Event Report

CloudSEK

The Anatomy of an Attack: Pakistan Based Infostealer Delivery Network Exposed

---

Category

Cybercrime Group

Region

Global

Pavan Karthick (Author)
Threat Researcher III

Vikas Kundu (Co-Author)
Threat researcher

Nivya Ravi (Co-Author)
Director of Products - BeVigil & SVigil

CloudSEK

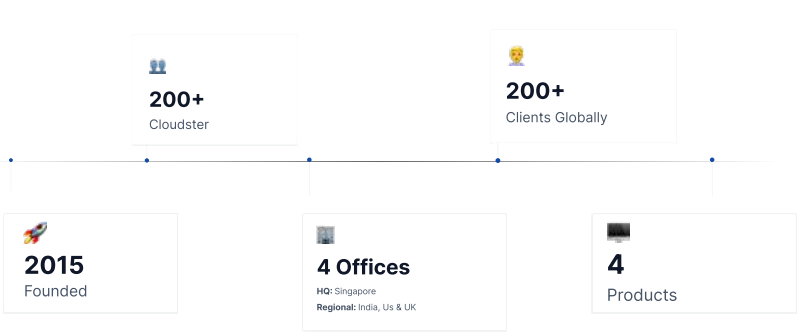
Table of Contents

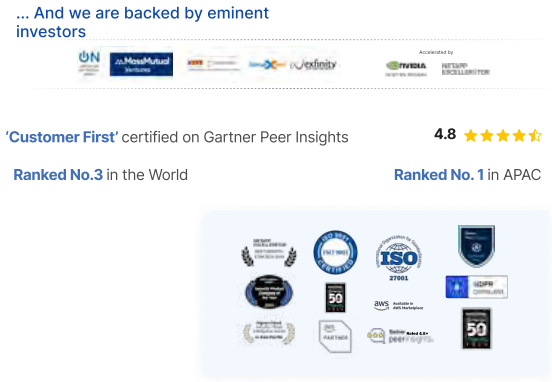
Page No.

1. Executive Summary 03
2. Key Findings 04
3. Investigation Methodology 04-05
4. Infrastructure Overlap & Stealer-Log Evidence 06-07
5. Pivot to Pay-Per-Install (PPI) Networks 07-09
6. Actor Landscape 10
7. Infrastructure Mapping 10-11
8. Financial Analysis 11-13
9. Traffic Analysis 14-15
10. Operational Insights & Attribution 15-16
11. Victimology & Impact 16
12. Detection & Mitigation Guidance 16-17
13. Conclusions & Strategic Implications 17
14. Appendices 17-24

About CloudSEK

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.





Executive Summary

This report details an extensive, long-running malware distribution campaign operated by a highly interconnected group of threat actors based primarily in **Bahawalpur and Faisalabad, Pakistan**. The investigation, initiated from a single forum post, unraveled a complex network, whose operations resemble direct-sales or "party plan" models akin to how consumer goods companies expand through social networks except here, the commodity is malicious software, distributed via a structured, trusted network of associates.

The group's primary modus operandi is **Search Engine Optimization (SEO)** poisoning and the abuse of legitimate online forums and platforms. They create posts for highly sought-after cracked software (e.g., Adobe After Effects, IDM) which, once indexed by Google, lure victims to a web of malicious WordPress sites. These sites deliver infostealer malware, most notably **Lumma Stealer** and **Meta Stealer**, and more recently **AMOS** concealed within password-protected archives.

Monetization is the core driver, achieved through a sophisticated **Pay-Per-Install (PPI)** scheme. The actors manage their own PPI networks, **SpaxMedia (now Installstera)** and the larger **InstallBank**, to pay themselves and their affiliates for successful malware installations.

The breakthrough in the investigation came ironically: the threat actors themselves were compromised by infostealer malware. The exfiltrated logs from their own machines provided unprecedented insight into their identities, command structure, infrastructure, communications, and finances, ultimately leading to their unmasking.

Key Findings

- **Scale & Impact:** 5,239 affiliates operated 3,883 sites, generating 449M+ clicks and 1.88M+ installs (documented period). Lifetime revenue: $4.67M tracked; actual likely higher due to off-ledger settlements.
- **Financial Insights:** $130,560.53 paid out (May–Oct 2020) at $0.0693 eCPI. Top earners captured 45%+ of funds. Payoneer (67%) > Bitcoin (31%).
- **Actor Attribution:** Pakistani-centric (Bahawalpur cluster); . Loose OpSec (reused creds) enabled deep pivots.
- **Evolution:** Shift from installs (2020: 2.4M) to downloads (2024: 68M+), with CTR rising to 60%. Long-haul sites (>1yr lifespan) drove 85% of installs.
- **Infrastructure:** Domains like ozycode.cfd orchestrates redirects; .cfd/.lol TLDs for disposables. SEO/forum spam seeds traffic.
- **Victimology:** Global, but warez seekers (e.g., Software cracks) primary; 4.67M revenue implies 10M+ potential victims (assuming $0.47/log resale).

Investigation Methodology

1. **Discovery & Triage:**

- Keyword searches ("* crack", "* free download") on Google/Bing identified warez sites.
- Forum analysis (e.g., Honor Club) for initial links; AI-OCR on screenshots for text extraction.

2. **OSINT Enrichment:**

- Email/domain pivots via HaveIBeenPwned, IntelX, and xeuledoc for ownership.
- Breach data cross-checks (e.g., Internet Archive breach) for leaked creds.

3. **Malware Analysis:**

- Detonated samples (e.g., SHA256: f0c3c758ab20867c4c1fc663c94211270849dba9bf386a0d20d3ce9049eb875e) on Public malware sandboxes.
- Identified Lumma/RedLine variants; extracted C2s (e.g., cloudewahsj.shop/api).

4. **Credential Exploitation:**

- Stealer logs yielded PPI panel creds of multiple PPI service associates and admins.
- SQLi on InstallBank & dumped DB; affiliate logins accessed SpaxMedia.

5. **Financial/Traffic Analysis:**

- SQLite queries on leaked DB (e.g., SELECT * FROM payouts) for ledgers.
- Blockchain explorers for BTC clustering.

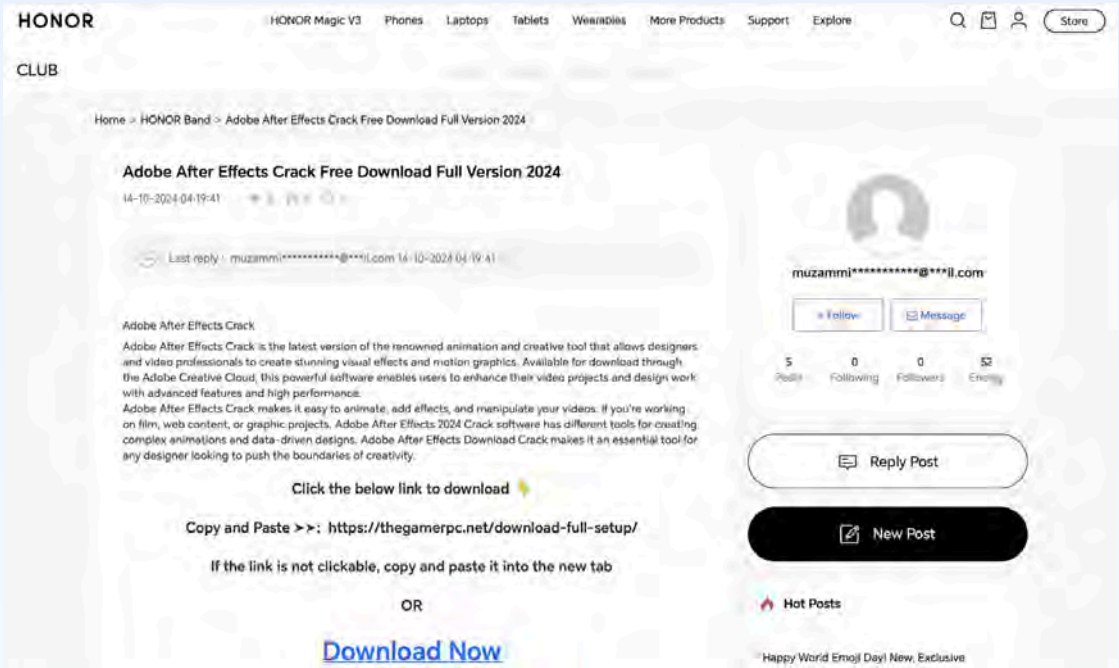
6. **Validation:**

- SQLite queries on leaked DB (e.g., SELECT * FROM payouts) for ledgers.
- Blockchain explorers for BTC clustering.

Investigation Methodology

The investigation commenced on October 14th, 2024, originating from a seemingly innocuous community forum post.

- **The Lure (Honor Forum Post):** A user account on the official HONOR UK community forum (honor.com/uk/club) published a topic titled "Adobe After Effects Crack Free Download Full Version 2024." This post, designed to be indexed by search engines, served as the initial entry point for potential victims.



https://www.honor.com/uk/club/topicdetail/adobe-after-effects-crack-free-download-full-version-2024/topicid-3625681748033537/ (Now Inactive)

- **Redirection and Initial Pivot:** The post contained a link to https://thegamerpc.net/download-full-setup/. This URL did not directly host the malware but redirected to a public Google Document. This use of a legitimate service like Google Docs is a common tactic to evade initial detection and lend an air of legitimacy.

