cybervergent

Breaking Down H1 Threats Like A Weight Loss Journey

INTRODUCTION

In the first half of 2024, as an organization, we did hit the gym pretty hard but not alone. Working out alongside over 100 organizations in the high-stakes world of payments and sensitive data, we focused on building their cyber resilience, helping them stay compliant and avoid getting knocked out by cyber threats.

Spotting the Weaknesses: Common Cyber Challenges

Like any good trainer, we identified common areas where organizations were struggling:

- **Outdated Equipment:** Legacy systems were holding many organizations back, making them easy targets for modern cyber threats.
- **Limited Resources:** Smaller organizations and even some larger ones were struggling to afford the right equipment (security tools) and trainers (skilled personnel) for a comprehensive workout.
- **Lack of Knowledge:** Many organizations were uninfomred about the latest fitness trends (security standards) like ISO 27001:2022, CBN Frameworks, and PCI DSS 4.0, leaving them vulnerable to injury (a data breach).
- **Human Error:** Even the best athletes make mistakes. Insufficient training led to avoidable errors, opening the door for cyber attackers.

We also noticed that certain industries faced specific challenges:

Healthcare:

Handling sensitive patient data while navigating complex systems is like juggling weights while on a balance beam.

Manufacturing:

Focusing on operational technology (OT) security without neglecting IT security is like neglecting your lower body while training for a marathon.

Education:

Limited budgets and resources often hinder their ability to invest in advanced security measures. This is akin to performing bicep curls with dumbbells made of feathers.

Retail:

Short-term gains often take priority over long-term security investments, like prioritizing quick fixes over a sustainable fitness plan

Despite facing a tough training regimen of challenges and obstacles, we've helped our clients level up and become certified fitness champions.

By equipping them with state of the art tools (top-tier gear), intensive security knowledge (expert coaching,) and strategic partnerships (a solid workout plan) ,we've boosted their overall strength and resilience. Clients have been crushing their fitness goals by:

The Cybervergent Difference: Your Personal Trainer

The Cybervergent digital trust platform has been a game-changer.

By automating routine tasks, we've freed up security teams to focus on more challenging activities like threat hunting. It's like having a personal trainer who handles the warm-up and stretches, allowing you to focus on building muscle

Looking Ahead: Building a Stronger You

Cybervergent is committed to being your long-term fitness partner.

We'll continue to develop innovative tools and provide expert guidance to help you navigate the ever-changing threat landscape.

Routine Workout

Cyber Threat Landscape: The Heavyweight Champion

In the past six months, the cybersecurity arena has been bulking up with threats, and we've seen gains in cyber-attacks that would make any bodybuilder jealous. Just like you can't skip leg day, we can't expect threat actors to take a rest day. Africa's been lifting some serious weight, with a 37% increase in cyber-attacks, averaging about 2,960 reps per organization weekly. Talk about a high-intensity interval training for our digital defenses!

Our Security Ops Team: The Ultimate Spotters

Our security operations team has been pumping iron 24/7, monitoring, detecting, and blocking threats like it's an endless CrossFit WOD. We've been crushing our PRs, identifying and squashing over 586,130 cyber threats. That's a 63% increase in events analyzed across client environments compared to Q1. We're not just maintaining our gains; we're bulking up our defenses across all sectors in Africa!

Malware Trends: The Heavyweight Division

According to Infosecurity Magazine, malware threats have been on a bulking cycle, up 30% compared to the same period last year. March to May saw these threats on a serious growth spurt, with May showing a 92% year-on-year increase. That's some serious muscle mass!

Let's break down these malware beasts:

- **SocGholish:**
  This sneaky trickster is like that guy at the gym who tries to sell you fake supplements. It uses social engineering to con users into downloading malicious files, often disguised as browser updates. Once it's in, it can deploy nasty stuff like Remote Access Trojans (RATs) and infostealers.
- **Scattered Spider (UNC3944):**
  This is the parkour expert of malware, bypassing MFA and infiltrating through cloud identities. It's all about that functional fitness, living off the land and moving through the entire enterprise ecosystem.

Rilide Stealer:

The pickpocket of the digital world, this one targets Chromium-based browsers. It's like that guy who steals your protein shake when you're not looking, snagging email credentials and crypto assets.

Vidar Infostealer:

This is the all-rounder at the gym, targeting everything from crypto wallets to web browsers and even 2FA apps on Windows. It's doing a full-body workout on your sensitive data.

In our client's digital gym, we've seen two main contenders dominating the floor:

XMRig: The Sneaky Powerlifter

This trojan is like that guy who looks legit but is actually on some questionable supplements. It often shows up disguised as an Adobe Flash Player update (which, by the way, is as outdated as using a Thighmaster). This bad boy hijacks your processing power to mine crypto, leaving your system gasping for air like it just did a set of burpees.

To defend against **XMRig,** we recommend:

- Keeping your software as up-to-date as your workout playlist.
- Using top-notch EDR solutions, like having a world-class personal trainer for your devices
- Educating your team on the risks, just like you'd warn them about bad form at the gym

Glupteba: The Stealthy Ninja

This malware is like that silent but deadly type at the gym. It sneaks in, looking all innocent, but before you know it, it's taken over your entire workout routine. Once it's installed, it's got more moves than a Zumba instructor, from stealing auth info to turning your system into a crypto mining slave.

