June 4, 2020

The Honorable Joseph V. Cuffari
Office of the Inspector General
Department of Homeland Security
245 Murray Lane SW
Washington, D.C., 20528-0305

Dear Inspector General Cuffari,

We write to you to urge you to initiate an investigation into the voting system vendor Voatz for potential misuse of Department of Homeland Security (DHS) branding in connection with its products that may violate 18 U.S.C. § 701, 18 U.S.C. § 1017, or DHS Management Directive 123-06 §§ 6(A)(3) and 6(A)(4).[1] In February 2020, Voatz distributed and published a report it created, representing it as a DHS report and branding the report with the DHS seal as well as the Cybersecurity and Infrastructure Security Agency (CISA) logo.

Voatz is a Boston-based startup company that is developing and marketing an internet-based voting system that enables voters to cast a ballot from an application loaded on their mobile devices.[2]

In September and October of 2019, at Voatz's request, the Hunt and Incident Response Team (HIRT) of DHS's Cybersecurity Infrastructure and Security Agency (CISA) conducted an assessment of Voatz's systems to determine if they contained any evidence or artifacts indicating Voatz had suffered an intrusion.[3] After its completion, the assessment was provided to Voatz only. As is CISA's practice, the assessment was not made public, nor was it classified.

In February of 2020, researchers at the Massachusetts Institute of Technology (MIT) were preparing to release a damning security review of Voatz's online voting application. The MIT researchers first alerted CISA to their findings. CISA in turn, facilitated a meeting between the researchers and Voatz to responsibly

[1] Free Speech for People is a non-profit, non-partisan public interest legal organization that works to renew our democracy and our United States Constitution for the people. As part of our mission, we are committed to promoting, through legal actions, secure, transparent, trustworthy, and accessible voting systems for all voters.
[2] *See generally* Voatz, https://www.voatz.com (last visited May 29, 2020).
[3] Voatz, Hunt Engagement Summary, https://voatz.com/Hunt-Engagement-Summary-Voatz.pdf (Feb. 14, 2020).

disclose the vulnerabilities that were uncovered. Voatz was made aware of the damaging findings, and that they would soon be reported in the New York Times.

In mid-February, with a media storm looming, Voatz delivered to the West Virginia Secretary of State's office, allegedly via a secure web portal, a purported summary of HIRT's findings.[4] Voatz itself drafted this summary. This version of Voatz's summary, provided February 11, 2020, prominently displays the DHS seal and CISA logo, as well as the Voatz logo.[5] It contains no disclaimer or mark alerting the reader that the document was not written by DHS or CISA.[6]

Once the MIT report was published by the New York Times, a media frenzy ensued. Voatz pushed back aggressively, publishing a response which called the research "flawed"[7] and holding a press call to criticize and disavow the researchers' findings. On the press call, Voatz's CEO Nimit Sawhney identified the report as a DHS security audit, telling reporters that "there are some audits happening for which information is publicly available. One of them was conducted by the DHS. That's [sic] report is available on our website. . . ."[8]

As one of the most vocal supporters of Voatz's system, the West Virginia Secretary of State's office fielded multiple calls from reporters regarding the MIT report. The Secretary of State shared the falsely labeled summary with several reporters and cited it to counter the damaging revelations in the MIT study.[9] Several media accounts described the summary as a declassified DHS report.[10]

Voatz publicly released an updated version of this report sometime after February 14, 2020, which removed the DHS seal and CISA logo, and added a disclaimer clarifying that Voatz created the summary.[11] Voatz's falsely labeled summary may constitute a violation of 18 U.S.C. § 701 (prohibiting use of government insignias except as provided by regulations),[12] 18 U.S.C. § 1017 (prohibiting false use of

---

[4] Attachment A, Email from Donald Kersey, General Counsel to West Virginia Secretary of State, about source of Voatz summary
[5] Attachment B, Initial Voatz Hunt Assessment Summary
[6] *Id.*
[7] https://blog.voatz.com/?p=1209
[8] https://blog.voatz.com/?p=1243
[9] AJ Vicens, *Security Researchers Find Flaws in Online Voting System Tested in Five States*, Mother Jones (Feb. 13, 2020), https://bit.ly/3dcuQjq
[10] The Mother Jones article continues to link to the original, falsely labeled, Voatz summary. *Id.* ("Warner's office also provided a copy of a declassified DHS assessment of the Voatz network.")
[11] Hunt Engagement Summary, *supra.*
[12] 18 U.S.C. § 701 (official badges, identification cards, other insignia).

