Ransomware Spotlight: Black Basta

Archived: 2026-04-05 14:36:08 UTC

Top affected countries and industries according to Trend Micro data

In this section, we discuss Trend Micro™ Smart Protection Network™ data on Black Basta's activity from April 1 to July 31, 2022, which refers to detections of the ransomware's attempts to compromise organizations.

Just two countries accounted for over half of the group's 44 ransomware attack attempts during this period, which were concentrated in the US at 43%, with Austria a distant second at 15%. As Black Basta has sought to purchase network access credentials for organizations located specifically in the US, among other countries, this may explain the higher number of attacks against US-based businesses.

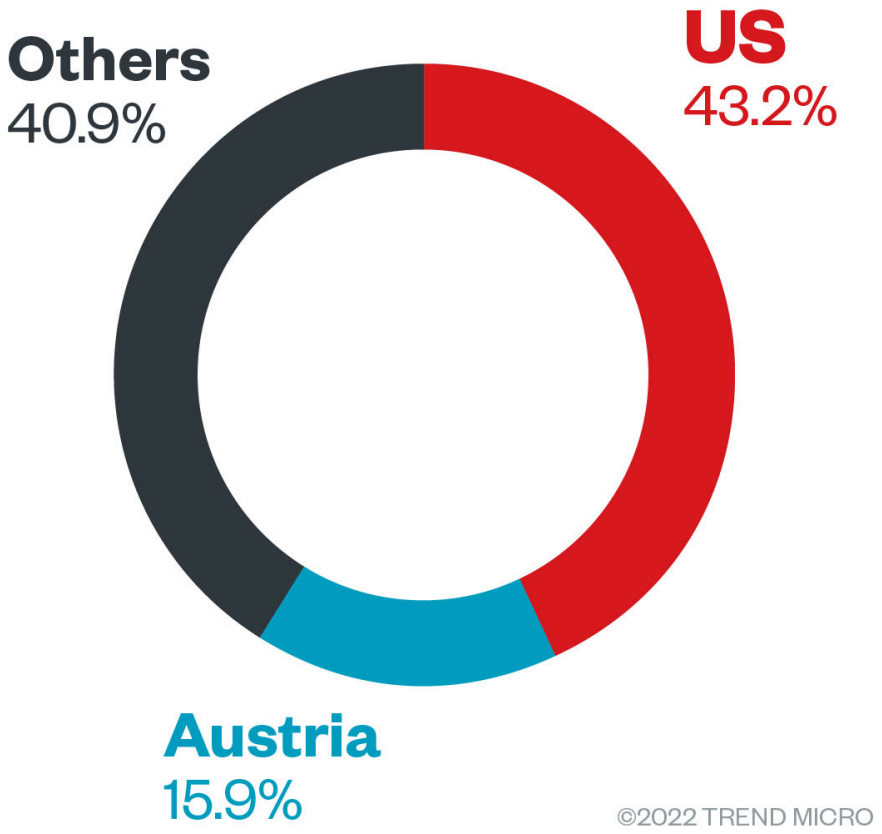


Figure 1. The countries with the most Black Basta ransomware attack attempts in terms of infected machines from April 1 to July 31, 2022
Source: Trend Micro™ Smart Protection Network™

As of this writing, our detections show that Black Basta activity is spread across many different industries. The group has been observed targeting businesses involved in technology, insurance, manufacturing, and utilities.

Although Black Basta is a relatively new arrival to the ransomware scene, its detections have been on a steady climb since the ransomware gang surfaced in April, peaking at 22 attack attempts in June before tapering down to 11 the following month.

