Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

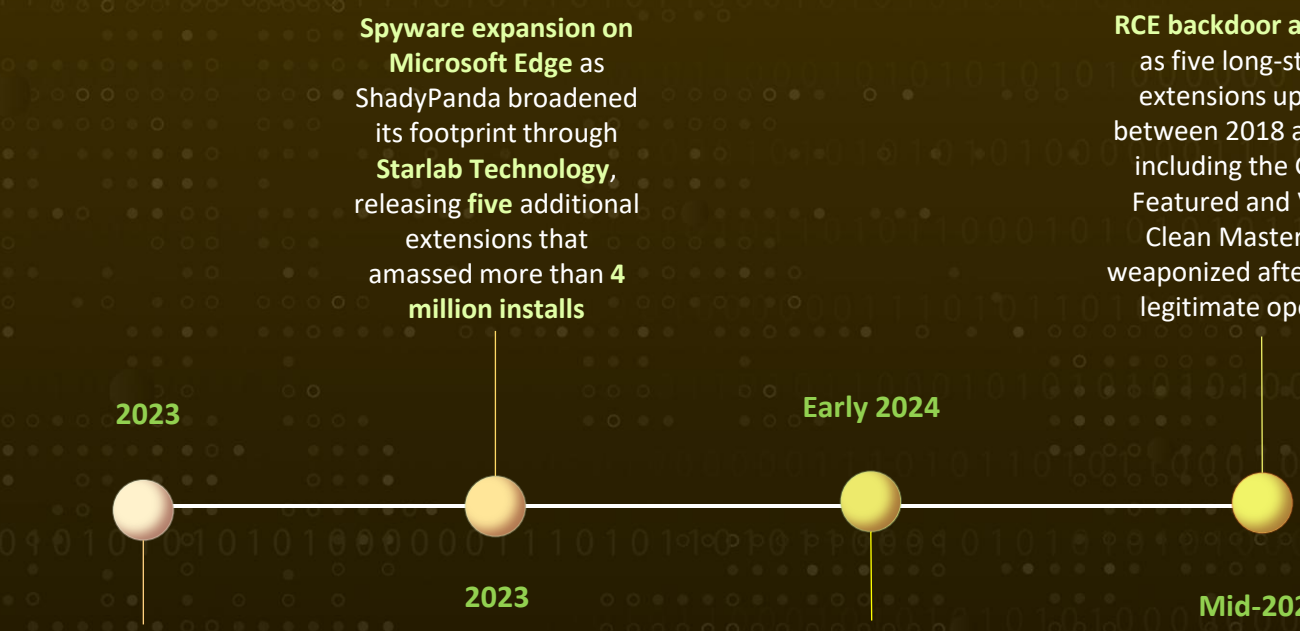
ShadyPanda's Seven-Year Operation Built a Browser Extension Spy Empire

