Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

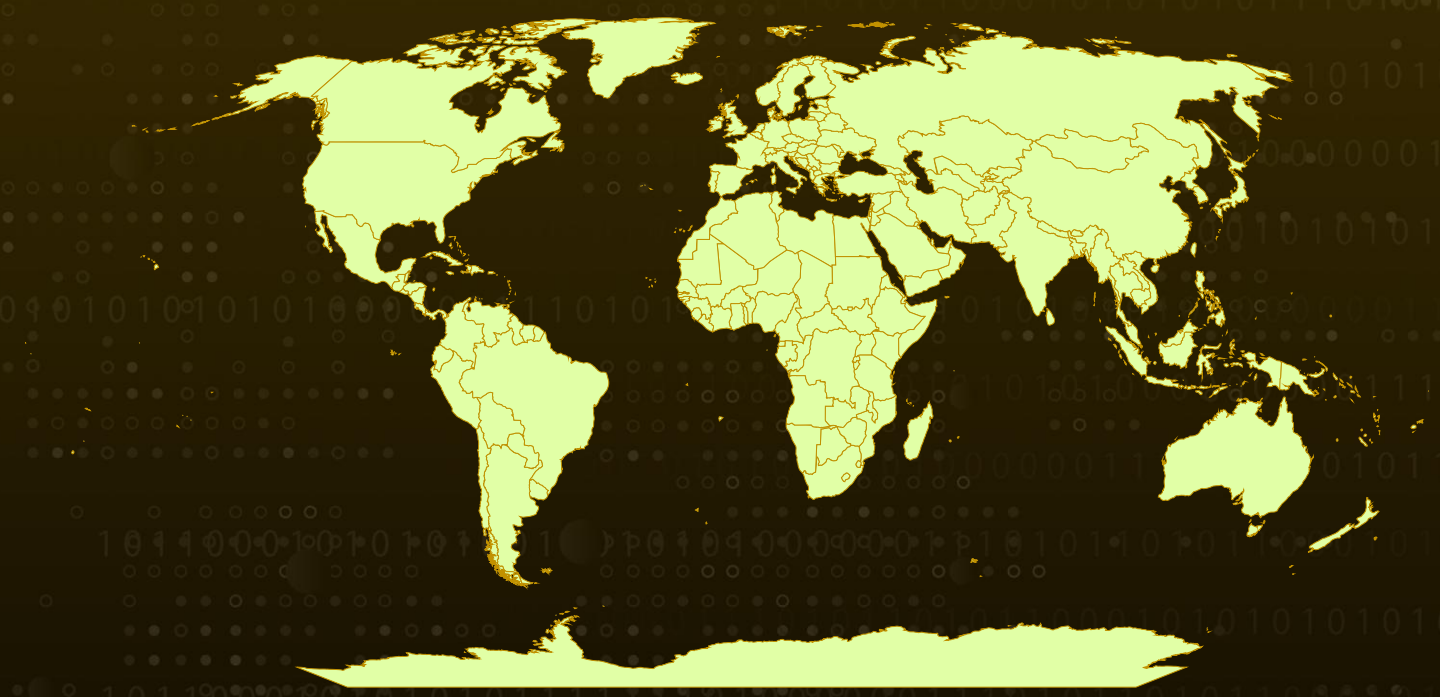
StaryDobry Campaign: Trojanized Games Fuel a Global Cybercrime Wave

Date of Publication	Admiralty Code	TA Number
February 19, 2025	A1	TA2025049

Summary

Attack Discovered: December 31, 2024
Targeted Country: Worldwide
Targeted Industries: Gaming
Campaign Name: StaryDobry
Malware: XMRig cryptominer
Attack: A large-scale malware campaign, dubbed "StaryDobry," has been spreading trojanized versions of cracked games to unsuspecting gamers worldwide. Games such as Garry's Mod, BeamNG.drive, and Dyson Sphere Program have been weaponized to distribute the XMRig cryptominer, impacting both individual users and businesses. This previously unidentified threat actor has been actively targeting users across multiple countries, including Russia, Brazil, Germany, Belarus, and Kazakhstan. By leveraging torrent sites as the primary distribution channel, the attackers have been able to infect a wide range of victims looking for pirated software. Once installed, the cryptominer covertly hijacks system resources to mine cryptocurrency, degrading performance while generating illicit profits for the attackers.

