



Inherent Vulnerability Threat Assessment

Dan Woods

F5 Global Head of Intelligence

d.woods@f5.com

December 1, 2021

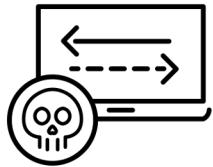
About your F5 Shape Researcher



Dan Woods spent 20+ years with local, state and federal law enforcement and intelligence organizations in the United States including the FBI as a special agent where he was assigned to cyber terrorism; and the CIA as a technical operations officer where he was assigned to cyber operations. He currently serves as the Global Head of Intelligence at F5. In this capacity, he provides companies all over the world with inherent vulnerability threat assessments. He also holds a BSE in Computer Systems Engineering.

Dan can be contacted at d.woods@f5.com

What's Included in Your Threat Assessment



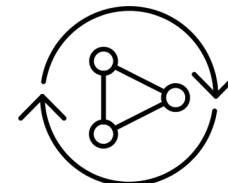
Review of your attack surfaces: We will identify your public-facing applications likely to be targeted by bots.



Explanation of attacker methods: You will understand attackers' objectives when launching automated attacks against your applications.



Reveal vulnerable information already out there: We will share information from the deep/dark web including proof of bots accessing your applications and attackers' use of your customers' digital fingerprints, if any.

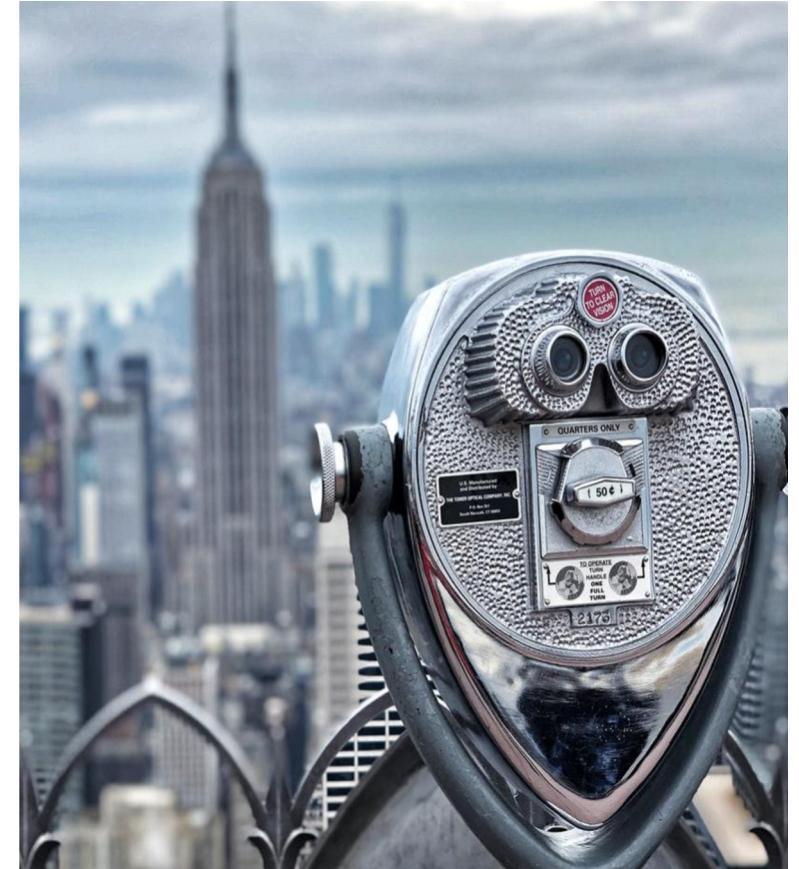


Recommended next steps: We will provide professional guidance for gaining more visibility and help quantify automated and manual attacks targeting your applications.

Assessment is limited to an outsider's perspective

The vulnerabilities identified in this report were derived from F5 Shape's experience mitigating automated and manual attacks across the F5 Shape Network and from analyzing publicly accessible web applications at your company. Admittedly, F5's observations are limited to an outsider's perspective with no visibility into what your company is doing behind the scenes.

F5 welcomes the opportunity to refine and improve its understanding through collaborative discussions with your security and fraud teams.



