



ENGAGEMENT REPORT

Hunt Engagement

2458780

NUMBER

October 23, 2019

DATE

Digital Media Analysis for Durham County Board of Elections

CONTENTS

Executive Summary.....	2
Background	2
Hunt.....	3
Findings and Analysis.....	5
Recommendations.....	6
Conclusion.....	12

HOW TO USE THIS REPORT

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) produced this report for Durham County Board of Elections (DCBoE) in support of hunt operations conducted on digital media provided by DCBoE.

CISA understands that DCBoE may distribute this report to its contractors and other support personnel who need to know the information to protect themselves or prevent further harm.

DISCLAIMER: This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information within. DHS does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:AMBER: Limited disclosure, restricted to participants' organizations. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see <https://www.us-cert.gov/tlp>.

WARNING: This document is UNCLASSIFIED//For Official Use Only (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with the DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need to know" without prior approval of an authorized DHS office.



CISA
CYBER+INFRASTRUCTURE

EXECUTIVE SUMMARY

The CISA Hunt and Incident Response Team (HIRT) provides hunt assessments, upon client request, to determine if an intrusion has occurred within the client's network environment. HIRT's goal during a hunt is to search throughout the client's critical, high-value network environment to determine if there is evidence of current or previous targeted malicious activity.

This report summarizes HIRT's activities, findings, and analysis from an off-site media analysis engagement in response to a written Analysis Request Form (ARF) signed June 5, 2019 and returned to HIRT by DCBoE.

On Election Day, November 8, 2016, the ePollbook laptops used in certain Durham County precincts presented inaccurate data to poll workers. The inaccuracies included erroneously identifying voters as having already voted, identifying registered voters as unregistered, and prompting poll workers to ask voters to present their identification (ID) when ID was not required under NC law. These ePollbooks proved sufficiently inaccurate and, as a result, Durham County reverted to paper registration tracking, which caused delays and inconvenienced Durham County voters. DCBoE and the North Carolina State Board of Elections (NCBoE) examined the cause of the erroneous ePollbook behavior. Following the release of the *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, DCBoE and NCBoE approached CISA because they were concerned about the possibility that advanced threat actors affiliated with Russia manipulated these ePollbooks or the voter registration information they contained.

HIRT deployed host-based analysis tools to examine various artifacts while searching for indicators of compromise (IOCs). HIRT assessed 24 ePollbook laptops, 21 USB drives, and 2 images of a desktop computer, all of which were provided by NCBoE Chief Investigator Fleming.

During its analysis, HIRT did not conclusively identify any threat actor activity. However, HIRT did identify aspects of DCBoE's security that could be improved. The Findings and Analysis section lists HIRT's observations related to these issues, and the Client-Tailored Recommendations section provides suggestions for appropriate mitigation actions. HIRT recommends DCBoE review this report and implement the suggested recommendations to further enhance their security posture.

BACKGROUND

DCBoE oversees elections administration in Durham County, NC, and NCBoE is the NC state agency charged with administering the elections process and working in conjunction with county boards of elections.

During the November 8, 2016, general election, the ePollbooks used in certain Durham County precincts presented inaccurate data to poll workers. Inaccuracies included erroneously identifying voters as having already voted, identifying registered voters as unregistered, and prompting poll workers to ask voters to present their ID when ID was not required under NC law. DCBoE, consequently, reverted to using paper voter registration tracking, which caused delays and inconvenienced Durham County voters. DCBoE and NCBoE worked to identify the underlying reasons for these computer errors. Following the release of the *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, both parties approached

CISA with concerns about potential nation-state threat actor interference with voter registration systems, software, and data. Their specific concerns were:

- If advanced threat actors planted malware on any of the devices identified in this report
- If advanced threat actors accessed the devices identified here in such a way that they were able to alter or corrupt voter registration data

