THREATX

WHAT LIES BENEATH

What You Need to Know About the Modern Threat Landscape

In recent years, the threat landscape has undergone a transformation in terms of sophistication, diversity, and sheer volume of attacks.

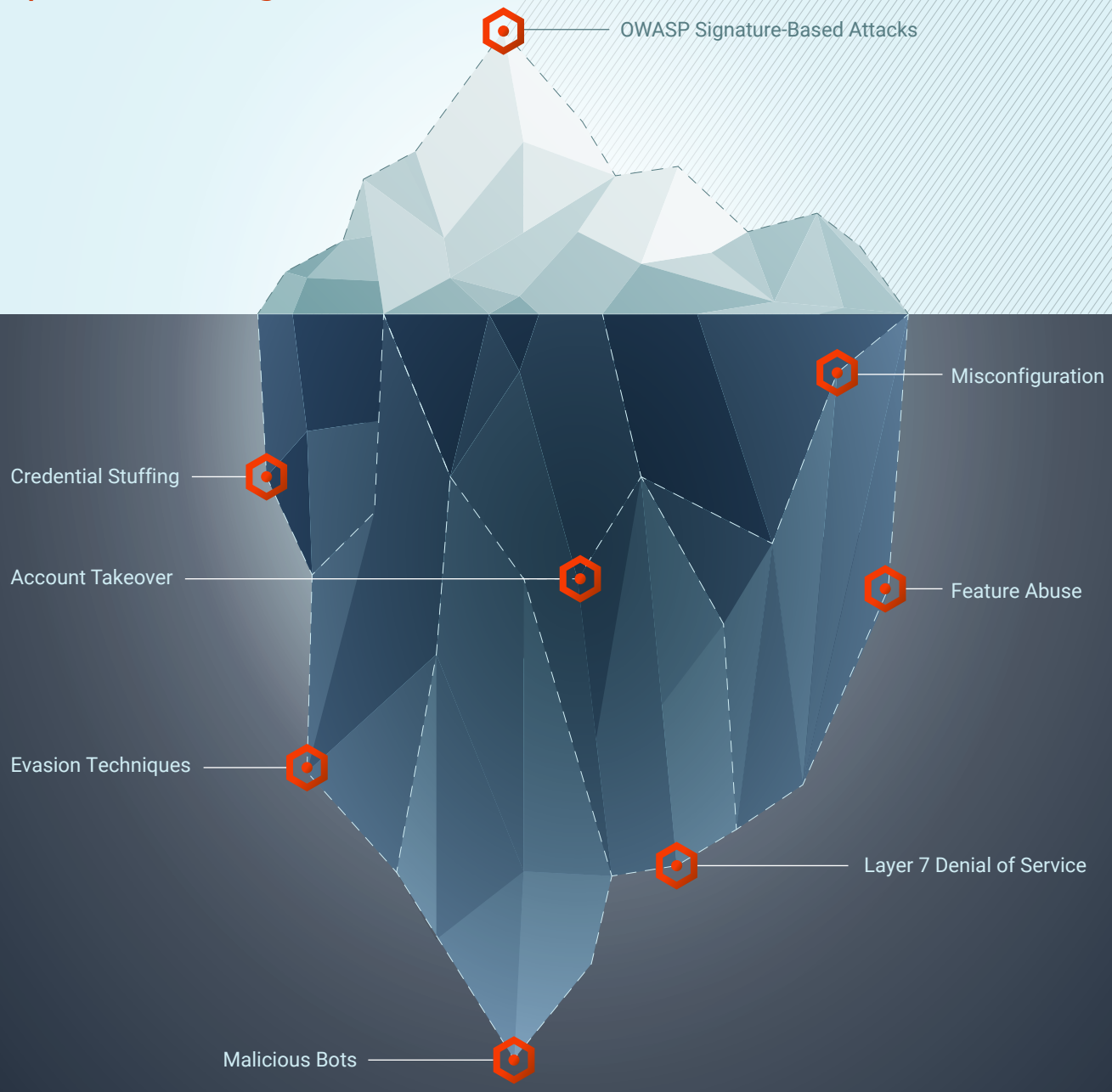
Contemporary attackers are patient. Attacks are developed over time and employ a wide array of innocuous-seeming tactics. They further mask their intention with evasion techniques to avoid detection by traditional security trip-wires. Bots are used for reconnaissance and exploitation. Automated attack platforms imitate legitimate users and, in so doing, abuse and exploit legitimate application functionality. DDoS attacks can be large-scale, volumetric attacks, or they can precisely target critical application-level functions via publicly exposed APIs.