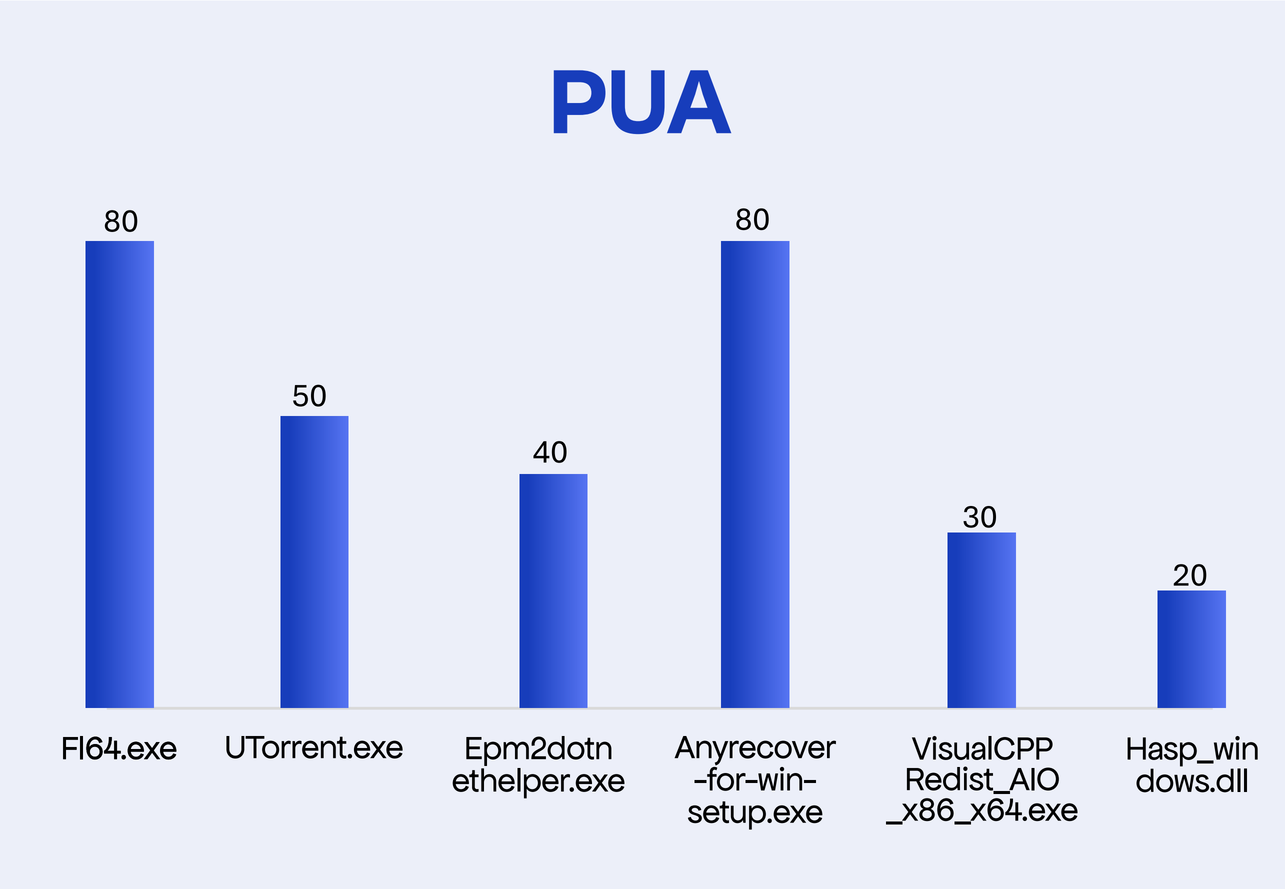
How it works: It installs itself like it's setting up a new piece of gym equipment, then uses HTTPS to communicate with its command servers, blending in with legit traffic like a chameleon on a treadmill.

To keep **Glupteba** out of your digital gym:

- Use URL filtering to block known bad sites, like putting “out of order”signs on sketchy gym equipment
- Scan downloads like you'd check your pre-workout for banned substances
- Train your team to spot these threats like they'd spot bad form
- Keep your systems patched and up-to-date, like maintaining your gym equipment
- Use solid endpoint security, like having a bouncer at the door of your digital gym

