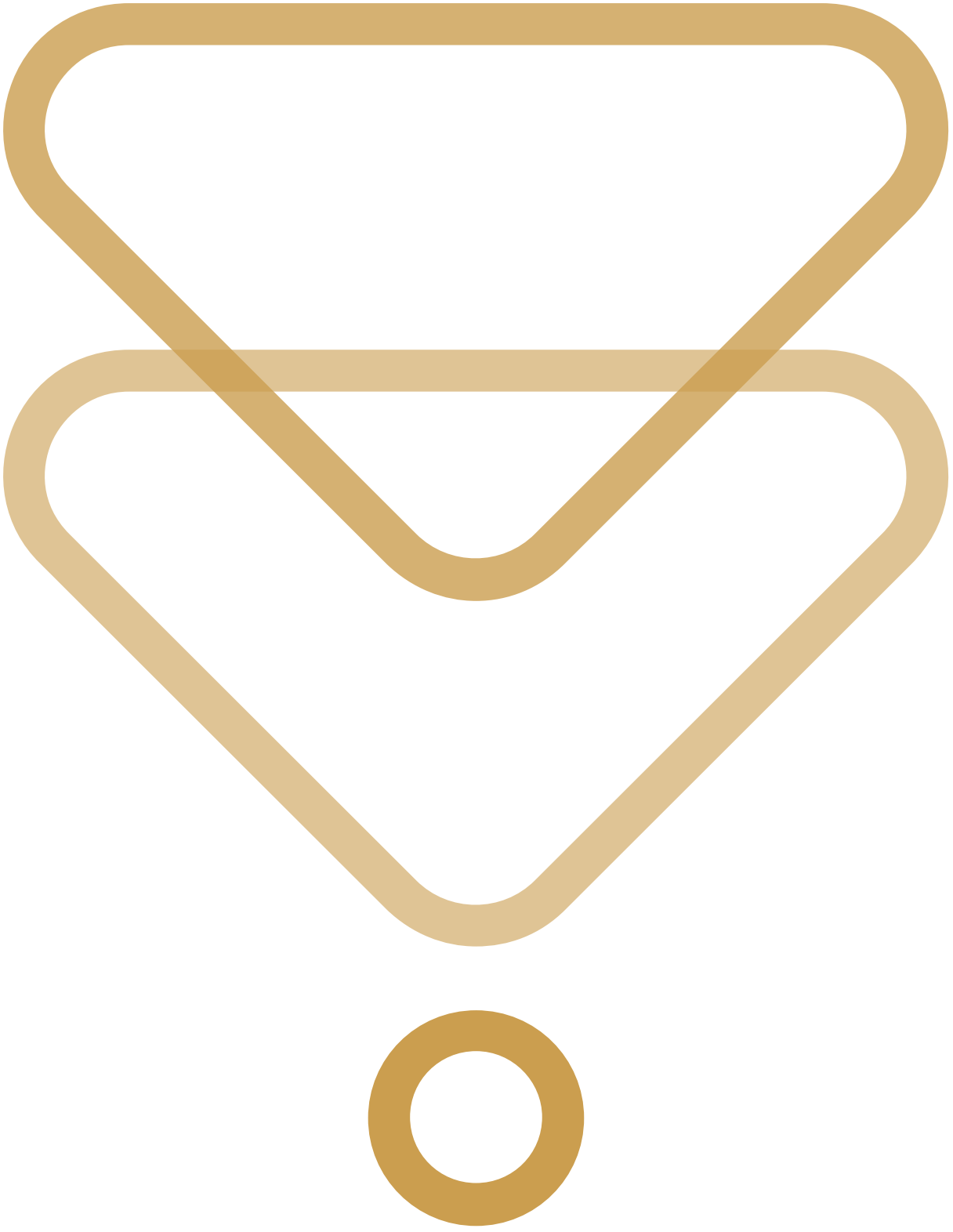
Categorisation is not a Security Boundary - MDSec