On or about May 31, 2019, NCBoE engaged with CISA to explore the possibility of CISA assisting with a technical analysis of the ePollbooks. Following discussions with CISA, NCBoE, and DCBoE representatives, DCBoE signed an ARF on June 5, 2019, covering 24 ePollbook laptops, 21 USB activators, and disk images of the desktop computer used to load voter registration information onto the USB activators. On June 11, 2019, Chief Investigator Fleming delivered to CISA's [REDACTED] facility 24 ePollbooks laptops, 21 USB drives known as activators, and 10 hard drives containing images taken by NCBoE, including an image of the desktop computer used to load voter registration information onto the activators. On September 24, 2019, Chief Investigator Fleming delivered to CISA's [REDACTED] facility one hard drive containing images taken by a third-party forensics firm on behalf of DCBoE containing, among other images, an image of the above-mentioned desktop computer. HIRT performed host forensic analysis on the above media at HIRT's [REDACTED] lab facility from June 11, 2019, through October 16, 2019.

HUNT

Engagement Scope

The scope of HIRT's hunt engagement included 24 ePollbook laptops, 21 USB activators, and 1 desktop computer image. HIRT created its own ePollbook laptop and USB activator images, and conducted its analysis on those images. Through discussions with DCBoE and NCBoE personnel, HIRT identified the desktop computer as a high value asset. The desktop is the system used by DCBoE employees who downloaded voter registration data from state servers and loaded it onto the activators for use with the laptops. HIRT also relied on images taken by third-party entities (NCBoE and a private forensics firm hired by DCBoE) because the desktop's original hard drive was not available for imaging. HIRT analyzed these systems for IOCs and artifacts consistent with advanced persistent threat access and activity.

Tools Used

HIRT used the following list of DHS-owned tools to conduct host analysis during the engagement (this list is not exhaustive):

- [REDACTED] – HIRT used [REDACTED] to perform forensic “deep dives” on images taken of the media provided for analysis.
- [REDACTED] – HIRT used [REDACTED] to perform forensic “deep dives” on images taken of the media provided for analysis.
- [REDACTED] – HIRT used [REDACTED] imaging systems to take original images of the laptops and USB activators for analysis.
- [REDACTED] – HIRT used [REDACTED] to perform IOC signature scans.
- **Anti-virus** – HIRT performed malware scans using a collection of anti-virus and malware scanning products.

- [REDACTED]
- [REDACTED]
- [REDACTED]

FINDINGS AND ANALYSIS

This section provides HIRT's technical findings and analysis for this engagement.

No Artifacts Suggesting Malware on or Remote Access to EPollbooks

HIRT examined 24 ePollbook laptops that ran EViD software, an application package used by poll workers at election precincts to view voter registration during the November 8, 2016 election. HIRT performed automated scans using a collection of IOCs and signatures and performed a manual analysis of the system configuration and common sources of artifacts. [REDACTED]

[REDACTED] After a review of these systems and the available data, HIRT was unable to identify any artifacts suggesting the presence of malware or unauthorized remote access.

No Artifacts Suggesting Malware on USB Activators

HIRT analyzed 21 USB activators that are used to transfer voter registration database files to the ePollbook laptops. The activators remain connected to the ePollbooks while the EViD software is in use. HIRT performed automated scans using a collection of IOCs and signatures and performed a manual analysis of file system configuration. After reviewing these systems and the available data, HIRT was unable to identify any artifacts demonstrating signs of malicious software.

Screen Sharing Occurred on the Desktop System

HIRT examined two images of a desktop computer that was used to download voter registration data from NCBoE servers and load it within EViD database files onto the USB activators. The image produced by NCBoE was taken sometime after July 20, 2017– after most artifacts corresponding to the November 8, 2016 election date had been overwritten through normal desktop use. In order to analyze a more complete set of artifacts contemporaneous to the election date, HIRT relied on the image taken by a private sector forensics firm hired by DCBoE

as that image was taken in mid-November 2016 – much closer to the November 8 election date. HIRT performed automated scans on this image using a collection of IOCs and signatures and performed a manual analysis of system configuration and common sources of artifacts. HIRT focused on artifacts that demonstrated unauthorized remote access and the presence of malicious software or scripts on the system.

