COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

SUFFOLK, ss. NO. SJC-12931

ROBERT GOLDSTEIN, KEVIN O'CONNOR, MELISSA BOWER SMITH, on behalf of themselves and others similarly situated,

Petitioners,

v.

WILLIAM FRANCIS GALVIN, in his Official Capacity as Secretary of the Commonwealth of Massachusetts,

Respondent.

AFFIDAVIT OF MICHELLE TASSINARI

I, Michelle Tassinari, do hereby depose and state as follows:

1. My name is Michelle Tassinari and I am the Director and Legal Counsel in the Elections Division of the Office of the Secretary of the Commonwealth (the "Secretary"). From my role in the Elections Division, I have direct, personal knowledge of the facts stated herein.

OBTAINING NOMINATION PAPERS

2. The Secretary's office provides a calendar of relevant deadlines and a booklet with instructions to all candidates when they obtain their nomination papers.

PROCESS BY WHICH LOCAL ELECTION OFFICIALS CERTIFY SIGNATURES

3. Candidates often submit more than the minimum number of certified signatures to the registrars for their review. Local election officials must continue reviewing all signatures that were timely submitted until the election officials have certified the "number of names that are required to make a nomination, increased by two fifths thereof." G.L. c. 53, § 7.

4. Local election officials perform these checks using the Voter Registration Information System ("VRIS"), a statewide, electronic database of registered voters.

5. VRIS is a closed system: it is not connected to the internet.

6. Access to VRIS is limited to computers that the Secretary's office provides to local election officials. These computers are connected to the VRIS database through a hardwired system and dedicated network. There is no way for local election officials to access these computers or the database remotely.

7. Thus, local election officials must manually check each name submitted on a candidate's nominating papers against the voter registration records maintained in the VRIS.

8. VRIS tracks the total number of names that have been certified in support of each candidate's nomination. *See* 950 C.M.R. § 55.04(4).

9. Every city and town in Massachusetts has a local chief election official. These officials have varying professional backgrounds; many also perform other local administrative duties, including keeping vital records.

10. The Secretary's office provides technical support and training to local election officials on how to perform their duties, including how to check the signatures on nominating papers and how to use the VRIS database.

11. Creating and implementing an electronic process for the submission of signatures to be checked by the registrars would require training all local election officials to use this process.

OBJECTIONS TO SIGNATURES

12. Common objections submitted by voters to certified signatures include that a signature was forged or fraudulent, or that a voter was not in fact registered to vote in the district

for which the candidate seeks nomination. *See* G.L. c. 55B, § 5.

THE PROCESS FOR PRODUCING BALLOTS

13. The 2020 September primary includes district, county and federal races, in which candidates seek the nomination of one of four political parties in the general election in November. Due to overlapping districts for congressional, Governor's Council, county, and state Legislature races, each political party requires 550 different ballot styles. This creates a total of 2,200 unique ballot styles that the Secretary's office must prepare for the primary.

14. All of the ballots must be proofread, and some must be translated into other languages, before they are ready for distribution to local election officials.

15. Once the ballots are prepared and printed, they must be distributed to the appropriate local election official for use in the election.

16. It takes approximately three weeks between the time that the Secretary finalizes the ballot contents to when the preparation is complete and the ballots are provided to the local election officials.

THE DEADLINE FOR LOCAL ELECTION OFFICIALS TO TRANSMIT BALLOTS

17. Once local election officials receive the ballots, they may begin transmitting the ballots to absentee voters.

18. In 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act ("UOCAVA") to consolidate and improve laws that allow military servicemembers and other overseas U.S. citizens ("UOCAVA voters") to vote. *See* Pub. L. No. 99-410, 100 Stat. 924.

19. In 2009, Congress enacted the Military and Overseas Voter Empowerment ("MOVE") Act, which requires that states transmit ballots to UOCAVA voters at least 45 days

before any federal election. *See* Pub. L. No. 111-84, § 579, codified at 52 U.S.C. § 20302(a)(8)(A).

20. The September primary includes federal races.

21. The September primary will be held on September 1, 2020.

22. Therefore, for the September 2020 primary, the MOVE Act requires that local election officials transmit ballots to UOCAVA voters no later than July 18, 2020.

ELECTRONIC SIGNATURES AND SUBMISSION OF ELECTRONIC DOCUMENTS

23. The Commonwealth's election laws, General Laws Chapters 50-57, contain no definition of the term "electronic signatures."

24. The term "electronic signatures," as used in the Court's April 9, 2020, Reservation and Report, could mean a variety of different things: scanned, electronic copies of documents signed by hand; electronic images of signatures dropped or pasted into electronic documents; images of signatures created using software such as DocuSign or by electronically signing with a finger, stylus, or mouse; or typed names on electronic forms.

25. A large portion of the challenges the State Ballot Law Commission ("SBLC") receives to certified signatures raise concerns regarding allegedly forged or fraudulent signatures. For example, since 2008, the SBLC has received 20 total objections related to party and non-party candidates for district and county office and to party candidates for federal office. Of these objections, 11 were challenges that signatures collected in support of nominations were forged or fraudulent.

26. If voters are permitted to sign nomination papers by typing their name into a form, rather than signing by hand, it would be difficult for someone to challenge the signature as fraudulent or forged, and likewise for the SBLC to adjudicate claims of fraud or forgery. This

could generate additional disputes before the SBLC, possibly leading to further litigation.

27. Local election officials throughout the Commonwealth have varying technological capabilities and resources, depending on factors such as the size of the municipalities they serve and the geographic area in which they are located.

28. Local election officials would have to use their municipal email accounts in order to accept emails with attachments containing the electronic copies of signatures or nomination papers. Municipal email systems may vary in terms of the size of attachments they can accept, the systems they use for cybersecurity, and their level of expertise in maintaining cybersecurity.

29. Some local election officials, particularly in Western Massachusetts, may have slower internet speeds due to limited broadband access in the area.

30. Advising local elections officials to open attachments from campaigns may make municipal offices vulnerable to malicious software such as viruses or ransomware attacks. *See* "1 in 6 Massachusetts Communities Hit By Ransomware Attacks", NBC10Boston, February 14, 2020.[1]

31. Law enforcement agencies such as the Department of Homeland Security ("DHS") Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Treasury Financial Crimes Enforcement Network ("FinCEN") have advised state and local government officials to be wary of opening unsolicited email attachments, even from known senders. *See* Exhibits A-C attached hereto. For example, FinCEN issued an advisory in July 2019 that specifically warned government entities about their vulnerability to schemes that compromise email systems used to do business. *See* Exhibit A. CISA has also issued warnings regarding the increased threat of cyberattacks such as phishing during the current pandemic. *See* Exhibit B.

[1] https://www.nbcboston.com/investigations/1-in-6-massachusetts-communities-hit-by-ransomware-attacks/2076600/

32. DHS has also designated the infrastructure used to implement United States elections as "critical," recognizing that "its incapacitation or destruction would have a devastating effect on the country." *See* Exhibit C.

33. The extent to which there may be unique technological impediments or security risks associated with requiring local election officials to open email attachments in order to process nomination signatures has not been studied.

34. Local election officials process signatures on nomination papers in hard copy. *See* 950 C.M.R. § 55.02. Local election officials' offices may lack resources, such as staff time and paper, to sort through and print large quantities of emailed signatures.

35. The Secretary's office is familiar with one state, New Jersey, where the Governor has issued an executive order that allowed campaigns for party candidates to submit nomination signatures "electronically" in light of the current public health emergency. See New Jersey Executive Order No. 105, ¶¶ 1-3, available at https://nj.gov/state/elections/assets/pdf/candidate/EO-105.pdf ("New Jersey EO"); New Jersey Division of Elections Candidate Information, available at https://nj.gov/state/elections/candidate-information.shtml.

36. The New Jersey executive order permits candidates to submit petitions containing nomination signatures electronically. New Jersey EO, ¶ 1. Pursuant to the order, the New Jersey Division of Elections permits candidates to submit forms on which the image of a signature appears; the image may be created by signing in hard copy and scanning, copying from an existing scanned signature, or by the voter creating a digital "handwritten" signature using software such as DocuSign or using their finger, stylus, or mouse. New Jersey does not accept nomination papers containing just the typed name of a voter.

