

MALWARE ANALYSIS REPORT

Evidence ID: MAL-2024-11-01

Source: Endpoint File Scan / Behaviour Analysis

Status: Player-facing

[2024-11-14 23:41:08] MALWARE_ANALYSIS_STARTED

Target File: BoosterMod_v2.exe

[2024-11-14 23:41:09] FILE_HASH_CALCULATED

SHA256: a3f9c1...

[2024-11-14 23:41:11] DETECTION_RESULT

Verdict: MALICIOUS

Classification: Infostealer.TokenGrabber

Risk Level: HIGH

[2024-11-14 23:41:14] BEHAVIOUR_ANALYSIS

Observed Behaviour: Reads browser cookie storage

Observed Behaviour: Searches for saved session tokens

Observed Behaviour: Extracts tokens matching ".ROBLOSECURITY"

Observed Behaviour: Extracts tokens matching "dcfduid"

[2024-11-14 23:41:18] NETWORK_ACTIVITY

Connection Type: HTTP POST

Destination IP: 185.220.xx.xx

Data Type: Extracted session token data

Status: Outbound transfer detected

[2024-11-14 23:41:21] DOWNLOAD_HISTORY_CHECK

Downloaded By: Alex Mercer

Download Date: 2024-11-01

Time Before Breach: 13 days

[2024-11-14 23:41:24] AUTHENTICATION_IMPACT

Login Alert Generated: NO

2FA Challenge Triggered: NO

Reason: Attacker used a valid stolen session token instead of a normal password login.

[2024-11-14 23:41:27] ANALYSIS_SUMMARY

The file BoosterMod_v2.exe appears to be a fake game booster or mod tool. After execution, it accessed browser cookie storage and extracted session tokens linked to gaming and chat accounts. The stolen token could allow an attacker to access Alex's account without triggering a normal password login or 2FA prompt.

[2024-11-14 23:41:30] FINAL_ASSESSMENT

Classification: CONFIRMED MALWARE

Likely Purpose: Session hijacking / Account takeover

Related Incident: Unusual login from Tallinn and later spam campaign

Recommended Evidence Link: Compare with account login log and phishing domain evidence.