

[Cybersecurity 101: The Fundamentals of Cybersecurity](#) > [Cyber Threat Intelligence Explained](#) > **Hacktivism: Types and Examples**

HACKTIVISM: TYPES AND EXAMPLES

Bart Lenaerts-Bergmans - July 07, 2022

I What is Hacktivism?

Hacktivism is a combination of the words “hack” and “activism.” Hacktivists engage in disruptive or damaging activity on behalf of a cause, be it political, social or religious in nature. These individuals or groups often see themselves as “virtual vigilantes,” working to expose fraud, wrongdoing or corporate greed, draw attention to human rights violations, protest censorship or highlight other social injustices.

Hacktivism attacks have increased exponentially in recent years. The rise in this activity is due in part to our collective reliance on the internet, social media and other forms of digital communication, as well as an emotionally-charged global political landscape.

Though many hacktivists claim to have noble intentions and often work in pursuit of equality, justice or improved human rights, it is important to remember that hacktivism falls into the category of cybercrime. It is illegal regardless of the hacker’s motivations or the attack’s outcomes.

I Who Do Hacktivists Target?

Hactivists target entities that they believe violate their values or stand in the way of their agenda. Common targets may include:

- Nation states
- Government agencies
- Corporations
- Religious institutions
- Terrorist organizations

I Common Forms Of Hacktivism

Hactivists rely on a variety of both legal and illegal activities to carry out their agenda. Common techniques include:

Denial of Service (DoS) Attacks:

Malicious, targeted attacks that flood a network with false requests in order to disrupt business operations. In a **DoS attack**, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are

Hacktivists rely on a variety of both legal and illegal activities to carry out their agenda. Common techniques include:

Denial of Service (DoS) Attacks:

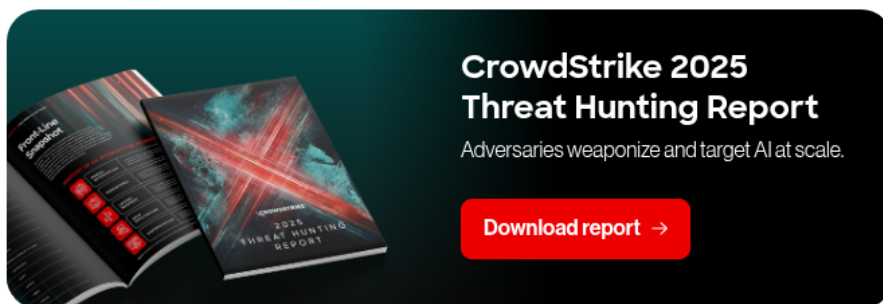
Malicious, targeted attacks that flood a network with false requests in order to disrupt business operations. In a **DoS attack**, users are unable to perform routine and necessary tasks, such as accessing email, websites, online accounts or other resources that are operated by a compromised computer or network. While most DoS attacks do not result in lost data and are typically resolved without paying a ransom, they cost the organization time, money and other resources in order to restore critical business operations.

Doxing:

Exposing personal identifiable information, or incriminating evidence, usually with the intention of having others use that information to harass, intimidate or scare the subject.

Data theft:

Stealing data, intellectual property (IP) or other proprietary information, typically with the intention of carrying out a **ransomware attack** or selling the data on the **dark web**.



I Examples of Hacktivism

Anonymous

One of the most famous hacktivist groups is Anonymous, or Anon. Formed in 2008, Anonymous rose to fame for their attacks on the Church of Scientology, which first involved leaking private video footage of celebrity members and later involved a **DDoS attack** on the organization's website.

In recent years, the Anonymous hacking group has claimed responsibility for some of the largest hacktivist attacks, including those on a number of prominent corporations and government agencies. Perhaps their most infamous hacktivist campaign is "Operation Tunisia", which targeted several government websites in support of the Arab Spring movement in 2010.

LulzSec

Another well-known hacktivist organization is LulzSec, which was formed by members of Anonymous.

Similar to Anonymous, LulzSec has successfully hacked a number of corporations and police servers, leaking data or defacing the site. Some of LulzSec's most ambitious targets are Fox.com, Sony and the CIA.

Wikileaks

Wikileaks is a political whistleblower site known for leaking classified information or other sensitive data. Wikileaks also waged DDoS attacks against Amazon, PayPal, Visa and Mastercard as a form of retaliation against those organizations for preventing the release of leaked information.

Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).



similar to a proxy mode, LulzSec has successfully hacked a number of corporations and police servers for the purpose of stealing data or defacing the site. Some of LulzSec's most ambitious targets are Fox.com, Sony and the CIA.

Wikileaks

Wikileaks is a political whistleblower site known for leaking classified information or other sensitive data. Wikileaks also waged DDoS attacks against Amazon, PayPal, Visa and Mastercard as a form of retaliation against those organizations for preventing supporters from donating to their cause. The attacks reportedly led to significant corporate losses due to disruption of web services.

I How to Prevent Hactivist Attacks

Given the unique nature of hactivist attacks, it is important to develop an incident response plan that specifically outlines the process the organization will take to minimize the damage of a hactivist attack and remediate it as quickly as possible. As part of that plan, organizations should keep in mind that many hactivists will announce their intention to carry out an attack in advance of such activity. As such, the organization should develop a comprehensive strategy that accounts for the threat of an attack as well as the attack itself.

In terms of prevention, inoculating the organization from hactivist attacks relies on many of the cybersecurity best practices we recommend for protecting against **malware**, ransomware and other cybersecurity threats. Our recommendations include:

1. Train all employees on cybersecurity best practices

Employees are on the front line of your security. Make sure they follow good hygiene practices — such as using strong password protection, connecting only to secure Wi-Fi and being on constant lookout for phishing — on all of their devices. This will make it more difficult for a hactivist to penetrate the network or computer system and carry out an attack.

2. Keep the operating system and other software patched and up to date

Hackers are constantly looking for holes and backdoors to exploit. By vigilantly updating your systems, you'll minimize your exposure to known vulnerabilities.

3. Use software that can prevent unknown threats

While traditional antivirus solutions may prevent known ransomware, they fail at detecting unknown malware threats and other obscure tools used by hactivists. The CrowdStrike Falcon® platform provides next-gen antivirus (NGAV) against known and unknown malware using AI-powered machine learning. Behavior-based **indicators of attack** (IOAs) are leveraged to prevent sophisticated fileless and malware-free attacks like ransomware. Rather than attempting to detect known malware iterations, Falcon looks for indicators of attack (IOAs) to stop ransomware before it can execute and inflict **damage**.

4. Continuously monitor the environment for malicious activity and IOAs

CrowdStrike® **Falcon Insight™** endpoint detection and response (EDR) acts like a surveillance camera, capturing raw events for automatic detection of malicious activity not identified by prevention measures. Falcon Insight is designed for **proactive threat hunting**.

Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).

For stealthy, hidden attacks that may not immediately trigger automated alerts, CrowdStrike offers **Falcon OverWatch™** managed threat hunting, which comprises an elite team of experienced hunters who proactively search for threats on your behalf 24/7.





Bart is Senior Product Marketing Manager of Threat Intelligence at CrowdStrike and holds +20 years of experience in threat monitoring, detection and intelligence. After starting his career as a network security operations analyst at a Belgian financial organization, Bart moved to the US East Coast to join multiple cybersecurity companies including 3Com/Tippingpoint, RSA Security, Symantec, McAfee, Venafi and FireEye-Mandiant, holding both product management, as well as product marketing roles.

Featured Articles

Backporting

Brute Force Attacks

Denial-of-Service (DoS) Attacks

Try CrowdStrike free for 15 days

[Start free trial →](#)[Contact us →](#)[View pricing >](#)

Welcome to CrowdStrike

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting





Backporting



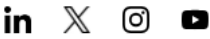
Brute Force Attacks



Denial-of-Service
(DoS) Attacks

Try CrowdStrike free for 15 days

- Start free trial →
- Contact us →
- View pricing >



Get Started	Company	Partners	Existing Customers	Support
Pricing Sale	About Us	Partner Programs	Support Portal	Call 1-888-512-8906 (US)
Free Trial Guide	Executive Leadership	Service Providers	Developer Portal	Experienced a Breach?
Falcon Flex	Board of Directors	Strategic Technology		Contact Us
Financing	Newsroom	Channel & Distributors		Schedule a Meeting
CrowdStrike Marketplace	Investor Relations	Become a Partner		FAQs
Cyber Monday Deals	CrowdStrike Racing & F1			
	Sustainability			

Welcome to CrowdStrike 

What are you looking for today?

CrowdStrike and our third-party vendors may monitor, record and access chats to respond to you, and for quality, training, improvement and other purposes. More info: [Privacy Notice](#).