Date of Publication
November 24, 2025

Hive Pro

Hiveforce Labs

WEEKLY

THREAT DIGEST

Attacks, Vulnerabilities, and Actors

17 to 23 NOVEMBER 2025

Table Of Contents

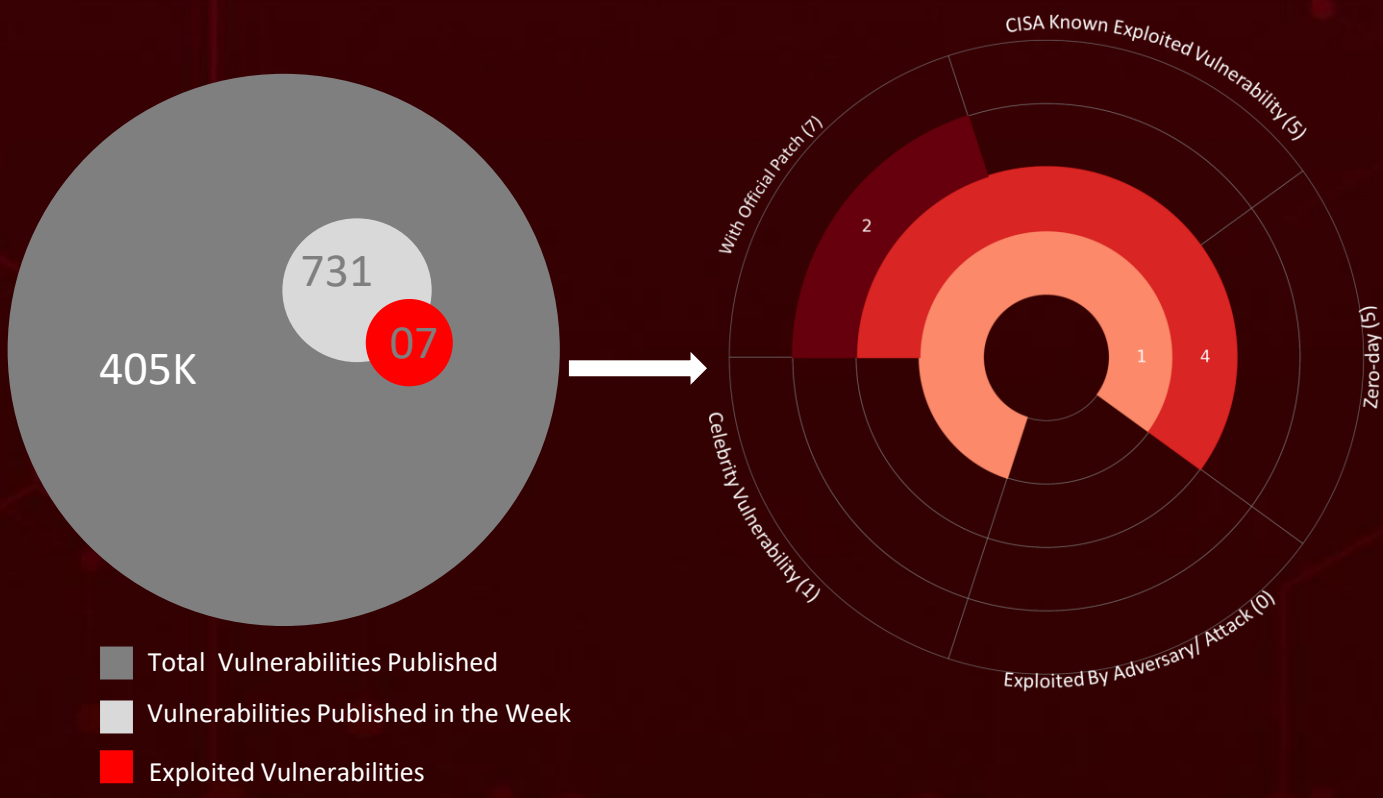
Summary

HiveForce Labs has reported a sharp rise in cybersecurity threats, highlighting the increasing complexity and frequency of global cyber incidents. Over the past week, **four** major attacks were detected, **seven** critical vulnerabilities were publicly disclosed, and **one** active threat actor group was monitored, signaling a concerning escalation in malicious activity.

Five zero-day vulnerabilities were tracked and confirmed as exploited in the wild: **CVE-2025-64446** (Fortinet FortiWeb), **CVE-2025-20337** (Cisco Identity Services Engine), **CVE-2025-13223** (Google Chrome), **CVE-2025-58034** (Fortinet FortiWeb), and **CVE-2025-5777**, known as **Citrix Bleed 2**. The confirmation that Citrix Bleed 2 was abused before disclosure amplifies its overall risk impact.

Dragon Breath (APT-Q-27) continues a rapid, high-volume campaign using multi-stage loaders, brand imitation, and disposable domains to distribute modified **Gh0st RAT** variants to Chinese-speaking users. Current activity clusters under **Campaign Trio** and **Campaign Chorus**.

Eternidade Stealer expands Brazil's WhatsApp-centered cybercrime landscape, underscoring the need for disciplined security updates and sustained monitoring in the face of fast-evolving attack methodologies.



