CYBERARK®

Enable secure access for any identity, human or machine, to any resource or environment from anywhere, using any device

Panagiotis Pantazis
Country Manager

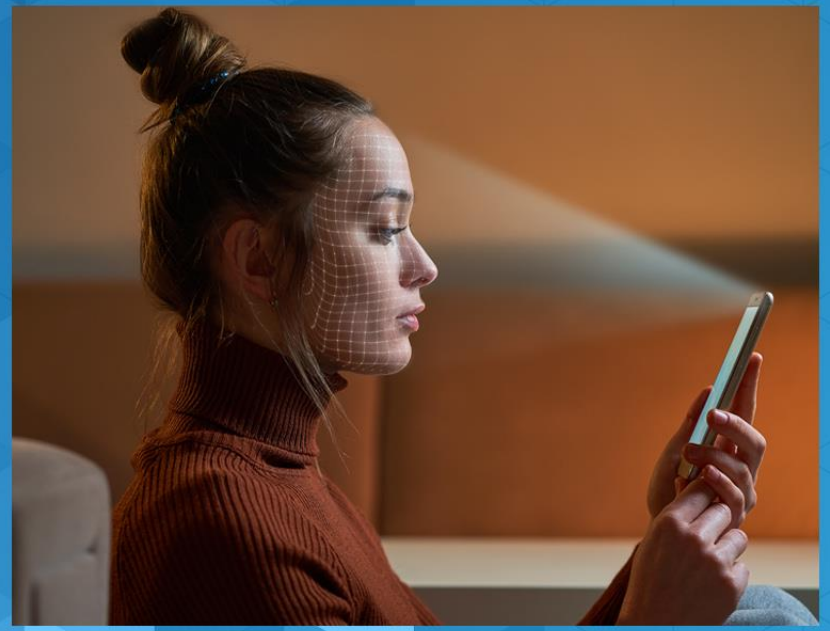
22 February 2023

cyberark.is/identity-security

WHAT JUST HAPPENED?

