9/30/2024

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

Important Reminder: Upcoming Mandatory MFA for Microsoft Azure (Entra ID)

On August 15, 2024, Microsoft announced that **starting October 15, 2024**, multi-factor authentication (MFA) will be mandatory for all Azure (Microsoft Entra ID) sign-ins, which may affect users relying on legacy Duo-protected integrations. Microsoft is transitioning from Custom Controls to a new External Authentication Methods (EAM) framework, requiring users to adjust their MFA configurations to comply with the updated requirements. While many Duo customers have implemented MFA through Microsoft Custom Controls, which lacks full integration recognition, Duo is one of the first third-party providers fully integrated into the EAM platform, allowing its MFA to meet Microsoft's policy. Users are advised to migrate to Duo solutions like Duo Single Sign-On for Microsoft 365 or Duo two-factor authentication for Entra ID EAM to ensure compliance.

***Why You Should Care**: For assistance, customers can contact duo-tech-comms@cisco.com or their Aspire Account Manager. For more information regarding this change, please see Aspire's General Communications article in the Customer Portal.*

Three Vulnerabilities in HPE Aruba Networking Access Points

This month, Hewlett Packard Enterprise (HPE) Aruba Networking issued patches to fix three critical command injection vulnerabilities (CVE-2024-42505, CVE-2024-42506, and CVE-2024-42507) in the Command Line Interface (CLI) of Aruba Access Points, which could allow unauthenticated attackers to execute remote code by sending crafted packets to the PAPI UDP port (8211). These vulnerabilities affect various AOS firmware versions, and while there is no active exploitation, Aspire recommends immediate patching. Workarounds include blocking UDP/8211 access for AOS-10 devices and enabling "cluster-security" for Instant AOS-8.x devices.

***Why You Should Care**: The vulnerabilities could allow unauthenticated attackers to remotely execute arbitrary code, giving them full control of affected devices. This could lead to data breaches, network disruptions, and unauthorized access to sensitive information. For more information and patch guidance, please see Aspire's Emergency Flash Notice.*

Cisco Patches IOS XE Software Web Vulnerability Amongst Others – CVE-2024-20437

Cisco has released patches for a high-severity vulnerability (CVE-2024-20437, CVSS 8.1) affecting the web-based management interface of IOS XE Software, which could allow remote attackers to exploit Cross-Site Request Forgery (CSRF) and execute unauthorized commands. The flaw stems from insufficient CSRF protection and can be triggered if an authenticated user clicks a malicious link. Additionally, Cisco has patched several other high-severity vulnerabilities in IOS XE Software, including denial-of-service (DoS) risks caused by crafted packets. There are no available workarounds for these vulnerabilities and Aspire strongly recommends applying the patches immediately to prevent potential exploitation.

***Why You Should Care**: The vulnerabilities could allow attackers to perform unauthorized actions such as command execution, denial-of-service (DoS) attacks, and even intercept network traffic. This could lead to network outages, data breaches, and loss of sensitive information. Given Cisco's widespread use in enterprise networks, routers, and critical infrastructure, the exploitation of these flaws could disrupt operations and compromise security. For more information on the vulnerabilities and for patch guidance, please see Aspire's Emergency Flash Notice.*

SQL Injection Vulnerability in Fortinet EMS Exploited – CVE-2023-48788

In March 2024, Fortinet disclosed and patched a critical SQL injection vulnerability (CVE-2023-48788, CVSS 9.8) in its FortiClient Endpoint Management Server (EMS). Recently, researchers have discovered active exploitation of this vulnerability by multiple threat actors, including APT-C-36, Maze, Medusa, and Blackbyte. The vulnerability affects EMS versions 7.2.0 to 7.2.2 and 7.0.1 to 7.0.10, allowing unauthorized code execution via specially crafted packets. Threat actors are using Remote Monitoring and Management (RMM) tools like Atera and

ScreenConnect to exploit unpatched systems. Aspire strongly advises organizations to apply Fortinet's patch immediately to prevent exploitation.

