

PREVIEW PREVIEW PREVIEW PREVIEW

Hacking

VOL. 10

NO. 06

ISSN 1733-7186



DARK WEB VOL. 2

A THREAT TO CORPORATE SECURITY

UNVEILING
THE
UNDERWORLD:
HOW
COMPANIES
ARE **TARGETED**
ON THE

HOW
HACKERS
ATTACK
BIG
CORPORATIONS

PROTECTING
YOUR
CORPORATE
FORTRESS:
STRATEGIES
TO THWART
DARK WEB

WHERE DO
RANSOMWARE
GANGS
RESIDE
IN THE
DARK WEB?

PREVIEW PREVIEW PREVIEW PREVIEW

EDITOR'S WORD

Dear Readers,

In the intricate tapestry of our digital era, the dark web looms as an enigmatic nexus of shadowy dealings and cyber threats—a subject both fascinating and formidable, with its tendrils silently entwined around the heart of our corporate world. This issue, "Dark Web 2.0 A Threat To Corporate Security," is a bold expedition into this obscured frontier, crucial for anyone vested in the security of corporate digital space.

Our cover story, "How Hackers Attack Big Corporations," peels back the layers of cyber threat actors tactics, elucidating the sophisticated methodologies employed to breach the fortresses of our business institutions. From the psychological cunning of social engineering to the ruthless efficiency of Advanced Persistent threats, We demystify the offensive tricks at the hacker's disposal.

In "Dark Web Marketplaces: Where Stolen Data Finds Its Buyers," we follow the journey of stolen data as it goes missing in the vastness of the internet, only to pop up again in the secretive marketplaces of the online shadow world.. This article is not merely a revelation—it's a stark warning of the commodification of corporate vulnerabilities.

Our investigative piece, "Unveiling the Underworld: How Companies are Targeted on the Dark Web," brings to light the deliberate targeting of enterprises, from SMEs to conglomerates, revealing how their defenses are probed and penetrated by faceless adversaries.

Moreover, "Where Do Ransomware Gangs Reside in the Dark Web?" leads you into the lairs of the online beast, mapping the operational bases of ransomware syndicates and their mechanisms of chaos, while offering strategies for your digital immune system.

The articles within these pages are penned by a cadre of seasoned cybersecurity experts, investigative journalists, and industry insiders. Each piece is meticulously crafted, not only to inform and enlighten but also to arm you with actionable knowledge and strategies, such as those found in "Virtualization Security Strategies: Safeguarding Data and Applications" and "DDoS ATTACK ORCHESTRATION ON THE DARK WEB: AN OVERVIEW."

Our discourse may traverse through shadows, but our aim is to illuminate and inspire. As you turn these pages, may you gain the insight to better navigate the murky waters of cyber threats and the wisdom to protect your corporate citadel in this ceaseless battle of bytes and breaches.

Welcome to a journey of understanding the unseen, a clarion call for action in the face of the concealed chaos of the dark web.

Together, let's shine a light on the dark.

Helena Piorun and the **Hakin9 Media** Team
helena.piorun@hakin9.org

EDITOR-IN-CHIEF
JOANNA KRETOWICZ
JOANNA.KRETOWICZ@HAKIN9.ORG

ASSOCIATE EDITOR
HELENA PIORUN
HELENA.PIORUN@HAKIN9.ORG

Cover Image
Wiktor Bukowska

Technical Editors
Lee Mckenziie

Cover Design
Wiktor Bukowska

Reviewers

Bev Robb, Jay Kay, Craig, Girshel C, Paul Mellen, Felipe Martins, Frank M, Luis Reyes, Morgan Weetman, Artur Artur, Dan, Frank M, Pawel Brzek, Ranjitha R, Fabrizio Baiardi, Amit Chugh, Michal Jachim, FREREBEAU Laurent, Humberto Júnior, Daniel Boughton, Raimundo Jiménez, jens ulrich, Arnold Chan, Momen Eldawakhly, Bibib, Gregory Chrysanthou, Zechariah Oluleke Akinpelu, Emanuele Placidi, Ross Moore, Gilbert Oviedo, Clancey, Tom Updegrove

