
Frank LaRose
Ohio Secretary of State

Frank LaRose

Ohio Secretary of State

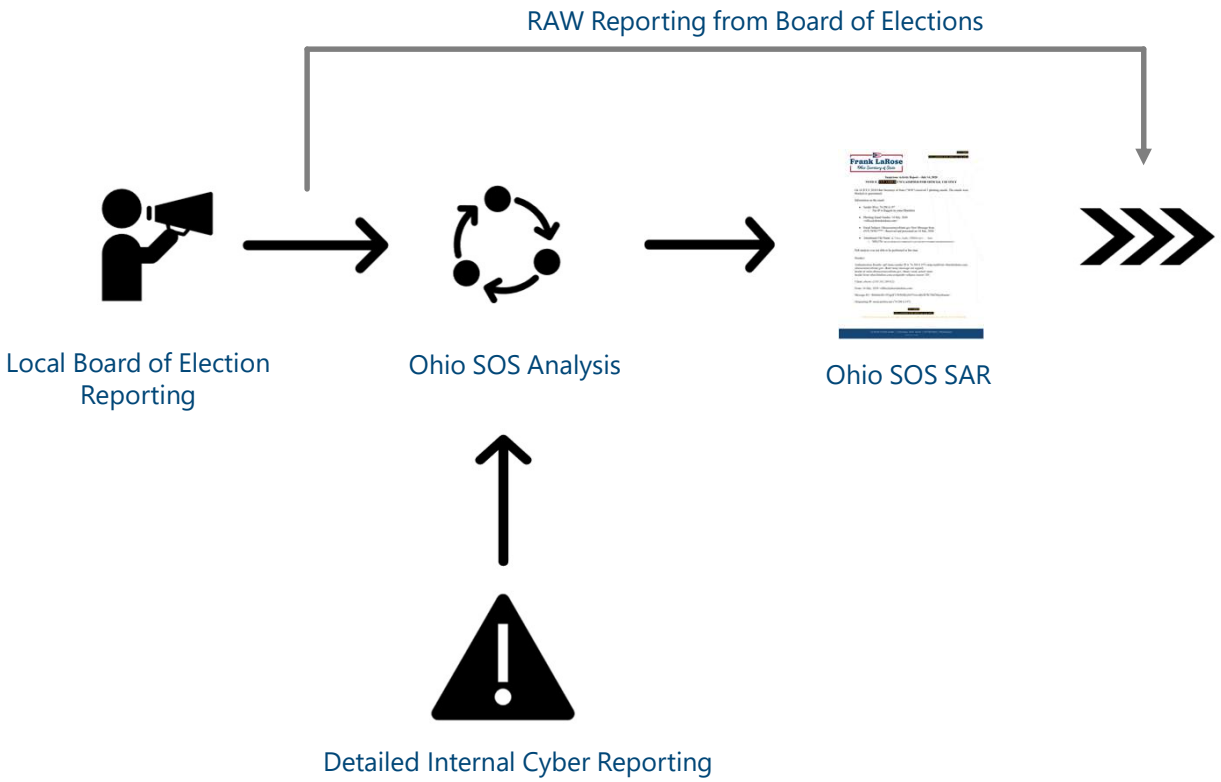
Suspicious Activity Reporting

July 2020

Cyber Security is a Team Sport

- Threat Intelligence Sharing is Highly Valuable
- Sharing is caring
- Who all receives our report
  - US Department of Homeland Security (CISA and I&A)
  - EI-ISAC
  - State of Ohio Fusion Center/State Highway Patrol
  - Ohio National Guard
  - Private Sector Cyber Security Partners