government insignias),[13] or DHS MD 123-06 (prohibiting the use of the DHS seal in a manner that implies endorsement of commercial products or services).[14]

18 U.S.C. § 701 prohibits use of government seals except as allowed by regulations:

> Whoever manufactures, sells, or possesses any badge, identification card, or other insignia, of the design prescribed by the head of any department or agency of the United States for use by any officer or employee thereof, or any colorable imitation thereof, or photographs, prints, or in any other manner makes or executes any engraving, photograph, print, or impression in the likeness of any such badge, identification card, or other insignia, or any colorable imitation thereof, except as authorized under regulations made pursuant to law, shall be fined under this title or imprisoned not more than six months, or both.

The statute was "intended to protect the public against use of a recognizable assertion of authority with intent to deceive," and its application extends beyond badges and identification cards.[15]

18 U.S.C. § 1017 prohibits fraudulent use of a government seal on documents:

> Whoever fraudulently or wrongfully affixes or impresses the seal of any department or agency of the United States, to or upon any certificate, instrument, commission, document, or paper or with knowledge of its fraudulent character, with wrongful or fraudulent intent, uses, buys, procures, sells, or transfers to another any such certificate, instrument, commission, document, or paper, to which or upon which said seal has been so fraudulently affixed or impressed, shall be fined under this title or imprisoned not more than five years, or both.

---

[13] 18 U.S.C. § 1017 (government seals wrongfully used and instruments wrongfully sealed).
[14] DHS, *Use of the Department of Homeland Security Seal*, Management Directive 123-06 (2013), https://www.dhs.gov/sites/default/files/publications/mgmt/administrative-management/mgmt-dir_123-06-use-of-dept-homeland-security-seal_revision-00.pdf
[15] *United States v. Goeltz*, 513 F.2d 193, 197 (10th Cir. 1975).

Violations of this statute have been found in cases where defendants misappropriated government forms and branding to give their products the appearance of official documents for commercial gain.[16]

Management Directive 123-06 § 6(A)(4) prohibits use of the DHS seal without an express written agreement with the department.[17] DHS itself is barred from using the seal in a way that implies a product endorsement,[18] and this generally extends to outside organizations.[19] Requests by outside groups to use the seal, either alone or in a co-branding arrangement, must be submitted to the department in writing and must specify in detail the intended use.[20]

Voatz does not appear to have complied with these DHS standards in its use of the seal on the original summary. And although the currently public version of the summary no longer uses the DHS seal, Voatz may have also used DHS branding on other materials it may have provided to its customers.

It appears that Voatz wrote and distributed its purported summary to blunt the impact of the MIT findings and maintain the company's standing in the marketplace. Such a use of the seal does not appear to "benefit the Department" in the manner required by MD 123-06.[21]

Instead, Voatz may have taken advantage of CISA's work to imply that DHS had fully evaluated and endorsed its products, thus using DHS branding for its own benefit.

We urge you to review this information and ask you to initiate an inquiry to determine if Voatz violated DHS policy, 18 U.S.C. § 701, or 18 U.S.C. § 1017.

---

[16] *See, e.g.*, *United States v. Godfrey*, 787 F.3d 72, 74, 80 (1st Cir. 2015) (affirming conviction under 18 U.S.C. § 1017 for using modified Treasury Department forms to defraud customers); *United States v. Goodyke*, 639 F.3d 869, 872–873 (8th Cir. 2011) (affirming conviction under 18 U.S.C. § 1017 for creating and selling fraudulent State Department diplomatic immunity cards).

[17] Management Directive 123-06, *supra* note 14, § 6(A)(4) ("Use of the DHS seal . . . by any persons or organizations outside DHS only can be done with the prior written approval of the Secretary or his/her designee.").