***Why You Should Care**: This Fortinet vulnerability could allow for unauthorized code execution, which could allow threat actors to take control of FortiClient Endpoint Management Servers. Once exploited, threat actors could access sensitive data, compromise systems, and potentially spread malware across the network. Leaving this vulnerability unpatched puts organizations at risk for a ransomware attack. For more information and for patch guidance, please see Aspire's Emergency Flash Notice.*

Vulnerability Found in Ivanti Cloud Services Appliance (CSA) – CVE-2024-8963

On September 19, 2024, Ivanti disclosed a critical path traversal vulnerability (CVE-2024-8963, CVSS 9.4) in its Cloud Services Appliance (CSA) version 4.6, which is being actively exploited. This flaw allows remote, unauthenticated attackers to access restricted functionality, and when combined with the previously disclosed CVE-2024-8190, it allows for admin authentication bypass and arbitrary command execution. CSA 4.6 is End-of-Life, and Ivanti strongly recommends upgrading to CSA 5.0, which is not affected.

***Why You Should Care**: Given the history of exploitation by Chinese threat actors, organizations are urged to patch immediately and upgrade to the supported version. For more information, please see Aspire's Emergency Flash Notice.*

Vulnerabilities in Microsoft SQL Server Reporting Services and Windows Task Scheduler

Two Microsoft vulnerabilities, CVE-2020-0618 and CVE-2019-1069, have been added to CISA's Known Exploited Vulnerabilities catalog this month. CVE-2020-0618 is a deserialization flaw in Microsoft SQL Server Reporting Services that allows authenticated attackers to execute arbitrary code, potentially compromising server data and functionality. CVE-2019-1069 is a privilege escalation flaw in Windows Task Scheduler, allowing local authenticated attackers to gain SYSTEM-level privileges. Both vulnerabilities require valid credentials for exploitation and **have been actively exploited**.

***Why You Should Care**: CVE-2020-0618 allows attackers to execute arbitrary code, potentially leading to unauthorized access and manipulation of sensitive data stored on the server. This could result in the installation of malicious software, alteration of system configurations, or complete system takeover. Exploitation can lead to financial losses and a disruption in productivity. For more information and for patch guidance, please see Aspire's Emergency Flash Notice.*

Google Chrome Security Update – Several Vulnerabilities Patched

Google has released an update for Chrome (version 129.0.6668.70/.71 for Windows and Mac, and version 129.0.6668.70 for Linux) addressing multiple security vulnerabilities, including five

critical ones that could allow arbitrary code execution. High-severity vulnerabilities patched include CVE-2024-9120 (Use after free in Dawn), CVE-2024-9121 (Inappropriate implementation in V8), CVE-2024-9122 (Type Confusion in V8), and CVE-2024-9123 (Integer overflow in Skia). Successful exploitation could enable attackers to execute arbitrary code, install programs, modify data, or create new accounts with full user rights.

***Why You Should Care**: Chrome is a widely used browser. Unpatched vulnerabilities can be exploited by attackers to execute arbitrary code, potentially leading to data breaches, malware infections, or unauthorized access to your system. Keeping your browser updated ensures you have the latest security patches and performance improvements, helping to protect your system and data. For more information, please see Aspire's Emergency Flash Notice.*

NVIDIA AI Vulnerability Impacts Containers Using NVIDIA GPUs – CVE-2024-0132

Wiz Research has identified a critical vulnerability, CVE-2024-0132, in the NVIDIA Container Toolkit, which is widely used to provide GPU resources to containerized AI applications. This flaw allows attackers controlling a container image to escape the container and gain full access to the host system, which is a risk to sensitive data and infrastructure. NVIDIA has released a security bulletin and a patched version of the toolkit. The urgency to fix this vulnerability depends on your environment's architecture and the trust level of the images you run. Environments allowing third-party container images or AI models are at higher risk from malicious images.

