



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

"CREDENTIALS ARE THE FAVORITE
DATA TYPE OF CRIMINAL ACTORS"

80%+

OF BASIC WEB APPLICATION
ATTACKS ATTRIBUTED TO
STOLEN CREDENTIALS

- 2022 Verizon Data Breach Investigations Report



**CYBER ATTACKERS
CONTINUE TO INNOVATE**

63%

of organizations have faced
a successful cybersecurity
attack due to an Identity
Security related issue



3. SECURING DIGITAL TRANSFORMATION

CYBERSECURITY DEBT
HAS CONSEQUENCES



Uber Breach

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

Uber Investigating Breach of Its Computer System

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

By Kate Conger and Kevin Roose
Sept. 15, 2022

Uber discovered its computer network had been breached on Thursday, and the company said it was looking into the scope of the breach.

The breach appeared to have compromised many of Uber's internal communications and engineering systems offline as it investigated. The breach appeared to have compromised many of Uber's internal communications and engineering systems offline as it investigated. The breach appeared to have compromised many of Uber's internal communications and engineering systems offline as it investigated.

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

Security incident"

on EDT

Uber Breach

HaaS: Hacker as a Service

Tor Browser File Edit View History Bookmarks Tools Window Help

The-Hidden-Wiki.com - Hidden... Disconnect Search: Search... US Fake ID Store - Drivers ...

About Me

Who am I ?

15y+ experienced hacker with a strong focus on Linux & Web technol

Bio

Extensive experience both from an attacker & guardian PoV of well-known digital properties on the clear giving me strong insights on how "real websites" are usually deployed, maintained, hardened (or not) and how to break them...

Having designed (infrastructure + security aspects) multiple critical high-traffic web properties, I can also provide you my services to help you build an highly attack resistant/performant infrastructure.

dition Affichage Historique Marque-pages Outils Fenêtre Aide 100 % ven. 16 août 01:02

Rent-A-Hacker - Hire a hacker for every job you can imagine, from DDOS to completely ruining people or destroy reputation of a company or individual

Amazon Business Rent-A-Hacker - Hire a hacker ... DrugMarket 504 Gateway Time-out

Startpage

Rent-A-Hacker

Products FAQs Register Login

Rent-A-Hacker

Experienced hacker offering his services!
(Illegal) Hacking and social engineering is my bussiness since i was 16 years old, never had a real job so i had the time to get really good at hacking and i made a good amount of money last +-20 years.
I have worked for other people before, now im also offering my services for everyone with enough cash here.

Prices:
Im not doing this to make a few bucks here and there, im not from some crappy eastern europe country and happy to scam people for 50 euro.

- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets

Technical skills:

- Web (HTML, PHP, SQL, APACHE)
- C/C++, Assembler, Delphi
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets
- Basically anything a hacker needs to be successfull, if i dont know it, ill learn it very fast
- Anonymity: noone will ever find out who i am.

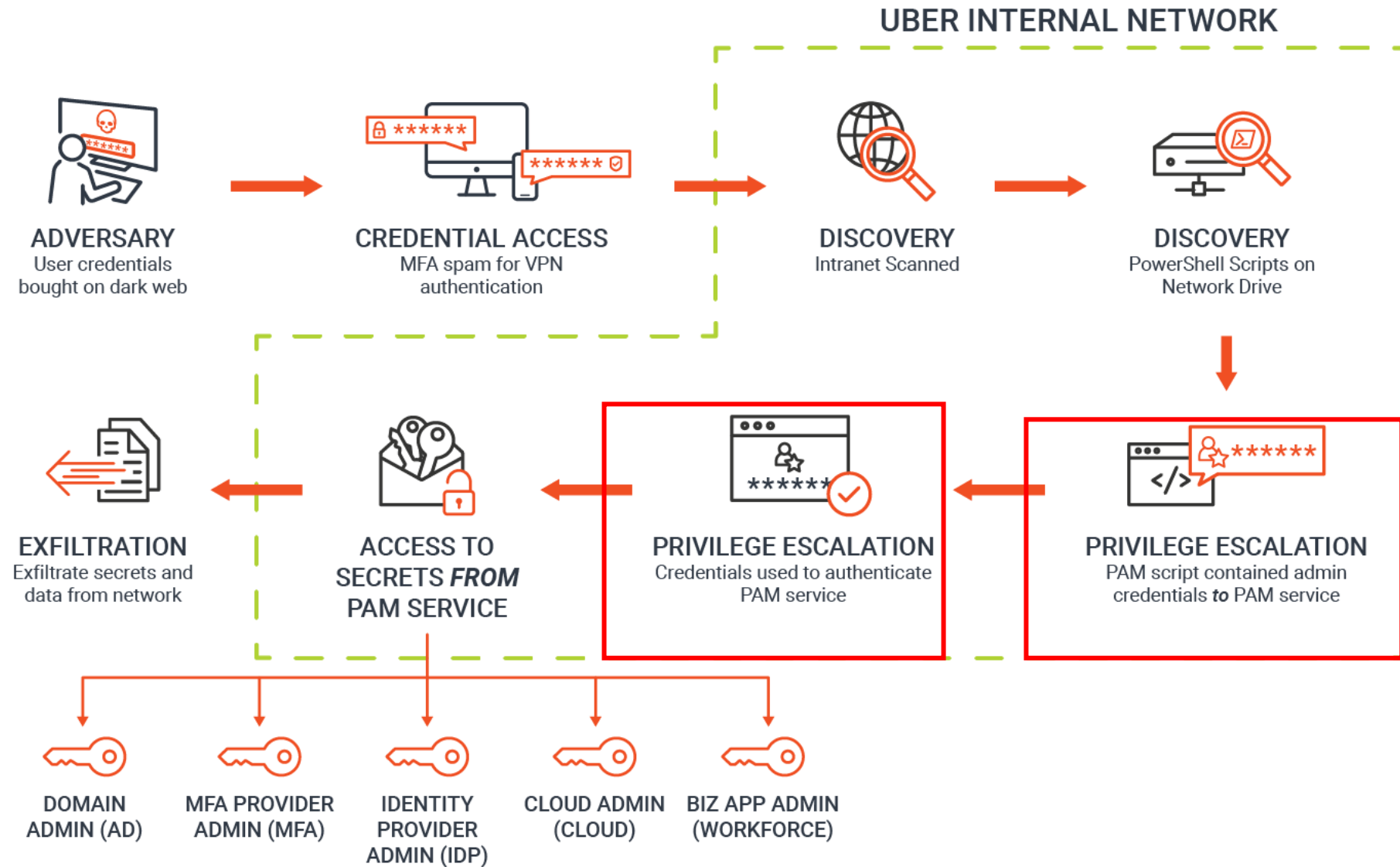
Social Engineering skills:

