

Xillen Stealer v5 Advanced Credential Theft and Loader Platform

 cybersecsentinel.com/xillen-stealer-v5-advanced-credential-theft-and-loader-platform

Cybersec Sentinel

November 24, 2025



Threat Group – Xillen Killers

Threat Type – Information stealer and loader operating under a Malware as a Service model

Exploited Vulnerabilities – Social engineering and opportunistic scanning for unpatched versions of Cisco AnyConnect, OpenVPN, FortiClient and Pulse Secure in order to access cached credentials

Malware Used – Xillen Stealer version five using a Python core with a Rust based polymorphic engine

Threat Score – **7.5 High** . This score reflects the confirmed presence of the AIEvasionEngine and AITargetDetection modules and the use of steganography and NTFS Alternate Data Stream staging which significantly increases the risk of undetected enterprise compromise

Last Threat Observation – 24 November 2025

Overview

Xillen Stealer version five represents a major escalation within the world of commodity information stealing malware. Early versions of this threat family operated as simple Python based stealers with predictable behaviour and minimal obfuscation. These earlier builds attempted to harvest

browser passwords and cryptocurrency wallets before transmitting them to a simple command and control endpoint. Their use was common in low sophistication criminal campaigns and their detection was relatively easy for modern endpoint security systems.

This is no longer the case. The fifth release of Xillen Stealer does not resemble a traditional commodity infostealer. Instead it has transformed into a modular, flexible and highly evasive platform that combines Python based orchestration with a powerful Rust compiled polymorphic engine. This engine modifies the structure of each payload at build time and produces a unique binary for every user. This significantly reduces the effectiveness of signature based antivirus approaches.

The group responsible for the development and distribution of this malware is known as the Xillen Killers. This community operates in large Telegram channels and has an approximate membership of three thousand individuals. The identified lead developer uses the alias Beng or jaminButton. They present themselves as a penetration testing specialist and claim to build the stealer as a research tool. However the behaviour of their Telegram ecosystem and the capabilities included in the builder strongly indicate that they are enabling widespread criminal misuse.

The architecture of version five introduces several advanced capabilities that are usually reserved for targeted malware. The most significant additions are the AIEvasionEngine and the AITargetDetection module. These components allow the malware to detect the value of a compromised environment and adapt its behaviour in order to avoid detection by artificial intelligence based endpoint security solutions.

The inclusion of steganography, Alternate Data Stream staging and polyglot file structures further enhances its stealth. The use of public cloud services for exfiltration and the ease with which attackers can modify payloads transforms Xillen Stealer version five into a serious enterprise threat.

This advisory provides a detailed analysis of the threat, its capabilities, its behaviour and the required mitigation actions.

Key Details

Delivery Method

Xillen Stealer version five is distributed through multiple channels that begin with social engineering. Threat actors offer cracked versions of software, game modifications, driver packages and productivity utilities. These are often distributed through Telegram groups, underground marketplaces and deceptive download pages. When a user runs one of these installers the payload executes silently and initiates reconnaissance.

The builder created by the Xillen Killers group allows attackers to produce custom versions of the malware within minutes. The builder includes templates for installers, update prompts, fake debugging tools, browser extensions and portable executables. This ensures that attackers can match the disguise to their campaign.

Although the primary method of infection continues to be user execution, version five includes opportunistic exploitation capabilities that were not present in earlier variants. The malware checks for installed versions of Cisco AnyConnect, OpenVPN, FortiClient and Pulse Secure. These products are widely used by enterprise workers and store cached credentials. Older unpatched versions contain weaknesses that allow stored passwords to be extracted. If Xillen Stealer detects one of these clients it attempts to harvest the cached secrets which can be used to move directly into enterprise networks.

This behaviour increases the overall risk of the malware since a personal device compromise can escalate to an organisational breach.

Target

Xillen Stealer version five does not collect data randomly. Earlier variants simply harvested all browser credentials and personal data. The current version includes logic for high value target identification. The AITargetDetection module examines the environment for contextual clues. These include the presence of cloud management tools, container orchestration utilities, programming languages, version control systems and administrative tools.