***Why You Should Care**: Organizations using the NVIDIA Container Toolkit are urged to update to version 1.16.2 to mitigate this vulnerability, especially in environments that run untrusted container images. You may find patch guidance in NVIDIA's advisory.*

Citrix and XenServer Vulnerability Patched

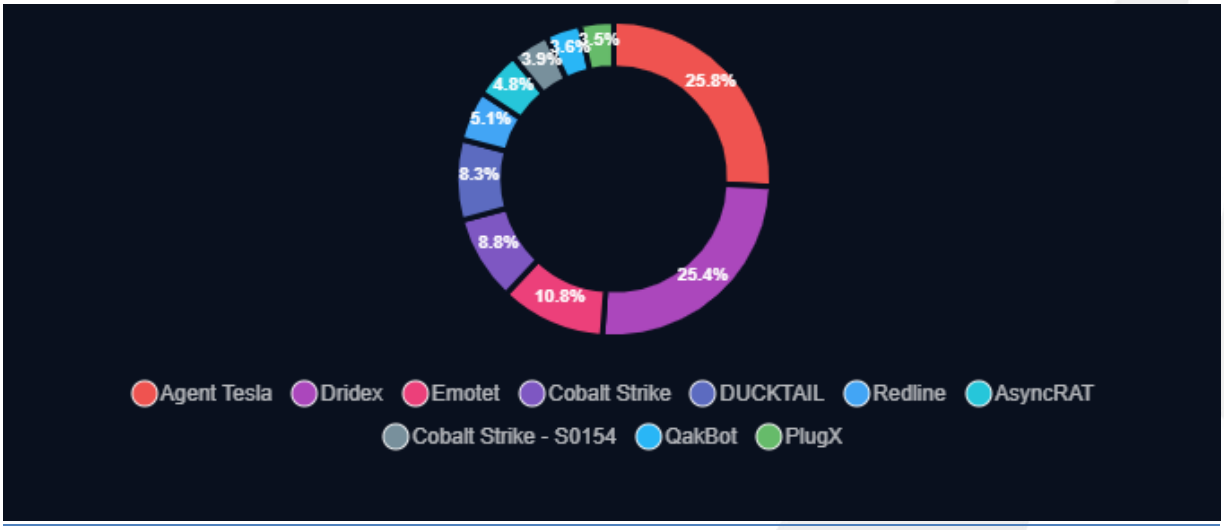
A security issue has been identified in XenServer 8 and Citrix Hypervisor 8.2 CU1 LTSR, allowing a malicious guest VM administrator to crash or render the host unresponsive (CVE-2024-45817). Additionally, two vulnerabilities in XenServer 8 (CVE-2022-24805 and CVE-2022-24809) could let an attacker on the management network crash the SNMP service. Customers using XenServer 8 should update via the Early Access or Normal channels, while those on Citrix Hypervisor 8.2 CU1 LTSR should apply the available hotfix

***Why You Should Care**: The vulnerabilities could allow a malicious guest VM administrator to crash or render your host system unresponsive, leading to downtime and disruption of services. Not patching in a timely manner could lead to the compromise of sensitive data. Citrix has published a security bulletin and recommends contacting their technical support for assistance.*

