CASE STUDY

Reducing Fraud and Protecting Citizen Information

GOVERNMENT AGENCY

- 100 million households
- +300 million citizens
- $2 trillion in benefits and payments

Loss of confidence in ability to protect citizen information

ACCOUNT TAKEOVER ATTEMPTS

- Attackers compromised extensive multi-step authentication process.
- Stolen passwords and personal information combined with intelligent algorithms to guess answers to authentication questions.
- Millions of account takeovers attempted.

Hundreds of thousands of account takeovers

F5 DISTRIBUTED CLOUD BOT DEFENSE

- Eliminated all account hijacking and saved tens of millions of dollars.
- Blocked malicious bots and automated attacks.
- Protected citizen information.

Millions of dollars in cyber fraud avoided

Overview: How F5 stopped targeted and highly sophisticated attacks.

The U.S. government serves over 100 million households and processes over $2 trillion in payment and benefits. Cybercriminals view government agencies as prime targets for large-scale automated attacks. Using credentials stolen from other websites, attackers use automation to test out large numbers of usernames and passwords with the aim of taking over citizen accounts and stealing valuable information and assets.

Cybercriminals using automated techniques and stolen credentials were able to take over half of the accounts they targeted at one U.S. government agency. Even though the agency authenticated website visitors by challenging them with a series of questions, based on information that was supposed to be only uniquely available to the agency, and that only the account holder should be able to answer, the cybercriminals were able to bypass these security measures.

The government agency under attack needed a new approach to fight fraud and deployed the F5® Distributed Cloud Bot Defense. Using this service, the government agency stopped the account takeover attacks within two days of deploying countermeasures and going into full blocking mode, thereby preventing hundreds of millions of dollars in cyber fraud.

Why F5?

The U.S. government agency evaluated anti-automation options and chose Distributed Cloud Bot Defense for its ability to effectively and transparently stop unwanted automation at the agency's operational scale. The agency must meet citizen demands for technology that is backward compatible with legacy web applications and also comply with regulations related to accessibility. F5's implementation team has deep skills in browser technologies and was able to work closely with the agency's security team to test and verify backward compatibility.

Distributed Cloud Bot Defense Implementation

Phase 1

Reconfigured application delivery controllers to route hardened pages through F5® Distributed Cloud Dynamic Modulator and validated traffic flows.

Phase 2

Began telemetry and activated supervised and unsupervised learning through the F5 threat intelligence team. Developed countermeasures based on gathered data.

WITH FULL SETS OF STOLEN CREDENTIALS AVAILABLE FOR PURCHASE ON DARKNET FOR AS LITTLE AS $5, AUTOMATION MAKES LARGE-SCALE CREDENTIAL STUFFING ATTACKS ECONOMICALLY FEASIBLE.

Phase 3

Activated F5 countermeasures in a non-blocking mode to verify countermeasure efficacy and browser compatibility.

Phase 4

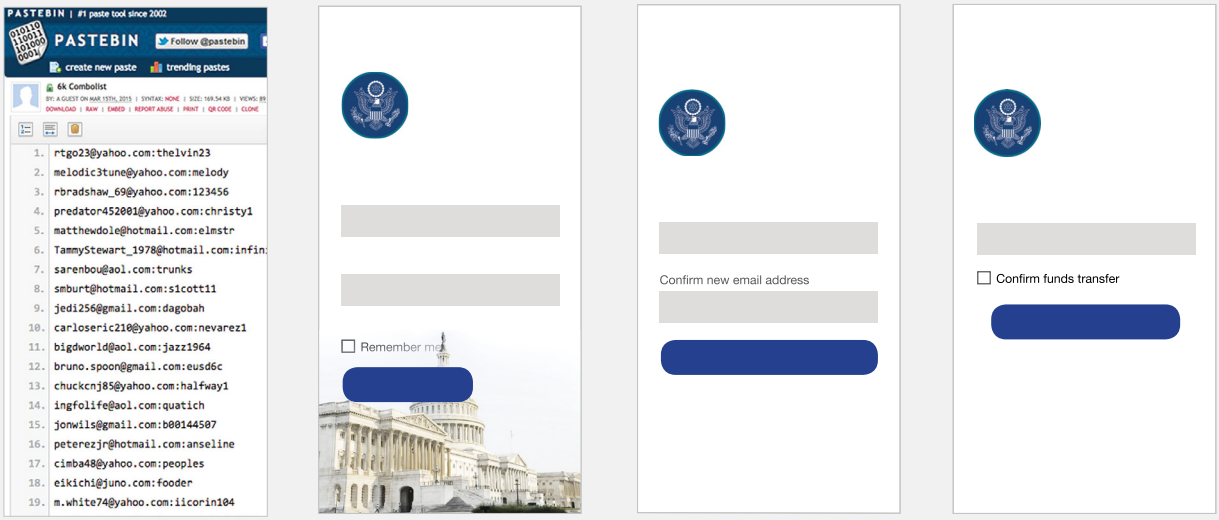
Put Distributed Cloud Bot Defense into production and began blocking unwanted automation.

Solution Benefits

- Dramatically reduced account takeovers and associated cyber fraud.
- Reduced fraud losses as cyberattackers abandoned account takeover attempts once F5 began blocking unwanted automated traffic.
- Met accessibility requirements (that precluded use of CAPTCHA) by delivering transparent access for human visitors.
- Provided comprehensive attack analytics to give a clear picture of all automation attacks.
- Enabled the agency to serve a broad population by offering backward compatibility with a wide variety of browsers.

The Anatomy of an Attack

Stolen credentials combined with AI



Stage 1

Attackers acquired spilled credentials from the open web of criminal marketplaces and password dump sites.

Stage 2

Attackers tested stolen passwords and personal information combined with intelligent algorithms to guess answers to authentication questions.

Stage 3

Attackers hijacked accounts when the credentials were valid.

Stage 4

Attackers then redirected payments and benefits.

Figure 1: The anatomy of an attack

Conclusion

This critical government agency was able to dramatically lower account takeover and associated fraud through the deployment of Distributed Cloud Bot Defense. Working with the agency's web application and network technologists, F5 was able to successfully integrate this service into the agency's web application platform while meeting all compatibility and accessibility requirements.

The agency continues to benefit on an ongoing basis from F5 threat intelligence, 24x7 monitoring, countermeasure updates, and threat research, enabling it to stay ahead of cybercriminals.

To learn more, contact your F5 representative, or visit f5.com.