37. In New Jersey, nomination papers are filed only with county election officials (for district or county offices) or state election officials (for statewide offices).

38. New Jersey does not have a certification process for voter signatures, but instead requires a witness to the signature. Due to the current pandemic, New Jersey has deemed it sufficient for the witness to be the individual who distributes the nomination papers to the voter by email and receives back the electronically signed copy.

39. Since the implementation of the executive order, election officials in New Jersey have reported problems with receiving files that exceed the maximum file size each county is capable of receiving. In addition, some candidates have submitted files via a link to an online storage site such as Google Drive or Dropbox, rather than sending the pages as attachments. When county officials would not click on the links to retrieve the papers, resulting in those candidates not being placed on the ballot, litigation has ensued.

SIGNATURE COLLECTING BEING UNDERTAKEN BY SOME CANDIDATES

40. Recognizing that traditional methods of signature gathering through in-person contact is now restricted due to social distancing mandates, some candidates have devised creative approaches to gathering signatures.

41. For example, the Secretary's office is aware of at least one candidate, State Representative Shawn Dooley, who placed blank signature pages on a table outside his house with boxes of clean pens. Representative Dooley then posted on social media that the signature pages were available for supporters to stop by and sign, using a clean pen each time. He posted on social media the following day that he had received more than 200 signatures.

42. The Secretary's office is aware of other candidates who also left signature pages in places accessible to the public and used social media to encourage registered voters to sign

them.

43. Senator Markey's reelection campaign created on online form where registered voters could request a paper copy of Markey's nomination papers. After signing the papers, the voters returned the papers to Markey's campaign in a prepaid, preaddressed envelope that the campaign had provided. "Ed Markey falling short of signatures ahead of May deadline", Boston Globe, April 7, 2020.

44. Padraic Rafferty, a first-time candidate for Governor's Council in the 7th district, has qualified for the Democratic Primary ballot by filing 1,109 certified signatures and additional required paperwork with the Secretary's office.

45. In January 2020, Representative Jose Tosado announced that he would not seek re-election as State Representative in the 9th Hampden District. Two candidates have qualified for the Democratic primary ballot in that district. Orlando Ramos has filed nomination papers containing 164 certified signatures with this Office and Denise Marie Hurst has filed nomination papers with 163 certified signatures. On April 7, 2020, Representative Angelo Scaccia announced that he would not seek re-election as State Representative in the 14th Suffolk District. Two candidates have qualified for the Democratic primary ballot in that district. Duckens Petit-Maitre has filed nomination papers containing 166 certified signatures with this Office and Gretchen Van Ness has filed nomination papers with 176 certified signatures. On April 8, 2020, Representative Harold Naughton announced that he would not seek re-election as State Representative in the 12th Worcester Representative District. One candidate, Ceylan Rowe, has filed nomination papers containing 314 certified signatures with this Office and qualified for ballot placement on the Democratic primary ballot. On March 26, 2020, Representative Elizabeth Poirier announced that she would not seek re-election in the 14th Bristol District. Since

that time, two candidates have taken out nomination papers. D. Michael Lennox took out nomination papers on April 2nd for the Republican nomination and has 36 certified signatures in VRIS as of April 14, 2020. Adam Scanlon took out papers seeking the Democratic nomination on March 29, 2020 and has 109 certified signatures in VRIS as of April 14, 2020.

46. The Secretary's office provides blank nomination papers on paper that is eight and one-half inches by fourteen inches (legal size). *See* G.L. c. 53, § 17. Candidates may make exact photocopies or scanned images of the blank nomination papers, so long as they are no larger eight and one-half inches by fourteen inches. G.L. c. 53, § 17; Robinson v. State Ballot Law Comm'n, 432 Mass. 145, 151-52 (2000). In response to inquiries from candidates, the Secretary's office has advised that local election officials will accept photocopies of nomination of papers that are identical to the originals in all respects, except that the photocopies have been shrunken to fit on paper that is eight and one-half inches by eleven inches (letter size).

47. As of 11 a.m. on April 14, 83 candidates have already qualified for the September 1, 2020 ballot, as follows:

COUNCILLOR	4
COUNTY COMMISSIONER	4
COUNTY TREASURER	1
REGISTER OF PROBATE	3
REPRESENTATIVE IN CONGRESS	1
REPRESENTATIVE IN GENERAL COURT	59
SENATOR IN GENERAL COURT	11
Grand Total	83

48. An additional 104 candidates appear to have obtained sufficient certified signatures to appear on the ballot, as reflected in VRIS, but have not yet filed their nomination papers with the Secretary.

49. Two candidates in State Representative Poirier's 14 Bristol District have

submitted certified signatures despite the fact that Poirier only announced on March 26 that she will not run for re-election. A Republican candidate, D. Michael Lennox, took out nomination papers on April 2 and has 36 certified signatures recorded in VRIS. A Democratic candidate, Adam Scanlon, took out papers on March 27 and has 109 certified signatures recorded in VRIS.

FACTS REGARDING THE PLAINTIFFS NAMED IN THE PETITION

50. The Secretary's office maintains records of which candidates have obtained or "pulled" nomination papers from the Secretary's office.

51. Each of the plaintiffs named in the petition pulled their nominating papers on February 11, 2020, the first day that papers became available.

52. The Secretary's office can determine how many signatures have been certified on behalf of each candidate by accessing that information in VRIS.

53. As of April 13, 2020, Robert Goldstein had 251 certified signatures in support of his nomination, according to VRIS data.

54. As of April 13, 2020, Kevin O'Connor had 173 certified signatures in support of his nomination, according to VRIS data.

55. As of April 13, 2020, Melissa Bower Smith had zero certified signatures in support of her nomination, according to VRIS data.

Sworn to, subject to the pains and penalties of perjury, this 14th day of April, 2020.

/s/ Michelle Tassinari
Michelle Tassinari

Exhibit A

FinCEN ADVISORY

FIN-2019-A005 July 16, 2019

Updated Advisory on Email Compromise Fraud Schemes Targeting Vulnerable Business Processes

Criminals continue to exploit vulnerable business processes with business email compromise schemes – over $9 billion in possible losses affecting U.S. financial institutions and their customers since 2016.

This Advisory should be shared with:

- *Chief Executive Officers*
- *Chief Operations Officers*
- *Chief Risk Officers*
- *Chief Compliance/BSA Officers*
- *BSA/AML Analysts/Investigators*
- *Information Technology staff*
- *Cybersecurity Units*
- *Fraud Prevention Units*
- *Legal Departments*

The Financial Crimes Enforcement Network (FinCEN) is issuing this update to the "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes" issued by FinCEN on September 6, 2016[1] ("2016 BEC Advisory") to alert financial institutions to predominant trends in reported business email compromise (BEC) fraud, including key sectors, entities, and vulnerable business processes targeted in many BEC schemes. This advisory (1) offers updated operational definitions for email compromise fraud; (2) provides information on the targeting of non-business entities and data by BEC schemes; (3) highlights general trends in BEC schemes targeting sectors and jurisdictions; and (4) alerts financial institutions to risks associated with the targeting of vulnerable business processes by BEC criminals. The information in this advisory, which complements the typologies and red flags identified in the 2016 BEC Advisory, may assist financial institutions in detecting, preventing, and reporting BEC fraud and associated money laundering activity. The red flags from the 2016 BEC Advisory remain relevant and can be useful to financial institutions in better identifying and reporting instances of BEC fraud.[2]

Based on FinCEN analysis of Bank Secrecy Act (BSA) data, discussions with law enforcement and other data, this advisory will assist financial institutions in recognizing and guarding against increasing email compromise fraud schemes and in considering their own or their customers'

1. *See* FinCEN Advisory FIN-2016-A003, "Advisory to Financial Institutions on E-mail Compromise Fraud Schemes," September 6, 2016.
2. For additional information regarding typologies and red flags of email compromise schemes in Suspicious Activity Reports (SARs), *see* FinCEN Advisory FIN-2016-A003, "Advisory to Financial Institutions on Email Compromise Fraud Schemes," September 6, 2016.

potential vulnerability to compromise of payment authorization and communications from email compromise fraud.[3] This advisory also highlights the potential for financial institutions to share information about subjects and accounts affiliated with email compromise schemes in the interest of identifying risks of fraudulent transactions, money laundering, and related crimes.

