


January
2022

Hacker Daily News



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






Data Breaches Digest

Home


MONDAY, 10 JANUARY 2022

Ransomware Operator Claims - Week 01 2022



Welcome to last week's ROC Report, an exclusive summary of Ransomware Operator's global victims that were claimed during the period between 3rd January and 9th January 2022, kindly provided by our partners.

Barbados has been reported to have its first ransomware attack of 2022. The **Grief** Ransomware Gang has the name of the local company disclosed as the victim of the attack and shows an invoice, payroll and employee badge IDs among the information exfiltrated during the attack.

 **DARKTRACE**

INVOICE

To: [Redacted]

St Michael
BB11000
Barbados

Darktrace Limited
Maurice Wilkes Building
St John's Innovation Park
Cowley Road
Cambridge
CB4 0DS
UK
Telephone: +44(0) 1223 394 100
Email: fingroup@darktrace.com
VAT Reg No: GB 290 0399 03


Invoice Details					
Customer VAT Number:	Invoice No	Invoice Date	Terms	Payment Due	
	65631	09 Dec 2020	30 Days	08 Jan 2021	

Description	Unit Price	Quantity	Net Amt	Tax %	Tax	Gross
Darktrace Enterprise Immune System						
Invoiced quarterly in advance						
01 Dec 2020 to 28 Feb 2021	7,140.00	1.00	7,140.00	0.000	0.00	7,140.00

Invoice 10 of 20

*F. Darli
Batch # 00582
6450010-1060-1*

PAYROLL AUTHORIZATION - SEPTEMBER 2019				
Please attach your signature to confirm the details below				
DEPARTMENT	GROSS SALARY	HEAD OF DEPARTMENT	HEAD OF DEPARTMENT (signature)	DATE
Accounts				
Archives and Information				
Engineering				
Human Resources				
ICT				
Multi-Choice				
News and Sports				
Radio Programming				
Sales and Marketing				
Television Programming				
Administration				

 [Redacted]

URL: [Redacted]

READ MORE

Views: 6418 | Published: 2022-01-07 13:42:05 | Updated: 2022-01-11 19:26:46



With the preliminary voters list disclosed online ahead of the 2022 general election, there have been concerns raised by the public about the personal information being made available online.

The ISSA Barbados Chapter made a blog post advising the public about the risks associated with the disclosure and background information about the Representation of the People Act and amendments which lead up to the disclosure.



Made for minds.

TOP STORIES MEDIA CENTER TV RADIO LEARN

CORONAVIRUS WORLD GERMANY BUSINESS SCIENCE ENVIRONMENT

TOP STORIES / WORLD

SERIES: HOW TO DEBUNK MISINFORMATION

Fact check: How do I spot fake news?

During the pandemic fake news about the virus, remedies and vaccines have perpetuated. Learn how to spot fake news effectively.

Checklist: How do I spot fake news?

- Fake news often appeals to emotions and instincts: Think about why the news appeals to you
- Is it clear where the information came from? Check if it is from the original source. If it's not, be skeptical
- Does the person or website spreading the information seem credible? It's worth taking a closer look
- Sensational wording, a dubious layout or spelling mistakes should make you suspicious
- Look for more information on the topic to compare and cross-check



Bug in backup software results in loss of 77 terabytes of research data at Kyoto University

by Bob Yirka , Tech Xplore



Computer maintenance workers at **Kyoto University** have announced that due to an apparent **bug in software used to back up research data**, researchers using the University's Hewlett-Packard Cray computing system, called Lustre, have lost approximately **77 terabytes** of data.



(Photo: CMC)

Bermudans lose millions to internet fraudsters

Bermuda police say internet fraudsters have swindled the country's residents out of almost **four million US dollars this year (2021)**.

The police said that “**entire life savings**” had been lost in some cases and authorities had managed to recover only US\$40,600 of the haul.