High Level Statistics

4
Attacks Executed

7
Vulnerabilities Exploited

1
Adversaries in Action

- RONINGLOADER
- Gh0st RAT
- Eternidade
- TamperedChef

- CVE-2025-64446
- CVE-2025-20337
- CVE-2025-13223
- CVE-2025-58034
- CVE-2025-5777
- CVE-2025-55241
- CVE-2025-11001

- Dragon Breath

Insights

CVE-2025-55241: Entra ID Token-Validation Failure Enabling Cross-Tenant Admin Impersonation

CVE-2025-64446: Critical Weakness Allowing Long-Term Attacker Residency in FortiWeb Systems

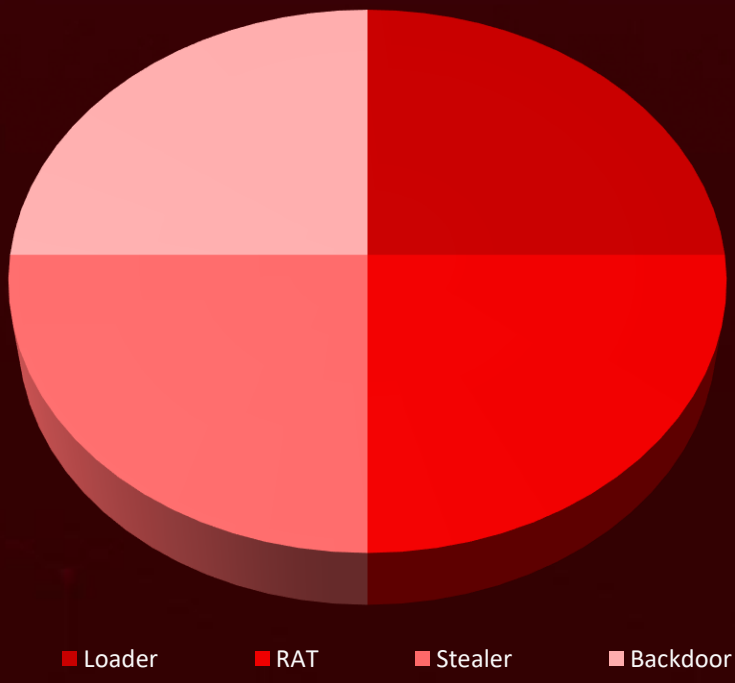
Eternidade Stealer: Precision Malware Framework Converting Routine Messages into Theft Vectors

CVE-2025-13223: Zero-Day Memory Corruption in Chrome's V8 Engine Under Active Exploitation

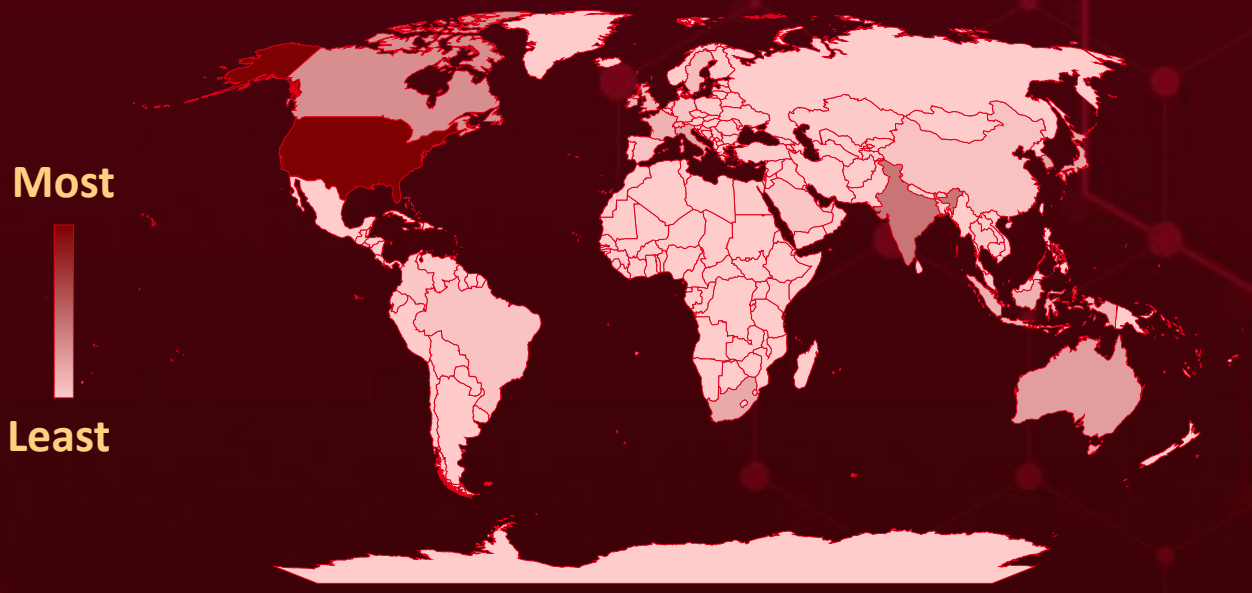
Dragon Breath: Brand-Impersonation Infrastructure Feeding Large-Scale Gh0st RAT Campaigns