While the U.S. government and industry are heavily engaged in efforts to prevent email compromise fraud, reported incidents and aggregate attempted fraudulent wire amounts continue to rise. For example, the Federal Bureau of Investigation (FBI) reported over $12 billion in potential losses domestically and internationally from October 2013 to May 2018 from email compromise fraud.[4] Since the 2016 BEC Advisory was issued, FinCEN has received over 32,000 reports involving almost $9 billion in attempted theft from BEC fraud schemes affecting U.S. financial institutions and their customers. This represents a significant economic impact on the businesses, individuals, and even governments that are targeted by these schemes.

Financial institutions have provided valuable reporting to FinCEN regarding the nature and victims of email compromise schemes, some of which this advisory will highlight. Financial institutions can continue to play an important role in identifying, preventing, and reporting fraud schemes. FinCEN notes the importance of communication and collaboration among internal anti-money laundering and countering financing of terrorism (AML/CFT), compliance, business, fraud prevention, legal, and cybersecurity departments within financial institutions as well as with other financial institutions across the sector.[5] FinCEN continues to encourage this collaboration where resources and authorities permit and whenever feasible.

Updated Operational Definitions for Email Compromise Fraud

FinCEN analysis of emerging email compromise fraud typologies indicated a need to update the original definitions of email compromise fraud, BEC, and email account compromise (EAC) provided in the 2016 BEC Advisory. FinCEN broadens its definitions of email compromise fraud activities below to clarify that such fraud targets a variety of types of entities and may be used to misdirect any kind of payment or transmittal of other things of value. For example, while many email compromise fraud scheme payments are carried out via wire transfers (as originally stated in the 2016 BEC Advisory definition), FinCEN has observed BEC schemes fraudulently inducing funds or value transfers through other methods of payment, to include convertible virtual currency payments, automated clearing house transfers, and purchases of gift cards. The updated and expanded definitions below may be useful for financial institutions to consider as they refine their AML/CFT frameworks to better identify and report suspected illicit finance activity, including instances of email compromise fraud affecting transactions.

3. Aside from the updated operational definitions of email compromise fraud and business email compromise, the information in this advisory is complementary to the 2016 BEC Advisory. Financial institutions should refer to the 2016 BEC Advisory for additional information on general email account compromise (EAC) and BEC typologies and red flags.

4. *See* FBI Alert I-071218-PSA, "Business E-mail Compromise the 12 Billion Dollar Scam," July 12, 2018.

5. *See* FinCEN Advisory FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016.

Email Compromise Fraud: Schemes in which 1) criminals compromise[6] the email accounts of victims to send fraudulent payment instructions to financial institutions or other business associates in order to misappropriate funds or value; or in which 2) criminals compromise the email accounts of victims to effect fraudulent transmission of data that can be used to conduct financial fraud. The main types of email compromise, the definitions of which have been modified to reflect the expansion of victims being targeted, include:

> ***Business Email Compromise (BEC):*** Targets accounts of financial institutions or customers of financial institutions that are operational entities, including commercial, non-profit, non-governmental, or government entities.
>
> ***Email Account Compromise (EAC):*** Targets *personal* email accounts belonging to an individual.[7]

Other Victims of BEC

FinCEN analysis has indicated criminal groups use a variety of techniques to conduct BEC fraud against individuals, particularly and increasingly those with high net worth, and entities that routinely use email to make or arrange payments between partners, customers, or suppliers. We have recently observed that targets of these schemes fall outside of the definition of traditional business customers, such as government entities and non-profit organizations or even the financial institutions themselves.

BEC Fraud against Governments

Dozens of government organizations, ranging from foreign national governments to municipal government offices, have been targets of BEC fraud. Such thefts have targeted accounts used for pension funds, payroll accounts, and contracted services, losses of which can impact government operations as well as government employees, citizens, and vendors.

Schemes against government victims are consistent with other common typologies in BEC fraud. For example, criminals hack accounts and spoof domains to send familiar-looking messages seemingly from a trusted party in the government—often someone in a leadership role in an agency or in an office that manages finances and contracts—requesting that a counterparty in the agency with the appropriate authority initiate or process a transaction. BEC schemes targeting government entities also often include vendor impersonation.

6. Criminals engaged in email compromise fraud may directly compromise email accounts through unauthorized electronic intrusions in order to leverage the compromised account for sending messages, or they may instead impersonate an email account through spoofing the email address or using an email account closely resembling a known counterparty or customer's email address (*i.e.*, that is slightly altered by adding, changing, or deleting one or more characters).
7. The definitions of email compromise fraud, BEC, and EAC supersede the definitions in the 2016 BEC Advisory.

BEC Fraud against Educational Institutions

Schools and universities, many of which are non-profit institutions, are also targets of BEC fraud. In 2016, financial institutions reported to FinCEN over 160 incidents of BEC targeting educational institutions where criminals attempted to steal over $50 million. The education sector has the largest concentration of high-value BEC attempts in financial sector reporting, even though only approximately 2% of BEC incidents affected educational institutions in 2017. Academic institutions regularly conduct or receive high dollar transactions in the form of tuition payments, endowments, grants, and renovation and construction costs, among others. This concentration of high value transactions establish both academic institutions and attending scholars as appealing targets for BEC criminals.

Schemes against educational institutions frequently involve vendor impersonation. Specifically, attackers will use compromised or spoofed email accounts to exploit existing business relationships between academic institutions and contracted service providers, such as facilities maintenance providers. Attackers use authentic-looking payment requests to direct funds to domestic bank accounts they control. Large-scale construction and renovation projects have repeatedly been targets of high-dollar thefts.

BEC Fraud against Financial Institutions

In some cases, BEC actors directly target the financial institutions themselves. This scheme typically involves spoofing bank domains and sending what appear to be credible messages to imitate official communications between bank employees, such as sending emails that appear to be from a financial institution's Society for Worldwide Interbank Financial Telecommunication (SWIFT) department with payment instructions and SWIFT reference numbers in the email text to enhance its apparent legitimacy to the victim.

Operation WireWire—Joint U.S.-International Law Enforcement Effort to Dismantle BEC Networks: In June 2018, federal authorities announced a major coordinated law enforcement effort by the U.S. Department of Justice, the U.S. Department of Homeland Security, the U.S. Department of the Treasury, the U.S. Postal Inspection Service, and international law enforcement authorities[8] to disrupt international BEC schemes and money laundering networks. The operation, called "Operation WireWire," resulted in 74 arrests across the United States and overseas, specifically, 42 arrests in the United States, 29 arrests in Nigeria, and one each in Canada, Mauritius, and Poland. Authorities seized nearly $2.4 million, and disrupted and recovered approximately $14 million in fraudulent wire transfers. U.S. law enforcement also charged 15 alleged money mules, which play a significant role in the laundering of proceeds fraudulently derived from BEC schemes, for their roles in defrauding victims in schemes targeted under Operation WireWire.[9]

8. Operation WireWire involved international cooperation between U.S. law enforcement and authorities in Canada, Indonesia, Malaysia, Mauritius, Nigeria, and Poland. *See*, FBI News, "International Business E-Mail Compromise Takedown: Multiple Countries Involved in Coordinate Law Enforcement Effort," June 11, 2018.

9. *Id*.