- **The OSINT Breakthrough:** Using the OSINT tool xeuledoc, the Google Document was analyzed. The tool revealed critical metadata:
  - **Owner's Name:** This email directly corresponded with the masked email of the user on the Honor forum, providing the first concrete link between the forum spam and a specific individual (M******* H*****).

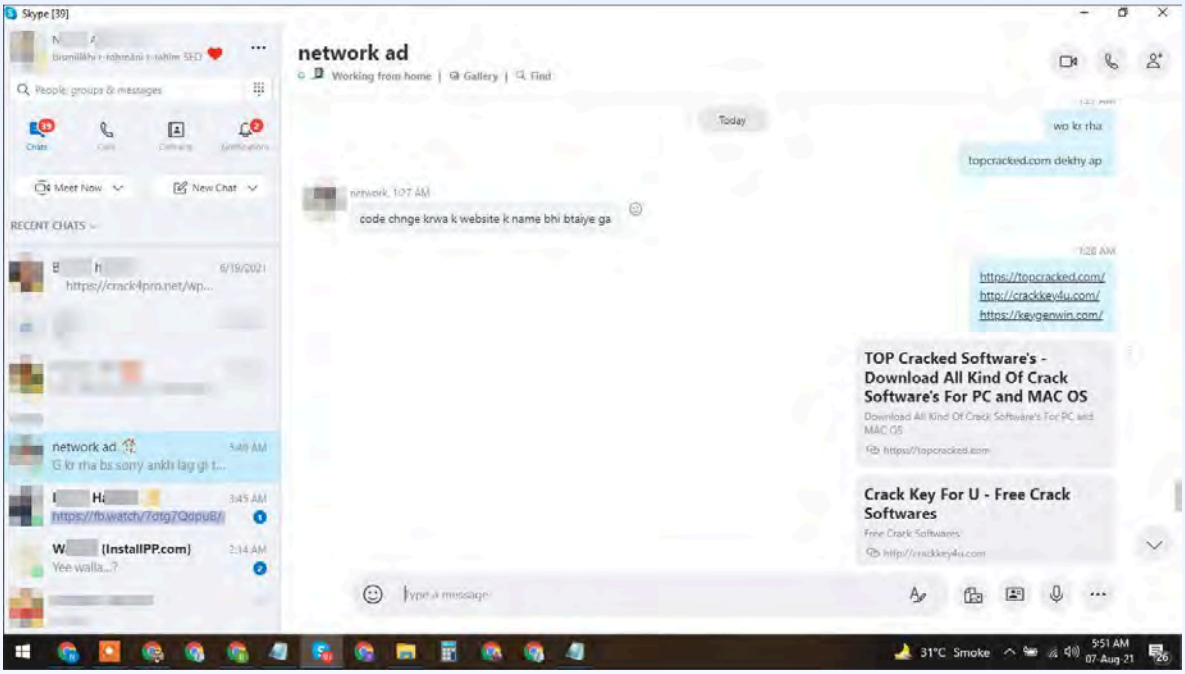
https://www.forumsforums.com/	[redacted]	[redacted]	ServiceAbuse
https://www.forumsforums.com/	[redacted]	[redacted]	ServiceAbuse
https://www.forumsforums.com/	[redacted]	[redacted]	ServiceAbuse
https://www.insta360.community/	[redacted]	[redacted]	ServiceAbuse
https://www.linkedin.com/checkpoint/lg/login-s	[redacted]	[redacted]	ServiceAbuse
https://www.plurk.com/signup	[redacted]	[redacted]	ServiceAbuse
https://www.quia.com/newstudent_info.html	[redacted]	[redacted]	ServiceAbuse
https://www.quia.com/newstudent_info.html	[redacted]	[redacted]	ServiceAbuse
https://www.quia.com/newstudent_info.html	[redacted]	[redacted]	ServiceAbuse
https://www.quia.com/newstudent_info.html	[redacted]	[redacted]	ServiceAbuse
https://www.quia.com/newstudent_info.html	[redacted]	[redacted]	ServiceAbuse
https://www.scoop.it/subscribe	[redacted]	[redacted]	ServiceAbuse
https://zubicrack.com/wp-login.php	[redacted]	[redacted]	ServiceAbuse
https://ariscommunity.com/users/[redacted]/edit	[redacted]	[redacted]	Service Abuse
https://app.ahrefs.com/user/login	[redacted]	[redacted]	SEO Tools
https://app.neilpatel.com/en/login	[redacted]	[redacted]	SEO Tools
https://app.neilpatel.com/en/register	[redacted]	[redacted]	SEO Tools
https://app.sparktraffic.com/reset-password-fi	[redacted]	[redacted]	SEO Tools

Snippet of the Log containing Threat Actor's Credentials to the admin portal of zubicrack.com

Infrastructure Overlap & Stealer-Log Evidence

Further investigation of malware logs associated with similar cracked domains uncovered a substantial overlap in WordPress sites. Another log belonging to another Threat Actor (N***** A*****/H*****), who is likely connected to the initial Threat Actor (M******* H*****) via surname, contained over **2500 credentials linked to WordPress delivery sites**, with numerous mentions of a common Surname. A screenshot from this TA's stealer log provided crucial details, including Skype conversations. Specifically, a chat with **another TA with the same surname (B***** H*****) discussed "crack4pro.net,"** a significant indicator.

The frequent recurrence of the surname "H*****" suggests a potential family-run operation. However, it's important to acknowledge that "H*****" could be a common family name in Pakistan.



*Malware's Screenshot of Second Threat Actor's (N***** A*****/H*****) computer*

Pivot to Pay-Per-Install (PPI) Networks

Key Findings

1. **Family-centred operation:** Credential patterns, shared payout accounts, and matching GMail IDs indicate a multi-generational "H*****" affiliate ring. This is strongly supported by the "Name Pattern" in the financial analysis showing multiple "H*****" surnames.
2. **Threat Actor Overlapp:** Both networks exhibited an overlap among established and long-standing participants, indicating competition between two distinct PPI networks operating within the same region.
3. **Law-enforcement leverage:** InstallBank's compromised backend and SQLi flaw provide a high-fidelity dataset for warrants and financial tracing; SpaxMedia/Installstera exposes enough operational metadata (domain analytics, payment tokens) to build probable-cause dossiers.

Credential-Based Lead Generation

- Leaked stealer logs for (M******* H*****) and N***** A*****/H***** contained dozens of credential pairs for accounts on two PPI panels.
- Parsing those logs surfaced two core affiliate networks that underpin the delivery ecosystem:
  - **InstallBank.com** – legacy network, operational since ≈ 2018.
  - **SpaxMedia.net** – later venture (2022–2024) that resurfaced as Installstera.com after takedown.

Network #1 – InstallBank.com

Attribute	Details
Status	**Defunct (as of Aug 2025) (Was Active May 2025)**
Age / First Seen	Defunct (as of Aug 2025) (Was Active May 2025)
Age / First Seen	Earliest indexed hostnames mid-2018; cited in Sophos 2021 blog on fake-pirated-software PPI. Database shows traffic data from May 2020 - May 2025.
Operator Linkage	Credential dumps include Admin login plus >130 PPI Affiliate accounts tied to Pakistani emails, some carrying the H***** surname.
Compromise Vector	Admin creds exposed in MetaStealer log → direct panel access recovered. SQLi vulnerability on id parameter allowed full database exfiltration (affiliate ledger, payout history).

Network #2 – SpaxMedia → Installstera

(Selected dashboard screenshots from the SpaxMedia panel are available in Appendix C;)

Attribute	Details
Timeline	SpaxMedia operational ca. 2022-07; suspended 2024-11 after possible LE action. Re-launched 2025-02 on Installstera.com with the same code-base & user-base.
Operator Linkage	Social ads & stealer logs tie S****** H***** (Instagram @s******h*****official) to both brand names. Likely mother/guardian of M******* H***** the initial Threat Actor; and shares Bahawalpur address.
OpSec Fail	Public Facebook/ profiles reuse corporate email — same address in panel footer for “Contact Us”. SpyCloud Intel Vendor identified the same.

Current Access	No working admin creds in leak corpus. Affiliate creds for m*******h********@gmail.com (TA1) initially failed but succeeded when switching to secondary password variant → revealed account dashboard. Notably, M*******'s payout ledger is blank, hinting at off-panel settlement (family bookkeeping).

Comparative Snapshot

Metric	InstallBank	SpaxMedia / Installstera
First seen	2018-2025	SpaxMedia operational
Current state	Offline (Host Down)	Installstera online; SpaxMedia offline
Compromised admin?	**Yes – full DB (Partial Access Logs)**	No
SQLi present?	**Yes – confirmed**	Unknown (not reproducible)
Unique affiliates	~5200 (InstallBank DB shows 5,239)	Unknown
Common Affiliates	Yes	

Limitations & Confidence

- **Data Gaps:** Only 6 months of payouts vs. 5 years of traffic; no full SpaxMedia DB (screenshots only). Confidence: Medium (75%) on lifetime revenue extrapolation.
- **Attribution Risks:** Family names (e.g., Hashmi) common in Pakistan; potential aliasing. Confidence: High (90%) via credential/email overlaps.
- **Traffic Inflation:** Bot traffic may skew clicks (e.g., gambling spam on compromised WP sites). Confidence: Medium (70%) on clean install counts.
- **Temporal Bias:** 2020 focus; post-2020 metrics shift to downloads. Confidence: High (85%) on trends.
- **Victim Impact:** No direct victim data; inferred from installs. Confidence: Low (60%).

