Appendix

TrendAI™ Research

Edge Under Siege: How State-Sponsored Actors Exploit Your Perimeter

APPENDIX A

Ivanti Connect Exploitation Case Study

Ivanti Connect Secure has been a recurring target since 2021, with four major campaigns within 18 months. With around 33,000 installations globally[1], concentrated in corporate and government sectors, and direct LDAP/AD integration, a single compromised device provides immediate network access.

CVE-2025-22457 is a stack-based buffer overflow in X-Forwarded-For header processing. CVSS 9.0, unauthenticated RCE affecting versions < 22.7R2.6. Patched on February 11, 2025; UNC5221 began exploitation mid-March, approximately 3-4 weeks post-patch. Mandiant published an advisory April 3.

UNC5221 deploys purpose-built tools for Ivanti persistence (the SPAWN Malware ecosystem). The next table shows some of the key elements:

Component	Function	SHA-256
SpawnMole	SOCKS5 tunneler, TLS certificate injection, magic byte activation	a3dbcc9d4e1dd523f2848689f7e0753465de6188c fac4d3a52389ab1ec3db83
SpawnSnail	Trojanized SSH backdoor, root privileges	4d7f4c330cdb4c16de4327b1b82f3cbe53d20c117 fffc972a2d3a47e01e0a65f
SpawnAnt	Installer/updater, redeploys other component	6f7e2148a5d20c17780a80e9bc9a198280820d 5340a77e11beed940124eadd7
SpawnSloth	Selective log wiper, timestamp manipulation	749cf36adc5513c92c7acc836d20935e3c433f3c 2d5641293e7a9c57c5ce22c2

Table 1. Spawn family components

SpawnMole hooks into the Ivanti web server process and patches TLS handshake functions. When it detects magic bytes (0x17 0x03 0x03 0x48 0x4F 0x4F 0x4B — “HOOK”) in a Client Hello, it redirects the connection to SpawnSnail on localhost:447. An embedded self-signed certificate (CN=QcCpIAsFy6cEI) authenticates the attacker. The certificate SHA-256:761bedf645f2dfc7c06538194da81499853944193356 94a73b4bd023d58bfd91

Certificate-based pivoting using the SpawnMole certificate identified two compromised hosts first seen in July 2024, six months before CVE-2025-0282 was publicly disclosed. This suggests either an earlier unknown zero-day or attacker test infrastructure. Once inside, attackers move quickly to consolidate access:

- **Credential harvesting:** UNC5330 stole LDAP bind credentials to escalate to domain admin.
- **Lateral movement:** FRP deployed to expose internal RDP (3389) and SMB (445) via outbound HTTPS.
- **Data exfiltration:** Custom framework stealing SSO cookies to access internal applications, bypassing MFA.

The following indicators can be used to detect SPAWN ecosystem activity.

File Hashes (SHA-256)

a3dbcc9d4e1dd523f2848689f7e0753465de6188cfac4d3a52389ab1ec3db836	*SpawnMole*
4d7f4c330cdb4c16de4327b1b82f3cbe53d20c117fffc972a2d3a47e01e0a65f	*SpawnSnail*
6f7e2148a5d20c17780a80e9bc9a1982f80820d5340a77e11beed940124eadd7	*SpawnArt*
749cf36adc5513c92c7acc836d20935e3c433f3c2d5641293e7a9c57c5ce22c2	*SpawnSloth*
c64f695e9e0855699d9e77790a56848b05b18390e8976815bcc1394a2aea6087	*RC4*
Webshell (key: ACcSPn2ZxBvmMapuTQJLezyFD3rbsqlO)	

Certificate Fingerprints

SHA-256: 761bedf645f2dfc7c06538194da8149985394419335694a73b4bd023d58bfd91 - SHA-1: c91c787c0a9d81faf149d3aa53ceab9fcabb3c20

Network Indicators

TLS magic bytes: 0x17 0x03 0x03 0x48 0x4F 0x4F 0x4B - Non-standard SSH ports: 447, 8447 - Fast Reverse Proxy (FRP) infrastructure

