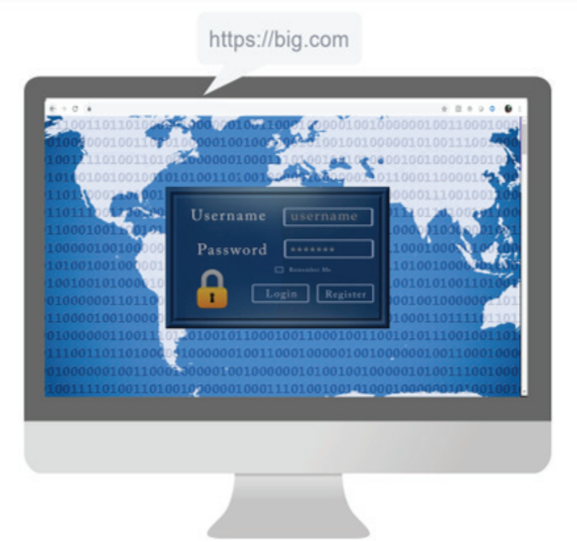
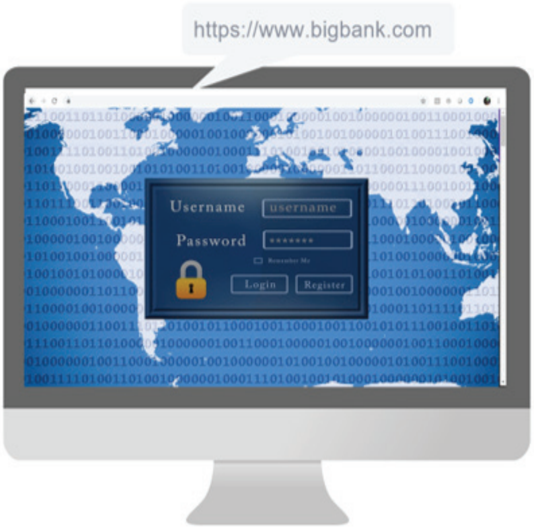
ALLURE SECURITY FOR WEBSITE SPOOFING

Protect your brand and your customers with digital risk detection and response

The familiar phrase “fake it till you make it” has taken on a whole new meaning in cybersecurity. Hackers and fraudsters are increasingly spoofing websites to masquerade as established brands and trusted organizations for personal gain. Whether the motivation is to spread fake news in pursuit of influence, steal customer login credentials or credit card numbers, or break into cloud shares and networks to steal intellectual property, website spoofing has devastating impacts on company reputation, consumer trust and revenues.

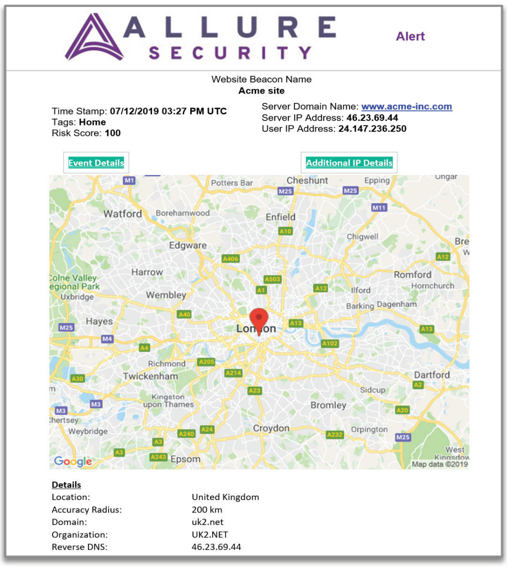




HOW EASY IS IT TO BE FOOLED BY A SPOOFED WEBSITE?

Which website would you log into?
Any one of us could be fooled, including your customers and employees.

Allure Security provides early detection, customer impact insights, adversary intel and active defense.



ALLURE SECURITY Alert

Website Beacon Name
Acme site

Time Stamp: **07/12/2019 03:27 PM UTC**
Tags: **Home**
Risk Score: **100**

Server Domain Name: www.acme-inc.com
Server IP Address: **46.23.69.44**
User IP Address: **24.147.236.250**

Details

Location:	United Kingdom
Accuracy Radius:	200 km
Domain:	uk2.net
Organization:	UK2.NET
Reverse DNS:	46.23.69.44

TRADITIONAL SOLUTIONS ARE LARGELY REACTIVE, SLOW AND DON'T DETER FUTURE ATTACKS

To date, options for detecting when a website have been spoofed has largely relied on monitoring domain registrations and manual web searches. However, this approach is susceptible to human error, only identifies spoofed websites after the fraud occurs, leaves the brand with no insight into how many and which of its clients were potentially impacted and does nothing to limit risk.

A prominent national bank found this out the hard way.

It had five website spoofs in a single month, all done with the intent to steal customer login information. Its digital risk protection service only identified four of them. The fifth one was reported by a customer. After the spoofed websites were taken down, the bank was still left with unanswered questions:

1. How long were the spoofed sites active?
2. Are there more spoofed sites that have gone unnoticed?
3. How many customers have been impacted and who are they?
4. Who did it, and what has he or she done with the stolen information?
5. How can the stolen information be poisoned to limit risk?

