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

> \u2018What\u2019s seems clear is that this campaign \u2014 which cybersecurity experts says exhibits the tactics and techniques of Russia\u2019s SVR foreign intelligence agency \u2014 will rank among the most prolific in the annals of cyberespionage.\u2019 https://t.co/KJGWwlhjrp
>
> — \U0001f1fa\U0001f1f8 \u0282\u0199\u10e7\u10e7\u025b \u0291\u0131\u026c\u0131\u014b\u0267\u0105 \U0001f1f5\U0001f1f9 (@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/aPiItn7gXo

> 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."

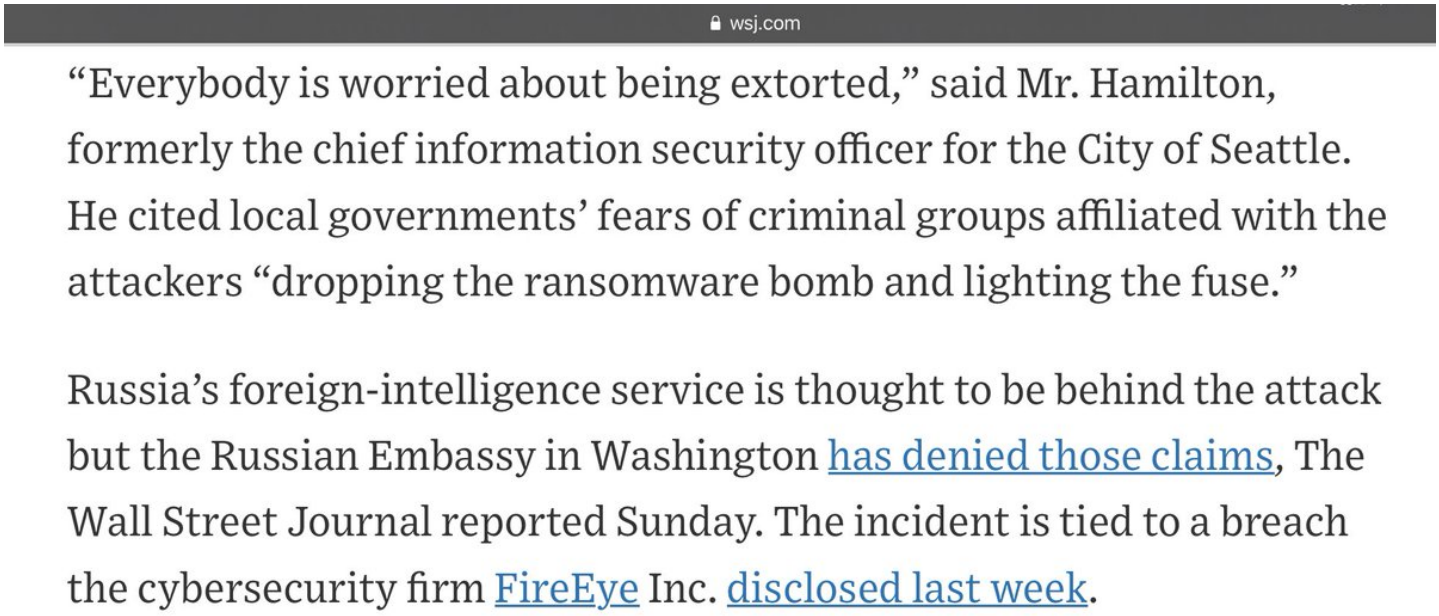
Russia's foreign-intelligence service is thought to be behind the attack but the Russian Embassy in Washington has denied those claims, The Wall Street Journal reported Sunday. The incident is tied to a breach the cybersecurity firm FireEye Inc. disclosed last week.

