202-447-(b)(6)

From: (b)(6) (b)(6)
Sent: Friday, December 16, 2016 10:51 AM
To: Fulghum, Chip (b)(6) Non Responsive (b)(6)
Etzel, Jeanne (b)(6)
Subject: FW: Preliminary update on GASOS

This is raw. I'll provide more information at the 4 pm update.

From: (b)(6) (b)(6)
Sent: Friday, December 16, 2016 10:49 AM
To: (b)(6) (b)(6) (b)(6)
Cc: Rohner, Boyden (b)(6) (b)(6) (b)((b)(6) (b)(6) (b)(6) (b)(6)
Subject: RE: Preliminary update on GASOS

Mr. (b)(6)

Please see below.

With regards to Georgia we have confirmed with that the traffic is legitimate and expected behavior along with verification from Microsoft. This traffic is not only from FLETC, but also includes ICE-CIS and FEMA.

- An interview was conducted with the FLETC user who generated the first traffic on November 15th and relayed his steps while he was on Georgia's SOS site. This included copy and pasting license plate numbers for law enforcement personnel to do their lookups. This copy and paste invokes the web traffic that Georgia's SOS identified to be suspicious.
- DHS ESOC regenerated traffic that matched this users activity and matched the logs directly up with the traffic that occurred on November 15th.
- Microsoft has validated our logs, the logs from FLETC and confirmed this traffic to be normal web behavior that would occur should you copy and paste from a website into a Microsoft office product.
    - Each of the other timestamps where we had logs available also matched with this same normal web behavior.

With regards to the other 10 timestamps, given that there are 14 IPs with over 350,000 users behind them, we have identified different components who have caused the same traffic as the FLETC user. Those components are broken down below.

- At this time, we cannot validate users with ease for these past timestamps due to DHCP and the lack of Authentication logs. Thus an interview was not done for these events.
    - Once we begin authenticating through the Proxies, we will have matching username and can proceed in the future

- September 12, 2016 12:52:32 EDT (11:52 CDT)

  - Host 10.61.22.222 (**ICE-CIS**)*
- September 28, 2016 08:54:15 EDT (07:54 CDT)
  - Host 10.56.189.94 (**ICE-CIS**)*
- October 3, 2016 11:41:32 EDT (10:41 CDT)
  - Host 10.101.194.178 (**ICE-CIS**)*
- October 6, 2016 11:14:16 EDT (10:14 CDT)
  - Host 10.32.82.42 (**FEMA**)
- November 7, 2016 13:15:43 EST (12:15 CST)
  - Host 10.56.189.65 (**ICE-CIS**)*
- November 8, 2016 08:35:21 EST (07:35 CST)
  - Host 10.243.15.188 (**FLETC**)

- May 23, 2016 08:42 CDT
  - Unknown component (verified similar activity) – alternate logs do not provide component information this far back
- February 28, 2016 13:19 CST
  - Unknown component (verified similar activity) – alternate logs do not provide component information this far back
- February 2, 2016 13:03 CST
  - Unknown component (verified similar activity) – alternate logs do not provide component information this far back

*note: The "ICE-CIS" components are listed due to ICE and CIS sharing much of their IP space.

v/r

(b)(6) (b)(6) PMP, CISSP, GCIA, GCIH, Sec+, ITILv3
ESOC Operations Manager
Department of Homeland Security (DHS) Enterprise Security Operations Center (ESOC)
MGMT/OCIO/CISO/SOC
BB: 202-309-(b)(6)
Office: 202-372-(b)(6)
DHS SOC: 1-877-347-(b)(6)

From: (b)(6)
Sent: Friday, December 16, 2016 10:30 AM
To: (b)(6) (b)(6) (b)(6)
Cc: Rohner, Boyden (b)(6) (b)(6) (b)((b)(6)
Subject: Preliminary update on GASOS

Can you shoot me a quick update on what was just discussed with the USM. I need to share that with him and Luke in written form.

Sender:	(b)(6) (b)(6) </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP (b)(6)
Recipient:	"Eisensmith, Jeffrey </O=DHS/OU=EXCHANGE ADMINISTRATIVE GROUP