HIRT was asked to identify the occurrence and nature of any connections allowing remote ability to manipulate or modify data. HIRT found artifacts indicating that screen sharing and file transferring occurred on November 8, 2016, but they did not find artifacts suggesting remote access (remote ability to manipulate systems or modify data) to the device occurring on or before that date. HIRT also identified the presence of the [REDACTED] remote support tool suite on the desktop computer. (During the timeframe under analysis, [REDACTED], a cloud-based service that enables users to access and control remote computers and other Internet-connected devices, was comprised of [REDACTED] and [REDACTED]) [REDACTED] is the component that allows remote control of the desktop. [REDACTED] allows screen sharing with remote viewers; however, it does not give remote users the ability to interact with the computer. The remote user can see everything on the desktop but is unable to issue commands. Considering this, HIRT determined that [REDACTED] was used once in September, twice in October, and once in November 2016. ([REDACTED] clears its logs after each use and HIRT was unable to recover more specific timestamps.) HIRT determined that this use did not give remote users the ability to send commands to the desktop computer. Also, HIRT determined that the [REDACTED] component was installed but never run.

On November 8, 2016, user [REDACTED] made an FTP connection to [REDACTED] and uploaded a file, but the content of the file was not preserved in a log, so HIRT could not analyze it. HIRT also found that users [REDACTED] and [REDACTED] were active on this desktop on November 8, 2016. User [REDACTED] accessed what appeared to be a personal Gmail account and clicked on a link to [REDACTED] which redirected to [REDACTED]. HIRT did not find artifacts indicating any files were downloaded from these website. These websites did not return any malicious results when looked up in [REDACTED] [REDACTED], nor did these URLs match any of the known bad IOCs that HIRT referenced. HIRT also found that the [REDACTED] user account was created on November 8, 2016.

HIRT identified security best practices that could be implemented on desktop computer systems, particularly the system handling election data, to harden the system and reduce the risk of compromise or exploitation.

RECOMMENDATIONS

The sections below provide HIRT's client-tailored and general recommendations based on this engagement.

Client-Tailored Recommendations

HIRT developed the following client-tailored recommendations—specific to DCBoE's network—from off-site and post-engagement findings and analysis. The implementation of these recommendations will help strengthen DCBoE's defensive cybersecurity posture.

