SECURITY ADVISORY

CYBER STASH

May, 2025

Silent, Modular, Dangerous: The Rise of StealC v2

Context

StealC v2 marks a significant advancement in the evolution of modern information-stealing malware, now operating as both a stealer and a loader—engineered for stealth, modularity, and operational precision. First observed in early 2023 as a browser-focused credential harvester, StealC has rapidly evolved into a highly adaptable tool leveraged by cybercriminals across diverse campaigns.

The latest version introduces notable enhancements, including advanced anti-analysis techniques, dynamic configuration logic, and staged data exfiltration routines. Its streamlined communication with command-and-control (C2) infrastructure enables fine-grained tasking, conditional payload delivery, and phased exfiltration—dramatically increasing its evasiveness and complexity in live environments.

Critically, StealC v2 can delay activation of its stealer functionality based on real-time C2 commands, allowing attackers to execute operations only when predefined conditions are met. This on-demand behavior, coupled with its support for post-exfiltration payload deployment, makes StealC v2 exceptionally difficult to detect using conventional signature- or behavior-based security mechanisms.

Mitigation

Defending against the StealC V2 requires proactive measures.

Targeted Defense Against StealC v2: By focusing on behaviors uniquely associated with StealC v2—often missed by Microsoft Defender and mainstream EDR tools—organizations can detect the malware's stealthy, tailored tactics that evade traditional IOC-based methods.

The **Recommendations section on page 4** outlines prioritized preventive and detective controls designed to disrupt StealC v2's attack chain with minimal impact on operations, strengthening overall cyber defense.

Technical Details

The Key tactics that differentiate StealC V2 updated campaign include:

1. Initial Communication

StealC v2 begins execution on the victim system. It sends a create request to its Command-and-Control (C2) server to register the victim with the C2 and requests configuration, including:

- Hardware ID (HWID)
- Build parameters

2. C2 Response with Access Token

The C2 server responds with:

- access_token
- Configuration flags (notably the loader flag)
- Operational parameters

Loader flag determines whether StealC immediately deploys additional payloads.

3. Information Exfiltration

- StealC collects system data (e.g., `system_info.txt`) and sends it via an `upload_file` request.
- C2 confirms with `opcode: success`, acknowledging receipt of stolen data.

4. Conditional Execution Logic

If the `loader` flag is set to:

- `0`: Loader functionality is deferred until after exfiltration.
- `1`: Loader functionality is triggered **immediately**, and StealC enters payload execution phase early.

5. Data Exfiltration Loop

- StealC enters a loop of exfiltrating additional victim data.
- Sends repeated exfil requests.
- C2 responds with `opcode: success` for each valid transfer.

6. Termination and Loader Engagement

- StealC sends a `done` request to signal end of data collection.
- C2 acknowledges and StealC then sends a `loader` request.

7. Payload Deployment

C2 may respond with:

- Empty list of payloads (indicating no further action)
- List of payload URLs for download and execution.
- StealC then downloads and executes these payloads (often additional malware, tools, or scripts).

8. Exit

- Once execution is complete or if the loader flag is disabled and payload list is empty, the malware exits cleanly to evade further detection.

StealC v2 represents a highly structured and stealth-oriented evolution of info-stealing malware. Its modular architecture and command-driven control flow enable precise execution of both data exfiltration and malware-loading operations. Together, these features make StealC v2 a silent but potent threat capable of long-lived intrusions, targeted exfiltration, and on-demand malware staging—requiring equally adaptive and behaviour-focused defences.

Recommendations

StealC V2—Specific Behavioural Indicators to Monitor

#	Behaviour to Monitor or Restrict	Why It's Unique to StealC v2	Recommended Action
1	Structured C2 Request Types with Tags Like type: create, type: upload_file, type: done, and type: loader	Most malware uses generic or obfuscated request patterns. StealC v2 uses predictable, plain-text indicators within the HTTP body or URI that map to its operational stages.	Inspect outbound HTTP/S for POST/GET traffic containing these specific request patterns. Add custom signatures to detect these markers in decrypted payloads or proxy logs.
2	Conditional Invocation of Loader Functionality Based on Remote 'loader' Flag	StealC v2 includes logic to defer loader activation until explicitly triggered by C2, enabling "silent mode" persistence before a secondary payload. This is uncommon in commodity loaders.	Correlate timeline of malware activity: flag cases where C2 communication occurs significantly before payload download. Monitor for processes exhibiting a dormant phase followed by suspicious child process creation.
3	Retroactive Stealing Triggered via C2 Post-Exfiltration	Unlike typical stealers that collect data immediately upon execution, StealC can trigger retroactive data theft after receiving C2 instructions, even if initial collection was skipped.	Track processes that upload minimal system data initially, but later initiate aggressive data harvesting routines after server interaction. This behavioural shift is subtle but rare.
4	Highly Regular, Loop-Based Data Exfiltration with opcode: success Response Handling	Rather than bulk exfiltration, StealC v2 uses a structured loop for chunked data uploads, confirming receipt with opcode: success. This tactic mimics reliability-layer protocols but is rare in low-tier malware.	Detect custom exfiltration loops where small, sequential POST requests are followed by uniform response codes. High-frequency, low-volume, successful POSTs from non-browser processes are a strong signal.
5	Delayed Loader Request Issued Only After 'type: done' Marker	StealC strictly follows its own internal state machine—issuing a loader request only after data exfiltration is complete. This disciplined flow control is uncommon in other stealers/loaders.	Profile HTTP sequences and build logic to detect this specific sequence: upload_file → done → loader. Trigger alerts if this flow occurs outside normal application behaviour.
6	Payload-Download Decision Logic Based on Empty vs Non-Empty JSON List in Loader Response	The use of an empty payload list as a deliberate C2 response is a unique stealth mechanism—often leading defenders to overlook later stages if nothing is downloaded.	Detect and log all C2 responses to loader requests, even if they result in "empty" lists. Flag this interaction as suspicious if the originating process had earlier upload activity.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to StealC V2 attack :