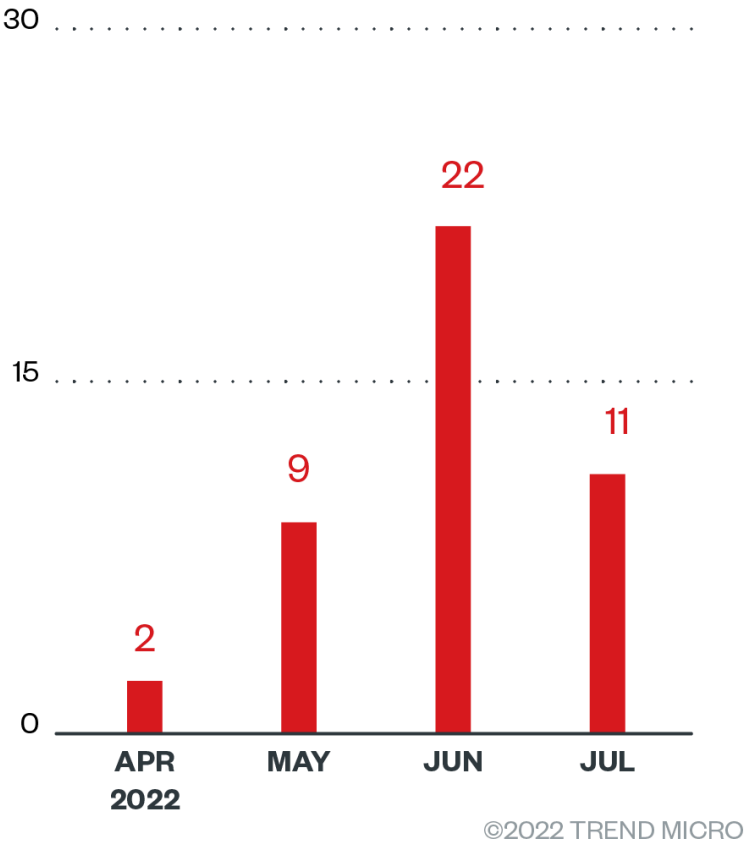


Figure 2. The numbers of detections of Black Basta ransomware attack attempts in terms of infected machines in each month from April 1 to July 31, 2022
Source: Trend Micro Smart Protection Network

Targeted regions and industries according to Black Basta's leak site

In this section, we look into the attacks recorded on the Black Basta group's leak site, which represent successfully compromised organizations that, as of this writing, have refused to pay ransom. Our detections, which pertain to Trend Micro customers, captured only a fraction of the victims found in Black Basta's leak site. Trend Micro's open-source intelligence (OSINT) research and investigation of the site show that from April 1 to July 31, 2022, the group compromised a total of 80 organizations.

The bulk of Black Basta' victims were based in North America, which had a victim count of 44, followed by Europe and the Asia-Pacific. More specifically, the US was at the receiving end of most of the attacks, with 38 affected organizations. Many confirmed ransomware attacks also took place in Germany, with 19 victims.

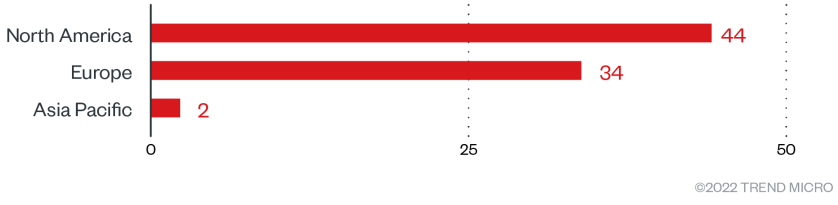


Figure 3. The distribution by region of Black Basta's victim organizations from April 1 to July 31, 2022
Sources: Black Basta's leak site and Trend Micro's OSINT research