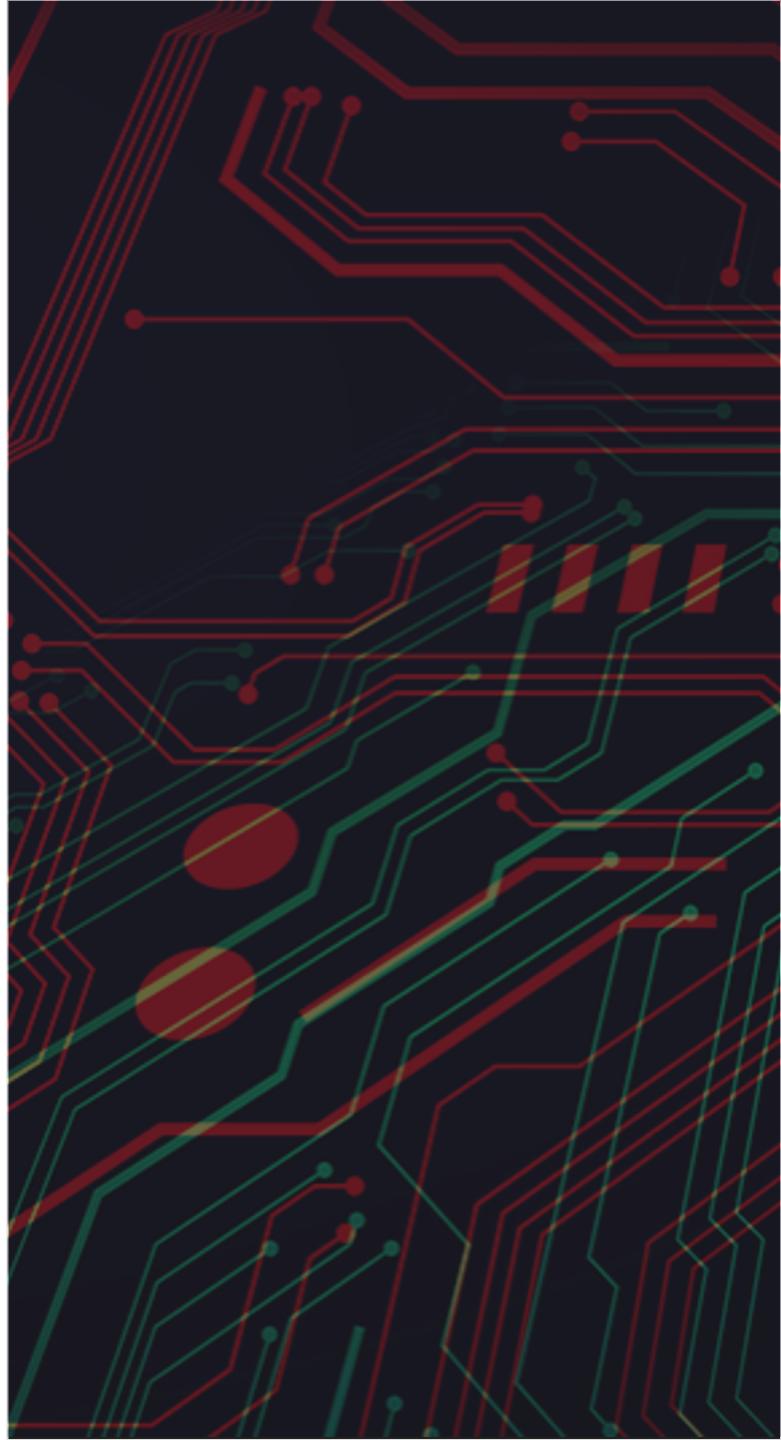
Area of Focus

Vulnerability assessments are typically focused on discovering inadvertent vulnerabilities, which are those that result from coding or configuration mistakes such as Cross-Site Scripting (XSS), SQL injection, and others as listed in the [OWASP Top 10](#). Once discovered, these sorts of vulnerabilities can typically be corrected or patched. These inadvertent vulnerabilities are not the focus of this assessment.

This assessment is instead focused on discovering inherent vulnerabilities, which do not result from mistakes, but from valid business requirements. As one example, an organization is vulnerable to Credential Stuffing if only two criteria are met:

1. Users can log into online accounts
2. Attackers perceive the accounts contain something of value

Inherent vulnerabilities need to be protected, but they cannot be “patched” in the conventional sense.



Findings

These logins vulnerable to credential stuffing

Credential Stuffing is when a bad actor uses automation to try hundreds of thousands, millions, or even billions of username/password pairs against the login application. Because of the way people reuse usernames and passwords, credential stuffing successfully takes over accounts 0.1% to 3% of the time. This leads to fraud, financial losses, embarrassing headlines, and damage to brand and reputation.

A screenshot of a standard web-based login form. It features two input fields: 'Username / Email *' and 'Password *'. Below the password field is a checkbox labeled 'Keep me signed in' with the option to 'Learn more'. A large red 'LOGIN' button is centered at the bottom of the form.

<https://acmegroup.com/login>

A screenshot of a specialized agent login form. The title 'Login with Username and Password' is displayed in green. The form includes two input fields: 'User:' and 'Password:', both containing placeholder text ('Agent User ID' and 'Agent Password' respectively). A 'Sign in' button is located below the password field. The entire form is enclosed in a light gray border.

