

# Risky Biz News: Doppelganger gets a kick in the butt from Uncle Sam

 [news.risky.biz/risky-biz-news-doppelganger-gets-a-kick-in-the-butt-from-uncle-sam/](https://news.risky.biz/risky-biz-news-doppelganger-gets-a-kick-in-the-butt-from-uncle-sam/)

Catalin Cimpanu

September 6, 2024

*This newsletter is brought to you by [GreyNoise](#). You can subscribe to an audio version of this newsletter as a podcast by searching for "Risky Business News" in your podcatcher or subscribing via [this RSS feed](#). On Apple Podcasts:*

[Risky Biz News: Doppelganger gets a kick in the butt from Uncle Sam](#)

[A short podcast updating listeners on the security news of the last few days, as prepared by Catalin Cimpanu and read by Claire Aird. You can find the newslett](#)



[Apple Podcasts](#)



The US government orchestrated its largest crackdown against Russia's disinformation apparatus on Wednesday, coming out with indictments, sanctions, visa restrictions, site takedowns, and rewards for information on some of the individuals involved.

US officials have formally accused the Kremlin of interfering again in the US Presidential Election, mainly through the work of several of its entities pushing to promote Donald Trump and the Republican Party.

The actions hit well-known purveyors of Russian propaganda, such as Doppelganger, Structura, RRN, SDA, and even RT (formerly Russia Today).

Some names might be familiar, some might not. Below, we're gonna aggregate some of the US actions, grouped by the major players, and the reasons behind them.

### **Rossiya Segodnya (RT's parent company)**

The organization that took the brunt of Wednesday's crackdown was **Rossiya Segodnya**, Russia's largest media group and the parent company for multiple state-funded news organizations such as RT, RIA Novosti, TV-Novosti, Ruptly, and Sputnik.

The Department of Justice indicted two RT employees with conspiracy to violate the Foreign Agents Registration Act (FARA) and conspiracy to commit money laundering.

Officials say RT's Digital Media Projects Manager Konstantin Kalashnikov and one of his employees, Elena Afanasyeva, secretly paid over \$10 million to a Tennessee-based online content creation company to produce Russian propaganda for US audiences under the guise of a grassroots movement.

Officials didn't name the company, but extensive details they left in court documents point the finger at TENET Media, the employer of several right-wing content creators such as Tim Pool, Benny Johnson, Dave Rubin, and Lauren Southern.

*"In order to carry out RT's secret influence campaign in the United States, Kalashnikov and Afanasyeva operated under covert identities at U.S. Company-1. Posing as an outside editor, Kalashnikov edited U.S. Company-1 content, monitored U.S. Company-1's funding and hiring, and introduced Afanasyeva as a member of his purported editing team. Using the fake personas Helena Shudra and Victoria Pesti, Afanasyeva posted and directed the posting by U.S. Company-1 of hundreds of videos. Afanasyeva also collected information from and gave instructions to U.S. Company-1 staff. For example, after the March 22, 2024, terrorist attack on a music venue in Moscow, Afanasyeva asked one of U.S. Company-1's founders to blame Ukraine and the United States for the attack, writing: 'I think we can focus on the Ukraine/U.S. angle. . . . [T]he mainstream media spread fake news that ISIS claimed responsibility for the attack yet ISIS itself never made such statements. All terrorists are now detained while they were heading to the border with Ukraine which makes it even more suspicious why they would want to go to Ukraine to hide.'"*

Officials said RT and one of TENET's founders deceived the creators about the source of their funding, statements echoed by the content creators themselves on social media once the indictment went live.

However, when you're getting between \$100,000 to \$400,000 per video, you may not want to ask those questions and play-pretend deceived once you get caught.



...

For people reading the indictment, some of the unnamed commentators are becoming clear.

Commentator 1: Dave Rubin

Commentator 2: Tim Pool

Commentator 3: Unclear

Commentator 4: Lauren Southern

Commentator 5: Unclear

Commentator 6: Matt Christiansen

That leaves Benny Johnson and Tayler Hansen unassigned.

4:17 AM · Sep 5, 2024 · 100K Views



**Kevin Collier**

@kevincollier@mastodon.social

ODNI officials said in July\* that their countering foreign malign influence process included potentially alerting Americans unwittingly spreading state-sponsored disinfo. The feds wouldn't and haven't named names. But an indication those names today may have gotten a heads up.

Sep 05, 2024, 02:16 AM · 🌐 · Tusky

3 boosts · 6 favorites



**Kevin Collier**

@kevincollier

🌙 8h

That was in a press call July 29 that focused particularly on broad warnings about Russia as the primary 2024 disinfo actor, and in retrospect it seems to have heavily referenced today's accusations. So the reference to potentially alerting Americans looms large to me today.



**Kevin Collier**

@kevincollier

🌙 8h

The officials wouldn't confirm at the time that they had alerted anyone recently, and certainly won't officially name anyone. But I think that's one of the big open questions remaining. Did any of these guys know they were getting RT money? When? Did they then change behavior?





**Michael Weiss** ✓  
@michaeldweiss



Elon Musk naturally promoted nonsense peddled by Tenet Media, which was financed by now-indicted Russian operatives.



**James** @GravitysRa1nbow · 12h

Lmao



**Elon Musk** ✓ [X] @elonmusk · Apr 6



Replying to @watchTENETnow and @Lauren\_Southern



86

75

863

79K



**Elon Musk** ✓ [X] @elonmusk · Aug 11



Replying to @dom\_lucre and @watchTENETnow

!

127

227

3.1K

197K



**Elon Musk** ✓ [X] @elonmusk · Aug 26



Replying to @watchTENETnow

!!

180

201

3.8K

65K



**Chris Krebs** ✓  
@C\_C\_Krebs



The charging documents for the RT-linked couple and Doppelgänger groups are an absolute intelligence gold mine. Perfect example of an effective speaking indictment by @TheJusticeDept, and a real service to security researchers who will be digging thru this stuff for years. Nicely done by the USG, a team effort across multiple agencies.

12:50 AM · Sep 5, 2024 · 327.2K Views

61

2K

6.8K

287





**Patrick Howell O'Neill**

@howelloneill.bsky.social

So for the guys who got a mountain of Russian cash, just wondering, what happens to that cash?

Sep 5, 2024 at 9:34 PM Everybody can reply



Kalashnikov and Afanasyeva were two of six RT executives who were also sanctioned. The Treasury didn't play around with words in their press release and just said the quiet part out loud, accusing RT staff of working on behalf of the Russian Federal Security Service (FSB).

The State Department also followed through and has classified Rossiya Segodnya and its subsidiaries as unregistered Russian government "foreign missions."

The classification comes with visa restrictions for its staff and the obligation to notify the State Department of any property or personnel working within the US—or face larger penalties.

### **Doppelganger cluster**

The DOJ also seized 32 domains that typosquatted the names of legitimate news outlets and hosted Kremlin propaganda.

Officials linked the domains to a threat actor the cybersecurity industry has been tracking for years as Doppelganger.

The DOJ says three Russian companies operated and published content on the domains:

- Social Design Agency (SDA)
- Structura National Technology (Structura)
- Autonomous Non-Profit Organization Dialog (ANO Dialog)

US officials say the companies were "operating under the direction and control of the Russian Presidential Administration, and in particular First Deputy Chief of Staff of the Presidential Executive Office Sergei Vladilenovich Kiriyeenko."

The indictment basically confirms previous research that claimed that Russia's disinformation efforts were controlled directly from Putin's Kremlin staff and executed through the FSB, GRU, and a slew of private contractors across the globe.

Officials say the recent domains were used to publish disinformation in the hopes of influencing the outcome of the US Presidential election—and the DOJ went as far as publishing internal notes from different Doppelganger campaigns:

- Good Old USA Project: Attachments [8A](#), [8B](#)
- The Guerilla Media Campaign: Attachments [9A](#), [9B](#)
- U.S. Social Media Influencers Network Project: Attachments [10A](#), [10B](#)

The campaigns focused on using a wide variety of topics to divide the American public and then gently push them toward the preferred Kremlin candidate.

## 2. Content of the campaign

We would like to reiterate that in the United States there are no pro-Russian and/or pro-Putin mainstream politicians or sufficiently large numbers of influencers and voters. There is no point of justifying Russia and no one to justify it to. All American politicians and influencers are patriots and supporters of American supremacy. However, there is a feeling among the **U.S. Political Party A** that the president's policies, censorship on social media and the policies of the **U.S. Political Party B** government are encroaching on their rights. They are dissatisfied of dramatic decline in the standard of living and large expenditures on offensive policy of the United States in Europe and Ukraine. They are afraid of losing the American way of life and the "American dream." It is these sentiments that should be exploited in the course of an information campaign in / for the United States.

The US sanctioned ANO Dialog and its Director Vladimir Grigoryevich Tabak, a man they say held several positions within the Russian Presidential Administration.

SDA and Structura didn't get away. The Treasury previously sanctioned them in March for their influence operations targeting Latin America, where they tried to sway elections towards preferred Kremlin candidates, tried to portray Russia as a "*champion against neocolonialization*," and ran their typical "*US bad, NATO bad, Russia good*" content meant to prevent any type of aid or support for Ukraine.

As for the recent sanctions, this marks the first official attribution of the Doppelganger group to ANO Dialog.

The Treasury sanctions specifically link ANO Dialog to the creation of "War on Fakes" and "Reliable Recent News" (RRN)—two major clusters of Doppelganger activity over the past years.

These clusters registered websites designed to look like legitimate Western news sources and then published content with misleading facts favorable to the Kremlin. Officials say the group often used AI and deepfakes and relied on other influencers, social media ads, and bot networks to boost their content as authentic.

This is where the handoff between Doppelganger and RT took place, with Doppelganger producing the content and RT working on amplifying it.

This week's revelations also shed some light on the mysterious attribution from July, when the DOJ took down a Twitter bot network and claimed it was operated by an editor-in-chief from RT's Moscow headquarters. The attribution kinda didn't make sense at the time, but makes more sense after this week, with that botnet being just another tool used by RT to boost Doppelganger's garbage.



[Watch Video At:](#)

<https://youtu.be/WEzCpoKFmAM>

### **RaHDit hacktivist group**

And last, the US has also imposed sanctions on Aleksey Alekseyevich Garashchenko, Anastasia Igorevna Yermoshkina, and Aleksandr Vitalyevich Nezhentsev.

Officials say the three are behind a pro-Kremlin hacktivist group known as **RaHDit** (Russian Angry Hackers Did It).

The group has a history of launching cyberattacks against Russia's opponents, leaking data, and, as of recently, disseminating disinformation with the goal of influencing elections across multiple countries.

The US Treasury says Garashchenko founded the group while working for the FSB. He now allegedly works with "*members of the Russian intelligence and security services, members of the Russian Presidential Administration, and employees from RT*" to direct the group's activity.



Yermoshkina and Nezhentsev help Garashchenko manage the group, and Nezhentsev is allegedly also a developer of cyber and surveillance tools for the FSB.

While other Russian hacktivist groups have been more visible in the media, the State Department seems to view RaHDit as a major threat for some reason. We suspect it's because the group is actually capable of orchestrating actual intrusions and successful hack-and-leak operations, known to be more effective in swaying public opinions—as opposed to the army of useless Russian hacktivists that can barely run a 5-minute DDoS attack properly.

Because of this, the State Department is now offering a reward of up to \$10 million or relocation to the US for anyone willing to share information on the group.



**REWARD UP TO \$10 MILLION FOR INFORMATION ON RUSSIAN HACKER GROUP RaHDit**

The hacking group RaHDit, also known as Russian Angry Hackers Did It, is linked to Russian state media outlet RT and Russian intelligence services. RaHDit is led by Russian Federal Security Service (FSB) officer Aleksey Garashchenko.

RaHDit has previously engaged in election interference in other countries and is a perceived threat to attempt to interfere in the 2024 U.S. presidential elections through cyber-enabled influence operations.

If you have information on RaHDit, associated individuals and entities, or Russian government-linked attempts to interfere in U.S. elections, contact us via the Tor tip line below. You may be eligible for a reward or relocation.

**Tor Link: [he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion](https://he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion)**

 U.S. Department of State  
Diplomatic Security Service  
Rewards for Justice

   +1-202-702-7843  
 @RFJ\_USA

## Breaches, hacks, and security incidents

**Iran paid ransom to save citizen data:** The Iranian government pushed a local company to pay a ransom and avoid hackers publishing the data of millions of citizens online. The ransom is related to a cyberattack that hit a software company providing services to Iran's Central Bank. A hacking group known as IRLeaks is believed to have hacked the company and stole data on customers of 20 Iranian banks. The data is believed to be extremely sensitive, containing everything for personal information to credit card numbers for millions of Iranians. According to *Politico Europe*, the hackers wanted \$10 million not to publish the files. They settled for \$3 million after the regime forced the company to pay, fearing a collapse of its financial system.

**Latvia DDoS attacks:** Latvian officials say they've been the target of DDoS attacks after announcing a new aid package for Ukraine. They've blamed it on Russian and Belarussian hackers. *[Additional coverage in [LSM](#)]*


**Planned Parenthood ransomware attack:** The Montana office of the Planned Parenthood organization has shut down its IT systems after a ransomware attack this week. A ransomware gang named RansomHub took credit for the intrusion and is now threatening to release almost 100GB of data from the non-profit. This marks the second time Planned Parenthood has suffered a ransomware attack after a similar incident at its LA office in 2021. *[Additional coverage in [PCMag](#)]*

**Cisco web shop incident:** A credit card e-skimmer was found in Cisco's official web shop. *[Additional coverage in [BleepingComputer](#)]*

**WazirX unrecoverable funds:** Indian cryptocurrency exchange WazirX says that 43% of customer funds lost in a recent hack are unlikely to be recovered. The sum represents nearly \$100 million of the \$230 million WazirX lost in July. The platform says it's undergoing a restructuring process and is looking for new investors to help cover the losses. The revelation that the funds are lost for good comes a month after WazirX announced a controversial plan to distribute the loss across all accounts instead of covering it from its reserve. *[Additional coverage in [CNBC-TV18](#)]*

**Penpie crypto-heist:** A threat actor has stolen \$27 million worth of cryptocurrency assets from the Penpie DeFi platform. The hack took place on Tuesday and caused the platform's PNP token to lose 40% of its value. Penpie has asked the attacker to return the stolen funds, promising not to file a legal action and let them keep a small portion under the guise of a bug bounty reward. *[Additional coverage in [CoinTelegraph](#)]*



Penpie ✓   
@Penpiexyz\_io



To the hacker: We acknowledge your exploit of our protocol and believe there's potential for a positive resolution that benefits all parties. Penpie is a community-driven project, and these funds mean a lot to our users. We are willing to negotiate a bounty for the safe return of the funds and offer you the opportunity to transition into a white-hat role, where your skills will be acknowledged and rewarded.

In exchange for your cooperation:

- No legal action will be pursued.
- Your identity will remain confidential.
- You'll receive a percentage of the funds as a bounty reward.

We hope you see the value in resolving this amicably. Please contact us to discuss the return of the funds and the reward details. You can reach us via Telegram, email, or any other channel you feel comfortable with.

Telegram: [@alan\\_magpie](#), [@grimmace123](#)

Email: [alan@magpiexyz.io](mailto:alan@magpiexyz.io), [grimmace@magpiexyz.io](mailto:grimmace@magpiexyz.io)

Sincerely,  
The Penpie Team

5:27 AM · Sep 4, 2024 · 38.6K Views

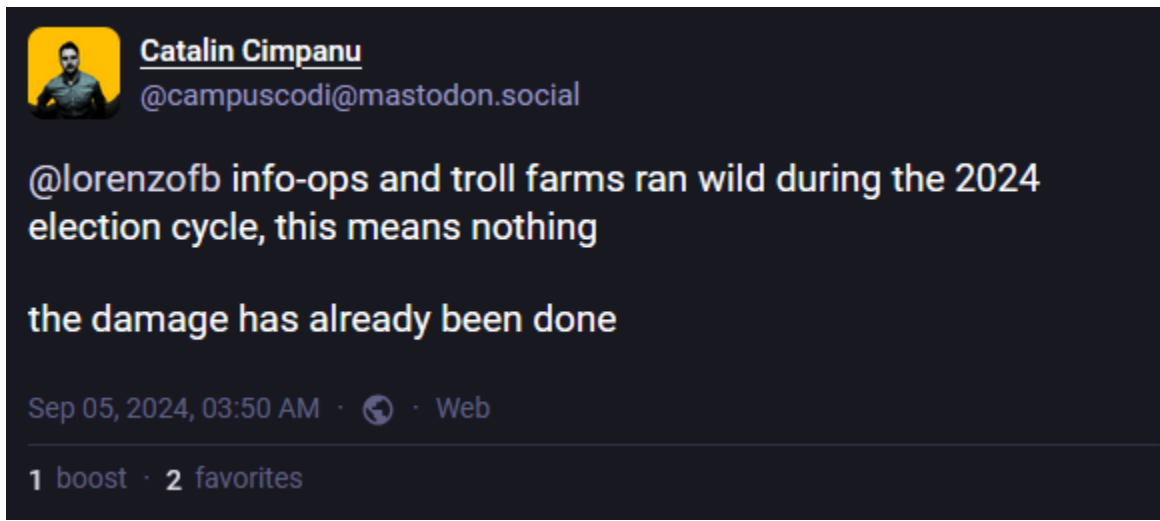
## General tech and privacy

---

**Telegram removes deepfake pr0n in KOR:** Instant messaging service Telegram has removed multiple channels hosting deepfake porn of local South Korean women. The company apologized for its late response to the police's request and provided authorities with a dedicated email where they can report future crimes. It's a surprise how responsive to law enforcement investigations a platform can get after you arrest its CEO. [*Additional coverage in [Yonhap News](#)*]

**Twitter looking for new security personnel:** X, formerly known as Twitter, is looking to hire new security staff to help moderate content and secure the platform. According to [TechCrunch](#), the company has posted over two dozen job openings for its safety and cybersecurity teams. The new hiring spree comes two years after Elon Musk fired most of

the site's trust, safety and security teams. The new hiring spree comes after troll farms ran wild and Twitter went without adequate content moderation staff for most of the 2024 election cycle.



**Rust in Google products:** Google has published [more details](#) about how it plans to use more Rust code in its products, especially for its core infrastructure.

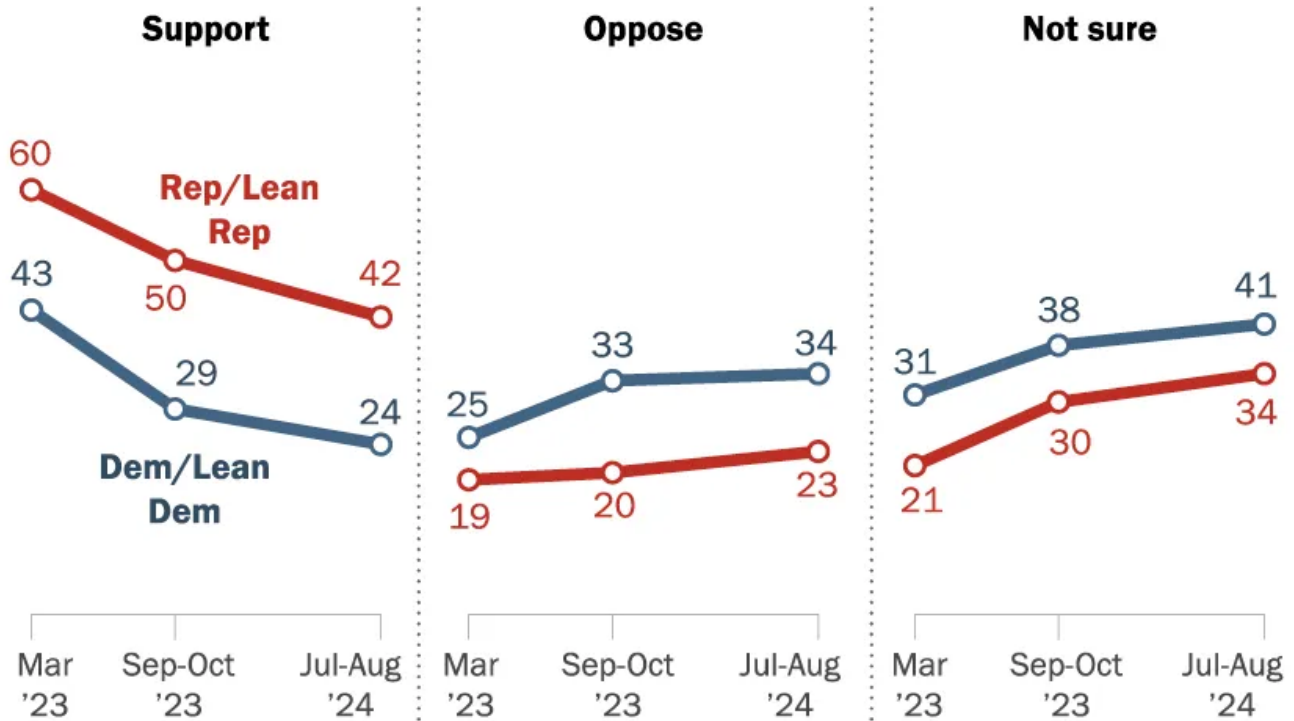
**Internet Archive loses appeal:** The Internet Archive has lost its appeal against French book publishing group Hachette and will have to remove free e-books from its service. [*Additional coverage in [Wired](#)*]

**Coda leaves Russia:** Another Western IT company has now left Russia after new US sanctions—this time it's the [Coda](#) collaboration workspace.

**TikTok ban public opinion:** The Pew Research Center has published a [report](#) on the public views of a possible TikTok ban.

# Support for a TikTok ban continues to fall in both parties, but Republicans remain more likely to back this than Democrats

% of U.S. adults who say they \_\_\_ the U.S. government banning TikTok



Note: Those who did not give an answer are not shown.  
 Source: Survey of U.S. adults conducted July 15-Aug. 4, 2024.

PEW RESEARCH CENTER

## Government, politics, and policy

**CISA drops online content moderation:** CISA has stopped advising social media companies on what type of election-related content they need to remove from their platforms. CISA Director Jen Easterly told reporters in a briefing this week that content moderation is not part of the agency's roles. The agency has taken a step back after several Republican-led states sued the agency for working with social media companies to remove disinformation from their platforms. Easterly says that for this election cycle, CISA will focus on the security of the election infrastructure itself and less on disinformation campaigns.

[Additional coverage in [CyberScoop](#)]

**Rural hospital support:** The White House says that roughly 350 of the 1,800 small and rural hospitals across the US are now using free cybersecurity resources provided by private sector partners. The resources were made available in June as part of the Biden Administration's response to the Change Healthcare cyberattack. These included free training, assessments, and consulting, and access to discounted security tools. [*Additional coverage in [NextGov](#)*]

**Colombia to investigate spyware abuses:** Colombian President Gustavo Petro has asked the country's attorney general to investigate the previous government for the purchase and use of the Pegasus spyware. Petro says the previous regime paid \$11 million to buy access to the Pegasus platform and then used it to spy on political rivals and journalists. The move comes after Poland has made strides in investigating the previous government for its use of the Pegasus spyware. Meanwhile, the current re-elected Greek ruling government has absolved itself for using a different spyware tool to spy on political rivals. [*Additional coverage in [Reuters](#)*]

**Russia threatens ISPs:** Russia's communications watchdog Roskomnadzor has warned local ISPs to implement its YouTube block or face losing their license. [*Additional coverage in [Forbes](#)*]

**Russia looking at "droppers" law:** The Russian government is preparing a bill to criminalize "droppers," a term used to describe individuals who provide intermediary accounts where fraudsters can store stolen funds. Officials have not decided on the jail time droppers could face but said individuals working as part of larger groups will see harsher penalties. The bill is expected by the end of the year. [*Additional coverage in [TASS](#)*]

## ***Sponsor section***

---

*In this Risky Business News sponsor interview, Catalin Cimpanu talks with Andrew Morris, founder of security firm GreyNoise. Andrew introduces Plasma, a new GreyNoise product that can allow customers to deploy custom GreyNoise sensors anywhere they want—on perimeters, on internal networks, on DMZs, or anywhere else.*

Sponsored: GreyNoise launches private preview of Plasma sensors

In this Risky Business News sponsor interview, Catalin Cimpanu talks with Andrew Morris, founder of security firm GreyNoise. Andrew introduces Plasma, a new Gre



Apple Podcasts



## Cybercrime and threat intel

---

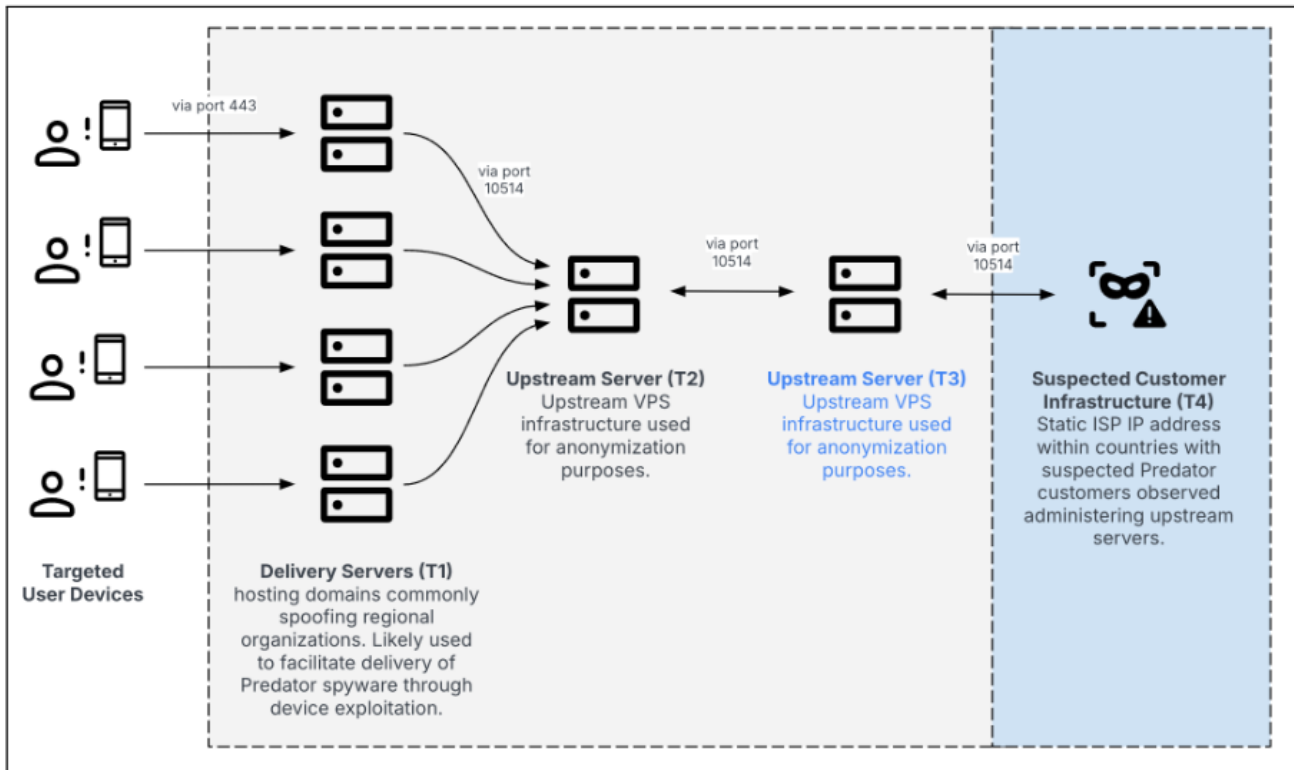
**Man charged for AI music and bot fraud scheme:** The US government has charged a North Carolina man for a novel scheme that defrauded music streaming platforms. Michael Smith created hundreds of thousands of songs using AI tools, uploaded the songs on popular streaming platforms, and used online bot accounts to stream his own music. The scheme began in 2018 and Smith allegedly had help from a music promoter and the CEO of a music company. Officials say the group made over \$10 million in royalty payments from platforms like Amazon Music, Apple Music, Spotify, and YouTube Music. Smith is the second person to be charged for defrauding streaming platforms after Danish authorities sentenced a local man to 18 months in prison for a similar scheme.

**Germany dismantles NWO harassment group:** German police has charged and raided the homes of ten individuals who are part of an online harassment group known as New World Order (NWO). The group used an online chatroom to select targets and directed members to attack victims on social media with hateful comments or insults. NWO also organized swatting events to disrupt the streams of online creators. It also social-engineered public authorities and private companies to obtain personal data, which they later used to harass and dox their victims.

**Two BEC scammers sentenced:** The US Department of Justice has sentenced two Nigerian men two prison for their roles in a major BEC scam that stole millions from US businesses. Ebuka Raphael Umeti was sentenced to ten years in prison, while his co-conspirator Franklin Ifeanyichukwu Okwonna received a five-year and three months prison sentence. The court also ordered each to pay \$5 million in restitution to their victims. According to court documents, the duo used phishing emails to infect victims with malware, downloaded victim data, and used the stolen information to redirect wire transfers to their accounts.

**Predator returns:** The company behind the Predator commercial spyware has established new infrastructure in multiple countries despite facing ongoing sanctions from the US government. According to Recorded Future, the new infrastructure appears to suggest the spyware is being used to target entities in Angola and the Democratic Republic of the Congo. Recorded Future's findings come a day after the Atlantic Council published a report on the state of the surveillance market. The report found that the recent US crackdown on spyware vendors has had a minimal impact. [*Atlantic Council interactive map of known surveillance market players*]

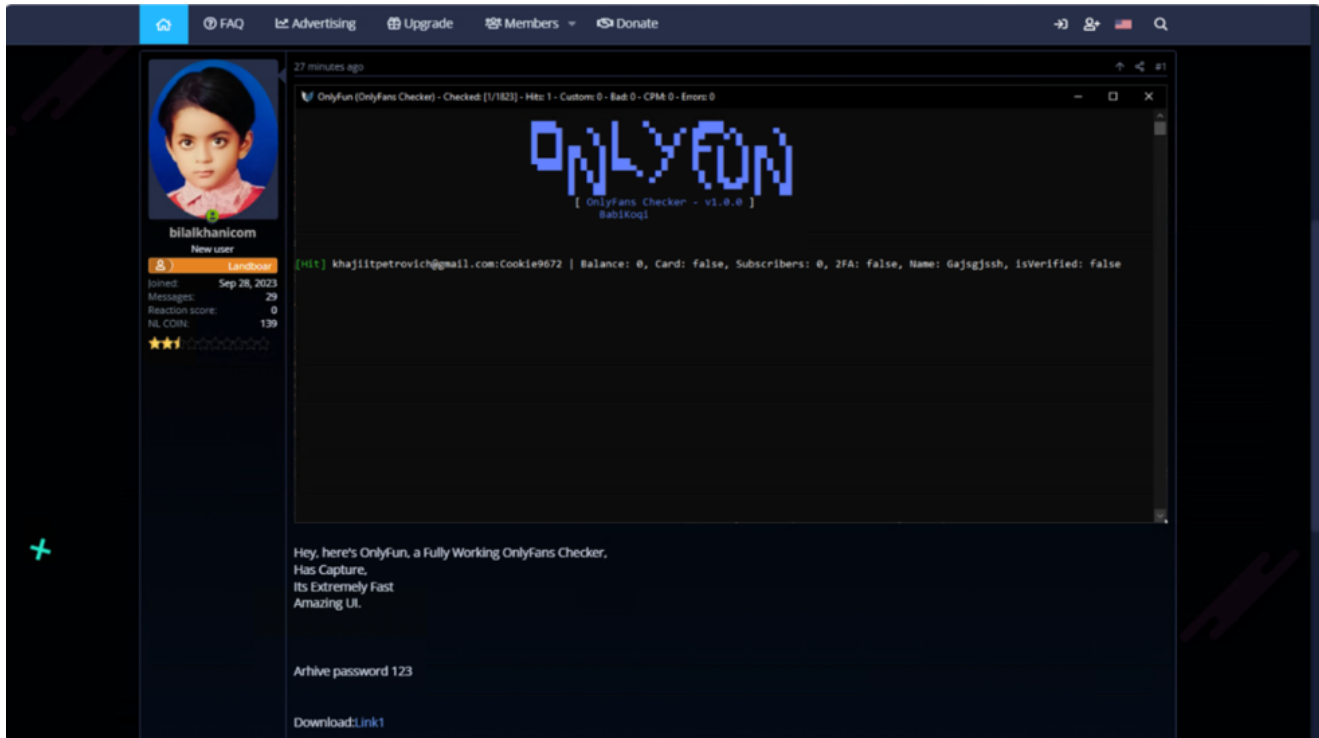




**Figure 2:** Multi-tiered Predator infrastructure with additional tier (Source: Recorded Future)

**Sextortion with home photos:** There's a new sextortion scam going around that uses the victim's name and photos of their house, usually taken from online mapping apps like Google Maps. [Additional coverage in [KrebsOnSecurity](#)]

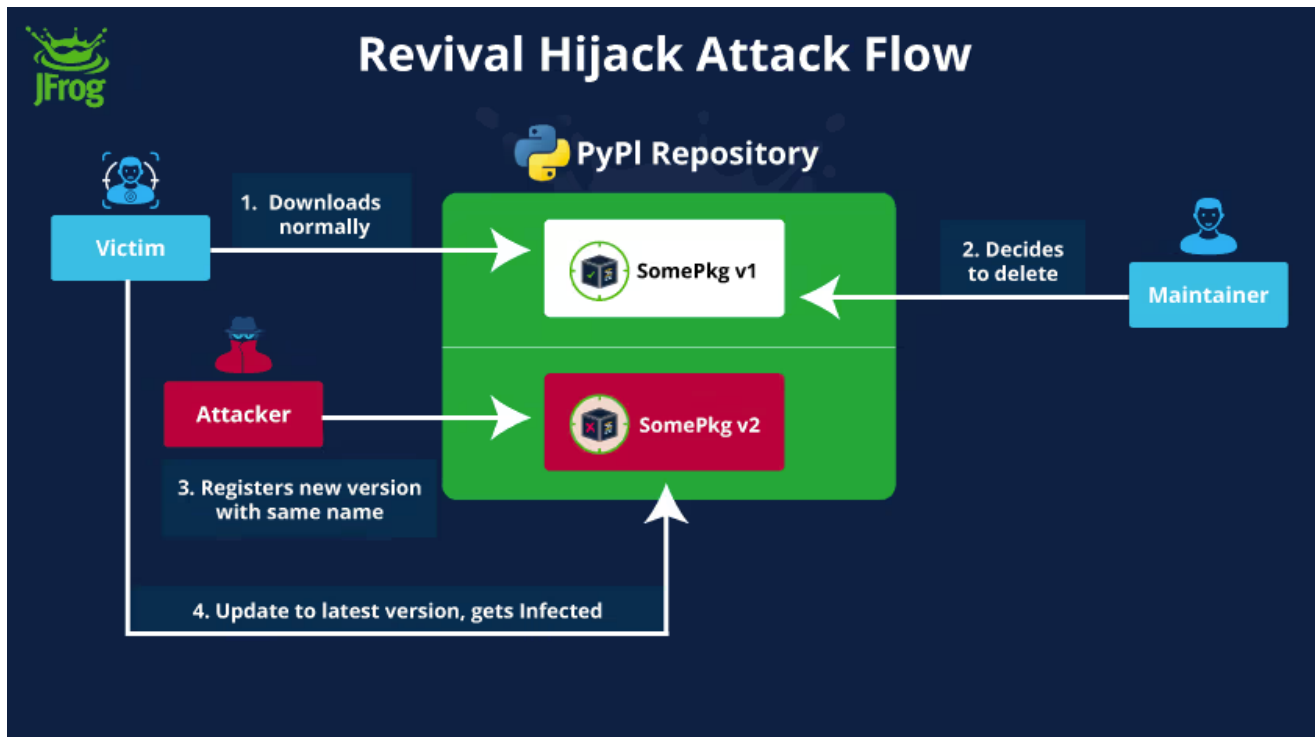
**Hacker on hacker crime:** Security firm [Veriti](#) has found that a threat actor infected other hackers with an infostealer by sharing a free tool that could check the validity of OnlyFans credentials. It's happened a bunch of times before, but this never gets old.



**#FreeDurov campaign:** Check Point, just like CyberKnow last week, looks at the hacktivist groups responding with DDoS attacks to France's arrest of Telegram CEO Pavel Durov.

**Yandex browser abuse:** Security firm Dr.Web has published a report on a spear-phishing attack that compromised a Russian rail freight operator in March this year and abused a novel technique to gain persistence on an infected host via the Yandex browser app itself.

**PyPI Revival Hijacking:** Threat actors are using a technique named Revival Hijacking to re-register deleted package names and deliver malware to projects where the old packages are still used. The technique has been observed being used in the wild on the Python Package Index (PyPI). Security firm JFrog says it reported the attacks to the PyPI team in June, but administrators have not yet removed the ability to re-register deleted package names. JFrog says that more than 22,000 Python libraries reference and still load deleted packages, exposing themselves to attacks.



## Malware technical reports

**LATAM trojans:** Trend Micro reports that two banking trojans named Mekotio and BBTok are having a resurgence across Latin America.

*"Mekotio's latest variant suggests the gang behind it is broadening their target, while BBTok is seen abusing MSBuild.exe to evade detection. Cybercriminals behind these known banking Trojans are using judicial-related phishing emails apart from the tried and tested business lures to target victims. Our investigation of Mekotio suggests that cybercriminals are likely to expand their targets beyond the Latin Americas."*

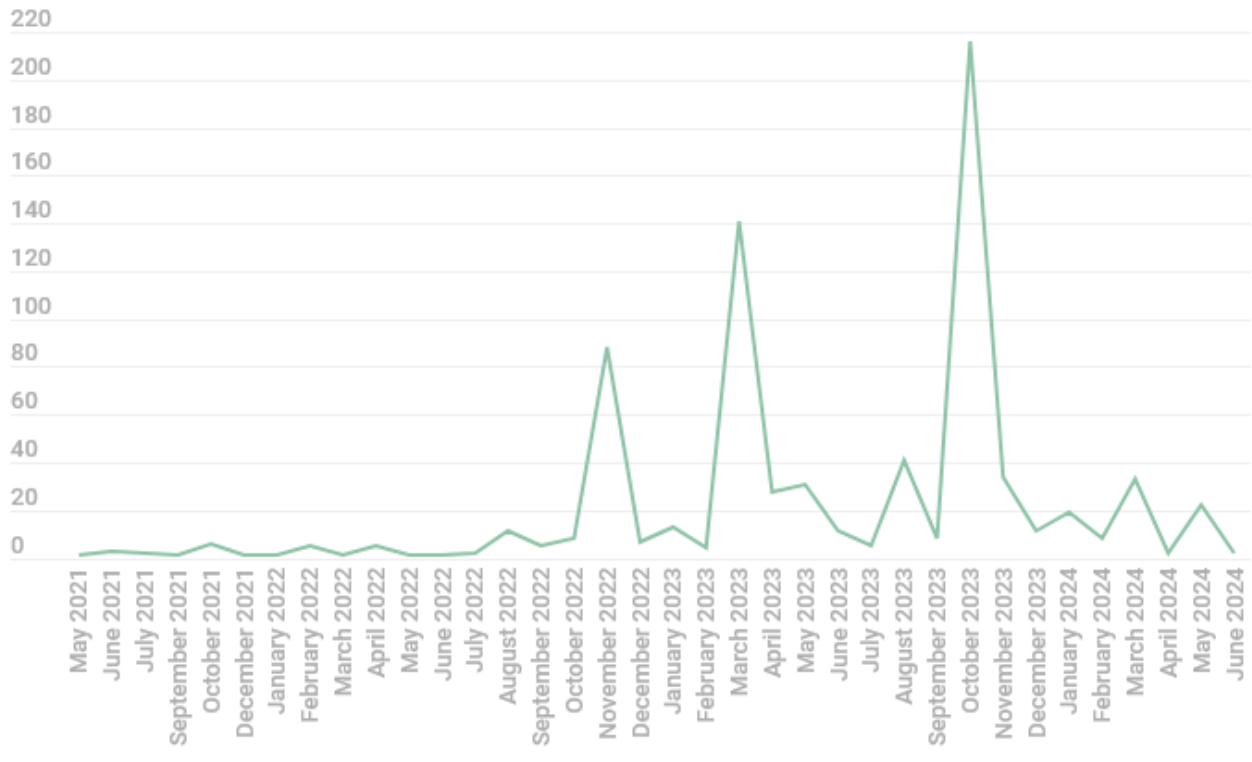
**AZORult:** ANY.RUN has published a technical report on the AZORult infostealer.

**SpyAgent:** McAfee has published a report on SpyAgent, a new Android malware campaign seeking to collect credentials for cryptocurrency accounts. The campaign has primarily targeted Korea and uses OCR to retrieve seed phrases from crypto wallets.

**Akira ransomware:** Hunt & Hackett researchers look at some of the technical oddities used by the Akira ransomware. More precisely, the report looks at Akira's abuse of Restart Manager—a Windows API designed for installers and updaters to temporarily shut down applications that lock specific files.

**Fog ransomware:** Adlumin researchers have published a report on the new Fog ransomware strain.

**Mallox ransomware:** The Mallox ransomware has slowly become one of the most active ransomware gangs over the past year. Security [Kaspersky says](#) it identified more than 700 different Mallox samples in 2023 alone. The group has continued to actively develop its code and is now also recruiting new affiliates for its RaaS program. Mallox is primarily known for using MSSQL and PostgreSQL database servers as initial entry points for its attacks. Their main tactics include exploiting unpatched database vulnerabilities or launching brute-force attacks against admin accounts.

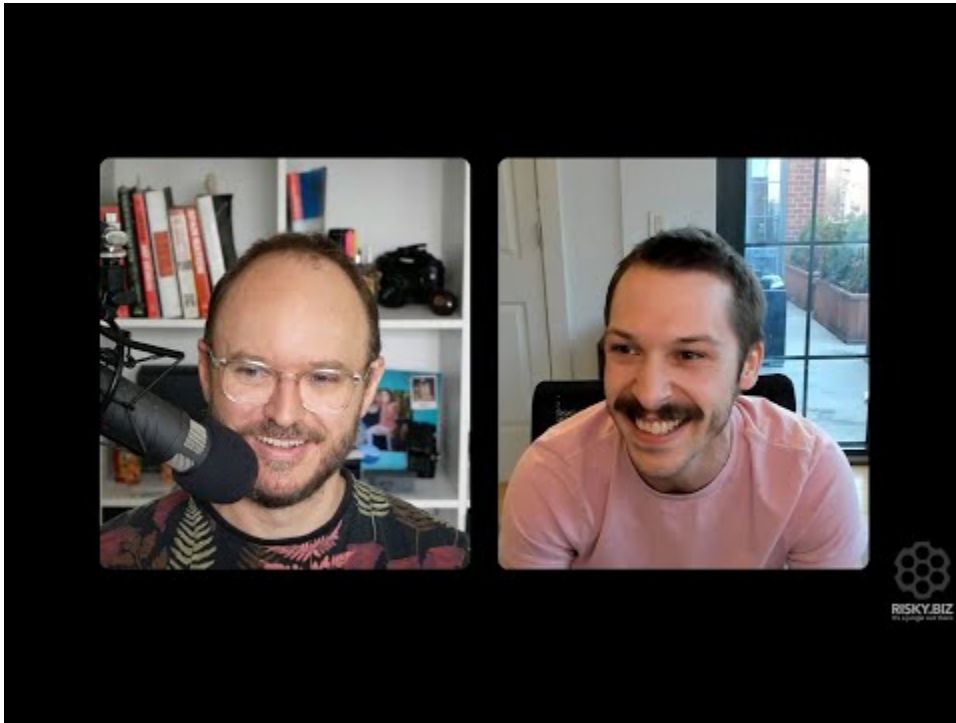


kaspersky

Discovered Mallox samples by PE timestamp

## Sponsor Section

*GreyNoise founder Andrew Morris demonstrates how people use the GreyNoise sensor network to find threats and detect attacks.*



[Watch Video At:](#)

[https://youtu.be/K\\_mYxCdqHDA](https://youtu.be/K_mYxCdqHDA)

## **APTs, cyber-espionage, and info-ops**

---

**US charges GRU cyber unit members:** The US government has charged five officers from a Russian military cyber unit involved in cyberattacks against Ukraine and NATO countries. Officials say the group launched the WhisperGate data-wiping malware ahead of Russia's invasion of Ukraine. The malware destroyed Ukrainian government systems in an attempt to delay its response to Russian invasion forces. The five allegedly worked with a sixth suspect, a Russian civilian the DOJ charged at the end of June. Officials say the five suspects are part of Unit 29155 in Russia's GRU military intelligence agency. The unit is considered one of the GRU's best and has also been involved in attempted coups, assassinations, and sabotage missions. The US State Department is also offering a \$10 million reward for information on the unit and its members.

## REWARD UP TO \$10 MILLION FOR INFORMATION ON RUSSIAN MILITARY INTELLIGENCE OFFICERS



VLADISLAV BOROVKOV



DENIS DENISENKO



YURIY DENISOV



DMITRIY GOLOSHUBOV



NIKOLAY KORCHAGIN

These individuals are members of Unit 29155 of the Russian General Staff Main Intelligence Directorate (GRU), which has conducted malicious cyber activity against U.S. critical infrastructure, particularly in the energy, government, and aerospace sectors.

These Unit 29155 GRU officers are responsible for targeting critical infrastructure in the Ukraine and dozens of allied Western countries.

Anyone with information on Vladislav Borovkov, Denis Igorevich Denisenko, Yuriy Denisov, Dmitry Yuryevich Goloshubov, and Nikolay Aleksandrovich Korchagin, GRU's malicious cyber activity, or associated individuals and entities should contact Rewards for Justice via the Tor-based tips-reporting channel below.



U.S. Department of State  
Diplomatic Security Service  
Rewards for Justice

Tor Link: [he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion](http://he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion)

**Russia targets Ukraine's military mobile apps:** Suspected Russian hackers are targeting Ukrainian soldiers with Signal phishing messages in an attempt to install malware on their phones. The malware was hidden in malicious versions of Eyes and GRISELDA, two mobile apps used by the Ukrainian Army. The purpose of the attacks is to steal authentication data to access military systems, as well as to exfiltrate the device's GPS coordinates. CERT-UA has linked the attack to a group it tracks as UAC-0210.

**Confucius:** Researchers with the Anheng Information Hunting Lab have published a report detailing a recent campaign linked to the Confucius APT group and utilizing a load of commodity tooling.

**Konni:** South Korean security firm Genians looks at a Konni APT campaign targeting Russia and South Korea.

**Lazarus:** Group-IB has put out a report on recent Lazarus social-engineering campaigns targeting developers at gaming and crypto companies.

*"They show no signs of easing their efforts, with their campaign targeting job seekers extending into 2024 and to the present day. Their attacks have become increasingly creative, and they are now expanding their reach across more platforms."*

**Earth Lusca's KTLVdoor:** Trend Micro has published a write-up on KTLVdoor, a new backdoor used by the Earth Lusca APT. The backdoor is written in Go specifically for the multi-platform support.

"The scale of the attack campaign is significant, with over 50 C&C servers found hosted at a China-based company; it remains unclear whether the entire infrastructure is exclusive to Earth Lusca or shared with other threat actors."

**Tropic Trooper:** A suspected Chinese APT group has hacked an online platform that published studies on human rights in the Middle East for the sole purpose of stealing research about the Israel-Hamas conflict. The attack was the work of Tropic Trooper, a Chinese APT active since 2011 and also known as KeyBoy and Pirate Panda. [Kaspersky](#) says that based on its analysis, the online platform was the sole target, and the group went to great lengths to maintain access once it was discovered.

**Chinese recon tools:** The [Natto Thoughts](#) team has put together a summary of the open-source and custom reconnaissance tools used by Chinese threat actors in their operations. See fancy table below.

<b>Tools &amp; Malware</b>	<b>Used by Threat Groups</b>	<b>Deployed in Threat Campaigns</b>
<b>NBTscan or modified NBTscan</b>	APT10, (aka: menuPass, Stone Panda, POTASSIUM, Purple Typhoon), GALLIUM, Stately Taurus (aka: Mustang Panda), Earth Lusca, TGR-STA-0043	Operation Cloud Hopper, Operation Soft Cell
<b>ScanBox malware</b>	APT40 (aka: TA423, Red Ladon, GADOLINIUM, Gingham Typhoon, Leviathan, MUDCARP, Temp.Periscope), APT3 (aka: Red Sylvan, Gothic Panda); APT10, Poison Carp (aka Evil Eye, Earth Empusa, Red Dev 16), LuckyCat (aka: TA413, White Dev 9)	
<b>Yasso</b>	TGR-STA-0043	Operation Diplomatic Specter
<b>LadonGo</b>	TGR-STA-0043, Stately Taurus	
<b>sqlmap</b>	Earth Krahang	
<b>nuclei</b>	Earth Krahang	
<b>xray</b>	Earth Krahang	
<b>vscan</b>	Earth Krahang	
<b>pocsuite</b>	Earth Krahang	
<b>wordpresscan</b>	Earth Krahang	
<b>shortname</b>		
<b>scanner</b>		
<b>veinmind</b>		
<b>Ehole</b>		

## Vulnerabilities, security research, and bug bounty

**Chrome zero-day PoC:** A security researcher going by Mistymntncop has released a [PoC exploit](#) for CVE-2024-5274, a Chrome zero-day that Google [patched](#) back in May.

**Windows zero-day:** QiAnXin has published a [report](#) on [CVE-2024-30051](#), a now-patched Windows zero-day that was abused in the wild by the now-defunct Qakbot botnet.

**Gatekeeper flaws:** Jamf researchers have published a [review](#) of recent techniques to bypass macOS Gatekeeper and deploy malware.

**Another LiteSpeed bug:** Patchstack has published details on [CVE-2024-44000](#), another bug in the LiteSpeed WordPress caching plugin that can be used to hijack admin-level accounts. The first one was [CVE-2024-28000](#), patched two weeks ago. The older one exploited a user ID function while this new one exploits a bug that lets attackers extract admin cookies from the plugin's debug feature.

**Android Security Bulletin:** Google has released the Android security updates for [September 2024](#). This month, the company has patched a zero-day tracked as CVE-2024-32896, which Google says may be "under limited, targeted exploitation." Google initially patched this for Pixel devices in June and has now backported the fix for the general Android population.

**Cisco security updates:** Cisco has released [five security advisories](#) for various products. [One](#) of them is a default admin account. [Another one](#) has a public exploit available.

**Zyxel security updates:** Zyxel has released [three security updates](#) to address nine vulnerabilities across routers, firewalls, and WiFi access points.

**Veeam security updates:** Backup service Veeam has released [security updates](#) for 18 vulnerabilities.

**Apache OFBiz security update:** The Apache OFBiz ERP has released a security update to fix [CVE-2024-45195](#), a new pre-auth RCE. See [Rapid7 write-up](#) for more details. The chances of this getting exploited are high since it's related to other OFBiz RCEs that are already being exploited in the wild.

## Infosec industry

---

**New tool—RedInfraCraft:** CyberWarFare Labs has released [RedInfraCraft](#), a tool to automate the deployment of red team infrastructure, such as C2s, phishing, and payload distribution servers.

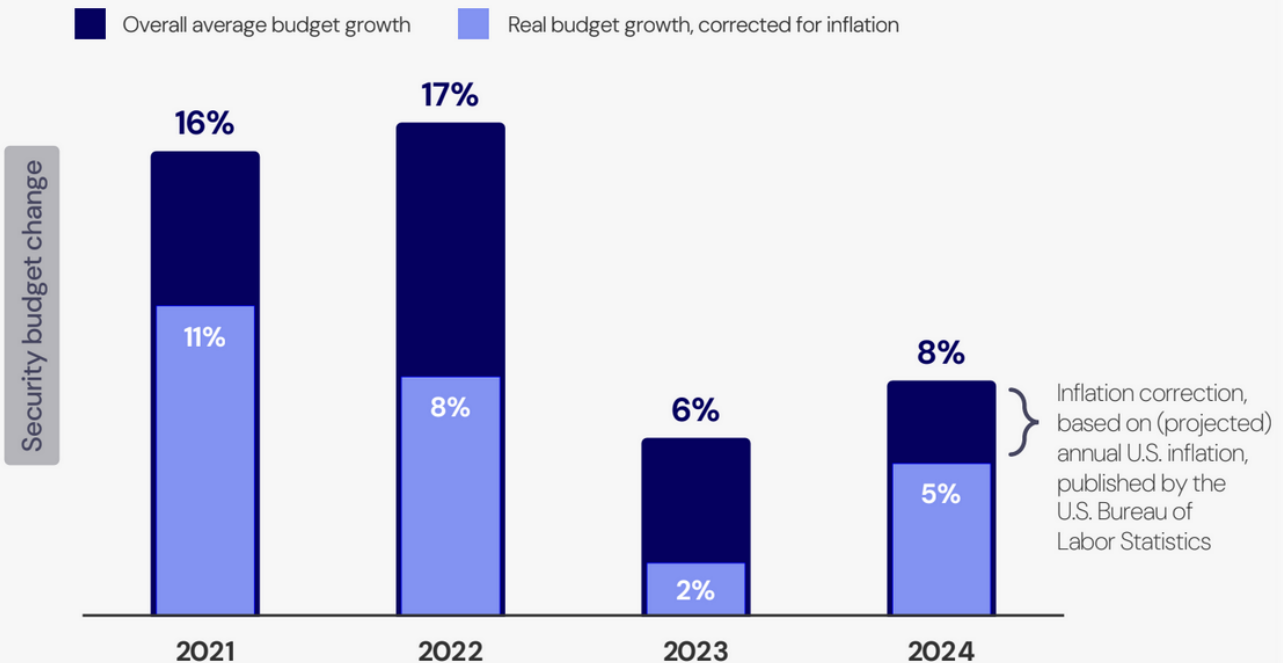
**Threat/trend reports:** [Cloudflare](#), [Gen Digital](#), [IANS](#), [Positive Technologies](#), and [Team Cymru](#) have recently published reports covering infosec industry threats and trends. From the IANS report:



"Nearly two-thirds of CISOs have reported receiving increased security budgets this year. An IANS Research survey found that budgets grew by 8% from 2023's numbers, but the growth rate is half of what it used to be at the start of the decade. Adjusted for inflation, IANS says the real increase is actually only 5%. The positive trend is that security budgets now account for more in a company's IT spending, rising from 8.6% in 2020 to 13.2% in 2024."

### Overall Security Budget Change Improves Modestly Versus 2023

Year-over-year change in the security budget



### Risky Business Podcasts

*In this edition of Between Two Nerds, Tom Uren and The Grugq talk to Alex Joske, author of a book about how the Chinese Ministry of State Security (MSS) has shaped Western perceptions of China. They discuss the MSS's position in the Chinese bureaucracy, its increasing role in cyber espionage, its use of contractors, and the PRC's vulnerability disclosure laws.*

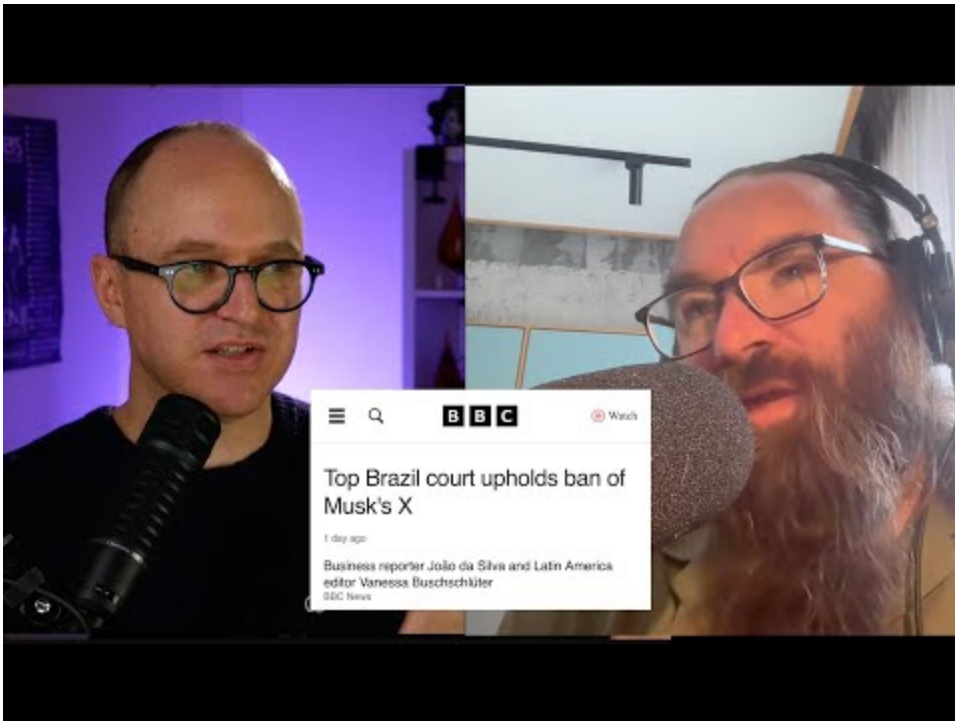
*In this podcast, Tom Uren and Patrick Gray discuss Russia's use of exploits from commercial spyware vendors. Bought through a front, or stolen with other bugs? They also discuss Iran's counter-intelligence innovations—if you apply for a job that's very clearly an Israeli front, then perhaps you're not that trustworthy after all?*



[Watch Video At:](#)

<https://youtu.be/3loM75K4e7k>

*Risky Business is now on YouTube with video versions of our main podcasts. Below is our latest weekly show with Pat and Adam at the helm!*



[Watch Video At:](#)

<https://youtu.be/u-Q9TzKPwqI>