General Trends in BEC Schemes and Financial Flows

Financial institution reporting of suspicious activity involving BEC schemes continues to grow since the issuance of the 2016 BEC Advisory. Instances of BEC reported to FinCEN have climbed from averaging just under 500 reports per month (averaging $110 million monthly in total attempted BEC thefts) in 2016 to over 1,100 monthly reports (averaging over $300 million monthly in total attempted BEC thefts) in 2018. FinCEN analysis of sensitive financial data revealed several prominent trends in BEC schemes affecting U.S. financial institutions and their customers, including a concentration of targeting of particular sectors as well as a prevalence of BEC schemes and movement of their proceeds through several key jurisdictions.

Top Sectors Targeted in BEC

FinCEN analysis reveals that the top three sectors commonly targeted in BEC schemes are (1) manufacturing and construction (25% of reported BEC cases); (2) commercial services (18%); and (3) real estate (16%). BEC criminals are likely tailoring their methods to targeted industries in order to increase their likelihood of success. For example, BEC scams, especially those targeting financial firms,[10] continue to leverage common typologies of impersonating organization executives (otherwise known as "Chief Executive Officer [CEO] Fraud")[11] to discourage employees receiving the fraudulent payment instructions from challenging or confirming the order.

Perpetrators of BEC fraud are using fraudulent vendor invoices when targeting certain industries (such as the education sector, as described above). Fraudulent vendor and client invoices are generally affiliated with larger BEC transaction amounts than even the CEO fraud scheme, likely due to higher expected and previously recurrent transaction amounts to pay for goods and services. Additionally, vendor impersonation scams often involve foreign intermediary beneficiaries receiving the initial flow of illicit funds. BEC criminals are likely exploiting the common use of foreign vendors and attempting to reduce the likelihood of (or at least cause a delay in) financial institutions and customers recognizing the suspicious nature of the transaction.

U.S. Accounts as the Top Destinations for BEC Proceeds

The majority of BEC incidents affecting U.S. financial institutions and their customers are increasingly involving initial domestic funds transfers, rather than international, likely taking advantage of money mule networks across the United States to move stolen funds.[12] For BEC-

10. FinCEN analysis revealed that approximately half of all BEC fraud targeting financial institutions was facilitated via emails impersonating the CEO or president.

11. For specific information on this scenario in BEC fraud, refer to Scenario 2 – "Criminal Impersonates an Executive," from the FinCEN 2016 BEC Advisory.

12. In the context of this advisory, money mules refer to persons and their accounts that are used to receive and transfer illegally acquired funds, generally on behalf of or at the direction of another and can be witting or unwitting. The FBI has highlighted the role that money mules play in moving stolen funds internationally to avert the scrutiny of financial institutions and mask the identity of individuals in criminal activity, including Internet-enabled crimes. For more information, *see* FBI News, "Don't Be a Mule: FBI Joins International Campaign to Stop Money Mules," December 17, 2018.

related transactions that either initially or subsequently transfer fraudulently derived funds outside of the United States, the FBI has reported China, Hong Kong, the United Kingdom, Mexico, and Turkey as prominent destinations of BEC-derived funds.[13]

Vulnerable Business Processes Compromised[14]

BEC perpetrators continue to refine their methodologies to ensure the greatest likelihood of success, taking into consideration industry, company size, existing relationships, and potential financial counterparties in planning their schemes. BEC perpetrators identify processes vulnerable to compromise, whether through openly available information about their targets or through cyber-enabled reconnaissance efforts (enabled through methods such as spear phishing or malware), and then insert themselves into communications by impersonating a critical player in a business relationship or transaction.[15] A scheme's probability of success and the potential payout from fraudulent payment instructions often depends on the criminal's knowledge of their victim's normal business processes, as well as weaknesses in the victim's authorization and authentication protocols.

Industries with public-facing information about their business transactions and processes can present attractive targets for BEC schemes. Such schemes have targeted the education, real estate, and agriculture sectors by leveraging publicly available information about the victim organization's vendors, contracts, and business processes.

Business Process Compromise Example—BEC Targeting Real Estate Transactions: Real estate transactions have been a particularly lucrative target for BEC schemes. The large dollar volumes involved in such transactions, whether for down payments on a property or the final transfer of proceeds upon closing, are an attractive target of opportunity for criminals engaged in BEC activity. FinCEN analysis reveals that BEC criminals often targeted several potential vulnerabilities of common real estate-related business processes:

a) Readily availability detailed public information regarding potential real estate transactions and counterparties (*e.g.*, real estate agents and homeowners);

b) General communication of transactions between real estate counterparties conducted via email; and

c) A common lack of strong authentication processes for verifying identity and validity of instructions in associated communications.

13. *See* FBI Alert I-071218-PSA, "Business E-mail Compromise the 12 Billion Dollar Scam," July 12, 2018.

14. The term "business processes" here refers to activities, protocols, and systems that support an organization's line of business and could be used in the conduct, facilitation, or affecting of transactions. This can include an organization's communications methods and schedules of transmitting payment information and the organization's payment authorization and authentication processes.

15. BEC perpetrators may leverage cyber-enabled reconnaissance efforts such as skillful social engineering or computer intrusions to gain sufficient knowledge of the organizations' business processes.

Communications that integrate publicly available information with private information obtained via email compromise can be extremely effective in fraudulently inducing an individual to send wires to accounts controlled by a BEC criminal. By understanding the nature of these social engineering schemes and assessing and mitigating their business process vulnerabilities to compromise, financial institutions and their customers can reduce their susceptibility to BEC fraud.

BEC Data Theft

As financial institutions consider their risk from BEC fraud, they should also consider their authentication and authorization processes for receiving sensitive data about the organization or their customers. The FBI and FinCEN have noted that email compromise scams have been used to deceive victims into providing criminals with protected information, such as Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for a business's employees.[16] Criminals often use stolen information in future fraudulent transactions, account takeovers, or other crimes.

Opportunities for Information Sharing Related to BEC Fraud

Many beneficiaries of BEC schemes play roles in larger networks of criminal activity and laundering of funds from illicit activity. Under the USA PATRIOT Act 314(b) safe harbor protections,[17] financial institutions may share information surrounding BEC fraud for purposes of identifying and, where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering.[18] Such information sharing may assist fellow institutions in identifying risks to the industry amounting to billions of dollars.

Since November 2016, financial institutions reported over 6,000 instances and over $2.6 billion in attempted and successful transactions affiliated with suspected money laundering activity through BEC schemes. FinCEN encourages financial institutions to share valuable information about BEC beneficiaries and perpetrators, for purposes of identifying and, where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering. Doing so may also help protect those institutions and their customers from facing the devastating losses often caused by these schemes and help identify and prevent financial crime and movement of funds through broader criminal money laundering networks.

16. For the FBI's latest Public Service Announcement on email compromise fraud, *see* FBI Alert I-071218-PSA "Business E-mail Compromise the 12 Billion Dollar Scam," July 12, 2018.

17. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act") Pub. L. No. 107-56, § 314(b); and 31 CFR § 103.110(b)(5).

18. For FinCEN's guidance clarifying that 314(b) participants may share information related to transactions, as well as the underlying specified unlawful activities, under the protection of the 314(b) safe harbor if the participant suspects that transactions may involve the proceeds of specified unlawful activities under money laundering statutes, *see* FinCEN Guidance FIN-2009-G002 "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," June 16, 2009.

Information for U.S. Financial Institutions[19]

Risk Management Considerations

FinCEN encourages financial institutions and their customers to assess the vulnerability of their business processes to compromise and consider if there are appropriate steps within their risk management approach to "harden" or increase the resiliency of their processes and systems against email fraud schemes. This can include considering the risk surrounding the financial institutions' or organizations' business processes and practices to 1) authenticate participants in communications, 2) authorize transactions, and 3) communicate information and changes about transactions.[20] The FBI has posted suggestions for internal protection techniques against email compromise fraud schemes that have been highly successful in recognizing and deflecting BEC/EAC attempts. Considering these steps could assist financial institutions in identifying and preventing transactions not authorized by their customers but requested fraudulently in BEC schemes that communicate directly with the financial institution.

