Cyber-Defense Strategies to Protect Cloud Resources & Identities

BASED ON: *Cloud Attack Vectors: Haber, Chappell, & Hills*

Building a Successful Cloud Security Strategy

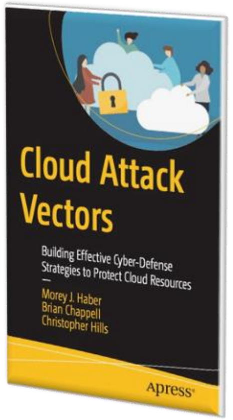
BeyondTrust

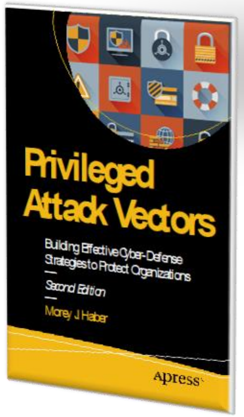
Agenda

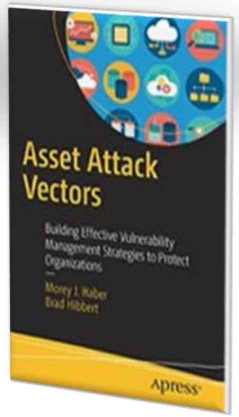
1. Introductions
2. The Cloud
3. Strategic & Security Challenges
4. Mitigation Strategies
5. Key Takeaways
6. About BeyondTrust

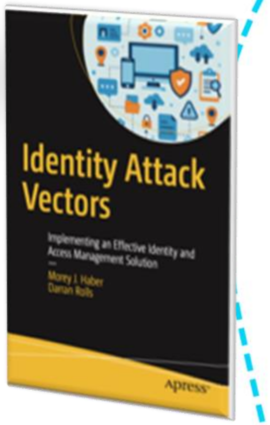
Morey Haber, CSO, BeyondTrust

- 20+ years security experience
- Founding member of the industry group Transparency in Cyber
- Elected in 2020 to the Identity Defined Security Alliance (IDSA) Executive Advisory Board
- Articles on Forbes, Secure World, CSO Online, Dark Reading, and more
- Author of 4 Cybersecurity Attack Vector Books from Apress Media
- Contributing Author to the *Great Power Competition* on Cyber Risks to Critical Infrastructure

