info@Horizon3.ai
www.Horizon3.ai
LinkedIn: Horizon3.ai
Twitter: @Horizon3ai

"Attackers don't hack in…they log in."

While defending Air Force networks, we'd be assessed by a Department of Defense (DoD) group with a congressional mandate to report back on the cybersecurity state of our unclassified and classified networks.

They would cordially coordinate with us, then bring in an Aggressor Squadron or NSA Red Team…and pwn us. Always. They'd harvest a credential from an Airman at some other base in a different operation, use it to log in, land, expand, and tell us about it later.

Why?

Because they could. It was easier than employing a zero day Remove Code Execution (RCE). Their approach to testing our ability to defend against a malicious adversary was aggravating. We called them cheaters.

Why?

Because we spent millions in malware signature detection and sandbox execution, endpoint detection, threat indicators, vulnerability assessments and scans, proxies and firewalls…but none of these is useful for recognizing compromised credentials attacks.

Why?

Excuses ranged from "that's a security training issue" to "that's a personal hygiene issue" to "that's a policy issue" to "that's an IT problem, not ops" to "that's an ops problem, not IT" to "You want me to make the Colonel get a new credential? Are you crazy?" to "No. That'll kill real operations." We'd even enable special password policy exceptions for senior leaders and operations floors—our most sought after targets!

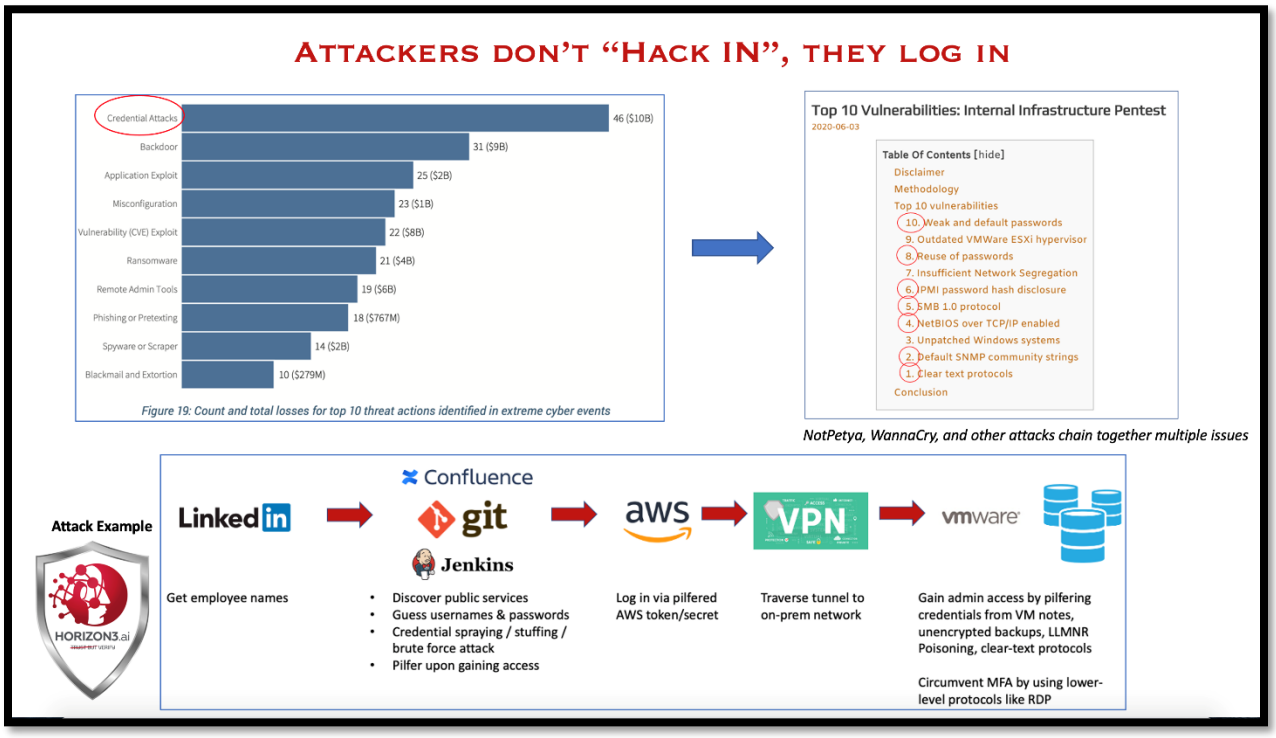
The Password Pandemic

We now exist in a world of ignored credential proliferation, and we're paying the price.