Think of this new threat landscape like thieves who, rather than simply brute-forcing their way into your house by breaking down your front door, instead test the defenses of your house in more subtle ways — over days or months. They observe your house for a while, they check if the front door is unlocked one day, check if there's a window unlocked another day, and try the garage a week later. Using the information gathered from all these attempts, they create the best plan of attack. You're less likely to notice these recon and information gathering activities — until the attack comes together. And then, it's too late. Focusing on hardening your front door, you don't notice the person across the street watching your house.

Similarly, the modern threat landscape features long-term, low-and-slow attack patterns. But security solutions haven't kept up with this evolving landscape. Most legacy web application firewalls (WAFs) look at individual ingress transactions and make crude, simple decisions: good traffic or bad traffic. They look at each inbound request and try to match it to a known signature. For instance, most OWASP types of signatures are looking for an exact expression match within a request — and it either matches or it doesn't. But with a multi-step, automated attack, it's difficult to detect and block the right ones without causing false positives or writing hundreds, sometimes thousands of rules.

And even with sophisticated solutions that look at more nuanced risk-signals, attackers understand how to live off the land and stay below the threshold of detection as they perform their surveillance and reconnaissance.

Your legacy WAF was designed for the easy-to-spot, tip-of-the-iceberg attacks.



It was not designed for the multitude of less-obvious attacks working together beneath the surface to create a Titanic-sized problem.

1

Credential Stuffing

You need passwords for your online banking, your grocery store app, your social media accounts, your email … the list goes on.

Inevitably, you struggle to remember them all, so you start using the same password over and over. Or maybe you cycle through a few easy-to-remember passwords, or worse, you enumerate, adding first a 1, then a 2 … and thus, credential stuffing attacks are born. This attack type uses credentials that were stolen in a prior breach. The attackers buy and sell databases of compromised, legitimate credentials, along with every password ever associated with those credentials.

Attack-bots attempt to log into an application by cycling through all combinations of these legitimate login credentials. To evade detection, the attackers will often try one username/password combination, then move on to another pair. To block this kind of attack, security teams need the ability to see very subtle differences between legitimate and nefarious behavior. This attack type is becoming more common, more sophisticated, and more successful.

Fraud ring *Proxy Phantom* recently used over **1.5 million sets of stolen account credentials in automated credential stuffing attacks** against online merchants.

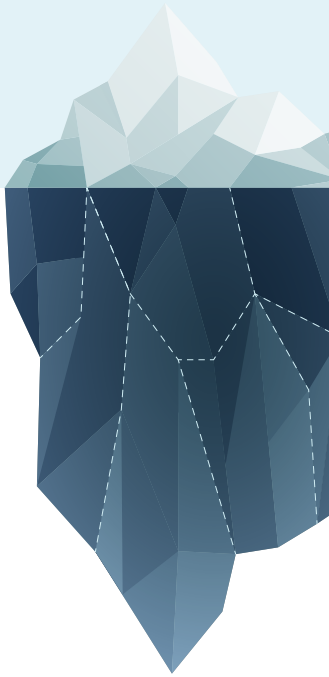
2

Account Takeover

Arkose Labs detected a **90 percent rise in account takeover attempts** on its network in the last quarter of 2020 alone.

This attack type includes activities like credential stuffing, brute force, or password spraying.

Attackers might know or guess that every application server from Company X has a specific password as the default, or they might guess a few common default passwords, like password1@. If they get blocked after five attempts in 10 seconds, they'll try four attempts in 10 seconds, or they'll distribute the guesses across multiple IPs, and so on and so on through an increasingly sophisticated and clever bag of tricks. Once they get a match and have access, attackers will go for the kill shot, initiating privilege escalation, or changing a real user's passwords.



3

Evasion Techniques

Attackers today will expect some level of inspection from the defense, and will therefore often use evasion techniques to disguise or redirect attention from their attacks.