IDENTITY SECURITY TRENDS

1.
The move to remote work



2.
The expansion of privileged identities

3.
Securing digital transformation

1.REMOTE WORK

Forbes estimates 30% of employees now primarily work from home

2. EXPANSION OF PRIVILEGED IDENTITIES

2. EXPANSION OF PRIVILEGED IDENTITIES

Hundreds of

Thousands of

IDENTITIES

Per average medium-to-large organizations

2. EXPANSION OF PRIVILEGED IDENTITIES

3. SECURING DIGITAL TRANSFORMATION

CYBERSECURITY DEBT HAS CONSEQUENCES

ZOLA WEDDING REGISTRY

mailchimp

COMITE INTERNATIONAL GENEVE

okta

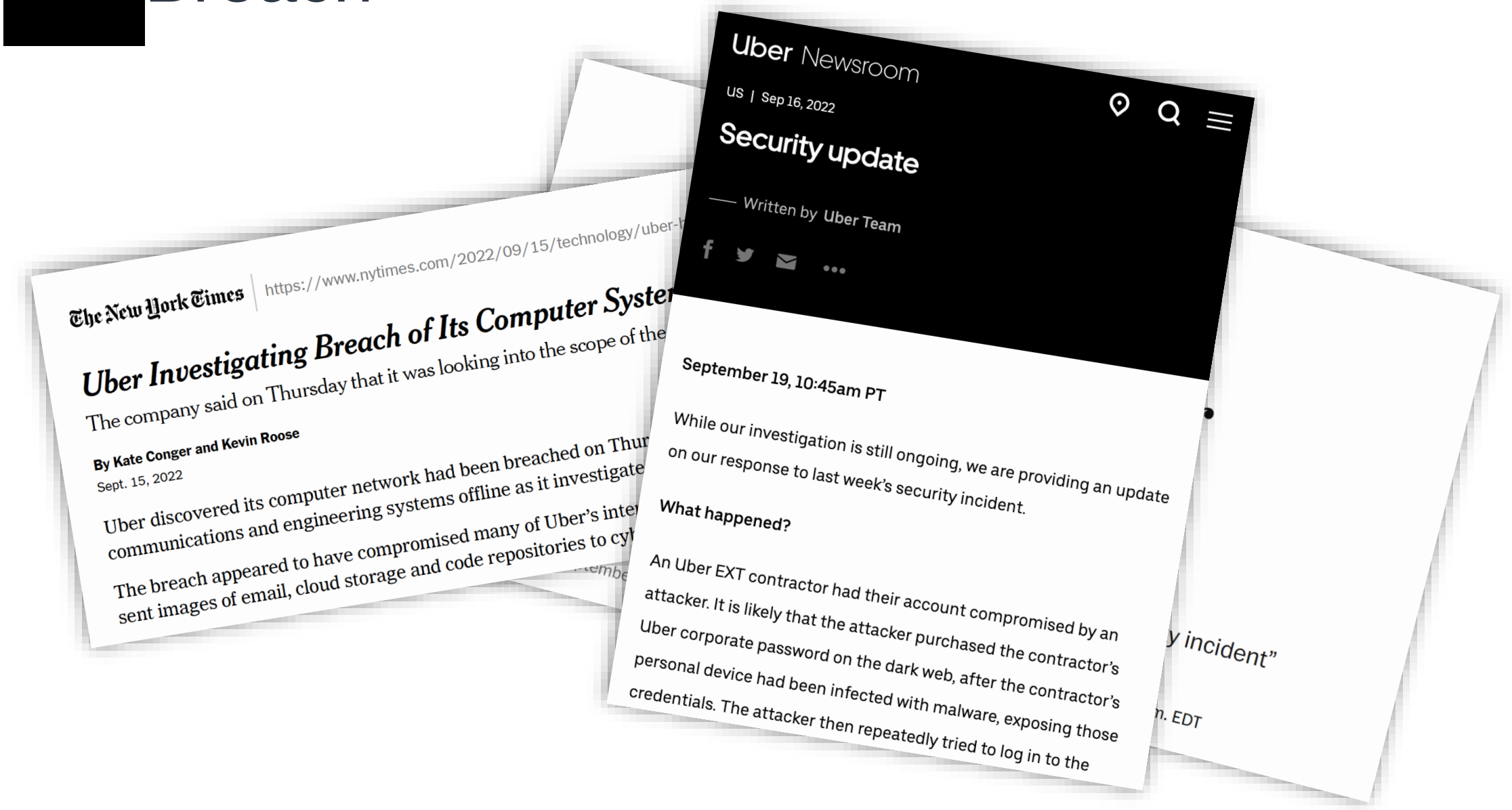
Microsoft

HARBOUR PLAZA

radius financial group inc.

COMMISSION ON ELECTIONS REPUBLIC OF THE PHILIPPINES

Uber Breach



The New York Times | https://www.nytimes.com/2022/09/15/technology/uber-

Uber Investigating Breach of Its Computer Syste

The company said on Thursday that it was looking into the scope of the

By Kate Conger and Kevin Roose

Sept. 15, 2022

Uber discovered its computer network had been breached on Thur
communications and engineering systems offline as it investigate

The breach appeared to have compromised many of Uber's inte
sent images of email, cloud storage and code repositories to cy

Uber Newsroom

US | Sep 16, 2022

Security update

Written by Uber Team

September 19, 10:45am PT

While our investigation is still ongoing, we are providing an update on our response to last week's security incident.

What happened?