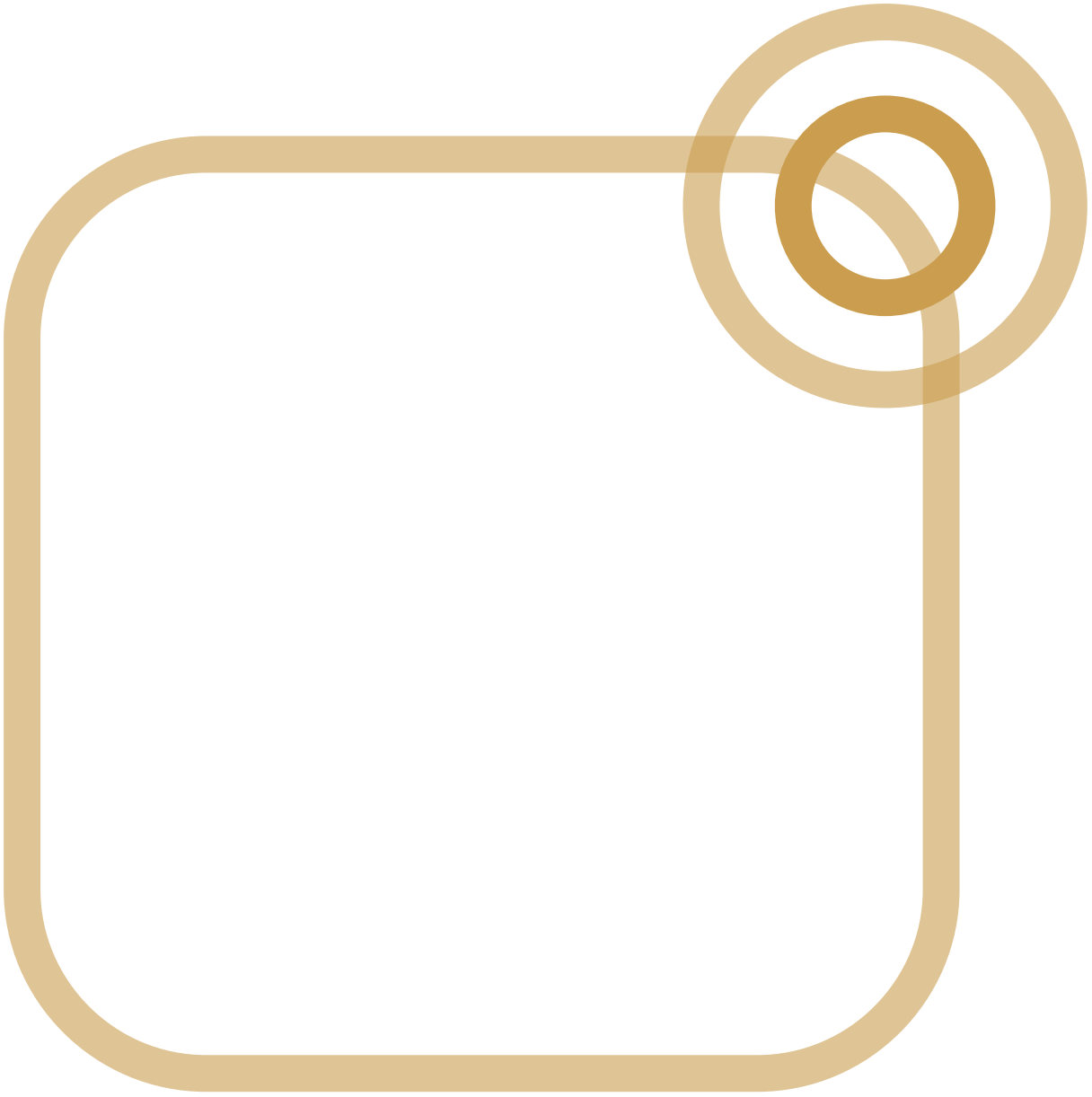
By Admin

Published: 2017-07-11 · Archived: 2026-04-05 20:19:37 UTC



Adversary Simulation

Our best in class red team can deliver a holistic cyber attack simulation to provide a true evaluation of your organisation’s cyber resilience.

