

October  
2021

# Hacker Daily News



A review of the past month's vulnerabilities, hacks, cracks and cyber attacks.



## Is the REvil ransomware set for a return?

By Mayank Sharma

First Published 1 month ago



There's been no official word from REvil yet



After being offline for about two months, several of the dark-web servers belonging to notorious [ransomware](#) operator REvil have come back online.

## REvil ransomware devs added a backdoor to cheat affiliates

By [Ionut Ilascu](#)

 September 23, 2021  02:26 AM  0



Cybercriminals are slowly realizing that the **REvil ransomware operators may have been hijacking ransom negotiations**, to cut affiliates out of payments.

By using a cryptographic scheme that allowed them to decrypt any systems locked by REvil ransomware, the operators **left their partners out of the deal and stole the entire ransom.**



## REvil ransomware shuts down again after Tor sites were hijacked

By Lawrence Abrams

 October 17, 2021  07:19 PM  2



The REvil ransomware operation has likely shut down once again after an unknown person **hijacked their Tor payment portal and data leak blog.**

The **Tor sites went offline earlier today**, with a threat actor affiliated with the REvil operation posting to the XSS hacking forum that someone hijacked the gang's domains.

## Hackers get data trove in U.N. breach

Reconnaissance, not damage, apparent goal; risks feared for some agencies

by WILLIAM TURTON AND KARTIKAY MEHROTRA BLOOMBERG NEWS (WPNS) | September 10, 2021 at 4:00 a.m.



Follow



Hackers breached the United Nations' computer networks earlier this year and made off with a **trove of data** that could be used to target agencies within the intergovernmental organization.

The credentials belonged to an account on the U.N.'s proprietary project management software, called **Umoja**. They **likely got in using the stolen username and password of a U.N. employee purchased off the dark web**.

ZDNet

SECURITY

DATA MANAGEMENT



MUST READ **GOOGLE TENSOR: EVERYTHING YOU NEED TO KNOW ABOUT THE PIXEL 6 CHIP**

## 91% of IT teams have felt 'forced' to trade security for business operations

When it comes to remote work, security is often the last thing on the priority list.



By Charlie Osborne for Zero Day | September 9, 2021 | Topic: Security

A new survey suggests that the majority of IT staff have felt pressured to ignore security concerns in favor of business operations.

In total, **91%** of those surveyed said that they have felt "**pressured**" to **compromise security due to the need for business continuity during the COVID-19 pandemic**. 76% of respondents said that security had taken a backseat, and furthermore, 83% believe that working from home has created a "ticking time bomb" for corporate security incidents.



## Israeli cybersecurity firm buys ExpressVPN for close to \$1b

Kape Technologies has been acquiring a number of companies in the VPN and data security space in recent years; this deal is one of the biggest buys by an Israeli company

By RICKY BEN-DAVID

13 September 2021, 7:50 pm



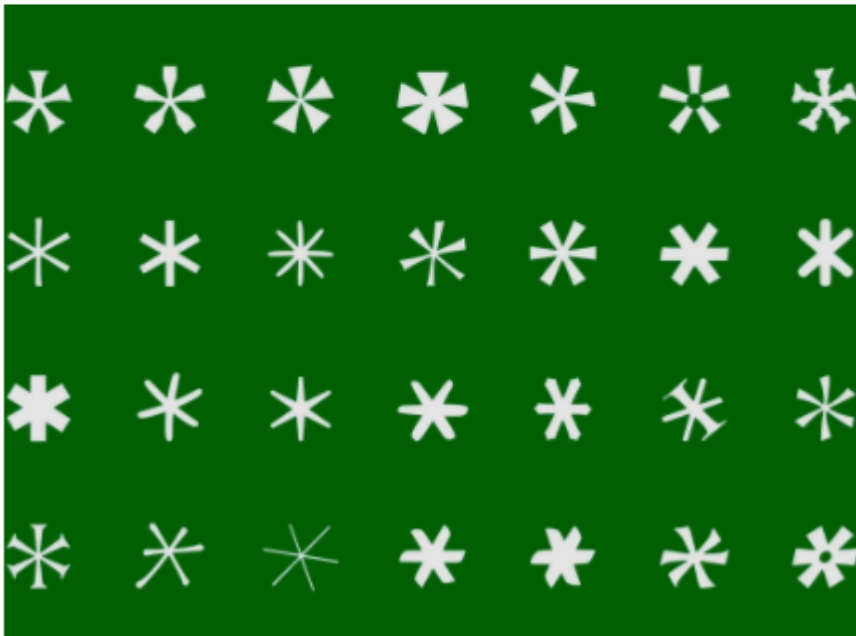
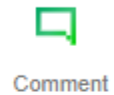
Israeli cybersecurity firm **Kape Technologies** announced it was acquiring leading virtual private network provider (VPN) ExpressVPN for **\$936 million**, in one of the biggest buys of a foreign outfit for an Israeli company to date.

