

From: Tsiumis, Allison R. (CYD) (FBI) <Allison.Tsiumis@ic.fbi.gov>
Sent: Tuesday, August 9, 2016 6:32 AM
To: Ferranti, Colleen P. (CYD) (FBI) <Colleen.Ferranti@ic.fbi.gov>
Cc: Holt, Joda D. (DN) (FBI) <Joda.Holt@ic.fbi.gov>
Subject: Fwd: (((SITREP))) [UPDATE-3] Compromise of the Democratic Congressional Campaign Committee (DCCC) Network

Colleen: Just FYI - Joda's team is on this with Ops III.

--

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

From: "Yearwood, Ronald J. (CYD) (FBI)" <Ronald.Yearwood@ic.fbi.gov>
Date: 08/09/2016 06:26 (GMT-05:00)
To: "Holt, Joda D. (DN) (FBI)" <Joda.Holt@ic.fbi.gov>, "Tsiumis, Allison R. (CYD) (FBI)" <Allison.Tsiumis@ic.fbi.gov>
Cc: "Farrar, Aubrey B. (CYD) (FBI)" <Aubrey.Farrar@ic.fbi.gov>, "Lowder, Jason P. (CYD) (FBI)" <Jason.Lowder@ic.fbi.gov>
Subject: Fwd: (((SITREP))) [UPDATE-3] Compromise of the Democratic Congressional Campaign Committee (DCCC) Network

Purpose for the paper I mentioned yesterday.

--

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

From: "Buie, Emmerson (CYD) (FBI)" <Emmerson.Buie@ic.fbi.gov>
Date: 08/09/2016 6:18 AM (GMT-05:00)
To: "Trainor, James C. (CYD) (FBI)" <James.Trainor@ic.fbi.gov>, "Sporre, Eric W. (CYD) (FBI)" <Eric.Sporre@ic.fbi.gov>, "Yearwood, Ronald J. (CYD) (FBI)" <Ronald.Yearwood@ic.fbi.gov>, "Kelly, Jordan R. (CYD) (FBI)" <Jordan.Kelly@ic.fbi.gov>
Subject: Fwd: (((SITREP))) [UPDATE-3] Compromise of the Democratic Congressional Campaign Committee (DCCC) Network

--

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

From: "Heinze, Jeffrey P. (CYD) (FBI)" <Jeffrey.Heinze@ic.fbi.gov>
Date: 08/08/2016 7:37 PM (GMT-05:00)
To: "Buie, Emmerson (CYD) (FBI)" <Emmerson.Buie@ic.fbi.gov>, "Kelliher, Carolyn J. (CYD) (FBI)" <Carolyn.Kelliher@ic.fbi.gov>, "Burnside, Jennifer S. (CYD) (FBI)" <Jennifer.Burnside@ic.fbi.gov>
Subject: Fwd: (((SITREP))) [UPDATE-3] Compromise of the Democratic Congressional Campaign Committee (DCCC) Network

In case you weren't on the original distribution...

--

FBI-DWS-12-0024234
SCO-011774

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

From: NCCIC@us-cert.gov

Date: 08/08/2016 7:30 PM (GMT-05:00)

To: NCCIC@us-cert.gov, NCCIC@hq.dhs.gov, ascyber@hq.dhs.gov, Danny.Toler@us-cert.gov, John.Felker@hq.dhs.gov, Gregory.Touhill@hq.dhs.gov, Tom.Baer@hq.dhs.gov, andy.ozment@hq.dhs.gov, NCCIC_Leadership@hq.dhs.gov, nccic_chiefs@hq.dhs.gov, daniel.medina@hq.dhs.gov, Eric.Goldstein@hq.dhs.gov