- The 2020 Verizon Data Breach Investigation Report claims over 80% of hacking-related data breaches involve brute force or the use of lost, stolen, or compromised passwords
- The FBI reported in a private industry notification that 41% of financial sector cyber attacks employ Credential Stuffing, which accounted for the greatest volume of security incidents against the financial sector in the past three years
- Crowdstrike's 2020 Global Threat Report identifies a continuing trend from malware to malware-free attacks, now 51% of attacks identified…which are incredibly difficult to identify and intercept reliably; additionally, they frequently observed adversaries using valid account credentials across an attack lifecycle, and identified credential dumping as one of the most prevalent techniques used
- Gartner estimates that through 2025, 99 percent of cloud security failures will be due to misconfigurations that expose passwords

- Varonis identified 61% of companies have over 500 accounts with non-expiring passwords.
- A Carnegie Mellon University study found that only one-third of users change their passwords following a data breach announcement
- Have I Been Pwned lists over 10 billion account details and over 600 million passwords from known breaches
- The estimated number of passwords used by humans and machines worldwide is growing past 300 billion in 2020

A $10 Billion Price Tag



Credential attacks are not detected by vulnerability scanners, endpoint detection, SOAR, SIEM, BAS tools, nor most penetration tests. These types of attacks led to the most financial damage, a little over $10B over the past 5 years:

- Not Petya ransomware uses credential access to spread without human intervention. Upon infection, it drops a credential theft module that extracts credentials on infected computers. It then uses the harvested credentials to connect and automatically spread to other computers across the network.
- Hackers obtained login credentials of two Marriott International employees and were then able to steal 5.2 million customers' records from the company's loyalty program.
- With COVID-19 forcing people to work from home, video collaboration application stocks—like Zoom—have risen, both on Wall Street and the Dark Web. Such applications have been relentlessly targeted by several cyberattacks, and once breached, hundreds of thousands of passwords, login credentials, personal meeting URLs and HostKeys were stolen and available for sale or for free across dark web forums.

For all intents and purposes, an attacker using credentials looks like a legitimate user. Coupled with the absence of malware, this type of attack is extremely difficult to detect. This is why ZeroTrust and

BeyondCorp are such popular security models right now; both are an attempt to limit the blast radius of a compromised credential.

This matters even more now, because 51% of people use the same passwords for both work and personal accounts and 39% of accounts use passwords which NEVER expire. In the Zoom attack, it is believed that attackers were able to use old stolen credentials, some from 2013, and compromised passwords from other accounts—i.e., credential stuffing. The ripple effects of these poor practices and policies carries into not just a personal account, but back to our work and the companies themselves.

More frustrating now is that attackers who employ credential stealing tools aren't going after organizations who spend millions on cybersecurity...but the much weaker and more vulnerable and most valuable: hospitals and schools.

Horizon 3 AI has seen this and--as a rainbow team--employed this attack path tactic with incredible success to help companies, hospitals and schools start fixing what matters.

Why? Because this matters.

Horizon 3 AI's 2020 Results

Horizon 3 AI's own 2020 results bear this data out. In hundreds of rainbow operations this past year, across financial, medical, manufacturing, consulting, and even cloud-native big data industries, we found and verified weak and default credentials to lead our Top 10 list—by far. If we account for the sheer number of weak or default credentials found:

- Each of the bold items in our Top 10 list are credential issues—the Top 4!
- Approximately 100 credentials per operation were exploitable across all industries and environments.
- On average, 1 out of every 8 hosts was associated with a weak or default credential
- 80% of those credentials led to critical resources & data
- In fact, 65% of the weaknesses Horizon 3 AI found and verified were security misconfigurations, including credentialed access
- 1/3 of all credentialed access was exploited through factory default credentials
- Several factory defaults are "anonymous" logon, meaning no logon or password required