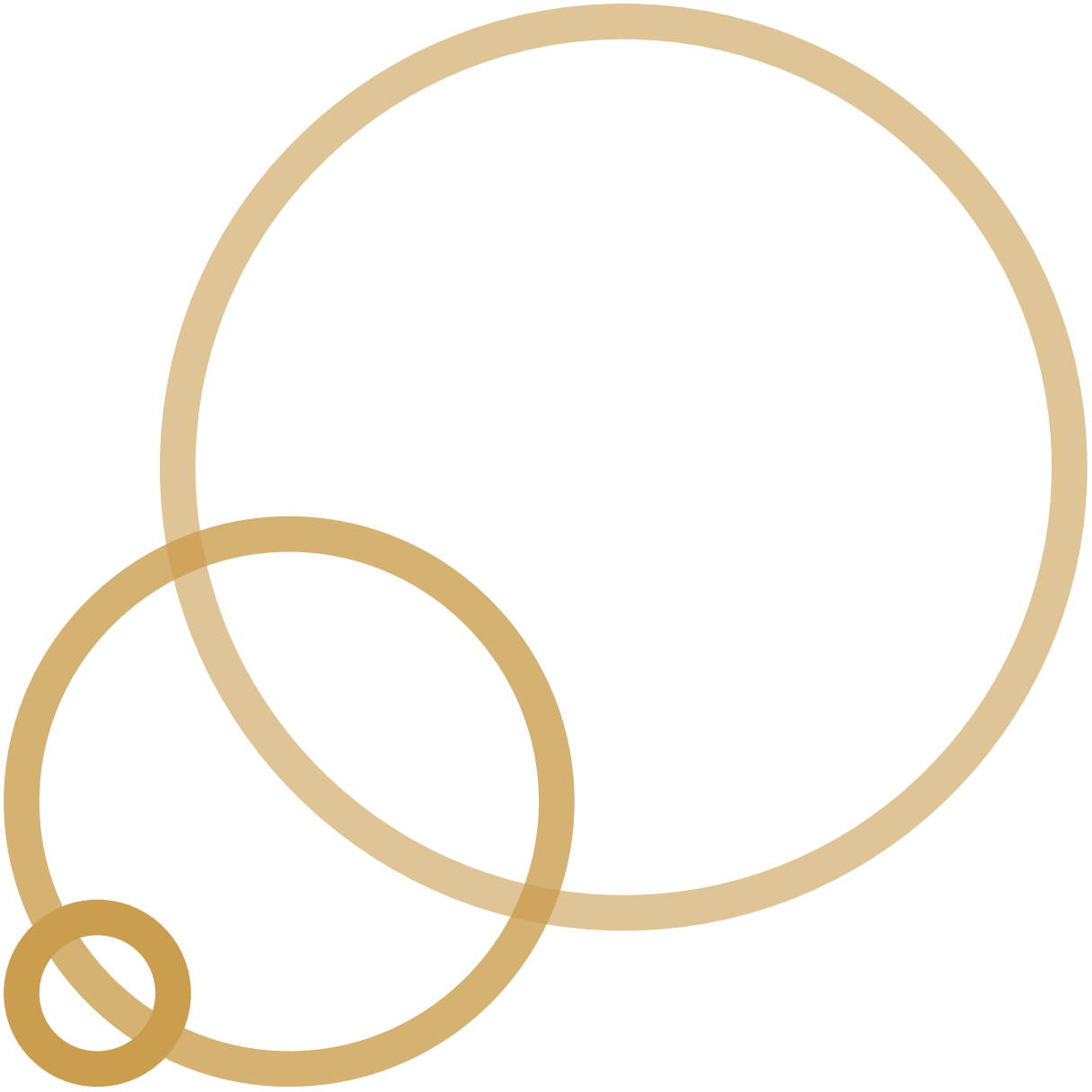


Application Security

Leverage the team behind the industry-leading Web Application and Mobile Hacker’s Handbook series.

