

## Fix What Matters to Your Business

### Summary of Vulnerabilities & Threats

14 – 20 November 2022

This week witnessed the discovery of 504 vulnerabilities out of which 11 gained the attention of security researchers worldwide. Among these 11, one Zero-day and six vulnerabilities are in RESERVED status on the NVD. Hive Pro Threat Research Team advises organizations to patch this vulnerability as soon as possible.


This week, we also witnessed KmsdBot exploits systems over an SSH connection with insecure login credentials. Batloader compromise via multi-stage infection chain. The BumbleBee leveraged Zerologon to escalate privileges. A novel variant of Typhon stealer. Venus Ransomware targets publicly exposed Remote Desktop services. RapperBot launches DDoS attacks on Game Servers.

Further, we also observed four Threat Actor groups being highly active in the last week. First Billbug, a Chinese threat actor, popular for Information theft and espionage targeted multiple government agencies across Asia. Second FRwL, Russian threat actors, popular for Financial crime targeted Ukraine with Somnia ransomware. Third Lazarus Group North Korean threat actors utilized DTrack Backdoor. Fourth Fox Kitten an Iranian threat actor leveraged Log4j to target the US federal. Common TTPs which could potentially be exploited by these threat actors or CVEs can be found in the detailed section.

Published Vulnerabilities	Interesting Vulnerabilities	Active Threat Groups	Targeted Countries	Targeted Industries	ATT&CK TTPs
504	11	4	65	23	142

# Detailed Report

## ⚙ Interesting Vulnerabilities

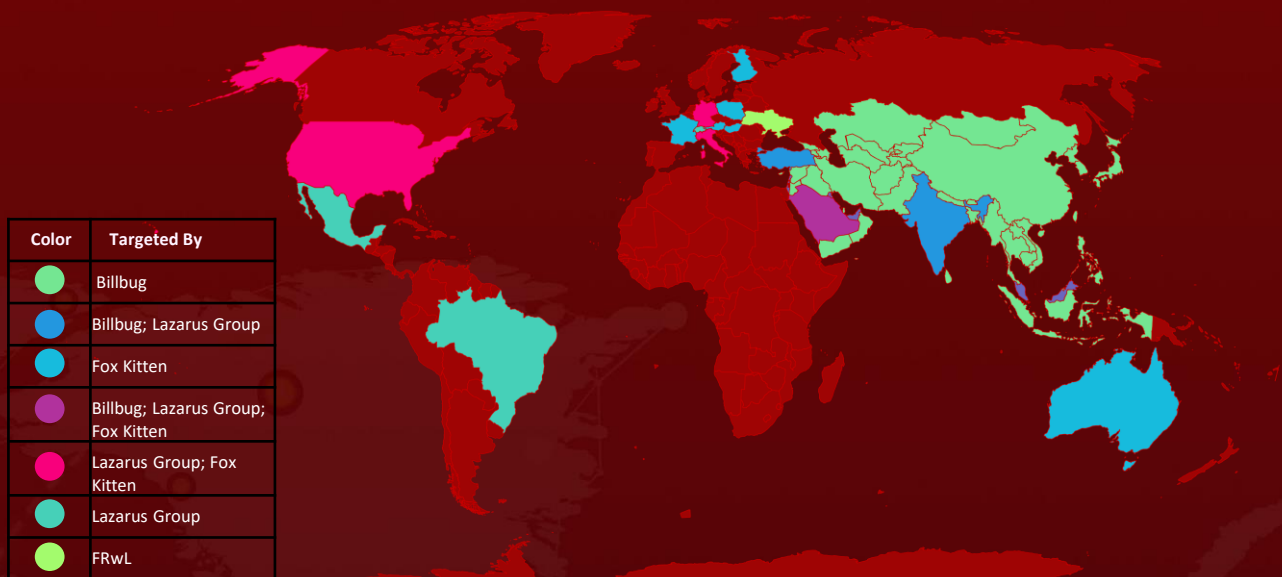
VENDOR	CVE	PATCH LINK
 Microsoft	CVE-2020-1472	<a href="https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472">https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472</a>
 vmware	CVE-2021-44228*	<a href="https://kb.vmware.com/s/article/87073">https://kb.vmware.com/s/article/87073</a> <a href="https://www.vmware.com/security/advisories/VMSA-2021-0028.html">https://www.vmware.com/security/advisories/VMSA-2021-0028.html</a>
	CVE-2022-41622 CVE-2022-41800	<a href="https://support.f5.com/csp/article/K94221585">https://support.f5.com/csp/article/K94221585</a> <a href="https://support.f5.com/csp/article/K13325942">https://support.f5.com/csp/article/K13325942</a>
	CVE-2021-3671 CVE-2019-14870 CVE-2022-3437 CVE-2022-41916 CVE-2022-42898 CVE-2022-44640 CVE-2021-44758	Upgrade to Heimdal version 7.7.1