Step	Description	Tactic	Technique & ID
1	Initial beaconing – StealC V2 initiates communication by sending HWID and build parameters to the C2 server (type: create).	Command and Control	Application Layer Protocol (T1071.001)
2	C2 setup response – Server replies with access_token, loader flag, and configuration settings to guide further actions.	Command and Control	Web Protocols (T1071.001)
3	System profiling – Victim host sends collected data (e.g., system_info.txt) to the C2 server (type: upload_file).	Discovery / Collection	System Information Discovery (T1082)
4	Data acknowledgment – C2 server confirms receipt of exfiltrated data with opcode suc-	Exfiltration	Exfiltration Over C2 Channel (T1041)
5	Continuous data theft – StealC V2 enters a loop, repeatedly sending additional data while receiving success replies from C2.	Exfiltration	Automated Exfiltration (T1020)
6	Termination of exfiltration – An end message (done) is sent when data theft completes.	Exfiltration	Exfiltration Over C2 Channel (T1041)
7	Payload loader request – Malware sends a loader request to C2 asking for follow-on pay-	Command and Control	Remote File Copy (T1105)
8	Loader response – C2 responds with either: a) no payloads, or b) URLs to fetch additional payloads.	Execution Command and Control	Malicious File Execution (T1059) User Execution (T1204.002)
9	Conditional execution logic – Based on loader flag value, payload execution occurs immediately (flag = 1) or exits (flag = 0).	Execution	Conditional Execution (T1622)
10	Post-exfiltration stealing – If loader flag = 1, stealer functionality (e.g., credential theft) is triggered retroactively.	Credential Access Collection	Input Capture (T1056) Data from Information Repositories (T1213)

Cyber Threat Intelligence

Threat Actor Attribution

StealC is attributed to a developer operating under the alias **"Plymouth"**, who has been active on Russian-speaking underground forums since January 2023. Plymouth markets StealC as a Malware-as-a-Service (MaaS) offering, emphasizing its modularity and non-resident design. The malware's development draws heavily from established infostealers like Vidar, Raccoon, Mars, and RedLine, suggesting a deliberate strategy to amalgamate proven techniques into a single, flexible platform. While Plymouth is the primary developer, StealC's distribution is decentralized, with multiple cybercriminal groups leveraging it for various campaigns. This widespread adoption complicates precise attribution but underscores its popularity within the cybercriminal ecosystem.

Motivation and Targeting

StealC is primarily financially motivated, designed to harvest a broad spectrum of sensitive data, including:

- Browser-stored credentials
- Email client data (e.g., Outlook)
- Cryptocurrency wallet information
- Messaging application data (e.g., Telegram, Discord)

Notably, StealC v2 has been linked to campaigns targeting:

- Financial institutions managing corporate banking accounts
- Retail businesses with extensive customer loyalty databases
- Technology firms storing API tokens and authentication secrets

Infrastructure and Delivery Mechanisms

StealC's infrastructure is characterized by:

- Command-and-Control (C2) Servers: Predominantly hosted on Russian-based servers, facilitating communication with infected hosts.
- Pyramid C2 Framework: Utilized for post-exploitation activities, indicating a layered approach to command and control.
- Malvertising Campaigns: Employed to distribute the malware, often redirecting users to malicious downloads.
- Impersonation Tactics: Instances of threat actors posing as legitimate organizations (e.g., the Electronic Frontier Foundation) to deceive targets.

Monetization and Dark Web Presence

StealC operates under a subscription-based MaaS model, with access priced between $200–$500 per month. This pricing strategy makes it accessible to a wide range of cybercriminals, from low-tier actors to more organized groups.

The malware's continuous development, including regular updates and feature enhancements, ensures it remains effective against evolving security measures, thereby maintaining its appeal in underground markets.

References

IOCs:

45[.]93[.]20[.]64	91[.]92[.]46[.]133	91[.]211[.]250[.]177	198[.]251[.]84[.]107
85[.]192[.]49[.]87	194[.]55[.]137[.]8	147[.]45[.]44[.]116	213[.]21[.]237[.]183
62[.]113[.]118[.]58	5[.]253[.]30[.]7	91[.]220[.]8[.]107	45[.]141[.]233[.]86
185[.]87[.]48[.]173	116[.]202[.]216[.]170	62[.]60[.]226[.]114	85[.]208[.]119[.]2
89[.]110[.]116[.]81	62[.]60[.]226[.]20	77[.]90[.]153[.]241	157[.]180[.]8[.]71
2[.]56[.]166[.]193	176[.]65[.]142[.]44	176[.]65[.]142[.]47	179[.]43[.]180[.]186
85[.]192[.]48[.]188	83[.]229[.]17[.]68	83[.]217[.]208[.]133	161[.]97[.]75[.]178
91[.]92[.]46[.]177	185[.]106[.]176[.]178	81[.]19[.]131[.]77	85[.]158[.]108[.]135
83[.]147[.]216[.]49	185[.]170[.]154[.]143	147[.]45[.]44[.]173	185[.]102[.]115[.]17
213[.]21[.]237[.]173	104[.]245[.]241[.]70		

Public Intelligence:

- https://www.bleepingcomputer.com/news/security/stealc-malware-enhanced-with-stealth-upgrades-and-data-theft-tools/
- https://trac-labs.com/autopsy-of-a-failed-stealer-stealc-v2-a4e32da04396
- https://dailysecurityreview.com/security-spotlight/stealc-malware-upgraded-with-advanced-data-theft-and-stealth-capabilities/