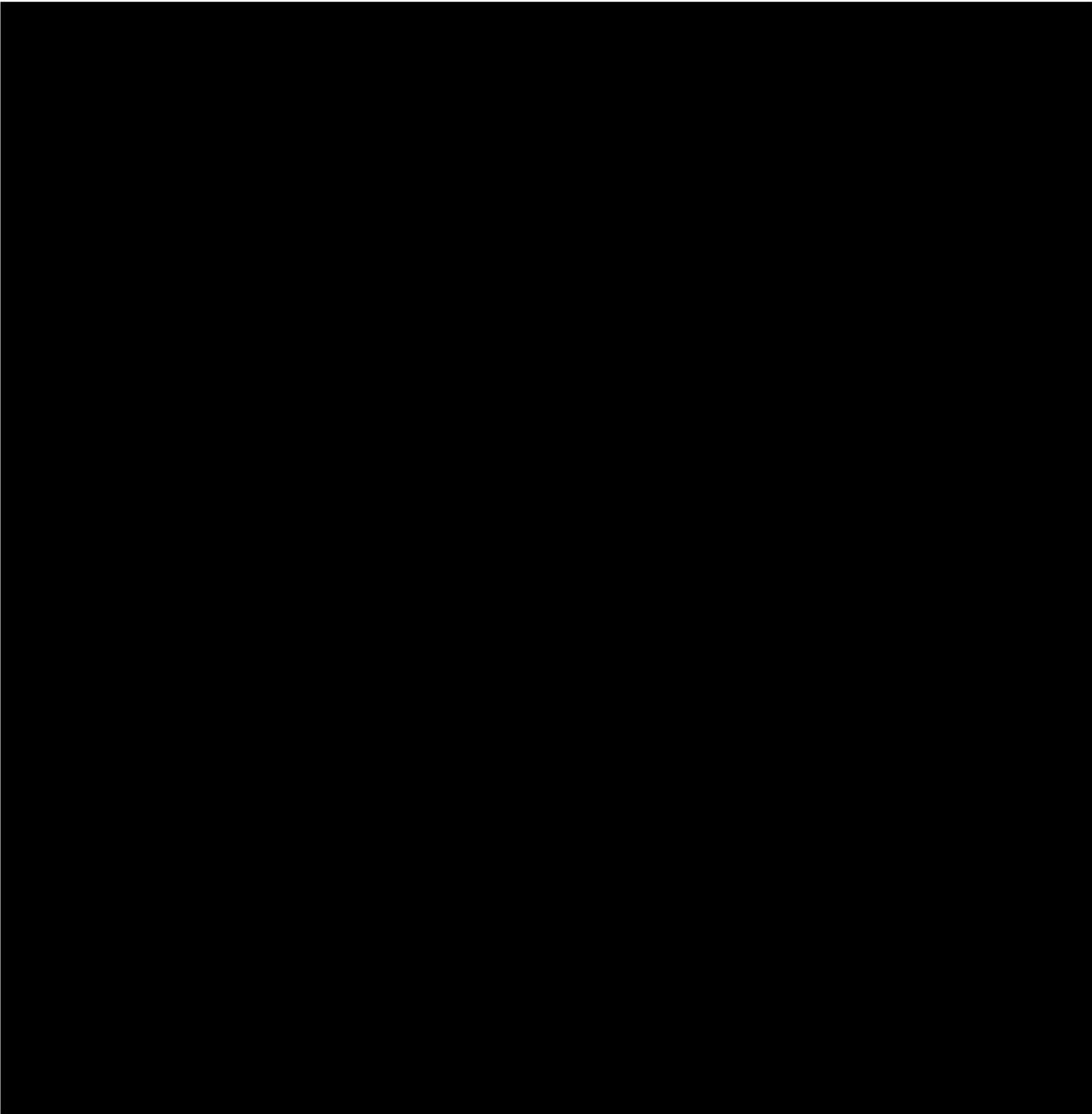
[REDACTED]

Note: These recommendations are not an exhaustive list of actions required to create a secure network environment. The recommendations do not constitute a complete assessment of the entire environment. HIRT recommends that DCBoE maintain continued vigilance when securing its networks and systems.

General Recommendations

Properly implemented defensive techniques and programs make it more difficult for a threat actor to gain access to a network and remain persistent yet undetected. When an effective defensive program is in place, attackers should encounter complex defensive barriers. Attacker activity

should also trigger detection and prevention mechanisms that enable organizations to contain and respond to the intrusion. There is no single or set of defensive techniques or programs that will completely avert all attacks. DCBoE should adopt and implement multiple defensive techniques and programs in a layered approach to provide a complex barrier to entry, increase the likelihood of detection, and decrease the likelihood of a successful attack. This layered mitigation approach is known as defense-in-depth. For additional, election specific, best practices, refer to CISA Security Tip ST19-002 "[Best Practices for Securing Election Systems](#)".



CONCLUSION

HIRT did not positively identify any threat actors or malware on the DCBoE systems provided for analysis. Additionally, HIRT did not identify remote access to the systems under analysis during the election timeframe. HIRT did identify several areas where defense-in-depth protections and system configurations could be improved to help DCBoE reduce risk of compromise in the future, which are documented in this report.