13th infocom SECURITY Conference & Expo

CYBERARK®

The Current Threat Landscape. Secure Your Identities. Go Fearlessly Forward.

Panagiotis Pantazis

27 April 2023

Cybercrime in Numbers

800%
Increase in ransomware attacks

667%
Increase in spear-phishing attacks

400%
Increase in cyberattacks

422 Million
individuals were impacted

80%+
of attacks exploit theft of credentials, privileges and identities

$20 BILLION
Estimated cost of global ransomware damage

6 TRILLION
Projected annual cost of cybercrime damage

33 BILLION
accounts will be breached

39 sec
A cyberattack occurs

https://www.cyberark.com/resources/blog/pandemic-cyber-crime-by-the-numbers

“CREDENTIALS ARE THE FAVORITE DATA TYPE OF CRIMINAL ACTORS”

80%+

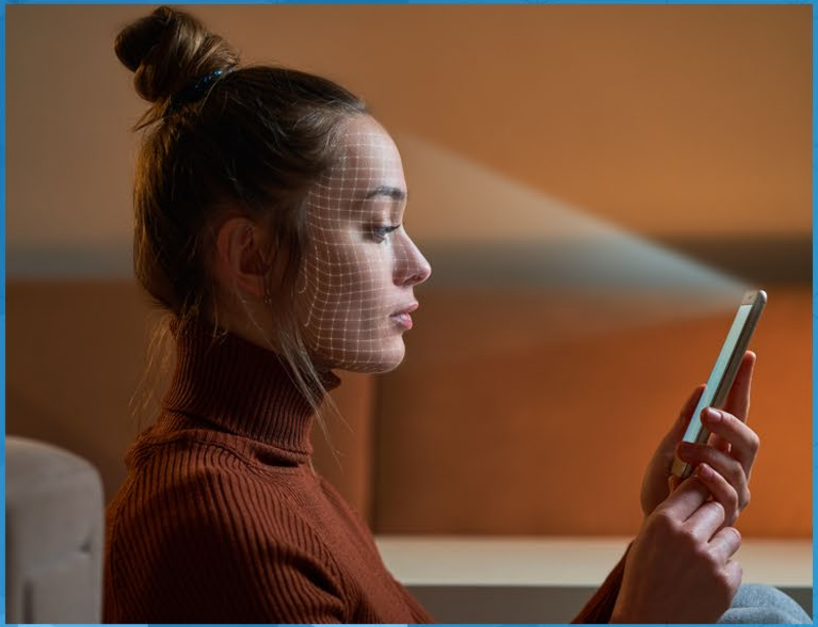
OF BASIC WEB APPLICATION ATTACKS ATTRIBUTED TO STOLEN CREDENTIALS

2022 Verizon Data Breach Investigations Report

WHAT JUST HAPPENED?

IDENTITY SECURITY TRENDS

1\.
Securing digital transformation



2\.
The expansion of privileged identities

3\.
The move to remote work

1. SECURING DIGITAL TRANSFORMATION

CYBERSECURITY DEBT HAS CONSEQUENCES

70%

of organizations experienced ransomware attacks

64%

lost data to a software supply chain attack

ZOLA WEDDING REGISTRY

mailchimp

COMITE INTERNATIONAL GENEVE

okta

Microsoft

HARBOUR PLAZA

radius financial group inc.

COMMISSION ON ELECTIONS REPUBLIC OF THE PHILIPPINES

2. EXPANSION OF PRIVILEGED IDENTITIES

ALL USERS CAN BE PRIVILEGED

52%

of all employee identities have access to sensitive systems and data

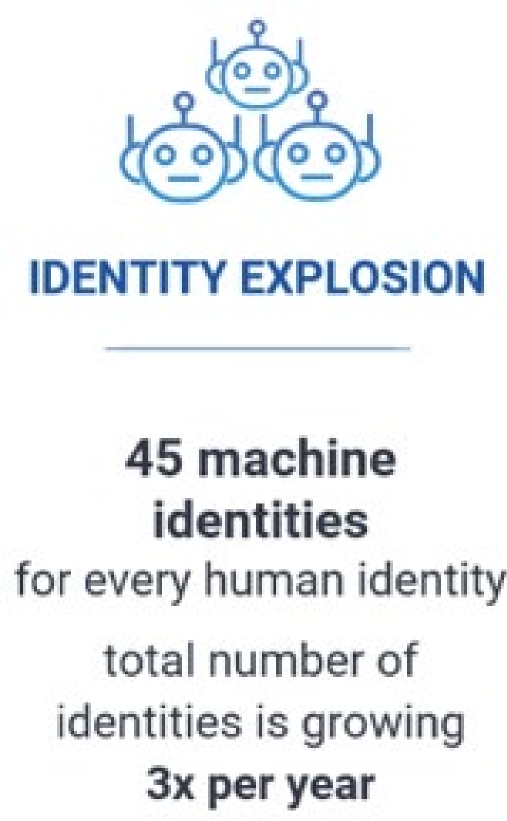
2. EXPANSION OF PRIVILEGED IDENTITIES

Hundreds of

Thousands of

IDENTITIES

Per average medium-to-large organizations

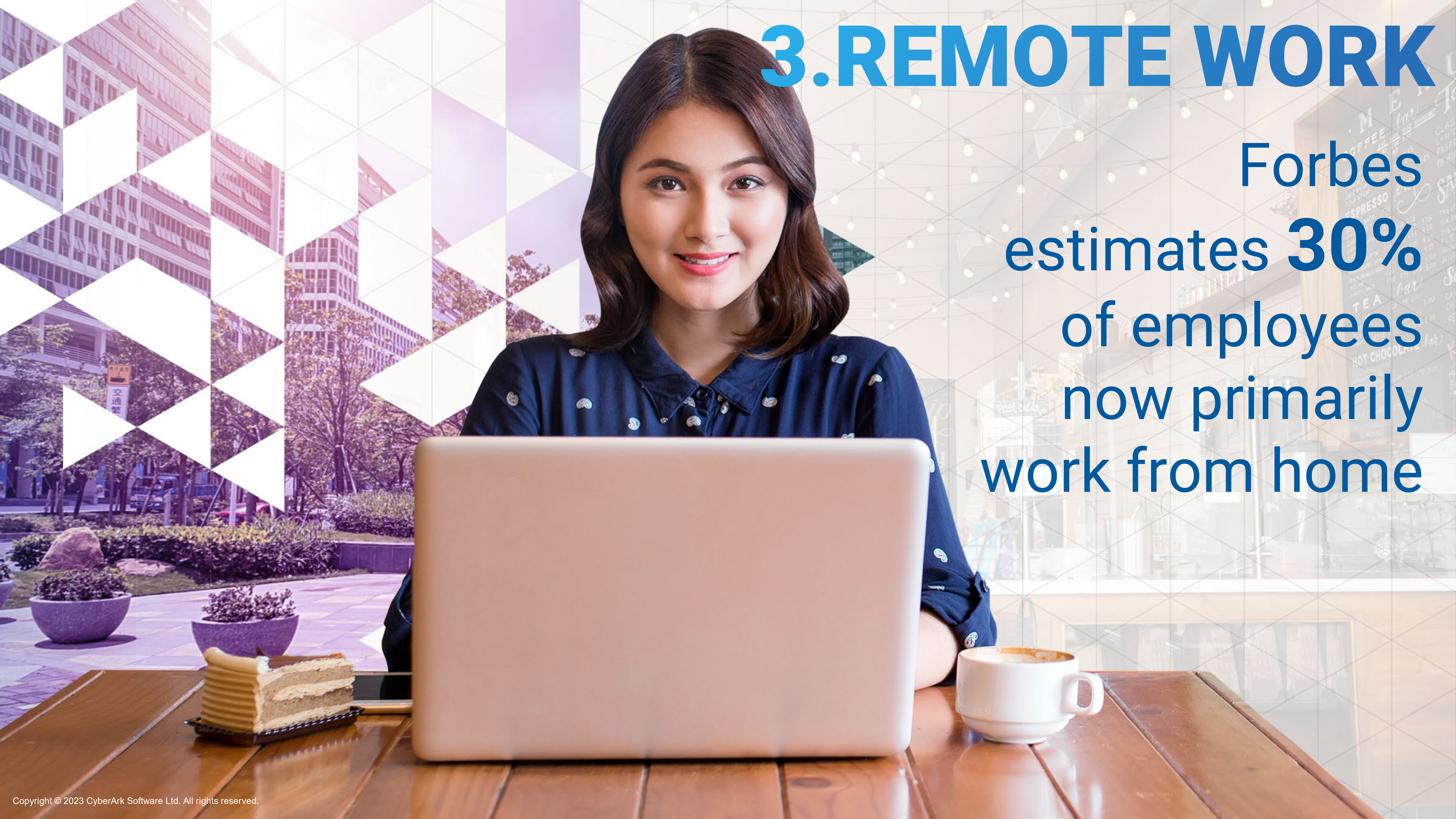


IDENTITY EXPLOSION

45 machine identities for every human identity

total number of identities is growing **3x per year**

3.REMOTE WORK



Forbes estimates **30%** of employees now primarily work from home

Uber Breach What Can we Learn?

Uber Newsroom

US | Sep 16, 2022

Securi

The New York Times | https://

Uber Investigating B

The company said on Thursd

By Kate Conger and Kevin Roose

Sept. 15, 2022

Uber discovered its compu
communications and engir

The breach appeared to h
sent images of email, clou

Unpacking the Uber Breach

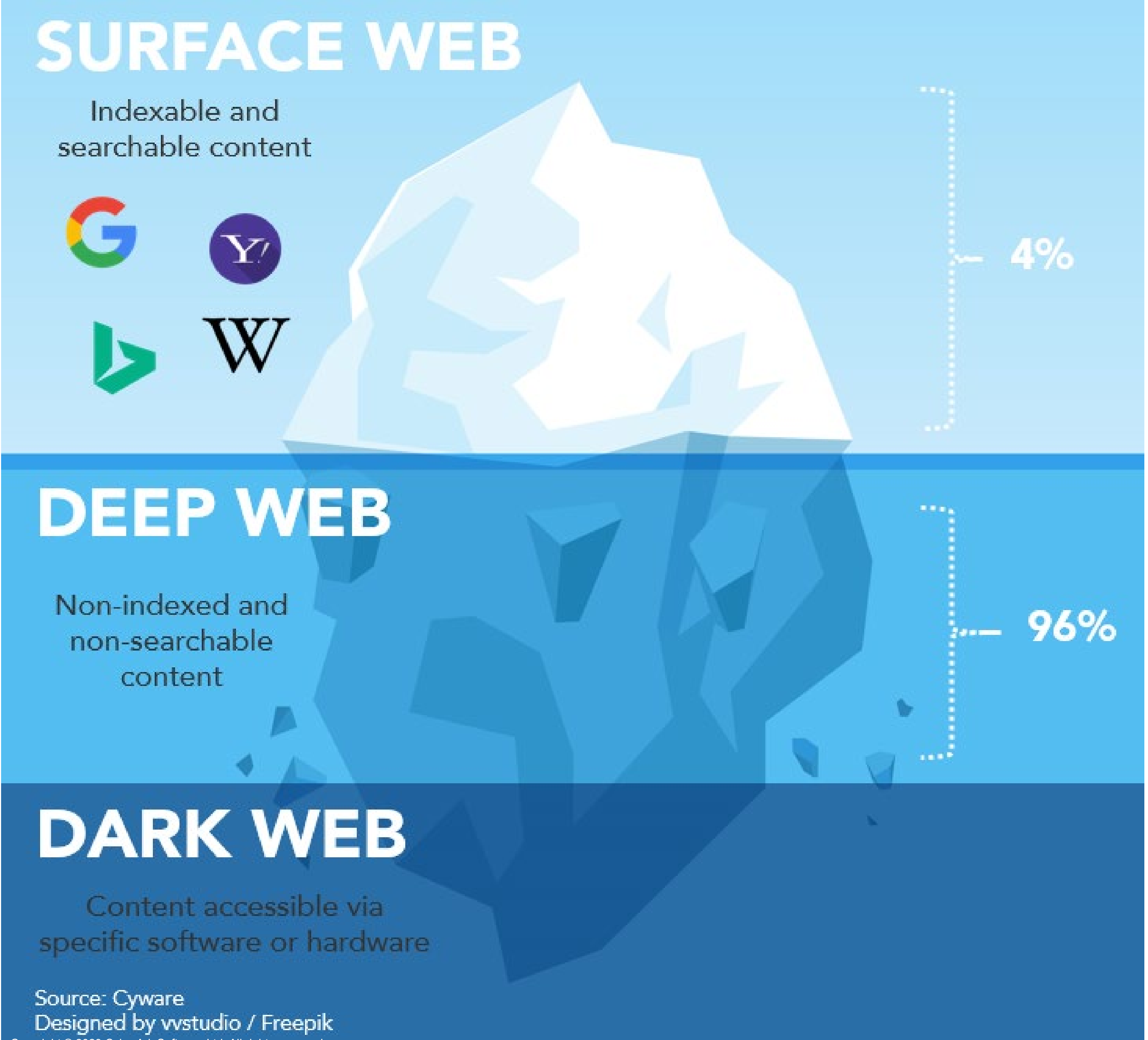
CyberArk Blog Team | 9/20/22

Share This!

een infected with malware, exposing those the contractor's
credentials. The attacker then repeatedly tried to log in to the

n. EDT

What is the Dark Web?