Potentially Unwanted Applications (PUAs): The Gym Leeches

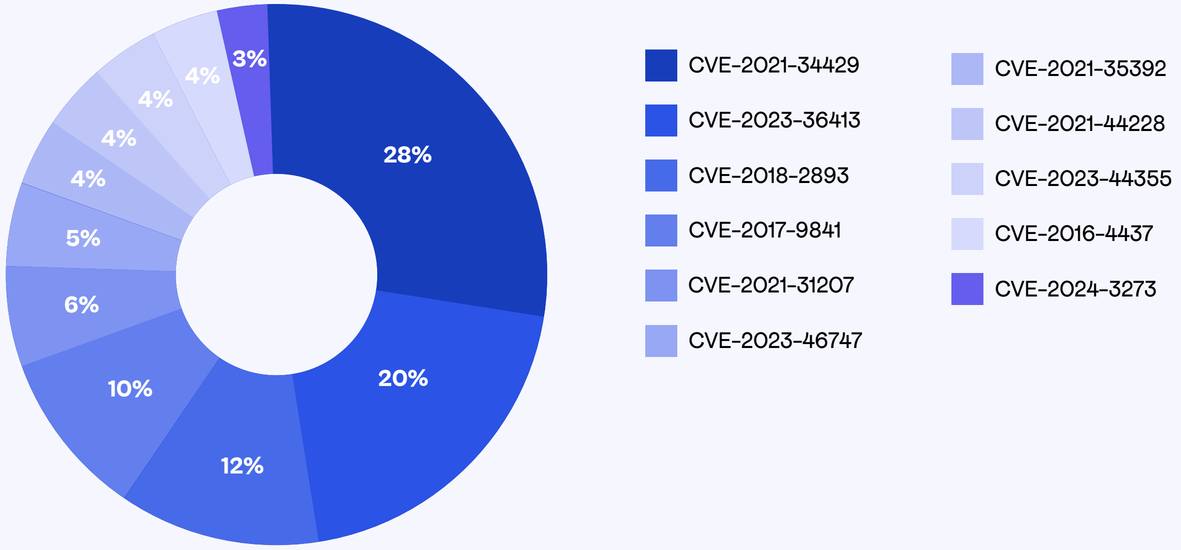
These are like those annoying people who hang around the gym without actually working out. They often come with free software, degrading your system's performance like that guy who doesn't wipe down the equipment after use.



Building on our earlier discussion, exploring another critical aspect of our cyber defense strategies is essential: understanding and mitigating known vulnerabilities. These CVEs are standardized, unique identifiers assigned to security vulnerabilities or exposures in software and hardware products.

Our team underscored various Common Vulnerabilities and Exposures (CVEs) that have emerged as prime targets for cybercriminals who aim to exploit weaknesses in various vulnerable web applications in our client environments.

This statistic shows commonly seen web application vulnerabilities that threat actors have attempted to exploit in our client's environment, which their CVEs represent. This statistic shows commonly seen web application vulnerabilities that threat actors have attempted to exploit in our client's environment, which are been represented by their CVEs.



This births the need for organizations to ensure regular application and systems updates are carried out on existing applications and systems to prevent these attacks at scale.

As we move forward, our Cyber Operations Center remains steadfast in its mission to anticipate, detect, and thwart evolving threats that seek to compromise the integrity of digital assets. With a deep understanding of the threat landscape and a relentless pursuit of innovative security solutions, we are poised to continue our unwavering defense of the financial sector and other industries' digital landscape, safeguarding organizations' trust and confidence in the face of ever-changing cybersecurity challenges.

Threat Details

Our security operations center (SOC) is like a personal trainer for your digital fitness. We've been closely monitoring cyber health by analyzing the sweat and grime—or rather, the alerts, events, and threat indicators—from hundreds of clients. Think of these clients as gym members with diverse fitness goals.

By studying their workout routines (IT environments) and injury reports (security incidents), we've identified the most common workout mistakes (cyber threats) and developed a personalized training plan (security recommendations) to help achieve fitness goals (a secure organization).

586,130
Total Threats Detected

19,920
Endpoints Protected

116,580
Detection Analytics Applied

42,200
Potentially Malicious Events Analyzed

226,103
Events Resolved by Automation

13,305
False positives identified by the platform and pared down

304,522
Events Analyzed by SOC Analysts

Let's pump up that cybersecurity game! In the first half of this year, the Cybervergent threat intelligence team spotted a massive bulk-up in credential leaks hitting the dark web like it's been on digital steroids. We've tracked down over 250 leaked employee and customer credentials from various organizations - that's some serious weight on the security bar!

It's like users are skipping leg day on their password routines, using the same credentials to bench press across multiple platforms. These commercial sites and sketchy watering holes are basically credential harvesting machines, and folks are falling for it harder than newbies on their first day at the gym.

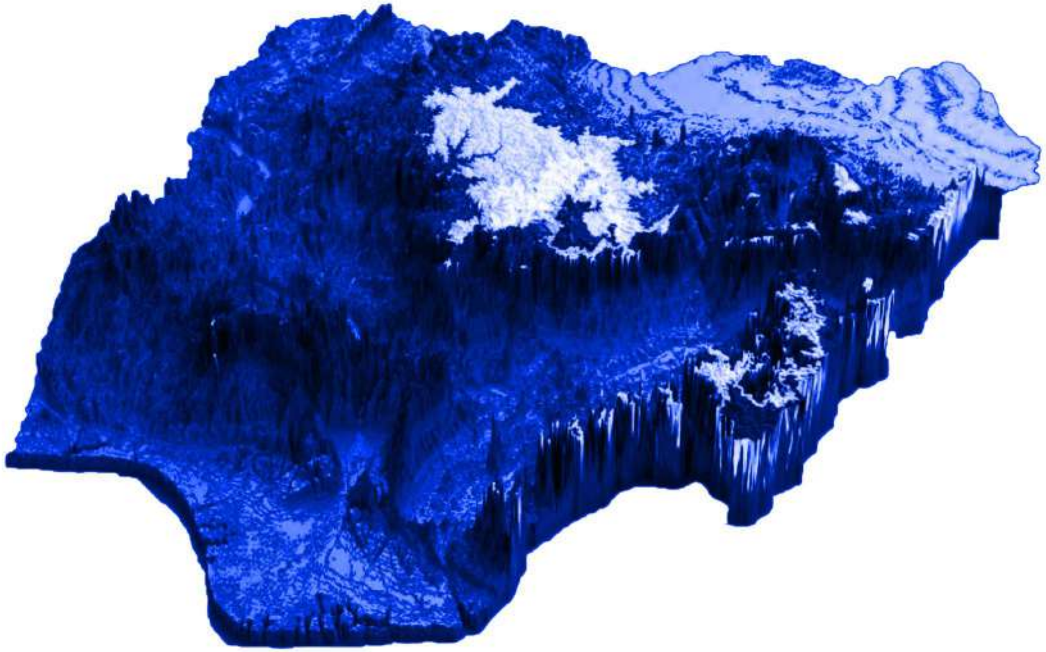
To spot our clients through these heavy lifts, we've been flexing our proactive muscles. Sometimes, we even carry out the cyber equivalent of buying protein shakes - strategically purchasing compromised accounts to keep our clients' gains protected.

