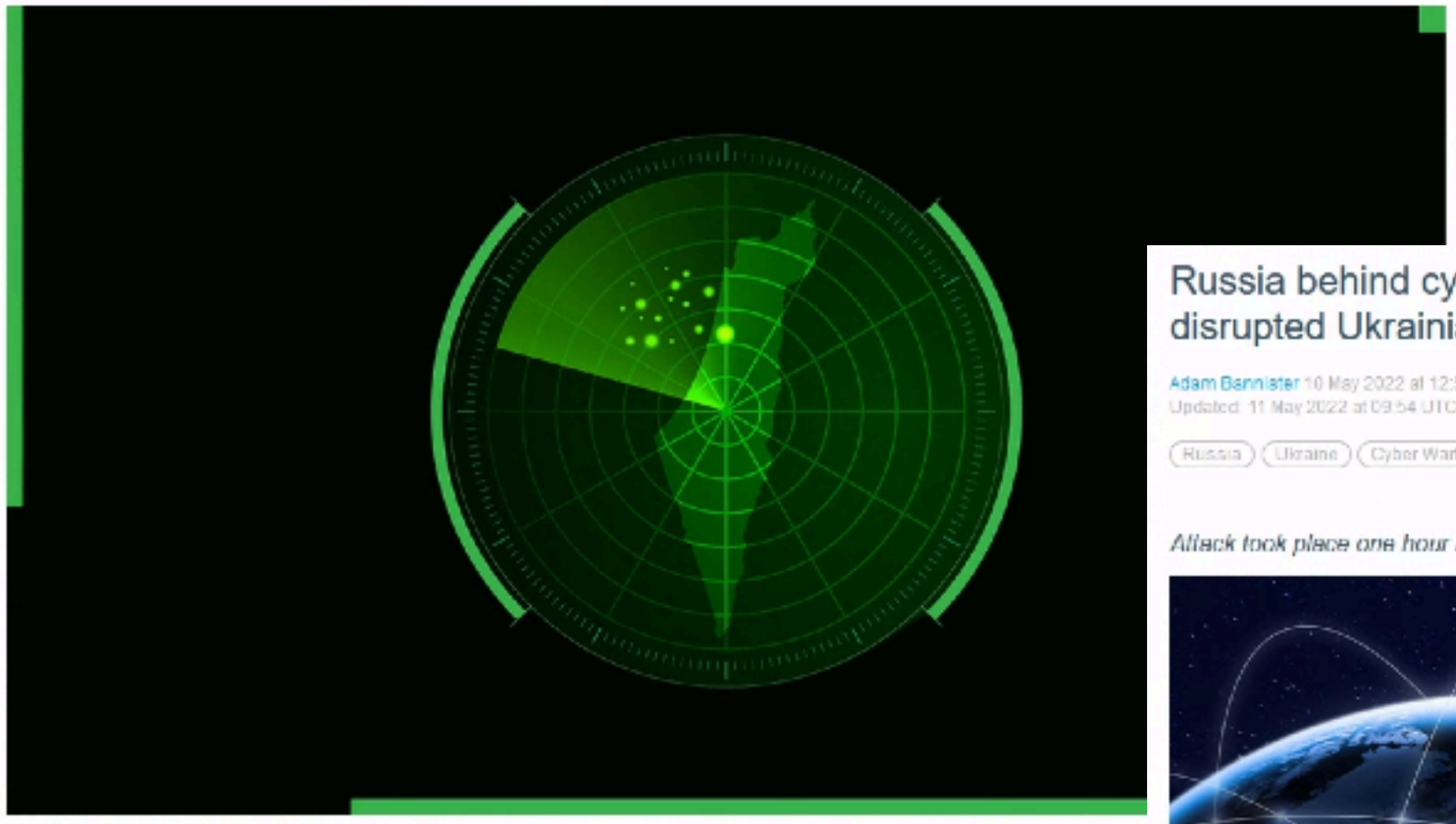
Israeli government websites temporarily knocked offline by 'massive' cyber-attack

Jessica Haworth 15 March 2022 at 11:55 UTC

Israel | DDoS | Cyber-attacks

DDoS assault blamed on Iran, local media reports



A "massive" cyber-attack knocked several Israeli government websites offline last night (March 14).

The incident was confirmed online by the Israel National Cyber Directorate, which said that a DDoS services "for a short time".

The Daily Swig

March 2022

Russia behind cyber-attack on satellite internet network KA-SAT that disrupted Ukrainian infrastructure – EU

Adam Bannister 10 May 2022 at 12:52 UTC
Updated 11 May 2022 at 09:54 UTC

Russia | Ukraine | Cyber Warfare

Attack took place one hour before Russia invaded Ukraine

UPDATED The EU has blamed Russia for a powerful cyber-attack that disrupted satellite broadband services in Ukraine and "helped facilitate President Vladimir Putin's invasion of the country".

Thousands of modems were knocked offline by the attack on the KA-SAT network, which took place one hour before Russia's invasion of Ukraine commenced on February 24.

The incident caused communication outages and other disruptions for government websites and banks in Ukraine, and affected several EU Member States that also use the KA SAT network.

The Daily Swig

May 2022

Hundreds of companies potentially hit by Okta hack

23 March

Hundreds of organisations that rely on Okta to provide access to their networks may have been affected by a cyber-attack on the company.

Okta said the "worst case" was 366 of its clients had been affected and their "data may have been viewed or acted upon" - its shares fell 9% on the news.

It says it has more than 15,000 clients - from big companies, including FedEx, to smaller organisations, such as Thanet District Council, in Kent.

Cyber-gang Lapsus$ is behind the hack.

BBC

March 2022

MSRC

March 2022

March 22, 2022 • 17 min read

DEV-0537 criminal actor targeting organizations for data exfiltration and destruction

Microsoft Threat Intelligence Center (MSTIC)

Detection and Response Team (DART)

Microsoft Defender Threat Intelligence

Share

March 24, 2022 update *– As Microsoft continues to track DEV-0537's activities, tactics, and tools, we're sharing new detection, hunting, and mitigation information to give you additional insights on remaining vigilant against these attacks.*

In recent weeks, Microsoft Security teams have been actively tracking a large-scale social engineering and extortion campaign against multiple organizations with some seeing evidence of destructive elements. As this campaign has accelerated, our teams have been focused on detection, customer notifications, threat intelligence briefings, and sharing with our industry collaboration partners to understand the actor's tactics and targets. Over time, we have improved