

From: Ryan McCombs <ryan.mccombs@crowdstrike.com>
Sent: Tuesday, August 16, 2016 12:56 PM
To: Adrian.Hawkins@ic.fbi.gov
Subject: [Suspect] RE: PurpleDay Compromised System Locations
Attach: smime.p7s; ATT00001.txt; ATT00002.htm

Excellent.

As discussed yesterday, document authentication will be a challenge, especially from CrowdStrike's perspective. I think the path of least resistance is, if provided the hashes, we check our collected data first. In the likely event we don't have the hashes in our data, the next step would be to approach MIS to query the DNC systems. I'm not sure what kind of push back would be received, but that's why Mr. Sussmann is here. This second option would be resource intensive, as they have many TB of data that would need to be hashed. Secondly, there's no guarantee that the original document hasn't been changed since released by G2, thereby changing the hash value. A tough nut to crack for sure.

We'd love to receive the docs. Please send to:

CrowdStrike Services, LLC
ATTN: Ryan McCombs
1807 Park 270 Drive
St Louis, MO 63146

Regards,

Ryan McCombs
Consultant, CrowdStrike Services
ryan.mccombs@crowdstrike.com
REDACTED.5254

From: Hawkins, E. A. (WF) (FBI) [mailto:Adrian.Hawkins@ic.fbi.gov]
Sent: Tuesday, August 16, 2016 11:37 AM
To: Ryan McCombs <ryan.mccombs@crowdstrike.com>
Subject: Re: PurpleDay Compromised System Locations

??Got it this time, thanks!

Only other thing outstanding for us right now, then, is for us to authenticate some docs. Understand hash match is machine intensive, computer scientist here was thinking maybe we scan for file name (much faster?), and do a hash comparison for just positive matches. Also, the looping structure can break if we find, say, 3 matches? Also don't know who will take that on as action item. I'm strung between three folks (MIS, Sussman, and yourselves) so apologize if I'm asking wrong person.?

Will be sending a CDROM with a copy of the docs to Sussmann via FedEx today. Happy to share with you as well, if needed.

v/r,
Adrian

FBI-DWS-05-0002622
SCO-011622

?

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

From: Ryan McCombs <ryan.mccombs@crowdstrike.com>
Sent: Tuesday, August 16, 2016 11:11 AM
To: Hawkins, E. A. (WF) (FBI)
Subject: [Suspect] FW: PurpleDay Compromised System Locations

Attempt #2

From: Ryan McCombs
Sent: Tuesday, August 16, 2016 9:53 AM
To: 'Adrian.Hawkins@ic.fbi.gov' <Adrian.Hawkins@ic.fbi.gov>
Cc: Shawn Henry <shawn@crowdstrike.com>; Christopher Scott <chris@crowdstrike.com>; 'MSussmann@perkinscoie.com' <MSussmann@perkinscoie.com>
Subject: FW: PurpleDay Compromised System Locations

Agent Hawkins,

Please see the responses below from the IT staff at DCCC in regards to locations of systems during compromise. It's not very telling for the workstations, however it does answer for the servers. When they reference the server room, they're referring to the server room within the DNC headquarters. Let me know if there is anything else you need from our end.

Regards,

Ryan McCombs
Consultant, Crowdstrike Services
ryan.mccombs@crowdstrike.com
REDACTED 5254

From: Ryan Borkenhagen [<mailto:Borkenhagen@DCCC.ORG>]
Sent: Monday, August 15, 2016 4:40 PM
To: Ryan McCombs <ryan.mccombs@crowdstrike.com>; David Winston <winston@dccc.org>
Cc: Christopher Scott <chris@crowdstrike.com>
Subject: RE: PurpleDay Compromised System Locations

All of our users (that have laptops) spend the majority of their time in our office. When on the road, they would be working out of local campaign offices, hotels, coffee shops... A lot of time they will be on a DCCC owned mifi device for internet but even then if there is a reliable wifi they can use (at hotel or campaign office) they will use that.

From: Ryan McCombs [<mailto:ryan.mccombs@crowdstrike.com>]
Sent: Monday, August 15, 2016 5:28 PM

FBI-DWS-05-0002623
SCO-011623

To: Ryan Borkenhagen <Borkenhagen@DCCC.ORG>; David Winston <winston@dccc.org>
Cc: Chris Scott <chris@crowdstrike.com>
Subject: RE: PurpleDay Compromised System Locations

Thanks, Ryan.

For the folks in the field, where do they typically operate?

Regards,

Ryan McCombs
Consultant, Crowdstrike Services
ryan.mccombs@crowdstrike.com
REDACTED5254

From: Ryan Borkenhagen [<mailto:Borkenhagen@DCCC.ORG>]
Sent: Monday, August 15, 2016 4:27 PM
To: Ryan McCombs <ryan.mccombs@crowdstrike.com>; David Winston <winston@dccc.org>
Cc: Christopher Scott <chris@crowdstrike.com>
Subject: RE: PurpleDay Compromised System Locations

Here you go. All of the users are based out of our office but regularly take their laptops home or on the road with them.

Just a quick note the highlighted laptop is a new one (I didn't have it on my list before).

Hostname	User (department)	Location
D3CBACKUP1	Backup Server	Server Room
D3CFILE01	File Server	Server Room
D3CMAIL04	Old Mail server	Server Room
D3CSQL03	SQL Server (hosts accounting DB)	Server Room
E54402XPTJ12	Joclyn Mund (Field)	Laptop
E54407HDTVZ1	Dan Sena Targeting and Field)	Laptop
LATE5440562PD12	Milly Velez (Accounting)	Laptop
LATE54406B4PD12	Dyland Gibson (Online)	Laptop
LATE63305J9PYW1	Alex Farrington (Field)	Laptop
LATE6330CRBPYW1	Sam Ward (Finance)	Laptop
LATE64201W444R1	Leif Warner (Accounting)	Laptop
LATE642026MQCS1	Ryan Thompson (Online)	Laptop
LATE64204PR7FV1	Agnes O'Hanlon (Accounting)	Laptop
LATE64205H747R1	Intern	Locked in office
LATE642086ZG5R1	Yule Kim (Research)	Laptop
LATE64208PH44R1	Intern	Locked in office
LATE72503SP8262	Steve Sisneros (Field)	Laptop
LATE725048J8262	Greg Diamond (Field)	Laptop
LATE72504CJ8262	Mario Salazar (Field)	Laptop
LATE7250675FN32	Amber Reeves (Targeting)	Laptop

FBI-DWS-05-0002624
SCO-011624

LATE725078RFN32	Barb Solish (Communications)	Laptop
LATE72509K4MN32	Jackie Forte (Accounting)	Laptop
LATE7250DWZ9262	Hayley Dierker (Operations)	Laptop
LATE7250HBXB262	Missy Kurek (Finance)	Laptop
LATE7250JF3GN32	Stella Ross (Finance)	Laptop
LATE72702JJFK72	Julia Ager (Online)	Laptop
LATE727094WFK72	John Malloy (Targeting)	Laptop
LATE72709FNFK72	Amy Drummond (Targeting)	Laptop
OPT70409JB9482	David Winston (IT)	IT Office
OPT70409JBB482	Ryan Borkenhagen (IT)	IT Office

FBI-DWS-05-0002625
SCO-011625