It also checks for specific keywords in file paths, cached browser sessions and user profile metadata. These keywords include references to senior positions, investment groups, financial accounts and privileged roles. Although some functions are dormant in this release the intent is clear. The malware is expanding towards targeted enterprise data theft.

The main targets of Xillen Stealer version five include

- Browser stored passwords
- Credential manager vaults
- Cryptocurrency wallets across more than seventy supported formats
- Kubernetes configuration files
- Docker config files and access tokens
- Cloud platform access keys and environment variables
- SSH keys and development environment credentials
- Messaging platform tokens including Slack and Discord
- Personal and corporate email tokens
- Password manager master vaults when auto unlock is enabled

Developer environments appear to receive special treatment. The stealer checks for cloud CLI tools and for container orchestration secrets. These secrets can unlock entire clusters if not properly secured.

Functions

Version five introduces an extensive list of malicious functions. The most important functions include the following.

- Collection of browser credentials from Chrome, Firefox, Edge and other Chromium based browsers
- Collection of session cookies for high value websites including cloud platforms
- Extraction of cryptocurrency wallet files and seed phrases
- Extraction of cloud keys stored in environment variable files
- Harvesting of AWS, GCP and Azure CLI configuration files
- Collection of Kubernetes config files and secret files
- Extraction of Docker credential stores
- Harvesting of password vault content when auto unlock is active
- Modification of Discord and Slack JavaScript files in order to inject token listeners
- Use of steganography to embed stolen data into image files
- Use of Alternate Data Streams to store hidden collected data on disk
- Deployment of secondary payloads through loader functionality
- Creation of polyglot image archive files to disguise exfiltration
- Use of the AITargetDetection module to increase targeting accuracy
- Use of the AIEvasionEngine module to produce statistical noise and disrupt detection

The loader capabilities are of particular concern. Xillen Stealer version five can download additional payloads after completing the theft of initial data. These may include backdoors or ransomware preparation tools.

Obfuscation

The malware uses a combination of evasion and obfuscation techniques that are designed to defeat both user awareness and advanced security tools.

The Rust based polymorphic engine rearranges code structures, replaces instructions, encrypts strings and modifies control flow. This ensures that each payload generated through the builder is unique. Traditional antivirus solutions struggle with this type of polymorphism.

The AIEvasionEngine produces artificial resource usage in order to confuse behavioural detection models. These models often look for consistent patterns of entropy, CPU cycles and memory access. By creating random noise the malware breaks these patterns.

The use of steganography allows the malware to hide data inside image files. These files appear normal to the user and to most scanning tools. The use of Alternate Data Streams further masks the presence of stolen information.

Polyglot files combine legitimate image headers with appended archive data. This allows exfiltration of large payloads through channels that appear to contain harmless media files.

The malware also includes anti analysis features. It checks for virtual machine environments, common forensic tools and sandboxing behaviour. If detection occurs the malware alters its behaviour or terminates.

Attack Vectors

The attack begins with execution of the malicious payload. After running, the malware performs a detailed scan of the system. It checks user directories for cloud configuration files and identifies where session tokens are stored. It determines which applications are installed and whether the user relies on cloud tooling.

Xillen Stealer then collects the data and stores it temporarily in an ADS or within a steganographic container. This data may remain on the system for up to several minutes before exfiltration begins.

The primary exfiltration method is the Telegram sendDocument function. The malware packages the stolen data into zip files or disguised image files and sends them directly through encrypted Telegram API calls. If Telegram is blocked the malware attempts uploads to public cloud buckets on AWS or GCP. These domains are heavily used within enterprise environments and therefore blend into normal traffic.

After exfiltration the malware may deploy additional tools if instructed to do so. These payloads extend the attack surface and may initiate persistence or ransomware preparation.