<https://acmegroup.com/agent/login.jsp>

Company employee login vulnerable to credential stuffing

While third party authentication services are not provided from a domain Acme Group can protect, relying on third parties for authentication can make the corresponding accounts vulnerable to credential stuffing and account validation attacks. In this case, the service Acme Group is using to authenticate employees is heavily targeted by bots.

Showing 10,000 of 47,238 Botnet data.

IP Address	Log Date	Import Time	Accessed Domain
49.37.68.106	2021-08-14 08:27:04	2021-09-20 18:34:14	login.microsoftonline.com
	accessed URL https:// login.microsoftonline.com /common/oauth2/authorize		
	username ballb0014@presidencyuniversity.in		
	password passmeli1321		
	user Dell		
	OS Windows 10 Home Single Language		
	country IN		
	continent Asia		
	latitude 20		
	longitude 77		
> 49.37.68.106	2021-08-14 08:27:04	2021-09-20 18:34:14	login.microsoftonline.com
> 185.93.61.7	2021-08-14 06:45:47	2021-09-20 18:31:06	login.microsoftonline.com
> 177.255.127.227	2021-08-14 06:14:46	2021-09-20 18:33:42	login.microsoftonline.com
> 177.255.127.227	2021-08-14 06:14:46	2021-09-20 18:33:42	login.microsoftonline.com
> 161.132.234.178	2021-08-14 04:48:42	2021-09-20 18:32:09	login.microsoftonline.com
> 180.241.46.25	2021-08-14 04:35:09	2021-09-20 18:23:49	login.microsoftonline.com

Botnet logs from dark web

Forgot password is not vulnerable (but not due to reCAPTCHA)

F5 Shape sees automated attacks against the Forgot Username/Password applications only when the applications give feedback as to whether or not the account exists. Acme Group follows best practice and does not give such feedback, so there is no incentive for an attacker to launch an automated attack and no reason for reCAPTCHA. In any case, reCAPTCHA does not stop motivated bots. Using it here only creates unwanted friction for your customers. Watch this video or this video to see how attackers beat reCAPTCHA.

The screenshot shows a web form titled "Forgot Username/Password". At the top, there is a red "Username" input field with the placeholder "Please enter your Username to reset your Password.". Below it is a "Username:" label followed by an empty input field. To the right of this input field is a link "I forgot my username". Underneath the input fields is a reCAPTCHA interface. It features a checkbox labeled "I'm not a robot" and a reCAPTCHA logo with the text "reCAPTCHA Privacy - Terms". At the bottom of the form are three buttons: "BACK", "CANCEL", and a red "CONTINUE" button.

<https://acmegroup.com/forgot>

Company enrollment vulnerable to automation

F5 Shape sees automation against Create Account applications for many reasons, e.g. money laundering, account enumeration, loyalty program abuse, influence amplification, and many more. The presence of reCAPTCHA here indicates that for some reason Acme Group anticipates unwanted automation; however, as stated previously, reCAPTCHA cannot stop motivated bots. A stronger countermeasure here would prevent the need for what appears to be an additional review (the process that takes 1-2 business days).

ACMEplus™ Enrollment

⚠ Users are enrolled by the [Master Administrative User](#) for your company. This person can setup and maintain all your users and their permissions. Please only enroll if you will be Master Administrative User!

Company

Customer ID

Name

Email

Confirm Email

Phone

Laufer Salesperson

I confirm that I am a Master Administrative User.
By enrolling, I agree to the [PeerPLUS Terms and Conditions](#).

I'm not a robot 
reCAPTCHA
Privacy - Terms

SUBMIT

<https://acmeplus.acmegroup.com/enroll>

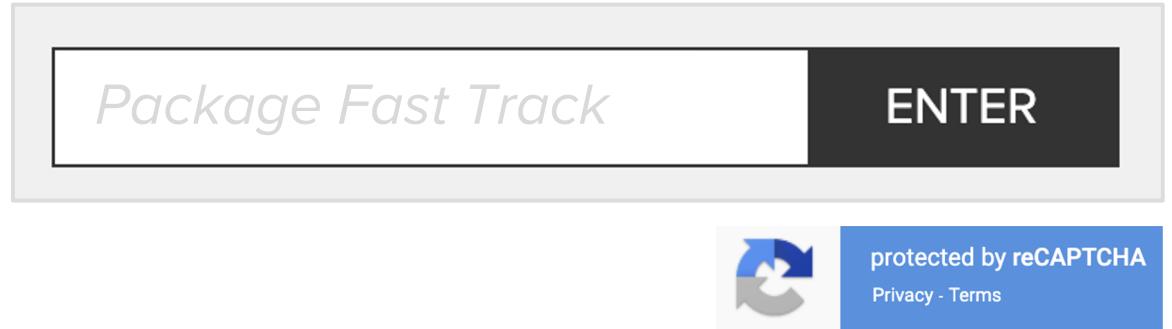
ACMEplus™ Enrollment

ℹ Thank you for your request, we will get back to you within 1-2 business days!