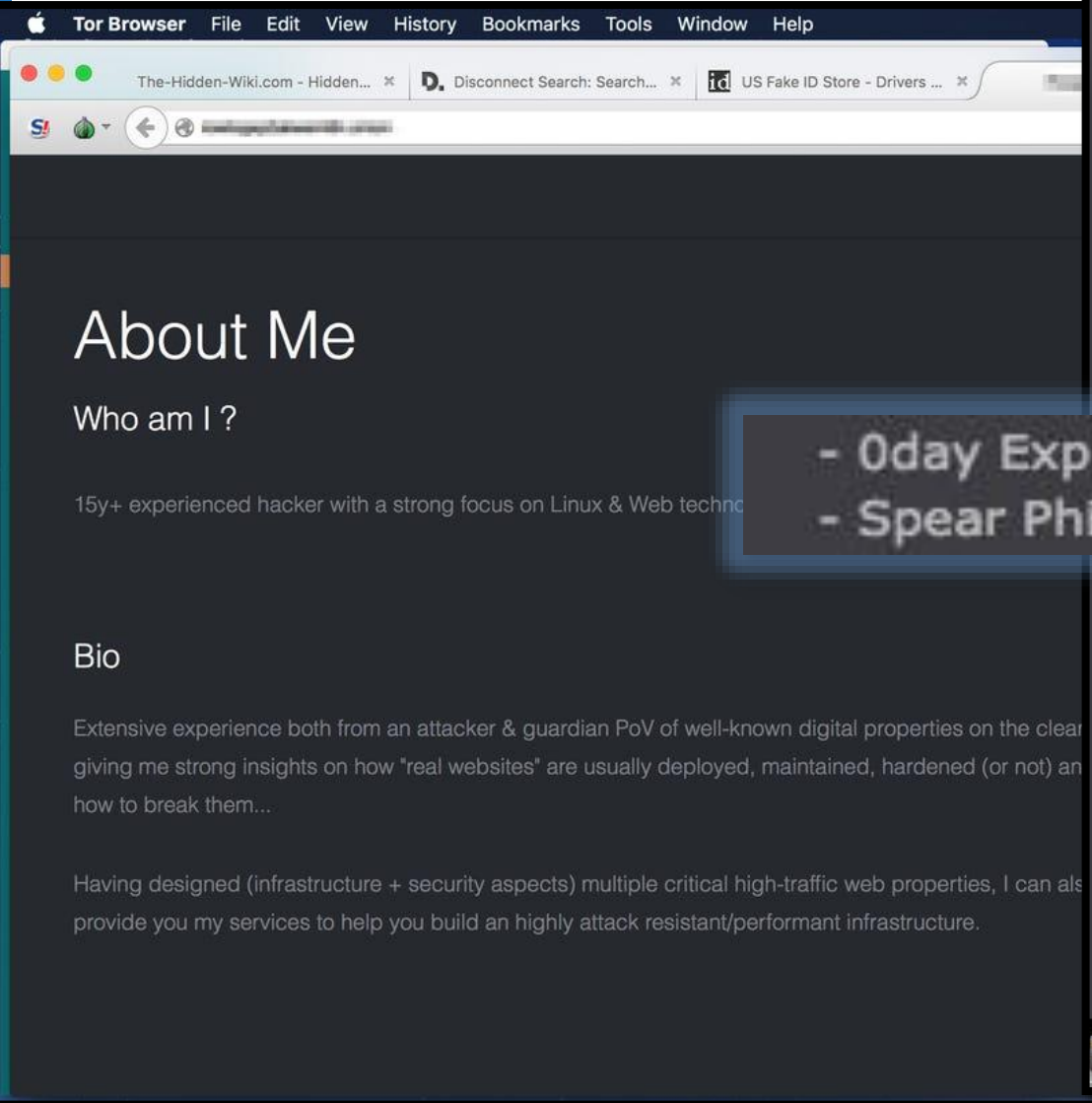
An Uber EXT contractor had their account compromised by an attacker. It is likely that the attacker purchased the contractor's Uber corporate password on the dark web, after the contractor's personal device had been infected with malware, exposing those credentials. The attacker then repeatedly tried to log in to the