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

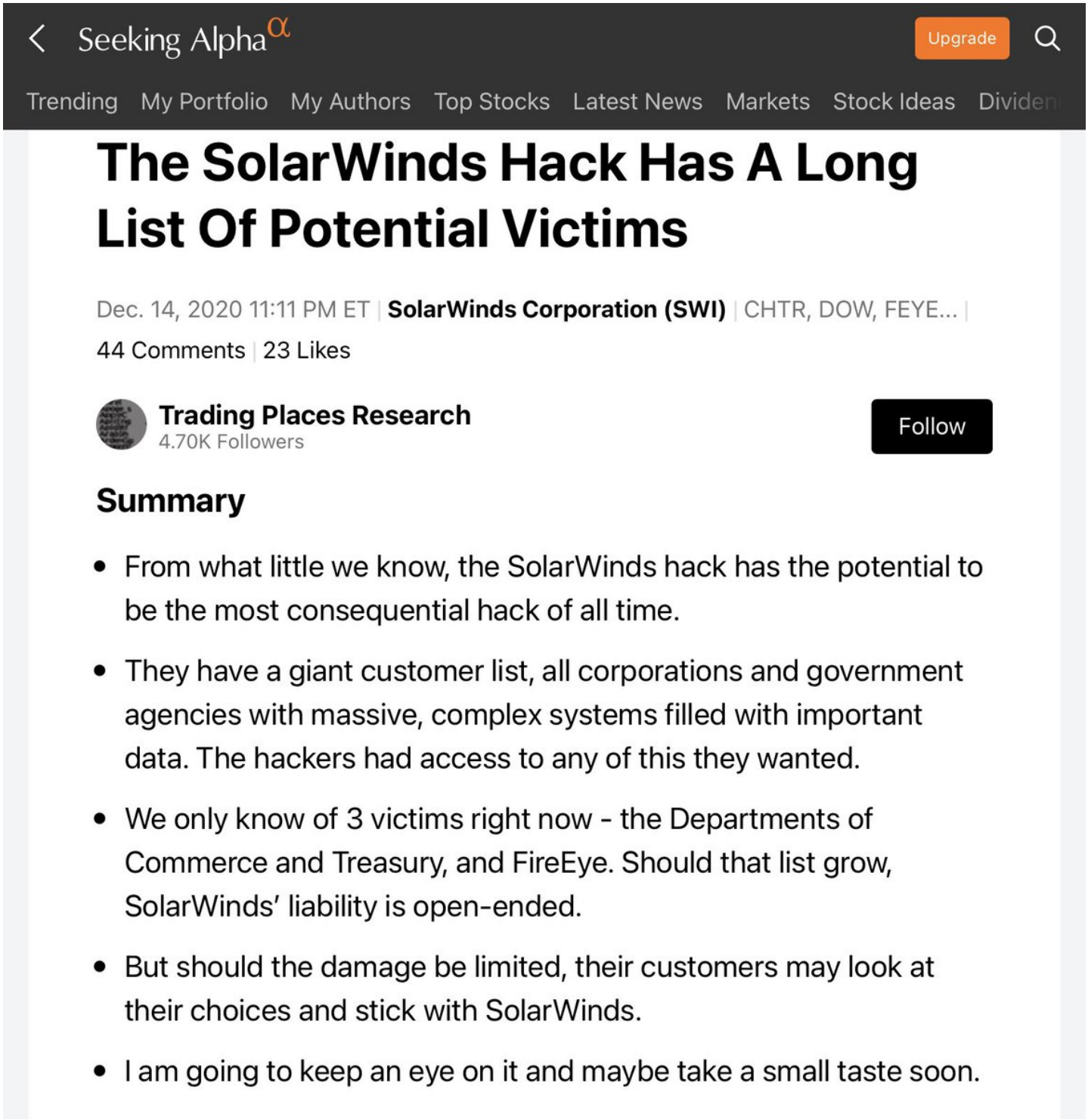
those claims.”