A multi-faceted transaction verification process, as well as training and awareness-building to identify and avoid spear phishing schemes, can help financial institutions guard against BEC and EAC fraud. For instance, financial institutions may verify the authenticity of suspicious emailed transaction payment instructions by using multiple means of communication or by contacting others authorized to conduct the transactions. The success of BEC and EAC schemes depends on criminals prompting financial institutions to execute seemingly legitimate but unauthorized or fraudulently induced transactions. Such transactions are often irrevocable, which renders financial institutions and their customers unable to cancel payments or recall the funds. Identifying fraudulent transaction payment instructions before payments are issued is therefore essential to preventing and reducing unauthorized transactions.

Response and Recovery of Funds

FinCEN, in partnership with the FBI, the U.S. Secret Service (USSS), HSI, and the U.S. Postal Inspection Service, as well as counterpart Financial Intelligence Units (FIUs) abroad, can help financial institutions recover funds stolen as the result of BEC schemes through its Rapid Response Program (RRP). Through these partnerships, FinCEN has successfully assisted in the recovery of over $515 million with the assistance of 64 countries. While the recovery of BEC stolen funds is not assured, **FinCEN has had greater success in recovering funds when victims or financial institutions report BEC-unauthorized and fraudulently induced wire transfers to law enforcement within 24 hours**.

19. This section supersedes the information for financial institutions in the 2016 BEC Advisory. The information in this section is consistent with that in the previous advisory but includes updated elements to account for trends FinCEN identified in the email compromise fraud reporting.

20. In considering the risk of their institution or organization's business processes to compromise by BEC, entities should consider the level of information available publicly about key financial counterparties and processes, including information on public websites or on the darknet (*e.g.*, email account login credentials that have been compromised and posted for sale).

To request immediate assistance in recovering BEC-stolen funds, financial institutions should file a complaint with the FBI's Internet Crime Complaint Center (IC3), contact their local FBI field office, or contact the nearest USSS field office. Contacting law enforcement for fund recovery assistance does not relieve a financial institution from its Suspicious Activity Report (SAR) filing obligations.

Information Sharing

Due to the nature of BEC and EAC schemes, FinCEN encourages communication among financial institutions under the auspices of Section 314(b) of the USA PATRIOT Act for purposes of identifying and, where appropriate, reporting activities that they suspect may involve possible terrorist activity or money laundering. Sharing of this information could also help prevent billions of dollars in potential losses to financial institutions and their customers. Financial institutions should be prepared to provide transactional details and cyber-related information surrounding the BEC scheme when requesting assistance in recovering funds.

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves or aggregates to $5,000 or more in funds or other assets and involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[21] With respect to email compromise fraud involving fraudulent payment instructions, a financial institution has a SAR filing obligation regardless of whether the scheme or involved transactions were successful, and regardless of whether the financial institution or its customers incurred an actual loss.[22]

Financial institutions are required to file complete and accurate reports that incorporate **all relevant information** available, including **cyber-related information**. When filing a SAR regarding suspicious transactions that involve cyber-events (such as BEC fraud), financial institutions should provide all pertinent available information on the event and associated suspicious activity, including cyber-related information, in the SAR form and narrative.[23] Specifically, the following information is highly valuable to law enforcement and FinCEN in investigating BEC/EAC fraud:

21. *See*, 31 CFR. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320. The monetary threshold for filing money services businesses SARs is, with one exception, set at or above $2,000 (*see* 31 CFR. § 1022.320(a)(2)).
22. *Id*.
23. *See* FinCEN Frequently Asked Questions, "Frequently Asked Questions (FAQs) regarding the Reporting of Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information through Suspicious Activity Reports (SARs)," October 25, 2016.

Transaction details:

1) Dates and amounts of suspicious transactions;
2) Sender's identifying information, account number, and financial institution;
3) Beneficiary's identifying information, account number, and financial institution; and
4) Correspondent and intermediary financial institutions' information, if applicable.

Scheme details:

1) Relevant email addresses and associated Internet Protocol (IP) addresses with their respective timestamps;
2) Description and timing of suspicious email communications and any involved compromised or impersonated parties; and
3) Description of related cyber-events and use (or compromise) of particular technology in the conduct of the fraud. For example, financial institutions should consider including any of the following information or evidence related to the email compromise fraud:
   a) Email auto-forwarding
   b) Inbox sweep rules or sorting rules set up in victim email accounts
   c) A malware attack
   d) The authentication protocol that was compromised (*i.e.*, single-factor or multi-factor, one-step or multi-step, etc.)

FinCEN continues to encourage financial institution collaboration among BSA/AML, cybersecurity, legal departments, fraud prevention, and other relevant units that can assist financial institutions to identify and report relevant technical indicators and other information related to cyber-events and cyber-enabled crime, including email compromise fraud schemes.[24]

The trends and typologies reported in this advisory, in conjunction with the red flags and other information in the 2016 BEC Advisory, should assist financial institutions in better identifying BEC-related activity and risk. As with red flags, financial activity involving the highlighted sectors and jurisdictions in this advisory associated with higher levels of BEC and EAC fraud

24. *See* FinCEN Advisory FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016.

may actually reflect legitimate financial activities, therefore financial institutions should evaluate indicators of potential BEC or EAC activity in combination with other red flags and the expected transaction activity before making determinations of suspiciousness.[25]

FinCEN requests that financial institutions **reference this advisory and include the following key terms in the SAR narrative**:

"BEC FRAUD" when **businesses or organizations** are the scheme victims

"EAC FRAUD" when **individuals** are the scheme victims

Financial institutions should also select SAR field 42 (Cyber event) as the associated suspicious activity type to indicate a connection between the suspicious activity being reported and possible BEC or EAC fraud. Financial institutions should include one or both key terms to the extent they are able to distinguish between BEC and EAC fraud. Additionally, financial institutions **should include any relevant technical cyber indicators** related to the email compromise fraud and associated transactions **within the available structured cyber event indicator SAR fields 44(a)-(j), (z)**.

In instances of **reporting of BEC** schemes that **result in the communication of *information*** that could be used to facilitate future fraudulent transactions, which may be voluntary, FinCEN requests that financial institutions include the following key term in the SAR narrative:

"BEC DATA THEFT"

This advisory does not establish new regulatory interpretations, expectations, or requirements. The obligations of regulated persons and financial institutions under the Bank Secrecy Act are subject to the applicable sections of the Code of Federal Regulations, and to subsequent administrative rulings that clarify the application of the rules within the context of specific sets of facts and circumstances. All definitions proposed in this advisory are for ease of reference only, and apply only within the scope of the advisory itself.

25. For additional information regarding typologies and red flags of email compromise schemes in Suspicious Activity Reports (SARs), *see* FinCEN Advisory FIN-2016-A003, "Advisory to Financial Institutions on Email Compromise Fraud Schemes," September 6, 2016.

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at frc@fincen.gov.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day). The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

Exhibit B

TLP:WHITE

More Alerts

Alert (AA20-099A)

COVID-19 Exploited by Malicious Cyber Actors

Original release date: April 08, 2020

Summary

This is a joint alert from the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC).

This alert provides information on exploitation by cybercriminal and advanced persistent threat (APT) groups of the current coronavirus disease 2019 (COVID-19) global pandemic. It includes a non-exhaustive list of indicators of compromise (IOCs) for detection as well as mitigation advice.

Both CISA and NCSC are seeing a growing use of COVID-19-related themes by malicious cyber actors. At the same time, the surge in teleworking has increased the use of potentially vulnerable services, such as virtual private networks (VPNs), amplifying the threat to individuals and organizations.

APT groups and cybercriminals are targeting individuals, small and medium enterprises, and large organizations with COVID-19-related scams and phishing emails. This alert provides an overview of COVID-19-related malicious cyber activity and offers practical advice that individuals and organizations can follow to reduce the risk of being impacted. The IOCs provided within the accompanying .csv and .stix files of this alert are based on analysis from CISA, NCSC, and industry.

Note: this is a fast-moving situation and this alert does not seek to catalogue all COVID-19-related malicious cyber activity. Individuals and organizations should remain alert to increased activity relating to COVID-19 and take proactive steps to protect themselves.

