Risky Biz News: Cyber Partisans hack and disrupt Kremlin censor

Risky Biz News: Cyber Partisans hack and disrupt Kremlin censor

In other news: Vanuatu government hit by ransomware; AWS shuts down free Wickr Me E2EE IM service; Zeppelin ransomware secretly decrypted for two years.

Catalin Cimpanu
Nov 21, 2022

This newsletter is brought to you by Airlock Digital, Proofpoint, runZero, 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.

Belarusian hacktivist group Cyber Partisans has hacked the Russian General Radio Frequency Center (GRFC), a smaller sub-agency that's part of the Roskomnadzor, the Russian government's telecommunications watchdog.

In Telegram and Twitter posts, the Cyber Partisans said they gained access to the agency's internal network, from where they stole more than 2TB of emails and documents before trashing its domain controller and encrypting local workstations.

"The work of the chief Kremlin censor has been disrupted," the group boasted.

"We also have a huge amount of material proving **large-scale surveillance** on the network and attempts to establish **total control over everyone** who has spoken out **against the Putin regime** over the past 20 years," they added, promising to share the stolen data with journalists.

The GRFC confirmed the breach to *Kommersant* and blamed the hack on the use of a "*previously unused vulnerability*," but the agency vehemently denied that any employee workstations were encrypted.

The incident marks the second time the Roskomnadzor has dealt with a major security breach this year after the Anonymous hacker collective also breached and then leaked more than 800TB of data from the agency's servers earlier this year in March. The leaked documents showed the agency actively intervening and censoring the narrative around Russia's role in Ukraine, such as prohibiting the use of the word invasion to describe Russia's so-called "*special military operation*."

Breaches and hacks

Vanuatu ransomware attack: The government of the small island nation of Vanuatu was hit by a ransomware attack that crippled most of the government's IT networks and forced staff back to pen and paper. According to a report from the Sydney Morning Herald, a team from the Australian Cyber Security Centre is currently helping Vanuatu officials recover their network from the attack.

AirAsia ransomware attack: Malaysian airline AirAsia was the victim of a ransomware attack earlier this month. According to a report in DataBreaches.net, the company was hit by the Daixin Team ransomware group, which claims to have stolen data on more than five million of the airline's passengers, data they are now threatening to leak online.