SURFACE WEB

Indexable and searchable content

4%

DEEP WEB

Non-indexed and non-searchable content

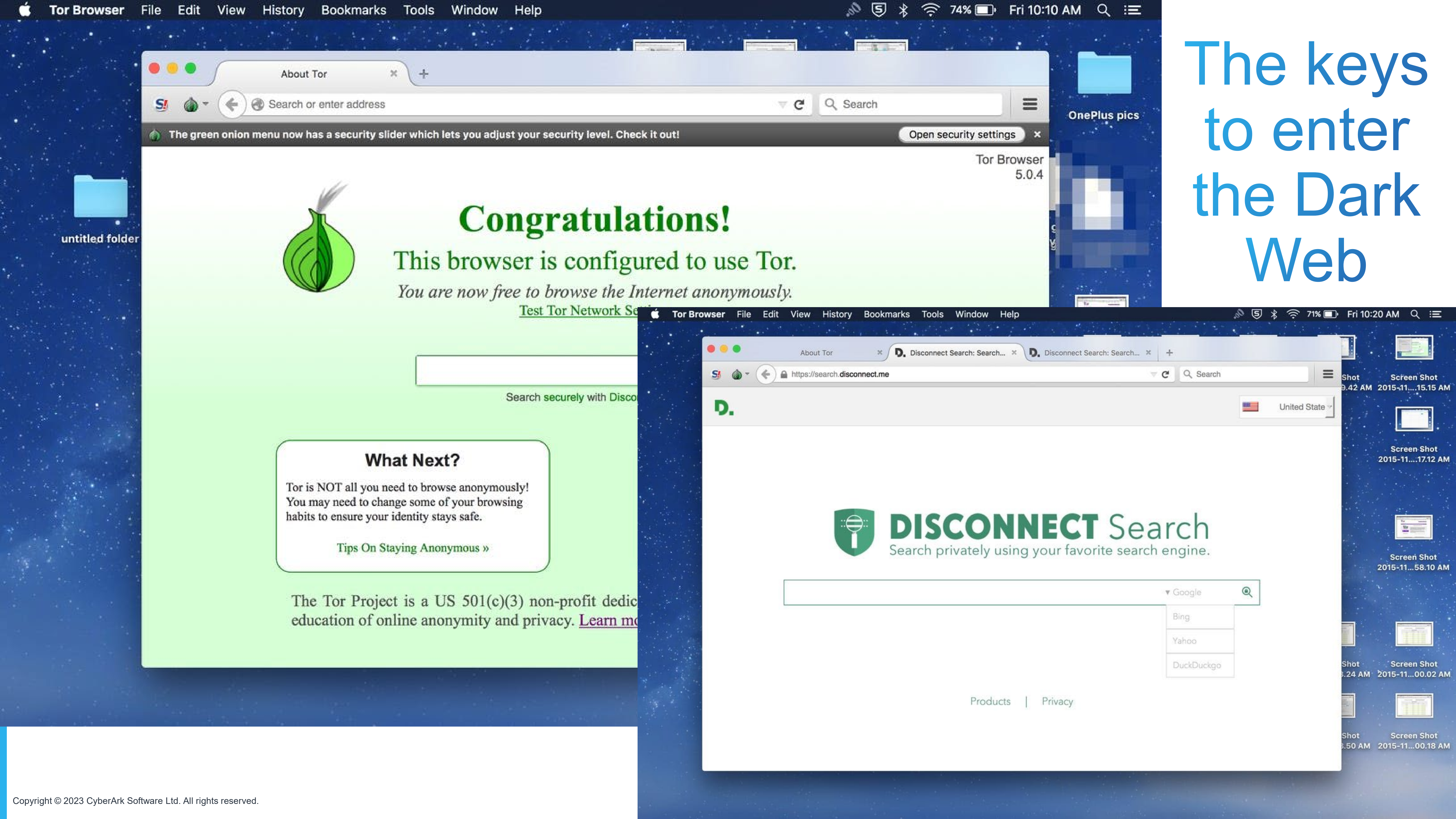
96%

DARK WEB

Content accessible via specific software or hardware

Source: Cyware
Designed by vvstudio / Freepik

The keys to enter the Dark Web



The green onion menu now has a security slider which lets you adjust your security level. Check it out!

Tor Browser 5.0.4

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

Test Tor Network Se

Search securely with Disco

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

Tips On Staying Anonymous »

The Tor Project is a US 501(c)(3) non-profit dedic education of online anonymity and privacy. Learn mo

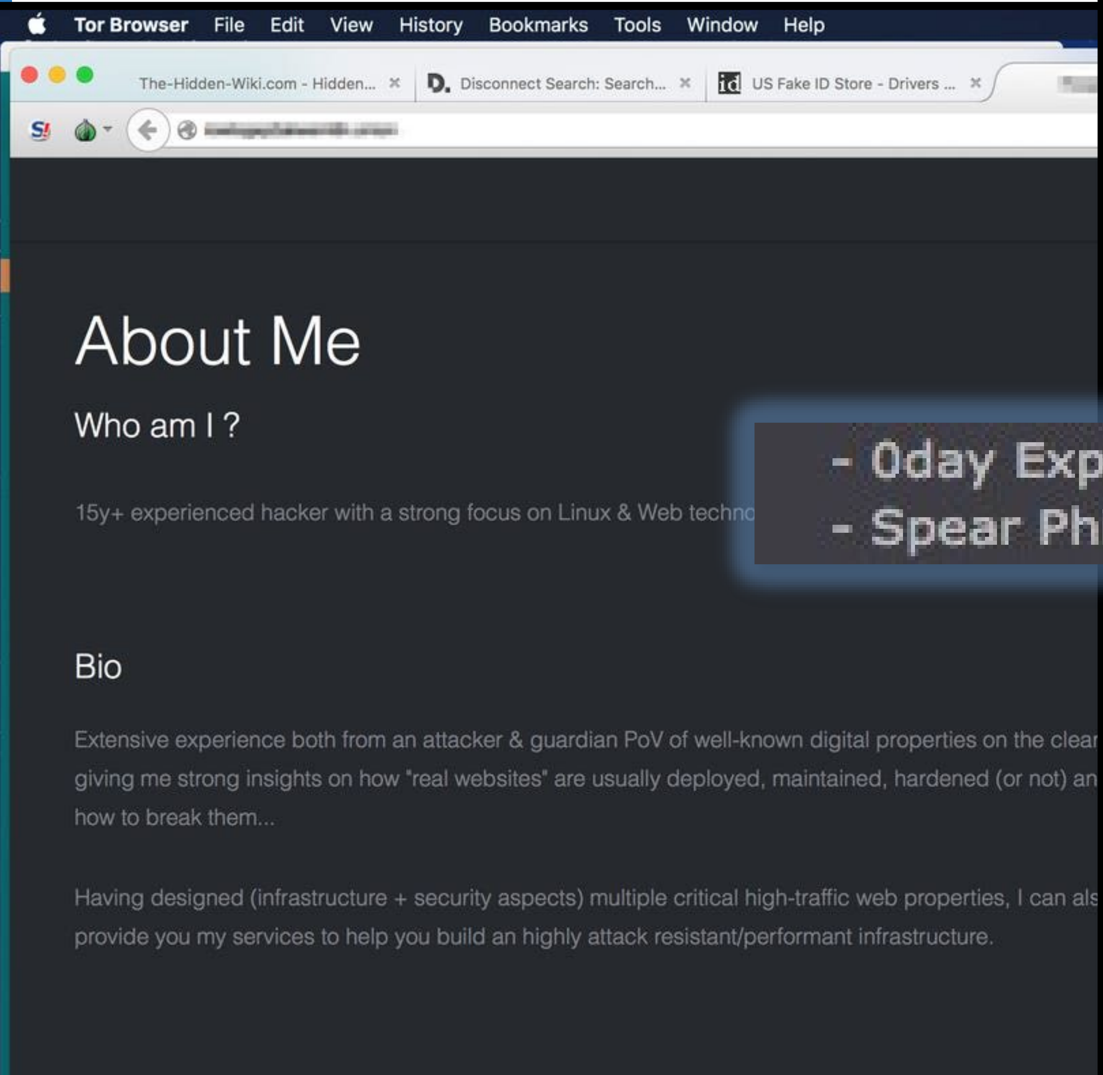
Tor Browser
File
Edit
View
History
Bookmarks
Tools
Window
Help
71%
Fri 10:20 AM
About Tor
Disconnect Search: Search...
Disconnect Search: Search...
https://search.disconnect.me
Search
United State
Screen Shot 2015-11....15.15 AM
Screen Shot 2015-11....17.12 AM
Screen Shot 2015-11....58.10 AM
Screen Shot 2015-11....00.02 AM
Screen Shot 2015-11....00.18 AM

DISCONNECT Search

Search privately using your favorite search engine.

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

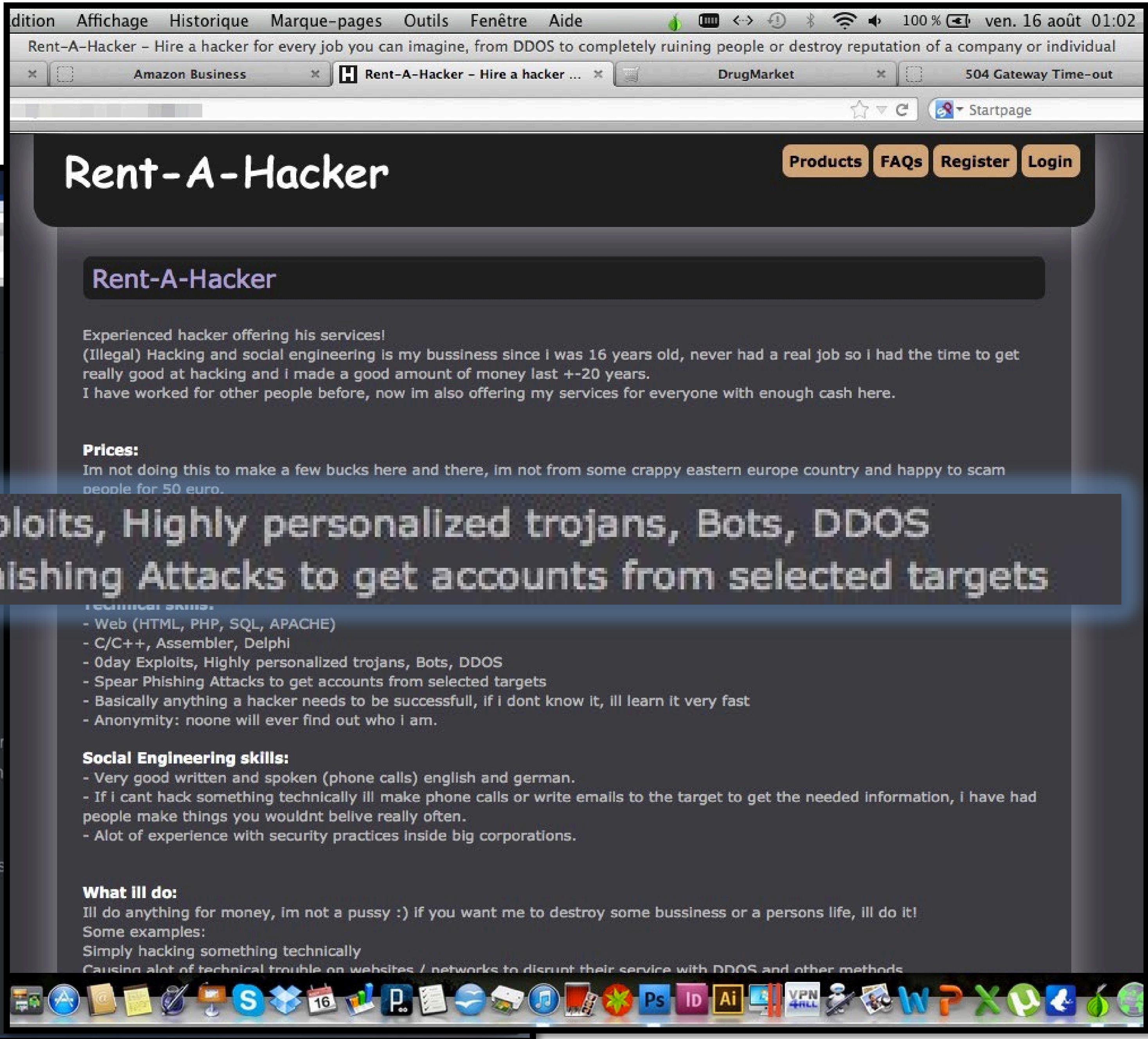
Who am I ?

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

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) an
how to break them...

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



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

Rent-A-Hacker

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.

