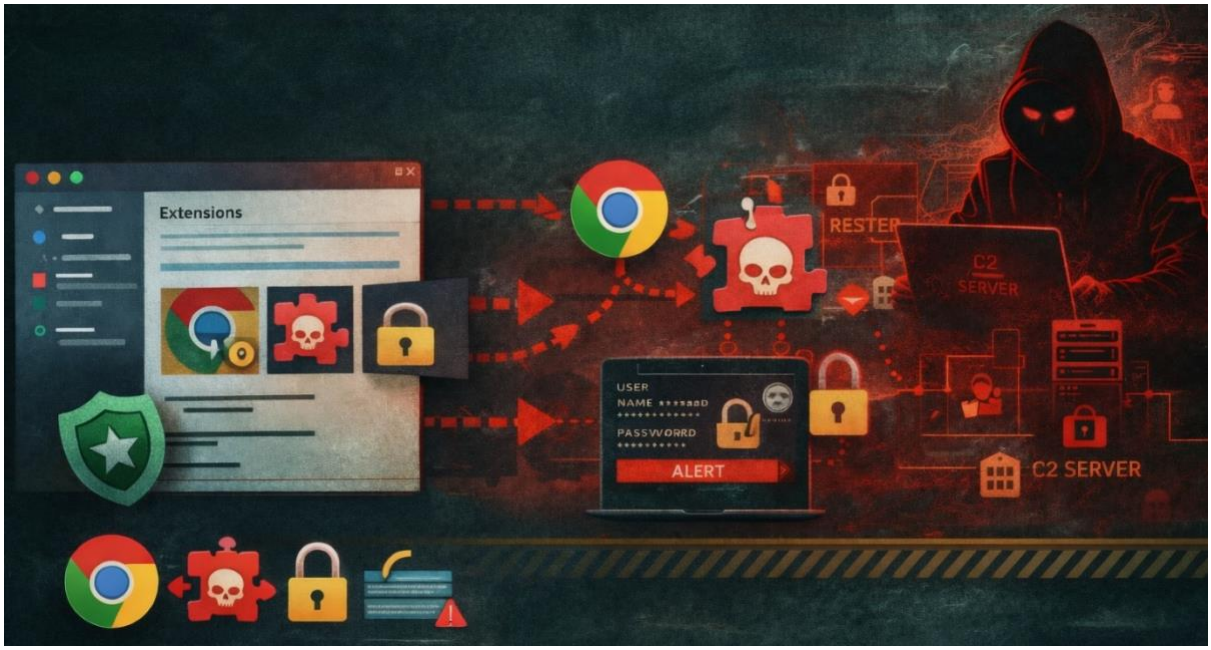
H E A D Q U A R T E R S
**CYBER COMMAND, ARMED FORCES OF THE PHILIPPINES**
Camp General Emilio Aguinaldo, Quezon City

**CYBERSECURITY BULLETIN 2026-04**

**Malicious Browser Extensions Enabling Data Theft and Session Hijacking**




**Overview**

Cybersecurity researchers have identified a coordinated campaign involving over 100 malicious Chrome extensions that appear legitimate but secretly perform malicious activities. These extensions are commonly disguised as:

- Productivity tools
- Translation services
- Social media enhancers
- Games and browser utilities

Despite functioning as advertised, these extensions silently collect user data, steal login sessions, and create backdoors in the browser.

All identified extensions are linked to a shared command-and-control (C2) infrastructure, indicating a coordinated operation by a single threat actor.

The attack typically follows this pattern:

1. Malicious extensions are uploaded to the official Chrome Web Store, appearing legitimate.
2. Users install the extension believing it is safe and useful.
3. The extension performs its advertised function to avoid suspicion.
4. In the background, it executes hidden malicious code that:

- Collects personal and account information
- Steals authentication tokens (login sessions)
- Communicates with attacker-controlled servers

5. Attackers use stolen session data to access accounts without passwords or multi-factor authentication.
6. Some extensions also enable persistent access by acting as backdoors.

Unlike traditional phishing attacks, this threat operates inside the browser, where sensitive activities occur (email, banking, official systems).

Successful compromise may result in:

- Unauthorized access to official accounts without login credentials
- Theft of sensitive personal and operational data
- Persistent monitoring of user activity
- Account takeover even with Multi-Factor Authentication (MFA) enabled
- Spread of compromise across synchronized devices

Certain extensions have been observed stealing session data repeatedly, allowing attackers to maintain continuous access.