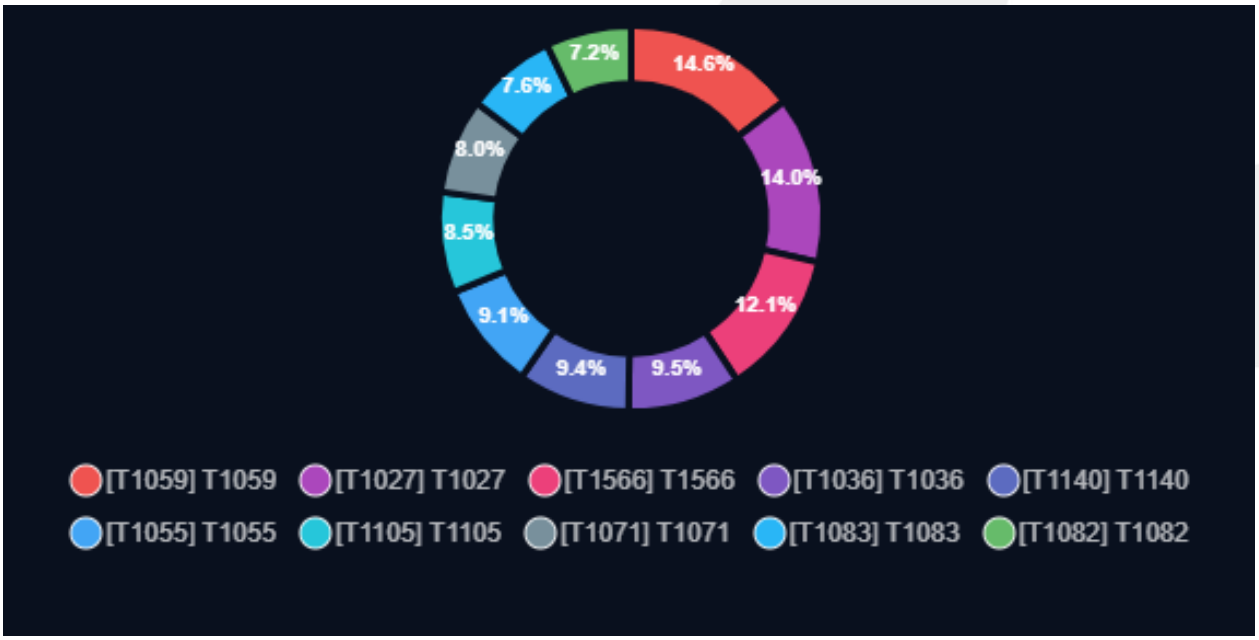
Industry Specific Threat Actors & Malware

Over the past 30 days, here is the latest research on the most prevalent malware distributed by threat actors, the top indicators of compromise (IoCs) by type, and the most common ATT&CK techniques used by threat actors.

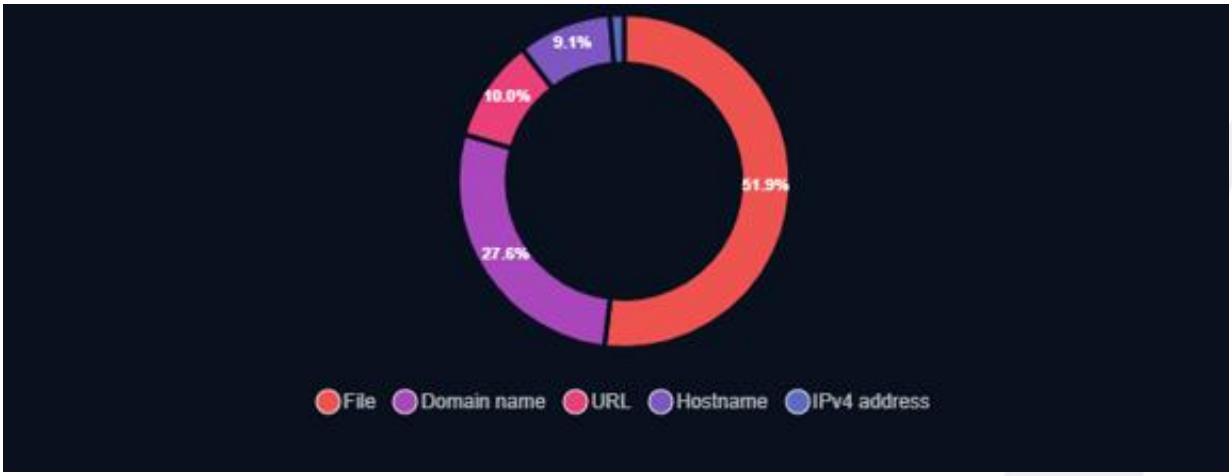
Top Malware Distributed by Threat Actors



Top ATT&CK Technique Distribution



Top Indicators by Type



In the past 7 days, the majority of attacks and malware activity we've observed have targeted the finance, government, and manufacturing sectors. Below are the leading threat actors and malware impacting these industries.

