4.3 Million Browsers Infected: Inside ShadyPanda's 7-Year Malware Campaign

By Tuval Admoni,,

Archived: 2026-04-05 15:11:59 UTC

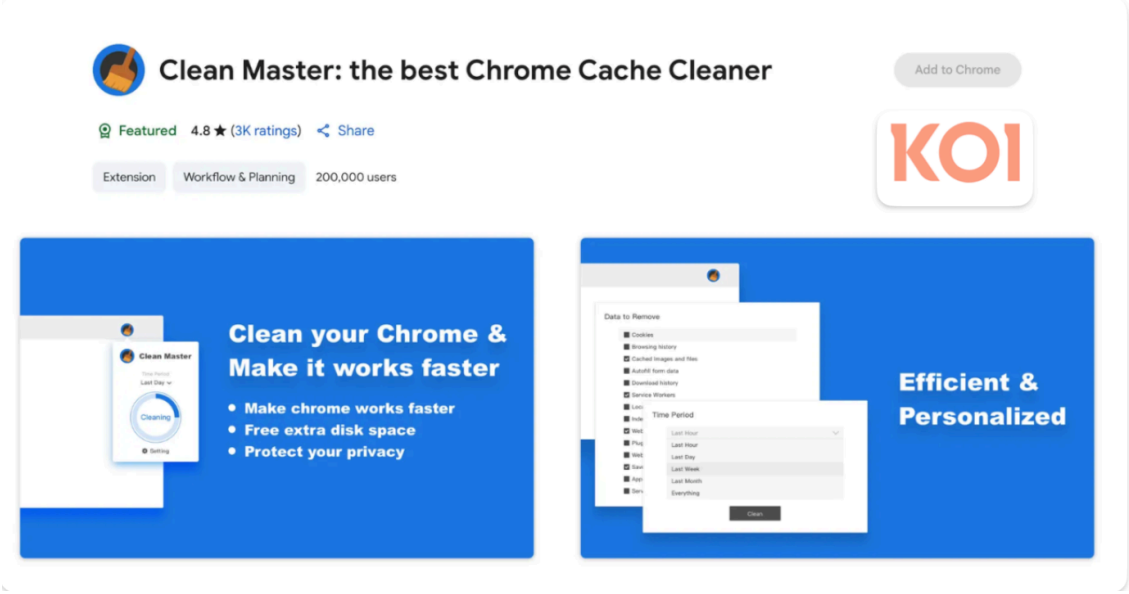
Koi researchers have identified a threat actor we're calling ShadyPanda - responsible for a seven-year browser extension campaign that has infected 4.3 million Chrome and Edge users.

Our investigation uncovered two active operations:

A 300,000-user RCE backdoor: Five extensions, including the "Featured" and "Verified" Clean Master, were weaponized in mid-2024 after years of legitimate operation. These extensions now run hourly remote code execution - downloading and executing arbitrary JavaScript with full browser access. They monitor every website visit, exfiltrate encrypted browsing history, and collect complete browser fingerprints.

A 4-million-user spyware operation: Five additional extensions from the same publisher, including WeTab with 3 million installs alone, are actively collecting every URL visited, search query, and mouse click - transmitting data to servers in China.

Some of ShadyPanda's extensions were featured and verified by Google, granting instant trust and massive distribution. For seven years, this actor learned how to weaponize browser marketplaces - building trust, accumulating users, and striking through silent updates.



Clean Master - the malware that was featured by Google

Phase 1: The Wallpaper Hustle (145 Extensions)

ShadyPanda's first campaign was straightforward but massive, and took place during 2023. 145 extensions total across both marketplaces - 20 on Chrome Web Store under publisher nuggetsno15, and 125 on Microsoft Edge under publisher rocket Zhang. All disguised as wallpaper or productivity apps.

The attack was simple affiliate fraud. Every time a user clicked on eBay, Amazon, or Booking.com, ShadyPanda's extensions silently injected affiliate tracking codes. Hidden commissions on every purchase. The extensions also deployed Google Analytics tracking to monetize browsing data - every website visit, search query, and click pattern logged and sold.

This phase wasn't sophisticated, but it was successful, ShadyPanda learned three critical lessons:

- Chrome's review process focused on initial submission, not ongoing behavior
- Users trust extensions with high install counts and positive reviews
- Patience pays off - some extensions operated for months before detection. The longer you look legitimate, the more damage you can do.