TamperedChef: EV-Certified Malware Supply Chain Targeting U.S. Healthcare

Threat Distribution

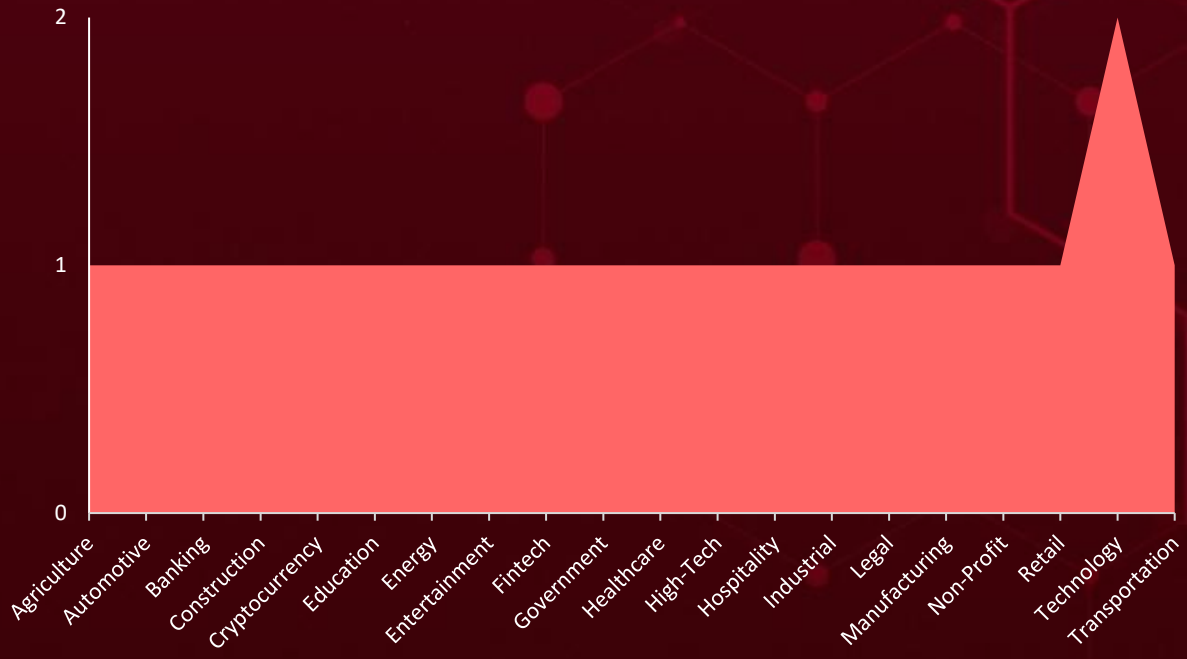


Targeted Countries



Countries	Countries	Countries	Countries
United States	Malaysia	Pakistan	Mali
India	Thailand	Nigeria	Burkina Faso
Canada	Ecuador	Russia	Malawi
Australia	Kenya	Ethiopia	Zambia
South Korea	Oman	Mexico	Chad
Hong Kong	Argentina	Philippines	Somalia
Italy	Bangladesh	DR Congo	Senegal
Japan	Belarus	Iran	Guatemala
South Africa	Peru	Tanzania	Cambodia
Indonesia	Qatar	Myanmar	Zimbabwe
Ireland	Bolivia	Sudan	Guinea
France	Chile	Uganda	Benin
United Kingdom	Czech Republic	Algeria	Burundi
Switzerland	Egypt	Iraq	Tunisia
Sweden	Finland	Afghanistan	South Sudan
Singapore	Kuwait	Yemen	Haiti
United Arab Emirates	Kazakhstan	Angola	Belgium
Israel	Sri Lanka	Ukraine	Jordan
Spain	North Macedonia	Morocco	Dominican Republic
China	Poland	Uzbekistan	Honduras
Bahrain	Romania	Mozambique	Cuba
Germany	Rwanda	Ghana	Tajikistan
Netherlands	Turkey	Madagascar	Papua New Guinea
Brazil	Taiwan	Cameroon	Portugal
Saudi Arabia	Venezuela	Nepal	Azerbaijan
Colombia	Vietnam	Niger	Greece
Latvia	Palestine	North Korea	Togo
	Macau	Syria	Hungary

Targeted Industries



TOP MITRE ATT&CK TTPs

T1059 Command and Scripting Interpreter	**T1036** Masquerading	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1071.001** Web Protocols
T1071 Application Layer Protocol	**T1055** Process Injection	**T1068** Exploitation for Privilege Escalation	**T1518** Software Discovery	**T1204** User Execution
T1203 Exploitation for Client Execution	**T1027** Obfuscated Files or Information	**T1204.002** Malicious File	**T1070** Indicator Removal	**T1573** Encrypted Channel
T1190 Exploit Public-Facing Application	**T1082** System Information Discovery	**T1547.001** Registry Run Keys / Startup Folder	**T1505.003** Web Shell	**T1057** Process Discovery