Threat Actors

Government, Manufacturing, & Finance

Water Bakunawa

The RansomHub ransomware group, tracked by Trend Micro as **Water Bakunawa**, uses advanced tactics to evade detection by endpoint detection and response (EDR) tools. A key component of their strategy is the use of EDRKillShifter, which disables EDR and antivirus protections by exploiting vulnerable drivers, ensuring persistence and allowing ransomware to spread undetected. This tool dynamically adapts to security measures, allowing RansomHub to remain hidden while executing its attack chain. The ransomware group exploits known vulnerabilities like Zerologon (CVE-2020-1472) and primarily targets critical sectors, including **finance, government, healthcare, and IT**, among others.

Through phishing, lateral movement, and data exfiltration techniques, they maximize their reach within compromised networks, while their affiliate model spreads the threat further. Recent attacks analyzed by Trend Micro's Vision One telemetry also show the use of spear-phishing and brute-force tactics to gain initial access, followed by the deployment of malicious scripts that disable Windows Defender and terminate security processes. The FBI has noted RansomHub's significant activity, having targeted over 200 organizations, demonstrating the growing threat ransomware groups like this pose to critical infrastructure.

***Why You Should Care**: Water Bakunawa uses tools like EDRKillShifter to disable endpoint detection and antivirus protections, allowing ransomware to bypass security systems and persist in compromised networks. This makes it harder for organizations to detect and respond to attacks. The group has a history of targeting high-value sectors such as finance, healthcare, IT, and government services, meaning that industries holding sensitive data or vital infrastructure are at risk of disruption or data theft. Organizations must take this group seriously and strengthen their defenses with proactive threat intelligence and patch management.*

Sloppy Lemming

The advanced threat actor **Sloppy Lemming**, also known as Outrider Tiger and Fishing Elephant, has been conducting cyberattacks across South and East Asia, targeting **government, law enforcement, energy, telecommunications, and technology** sectors. Active since at least July 2021, the group uses spear-phishing emails and cloud services like Cloudflare Workers to harvest credentials and deploy malware, including Ares RAT and WarHawk, which have links to well-known groups like SideWinder and SideCopy. Sloppy Lemming's operations span countries such as Pakistan, Sri Lanka, Bangladesh, China, and Indonesia, with specific attacks on law enforcement and military entities, as well as attempts to infiltrate Pakistan's nuclear facility. Their sophisticated tactics include exploiting Google OAuth tokens and using malicious RAR archives to deliver trojans via cloud platforms like Dropbox.

***Why You Should Care**: Sloppy Lemming focuses on critical sectors like government, law enforcement, energy, telecommunications, and technology. The threat actor uses spear-phishing and cloud services to steal sensitive login credentials, allowing for unauthorized access. It's important for organizations to stay vigilant, as Sloppy Lemming could be a national security risk.*

Rast Ransomware Gang

Since December 2023, the QiAnXin Threat Intelligence Center has tracked a highly active ransomware campaign targeting Chinese government and enterprise systems. Known as **Rast ransomware**, it is written in Rust and has affected over 6,800 systems, successfully encrypting more than 5,700 terminals. Rast operates by infiltrating boundary servers through methods like RDP brute force and exploiting known vulnerabilities (Nday). Once inside, it deploys ransomware, uploading victim details to a remote MySQL database. **Rast Gang**, the group behind the ransomware, is fast-moving and targets organizations without pursuing lateral network movement. Despite being a newer group, Rast Gang's tactics resemble those of older ransomware operators such as GandCrab and Phobos. The group's rapid rise in less than a year highlights both their technical capabilities and the current vulnerabilities in cybersecurity defenses.

***Why You Should Care**: Rast ransomware has already infected over 6,800 machines, primarily targeting government and enterprise networks, disrupting essential operations and services.*

Organizations must prioritize strengthening their security measures and monitoring systems to defend against Rast ransomware.

Storm-0501

The **Storm-0501** gang, active since 2021, is targeting hybrid cloud environments in the U.S., focusing on government and commercial sectors. They exploit vulnerabilities in systems like Zoho ManageEngine, Citrix NetScaler, and Adobe ColdFusion to gain access, steal credentials, establish persistent backdoors, and sometimes deploy ransomware. Their method involves moving laterally from on-premises systems into cloud environments, a tactic used by other cybercriminal groups. While Storm-0501 has previously deployed ransomware like Sabbath and Embargo, their evolving techniques highlight the growing risks in hybrid cloud systems.