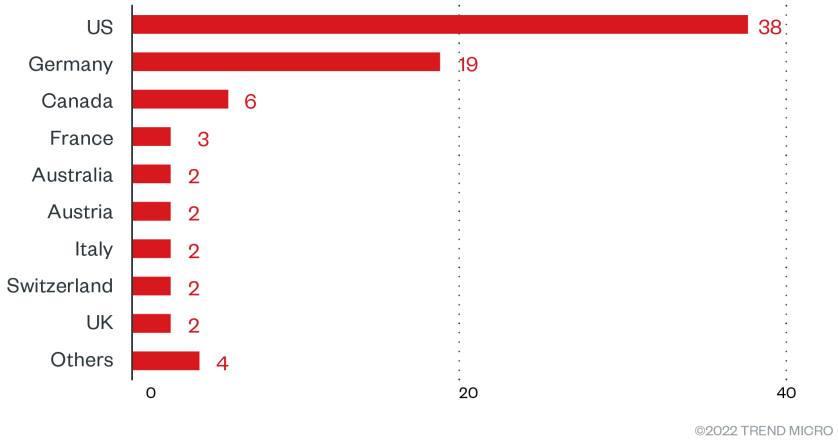


Figure 4. The distribution by country of Black Basta's victim organizations from April 1 to July 31, 2022
Sources: Black Basta's leak site and Trend Micro's OSINT research

. . .

Black Basta's attacks affected a variety of organizations. Construction businesses topped the list with a victim count of 10, while businesses involved in professional services came in second with nine victims. Medium-size organizations made up the lion's share of recorded Black Basta victims.

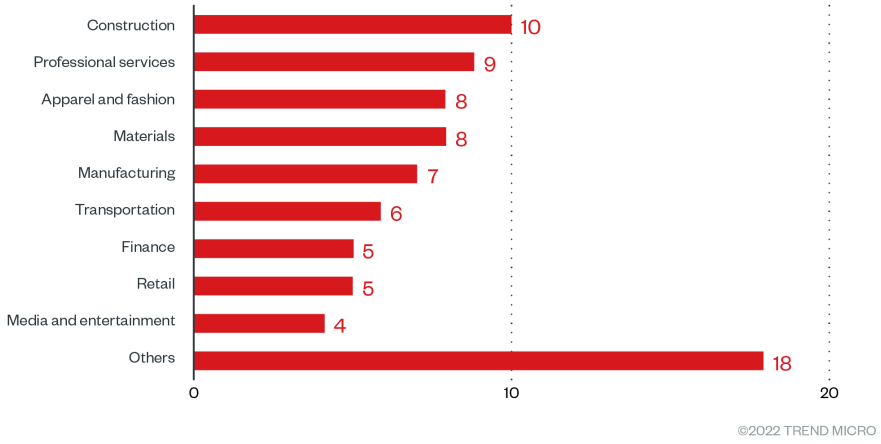


Figure 5. The distribution by industry of Black Basta's victim organizations from April 1 to July 31, 2022
Sources: Black Basta's leak site and Trend Micro's OSINT research

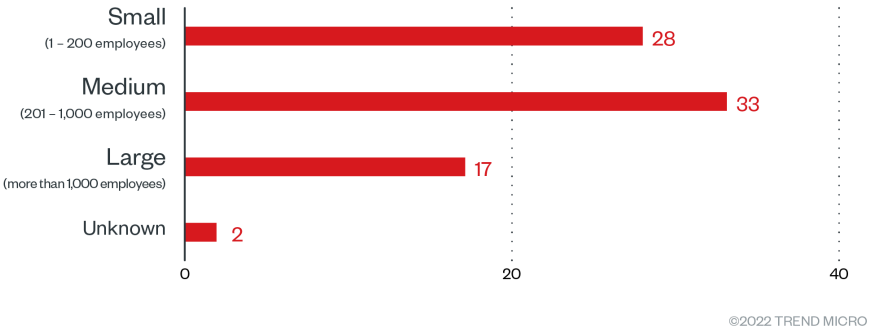


Figure 6. The distribution by organization size of Black Basta's victim organizations from April 1 to July 31, 2022
Sources: Black Basta's leak site and Trend Micro's OSINT research

Infection chain and techniques

As Black Basta's operations are based on the RaaS model, its infection chain might vary depending on the target. The infection chain illustrated below details the variety of tactics and tools the group uses.

