Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

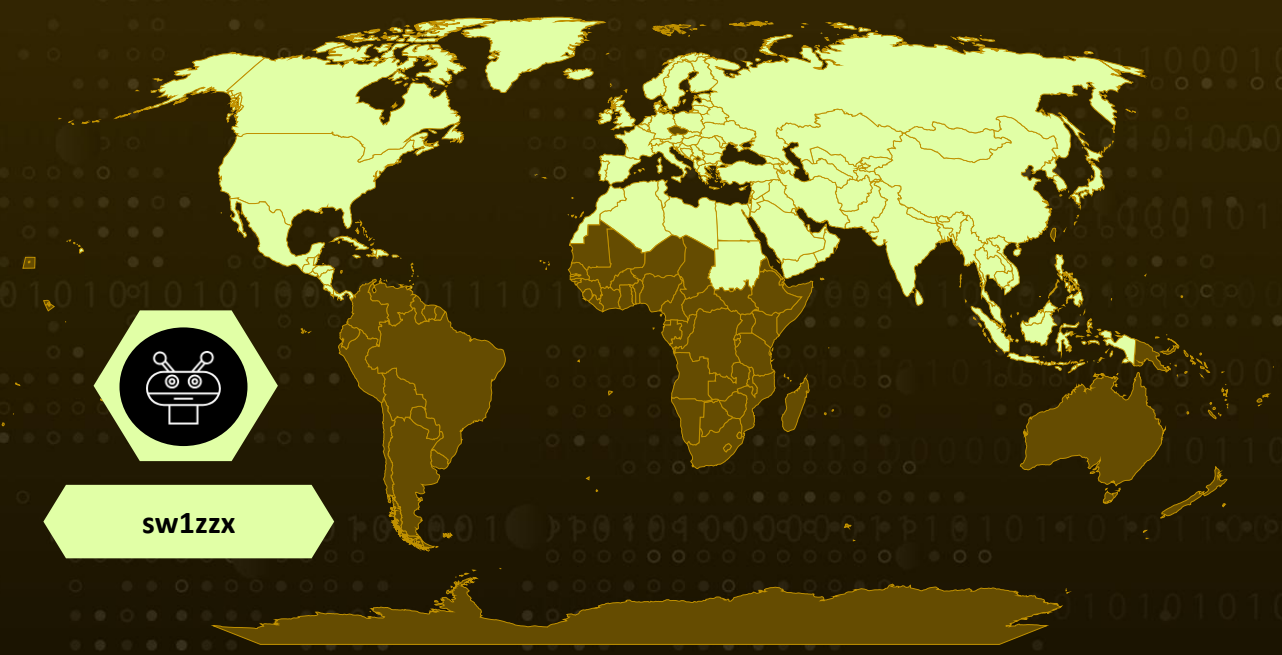
Blitz Malware Exposed: The Dark Side of Free Game Cheats

Date of Publication	Admiralty Code	TA Number
June 10, 2025	A1	TA2025179

Summary

First Seen: 2024
Targeted Region: Europe, Asia, North Africa and North America
Malware: Blitz, XMRig
Affected Platform: Windows
Targeted Industry: Gaming
Treat Actor: sw1zzx
Attack: Blitz is a Windows-based malware first identified in 2024, spread through fake game cheats for Standoff 2 via Telegram. It uses a two-stage infection chain involving a downloader and a multi-functional bot capable of keylogging, DoS attacks, and cryptomining. The malware abuses Hugging Face Spaces for hosting payloads and managing command-and-control operations, enhancing its stealth. Despite the developer's claimed exit in May 2025, Blitz remains a sophisticated example of how legitimate platforms can be misused for cybercrime.

Attack Regions



Attack Details

#1

Blitz is a sophisticated Windows-based malware first observed in 2024 and actively maintained into 2025. It primarily spreads through malicious ZIP archives masquerading as cracked cheat packages for the popular mobile game Standoff 2. These packages are promoted via Telegram by a Russian-speaking actor known as "sw1zzx." When a user runs the compromised executable, it initiates a two-stage infection: the first stage installs a downloader, which then retrieves and executes the main malware payload, the Blitz bot.