Attacks Executed

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
RONINGLOADER	RONINGLOADER is a multi-stage loader that begins by checking for administrative rights. If it lacks them, it uses the runas command to relaunch itself with elevated privileges, then shuts down the original process.	Trojanized Installer	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Execution of additional malicious payloads	-
Loader			**PATCH LINK**
ASSOCIATED ACTOR			-
Dragon Breath			
IOC TYPE	**VALUE**		
SHA256	c84764a19543e9bdfe06263d3dd68bbf9df381bbe4d0c0da480bc4eddea293b6, 1613a913d0384cbb958e9a8d6b00fffaf77c27d348ebc7886d6c563a6f22f2b7		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Gh0st RAT	Gh0st RAT connects to a remote command-and-control server to receive instructions that allow system manipulation, file retrieval and execution, command execution, and activation of stored payloads. It also supports spying functions such as keylogging, clipboard capture, and active window monitoring.	Trojanized Installer	-
		IMPACT	**AFFECTED PLATFORM**
TYPE		Remote system compromise, Data exposure	-
RAT			**PATCH LINK**
ASSOCIATED ACTOR			-
Dragon Breath			
IOC TYPE	**VALUE**		
SHA256	3dd470e85fe77cd847ca59d1d08ec8ccebe9bd73fd2cf074c29d87ca2fd24e33, 299e6791e4eb85617c4fab7f27ac53fb70cd038671f011007831b558c318b369, 1395627eca4ca8229c3e7da0a48a36d130ce6b016bb6da750b3d992888b20ab8		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
Eternidade	Eternidade is a Delphi-based stealer that uses IMAP to dynamically update its C2 servers for added resilience. It also spreads via a new Python-based WhatsApp worm that hijacks WhatsApp Web to send malicious attachments to a victim's contacts.	Social Engineering	-
		IMPACT	AFFECTED PRODUCT
TYPE		Data exposure, Financial Loss	Windows, Linux, MacOS, Android
Stealer			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	5cb86ca4b4017726ea2c60b754e27d4440e8fec490b9bd8eab7b5d87a0f0987b		

NAME	OVERVIEW	DELIVERY METHOD	TARGETED CVE
TamperedChef	TamperedChef is a backdoor that establishes persistence via a scheduled task, performs system reconnaissance, and quietly exfiltrates data while maintaining communication with attacker-controlled servers.	Malvertising	-
		IMPACT	AFFECTED PRODUCT
TYPE		Persistent Access, Covert data exfiltration	Windows
Backdoor			
ASSOCIATED ACTOR			PATCH LINK
-			-
IOC TYPE	VALUE		
SHA256	a16ecfcf5e6d7742f0e642309c3a0bf84eaf21962e663ce728f44c93ee70a28e, 0826824694c80b854603f4c4103133113a197d3ecbca4308899ae9d6f05847fa, 08ea829d5c97aab089abe19686d274f829aa1cee3670d2819885e33f39a4d602, 2a3a9ab2ad245d3464b5cc1bc8270568b5c490e4972e99e8f94ab2177874d81a, 2fee5916dad509ff4fea4f4b17795677bda7316253111b2abf7f523bae2a973e		

The IOCs (Indicators of Compromise) for the attacks executed are listed in the appendix section at the end of the report.

Vulnerabilities Exploited

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-64446	✗	Fortinet FortiWeb 8.0 - 8.0.0 through 8.0.1 Fortinet FortiWeb 7.6 - 7.6.0 through 7.6.4 Fortinet FortiWeb 7.4 - 7.4.0 through 7.4.9 Fortinet FortiWeb 7.2 - 7.2.0 through 7.2.11 Fortinet FortiWeb 7.0 - 7.0.0 through 7.0.11	-
	ZERO-DAY		
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	-
Fortinet FortiWeb Path Traversal Vulnerability	✓		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINK**
	CWE-23	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation	https://fortiguard.fortinet.com/psirt/FG-IR-25-910

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-20337	✗	Cisco ISE and ISE-PIC releases 3.3 and 3.4	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*:*	-
Cisco Identity Services Engine Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-74	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-13223	✗	Google Chrome prior to 142.0.7444.175	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-843	T1189: Drive-by Compromise, T1059: Command and Scripting Interpreter, T1203: Exploitation for Client Execution	https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-58034		FortiWeb 8.0 - 8.0.0 through 8.0.1 FortiWeb 7.6 - 7.6.0 through 7.6.5 FortiWeb 7.4 - 7.4.0 through 7.4.10 FortiWeb 7.2 - 7.2.0 through 7.2.11 FortiWeb 7.0 - 7.0.0 through 7.0.11	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:fortinet:fortiweb:*:*:*:*:*:*:*:*	-
Fortinet FortiWeb OS Command Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-78	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	https://fortiguard.fortinet.com/psirt/FG-IR-25-513