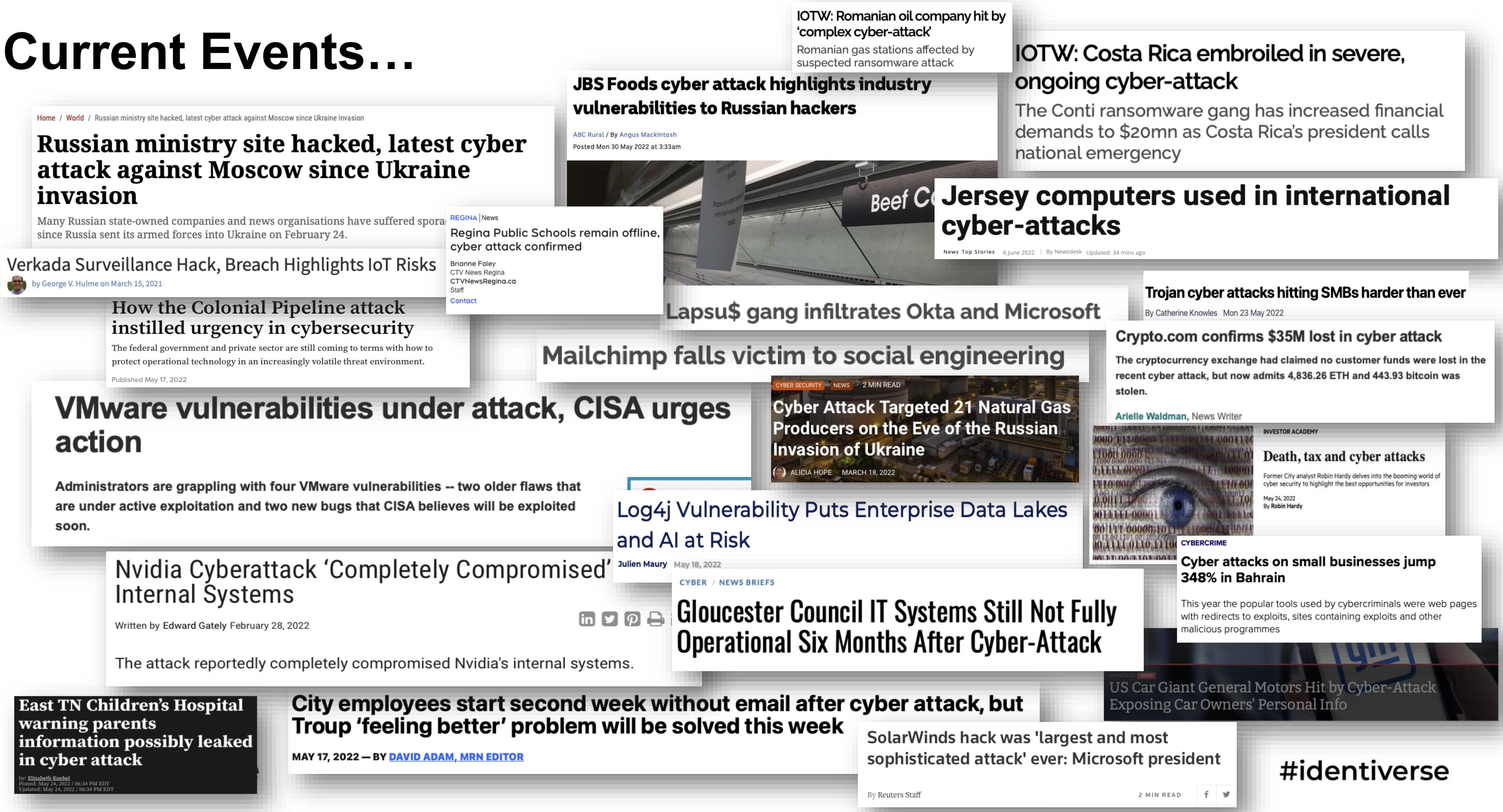



Privileged Attack Vectors
Building Effective Cyber-Defense Strategies to Protect Organizations
Second Edition
Morey J Haber
Apress


Asset Attack Vectors
Building Effective Vulnerability Management Strategies to Protect Organizations
Morey J. Haber
Brad Hibbert
Apress


Identity Attack Vectors
Implementing an Effective Identity and Access Management Solution
Morey J. Haber
Darran Rolls
Apress

Current Events…



IOTW: Romanian oil company hit by 'complex cyber-attack'

Romanian gas stations affected by suspected ransomware attack

IOTW: Costa Rica embroiled in severe, ongoing cyber-attack

The Conti ransomware gang has increased financial demands to $20mn as Costa Rica's president calls national emergency

JBS Foods cyber attack highlights industry vulnerabilities to Russian hackers

ABC Rural / By Angus Mackintosh

Posted Mon 30 May 2022 at 3:33am

Home / World / Russian ministry site hacked, latest cyber attack against Moscow since Ukraine invasion

Russian ministry site hacked, latest cyber attack against Moscow since Ukraine invasion

Many Russian state-owned companies and news organisations have suffered spora
since Russia sent its armed forces into Ukraine on February 24.

REGINA | News

Regina Public Schools remain offline, cyber attack confirmed

Brianne Foley
CTV News Regina
CTVNewsRegina.ca
Staff
Contact

Jersey computers used in international cyber-attacks

News Top Stories 6 June 2022 | By Newsdesk Updated: 34 mins ago

Verkada Surveillance Hack, Breach Highlights IoT Risks

by George V. Hulme on March 15, 2021

Trojan cyber attacks hitting SMBs harder than ever

By Catherine Knowles Mon 23 May 2022

Lapsu$ gang infiltrates Okta and Microsoft

How the Colonial Pipeline attack instilled urgency in cybersecurity

The federal government and private sector are still coming to terms with how to protect operational technology in an increasingly volatile threat environment.

Published May 17, 2022

Mailchimp falls victim to social engineering

Crypto.com confirms $35M lost in cyber attack

The cryptocurrency exchange had claimed no customer funds were lost in the recent cyber attack, but now admits 4,836.26 ETH and 443.93 bitcoin was stolen.

Arielle Waldman, News Writer

VMware vulnerabilities under attack, CISA urges action

Administrators are grappling with four VMware vulnerabilities -- two older flaws that are under active exploitation and two new bugs that CISA believes will be exploited soon.

CYBER SECURITY NEWS 2 MIN READ

Cyber Attack Targeted 21 Natural Gas Producers on the Eve of the Russian Invasion of Ukraine

ALICIA HOPE · MARCH 18, 2022

INVESTOR ACADEMY

Death, tax and cyber attacks

Former City analyst Robin Hardy delves into the booming world of cyber security to highlight the best opportunities for investors

May 24, 2022
By Robin Hardy

Log4j Vulnerability Puts Enterprise Data Lakes and AI at Risk

Julien Maury May 18, 2022

Nvidia Cyberattack 'Completely Compromised' Internal Systems

Written by Edward Gately February 28, 2022

The attack reportedly completely compromised Nvidia's internal systems.

CYBERCRIME

Cyber attacks on small businesses jump 348% in Bahrain

This year the popular tools used by cybercriminals were web pages with redirects to exploits, sites containing exploits and other malicious programmes

CYBER / NEWS BRIEFS

Gloucester Council IT Systems Still Not Fully Operational Six Months After Cyber-Attack

24 MAY 2022 NEWS

US Car Giant General Motors Hit by Cyber-Attack Exposing Car Owners' Personal Info

East TN Children's Hospital warning parents information possibly leaked in cyber attack

by: Elizabeth Kuebel
Posted: May 24, 2022 / 06:34 PM EDT
Updated: May 24, 2022 / 06:34 PM EDT

City employees start second week without email after cyber attack, but Troup 'feeling better' problem will be solved this week

