We collect data in an on-site assessment and combine it with national threat that adversaries could potentially exploit to compromise security controls.

Risk and Vulnerability Assessment: Upon request, CISA can identify vulnerabilities.

MTIERR TACTICS AND TECHNIQUES

**Initial Access**
- Spearphishing Link
- Exploit Public-Facing Application
- Spearphishing Attachment

**Execution**
- PowerShell
- Command-Line Interface
- MShta
- Service Execution
- Windows Management Instrumentation
- Graphical User Interface
- Scripting
- User Execution
- Exploitation for Client Execution
- Execution through API

**Persistence**
- Valid Accounts
- New Service
- Create Account
- Windows Management Instrumentation Event Subscription
- Registry Run Keys/Startup Folder
- Launch Agent

**Privilege Escalation**
- Valid Accounts
- Exploitation for Privilege Escalation
- Access Token Manipulation
- Process Injection
- New Service
- Bypass User Account Control
- Sudo

**Credential Access**
- Credential Dumping
- LLNMR/NBT-NS Poisoning
- Credentials in Files
- Kerberoasting
- Brute Force
- Network Sniffing
- Input Capture
- Account Manipulation
- Exploitation of Credential Access
- Private Keys
- Forced Authentication
- Credentials in Registry
- Bash History

**Discovery**
- Account Discovery
- Network Service Scanning
- File & Directory Discovery
- Network Share Discovery
- Remote System Discovery
- Process Discovery
- Password Policy Discovery
- System Owner/User Discovery
- Permission Groups Discovery
- Service Discovery
- Security Software Discovery
- System Information Discovery
- System Network Configuration Discovery

**Defense Evasion**
- MShta
- Process Hollowing
- Valid Accounts
- Access Token Manipulation
- Process Injection
- Scripting
- Obfuscated Files or Information
- Bypass User Account Control
- Indicator Removal Tools
- Hidden Window
- File Deletion
- Masquerading
- DLL Side-Loading
- ProcessDuppleganging
- Disabling Security Tools

**Credentialed Access**
- Credential Dumping
- LLNMR/NBT-NS Poisoning
- Credentials in Files
- Kerberoasting
- Brute Force
- Network Sniffing
- Input Capture
- Account Manipulation
- Exploitation of Credential Access
- Private Keys
- Forced Authentication
- Credentials in Registry
- Bash History

**Collection**
- Screen Capture
- Data from Local System
- Data from Network Shared Drive
- Automated Collection
- Man in the Browser
- Input Capture
- Email Collection
- Data from Information Repositories
- Clipboard Data

**Command & Control**
- Commonly Used Port
- MShta
- Commonly Used Port
- MShta
- Commonly Used Port
- MShta
- Commonly Used Port
- MShta

**Lateral Movement**
- Pass the Hash
- Remote Desktop Protocol
- Windows Admin Shares
- Remote Services
- Exploitation of Remote Services
- Pass the Ticket
- Remote File Copy
- Distributed Component Object Model

**Exfiltration**
- Scheduled Transfer
- Exfiltration over Communication Channels
- Data Encrypted
- Data Compressed
- Automated Exfiltration

**Mitigations for Top Techniques**

*Top techniques and mitigations vary by sector and environment. Organizations should consider additional sector-specific and mitigation strategies based on their unique environment.*