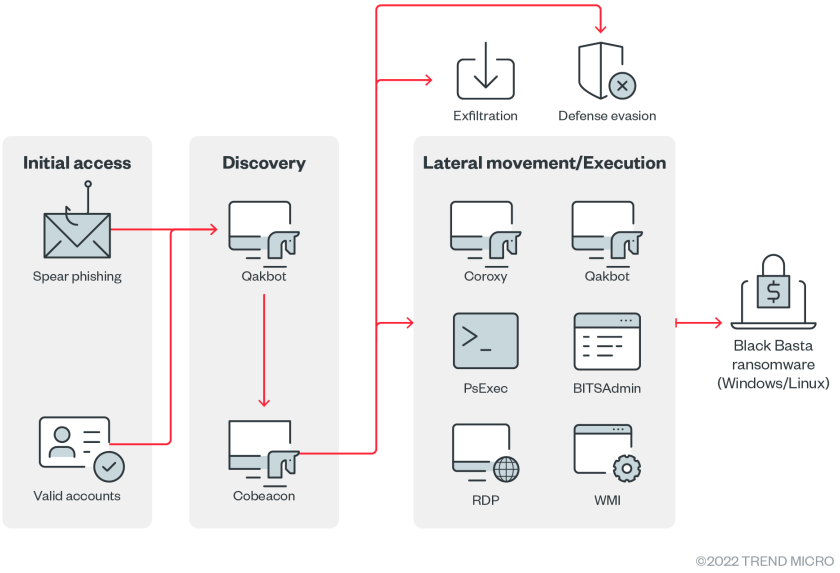


Figure 7. Black Basta's infection chain

Initial access

- External data reports that a user named "Black Basta" posted on underground forums seeking corporate network access credentials, offering a share of the profit from their attacks as payment. These reports are supported by the fact that a unique ID is hard-coded in each Black Basta build, which could also mean that the ransomware gang does not distribute its malware sporadically.
- Our internal telemetry shows another set of samples, which were monitored within a 72-hour time frame, that were using Qakbot. The malware is downloaded and executed from a malicious Excel file and then executes certain PowerShell commands as part of its staging phase

Discovery

- Black Basta uses PowerShell scripts to scan information about the compromised system or network.
- It uses Qakbot's and Cobeacon's information-gathering capabilities to scan the compromised system or network.
- It uses third-party tools such as Netcat to scan the compromised system or network.

Defense evasion

- Black Basta uses a batch script containing PowerShell commands to disable antimalware applications.
- It uses Group Policy Objects (GPOs) to disable Windows Defender and Security Center.
- It reboots the victim's computer in safe mode to circumvent any antimalware applications.

Privilege escalation

- Black Basta exploits the PrintNightmare vulnerability (CVE-2021-34527)open on a new tab to perform privileged operations and deliver the Cobalt Strike beacon (aka Cobeacon) or other payloads.

Credential access

- Black Basta uses Mimikatz to dump credentials.

Lateral movement

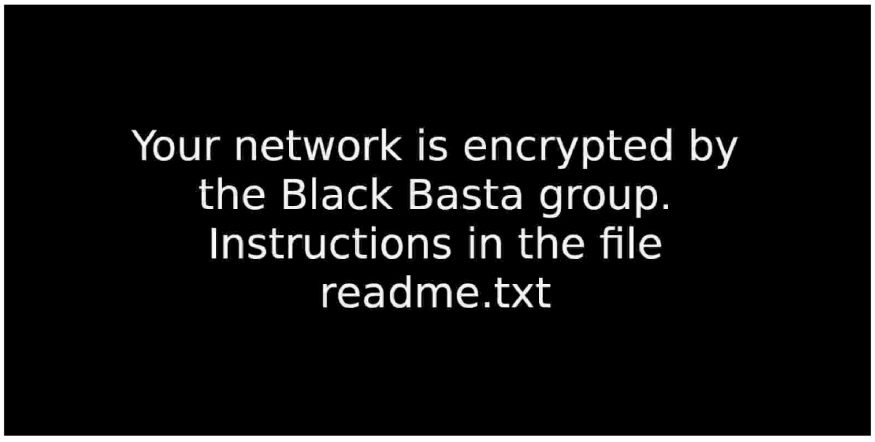
- Black Basta uses different tools and pieces of malware to spread its ransomware to other remote systems in the network:
  - BITSAdmin
  - PsExec
  - Windows Management Instrumentation (WMI)
  - RDP
  - Qakbot
  - Cobeacon

Exfiltration

- Black Basta uses Cobeacon to exfiltrate the stolen data on an established command-and-control (C&C) server.
- It uses Rclone to exfiltrate data from compromised systems.