Full #LavrovLaffOff. ■■



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 ■



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

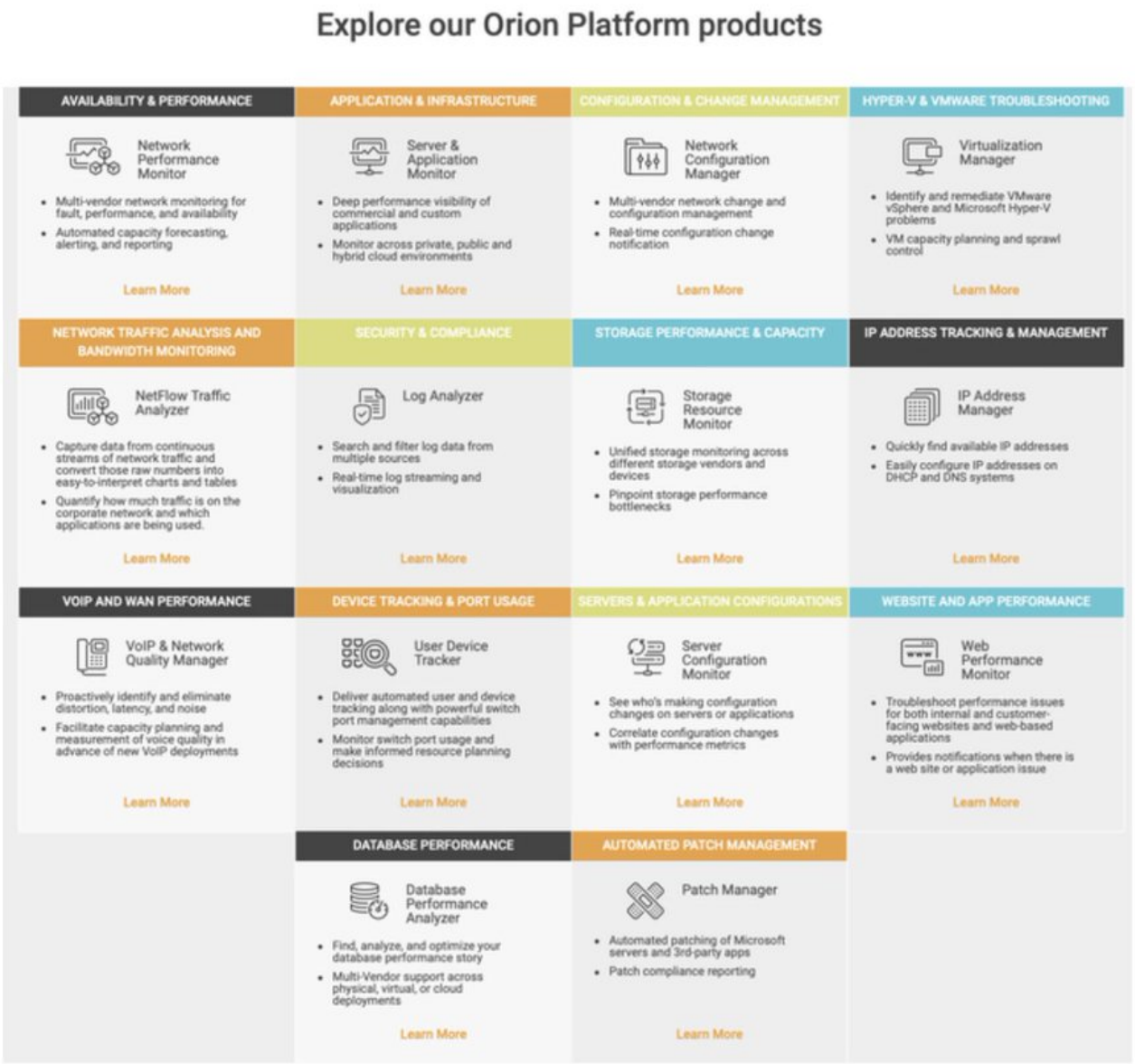
Partial customer listing:

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

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.

SolarWinds provides IT management software to a large variety of customers in both the public and private sectors. They have over 50 products for specific IT tasks, but they are unified under a single interface SolarWinds calls the Orion Platform. "One vendor. One platform. One single pane of glass," is the marketing.

