An ethical hacker can help you beat a malicious one

19 May 2017, by Georg Thomas

Not all hackers can be bad for an organisation: the white hat or ethical hacker can help. Credit: Shutterstock/napocska

The recent spate of cyber attacks on computer systems across the world shows how some organisations are not doing enough to protect their systems against malicious hackers.

But if organisations had engaged the services of an ethical hacker then many of the vulnerabilities on their systems could have been found and fixed, rather than exploited.

There are many instances in which ethical hacking has successfully prevented a potential attack, but because of the sensitive nature of such information, few cases are made public. This anonymised example highlights the type of issues that can be uncovered by an ethical hacker, which can then be addressed by the client.

Putting on your hacker hat

There are typically three types of hacker: "black hat", "grey hat" and "white hat".

Black hat hackers are typically malicious; they operate illegally and attempt to breach or bypass security controls. Their motivation can be for personal, political or financial gain, or simply to cause havoc.

Grey hat hackers also try to find vulnerabilities in an organisation, and may then alert the organisation or publish the vulnerability.

Grey hats can sometimes sell the vulnerabilities to government or law-enforcement agencies, who may use them for questionable means in conflict or enforcement. The activities of a grey hat are not only questionable, but also seen as illegal because they are not given permission to conduct their operations.

White hat hackers use the same tools and techniques as their black and grey hat counterparts, but they are engaged and paid by organisations to find vulnerabilities. That's why they are known as ethical hackers.

A contract and non-disclosure agreement (NDA) is usually signed between the ethical hacker and the organisation. This ensures that what they are doing is legal and that both parties are protected.

The ethical hack-attack

Ethical hackers will typically follow a phased approach to conducting their tests. Depending on their methods, this will usually begin with a reconnaissance phase in which information is gathered and potential target systems are identified.

From there the computer network will be scanned (externally, internally or both, depending on the engagement) to examine it in more depth so as to identify any known vulnerabilities.

If vulnerabilities are found, an attempt to exploit them may follow, and ultimately access may be gained. An ethical hacker would also attempt to break into system that don't necessarily have a

known vulnerability, but are simply exposed.

Three types of hacker: Black hat, grey hat and white hat. Credit: Shutterstock/MatiasDelCarmine

Ethical hackers will then document their work and capture evidence to report back to the client. Hopefully they will find any vulnerabilities first, before they are exploited by others with less beneficent aims.

Becoming an ethical hacker

Ethical hackers gain their skills mainly through experience.

There are also many courses and certifications that teach ethical hacking, including the CREST Certified Tester, EC-Councils Certified Ethical Hacker, GIAC Penetration Tester and Offensive Security Certified Professional

But these courses can't teach everything. Organisations can differ vastly from one another, and the way to penetration-test each organisation is different and by no means prescriptive.

A good ethical hacker requires a great deal of skill and experience, not just the ability to blindly run a tool or script (also known as "script kiddie").

Ethical hackers, like any other hacker, may also venture into the dark web to gain intelligence and learn about new exploits.

Asking for trouble

One of the frustrations over this month's ransomware attack on Microsoft's Windows systems is that the software giant had already issued a patch in March, to protect PCs from this type of attack.

Despite the warnings, several organisations had not installed the patch, and others were running old Windows XP systems that Microsoft stopped supporting back in 2014. Windows 2003 systems were also vulnerable, having been unsupported since 2015.

This left these systems open to attack by ransomware known by a variety of names, including WannaCrypt and WannaCry. It encrypts files on infected systems, requiring a ransom for their unencryption.

Another attack

It has now been revealed that the same vulnerabilities that allowed this ransomware to infect systems has allowed the spread of a new threat, the Adylkuzz Cryptocurrency Mining Malware.

This ransomware is thought to have gone largely undetected until now because it isn't destructive. Instead, it mines a cryptocurrency called Monero, which can generate income for the attackers.

Wana Decrypt0r 2.0 Ransomware Screen. Credit: Avast

Both outbreaks highlight the importance of practising diligent security and making sure that unsupported systems are upgraded or decommissioned.

The majority of advice so far has focused on appropriate defences such as the Australian Signals Directorate's Essential Eight. This covers issues such as patching, application white-listing, appropriate firewall configuration, and using vendor-supported platforms.

But having a vigilant IT department that follows such guidance may not be enough.

Some focus should be given to how an ethical hacker can be used to help protect organisations against malicious attacks.

More than just an IT check

This approach to using an ethical hacker differs from the traditional internal IT team approach, as the focus is shifted from a defensive to an offensive mindset.

While the importance of solid defences can't be understated, augmenting this with ethical hacking can greatly increase the resilience of an organisation's networks. This approach tests the effectiveness of the controls in place and may identify previously unknown exposures.

But this approach is fairly limited to organisations. Engaging the services of an ethical hacker can cost tens of thousands of dollars, depending on the size of the job.

A typical home user would not have the resources to hire such help. In that case, adequate security controls and awareness would still be the best way to stop many attacks.

Microsoft's Windows 10, for example, installs updates automatically, which can't be deferred like previous versions. Windows 8 and 10 also come with Windows Defender pre-installed.

People should also make sure not to open suspicious emails, including those from unknown recipients. This will go a long way towards preventing infection.

The future of hack attacks

Telstra's latest security report says that 59.6% of future potential attacks in Asia and 52.6% in Australia will be due to external hackers. These attackers will use vulnerabilities (known or unknown) to carry out their attacks.

So there is merit in further research to determine how an ethical hacker can help organisations prevent attacks and infections from unknown vulnerabilities. The ability for a penetration test to identify vulnerabilities in advance before software vendors are aware and can release any patches would be invaluable.

But there are certain ethical issues that need to be considered, given that an ethical hacker often needs to use questionable means, such as through the dark web. There is a fine line between what constitutes an ethical approach and an unethical one.

This article was originally published on The Conversation. Read the original article.

Provided by The Conversation

APA citation: An ethical hacker can help you beat a malicious one (2017, May 19) retrieved 1 December 2020 from https://techxplore.com/news/2017-05-ethical-hacker-malicious.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.