

in f
co dEn
m/c try-
om Sec
pan urit
y/re y-
den 103
try) 663
208
083
942)

(/en/)

Book a Consult
(<https://redentry.co/en/contact-our-team/>)



Hebrew (<https://redentry.co/blog/anonymous>)

Anonymous Cyber Attack History

Get a Quote



[Main \(https://redentry.co/en/\)](https://redentry.co/en/) » [Cyber Security \(https://redentry.co/en/cyber-security/\)](https://redentry.co/en/cyber-security/) » Anonymous Cyber Attack History

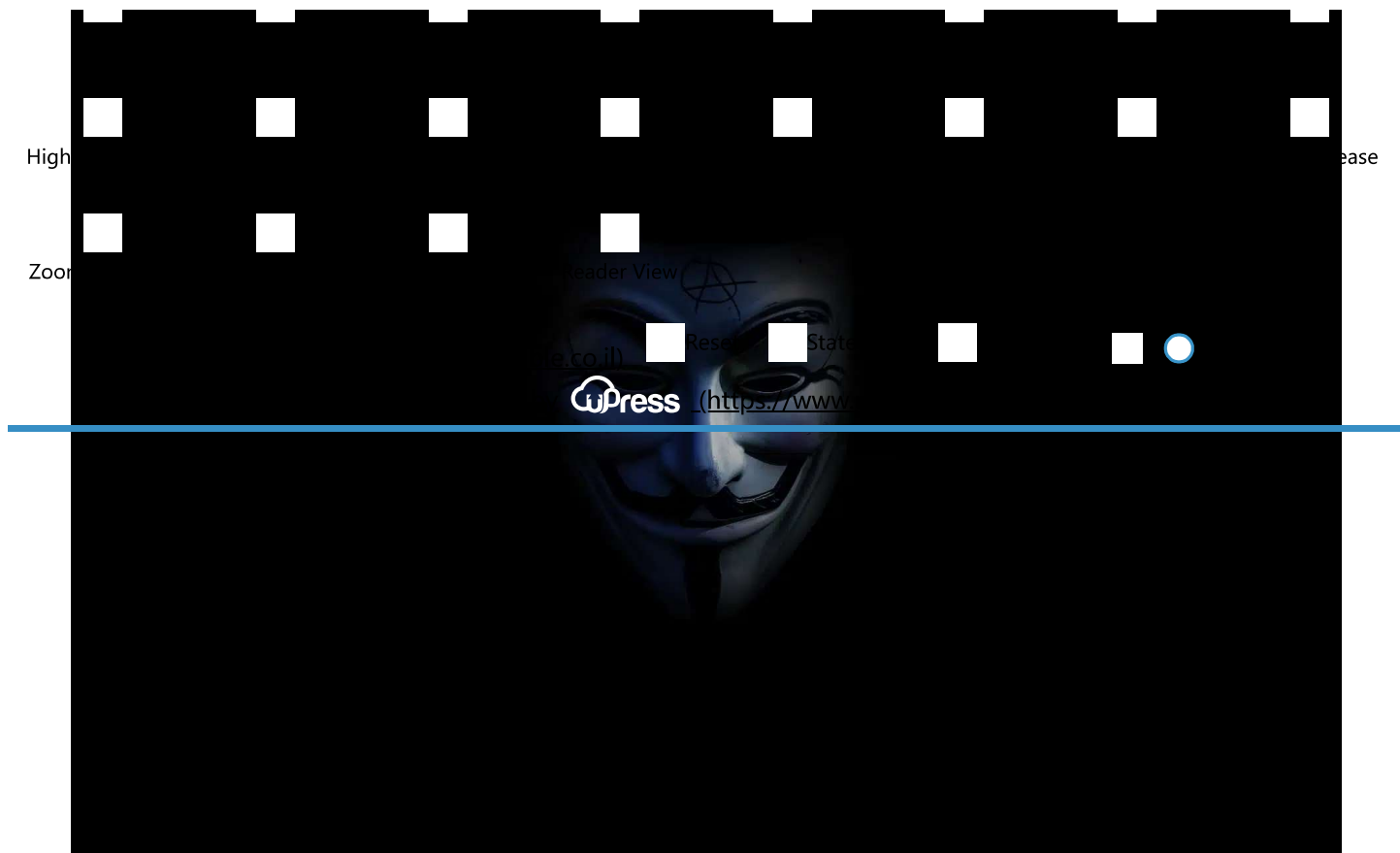
📅 10/12/2022 👤 Tal Yahel ≡ Cyber Security ⌚ Reading Time: 5 minutes

Anonymous Group Attacks

The notorious hacker group Anonymous has been operating in the shadows of the cyber world for two decades, wreaking havoc and making global headlines by hacking into the biggest companies and the most powerful governments. Let's dive deep into the world of Anonymous, and read about the fascinating history of the hacker group



that will be remembered for generations.