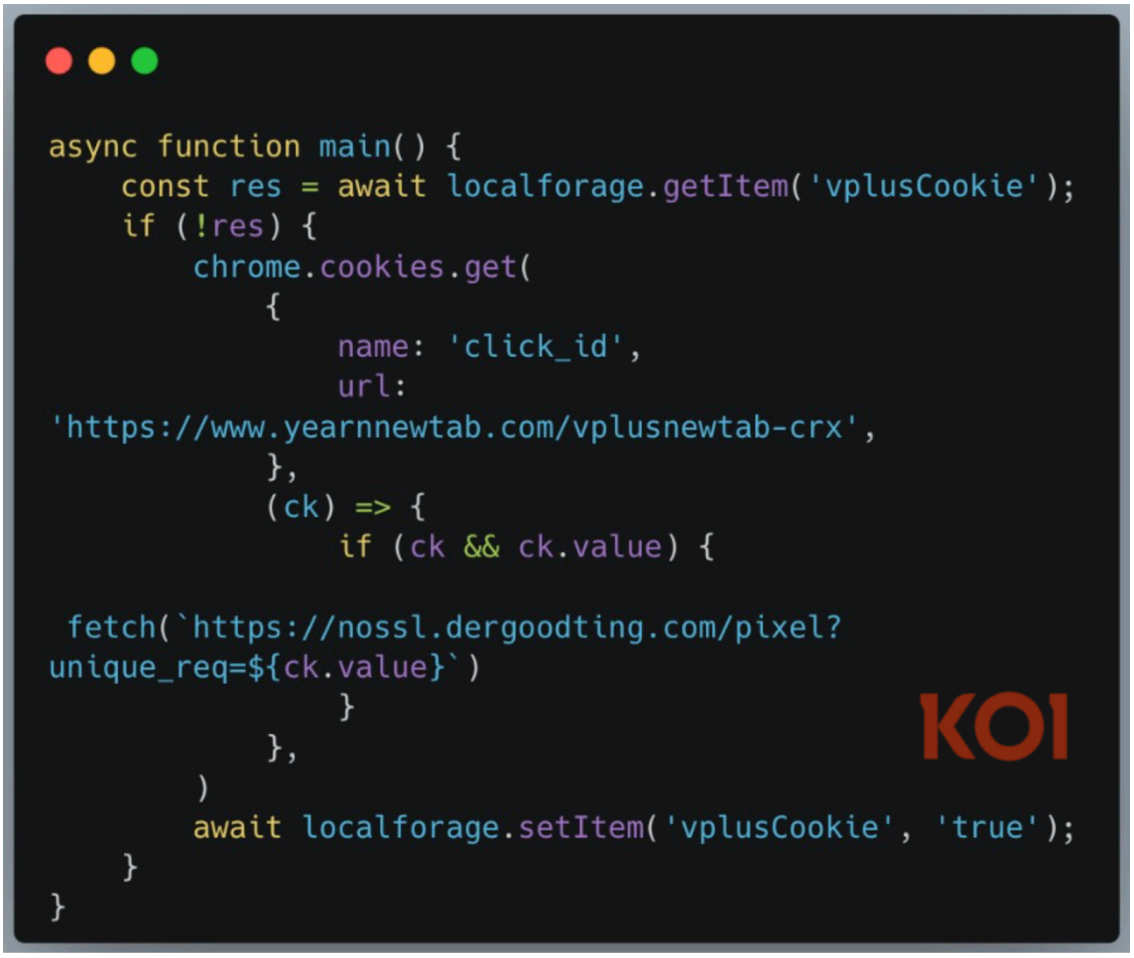
Phase 2: Search Hijacking Evolution

ShadyPanda got bolder. The next wave, in early 2024, shifted from passive monetization to active browser control.

The Infinity V+ extension exemplifies this phase. Disguised as a new tab productivity tool, it hijacked core browser functionality:

Search redirection: Every web search was redirected through trovi.com - a known browser hijacker. Search queries logged, monetized, and sold. Search results manipulated for profit.

Cookie exfiltration: Extensions read cookies from specific domains and send tracking data to nossl.dergoodting.com. Created unique identifiers to monitor browsing activity. All without consent or disclosure.



Cookie exfiltration

Search query harvesting: Every keystroke in the search box sent to external servers (`s-85283.gotocdn[.]com` and `s-82923.gotocdn[.]com`). Real-time profiling of user interests before you even hit enter. The extension captures partial queries, typos, corrections - building a detailed map of your thought process. All transmitted over unencrypted HTTP connections, making the data easy to intercept and monetize. Not just what you search for, but how you think about searching for it.