Impact

- Black Basta uses the ChaCha20 algorithm to encrypt files. The ChaCha20 encryption key is then encrypted with a public RSA-4096 key that is included in the executable.
- Multiple builds of Black Basta ransomware have been found in the wild
  - One build restarts the victim's system in safe mode, most likely for evasion purposes, before performing encryption. This build also modifies the "Fax" service to enable it to run in safe mode and with service-level access.
  - Another build contains only the ransomware's core capabilities, such as wallpaper defacement, file encryption, and deletion of shadow copies.
  - A newly found build has a new addition: the *-bomb* argument, which theoretically allows the ransomware to automatically target all connected machines for encryption.
  - The Linux build of the ransomware targets the folder */vmfs/volumes*, where images from virtual machines are contained, for encryption. To encrypt other folders, the ransomware actors include the *-forcepath* argument.
- Black Basta displays a ransomware note as the victim's wallpaper directing them to a .txt file with more details.



Other technical details

- Black Basta avoids encrypting files in these folders:
  - *$Recycle.Bin*
  - *Windows*
  - *Local Settings*
  - *Application Data*
  - *boot*
- It avoids encrypting files with these strings in their file names:
  - *OUT.txt*
  - *NTUSER.DAT*
  - *readme.txt* (the ransom note)
  - *dlaksjdoiwq.jpg* (a desktop wallpaper found in the *%TEMP%* folder)
  - *fkdjsadasd.ico* (an icon used for encrypted files, found in the *%TEMP%* folder)

- It drops a ransom note as a .txt file in an encrypted folder in the victim's machine.