#2

The downloader is engineered for stealth and persistence. It checks for internet connectivity and employs anti-sandboxing techniques to evade automated analysis environments. Once active, it downloads the Blitz bot from a Hugging Face Space, a platform typically used for sharing AI models, but here repurposed to host malware. The downloader then injects the bot into a legitimate system process (RuntimeBroker.exe), enabling it to operate covertly.

#3

The Blitz bot functions as a powerful remote access tool with multiple capabilities. It supports keylogging, screenshot capture, file transfer, code injection, and denial-of-service (DoS) attacks. It can also deploy secondary payloads such as the XMRig miner to perform unauthorized Monero cryptocurrency mining. Additionally, the bot collects system metadata, including device GUIDs, usernames, and file paths, which it sends back to the command-and-control (C2) infrastructure.

#4

A distinctive feature of Blitz is its abuse of legitimate cloud services. By hosting payloads and handling C2 communications through Hugging Face Spaces, the attackers increase the malware's resilience and make it harder to detect. This trend, leveraging trusted platforms for malicious operations, reflects broader changes in how modern threat actors operate, blending social engineering with advanced infrastructure evasion.

#5

In May 2025, the malware’s developer announced their supposed exit and released a flawed cleanup tool. Although the tool was intended to remove Blitz, it contained errors and failed to fully clean infected systems. Hugging Face later suspended the actor’s account and removed the malicious content. Despite this takedown, Blitz remains a stark example of how cybercriminals exploit gaming communities and public cloud platforms to distribute advanced, multi-purpose malware.

Recommendations

Avoid Cracked Software and Game Cheats: Never download or run cracked software, cheat tools, or unofficial game modifications—especially from forums or Telegram channels. Educate users, especially younger gamers, about the risks associated with "free cheats" and pirated content.

Implement Robust Endpoint Protection: Use modern endpoint detection and response (EDR) tools with behavioral analysis and sandboxing to detect suspicious activity like process injection or PowerShell abuse. Enable automatic updates and ensure antivirus definitions are current across all devices.

Network and Web Filtering: Implement Advanced URL Filtering and Advanced DNS Security to block access to malicious domains and URLs associated with Blitz and similar malware. Monitor for and block attempts to reach known C2 infrastructure, including abused cloud services like Hugging Face Spaces.

Validate "Cleanup Tools" Carefully: Never trust removal tools distributed by malware authors. Instead, rely on vetted tools from trusted cybersecurity vendors. If infection is suspected, reimage the system or restore from a clean backup after thorough forensic analysis.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0040 Impact	TA0005 Defense Evasion	TA0002 Execution
TA0007 Discovery	TA0011 Command and Control	TA0009 Collection	T1496 Resource Hijacking
T1204 User Execution	T1059.001 PowerShell	T1059 Command and Scripting Interpreter	T1497 Virtualization/Sandbox Evasion

T1204.002 Malicious File	T1547.001 Registry Run Keys / Startup Folder	T1547 Boot or Logon Autostart Execution	T1497.001 System Checks
T1574.001 DLL	T1574 Hijack Execution Flow	T1036 Masquerading	T1071.001 Web Protocols
T1071 Application Layer Protocol	T1082 System Information Discovery	T1056.001 Keylogging	T1056 Input Capture
T1113 Screen Capture	T1499 Endpoint Denial of Service		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	14467edd617486a1a42c6dab287ec4ae21409a5dc8eb46d77b853427b67d16d6, 1bd55796ec712a98cf30fac404b29fcb2cdaa355cb596edcc12d8fbd918b4138, 2007069b32bb9a7f87298fe3c1a87443c21f187ab8465c5b4a1505f0e5c7b898, 3099f41fb60e6f7fe5c1ae2141d4ac5d6f78c763f8cf3e68b2f154cf1a93faa7, 3c77173659b8049b96ca08fc1b8c6122e8d0cfb365920028dc3d18e95cf32ab2, 49b50765749c5e95c2010d790a691689b01e3f844636cd0d47e9fcfe346d7f40, 541a94110a0f9f73722bb9dd7d05b8d1822ad496084d39a777cb39f3b092b6e1, 54f254344ddff0763208c9739bd774d6f467009faa49d47468a8505c0e60dcfc, 6e8f4286ff63acda3a04fca3af7f9fc0962dc84ce889c0b51e5e5768043cbdad, 7dd49c0128aaec33d33a5897cee0b79e91c935f1530993e5c845e35e03d7ed78, 84b654b32b478144d9eec3d923d7e387ec3aed83d7640c32a4d1f5e593750b80,

