

NETACEA

GUIDE

Getting Started with The BLADE Framework[®]

Contents

Introducing The BLADE Framework.....	3
What are business logic attacks?.....	3
What are kill chains, phases, tactics, and techniques?.....	3
Using The BLADE Framework.....	4
Navigating the matrix.....	4
Drilling down into tactics and techniques.....	5
Search.....	6
Acting against adversaries.....	8
Next steps.....	8
Quick reference glossary.....	9

Introducing The BLADE Framework

The **BLADE Framework**[®] is an open-source standard for distinguishing, categorizing and modeling business logic and automated attacks.

Just as **MITRE ATT&CK** and the **Lockheed Martin Cyber Kill Chain** have given businesses a way to understand and defend against technical vulnerabilities, The BLADE Framework (Business Logic Attack Definition Framework) is a much-needed educational resource in the fight against automated threats and bad bots.

The framework was developed by the **Netacea** Threat Research team with contributions from experts at organizations including Adidas, OVO Energy and Anora Security. It is now an open-source project, with change proposals managed via **GitHub**.

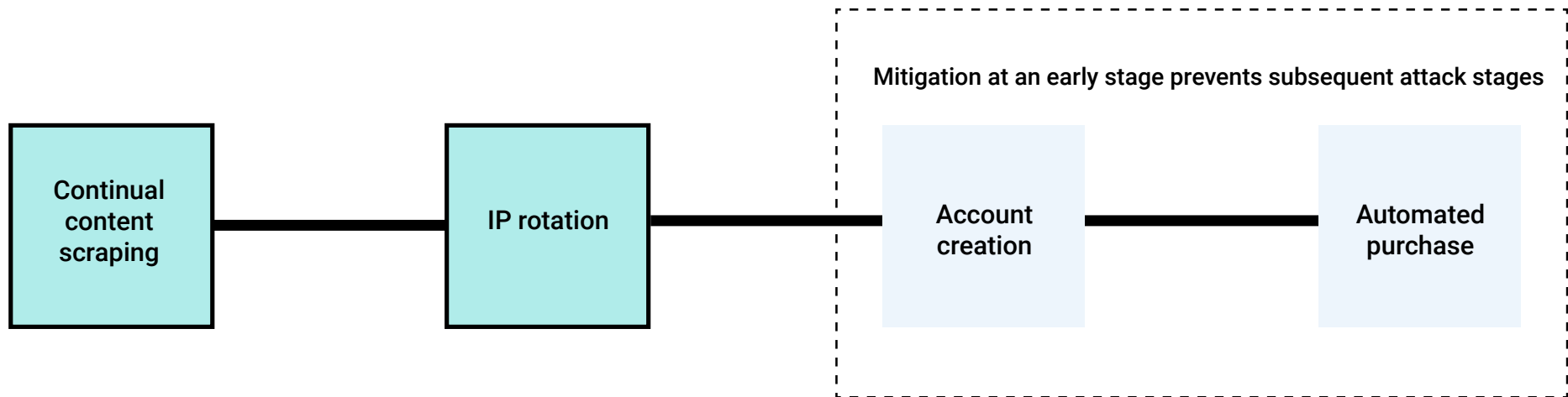
What are business logic attacks?

Business logic is simply what an application does to achieve business objectives. A basic example in eCommerce is the process of buying a product online – to do this, the customer must be able to browse the website, add a product to the cart, sign up for an account or log in, make the purchase, then receive the product. All these steps are facilitated by technical processes defined by the needs of the business and customer.

Business logic attacks use legitimate activity to exploit weaknesses in business logic. In another simple eCommerce example, business logic dictates that the price for items should be displayed on product pages so customers know how much they need to pay and can compare prices. Attackers might exploit this by scraping pricing information in high volumes using automated bots, using this information to undercut prices on another website. No ‘hacking’ or traditional security breach has occurred, but this attack still harms the business.

What are kill chains, phases, tactics, and techniques?

