Recent Cyber Chaos is a Structural Shift

By Tom Uren

Published: 2023-09-14 · Archived: 2026-04-05 14:48:22 UTC

Your weekly dose of Seriously Risky Business news is written by Tom Uren, edited by Patrick Gray and supported by the Cyber Initiative at the Hewlett Foundation and founding corporate sponsor Proofpoint.

From crypto thieves to ransomware attackers and state-backed groups hellbent on sowing chaos, it's been a rough month in the cybers. But what does this recent chaos tell us about where policymakers' heads should be? First, let's look back at what's been happening.

This week, *The Record* reported that Balkan country Bosnia and Herzegovina was hit by a ransomware attack that crippled the country's parliament. This follows a late-August Cuba ransomware attack on the government of Montenegro and an April Conti ransomware attack on the government of Costa Rica. The Chilean government also suffered a crippling ransomware attack.

Even leaving aside the invasion of Ukraine, destructive state-backed cyber attacks are also on the rise. Iran attacked Albanian government systems in mid-July. Albania claims it was attacked *again* earlier this month after it severed diplomatic ties with Iran in protest. Meanwhile, Iran and Israel's ongoing, destructive cyber tit-for-tat continues.

Effective, genuine hacktivists — as opposed to state-backed operators masquerading as hacktivists — are also coming out of the woodwork. This week, a group calling itself Guacamaya, the Mayan word for macaw, released 10TB (Yes! That's a T!) of emails and files from Latin American military and police units. The group, which says it is motivated by environmental degradation and repression of indigenous populations in Central and South America, has been active since at least March this year. In its first publicly known hack, it compromised a mining company operating in Guatemala and shared documents with Forbidden Stories, the journalist collaboration network, which operates so that "killing the journalist won't kill the story". This leak appeared in March as the "Mining Secrets" series of articles on Forbidden Stories.

Screen capture from Guacamaya's recent video

This week's release is Guacamaya's fourth since March and it has also compromised mining and oil companies and government offices in a number of different countries. In each case it releases data via Enlace Hacktivista, a website that documents hacker history, and/or via Distributed Denial of Secrets. Each release is accompanied by a statement, sometimes a video, that documents the hacking process and, once, even a poem.

The Ukraine IT Army also claimed some success this week and claims to have hacked the personal data of mercenaries from the Russian Wagner Group.

This week *The Record* published a comprehensive overview of the Belarusian Cyber Partisans, covering the group's founding, some of its successful operations and also interviews with its spokesperson Yuliana Shemetovets. This newsletter has covered the activities of the Belarusian Cyber Partisans several times, and an early episode of our *Between Two Nerds* podcast discussed how the Cyber Partisans evolved to become a very effective group.

Even teenagers, in the form of the Lapsu$ group, are chalking up some "wins". After being on a tear earlier this year, arrests in Britain and police investigations in Brazil seemed to have slowed Lapsu$ down until both Rockstar games and Uber were hacked by one of its members this week. The details of the Uber hack are interesting and this week's edition of the *Risky Business* podcast has an excellent dissection of "Uber's very bad week".

And of course, massive cryptocurrency thefts continue — this week DeFi platform Wintermute lost USD$160m worth of cryptocurrency.

The abhorrent Kiwi Farms website we wrote about two weeks ago has also been hacked, perhaps even twice, by people apparently trying to steal user information. Given the average Kiwi Farmer probably doesn't have amazing OPSEC, we think the forecast is sunny with a 90% chance of heavy doxxing.

You add up all these incidents — keep in mind they're all from the last month — and you have to wonder: are we the proverbial frog in boiling water? Just how did things get so f***ed up? How long has it been like this? We've seen various classes of attackers hit the limelight over the years, but lately it feels like they're all causing problems at once. In our view, this is a structural shift and not a coincidence.

If this is indeed the new normal it won't be enough for policymakers to target their efforts on either winding back the chaos *or* adapting to it, they'll need to do both. The only question is how those efforts should be divided in terms of focus and resources.