Date of Publication	Admiralty Code	TA Number
December 8, 2025	A1	TA2025371

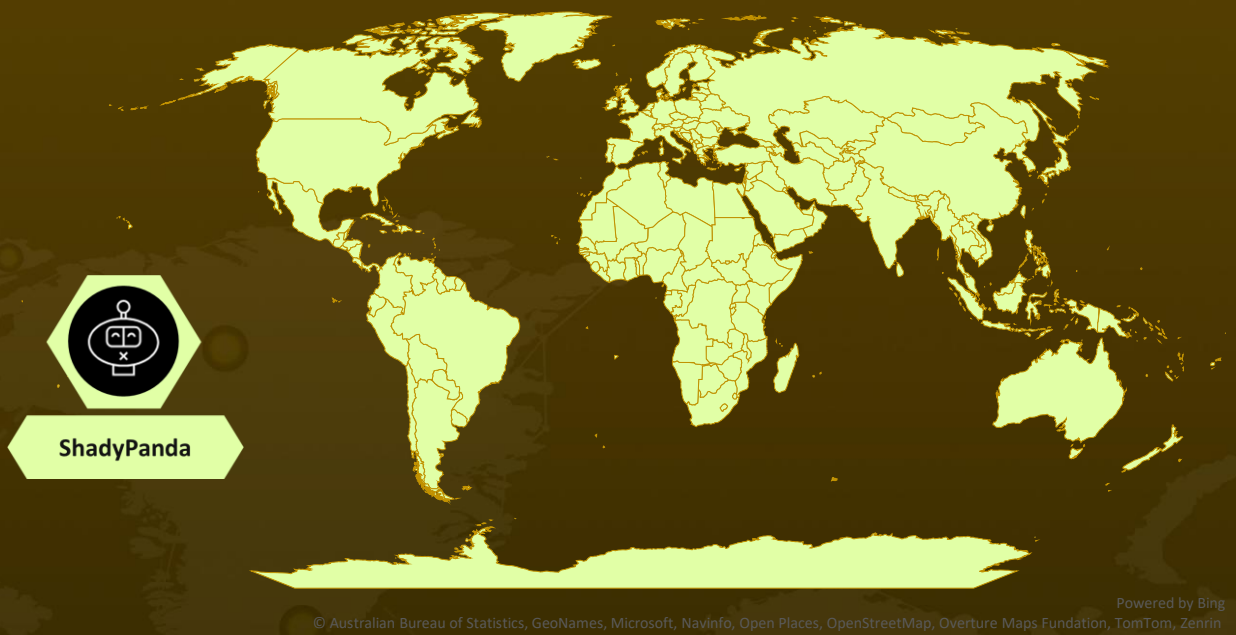
Summary

First Seen: 2017
Threat Actor: ShadyPanda
Targeted Platforms: Chrome, Edge
Targeted Regions: Worldwide

Attack Timeline



Actor Map



Actor Details

#1 ShadyPanda is a likely China-based threat actor behind a seven-year browser-extension operation that compromised more than 4.3 million Chrome and Edge users. The group exploited the trust built into extension marketplaces, running clean, functional extensions for years before converting them into delivery systems for silent malicious updates.

#2 The operation split into two core tracks, a remote code execution backdoor affecting roughly 300,000 users through five extensions, including Google “Featured” and “Verified” Clean Master, and a large-scale spyware effort reaching more than 4 million users through five additional extensions that funneled browsing data to servers in China.

#3 The threat actor ShadyPanda demonstrated long-term discipline and a precise understanding of marketplace blind spots. Its strategy hinged on patience, maintaining legitimate behavior to grow large user bases before activating malicious payloads.

#4 Google's endorsement of these extensions amplified reach and credibility, enabling the threat actor to weaponize the marketplace itself. Over seven years, ShadyPanda refined a method that blended trust-building, mass adoption, and silent update delivery.

#5 The core profit engine was affiliate fraud. When users visited platforms like eBay, Amazon, or **Booking.com**, the extensions injected hidden affiliate codes, diverting commissions to the threat actor. They also embedded Google Analytics trackers to harvest and monetize detailed behavioral data, logging queries, site visits, and click patterns.

#6 Each infected browser carried a remote execution framework that polled for new commands, retrieved arbitrary JavaScript, and executed it with full browser permissions. The extensions also enabled adversary-in-the-middle capabilities, supporting credential theft, session hijacking, and live code injection across websites. Even after several extensions were taken down, the threat actor ShadyPanda continued refining its tactics and pursuing new delivery paths.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRY
ShadyPanda	China **MOTIVE** Information theft, Financial gain, and Espionage	Worldwide	All

Recommendations

Eliminate Trust-Based Extension Approval: Remove reliance on marketplace verification labels. Treat Featured and Verified badges as non-security indicators and apply independent vetting before deployment.

Harden Enterprise Browser Baselines: Minimize permitted extensions to a vetted set. Block consumer-grade tools that provide an attack surface with no operational value.

Mandate Network Controls for Extension Traffic: Inspect outbound connections from extension processes. Flag analytics beacons, suspicious domains, and data exfiltration paths.