$229 M

British Airways faced a record GDPR fine after website attack compromised roughly 5,000 customers

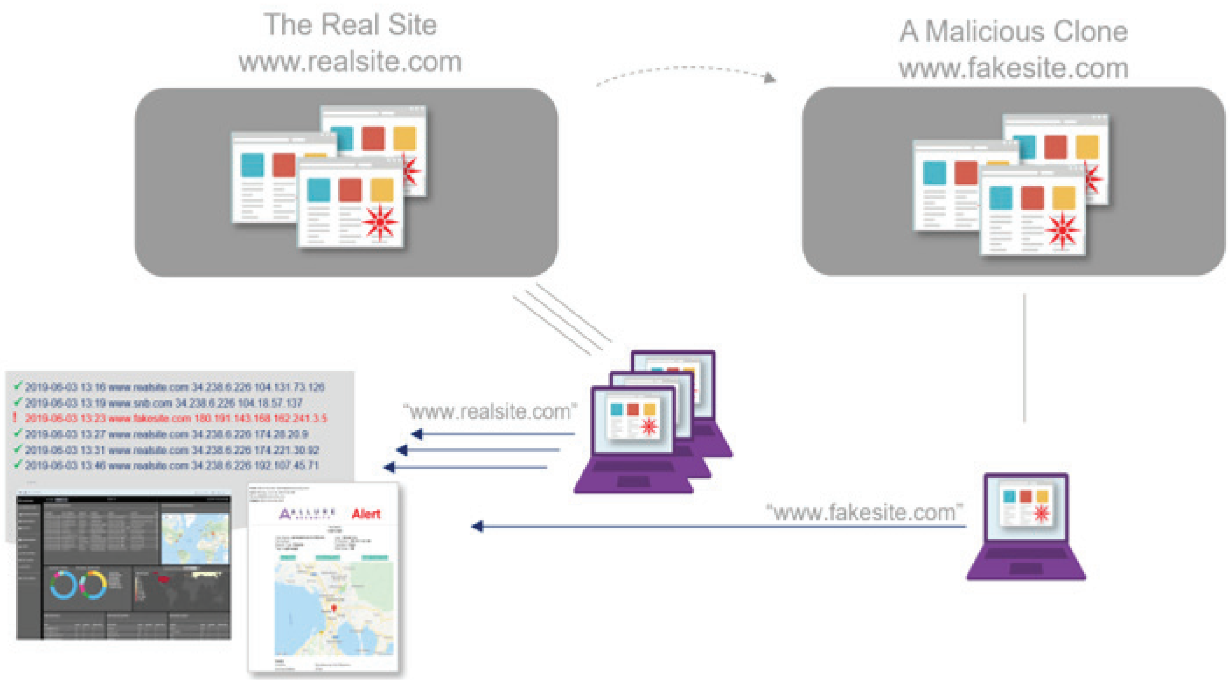
$2.7 B

Financial losses related to Internet-enabled theft, fraud, and exploitation reached staggering heights in 2018

- FBI's Internet Crime Report

USING THREAT DETECTION AND RESPONSE TO LIMIT AND ADDRESS DIGITAL RISK

> Allure Security answers all the questions the prominent national bank could not.



```
✓ 2019-06-03 13:16 www.realsite.com 34.238.6.226 104.131.73.126
✓ 2019-06-03 13:19 www.snb.com 34.238.6.226 104.18.57.137
! 2019-06-03 13:23 www.fakesite.com 180.191.143.168 162.241.3.5
✓ 2019-06-03 13:27 www.realsite.com 34.238.6.226 174.28.20.9
✓ 2019-06-03 13:31 www.realsite.com 34.238.6.226 174.221.30.92
✓ 2019-06-03 13:46 www.realsite.com 34.238.6.226 192.107.45.71
```

HOW IT WORKS

Allure Website Beacons detect a spoofed website as soon as it is viewed by the first visitor, which initiates the take down process immediately upon fraud being committed.

Intelligence is collected to quantify customer and brand impact, inform responses (i.e. notify impacted clients to reset passwords) and uncloak attackers.

The spoofed website can be flooded with decoy credentials until the site is taken down to devalue the information collected by the adversary.

Allure Decoy Documents are used to detect intrusions resulting from attacks, provide adversary intelligence for attackers phishing employees, and extend depth of defense against intrusions.

ALLURE
SECURITY

Allure Security is a digital risk detection and response company that limits and addresses digital risks associated with website spoofing, cloud-share storage, insider threats and intrusions. Allure's patented technology detects threats in the early stages of an attack, collects proprietary intel on adversaries and customer impact to better inform responses, and provides active defense measures to poison acquired assets and imit risk.

200 5th Avenue
Waltham, MA 02451

☎ 877.669.8883

✉ sales@alluresecurity.com

https://www.alluresecurity.com

> "We rely on Allure Security as a force multiplier for our security team."
>
> --- Antonio Garcia, CISO at GRA