TYPE	VALUE
SHA256	931b5b2436c1d7f0ab9cfd6202dd18096d94317fdb7b492b63b16b730e2dff24, 9994bb896944e667b1d1536fa64a235501817540bc6c338790d2f46d58b512c1, a2e9b708c7352205b62c2609d1fe43a034f7eb498daf116fb1f85ba2fb01b08b, a8d65fcf7c0f46fd761191b959571a7cc52ae8d0860c79595a28ad2a56d50186, 056fb07672dac83ef61c0b8b5bdc5e9f1776fc1d9c18ef6c3806e8fb545af78c, 1697daef685ce47578e44e2d19fa8e01c755de7fa297716b89e764ea046db1a0, 1d9f12e356367c533ef756ab74d70fc537a580ec5ab904a4d583cebe0b89b4c4, 23086a1d207166154a1b1451f3174f7c5f5299dd4385d83fd8199833ce34325f, 27d074c6cfb079be8d087a0efa0ec24994972d1033fb4c72a2b479790cb3bb31, 2a279f345126141019fe836cea88f61e5b0449487a5a411bac53ad8273a3eac1, 2e543a246f3390bd3f9102af275e4a57f2c057bedad10079f5d2402ad9bd6421, 3064b4dd3e2c44c986f2c247a888c530b855db8fd7dd6d345cf187d873792fc7, 35696115cfd23a6d128da932be20a784f2a82ff411eca99c2c33bb2d1bd4026c, 39d8a45108ab3ec5b56aca989f268c434957fa1dc160d0fe654cf0d5910bf4ce, 3aaaab12ad5cc2571bf935ab248419c535577220571f76f84a37db5623956da9, 3f85d0c73ec6c8e45a24df14759f351aaf456d1eab3afbacc1d8ed95bb062a7b, 450e33d866848c10ed3493bb1edf0a95084b8d69b963fb0aa72ba8d27c3110ab, 46f11cbba1fea180d03b5ac2b68070cbbfa515131957db1d0551209220f7f045, 4f8031cabbc1f5b7574dbde4a251f8cb15ea8b0f7c151bdbb301dd017fedc944, 5ca0bc0b16b2107048b804936b8d52f90e3ba3a6bf7916732541cd1b3b6f962f, 5d30045ce82f6e2431d6fd4dccb3ffd565820617d92763993dbbf4ddb9dde938, 67b3b8b8c63e2fa103143efc67536c0fe6a58f9e004e362c3df686951f59e2e0,

