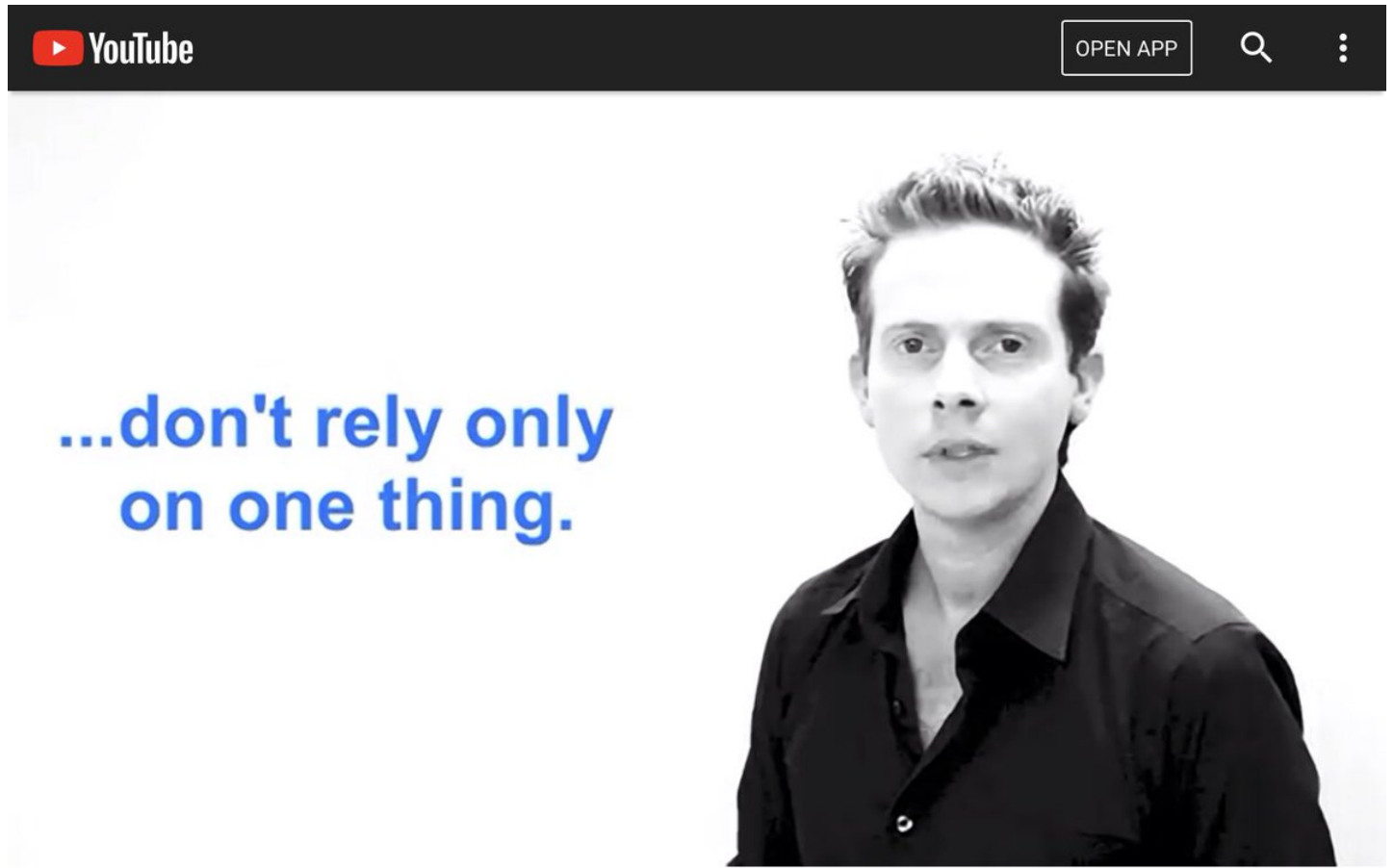
AVAILABILITY & PERFORMANCE Network Performance Monitor - Multi-vendor network monitoring for fault, performance, and availability - Automated capacity forecasting, alerting, and reporting Learn More	APPLICATION & INFRASTRUCTURE Server & Application Monitor - Deep performance visibility of commercial and custom applications - Monitor across private, public and hybrid cloud environments Learn More	CONFIGURATION & CHANGE MANAGEMENT Network Configuration Manager - Multi-vendor network change and configuration management - Real-time configuration change notification Learn More	HYPER-V & VMWARE TROUBLESHOOTING Virtualization Manager - Identify and remediate VMware vSphere and Microsoft Hyper-V problems - VM capacity planning and sprawl control Learn More
NETWORK TRAFFIC ANALYSIS AND BANDWIDTH MONITORING NetFlow Traffic Analyzer - Capture data from continuous streams of network traffic and convert those raw numbers into easy-to-interpret charts and tables - Quantify how much traffic is on the corporate network and which applications are being used. Learn More	SECURITY & COMPLIANCE Log Analyzer - Search and filter log data from multiple sources - Real-time log streaming and visualization Learn More	STORAGE PERFORMANCE & CAPACITY Storage Resource Monitor - Unified storage monitoring across different storage vendors and devices - Pinpoint storage performance bottlenecks Learn More	IP ADDRESS TRACKING & MANAGEMENT IP Address Manager - Quickly find available IP addresses - Easily configure IP addresses on DHCP and DNS systems Learn More
VOIP AND WAN PERFORMANCE VoIP & Network Quality Manager - Proactively identify and eliminate distortion, latency, and noise - Facilitate capacity planning and measurement of voice quality in advance of new VoIP deployments Learn More	DEVICE TRACKING & PORT USAGE User Device Tracker - Deliver automated user and device tracking along with powerful switch port management capabilities - Monitor switch port usage and make informed resource planning decisions Learn More	SERVERS & APPLICATION CONFIGURATIONS Server Configuration Monitor - See who's making configuration changes on servers or applications - Correlate configuration changes with performance metrics Learn More	WEBSITE AND APP PERFORMANCE Web Performance Monitor - Troubleshoot performance issues for both internal and customer-facing websites and web-based applications - Provides notifications when there is a web site or application issue Learn More
DATABASE PERFORMANCE Database Performance Analyzer - Find, analyze, and optimize your database performance story - Multi-Vendor support across physical, virtual, or cloud deployments Learn More		AUTOMATED PATCH MANAGEMENT Patch Manager - Automated patching of Microsoft servers and 3rd-party apps - Patch compliance reporting Learn More	