Our brand protection monitoring is like having a personal trainer for your online reputation. We're keeping a hawk eye on those rogue actors trying to steal your identity gains. With our swift takedown moves, we've knocked out numerous impersonations attempts faster than you can say "burpee," keeping brand integrity and customer trust as solid as a six-pack.

We're also tackling those pesky rogue mobile apps - they're like those sketchy supplements that promise quick gains but end up wrecking your system. We're using our advanced detection techniques like a finely tuned fitness tracker, coordinating with app store providers to spot and remove these fraudulent apps before they can mess up anyone's digital health.

Think of our cybersecurity approach as your all-in-one gym membership. We're working every muscle group in the digital body, from cardio (constant monitoring) to strength training (security practices). We spot our clients during their toughest security squats and provide the warmup and cooldown routines to prep for and recover from cyber workout sessions.

Threat Actors That Targeted Nigeria In The First Half



The Nigerian digital landscape is exploding like a pre-workout protein shake – it's energetic, it's powerful, but it also requires the right supplements to avoid a crash. In this high-octane environment, cyber threats lurk like shadow boxers, waiting to land a knockout blow on your data and operations.

This report is your ultimate cyber-defense performance enhancer. Below we will identify the most aggressive threat actors that targeted Nigeria in H1 2024, providing battle-tested strategies to build your cyber resilience like iron. Forget generic gym routines – we're talking advanced techniques, threat intelligence on steroids, and the agility of a seasoned Muay Thai fighter.

Gelsemium

Description

Gelsemium is a sophisticated cyber espionage group known for its targeted attacks on high-profile organizations across various sectors.

The group has been active since at least 2014 and is known for its stealthy and persistent attack methods.

They use custom malware and advanced techniques to evade detection.

Targeted Sectors

- Public Administration
- Educational Services
- National Security and International Affairs
- Arts, Entertainment, and Recreation

Associated Malware/software

Cobalt Strike
Win.owlproxy
Gelsemium
STA-0046
SessionManager IIS

EQUATION GROUP

Description

Equation Group is a highly sophisticated cyber-attack group believed to be tied to the U.S. National Security Agency.

They are known for their advanced hacking techniques and long-term persistent attacks.

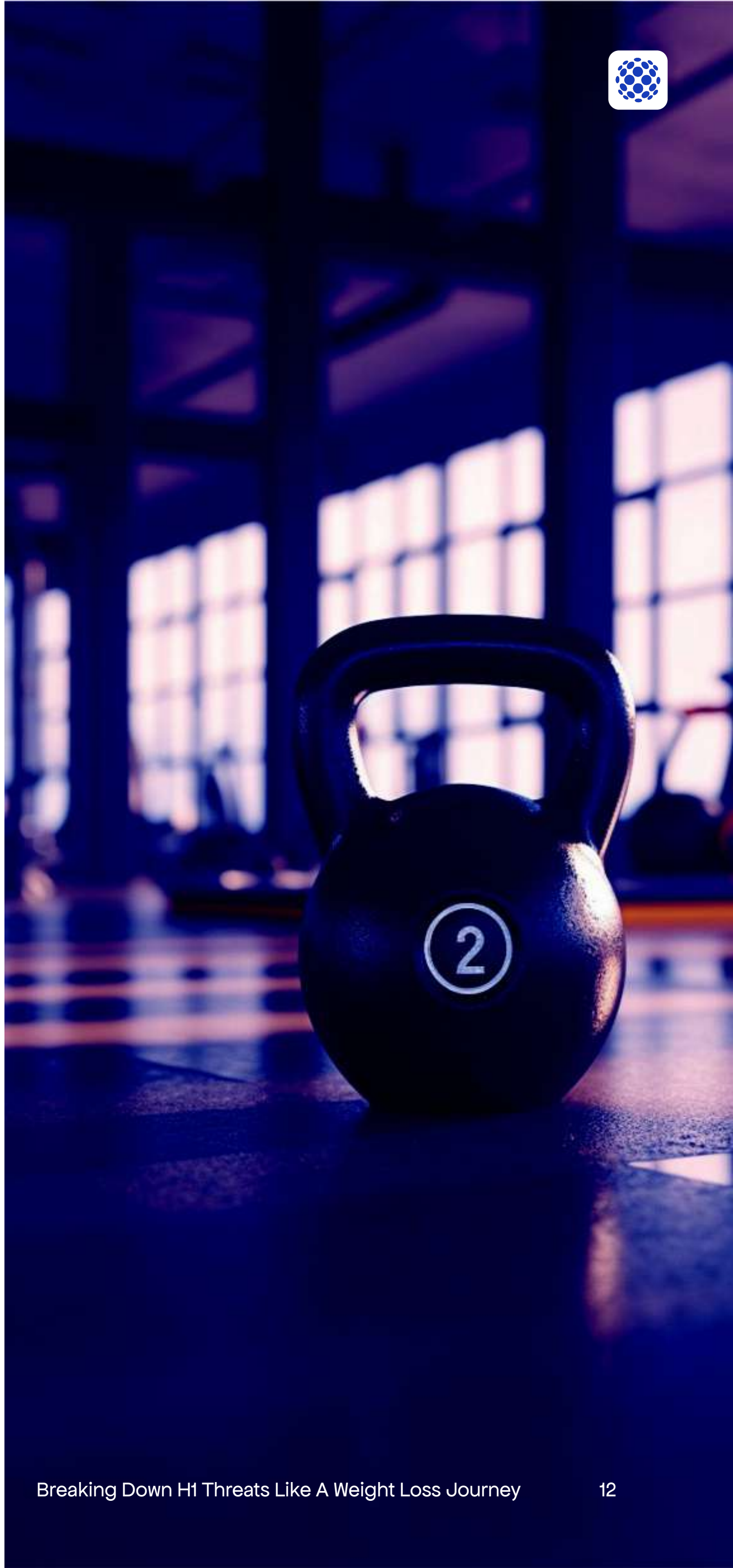
The group has been active since at least 2001 and has targeted numerous high-profile individuals and organizations.