- Very good written and spoken (phone calls) english and german.
- If i cant hack something technically ill make phone calls or write emails to the target to get the needed information, i have had people make things you wouldnt believe really often.
- Alot of experience with security practices inside big corporations.

What ill do:
Ill do anything for money, im not a pussy :) If you want me to destroy some bussiness or a persons life, ill do it!
Some examples:
Simply hacking something technically
Causing alot of technical trouble on websites / networks to disrupt their service with DDOS and other methods

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



Disk Wipe

Sub-techniques (2)

ID: T1561

direct access to the hard drive

Permissions Required: Administrator, SYSTEM, User, root

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

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

Securing Identities is Critical for Zero Trust



Identity Security Platform

SaaS | Hybrid | Self-Hosted

Seamless &
Secure
Access for
All Identities

Intelligent
Privilege
Controls

Flexible Identity
Automation &
Orchestration

Workforce &
Customer
Access

- Secure Web Sessions
- SSO & Adaptive MFA (Workforce and Customer)
- Workforce Password Management

Endpoint
Privilege
Security

- Endpoint Privilege Manager: Workstations & Servers
- Secure Desktop

Privileged
Access
Management

- Privilege Cloud & PAM Self-Hosted
- Vendor PAM
- Dynamic Privileged Access

Secrets
Management

- Secrets Hub
- Conjur Cloud, Enterprise & OSS
- Credential Providers

Cloud
Privilege
Security

- Secure Cloud Access
- Cloud Entitlements Manager

Identity
Management

- Identity Lifecycle Management
- Identity Flows
- Identity Compliance

Identity Security Intelligence



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

Identities



Admins



Workforce



Third Parties



Customers



DevOps



Workloads



Devices

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

Inglorious 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)

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

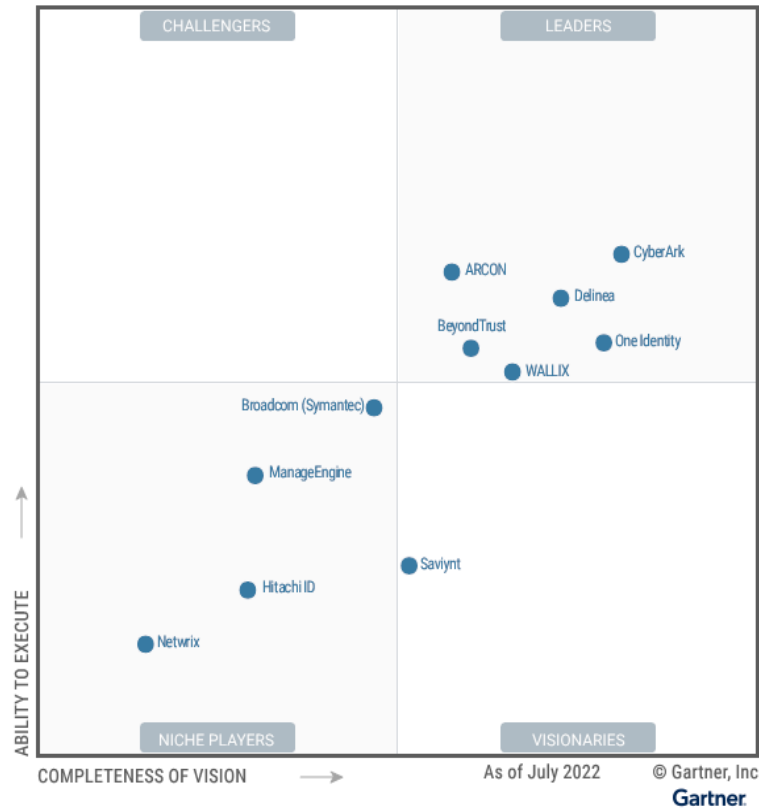
```

graph LR
    CPM[CPM Plug-ins]
    PSM[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 and Magic Quadrant are registered trademarks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

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, Abhyuday Data, Michael Kelley, James Hoover, Brian Guthrie, 1 November 2022

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from CyberArk.