October 2024

Welcome to our new CTI Threat Briefing! This monthly update is your go-to source for industry-specific threat intelligence tailored to Aspire's clientele. Each month, our briefing will dive into threat intelligence tailored to the specific industries within Aspire's customer base. From updates on threat actors to the latest malware trends, we'll dissect information to keep you informed.

Unless otherwise flagged all content is TLP:GREEN. If you are unfamiliar with the TLP protocol, please check this out: https://www.first.org/tlp/ . In short:

TLP:RED = Do not share with anyone
TLP:AMBER+STRICT = Limited to need to know within Aspire only.
TLP:AMBER = Limited to need to know
TLP:GREEN = Limited to sharing within your community. This includes clients and others within the security community, but it is not for publishing publicly.
TLP:CLEAR = shout it from the rooftops!

Aspire Emergency Flash Notices, Threat Intelligence Reports, and other Vulnerabilities TLP:CLEAR

Four CUPS Vulnerabilities Expose Linux and Unix Systems to Remote Code Execution (RCE)

In October 2024, four zero-day vulnerabilities in the Common UNIX Printing System (CUPS) exposed Linux and Unix-like systems to remote code execution (RCE) attacks, affecting distributions like ArchLinux, Debian, Fedora, and Red Hat Enterprise Linux. These vulnerabilities, tracked as CVE-2024-47176, CVE-2024-47076, CVE-2024-47175, and CVE-2024-47177, allow remote, unauthenticated attackers to manipulate printer configurations, inject harmful data, and execute arbitrary commands via compromised CUPS components such as cups-browsed, libcupsfilters, libppd, and cups-filters. By chaining these flaws, attackers could replace or install printers with malicious configurations, triggering RCE upon job initiation.

***Why You Should Care**: Although exploitation has not been reported, a proof-of-concept (PoC) is available. Aspire to recommends immediate patching and applying workarounds like blocking UDP Port 631, restricting DNS-SD traffic, and disabling cups-browsed if unnecessary. See Aspire's Emergency Flash Notice for further details.*

Microsoft SharePoint Vulnerability

CVE-2024-38094 is a high-risk vulnerability (CVSS 7.8) in Microsoft SharePoint, which was patched in July 2024 but has recently been added to CISA's Known Exploited Vulnerabilities (KEV) catalog due to the increased likelihood of exploitation. This deserialization flaw allows attackers with Site Owner permissions to inject and execute arbitrary code, which could cause data breaches within affected SharePoint versions, including SharePoint Server Subscription Edition, SharePoint Server 2019, and SharePoint Enterprise Server 2016. While no active exploitation has been reported, the existence of a proof-of-concept (PoC) raises the likelihood of attacks.

Why You Should Care: This vulnerability allows attackers with Site Owner permissions to execute arbitrary code within SharePoint, potentially leading to data breaches, unauthorized data access, and disruption of business operations. Exploiting CVE-2024-38094 could allow attackers to inject malicious code, exfiltrate sensitive information, or establish persistence within an organization's network. See Aspire's Emergency Flash Notice for further details.

Active Exploitation of Critical SolarWinds Help Desk Software Vulnerability

CVE-2024-28987 is a critical vulnerability (CVSS 9.1) in SolarWinds Web Help Desk (WHD) software, actively exploited to gain unauthorized access to sensitive information such as passwords and service account credentials. This hardcoded credential flaw allows remote attackers to access and modify internal help desk data without authentication. Disclosed in August 2024, the vulnerability affects WHD versions prior to 12.8.3 Hotfix 2. CISA has mandated immediate patching for federal agencies and advises all affected organizations to apply the latest SolarWinds update (Hotfix 3) by November 5, 2024, to prevent data breaches and potential lateral movement across systems.

***Why You Should Care**: Hardcoded credentials give attackers remote, unauthorized access to Web Help Desk systems. Attackers can view passwords and shared service account credentials. Unpatched WHD instances are at risk for lateral movement, allowing attackers to move deeper into networks. See Aspire's Emergency Flash Notice for further details.*

Cisco ASA and FTD Software Vulnerability Under Active Exploitation

Cisco has patched a vulnerability, CVE-2024-20481 (CVSS 5.8), in its Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software, addressing an active exploit targeting the Remote Access VPN (RAVPN) service. This vulnerability allows unauthenticated attackers to cause a denial-of-service (DoS) condition through resource exhaustion, potentially necessitating a device reload to restore full functionality. Actively exploited in brute-force attacks, CVE-2024-20481 affects all ASA and FTD versions. Cisco also patched several other critical vulnerabilities in these systems, including CVE-2024-20424 and CVE-2024-20329 (both CVSS 9.9), which allow command injection, and CVE-2024-20412 (CVSS 9.3) due to static credentials on certain Firepower models.