Overall Confidence: High (85%) – Leaked DB provides ground truth; stealer logs add corroboration.

Actor Landscape

Primary operators

Four principal operators—M***** H*****, M******* S****, Z***** I******, and N***** I*****/H*****/A***** along with S****** H*****—are identified as key figures in this multi-actor network. These individuals are the owners and primary operators of both interconnected PPI networks. A* and M* oversee and run InstallBank, while the others manage SpaxMedia, coordinating its underlying infrastructure and actively promoting the warez sites.

Organisational structure & roles

The network exhibits a clear division of labor:

- **Primary Operators:** Likely handle the strategic direction, PPI panel management (InstallBank, SpaxMedia/Installstera), and overall financial operations.
- **Affiliates/Publishers:** Responsible for generating traffic by creating and maintaining warez distribution websites, leveraging SEO and forum spam, and directing victims to the PPI loaders.
- **Financial Facilitators:** Manage the payouts and potentially off-ledger settlements, utilizing methods like Payoneer and Bitcoin.

Infrastructure Mapping

The network operates across thousands of domains and utilizes various tactics to deliver malware.

Delivery Domain Taxonomy

The network employs a diverse range of domains for different purposes:

- **High-value blogs:** Long-running WordPress sites like pcgamez-download.com, up4pc.com (with pcgamez-download.com alone accounting for 1.3 million installs and over $100k revenue). These sites generate significant click-throughs (≥ 500 k clicks each).
- **Throw-away redirectors:** Short-lived domains using TLDs like .cfd, .lol, .cyou, often with < 30-day lifespans, used to create distance between the initial compromised entry point and the final payload.

PPI Networks & Monetisation

The core of the operation revolves around Pay-Per-Install (PPI) networks, primarily **InstallBank.com** and **SpaxMedia/Installstera.com.** These platforms serve as the monetization engine, paying affiliates for each successful install or download of their payloads. The database analysis reveals:

- **Total Users:** 5,239 registered affiliates.
- **Total Websites:** At least 3500 websites were used to drive traffic.
- **Monetization Model:** Affiliates are paid per successful "install" or "download" as tracked by the PPI network. The eCPI (Effective Cost Per Install/Download) was analyzed at ~$0.0693 based on actual payouts, with the network capturing a significant profit margin.

SEO & Forum-Spam Infrastructure

The primary traffic generation mechanism relies heavily on:

- **Search Engine Optimisation (SEO):** Malicious warez sites are optimized to rank highly for piracy-related keywords.
- **Forum Spam:** Exploiting public discussion forums (e.g., Honor website forum post) to inject malicious links and enhance SEO. The use of SEO and marketing tools was explicitly noted for indexing sites and generating backlinks.

Financial Analysis

The InstallBank database, providing 5 years of traffic data (May 2020 - May 2025) and 6 months of detailed financial records (May - October 2020), offers an unprecedented view into the financial workings of a major PPI network.

InstallBank (May–Oct 2020 Ledger Snapshot)

Headline numbers

- Total installs recorded in ledger (payment period): **1,883,399**
- Total publisher payouts (6 months): **$130,560.53**
- Average eCPI (payout per install, 6-month period): **$0.0693**
- **Total Lifetime Revenue Tracked (2020-2025): $4,672,823**

Monthly Breakdown of Payouts

Month	Total Payout	Payment Count	Average Payment
2020-05	$20,242.52	23	$880.11
2020-06	$8,814.72	16	$550.92
2020-07	$46,304.87	67	$691.12
2020-08	$10,837.54	22	$492.62
2020-09	$31,916.91	73	$437.22
2020-09	2020-10	22	$565.63

Total Documented Payouts: $130,560.53

Payment Method Analysis

The payment distribution reveals a surprising preference for traditional payment processors over cryptocurrency, contrary to typical cybercrime patterns:

Payment Method	Amount	Percentage	Payment Count
Payoneer	$87,566.61	67.10%	156
Bitcoin	$40,329.55	30.90%	45
WebMoney	$2,132.72	1.60%	13
PayPal	$531.65	0.40%	9

Headline numbers

- **Payoneer dominates** with 2/3 of all payments, suggesting sophisticated financial operations and a facade of legitimacy.
- **Bitcoin usage (31%)** indicates OpSec awareness but is not the primary preference for payouts during this period.
- The reliance on traditional processors suggests these operators may have appeared legitimate to payment providers.
- **High average payouts ($585.47)** indicate significant revenue per affiliate.

eCPI (Effective Cost Per Install) Analysis

For the documented payment period (May-October 2020):

- **Period Installs:** 1,883,399
- **Period Revenue:** $191,249.86 (revenue associated with these installs)
- **Actual Payouts:** $130,560.53
- **eCPI (Revenue Basis):** $0.1015
- **eCPI (Actual Payout):** $0.0693

Analysis: The network captured approximately **68% of tracked revenue as profit margin ($60,689.33)** during this specific period, indicating a sustainable and highly profitable operation.

Preliminary Observations (sourced from leaked dashboard screenshots for SpaxMedia)

- **Payout data origin** – Unlike InstallBank (SQL-backed), SpaxMedia figures are gleaned from front-end dashboard access via reused/compromised affiliate credentials. No direct database dump was available, so the amounts are sampled from the screenshots you provided (PNG set, June 2021 → Mar 2025).

- **Regional footprint** – User roster skews heavily toward Pakistani names, hinting that SpaxMedia relied on Facebook ads, WhatsApp groups, and word-of-mouth in local circles rather than broad SEO spam.
- **Marketing strategy** – Evidence of sponsored posts and affiliate-recruitment creatives on Facebook and other surface-web platforms. This contrasts with InstallBank's longer-running, forum-based promotion on BlackHatWorld, BeerMoneyForum, and similar "earn-online" boards.
- **Scale comparison** – Screenshot sample shows dozens of payouts per affiliate, typically in the US $50 – $300 range. While sizable, this is an order of magnitude smaller than InstallBank's top-tier payouts and suggests a more modest install volume.

See Appendix C for full-resolution SpaxMedia payment dashboard captures.

Blockchain Clustering Insights

While the InstallBank database provides explicit Bitcoin payout data, deeper blockchain analysis is needed to cluster associated wallets and trace funds, especially for off-ledger revenue. The documented 31% Bitcoin usage provides a strong starting point for such investigations.

After some basic analysis we can see that the threat actors use common methods like:

1. Mixers
2. Automated transfers
3. Onion peeling

Etc to make it difficult for investigators to analyse the block.

There were 19 unique BTC addresses that were being used for transfer of capital. At the point of writing this report all the wallets have been emptied out.

The addresses were in use from early 2018 to the last transaction in late 2024, which also confirms our timeline of traffic analysis.

A total of 145.806 BTC moved across these 19 addresses during that time and a total ~2000 transactions were made.

Traffic Analysis

The **InstallBank** database offers a 5-year view of traffic data (May 1, 2020 - May 7, 2025), revealing significant growth and an evolution in the network's operational strategy.

Yearly Evolution (2020-2025)

Year	Clicks	Downloads	Installs	Revenue	CTR	Install Rate
2020	25,661,566	0	2,439,515	$292,229	0%	N/A
2021	78,555,935	15,074,201	663,493	$865,188	19.20%	4.40%
2022	90,299,338	12,762,457	1	$1,184,530	14.10%	0%
2023	103,205,747	54,715,538	2	$1,474,169	53%	0%
2024	125,736,141	68,654,562	9,318	$813,012	54.60%	0%
2025	26,032,744	15,637,564	0	$43,902	60.10%	0%

Website Lifespan Categories

Category	Website Count	Total Installs	Average Lifespan
Long-haul (>365d)	383	2,642,227	>1 year
Medium (90-365d)	248	287,167	3-12 months
Short-lived (<90d)	145	182,935	<3 months

Key Trends Identified

1. **Business Model Evolution:** There's a clear **shift from install-focused (2020) to download-focused (2021+)**. This suggests a change in how the network tracks and monetizes successful victim engagements, potentially to evade traditional install-based detection or to diversify their revenue streams.
2. **Traffic Growth:** The network experienced significant growth, with a **4.9x increase in yearly clicks from 2020 to its peak in 2024**. This demonstrates substantial SEO and marketing capabilities.
3. **CTR Improvement:** The click-through rate (CTR) improved dramatically from 19% in 2021 to 60.1% in 2025, indicating more effective targeting and content optimization.
4. **Install Rate Collapse:** Install tracking nearly ceased after 2020 (dropping to near zero in 2022, 2023, and 2025). This could suggest:
    - A change in payload deployment/tracking methodology.
    - Improved anti-detection measures by the operators, making install tracking by the panel less reliable.
    - A shift in focus towards different monetization models not solely reliant on direct "installs" as defined by the panel.