(<https://redentry.co/wp-content/uploads/2022/10/אנונימוס.jpg>)

The Birth Of Anonymous

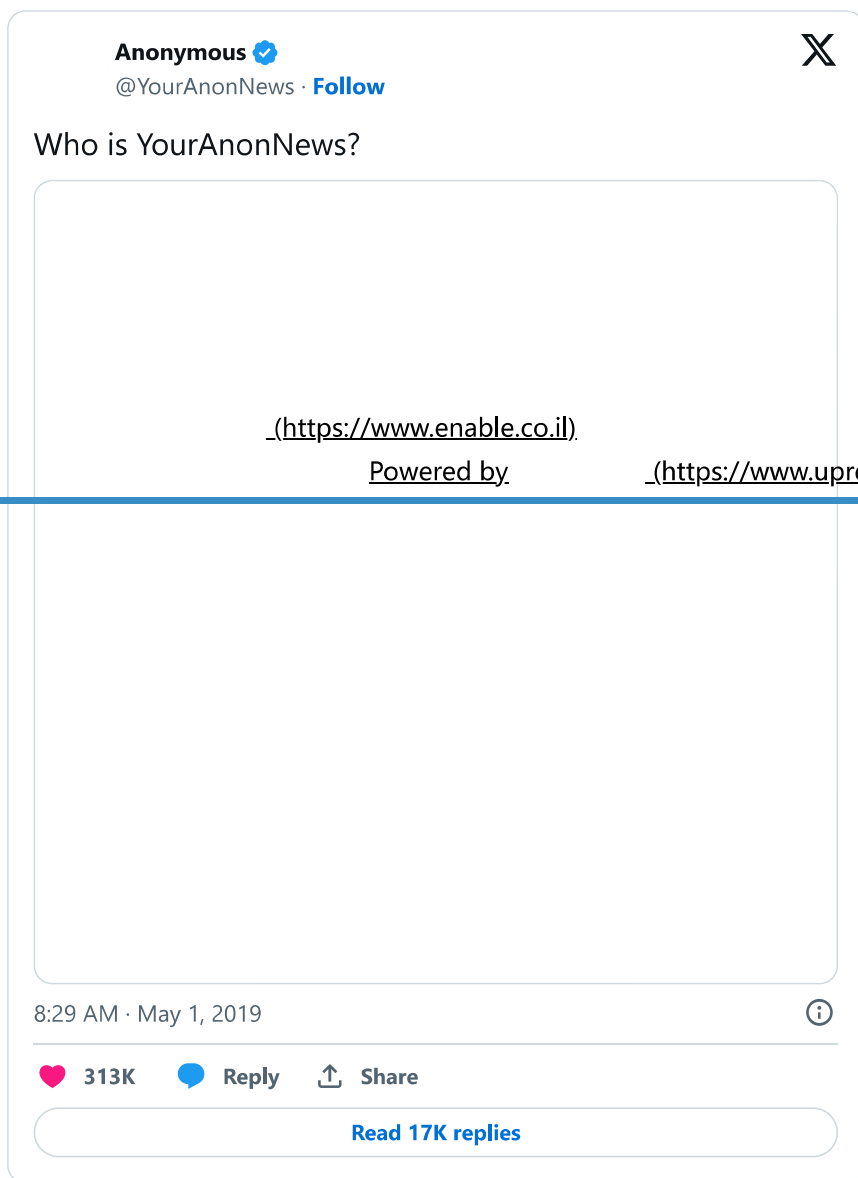
Anonymous first appeared in 2004, on the 4chan message forum that had been created a year earlier. In the early days of the forum, many users would flood game chat rooms and other forums with what they called "Raids". The traffic overload caused these chat rooms to shut down.

This created the basis for what we know today as Anonymous- a movement of individuals gathering through secure chat rooms to plan and execute disruptive cyberattacks. At first, done as pranks for amusement, soon the group began to carry out ideology-driven attacks.

Anonymous Ideology & Philosophy

The main philosophy of the hacker group Anonymous is opposition to governments and private organizations that work to promote inequality and censorship, according to the view of the group's members. However, it is important to remember that because the group is decentralized and does not have a single leadership, there are no clear guidelines, and among the group members there are many debates on which causes to support.

In a post published on Twitter in 2019, a member of the Anonymous group, who emphasized that he does not speak for the entire group, claimed that Anonymous is made up of working-class people who seek to create a better world for all of humanity and that its main principles are freedom of information, freedom of expression, privacy for citizens and holding companies and governments accountable for their actions.