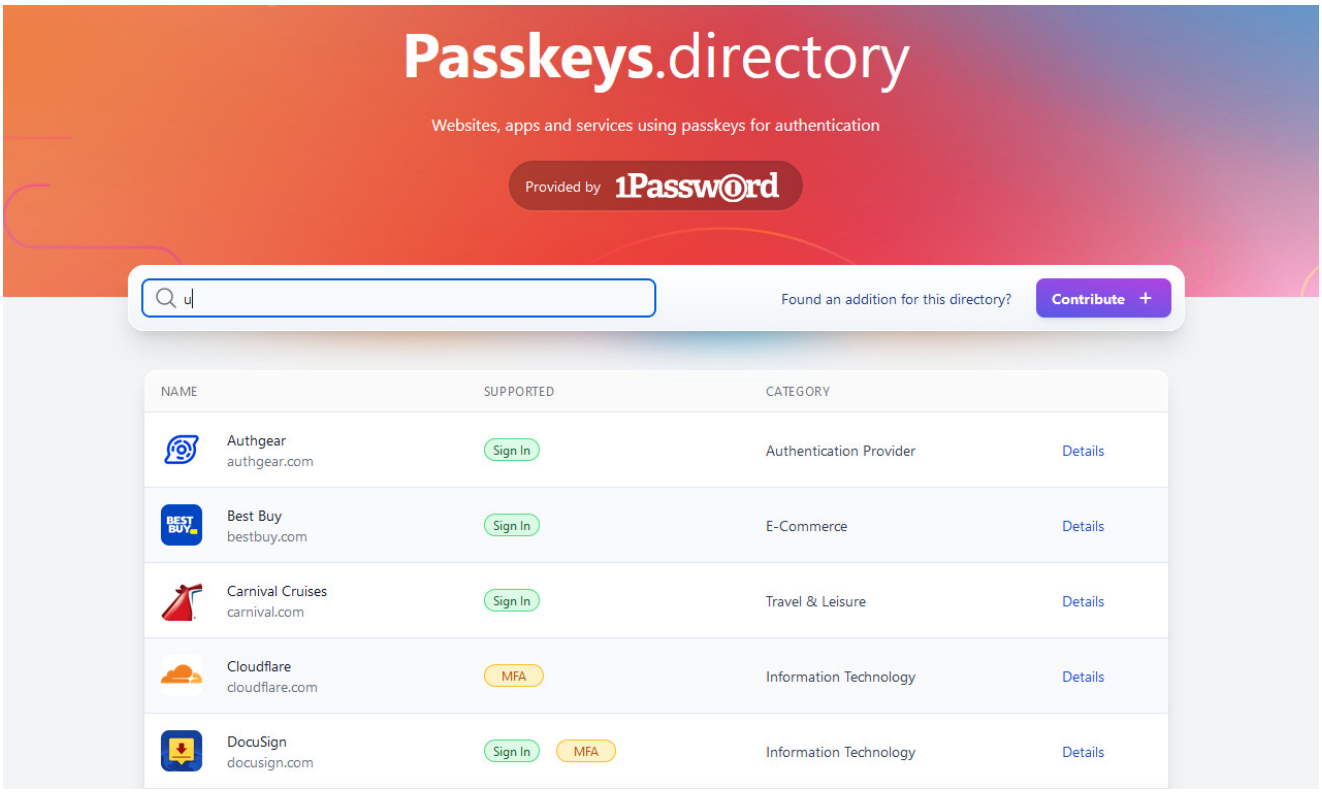
General tech and privacy

Wickr shuts down free IM service: Secure instant messaging service Wickr announced that it would shut down its free service to focus on its commercial offering. The company said it would not accept new user registrations after December 31, 2022, and will discontinue the Wickr Me service on December 31, 2023. Amazon acquired Wickr in June 2021 and was planning to use it as an E2EE service for its commercial enterprise offerings—now known as AWS Wickr.

Twitter does its thing: A network of Twitter bot accounts has been blamed for stoking riots and physical clashes between Indian and Pakistani supporters at the end of August in the UK city of Leicester. More than 500 accounts were spotted urging both groups to violence, with some accounts tweeting as much as 500 times per minute. [*Additional coverage in Bloomberg*/non-paywalled]

> "After the first instances of fake videos spread on Twitter, a 'highly orchestrated echo chamber,' from India kicked into amplify tweets 'solely blaming Muslims for the events in Leicester,' the report claimed, which in turned spurred even more violence against Hindus in Leicester."

Passkeys support directory: After it added support for passkeys in its password manager, 1Password has also created a web directory listing all online services currently supporting passkey authentication.



Government, politics, and policy

Quantum encryption deadline: The Office of Management and Budget has ordered federal agencies to scan their systems and provide an inventory of assets containing cryptographic systems that could be cracked by quantum computers in the coming years. Agencies have a deadline until May 4, 2023, according to an OMB memo [PDF]. The memo comes after the White House directed US government agencies to mitigate risks from quantum computers earlier this year and after the NSA ordered that all government agencies that handle classified information must use quantum-resistant encryption algorithms by 2035. [*Additional coverage in FedScoop*]

AGs ask FTC for online privacy regulation: A coalition of 33 state attorneys general have urged the US Federal Trade Commission to pass regulation around online data collection practices. AGs said they are "concerned about the alarming amount of sensitive consumer

data that is amassed, manipulated, and monetized," and that they regularly receive inquiries from consumers about how their data is being hoarded and abused. [*Read the full letter here/PDF*]

Indian privacy regulation: The Indian government has published the long-awaited first public draft of its upcoming data privacy law—known as the Digital Personal Data Protection Bill. According to the law's text, companies that operate in India and handle the personal data of Indian citizens must use clear and plain language to describe what data they collect and for what purpose. The new law includes many clauses similar to the EU GDPR, such as requiring companies to notify users about security breaches, and allowing users to delete their data from online services. Companies that fail to comply with this upcoming regulation risk some of the largest fines in the world for a privacy breach, fines of up to 500 crore rupees—up to $61 million.