***Why You Should Care**: Exploiting CVE-2024-20481 can cause a denial-of-service (DoS) that may require a complete device reboot, interrupting essential VPN services. Leaving this vulnerability unpatched puts the network at risk for further attacks, potentially exposing sensitive data and resources. See Aspire's Emergency Flash Notice for further details.*

Zimbra Vulnerability Exploited in the Wild

The critical vulnerability CVE-2024-45519 in Zimbra Collaboration Suite, which allows attackers to deploy web shells and execute arbitrary commands on compromised systems, was exploited shortly after a proof-of-concept (PoC) was released. The flaw was traced to Zimbra's postjournal service, where improper input sanitization enabled command injection through specially crafted SMTP messages. Researchers at Proofpoint observed attackers sending spoofed Gmail emails with base64-encoded strings in the CC fields to exploit this flaw, allowing for remote code execution when the service was active and accessible within allowed network ranges.

***Why You Should Care**: The vulnerability allows for the installation of web shells, which can facilitate further attacks, data theft, and system manipulation. Zimbra released patches for affected versions, including 9.0.0 Patch 41, 10.0.9, 10.1.1, and 8.8.15 Patch 46, urging immediate updates to prevent further exploitation. Please see Aspire's Emergency Flash Notice for further details.*

Nvidia High Severity Graphics Driver Vulnerabilities

Nvidia issued critical security patches for eight high-severity vulnerabilities affecting its GPU drivers on Windows and Linux, as well as its vGPU software. These updates addressed issues in Windows drivers that could allow code execution, privilege escalation, denial-of-service, information leaks, and data tampering, with vulnerabilities tracked as CVE-2024-0117 through CVE-2024-0126. The patches also resolved two vulnerabilities in vGPU software, which could be exploited for privilege escalation and information disclosure.

***Why You Should Care**: These vulnerabilities allow for information disclosure and data tampering, threatening the integrity and confidentiality of an organization's data, which could result in data loss, unauthorized data manipulation, or leakage of sensitive information. Nvidia's updated drivers now include fixes across multiple product lines, and users were strongly advised to apply these patches to ensure system security. See Nvidia's advisory for further details.*

APT34 Exploits Windows Vulnerability – CVE-2024-30088

Iranian state-sponsored APT34 (OilRig) is exploiting the Windows vulnerability CVE-2024-30088 (CVSS 7) in recent attacks targeting government and critical infrastructure in the UAE and Gulf region. This vulnerability, involving a race condition in the Windows kernel, allows privilege escalation to SYSTEM level, granting attackers significant control over affected devices. The

campaign also leverages on-premise Microsoft Exchange servers and a new backdoor called StealHook to steal credentials.

***Why You Should Care**: Although Microsoft patched CVE-2024-30088 in June 2024 and released a proof-of-concept, CISA added it to their Known Exploited Vulnerabilities (KEV) catalog in October, urging organizations to patch Windows 10, 11, and Windows Server 2016, 2019, and 2022 immediately. See Aspire's Emergency Flash Notice for further details.*