\* zero-day vulnerability

## 👤 Active Actors

ICON	NAME	ORIGIN	MOTIVE
	Billbug(Lotus Blossom, Spring Dragon, Dragonfish, Thrip, Bronze Elgin, CTG-8171, ATK 1, ATK 78)	China	Information theft and espionage
	FRwL	Russia	Financial crime
	LazarusGroup(Labyrinth Chollima,Group 77, Hastati Group,Whois HackingTeam,New RomanicCyberArmyTeam,Zinc,Hidden Cobra ,Appleworm ,APT-C-26 ,ATK3,SectorA01,ITG0)	North Korea	Information theft and espionage, Sabotage And destruction, Financial crime
	Fox Kitten	Iranian	Information theft and espionage

# Targeted Locations



Powered by Bing  
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

## Targeted Industries





# Common MITRE ATT&CK TTPs

TA0043: Reconnaissance	TA0042: Resource Development	TA0001: Initial Access	TA0002: Execution	TA0003: Persistence	TA0004: Privilege Escalation	TA0005: Defense Evasion
T1590: Gather Victim Network Information	T1584: Compromise Infrastructure	T1078: Valid Accounts	T1047: Windows Management Instrumentation	T1037: Boot or Logon Initialization Scripts	T1037: Boot or Logon Initialization Scripts	T1027: Obfuscated Files or Information
T1595: Active Scanning	T1584.005: Botnet	T1078.001: Default Accounts	T1053: Scheduled Task/Job	T1053: Scheduled Task/Job	T1053.005: Scheduled Task	T1036: Masquerading
	T1587: Develop Capabilities	T1133: External Remote Services	T1053.005: Scheduled Task	T1053.005: Scheduled Task	T1053: Scheduled Task/Job	T1055: Process Injection
	T1587.001: Malware	T1190: Exploit Public-Facing Application	T1059: Command and Scripting Interpreter	T1078: Valid Accounts	T1055.012: Process Hollowing	T1055.012: Process Hollowing
	T1588: Obtain Capabilities	T1195: Supply Chain Compromise	T1059.001: PowerShell	T1078.001: Default Accounts	T1055: Process Injection	T1070: Indicator Removal
			T1059.003: Windows Command Shell	T1098: Account Manipulation	T1068: Exploitation for Privilege Escalation	T1070.004: File Deletion
	T1588.001: Malware	T1566: Phishing		T1133: External Remote Services	T1078: Valid Accounts	T1078.001: Default Accounts
	T1588.006: Vulnerabilities	T1566.002: Spearphishing Link	T1106: Native API	T1136: Create Account	T1078.001: Default Accounts	T1078: Valid Accounts
	T1608: Stage Capabilities		T1129: Shared Modules	T1136.001: Local Account	T1134: Access Token Manipulation	T1112: Modify Registry
	T1608.006: SEO Poisoning		T1203: Exploitation for Client Execution		T1543: Create or Modify System Process	T1134: Access Token Manipulation
			T1204: User Execution	T1136.002: Domain Account		T1140:
				T1543: Create or Modify System Process	T1547: Boot or Logon Autostart Execution	Deobfuscate/Decode Files or Information
			T1204.002: Malicious File		T1547.001: Registry Run Keys / Startup Folder	T1202: Indirect Command Execution
			T1569: System Services	T1547: Boot or Logon Autostart Execution	T1548: Abuse Elevation Control Mechanism	T1218: System Binary Proxy Execution
			T1569.002: Service Execution	T1547.001: Registry Run Keys / Startup Folder		
				T1554: Compromise Client Software Binary	T1548.002: Bypass User Account Control	T1218.011: Rundll32
				T1574: Hijack Execution Flow	T1574: Hijack Execution Flow	T1497: Virtualization/Sandbox Evasion
				T1574.002: DLL Side-Loading	T1574.002: DLL Side-Loading	T1497.001: System Checks
						T1548: Abuse Elevation Control Mechanism
						T1548.002: Bypass User Account Control
						T1550: Use Alternate Authentication Material
						T1550.002: Pass the Hash
						T1553: Subvert Trust Controls
						T1553.004: Install Root Certificate
						T1553.005: Mark-of-the-Web Bypass
						T1562: Impair Defenses
						T1562.001: Disable or Modify Tools
						T1562.004: Disable or Modify System Firewall
						T1564: Hide Artifacts
						T1564.003: Hidden Window
						T1574: Hijack Execution Flow
						T1574.002: DLL Side-Loading