Although business logic attacks typically have an overall objective, they are made up of multiple stages, with each prior action designed to set up a subsequent step. For example, to achieve the general goal of a scalping attack, the attacker may first need to scrape product pages continually to pinpoint the exact second items go on sale, rotate their IP addresses and create multiple fake accounts to bypass purchases-per-customer limitations, and automate ‘Add to cart’ and purchase activity – this sequence is what we call the ‘**kill chain**’, representing the overall lifecycle of an attack objective.



By recognizing distinct **phases**, you can identify what the overall objective of an attack might be and proactively block parts of the attack in an efficient manner. Phases identified within The BLADE Framework are:

- **Resource Development**
Ahead of the actual attack, the adversary establishes resources to aid their operations against the primary targeted victim.
- **Reconnaissance**
The adversary identifies the target and/or ascertains strategic information to inform the latter stages of the attack.
- **Defense Bypass**
The adversary attempts to bypass defense measures.

- **Attack Execution**
The adversary launches their attack against their target.
- **Actions on the Objective**
The adversary performs the intended activity on their target.
- **Post-Attack**
The adversary completes their attack by receiving or reselling the products, services, or information they acquired during their attack.

Within these phases, **tactics** describe overall strategies to achieve the objective, whilst **techniques** are specific actions for fulfilling those tactics. Many tactics and techniques are not unique to one kill chain, so detecting one specific technique could mean an attacker is attempting to achieve one or multiple overall objectives.

Using The BLADE Framework

Navigating the matrix

The **BLADE matrix** is a visual overview of the phases, tactics and techniques used by attackers, and how these relate to each other. You can click on the name of any of these to read a description, and how that specific item relates to others in the matrix directly.

When you first open the matrix, you can see everything expanded by default. For now, start by changing the view to 'phases only' using the view option above the matrix.

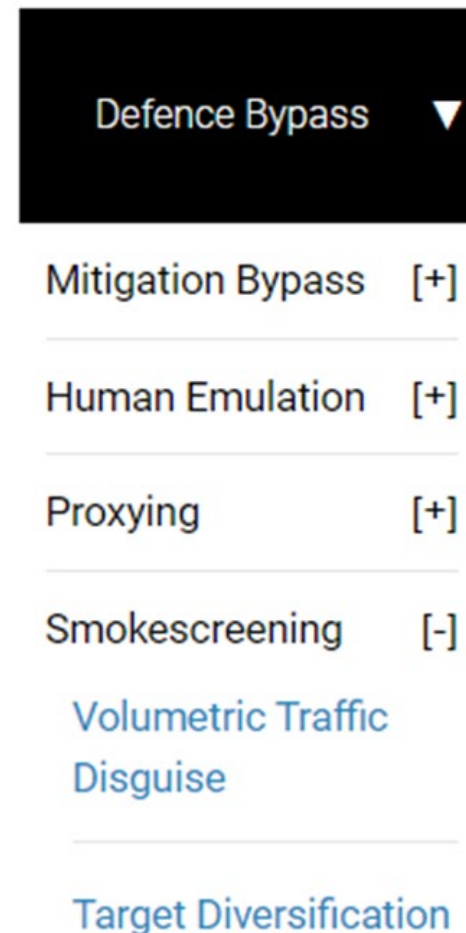
View: [Phases Only](#) | [Phases and Tactics](#) | [Full](#)



From this view you can quickly see all the phases in order. It's important to note that not every attack kill chain runs through all the phases in a linear fashion – Some skip phases or go back and forth depending on the needs of the attacker to reach their objective. However, the matrix presents the phases in a generally linear order.

Expanding the drop-down arrows by each phase reveals the tactics related to it. For example, the defense bypass phase contains the mitigation bypass, human emulation, proxying and smokescreening tactics. If you then expand one of these tactics by clicking the plus sign, you can see the techniques attackers use to achieve these tactics.

To demonstrate, expand the smokescreening tactic in the defense bypass phase. The techniques to achieve this tactic are listed in the dropdown – in this case, volumetric traffic disguise and target diversification.



Drilling down into tactics and techniques

You can get more detailed information about specific tactics and techniques by clicking on their names.