2020 Monthly Breakdown (Payment Period Context)

Category	Installs	Downloads	Revenue
2020-05	261,072	0	$25,744
2020-06	207,529	0	$21,488
2020-07	275,819	0	$30,197
2020-08	230,144	0	$22,844
2020-09	518,402	0	$44,832
2020-10	390,433	0	$46,145

Notable: September 2020 shows a significant spike in installs (518k vs ~250k average), correlating directly with higher payouts in that month.

Key Insights:

- **Long-term Operations: 383 sites operated for over a year**, generating **85% of total installs**, indicating significant investment in persistent infrastructure.
- **Burn Rate: 145 sites (18%) lasted less than 90 days**, suggesting a high takedown or abandonment rate for disposable infrastructure.
- **Domain Strategy:** The network employs a mixed strategy of maintaining long-term, high-value sites alongside a churn of short-lived, throwaway domains.

Operational Insights & Attribution

The comprehensive database analysis provides deep insights into the operators' identity, sophistication, and structure.

Geographic Concentration

Based on operator names, email domains, and payment preferences:

- **Primary Base:** Pakistan is clearly the primary operational base, evidenced by prevalent names and the significant number of Pakistani-tied email addresses and bank accounts.
- **Payment Infrastructure:** The reliance on Payoneer and other traditional payment processors suggests that operators have access to and are comfortable using legitimate financial services.

Geographic Concentration

- **Financial Management:** The professional use of **Payoneer for two-thirds of payments** suggests a facade of business legitimacy and a sophisticated approach to financial transactions, avoiding sole reliance on less traceable methods.

- **Infrastructure Resilience:** A **5-year operational lifespan** for the network and the existence of **383 "long-haul" websites** operating for over a year indicate highly resilient operations capable of withstanding various disruption attempts.
- **Scale:** With **over 449 million clicks** and an estimated **$4.67 million in lifetime revenue**, the network demonstrates exceptional SEO and marketing capabilities to attract and convert a massive user base.

Victimology & Impact

The campaign's global reach, primarily targeting consumers searching for pirated software, has led to a significant number of infections and data breaches.

Detection & Mitigation Guidance

Effective disruption requires a multi-pronged approach targeting various aspects of the PPI network's operations:

- **User Education:**
  - Educate users about the dangers of downloading cracked software from unofficial sources.
  - Promote the use of legitimate software and strong security practices (e.g., password managers, multi-factor authentication).
- **DNS & Domain Takedowns:**
  - Target **long-haul domains (383 sites operating >1 year)** for maximum operational impact.
  - Collaborate with registrars like Cloudflare (often used by these operators) to report abuse and suspend malicious domains.
- **Payment Processor Interdiction:**
  - **Coordinate with Payoneer** and other traditional payment providers to investigate and freeze accounts linked to known operators and their significant payouts.
  - Share intelligence on Bitcoin addresses used for payouts to aid cryptocurrency tracing and interdiction.
- **Search Engine & Content Platform Action:**
  - Platform providers like Honor Club forum, Community Forums and Google should continuously monitor public data for better internet safety.
  - Monitor for new SEO and forum spam campaigns.

- **Endpoint Detection & Response (EDR) / Antivirus (AV):**
  - Develop and update signatures for common PPI loaders and commodity stealers (Lumma, Meta, RedLine) used by these networks.
  - Monitor for unusual process execution chains, particularly those originating from common download directories or associated with cracked software.
- **Network Perimeter Defenses:**
  - Implement robust web filtering to block access to known malicious domains and IP addresses (IOCs from Appendix A).
  - Employ intrusion detection/prevention systems (IDS/IPS) to identify and block C2 communication patterns associated with infostealers.

Future work should focus on

- Continuous monitoring of warez ecosystems for new domain registrations and affiliate activity.
- Leveraging additional compromised data sources (if available) to fill financial and operational gaps.
- Proactive engagement with payment processors and domain registrars for rapid disruption.
- Developing and deploying automated tools for tracking and analyzing PPI network evolution.

Conclusions & Strategic Implications

The InstallBank database represents one of the most comprehensive views into a major pay-per-install network operation. The warez ecosystem effectively turns software-piracy demand into a turnkey malware channel. Each new cracked-software trend sparks an infection wave, and defenders must treat high-ranking warez domains as critical infrastructure for cyber-crime.

The financial analysis reveals a **sophisticated, profitable operation generating significant revenue through traditional payment channels like Payoneer**. The traffic analysis demonstrates remarkable scale and evolution, with the network successfully adapting to the changing cybersecurity landscape over 5 years. The clear attribution to **Pakistani operators**, combined with detailed financial records, provides law enforcement with exceptional opportunities for disruption. The scale of operations—**449 million clicks generating over $4.6 million in estimated revenue**—demonstrates the urgent need for coordinated international response to PPI networks.

Most significantly, this analysis reveals that major cybercrime infrastructure can operate successfully using **legitimate financial services**, suggesting that enhanced due diligence and cooperation between financial institutions and law enforcement may be the most effective disruption strategy. Coordinated action across search-engines, ad-networks, registrars, and PPI providers could reduce install volumes by > 70 % within a quarter.

Appendices

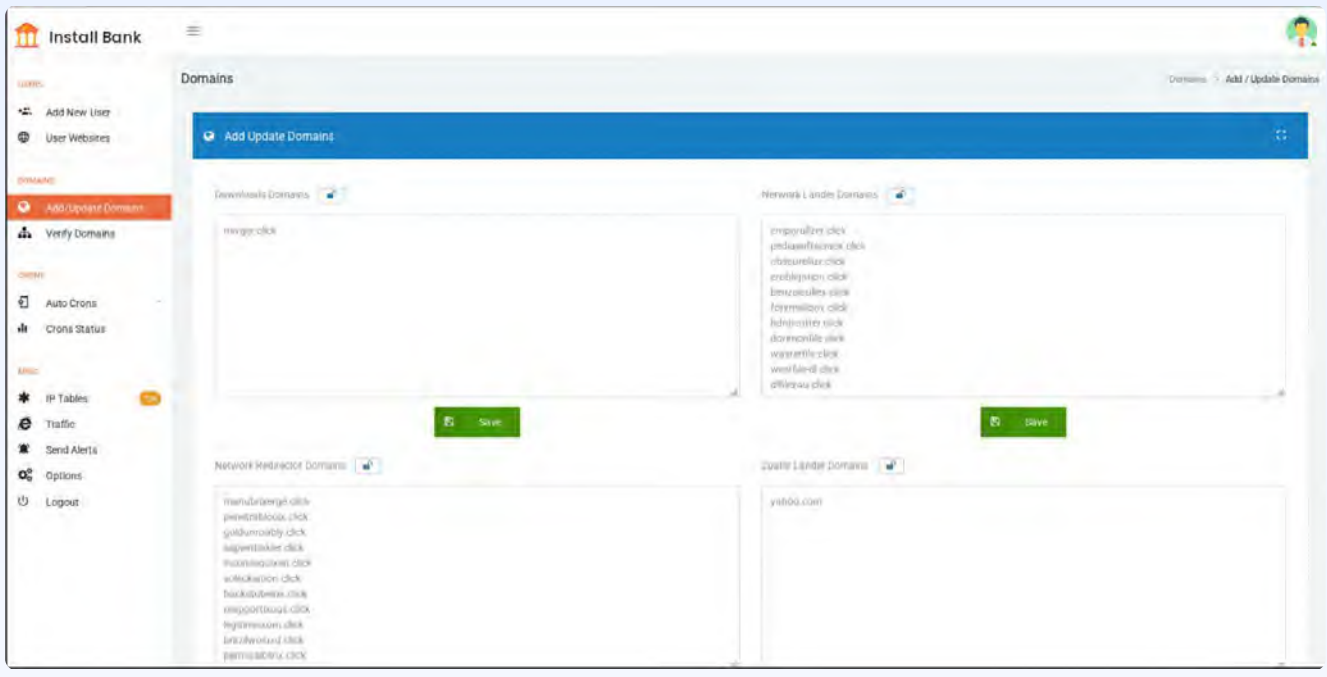
Appendix A Indicators of Compromise:

Link: https://drive.google.com/file/d/1djq3Sm2jgUHSfaKirIQRBIu42i4zR_fi/view?usp=sharing