TYPE	VALUE
SHA256	688754743476df47e612190ef790105efab8c611a5b5e2cbecb3c6b764bb9dd7, 7b4aa0351f8fb71f0e1ccedc6998fc06945f1a77c7fb15f3448eaa483190a111, 7dc8f1ab3638fb64b809078856ac7500a1b8aa1bcf6bc74e88af59b7e3a31407, 839b2b72fc672549e7daefc08d28e74768d0b2b2b12662b799f46340e8bccf80, 83fc11bebb07f59cc86e2fd4c80936ecc6d1e0a21978ba1a9b09d3639f64844d, 84a1d2bfe9bba6387e3752978aec1c0871fecf7844e23b72e4d6a046f58f4692, 995740e8cf0b6c44b1e3dbd1e983f3fdaa2dac6bd6db399efabd957794cf3954, 99598079794e4ff65a641828e1403b75362a7f732db4c938b9ded25f789d1793, 9a5b4a4770c6d26fcd06dd53fc68dc5ee739fd5ed52530e80b5dfd4314dcbc6d, 9c802ce1c678791b23a04027997d6cfa4ba1b2f0d54d9fb1051d870f05c2a746, b1d7fb16f057318c1f0727a46df7ad755361311ba22eddd1f5d397ef0e648c42, b3bfa58ca38918d97ead9a0f7f799b08fbc082f9f844ef765c3acda4711b2888, b43451cb80a77e30b4db51b371ad410e22a8921cd015cb4362dcdecd7a0fadce, b8c37133dc58e4f46efcac7254dee28c6cca6c9627d0d6ab0741fbce370996c2, bbaa7bdd67822be567c1ed749c1ea42322bb1b9bc06470977597c7bf385f5aad, c0309ce6f86c5e83d18422a045367f7f9148b8b013093113bf08de4a262c1ee7, c3520f7fc3452106ce43f17ea7db90d72c7ffed28a0d9431c84900cfdc08cfa7, c6161b8f85c15f2a88f1dcb5204161ce7c294aa408cba11dabf57a016d8d548f, d7d98f3427bf7fa0f936472e9abaedfc38ea3e1a83a6c3bddec55b177b70e743, fa0d069156d4913607fed8321ff5f7f4758a51e9ece2d00ccade8cb2e40e3374, 6a55b7b01a8f7001e0e654f5feddcd0561b3694bcd2a9f9ca3e5f5e33dbbfc11, 8ed77eb6cd203e20b467d308bf7ee5213cbb2c055c4896b0af04e323bf67b887,

TYPE	VALUE
SHA256	ce1940eb26f0609fc25aaecbf998d01f5a7d5420c91bfe5c4b710d057981850c, 0e80fe5636336b70b1775e94aaa219e6aa27fcf700f90f8a5dd73a22c898d646, cacc1f36b3817e8b48fabbb4b4bd9d2f1949585c2f5170e3d2d04211861ef2ac, aa5cd0219e8a0bd2e7d6c073f611102d718387750198bff564c20ca7ebada309, f3b7bbe1079974fd505abaadbcf4dc0517620592eacbbe5f314a76775dd760c2, cdf192e92d14b9d7e1201c23621c4e0b8ee0673c192bdd734afd97519afef271, 6441e7000713f96c7ae114ce62378556d01fa29d435a5be0f11a5e80be9a26ed, b1b1ce259fcf5127c3477e278c3696dc7d15db63b673fdcf75e1deb89a0f6fd1, 5ef29d6d4f72e62e0d5a1d0b85eed70b729cd530c8cb2745c66a25f5b5c7299e, 5fc132b054099a1a65f377a3a22b003a6507107f3095371b44dbf5e098b02295, b18e21e50f1c346c83c4cba933b6466ada22febaafa25c03ac01122a12164375, a34a4a7c71de2d4ec4baf56fd143d27eeedebb785a2ba3e0740b92e62efd81ea, bedeafd3680cad581a619fb58aa4f57ed991c4a8dd94df46ef9cbd08a8dd6052, ae2f4c49f73f6d88b193a46cd22551bb31183ae6ee79d84be010d6acf9f2ee57, 88e2d0d59a9751e4ce5223951f5a75b1731b1ee82d18705aba83ba4bd7e8e5c1, 47ce55095e1f1f97307782dc4903934f66beec3476a45d85e33e48d63e1f2e15, abcc59ab11b6828ad76a4064d928b9d627a574848a5a6e060b22cb27cd11b015, 7891bb5a4656469ada072f0081c5149251b9ad49dfcf64bdb02704edaa73548a, b795cbacd5bf60399a3885e69dc7b2cbc75e8ddae01cee15e3c9fe1a3f953aa9, c53f86ca9dba6930087b564a9588ecd3a1073b8886bbca387484bef937fb1598, 2abb14bdf0f7f159c90183679729361102f0b46e5207a36c3f292adf7d0b1dd3, 1b80f8a985027aac004ef89caf9daa2ebbec7eece4ee442270e1d417092b88ef, 7d082878c654ffdea32f15e258aae09d5375932499411b61e3b9189a2c906504,