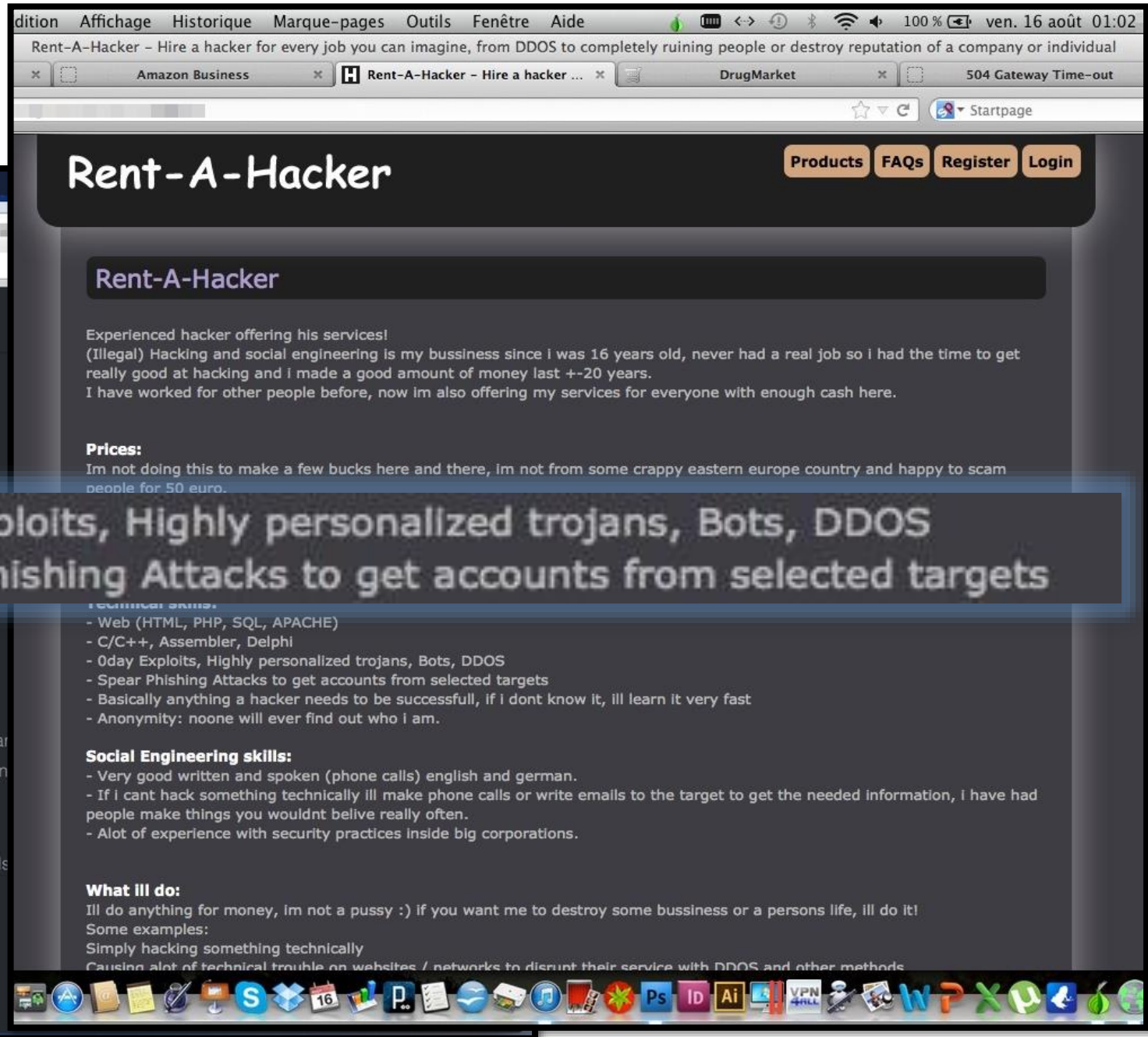
y incident"