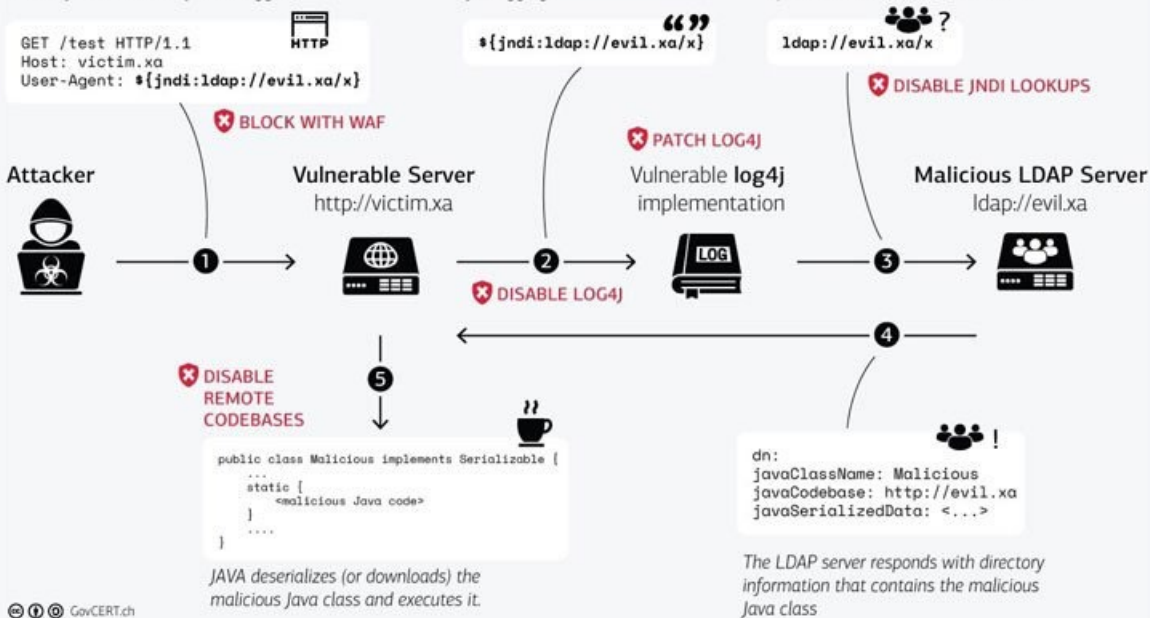
Detective Chief Inspector, Sherwin Joseph, of the Bermuda Police Service's special investigations unit, said the cost of computer crime added up to more than **US\$3.8 million for the year**.

Apache Log4j Vulnerability — Log4Shell — Widely Under Active Attack

December 12, 2021 Ravie Lakshmanan

The log4j JNDI Attack and how to prevent it

An attacker inserts the JNDI lookup in a header field that is likely to be logged.



Threat actors are actively weaponizing unpatched servers affected by the newly identified "Log4Shell" vulnerability in Log4j to install cryptocurrency miners, Cobalt Strike, and recruit the devices into a botnet, even as telemetry signs point to exploitation of the flaw nine days before it even came to light.

Fintech firm hit by Log4j hack refuses to pay \$5 million ransom



By **Ax Sharma**

December 29, 2021 07:07 AM



One of the largest **Vietnamese** crypto trading platforms, **ONUS**, recently suffered a cyber attack on its **payment system** running a vulnerable Log4j version.

Soon enough, threat actors approached ONUS to extort a **\$5 million** sum and threatened to publish customer data should ONUS refuse to comply.