File Paths

/lib/libsecure.so.1 (SpawnSnail) - /lib/libdsproxy.so, /lib/libdsplibs.so (SpawnMole variants) - /lib/libupgrade.so (SpawnAnt) - Modified /data/runtime/scripts/checkintegrity.sh

APPENDIX B

Vulnerability Broker Pricing

TrendAI's ZDI has operated the world's largest vendor-agnostic bug bounty program since 2005, purchasing thousands of vulnerabilities from independent researchers and leading coordinated disclosure to affected vendors. Over two decades, ZDI has paid out tens of millions of dollars across virtually every software and hardware category. This gives us direct, first-hand visibility into what vulnerabilities are genuinely worth in a transparent, legitimate market.

The market data tells an important story about why edge devices have become the preferred target for state-sponsored espionage. ZDI's annual Pwn2Own competitions, where researchers compete to exploit fully patched devices for cash prizes, provide the most transparent public benchmark for vulnerability value across categories. What those figures reveal, when placed alongside pricing from offensive exploit acquisition markets that operate in parallel, is a structural anomaly: Edge device vulnerabilities are significantly underpriced relative to the strategic access they provide.

This appendix documents that pricing landscape across four market segments:

- China's state-directed domestic market
- Western nondefensive acquisition brokers
- Russian state-aligned procurement
- ZDI's own coordinated disclosure benchmark

Together, they explain why edge device exploits have become the tool of choice for cost-conscious state actors — affordable enough to burn, valuable enough to win.

Nvwa (女娲)

Source: https://web.archive.org/web/20250227080447/https://nvwa.org/

Open vulnerability acquisition programs once operated in China, though recent regulatory changes have made most of them publicly invisible. Historical data[2] from the Nvwa (女娲) Project's website nvwa.org provides insight into pricing and shows detailed pricing across categories, confirming that edge-device vulnerabilities were significantly cheaper than endpoint exploits.

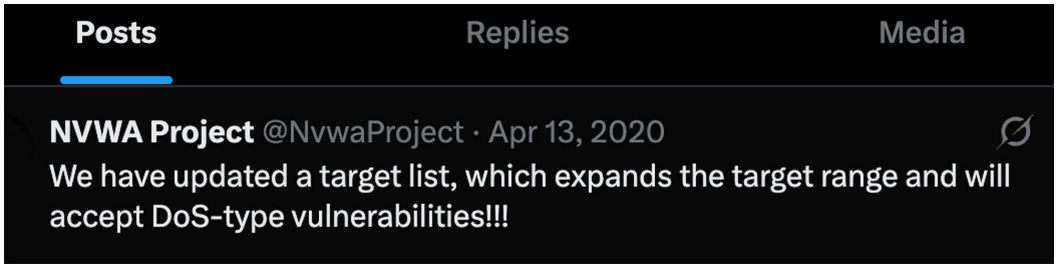

Figure 1. Nvwa Project's social media post showing how they were active in 2020[3]

F5	-	RCE	Zero-Click	2020-09-04	∞	500,000
F5 BIG-IP	-	RCE	Zero-Click	2021-01-05	∞	500,000
Fastjson	-	RCE	Zero-Click	2021-01-05	∞	500,000
Firefox	-	RCE+LPE	Zero-Click	2019-11-01	∞	800,000
FortiGate	-	RCE	Zero-Click	2020-08-07	∞	350,000
Fortigate-Firewall	-	RCE	Zero-Click	2019-11-08	∞	800,000
FortiNet	-	RCE	Zero-Click	2020-09-04	∞	350,000
Fortinet(飞塔) Firewall	-	RCE	Zero-Click	2021-01-05	∞	50,000
Foxit	-	RCE+LPE	1-Click	2020-09-04	∞	500,000
FreeBSD	-	LPE	Zero-Click	2020-08-07	∞	500,000

Figure 2. An archived screenshot from the now-defunct Nvwa website

To contextualize China's pricing, we surveyed the global vulnerability market. The breakdown below is compiled from publicly available price lists of several programs as of early 2026.

Crowdfense Exploit Acquisition Program (2024, USUS$30M total budget)

Crowdfense[4] is a high-end, UAE-based "exploit broker". Crowdfense buys zero-day exploits and sells them to a group of institutional clients. Their pricing confirm that edge device vulnerabilities are priced much lower than other exploits.