01	THE DARK WEB
20	HOW HACKERS ATTACK BIG CORPORATIONS
27	DARK WEB MARKETPLACES: WHERE STOLEN DATA FINDS ITS BUYERS
36	PROTECTING YOUR CORPORATE FORTRESS: STRATEGIES TO THWART DARK WEB THREATS
44	WHERE DO RANSOMWARE GANGS RESIDE IN THE DARK WEB?
56	UNVEILING THE UNDERWORLD: HOW COMPANIES ARE TARGETED ON THE DARK WEB
65	DDOS ATTACK ORCHESTRATION ON THE DARK WEB: AN OVERVIEW BEHIND THE SCENES OF A CYBERTHREAT
79	VIRTUALIZATION SECURITY RECOMMENDATIONS: SAFEGUARDING DATA AND APPLICATIONS
85	OVERVIEW OF DATA PRIVACY IN THE MIDDLE EAST
92	Q&A WITH KATE LIBBY – KISMET COURSE

All trademarks, trade names, or logos mentioned or used are the property of their respective owners. The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Ross More

How hackers attack big corporations

Introduction

Crime, especially organized crime, is a business. Return on investment, risk vs. reward, balance sheets, cost of inventory and personnel, software and hardware costs – these and many more factors (including attitude factors such as loyalty and customer service) create an ironic connection between criminal activities and business ventures.

The bigger the potential payout, the better chance that the crime will be attempted. While no one is immune to cybercrime, a big payout is attacking big corporations.

Nothing in this writing is intended to shame or blame any companies that were attacked. Many attacks – including the ones noted here – are comprised of multiple exploits. Maybe it's a combination of an accidental download of fileless malware, and a months-long intrusion (pointing to a lack of internal monitoring). Or it's a disgruntled employee who is bribed to give a username and password to the thief to install spyware on a laptop so they can discover admin credentials to SSH into an externally-facing server. Perhaps it's infiltrating a third-party, staying under the radar for months to map the network of the customers, then distribute malware.

Chained attacks like these make it difficult, if not impossible, to find the exact point at which the network is compromised. And this complication makes it that much harder for companies to defend against them. Layered defense is the security principle, but the more layers, the more costly in terms of personnel, talent, and financial resources.

Let's cover several of the techniques used in recent breaches.

Social Engineering

In September 2023, MGM Resorts shut down various systems because of a noted “cybersecurity issue.” After investigation, MGM sent an update that a) ransomware had impacted numerous systems but they were restored and b) private customer information had been compromised. [1]

The initial vector of attack appears to be social engineering via phone call – aka, vishing. One of the criminals gathered publicly available information from a LinkedIn profile, imitated that person when calling the MGM support number, was able to smooth talk their way into getting credentials, and it was the fast track to game over. [2]

The proposed culprit? The group Scattered Spider, a fairly recent big game hunter (a group that targets high-value organizations, often using ransomware) that teamed up with the Russian group BlackCat for the attack. [3]

Exposed API

An API is a marvelous technology for accelerating and innovating business, but APIs also open up new avenues for attacks due to their architecture. They are made to be heavily used and can be easy to implement. These and other factors make them susceptible to abuse that is hard to track and detect.

August 2023 found Duolingo reporting about an exposed API that was exploited. The API allowed anyone to verify if email addresses are valid. The attacker used millions of email addresses (likely from previous breach lists), fed them into the API to confirm their validity, and now has a list of valid email addresses that can be used for targeted phishing attacks.

“This data was scraped using an exposed application programming interface (API) that has been shared openly since at least March 2023, with researchers tweeting and publicly documenting how to use the API.” [4]

OWASP has a great list of common API vulnerabilities and how to address those in their OWASP API Top Ten Project. [5]

Third-party vulnerability /MOVEit

Third-party vulnerabilities are a sore spot for many. Everybody has a third-party or a vendor; large organizations have hundreds, perhaps thousands. Attackers leverage the enormous customer base of vendors, suppliers, and even consultants. This attack surface makes it more difficult for customers as they are completely dependent on the security of the vendor, knowing that if the vendor gets hacked, then they themselves get hacked.

An attack on the Norway government was reported in July 2023. The cause? Third-party vulnerability.

“We identified a weakness in the platform of one of our suppliers. That weakness has now been shut.”

The attack affected twelve government ministries and appears to be a targeted critical infrastructure attack because Norway is the largest gas supplier to Europe. [6]

In early October 2023, Microsoft researchers disclosed that “North Korean nation-state threat actors tracked as Diamond Sleet and Onyx Sleet are exploiting a remote code execution vulnerability affecting multiple versions of the JetBrains TeamCity server.” [7]

The Ontario BORN (Better Outcomes Registry and Network) birth registry was subjected to exploitation via the MOVEit vulnerability. More than three million people had their personal data breached. This could be considered a fourth-party breach. BORN is the third-party that keeps a registry of numerous customers, and the attackers leveraged the exploit of a vendor of a vendor. [8] [9]

M MOVEit is linked to the Russia-linked Cl0p ransomware group, and its effect so far is far from trivial: it has “exposed data from more than 2,000 organizations and 60 million individuals.”