Anonymous Famous Cyber Attacks

Although the group has carried out countless small and medium-sized cyber attacks, some of which are probably unknown to the world, we have collected a respectable list of the famous attacks that made them a household name in the world of hacktivism:

2008 – Attack on the Church of Scientology – Operation Chanology is the name given to a series of attacks on the famous church in January 2008. These attacks included disabling the church's websites using DDOS (<https://redentry.co/en/blog/what-is-ddos-attack/>), prank calls, and black faxes designed to use all the church's ink. Although it might sound unimpressive and even a bit low-tech in 2022, in 2008 fax was still one of the main means of communication, and the attack cost the church not only its reputation but also a considerable financial cost.

The Anonymous group posted a video on YouTube that takes responsibility for the attack, explaining that these attacks were done so that the church would stop the financial exploitation of its believers.

Anonymous called on people to protest against the church, and in February thousands of people gathered in various centers in demonstrations against the church, some wearing mask for the movie "V for Vendetta" to protect their identity.

[_ \(https://www.enable.co.il\)](https://www.enable.co.il)

Powered by

[_ \(https://www.upress.co.il\)](https://www.upress.co.il)

2009- Protest against the falsification of the elections in Iran. In June 2009, presidential elections took place in Iran, in which, not surprisingly, Mahmoud Ahmadinejad won. Allegations of fraud in the elections led the Anonymous group along with The Pirate Bay to create an opposition website to the Iranian regime that attracted tens of thousands of visitors and allowed the free transfer of information in the censored country.

2010- Operations Payback- The giant conglomerate Sony caught the attention of Anonymous after it became known that Sony is suing individuals who created software that allows users to run PlayStation 3 on Linux. Anonymous responded by shutting down Sony's website, harassing employees, and creating disruptions in the corporate network.

2010 – Support for the WIKILEAKS site – In February 2010, the site used by whistleblowers to publish classified and stolen documents was under pressure from many parties to stop its operations.

Anonymous announced their full support for WIKILEAKS and began DDOS attacks on Mastercard, Visa, PayPal, Amazon, and SWISS Bank in response to actions seen as anti-WIKILEAKS, such as stopping the possibility of donating to the site.

After the founder of the site was arrested in London, Anonymous disabled the website of the Swiss Ministry of Justice because they demanded that England hand over the detainee. The website of the Zimbabwean government was also taken down by hackers because they censored the site.



(<https://redentry.co/wp-content/uploads/2022/10/Julian-assang-wikileaks-min.jpg>)

2011- The Arab Spring. Many countries that took part in the Arab Spring became a target in the hands of the hacker group that supported the protesters, including countries such as Tunisia, Egypt, Bahrain, Libya, Jordan, and Morocco.

2011- In June, Anonymous attacked over 90 Indonesian government websites in response to the blocking of WikiLeaks and The Pirate Bay.

2011 – Anonymous announced that in response to the Stuxnet virus created by the United States and Israel designed to target the Iranian nuclear program, Anonymous would attack the Knesset website and disable it.

ESC



2012 – Megaupload website that provided file-sharing services were shut down by the United States Department of Justice and the FBI, which led to an attack by Anonymous on the US government, taking down the Department of Justice website.

The attack included, among other things, the use of new and sophisticated attack methods, in which various Internet users who clicked on links in chat rooms and on Twitter actually participated, even without their knowledge, in denial of service attacks.

2013 – Opisrael (<https://redentry.co/en/blog/opisrael-attacks/>)– Planned for Holocaust memorial Day – April 7, 2013. The website of the “Bigger Than Life” organization, which accompanies families whose children are diagnosed with cancer, was attacked and its home page was vandalized with antisemitic and anti-Israel messages. Other sites such as Yad Vashem, the Ministry of Defense, the Election Commission, and the Ministry of Foreign Affairs were shut down for several hours. [_ \(https://www.enable.co.il\)](https://www.enable.co.il)

Powered by [_ \(https://www.upress.co.il\)](https://www.upress.co.il)

The attack was also accompanied by false reports published by the hackers, including damages worth \$5 billion allegedly caused.

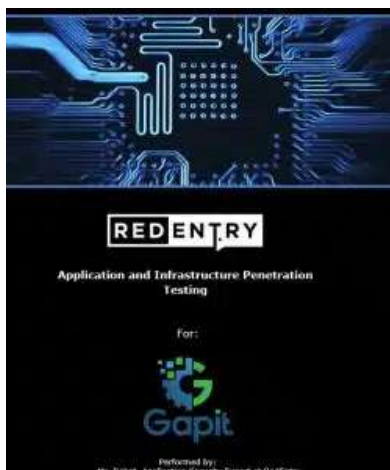
2014- Support for Hong Kong’s independence- Following the riots in Hong Kong, the people’s demand for independence, and the violent response of the Chinese government to suppress the riots, Anonymous declared support for the protesters and began attacks on private companies in Hong Kong that support the Chinese regime.