A new Atlantic Council report examines whether 2021 changes to Chinese cyber security laws have had an effect on the responsible disclosure vulnerabilities by the Chinese research community.

We don't entirely agree with the premise of the paper, which is that these laws could stifle vulnerability disclosure across borders. The paper cites Alibaba being punished after it privately told the Apache Software Foundation about the Log4J vulnerability as an example case where the laws might hinder disclosure. In this case, however, we think Alibaba wasn't punished for sharing information with the vendor — the law actually requires it — but was instead punished for not promptly informing the Ministry of Industry and Information Technology (MIIT).

So it's perhaps not surprising then, that the report found the laws themselves didn't have a "significant impact".

Despite this, the paper does find a definite trend towards decreased disclosure by Chinese entities, but much of this decrease is explained by the addition of Chinese security company Qihoo 360 to the US Entity List in 2020. Before then, Qihoo 360 dominated Chinese vulnerability reports. Since it was added to the US government's naughty entities list its reports essentially evaporated, and other Chinese groups just haven't stepped up to replace its public research.

There are other factors at play too. There's no doubt the PRC wants to increase its control over its hacker community, which is cause for concern. But it's a concern that has little to do with Chinese vulnerability disclosure laws and more to do with the PRC's intent, which can change faster than you can say "Nancy Pelosi is visiting Taiwan".

Despite our quibbles with its premise, we are fans of the report's data analysis and think the recommendations are interesting. In brief, they are:

1. Harmonise vulnerability disclosure across the United States and allies
2. Improve the quality and consistency of support of vulnerability discovery tools
3. Track vulnerability disclosure patterns and "invest against gaps"

The first two are both sensible ideas and simply aim to make vulnerability disclosure practices both better (with better tools) and more global (by bringing in more countries).

The third recommendation is interesting, though. The paper speculates that by tracking vulnerability disclosures over time it may be possible to see "gaps" where disclosures against a particular class or cluster of software significantly decline. These gaps could, for example, indicate that the easy bugs have been discovered. Or they could result from a change in laws in another jurisdiction that impede disclosure. Regardless of the reason, the paper argues that the presence of gaps makes any vulnerabilities discovered there more valuable and would justify countercyclical investment to "help incentivize further disclosure against critical software and offset the effects of policies that limit disclosures".

1. **A billion reasons to be happy:** the Biden Administration has launched a federal grant program that will provide up to USD$1bn for state and local government cyber security upgrades.

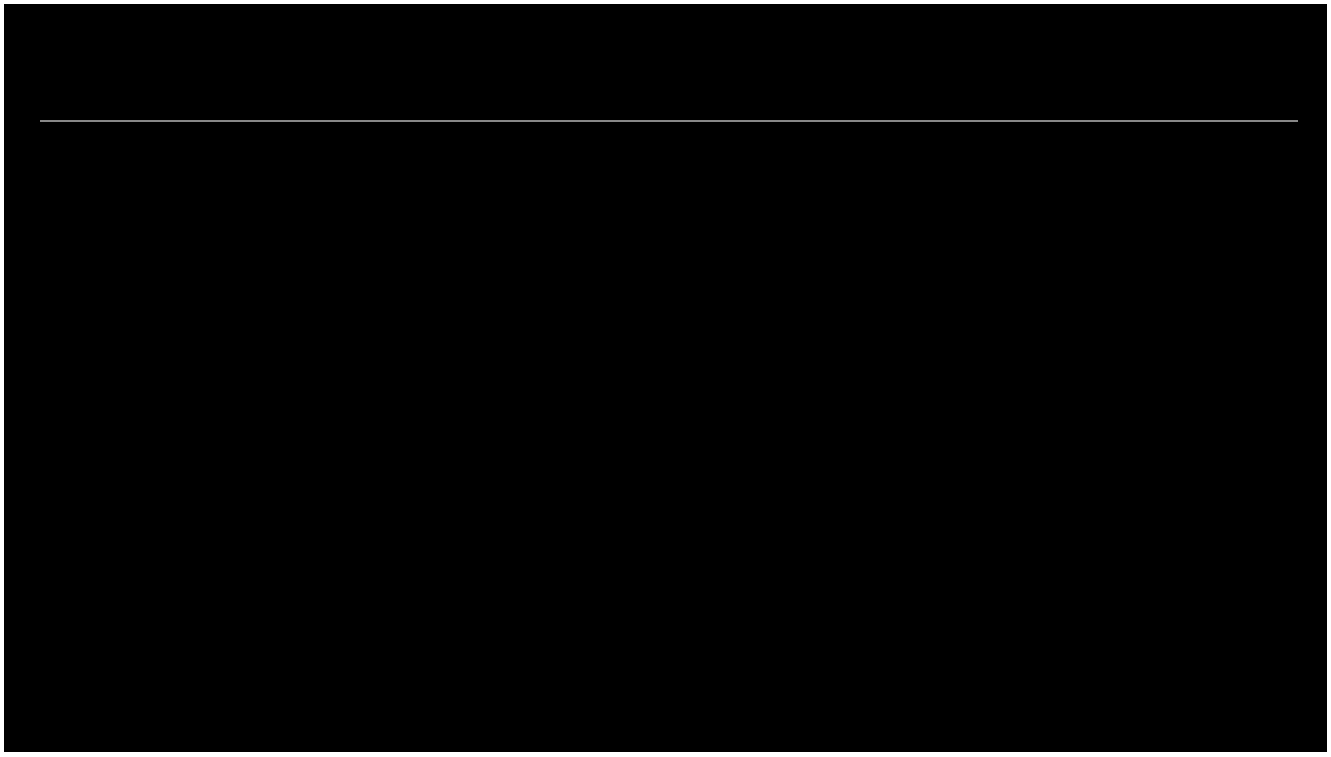
2. **European cyber security rules for smart devices:** The European Commission has proposed some pretty sensible regulation to improve the security of network connected devices in the Cyber Resilience Act. Manufacturers will have to deliver products without known vulnerabilities and be able to deliver security updates, among other things.

3. **Going after ransomware top dogs:** the US Joint Ransomware Task Force, which includes representatives from CISA, the FBI, the DOJ, cyber security companies and the private sector plans to prioritise "operations to disrupt specific ransomware actors". More coverage at *Risky Business News*.

A recent Proofpoint report examines an Iran-aligned threat actor TA453's use of a technique that it calls "Multi-Persona Impersonation" or MPI. Rather than trying to socially engineer a victim with a single persona, TA453 introduces a second attacker-controlled persona, often by cc'ing them into an ongoing email conversation in the cases that Proofpoint has seen. MPI leverages "the psychology principle of social proof to prey upon its targets and increase the authenticity of the threat actor's spear phishing".

Risky Business publishes sponsored product demos to YouTube. They're a great way for you to save the time and hassle of trying to actually get useful information out of security vendors. You can subscribe to our product demo page on YouTube here.

In our latest demo, Mike Wiacek shows Patrick Gray how to hunt down and triage suspicious files within your enterprise using Stairwell's file analysis and threat detection platform.



CISA published its 2023-2025 strategic plan last week. It spells out four major goals for the agency:

1. Spearhead national cyber defence efforts

2. Reduce risk to America's critical infrastructure

3. Strengthen whole-of-nation collaboration and information sharing

4. Unify CISA capabilities

Well duh. Of course CISA would like to be better at everything, but the plan doesn't articulate how CISA will 'win' other than perhaps by trying really hard. Many of CISA's goals require improved information sharing or increased visibility into risks, so a plan to win might look like "CISA will improve its information gathering to identify and fix the weaknesses in America's cyber security posture". Improved information, analysis, action.

Something like that would be nice… this newsletter isn't a fan of strategic plans that only consist of motherhood statements.

The Atlantic Council has an Issue Brief out this week examining the variety of Russian cyber actors. One key takeaway that resonated with us:

> The Putin regime perceives that it benefits—and in many cases, does materially benefit—from leveraging the Russian cyber web *[Ed: Cyber web? Really?]* because it can claim deniability, has more power to wage covert political warfare below the threshold of outright war, and has potentially lower costs for cyber capabilities. Cybercriminals also bring money into Russia, an increasingly important factor for a heavily sanctioned country with a declining economy. Overall, the Putin regime has many incentives for continuing to allow cybercrime to thrive in Russia, as well as for creating front companies, leveraging cybercriminals and patriotic hackers, filching private company employees, and letting private military companies develop cyber capabilities.

The *Washington Post* reports the Pentagon is reviewing the conduct of its clandestine social media influence operations after some of these actions were recently uncovered. The review is motivated by fears in government about the conduct of these operations. *The Post* does a good job examining the issues and the article ends up reinforcing views we've previously published.

"Our adversaries are absolutely operating in the information domain," a senior defense official told *The Post* . "There are some who think we shouldn't do anything clandestine in that space. Ceding an entire domain to an adversary would be unwise. But we need stronger policy guardrails."

These types of operations have not been particularly effective and undermine the appeal of our democracies when they are uncovered. In other words, lots of risk, not much reward. We need more than stronger policy guardrails — we need to respond in a way that is both effective *and* plays to the strengths of liberal democracies. That's not ceding the domain. That's being smart rather than responding reflexively because we don't like what Russia and China do on Facebook and Twitter.

Casey Newton at *The Verge* has published a good examination of the increasing US political pressure on TikTok. Newton's take: lawmakers have legitimate concerns about Chinese Communist Party influence over TikTok and it will be very difficult to convince them that everything is ok.

In addition to a podcast version of this newsletter (last edition here), the Risky Biz News feed (RSS, iTunes or Spotify) also publishes interviews.

In our last "Between Two Nerds" discussion Tom Uren and The Grugq how SIGINT agencies in different regions have different cultures, and how these differences are rooted in the military traditions and hacker cultures of various countries.

Poland refuses to cooperate with the EU in spyware scandal: Polish authorities are flat-out refusing to cooperate with EU officials in the investigation into their abusive use of advanced spyware against its political rivals, the EU's PEGA committee said in a statement on Thursday.

> We strongly condemn the fact that the Polish government has refused to collaborate with the Inquiry Committee by declining the invitation to the hearing and refusing to meet with the fact-finding mission next week. We believe that such meetings would give the Government opportunity to respond to reports about illegal use of intrusive surveillance against persons deemed as political opponents.

Catalin is shocked-not-shocked that the Polish government refuses to investigate the hacking of its political rivals (continued).

IHG hackers come forward: Hackers describing themselves as a couple from Vietnam took credit for the hack of the InterContinental Hotel Group earlier this month. The duo told the BBC they gained access to the hotel's network after tricking an employee into downloading and installing malware on their system through a booby-trapped email attachment. The hackers said they then found a password vault for several of the hotel group's internal systems, including its main database, which was allegedly protected by a password of "Qwerty1234." The hackers said they tried to install ransomware on the hotel's network, but after failing, they just wiped the database instead, in frustration.

Wintermute crypto-heist: Cryptocurrency DeFi platform Wintermute said it was hacked and lost $160 million in a security breach that took place on Tuesday, September 20. Most of the cryptocurrency security space appears to believe the attacker exploited a recently-disclosed vulnerability in an Ethereum vanity address generator tool to steal funds from Wintermute's main ETH wallet. Wintermute's CEO said the company remains solvent and said they are still open to the idea of offering a bug bounty payout to the attacker if they return the stolen funds.

web3 is going just great@web3isgreat

Wintermute is named after the AI in the cyberpunk novel Neuromancer, written by William Gibson.

William Gibson @GreatDismal

Startups or products named after characters in my books have never done too well. It's sort of like the Blade Runner curse, but in reverse.

2:41 PM · Sep 20, 2022

63 Reposts · 426 Likes

Source: https://srslyriskybiz.substack.com/p/recent-cyber-chaos-is-a-structural