Rank	Weakness	ID
1	**Weak or Default Credentials**	**H3-2020-0014**
2	**Fundamentally Insecure Protocols Detected**	**H3-2020-0018**
3	**Anonymous Access to Printer using PJL or PS**	**H3-2020-0003**
4	**Anonymous FTP Enabled**	**H3-2020-0005**
5	OpenSSL Lucky 13 Vulnerability	CVE-2013-0169
6	**LDAP Null Bind Allowed**	**H3-2020-0006**
7	**SMB Null Bind Allowed**	**H3-2020-0007**
8	Guest Account Enabled	H3-2020-0008
9	SSL Beast Vulnerability	CVE-2011-3389
10	Breach Attack Vulnerability	CVE-2013-3587

~~TRUST BUT~~ VERIFY

Why We Win

Being vulnerable doesn't mean you are exploitable. That's why Horizon 3 AI focuses on attack vectors, chaining techniques an attacker uses with harvested credentials, technical misconfigurations, and exploitable software vulnerabilities—regardless of CVSS score—and operationally context-scores the results based on an attacker's perspective of your environment.

And we prove it.

- By using lower-level protocols like RDP and SMB, Horizon 3 AI shows how an attacker can manipulate guest access or circumvent multi-factor authentication services you've enabled, and we show you have to remediate such attack vectors.
- Horizon 3 AI shows how user credentials are harvested via LinkedIn and then stuffed or password sprayed to gain initial access.
- From brute force to hash cracking, Horizon 3 AI leverages the tactics and tools attackers use to show you where you are exploitable, so you can fix what matters.

In 2 hours, Horizon 3 AI's automated AI-driven Node Zero recon'd a mid-size environment for a FinTech company and identified 2 SQL database default credentials which led to 13B+ sensitive records at risk, including accounts, cases, and business operations file structures.

We're able to quickly conduct a credential attack against your organization, talk through the findings, and help you identify critical weaknesses.

This is an actual timeline for our Deep Red Team executing a medical company op:
Wednesday 4:40 PM - Harvested ~800 names from LinkedIn
Wednesday 4:45 PM - Confirmed ~500 valid domain usernames using Kerbrute against the DC
Wednesday 4:50 PM - Attempted two password spray attacks, no success
Wednesday 5:50 PM - Attempted one password spray attack, compromised 8 users, waited one hour to avoid potential lockout
Wednesday 5:55 PM - Discovered there is no domain password lockout policy
Wednesday 6:00 PM - Attempted 20 more password spray attacks, compromised 6 more users

Horizon 3 AI confirmed administrator access to shares and a storage array, including "crown jewel" access which could lead to business IP data exposure, PII/PHI data leaks/infractions, ransomware risks, data destruction – all impacting reputation and revenue stream

RECOMMENDATION

Every CEO and CISO and MSSP needs to ask and answer: "Are we vulnerable to credential attacks compromising our business and brand?"

Then verify the answer. Horizon 3 AI can help.

Because if I appear legitimate, why would your defenses stop me?

Resource Links

https://securityboulevard.com/2020/09/the-pandemic-of-credential-based-cyberattacks/
https://www.zdnet.com/article/fbi-says-credential-stuffing-attacks-are-behind-some-recent-bank-hacks/
https://www.rangeforce.com/blog/10-ways-security-hackers-exploit-passwords-and-enterprise-credentials
https://www.crowdstrike.com/blog/adversary-credential-theft/
https://www.scmagazine.com/home/research/video-300-billion-passwords-by-2020-report-predicts/
https://www.varonis.com/2019-data-risk-report/
https://dataprot.net/statistics/password-statistics/
https://techcrunch.com/2018/10/05/california-passes-law-that-bans-default-passwords-in-connected-devices/
https://www.infosecmatter.com/top-10-vulnerabilities-internal-infrastructure-pentest/
https://blog.tbicom.com/biggest-cyber-attacks-of-2020

Horizon 3 AI focuses on attack vectors, chaining methods an attacker manipulates such as harvested credentials, tech misconfigurations, and exploitable software vulnerabilities and operationally context-scores the results based on an attacker's perspective of your environment. Bottom Line: this ain't some CVE scanner. This is an attacker's perspective of what's most valuable and vulnerable.