Indicators of Compromise

The following indicators represent behavioural and contextual evidence of Xillen Stealer version five activity. All items are fully defanged.

Behavioural and Network Indicators Table

Indicator Type	Value or Pattern	Description
Network C2	<code>api[.]telegram[.]org/bot<token removed>/sendDocument</code>	High frequency POST requests carrying zip or jpg content that contains staged data
Network Exfiltration	<code>*.amazonaws[.]com</code> and <code>*.googleapis[.]com</code>	Unexpected POST requests containing Base sixty four encoded JSON data
File Artefact	<code>\Stream:\$DATA</code> ADS entries in <code>C:\Users\<user>\AppData\Local\Temp\</code> or <code>C:\Users\<user>\AppData\Roaming\</code>	Hidden Alternate Data Stream content attached to seemingly harmless files
File System Marker	<code>AITargetDetection.pyc</code> and <code>AIEvasionEngine.pyc</code>	Evidence of internal module files exposed through memory dumps or partially packed binaries
Registry Persistence	<code>HKCU\Software\Microsoft\Windows\CurrentVersion\Run</code> with random eight character entries	Persistence using names such as <code>Xy8z1aB.exe</code>
Author Metadata	<code>Beng/jaminButton</code> as a defanged PDB string	Identifies the developer within builder produced artefacts
Application Tampering	Modified Discord or Slack JavaScript files such as <code>index[.]js</code>	Token listeners injected into messaging platforms
Cloud Credential Access	Commands referencing <code>~/.aws/credentials</code> or <code>~/.kube/config</code>	Evidence of cloud key harvesting

Indicator Type	Value or Pattern	Description
Behaviour	Hidden PowerShell commands such as <code>powershell[.]exe - WindowStyle Hidden</code>	Attempts to extract environment variables and configuration files

Mitigation and Prevention

This section outlines the recommended defences and controls needed to reduce the risk of compromise.

Mitigation Checklist for Gap Analysis

- Patch all endpoints especially those running older versions of VPN clients
- Restrict execution of Python and Rust compiled binaries from user profile directories
- Enforce the separation of cloud credentials from local development environments
- Use endpoint detection systems that focus on behavioural analysis
- Block Telegram at the network boundary unless required
- Monitor outbound traffic for unexpected JSON uploads from user devices
- Enforce hardware token based two factor authentication
- Rotate cloud keys regularly and reduce reliance on static secrets
- Conduct DLP style checks on messaging platform directories
- Audit developer workstations for Kubernetes and Docker secrets
- Scan for Alternate Data Streams on a routine schedule
- Teach users to avoid cracked software and suspicious installers

User Awareness

Users must be reminded that the malware often appears in trusted formats. They should avoid downloading unofficial software. They must also understand that token theft can occur without visible prompts.

Email Filtering

Ensure that email systems block executable attachments and use sandboxing. Quarantine emails that reference updates, driver packs or urgent account messages.

Antivirus Protection

Modern behavioural antivirus systems must be used. The antivirus must track access to credential stores, cloud config files and unexpected CPU spikes.

Two Factor Authentication

Hardware tokens must be used for sensitive systems. Software based tokens or SMS based two factor methods are vulnerable due to the malware's ability to collect TOTP seeds.

Log Monitoring

Logs should be configured to detect access to browser credential stores, changes to messaging client JavaScript files, creation of ADS entries and calls to cloud APIs from user devices.

Regular Updates

Maintain regular update cycles. Keep an active inventory of developer tools. Ensure that cloud keys are rotated and that developer machines do not store sensitive cluster secrets.

Risk Assessment

Xillen Stealer version five must be considered a high severity enterprise threat. Its artificial intelligence aware evasion functions, its ability to harvest cloud and container secrets and its capacity to deploy additional payloads show that it is far beyond a simple infostealer.

The threat group behind it maintains active development. Each update expands the functionality. The use of a Rust based polymorphic engine removes the reliability of traditional defences. The presence of targeted data theft modules indicates that the malware will continue to evolve into a more selective and more damaging tool.