Iran info-op in Latin America: Threat intelligence company Recorded Future has published a report detailing a years-long influence operation carried out by the Iranian and Venezuelan governments that targeted audiences in Latin America. The campaign revolves around the Colombian businessman Alex Saab, detained and extradited by the US from Cape Verde in 2020 for helping the Venezuelan government establish business ties with Iran and avoid US sanctions. Recorded Future claims that since Saab's arrest, news outlets associated with the Iranian and Venezuelan governments, together with social media "influencer" accounts, have promoted the idea across Latin America that Saab, who was appointed as a special envoy for the Venezuelan government, was kidnapped by the US in contradiction to diplomatic immunity and international norms.

Russian bill to seize cybercrime profits: Two Russian government officials have submitted a bill to the Russian State Duma with an amendment to the Russian criminal code that would allow the Russian government to easily seize funds obtained through cybercrime offenses, Kommersant reported. According to the bill's text, the government plans to use the seized funds to compensate victims.

Sponsor section

RunZero is one of this newsletter's four main supporters and this week's featured sponsor. The company's main product is its network discovery and asset inventory platform, which can be used to find any managed and unmanaged assets inside a customer's network. To learn more, please check out this runZero product demo below:

Cybercrime and threat intel

Hackers detained in South Korea: South Korean police have arrested ten suspects who allegedly orchestrated a very targeted phishing campaign against the owners of popular Naver blogs. Police said the gang targeted only 500 of the most popular Naver blogs,

managed to hack into 18, and made 200 million won ($149,000) from reselling the accounts to third parties. Officials said they are still hunting for other suspects who they believe helped the hackers.

New threat actor: A threat actor going by the name of IntelBroker is claiming to have breached several US government agencies and is now running ads on underground hacking forums claiming to sell more than 2 GB of files stolen from the agencies' networks. While the group has made bold claims, several security researchers have indicated that the ad might be a scam, as the actor has not provided any evidence of a widespread breach of the US government. The threat actor's name also seems to be tied to a new Ransomware-as-a-Service portal called Endurance, and security researchers believe this might be a clever ruse to draw affiliates to the new service. "Not sure what their angle is, but it seems like notoriety maybe for a quick exit scam," threat intel analyst CyberKnow told *RiskyBizNews* over the weekend.

Aleksandar Milenkoski @milenkowski

The repository hosts the source code of the Endurance #wiper. A comment in the source code indicates that IntelBroker is not part of a group and that #Endurance is an on-going project.

```
/*
hello! this is the early development stage that this wiper is currently at.
at the current time this is the first major section finished. MBR hijacking still has to be implemented
and will take some time to work out.
i am a single person doing this in my free-time. so please dont try to piss me off about the code being trash.

please run in debug mode. i have not setup the release version yet.

if u want to see what is being added or worked on. please check the TODO section of the thread.
*/
```

7:10 PM · Nov 16, 2022

DDoS attacks on DNS servers: A CAIDA research paper has found that DDoS attacks targeted "millions of domains (up to 5% of the DNS namespace)" but that "most attacks did not substantially harm DNS performance," even if some attacks did end up bringing down services or increasing resolution times of up to 100 times. The research paper analyzed data from a 17-month period between November 2020 and March 2022.

Malware on Telegram: Russian security firm Positive Technologies published a report on Telegram's budding cybercrime ecosystem. According to the company's scans, Telegram has slowly replaced hacking forums and is currently being used for advertising a wide spectrum

