

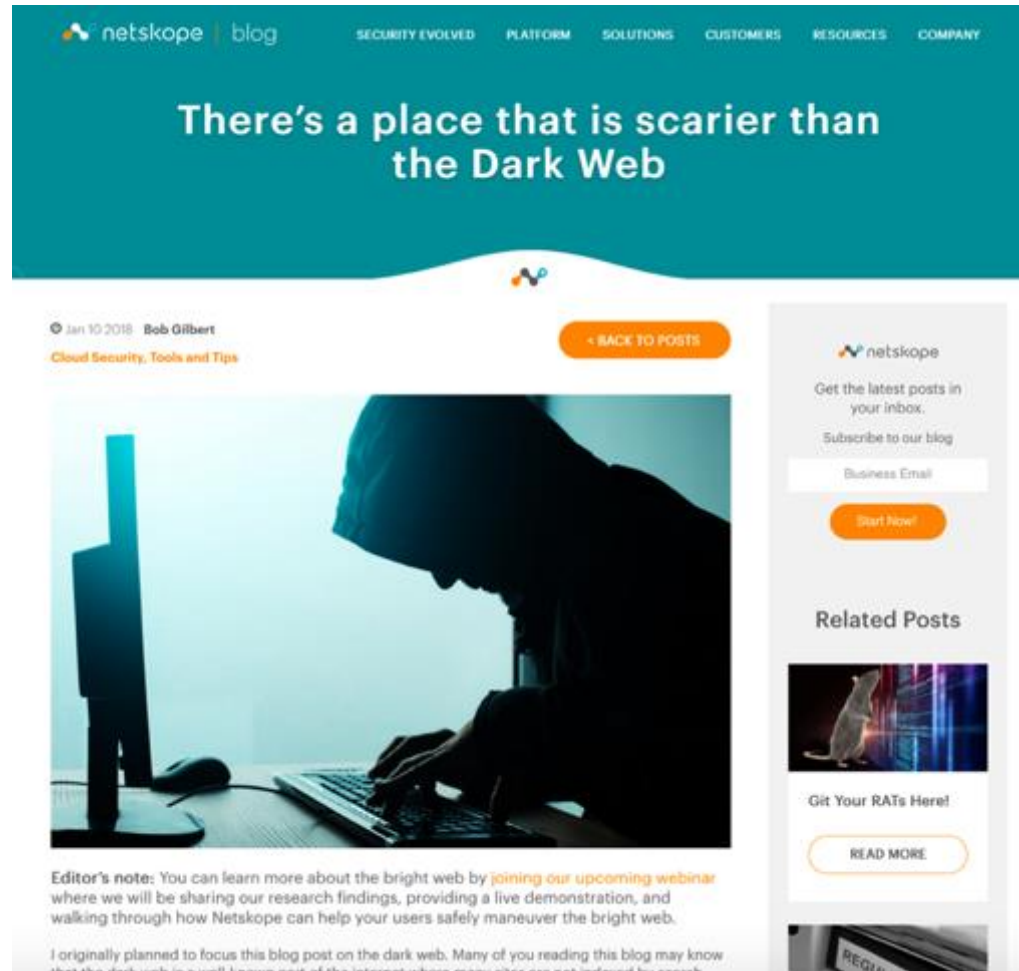


Keeping your cloud secure

(and a tour of the latest cyber threats)

Ross Asquith – ross@netskope.com

Why worry about data being stolen when your employees are giving it away?!



The screenshot shows a Netskope blog post. The header is teal with the Netskope logo and navigation links: SECURITY EVOLVED, PLATFORM, SOLUTIONS, CUSTOMERS, RESOURCES, COMPANY. The main title is "There's a place that is scarier than the Dark Web". Below the title is a date "Jan 10 2018" and author "Bob Gilbert". A category tag "Cloud Security, Tools and Tips" is visible. A "BACK TO POSTS" button is in the top right. The main image shows a person in a hoodie typing on a laptop in a dimly lit room. Below the image is an "Editor's note" and a "READ MORE" button. On the right side, there is a subscription form for "Business Email" with a "Start here!" button, and a "Related Posts" section with a thumbnail for "Get Your RATs Here!" and a "READ MORE" button.


netskope | blog SECURITY EVOLVED PLATFORM SOLUTIONS CUSTOMERS RESOURCES COMPANY

There's a place that is scarier than the Dark Web

Jan 10 2018 Bob Gilbert

Cloud Security, Tools and Tips

BACK TO POSTS



Editor's note: You can learn more about the bright web by [joining our upcoming webinar](#) where we will be sharing our research findings, providing a live demonstration, and walking through how Netskope can help your users safely maneuver the bright web.