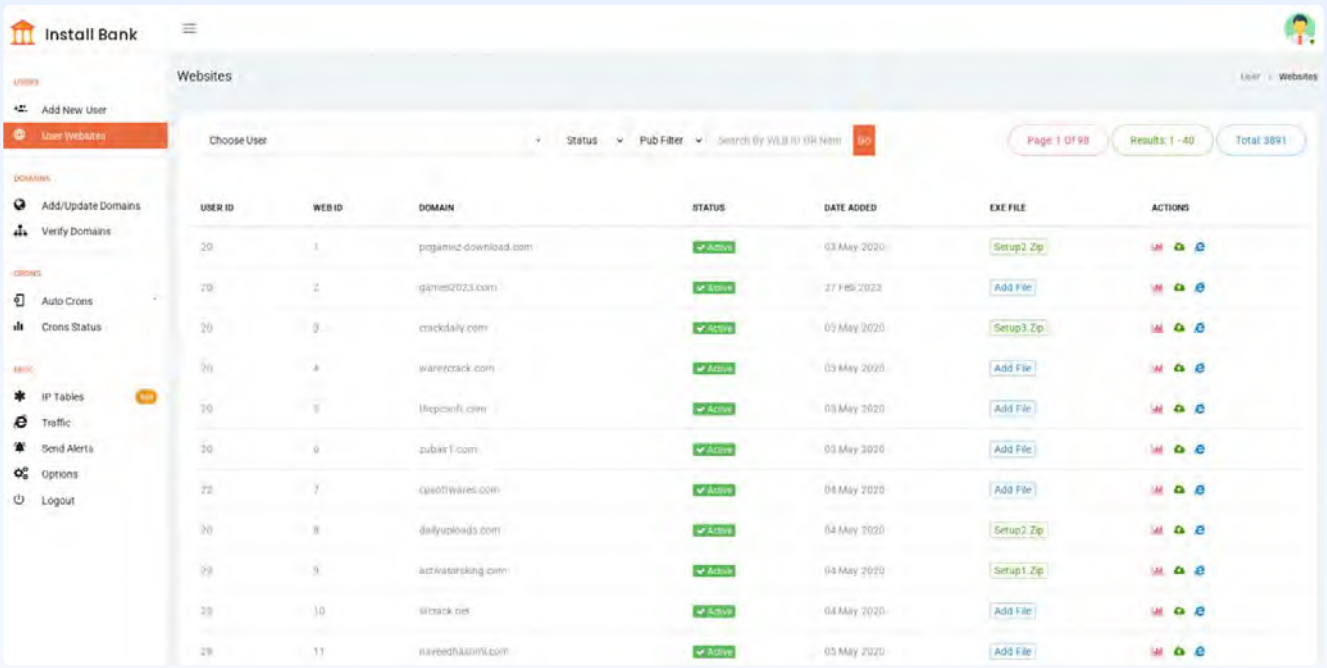
Appendix B Cryptocurrency Addresses used for Payouts - InstallBank Associated 2020 May-Oct :

129kSbWrWZCqhneqFhsRWoHKJ9qYLi5TMD
12GM9NMPuWc75b2NaptvcGaKgE9LzHrvjq
13JKkTjPHo2QJhrsogXhiJMY4tRorVaE5n
16phv2RLJMDWzf17LSWXfmpP3UQqu21UBc
17y3fnhGkANogmE74UCyguL32gkw5y2kM2
18RNr8tFqhZcXoKbWqDeq6eixkTDJgMMre
19PCyFzjjEQtLX2T7TUhGk2emNTZy78eVc
19YTuw79A4vhB6yZpJF8PvTcKLbHAcDkgz
1AE4HSDfdXii6STKNxbXk51DVvDu477ki8
1AyU68GmKLfaUgtXeHabivtcQ2RqYKXCn6
1HozE7DbD2Zf1VXHGL63Q1iTF9zGqitMw
1Lcm9psYbycgzkUSnNCzNZXUxafvEaNJAS
1LDpLdMo9otNYoPFmXf7auR1rd3fM8yo6E
1NnEzTBUyNqFcxPTA8ZyKbsQttkpPhE7u8
1oYP8ehHTRgK3MXPirsyii1owuhNYKYQe
1t6L4P1Nqw29HH2qT18rCSMfqUVcNVGNU
3DUFTHZ5zrrEuzVaxxd7HRFwYGU8fuVRuS
3EWJKza3a9PnYaiFBvNXzjzGfhhx2TejFV
3QTKaWZhGwoyaBCsFYpdbAWJF7CNtcAW8D

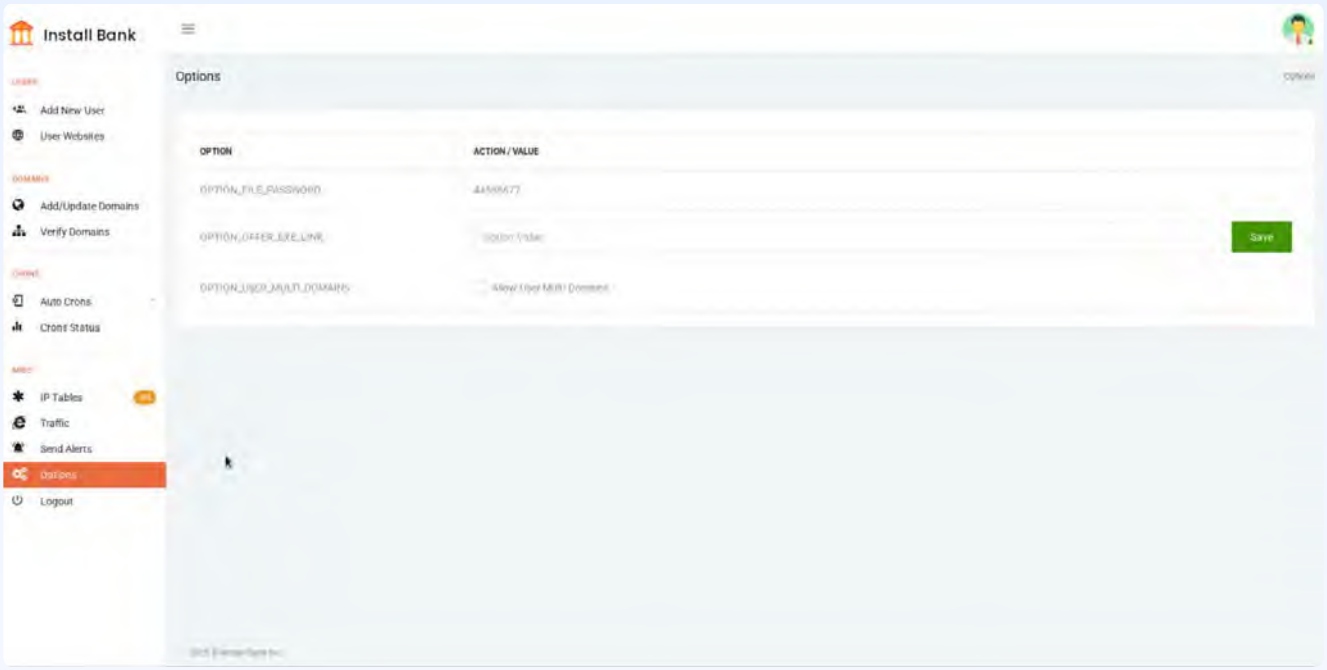
Appendix C SpaxMedia/Installstera Panel Screenshots:



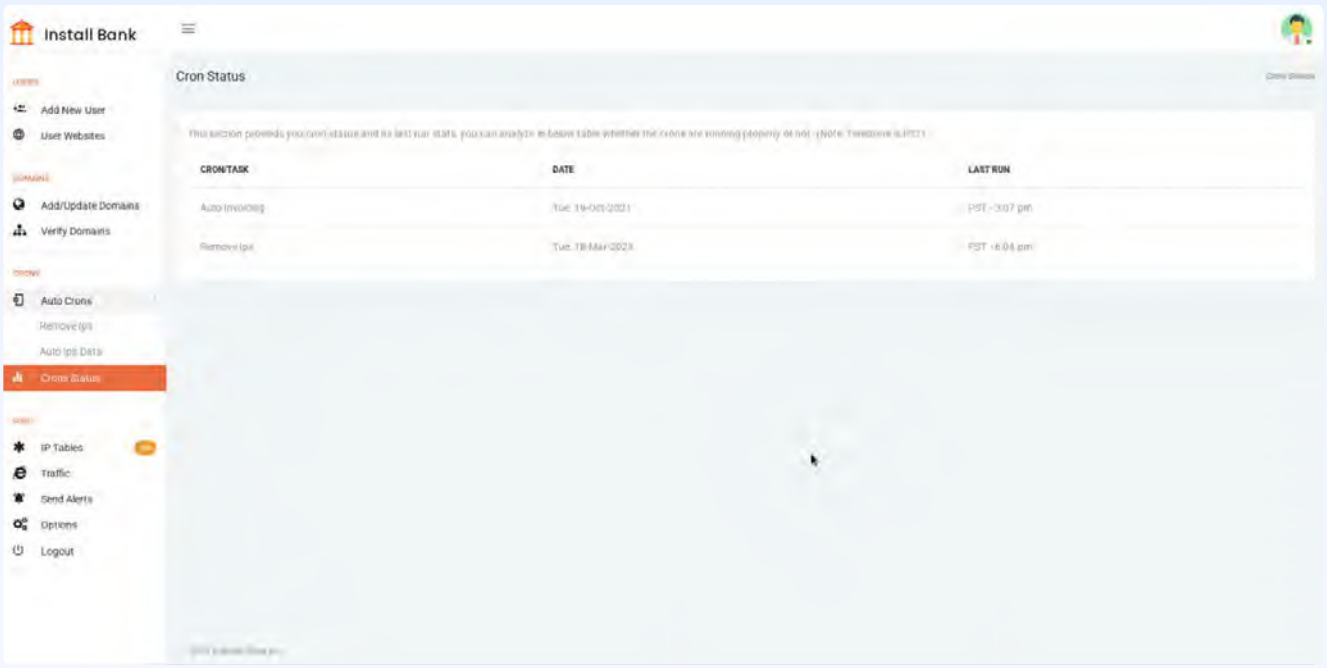
Redirection Domain Configuration page for InstallBank PPI Network



