ENGAGEMENT REPORT

INC00001021672 NUMBER

November 2, 2018 DATE

Maryland State Board of Elections

CONTENTS

HOW TO USE THIS REPORT

The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) produced this report for the Maryland State Board of Elections (MDSBE) in support of hunt operations conducted at their Annapolis, MD, location and at the offices of ByteGrid, a managed service provider (MSP) for MDSBE.

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

NCCIC

EXECUTIVE SUMMARY

The NCCIC 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 identify evidence of current or previous targeted malicious activity.

This report summarizes activities taken by HIRT during an on-site engagement in response to a written Request for Technical Assistance (RTA) from the MDSBE State Administrator, signed on July 17, 2018.

Following the submission of the MDSBE RTA, HIRT negotiated a separate RTA with ByteGrid, dated August 10, 2018, and deployed a team to conduct a proactive hunt on MDSBE's corporate network and election infrastructure network enclave (hereafter known as "the Enclave")—which is hosted and maintained by ByteGrid, operating as a MSP. HIRT coordinated with MDSBE and ByteGrid to perform on-site engagement activities, at the Annapolis based offices of both entities, from August 20, 2018, to August 31, 2018. MDSBE had not identified any known indicators of compromise (IOCs) or suspicious activity in their network environment at the time of the RTA. However, because MDSBE hosts the state's election infrastructure, their networks are a high-value target to cyber threat actors. It is best practice to periodically perform proactive hunts on high-value targets.

During the engagement, HIRT did not identify any indications that a compromise had occurred on the MDSBE corporate network or within the Enclave. This report details the findings and analysis from the engagement and provides tailored and general recommendations for cybersecurity improvements.

HUNT

Deployment

On August 20, 2018, HIRT arrived onsite at the ByteGrid office to hunt for threat actor behavior on the corporate network of ByteGrid and the Enclave. During the on-site engagement, HIRT worked with the MDSBE information technology (IT) personnel to a collect and analyze data from the MDSBE corporate network and worked with ByteGrid IT personnel to collect and analyze data from the Enclave network.

On August 20, 2018, HIRT deployed its internal Technical Engagement Network (TEN) at the ByteGrid office, to facilitate the analysis of host and network sensor data from the ByteGrid network and the Encalve.

On August 23, 2018, HIRT deployed a network sensor to the MDSBE office, in preparation for HIRT's transition to that location.

On August 27, 2018, HIRT deployed its TEN at the MDSBE office and collected host data and reviewed the collected network data. HIRT's tools scanned 92 endpoints for relevant IOCs using rule-sets associated with election infrastructure.

Engagement Scope

HIRT deployed to the MDSBE and ByteGrid corporate networks and the Enclave systems. In consultation with MDSBE and ByteGrid IT personnel, HIRT designated the Enclave as Cyber Key Terrain (CKT). CKT systems represent systems that serve a mission essential purpose to an organization and any cessation in their operations would cause an immediate negative impact. HIRT provides a more detailed analysis of any activity identified as unusual or unexpected on CKT-designated systems. Over the course of the on-site engagement at the MDSBE and ByteGrid corporate offices, HIRT analyzed the following systems and network events:

- 92 systems analyzed
  - 31 Windows servers
  - 61 Windows hosts/workstations
- 255,322,300 network events

HIRT placed one network sensor at the MDSBE office and two network sensors at the ByteGrid office to monitor internal and external traffic on the MDSBE, Enclave, and ByteGrid networks. In addition, HIRT—in conjunction with MDSBE and ByteGrid IT personnel—deployed host-based agents on MDSBE and ByteGrid network systems and utilized scripts to collect triage data from the CKT systems within the Enclave.

Tools Utilized

HIRT used the following DHS-owned tools during the engagement:

- **Splunk.** HIRT used Splunk, a security information and event management (SIEM) platform, to analyze network metadata and the results from HIRT ran collection scripts on individual endpoints and uploaded the collected data manually into Splunk. Splunk coalesced the raw metadata from the network sensors, logs, and individually collected data.
- **FireEye Endpoint Security (HX).** HIRT used FireEye HX to collect and analyze specific configuration datasets residing on each host. HIRT deployed HX host-based agents to 100 percent of user workstations within the MDSBE and ByteGrid networks, as identified by MDSBE and ByteGrid IT personnel.
- **Bro Intrusion Detection System (IDS) sensors.** HIRT leveraged Bro IDS sensors to capture metadata collected from MDSBE and ByteGrid network span ports. MDSBE and ByteGrid configured span ports on the interior of their firewall to collect netflow information specific to the MDSBE and ByteGrid network and metadata from general network egress traffic, and forward this information to HIRT's Bro sensors.