Technical Details

Summary of Attacks

APT groups are using the COVID-19 pandemic as part of their cyber operations. These cyber threat actors will often masquerade as trusted entities. Their activity includes using coronavirus-themed phishing messages or malicious applications, often masquerading as

trusted entities that may have been previously compromised. Their goals and targets are consistent with long-standing priorities such as espionage and “hack-and-leak” operations.

Cybercriminals are using the pandemic for commercial gain, deploying a variety of ransomware and other malware.

Both APT groups and cybercriminals are likely to continue to exploit the COVID-19 pandemic over the coming weeks and months. Threats observed include:

- Phishing, using the subject of coronavirus or COVID-19 as a lure,
- Malware distribution, using coronavirus- or COVID-19- themed lures,
- Registration of new domain names containing wording related to coronavirus or COVID-19, and
- Attacks against newly—and often rapidly—deployed remote access and teleworking infrastructure.

Malicious cyber actors rely on basic social engineering methods to entice a user to carry out a specific action. These actors are taking advantage of human traits such as curiosity and concern around the coronavirus pandemic in order to persuade potential victims to:

- Click on a link or download an app that may lead to a phishing website, or the downloading of malware, including ransomware.
  - For example, a malicious Android app purports to provide a real-time coronavirus outbreak tracker but instead attempts to trick the user into providing administrative access to install "CovidLock" ransomware on their device.[1]
- Open a file (such as an email attachment) that contains malware.
  - For example, email subject lines contain COVID-19-related phrases such as “Coronavirus Update” or “2019-nCov: Coronavirus outbreak in your city (Emergency)”

To create the impression of authenticity, malicious cyber actors may spoof sender information in an email to make it appear to come from a trustworthy source, such as the World Health Organization (WHO) or an individual with “Dr.” in their title. In several examples, actors send phishing emails that contain links to a fake email login page. Other emails purport to be from an organization’s human resources (HR) department and advise the employee to open the attachment.

Malicious file attachments containing malware payloads may be named with coronavirus- or COVID-19-related themes, such as “President discusses budget savings due to coronavirus with Cabinet.rtf.”

Note: a non-exhaustive list of IOCs related to this activity is provided within the accompanying .csv and .stix files of this alert.

Phishing

CISA and NCSC have both observed a large volume of phishing campaigns that use the social engineering techniques described above.

Examples of phishing email subject lines include:

- 2020 Coronavirus Updates,
- Coronavirus Updates,
- 2019-nCov: New confirmed cases in your City, and
- 2019-nCov: Coronavirus outbreak in your city (Emergency).

These emails contain a call to action, encouraging the victim to visit a website that malicious cyber actors use for stealing valuable data, such as usernames and passwords, credit card information, and other personal information.

SMS Phishing

Most phishing attempts come by email but NCSC has observed some attempts to carry out phishing by other means, including text messages (SMS).

Historically, SMS phishing has often used financial incentives—including government payments and rebates (such as a tax rebate)—as part of the lure. Coronavirus-related phishing continues this financial theme, particularly in light of the economic impact of the epidemic and governments' employment and financial support packages. For example, a series of SMS messages uses a UK government-themed lure to harvest email, address, name, and banking information. These SMS messages—purporting to be from "COVID" and "UKGOV" (see figure 1)—include a link directly to the phishing site (see figure 2).

Figure 1: UK government-themed SMS phishing

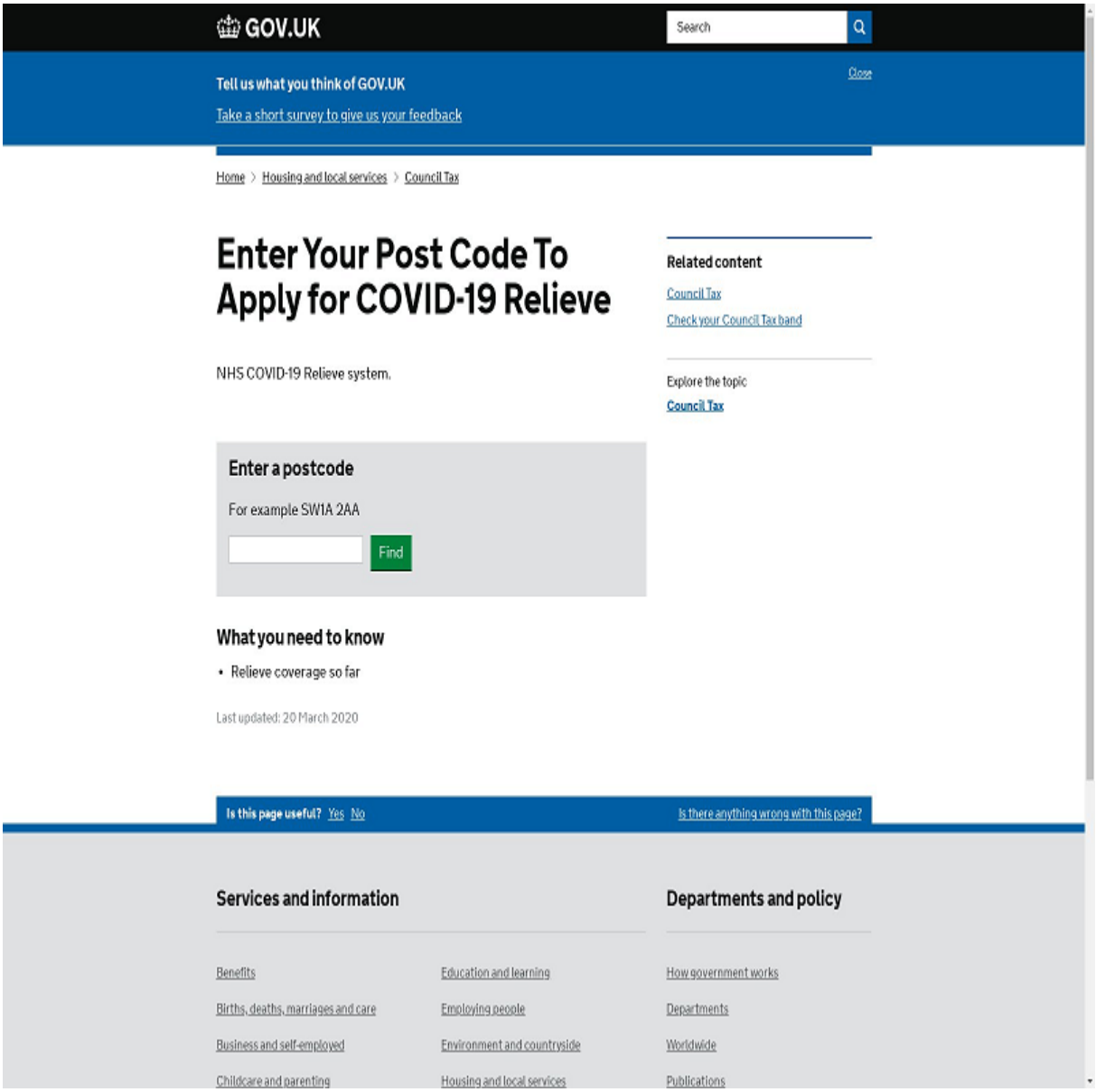

Figure 2: UK government-themed phishing page

As this example demonstrates, malicious messages can arrive by methods other than email. In addition to SMS, possible channels include WhatsApp and other messaging services. Malicious cyber actors are likely to continue using financial themes in their phishing campaigns. Specifically, it is likely that they will use new government aid packages responding to COVID-19 as themes in phishing campaigns.

Phishing for credential theft

A number of actors have used COVID-19-related phishing to steal user credentials. These emails include previously mentioned COVID-19 social engineering techniques, sometimes complemented with urgent language to enhance the lure.

If the user clicks on the hyperlink, a spoofed login webpage appears that includes a password entry form. These spoofed login pages may relate to a wide array of online services including—but not limited to—email services provided by Google or Microsoft, or services accessed via government websites.