[READ MORE](#)

Get the latest posts in your inbox.
Subscribe to our blog

Business Email

[Start here!](#)

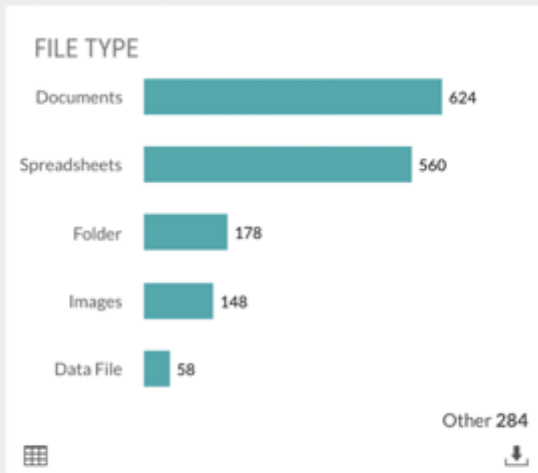
Related Posts

[Get Your RATs Here!](#)

[READ MORE](#)

🔍 [Search] [Dropdown]

Schedule PDF



TOTAL FILES: 978

File Name	File Owner (User)	File Size	File Type	Policy Hit	Exposure
Madness-ALN-AS-002-Desktop-Work-Instructions_draft		462 KB	Documents		

Cyber Crime is Big Business!

- A flourishing economy generating over \$1.5 trillion in revenues every year.
- Increasing commoditization of malware: minimum effort and technical skills required.
- Growing adoption of cloud services brings new methods of attack
- Destruction of your data is a feature of recent attacks



Ransomware: King of 2017

- In 2016 revenues rose to \$1 Billion
- In 2017 ransomware attack volumes grew by 2,500%
- SMB and consumers preferred targets (poorly protected)



WannaCry - May 2017

- Estimates suggest WannaCry affected around 300,000 organisations worldwide
- Encrypted user's files and demanded \$300 worth of Bitcoins



The screenshot shows a BBC News article from October 12, 2018. The article title is "WannaCry Ransomware Cost The NHS £92m". The author is Holly Brockwell. The article text states that the ransomware cost the NHS close to £100m and that it ripped through vital computer systems. It also mentions that according to Techradar, the Department of Health and Social Care has revealed that the attack cost the region of £92,000,000. A bulleted list breaks down the costs: £500k on IT support during the attack, £72m on IT support in the months following, and £19m from not having access to patient information in the week after the attack.

WannaCry Ransomware Cost The NHS £92m

By Holly Brockwell on 12 Oct 2018 at 4:00PM

The ransomware nightmare that was [WannaCry](#) cost the NHS close to £100m when it ripped through vital computer systems like a digital plague last year.

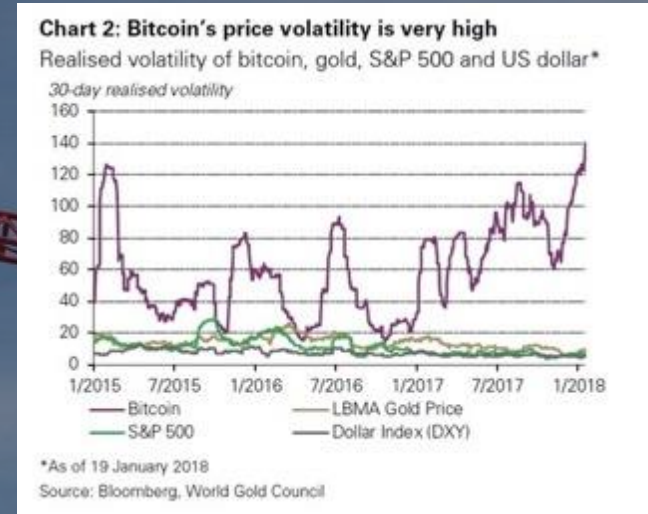
According to [Techradar](#), the Department of Health and Social Care has revealed that the attack cost in the region of £92,000,000. Here's how that breaks down:

- £500k on IT support during the attack
- £72m on IT support in the months following
- £19m from not having access to patient information in the week after the attack

- WannaCry is one of the fastest spreading ransomware strains ever
- Within four days of its discovery, Avast had detected 250,000 instances across 116 countries
- The malware was still active a year later

But the ransomware business model is facing some challenges...

