Orange
Cyberdefense

Managed Cybercrime Monitoring [fraud]

Surveillance of fraudulent activity. Focusing on phishing sites and domain impersonation, as well as specialised areas such as credit card fraud monitoring

What we do:

- Detection of Phishing through external multivector tools (domains, spamtraps, feeds etc.) and customer asset data
- Monitor similar new domain name registration, with first-hand data due to specific agreements in place with internet hosting and security companies
- Credit Card data gathered via proprietary crawlers and strategic partnership with enterprise Digital Risk Management platforms
- Monitoring of former fraudulent URLs for 12 months
- Triage of all alerts by Intelligence Analysts
- Assistance with takedowns if required and where possible

Striking back

On average Orange Cyberdefense take down nearly 20,000 malicious websites/domains each year. It takes a median time of around four hours to close a fraudulent site so we are efficient too.

It takes experience, partnerships and persistence but our experts make it happen!

What you get:

- Alert notification upon detection
- Full analysis, qualification and investigation of each case and criticality scoring
- Full domain analysis (including owner, content)
- Recommendations
- Optional Takedown service for domains and phishing sites

Cybercrime: infrastructure sphere

When criminals want to host a malicious website or content for phishing, scams or carding sites or rent a server for command and control for example, they may prefer a hosting service that ignores complaints made by visitors and other hosting providers.

The types of malicious sites can include fake shopping sites, torrent and streaming sites, brute force tools and ad sites or porn.

This brings us to infrastructure. Bulletproof hosting is a profitable cybercrime business area that is often overlooked.

There are generally three types of hosting customers can buy:

- A dedicated server, where the provider knows and is okay with hosting malicious content.
- Dedicated servers that have been compromised, are rented out, without the knowledge of the legitimate owner.
- Legitimate cloud servers being rented for malicious use. For example, an article by SpamHaus noted that there is a recent operation renting legitimate virtual private servers (VPS) using fake identities.