[18] *Id.* § 6(A)(3) ("The DHS seal cannot be used in any manner that implies DHS endorsement of commercial products or services . . . .").

[19] *Id.* § 6(A)(4) ("Generally, agreements for outside use of the DHS seal only are approved when such use does not imply an endorsement of products or services by the Department or a component . . . .").

[20] *Ibid.*

[21] *Ibid.* ("All agreements must benefit the Department; tie to a key communication or operational objective; and demonstrate the ability for significant impact.").

Thank you very much for your consideration. Please do not hesitate to reach out to us if you have any questions or if we can be of any assistance.

Sincerely,

Susan Greenhalgh, Senior Advisor on Election Security
Ron Fein, Legal Director

Attachment A – Email from Donald Kersey, General Counsel to West Virginia Secretary of State, about source of Voatz summary

On Tue, Apr 21, 2020 at 5:58 PM Donald Kersey <DKersey@wvsos.com> wrote:

Hi Susan,

Thanks for the follow-up. My previous response does include all responsive documents in my possession for the time period requested. To your specific concerns, the report summary was obtained by our office through a secure web portal rather than email—hence the lack of communications. I conducted another search of all my email folders just now to confirm.

To explain, the vendor granted permissions to our office to access the specific document on a secure web portal, which is how we obtained the summary report and subsequently shared it with other reporters. We had a teleconference (perhaps two, but my notes are not clear) regarding the public release of the summary report, but I do not have any public records showing those communications.

To be fully transparent, I will forward you a FOIA response sent to one reporter regarding the summary report, which includes a fairly detailed narrative for background information. The inquiry was slightly different than yours, but should be helpful nonetheless.

If there are any other records or information you're seeking specifically, please feel free to write or call at your convenience. We are dedicated to full transparency, so I'll do all I can within the law to provide the facts and records requested.

All my best,
Deak

--

Donald M. Kersey, III
General Counsel
West Virginia Secretary of State's Office
304-558-6000 (Office)
304-368-6344 (Direct Dial)
304-558-0900 (Fax)

Attachment B – Initial Voatz Hunt Assessment Summary

Voatz

Hunt Engagement Summary
Voatz, Inc.

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 document summarizes HIRT's activities, findings, and analysis from an on-site engagement in response to a written Request for Technical Assistance (RTA) signed on May 13, 2019 and is based on the final report received by Voatz in January 2020.

On September 23, 2019, HIRT arrived at Voatz's corporate headquarters in Boston, MA, to conduct a proactive hunt operation. The hunt included the internal corporate network (including the corporate email servers), and Amazon Web Services (AWS) and Microsoft Azure cloud networks that support the mobile-based election infrastructure. HIRT deployed both network and host-based analysis tools across Voatz's networks to examine various artifacts as well as current activity, while searching for indicators of compromise (IOC). HIRT assessed 14 servers and 21 workstations and monitored network traffic from Voatz's corporate headquarters located in Boston, MA. The onsite engagement ended on September 27, 2019, and post-engagement analysis concluded on October 4, 2019. HIRT did not identify any threat actor activity within Voatz's network environment.

During the hunt, HIRT identified some issues that while unrelated to threat actor activity, could pose threats to Voatz's networks in the future and suggested some recommendations to further enhance the security posture.

CONCLUSION

During the one-week on-site engagement and subsequent remote analysis on the data collected, HIRT analysts did not detect threat actor behaviors or artifacts of past activities on the in-scope portions of the Voatz networks. HIRT identified some areas where defense-in-depth protections and configurations could be improved to help Voatz's IT security personnel defend their enterprise network. HIRT commends Voatz for their proactive measures in the use of canaries, bug bounties, Shodan alerts, and active internal scanning and red teaming.

Appendix

Deployment

On September 23, 2019, HIRT arrived on-site at Voatz's corporate headquarters in Boston, MA, to hunt for threat actor behavior within Voatz's internal corporate network and the cloud networks of the mobile election system. During the on-site engagement, HIRT worked with Voatz's cybersecurity team to collect and analyze data from the internal corporate network and cloud networks.