Attack Regions



Attack Details

#1 Cybercriminals executed a large-scale malware campaign, infecting thousands of systems worldwide. The attack, which lasted a month, relied on trojanized versions of popular games distributed via torrent sites. By employing advanced evasion techniques, the attackers bypassed security defenses, allowing the malware to spread undetected. At its core, the campaign deployed a modified **XMRig** cryptominer, hijacking victims' CPU and GPU resources to mine cryptocurrency, significantly degrading system performance.

#2 The infection wave peaked on December 31, 2024, when compromised game installers flooded torrent trackers. However, this was a calculated operation—threat actors had preloaded these malicious repacks as early as September 2024. They specifically targeted lightweight simulator and sandbox games, ensuring a broad reach among users.

#3 The malware activates when a victim launches what appears to be a legitimate 32-bit Windows game installer. Instead of delivering the expected game, it triggers a multi-stage attack designed to evade detection and establish persistence. It first extracts its malicious payload and performs environment checks to detect debugging or virtualized setups, attempting to thwart security researchers. To further obscure its presence, the malware registers unrar.dll as a command handler using regsvr32.exe and queries the victim's IP address to determine their location. If this check fails, it defaults the region to China (CN) or Belarus (BY), likely as a misdirection tactic.

#4 Once these checks are complete, the malware contacts a hardcoded command-and-control (C2) server, enabling attackers to issue commands and update the payload. To uniquely identify each infected system, it generates a Base64-encoded fingerprint using MachineGUID from the Windows registry, encrypts it using SHA-256, and stores it in a decoy file to mislead security tools.

#5 At this stage, unrar.dll delivers the final payload, MTX64.exe, encrypted with AES-128. To blend in, the malware spoofs system resources, embedding legitimate DLL properties and modifying timestamps to avoid detection. Once executed, it masquerades as a Windows Shell Extension Thumbnail Handler, using the GetThumbnail function to launch a hidden execution thread.

#6 For persistence, the malware continuously verifies its presence by checking the hashed MachineGUID. It also listens for JSON-formatted commands from its C2 server. If specific codes (322 or 200) are received, the malware extracts an MD5 checksum, downloads the next-stage payload, verifies its integrity, decrypts it, and stores it for execution. To automate the attack, it creates a scheduled task using Windows Task Scheduler.

#7 The StaryDobry campaign highlights the growing threat of malware-laced pirated software. By embedding malicious code into game installers, cybercriminals have compromised thousands of systems worldwide. As torrent sites remain a key vector for malware distribution, users must exercise caution, while organizations should strengthen their defenses with network monitoring, endpoint detection, and PowerShell logging to mitigate such threats.

Recommendations

Use Licensed Software: Avoid pirated or unlicensed software, as it poses significant security risks. Cybercriminals frequently embed malware in such tools, making them a common attack vector. To ensure system integrity and security, always obtain software from official and trusted sources.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Monitor and Restrict Network Traffic: Continuously analyze outbound connections to identify potential communication with malicious command-and-control (C2) servers. Implement DNS filtering and block access to known harmful domains to prevent unauthorized data exfiltration.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0011 Command and Control	T1190 Exploit Public-Facing Application

T1053 Scheduled Task/Job	**T1053.005** Scheduled Task	**T1033** System Owner/User Discovery	**T1036** Masquerading
T1036.005 Match Legitimate Name or Location	**T1204** User Execution	**T1204.002** Malicious File	**T1497** Virtualization/Sandbox Evasion
T1497.001 System Checks	**T1553** Subvert Trust Controls	**T1553.002** Code Signing	**T1082** System Information Discovery
T1140 Deobfuscate/Decode Files or Information	**T1055** Process Injection	**T1016** System Network Configuration Discovery	**T1083** File and Directory Discovery
T1057 Process Discovery	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1027** Obfuscated Files or Information
T1012 Query Registry	**T1059** Command and Scripting Interpreter	**T1059.003** Windows Command Shell	**T1070** Indicator Removal
T1070.004 File Deletion	**T1027.002** Software Packing	**T1068** Exploitation for Privilege Escalation	**T1218** System Binary Proxy Execution
T1218.010 Regsvr32			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	15c0396687d4ff36657e0aa680d8ba42, 461a0e74321706f5c99b0e92548a1986, 821d29d3140dfd67fc9d1858f685e2ac, 3c4d0a4dfd53e278b3683679e0656276, 04b881d0a17b3a0b34cbdbf00ac19aa2, 5cac1df1b9477e40992f4ee3cc2b06ed
URLs	hxxps[:]//promouno[.]shop, hxxps[:]//pinokino[.]fun