n. EDT

Uber Breach

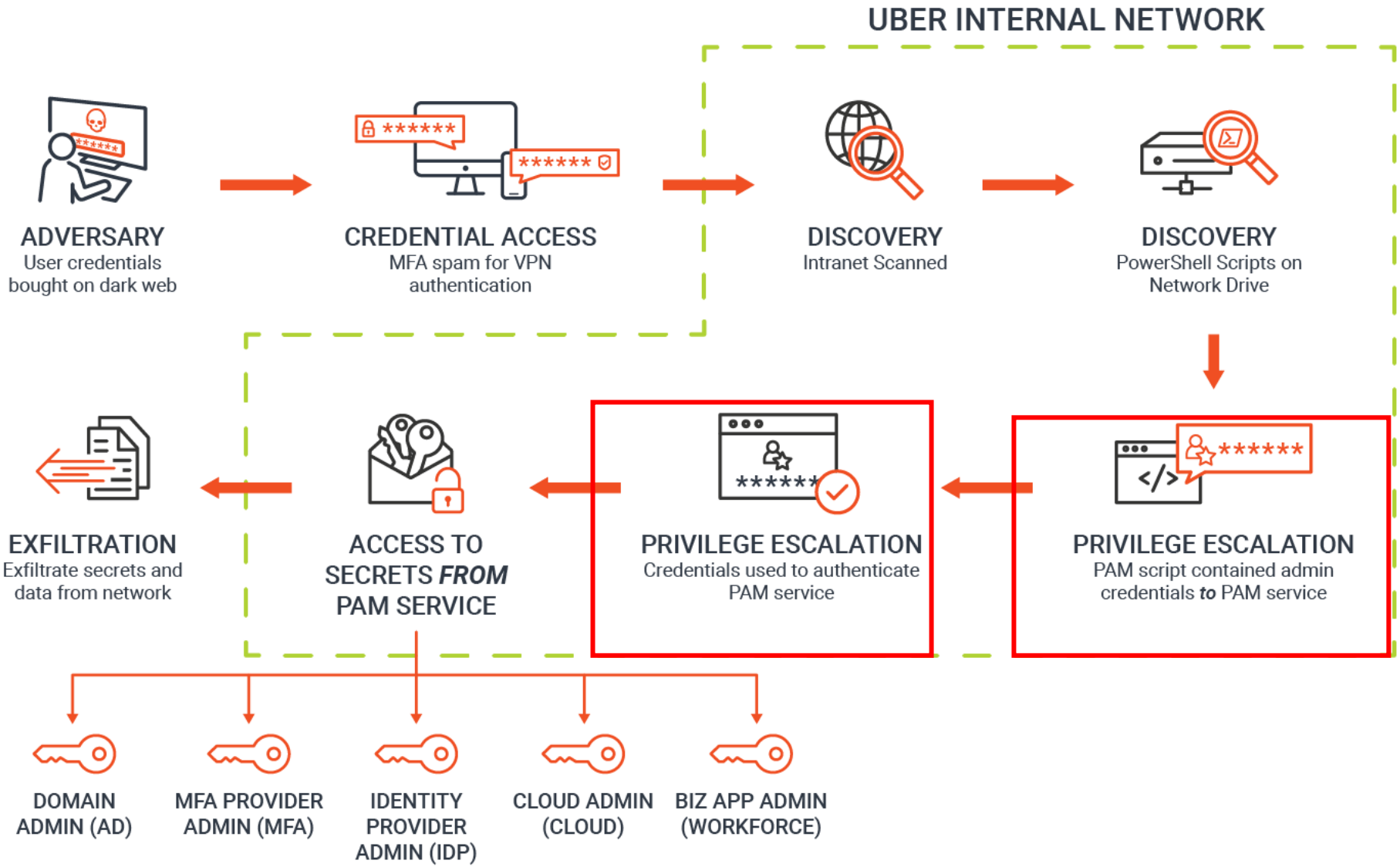
HaaS: Hacker as a Service





Uber Breach

- Social engineering and multiple MFA attack vectors
- Harvesting credentials for a PAM solution that allowed the attacker to gain high-level access, escalate privileges, and exfiltrate.



Russia-Ukraine War | Cyber Warfare Aspect

Ukraine has been a permanent target of cyber-attacks since 2014. Thousands of attacks occur every month, making Ukraine the **"perfect sandbox for those looking to test new cyberweapons, tactics and tools"** POLITICO

Examples of cyberwarfare:

- An attack on the **communication systems of the Kyiv Post** and the **KA-SAT satellite network** an hour before the invasion (24 Feb 2022)
- An **IsaacWiper attack against government websites** (25 Feb 2022)
- A cyber-attack targeting a **border control station** with the aim of preventing refugees from entering Romania (25 Feb 2022)
- Attacks on **Ukraine's digital infrastructure**, blocking access to financial services and energy (28 February), etc.

