SHAPE SECURITY PREDICTIONS 2020

Key Predictions for App Security and Fraud for the New Year

Michael Plante
VP Marketing, Shape Security

January 2020
Welcome to the App Security and Fraud Summit

✓ Industry’s first virtual summit dedicated to protecting the critical web and mobile applications that power our modern economy

✓ Seven sessions throughout today

✓ Sign up to attend additional sessions live today or on demand
About Shape Security
Now part of F5

- World leader in fraud and abuse protection for web and mobile applications
- Advanced defenses against credential stuffing, account creation fraud and other types of automation attacks covered by the OWASP Automated Threats Handbook
- Also defenses against manual fraud attacks, Magecart-style attacks, aggressive aggregators, etc.
- Shape’s defenses mitigate more than a billion application attacks per day
- Joined forces with F5 on January 24
Four Megatrends Underpinning our 2020 Predictions

● Accelerating digital transformation continues to move more workloads – and value – to the cloud
  ○ Makes applications the most lucrative targets for cybercriminals, aggressive nation states and other bad actors

● Continued acceleration in spilled or stolen credentials
  ○ Continuous, fresh ammunition for larger, more varied attacks

● Continued escalation in attacker sophistication to sneak past web and mobile application defenses

● Continued creativity in devising new ways to monetize attacks
2020 PREDICTION #1:
The Criminal Weaponization of AI
We predict that during 2020, we'll see the first attack framework and/or botnet that leverages trained AI models to bypass risk-based authentication.

✓ Natural evolution of continued criminal pursuit to replicate organic human traffic

✓ Rules- or signature-based technologies will prove increasingly insufficient against weaponized AI

✓ Fight AI with big data, ML and AI
2020 PREDICTION #2: B2B Sites Get Credential-Stuffed
In 2020, we predict the first publicly announced major credential stuffing attack of a popular B2B application, potentially in the CRM, HRM or financial applications space.

✓ Likely already happening
✓ Different actors (nation state actors, corporate competitors, criminal ransomware attacks)
✓ Different motivations
✓ Business does not need to be breached to be attacked
✓ Discuss with your B2B application providers
2020 PREDICTION #3: Automated Extortionware Attacks
We predict that during 2020, we'll see the first general purpose, automated extortionware that takes over social accounts using credential stuffing or similar brute force attacks to extort money from victims.

✓ Similar to traditional ransomware-style attacks, but scaled up with automated credential stuffing or similar brute force attack types (instead of spearphishing and/or malware-centric approaches)

✓ Brands could be impacted by

✓ Reputational damage
✓ Consumer re-assessment of social media consumption
✓ Disruption to advertising and influencer business models
2020 PREDICTION #4:
Attack Once, Steal From Many
A major infrastructure provider will be breached through automation attacks or Magecart-style attacks, exposing hundreds of brands.

- As attackers move down-market, they are looking for right-sized attacker economics.
- Instead of devising brand-specific attacks, we believe attackers will concentrate on figuring out how to attack multiple mid-market brands in a category through a common infrastructure provider.
- Have discussions with your infrastructure provider: “How are you preparing for these types of attacks?”
2020 PREDICTION #5:
Brute Force Automation Attacks on Critical Infrastructure
We’ll see our first major reported nation state attack using credential stuffing against critical infrastructure (e.g., utilities, telecomms network, transportation network, etc.)

✓ Same brute-force automation attacks that we’re seeing against large B2C brands, but deployed by nation-state and cyberterrorist actors against critical infrastructure targets

✓ Goal of gain access into or control over OT systems to disrupt or damage critical infrastructure
2020 PREDICTIONS:

Additional Predictions
Additional 2020 Predictions

- Brute Force Attacks Break into the Smart Home
- “Mrs. Jones, We’ve Already Received Your Vote”
- Introducing “CoT” (Credential Stuffing of Things)
- Cracked Access through Aggregators
THANK YOU

shapeseecurity.com