TYPE	VALUE
URLs	hxxp[://]huggingface[.]co/spaces/e445a00fffe335d6dac0ac0fe0a5accc/9591beae439b860a9cf93b26b2dc97e0, hxxp[://]huggingface[.]co/spaces/e445a00fffe335d6dac0ac0fe0a5accc/2c5dd233ee36705a817b323471be2fe5, hxxp[://]huggingface[.]co/spaces/swizxx/blitz[.]net, hxxp[://]pastebin[.]com/raw/FSziK5eW, hxxp[://]pastebin[.]com/raw/RzLEd17Z, hxxp[://]paste[.]rs/ABNe6, hxxp[://]files[.]catbox[.]moe/tmcbms[.]dll, hxxp[://]files[.]catbox[.]moe/5byj86, hxxp[://]t[.]me/sw1zzx_dev
Domains	e445a00fffe335d6dac0ac0fe0a5accc-9591beae439b860-b5c7747[.]hf[.]space, swizxx-blitz-net[.]hf[.]space
Telegram Channel	t[.]me/sw1zzx_dev

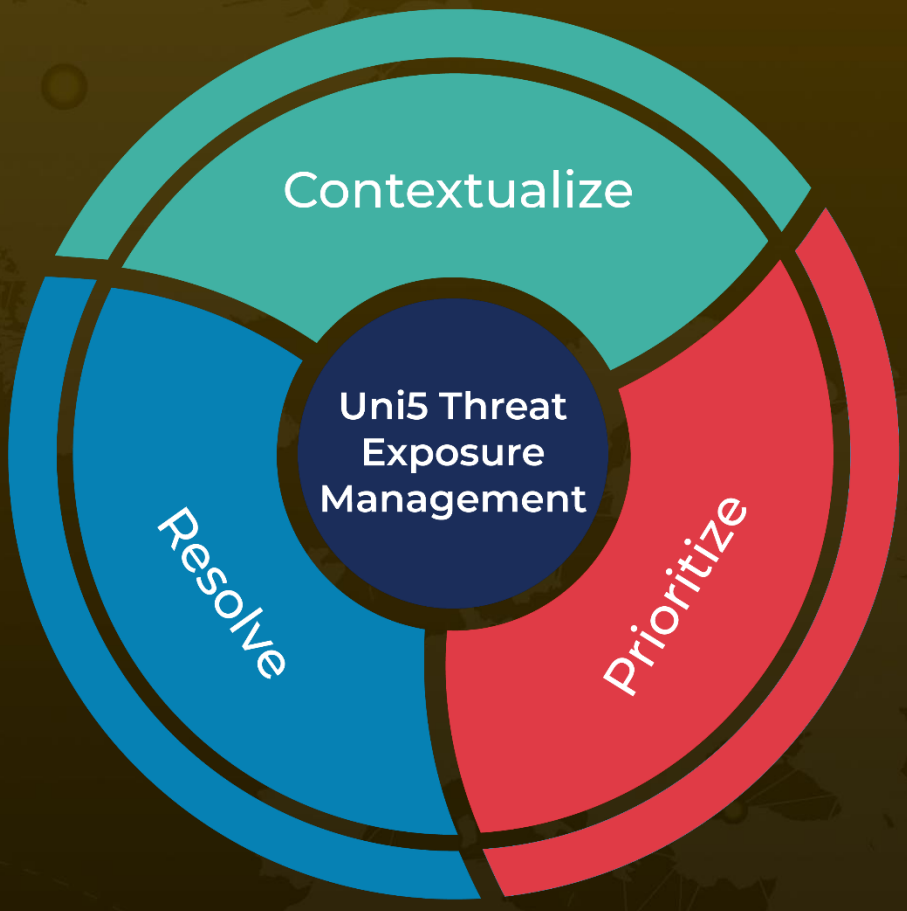
References

https://unit42.paloaltonetworks.com/blitz-malware-2025/

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

June 10, 2025 • 3:30 AM

More at www.hivepro.com