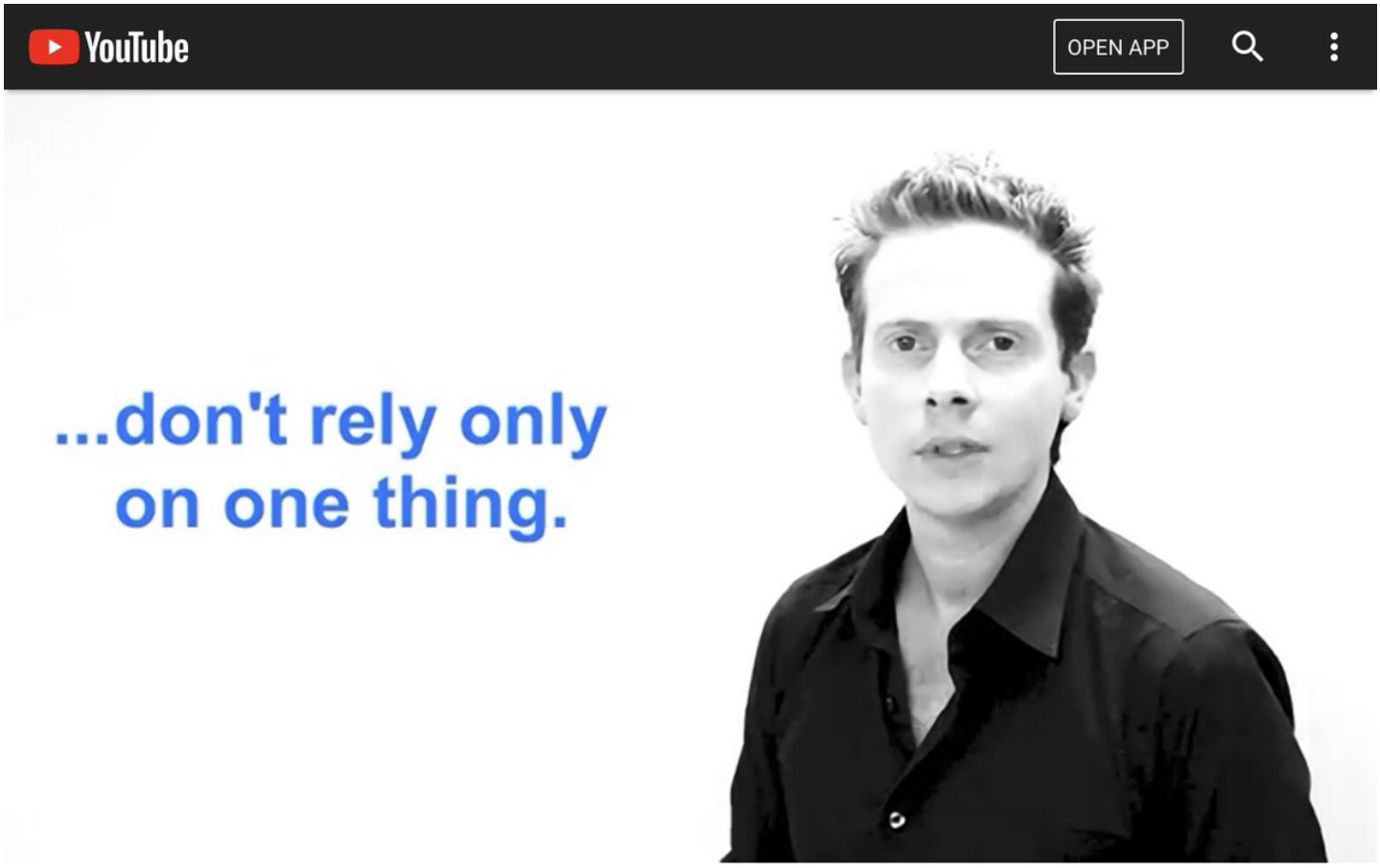


What's that saying?

DON'T PUT ALL YOUR EGGS IN ONE BASKET

■■■■■■■■■■■■■■■■■■■■■

https://t.co/Ojiviq2R08
Cute accent and some nice blues guitar are bonuses on this explainer.



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