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