Targeted Sectors

- Public Administration
- Educational Services
- Mining, Quarrying, and Oil and Gas Extraction
- Telecommunications

Associated Malware/software

win.fancyfilter
win.tildeb
win.doublefantasy
elf.vault8_hive
win.peddlecheap
win.oddjob
win.mistyveal
win.lambert



LYCEUM

Description

LYCEUM, also known as Hexane, is a cyber espionage group primarily targeting the energy and telecommunications sectors in the Middle East and Africa.

They employ a mix of spear-phishing, social engineering, and custom-built malware to infiltrate systems and exfiltrate sensitive data.

Their tactics include the use of backdoors and PowerShell scripts to maintain persistent access, often exploiting vulnerabilities in remote access services to gain initial entry.

Targeted Sectors

- Telecommunications
- Agriculture, Forestry, Fishing and Hunting
- Computer and Electronic Product Manufacturing
- Commercial Banking Finance and Insurance
- Professional, Scientific, and Technical Services
- Health Care and Social Assistance

Targeted Sectors

win.lyceum_http_backdoor_golang

win.lyceum_dns_backdoor_dotnet

win.lyceum_http_backdoor_dotnet

GAMAREDON

Description

Gamaredon, a cyber espionage group linked to Russian intelligence, has relentlessly targeted Ukrainian entities since 2013.

Employing a mix of phishing, malware, and social engineering, they focus on government and critical infrastructure.

Their toolkit includes custom-built malware and the exploitation of remote access services to maintain persistent access and exfiltrate sensitive data

Targeted Sectors

- Public Administration
- National Security and International Affairs

Targeted Sectors

elf.evilgnome
Win.pteranodonwin.
dilongtrash

CIRCUS SPIDER

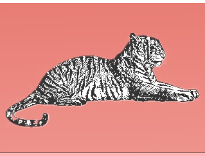
Description

CIRCUS SPIDER is a cybercrime group specializing in ransomware attacks against large enterprises. Operating as a Ransomware-as-a-Service (RaaS) since at least 2020, they employ a versatile toolkit including phishing, brute force, and custom ransomware.

Initial access is often gained through exploited RDP vulnerabilities. The group's rapid adaptation to new tactics poses a significant threat to businesses worldwide.

Targeted Sectors

- Utilities
- Manufacturing
- Transportation and Warehousing
- Educational Services
- Health Care and Social Assistance
- Public Administration



MIRAGE

Description

Mirage, a suspected Chinese state-sponsored group, specializes in cyber espionage targeting aerospace and defense sectors.

Known for advanced persistent threat (APT) operations, they employ custom malware, spear-phishing, and compromised websites to infiltrate their targets and steal sensitive information.

Targeted Sectors

- Air Transportation
- Manufacturing
- Public Administration
- Space Research and Technology
- Utilities
- Chemical Manufacturing (Chemical & Pharmaceutical Manufacturing)

Targeted Sectors

ipconfig
win.ketrican
win.ketrum
win.bs2005
win.mirage
netstat
win.plugx
apk.badbazaar Net
win.royalci
win.miragefox
spwebmember
Systeminfo

‹ ›

COMMON RAVEN

Description

Common Raven is a persistent threat actor targeting government and financial sectors. Operating since 2018, they specialize in covert operations using advanced malware and spear-phishing tactics.

Their ability to maintain long-term access and exploit zero-day vulnerabilities underscores their sophistication. Long-term surveillance on their targets.

Targeted Sectors

- Finance and Insurance
- Telecommunication

BRONZE HIGHLAND

Description

BRONZE HIGHLAND is a cyber threat actor known for conducting cyber espionage operations.

They are believed to be state-sponsored and primarily target organizations in specific regions for intelligence gathering.

Targeted Sectors

- Educational Services
- Other Services (except Public Administration)
- Public Administration

Telecommunications

Earth Krahang

Description

Earth Krahang is a cyber threat group originating from Southeast Asia, targeting organizations across the Asia-Pacific region since 2018.