2015- Anonymous declared that it is against the terrorist organization ISIS after the terrorist attack in Paris

2022- Anonymous made headlines for a string of successful attacks against Russia as part of its support for Ukraine, leaking documents and information about senior military personnel. Blocking websites of individual organizations

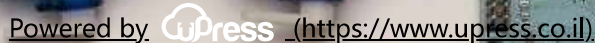
Those who continue to do business with Russia, shutting down government websites of Russia and Belarus, bypassing censorship in Russia and publishing photos from the war, and training other activists who will fight for Ukraine.

View Free Pen Test Report



Download Report

.....



IoT, or Internet of Things refers to a network of interconnected devices that may range from laptops, smartphones, wearables, sensors and more.



Cyber Security For E-Commerce Sites (<https://redentry.co/en/blog/cyber-security-for-e-commerce-sites/>)

The rise of e-commerce sites has revolutionized the way people shop. However e-commerce sites are a prime target for hackers.

_(<https://www.enable.co.il>)

Powered by

_(<https://www.upress.co.il>)

(<https://redentry.co/en/blog/cyber-security-in-saas-industry/>)

Cyber Security for SaaS (<https://redentry.co/en/blog/cyber-security-in-saas-industry/>)

Companies that provide software as a service (SaaS) face cyber threats that are unique to them. Protecting these softwares is critical



(<https://redentry.co/en/blog/cyber-threats-on-supply-chain-industry/>)

Cyber Threats On Supply Chain Industry (<https://redentry.co/en/blog/cyber-threats-on-supply-chain-industry/>)

The supply chain industry is an integral part of the global economy, responsible for moving goods and products from manufacturers to retailers and ultimately, to end consumers. However, this

Start Your Path Towards a
Safer Cyber-World

Join Us
(<https://redentry.co/en/contact-our-team/>)

Get a Customized Price Quote

Powered by [_ \(https://www.upress.co.il\)](https://www.upress.co.il)

Our questionnaire is designed to provide us with the necessary information to produce a customized price quote, tailor-made to your needs.

If you wish to save time by filling the questionnaire, click the "Scope my project" button.

Otherwise, you are welcome to contact us at +972-79-639-9021 (tel:+972796399021) or leave your details and one of our cyber experts will get in touch with you as soon as possible.

Name *

Email *

Company *

Phone

Yes, contact me

or

Scope my project
(<https://redentry.co/en/scope-my-cybersecurity-project/>)

Resources

About(<https://redentry.co/en/about/>)
Blog(<https://redentry.co/en/cyber-security-blog/>)
Contact Us (<https://redentry.co/en/contact-our-team/>)
Customer Support (<https://redentry.co/en/customer-support-en/>)

Penetration Testing (<https://redentry.co/en/pen-testing/>)
Web PT (<https://redentry.co/en/web-application-pen-PT-testing/>)
Network PT(<https://redentry.co/en/network-pen-testing/>)
Mobile PT (<https://redentry.co/en/mobile-penetration-PT-testing/>)
Phishing test(<https://redentry.co/en/phishing-test/>)

Cyber Security Services (<https://redentry.co/en/cybersecurity-services/>)
Powered by (<https://www.enable.co.il>)

Managed Security Services (<https://redentry.co/en/managed-security-service/>)
Powered by (<https://www.upress.co.il>)

CISO as a Service (<https://redentry.co/en/ciso-as-a-service/>)
System Intergration (<https://redentry.co/en/security-system-integration/>)
Security Architecture (<https://redentry.co/en/security-architecture/>)
Cloud Security (<https://redentry.co/en/cloud-security-services/>)
Cyber Compliance (<https://redentry.co/en/cybersecurity-compliance/>)
Risk Managment (<https://redentry.co/en/cybersecurity-risk-management/>)

Managed EDR Service (<https://redentry.co/en/managed-edr-services/>)
Managed SIEM Service (<https://redentry.co/en/managed-siem/>)

Join Our Newsletter

Sign me up!

Privacy Policy (<https://redentry.co/en/en-privacy-policy/>)

All Rights Reserved to Redentry

(<https://www.facebook.com/Redentry>)
(<https://www.linkedin.com/company/redentry>)
(<https://www.instagram.com/redentry>)
(<https://www.youtube.com/channel/UC63208083942>)