<table>
<tr><th>CVE ID</th><th>CELEBRITY VULNERABILITY</th><th>AFFECTED PRODUCT</th><th>ASSOCIATED ACTORS</th></tr>
<tr><td rowspan="3">CVE-2025-5777</td><td>CitrixBleed 2</td><td rowspan="2">NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56, 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS</td><td rowspan="2">-</td></tr>
<tr><td>ZERO-DAY</td></tr>
<tr><td>✓</td><td>AFFECTED CPE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td></tr>
<tr><td>NAME</td><td>CISA KEV</td><td rowspan="2">cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_gateway:*:*:*:*:*:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:fips:*:*:* cpe:2.3:a:citrix:netscaler_application_delivery_controller:*:*:*:*:ndcpp:*:*:*</td><td rowspan="2">-</td></tr>
<tr><td rowspan="2">CitrixBleed 2 (Citrix NetScaler Gateway Out-of-Bounds Read Vulnerability)</td><td rowspan="2">✓</td></tr>
<tr><td>CWE ID</td><td>ASSOCIATED TTPs</td><td>PATCH LINK</td></tr>
<tr><td></td><td>CWE-125</td><td>T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation</td><td>https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420</td></tr>
</table>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-55241	✗	Microsoft Azure Entra ID	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:microsoft:entra_id:-:*:*:*:*:*:*:*	-
Azure Entra ID Elevation of Privilege Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-287	T1068: Exploitation for Privilege Escalation	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2025-55241

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCT	ASSOCIATED ACTORS
CVE-2025-11001	✗	7-Zip before version 25.00	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:7-zip:7zip:*:*:*:*:*:*:*:*	-
7-Zip Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-22	T1059: Command and Scripting Interpreter, T1204.002: Malicious File	https://www.7-zip.org/download.html

Adversaries in Action

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGETED INDUSTRIES</th><th>TARGETED REGIONS</th></tr>
<tr><td rowspan="4"> 
Dragon Breath (alias Golden Eye Dog, APT-Q-27)</td><td>Unknown</td><td rowspan="3">Technology, Entertainment, High-Tech</td><td rowspan="3">Worldwide (Major Chinese-Speaking Territories)</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Financial gain, Information Theft</td></tr>
<tr><td>TARGETED CVE</td><td>ASSOCIATED ATTACKS/RANSOMWARE</td><td>AFFECTED PRODUCT</td></tr>
<tr><td>-</td><td>RONINGLOADER, Gh0st RAT</td><td>-</td></tr>
<tr><td colspan="4">TTPs</td></tr>
<tr><td colspan="4">TA0001: Initial Access; TA0002: Execution; TA0003: Persistence; TA0004: Privilege Escalation; TA0005: Defense Evasion; TA0006: Credential Access; TA0007: Discovery; TA0009: Collection; TA0040: Impact; TA0011: Command and Control; TA0042: Resource Development; T1059: Command and Scripting Interpreter; T1059.003: Windows Command Shell; T1569: System Services; T1569.002: Service Execution; T1566: Phishing; T1543: Create or Modify System Process; T1543.003: Windows Service; T1548: Abuse Elevation Control Mechanism; T1548.002: Bypass User Account Control; T1134: Access Token Manipulation; T1562.001: Disable or Modify Tools; T1562: Impair Defenses; T1562.004: Disable or Modify System Firewall; T1070: Indicator Removal; T1070.001: Clear Windows Event Logs; T1574: Hijack Execution Flow; T1574.001: DLL; T1055: Process Injection; T1036.005: Match Legitimate Resource Name or Location; T1036: Masquerading; T1112: Modify Registry; T1553: Subvert Trust Controls; T1553.006: Code Signing Policy Modification; T1056: Input Capture; T1056.001: Keylogging; T1115: Clipboard Data; T1057: Process Discovery; T1082: System Information Discovery; T1033: System Owner/User Discovery; T1518: Software Discovery; T1518.001: Security Software Discovery; T1095: Non-Application Layer Protocol; T1573: Encrypted Channel; T1573.001: Symmetric Cryptography; T1583: Acquire Infrastructure; T1204: User Execution; T1204.002: Malicious File; T1059.005: Visual Basic; T1059.001: PowerShell; T1218: System Binary Proxy Execution; T1218.007: Msiexec; T1071: Application Layer Protocol; T1071.001: Web Protocols</td></tr>
</table>

Recommendations

Security Teams

This digest can be utilized as a drive to force security teams to prioritize the **seven exploitable vulnerabilities** and block the indicators related to the threat actor **Dragon Breath,** and malware **RONINGLOADER, Gh0st RAT, Eternidade, TamperedChef.**

Uni5 Users

This is an actionable threat digest for HivePro Uni5 customers, and they can get comprehensive insights into their threat exposure and can action it effortlessly over the HivePro Uni5 dashboard by

- Run a Scan to discover the assets impacted by the **seven exploitable vulnerabilities.**
- Testing the efficacy of their security controls by simulating the attacks related to the threat actor **Dragon Breath,** and malware **RONINGLOADER, Gh0st RAT, Eternidade Stealer, TamperedChef** in Breach and Attack Simulation(BAS).