ShadyPanda was learning and getting more aggressive. But they were still getting caught. Extensions were being reported and removed within weeks or months of deployment.

They needed a better strategy.

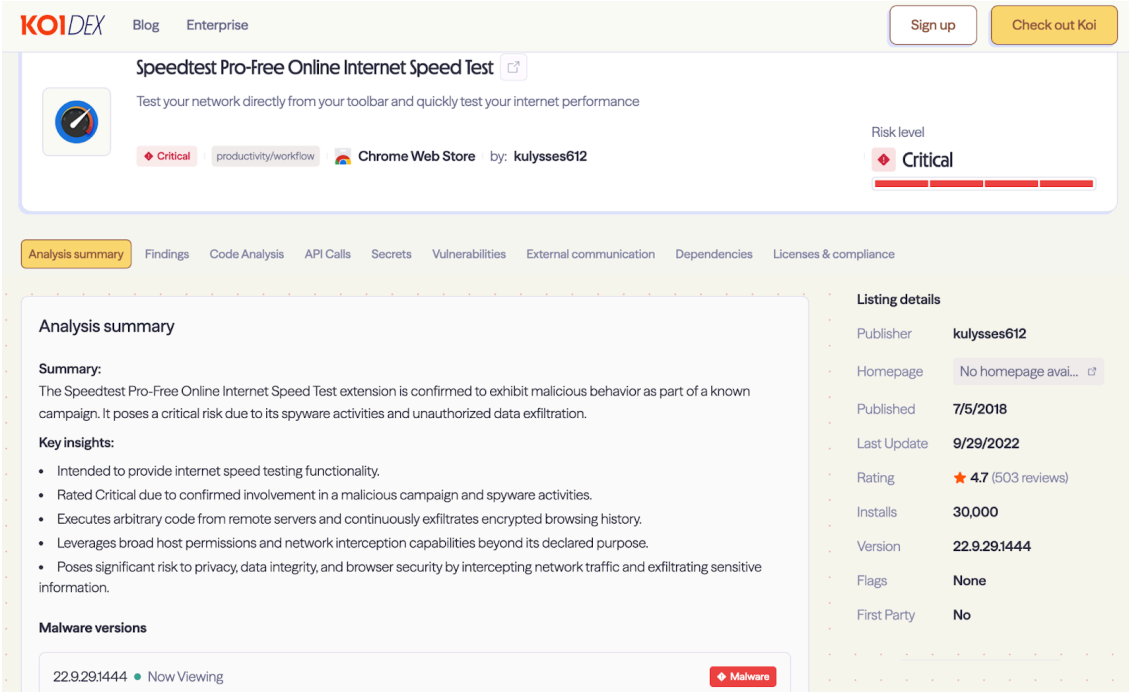
Phase 3: The Long Game

Five extensions. Three uploaded in 2018-2019 - including Clean Master with 200,000+ installs. All operated legitimately for years, gaining Featured and Verified status.

The strategy: build trust, accumulate users, then weaponize via a single update.

Before weaponization, ShadyPanda deployed covert installation tracking to optimize distribution. Data-driven malware development.

Mid 2024: After accumulating 300,000+ installs, ShadyPanda pushed the malicious update. Automatic infection via Chrome and Edge's trusted auto-update mechanism. All five extensions now run identical malware.