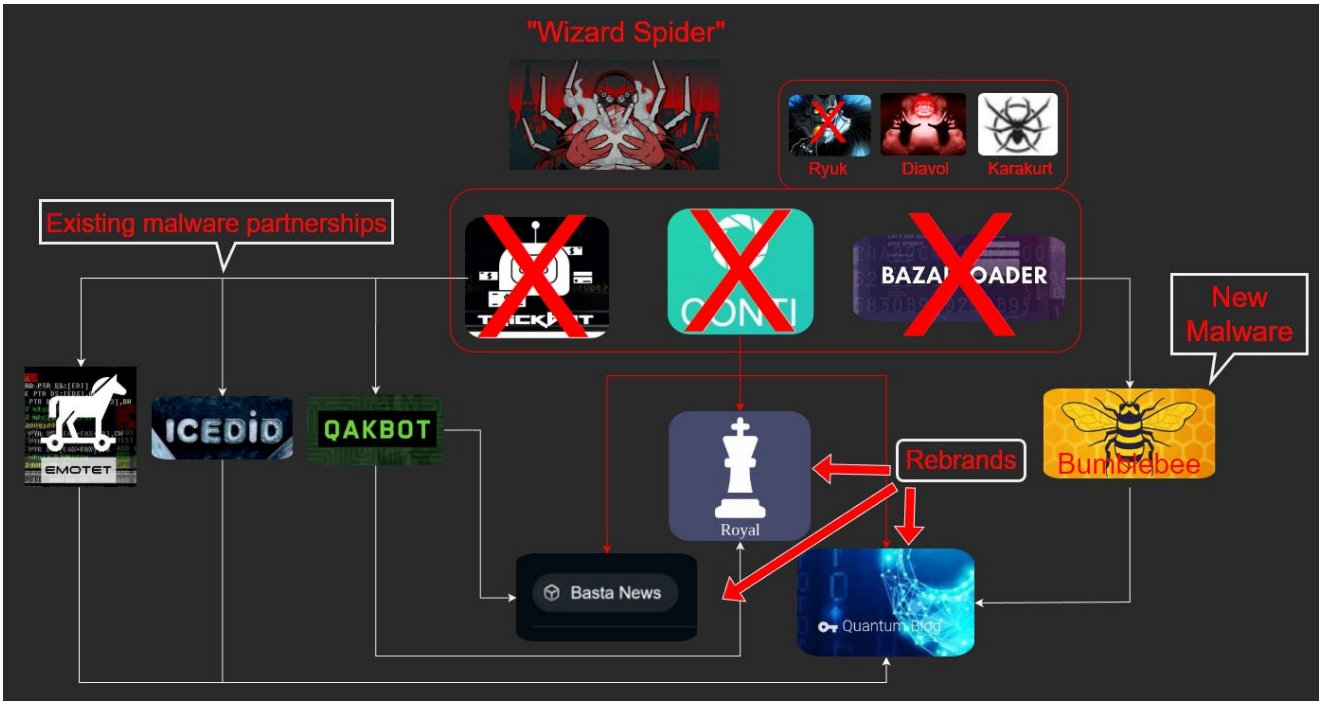
of hacking services and malware, with the sale of remote access trojans, corporate network accounts, and cash-out services being some of the most popular topics on the platform.

New npm malware: Check out GitHub's security advisory portal for details.

Emotet's return: Deep Instinct researchers have an analysis of Emotet's return, the infamous spam botnet that has been asleep since June this year. More on this from Proofpoint too.

Conti off-shoots: Equinix security researcher William Thomas has a report on how members of the former Conti gang have scattered across the malware ecosystem since disbanding in early 2022.

> "The members of Conti have continued attacks, but seemingly under several different names, including Quantum, Royal, and Black Basta (also highlighted by Vitali Kremez here). Campaigns previously attributed to Conti such as Karakurt and Diavol have also continued in 2022 since the leaks. These new data-theft-extortion ransomware campaigns, though, have been supported by malware other than Trickbot and BazarLoader, this includes the new BumbleBee malware, as well as three malware botnets previously associated with Conti attacks: IcedID, Qakbot, and Emotet."



Malware technical reports

Zeppelin ransomware decrypter: Cybersecurity firm Unit221b said it found a design flaw in the encryption scheme of the Zeppelin ransomware in February 2020, and for the past two years, the company has been using this vulnerability to allow victims to recover their files without paying the attackers. Unit221b disclosed their findings at the Black Hat security conference held last week in Riyadh, Saudi Arabia, after noticing that attacks with the Zeppelin ransomware slowed down to a crawl this year, suggesting that the gang's had lost faith in their encrypter. [*Additional coverage in KrebsOnSecurity*]

Venus ransomware: SentinelOne has published a technical breakdown of the Venus ransomware, also known as Goodgame ransomware. The ransomware is known for targeting systems and networks that run unprotected RDP endpoints, which it uses as entry points for the attack, and has been recently at the center of a security alert [PDF] issued by the US Department of Health and Human Services.