DON'T PUT ALL YOUR EGGS IN ONE BASKET



<https://t.co/Ojviiq2R08>

Cute accent and some nice blues guitar are bonuses on this explainer.



IDIOM OF THE DAY - Don't Put All Your Eggs In One Basket



Let's look at why, why is Cozy Bear so hangry?

Well, back in 2014 Putin annexed Crimea from Ukraine.
EU & USA slapped on sanctions.

Sanctions hurt Russia bigly.

Rather than free Crimea, Putin installed his orange puppet...& here we are.

Just on the little information we have, this looks me to be about Russian sanctions, which are administered by those two Departments.

Microsoft ([MSFT](#)) has [a lot more technical detail](#) on the hack if you are interested, but the short of it:

- It is unclear how, but the attacker injected code into a legitimate Orion library.
- The library got distributed and signed by SolarWinds.
- The code loaded before the legitimate code in the library, so it went undetected, since it was all signed by SolarWinds.
- The code allowed the attacker to manually remotely escalate a user privilege to the highest level with unfettered access.

Where we are is pretty grim. FSB can set its users to highest level of permissions. This is going to take a long time to undo, and even then, all that government information and private sector financial information is now in the Kremlin's hands. The horse is out of the barn.



And Trump will do nothing. We don't even have the people in place to lead a response. Coincidence? Oh, please.

The White Rabbit & Cozy Bear are drinking vodka in the banya, gloating with glee at what they have done. As for the leadership at \$SWI, that's a thread for another day.

I've seen some weird shit