Koidex report on Speedtest Pro-Free

Remote Code Execution: The Hourly Weapon

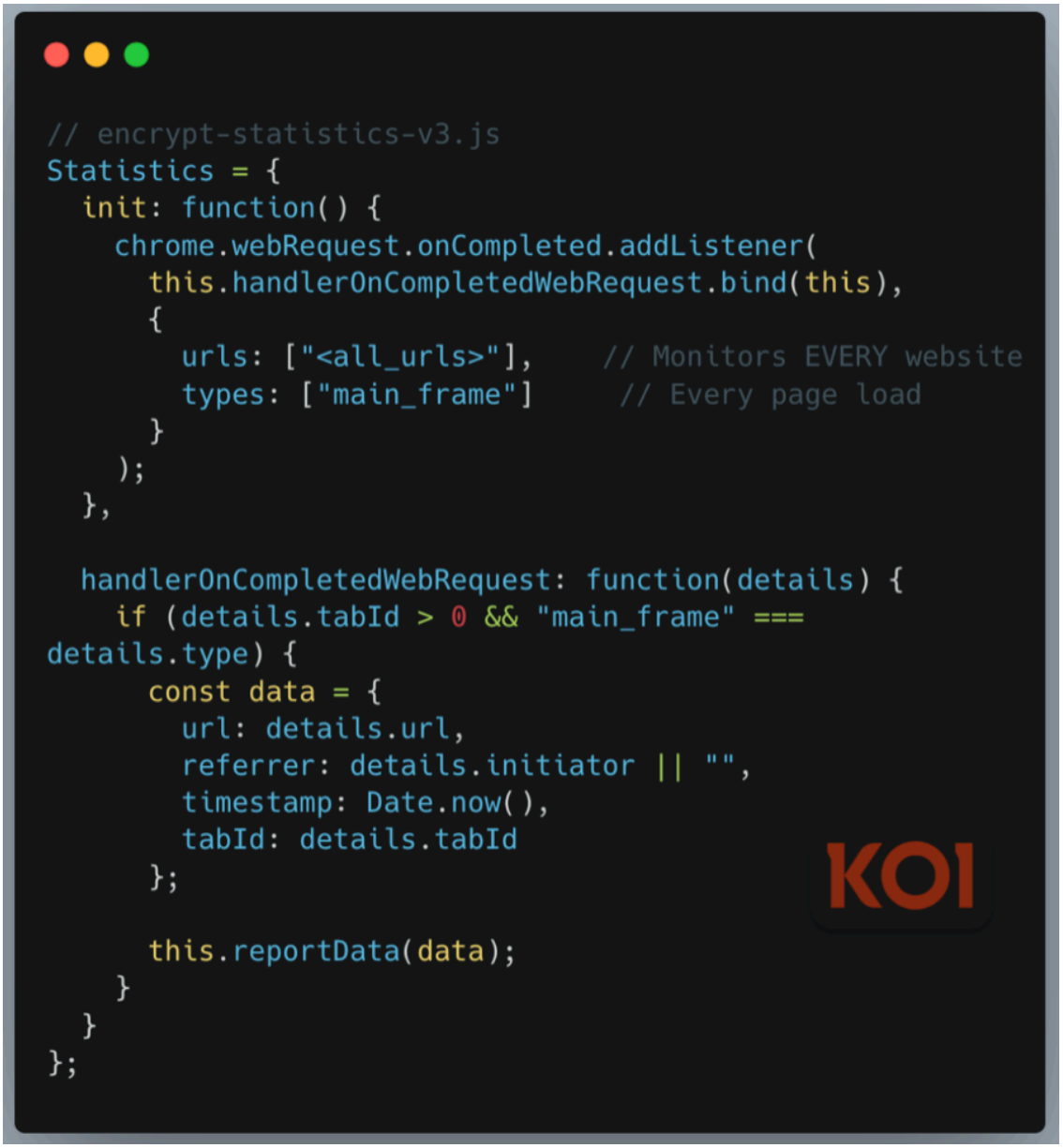
Every infected browser runs a remote code execution framework. Every hour, it checks api.extensionplay[.]com for new instructions, downloads arbitrary JavaScript, and executes it with full browser API access.

Remote code execution

This isn't malware with a fixed function. It's a backdoor. ShadyPanda decides what it does. Today it's surveillance, tomorrow it could be ransomware, credential theft, or corporate espionage. The update mechanism runs automatically, hourly, forever.

Complete Browser Surveillance

The current payload monitors every website visit and exfiltrates encrypted data to ShadyPanda's servers:



What gets collected and exfiltrated:

- Every URL visited with full browsing history
- HTTP referrers showing navigation patterns
- Timestamps for activity profiling
- Persistent UUID4 identifiers (stored in chrome.storage.sync, survives across devices)
- Complete browser fingerprints: user agent, language, platform, screen resolution, timezone
- All data encrypted with AES before sending to api.cleanmasters.store

Evasion & Attack Capabilities

Anti-analysis: If a researcher opens developer tools, the malware detects it and switches to benign behavior. The code uses heavy obfuscation with shortened variable names and executes through a 158KB JavaScript interpreter to bypass Content Security Policy.

Man-in-the-Middle: Service worker can intercept and modify network traffic, replace legitimate JavaScript files with malicious versions, enabling credential theft, session hijacking, and content injection into any website - even HTTPS connections.

ShadyPanda can update any of these capabilities hourly. Even though the extensions were recently removed from marketplaces, the infrastructure for full-scale attacks remains deployed on all infected browsers.