Click on **'Automated Purchase'** to read a short description of the technique, and quickly find out which phase it's part of – in this case, 'Attack Execution'. You can also see which tactics it is used to fulfill ('Stock Purchase', 'Spinning' or 'Sniping'), and which kill chains it's part of, including 'Scalper Bot' and 'Gift Card Cracking Bot'. You can click on any of these to find out more about them too

Automated Purchase

ID: [TEQ-050](#)

Phase(s): [Attack Execution](#)

Tactic(s): [Stock Purchase](#) [Spinning](#) [Sniping](#)

An adversary uses automated means to complete a purchase, generally far faster than any human could do so.

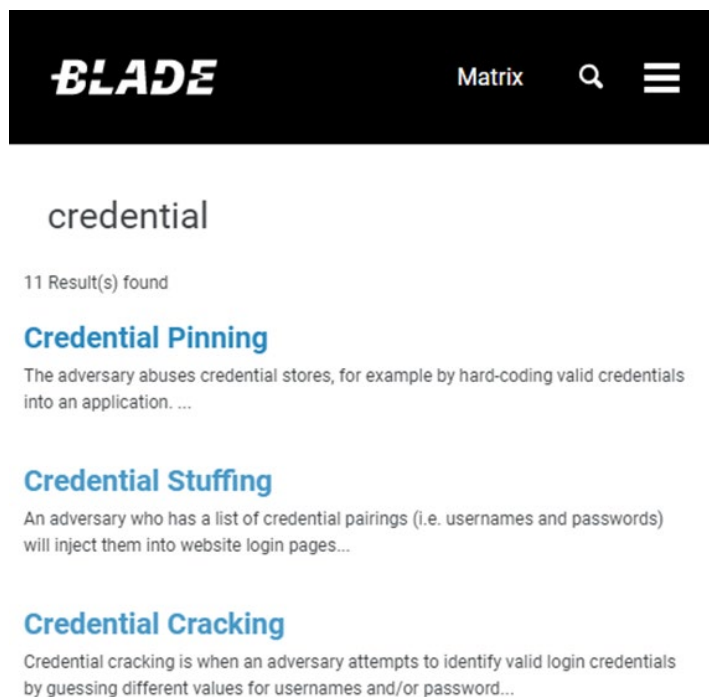
Related Kill Chains

- [Arbitrage Betting Bot](#)
- [Carding Bot](#)
- [Gift Card Cracking Bot](#)
- [Inventory Hoarding Bot](#)
- [Loyalty Points Bot](#)
- [Scalper Bot](#)
- [Sniper Bot](#)

Search

By clicking on the search icon at the top right of any page, The BLADE Framework allows you to quickly search for any kill chain, phase, tactic, or technique. This is useful if you have identified a particular type of activity on your application or API and want to know what the overall objective of the attack might be, what activity to expect next, and how to mitigate further stages.

For example, you might have evidence of a credential stuffing attack on your login page, characterized by a sudden high volume of failed login requests. Searching for 'credential stuffing' will take you to the credential stuffing page, where you can find out that it's a technique within the Account Takeover tactic.



BLADE Matrix 🔍 ☰

credential

11 Result(s) found

Credential Pinning
The adversary abuses credential stores, for example by hard-coding valid credentials into an application. ...

Credential Stuffing
An adversary who has a list of credential pairings (i.e. usernames and passwords) will inject them into website login pages...

Credential Cracking
Credential cracking is when an adversary attempts to identify valid login credentials by guessing different values for usernames and/or password...

Search dynamically then click through for more information on related phases, tactics and kill chains.

Credential Stuffing

ID: TEQ-041

Phase(s): [Attack Execution](#)

Tactic(s): [Account Takeover](#)

An adversary who has a list of credential pairings (i.e. usernames and passwords) will inject them into website login pages in the effort to determine which ones are accepted as legitimate login credentials. The target of such an attack may not be the organisation from which the credentials were initially stolen.

