Media Coverage Doesn’t Deter Actor From Threatening Democratic Voters

proofpoint.com/us/blog/threat-insight/media-coverage-doesnt-deter-actor-threatening-democratic-voters

October 21, 2020

Blog
Threat Insight
Media Coverage Doesn’t Deter Actor From Threatening Democratic Voters

October 21, 2020 Cory Altheide, DAnon, Sam S., and the Proofpoint Threat Research Team

On October 20, 2020, WUFT reported that Democratic-registered voters in Florida were receiving threatening emails purporting to be from the violent, right-wing hate group the Proud Boys. The reported emails direct recipients to “Vote for Trump or else!” in the subject lines and indicate that the senders will “know which candidate” the recipients vote for, in addition to claiming to have “gained access into the entire voting infrastructure.”

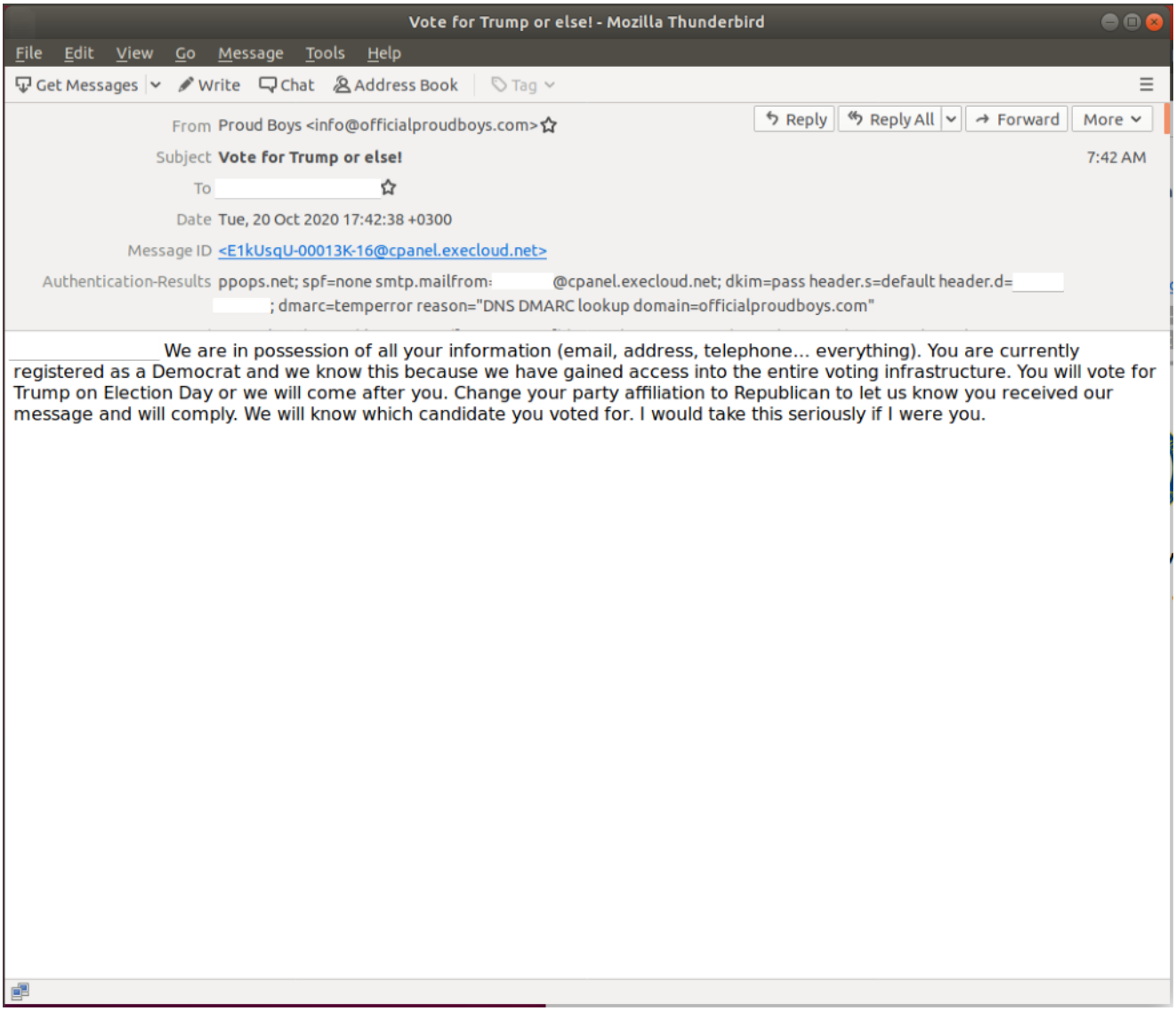

Figure 1: Email message from October 20 found in Proofpoint data, purporting to be from the Proud Boys, threatening the recipient to "Vote for Trump or else!"

October 21 messages

Multiple media outlets have reported on these messages, and on October 21, 2020, Proofpoint researchers discovered additional messages, suggesting that the widespread media coverage did not deter the actor responsible for this activity.

While the messages sent on October 20 are from "Proud Boys <info[@]officialproudboys[.]com>", messages sent on October 21 are from "Proud Boys <info[@]proudboysusa[.]com>".

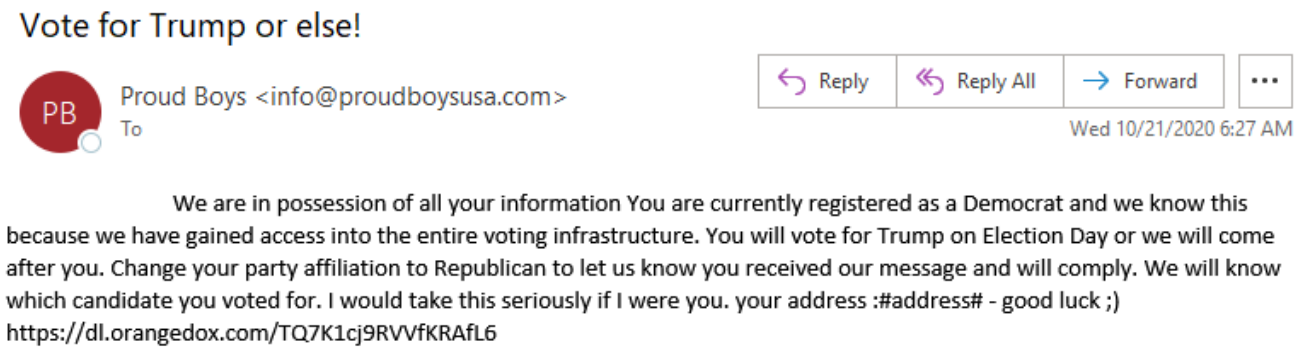

Figure 2: Email message from October 21, again threatening the recipient to "Vote for Trump or else!", with link to a Proud Boys-branded video

Emails from October 21 are sent from 162.13.192.136, an IP associated with eibank[.]com. While earlier messages included no address or what appears to be the recipient's actual address, messages observed on October 21 have a placeholder value of "#address#".

The URL on the last line of the message, "hxxps://dl.orangedox[.]com/TQ7K1cj9RVVfKRAfL6," links to a Proud Boys-branded video demonstrating a Kali Linux user filling out voter registration and absentee ballots for Alaskan citizens. We only observed two intended recipients of these messages, both of whom appear to reside in Florida. As of this posting, the video does not appear to be available via the URL above.

The video depicts registration and ballots requested through the Federal Voting Assistance Program's online portal meant to aid US service members and overseas citizens. The Kali user populates request forms with data from the Alaskan voter database while claiming each is an active duty service member. The user then demonstrates they have repeated this process multiple times, insinuating volumes in the thousands. It's not clear that this would be an effective technique to void a voter's ballot, though attempting to register a voter in multiple states could lead to confusion.

Upon examination of the video's metadata, we discovered a File Modification Date/Time of "2020:10:21 06:18:36-07:00" and Handler Vendor ID of "Apple".