Phase 4: The Spyware Empire (5 Extensions, 4M+ Users)

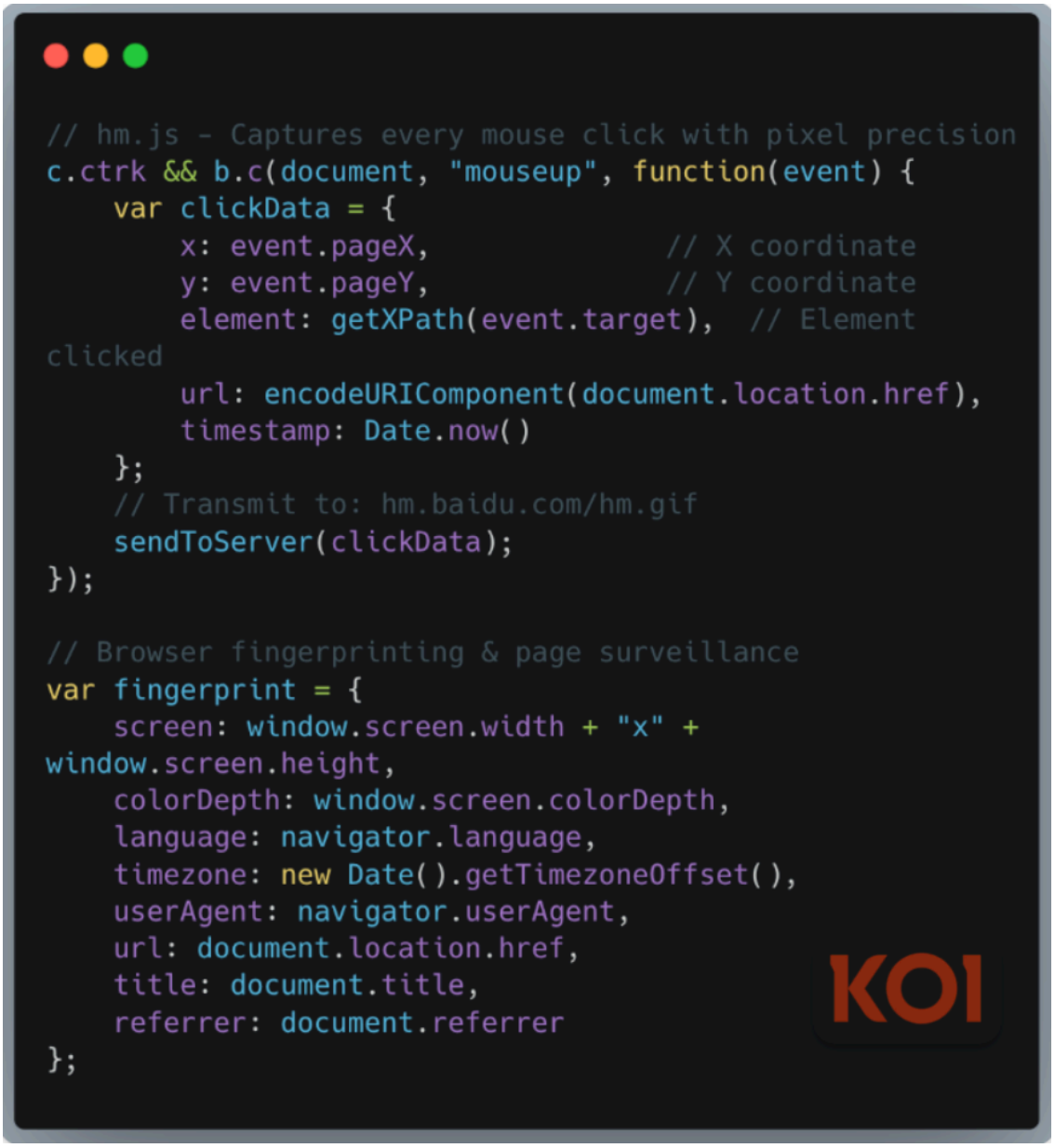
However, ShadyPanda's biggest operation wasn't Clean Master. The same publisher behind Clean Master in Edge - Starlab Technology - launched 5 additional extensions on Microsoft Edge around 2023, accumulating over 4 million combined installs.

And here's the problem: ALL 5 extensions are still live in the Microsoft Edge marketplace. Unlike Phase 3's removed extensions, this 4-million-user surveillance operation is active right now.

Two of the five are comprehensive spyware. The flagship, WeTab 新标签页 (WeTab New Tab Page), has 3 million installs alone and functions as a sophisticated surveillance platform disguised as a productivity tool.