Penetration Testing

MDSec's penetration testing team is trusted by companies from the world's leading technology firms to global financial institutions.



Response

Our certified team work with customers at all stages of the Incident Response lifecycle through our range of proactive and reactive services.

Research

MDSec's dedicated research team periodically releases white papers, blog posts, and tooling.

Training

MDSec's training courses are informed by our security consultancy and research functions, ensuring you benefit from the latest and most applicable trends in the field.

Insights

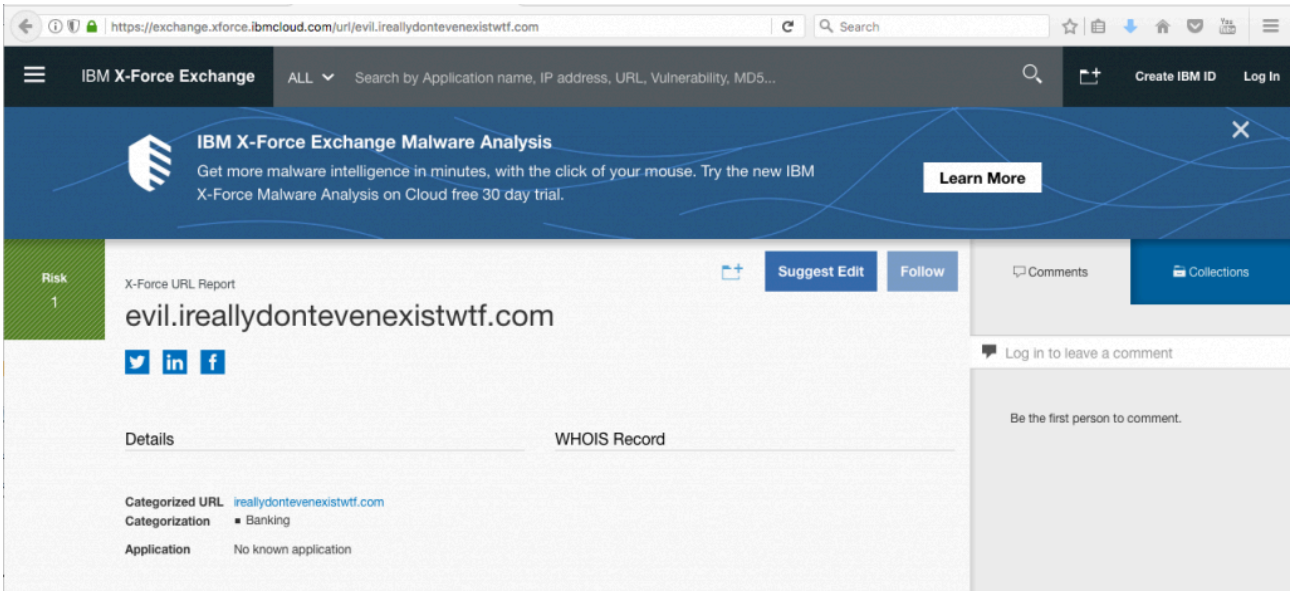
View insights from MDSec's consultancy and research teams.

Prior to commencing any red team engagement, it is important to carefully consider how your infrastructure will be designed. As part of this process, one pivotal consideration is the host/domains you will use for phishing, c2 and exfiltration. In February, we discussed how Domain Fronting could be used to evade security controls such as categorisation and domain reputation. There are however some drawbacks to this technique, namely the limitations when encountering a RFC 2616 compliant proxy.