MOVEit is considered the biggest data theft of 2023. At the time, it was a zero-day (0-day) exploit but has since been patched. That leads to a remote code execution (RCE).

[10] [11] [12]

Credential stuffing

Regrettably, even our DNA isn't safe. News broke in early October 2023 that the genetic testing company, 23andMe, had user data stolen, to the count of about 1 million data fields. [13]

The attack vector this time? Credential stuffing.

What is credential stuffing? It's an attack method where an attacker uses stolen username and password combinations, often obtained from previous data breaches or other sources, to gain unauthorized access to online user accounts. The attacker can essentially "stuff" these stolen credentials into login forms or APIs on different websites or applications in the hope that some of the combinations will work, as people often reuse passwords across multiple accounts.

Here's how credential stuffing typically works:

Data Breaches: Hackers acquire large databases of usernames and passwords through data breaches or by purchasing them from the dark web. These credentials may not be immediately valuable to the attacker, but they represent a valuable resource for future attacks.

Automated Attacks: Attackers use automated scripts or software to systematically try these stolen credentials on various websites, online services, or applications, often at a high rate of speed. They might also employ proxies and techniques to obfuscate their identity.

Success and Unauthorized Access: If a set of credentials is valid and matches an account on the targeted platform, the attacker gains unauthorized access to the victim's account. The thieves may then misuse this access for other malicious purposes, such as data theft,

fraud, or spreading spam or malware, likely chaining the attacks to make the attacks more nefarious.

As an update, in mid-October 2023, the cybercriminal Golem claims to have put up millions more 23andMe records for sale on the dark web. Golem posted over 4 million records of sensitive information, and 23andMe is determining if the data is real. [14]

Malware/Ransomware

The Cloud Security Alliance (CSA) recently published an excellent resource – Top Threats to Cloud Computing: Pandemic 11 Deep Dive – that analyzes several recent major breaches and attacks. [15]

According to their analysis of the 2022 attack on the Portuguese and Brazilian Embassies, APT29 – the hacking group known as CozyBear – attached malicious files to spear phishing emails, which after opened spread malware through the network. The malware exfiltrated data to valid hosted solutions (e.g., Dropbox, Google Drive). APT29's cyberespionage campaign was successful in that they retrieved sensitive information from government computer resources. According to the report, one of the threats included, "Malicious files installed using HTML smuggling techniques to deliver an image or ISO file."

What Can Be Done?

While attackers have to have a much larger budget, more personnel, and more compute resources to attack large corporations, and while the attacks are more complex and use a larger and often more widely distributed resources, the categories are the same as used against smaller companies. Attackers will use social engineering, DDoS attacks, malware, ransomware, API abuse, physical infiltration, and many others – all of which are known and typical attack methods.

Corporations should find a trusted advisor to assist in performing a risk assessment and proceed accordingly. The MGM breach is expected to have cost them \$100 million when it's all said and done. Part of assessing the risk to your org is to include how much a breach would cost. Then,

invest a reasonable amount of that to ensure the breach doesn't happen and include reasonable protections to prove that there was no lack of due diligence and reasonable security.

Crime happens, and will continue to occur, but that doesn't mean we can't protect our organizations and prove to our customers that we truly do take security seriously.

References

- [1] <https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware>
- [2] <https://www.cybersecuritydive.com/news/mgm-caesars-attacks-social-engineering/693956/>
- [3] <https://www.trellix.com/en-ca/about/newsroom/stories/research/scattered-spider-the-modus-operandi/>
- [4] <https://www.bleepingcomputer.com/news/security/scraped-data-of-26-million-duolingo-users-released-on-hacking-forum/>
- [5] <https://owasp.org/API-Security/editions/2023/en/0x00-header/>
- [6] <https://www.reuters.com/technology/norway-government-ministries-hit-by-cyber-attack-2023-07-24/>
- [7] <https://www.databreachtoday.com/north-korean-hackers-exploiting-critical-flaw-in-devops-tool-a-23350>
- [8] <https://globalnews.ca/news/9983285/ontario-birth-registry-data-breach-born/>
- [9] <https://www.bleepingcomputer.com/news/security/sickkids-impacted-by-born-ontario-data-breach-that-hit-34-million/>
- [10] <https://www.securityweek.com/zero-day-in-moveit-file-transfer-software-exploited-to-steal-data-from-organizations/>

[11] <https://www.securityweek.com/sec-investigating-progress-software-over-moveit-hack/>