Target Category	Price Range
iOS zero-click full chain (iMessage	US$5,000,000 – US$7,000,000
Android zero-click full chain (WhatsApp, RCS)	US$5,000,000
Chrome one-click full chain (RCE+SBX+LPE)	US$2,000,000 – US$3,000,000
Safari one-click full chain (RCE+SBX+LPE)	US$2,500,000 – US$3,500,000

Table 2. Mobile (up to USUS$7M)

Target Category	Price Range
Windows zero-click full chain	US$1,000,000
Chrome full chain (desktop)	US$1,500,000
Firefox full chain	US$300,000
Word/Excel RCE	US$500,000
Outlook RCE	US$300,000
Windows LPE	US$100,000
Linux LPE	US$100,000

Table 3. Desktop (up to US$1.5M)

Target Category	Price Range
Cisco RCE	US$100,000
Fortinet RCE	US$100,000
Citrix RCE	US$100,000
SonicWall RCE	US$100,000
MikroTik RCE	US$100,000
Huawei RCE	US$100,000
Sophos RCE	US$100,000
Juniper RCE	US$75,000
D-Link / TP-Link / Netgear RCE	US$50,000
Ubiquiti RCE	US$50,000

Table 4. Routers, Firewalls, and Edge Appliances (up to US$100K)

Target Category	Price Range
Apache HTTP Server RCE	US$500,000
Microsoft IIS RCE	US$500,000
WordPress RCE	US$500,000
Microsoft Exchange RCE	US$250,000
Microsoft SharePoint RCE	US$250,000
SAP RCE	US$250,000
VMware ESXi / Hyper-V escape	US$500,000

Table 5. Enterprise Software

Other notable entries:

Ivanti, Zyxel VPN Firewall, WatchGuard, pfSense, F5 Big-IP, and KerioControl are listed but don't have published prices.

Zerodium (Historical Reference)

Zerodium[5] was the first company to publish a full zero-day pricing chart. Their last known public pricing similarly reflected how edge device exploits were significantly cheaper than mobile exploits.

Target Category	Price Range
Android zero-click full chain + persistence	US$2,500,000
iOS zero-click full chain	US$2,000,000
WhatsApp/iMessage RCE+LPE (zero-click)	US$1,500,000
Windows RCE (zero-click)	US$1,000,000
Chrome RCE (full chain)	US$500,000
Apache/IIS/Nginx RCE	US$200,000 – US$500,000

Table 6.

Zero Day Initiative (ZDI) — TrendAI's Coordinated Disclosure Program

ZDI[6] is the world's largest vendor-agnostic bug bounty program, operated by Trend AI since 2015. Unlike Zerodium or Crowdfense, ZDI is a coordinated disclosure program. Vulnerabilities are reported to the affected vendor and patched before any public release. ZDI does not sell exploits to other parties.

Important caveat for comparison: ZDI payouts are structurally lower than nondefensive brokers because researchers trade immediate payment for coordinated disclosure (e.g., vendor notification, patch coordination, and public credit). Nondefensive brokers like Crowdfense pay a premium precisely because the vulnerability remains secret and weaponizable.

ZDI does not publish a fixed price list. Payouts are individually assessed based on:

- Product deployment breadth and criticality (for example, databases, routers, firewalls are considered high-value).
- Severity and exploitability (unauthenticated RCE commands highest payouts).
- Default configuration exposure.
- Whether social engineering is required.