Cc: Carl.Deputy@hq.dhs.gov, eric.schneider@hq.dhs.gov, NCCIC@hq.dhs.gov, ncc@hq.dhs.gov, SWO@us-cert.gov, ics-cert@hq.dhs.gov, NICC@HQ.DHS.GOV, ogc@hq.dhs.gov, michael.howell@hq.dhs.gov, noc.ndd@hq.dhs.gov, noc.swo.restricted@hq.dhs.gov, alexandra.friedman@HQ.DHS.GOV, Richard.Harris@hq.dhs.gov, Daniel.Donahue@us-cert.gov, john.robinson@hq.dhs.gov, Dennis.Lalena@hq.dhs.gov, Carl.Deputy@hq.dhs.gov, eric.schneider@hq.dhs.gov, NCCIC@hq.dhs.gov, ncc@hq.dhs.gov, SWO@us-cert.gov, ics-cert@hq.dhs.gov, NICC@HQ.DHS.GOV, ogc@hq.dhs.gov, michael.howell@hq.dhs.gov, noc.ndd@hq.dhs.gov, noc.swo.restricted@hq.dhs.gov, alexandra.friedman@HQ.DHS.GOV, Richard.Harris@hq.dhs.gov, Daniel.Donahue@us-cert.gov, DL-CyberCenters@us-cert.gov, nccicinternallno@hq.dhs.gov, SOC@msisac.org, "Buic, Emmerson (CYD) (FBI)" <Emmerson.Buic@ic.fbi.gov>, "Buic, Emmerson (DHS)" <ebuic@hq.dhs.gov>, "Heinze, Jeffrey P. (CYD) (FBI)" <Jeffrey.Heinze@ic.fbi.gov>, jeffrey.p.heinze@hq.dhs.gov, jeanette.manfra@hq.dhs.gov, monica.leon@hq.dhs.gov, angela.m.kouters@hq.dhs.gov, eric.tamarkin@hq.dhs.gov, jason.lamote@hq.dhs.gov, bridgette.walsh@hq.dhs.gov, alexandra.friedman@hq.dhs.gov

Subject: (((SITREP))) [UPDATE-3] Compromise of the Democratic Congressional Campaign Committee (DCCC) Network

(U//FOUO)

TLP: AMBER



National Cybersecurity & Communications Integration Center

NCCIC

NCCIC Situational Report (((SITREP))) [UPDATE-3]

August 8, 2016

This SITREP pertains to intrusions into the Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC). NCCIC has deemed it necessary to raise the severity schema from Level 2 Medium (Yellow) to Level 3 High (Orange) based on an assessment that the incident likely has had a demonstrable impact on foreign relations and public confidence.

INCIDENT:

Friday, August 5, 2016 - The NCCIC initiated a dialogue with the Clinton Presidential campaign Chief Operating Officer (COO) and Chief Information Officer (CIO) to offer NCCIC's technical assistance.

FBI-DWS-12-0024235

SCO-011775

Friday, August 5, 2016 - the FBI delivered a DVD of artifacts from the DNC and DCCC investigation to NCCIC for analysis. The initial analysis will be completed this week.

Wednesday, August 3, 2016 - NCCIC conducted a conference call, with Mr. Michael Sussmann, Attorney for Perkins Coie representing DNC / DCCC. NCCIC will continue further discussions with Mr. Sussmann at a later date.

The dialogue with the Republican National Committee (RNC) was established to offer NCCIC's technical assistance. Further discussions will likely take place this week.

NCCIC expects to receive a call from the Trump Campaign this week at which time there will be an offer made to provide technical assistance.

Wednesday, June 22, 2016 - NCCIC was notified by a trusted private sector partner of a potential network breach of the DCCC network. NCCIC shared the information with the FBI, who recognized that this was likely tied to the ongoing investigation of the DNC incident. The FBI is the investigative lead for this incident.

The DNC hired a cybersecurity firm to conduct an in-depth investigation of their network. The FBI is investigating the DNC incident.

CAUSE: Malicious cyber actors gained unauthorized access the DCCC network.

CURRENT ACTIONS:

NCCIC will notify the Cyber Response Group (CRG) of the elevation change to Level 3 Orange.

NCCIC will offer technical assistance to all U.S. Presidential candidates who are qualified for USSS protection.

NCCIC is maintaining situational awareness with FBI CyWatch and the other Federal Cyber Centers.

INFORMATION:

Schema: Level 3 High (Orange) "Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence."

FBI-DWS-12-0024236
SCO-011776

National Cybersecurity & Communications Integration Center

Department of Homeland Security

COMM/STE: (703) 235-5273

Unclassified: NCCIC@us-cert.gov

HSDN: NCCIC@dhs.sgov.gov

JWICS: NCCIC@dhs.ic.gov

OV

Info addressees:

CS&C Leadership

NCCIC Director

NCCIC Deputy Director

NCCIC Chiefs

NCCIC Components

NCCIC Internal LNOs

NICC

DHS NOC

CyWatch

NSC

Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need-to-know without prior approval of an authorized DHS official.

TLP: AMBER

(U//FOUO)

FBI-DWS-12-0024237

SCO-011777