- Value of Cryptocurrencies is a rollercoaster
- A problem for a business model that relies on carefully selected price points for ransoms



- New attack vectors were needed that provided a better payout...

Move over ransomware... There's a new kid on the block

Cryptojacking

- “Whatever you are... Wherever you are... You can mine...”
- Does not require high technical skills
- Unlike ransomware, it offers a potential 100% pay-out ratio

Cyber crime has a new business model – a **subscription-based revenue...**

13,769 views | Aug 3, 2018, 02:00pm

200,000 Routers Turned Into Mindless Crypto Coin Mining Zombies

**Lee Mathews** Contributor

Security

Observing, pondering, and writing about tech. Generally in that order.

Somewhere out there a cybercriminal is lining his or her pockets with cryptocurrency. Whoever it is isn't using powerful computers to do the mining. Instead, this individual is using an ever-growing army of enslaved routers to do the dirty work.

CoinHive is generating **\$250,000** worth of Monero **every month**



Security

Not even ordering pizza is safe from the browser crypto-mining scourge

Coin Hive JavaScript increasingly pops up in top 3 million websites

By John Leyden 9 Nov 2017 at 12:33

23 SHARE

Elsewhere Netskope discovered a Coin Hive miner installed as a plugin on a tutorial webpage for Microsoft Office 365 OneDrive for Business.

The offending website – [https://www.sky-future\[.\]net](https://www.sky-future[.]net) – removed the Coin Hive plugin after it was notified about the issue. "The tutorial webpage hosted on the website was saved to the cloud and then shared within an organisation," according to Netskope.



Software as a Service
SaaS



Infrastructure as a Service
IaaS



\$1.70 per hour = \$1,124 per month

.000017 BTC per month

\$0.10 per month

Browser address bar: <https://hackernoon.com/eth>

HACKERNOON Sign in Get started

HOME READ LATEST BLOCKCHAIN DEV AI CRYPTO STARTUP ECONOMICS HACKER JOBS

Ethereum mining on AWS in 5mins



SC MEDIA NEWS **SC US** SC UK **CYBERCRIME** NETWORK SECURITY PRODUCT REVIEWS IN DEPTH EVENTS WHITEPAPERS

THE CYBERSECURITY SOURCE

February 20, 2018

Tesla's AWS servers hijacked by cryptominers

f t in G+ r

The hijacking of Tesla's Amazon Web Server cloud system by rogue cryptominers is proof that no one is immune to a misconfigured AWS server nor cryptomining attacks.



misconfigured s3

Web Images Videos **News**



Italy Safe Search: Moderate Any Time

AWS Employee Flub Exposes S3 Bucket Containing GoDaddy Server ...
 According to one study earlier this year by Digital Shadows, researchers estimated that 1.5 billion sensitive files were visible on the internet from **misconfigured S3 buckets**, NAS devices, FTP servers, and other cloud storage systems. Configuration ...
 Dark Reading | 8 hours ago

GoDaddy data exposed by AWS employee misconfiguring cloud instan...
 Data exposures caused by **misconfigured Amazon Web Services Inc. cloud storage** ... first uncovered by security firm UpGuard Inc., involved GoDaddy data found to be residing on an Amazon **S3 bucket open to the public**. The data included high-level ...
 SiliconANGLE | 6 hours ago

Web doc iCliniq plugs leaky S3 bucket stuffed full of medical records
 However, iCliniq stored these private medical documents in a **misconfigured wide-open AWS S3 bucket** that could have been potentially pored over by anyone. This cloud storage box, according to Gilwka, contained about 20,000 medical documents, such as ...
 The Register | 7 days ago

Millions of U.S. Voter Records Exposed on Robocall Company RoboCent's Poorly Configured AWS Cloud Storage
 They were grouped into two buckets on Amazon Simple Storage Service (**S3**), one of the products available through AWS. **Misconfigured cloud storage** has led to the exposure of a staggering number of sensitive records in recent years. One report found that ...
 IEEE Spectrum | 5 days ago