Tools Used

During the on-site engagement, HIRT used CISA-owned tools. Voatz personnel provided aggregated files and support upon request. HIRT used several tools during the engagement some of which included the following:

- HIRT leveraged its network security monitors to capture metadata of the network traffic traversing Voatz's aggregation network. Voatz configured its network appliances to collect netflow information specific to general network egress traffic and forwarded this information to the HIRT sensors.
- HIRT used the Snort IDS sensor to review signature-based alerts generated by data analyzed from the Voatz network.
- HIRT used several host-based collection scripts to collect host artifacts (e.g. ARP tables, DNS caches, registry information, autoruns, system info/logs, bash history, etc.) for analysis.
- HIRT used Splunk as the data aggregation/security information and event management (SIEM) tool. Data was ingested from the beforementioned tools to allow HIRT to hunt efficiently across all the data ingested.

Artifacts Collected

Over the course of the engagement, HIRT collected various host, network, and cloud artifacts.

Analytical Techniques

HIRT used a variety of techniques to analyze the data collected during the engagement, including those listed below:

- IOC Search – HIRT conducted a known bad indicator search of approximately 144,000 indicators, 8,000 derived from a group of cyber threat actor campaigns of interest. These campaigns all occurred within the past 18 months and targeted U.S. local government and election sector critical infrastructure assets, the respective asset owners, and their respective asset operators. This search was conducted on a wide scale and the indicators were compared against the host and network-based data HIRT collected.

- Frequency Analysis – HIRT leveraged large datasets to calculate normal behavioral patterns in both network and host behavior. HIRT used these predictive algorithms to identify activity that was inconsistent with the norm. Variables taken into consideration included timing, source location, destination location, port utilization, protocol adherence, file location, integrity via hash, file size, naming convention, and other attributes.
- Pattern and Behavioral Analysis – HIRT leveraged the data collected to identify repeating patterns, indicative of either automated mechanisms (e.g., malware, scripts), as well as human behavior consistent with advanced threat actor activity.
- Anomaly Detection – HIRT conducted a human analyst review—based on the team's knowledge of, and experience with, system administration—of various artifacts to isolate any errors. Analysts reviewed unique values for various datasets and researched surrounding data, where appropriate.
- Architecture Review – HIRT conducted a cursory review of the network architecture and host configuration standard. The team primarily conducted this review during interviews regarding specific events. As HIRT identified potential concerns about design, they reviewed related data to determine if further security risks were present. The purpose of the hunt was not to provide a comprehensive design analysis, and this report should not be considered a full architecture review.

FINDINGS AND RECOMMENDATIONS

The table below provides HIRT's technical findings, analysis and recommendations for this engagement.

FINDINGS	**RECOMMENDATIONS / ACTIONS TAKEN**
(1) Scripting Usage Is Unmonitored HIRT observed that Voatz did not have an active plan in place to monitor or validate the scripts that ran on the network. While none of the scripts HIRT scrutinized were indicative of an active threat inside Voatz's network, unidentified scripts are common practice of a threat actor's tactics, techniques, and procedures (TTPs).	(1) Review Use of PowerShell/Bash and Enable PowerShell Logging HIRT recommends that Voatz routinely reviews the use of scripts within the network and standardizes locations from which scripts may be executed. *Action Taken*: *Voatz has upgraded to PowerShell v5 on Windows systems and enabled ScriptBlock logging. Voatz routinely reviews Bash history on the Mac and Linux computers to look for malicious command and/or configuration changes that can weaken Voatz's security posture.*
(2) Unmanaged Local Account Objects HIRT observed that local accounts did not have a consistent naming standard nor were they managed in an effective way.	(2) Routinely Review Local Account Objects HIRT did not notice the use of an account naming standard at the Voatz site. Despite the nonconformity, no accounts appeared to be engaged in malicious behavior. While there is no inherent risk in the account name per se, a naming standard allows for easier anomaly detection as well as provides greater insight into Voatz's system configuration rational for third-party auditors or incident responders. *Action Taken*: *Voatz has established a naming standard, formalized a process for ensuring that the account lists are accurate and routinely performs security risk assessments of the account environment for full discovery of security risks, which include stale (i.e., active but unused) objects or objects that do not conform to the standard.*