[Visit Laufer website](#)

Package tracker vulnerable to automation

The presence of reCAPTCHA on Fast Track indicates that Acme Group anticipates unwanted automation; however, as stated previously, reCAPTCHA cannot stop motivated bots. F5 Shape shipping customers offer an API for these sorts of queries, but not everyone wants to register or follow the rules associated with the API. For this reason, F5 Shape still sees significant unwanted automation on these sorts of applications. It's not always malicious, but it's a nuisance typically caused by competitors or other third parties.



Contact form vulnerable to automation

It's not common but some F5 Shape customers experience significant spikes of automation on forms like these. Sometimes it's a competitor or disgruntled employee just trying to be a nuisance.

Let's Start a Conversation

Name *

Company

Email *

Title

Phone

Message *

SEND

Dark web contains 700+ passwords for 619 users @acmegrp

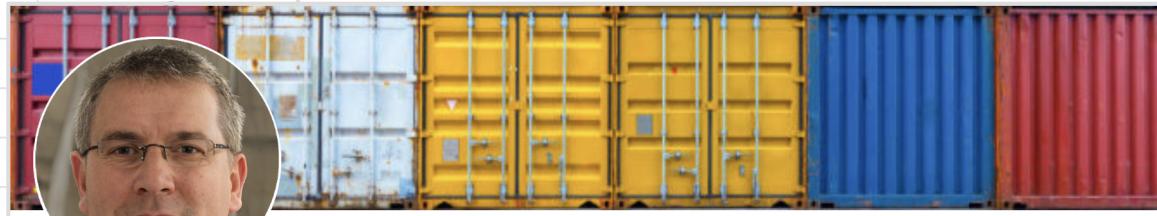
This does NOT typically indicate a compromise at Acme Group. More often, Acme Group employees used their work email address to register at some other website, such as LinkedIn, and then that company was compromised.

A lot of dark web data are old and stale but F5 Shape recommends these accounts be reset out of an abundance of caution. Please email d.woods@f5.com for a .csv of the entire list.

count	username	password	times_seen
1	jms	w*****t	3
2	ewilliams	r*****d	3
3	gbrown	M*****2	4
4	lbayles	l*****1	2
5	pmortenson	t*****3	1
6	tgunter	l*****4	3
7	rconner	K***h	2
8	mvangorp	G*****m	6
9	mvangorp	p*****r	2
10	bbrockman	i*****l	2

While likely old and stale, some appear to match current staff

count	username	password	times_seen
1	jms	w*****t	3
2	ewilliams	r*****d	3
3	gbrown	M*****2	4
4	lbayles	*****1	
5	pmortenson	t*****3	
6	tgunter	*****4	
7	rconner	K****h	
8	mvangorp	G*****m	
9	mvangorp	p*****r	
10	bbrockman	j*****j	



Peter Mortenson

Accounts Payable at Acme Group
International
Chicago, Illinois, United States - [Contact info](#)



General Dynamics
243,469 followers

500+ connections

[Connect](#)

[Message](#)

[More](#)

Conclusion

- Several applications at your company are inherently vulnerable to attack or abuse.
- F5 Shape can give your company the visibility it needs to determine if the applications are actually under attack (just because they're vulnerable doesn't mean they're under attack right now).
- If they are under attack, or ever become under attack in the future, F5 Shape can protect your company, its staff, its agents and its brand and reputation.

F5 Shape offers an outcome as a fully managed service. We use client-side web and mobile signals, and human-supported AI/ML, to detect and prevent malicious or other unwanted traffic.

F5 Shape Offers Real-Time Protection

F5 Shape's platform safeguards the world's largest brands, protecting billions of accounts and transactions every day



F5 Shape makes it possible to stop malicious automated attacks, identify fraudulent human activity, and reward legitimate users—all in real time. Interested in seeing Shape's defense in action? Visit www.f5.com/products/security/shape-security

Prevent Attacks That Start with Bots and Evolve into Fraud

BOT DEFENSE

Prevent sophisticated, human-emulating automation and retooling

AUTHENTICATION INTELLIGENCE

Securely reduce friction to improve customer experience

ACCOUNT PROTECTION

Monitor every transaction for signs of fraud or risky behavior

DEPLOY TO FIT YOUR NEEDS

F5 Shape fits into your existing infrastructure