

Hacktivism, explained

These freelancer groups are more than just people in black hoodies looking for a quick laugh

BACKGROUND

Cisco Talos defines hacktivism as, “cyber operations performed in order to call the public's attention to a political, religious, social, environmental or other ideological cause.” These types of groups, widely stereotyped to operate like the “Anonymous” hacking group, differ from APTs, as they operate independently from and do not have a stated affiliation with a government entity. These groups also differ from most criminal cyber actors as they are not primarily motivated by monetary gain.

TACTICS

- Hacktivist groups typically use several unsophisticated attack methods to achieve their goals, such as disrupting access to targets’ online assets through distributed denial-of-service (DDoS) attacks, defacing their websites, exfiltrating and publicly releasing sensitive or confidential data from targets’ networks, and exposing targets’ personal information.
- Hacktivist groups are also responsible, to a lesser extent, for sophisticated attacks that penetrate or disrupt the networks of government and critical infrastructure entities.
- Recently, some hacktivist groups have begun pursuing methods to monetize their operations through offering services such as DDoS-for-hire and integrating extortion tactics into their efforts to increase pressure on a targeted organization.

OUTLOOK

- We have observed an increasing number of hacktivist groups, including many that were created following Russia’s invasion of Ukraine, organize their members by modeling themselves after structured organizations with business-like tactics.
 - Some of these tactics, aimed at providing structure and maximizing efficiency, include specialized sub-

teams, formalized recruitment processes, monetary bonuses, and marketing campaigns.

- Talos assesses certain nation states may increasingly seek to co-opt or task existing hacktivist groups to perform operations on their government’s behalf.
 - Countries such as Iran and China already employ similar approaches to espionage operations, tasking non-government groups, namely technology companies, to take on these activities.

COVERAGE

- Talos conducts regular open-source research on hacktivism-related threat information that leads to protections across the [Cisco Secure product portfolio](#). This includes numerous [Snort rules](#) and [ClamAV anti-virus signatures](#).
- Ensure you have a business continuity plan in place to be prepared for any potential DDoS attacks.
 - Deploy high-performance DDoS devices external-ly to auto-mitigate DDoS attacks, such as [Cisco Secure Firewall](#), which integrates with [Radware](#) to defend against this threat.
- Use multi-factor authentication (MFA), like [Cisco Duo](#), for social media accounts to avoid potential hostile takeovers or doxing by hacktivist groups.