***Why You Should Care**: This threat actor specifically targets vulnerabilities in on-premises systems and cloud interfaces, allowing them to steal sensitive data, exploit credentials, and establish persistent access across entire networks. Once they gain entry, Storm-0501 can move laterally between systems, leading to widespread damage.*

Security Reports

DragonRank

Cisco Talos has revealed a new threat actor dubbed "DragonRank," which focuses on manipulating search engine rankings primarily across Asian and some European countries by leveraging malware like PlugX and BadIIS. DragonRank targets web application services, deploying web shells to gather system data and facilitate malware distribution. They are noted for their sophisticated techniques, such as utilizing the Windows Structured Exception Handling (SEH) mechanism to covertly load PlugX without arousing suspicion. So far, over 35 compromised IIS servers have been identified in countries like Thailand, India, and Belgium, demonstrating a wide-ranging attack strategy across various sectors, including healthcare and media.

Unlike traditional black hat SEO groups, DragonRank adopts a more targeted approach, focusing on lateral movement within networks to gain broader control. Their operations involve creating scam websites optimized for SEO manipulation, harming the online reputation of their victims while promoting deceptive content. The group's connection to Simplified Chinese-speaking actors is further evidenced by their operational infrastructure and promotional tactics, which include advertisements for SEO services on legitimate sites and communication through platforms like Telegram and QQ.

***Why You Should Care**: DragonRank targets a diverse range of industries globally, compromising various sectors such as healthcare, transportation, and media, which may directly affect many organizations. By altering search engine rankings, DragonRank can harm a company's online*

visibility and reputation. The group's tactics reflect a growing trend in cybercrime, blending traditional hacking with digital marketing manipulation. Organizations must be aware of these threats and adapt their cybersecurity strategies accordingly.

U.S. Targeted by Russian Military Cyber Threat Actors

Cyber actors associated with the Russian General Staff Main Intelligence Directorate (GRU), particularly the 161st Specialist Training Center **(Unit 29155)**, have been engaged in malicious cyber activities targeting global critical infrastructure since at least 2020. These operations are characterized by espionage, sabotage, and efforts to inflict reputational damage. The deployment of the destructive WhisperGate malware against Ukrainian organizations was one of their initial actions. Unit 29155 is distinct from other established GRU cyber groups, and the FBI, CISA, and NSA have issued advisories detailing their tactics, techniques, and procedures (TTPs).

The cyber operations attributed to Unit 29155 are extensive and have impacted numerous NATO countries and various sectors, including government services, finance, transportation, energy, and healthcare. The group utilizes common cyber tools for reconnaissance, vulnerability exploitation, and data exfiltration, often relying on publicly available malware and hacker resources. Their tactics include exploiting weaknesses in internet-facing systems, conducting extensive scanning activities, and engaging in data leak operations. The FBI has reported over 14,000 instances of domain scanning linked to these actors, demonstrating their intent to disrupt aid efforts in Ukraine and compromise critical infrastructure in allied nations.

***Why You Should Care**: Unit 29155 has been linked to cyber operations that directly target essential sectors, including government services, healthcare, energy, and finance. Disruptions in these areas can lead to severe operational and financial consequences, not only for individual organizations but also for national security and public safety. The activities of Unit 29155 are part of a broader geopolitical context, where cyber warfare is increasingly used as a tool for influence and aggression. Organizations operating in sensitive sectors may become unintended targets in these geopolitical conflicts.*

Monthly Wins TLP:AMBER

This space is dedicated to acknowledging and celebrating successful project completions that contribute to both customer satisfaction and Aspire's overarching goals.

- Aspire Technology Partners is thrilled to launch our new Cyber Threat Intelligence (CTI) team, enhancing our commitment to your security. This team will collaborate with our Security Operations Center (SOC) to deliver timely, actionable intelligence for strengthening your cybersecurity defenses.
- You can find updates from our CTI team in Aspire's Managed Services Customer Portal, keeping you informed about the latest intelligence. Our CTI team will be your go-to source for information on various cybersecurity threats.

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.