Business Enablement Bots

Security and fraud teams must account takeover (ATO) and fraud. Customer accounts—resulting in tools that can be used to compromise journey. But in the wrong hands, customers early in their buying raise brand awareness, and engage Bots automate repetitive tasks, The Convergence of Cybersecurity and Fraud

Bots, Automation, and Fraud

For fraud prevention, visit f5.com/fraudprevention.

The Industrialized Attack Lifecycle

Automated and Manual Fraud

The Threat Ecosystem At-a-Glance

• Increased operational efficiencies
• Reduced complexity
• Decreased bottom-line fraud losses
• Increased top-line revenue
• Improved conversion, retention, loyalty
• Less fraud, less friction, less effort

F5 offers an integrated platform that mitigates malicious to compete in a digital-first world, organizations need here's how it works:

1. Gain visibility across data centers, clouds, and transactions or money balances, and launder money.
2. Leverage aggregators as a backdoor into banks in order to steal information, check account balances, and launder money.
3. Capitalize on web page data used by search engines.
4. Client-side Attacks
5. Search Engine Bots

Automated and Manual Fraud

TABLE: ATTACK METHODS

<table>
<thead>
<tr>
<th>ATTACK TYPES</th>
<th>ATTACK GOALS</th>
<th>ATTACK METHODS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1st-party fraud</td>
<td>3rd-party fraud</td>
<td>crime syndicate, fraud, and credit application fraud.</td>
</tr>
<tr>
<td>2nd-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>3rd-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>4th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>5th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>6th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>7th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>8th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>9th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
<tr>
<td>10th-party fraud</td>
<td>3rd-party fraud</td>
<td>criminals pivot to use human engineering, and manual hacking.</td>
</tr>
</tbody>
</table>

Here's how it works:

Here's how it works:

1. Remove unnecessary authentication challenges
2. Confuse attackers
3. Encrypt and obfuscate
4. Collect device, network, and environmental telemetry
5. Maintain resilience and efficacy
6. Mitigate malicious automation
7. Reconnaissance and prevent bypass by sophisticated
8. Emulators, anti-fingerprinting tools, stolen tokens from CAPTCHA solvers, headless browsers, web stack
9. Mitigate malicious automation
10. Attackers that spoof signals to evade detection.

Criminals pivot to use human engineering, and manual hacking. Credentials are)

A table is shown with the following columns:

- ATTACK TYPES
- ATTACK GOALS
- ATTACK METHODS

The table includes various types of attacks such as 1st-party fraud, 2nd-party fraud, 3rd-party fraud, and 4th-party fraud, among others. Each type of attack has its own goals and methods of execution, such as crime syndicate, fraud, and credit application fraud. The methods include criminals pivot to use human engineering, and manual hacking. This highlights the complexity and variety of fraud attacks in today's digital environment.