Domain categorisation can often prove a thorn in the side of many red teams, as new domains are always uncategorised and are therefore likely to be blackholed by most corporate proxies. Additionally, more mature environments are highly likely to restrict the categories that can be accessed to only those that are most trusted such as Finance or Government. If your phishing or c2 domain is blocked due to categorisation by the proxy it often means the end of that campaign unless by chance it lands on a user outside of the network controls or with a less restrictive policy applied. An example of what the user may see if the domain is not in a permitted category is shown below, courtesy of @_RastaMouse:

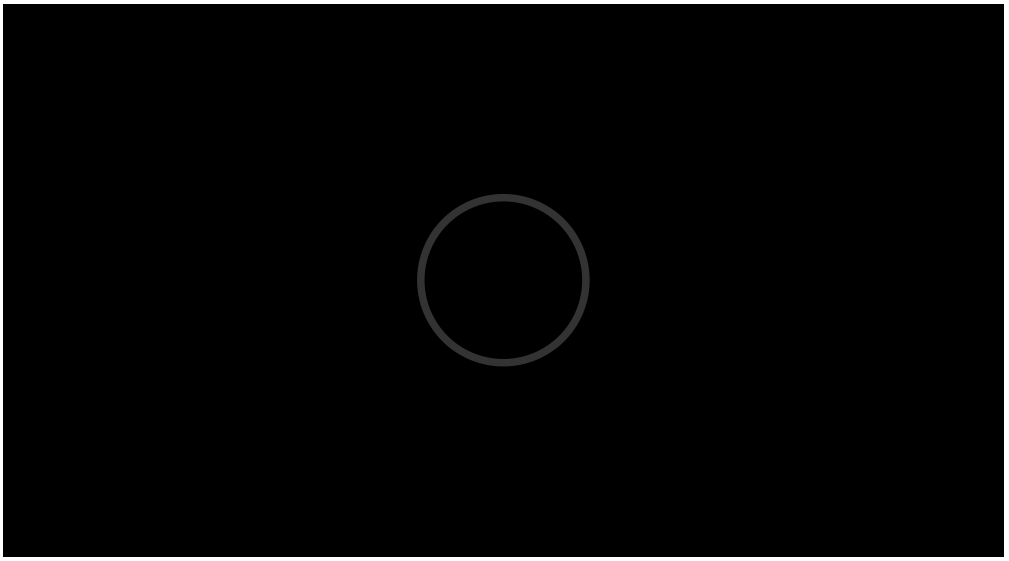
Traditionally, the approach for evading categorisation has been to acquire domains that have been previously categorised and have recently expired. Tools such as CatMyFish and DomainHunter somewhat automate this process and can prove effective in identifying domains to use during your campaigns. There are however drawbacks to this technique, namely it becomes less likely you will find target relevant domains that would add authenticity to your campaigns, e.g. acmecorp.com might mean you want to use acmecorpservices.com, as well as typo-squatted domains.

With this in mind, the ActiveBreach team started to research how categorisation was determined and how sites could be submitted for categorisation. To our surprise, we quickly found that in most cases, little validation was done when a new site was submitted for categorisation. While in other cases, we found flaws in how the validation was performed such that we could instantly fool the proxy service in to categorising our domain to an arbitrary category. An example of categorising an non-existent domain with IBM X-Force is shown below:



This ultimately led to the development and release of the Chameleon tool which assists red teams in categorising their infrastructure under arbitrary categories. Currently, the tool supports arbitrary categorisation for Bluecoat, McAfee Trustedsource and IBM X-Force. However, the tool is designed in such a way that additional proxies can be added with ease.

A video of Chameleon instantly categorising a newly created host, on a newly registered domain against Bluecoat can be seen below:



This blog post was written by @domchell of the MDSec ActiveBreach team.

Chameleon can be downloaded from the MDSec ActiveBreach github page.

Ready to engage with MDSec?

Stay updated with the latest
news from MDSec.
