Business Enablement Bots

org chart with sophisticated tools that exploit business logic and the convergence in order to stop criminals. Security and fraud teams must use tools that can be used to compromise journeys. But in the wrong hands, customers early in their buying.

Bots automate repetitive tasks, the Convergence of Cybersecurity and Fraud. The F5 integrated platform mitigates malicious automation and stops fraudulent transactions with the highest security effectiveness while removing friction.

Better Together

F5 offers an integrated platform that maximizes the customer experience. To compete in a digital-first world, organizations need better business outcomes. F5 ensures better business outcomes for fraud prevention, visit f5.com/stopfraud.

How Fraud Impacts the Business

- Poor business and marketing insights
- Damaged brand
- Lost customer trust
- Top-line transaction and revenue abandonment

ATTACK METHODS

- Automated and Manual Fraud
- Automated and Manual Fraud

ATTACK TARGETS

- Login Apps and APIs
- Login Apps and APIs

ATTACK GOALS

- Protect customers across the entire user journey from web/mobile/API endpoints.
- Confuse attackers
- Maintain resilience and efficacy

ATTACK TYPES

- Crawl the Internet fetching key balances, and launder money.
- Leverage aggregators as a backdoor into banks in order to steal large-scale account compromise.
- Use stolen credit card numbers to launder money through gift cards.
- Use stolen credit card numbers to move from targeting web to mobile and API endpoints.
- Collect proprietary data that can be used to scale credential-based attacks using cURL and highly distributed botnets.
- Commit 3rd-party fraud by leveraging CAPTCHA solvers, headless browsers, web stack emulators, anti-fingerprinting tools, stolen tokens from the dark web, malicious scripts, or even when attackers use stolen or acquired credentials.
- Steal money; abuse PII for future schemes.
- Attackers that spoof signals to evade detection.
- Reconnaissance and prevent bypass by sophisticated all telemetry to thwart network traffic, and HTTP headers.

FAKE ACCOUNTS

- Create and consolidate fake accounts, to manipulate pricing items in shopping carts, usually in difficult to identify and stop.
- Identity theft, synthetic identity attacks with different tactics to bypass security countermeasures.
- After being blocked, sophisticated attackers adapt and move from targeting web to mobile and API endpoints.
- The dark web, malicious scripts, or even when attackers try to stay one step ahead by employing CAPTCHA solvers, headless browsers, web stack emulators, anti-fingerprinting tools, stolen tokens from the dark web.
- Achieve larger return policies; and obtain promotional, loyalty, and revenue.

TABLE 1: ATTACK GOALS

<table>
<thead>
<tr>
<th>ATTACK GOALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect customers across the entire user journey from web/mobile/API endpoints.</td>
</tr>
<tr>
<td>Confuse attackers</td>
</tr>
<tr>
<td>Maintain resilience and efficacy</td>
</tr>
</tbody>
</table>

TABLE 2: ATTACK TYPES

<table>
<thead>
<tr>
<th>ATTACK TYPES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crawl the Internet fetching key balances, and launder money.</td>
</tr>
<tr>
<td>Leverage aggregators as a backdoor into banks in order to steal large-scale account compromise.</td>
</tr>
<tr>
<td>Use stolen credit card numbers to launder money through gift cards.</td>
</tr>
<tr>
<td>Use stolen credit card numbers to move from targeting web to mobile and API endpoints.</td>
</tr>
<tr>
<td>Collect proprietary data that can be used to scale credential-based attacks using cURL and highly distributed botnets.</td>
</tr>
<tr>
<td>Commit 3rd-party fraud by leveraging CAPTCHA solvers, headless browsers, web stack emulators, anti-fingerprinting tools, stolen tokens from the dark web, malicious scripts, or even when attackers try to stay one step ahead by employing CAPTCHA solvers, headless browsers, web stack emulators, anti-fingerprinting tools, stolen tokens from the dark web.</td>
</tr>
<tr>
<td>Achieve larger return policies; and obtain promotional, loyalty, and revenue.</td>
</tr>
</tbody>
</table>