www.pwc.lu/cybersecurity

Watering Hole as a Service

Watering Hole is a 2-step attack where hackers corrupt a trusted website that is expected to be visited by the actual targets. The intermediary website becomes infected with a payload that, once loaded, will ultimately give some level of access to the victims' browser or system.

Hackers can use various types of payloads, from sophisticated 0-days that exploit programs flaws to simple, known files types having dangerous features enabled by unaware individuals.

It is a very versatile threat: it can be tailored to a particular victim or impact millions of hosts. What makes it so effective is that it can combine human flaws (credulity) with technical flaws (either vulnerabilities or dangerous features).

Your challenges

- ☑ Is some of your teams' duty to download files coming from the Internet?
- ☑ Do you have dedicated workstations to browse Internet resources?
- ☑ Have you hardened the configuration(s) of your end-user endpoints?
- ☑ Have you already assessed the effectiveness of your web proxy?
- ☑ Do you want to evaluate your exposure to the client-side vulnerabilities?

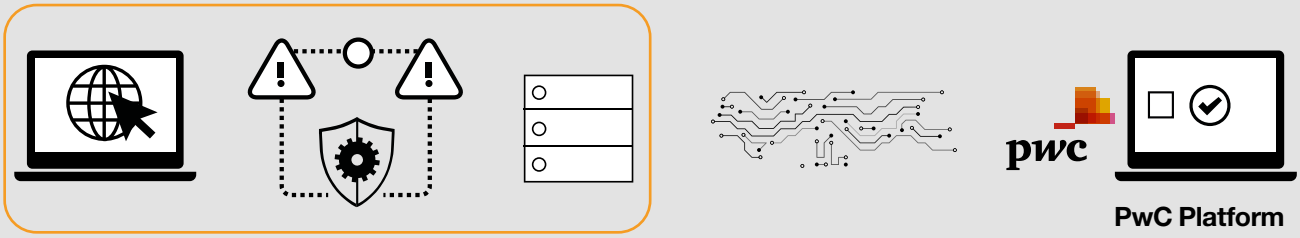
Our Cybersecurity team can help you tackle these challenges!

pwc

How we can help

Our dedicated infrastructure enables us to simulate realistic watering hole attacks and assess your company's defences (endpoint configuration, antivirus/EDR, IDS/IPS, web proxy) all at once and without false-positives. Our report will help you tangibly increase your cybersecurity posture towards evolving Internet threats.

Corporate technical controls to assess



We provide you with a unique simulation to challenge your posture against Internet threats

Why PwC Luxembourg?

Our Cybersecurity team is made up of experienced cybersecurity professionals who hold highly technical and scientific degrees. Our Watering Hole simulation is continuously improved thanks to the relentless Threat Intelligence we perform to provide you with the most recent and realistic attack variants. The clear report you will get after the tests allows for quick understanding of the demonstrated vulnerabilities as well as practical mitigation measures.

Success stories

Our unique approach was taken in various industries such as banks, European Institutions, multinational companies and financial-services firms. These varying organisations with highly secure endpoints have trusted us to assess and optimise their defences against external threats.

For more information, please contact:

Simon Petitjean
Director
+352 49 48 48 4374
simon.petitjean@pwc.lu

Maxime Pallez
Director
+352 621 334 166
maxime.pallez@pwc.lu

Maxime Clementz
Senior Manager
+352 49 48 48 4355
maxime.clementz@pwc.lu

pwc