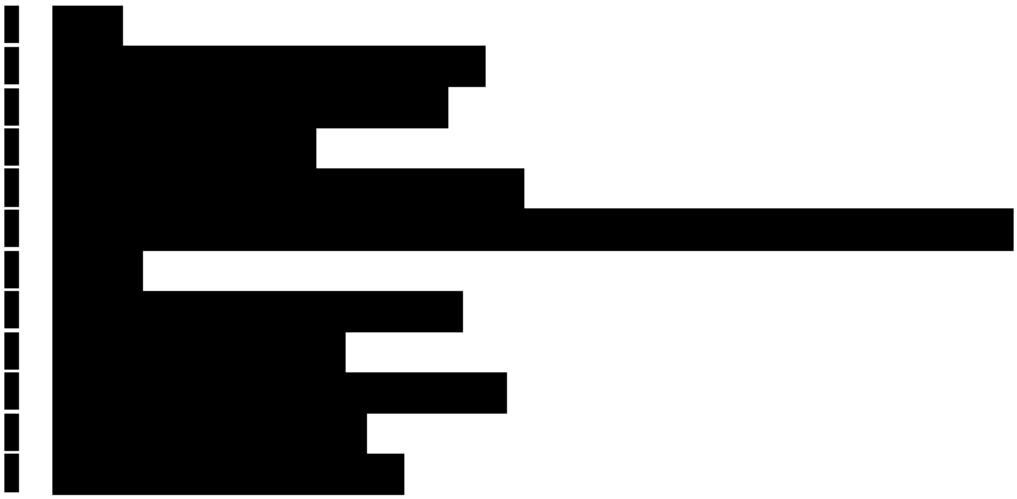
Data Collected

Host-Based Artifacts

HIRT worked with MDSBE and ByteGrid IT personnel on-site to deploy 61 host-based agents to collect and triage data from user workstations and used collection scripts to gather triage data from 30 CKT systems, all hosted in the Enclave. HIRT collected the following operating system (OS) artifacts:[1]

Network-Based Artifacts

Over the course of the engagement, HIRT collected network-based artifacts. The following list represents the primary artifacts (collected from traffic related to the following protocols and services during the hunt:



[1] HIRT defines an artifact as any portion of the data collected that is relevant to the hunt (i.e., processes, file activity, network statistic data).

[redacted]

Network Sensor Deployment and Analysis

HIRT worked with MDSBE and ByteGrid personnel to deploy network sensors to monitor network traffic and compile non-content metadata from the traffic traversing the MDSBE and ByteGrid networks. This data provided HIRT with insight into internal and external MDSBE and ByteGrid network traffic events. HIRT's collection of network traffic metadata facilitated the analysis and identification of the following types of activity across the MDSBE and ByteGrid networks:

- Hosts communicating with known malicious domains,
- Hosts communicating with known malicious IP addresses,
- Lateral movement within the network,
- Unauthorized remote access,
- Suspicious data transfers,
- Communication with Tor network nodes,
- Beaconing activity,
- Known malicious traffic patterns, and
- Statistical anomalies.

Hunt Methodology

HIRT designed and employed methodologies to detect malicious activity, including advanced persistent threat (APT) actor tactics, techniques, and procedures (TTPs) and non-advanced threats (e.g., commodity malware). The methodologies HIRT used for this hunt have been categorized into the following three groups:

- IOC detection,
- Behavioral analysis, and
- Statistical analysis.

Indicators of Compromise

HIRT uses IOC detection to quickly identify known threat actors and as a springboard for a deep-dive analysis. While onsite at MDSBE and ByteGrid, HIRT used several IOC sets to detect known malicious activities, including those related to

- Russian state-sponsored malicious cyber activity (known as GRIZZLY STEPPE), including activity associated with APT groups APT28 and APT29;[2]
- North Korean state-sponsored malicious cyber activity (known as HIDDEN COBRA);[3] and

[2] NCCIC, *Joint Analysis Report JAR-16-20296A: GRIZZLY STEPPE – Russian Malicious Cyber Activity*, December 29, 2016, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf. For additional information and IOCs related to GRIZZLY STEPPE, see: https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity.

[3] For additional information and IOCs related to HIDDEN COBRA, see: https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity.