BumbleBee Malware is Back

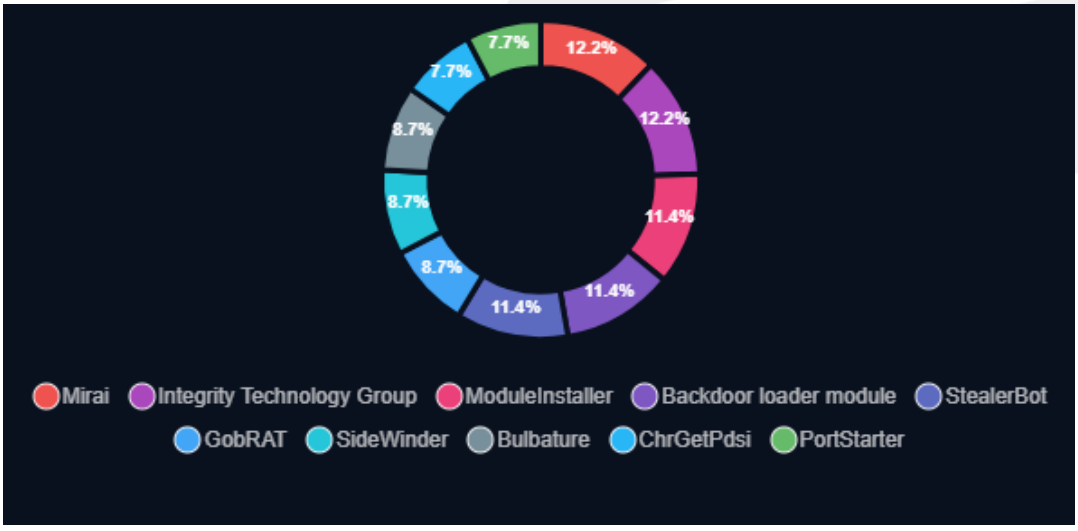
The Bumblebee malware loader, associated with Trickbot developers and previously disrupted in Operation Endgame, resurfaced in recent attacks, using phishing emails with malicious ZIP archives that impersonated NVIDIA drivers and Midjourney installers. Netskope researchers observed that executing these files triggered a sequence exploiting the MSI SelfReg table to load a DLL, ultimately delivering Bumblebee in memory without writing to disk.

This campaign marks the first infection chain using Bumblebee since the May 2024 takedown of other botnets like IcedID and Pikabot. Indicators of a comeback include the loader's deployment of unique identifiers like "NEW_BLACK" and "msi" in configuration, though the specific payloads remain unclear. Experts suggest heightened anomaly detection and enhanced memory analysis to identify in-memory DLL injection and recognize familiar tactics associated with the Trickbot group, advising security teams to share intelligence on new techniques to improve sector-wide defenses.

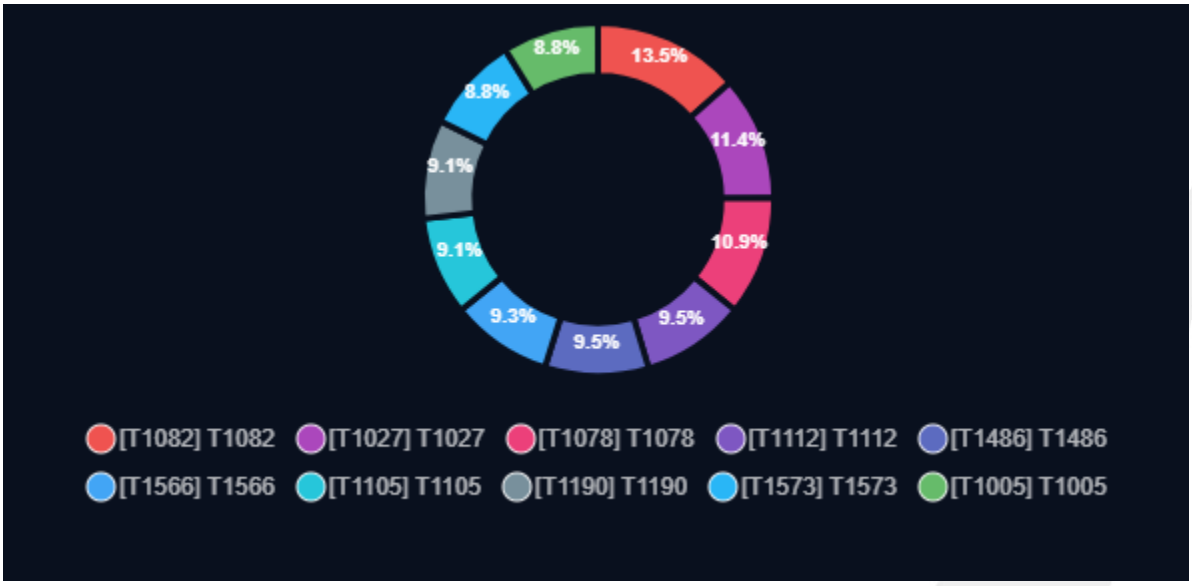
***Why You Should Care**: Bumblebee uses trusted names like NVIDIA to make phishing harder to detect and leverages DLL injection to evade defenses, especially in less monitored environments. Its quick return after disruption shows adaptability and potential for future, similar attacks.*