Cyber Security is a Team Sport



Frank LaRose
Ohio Secretary of State

What we report

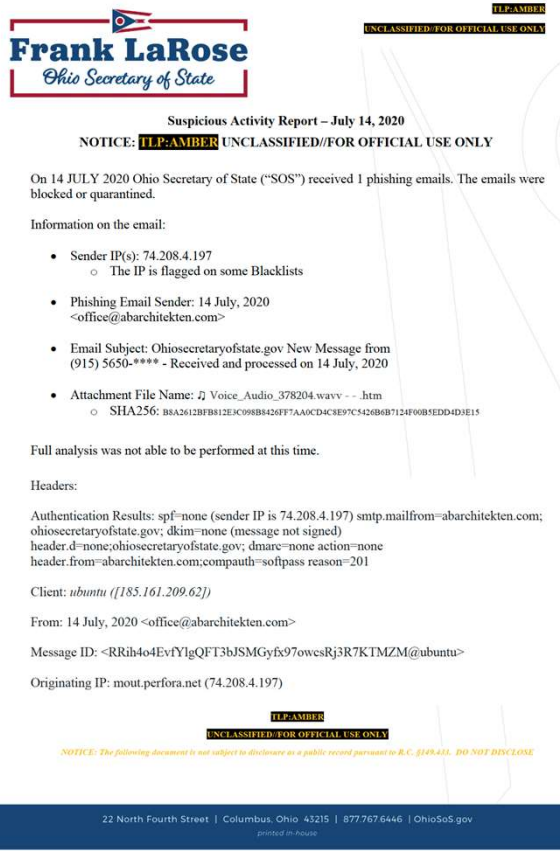
- Anything “suspicious”
- Phishing Campaigns
- SQL Injection Attempts
- Network traffic that isn’t “normal”
- Include as much information as possible!
- Look beyond your election related systems

Specific example of it making a difference

- Late in 2019, the Ohio Secretary of State filed a Suspicious Activity Report showing a high volume of scans against our Online Voter Registration System.
- Early in 2020, the Ohio Secretary of State received information from a trusted third party that the same addresses listed in the Suspicious Activity Report was also performing additional scans of another Secretary of State's network.
- The affected State was contacted, and scanning was remediated.

Frank LaRose
Ohio Secretary of State

Phishing Suspicious Activity Report Example



Frank LaRose
Ohio Secretary of State

TLP:AMBER
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Suspicious Activity Report – July 14, 2020

NOTICE: TLP:AMBER UNCLASSIFIED//FOR OFFICIAL USE ONLY

On 14 JULY 2020 Ohio Secretary of State ("SOS") received 1 phishing emails. The emails were blocked or quarantined.

Information on the email:

- Sender IP(s): 74.208.4.197
  - The IP is flagged on some Blacklists
- Phishing Email Sender: 14 July, 2020 <office@abarchitekten.com>
- Email Subject: Ohiosecretaryofstate.gov New Message from (915) 5650-**** - Received and processed on 14 July, 2020
- Attachment File Name: ♫ Voice_Audio_378204.wavv - - .htm
  - SHA256: B8A2612BFB812E3C098B8426FF7AA0CD4C8E97C5426B6B7124F00B5EDD4D3E15

Full analysis was not able to be performed at this time.

Headers:

Authentication Results: spf=none (sender IP is 74.208.4.197) smtp.mailfrom=abarchitekten.com; ohiosecretaryofstate.gov; dkim=none (message not signed) header.d=none;ohiosecretaryofstate.gov; dmarc=none action=none header.from=abarchitekten.com;compauth=softpass reason=201

Client: *ubuntu ([185.161.209.62])*

From: 14 July, 2020 <office@abarchitekten.com>

Message ID: <RRih4o4EvfYlgQFT3bJSMGyfx97owcsRj3R7KTMZM@ubuntu>

Originating IP: mout.perfora.net (74.208.4.197)

TLP:AMBER
UNCLASSIFIED//FOR OFFICIAL USE ONLY

NOTICE: The following document is not subject to disclosure as a public record pursuant to R.C. §149.433. DO NOT DISCLOSE

22 North Fourth Street | Columbus, Ohio 43215 | 877.767.6446 | OhioSoS.gov
printed in-house

Frank LaRose
Ohio Secretary of State

TLP:AMBER
UNCLASSIFIED//FOR OFFICIAL USE ONLY

Received SPF: None (protection.outlook.com: abarchitekten.com does not designate permitted sender hosts)

Reply-To: *not specified*

Screenshot of email:

From: 14 July, 2020 <office@abarchitekten.com>
Sent on: Tuesday, July 14, 2020 5:27:27 PM
To: [redacted]
Subject: Ohiosecretaryofstate.gov New Message from (915) 5650-**** - Received and processed on 14 July, 2020
Attachments: ♫ Voice_Audio_378204.wavv - - .htm (827 Bytes)

File Sent Via Microsoft Voice

Please note: These attempts were not blocked, but no users clicked on the email after review by the security team. Each email was hard deleted from the system.

Any questions, please contact [redacted]

TLP:AMBER
UNCLASSIFIED//FOR OFFICIAL USE ONLY

NOTICE: The following document is not subject to disclosure as a public record pursuant to R.C. §149.433. DO NOT DISCLOSE

22 North Fourth Street | Columbus, Ohio 43215 | 877.767.6446 | OhioSoS.gov
printed in-house

Frank LaRose
Ohio Secretary of State

Questions

Frank LaRose
Ohio Secretary of State