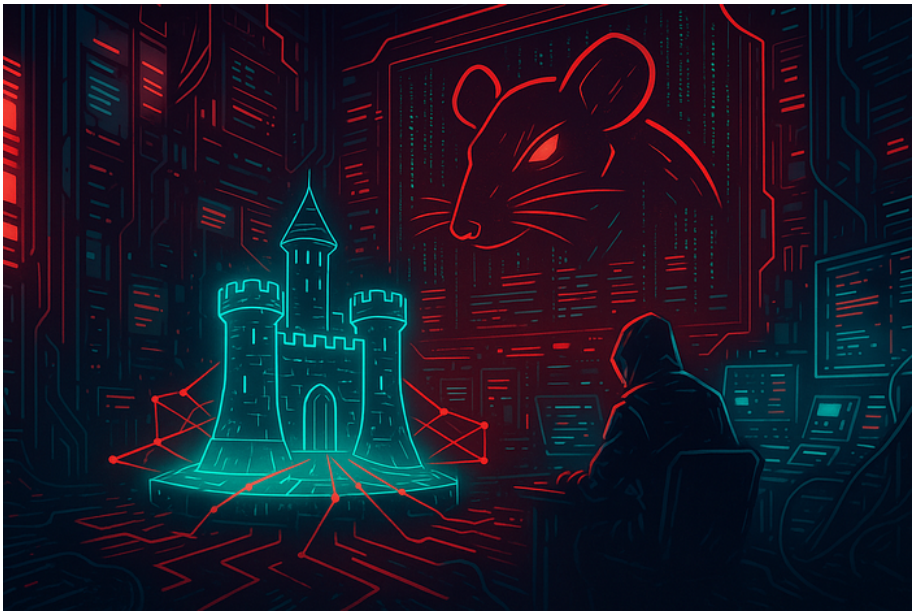
CastleRAT: TAG-150's New Remote Access Trojan (September 2025)

Deniz Topaloglu ⋮ ⋮ 9/12/2025



Modular Malware and Multi-Stage Intrusions

Executive Summary

In September 2025, researchers documented a new remote access trojan named CastleRAT, linked to the financially motivated threat actor TAG-150. CastleRAT is not a standalone tool but part of a broader ecosystem including CastleLoader, WarmCookie, and Stealc. The RAT has been observed in both Python and C variants, with a supporting infrastructure that uses multi-tier VPS servers, decoy domains, and dead-drop channels on legitimate services such as Steam Community pages.

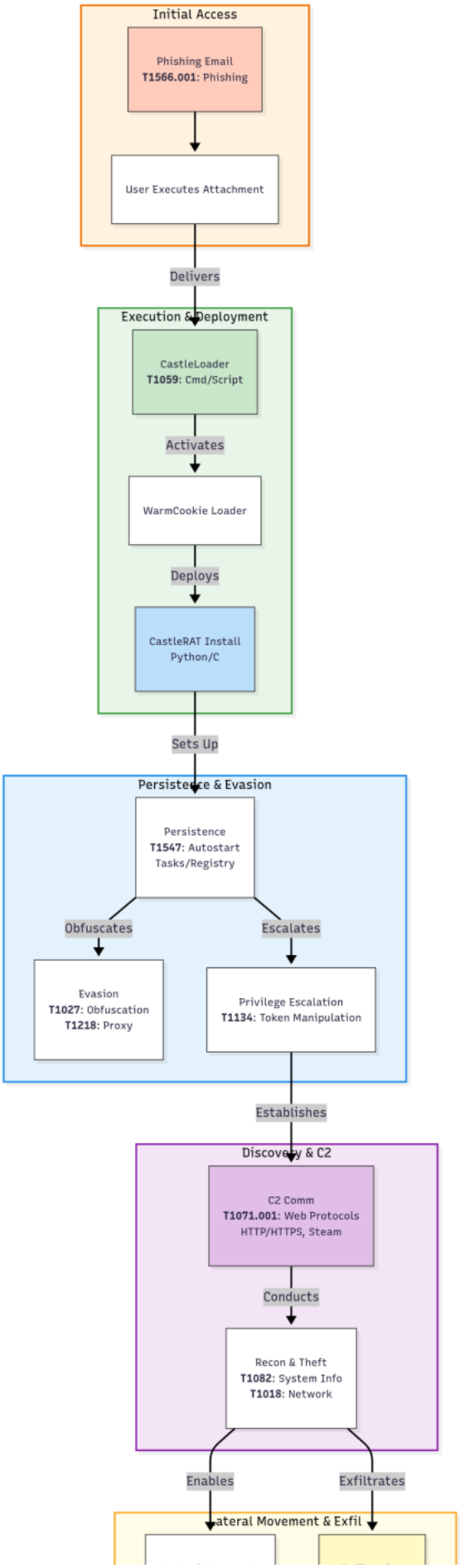
CastleRAT's discovery highlights the growing professionalization of mid-tier threat actors who increasingly operate with modular infrastructures that blend loaders, stealers, and RATs.

