NETACEA

Netacea Threat Research Services

If your business operates online, it is a target for criminal activity. Worse, criminals are increasingly focusing their attacks on specific businesses, making them much more dangerous.

Are your website's assets and user accounts for sale on the dark web? Illicit forums and marketplaces are so closely guarded that it's almost impossible to know how many stolen user accounts, digital assets or data leaks are exposed, let alone who is responsible.

Yet without this information, your security initiatives will be misdirected, leaving the business exposed to the most malicious threats.

Dedicated in-house threat intelligence requires highly specialized skills that are prohibitively expensive to resource, as well as a presence in underground marketplaces that takes considerable time to establish, with most forums requiring prolonged membership before granting full access.

Customized threat intelligence directly related to your business

Netacea's Threat Research service is your secret weapon against even the most secretive threat groups. Our highly specialized professionals have successfully infiltrated criminal forums and communities, silently gathering intelligence about ongoing and new threats, and the crooks responsible for them.

Backed by Netacea's expertise in cutting-edge bot management, our threat researchers are well established in the bot space. We filter through the noise of online gossip, only providing intelligence relevant to your business so you can supercharge your security initiatives.

Threat Research and Bot Management

As standard, Netacea Bot Protection includes access to industry vertical trends, research into attacker capabilities and contextualization bot attacks to aid your response.

For businesses needing more detailed intelligence, Netacea offers more frequent fine-tuned threat research and reporting services designed to closely monitor the threat actors that are specifically targeting your organization. This can act as a stand-alone threat intelligence report for your security team or as an upgrade to augment your Bot Protection solution.

In action

A leading German retailer was subjected to repeated, mass account takeover attacks that appeared to be performed by an individual. When German law enforcement had no luck stopping the individual, the retailer turned to Netacea to find suspects and gather evidence proving a connection between the attacker and the crime.

- Within 72 hours Netacea had identified five threat actors active within adversarial communities that were potential suspects. These five were prioritised according to likelihood of being the attacker.
- Netacea interacted with the most likely threat actor, socially engineering them and purchasing taken-over accounts to link the individual to the activity. All evidence was gathered in accordance with requirements outlined by German law enforcement.
- The evidence gathered by Netacea was sent to German law enforcement to aid in the prosecution of a legal case.

NETACEA

Threat Research Packages

The frequency and level of detail of our threat research reports can be tailored to suit the needs of your security team.

Tier 1: Standard

A detailed yearly report on attack groups targeting your business specifically, plus red alerts on critical threats.

Features

- ✓ Annual threat report
- ✓ Automated (passive monitoring of bot forums and marketplaces
- ✓ Insight into the threat groups targeting your business
- ✓ More detail on bot attacks against your sites, apps and APIs
- ✓ Red alert reporting on critical threats

Tier 2: Advanced

Supercharge your threat research with active monitoring and exclusive whitepapers.

Features

Everything in Standard, plus:

- ✓ Quarterly threat report
- ✓ Active monitoring of bot forums and marketplaces
- ✓ Detailed insights into how threat actor groups relate to one another
- ✓ Correlation of attacks seen in Netacea Bot Management with specific groups
- ✓ Access to our research library of whitepapers

Tier 3: Pinnacle

Our top level includes an expert analyst integrated into your team, plus attacker disruption opportunities.

Features

Everything in Advanced, plus:

- ✓ Monthly threat report
- ✓ Dedicated senior threat researcher integrated with relevant teams in your organization
- ✓ Identification of potential pressure points from which to disrupt your attackers