CRYPTOBROWSER

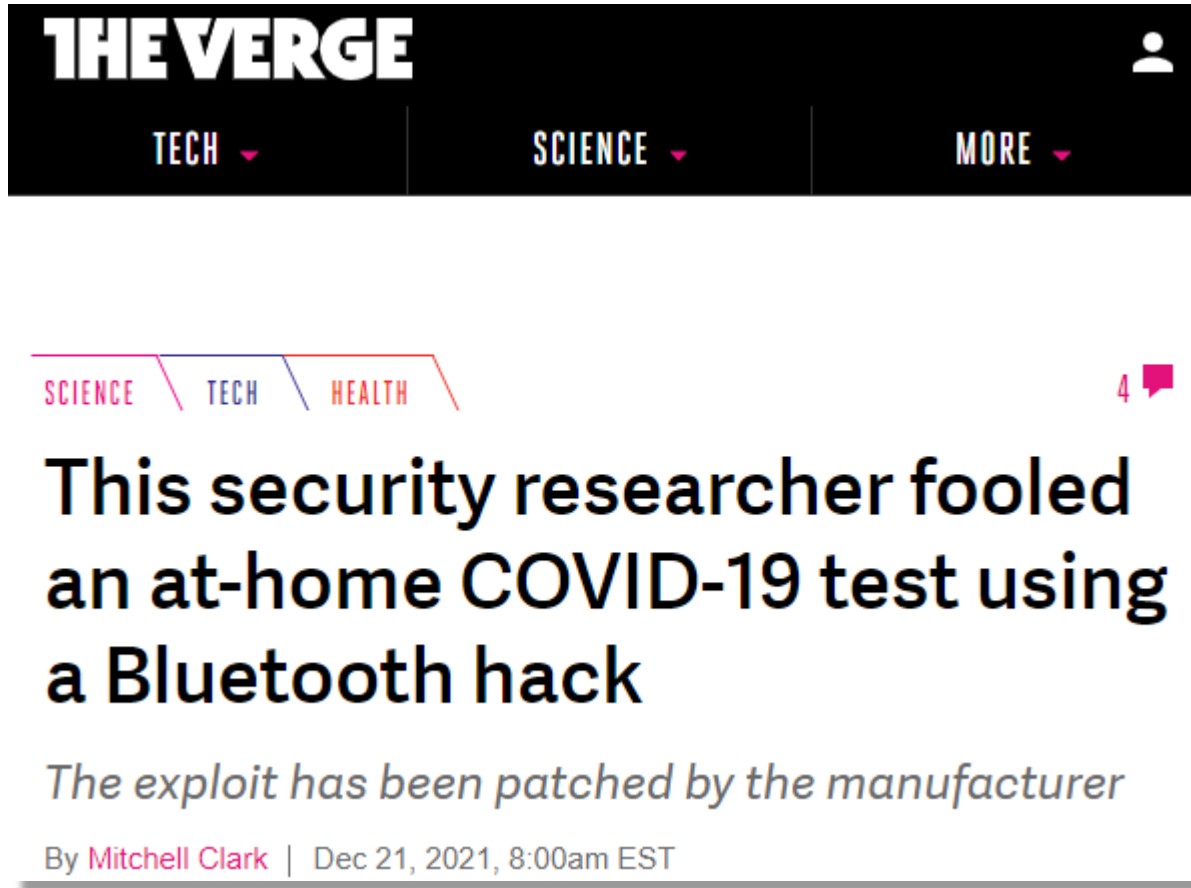
Cryptocurrencies 1234 Markets 0 Market Cap \$1,613,509,588,284 24h Vol \$12,946,680,569



The Leader In Security Breaches Was The DeFi Sector, With Poly Network Recording The Biggest DeFi Attack In History

The crypto sector evolved massively from its initial form in 2009, but one major issue still persists when it comes to digital currencies – the risk of illicit entities, which would try to steal them.

And despite the technological advances of crypto projects in the past couple of years, **in 2021 hackers got away with \$4.25 billion worth of cryptocurrencies**, which is almost a three-fold increase over 2020 and its \$1.49 billion stolen in crypto assets.



THE VERGE

TECH ▾ SCIENCE ▾ MORE ▾

SCIENCE / TECH / HEALTH

This security researcher fooled an at-home COVID-19 test using a Bluetooth hack

The exploit has been patched by the manufacturer

By Mitchell Clark | Dec 21, 2021, 8:00am EST

A security researcher was able to change the results of an at-home COVID test and get those results certified by **intercepting and modifying Bluetooth traffic** from the device before it reached the app.

The process of falsifying results wasn't a simple one — according to F-Secure's writeup, the researcher used a **rooted Android device** to tap into and analyze the data the tester was sending to the app.




Microsoft's Digital Crimes Unit has disrupted the activities of a **China-based** hacking group called **Nickel**. Countries in which Nickel has been active include: United States, Argentina, Brazil, Chile, Colombia, Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, **Jamaica**, Mexico, Panama, Peru, **Trinidad and Tobago** and Venezuela.