Technical Analysis

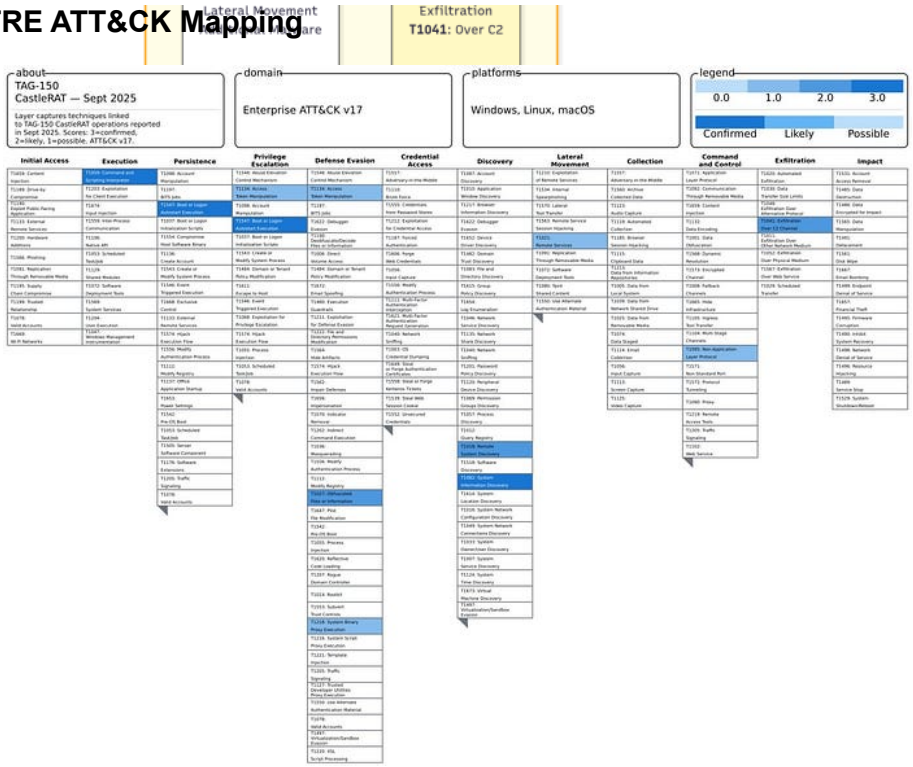
Capabilities

- Remote command execution and process control
- File manipulation and data exfiltration
- System and network reconnaissance
- Persistence through scheduled tasks or registry keys
- Encrypted C2 communication over HTTPS or custom TCP channels

Execution Flow


Initial Access
Phishing Email
T1566.001: Phishing
User Executes Attachment
Delivers
Execution & Deployment
CastleLoader
T1059: Cmd/Script
Activates
WarmCookie Loader
Deploys
CastleRAT Install
Python/C
Sets Up
Persistence & Evasion
Persistence
T1547: Autostart
Tasks/Registry
Obfuscates
Escalates
Evasion
T1027: Obfuscation
T1218: Proxy
Privilege Escalation
T1134: Token Manipulation
Establishes
Discovery & C2
C2 Comm
T1071.001: Web Protocols
HTTP/HTTPS, Steam
Conducts
Recon & Theft
T1082: System Info
T1018: Network
Enables
Exfiltrates
ateral Movement & Exfil

MITRE ATT&CK Mapping



- Initial Access

- Execution

– and → execution through

- Persistence

T1547 – Boot Logon Autostart → Scheduled tasks, registry

- Defense Evasion

T1027 – Obfuscated Files → Payload obfuscation packing

T1218 – Signed Binary Proxy Execution → Suspected in some CastleRAT deployments

- Discovery

T1082 – System Information Discovery → Collects host

T1018 – Remote System Discovery → Enumerates networked systems

- Privilege Escalation

– → plausible the campaign

- Lateral Movement

– → movement post-foothold

- Command & Control

T1071 – Web → C2 traffic over decoy domains

T1095 – Non-Standard Port → Observed high-number TCP ports

- Exfiltration

T1041 – Exfiltration C2 Channel → Data sent through existing C2 channels

Indicators of Compromise

Domains

```
panelv1hostingzealofttoday

castlepanel[.]workers[.]camserviceload[.]net
```