Related Kill Chains

- [Credential Stuffing Bot](#)

Credential Stuffing Bot

A credential stuffing bot is used to test previously leaked credentials (typically username and password pairs) to determine if they are valid on a target webservice or API. These bots validate credential pairs against their target webservice or API by automating login attempts, allowing adversaries to test and validate credentials at mass scale.

[Show Techniques](#) | [Hide Techniques](#)

By clicking on the 'Credential Stuffing Bot' kill chain you can identify previous steps you could correlate to the attack and be prepared for subsequent stages. In this case, you could correlate the credential stuffing attack with IP rotation to explain a high distribution of IP addresses failing authentication on the login page in a short span of time, then keep a close eye on dark web marketplaces for validated credentials based on the volume of successful logins.

Resource Development 3 Tactics	Reconnaissance 1 Tactics	Defence Bypass 4 Tactics	Attack Execution 1 Tactics	Actions on the Objective 1 Tactics	Post-Attack 1 Tactics
Credential Acquisition ▼	Specific Target ▼	Mitigation Bypass ▼	Account Takeover ▼	Exfiltration ▼	Sale ▼
Data Dumps	Technical Reconnaissance	CAPTCHA Farm	Credential Stuffing	Credential Dumping	Information Brokerage
Infrastructure Acquisition ▼		Automated CAPTCHA Bypass			Automated Sale
Botnet		MFA Bypass			Manual Sale
Command & Control		Human Emulation ▼			
Proxies		User Agent Spoofing			
Tool Development ▼		Proxying ▼			
Development of Tools		Botnet			
Campaign Reuse		User Agent Spoofing			
		IP Rotation			
		Smokescreening ▼			
		Volumetric Traffic Disguise			
		Target Diversification			

Acting against adversaries

How you react to these techniques once detecting them will likely modify the course of the overall attack and kill chain. For example, blocking an IP address or datacenter in response to a technique detected at the attack execution stage may push the adversary back to the defense bypass phase, where they will retool or acquire new routes for their traffic to try to execute the attack again. However, knowing the behavior needed to achieve their ultimate goal will help you look out for these patterns coming from different origins and quickly defend against them, until the attacker moves on. The BLADE Framework can also be used to post-mortem attacks and bolster defenses in future.

Unlike technical vulnerabilities, most business logic vulnerabilities can't be patched in the traditional sense because the organization relies on business logic to operate. New functionality or ways of achieving business objectives will in turn increase the business logic attack surface. This means constant vigilance against abuse is needed, and The BLADE Framework will grow, change and develop organically as businesses themselves evolve.

With so many techniques available to attackers to bypass defenses, and automation allowing attacks to start and stop so suddenly, looking for just one attack signal and attempting to block via manual rule changes is not enough. That's why machine learning models with real-time intervention has become the standard approach to suppressing automated bot attacks.

Netacea Bot Management uses a combination of our Active Threat Database, a proactively updated database of known threats sourced from its whole estate of protected domains, alongside Intent Analytics®, a collection of generic and specifically tuned machine learning and anomaly detection models for each customer and use case, to root out business logic attacks in real time. This information can be fed directly into SOC teams or SIEM tools, automatically mitigated, or analyzed for more context by Netacea bot experts.

Next steps

We recommend taking time to browse through as much of The BLADE framework as possible so you can better identify bot activity on your website, applications, or APIs. You will gain a better understanding of what these bots are aiming to achieve, where your business might be compromised, and what you can do to stop it sooner.

Quick reference glossary

Kill chain

The overall phases of an attack, their order and the tactics and techniques employed therein.

[Examples: Account Takeover Bot, Inventory Hoarding Bot, Scalper Bot](#)

Phase

The distinct stages an attack goes through. The phases required and their order depend on the adversary's goal.

[Examples: Resource Development, Defense Bypass, Attack Execution](#)

Tactic

The high-level strategies and activities that make up the phases of an attack.

[Examples: Credential Acquisition, Proxying, Invoice Abuse](#)

Technique

A specific action designed to fulfill a tactic. There could be multiple techniques within one tactic, and one technique could be part of several tactics depending on the overall objective of the attack.

[Examples: User Agent Spoofing, IP Rotation, Automated Purchase](#)