- Russian government malicious cyber activity targeting U.S. critical infrastructure sectors and subsectors, including Elections Infrastructure and Energy.[4]

In addition to leveraging IOCs from known APT actors, HIRT searched for general IOCs to identify a wider range of activity on MDSBE's and ByteGrid's networks. HIRT designed these IOC sets to detect general threats and malicious behavior used by a variety of threat actors.

Behavioral Analysis

HIRT searched for patterns of activity that resembled common threat actor TTPs, including

- Unusual or unauthorized remote access (e.g., via RDP, PsExec, PuTTY);
- Processes with connections external to the organization;
- Processes with odd or unusual commands or launch strings;
- Execution or other file activity from odd or unusual locations (e.g., temp, AppData, user space);
- Persistence mechanisms (e.g., survival across reboots); and
- CKT analysis (e.g., unusual or unexpected activity to and from the server or operational technology network environments).

Statistical Analysis

HIRT performed analysis on OS artifacts to determine statistical outliers, which can be an effective way to identify anomalies related to malicious activity. Examples of artifacts on which HIRT performed statistical analysis include

- Artifacts appearing on only a few hosts (stacked by host count),
- Artifacts appearing in atypical or unusual locations (stacked by path),
- Network artifacts by host and by destination address (stacked by host and by destination IP), and
- Artifacts appearing only a few times by name (e.g., scheduled tasks, services) (stacked by name).[5]

HIRT reviewed the collected output and—upon the discovery of a file or artifact of interest—triaged it for additional information. If further questions regarding a file's or an artifact's legitimacy surfaced, HIRT worked with MDSBE or ByteGrid personnel to evaluate the findings.

Technical Findings: IOCs

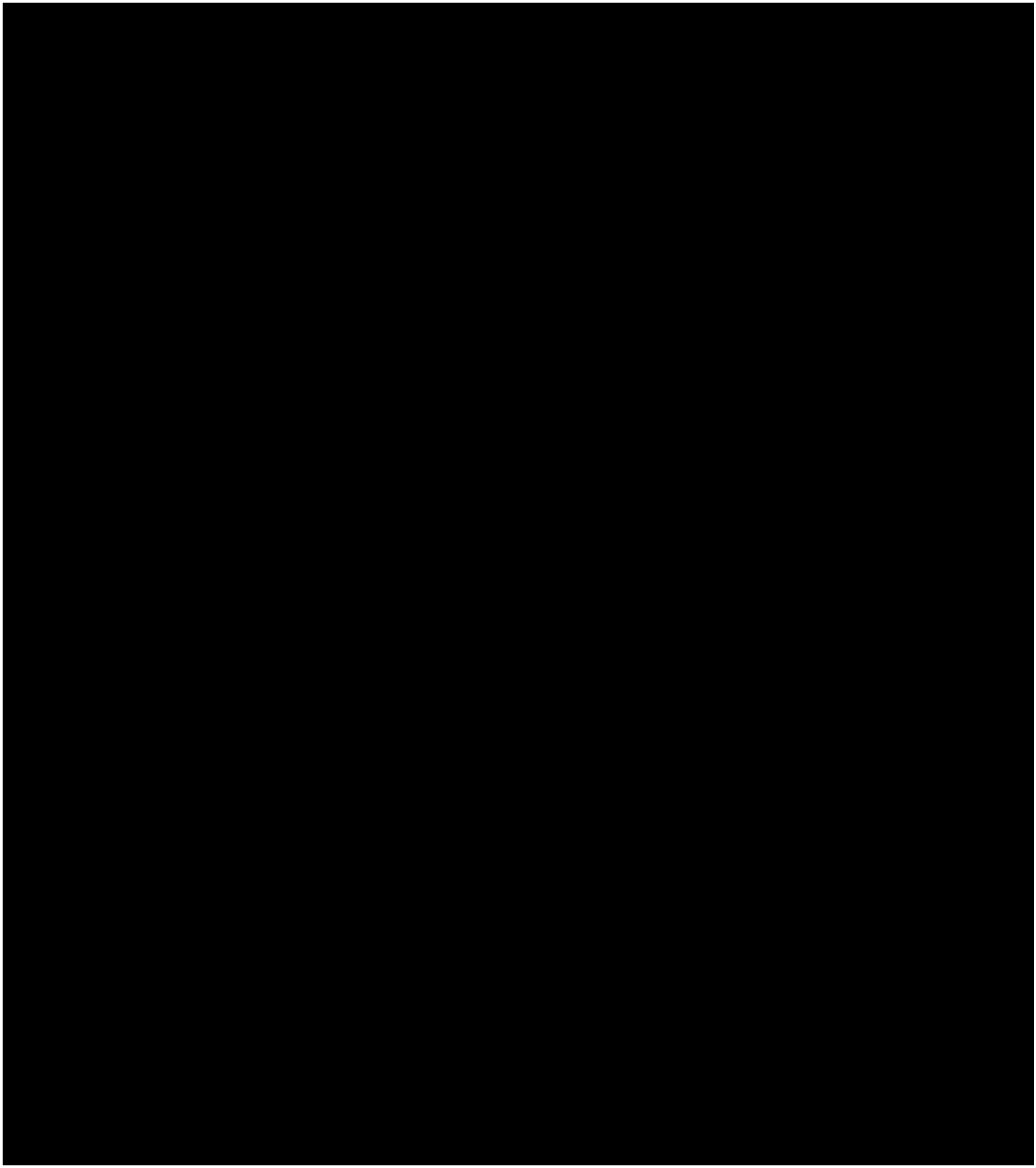
None of the IOCs or IOC sets HIRT used during the hunt (described in the Hunt Methodology section) yielded true positive results (i.e., results of an actual compromise).