Intelligence for October 2024

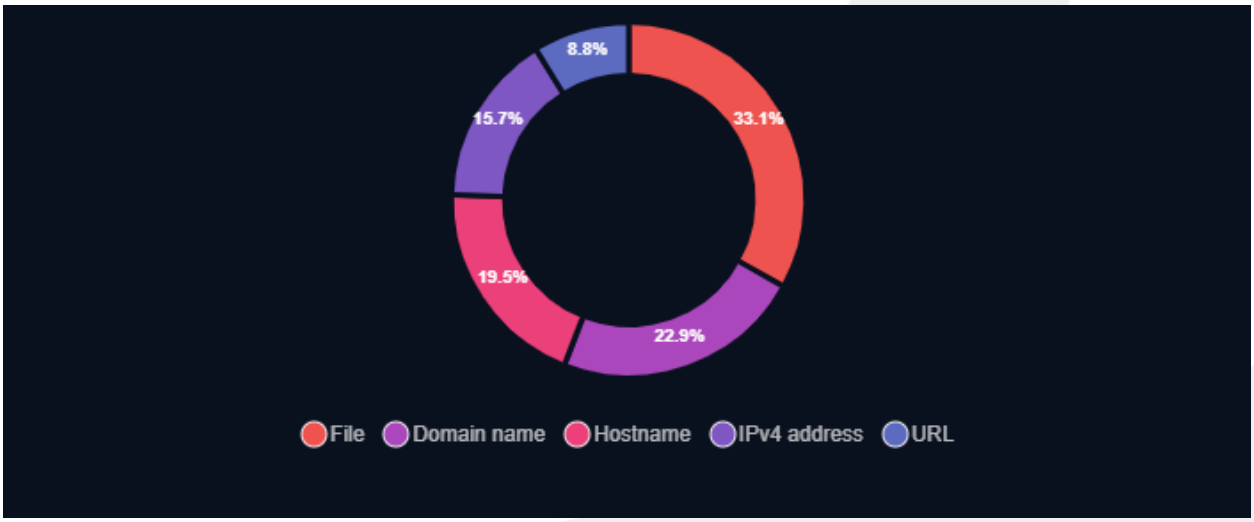
Top Threat Actors



Top ATT&CK Techniques



Top Indicators by Type



Industry Specific Threat Actors & Malware

Over the past month, most attacks and malware activity we have observed in our collection focused on the healthcare, human services, manufacturing, and government sectors. Here is the latest research for those sectors.

Top Threat Actors for October 2024

- **Healthcare** - Targeted by BlackSuit, Fog, Hunters, Lynx, Akira, ThreeAM, APT73, Abyss
- **Human Services** - Targeted by BlackSuit, Fog, Meow, Play, Lynx, Akira, Qilin, ThreeAM, APT73, Cactus, RAWORLD
- **Manufacturing** - Targeted by BlackSuit, Fog, Meow, Play, Hunters, Akira, Qilin, ThreeAM, APT73, Cactus, RAWORLD, Abyss
- **Government** - Targeted only by Akira

BlackSuit

- The BlackSuit ransomware gang claims to have hacked Kansas City Hospice, a non-profit providing end-of-life care in Kansas City. The organization detected unusual activity on its IT systems on October 19th and began an investigation with third-party experts. Despite some systems being affected, Kansas City Hospice continued its services and has since fully recovered. The BlackSuit gang, linked to the former Royal ransomware group, has targeted critical infrastructure and demanded ransoms up to $60 million.

Fog

- Fog and Akira ransomware groups are exploiting a critical SonicWall VPN vulnerability (CVE-2024-40766) to breach corporate networks. SonicWall patched the flaw in August 2024, but it has been actively exploited since. According to Arctic Wolf, the two ransomware operations have conducted over 30 intrusions through SonicWall VPNs, with Akira responsible for 75% of these attacks. The groups often collaborate, sharing infrastructure to facilitate breaches, which sometimes lead to rapid data encryption within hours. Many breached organizations failed to patch their systems or enable multi-factor authentication on SSL VPN accounts. Currently, over 168,000 SonicWall endpoints remain vulnerable, with potential exploitation by other ransomware groups, including Black Basta.