IP Addresses

.

```
104.21.42[.]73172.67.154[.]215
```

- File Hashes (SHA256)

```
9a41e2c4df46c7e3f0b73c26e6e4b6f14a4d9d4ef78d0c7cfb14e92e3b5c90a8

d21f6a3e3562d0c4d8a728f8b9c7fa37b6e6e712ff4ac4c37b08432c4a1f98bdf53c2c1a1cb60a0de91f87f21380d3bbd925bff3f
```

- Mutex / Process Artifacts

```
 \CastleMutex123

Process names: setup64.exe, updatehelper.exe
```

- Ports

```
 /  (HTTP/S)

7777 (custom TCP)
```

Threat Hunting Queries and Detection Rules

DNS & Proxy Query (Monitors for C2 domains and ports):

```
indexdns OR indexproxy search  IN , ,  OR dest_port IN , ,  stats count by src_ip, ,
dest_port eval domaincoalesce, dest_domain table src_ip, domain, dest_port, count
```

Endpoint & Sysmon Query (Detects suspicious processes with context):

```
indexendpoint  indexsysmon  process_name  ("setup64.exe", "updatehelper.exe")
parent_process_name  ("msiexec.exe", "cmd.exe", "powershell.exe")
CommandLine"*Global\\CastleMutex123*" stats (parent_process_name) (CommandLine)  host,
process_name  host, process_name, parent_process_name, CommandLine
```

Elastic EQL Queries

Get Deniz Topaloglu’s stories in your inbox

Join Medium for free to get updates from this writer.

Process Query (Detects suspicious processes with parent and mutex context):

```
process where process.name   and  (process.parent.name   or   process.command_line : )
```

Network Query (Detects C2 domains and ports):

```
network where destination.domain   or destination.port
```

Sigma Rules

CastleRAT Suspicious Process Execution (Detects process creation with parent and mutex filters)

```
 CastleRAT Suspicious Process Execution b05c3f2-f38-c3b-a872-castlerat-proc
experimental Detects CastleRAT-related process execution  context  category:
process_creation  product: windows  selection:    Image|endswith:      -       -
ParentImage|endswith:      -       -       -   mutex:    CommandLine|contains:
condition: selection  mutex  - Image  - ParentImage  - CommandLine medium  -
attack.execution  - attack.t1059  - malware.castlerat
```

CastleRAT Known C2 Domains (Detects DNS queries to confirmed C2 domains):

```
 CastleRAT Known C2 Domains a9cb43d-c12-da-a187-castlerat-dns experimental Detects DNS
queries  CastleRAT C2 domains  category: dns  selection:    query:      -       -
-   condition: selection  - query  - client_ip  - destination_port medium  -
attack.command_and_control  - attack.t1071.  - malware.castlerat
```

YARA Rule

CastleRAT Binary Detection (Detects binaries with confirmed domains and behavioral strings)

```
rule {    meta:        description          author          date          reference
strings:           wide ascii           wide ascii           wide ascii
ascii           ascii           ascii           ascii             ascii
condition:        uint16()   and           of (, , , , , , , )}
```

Defensive Recommendations

- Monitor for DNS queries to hostingzealoft[.]today and related infrastructure.
- Block outbound traffic on uncommon high-numbered ports (e.g. 7777).
- Deploy EDR detections for suspicious processes such as updatehelper.exe.
- Hunt for mutex CastleMutex123 in memory analysis.
- Inspect network telemetry for encrypted HTTPS traffic toward unknown VPS nodes.
- Track potential abuse of Steam Community or other legitimate platforms as dead-drop channels.

Conclusion

CastleRAT is not simply another RAT. It is part of an integrated, modular campaign framework that demonstrates how actors like TAG-150 blur the line between traditional cybercrime and advanced intrusion sets. Defenders should treat CastleRAT infections as a strong precursor to secondary payloads, lateral movement, and possible extortion. Proactive hunting, continuous monitoring, and contextual threat intelligence integration remain the most effective defenses.

Works Cited

“From CastleLoader to CastleRAT: TAG-150 Advances Operations.” Recorded Future, Sept. 2025, https://www.recordedfuture.com/research/from-castleloader-to-castlerat-tag-150-advances-operations.

“ChillyHell macOS Backdoor and ZynorRAT Uncovered.” The Hacker News, Sept. 2025, https://thehackernews.com/2025/09/chillyhell-macos-backdoor-and-zynorrat.html.