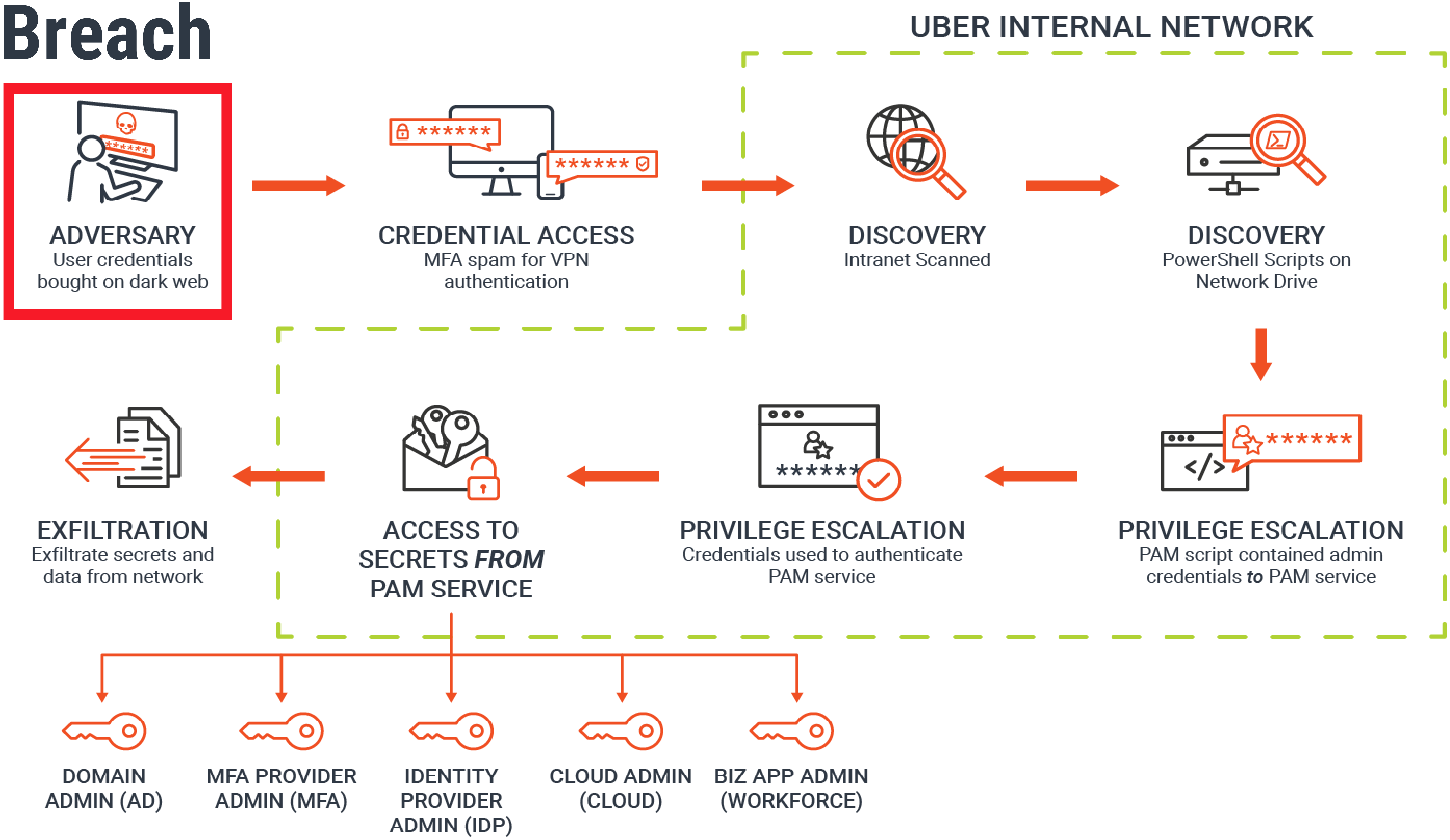
- 0day Exploits, Highly personalized trojans, Bots, DDOS
- Spear Phishing Attacks to get accounts from selected targets

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 belive 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



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

DOMAIN ADMIN (AD)

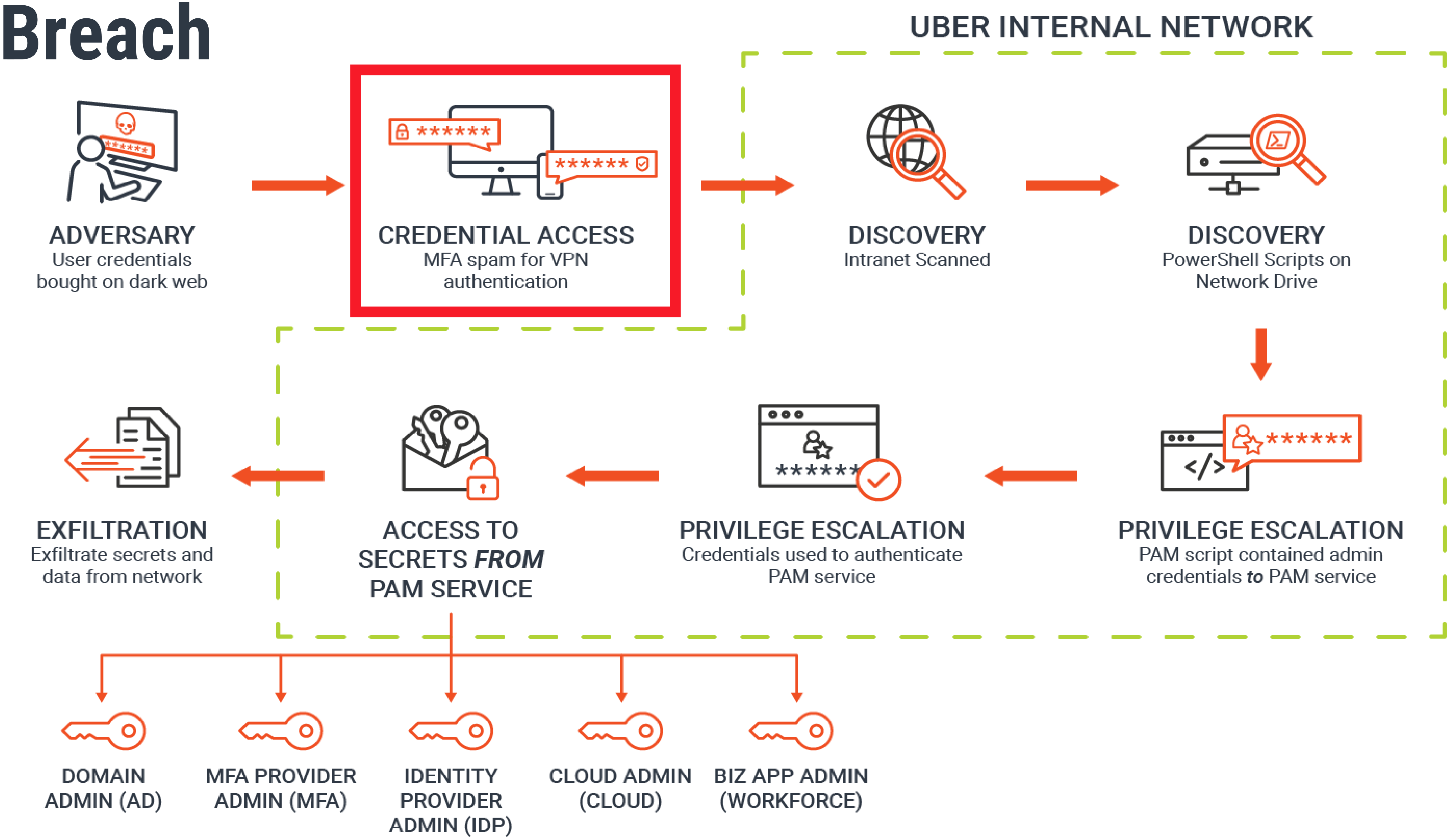
MFA PROVIDER ADMIN (MFA)

IDENTITY PROVIDER ADMIN (IDP)

CLOUD ADMIN (CLOUD)

BIZ APP ADMIN (WORKFORCE)

Uber Breach



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

DOMAIN ADMIN (AD)

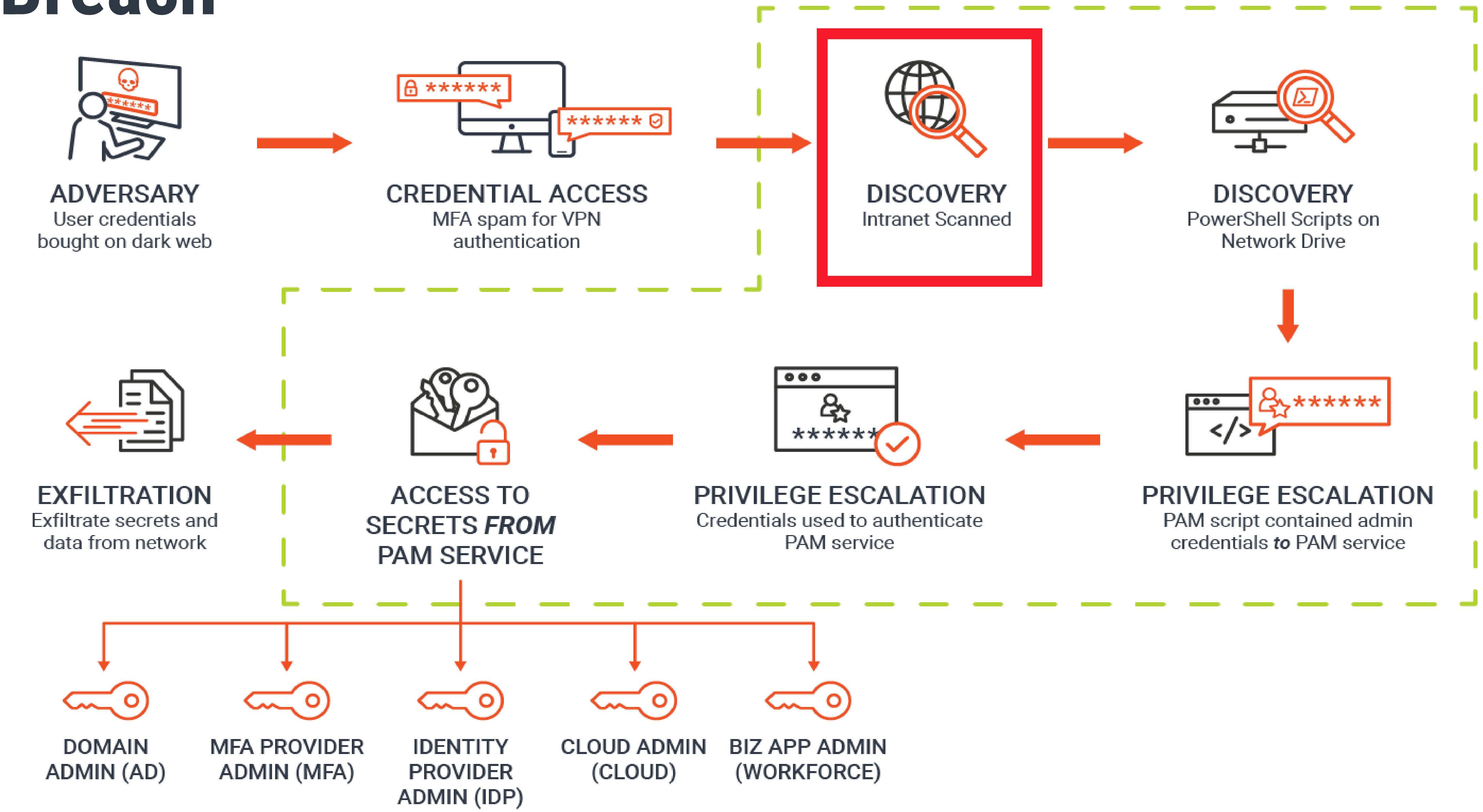
MFA PROVIDER ADMIN (MFA)

IDENTITY PROVIDER ADMIN (IDP)