To further entice the recipient, the websites will often contain COVID-19-related wording within the URL (e.g., “corona-virus-business-update,” “covid19-advisory,” or “cov19esupport”). These spoofed pages are designed to look legitimate or accurately impersonate well-known websites. Often the only way to notice malicious intent is through examining the website URL. In some circumstances, malicious cyber actors specifically customize these spoofed login webpages for the intended victim.

If the victim enters their password on the spoofed page, the attackers will be able to access the victim’s online accounts, such as their email inbox. This access can then be used to acquire personal or sensitive information, or to further disseminate phishing emails, using the victim’s address book.

Phishing for malware deployment

A number of threat actors have used COVID-19-related lures to deploy malware. In most cases, actors craft an email that persuades the victim to open an attachment or download a malicious file from a linked website. When the victim opens the attachment, the malware is executed, compromising the victim’s device.

For example, NCSC has observed various email messages that deploy the “Agent Tesla” keylogger malware. The email appears to be sent from Dr. Tedros Adhanom Ghebreyesus, Director-General of WHO. This email campaign began on Thursday, March 19, 2020. Another similar campaign offers thermometers and face masks to fight the epidemic. The email purports to attach images of these medical products but instead contains a loader for Agent Tesla.

In other campaigns, emails include a Microsoft Excel attachment (e.g., “8651 8-14-18.xls”) or contain URLs linking to a landing page that contains a button that—if clicked—redirects to download an Excel spreadsheet, such as "EMR Letter.xls”. In both cases, the Excel file contains macros that, if enabled, execute an embedded dynamic-link library (DLL) to install the “Get2 loader" malware. Get2 loader has been observed loading the “GraceWire” Trojan.

The "TrickBot" malware has been used in a variety of COVID-19-related campaigns. In one example, emails target Italian users with a document purporting to be information related to COVID-19 (see figure 3). The document contains a malicious macro that downloads a batch file (BAT), which launches JavaScript, which—in turn—pulls down the TrickBot binary, executing it on the system.

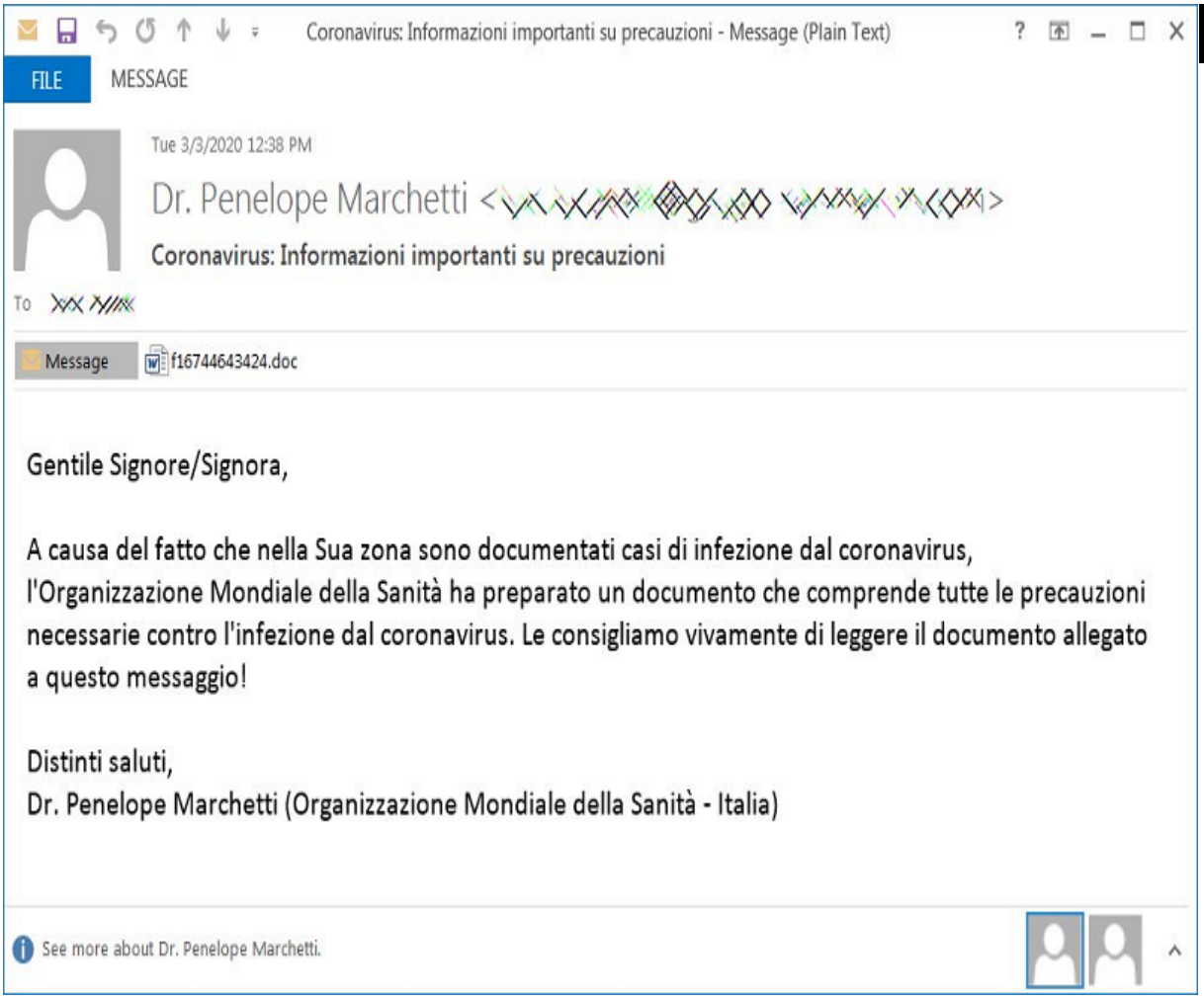

Figure 3: Email containing malicious macro targeting Italian users[2]

In many cases, Trojans—such as Trickbot or GraceWire—will download further malicious files, such as Remote Access Trojans (RATs), desktop-sharing clients, and ransomware. In order to maximize the likelihood of payment, cybercriminals will often deploy ransomware at a time when organizations are under increased pressure. Hospitals and health organizations in the United States,[3] Spain,[4] and across Europe[5] have all been recently affected by ransomware incidents.

As always, individuals and organizations should be on the lookout for new and evolving lures. Both CISA[6],[7] and NCSC[8] provide guidance on mitigating malware and ransomware attacks.

Exploitation of new teleworking infrastructure

Many organizations have rapidly deployed new networks, including VPNs and related IT infrastructure, to shift their entire workforce to teleworking.

Malicious cyber actors are taking advantage of this mass move to telework by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. In several examples, CISA and NCSC have observed actors scanning for publicly known vulnerabilities in Citrix. Citrix vulnerability, CVE-2019-19781, and its exploitation

have been widely reported since early January 2020. Both CISA[9] and NCSC[10] provide guidance on CVE-2019-19781 and continue to investigate multiple instances of this vulnerability's exploitation.