Pwn2Own as a pricing proxy

ZDI's annual Pwn2Own competitions provide the most transparent public signal of how ZDI values specific categories. These are competition prizes and not standard acquisition prices, but reflect ZDI's internal valuation model:

Target Category	Price Range
SOHO Smashup (chained router + NAS, 9-vulnerability chain)	US$100,000
SOHO Smashup (chained router + NAS, single team)	US$50,000
SOHO Smashup category award	US$25,000
Individual NAS device exploit (QNAP, Synology, TrueNAS)	US$3,000 – US$25,000
Individual router exploit	US$3,000 – US$25,000
Printer exploit (Canon, Lexmark)	US$3,000 – US$10,000
Camera exploit (Lorex)	US$3,000 – US$5,000

Table 7. Pwn2Own Ireland 2024 - Consumer/SOHO Focus (US$1,066,625 total)

Target Category	Price Range
SOHO Smashup (router + NAS within 30 min)	US$100,000
Mobile phone full chain (iPhone/Pixel, kernel-level)	US$250,000
NAS device exploit	US$5,000 – US$40,000
Printer exploit	US$5,000 – US$20,000
Smart speaker exploit	US$5,000 – US$20,000

Table 8. Pwn2Own Toronto 2023 — Consumer/SOHO Focus (~US$1,000,000 total)

Target Category	Price Range
Browser full chain (Chrome, Safari, Firefox)	US$85,000 – US$200,000
Windows kernel escalation	US$30,000 – US$90,000
VMware ESXi/Workstation escape	US$150,000 – US$250,000
Tesla infotainment	US$100,000 – US$200,000

Table 9. Pwn2Own Vancouver 2024 — Enterprise/Desktop Focus (US$1,132,500 total)

ZDI vs. nondefensive brokers — key distinction:

ZDI prices reflect the ethical floor of what edge device and SOHO vulnerabilities are worth in a coordinated disclosure context. One of the things that sellers get by selling the vulnerabilities to ZDI, though, is the guarantee that the sold information would be used in strictly ethical manner. For example, **ZDI often takes responsibility for vendor mitigation and coordinated disclosure**.

Other brokers like Crowdfense pay up to US$100,000 for the same Cisco or Fortinet RCE, but that is the acquisition price for possibly a secret, weaponizable exploit. The true operational value to a potential customer of these services is far higher, as demonstrated by campaigns that used a single edge device exploit across hundreds of victims globally.

The comparison below shows how ZDI's Pwn2Own prizes for SOHO/edge devices (US$3,000 – US$100,000) is below Crowdfense's acquisition prices (US$50,000 – US$100,000). However, it confirms the broader market pattern:

Target	ZDI Pwn2Own Prize	Crowdfense Acquisition	Difference
Enterprise firewall/router RCE (Cisco, Fortinet)	Not in Pwn2Own scope	US$100,000	
SOHO router RCE (D-Link, Netgear, QNAP)	US$3,000–US$25,000	US$50,000	~2x – 5x
Chained SOHO attack (router + NAS)	US$25,000–US$100,000	Not listed separately	
Mobile OS full chain	US$150,000–US$250,000 (competition)	US$5,000,000–US$7,000,000	~20x – 40x

Table 10.

The 20x – 40x premium that nondefensive brokers pay over Pwn2Own for mobile, compared with the 2x – 5x premium for SOHO/edge devices, further confirms that edge devices are underpriced relative to their strategic value. This makes them especially attractive to state-sponsored buyers.

APPENDIX C

Leaked Workstation Analysis

In August 2025, Phrack Magazine (Issue 72, Article 7) published an analysis of a compromised threat actor's workstation. The article attributed the actor to a North Korean-aligned group called Kimsuky. Subsequent analysis by Intel471[7] , S2W[8], and our own investigation indicates that the actor is more likely China-aligned, mimicking DPRK's tactics, techniques, and procedures (TTPs) for misdirection. Evidence for the actor being rather China-aligned includes:

- Extensive use of Simplified Chinese without translation tools.
- Heavy reliance on Chinese services (Baidu, CSDN, Freebuf, FOFA).
- Inactivity during Chinese holidays and noticeable activity during North Korean holidays.
- Use of Apple TLS proxies for Great Firewall circumvention, with exit nodes in Taiwan.
- Possession of Ivanti exploit tools matching UNC5221 operations.
- Use of private tools and exploit code known to be associated with China-aligned groups.