Known for advanced phishing campaigns and exploitation of vulnerabilities, they've been implicated in numerous data breaches and espionage operations.

Their expertise in social engineering and custom malware development enables persistent access to compromised networks

Targeted Sectors

- Manufacturing
- Public Administration
- Educational Services
- National Security and International Affairs
- Telecommunication
- Retail Trade
  Finance and Insurance
- Health Care and Social Assistance

Targeted Sectors

The Insider Threat Syndrome: A Silent Assassin in the Cybersecurity Gym

In the high-octane world of cybersecurity, everyone's got their eyes on the flashy ring entrances – hackers with their zero-day exploits and cybercrime gangs throwing cyber punches. But lurking in the shadows, a more insidious threat warms up: the insider threat.

Often underestimated and underestimated, insider threats are like the silent assassins in the gym, packing a knockout punch despite always being overlooked.

In the first half of 2024 there has been a 50% increase in successful Insider threat attacks within Nigeria alone.

Why "Silent Assassin?" A Deceptive Advantage

Unlike external attackers who rely on fancy footwork and social engineering jabs, insider threats have a secret weapon – **trusted access**. They're already inside the gym, bypassing security ropes with their legitimate credentials. They know the routines, the weaknesses in the defenses, and can land a surprise blow before anyone notices.

The Knockout Punch: Real-World Impact in the Ring

While the numbers don't lie, recent incidents paint a brutal picture:

- **A recent study by IBM** revealed that insider threats are the heavyweight champions of cybercrime costs, averaging a global KO of $11.4 million per incident.
- **Just this July 2024, a disgruntled employee at a major cloud service provider** allegedly leaked confidential data and source code like a rogue weightlifter dropping weights on the competition. This disrupted operations and left the company with a reputation bruised and battered.
- **Earlier in April 2024, a healthcare organization got sucker-punched by a data breach** traced back to a healthcare worker who sold patient records on the dark web. These exposed thousands of individuals' sensitive medical information, leaving them vulnerable..

The Insider Threat Spectrum: Beyond the Disgruntled Employee

Here's a breakdown of the different types of insider threats lurking in the gym:

- **Disgruntled Employees:** Motivated by anger, financial gain, or a feeling of being benched, these individuals can inflict serious damage.
- **Accidental Insiders:** These are the athletes who forget their water bottles and leave the locker room door open – a simple mistake with potentially big consequences. They highlight the importance of solid security training programs.
- **Negligent Insiders:** These are the gym rats who forget their water bottles and leave the locker room door open – an employee working from a public space and leaving his/her laptop unlocked to dash to the restroom or pick a call ; a simple mistake with potentially big con sequences. They highlight the importance of solid security training programs.
- **Credential Compromise:** Insiders with compromised credentials, either through phishing scams or malware, become unwitting accomplices, letting attackers into the gym through the back door.
- **Industrial Espionage:** Competitors or foreign agents might try to recruit insiders to steal your intellectual property – like spying on your secret training techniques.

Combating the Silent Assassin: Building a Security Culture

Defending against insider threats requires a multi-layered approach, not just a single high kick. Here's how to build a strong defense:

- **The Principle of Least Privilege:** Give everyone only the access they need to perform their exercises, no more..
- **Continuous Security Awareness Training:** Train your team to spot suspicious activity – like someone trying to sneak into the restricted training area.
- **Data Loss Prevention (DLP) Solutions:** Think of these like security guards watching the exits, monitoring and stopping anyone trying to take unauthorized equipment (data) out of the gym.
- **User Activity Monitoring (UAM):** Keep an eye on everyone's training routines. UAM helps identify unusual behavior – like someone suddenly lifting weights they shouldn't be able to.
- **Exit Procedures:** Just like having a cool-down routine, have a clear exit process for departing employees and contractors. Revoke their access so they can't come back in and mess with the equipment.

> **The Insider Threat is Here to Stay**
>
> Don't underestimate the insider threat. They're not the underdog; they're a cunning opponent with the potential to land a devastating blow.

Cardio

In the first half of 2024, our cyber offense team put various digital infrastructure through an intense endurance test. We sprinted through over 50 different security obstacles, pushing the limits of internal networks, external-facing applications, and mobile platforms. Our goal: to outlast and outpace defenses and find weaknesses.

High-Intensity Interval Training (HIIT) Breakthroughs:

Unlike external attackers who rely on fancy footwork and social engineering jabs, insider threats have a secret weapon – **trusted access**. They're already inside the gym, bypassing security ropes with their legitimate credentials. They know the routines, the weaknesses in the defenses, and can land a surprise blow before anyone notices.