Threat Advisories

FortiWeb Hijack: The Hidden Vulnerability Fueling Admin Account Creation

Critical Cisco ISE Flaws Actively Exploited in the Wild

Google Patches High-Risk V8 Zero-Day Hitting Chrome Users

FortiWeb Flaw Exploited in the Wild: Patch Immediately

Multiple Flaws in Citrix NetScaler ADC and Gateway Pose Immediate Threat

Gh0st RAT Multi-Campaign Delivery Surge Targets Chinese Speakers

Eternidade Stealer: Brazil's New WhatsApp-Driven Cybercrime Engine

TamperedChef: A High-Severity Multi-Stage Infostealer Operation

CVE-2025-55241: Critical Cross-Tenant Privilege Escalation in Microsoft Entra ID

CVE-2025-11001 Turns a Simple Unzip into a System-Level Ambush

Appendix

Known Exploited Vulnerabilities (KEV): Software vulnerabilities for which there are public exploits or proof-of-concept (PoC) code available, and for which there is a high risk of potential harm to an organization's systems or data if left unaddressed.

Celebrity Vulnerabilities: Software vulnerabilities that have gained significant attention and have been branded with catchy names and logos due to their profound and multifaceted impact. These vulnerabilities provide threat actors with opportunities to breach sensitive systems, potentially resulting in unauthorized access and the compromise of critical information.

Indicators of Compromise (IOCs)

Attack Name	TYPE	VALUE
RONINGLOADER	SHA256	c84764a19543e9bdfe06263d3dd68bbf9df381bbe4d0c0da480bc4eddea293b6, 1613a913d0384cbb958e9a8d6b00fffaf77c27d348ebc7886d6c563a6f22f2b7
	Domain	qaqkongtiao[.]com
Gh0st RAT	SHA256	3dd470e85fe77cd847ca59d1d08ec8ccebe9bd73fd2cf074c29d87ca2fd24e33, 299e6791e4eb85617c4fab7f27ac53fb70cd038671f011007831b558c318b369, 1395627eca4ca8229c3e7da0a48a36d130ce6b016bb6da750b3d992888b20ab8
Eternidade	SHA256	5cb86ca4b4017726ea2c60b754e27d4440e8fec490b9bd8eab7b5d87a0f0987b
TamperedChef	SHA256	a16ecfcf5e6d7742f0e642309c3a0bf84eaf21962e663ce728f44c93ee70a28e, 0826824694c80b854603f4c4103133113a197d3ecbca4308899ae9d6f05847fa, 08ea829d5c97aab089abe19686d274f829aa1cee3670d2819885e33f39a4d602, 105e58c4c04b56607badd705411e3322c152b8dbb21d994e7cdec62253a0e454, 244251cab1f6df4bb39ba28645cbc4e26f84298b588b568a796d6520912c6156,

Attack Name	TYPE	VALUE
TamperedChef	SHA256	26163c7da9f0d9000937663497d7eb15df5c205cc2edbb71d664f08a5b1f80ce, 2a3f76fc7f953403653eff71f21c16d40512c1bcd7a038657bb1d0a4efbee677, 2bfa87dee2000f4e7889174f051ab88f4b690d08629b94721e321c44b7cf1bd3, 2c9895fbdf8b86715a8e501f85d206b28cf9b61478826409a8a8ea17a067da22, 35c34043a4a8b1f15ce9ab7661be6ace91348f725d59e53f04a36c41999812c7, 3d4bdd41ebc630b8b676fc39e14de75a59cebf545cf342a4dea8072f5768c13e, 406e26453a9eb779da6dd792e82cf904fbaf11b9e15471316276bb49098bdbf6, 504a614d8baae84c7c57e1786d22981fb016e4c9396ab10cc73197aa483d9261, 6438b3c4eb5810c003d6f2cf1712652d3ce0504f08ae05aec1f07594e0a58a52, 6c4e54bbf98113068bdeef172ae6fb05fe1e99bb50ae4622b06e06af35b2b043, 6e4cd57e87e034723d4c1a3ff93e8c9def0f27961da3e5bc361536e847a119cb, 898aa0bca40ec01d3564cb33f7a79f2e651f987ea65db913a62d427973ba5478, 94acbfe1958b1b985701c8232fd3262ee01ef665ba59a92489b900d8f988b233, 9704e97a395649e9ea4450b3afde5c1f1b22caa05407c4db3ef1625b9db05324, 9f572779dba2ef760f8a2bd7391dcafc099c430bcbd94c7d5247b210e1f095da, abb7541aba5abe1ff27b3867c1d45cea9c678743648ed8eed50bf32f8676e510, af1185876d9d71955e6829f2475c1dce06d33522d0d0e66817d47b9318951314, b66d89ee13a48e9c8d4a7aa2e3e1cb2b79f0b95e4f74f4184b85628656281588, b9906cc6622a11fb67d5ad9db784dc9b62a0da5bd1fd4fe8887f74bfbbfe125d, b9b4375c1992b71f9dc08ee613b2b316b8df8b9e1fdd2c7a1e98d89f43a1625f, bfdb330a8c56def312154c44aed2b36705850adaf6febced8d6d7740beb27715, c0308cc7c56443ad23fbb26671dc8f77d253e873f77c4c3d2486b34317feb417, c4f0b51308eb02c20e9bb33df80442b85b0cc0ad3ccf2598546d67c49242d506,