Likewise, following are the list of the said malicious extensions:

1. Telegram Multi-account
2. Web Client for Telegram - Teleside
3. YouSide - Youtube Sidebar
4. Web Client for Youtube - SideYou
5. Web Client for TikTok
6. Text Translation
7. Page Locker
8. Page Auto Refresh
9. Web Client for Rugby Rush - SideGame
10. Formula Rush Racing Game
11. Piggy Prizes - Slot Machine
12. Slot Arabian
13. Frogtastic
14. Black Beard Slot Machine
15. Indian - Slot Machine
16. Mahjong Deluxe
17. Crazy Freekick
18. Slot Car Racing
19. Clear Cache Plus
20. Galactica Delux - Slot Machine
21. Speed Test for Chrome - WiFi SpeedTest
22. Game SkySpeedster
23. Master Chess
24. Hockey Shootout
25. Odds Of The Gods - Slot Machine
26. Billiards Pro
27. Three Card Poker
28. Donuts - Slot Machine
29. Archer - Slot Machine
30. Rugby Rush
31. Bingo

32. Web Client for game Cricket Batter Challenge
33. Slot Machine Zeus Treasures
34. Horse Racing
35. Aztec - Slot Machine
36. Straight 4
37. Slot The Gold Pot
38. American Roulette Royale
39. Asia Slot
40. Web Client for game Drive Your Car
41. Jurassic Giants - Slot Machine
42. Street Basketball
43. Tarot Side Panel
44. Dragon Slayer - Slot Machine
45. Best Blackjack
46. Book Of Magic - Slot Machine
47. Snake - Slot Machine
48. Dice King - Classic Craps And Roll Game
49. Slot Ramses
50. Battleship War
51. Gold Miner 2
52. Greyhound Racing - Dog Race Simulator
53. Hercules: Sports Legend
54. Flicking Soccer
55. Voodoo Magic - Slot Machine
56. Web Client for Hockey Shootout - SideGame
57. MASTER CHECKERS
58. Watercraft Rush
59. Car Rush
60. Video Poker Deuces Wild
61. Slot Machine Ultimate Soccer
62. Christmas Eve - Slot Machine
63. Columbus Voyage - Slot Machine
64. High or Low Casino Game
65. Goalkeeper Challenge
66. Tropical Beach - Slot Machine
67. BlackJack 3D
68. Web Client for game Classic Bowling
69. Raging Zeus Mines
70. Classic Backgammon
71. Slot Machine The Fruits
72. Baccarat
73. Mini Golf World
74. Gold Rush - Slot Machine
75. Pirat Slot
76. 40 Imperial Crown - Slot Machine
77. 3D Soccer Slot Machine
78. Premium Horse Racing
79. Tanks Game
80. Caribbean Stud Poker
81. Wild Buffalo - Slot Machine
82. Aqua - Slot Machine
83. Game Crypto Merge
84. Sherwood Forest - Slot Machine
85. Web Client for game Fatboy Dream
86. Lone Star Jackpots - Slot Machine

87. Hidden Kitty Game
88. Keno
89. Jokers Bonanza - Slot Machine
90. Penalty Kicks
91. Pai Gow Poker
92. Metal Calculator
93. Farm - Slot Machine
94. Rail Maze Puzzle
95. RED DOG CARD GAME
96. Coin Miner 2
97. Black Ninja - Slot Machine
98. Pyramid Solitaire
99. Chrome Client for Downhill Ski - SideGame
100. Slot Machine Mr Chicken
101. Web Client for French Roulette - SideGame
102. 3D Roulette Casino Game
103. Slot Machine Space Adventure
104. Whack 'em All
105. Video Poker Jacks or Better
106. Swimming Pro
107. InterAlt
108. Gold of Egypt - Slot Machine

**Recommendations:**

In this regard, AFP personnel should be cautious of the following warning signs:

- Installing browser extensions without proper verification
- Extensions requesting excessive permissions
- Unknown or newly published extensions with few reviews
- Unusual browser behavior (pop-ups, redirects, unauthorized logins)
- Alerts of suspicious account activity

Moreover, all AFP personnel are directed to observe the following:

- Install only essential browser extensions from verified publishers
- Avoid installing extensions from unknown or untrusted sources
- Review permissions before installation
- Regularly audit and remove unused or suspicious extensions
- Use official devices only for authorized tasks
- Enable Multi-Factor Authentication (MFA) on all accounts
- Report suspicious browser behavior immediately

Further. if an AFP personnel suspect a malicious extension is installed:

1. Immediately remove the suspicious extension
2. Disconnect the device from the network if necessary
3. Change all account passwords using a clean device
4. Enable or reset Multi-Factor Authentication (MFA)
5. Check for unauthorized account access or activity
6. Report the incident to ICT and chain of command
7. Avoid logging in again until the system is verified secure

**Conclusion:**

Malicious browser extensions represent a high-risk and often overlooked attack vector. These threats exploit trust in official platforms and operate silently within the user's environment. Not all tools in official stores are safe. Verify before you install. Maintaining discipline in software usage and practicing cybersecurity awareness are essential in protecting AFP systems, personnel, and operations.

*Source: https://socket.dev/blog/108-chrome-ext-linked-to-data-exfil-session-theft-shared-c2*