Comprehensive Data Collection

WeTab collects and exfiltrates extensive user data to 17 different domains (8 Baidu servers in China, 7 WeTab servers in China, and Google Analytics):



What gets collected:

- Every URL visited - complete browsing history transmitted in real-time
- All search queries - keystroke-level monitoring of what users search for
- Mouse click tracking with pixel-level precision - X/Y coordinates and element identification
- Browser fingerprinting - screen resolution, language, timezone, user agent
- Page interaction data - time on page, scroll behavior, active viewing time
- Storage access - reads localStorage, sessionStorage, and can access all cookies

Phase 4 dwarfs the Clean Master operation: 4 million infected users versus 300,000. The extensions remain live in Microsoft Edge marketplace - the extension already has dangerous permissions including access to all URLs and cookies, users are downloading them right now. ShadyPanda can push updates at any time, weaponizing 4 million browsers with the same RCE backdoor framework from Phase 3, or something even worse. The infrastructure is in place. The permissions are granted. The update mechanism works automatically.

Seven Years of Exploitation

ShadyPanda's success isn't just about technical sophistication. It's about systematically exploiting the same vulnerability for seven years: Marketplaces review extensions at submission. They don't watch what happens after approval.

What linked all these campaigns together: code signing similarities, overlapping infrastructure, identical obfuscation techniques evolving over time. Same actor. Different masks. Each phase learned from the last - from crude affiliate fraud to patient five-year operations.

The auto-update mechanism - designed to keep users secure - became the attack vector. Chrome and Edge's trusted update pipeline silently delivered malware to users. No phishing. No social engineering. Just trusted extensions with quiet version bumps that turned productivity tools into surveillance platforms.

ShadyPanda controls what happens next: session hijacking, credential harvesting, account takeover, supply chain attacks through compromised developers. For enterprises, infected developer workstations mean compromised repositories and stolen API keys. Browser-based authentication to SaaS platforms, cloud consoles, and internal tools means every login is visible to ShadyPanda. Extensions bypass traditional security controls. ShadyPanda has been inside your network for over a year.

The systemic problem isn't just one malicious actor. It's that the security model incentivizes this behavior:

1. Build something legitimate
2. Pass review and gain trust signals (installs, reviews, verified badges)
3. Collect large user base
4. Weaponize via update
5. Profit before detection

ShadyPanda proved this works. And now every sophisticated threat actor knows the playbook.

Final Thoughts

One patient threat actor and one lesson: Trust is the vulnerability.

ShadyPanda proved that marketplaces still review extensions the same way they did seven years ago - static analysis at submission, trust after approval, no ongoing monitoring. Clean Master operated legitimately for five years. Static analysis wouldn't catch this.

This writeup was authored by the research team at Koi Security.

We've built Koi for this moment. Behavioral analysis and risk scoring for everything your teams pull from marketplaces. We watch what extensions do after installation, not what they claim to be.

Book a demo to see how behavioral monitoring catches threats that evolve after approval.

IOCS

C&C Domains:

- extensionplay[.]com
- yearnnewtab[.]com
- api.cgatgpt[.]net

Exfiltrations Domains:

- dergoodting[.]com
- yearnnewtab[.]com
- cleanmasters[.]store
- s-85283.gotocdn[.]com
- s-82923.gotocdn[.]com

Chrome Extensions:

- eagiakjmjnblliacokhcalebgnhellfi
- ibiejjpajlfljcgjndbonclhcbdcamai
- ogjneoecnllmjcegcfpaamfpbiaaiekh
- jbnopeoocgbmnochaadfnhiiimfpbpmf
- cdgonefipacceedbkflolomdegncceid
- gipnpcencdgljnaecpekokmpgnhgpela
- bpgaffohfacaamplbbojgbiicfgedmoi
- ineempkjpmbdejmdgienaphomigjjiej
- nnnklgkfdfbdijeeglhjfleaoagiagig
- Mljmfnkjmcdmongjnnnbbnajjdbojoci
- llkncpcdceadgibhbedecmkencokjajg
- nmfbniajnpceakchicdhfofoejhgjefb
- ijcpbhmpbaafndchbjdjchogaogelnjl
- olaahjgjlhoehkpemnfognpgmkbedodk
- gnhgdhlkojnlgljamagoigaabdmfhfeg
- cihbmmokhmieaidfgamioabhhkggnehm
- lehjnmndiohfaphecnjhopgookigekdk
- hlcjkaoneihodfmonjnlnnfpdcopgfjk
- hmhifpbclhgklaaepgbabgcpfgidkoei
- lnlononncfdnhdfmgpkdfoibmfdehfoj
- nagbiboibhbjbclhcigklajjdefaiidc
- ofkopmlicnffaiiabnmnaajaimmenkjn
- ocffbdeldlbilgegmifiakciiicnoaeo
- eaokmbopbenbmgegkmoiogmpejlaikea
- lhiehjmkpbhhkfapacaiheolgejcifgd
- ondhgmkgppbdnogfiglikgpdkmkaiggk
- imdgpklnabbkghcbhmkbjbhcomnfdige