Attack Name	TYPE	VALUE
TamperedChef	SHA256	cdf51e7f8f24b01bed83da50839b15f143569740c88c2033c43cfc9c17c1b5c8, d162b02a9163fc68ece3db162af0da2c33a595e2258aff171064a5383f41a566, e11aa8dd0b0bc4c21cb081f70565225abc192159f7deb4396aec5720941841ae, f145e61e5d89f51fd3b94fef3e8bc2571aeae4c91c701751e9f603dfd5037dd9, f181501175a30d5fce22af768321cd3de000bba5b19281f39abed236862a3107, f748022beadc73f905f9cd2d5b94be2095265433f6c9770860facda2f6b623c6, fbc7ffc5bdda978afe0f20910210752d91762b97d6d7719a5b3a1e352a4717c3, fde67ba523b2c1e517d679ad4eaf87925c6bbf2f171b9212462dc9a855faa34b, 09207f1dfdd000b42b3433b85d051e8e446a1a1f2f63ab66d47edb9b196f618c, 231ddfa8114475892dd404f27b769ab2e43e9101ec7a7d3608546154a8b75d4d, 255062c602a36f649baaec922cc8b98b27854e8e90b6ee8ded660a2e4e101b77, 37bd388296f6c46e45aa42053758ae17328cfa677ac9ba41ef925d3c8bccfb99, 3c702aa9c7e0f2e6557f3f4ac129afd2ad4cfa2b027d6f4a357c02d4185359c4, 5273bcdeb88ae274294ce71831b63a54ea8b1dd55b4b2222b5eeb0f44150f931, 69b373084e47cbb54a9003ae2435adb49f184bfa11989a2800700da22a153dff, 6e8b48972fab5610363cf4063c289e1670a252fdd40c020de0e3cfcd33c819f4, 7dfa0774992032810660b413836e92f8ac3a4f6de5fa94c5f08c8159c34270e4, 83efb5f2688207a7ccf49ddb81cb094543c2fef5bf73f01342cc39b0af68e72b, 98bb0ab170efdf98414114d6c14a047d2144730f3552bb4aea36198fc49083ac, a3fc5447a9638a3469bab591d6f94ee2bc9c61fc12fd367317eec60f46955859, a696cf7cead8a2219559c802ecc395dcafd2e8f084bfcb8b011c0454519dc5f2, afb0c6b4b0af0a14ac725c025ac70e8b2d8b392094ecdb10e8a2afe2ecf47ea8,

Attack Name	TYPE	VALUE
TamperedChef	SHA256	bcb46bf1c909958a09c52d22ca54dc281357e3c5bdc0f87a6f54553b7c31af9d, c541cfe6baea9c48e44f808977846c2f2a2dab4cfcca677701ceac6d8fc4e1cc, d3b7e26ed39783a6dd8fd107795d4afcf0a28dc5d9da1f4dd54ee905d9fb8f89, da3c6ec20a006ec4b289a90488f824f0f72098a2f5c2d3f37d7a2d4a83b344a0, f97c7edb0d8d9b65bf23df76412b6d2bbfbab6e3614e035789e4e1a30e40b7f1, 847dd2b363fc02d1f501207074eb4eecdff19063cc0cd7adce1572b428f970d8, bb3a744ac6a75e732dea1bd2110bc101205a2d19fdc7fbca82058f287cd61f3b, c6dddeb7286806a99a2f208d094298d7fcaaae3cfba0103f9e0fe02ff6759069, 1bbf0e1323cff3168b548c4a80ec40fd3bed7630dccb7474ba4b8099df5e79d0, 1dcd142daf1116b6a3fac113c638248bf2e0859bb55411cec2256e3d6e9e94ae, 1e351bbae5338f24ce217ac182317ac7a4aee825cbaa5fe55cc347b650d2e987, 216e604948812db2d5062b20504e9acaf271d745da544a2c5d074a5fbf111ac9, 2a3a9ab2ad245d3464b5cc1bc8270568b5c490e4972e99e8f94ab2177874d81a, 2fee5916dad509ff4fea4f4b17795677bda7316253111b2abf7f523bae2a973e, 3ea32c0cb15693383604ac493638e38c43c82946e8fd33825e11d0b8a19d2e60, 41dd100a033fb11430c6f656af92aa97894aa63832171d32dc70c90e8c2733ee, 4de81d968d1c032a49d48d6a67ca282d0b1702167e158b374896f2f04fe3ca83, 645e96594ec5fd50ed2d50fa7de20f33dc15ce4c13aecc5564a051f24770b4bb, a68cb60c61cb31cbe23abe885ca4bd8694e2bd2dcbbd86d12a4fbf6b0cbd0a37, a92b89e5f05393f4844b85681cf5df63b9eb0ca49bb916dd60ed133eb9727bb3, ac1042c8e64165945b0b07972b16d9d6d0235110d9ff0701f889fcc30cfa4859, b3ef2e11c855f4812e64230632f125db5e7da1df3e9e34fdb2f088ebe5e16603,