Informa**tor**lik
IT NETWORK


Darkreading Network Computing

About Us **Advertise** Register Login to your account Welcome Guest

DARKReading

Search Dark Reading

Authors Slideshows Video Tech Library University Radio Calendar Black Hat News

Follow DR: 

ANALYTICS **ATTACKS / BREACHES** **APP SEC** **CAREERS & PEOPLE** **CLOUD** **ENDPOINT** **IoT** **MOBILE** **OPERATIONS** **PERIMETER** **RISK** **THREAT INTELLIGENCE** **VULNS / THREATS**

Time Warner Cable

Kromtech Security Center found **two AWS S3 buckets exposed on the Internet** [...] included internal development information like SQL database dumps, code with access credentials, and access logs. One text file contained more than **four million records with information like user names, Mac accesses, serial numbers, account numbers**, and transaction IDs.

Accenture

The Cyber Risk Team at UpGuard recently discovered that Accenture left **at least four AWS S3 storage buckets unsecured and publicly available for download**. Accenture's slip-up exposed **authentication credentials, secret API data, digital certificates, decryption keys, customer information**, and other data that could be leveraged to target both Accenture and its clients.

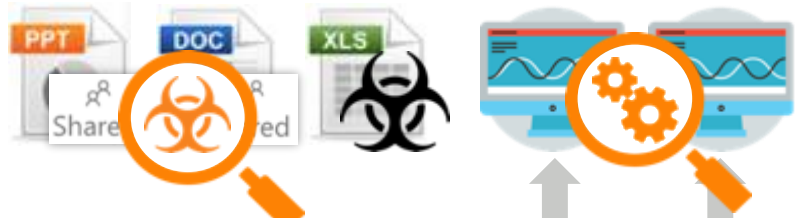
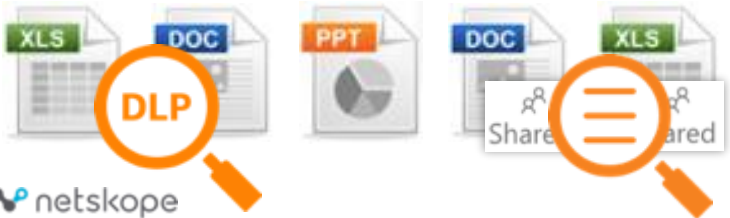
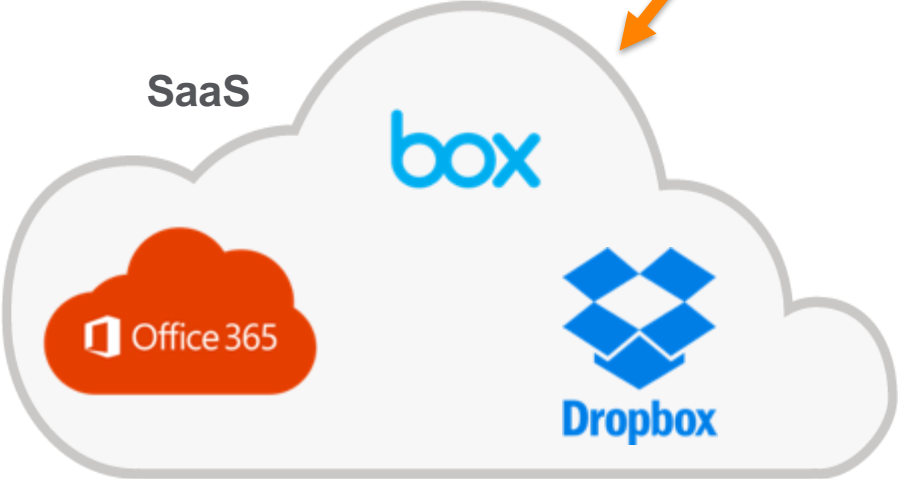
<https://www.darkreading.com/cloud/10->

KICKING THE BUCKET —

Researcher discovers classified Army intel app, data on open public AWS bucket

Failed intelligence system, with data labeled "Top Secret," left open by contractor.

SEAN GALLAGHER - 11/28/2017, 7:02 PM







Thank you

Ross Asquith – ross@netskope.com