A simple form of evasion employs an anonymizer to mask the location of the attacker. However, anonymizers are relatively easy to detect, so attackers often attempt to impersonate a legitimate user with false user agent information. A simple example would be a Russian attacker spoofing a location to appear to come from the US. Simple enough, but once malicious activity is detected, most solutions will block or flag the IP. Therefore, the attacker will use multiple IPs and vary multiple elements of the request identifiers to attempt to evade detection and learn defense thresholds. Another insidious attack type includes TLS spoofing. A compromised server certificate may allow the attacker to spoof the target site or mount a man-in-the-middle attack.

Ultimately, most modern attackers combine numerous evasion techniques with various attack types, making it nearly impossible for a signature-based solution to identify every combination.

A Magecart attack will often employ man-in-the-middle techniques to **skim personal information including credit card numbers or other financial information.**

LexisNexis Risk Solutions has found that **bot attacks continue to explode in 2021,** growing by 41% in the first half of the year.

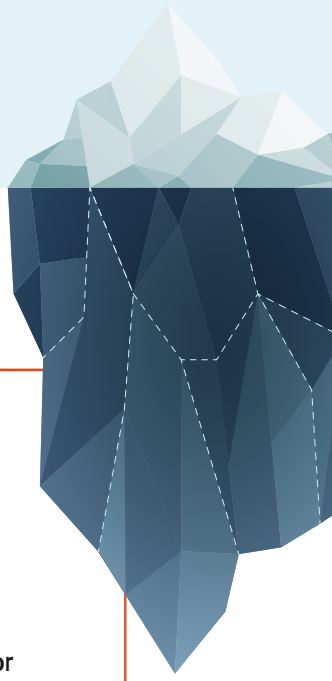
4

Malicious Bots

Attackers are now making many of the attack types listed here more effective and more dangerous by using botnets.

With botnets, an attacker could use multiple IPs (sometimes tens of thousands), making the attack that much harder to identify. Attackers use bots for everything from general scanning and reconnaissance to attacks like scraping proprietary pricing information from web storefronts. The challenge with mitigating bot traffic is that not all bots are malicious (think search engine spiders). Coarse-grained bot mitigation efforts can disrupt or degrade legitimate user experience. It's long been known that the use of CAPTCHA to identify humans vs. bots leads to a sub-optimal customer experience.

Advanced bots may also use headless browsers or impersonate legitimate users, which can easily defeat user-agent based detection and fool WAFs and web applications into thinking the attacking bots are, in fact, a normal human user.



5

Layer 7 Denial of Service

These attacks often attempt to disrupt an application by exploiting standard services provided by websites.

They rely on a wide variety of amplification techniques to drive massive amounts of traffic to a target application and consume vital application and server resources. After finding the longest-running query in the application, the attackers then spray legitimate calls at that service. Because the application is now spending all its time and resources trying to respond to those legitimate-looking calls, it will eventually become overwhelmed. These attacks can be especially difficult to defend against because they are abusing legitimate application functionality.

In the first half of 2021, cybercriminals launched approximately 5.4 million DDoS attacks, representing an 11 percent increase over the same period in 2020.

6

Feature Abuse

Like DDoS attacks, feature abuse involves identifying components of a web application or API that can be expensive from a performance or availability perspective.