Kape has made a number of major acquisitions in the VPN and data security space in recent years including privacy and security solutions provider GhostVPN in 2017, Zenmate, another VPN provider, in 2018, and most recently Webselenese, an Israeli provider of privacy and security-related news and product information, six months ago.

## Microsoft now lets you sign in without a password

Carly Page

@carlypage\_ / 11:35 AM GMT-4 • September 15, 2021



Microsoft is rolling out its passwordless sign-in option, previously available **only to commercial** customers, to **all Microsoft accounts**.

This means that users will be able to sign-in to services, such as **Outlook** and **OneDrive**, without having to use a password. Instead, **users can use the Microsoft Authenticator app, Windows Hello, a security key and SMS or emailed codes**.



## Ransomware encrypts South Africa's entire Dept of Justice network

By [Ionut Ilascu](#)

 September 15, 2021  03:35 PM  1



The justice ministry of the South African government is working on restoring its operations after a recent ransomware attack.

“[The attack] has led to **all information systems being encrypted and unavailable** to both **internal employees as well as members of the public**. As a result, **all electronic services** provided by the department are affected, including the issuing of letters of authority, bail services, e-mail and the departmental website”

## US will reportedly impose crypto sanctions amid ransomware attacks



Igor Bonifacic

September 17, 2021, 12:50 pm



The Biden administration plans to implement **new measures to make it more difficult for hackers to profit from ransomware attacks using cryptocurrencies**. The Treasury Department will reportedly **impose sanctions and guidance designed to discourage organizations from using digital currencies to pay for ransoms**.

Later in the year, the Treasury Department is also expected to implement **new anti-money laundering and terror-financing regulation** to limit further the use of cryptocurrencies as a payment method for ransoms and other illegal activity.

[Markets](#) **News Report**

## AT&T Sued After SIM Swap Attack Results in \$560K Crypto Loss for Customer

By [Martin Young](#)

20 September 2021, 09:17 GMT+0000

Updated by [Kyle Baird](#)

20 September 2021, 09:56 GMT+0000

A Texas resident, filed the suit in the state's District Court on Sept 15. In it, Etheridge is **claiming** that AT&T failed to provide reasonable and appropriate **security** to prevent unauthorized access to his wireless account.

The plaintiff was unable to use his cell phone number to mitigate the incursion and ended up losing **159.8 in ETH** worth approximately **\$560,000** at the time.

The scammer then asks the carrier to **activate a new SIM in their possession** and proceeds to port the victim's number to the new SIM. **Then they can access financial accounts that rely on phones for authentication methods** such as one-time SMS passcode



