Investigating Abuse Within Domain Portfolios

ICANN84 Breakout Session 3 | Summary & Key Takeaways

What Happened in This Session

The discussion focused on how domain registries can fight abuse by looking at entire portfolios of domains rather than just individual bad actors. The .US registry shared their real-world approach to detecting and stopping cybercriminals who hide behind multiple domain names.

Think of it like this: if someone robs a bank using a stolen car, you don't just look for that one car—you check if they've stolen others. The .US registry does something similar with domain names, tracking patterns across multiple domains owned by the same person or organization.

The .US Advantage: Real Data, Real Fast

The .US TLD has a unique edge in fighting abuse: it's one of the few registries that prohibits privacy and proxy services. This means every domain registration contains actual, verified contact information—no hiding behind fake names or anonymous services. When abuse happens, investigators can immediately see who's behind it.

Speed matters in cybersecurity. The .US registry operates on tight timelines: most investigations wrap up within five days, with simple cases resolved in just 24 hours. Once they contact a registrant about potential abuse, that person gets 72 hours to respond before action is taken.

What makes this more powerful? The registry serves 2.5 million registrants with verified addresses that registrars must check monthly for new domains. This isn't just good recordkeeping—it's the foundation of their entire abuse-fighting strategy.

How Portfolio Detection Actually Works

When an abuse report comes in, .US investigators don't just look at the reported domain. They dig deeper, searching for connected domains through multiple data points: WHOIS records, user data from other sites, SSL certificate logs, and activity patterns across the web. It's detective work backed by technology.

Here's where AI enters the picture. The registry uses artificial intelligence to quickly distinguish between a compromised website (maybe someone's WordPress site got hacked) and truly malicious activity (someone deliberately running a phishing operation across dozens of domains). This matters because the response is very different—one needs help, the other needs to be shut down.

The Power of the 'Nexus' Approach

The registry introduced a concept called "nexus"—essentially, connecting the dots between domains and registrants to spot patterns of abuse. When investigators notice the same person or entity behind multiple problematic domains, they can trigger a broader review that might lead to multiple domains being suspended or deleted.

This nexus process happens collaboratively. The .US registry works within a community of security professionals who widely share intelligence about threats. When one organization spots a pattern, others benefit from that knowledge, creating a network effect that makes it harder for bad actors to simply move from one domain to another.

Taking Action: Tools and Remedies

Once abuse is confirmed, the .US registry has several tools at its disposal:

- Server holds that freeze the domain in place
- Removing domains from DNS resolution so they can't be accessed
- Working with registrars to place account holds
- Complete deletion of domains involved in confirmed abuse

Remarkably, no court order is required for these actions. As the authoritative source for .US registration data and under the authority of NTIA (the U.S. policy authority for domains), the registry can act quickly when abuse is confirmed. They're careful about this power, though, using screenshots and thorough documentation to avoid wrongly taking down legitimate businesses.

Emerging Themes and Questions

Portfolio-Based Thinking: The session highlighted a shift from looking at individual domain abuse to understanding portfolios of domains owned by the same actors. This approach could become a model for other registries looking to improve their abuse mitigation strategies.

The Accuracy Foundation: Much of what makes the .US approach work depends on accurate WHOIS data. This raises questions about how other TLDs that allow privacy services might adopt similar portfolio detection methods. Can you fight portfolio abuse without knowing who owns the domains?

Speed vs. Due Process: The five-day timeline and 72-hour response window strike a balance between acting quickly to stop abuse and giving registrants time to respond. This balance will likely be debated as ICANN develops associated domain check policies.

AI as an Investigative Tool: The use of artificial intelligence to distinguish compromised domains from malicious operations points to where abuse detection is heading. As AI tools improve, they could help registries make faster, more accurate decisions about when to intervene.

Community Intelligence Sharing: The session emphasized that no registry fights abuse alone. The .US approach relies heavily on sharing threat intelligence within a trusted community. This collaborative model could be expanded across more TLDs and registries.

Policy Development Implications: As ICANN moves forward with policy development for associated domain checks, the .US registry's practical experience offers concrete examples of what works—and what challenges remain—in detecting and mitigating portfolio-based abuse.

The Bottom Line

This breakout session revealed that fighting domain abuse isn't just about reacting to individual complaints—it's about seeing the bigger picture of how bad actors operate across multiple domains. The .US registry's approach shows what's possible when you have accurate data, smart technology, fast processes, and a collaborative community.

For other registries considering similar approaches, the message is clear: portfolio detection works, but it requires a foundation of accurate registration data and the willingness to act quickly when abuse is confirmed. The conversation is just beginning about how these practices might shape future work on associated domain checks.