Agent Tesla: The Splunk team has a report out on the Agent Tesla remote access trojan and its technical guts and modus operandi. OALABS also has some IOCs and detecting advice for it too.

QakBot updates: Securonix researchers have published a report on the recent updates to the QakBot (Qbot) malware code. For the technical only.

W4SP Stealer: Checkmarx researcher Jossef Harush Kadouri has published an analysis of the W4SP Stealer (or WASP Stealer) that was recently used in two PyPI-based supply chain attacks. In a more recent attack spotted by Phylum, the group behind this malware appears to be using the names of popular organizations to continue to spread their RAT via boobytrapped PyPI packages.

Cobalt Strike detections: The Google Cloud security team has released a set of open-source YARA Rules and a VirusTotal Collection to help security practitioners flag and identify Cobalt Strike components and specific Cobalt Strike versions on their networks.

> "We decided that detecting the exact version of Cobalt Strike was an important component to determining the legitimacy of its use by non-malicious actors since some versions have been abused by threat actors."

APTs and cyber-espionage

Earth Preta: Trend Micro has an analysis of some recent spear-phishing operations carried out by the Earth Preta APT against government networks worldwide. The operation began in March this year and tried to infect victims with malware such as TONEINS, TONESHELL, and PUBLOAD. The group is also known as Mustang Panda and Bronze President.

GRU 26165: The Atlantic Council has a report on GRU Unit 26165, a cyber unit of the Russian military intelligence service that has used on-site agents to hack into their targets' networks. The unit has been linked to an attempted hack of the Organization for the Prohibition of Chemical Weapons (OPCW), based in Amsterdam, the Netherlands.

> "After loading a car with technical equipment—including a wireless network panel antenna to intercept traffic—the four individuals scouted the OPCW's headquarters in The Hague for days, taking photos and circling the building before being intercepted by the Dutch General Intelligence and Security Service (*Algemene Inlichtingen- en Veiligheidsdienst* or AIVD) and sent back to Moscow. Seemingly, the plan had been for the operatives to hack into the OPCW's systems to disrupt investigations into the attempted GRU chemical weapon attack [*on former Russian intelligence officer Sergei Skripal and his daughter Yulia in Salisbury, England*]."

Vulnerabilities and bug bounty

Infineon vulnerability: German chipmaker Infineon is apparently using an eight-year-old version of OpenSSL for the trusted-platform module (TPM) for some of its chips, according to a report from Binarly, a security firm specialized in firmware security. Other companies like Lenovo, Dell, and HP were also found to use extremely old versions of OpenSSL as well, with Lenovo and Dell using an OpenSSL version released back in 2009.

CVE-2022-35803: NorthSec researchers have published details on CVE-2022-35803, a vulnerability in the Windows Common Log File System (CLFS) logging service that Microsoft patched earlier this year in September.

CVE-2022-26696: SecuRing researcher Wojciech Reguła has published details on CVE-2022-26696, a vulnerability in the macOS Terminal that can be exploited to escape the macOS sandbox. The bug was fixed in mid-September 2022.

Infosec industry

Acquisition news: Palo Alto Networks announced plans to buy Cider Security, a company that develops application security (AppSec) and software supply chain security solutions.

OpenSSF adopts S2C2F: The Open Source Security Foundation (OpenSSF) has adopted the Secure Supply Chain Consumption Framework (S2C2F), a policy framework developed by Microsoft for hardening projects against supply chain attacks.

Project Spaceman: An article from Richard J. Aldrich goes into Project Spaceman, a project by British computer maker ICL that provided secure systems to the MI5 and the British government in the early 80s.

New tool—MI-X: Cybersecurity firm Rezilion has open-sourced a tool named MI-X (Am I Exploitable?) that allows researchers and developers to know if their containers and hosts are impacted by specific, high-profile vulnerabilities.

ResponderCon 2022 videos: Talks from the ResponderCon 2022 security conference, which took place in September, are available on YouTube.

Share