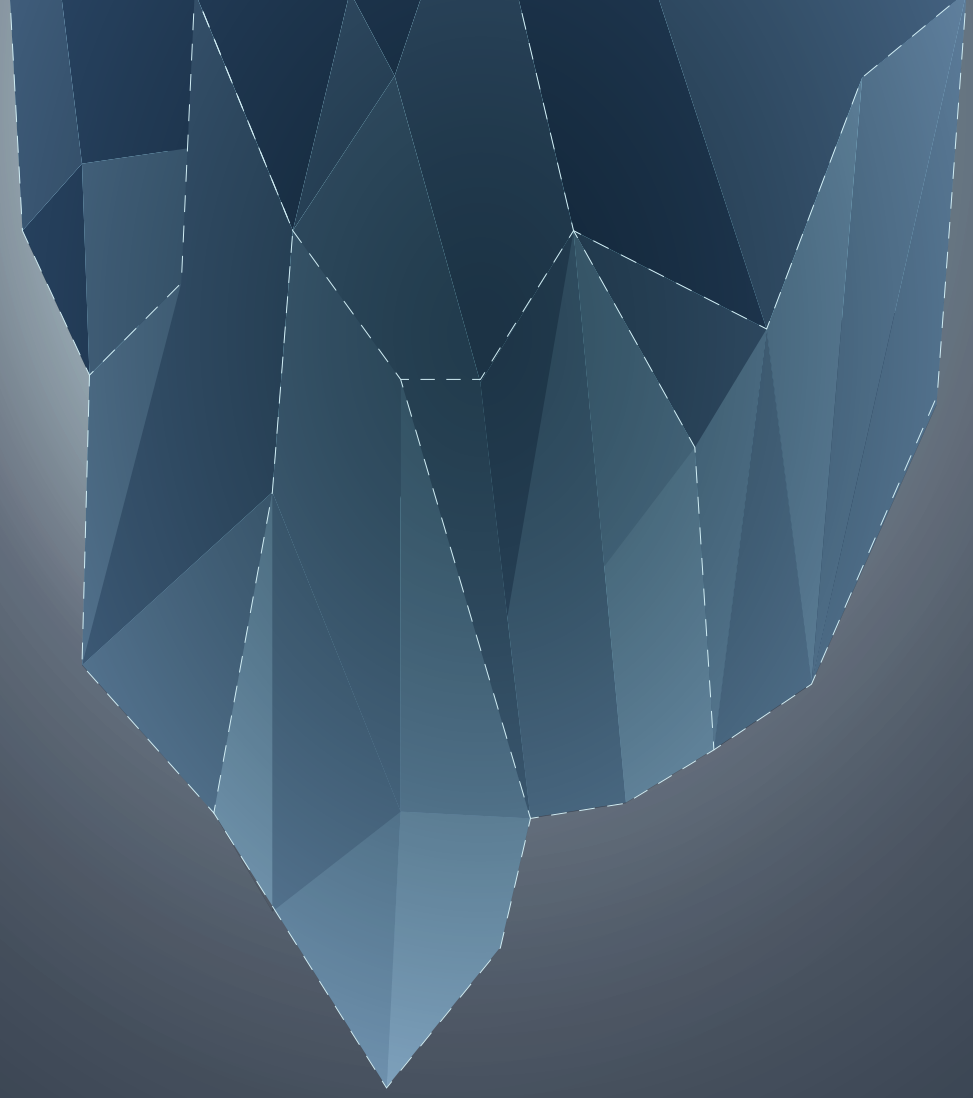
Authentication functionality is a common target of feature abuse. An attacker might engage the authorization service, which will then wait for a user input response, but the attackers don't respond, but instead load it up again with thousands of similar calls. The end result is an application with thousands of open sessions doing nothing, without the ability to open any new sessions.

7

Misconfiguration

A security misconfiguration is any failure to correctly implement industry-standard security controls for a server or web application.

Updating servers, patching vulnerabilities, and ensuring all applications and endpoints are secured can be a full-time job; and attackers know security teams are stretched thin. To exploit this weakness, attackers are constantly probing web applications and APIs to detect potential vulnerabilities or technology stacks particularly suited to specific attacks. And to make matters worse, known vulnerabilities are often disclosed with programmatic cookbooks for exploiting the unpatched vulnerability.



The threat landscape is an iceberg, vast and vexing.

Most of its danger lies below the waterline, and the attacks listed here are just a few examples. Your security solution needs to do more than identify explicit, known bad IP addresses. It needs to identify a combination of moderately suspicious behaviors — helping you steer a course through a cold and hostile sea of risk.