October 20 messages

Proofpoint researchers also discovered messages from October 20 in our data. When examining those messages, Proofpoint researchers confirmed that some of the threatening emails contain the recipient's home address, indicating that the sender has information that could be used to follow through on the threats should they choose. While we initially believed these messages were targeting universities, we've now observed messages to intended recipients in the manufacturing industry, among others. We identified over a thousand of these messages in our data, and the messages can be broken down into two distinct sets. In addition to the "Vote for Trump or else!" subject, we also observed subjects 'vote', 'voteing' (sic) and an empty subject line.

Set One

The initial set accounts for several hundred of the messages observed with this theme. The format of these messages appears to directly match the format of the voter records presented on flvoters[.]com, a website operated by Tom Alciere which provides a mirror of Florida's voter information public records.

Messages in this set can be traced back to a PHPmailer script hosted on a likely compromised Saudi Arabian insurance company website.

```
X-PHP-Script: [redacted]/cli/post.php for 195.181.170.244
envelope-from <[redacted]@cpanel.execloud.net>)
X-Authenticated-Sender: cpanel.execloud.net: [redacted]
X-Source: /opt/cpanel/ea-php72/root/usr/bin/php-cgi
X-Source-Args: /opt/cpanel/ea-php72/root/usr/bin/php-cgi
X-Source-Dir: [redacted]com:/public_html/[redacted]/cli
```

Figure 3: Sample from email headers indicating the message origin; 195.181.170.244 is a VPN (superhosting.cz)

The actor accessed the PHPmailer script from a DataCamp Limited IP frequently used for malicious purposes. Notably, messages in this set address the recipient as "Lastname, Firstname" and do not appear to include any further personal information.

Set Two

After the set of messages using the compromised Saudi insurance company's infrastructure, the actor shifted to routing messages through the website of an Estonian textbook publisher, as reported by Vice. Notably, messages in this wave include the recipient's address-of-record. Nearly 1,500 messages were sent in this set, making it noticeably larger than the set exploiting the Saudi company.

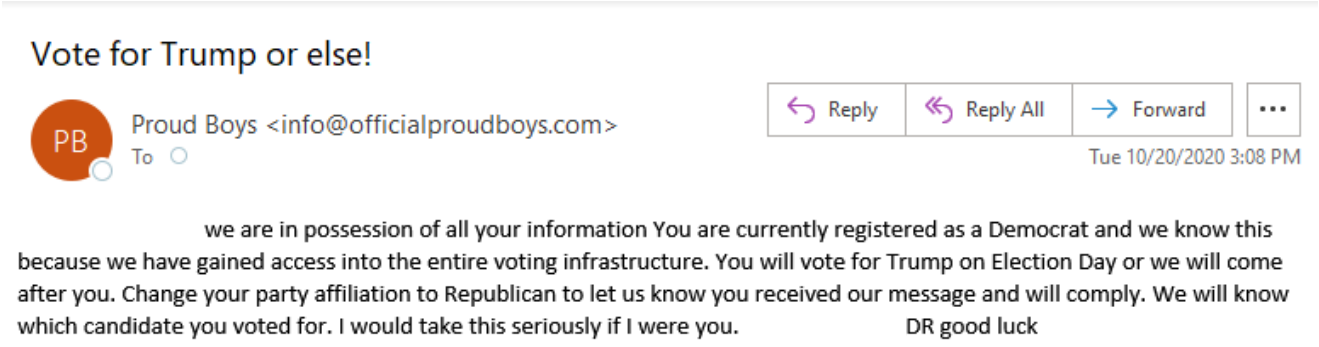

Figure 4: Message sent through Estonian infrastructure, including the recipient's name and address (redacted here)

Based on our observations, the actor appears to have made small changes to their sending script when they shifted to exploiting the Estonian publisher. Messages sent in this set included what appears to be the recipient's home address, while earlier messages only mention that the actor has the recipient's address.

Conclusion

Explicitly threatening voters to support a specific candidate is a departure from the election-themed activity we've recently observed, such as impersonation of the Democratic National Committee and various fraudulent voter registration portals. Previous activity used political themes to entice users to click on links or open attachments but did not appear especially politically motivated. Given the threatening and personalized nature of these messages, they could be sincere–though likely ineffective–attempts to carry out voter intimidation via email.

Subscribe to the Proofpoint Blog