TA0006: Credential Access	TA0007: Discovery	TA0008: Lateral Movement	TA0009: Collection	TA0011: Command and Control	TA0010: Exfiltration	TA0040: Impact
T1003: OS Credential Dumping	T1007: System Service Discovery	T1021: Remote Services	T1005: Data from Local System	T1001: Data Obfuscation	T1041: Exfiltration Over C2 Channel	T1485: Data Destruction
T1003.001: LSASS Memory	T1012: Query Registry	T1021.001: Remote Desktop Protocol	T1056: Input Capture	T1071: Application Layer Protocol	T1567: Exfiltration Over Web Service	T1486: Data Encrypted for Impact
T1003.002: Security Account Manager	T1016.001: Internet Connection Discovery	T1021.002: SMB/Windows Admin Shares	T1056.001: Keylogging	T1071.001: Web Protocols		T1489: Service Stop
T1056: Input Capture	T1016: System Network Configuration Discovery	T1210: Exploitation of Remote Services	T1113: Screen Capture	T1090: Proxy		T1490: Inhibit System Recovery
T1056.001: Keylogging	T1018: Remote System Discovery	T1550: Use Alternate Authentication Material	T1114: Email Collection	T1095: Non-Application Layer Protocol		T1491: Defacement
T1110: Brute Force	T1046: Network Service Discovery	T1550.002: Pass the Hash	T1560: Archive Collected Data	T1102: Web Service		T1499: Endpoint Denial of Service
T1187: Forced Authentication	T1057: Process Discovery	T1570: Lateral Tool Transfer		T1105: Ingress Tool Transfer		
T1528: Steal Application Access Token	T1069: Permission Groups Discovery			T1219: Remote Access Software		
T1539: Steal Web Session Cookie	T1069.002: Domain Groups			T1573: Encrypted Channel		
T1552: Unsecured Credentials	T1082: System Information Discovery			T1573.001: Symmetric Cryptography		
T1555: Credentials from Password Stores	T1083: File and Directory Discovery					
T1555.003: Credentials from Web Browsers	T1087.002: Domain Account					
	T1087: Account Discovery					
	T1120: Peripheral Device Discovery					
	T1124: System Time Discovery					
	T1135: Network Share Discovery					
	T1497: Virtualization/Sandbox Evasion					
	T1497.001: System Checks					
	T1518: Software Discovery					
	T1518.001: Security Software Discovery					
	T1614: System Location Discovery					