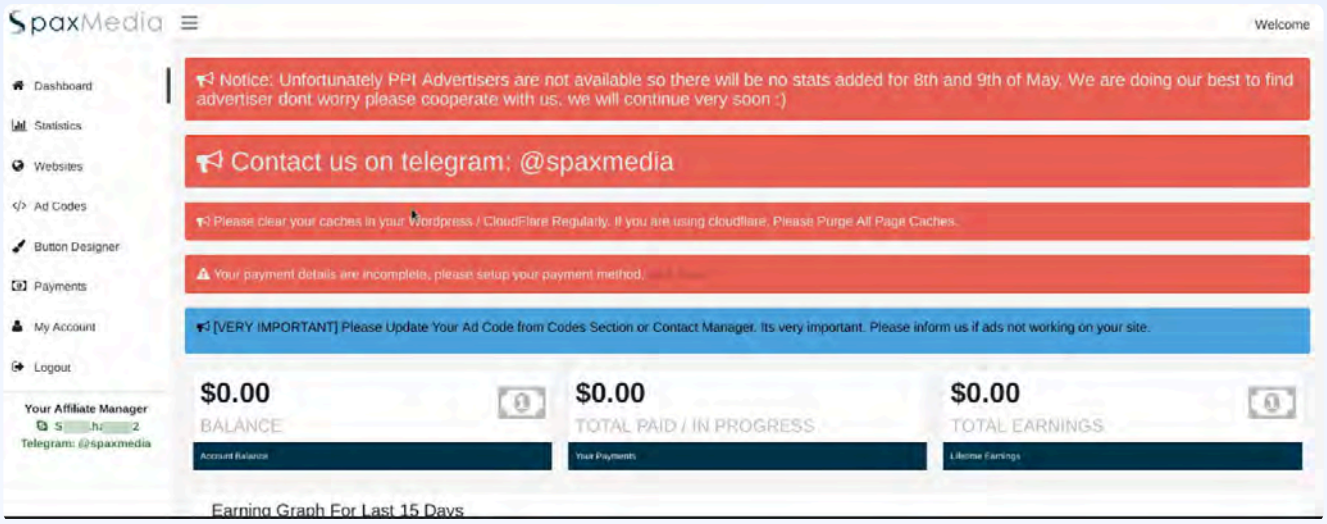
Domain Management Page of InstallBank Admins



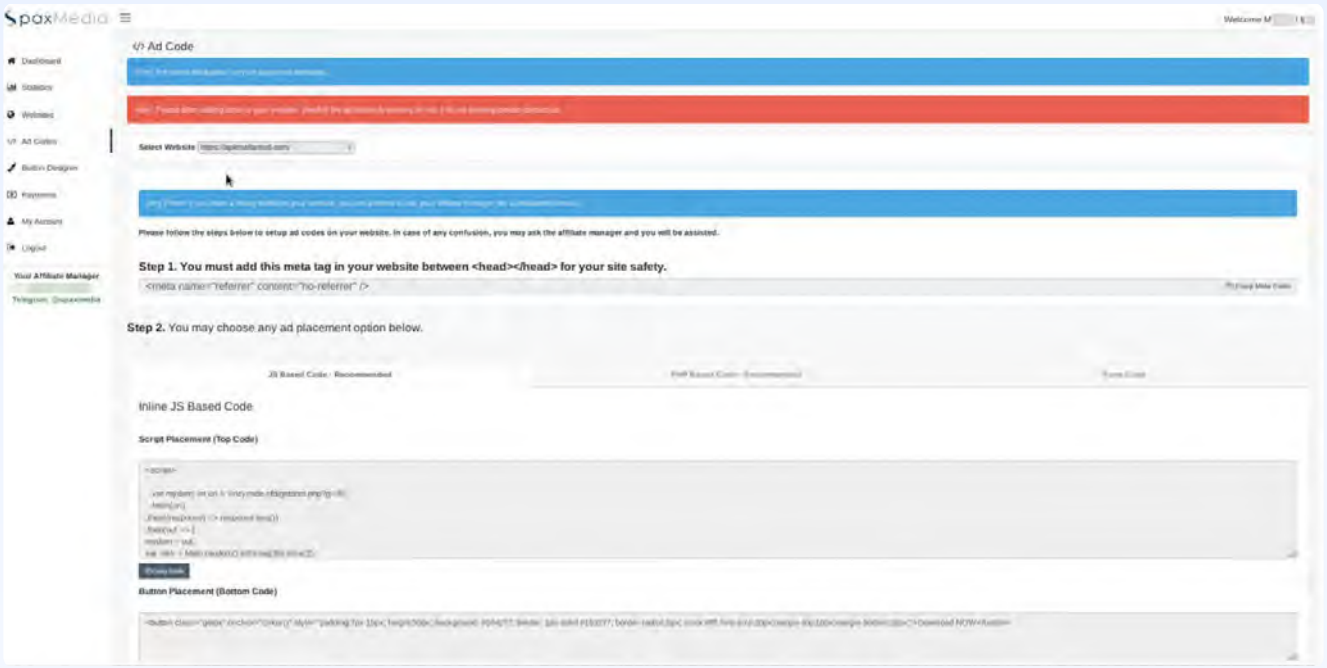
Trojanized Warez Configuration page, with Archiving Password and File Links.



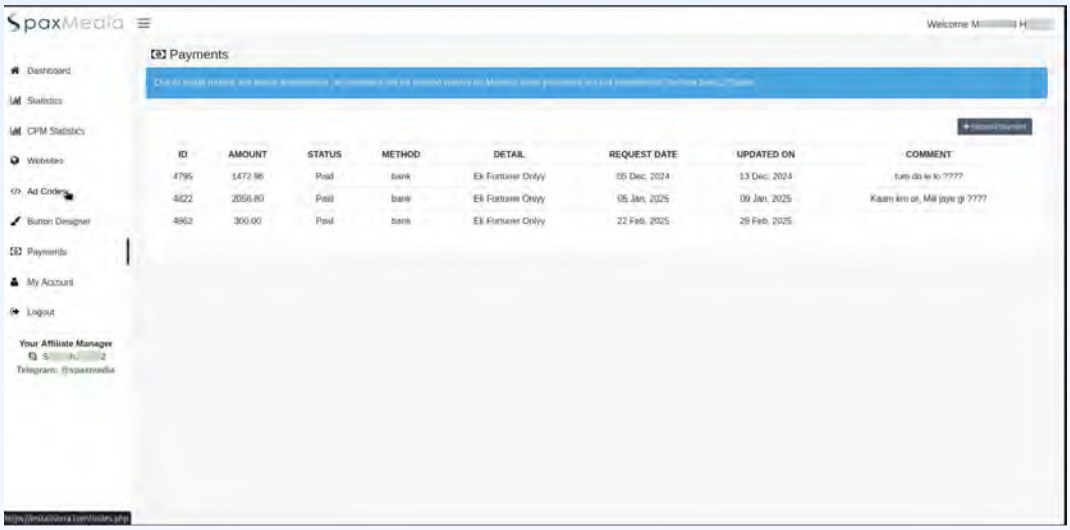
Admin's Cron Configurations for Site Management



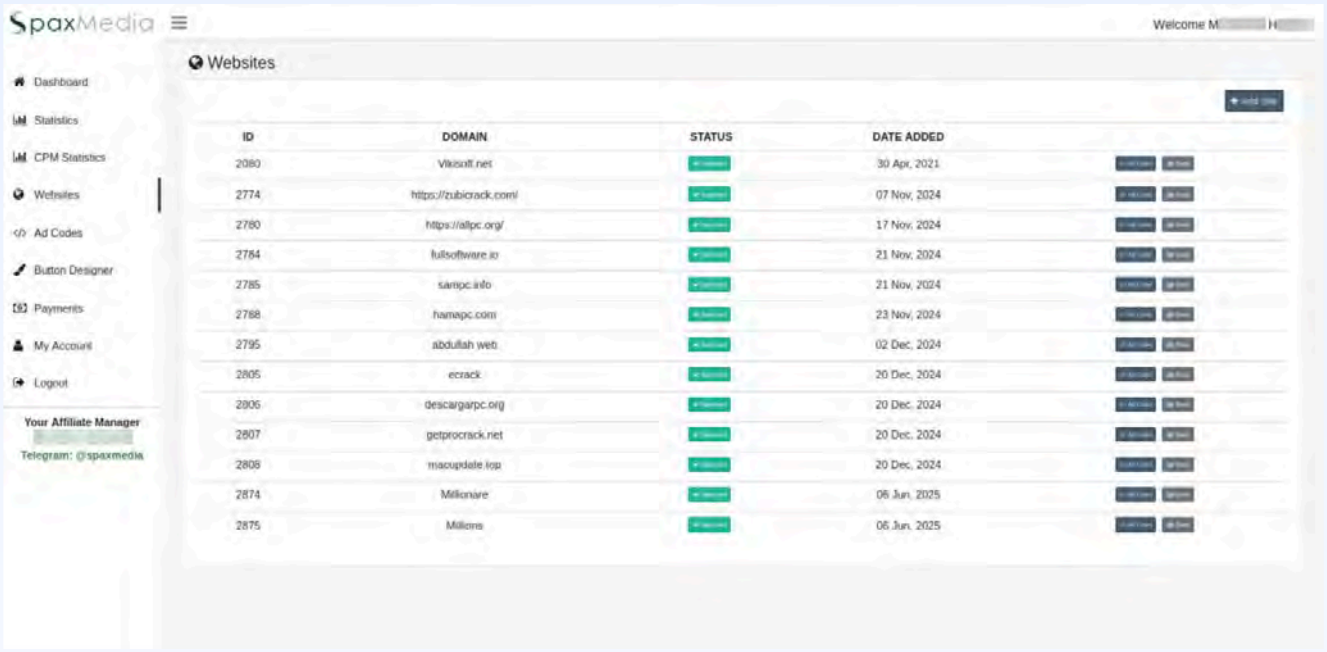
Affiliate view of SpaxMedia(Installstera)