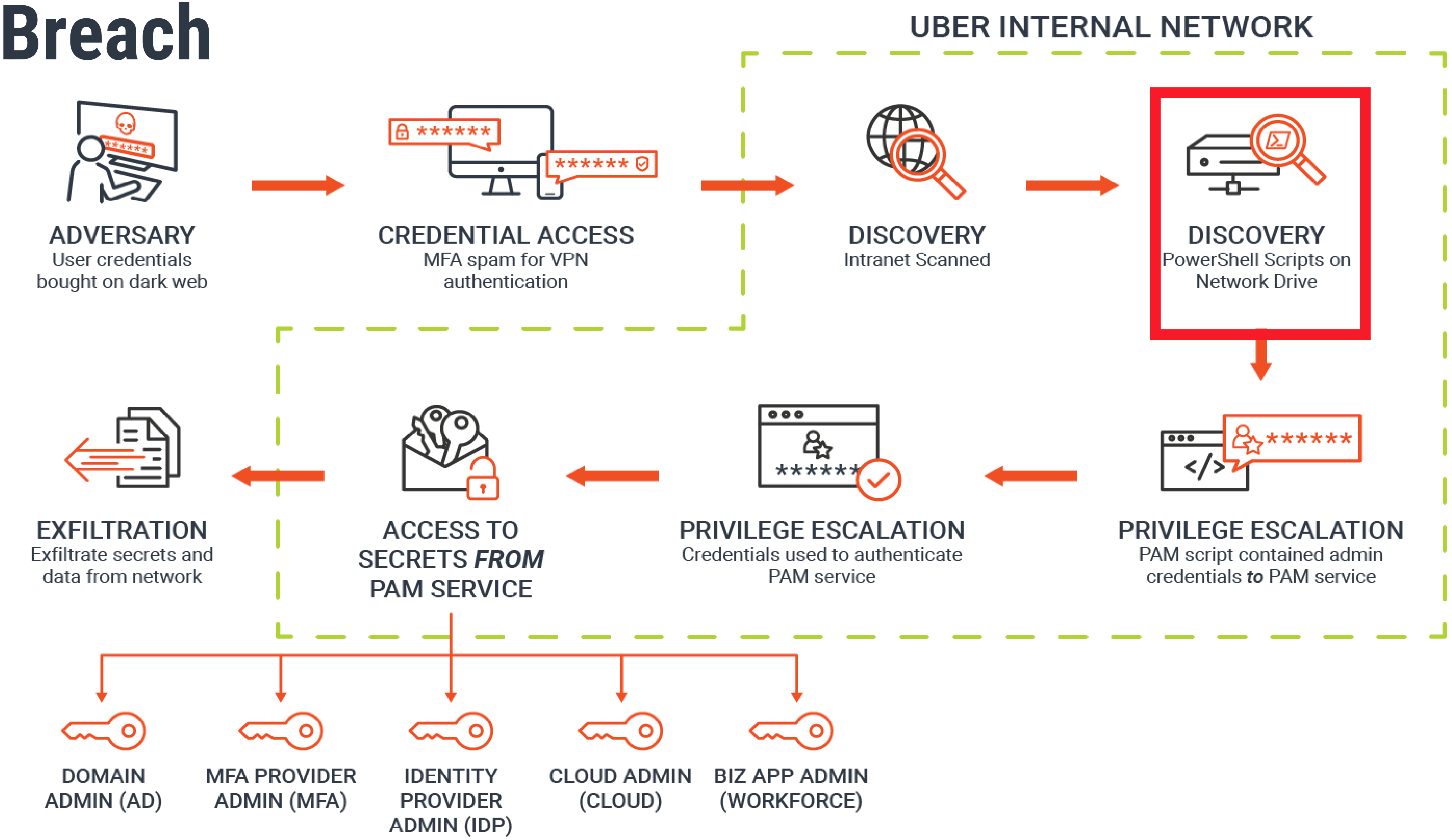
CLOUD ADMIN (CLOUD)

BIZ APP ADMIN (WORKFORCE)

Uber Breach


UBER INTERNAL NETWORK
ADVERSARY
User credentials bought on dark web
CREDENTIAL ACCESS
MFA spam for VPN authentication
DISCOVERY
Intranet Scanned
DISCOVERY
PowerShell Scripts on Network Drive
PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service
PRIVILEGE ESCALATION
Credentials used to authenticate PAM service
ACCESS TO SECRETS *FROM* PAM SERVICE
EXFILTRATION
Exfiltrate secrets and data from network
DOMAIN ADMIN (AD)
MFA PROVIDER ADMIN (MFA)
IDENTITY PROVIDER ADMIN (IDP)
CLOUD ADMIN (CLOUD)
BIZ APP ADMIN (WORKFORCE)

Uber Breach



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

DOMAIN ADMIN (AD)

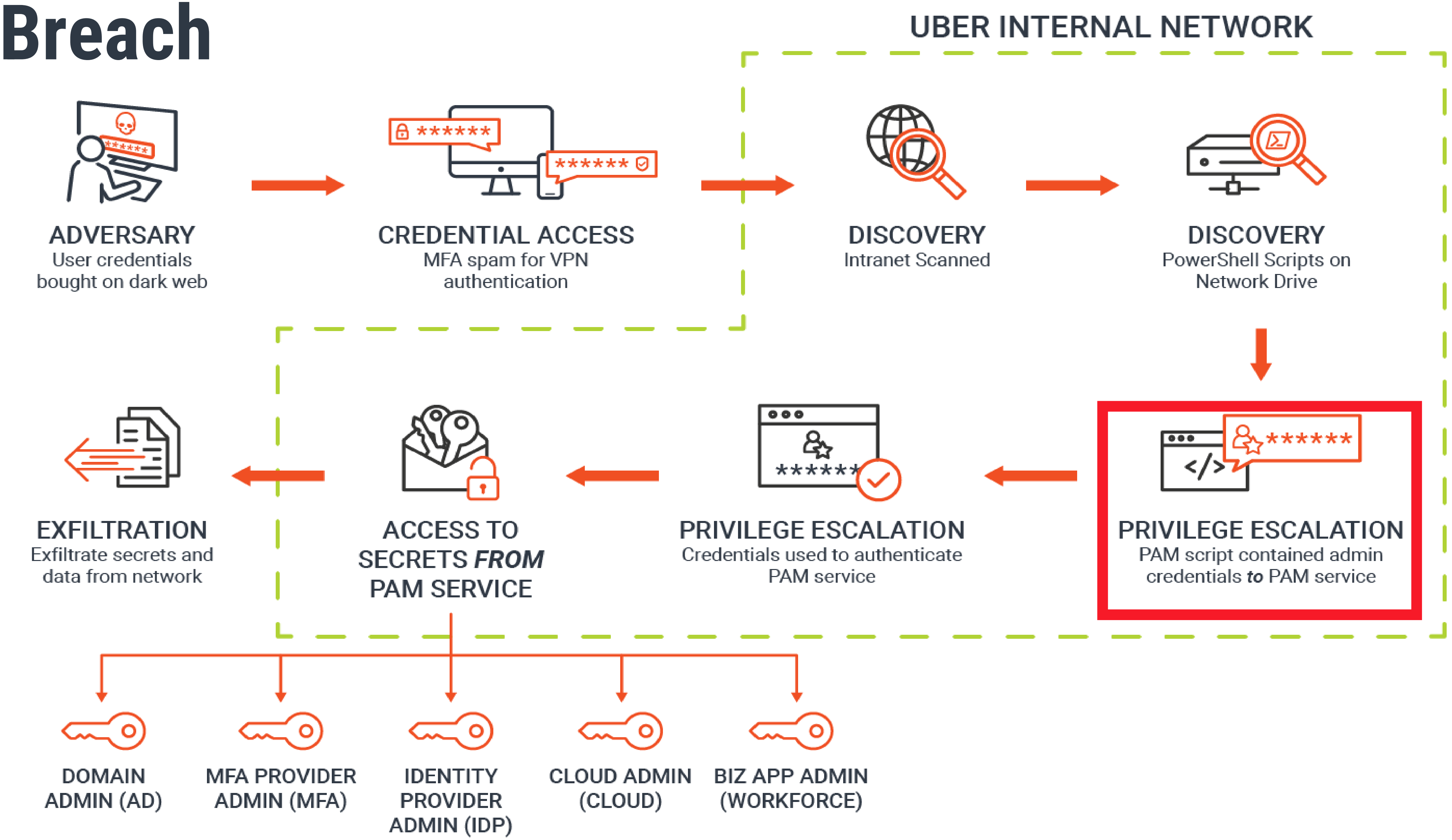
MFA PROVIDER ADMIN (MFA)

IDENTITY PROVIDER ADMIN (IDP)

CLOUD ADMIN (CLOUD)

BIZ APP ADMIN (WORKFORCE)

Uber Breach



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

DOMAIN ADMIN (AD)

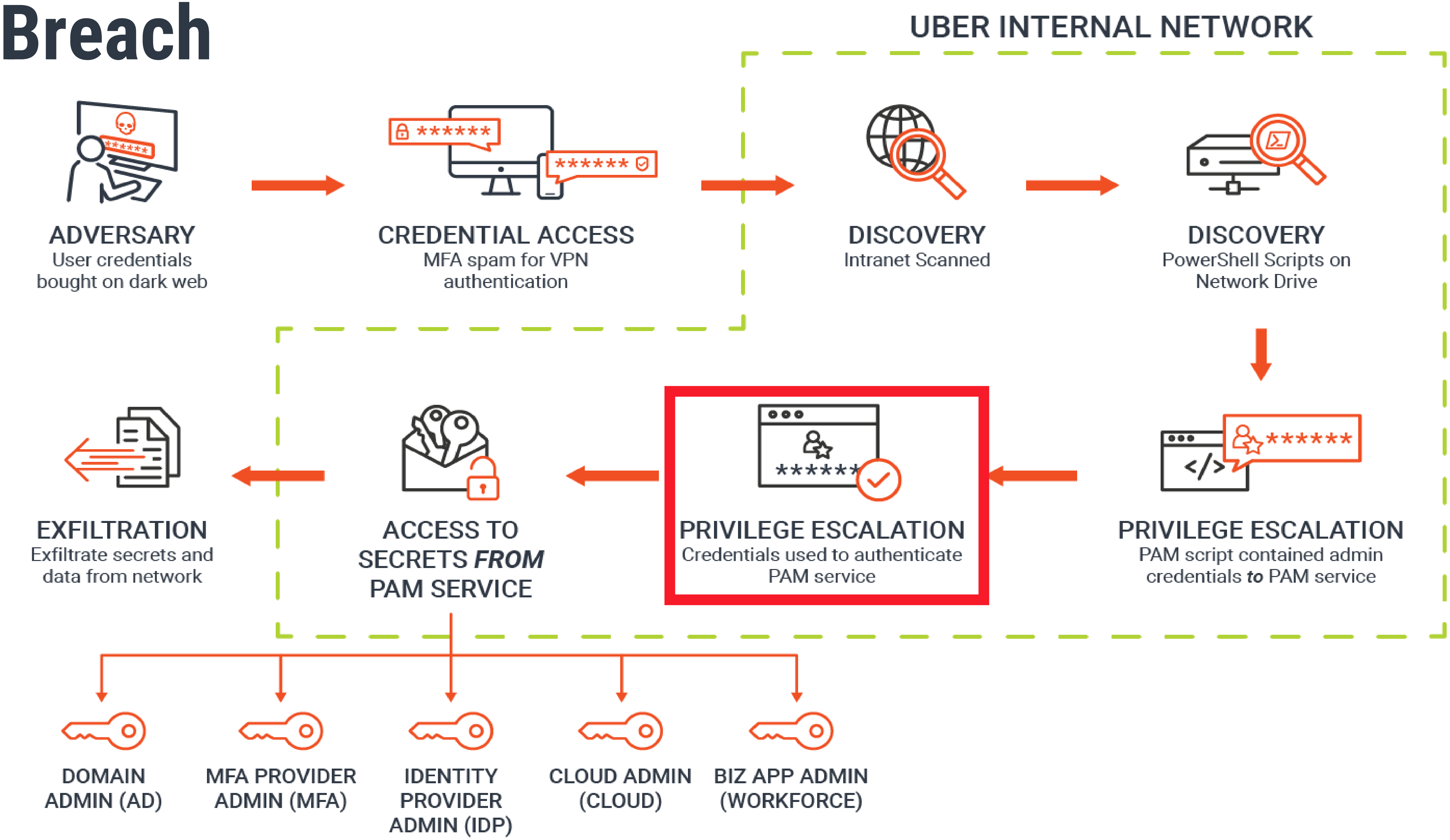
MFA PROVIDER ADMIN (MFA)

IDENTITY PROVIDER ADMIN (IDP)

CLOUD ADMIN (CLOUD)

BIZ APP ADMIN (WORKFORCE)

Uber Breach



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

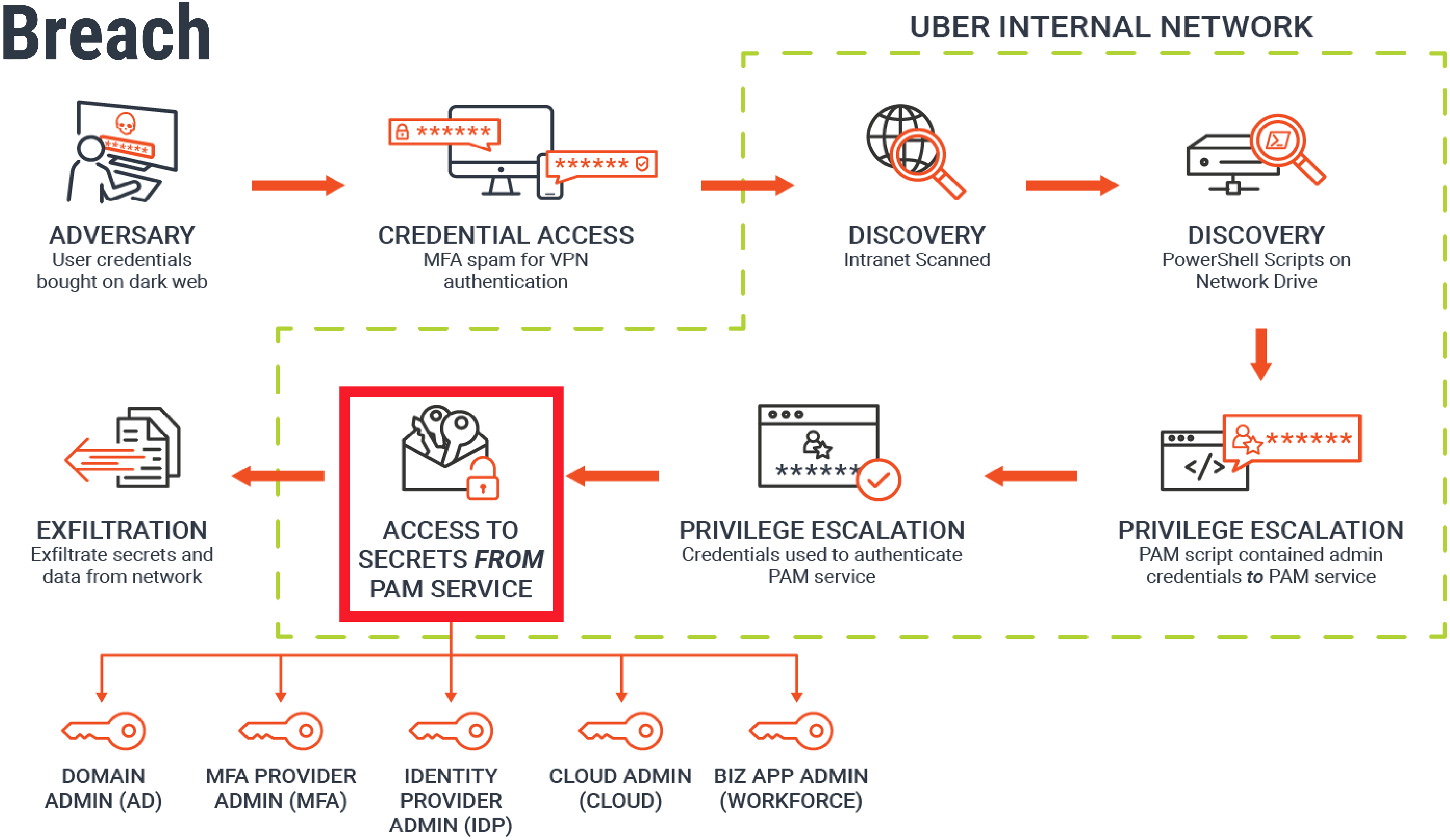
PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