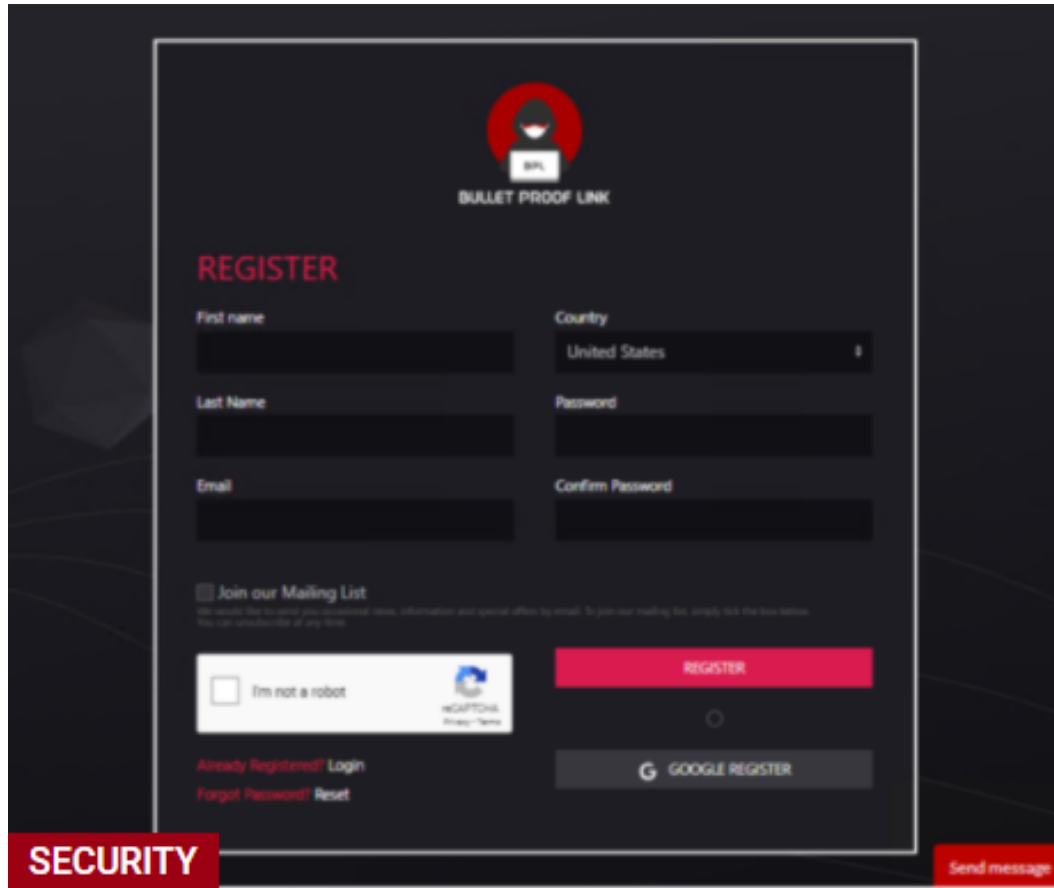


## Security Lapse

Audit uncovers information safety weaknesses at passport agency

An information technology audit of the **Jamaican Passport, Immigration and Citizenship Agency (PICA)** has **uncovered critical information security weaknesses which could put records and people's identity at risk for theft.**

“Absence of a robust access control system may result in unauthorised access and use of confidential information. Additionally, weaknesses in the administration of user accounts, combined with an insufficiently enforced password policy, may result in the compromise of user accounts, unauthorised modification of records and enable identify theft,” she reported.



## Microsoft Security details extensive 'phishing-as-a-service' operation

Microsoft detailed an **extensive phishing-as-a-service operation** that provides various services to those wishing to undertake phishing campaigns.

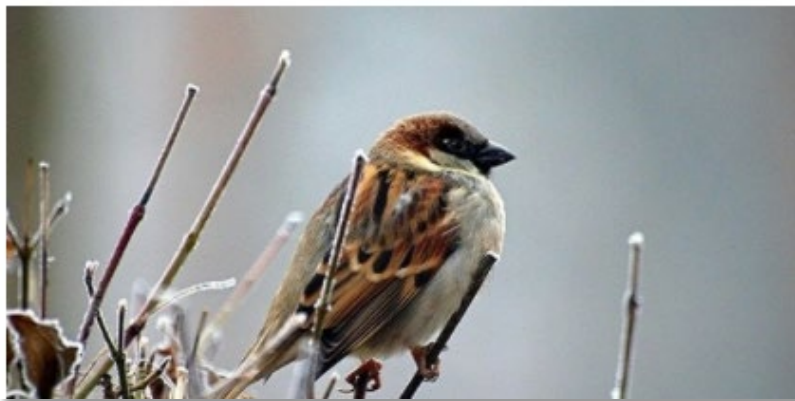
Called **BulletProofLink**, the operation sells **phishing kits, email templates, hosting and automated services** at what's described as a relatively low cost. The service offers over 100 phishing templates that mimic known brands, including Microsoft, and provides a service that's nearly effortless to use. **The service cost as little as \$50**, up to a full range of services on a **subscription basis pay \$800 a month**

## Newly unmasked 'FamousSparrow' APT group is targeting hotels and governments worldwide

Dev Kundaliya

24 September 2021 • 2 min read

SHARE



ESET researchers have uncovered a new cyberespionage group targeting hotels, governments, and private companies worldwide. We have named this group **FamousSparrow** and we believe it has been active since at least **2019**.