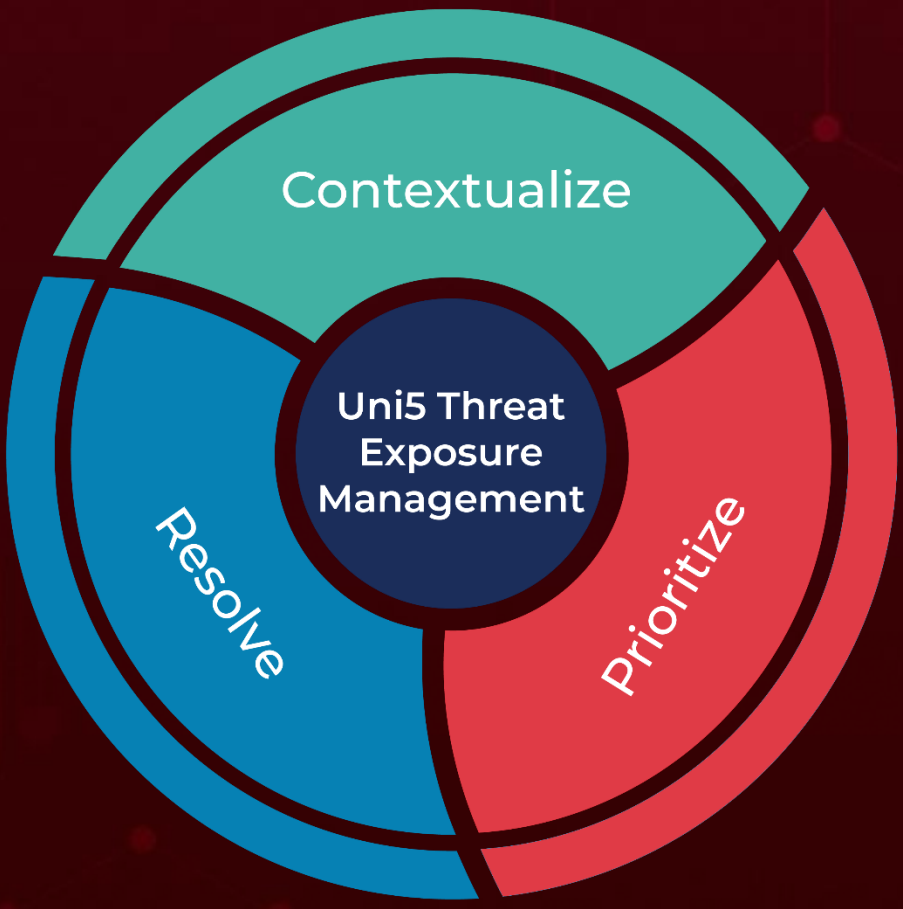
Attack Name	TYPE	VALUE
TamperedChef	SHA256	cc5f29470a11fadf33e39fc0561ae781b1759ff3a314251111356fe51007945e, e954548717c4c538b53ae4cc845cbfe5406b78ede79e4fd509ad2f2dfc4429ab, f3f6d8f2d22040811bd3d06f488cd84f146f3093d6ac79bf68cc522e73c88765, 136836f64f7559868e01db4cbbef9f90f81bdea1278d6605fa13654134279e0c, 6022fd372dca7d6d366d9df894e8313b7f0bd821035dd9fa7c860b14e8c414f2, 9becf480290d3ae7d368d291999c81aa9f47944a90633567e54c4049bcfa3eb4, 2e846b8861d66d9bcaaf9615dc03798cf7f9c3231f2a1d2d31e3e652b954d4f5, b0f8fcb1622eef0a6b398425dd13cbf608771ba2042f32ec3282933a141eec77, 16f854f6399f1c104446d3a3e2d25eb2088bf665186d892903f50ff4ed994181, b8bbf5aecfe0f437758f3f200539e51acfccf5ad9212c20967cfa4037b5a7e0d, 4d986e01e40ebcc495a1c4d98d7ee370b787dbe05da2954c0d8d49c5dcd4b345, ce27671c966d723f45522525fa4dd8912d09cae0f62b893870deb7ee1e7f4e0c, 018ea246585f9def1a14a2690afab6f9e8fcbf1febb6bf9b8463a204a50a5411, 003a69a0a2de87bcfd3982da1068478a8c2828eb07dc24edd93b419eb37d1980, 800a745e7a9f34064b79408aeac2b87515c49e5627dc344124c017ce86f43d3c, 1946d13a16aed7247ed341db933f34b61fc9bb1dcdbd81102c9c54f0ba566851
	Domains	y2iax5[.]com, abf26u[.]com, mka3e8[.]com, 5b7crp[.]com

A comprehensive list of IOCs (Indicators of Compromise) associated with the executed attacks is available on the Uni5Xposure platform.

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**:Threat Exposure Management Platform.



REPORT GENERATED ON

November 24, 2025 . 10:00 PM

More at www.hivepro.com