- DOMAIN ADMIN (AD)
- MFA PROVIDER ADMIN (MFA)
- IDENTITY PROVIDER ADMIN (IDP)
- CLOUD ADMIN (CLOUD)
- BIZ APP ADMIN (WORKFORCE)

Uber Breach



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

DOMAIN ADMIN (AD)

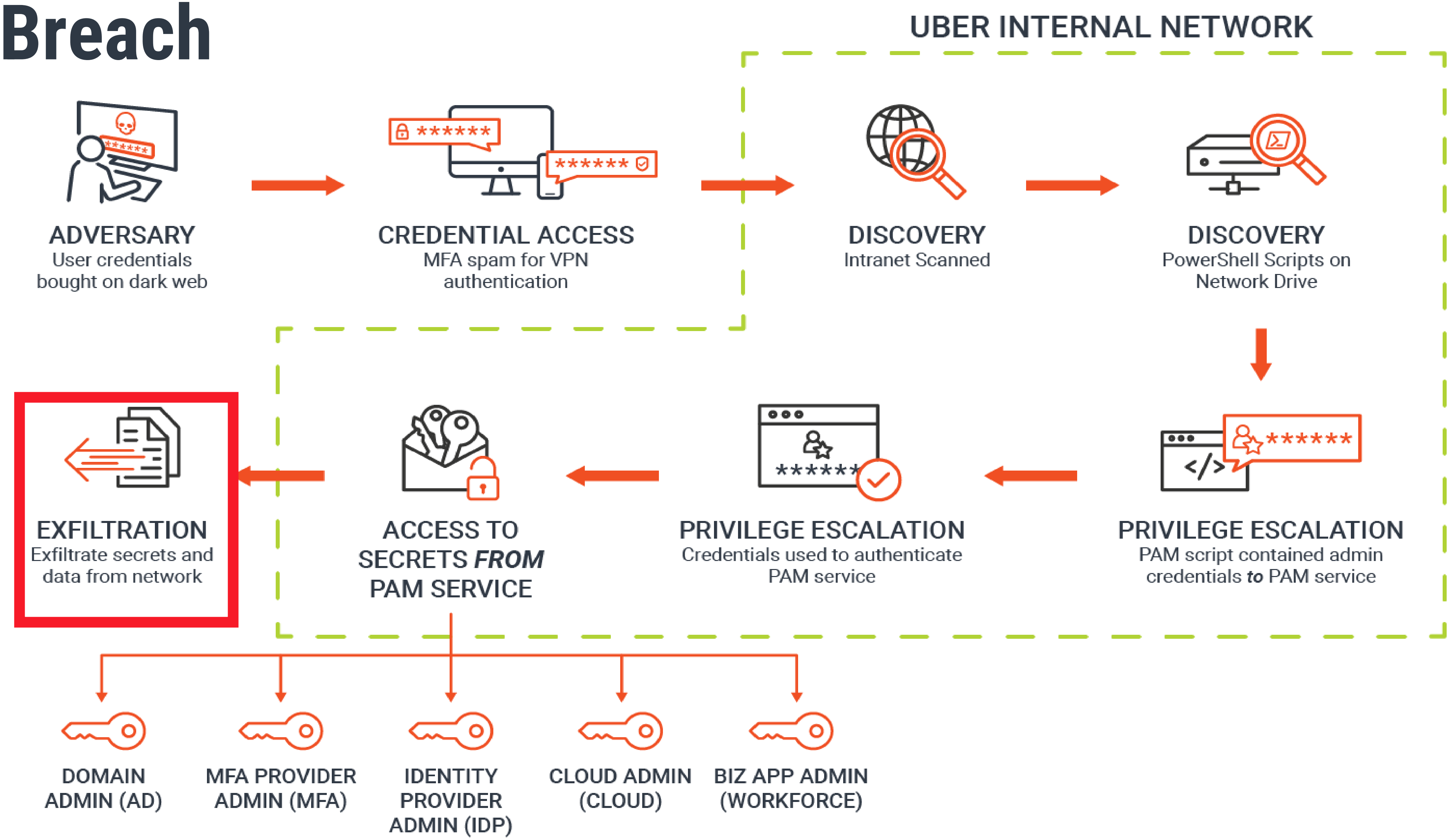
MFA PROVIDER ADMIN (MFA)

IDENTITY PROVIDER ADMIN (IDP)

CLOUD ADMIN (CLOUD)

BIZ APP ADMIN (WORKFORCE)

Uber Breach



UBER INTERNAL NETWORK

ADVERSARY
User credentials bought on dark web

CREDENTIAL ACCESS
MFA spam for VPN authentication

DISCOVERY
Intranet Scanned

DISCOVERY
PowerShell Scripts on Network Drive

PRIVILEGE ESCALATION
PAM script contained admin credentials *to* PAM service

PRIVILEGE ESCALATION
Credentials used to authenticate PAM service

ACCESS TO SECRETS *FROM* PAM SERVICE

EXFILTRATION
Exfiltrate secrets and data from network

DOMAIN ADMIN (AD)

MFA PROVIDER ADMIN (MFA)

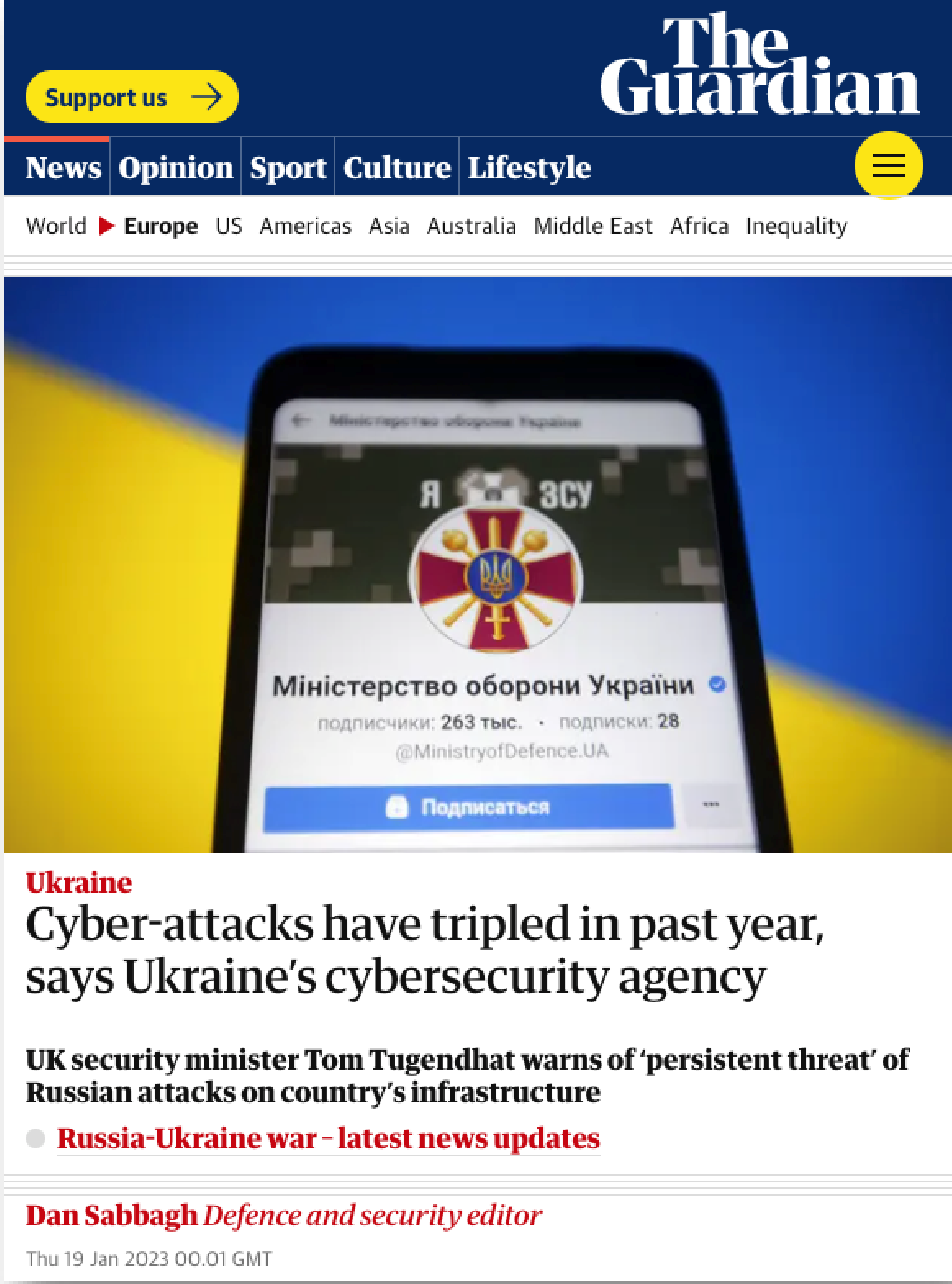
IDENTITY PROVIDER ADMIN (IDP)

CLOUD ADMIN (CLOUD)

BIZ APP ADMIN (WORKFORCE)

Russia-Ukraine War
Cyber Warfare Aspect

Ukraine has been a permanent target of cyber-attacks since 2014



Support us →
Я ЗСУ
Міністерство оборони України
подписчики: 263 тыс. · подписки: 28
@MinistryofDefence.UA
Подписаться

The Guardian

News | Opinion | Sport | Culture | Lifestyle

World ▶ Europe US Americas Asia Australia Middle East Africa Inequality

Ukraine

Cyber-attacks have tripled in past year, says Ukraine's cybersecurity agency

UK security minister Tom Tugendhat warns of 'persistent threat' of Russian attacks on country's infrastructure

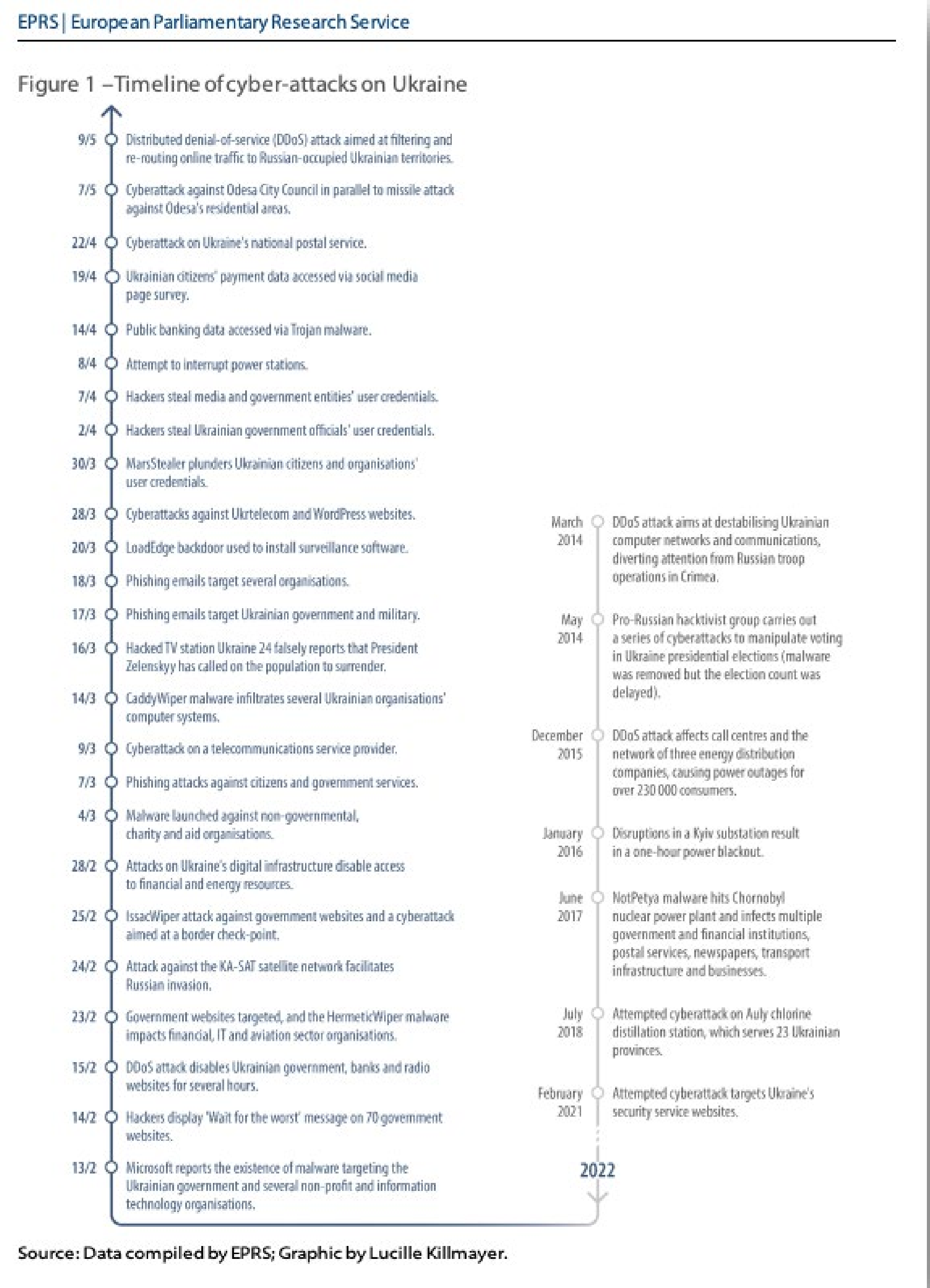
- Russia-Ukraine war - latest news updates