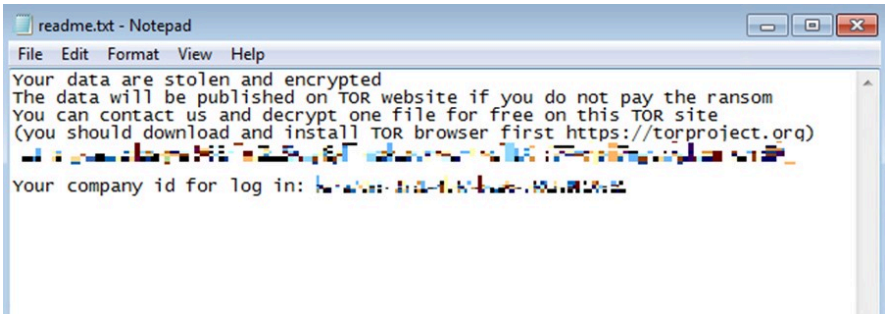


Figure 9. An example of the contents of the ransom note .txt file

MITRE ATT&CK tactics and techniques

Initial access	Execution	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Exfiltration	Impact
T1078 - Valid accounts *Has been reported buying compromised accounts on underground forums to access victim systems.* **T1566.001** - Phishing: Spear-phishing attachment *Mirrors technique used by Qakbot operators to distribute their payload that will deliver the ransomware.*	**T1059.003** - Command and scripting interpreter *Uses various scripting interpreters like PowerShell and Windows command shell.* **T1569.002** - System services: Service execution *Stops and deletes the service named "Fax", which it then impersonates for its encryption routine.* **T1047** - Windows Management Instrumentation *Has been observed to use Windows Management Instrumentation (WMI) to spread and execute files over the Network.*	**T1068** - Exploitation for privilege escalation *Exploits the PrintNightmare vulnerability (CVE-2021-34527) to perform privileged operations*	**T1112** - Modify registry *Modifies registry entries to enable it to replace the desktop wallpaper, set the icon associated with encrypted files, establish persistence, and disable defenses.* **T1484.001** - Domain policy modification: Group policy modification *Employs a technique involving the creation of a Group Policy Object (GPO) on a compromised domain controller, which will push out the changes (disable defenses) to the Windows registry of*	**T1003** - OS credential dumping *Uses Mimikatz to dump credentials.*	**T1082** - System information discovery *Uses tools for local system scans.* **T1018** - Remote system discovery *Uses tools for remote network scans.* **T1083** - File and directory discovery *Searches for specific files and directories related to its ransomware encryption.*	**T1570** - Lateral tool transfer *Uses tools like PsExec and BITSAdmin to spread the malware laterally across the network.* **T1021.001** - Remote services: Remote Desktop Protocol *Uses RDP to spread and execute the malware across the network.*	**T1041** - Exfiltration over C&C channel *Uses an established command-and-control (C&C) channel to exfiltrate data.* **T1567** - Exfiltration over web service *Uses a tool like Rclone to copy stolen data from a client to its cloud server.*	**T1490** - Inhibit system recovery *Deletes shadow copies.* **T1489** - Service stop *Stops and deletes a service named "Fax", which it then impersonates for its encryption routine.* **T1486** - Data encrypted for impact *Encrypts files and adds the extension* ".basta". **T1491** - Defacement *Replaces the desktop wallpaper to display the ransom note.*

Initial access	Execution	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Exfiltration	Impact
			domain-joined hosts. **T1562.001** - Impair defenses: Disable or modify tools *Disables Windows Defender and Security Center.* **T1562.009** - Impair defenses: Safe mode boot *Disables Windows recovery and repair features and restarts the machine in safe mode.* **T1620** - Reflective code loading *Has some builds that are known to use reflective code loading when executing themselves.*					

Summary of tools, exploit, and other malware used

Security teams can keep an eye out for the presence of these tools, exploit, and other malware that are typically used in Black Basta's ransomware attacks:

Initial access	Discovery	Privilege escalation	Credential access	Lateral movement	Execution	Exfiltration	C c
• Spear phishing	• Netcat	• PrintNightmare vulnerability (CVE-2021-34527)	• Mimikatz	• BITSAdmin • Coroxy • PsExec • RDP • WMI	• PowerShell • Windows command shell • WMI	• Cobeacon • Rclone	

Security recommendations

Security researchers have speculated that Black Basta might be an offshoot open on a new tab of the infamous Continews article ransomware gang. It has also exhibited similarities to the Black Matter ransomware gang, including a resemblance between their respective leak sites. Its possible connection to these ransomware groups might explain the high level of in-house expertise behind Black Basta's attacks.

In defending systems against threats like Black Basta, organizations can benefit from establishing security frameworks that can allocate resources systematically for establishing solid defenses against ransomware. Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data.
- Identify authorized and unauthorized devices and software.
- Make an audit of event and incident logs.

Configure and monitor

- Manage hardware and software configurations.
- Grant admin privileges and access only when necessary to an employee's role.
- Monitor network ports, protocols, and services.
- Activate security configurations on network infrastructure devices such as firewalls and routers.
- Establish a software allowlist that only executes legitimate applications.

Patch and update

- Conduct regular vulnerability assessments.
- Perform patching or virtual patching for operating systems and applications.
- Update software and applications to their latest versions.

Protect and recover

- Implement data protection, backup, and recovery measures.
- Enable multifactor authentication (MFA).

Secure and defend

- Employ sandbox analysis to block malicious emails.
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network.
- Detect early signs of an attack such as the presence of suspicious tools in the system.
- Use advanced detection technologies such as those powered by AI and machine learning.

Train and test

- Regularly train and assess employees on security skills.
- Conduct red-team exercises and penetration tests.

A multilayered approach can help organizations guard possible entry points into the system (endpoint, email, web, and network). Security solutions that can detect malicious components and suspicious behavior can also help protect enterprises:

- Trend Micro Vision One™products provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ – Workload Securityproducts protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspectorproducts employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™products offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of compromise (IOCs)

The indicators of compromise (IOCs) for the threat discussed in this article can be found hereopen on a new tab. Actual indicators might vary per attack.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---