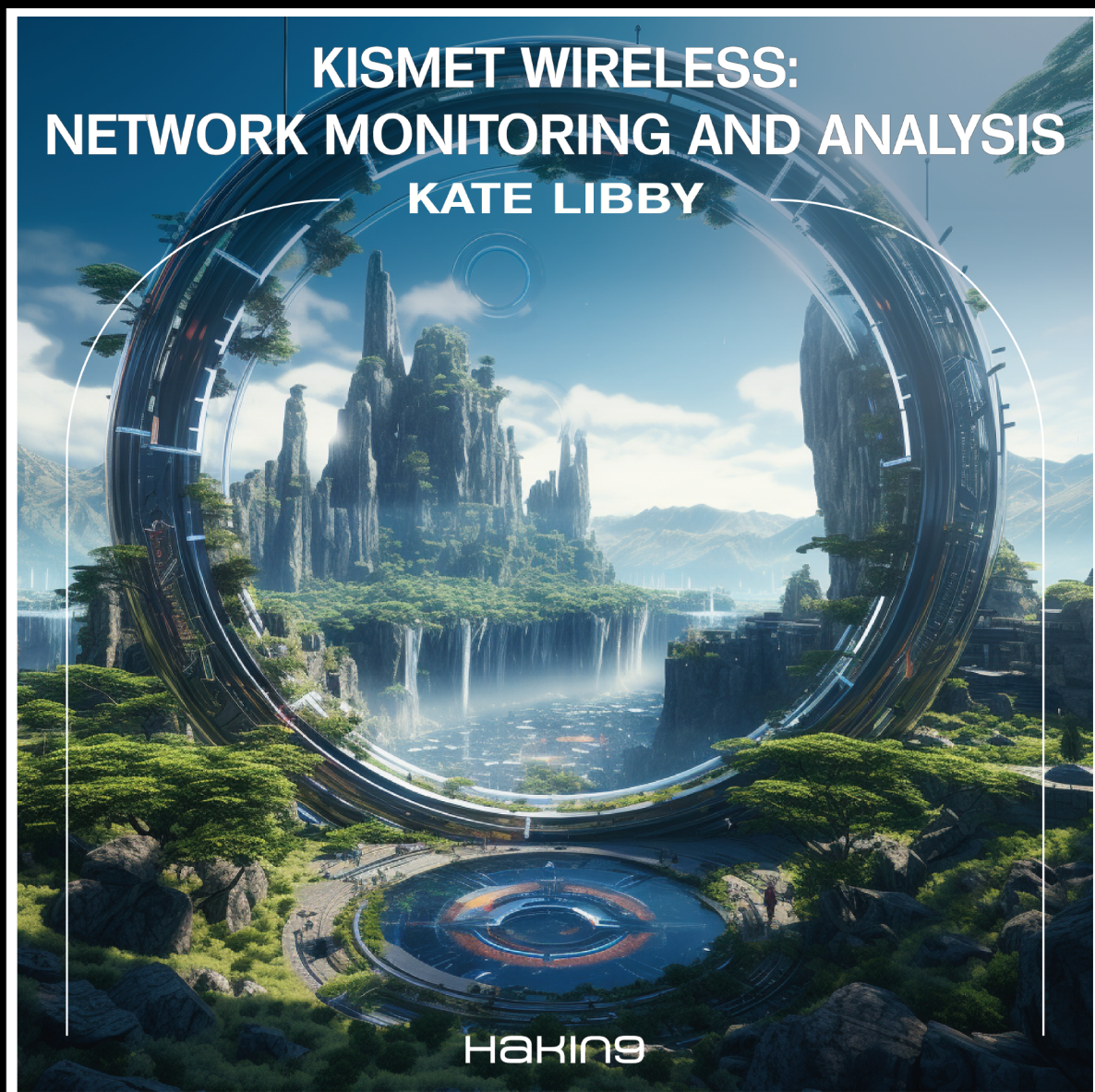
[12] <https://nvd.nist.gov/vuln/detail/CVE-2023-34362>

[13] <https://tech.co/news/23andme-breach-stolen-data>

[14] <https://www.thehindu.com/sci-tech/technology/how-hackers-launch-credential-stuffing-attacks-explained/article67425855.ece>

[15] <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven-deep-dive/>

GET YOUR SEATS NOW!



COMPREHENSIVE COURSE, DESIGNED TO PROVIDE YOU
WITH A DEEP UNDERSTANDING OF KISMET WIRELESS, A
POWERFUL OPEN-SOURCE WIRELESS NETWORK
MONITORING AND ANALYSIS TOOL.