Dan Sabbagh *Defence and security editor*

Thu 19 Jan 2023 00.01 GMT

Russia-Ukraine War
Cyber Warfare Aspect

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

9/5	Distributed denial-of-service (DDoS) attack aimed at filtering and re-routing online traffic to Russian-occupied Ukrainian territories.
7/5	Cyberattack against Odesa City Council in parallel to missile attack against Odesa's residential areas.
22/4	Cyberattack on Ukraine's national postal service.
19/4	Ukrainian citizens' payment data accessed via social media page survey.
14/4	Public banking data accessed via Trojan malware.
8/4	Attempt to interrupt power stations.
7/4	Hackers steal media and government entities' user credentials.
2/4	Hackers steal Ukrainian government officials' user credentials.
30/3	MarsStealer plunders Ukrainian citizens and organisations' user credentials.
28/3	Cyberattacks against Ukrtelecom and WordPress websites.
20/3	LoadEdge backdoor used to install surveillance software.
18/3	Phishing emails target several organisations.
17/3	Phishing emails target Ukrainian government and military.
16/3	Hacked TV station Ukraine 24 falsely reports that President Zelenskyy has called on the population to surrender.
14/3	CaddyWiper malware infiltrates several Ukrainian organisations' computer systems.
9/3	Cyberattack on a telecommunications service provider.
7/3	Phishing attacks against citizens and government services.
4/3	Malware launched against non-governmental, charity and aid organisations.
28/2	Attacks on Ukraine's digital infrastructure disable access to financial and energy resources.
25/2	IssacWiper attack against government websites and a cyberattack aimed at a border check-point.
24/2	Attack against the KA-SAT satellite network facilitates Russian invasion.
23/2	Government websites targeted, and the HermeticWiper malware impacts financial, IT and aviation sector organisations.
15/2	DDoS attack disables Ukrainian government, banks and radio websites for several hours.
14/2	Hackers display 'Wait for the worst' message on 70 government websites.
13/2	Microsoft reports the existence of malware targeting the Ukrainian government and several non-profit and information technology organisations.

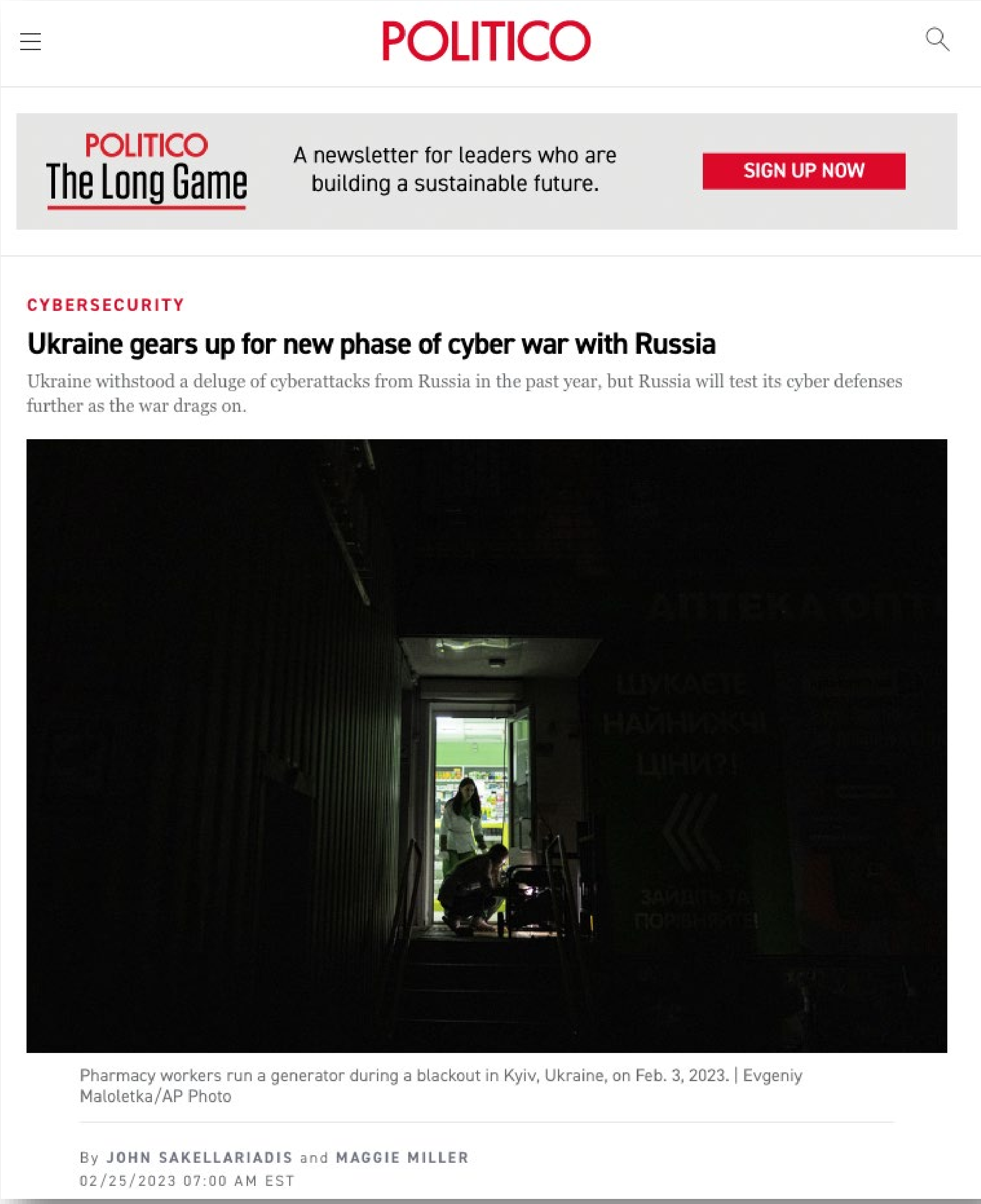
March 2014	DDoS attack aims at destabilising Ukrainian computer networks and communications, diverting attention from Russian troop operations in Crimea.
May 2014	Pro-Russian hacktivist group carries out a series of cyberattacks to manipulate voting in Ukraine presidential elections (malware was removed but the election count was delayed).
December 2015	DDoS attack affects call centres and the network of three energy distribution companies, causing power outages for over 230 000 consumers.
January 2016	Disruptions in a Kyiv substation result in a one-hour power blackout.
June 2017	NotPetya malware hits Chornobyl nuclear power plant and infects multiple government and financial institutions, postal services, newspapers, transport infrastructure and businesses.
July 2018	Attempted cyberattack on Auly chlorine distillation station, which serves 23 Ukrainian provinces.
February 2021	Attempted cyberattack targets Ukraine's security service websites.

2022

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

Russia-Ukraine War
Cyber Warfare Aspect

Thousands of attacks occur every month, making Ukraine the **"perfect sandbox for those looking to test new cyberweapons, tactics and tools"**



POLITICO

CYBERSECURITY

Ukraine gears up for new phase of cyber war with Russia

Ukraine withstood a deluge of cyberattacks from Russia in the past year, but Russia will test its cyber defenses further as the war drags on.

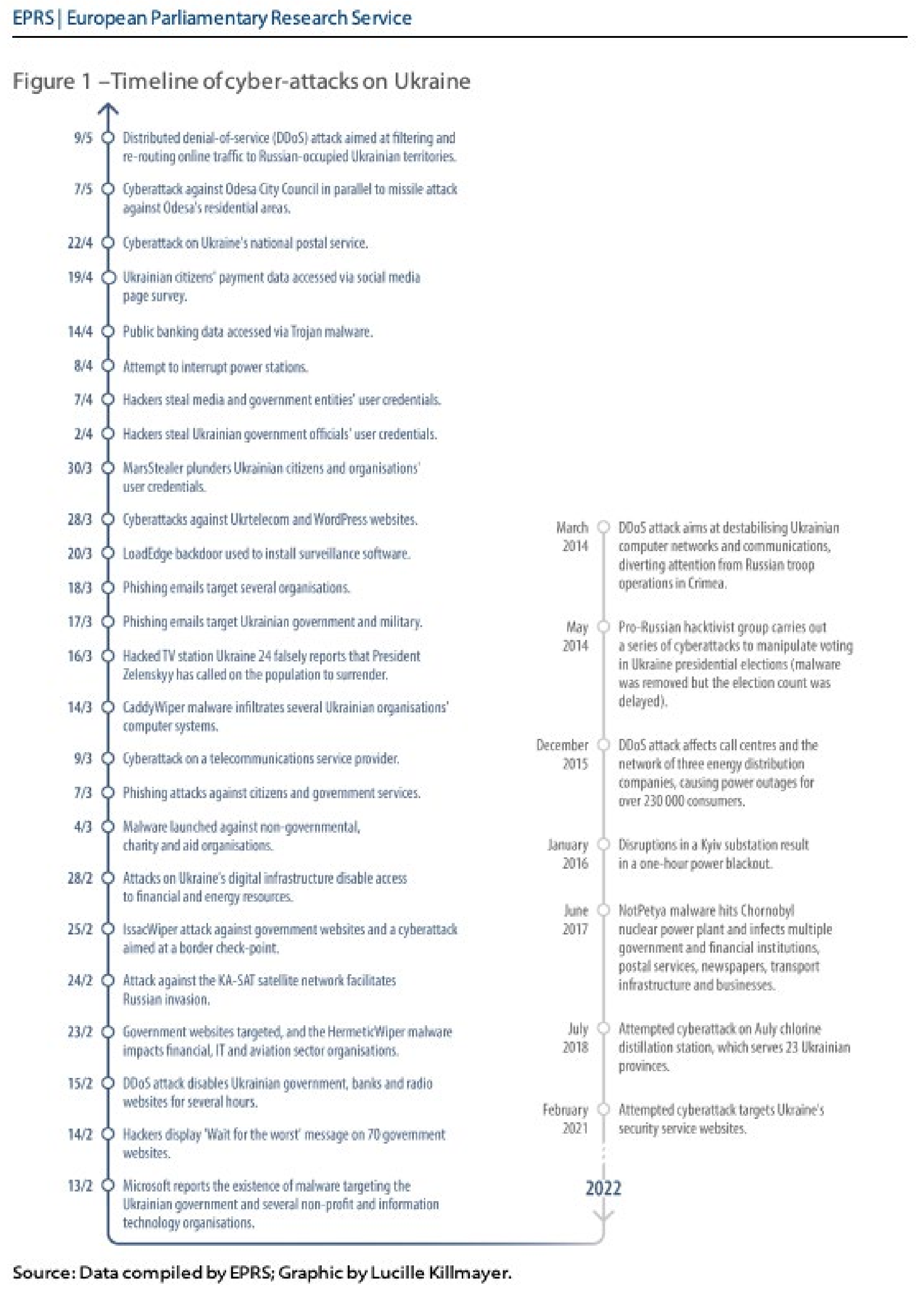
Pharmacy workers run a generator during a blackout in Kyiv, Ukraine, on Feb. 3, 2023. | Evgeniy Maloletka/AP Photo

By JOHN SAKELLARIADIS and MAGGIE MILLER
02/25/2023 07:00 AM EST

Russia-Ukraine War

Cyber Warfare Aspect

- 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)
- …



EPRS | European Parliamentary Research Service

Figure 1 –Timeline of cyber-attacks on Ukraine

9/5 Distributed denial-of-service (DDoS) attack aimed at filtering and re-routing online traffic to Russian-occupied Ukrainian territories.

7/5 Cyberattack against Odesa City Council in parallel to missile attack against Odesa's residential areas.