The attacks Microsoft's Threat Intelligence Center (MSTIC) observed are very sophisticated and use a variety of techniques, but they almost always had **one goal: to insert hard-to-detect malware that facilitates intrusion, surveillance, and data theft**. Sometimes, Nickel attacks used compromised **third-party virtual private network (VPN)** providers or **stolen credentials** obtained from spear phishing campaigns.

autoevolution

Search here...

FEATURED  autoevolution's **Porsche Month** →

Ransomware Group Claims Volvo Attack, Screenshots of the Stolen Files Released

Home > News > Technology

11 Dec 2021, 23:58 UTC · by Bogdan Popa



Volvo has recently been the victim of a data breach, with the company explaining in an advisory that hackers managed to steal what it described as a limited amount of the company's R&D property.

The carmaker, however, hasn't provided any specifics on the hack itself, and while it did say an investigation is already underway, it wasn't clear if its servers ended up infected with ransomware or not.

But as it turns out, this is exactly what happened, with ransomware group **Snatch** recently claiming the attack on its very own darknet website. **The gang has also published screenshots with the stolen files**, though no further specifics on the leak were shared.



TL; DR Breakdown

- Hackers drain \$80 million from **AscendEx**
- Wallets on three blockchains were compromised including **Ethereum**, **Polygon**, and the **Binance Smart Chain** network
- Hackers are now targeting exchanges' hot wallets



CNBC WATCH LIVE

TECH

BitMart says it will compensate victims of \$196 million hack and restore trading by Tuesday

PUBLISHED SUN, DEC 5 2021•5:56 PM EST UPDATED MON, DEC 13 2021•5:06 PM EST

 MacKenzie Sigalos
@KENZIESIGALOS

WATCH LIVE

Crypto trading platform **Bitmart** said on it had experienced “**a large-scale security breach**” and that hackers had **withdrawn about \$150 million in assets**. A third-party security firm, Peckshield, which first publicized the breach, put it closer to \$200 million.

The affected **ethereum** and **binance** smart chain “hot wallets” carried only a “small percentage” of the exchange’s assets, according to the company.

 HOME

THE EPOCH TIMES

 SUBSCRIBE



Bayswater Power Station near Muswellbrook in the Hunter Valley in Australia, on July 28, 2010. (TORSTEN BLACKWOOD/AFP via Getty Images)

AUSTRALIA

Hackers Came Within Minutes of Crippling Australian Power Grid

December 8, 2021 0:17, Last Updated: December 8, 2021 15:43

Queensland's CS Energy was the target of a sustained ransomware attack on Nov. 27, in what the utility's chief executive officer has described as a worryingly accelerating trend.




The attack was thwarted before it had the potential to shut the company's two thermal coal plants. Had the damage taken hold, it could have affected 35,000 megawatts of power, leaving 1.4 million to 3 million homes in the dark.



Microsoft has hit a new blow against a cyberespionage group coordinated from China. As the group has now announced, **42 domains were confiscated** that were used by the cyberespionage group **Nickel** alias **APT15**.

Microsoft had discovered some domains that were **used for data collection and transmission** to Nickel. A court in the US state of Virginia has now confirmed the confiscation of the domains.

Someone has been hacking Tor servers to de-anonymize users for four years

 By Kamal Saini | December 4, 2021 |  214 |  0



For the last four years, a shadowy individual or organization known as 'KAX17' has been joining malicious servers to the Tor network, converting them into nodes at a time when the network is running out of bridges to evade censorship.

And, so far, all evidence point to KAX17's objective to de-anonymize Tor users, according to cybersecurity experts.

That is, **up to 10% of Tor nodes ended up in the hands of an unknown malicious actor**; at the time, there was a 16% probability that a Tor user would connect to the network via one of KAX17's servers... and a 35% likelihood that their traffic would be routed through one of its mid-nodes.



FBI

Document shows how FBI can access your data on WhatsApp, Telegram, iMessage, others

An internal guide to how the FBI can snoop on targets using data requested from nine companies and their services: Apple's **iMessage**, **Line**, **Signal**, **Telegram**, **Threema**, **Viber**, Tencent's **WeChat**, Meta's **WhatsApp** and **Wickr**.

Information accessible include subscriber data, messenger sender-receiver data, device backup, IP address, encryption keys, date/time information, registration time information and user contacts. All but one (IP address) of iMessage can be accessed by the FBI.

The End