On the machine, these tools were found:

- **Exploit development:** IDA Pro 8.3, Ghidra, and LLM/AI-powered tools for code transformation and analysis.
- **Custom malware:** SPAWN ecosystem (SpawnAnt, SpawnMole, SpawnSnail, SpawnSloth), Ivanti-specific rootrot (perl-based webshell), and hotpatching frameworks for Ivanti "web" binary.
- **Rootkits:** Interest in multiple open-source rootkits (browsing history analysis), plus source code of a custom syslogk rootkit not previously attributed to any threat actor
- **C&C and tunneling:** Mythic framework (Kharon, Velkor agents), Havoc, SNIPROXY, FRP, and custom SOCKS implementations
- **Anti-EDR:** Testing frameworks for specific EDR products and custom Cobalt Strike modules

Among the targets were the following:

- **South Korea:** Evidence by extensive FOFA searches for Ivanti devices in South Korea; multiple datasets, source code, and data related to South Korean targets; phishing tools tailored for South Korean victims; telecommunications sector interest
- **Taiwan:** Login attempts toward Taiwanese IPs/domains; FOFA searches for FortiGate devices in Taiwan

The leaked data confirms that edge devices are strategic entry points. The toolkits found in the data are explicitly designed for edge device compromise. The mix of open-source and custom tools suggests constrained resources, with edge exploits treated as expendable for initial access. The reconnaissance is systematic, not opportunistic, and targeting aligns with China-aligned strategic intelligence priorities.

Early adoption of AI tools in workflow

Another noteworthy observation is the study of browsing history of the actor, which revealed the attacker's high level of adoption of AI and AI-powered tools. Even in 2025, the threat actor was observed using a range of AI-powered platforms throughout the workflow. Most notably, the actor made heavy use of code conversion tools, such as **codeconvert.ai** and **syntha.ai**, specifically targeting language pairs including Rust-to-C, Rust-to-C++, Golang-to-C, Golang-to-Python, and Assembly-to-C. This implies active efforts to port or translate tooling across language boundaries. This technique is consistent with malware retooling or evasion of language-specific detection signatures.

Alongside these, the actor was observed using AI-assisted development platforms, such as **blackbox.ai**, **code-mentor.ai**, and **sourcery.ai**, for code review and interactive coding guidance. This implies a reliance on AI not just for mechanical translation, but also for iterative development and debugging assistance. The actor also used general-purpose AI chat platforms, including **deepseek.chat**, **deepai.org**, **yeschat.ai**, and several chatbot services, along with research and discovery tools like **zhuanzhi.ai** and **toolify.ai**. This further implies that AI is being integrated broadly into the actor's operational workflow, from initial research, tool discovery, and code development to final payload preparation.

References

1 Censys. (2026). *Censys.* “Censys | The Authority for Internet Intelligence and Insights.” Accessed Apr. 4, 2026, at: Link.

2 NUWA Project. (n.d.) *NUWA Project.* Accessed Apr. 4, 2026, at: Link.

3 NVWA Project [@NvwaProject]. (Apr. 13, 2020). *NVWA Project.* “We have updated a target list, which expands the target range and will accept DoS-type vulnerabilities!!! Very generous bonus is waiting for you here: https://nvwa.org/index.php .” Accessed Apr. 4, 2026 at: Link.

4 Crowdfense (n.d.). *Crowdfense.* “Exploit Acquisition Program”. Accessed Apr. 4, 2026, at: Link.

5 Zerodium. (n.d.) *Zerodium.* Accessed Apr. 4, 2026, at: Link.

6 TrendAI Zero Day Initiative (ZDI). (n.d.). *ZDI.* “Program Benefits.” Accessed Apr. 4, 2026, at: Link.

7 Intel 471. (Sep. 5, 2025). *Intel 471.* “The Phrack leak: Examining an APT’s workstation.” Accessed Apr. 4, 2026, at: Link.

8 S2W. (Aug. 22, 2025). *S2W Inc.* “Detailed Analysis of Phrack’s APT Down: The North Korea Files.” Accessed Apr. 4, 2026, at: Link.

TrendAI™

TrendAI™, the global AI security leader and enterprise business unit of Trend Micro, empowers organizations with full AI visibility and consolidated security that inspires confidence, drives innovation, and eliminates risk.

Trusted by the largest enterprises and governments across 185 countries, TrendAI™ secures the entire organization, from identities to infrastructure to data.

AI Fearlessly.

Learn more: **trendaisecurity.com**