# Threat Advisories

<https://www.hivepro.com/frwl-destroys-data-with-somnia-to-disrupt-operations-in-ukraine/>

<https://www.hivepro.com/kmsdbot-cryptominer-targets-the-gaming-industry/>

<https://www.hivepro.com/batloader-evasive-malware-leverages-seo-poisoning/>

<https://www.hivepro.com/bumblebee-leverages-zeroologon-to-get-domain-controller-access/>

<https://www.hivepro.com/billbug-returns-after-two-years-to-conduct-an-espionage-campaign/>

<https://www.hivepro.com/the-dtrack-backdoor-campaigns-aimed-european-organizations/>

<https://www.hivepro.com/typhon-stealer-back-with-new-variant-named-typhon-reborn/>

<https://www.hivepro.com/iranian-hackers-leveraged-log4shell-to-penetrate-us-federal-agency/>

<https://www.hivepro.com/new-venus-ransomware-targets-healthcare-industry/>

<https://www.hivepro.com/rce-flaw-in-f5-big-ip-and-big-ig/>

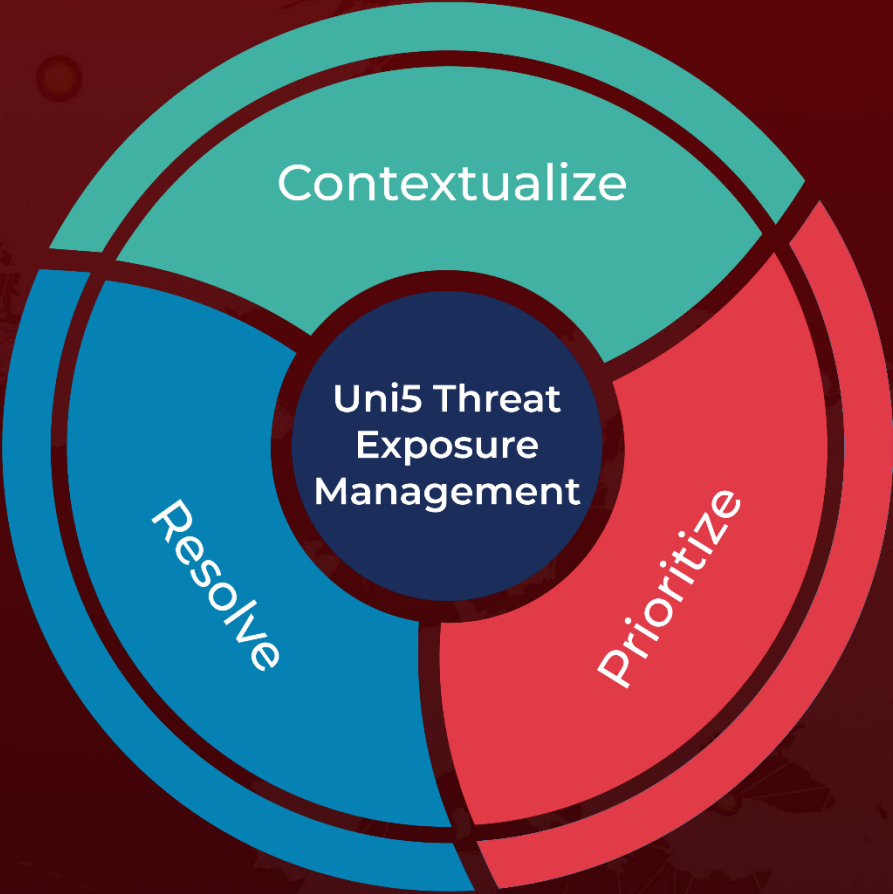
<https://www.hivepro.com/heimdal-addresses-multiple-vulnerabilities-in-v7-7-1/>

<https://www.hivepro.com/rapperbot-campaign-launches-ddos-attacks-on-game-servers/>

# What Next?

At HivePro, 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 Hive Pro Uni5: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 21, 2022 • 2:32 AM

© 2022 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)