* European parliament briefing paper "Russia's war on Ukraine: Timeline of cyber-attacks" (June 2022)

EPRS | European Parliamentary Research Service

Figure 1 –Timeline of cyber-attacks on Ukraine

Source: Data compiled by EPRS; Graphic by Lucille Killmayer.

Russia-Ukraine War | Top Attack Types

MITRE | ATT&CK®

Disk Wipe

Sub-techniques (2)

ID: T1561

direct access to the hard drive

Permissions Required: Administrator, SYSTEM, User, root

rupt availability to system
may opt to wipe arbitrary p
ed.

To maximize impact on the target organization in operations where network-wide availability interruption is the goal, malware used fo
worm-like features to propagate across a network by leveraging additional techniques like Valid Accounts, OS Credential Dumping, an
Shares.[1]

Created: 20 February 2020
Last Modified: 28 March 2020

Live Version

Data Component	Detects
Command Execution	Monitor executed commands and numbers in a network to interrupt
Drive Access	Monitor for newly constructed dri like the partition boot sector, mas
Drive Modification	Monitor for changes made to driv like the partition boot sector, mas
Driver Load	Monitor for unusual kernel driver numbers in a network to interrupt
Process Creation	Monitor newly executed processe a network to interrupt availability

Miti

ID	
M105	ps that can be used to restore organizational data.[2] Ensure backups are stored off system and is protected ry.

Dete

ID	
DS00	for unusual kernel driver installation activity.
DS00	e for attempts to write to sensitive locations like the partition boot sector, master boot record, disk partition
	for attempts to read to sensitive locations like the partition boot sector, master boot record, disk partition table,
DS00	disk data on specific systems or in large numbers in a network to interrupt availability to system and network
DS00	ific systems or in large numbers in a network to interrupt availability to system and network resources.

1. Disk Wipe (Wiper)
2. Defacement
3. Cyber Espionage
4. Malware
5. Phishing
6. Hack and Leak

Securing Identities is Critical for Zero Trust

Identities

- Admins
- Workforce
- Third Parties
- Customers
- DevOps
- Workloads
- Devices

CYBERARK®

Identity Security Platform

SaaS | Hybrid | Self-Hosted

Seamless & Secure Access for All Identities

Intelligent Privilege Controls

Flexible Identity Automation & Orchestration

Workforce & Customer Access	Endpoint Privilege Security	Privileged Access Management	Secrets Management	Cloud Privilege Security	Identity Management
• Secure Web Sessions • SSO & Adaptive MFA (Workforce and Customer) • Workforce Password Management	• Endpoint Privilege Manager: Workstations & Servers • Secure Desktop	• Privilege Cloud & PAM Self-Hosted • Vendor PAM • Dynamic Privileged Access	• Secrets Hub • Conjur Cloud, Enterprise & OSS • Credential Providers	• Secure Cloud Access • Cloud Entitlements Manager	• Identity Lifecycle Management • Identity Flows • Identity Compliance

Identity Security Intelligence

Shared Services | Single Admin Portal | Workflows | Unified Audit | Authentication & Authorization

Resources

- Applications & Services
- Infrastructure & Endpoints
- Data

Environments

- Data Centers
- OT
- Hybrid & Multi-Cloud
- SaaS

CYBERARK BLUEPRINT FOR IDENTITY SECURITY SUCCESS

A vendor-agnostic framework for assessing your current strategy and defining a roadmap for success.

- Prevent credential theft
- Stop lateral and vertical movement
- Limit privilege escalation & abuse

CHART YOUR COURSE

Identity Security offers organizations the peace of mind that their most critical assets are secure while accelerating business agility. But putting a plan in place that effectively secures the expanding number and types of identities and their access can feel daunting. The CyberArk Blueprint was designed with this in mind, allowing organizations to better understand the attack chain, assess their own security, educate themselves on Identity Security best practices, and ultimately help them build a plan to measurably reduce risk. You don't have to go it alone, and the Blueprint is here to be your companion for the journey ahead.

Best Practice

Practical guidance across the people, process and technology domains.