Enforce Continuous Extension Behavior Monitoring: Track real-time behaviors such as search redirection, affiliate code injection, or unauthorized data transmission. Detect malicious shifts instead of relying on static reviews.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1189 Drive-by Compromise	**T1176** Software Extensions	**T1176.001** Browser Extensions	**T1059** Command and Scripting Interpreter
T1059.007 JavaScript	**T1027** Obfuscated Files or Information	**T1480** Execution Guardrails	**T1036** Masquerading
T1539 Steal Web Session Cookie	**T1185** Browser Session Hijacking	**T1005** Data from Local System	**T1056** Input Capture
T1056.004 Credential API Hooking	**T1041** Exfiltration Over C2 Channel	**T1217** Browser Information Discovery	**T1567** Exfiltration Over Web Service
T1071 Application Layer Protocol	**T1071.001** Web Protocols	**T1573** Encrypted Channel	**T1557** Adversary-in-the-Middle

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	extensionplay[.]com, yearnnewtab[.]com, api[.]cgatgpt[.]net, dergoodting[.]com, yearnnewtab[.]com, cleanmasters[.]store, s-85283[.]gotocdn[.]com, s-82923[.]gotocdn[.]com
Browser Extension ID	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, bpelnogcookhocnaokfpoeinibimbeff, enkihkfondbngohnmlefmobdgkpmejha, hajlmbnnniemimmaehcefkamdadpjlfa, aadnmeanpbokjjahcnikajejglihibpd,

TYPE	VALUE
Browser Extension ID	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,

TYPE	VALUE
Browser Extension ID	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,

TYPE	VALUE
Browser Extension ID	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, lbmgdfenfldppaodbahpgcoebmmkdbac

References

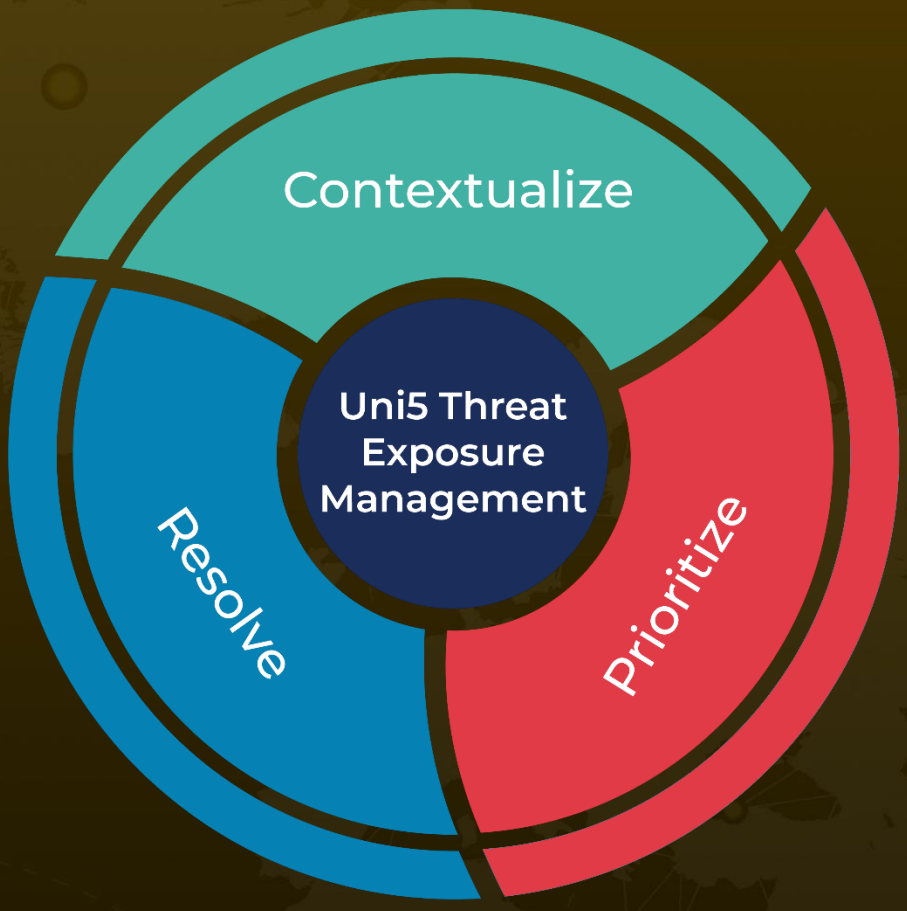
https://www.koi.ai/blog/4-million-browsers-infected-inside-shadypanda-7-year-malware-campaign

https://hivepro.com/threat-advisory/i-paid-twice-inside-the-booking-com-phishing-fraud/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 8, 2025 • 1:30 AM

More at www.hivepro.com