22/4 Cyberattack on Ukraine's national postal service.

19/4 Ukrainian citizens' payment data accessed via social media page survey.

14/4 Public banking data accessed via Trojan malware.

8/4 Attempt to interrupt power stations.

7/4 Hackers steal media and government entities' user credentials.

2/4 Hackers steal Ukrainian government officials' user credentials.

30/3 MarsStealer plunders Ukrainian citizens and organisations' user credentials.

28/3 Cyberattacks against Ukrtelecom and WordPress websites.

20/3 LoadEdge backdoor used to install surveillance software.

18/3 Phishing emails target several organisations.

17/3 Phishing emails target Ukrainian government and military.

16/3 Hacked TV station Ukraine 24 falsely reports that President Zelenskyy has called on the population to surrender.

14/3 CaddyWiper malware infiltrates several Ukrainian organisations' computer systems.

9/3 Cyberattack on a telecommunications service provider.

7/3 Phishing attacks against citizens and government services.

4/3 Malware launched against non-governmental, charity and aid organisations.

28/2 Attacks on Ukraine's digital infrastructure disable access to financial and energy resources.

25/2 IssacWiper attack against government websites and a cyberattack aimed at a border check-point.

24/2 Attack against the KA-SAT satellite network facilitates Russian invasion.

23/2 Government websites targeted, and the HermeticWiper malware impacts financial, IT and aviation sector organisations.

15/2 DDoS attack disables Ukrainian government, banks and radio websites for several hours.

14/2 Hackers display 'Wait for the worst' message on 70 government websites.

13/2 Microsoft reports the existence of malware targeting the Ukrainian government and several non-profit and information technology organisations.

March 2014 DDoS attack aims at destabilising Ukrainian computer networks and communications, diverting attention from Russian troop operations in Crimea.

May 2014 Pro-Russian hacktivist group carries out a series of cyberattacks to manipulate voting in Ukraine presidential elections (malware was removed but the election count was delayed).

December 2015 DDoS attack affects call centres and the network of three energy distribution companies, causing power outages for over 230 000 consumers.

January 2016 Disruptions in a Kyiv substation result in a one-hour power blackout.

June 2017 NotPetya malware hits Chornobyl nuclear power plant and infects multiple government and financial institutions, postal services, newspapers, transport infrastructure and businesses.

July 2018 Attempted cyberattack on Auly chlorine distillation station, which serves 23 Ukrainian provinces.

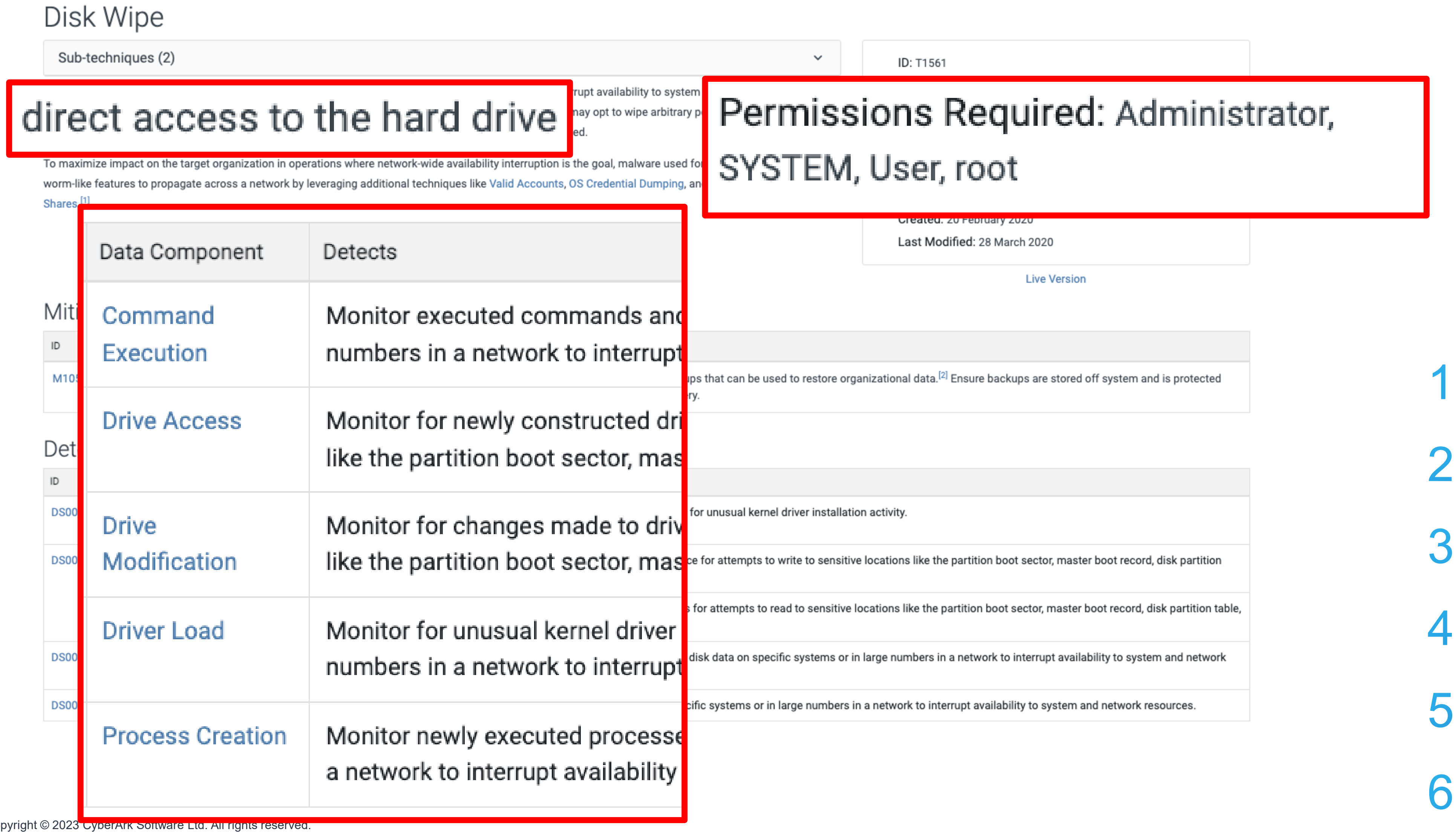
February 2021 Attempted cyberattack targets Ukraine's security service websites.

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

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

Russia-Ukraine War | Top Attack Types

MITRE | ATT&CK®



Disk Wipe

Sub-techniques (2)

ID: T1561

rupt availability to system

nay opt to wipe arbitrary p

ed.

direct access to the hard drive

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]

Permissions Required: Administrator, SYSTEM, User, root

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.

Det

ID

DS00 for unusual kernel driver installation activity.

DS00 ce for attempts to write to sensitive locations like the partition boot sector, master boot record, disk partition

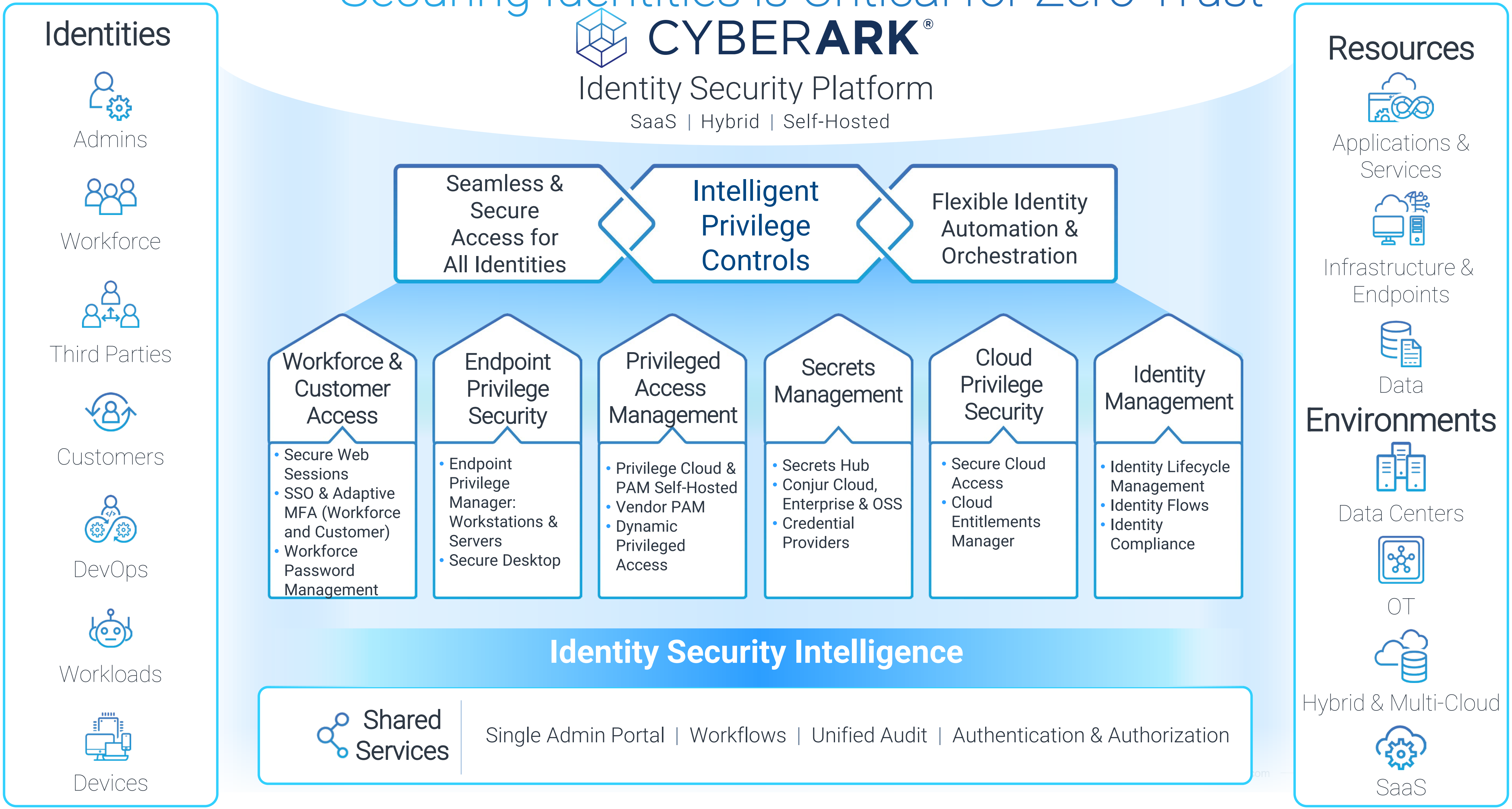
for attempts to read to sensitive locations like the partition boot sector, master boot record, disk partition table,

DS00 disk data on specific systems or in large numbers in a network to interrupt availability to system and network

DS00 cific 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



CYBERARK®

Identity Security Platform

SaaS | Hybrid | Self-Hosted

Identities

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

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

Shared Services

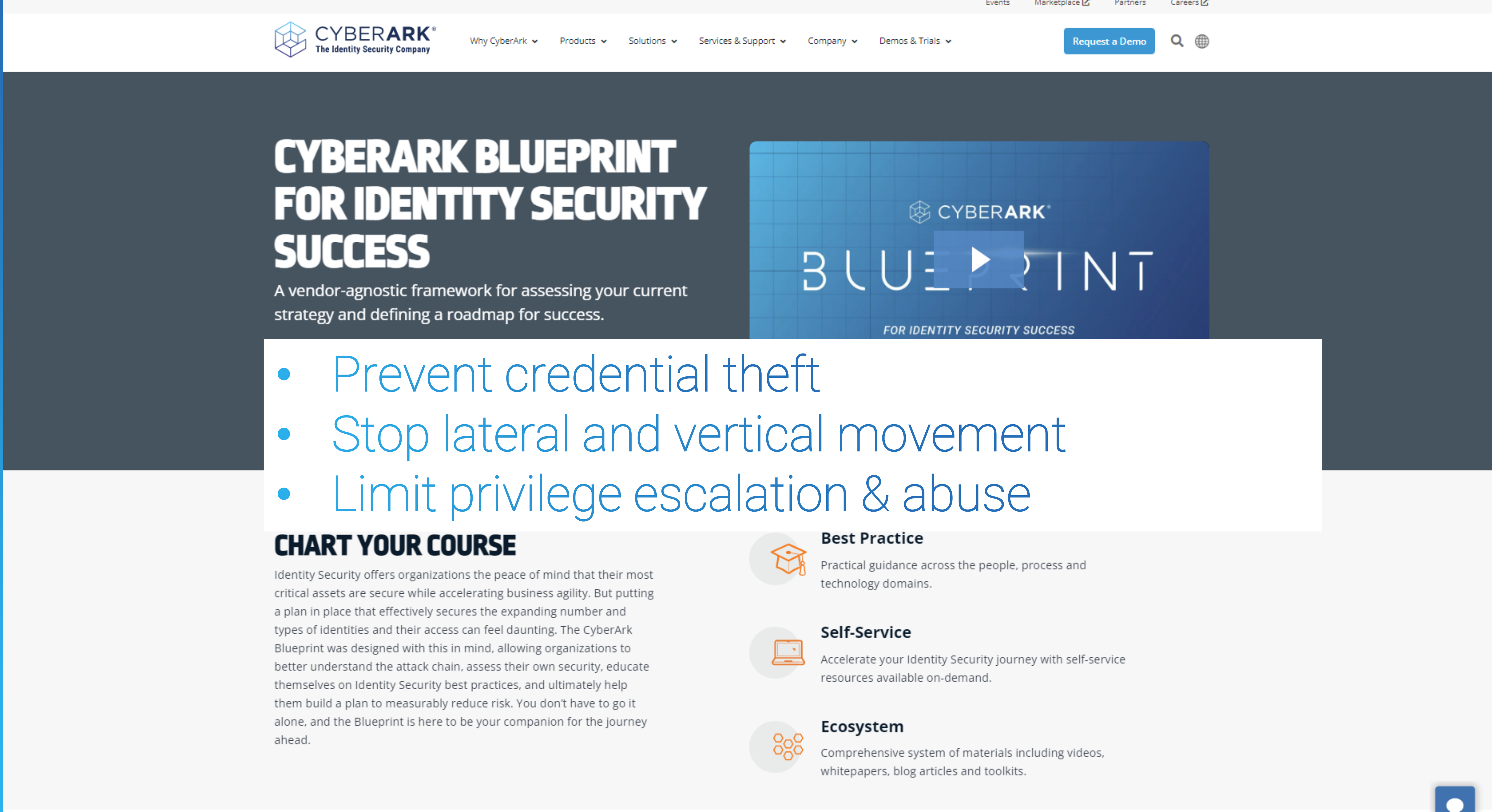
Single Admin Portal | Workflows | Unified Audit | Authentication & Authorization

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.