Self-Service

Accelerate your Identity Security journey with self-service resources available on-demand.

Ecosystem

Comprehensive system of materials including videos, whitepapers, blog articles and toolkits.

CYBERARK LABS

Innovation From the Cutting Edge of Cybersecurity Research.

FEATURED RESEARCH

BLOG

The Linux Kernel and the Cursed Driver

BLOG

Breaking Docker Named Pipes SYSTEMatically: Docker Desktop Privilege Escalation – Part 1

BLOG

Inglourious Drivers – A Journey of Finding Vulnerabilities in Drivers

BLOG

Chatting Our Way Into Creating a Polymorphic Malware

BLOG

What I Learned from Analyzing a Caching Vulnerability in Istio

BLOG

Decentralized Identity Attack Surface – Part 2

BLOG

Decentralized Identity Attack Surface – Part 1

BLOG

Fantastic Rootkits: And Where to Find Them (Part 1)

CYBERARK®

C³ Alliance

200+ Certified Partners

300+ Certified Joint Solutions

- Analytics
- ICS
- Identity & Access Management
- Authentication
- ITSM
- Detection
- Orchestration & Response
- DevOps
- Robotic Process Automation
- Discovery
- SIEM
- Governance
- HSM
- Vulnerability Management

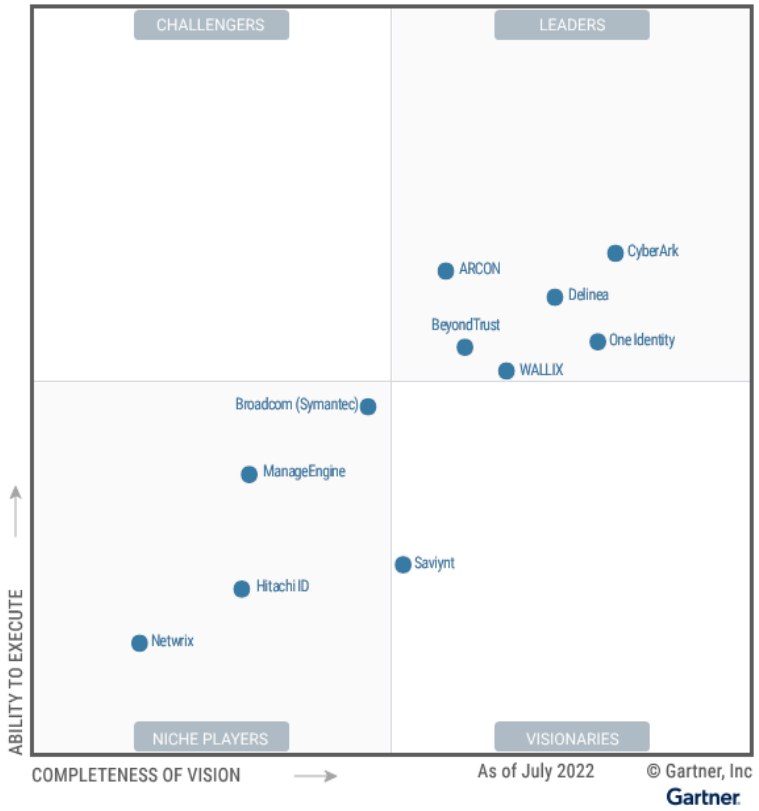
200+ Plug-ins

- CPM Plug-ins
- PSM Plug-ins

The FIRST and ONLY Leader in Both Gartner® Magic Quadrant™ Reports for Access Management and PAM. EVER.

Gartner evaluated more than 20 vendors across the two reports, and CyberArk is the only Leader in both Access Management and Privileged Access Management.

Magic Quadrant for Privileged Access Management



Magic Quadrant for Access Management

Gartner® Magic Quadrant™ for Privileged Access Management, by Michael Kelley, James Hoover, Felix Gaehtgens, Abhyuday Data, 19 July 2022
Gartner® Magic Quadrant for Access Management, by Henrique Teixeira, Abhuday Data, Michael Kelley, James Hoover, Brian Guthrie, 1 November 2022