Edge Add-ons:

- bpelnogcookhocnaokfpoeinibimbeff
- enkihkfondbngohnmlefmobdgkpmejha
- hajlmbnnniemimmaehcefkamdadpjlfa
- aadnmeanpbokjjahcnikajejglihibpd
- ipnidmjhnoipibbinllilgeohohehabl
- fnnigcfbmghcefaboigkhfimeolhhbcp
- nlcebdoehkdiojeahkofcfnolkleembf
- fhababnomjcnhmobbemagohkldaeicad
- nokknhlkpdfppefncfkdebhgfpfilieo
- ljmcneongnlaecabgneiippeacdoimaa
- onifebiiejdjncjpjnojlebibonmnhog
- dbagndmcddecodlmnlcmhheicgkaglpk
- fmgfcpjmmapcjlknncjgmbolgaecngfo
- kgmlodoegkmpfkbepkfhgeldidodgohd
- hegpgapbnfiibpbkanjemgmdpmmlecbc
- gkanlgbbnncfafkhlchnadcopcgjkfli
- oghgaghnofhhoolfneepjneedejcpiic
- fcidgbgogbfdcgijkcfdjcagmhcelpbc
- nnceocbiolncfljcmajijmeakcdlffnh
- domfmjgbmkckapepjahpedlpdedmckbj
- cbkogccidanmoaicgphipbdofakomlak
- bmlifknbfonkgphkpmkeoahgbhbdhebh
- ghaggkcfafofhcfppignflhlocmcfimd
- hfeialplaojonefabmojhobdmghnjkmf
- boiciofdokedkpmopjnghpkgdakmcpmb
- ibfpbjfnpcgmiggfildbcngccoomddmj
- idjhfmgaddmdojcfmhcjnnbhnhbmhipd
- jhgfinhjcamijjoikplacnfknpchndgb
- cgjgmbppcoolfkbkjhoogdpkboohhgel
- afooldonhjnhddgnfahlepchipjennab
- fkbcbgffcclobgbombinljckbelhnpif
- fpokgjmlcemklhmilomcljolhnbaaajk
- hadkldcldaanpomhhllacdmglkoepaed
- iedkeilnpbkeecjpmkelnglnjpnacnlh
- hjfmkkelabjoojjmjljidocklbibphgl
- dhjmmcjnajkpnbnbpagglbbfpbacoffm
- cgehahdmoijenmnhinajnojmmlnipckl
- fjigdpmfeomndepihcinokhcphdojepm
- chmcepembfffejphepoongapnlchjgil
- googojfbnbhbbnpfpdnffnklipgifngn
- fodcokjckpkfpegbekkiallamhedahjd

- igiakpjhacibmaichhgbagdkjmjbnanl
- omkjakddaeljdfgekdjebbbiboljnalk
- llilhpmmhicmiaoancaafdgganakopfg
- nemkiffjklgaooligallbpmhdmmhepll
- papedehkgfhnagdiempdbhlgcnioofnd
- glfddenhiaacfmhoiebfeljnfkkkmbjb
- pkjfghocapckmendmgdmppjccbplccbg
- gbcjipmcpedgndgdnfofbhgnkmghoamm
- ncapkionddmdmfocnjfcfpnimepibggf
- klggeioacnkkpdcnapgcoicnblliidmf
- klgjbnheihgnmimajhohfcldhfpjnahe
- acogeoajdpgplfhidldckbjkkpgeebod
- ekndlocgcngbpebppapnpalpjfnkoffh
- elckfehnjdbghpoheamjffpdbbogjhie
- dmpceopfiajfdnoiebfankfoabfehdpn
- gpolcigkhldaighngmmmcjldkkiaonbg
- dfakjobhimnibdmkbgpkijoihplhcnil
- hbghbdhfibifdgnbpaogepnkekonkdgc
- fppchnhginnfabgenhihpncnphhafmac
- ghhddclfkljabeodmcejjjlhoaaiban
- bppelgkcnhfkicolffhlkbdghdnjdkhi
- ikgalegglchgbihlaanjbkekmmgccam
- bdhjinjoglaijpffoamhhnhooeimgoap
- fjioinpkgmlcioajfnncgldldcnabffe
- opncjjhgbllenobgbfjbblhghmdpmpbj
- cbijiaccpnkbdpgbmiiipedpepbhioel
- fbbmnieefocnacnecccgmedmcbhlkcpm
- hmbacpfgehmmoloinfmkgkpjoagiogai
- paghkadkhiladedijgodgghaajppmpcg
- bafbmfpfepdlgnfkgfbobplkkaoakjcl
- kcpkoopmfjhdpgjohcbgkbjpmbjmhgoi
- jelgelidmodjpmohbapbghdgcpncahki
- lfgakdlafdenmaikccbojgcofkkhmolj
- hdfknlljfbdfjdjhfgoonpphpigjjjak
- kpfbijpdidioaomoecdbfaodhajbcjfl
- fckphkcbpgmappcgnfieaacjbknhkhin
- lhfdakoonenpbggbeephofdlflloghhi
- ljjngehkphcdnnapgciajcdbcpgmpknc
- ejfocpkjndmkbloiobcdhkkoeekcpkik
- ccdimkoieijdbgdlkfjjfncmihmlpanj
- agdlpnhabjfcbeiempefhpgikapcapjb
- mddfnhdadbofiifdebeiegecchpkbgdb