[4] NCCIC, *TA18-074A: Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, March 16, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.
[5] This list is not exhaustive; it contains examples of artifacts and is meant to provide insight into the statistical analysis methodologies HIRT used.

HIRT reviewed and triaged a number of IOC "hits" (e.g., RDP, binary execution). However, upon review of the context (source and destination) of the tool usage, HIRT determined that none of the occurrences appeared to be malicious and that all the hits were false positives.

FINDINGS AND ANALYSIS

[redacted]



[redacted]

RECOMMENDATIONS

Client-Tailored Recommendations

[redacted]

[redacted]

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 prevent all attacks. MDSBE and ByteGrid should adopt and implement multiple defensive techniques and programs in a layered approach to provide a complex barrier to entry,

[redacted]

increase the likelihood of detection, and decrease the likelihood of a successful attack. This layered mitigation approach is known as defense-in-depth.

Whitelisting

- Enable application directory whitelisting through Microsoft Software Restriction Policy or AppLocker.
- Use directory whitelisting rather than attempting to list every possible permutation of applications in a network environment. Safe defaults allow applications to run from `PROGRAMFILES`, `PROGRAMFILES(X86)`, and `SYSTEM32`. Disallow all other locations unless an exception is granted.
- Prevent the execution of unauthorized software by using application whitelisting as part of the OS installation and security hardening process.

Account Control

- Decrease a threat actor's ability to access key network resources by implementing the principle of least privilege.
- Limit the ability of a local administrator account to log in from a local interactive session (e.g., "Deny access to this computer from the network") and prevent access via an RDP session.
- Remove unnecessary accounts and groups, and restrict root access.
- Control and limit local administration.
- Make use of the Protected Users AD group in Windows domains to further secure privileged user accounts against pass-the-hash attacks.

Workstation Management

- Create and deploy a secure system baseline image to all workstations.
- Mitigate potential exploitation by threat actors by following a normal patching cycle for all OSs, applications, software, and all third-party software.
- Apply asset and patch management processes.
- Reduce the number of cached credentials to one (if a laptop) or zero (if a desktop or fixed asset).

Host-Based Intrusion Detection

- Configure and monitor system logs through a host-based IDS and firewall.
- Deploy an anti-malware solution to prevent spyware, adware, and malware as part of the OS security baseline.
- Monitor antivirus scan results on a regular basis.

Server Management

- Create a secure system baseline image and deploy it to all servers.
- Upgrade or decommission end-of-life non-Windows servers.
- Upgrade or decommission servers running Windows Server 2003 or older versions.

- Implement asset and patch management processes.
- Audit for and disable unnecessary services.

Server Configuration and Logging

- Establish remote server logging and retention.
- Reduce the number of cached credentials to zero.
- Configure and monitor system logs via a centralized SIEM appliance.
- Add an explicit DENY for `%USERPROFILE%`.
- Restrict egress web traffic from servers.
- In Windows network environments, use the Restricted Admin mode or remote credential guard to further secure remote desktop sessions against pass-the-hash attacks.
- Restrict anonymous shares.
- Limit remote access by only using jump servers for such access.

Network Security

- Implement IDS.
  - Apply continuous monitoring.
  - Send alerts to a SIEM tool.
  - Monitor internal activity (this tool may use the same tap points as the netflow generation tools).
- Employ netflow capture.
  - Set a minimum retention period of 180 days.
  - Capture netflow on all ingress and egress points of network segments, not just at the Managed Trusted IP Services or Trusted Internet Connections locations.
- Execute network packet capture (PCAP).
  - Retain PCAP data for a minimum of 24 hours.
  - Capture traffic on all network ingress and egress points.
- Use VPNs.
  - Maintain site-to-site VPNs with customers.
  - Authenticate users utilizing site-to-site VPNs through an adaptive security appliance (ASA).
  - Use authentication, authorization, and accounting for controlling network access.
  - Require personal identity verification (PIV) authentication to an HTTPS page on the ASA to control access. Authentication should also require explicit rostering of permitted PIV distinguished names to enhance the security posture on both networks participating in the site-to-site VPN.
  - Establish appropriate secure tunneling protocol and encryption.
- Strengthen router configuration (e.g., avoid enabling remote management over the internet and using default IP ranges, automatically log out after configuring routers, use encryption.).
- Turn off wireless protected setup, enforce the use of strong passwords, and keep router firmware up-to-date.

- Improve firewall security (e.g., enable automatic updates, revise firewall rules as appropriate, implement whitelists, establish packet filtering, enforce the use of strong passwords, encrypt networks).
- Conduct regular vulnerability scans of the internal and external networks and hosted content to identify and mitigate vulnerabilities.
- Define areas within the network that should be segmented to increase the visibility of lateral movement by a threat and increase the defense-in-depth posture.
- Develop a process to block traffic to IP addresses and domain names that have been identified as being used to aid previous attacks.

Network Infrastructure Recommendations

- Remove unnecessary OS files from the Internetwork Operating System (IOS) and ASA devices. This will limit the possible targets of persistence (i.e., files to embed malicious code) if the device is compromised and will align with National Security Agency Network Device Integrity best practices.
- Remove vulnerable IOS/ASA OS files (i.e., older iterations) from the device's boot variable (i.e., `show boot` or `show bootvar`).
- Update to the latest available OS for Cisco IOS and Cisco ASA devices.
- On ASA devices, update the Cisco Adaptive Security Device Manager to version 7.6.2 or later to reduce vulnerabilities and maintain consistent software versions on firewalls throughout the organization.
- On ASA devices with SSL VPN enabled, routinely verify customized web objects against the organization's known good files for such VPNs, to ensure the ASA devices remain free of unauthorized modification.

Host Recommendations

- Implement policies to block workstation-to-workstation RDP connections through a Group Policy Object on Windows, or by a similar mechanism.
- Store system logs of mission critical systems for at least one year within a SIEM tool.
- Review the configuration of application logs to verify that recorded fields will contribute to an incident response investigation.

User Management

- Immediately set the password policy to require complex passwords for all users (e.g., a minimum of 16 characters) and enforce this new requirement as user's passwords expire.
- Reduce the number of Domain and Enterprise Administrator accounts.
- Create non-privileged accounts for privileged users and ensure they use the non-privileged accounts for all non-privileged access (e.g., web browsing, email access).
- If possible, use technical methods to detect or prevent browsing by privileged accounts (authentication to web proxies would enable blocking of Domain Administrators).

- Use two-factor authentication (e.g., security tokens for remote access and access to any sensitive data repositories).
- If soft tokens are used, they should not exist on the same device that is requesting remote access (e.g., a laptop) and instead should be on a telephone or other out-of-band device.
- Create privileged role tracking.
- Create a change control process for all privilege escalations and role changes on user accounts.
- Enable alerts on privilege escalations and role changes.
- Log privileged user changes in the network environment and create an alert for unusual events.
- Establish least privilege controls.
- Implement a security-awareness training program.

Best Practices

- Implement a vulnerability assessment and remediation program.
- Encrypt all sensitive data in transit and at rest.
- Create an insider threat program.
- Assign additional personnel to review logging and alerting data.
- Complete independent security (not compliance) audits.
- Create an information sharing program.
- Complete and maintain network and system documentation to help with timely incident responses, including
    - Network diagrams,
    - Asset owners list,
    - Asset inventory, and
    - An up-to-date incident response plan.

CONCLUSION

During the course of the on-site engagement, HIRT did not positively identify any threat actor activity on the MDSBE, ByteGrid, or Enclave networks. [redacted] HIRT documented a number of recommendations in this report, which will help to strengthen the overall resilience of these networks.