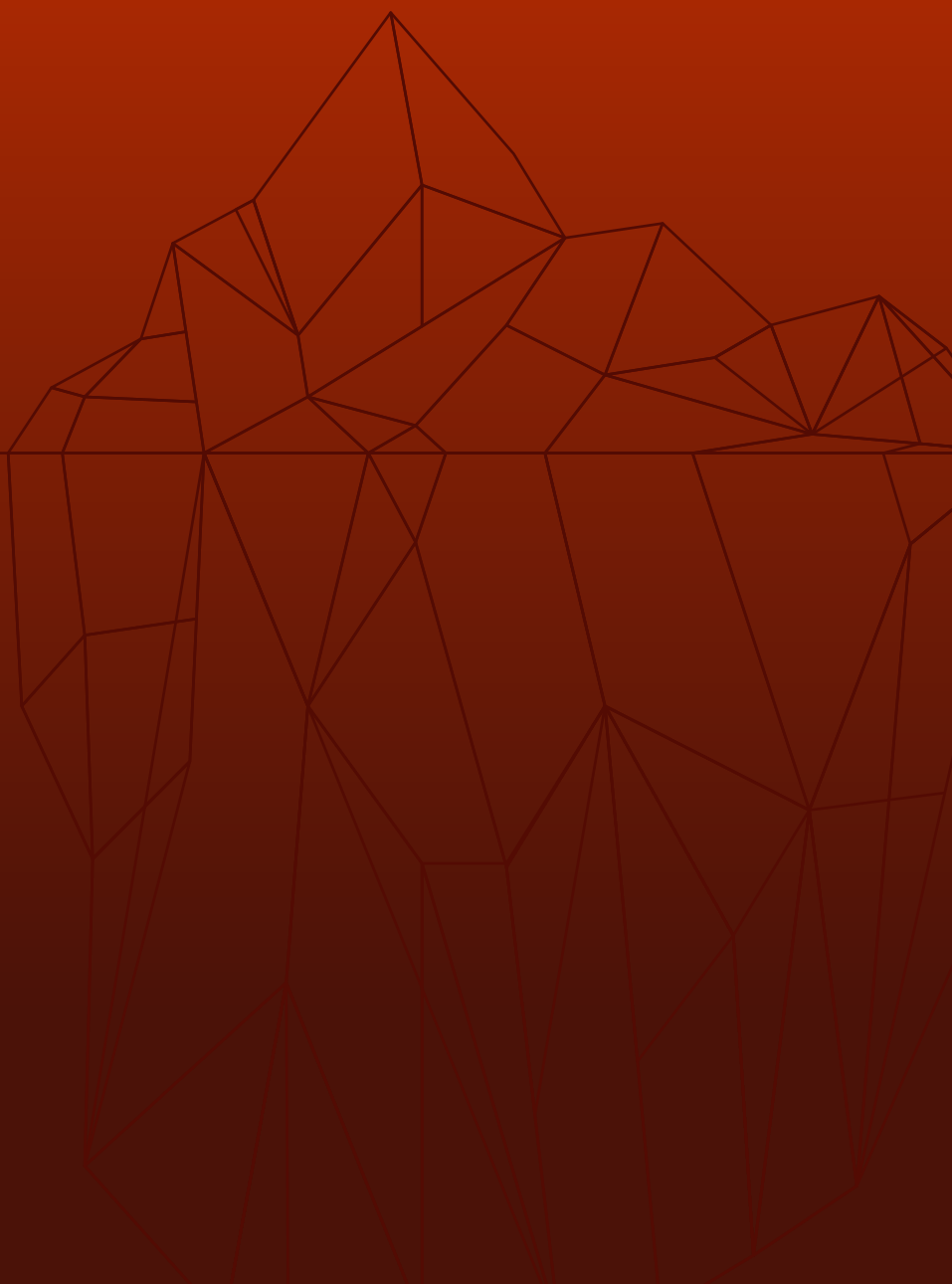
AVOID THE ICEBERG. LET US HELP.

Get details on how our entity and behavior analytics can track and block modern threats.

Learn more, ask questions, and see our solution in action by requesting a demo today.

THREATX

www.threatx.com
info@threatx.com



ABOUT THREATX

ThreatX's web application and API protection (WAAP) platform makes the world safer by protecting web applications and APIs from all threats, including DDoS attempts, BOT attacks, API abuse, exploitations of known vulnerabilities, and zero-day attacks. Its multi-layered detection capabilities accurately identify malicious actors and dynamically initiate appropriate action. ThreatX effectively and efficiently protects web applications and APIs for companies in every industry across the globe. For more information, visit: www.threatx.com