

From: Hawkins, E. A. (WF) (FBI) <Adrian.Hawkins@ic.fbi.gov>
Sent: Friday, September 16, 2016 9:01 PM
To: Frasch, Jennifer J. (WF) (FBI) <Jennifer.Frasch@ic.fbi.gov>
Cc: Garrett, Lafayette M. (WF) (FBI) <Lafayette.Garrett@ic.fbi.gov>
Subject: Re: APT 28

Request sent. This seems extraordinary. I'd call his cell but only have his office, so sent email to two contacts. Generally they check their emails after hours.

E. Adrian Hawkins
Special Agent
Washington Field Office
REDACTED-6674

From: Frasch, Jennifer J. (WF) (FBI)
Sent: Friday, September 16, 2016 7:42 PM
To: Hawkins, E. A. (WF) (FBI)
Cc: Garrett, Lafayette M. (WF) (FBI)
Subject: Fwd: APT 28

Hi Adrian,
Sorry for the late night request...
I spoke with both Doreen and Josh regarding the following and as Doreen will attempt to get more info from MS, Josh requested WFO reach out to Sussmann to see if by chance he might have contact information for Leslie Dach. Trying to determine where Dach is located for appropriate office make notification.
Thanks in advance!
Jennifer

--

----- Original message -----

From: "Hubiak, Joshua J. (PH) (FBI)" <Joshua.Hubiak@ic.fbi.gov>
Date: 09/16/2016 8:04 PM (GMT-05:00)
To: "Frasch, Jennifer J. (WF) (FBI)" <Jennifer.Frasch@ic.fbi.gov>
Subject: Fwd: APT 28

Jennifer,
When you get this email, can you give me an email at your earliest convenience please.

Thanks,

SA Joshua J Hubiak

FBI-DWS-05-0002048
SCO-011212

Philadelphia Division
Cyber Squad - CYB1
Primary Relief Supervisor
Office: (215) 418-4036
Cell: REDACTED-7264

----- Original message -----

From: "Moore, Doreen M. (SE) (FBI)" <Doreen.Moore@ic.fbi.gov>
Date: 09/16/2016 7:54 PM (GMT-05:00)
To: "Hubiak, Joshua J. (PH) (FBI)" <Joshua.Hubiak@ic.fbi.gov>
Subject: APT 28

Hi Joshua -

I have an odd situation that you may or may not be able to help me out with.

Microsoft contacted me regarding an Outlook account they believe has been compromised by APT 28 actors. The account appears to belong to an individual named Leslie Dach, who based on open source research appears to be a bigwig and is currently serving a role on the Clinton campaign and the Board of Directors of Sunrun (solar energy company in bay area).

Microsoft has locked the account so the bad guys can't access it, but that also locks it so Dach can't access it either. Given that he appears to be someone of significant importance, Microsoft will not grant access to the account until they are certain they are granting it to the actual owner, hence their call to me. They would like to have the FBI notify Dach of the compromise, confirm it is his account and then put him in touch with Microsoft so he can get his email account back.

I currently only have his name and the account, I don't have any info as to how they found the compromise or why they claim APT 28 is behind it. But they will generally share this information with us when we ask.

As STRAT for this threat, I thought I would reach out to you to see if you guys already know of this compromise and if not would you like to take the lead in notification to Dach? I have not yet determined where he is physically located but recent positions/jobs had him in the DC area.

What are your thoughts? You are welcome to call cell phone if you would like to chat about it.

SA Doreen Moore
Seattle - CY-1
REDACTED-7639

--

FBI-DWS-05-0002049
SCO-011213