From: (b)(6)
Sent: Saturday, December 10, 2016 12:15:08 AM
To: Rohner, Boyden
Cc: (b)(6) DHS ESOC
Subject: RE: (Easy) Request assistance for DHS

I'll have our team take a look at this and get back to you.

Thanks,

(b)(6)
Chief, Justice Security Operations Center (JSOC)
US Department of Justice
202-357-0198

From: Rohner, Boyden [mailto:(b)(6)]
Sent: Friday, December 9, 2016 6:36 PM
To: (b)(6) (JMD) <(b)(6)>
Cc: (b)(6) DHS ESOC <DHSESOC@hq.dhs.gov>
Subject: (Easy) Request assistance for DHS

Good afternoon, (b)(6) –

(b)(6) suggested I reach out to you for some assistance on an investigation we're conducting. We're investigating some claims by the State of Georgia that we've been scanning their website. A review of our logs indicates that Microsoft Office generates an HTTP.request.method=OPTIONS which is the event that triggered the suspicion by the State of GA.

When we pull our logs over a three hour period, we see that we have about 1800 similar requests. Do you see this type of network traffic regularly as well? Specifically, can you search your proxy logs to confirm the following traffic pattern when a user views a Microsoft Office file from a website? Before the get request, the user's browser would send an HTTP request method =OPTIONS and user agent string ="Microsoft Office discovery protocol". Here's an example of what we're seeing:

cid:image001.jpg@01D25265.91CF9280

Thank you very much for your help. Please email me or (b)(6) (copied) if you have any questions.

Boyden Rohner

Director, Cybersecurity Operations
DHS
(202) 657-(b)(6)

Sender:	DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=SOCDHSONENET.CBP.DHS.GOV3A5>; "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>
Recipient:	(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "DHS ESOC </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"; "(b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6) "(b)(6) (CTR) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=(b)(6)>"
Sent Date:	2016/12/09 22:26:29
Delivered Date:	2016/12/09 22:26:30