FamousSparrow is a group that we consider as the only current user of the custom backdoor, **SparrowDoor** (which we cover in detail in the later sections of this blogpost). It also uses **two custom versions of Mimikatz**. **Attacks have been linked to countries such as** Brazil, Burkina Faso, South Africa, Canada, Israel, France, Guatemala, Lithuania, Saudi Arabia, Taiwan, Thailand and United Kingdom.



## Twitch Confirms Major Breach

Data including its source code and payouts to creators was posted to 4chan

By David Cohen | October 6, 2021



[Amazon](#)-owned streaming platform [Twitch](#) confirmed reports of a **major breach**.

Chris Scullion of [Video Games Chronicle](#) was the first to report the breach, saying that an anonymous hacker posted a **125-gigabyte** torrent link to [4chan](#) Wednesday containing information such as Twitch's source code and payouts to creators.



Google has announced that it is planning to **auto-enroll 150 million users into the company’s “two-step verification” system by the end of this year.**

With 2FA/2SV, when entering the password to open an app the user will receive a text message on his/her personal device with a unique one-time code to verify identity and open the app.

## Russia poses the biggest nation-state cyber threat, says Microsoft

Microsoft's Digital Defense Report points the finger at Russia, North Korea, Iran and China, among others.



By [Liam Tung](#) | October 8, 2021 | Topic: [Security](#)



"During the past year, 58% of all cyberattacks observed by Microsoft from nation-states have come from Russia," Tom Burt, Microsoft corporate vice president [said in a blogpost detailing government-backed hacking over the past year.](#)




"Russian nation-state actors are **increasingly targeting government agencies for intelligence gathering**, which jumped from 3% of their targets a year ago to 53% -- largely agencies involved in foreign policy, national security or defense," he explained.



## CIA Funding Arm Gave Encrypted App Wickr \$1.6 Million

The funding solidifies Wickr's position as an encrypted chat platform for government agencies.

By [Joseph Cox](#)

Oct 12 2021, 1:51pm  [Share](#)  [Tweet](#)  [Snap](#)



In-Q-Tel, a nonprofit investment firm started by the Central Intelligence Agency (CIA), recently poured more than **\$1.6 million into encrypted messaging platform Wickr.**

The \$1.6 million was transferred before Amazon purchased the company, but **highlights Wickr's continuing position as an end-to-end encrypted messaging app for government agencies.**

## Fired IT admin revenge-hacks school by wiping data, changing passwords

By [Ionut Ilascu](#)

 October 6, 2021  03:34 AM  3



**A 29-year old wiped data on systems of a secondary school in the U.K. and changed the passwords at an IT company, in retaliatory cyber attacks for being fired.**

As a result of his actions, the school's systems could no longer be accessed and remote learning was impacted at a time when pupils were at home due to the Covid-19 pandemic.



**Attacks using password-stealing malware have surged by 45% over the past six months,** highlighting the continued need for additional log-in security measures, according to Kaspersky

The Russian AV vendor analyzed incidents of **Trojan-PSW** - a specialized stealer capable of gathering login and other account information. It noted 160,000 more targets in September 2021 than April, with the total number reaching nearly half a million. That's an increase of 45%.

**As statistics show, logins, passwords, payment details and other personal data continue to be an attractive target for cyber-criminals** and they remain a popular commodity on the dark market



## This malware botnet gang has stolen millions with a surprisingly simple trick

Malware researchers reckon this botnet has made millions by exploiting an easy shortcut taken by many.



By Liam Tung | October 15, 2021 | Topic: Security



The long-running botnet known as MyKings is still in business and has raked in at least **\$24.7 million** by using its network of compromised computers to mine for cryptocurrencies.

MyKings, also known as **Smominru** and Hexmen, is the world's largest botnet dedicated to mining cryptocurrencies by **free-riding off its victims desktop and server CPUs**. It's a lucrative business that gained attention in 2017 after infecting more than half a million Windows computers to mine about **\$2.3 million** of Monero in a month.



# The End