Similarly, known vulnerabilities affecting VPN products from Pulse Secure, Fortinet, and Palo Alto continue to be exploited. CISA provides guidance on the Pulse Secure vulnerability[11] and NCSC provides guidance on the vulnerabilities in Pulse Secure, Fortinet, and Palo Alto.[12]

Malicious cyber actors are also seeking to exploit the increased use of popular communications platforms—such as Zoom or Microsoft Teams—by sending phishing emails that include malicious files with names such as "zoom-us-zoom_##########.exe" and "microsoft-teams_V#mu#D_##########.exe" (# representing various digits that have been reported online).[13] CISA and NCSC have also observed phishing websites for popular communications platforms. In addition, attackers have been able to hijack teleconferences and online classrooms that have been set up without security controls (e.g., passwords) or with unpatched versions of the communications platform software.[14]

The surge in teleworking has also led to an increase in the use of Microsoft's Remote Desktop Protocol (RDP). Attacks on unsecured RDP endpoints (i.e., exposed to the internet) are widely reported online,[15] and recent analysis[16] has identified a 127% increase in exposed RDP endpoints. The increase in RDP use could potentially make IT systems—without the right security measures in place—more vulnerable to attack.[17]

Indicators of compromise

CISA and NCSC are working with law enforcement and industry partners to disrupt or prevent these malicious cyber activities and have published a non-exhaustive list of COVID-19-related IOCs via the following links:

- AA20-099A_WHITE.csv
- A20-099A_WHITE.stix

In addition, there are a number of useful publicly available resources that provide details of COVID-19-related malicious cyber activity:

- Recorded Futures' report, *Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide*
- DomainTools' *Free COVID-19 Threat List - Domain Risk Assessments for Coronavirus Threats*
- GitHub list of IOCs used COVID-19-related cyberattack campaigns gathered by GitHub user Parth D. Maniar
- GitHub list of Malware, spam, and phishing IOCs that involve the use of COVID-19 or coronavirus gathered by SophosLabs
- Reddit master thread to collect intelligence relevant to COVID-19 malicious cyber threat actor campaigns

- Tweet regarding the MISP project's dedicated #COVID2019 MISP instance to share COVID-related cyber threat information

Mitigations

Malicious cyber actors are continually adjusting their tactics to take advantage of new situations, and the COVID-19 pandemic is no exception. Malicious cyber actors are using the high appetite for COVID-19-related information as an opportunity to deliver malware and ransomware, and to steal user credentials. Individuals and organizations should remain vigilant. For information regarding the COVID-19 pandemic, use trusted resources, such as the Centers for Disease Control and Prevention (CDC)'s COVID-19 Situation Summary.

Following the CISA and NCSC advice set out below will help mitigate the risk to individuals and organizations from malicious cyber activity related to both COVID-19 and other themes:

- CISA guidance for defending against COVID-19 cyber scams
- CISA Insights: Risk Management for Novel Coronavirus (COVID-19), which provides guidance for executives regarding physical, supply chain, and cybersecurity issues related to COVID-19
- CISA Alert: Enterprise VPN Security
- CISA webpage providing a repository of the agency's COVID-19 guidance
- NCSC guidance to help spot, understand, and deal with suspicious messages and emails
- NCSC phishing guidance for organizations and cyber security professionals
- NCSC guidance on mitigating malware and ransomware attacks
- NCSC guidance on home working
- NCSC guidance on end user device security

Phishing guidance for individuals

The NCSC's suspicious email guidance explains what to do if you've already clicked on a potentially malicious email, attachment, or link. It provides advice on who to contact if your account or device has been compromised and some of the mitigation steps you can take, such as changing your passwords. It also offers NCSC's top tips for spotting a phishing email:

- **Authority** – Is the sender claiming to be from someone official (e.g., your bank or doctor, a lawyer, a government agency)? Criminals often pretend to be important people or organizations to trick you into doing what they want.
- **Urgency** – Are you told you have a limited time to respond (e.g., in 24 hours or immediately)? Criminals often threaten you with fines or other negative consequences.
- **Emotion** – Does the message make you panic, fearful, hopeful, or curious? Criminals often use threatening language, make false claims of support, or attempt to tease you

into wanting to find out more.

- **Scarcity** – Is the message offering something in short supply (e.g., concert tickets, money, or a cure for medical conditions)? Fear of missing out on a good deal or opportunity can make you respond quickly.

Phishing guidance for organizations and cybersecurity professionals

Organizational defenses against phishing often rely exclusively on users being able to spot phishing emails. However, organizations that widen their defenses to include more technical measures can improve resilience against phishing attacks.

In addition to educating users on defending against these attacks, organizations should consider NCSC's guidance that splits mitigations into four layers, on which to build defenses:

1. Make it difficult for attackers to reach your users.
2. Help users identify and report suspected phishing emails (see CISA Tips, Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Scams).
3. Protect your organization from the effects of undetected phishing emails.
4. Respond quickly to incidents.

CISA and NCSC also recommend organizations plan for a percentage of phishing attacks to be successful. Planning for these incidents will help minimize the damage caused.

Communications platforms guidance for individuals and organizations

Due to COVID-19, an increasing number of individuals and organizations are turning to communications platforms—such as Zoom and Microsoft Teams— for online meetings. In turn, malicious cyber actors are hijacking online meetings that are not secured with passwords or that use unpatched software.

Tips for defending against online meeting hijacking (Source: FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic, FBI press release, March 30, 2020):

- Do not make meetings public. Instead, require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a meeting on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. Change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications.
- Ensure telework policies address requirements for physical and information security.

Disclaimers

TLP:WHITE

This report draws on information derived from CISA, NCSC, and industry sources. Any findings and recommendations made have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

CISA does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by CISA.

References

[1] CovidLock ransomware exploits coronavirus with malicious Android app. TechR…
[2] TrickBot Malware Targets Italy in Fake WHO Coronavirus Emails. Bleeping Com…
[3] Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-1…
[4] Spanish hospitals targeted with coronavirus-themed phishing lures in Netwal…
[5] COVID-19 Testing Center Hit By Cyberattack. Bleeping Computer. March 14, 20…
[6] CISA Tip: Protecting Against Malicious Code
[7] CISA Ransomware webpage
[8] NCSC Guidance: Mitigating malware and ransomware attacks
[9] CISA Alert: Detecting Citrix CVE-2019-19781
[10] NCSC Alert: Actors exploiting Citrix products vulnerability
[11] CISA Alert: Continued Exploitation of Pulse Secure VPN Vulnerability
[12] NCSC Alert: Vulnerabilities exploited in VPN products used worldwide
[13] COVID-19 Impact: Cyber Criminals Target Zoom Domains. Check Point blog. Ma…
[14] FBI Press Release: FBI Warns of Teleconferencing and Online Classroom Hija…
[15] Microsoft Security blog: Human-operated ransomware attacks: A preventable …
[16] Reposify blog: 127% increase in exposed RDPs due to surge in remote work. …
[17] CISA Tip: Securing Network Infrastructure Devices

Revisions

April 8, 2020: Initial Version

TLP:WHITE

Exhibit C

TLP:WHITE

ELECTION INFRASTRUCTURE SECURITY

Fair and free elections are a hallmark of American democracy. The American people's confidence in the value of their vote is principally reliant on their confidence in the security and resilience of the infrastructure that makes the Nation's elections possible. Accordingly, an electoral process that is both secure and resilient is a vital national interest and one of CISA's highest priorities.

CISA is committed to working collaboratively with those on the front lines of elections—state and local governments, election officials, federal partners, and vendors—to manage risks to the Nation's election infrastructure. CISA will remain transparent and agile in its vigorous efforts to secure America's election infrastructure from new and evolving threats.

Every year, citizens across the United States head to their local polling stations in order to cast their ballots for the candidates of their choice. The Cybersecurity and Infrastructure Security Agency (CISA) works to ensure the physical security and cybersecurity of the systems and assets that supports the Nation's elections. Known as election infrastructure, this assembly of systems and networks includes but is not limited to:

- Voter registration databases and associated IT systems
- IT infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results, and post-election reporting to certify and validate results)
- Voting systems and associated infrastructure
- Storage facilities for election and voting system infrastructure
- Polling places to include early voting locations

In January 2017, the Department of Homeland Security (DHS) designated the infrastructure used to administer the Nation's elections as critical infrastructure. This designation recognizes that the United States' election infrastructure is of such vital importance to the American way of life that its incapacitation or destruction would have a devastating effect on the country.

CISA is committed to working collaboratively with those on the front lines of elections—state and local governments, election officials, federal partners, and vendors—to manage risks to the Nation's election infrastructure. CISA will remain transparent and agile in its vigorous efforts to secure America's election infrastructure from new and evolving threats.

CISA'S ELECTION SERVICES

TLP:WHITE

While ultimate responsibility for administering the Nation's elections rests with state a governments, CISA offers a variety of free services to help states ensure both the physical security and cybersecurity of their elections infrastructure. Additionally, election infrastructure's critical infrastructure designation enables CISA to provide services on a prioritized basis at the request of state and local elections officials.

Cybersecurity Assessments

Detection and Prevention

Information Sharing and Awareness

Training and Career Development

TLP:WHITE