What is hacktivism?

Hacktivism is cyber-enabled social activism. Like traditional activism, hacktivist activities range from peaceful protest to highly damaging criminal activity.

Hacktivist attacks are highly targeted and use familiar methods including network penetration, social engineering and denial-of-service attacks.

Most hacktivists are ideologically motivated rather than profit-driven, consequently widening the threat to include organisations and systems that might not otherwise be targeted.

Whereas the definition of hacktivism includes both lawful and unlawful activity, this briefing paper focuses on the highly damaging activity, most of which is criminal.

Why is understanding hacktivism important for the information security function?

Hacktivist attacks have caused considerable damage, costing organisations over 200 million dollars in the past year alone.

These high-profile cases have shown activists what profit-driven criminals have known for some time: that technology and the Internet confer great advantage on attackers: the cost, effort and risk to the attacker are low, the reward is high, and the targets are all in one place – the Internet. As more activists see the power of online activism, the number of attacks is likely to rise, increasing the chance that your organisation will be targeted.

Hacktivists want publicity, either to advance their ideology or cause reputational damage to the target. When they expose weaknesses in systems, it can open the door for opportunistic cyber crime, or necessitate shutting down systems, resulting in lost business, reputational damage or other costs.

What can I do to reduce the risk or impact of the hacktivism threat?

First, revisit the fundamentals of information security, since the methods of attack are largely the same as those for traditional attacks.

Next, develop an understanding of the hacktivist threat and use that to engage with other functions in your organisation to assess your organisation’s risk. Determine potential flash points where your organisation could become subject to negative public opinion or protest – such as controversial policies, defective products, business ethics risks, etc.

Based on the results of that analysis, identify which systems or information might be potential targets, especially those that might otherwise not be targeted. Consider isolating potentially at-risk systems or shoring them up with load balancing or additional capacity. Update and test your incident response plan.
COMMENTARY

Ideally, organisations should plan for the capacity attackers have to attack, rather than the likelihood of attack. But this is probably not an option given budget constraints, so organisations end up prioritising and taking a calculated risk based on likelihood. Hacktivism is likely to increase as those activists who engage in illegal activity move their protests online, increasing the probability of cyber attack. This increase in the threat level should prompt organisations to re-calculate the risk.

Further reading

The following ISF briefing papers include information that is relevant to mitigating the threat of hacktivism:

- Social Engineering – A Guide to Potential Dangers
- Cyber Citizenship in an Enterprise Environment
- Profit-Driven Attacks
- Electronic Evidence

This executive summary of the full ISF briefing paper on hacktivism has been released for distribution to the public. The full briefing paper is available to ISF Members; for information on how your organisation can join the ISF, please visit www.securityforum.org or contact Steve Durbin using the details below.

About the ISF

Founded in 1989, the Information Security Forum is an independent, not-for-profit association of leading organisations from around the world. It is dedicated to investigating, clarifying and resolving key issues in information security and developing best practice methodologies, processes and solutions that meet the business needs of its Members.

ISF Members benefit from harnessing and sharing in-depth knowledge and practical experience drawn from within their organisations and developed through an extensive research and work program. The ISF provides a confidential forum and framework, which ensures that Members adopt leading-edge information security strategies and solutions. And by working together, Members avoid the major expenditure required to reach the same goals on their own.

For further information on ISF Membership contact:

Steve Durbin
UK Tel: +44 (0)20 7213 1745
US Tel: +1 (347) 767 6772
Fax: +44(0)20 7213 4813
Email: steve.durbin@securityforum.org
Web: www.securityforum.org

Disclaimer

This document has been published to provide general information only. It is not intended to provide advice of any kind. Neither the Information Security Forum nor the Information Security Forum Limited accept any responsibility for the consequences of any use you make of the information contained in this document.