✓ Access Control Circuit Breaker:

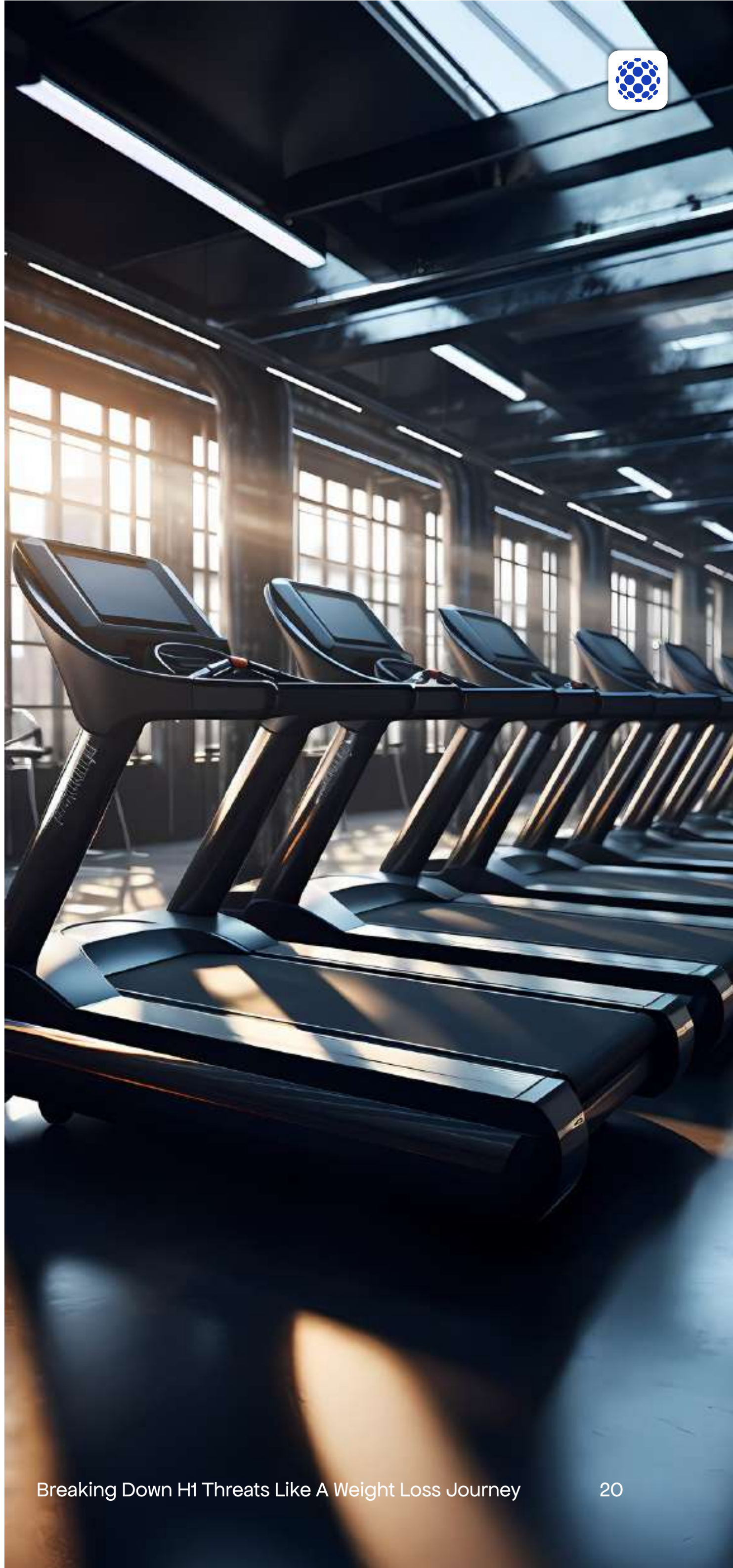
We found ways to leap over access control hurdles in external systems, potentially allowing us to sprint through restricted areas without breaking stride. On the mobile track, we discovered a shortcut that lets us adjust the digital pedometer, tricking the system into recording unauthorized laps.

✓ Recurring Moderate-Intensity Challenges:

Several mid-level hurdles kept appearing on our cyber track. Missing security headers were like finding gaps in the running fence - perfect for slipping through unnoticed. Lack of rate limiting on certain routes gave us unlimited sprints, letting us try different paces until we found the right rhythm to break through. Outdated components were like worn-out treadmills - easier to exploit and control the speed.

✓ Low-Impact but Useful Findings:

We noticed some easy jogs in our routine too. Improperly set cookies and missing email authentication records were like finding unlocked gates on the track - not a major breakthrough, but convenient for future runs.



Endurance Analysis:

The variety and frequency of these vulnerability assessments and penetration testing cardio opportunities suggest many organizations are skipping essential warm-ups in their security routines. Recurring issues with security headers and rate limiting are like leaving the gym door wide open - it's an invitation for uninvited runners.

High-risk vulnerabilities we found are equivalent to major gaps in a marathon's security perimeter. These could lead to significant breaches in the race's integrity if exploited.

The prevalence of outdated components is like finding sections of the track still using old, worn-out materials - much easier for us to sprint across without detection.

Cardio Enhancement Plan:

- **Interval Training Focus:** Prioritize exploiting high-risk vulnerabilities, as these offer the best " calorie burn" for our efforts.
- **Improve Running Techniques:** Refine our methods for bypassing security measures, making our sprints more efficient and harder to detect.
- **Track Scouting Schedule:** Regularly scan for outdated components, as these provide the easiest terrain for our cyber runs.
- **Core Authentication Challenges:** Develop new techniques to bypass multi-factor authentication, like training to jump higher hurdles.
- **Regular Endurance Tests:** Schedule frequent penetration tests to keep our cyber cardio team in top form.
- **Team Cross-Training:** Expand our skill set to cover a wider range of cyber terrains and obstacles.

Conclusion:

Our H1 2024 cyber cardio assessment shows we've got numerous opportunities to improve our endurance and speed in penetrating digital defenses. By focusing on these weak spots and continuously improving our techniques, we can enhance our ability to outpace and outlast cyber security measures. Let's lace up our digital running shoes and push our cyber cardio to the next level!