TYPE	VALUE
SHA256	E60EF7DE4D1E27944469CE534B113B6D49DDD266FEBBA5FC8D02E77A3B6D5B08, 12B63E6DE43867516A20188FBA9A8F0B2BEE59FC9993B1C94CBAB4E688C46CBE, 4BD38E72049F7FE4D9F8BDBF96A41DFE4FE5596B77151510DC8EA0CCD2A1114F, 81C53ABCD10471C8CB8E41CD5693AC0319650CC945832853DC49C629EECC8448, C5A73E3AD1FC43C04B344F81507CAFBA731122AD01960495DA5D088F7E956F41, E4A0ACDC73B1504FAB0D68A8A59D7F409220B1A2AD5DC75E8163286667A4FEA9
IPv4	45[.]200[.]149[.]58, 45[.]200[.]149[.]146, 45[.]200[.]149[.]148

References

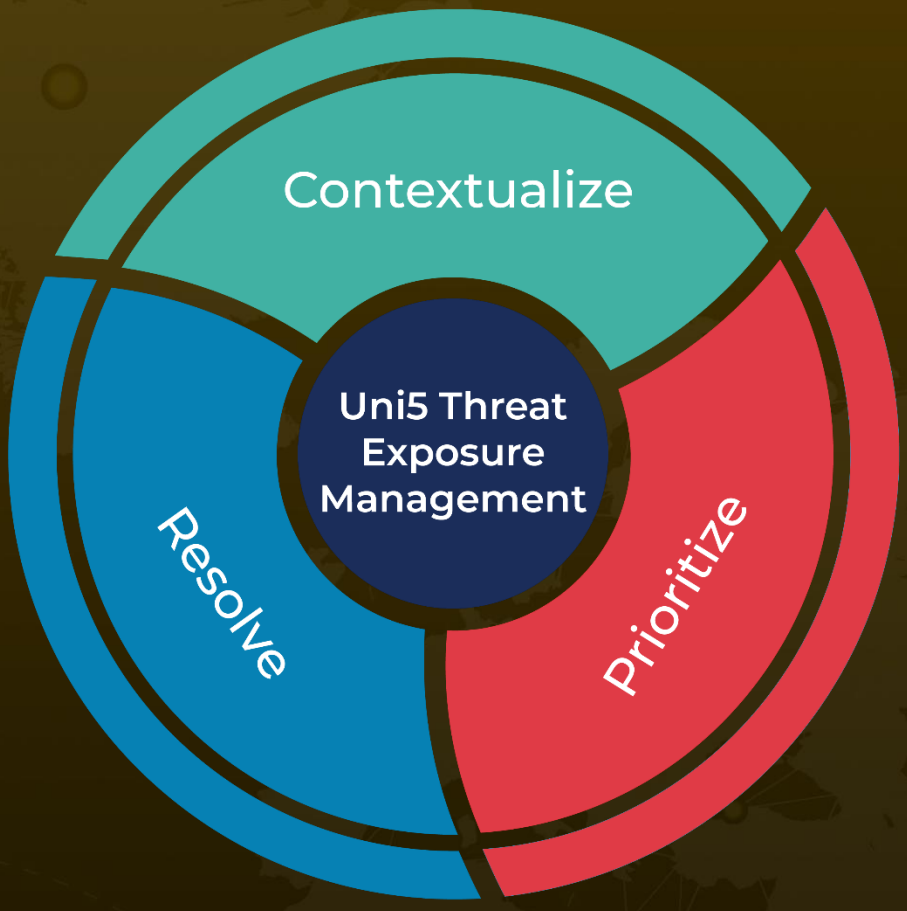
https://securelist.com/starydobry-campaign-spreads-xmrig-miner-via-torrents/115509/

https://www.hivepro.com/threat-advisory/sysrv-harnessing-google-subdomains-to-circulate-xmrig/

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

February 19, 2025 • 5:00 AM

More at www.hivepro.com