Play

- North Korean state-sponsored group Jumpy Pisces, tied to the Reconnaissance General Bureau, is now collaborating with Play ransomware (Fiddling Scorpius), marking a shift in its tactics. Initially accessing networks in May 2024 through a compromised account, Jumpy Pisces deployed malware, including Sliver and DTrack, to maintain persistence until September, when Play ransomware was launched. This partnership, the first recorded instance of Jumpy Pisces using third-party ransomware infrastructure, could indicate an emerging trend where North Korean actors expand into ransomware attacks beyond espionage. Security experts advise heightened vigilance, as this development could lead to more frequent and severe attacks globally.

Top Malware for October 2024

- **Government** - Targeted by Play, Qilin, ModuleInstaller, Backdoor Loader Module, IcedID, RTM Locker, Babuk
- **Healthcare** - Targeted by Play, Qilin, IcedID, Hiloti, RTM Locker, Prometei, Vasa Locker, Vulmap, Xray
- **Manufacturing** - Targeted by Play, Qilin, IcedID, Hiloti, Meow, Prometei

Qilin

- The Qilin ransomware operation has launched an updated variant called Qilin.B, which features stronger encryption, improved evasion techniques, and enhanced disruption of backup systems, according to a report from Halcyon. Originally emerging in 2022 as a rebranded version of Agenda ransomware, Qilin is now rewritten in Rust for faster, more persistent attacks. Known for targeting high-value industries like healthcare, Qilin offers affiliates up to 85% of ransoms. The new variant uses advanced obfuscation, making it harder to detect and analyze, and employs AES-256-CTR and RSA-4096 encryption to complicate decryption efforts without the private key.

Prometei

- Prometei is a modular botnet that primarily targets systems for cryptocurrency mining and credential theft, dating back to 2016. It has been responsible for over 10,000 global compromises, with significant activity in countries like Brazil, Indonesia, and Turkey. Utilizing tactics like brute force attacks and exploiting vulnerabilities (such as BlueKeep and Microsoft Exchange), Prometei can remotely control infected machines and deploy malware. It employs a domain generation algorithm for command-and-control operations and includes self-updating capabilities to evade detection, making it a persistent threat to compromised systems.

Security Incidents

Cisco Breach

This month, Cisco confirmed a security incident involving its DevHub environment, where a hacker known as IntelBroker allegedly accessed and offered to sell Cisco's files. The breach announcement surfaced on a prominent cybercrime forum, where the attacker claimed to possess various sensitive materials, such as source code, hardcoded credentials, encryption keys, API tokens, and confidential documents. Although IntelBroker presented screenshots to substantiate access to Cisco's systems, the company has stated that no internal systems were compromised, attributing the exposure to files mistakenly available on its publicly accessible DevHub, used for sharing resources with customers.

In response, Cisco disabled public access to DevHub and launched an investigation, assuring that thus far, no personal data or financial information appears compromised. While the investigation is ongoing, Cisco has engaged law enforcement and continues to

analyze the affected files, pledging to inform customers should any confidential information be confirmed as part of the exposed data. Cisco's approach emphasizes caution, ensuring that potentially impacted clients are notified, while they work to secure all public-facing environments.

Chinese Hackers Breach U.S. Telecom Providers

The FBI and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) have confirmed that Chinese hackers have infiltrated multiple commercial telecommunications service providers in the United States. In response to this breach, the agencies have alerted the affected companies and are actively informing other potential targets of the increased cyber threats. The announcement stated that the U.S. Government is investigating the unauthorized access to telecom infrastructure by actors associated with China. While details remain limited as the investigation continues, organizations suspecting they may have been compromised are encouraged to report to their local FBI office or CISA. Additionally, U.S. agencies are collaborating with industry partners to enhance cyber defenses across the telecommunications sector, particularly in light of the heightened cyber espionage activity.