(3) Unsigned Applications Installed on Workstations HIRT identified unsigned applications on workstations, which are applications that cannot be provably authenticated as having originated from a trusted developer. Many unsigned applications are legitimate and do not pose a threat to the corporate network.	(3) Remove or Document Programs Without Valid Signatures HIRT discovered several executables within the Voatz network that did not have valid signatures. An executable without a valid signature is not by itself an indication of malware. However, threat actors can use unsigned or invalid signatures to further their actions within a network. HIRT recommends that Voatz routinely collects, documents, and reviews improperly signed executables for valid business requirements on both Mac and Windows computers to reduce the risk related to this issue. *Action Taken*: *The unsigned executables (all being used for a valid business purpose) were installed on Windows machines and not on any of the designated developer machines which run Mac OS and have some additional controls in place. Voatz has established an internal review process to reduce the risks related to this issue across all workstations being used by the team.*
(4) Centralized Logging Not Established HIRT identified that logging was not centralized across Voatz's enterprise. The ability to collect, consolidate, and save logs is especially important for some of the cloud assets because of 1) the inevitably that servers will be deprovisioned, and 2) the probability that without the implementation of a log preservation scheme, Voatz will not be able to review the logs in the future to look for IOCs based on new information.	(4) Establish Centralized Logging HIRT recommends that Voatz establish centralized logging in the form of a SIEM server. Aggregation and real-time searchability of log data is important to be able to determine if a compromise has occurred. Logs can be tampered with at individual endpoints and centralized logging adds a layer of integrity to mitigate that risk. *Action Taken*: *Voatz has started the process of establishing centralized logging (based on graylog) and completed 50% of this setup as of 1st February 2020.*
(5) Cloud Findings HIRT observed some configurations in the cloud environment that may unintentionally lead to a reduced security posture. AWS Observations HIRT leveraged the AWS Management Console to conduct a review of cloud computing assets, privileged identities, and all available logs. At the time of analysis, HIRT did not find evidence of malicious activity or persistence. However, HIRT did observe the following: • Currently Voatz is not synching identities from on-premises and is administrating the environment from cloud-only accounts. • Logs indicate that there are only two accounts accessing the environment and all admin functions are accomplished using the root AWS account. • The customer license provided access to 90 days of CloudTrail event logs but not Virtual Private Cloud (VPC) flow logs. • There are eight virtual machines (VM) used for production and the testing that is associated with one of three security groups. HIRT conducted an open source search of Voatz's public-facing IPv4 addresses using shodan.io which indicated that three of the instances have known vulnerabilities. Voatz confirmed that these devices are honeypots used for testing purposes. Azure Observations HIRT leveraged the Azure portal to conduct a review of cloud computing assets and privileged identities. At the time of analysis, HIRT did not find evidence of malicious activity or persistence. However, HIRT did observe the following: • There are 14 VMs located in one resource group. Consolidation of virtual resources makes for ease of administration. • Voatz has only one subscription that provides ease of administration and control. Having a single subscription allows for ease of tracking consumption charges directly	(5) Obtain Licenses to Improve Cloud Account Management and Monitoring HIRT recommends that Voatz procures enhanced licenses to enable the retention of Azure logs beyond seven days, enable AWS CloudWatch VPC flow log storage and monitoring, or develop a solution to store the logs on a third-party log aggregator. In addition, HIRT recommends that Voatz reduces the assigned permissions for day-to-day cloud account administration *Action Taken*: *Voatz has initiated the process of acquiring enhanced corporate licenses for improved monitoring.*

related to virtual resources of the organization. • Voatz is currently not synching identities from the on-premises system and is administrating the environment from cloud-only accounts. Utilizing cloud only accounts for administration ensure that if an on-premises identity is compromised, cloud compromise is not possible. This administration model separates administrative accounts enhancing security by limiting the opportunity of adversary access if an account is compromised. • There is currently only one member of the Global Admins group, which reduces the probability or risk of compromise and persistence. • Due to current license restrictions, the monitoring of "Sign-ins" is not allowed and only the last seven days of audit logs, which only represent the most recent cloud account usage activity, are available for review. Consequently, Voatz is unable to review older audit logs.	

Last Updated: February 11, 2020