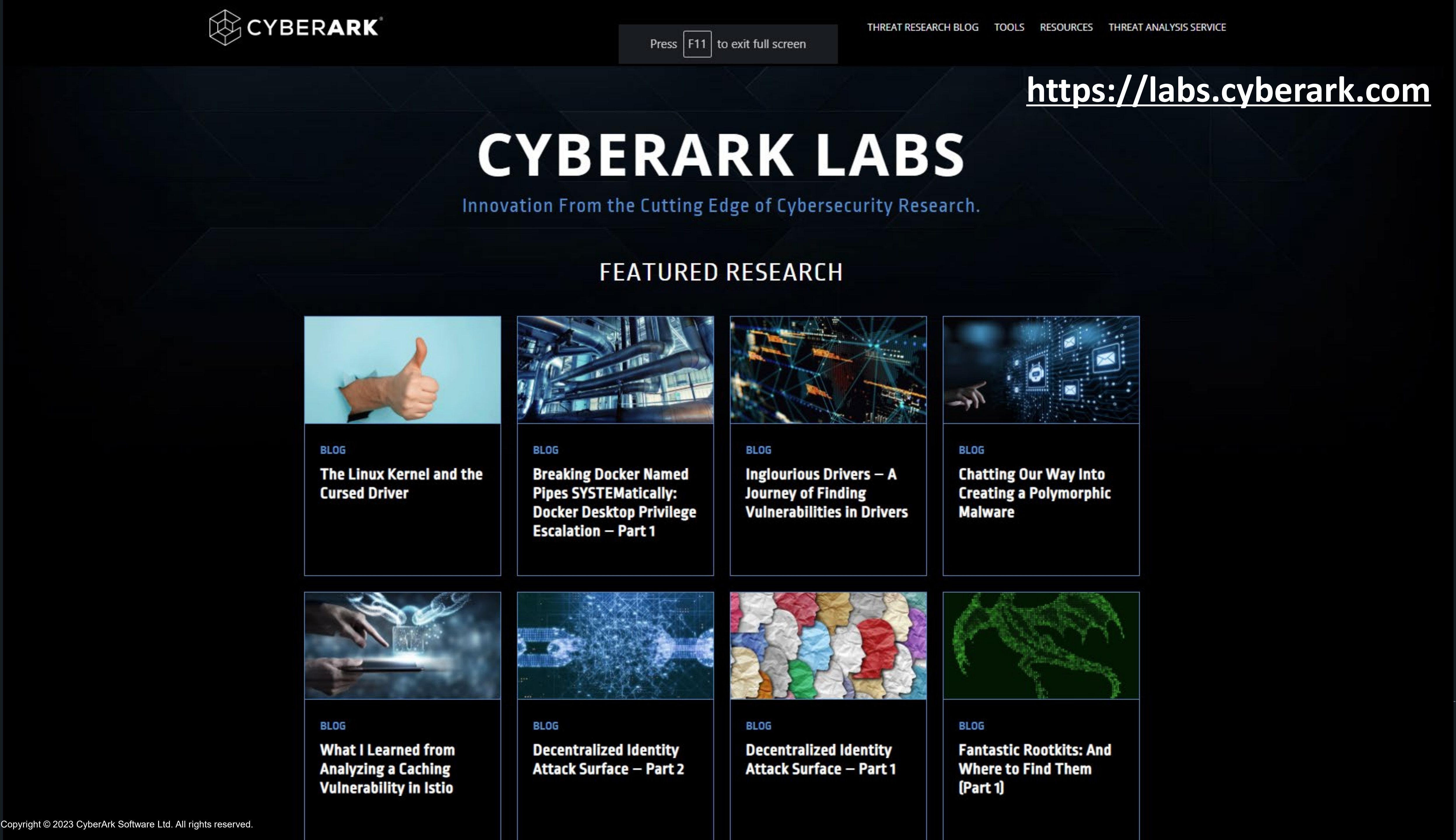
Self-Service

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

Ecosystem

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

https://labs.cyberark.com



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)

https://www.cyberark.com/cyberark-ventures/

CYBERARK®

C³ Alliance

200+ Certified Partners

1KOSMOS
Ab Initio
Active Navigation
ANTWORKS Reimagine . Rethink . Recreate
ActiveBatch
algosec
amdocs
Apica
APPDYNAMICS
appviewX
aqua
asg technologies
atarlabs
Atos
AUTOMATION ANYWHERE

aws
AXIS COMMUNICATIONS
Axios Systems ITSM & ITOM SOFTWARE
AXONIUS
ayehu
BACKBOX INTELLIGENT AUTOMATION
bambooHR
BigID
bitglass
bertin
beyond security
IB
blueprism Robotic Process Automation Software
bmc
Brainwave GRC

Bromium
ca technologies A Broadcom Company
cavirin
celonis
Check Point SOFTWARE TECHNOLOGIES LTD.
CHEF
cherwell
CIGENT
CLANGO
cloudbees
Cognizant
collibra
COMMVAULT
CONTRAST SECURITY
cortex

AutomationEdge
CROWDSTRIKE
CYBERBIT PROTECTING A NEW DIMENSION
CYBER OBSERVER
CRYPTOMATHIC
DATA443
datablink
DATAGUISE
DATAMATICS
DataSunrise
DB NETWORKS
DBmaestro DevOps for Database
DBSH BIG DATA INTEGRATION
denodo
DETACK
DELPHIX

Devolutions
BRANDLE
DEVICE42
digitate
docker
DUO
EATON
edgeverve An Infosys company
EKATA
elastic
EMERGYNT
Epic
Eracent
Evidian
exabeam
EZMCOM CONVENIENTLY SECURE
FIREEYE

FLEXAGON
CRYPTO4A
FLEXERA SOFTWARE
FOCAL POINT DATA RISK
FORESCOUT
FORTINET
FUTUREX
GitLab
GE Power
Google
harness
HCL
HIDEEZ
I4P
IBM
iCONDUCT integrating intelligence
ilantus The Cloud Identity People

illusive
IMAGEWARE SYSTEMS
IMPINJ
indeni
Informatica
Invicti
IP SOFT
iQuate
ITRS
JDisc
SONAR NoSQL Analytics
KEYFACTOR
Kleverware
KOFAX
Lenovo
leidos
Liquibase

logpoint
LogRhythm
LogicMonitor
Logsign
LUCIDEUS | SAFE
McAfee
Microsoft
METRIC INSIGHTS
CIPHER
NETSOL
netskope
netwrix
NICE
okta
Omada
onelogin
OpsRamp

Outpost24
paloalto NETWORKS
PCYSYS
PEGA
PENSANDO
Phantom
Phosphorus
Ping Identity
Pivotal
preempt
proofpoint
PROTEGRITY
PRi pontis research
protegrity
puppet
Qualys
RADIANT LOGIC

Red Hat
RAPID7
RICOH imagine. change.
RSA
SAASPASS
SailPoint
SAP
SCADAfence
ScriptRunner
SECRET DOUBLE OCTOPUS
SECUREAUTH
SECURONIX
servicenow
SIEMPLIFY
SILVERFORT
simeio
SKYBOX SECURITY

SmartRPA
SOROCO
SOFT WARFARE
solarwinds
SPHERE TECHNOLOGY SOLUTIONS
splunk>
STEALTHbits TECHNOLOGIES
StreamSets
SWIMLANE
SyferLock
Symantec
talend
TCPWave
HashiCorp Terraform
TEMPERED NETWORKS
tenable
THALES

transmit SECURITY
tripwire
TRUSONA
UiPath
UNBOUND
UKG
USERCUBE
utimaco
VENAFI
VARONIS
VISTARA
WorkFusion
WATERFALL Stronger Than Firewalls
workday
XYPRO Mission Critical Security
yubico
zenoss Own IT.

300+ Certified Joint Solutions

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

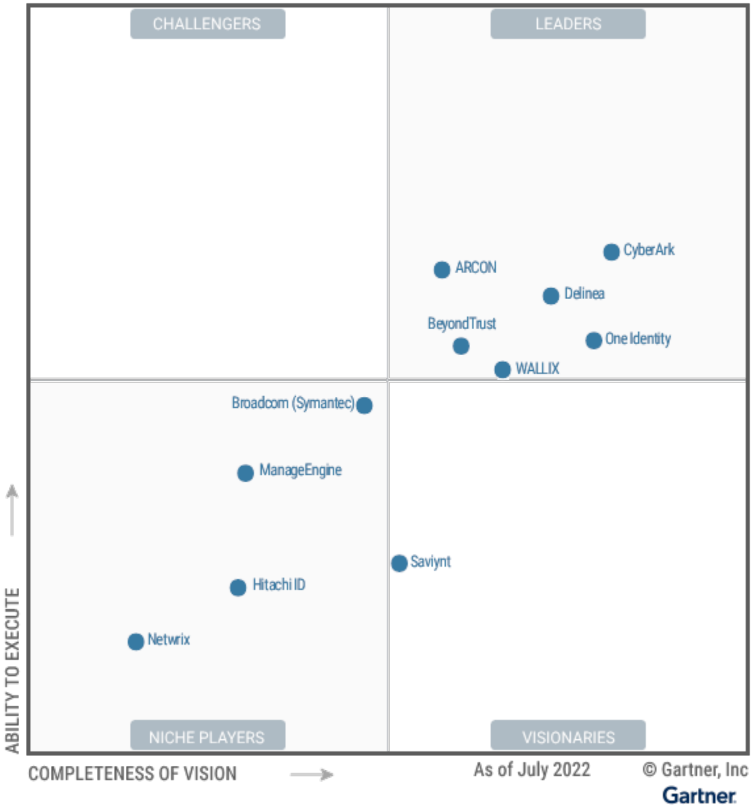
200+ Plug-ins

CPM Plug-ins
PSM Plug-ins

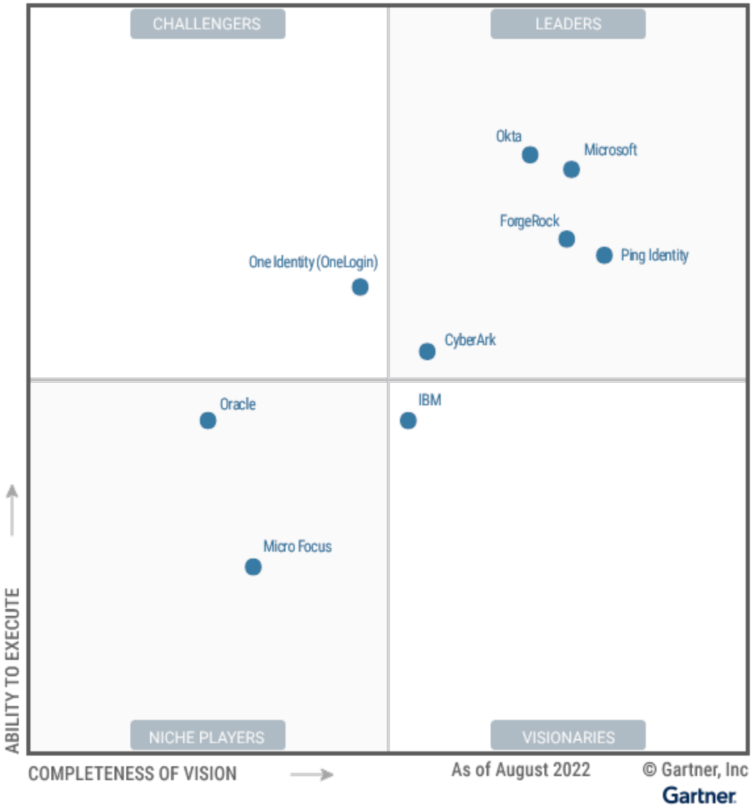
The FIRST and ONLY Leader in Both Gartner® Magic Quadrant™ Reports for Access Management and PAM. EVER.

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 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, Abhuday 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.