Security Reports

Fortinet's FortiGuard Labs Report on the 2024 Presidential Election

Fortinet's FortiGuard Labs report highlights active darknet activity targeting the 2024 U.S. presidential election, revealing a range of threats to voters, campaigns, and government institutions. Darknet phishing kits tailored to impersonate presidential candidates are being sold to steal personal data from voters and donors, while over 1,000 new malicious election-related domains have been registered in 2024, many hosted on major platforms like AWS and Cloudflare to appear more legitimate. Additionally, billions of sensitive U.S. records, including Social Security numbers, personal details, and government credentials, are being sold on darknet forums, raising risks of misinformation, phishing, and fraud.

The report also underscores a 28% year-over-year rise in ransomware attacks against U.S. government agencies, with threat actors increasingly targeting government data to disrupt public services and damage election integrity. FortiGuard Labs suggests strengthening cybersecurity measures, such as enforcing multi-factor authentication, training employees, installing endpoint protection, and patching systems, as critical steps to protect against these threats during the election season.

***Why You Should Care**: Cybercriminals are actively selling phishing kits designed to target election-related entities, increasing the likelihood of widespread phishing attempts that could compromise sensitive information. With over 1,000 new domains created to mimic legitimate election resources, organizations and individuals are at greater risk of accidentally engaging with malicious sites.*

Notable TTPs TLP:AMBER

Discovery

- T1082 - Adversaries may seek detailed information about a target's operating system and hardware, including its version, patches, and architecture, to inform their attack strategies. They can use tools like Systeminfo on Windows or the systemsetup tool on macOS to gather this data, and commands like df -aH to check mounted disks. Additionally, they can access detailed system information from network devices using command-line interfaces (e.g., show version). In cloud environments like AWS, GCP, and Azure, attackers can exploit APIs to retrieve information about instances and virtual machines, including operating system details and status. This information aids in payload development and evasion tactics.
- Mitigations - Preventive controls are limited due to the nature of the attack, which exploits system features.
- Detections
    - Command Execution - Monitor commands and arguments for attempts to gather OS and hardware details. Check AAA logs on network devices for commands from unauthorized users.
    - OS API Execution - Monitor API calls that gather OS and hardware information. Watch for interactions with the Windows API and system management tools like WMI and PowerShell.
    - Process Creation - Monitor newly created processes that may seek OS and hardware details.

Defense Evasion

- T1027 - Adversaries may use encryption, encoding, or obfuscation to make executable files harder to detect or analyze, employing these tactics across various platforms and networks to evade security measures. Payloads can be compressed, archived, or encrypted to avoid detection, and may require user interaction, such as entering a password, to access them. Additionally, files can be split into benign-looking components that only reveal their malicious intent when reassembled. Command obfuscation techniques may also be used to conceal executed commands, utilizing environment variables and other platform-specific methods to bypass detection systems.
- Detections
    - Application Log - Monitor application logs for alerts from antivirus or security tools. Investigate initial detections as they may indicate deeper intrusions.
    - Command Execution - Watch executed commands for signs of obfuscation and unusual syntax. Look for specific command-line variations that suggest encoding.

- File Creation - Detection of obfuscated files is challenging; focus on detecting the activity that created or modified them. Monitor file metadata for contextual information, which may help identify malicious files.
- Module Load - Monitor module loads that are not in import tables for signs of obfuscated code. Use dynamic analysis to find indications of code obfuscation.
- Process Creation - Monitor newly executed processes for signs of content obfuscation or encryption.
- Script Execution - Check executed scripts for obfuscation indicators and suspicious syntax. Look for unreadable characters or encoded content within scripts.
- Windows Registry - Monitor for new registry keys that may store malicious commands or data.
- WMI Creation - Watch for the creation of WMI objects that might indicate the storage of malicious data.

Contributor(s)

Portia Cole

About Aspire

Aspire is a professional technology services firm specializing in the delivery of digital infrastructure solutions and managed services designed specifically to achieve our clients' business goals. We believe technology sits at the heart of every enterprise strategy. Our team takes time to understand your business initiatives and align technology solutions to drive the organization forward. Aspire's outcome-driven approach accelerates your journey by combining secure digital infrastructure, world-class design and implementation expertise, and managed services – all centered around transforming today's multi-cloud architectures into enablers of business value. Headquartered in Eatontown, New Jersey, Aspire is focused on serving the tri-state, mid-Atlantic, and New England regions with local operations in Mount Laurel, NJ; Conshohocken, PA; Albany and White Plains, NY; and Cambridge, MA.