- alknmfpopohfpdpafdmobclioihdkhjh
- hlglicejgohbanllnmnjllajhmnhjjel
- iaccapfapbjahnhcmkgjjonlccbhdpjl
- ehmnkbambjnodfbjcebjffilahbfjdml
- ngbfciefgjgijkkmpalnmhikoojilkob
- laholcgeblfbgdhkbiidbpiofdcbpeeo
- njoedigapanaggiabjafnaklppphempm
- fomlombffdkflbliepgpgcnagolnegjn
- jpoofbjomdefajdjcimmaoildecebkjc
- nhdiopbebcklbkpfnhipecgfhdhdbfhb
- gdnhikbabcflemolpeaaknnieodgpiie
- bbdioggpbhhodagchciaeaggdponnhpa
- ikajognfijokhbgjdhgpemljgcjclpmn
- lmnjiioclbjphkggicmldippjojgmldk
- ffgihbmcfcihmpbegcfdkmafaplheknk
- lgnjdldkappogbkljaiedgogobcgemch
- hiodlpcelfelhpinhgngoopbmclcaghd
- mnophppbmlnlfobakddidbcgcjakipin
- jbajdpebknffiaenkdhopebkolgdlfaf
- ejdihbblcbdfobabjfebfjfopenohbjb
- ikkoanocgpdmmiamnkogipbpdpckcahn
- ileojfedpkdbkcchpnghhaebfoimamop
- akialmafcdmkelghnomeneinkcllnoih
- eholblediahnodlgigdkdhkkpmbiafoj
- ipokalojgdmhfpagmhnjokidnpjfnfik
- hdpmmcmblgbkllldbccfdejchjlpochf
- iphacjobmeoknlhenjfiilbkddgaljad
- jiiggekklbbojgfmdenimcdkmidnfofl
- gkhggnaplpjkghjjcmpmnmidjndojpcn
- opakkgodhhongnhbdkgjgdlcbknacpaa
- nkjomoafjgemogbdkhledkoeaflnmgfi
- ebileebbekdcpfjlekjapgmbgpfigled
- oaacndacaoelmkhfilennooagoelpjop
- ljkgnegaajfacghepjiajibgdpfmcfip
- hgolomhkdcpmbgckhebdhdknaemlbbaa
- bboeoilakaofjkdmekpgeigieokkpgfn
- dkkpollfhjoiapcenojlmgempmjekcla
- emiocjgakibimbopobplmfldkldhhiad
- nchdmembkfgkejljapneliogidkchiop
- lljplndkobdgkjilfmfiefpldkhkhbbd
- hofaaigdagglolgiefkbencchnekjejl
- hohobnhiiohgcipklpncfmjkjpmejjni

- jocnjcakendmllafpmjailfnlndaaklf
- bjdclfjlhgcdcpjhmhfggkkfacipilai
- ahebpkbnckhgjmndfjejibjjahjdlhdb
- enaigkcpmpohpbokbfllbkijmllmpafm
- bpngofombcjloljkoafhmpcjclkekfbh
- cacbflgkiidgcekflfgdnjdnaalfmkob
- ibmgdfenfldppaodbahpgcoebmmkdbac

Source: https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign