Risky Biz News: Google shuts down YouTube Russian propaganda channels

riskybiznews.substack.com/p/risky-biz-news-google-shuts-down

Catalin Cimpanu

In other news: German energy suppliers get hacked, and Finnish police arrest scammer after he accidentally took a photo of his fingerprint.

Catalin Cimpanu
Jun 13, 2022

Share

This newsletter is brought to you by Airlock Digital, Rumble Network Discovery, Proofpoint, and Thinkst Canary. 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.

In its quarterly disinformation report for Q2 2022, Google said last week that it suspended more than 190 YouTube channels and 12 Google Ads accounts linked to Russia's disinformation efforts surrounding its invasion of Ukraine. Forty-four of these accounts were linked to the Internet Research Agency (IRA), the Russian internet troll farm based in Sankt Petersburg, an entity that has been active for years and still operates despite several US Treasury sanctions.

Google said these accounts published content that was supportive of Russia's invasion of Ukraine and Russian President Vladimir Putin and critical of NATO, Ukraine, Ukrainian President Volodymyr Zelenskyy, and Russian opposition politician Alexei Navalny. Some accounts also tried to justify the activity of Russian private military contractor Wagner Group in Ukraine and Africa, where they have been accused of civilian killings and other atrocities.

Google's crackdown comes as the company also suspended in the first quarter of the year more than 715 YouTube accounts used for the same purpose and after the company also delisted multiple Russian state-media news outlets from its Google News section in March.

"The information domain is a critical theater of war for the Kremlin," said researchers from the Brookings Institution think tank earlier this year in March in a report analyzing news search results for Ukraine-related terms. The report—published before Google moved to remove Russian state media outlets from its News section—found that sites like TASS dominated Google's search results, helping the Kremlin drive its message to huge audiences.

Companies like Google, Microsoft, Twitter, and Meta (formerly Facebook) have been trying to shut down Russia's genocide-washing propaganda but with little results, especially on Twitter and Facebook, where copy-pasta bot networks and especially troll farms continue to dominate discussions.

While Twitter and Meta have intervened to limit the reach of official Russian state news outlets, tweets about Ukraine, Russia, and NATO are often flooded with bots and trolls. Similarly, on Facebook, bots and trolls also flood the comments sections in news stories from western media outlets, often driving the discussions toward Russian-friendly narratives.

In most cases, these disinformation and propaganda efforts often follow the same patterns, namely that Ukraine has committed genocide against its Russian-speaking minority and Russia is only trying to save them, narratives that have been thoroughly debunked by multiple sources ranging from Russian independent media to the EU itself.

Breaches and hacks

Optimism hack happy ending: The threat actor who intercepted a transfer of nearly $19 million (at the time) between the Wintermute and Optimism cryptocurrency platforms last week has decided to return the stolen funds, according to blockchain security firm PeckShield.

German energy suppliers: German energy suppliers Entega and Mainzer Stadtwerke were hit by a cyber-attack over the weekend. The attacks, believed to be unrelated, blocked access to companies' email servers and public websites, but industrial systems remained unaffected.

General tech and privacy

Cloud middleware: Wiz, the cloud security firm that discovered the OMIGOD vulnerability last year, has continued its research into the types of middleware products installed by default on cloud servers. The company has published a GitHub repo with cloud middleware (aka cloud agents) installed and used across the major cloud service providers (Azure, AWS, and GCP). These agents—13 right now— are usually installed without the customers' awareness or explicit consent.

Firefox reducing sandbox escape attack surface: In its quarterly security newsletter for Q1 2022, Mozilla said it deployed a new security feature to Firefox in v96 that will reduce the attack surface for Firefox sandbox escapes (attack from the browser to the underlying OS).

Government, politics, and policy

More surveillance in Russia: The Russian government has updated its SORM technical guide to specifically tell network operators to intercept and store data from their customers, such as internet calls, browsing history, and user geo-location. According to Kommersant, a new legislation draft proposed last week corrects technical requirements needed for data collection and storage of certain parameters; for a better compatibility between SORM systems and the control panel used by the FSB to access this data. The news outlet said that certain network operators will have to update SORM equipment to comply with the government's new user data collection methodology.

Cybercrime and threat intel

Confluence exploitation: Microsoft's security team said on Saturday that at least two nation-state groups—tracked as DEV-0401 and DEV-0234—are now exploiting the Atlassian Confluence RCE zero-day vulnerability CVE-2022-26134 that was disclosed last week. Microsoft researchers said that this vulnerability has also been used for device and domain discovery, but also for the deployment of payloads like Cobalt Strike, web shells, botnets like Mirai and Kinsing, coin miners, and even ransomware.

Microsoft Security Intelligence @MsftSecIntel

Multiple adversaries and nation-state actors, including DEV-0401 and DEV-0234, are taking advantage of the Atlassian Confluence RCE vulnerability CVE-2022-26134. We urge customers to upgrade to the latest version or apply recommended mitigations:

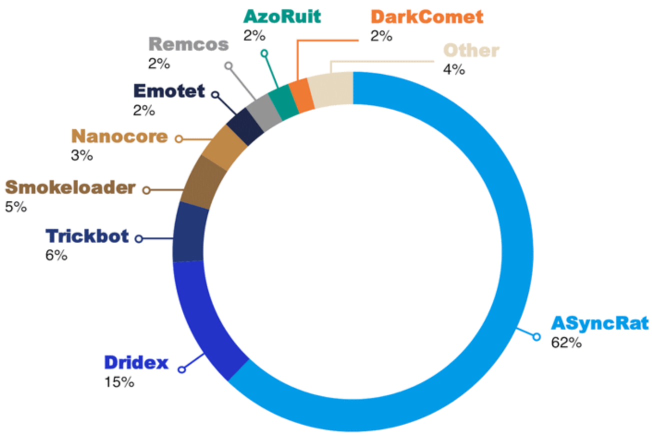
msft.itConfluence Security Advisory 2022-06-02 | Confluence Data Center and Server 7.18 | Atlassian Documentation

12:24 AM · Jun 11, 2022

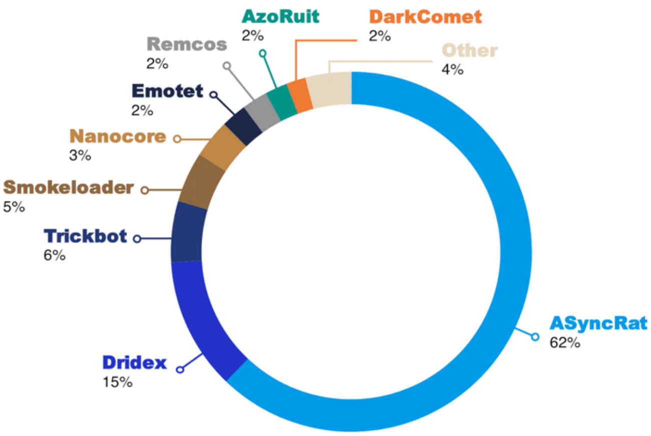
152Likes78Retweets

SeaFlower group: Confiant said in a report last week that it detected a new threat actor—that it named SeaFlower—targeting cryptocurrency users. Since at least March this year, the group has operated websites cloned after legitimate cryptocurrency wallets. These websites, which target Chinese-speaking audiences, host backdoored wallet apps that steal users' private wallet seeds.

ASyncRAT stats: Malwarebytes reported this week that its telemetry indicated that ASyncRAT had become the most widespread malware payload delivered via email spam in the first half of 2022. ASyncRAT was ranked #3 throughout 2021, behind Dridex and TrickBot.



Email threat detections in the first half of 2022


Email threat detections in the first half of 2022

Finland arrest: An online scammer was detained in Finland last week after defrauding local car dealerships. Investigators said they were able to identify the suspect after they took a high-quality photo of a fake check where one of their fingertips was also visible, allowing them to identify them based on police records. (h/t @mikko)

Nigerian bank robbers: Nigerian police said they detained three suspects for a daring scheme to hack into the networks of at least 11 Nigerian banks and steal funds. According to authorities, the group had bribed an employee at one of the banks to leave critical network gateways open so they could gain access to the bank network and steal funds. Per data recovered from seized devices, the group was planning to use the same method on 10 other banks if this first intrusion went without a hitch. *[Coverage in BankInfoSecurity]*

Adconion execs plead guilty: Three of four Adconion executives pleaded guilty last week to fraud and misrepresentation via email. The three were charged in 2018 for hijacking IP address blocks from their inactive owners. Some of these IP addresses were later used to send email spam.

Few NetWalker victims complained: Speaking at the RSA security conference last week, FBI and DOJ officials said that only a quarter of all victims of the NetWalker ransomware filed complaints with authorities. Law enforcement seized NetWalker's infrastructure in January 2021, and the gang ceased operations following the law enforcement crackdown.

Malware technical reports

HelloXD ransomware: Palo Alto Networks has published a technical report on HelloXD, a ransomware strain that has been active since November 2021. The security firm also managed to link the ransomware to a threat actor active on underground cybercrime forums named "**x4k**."

Android malware: Security firm McAfee said it found malicious functionality designed to steal Instagram account credentials in an Android app designed to allow users to modify the default Instagram app and in several apps designed to increase Instagram account followers and post likes.

APTs and cyber-espionage

Sandworm: CERT Ukraine said in a security alert on Friday that the Sandworm APT group was targeting Ukrainian news organizations with malicious emails. Officials said that more than 500 radio stations, newspapers, and news agencies were targeted with malicious Office files that tried to weaponize the still-unpatched Office Follina zero-day.

Lyceum APT: Zscaler has published a report on a .NET-based backdoor used by the Lyceum APT that the group had been using to target Middle Eastern organizations in the energy and telecommunication sectors. According to researchers, the malware uses a technique called "*DNS Hijacking*" in which an attacker-controlled DNS server manipulates the responses of DNS queries to redirect targets to malicious sites.

Vulnerabilities and bug bounty

PACMAN attack: Academics from MIT CSAIL have disclosed a novel attack against Apple M1 processors. The attack, named PACMAN, can elevate access from userland to kernel space by bypassing Pointer Authentication (PAC). The PACMAN attack can be executed via a network connection, and is the third side-channel attack against Apple CPUs after Augury and M1racles.

K8s vulnerability: Kubernetes servers are affected by a vulnerability (CVE-2021-25748) in their Nginx integration where "a user that can create or update ingress objects can use a newline character to bypass the sanitization" and "obtain the credentials of the ingress-nginx controller." The Kubernetes team said that in default Kubernetes configurations, this credential has access to all secrets in the cluster.

Trendnet vulnerabilities: Trendnet TEW-831DR WiFi routers have been found to have multiple vulnerabilities exposing the owners of the router to potential intrusions of their local WiFi network and possible takeover of the device.

Drupal bugs: The Drupal CMS has released out-of-cycle security updates to fix bugs in third-party libraries.

Backdoor account in thermal cameras: IoT security company SEC-Consult disclosed last week that IRAY A8Z3 thermal cameras contain hardcoded credentials for their web application in one of its firmware binary, which can be extracted and used by attackers to modify camera settings. In addition, the same camera model also contains several other vulnerabilities. After 16 months, the vendor has yet to patch any of the reported issues.

Backdoor in Mitel VoIP phones: Mitel Networks has patched its 6900 IP Series VoIP phones and removed a backdoor functionality from the firmware that would have allowed remote attackers to run malicious commands on its devices[1, 2]. The vulnerability was found and reported by German pen-testing firm Syss.

Share