Organisations that rely heavily on cloud systems or development platforms are at significant risk. The theft of a single Kubernetes config file can result in cluster compromise. The theft of cloud environment files can grant access to production environments. The risk of financial crime, data exposure, identity compromise and ransomware escalation must be treated as critical concerns.

Failure to take immediate defensive action exposes organisations to silent credential loss followed by long term access by malicious actors.

Engineer Technical Addendum

This section provides actionable detection and response items for security engineers and SOC teams.

Hunting for Artificial Noise

The AIEvasionEngine creates rapid process churn and micro bursts of resource use. Correlate this activity with outbound traffic to defanged Telegram endpoints. Investigate any python.exe or unnamed executables that access browser profile paths.

Alternate Data Stream Detection

Use PowerShell scanning across high value endpoints to identify hidden streams. ADS entries in Temp and AppData directories must be considered high risk.

YARA Memory Detection Rule

Memory scanning is essential since disk based detection is ineffective. Use the rule below in EDR tools that support memory inspection.

```
rule Xillen_v5_Memory_Indicator {
meta:
  description = "Detects Xillen v5 Python modules in memory"
  author = "Threat Intelligence Team"
  date = "2025-11-24"
  threat_level = "High"
strings:
  $s1 = "AITargetDetection"
  $s2 = "AIEvasionEngine"
  $s3 = "Beng/jaminButton" nocase
  $s4 = "wallet.dat"
  $s5 = "/.kube/config"
condition:
  2 of ($s1, $s2, $s3) or ($s1 and ($s4 or $s5))
}
```

Network Filtering

Blocking Telegram eliminates the primary exfiltration channel. Cloud bucket uploads must be inspected for Base sixty four encoded data. Monitor for JSON uploads from workstations that do not normally interact with cloud APIs.

Conclusion

Xillen Stealer version five is a sophisticated and actively developed information stealer that now operates at the level of a fully capable enterprise threat. Its technical features, its integration of machine learning evasion techniques and its targeted cloud and developer data harvesting elevate its risk well above that of earlier commodity malware families.

To protect against this malware organisations must deploy strong behavioural detection, secure all cloud credentials, restrict developer tool placement, inspect messaging platform files, block known exfiltration channels and maintain an active threat monitoring program.

Immediate action is required in order to reduce the risk of credential loss, cloud compromise and major operational disruption.

Sources

Darktrace Intelligence – Xillen Stealer Updates to Version Five to Evade AI Detection –

<https://www.darktrace.com/blog/xillen-stealer-updates-to-version-5-to-evade-ai-detection>

SecurityOnline – Xillen Stealer New Opensource Malware Lowers Cybercrime Barrier –

<https://securityonline.info/xillenstealer-new-open-source-malware-lowers-cybercrime-barrier>



[Threat Group – Crimeware cluster similar to UNC5142 access brokers and web compromise crews using Matrix Push C2](#) [Threat Type – Browser based C2 platform, phishing delivery system and malware loader sold as a MaaS service](#) [Exploited Vulnerabilities – Abuse of W3C Push API, Service Workers, notification prompts, clipboard and Run dialog through](#)



[Threat Group – UNC2565 \(also tracked as Storm-0494\)](#) [Threat Type – Malware Loader and Initial Access Platform](#) [Exploited Vulnerabilities – No specific CVE confirmed. Campaign relies on SEO poisoning, compromised WordPress sites, archive format inconsistencies, Windows Script Host](#)

[execution, and legacy filename behaviour. Malware Used – GootLoader, GootBot, secondary payloads such as Cobalt Strike](#)



[Threat Group – Unknown actor likely a financially motivated Malware as a Service operator Threat Type – Remote Access Trojan and Malware as a Service Exploited Vulnerabilities – No specific CVEs publicly linked at time of writing. Built in UAC bypass and a Local Vulnerability Scanner enable dynamic post infection exploitation Malware Used Cybersec Sentinel © 2025](#)