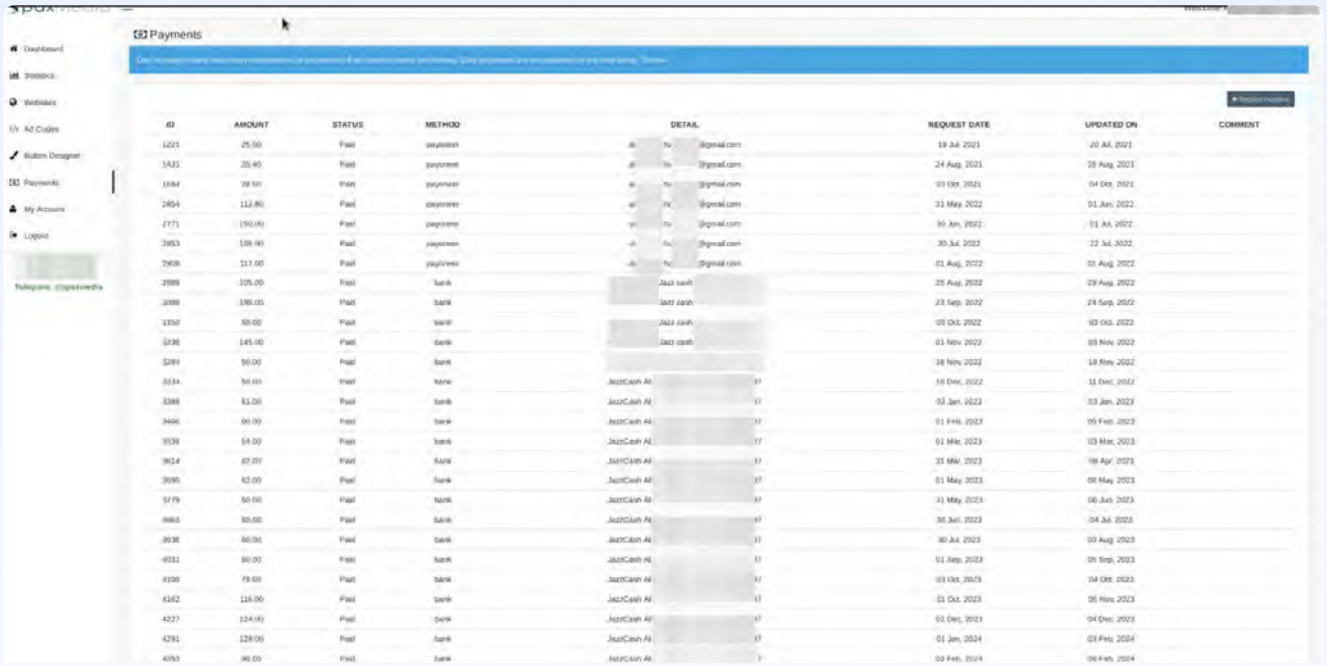
Installstera/SpaxMedia's configuration instructions for the Warez Websites using dynamic domain generator via ozycode.cfd



*M******* H*****'s Installstera/SpaxMedia Payouts further cementing the "Family Relations" between the Affiliates*

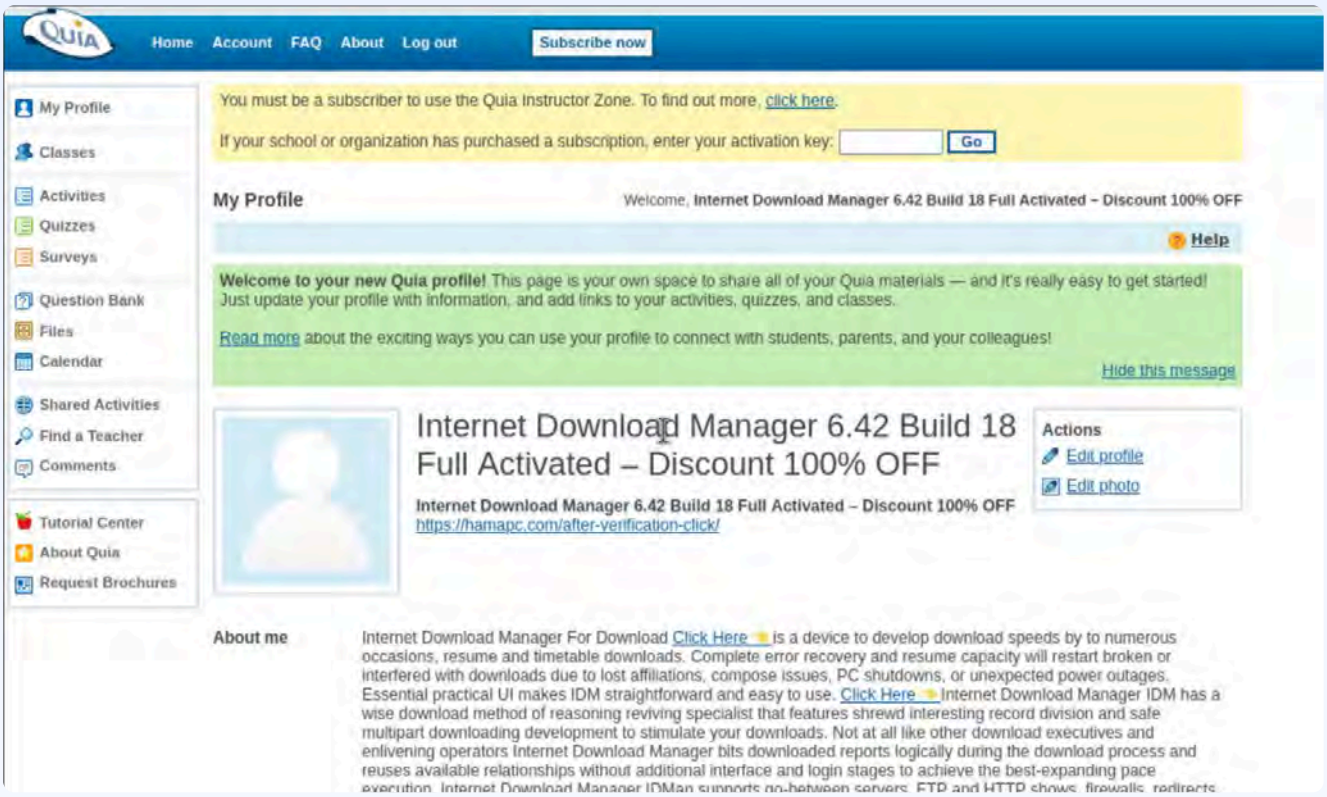


Affiliate's Warez Website Addition/Configuration Page of Spaxmedia/Installstera.com

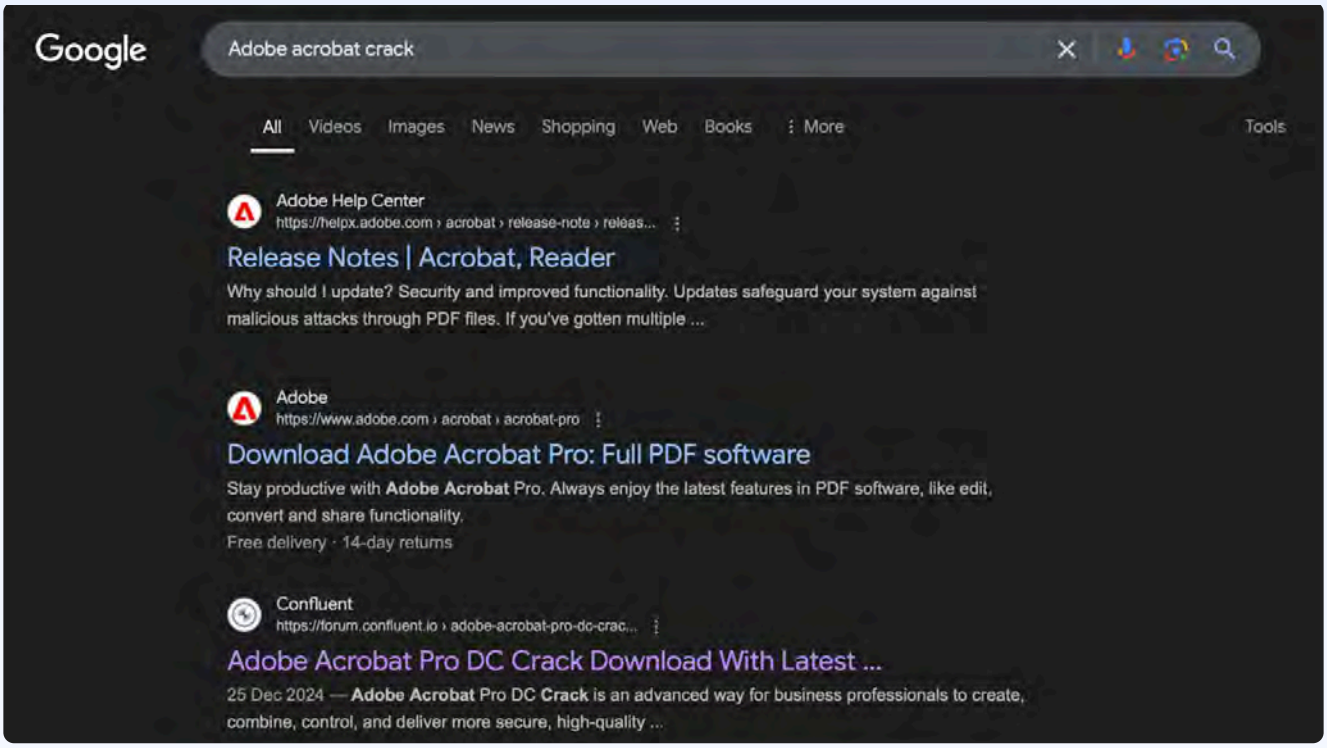


Other Affiliate's Payouts to JazzCash - Pakistani Mobile Wallet

Appendix D Forum Abuse Screenshots:

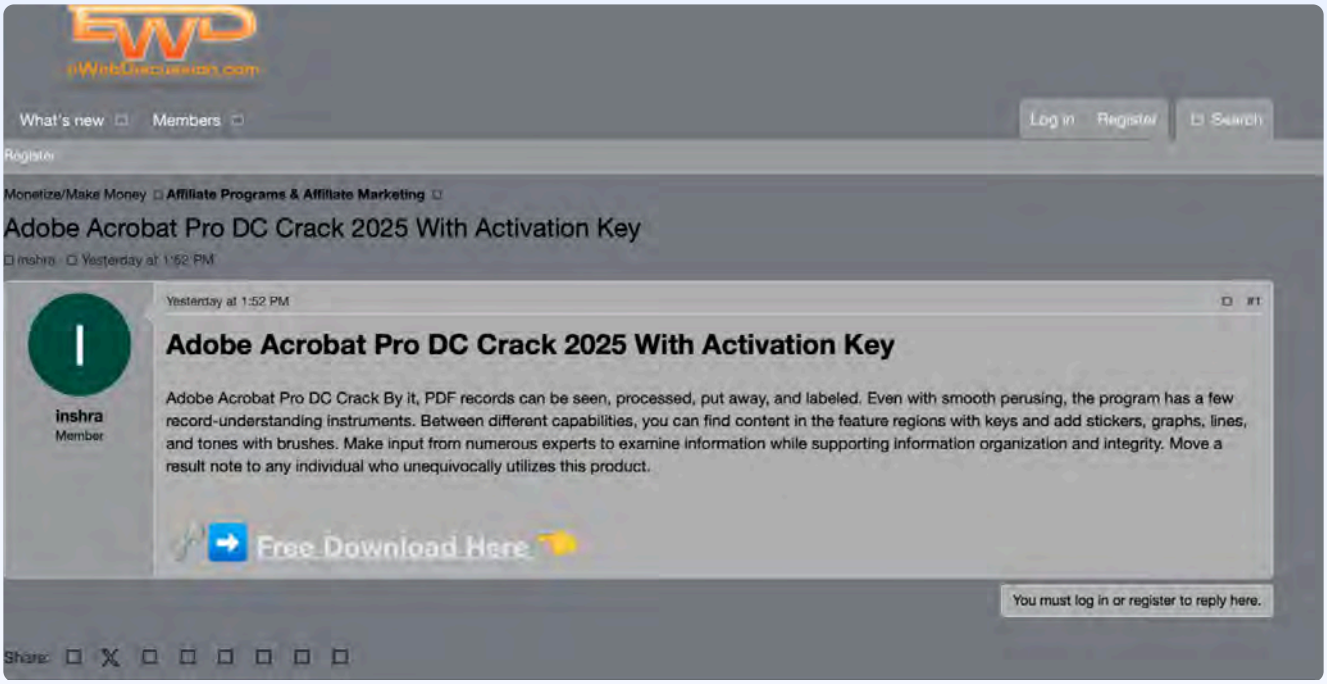


Educational Platform Quia Abused to spread Trojanized IDM Warez

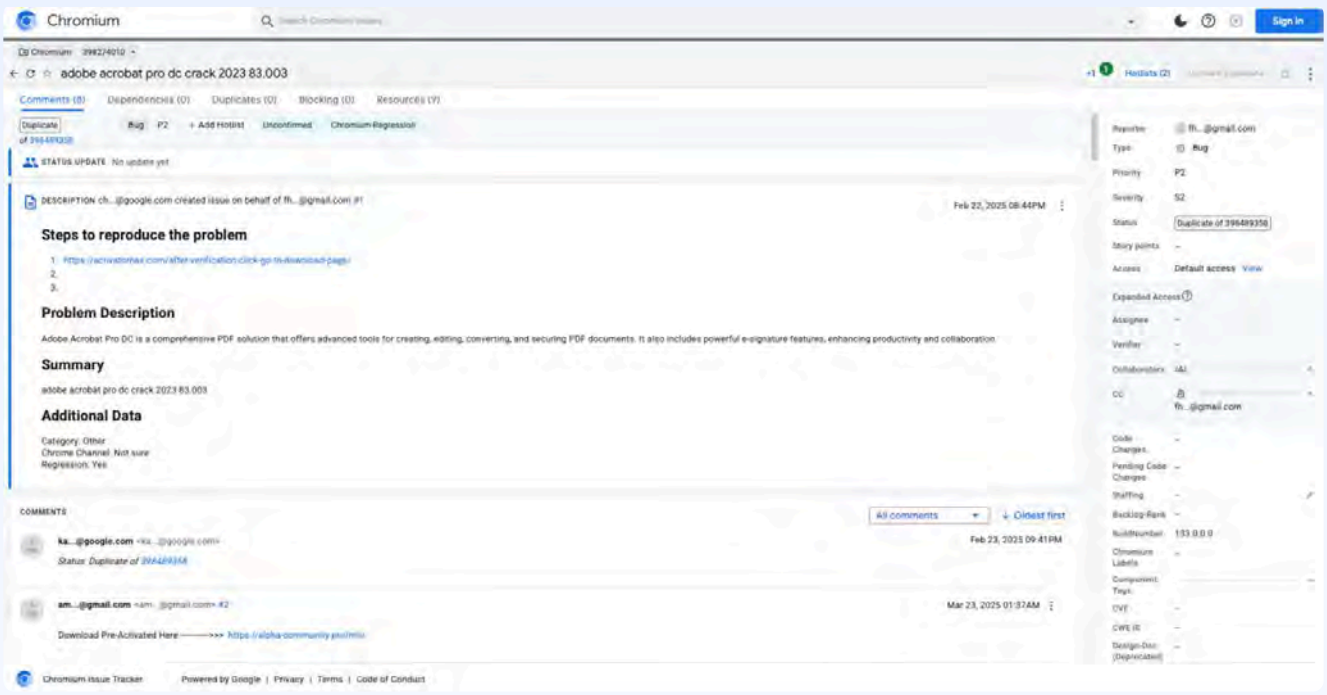


Confluent Forum Abuse to spread Trojanized Adobe Acrobat Warez

Appendix D Forum Abuse Screenshots:



EWD forum abuse to spread Trojanized Adobe Acrobat Warez



Confluent Forum Abuse to spread Trojanized Adobe Acrobat Warez

CloudSEK

Predict | Protect | Quantify

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.

Our Capabilities

- **Digital Risk Monitoring:** Real-time visibility and control over your digital assets.
- **External Attack Surface Monitoring:** Detect and mitigate vulnerabilities across 8+ Attack surfaces.
- **Third-party software & Supply Chain Monitoring:** Safeguard vendor ecosystems to prevent Supply chain breaches.
- **Cyber Threat Intelligence:** Proactively identify Indicators of Attack (IOAS) to stop threats in their tracks.
- **Cyber Risk Quantification:** Put a dollar value on potential threats to prioritize mitigation and demonstrate ROI.

95% Faster Threat Detection	**80% Reduced** Response time	**Zero** False Positives	**200+IAV** Use Cases

Why CloudSEK?

- **Predict Threats Before They Strike:** AI-driven intelligence to identify and mitigate threats at their source-before they become incidents.
- **Comprehensive Coverage:** Monitor 8+ attack surfaces and 200+ Initial Attack Vectors for full-spectrum visibility.
- **Contextual Intelligence:** Unified platform combines Cyber Intelligence, Brand Monitoring, Attack Surface Management, & Supply Chain Risk Analysis for actionable insights.

Trusted by Industry Leaders

NIC HCLTech HDFC BANK MetLife EMAAR & 300+ Organisation

ISO 9001 CERTIFIED · ISO 27001

#1 Threat Intelligence Vendor in APAC | Rated 4.8+ Gartner Peer Insights

aws Available in AWS Marketplace

GDPR COMPLIANT

info@cloudsek.com

www.cloudsek.com

Scan QR to Book a Demo