Remember, in the world of ethical hacking and cybersecurity testing, always ensure you have proper authorization before conducting any penetration tests or vulnerability assessments.

Hitting the Gym This Fall:
Cybersecurity Trends to Tackle in H2 2024

Forget the summer bod, it's time to bulk up your cybersecurity defenses! Here's a look at the top threats to watch out for in the second half of 2024, using our metaphorical gym analogy:

Zero-Day Exploits: Dodging Surprise Punches

Imagine a surprise attack in the ring – that's what zero-day exploits are like. Hackers exploit these unknown vulnerabilities before anyone can patch them, leaving your defenses wide open. Proactive vulnerability management is like scouting your opponent – identify weaknesses and fix them before they get exploited.

- **Statistic:**
  In the first half of 2024 alone, over 1,200 zero-day vulnerabilities were discovered across various software applications, according to a report by Cybersecurity firm RiskIQ. This represents a 25% increase compared to the same period in 2023.

- **Action:**
  Step up your vulnerability scanning and patching routine. Regularly assess your systems for weaknesses and prioritize fixing them before attackers land a knockout blow.

Cloud Security Focus: Securing Your Digital Locker

As everyone moves their data to the cloud (think of it as your digital locker), attacks on cloud infrastructure will get more complex. You need strong cloud security measures like encryption and access control protocols – like high-tech combo locks on your locker – to keep your data safe and meet compliance standards.

Incident:

In March 2024, a major cloud storage provider suffered a data breach due to a misconfigured cloud storage bucket. The exposed data belonged to millions of users, including sensitive information like social security numbers and credit card details.

Action:

Double-check your cloud security posture. Ensure proper encryption, access controls, and configuration settings are in place to protect your data from unauthorized access, even within the cloud environment.

Cybercrime-as-a-Service (CaaS): Fitness for All Threat Levels

Cybercrime is becoming a service, with easy-to-use tools available for even newbie attackers. This means more frequent and diverse attacks. It's like a one-size-fits-all workout plan for cybercriminals – they don't need to be experts to cause damage.

Statistic:

A recent report by McAfee suggests that the CaaS market is expected to reach a staggering $20 billion by 2025. This significant growth highlights the growing accessibility of cybercrime tools and the need for heightened vigilance.

Action:

Strengthen your perimeter defenses. Implement firewalls, intrusion detection systems, and other security measures to make it harder for attackers, regardless of their skill level, to infiltrate your network.

Ransomware Surge: The Ultimate Data Hostage Situation

Ransomware isn't going anywhere. Expect attackers to use even more sophisticated encryption and sneaky tactics to avoid detection and maximize the impact. Think of it as a high-stakes hostage situation with your data – prepare your defenses!

Variant:

A new ransomware variant called "Hades" emerged in April 2024. Hades encrypts a victim's data and threatens to leak it on the Dark Web if the ransom demand is not met. Unlike traditional ransomware, Hades also targets a victim's social media accounts, exfiltrating personal information and using it to pressure them into paying.

Action:

Backup your data regularly. Implement a robust backup and recovery plan to ensure you can restore your data quickly in the event of a ransomware attack. Additionally, train your employees to identify and avoid phishing attempts, a common tactic used to deploy ransomware.

Cloud Security Focus: Securing Your Digital Locker

Instead of attacking you directly, hackers might target your weaker partners in the supply chain (like your workout buddy). This lets them infiltrate your network indirectly. It's crucial to ensure strong security measures across your entire "cyber supply chain" to avoid these surprise attacks.

Incident:

In June 2024, a software company experienced a major supply chain attack. Hackers infiltrated a third-party vendor used by the company and injected malicious code into a widely used software update. This code allowed hackers to gain access to the systems of thousands of companies that had installed the update.

Action:

Vet your third-party vendors carefully. Ensure they have adequate security practices in place to minimize the risk of them becoming a vulnerability in your supply chain.

Insider Threats: The Enemy Within Your Fitness Circle

Just as a trusted workout partner could sabotage your fitness goals, insider threats pose a significant risk to your organization's cybersecurity. These threats come from within – employees, contractors, or partners who have legitimate access to your systems but misuse it, either intentionally or accidentally.

Statistic:

According to a 2024 Insider Threat Report by Cybersecurity Insiders, 74% of organizations feel vulnerable to insider threats, with 34% reporting an increase in insider incidents over the past 12 months.

Incident:

In May 2024, a major financial institution discovered that a disgruntled employee had been slowly exfiltrating customer data over a period of six months before being detected. The employee had used their authorized access to bypass many of the company's security controls.

Action:

Implement robust access controls and monitoring systems. Use the principle of least privilege to ensure employees only have access to the data and systems they need for their roles. Deploy User and Entity Behavior Analytics (UEBA) tools to detect unusual patterns that might indicate insider activity. Additionally, foster a positive work culture and provide channels for addressing employee grievances to reduce the risk of malicious insider actions.

Contact us

info@cybervergent.com

☎ +234-1-2900808

+233-256743669

🌐 www.cybervergent.com

212/214 Herbert Macaulay Way,
Yaba, Lagos, Nigeria

39 Kofi Annan Street, Airport
Residential Area, Accra, Ghana

4320 Stevens Creek Boulevard Ste
175 San Jose CA 95129 United States