MAY 17, 2022 — BY DAVID ADAM, MRN EDITOR

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president

By Reuters Staff 2 MIN READ

#identiverse

Cloud Attack Vectors

… to name a few

Phishing

Privileged Attacks

Configuration Anomalies

Vulnerabilities

Default Settings

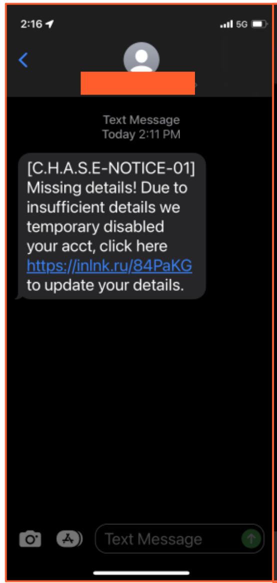
Poor Hardening

Supply Chain Attacks

Insider Threats

… that is what we are seeing in the news.

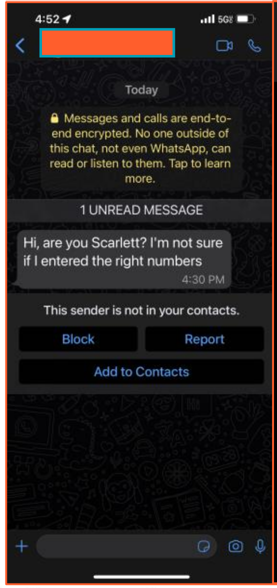
Even Basic Communications Can Be An Attack Vector* . . .



[redacted]

Text Message
Today 2:11 PM

[C.H.A.S.E-NOTICE-01] Missing details! Due to insufficient details we temporary disabled your acct, click here https://inlnk.ru/84PaKG to update your details.



[redacted]

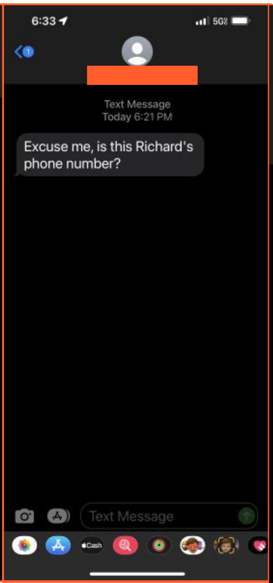
Today

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

1 UNREAD MESSAGE

Hi, are you Scarlett? I'm not sure if I entered the right numbers 4:30 PM

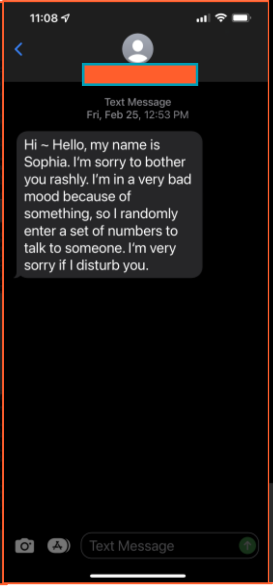
This sender is not in your contacts.



[redacted]

Text Message
Today 6:21 PM

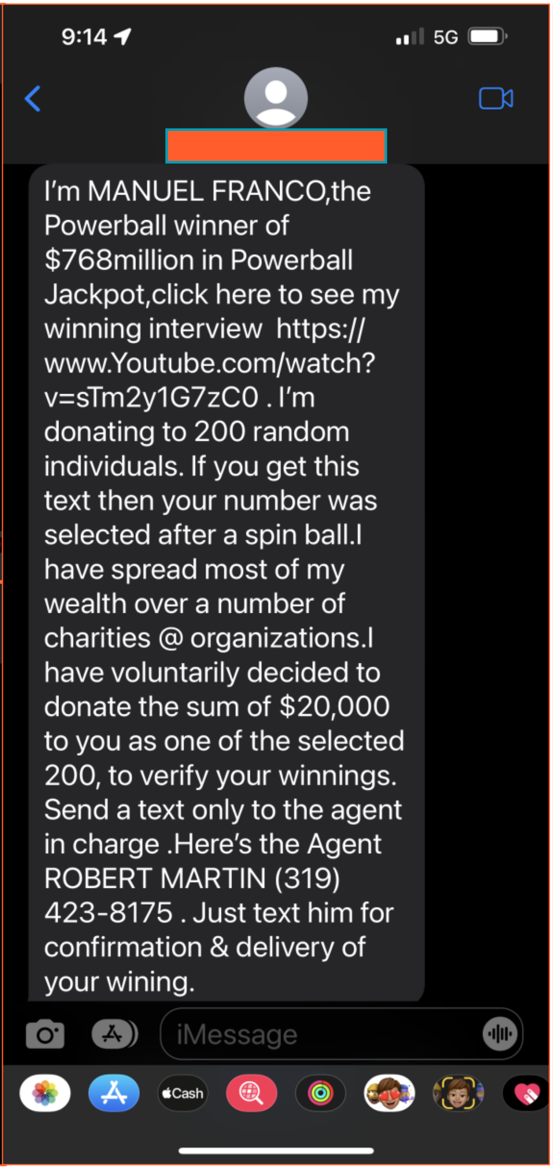
Excuse me, is this Richard's phone number?



[redacted]

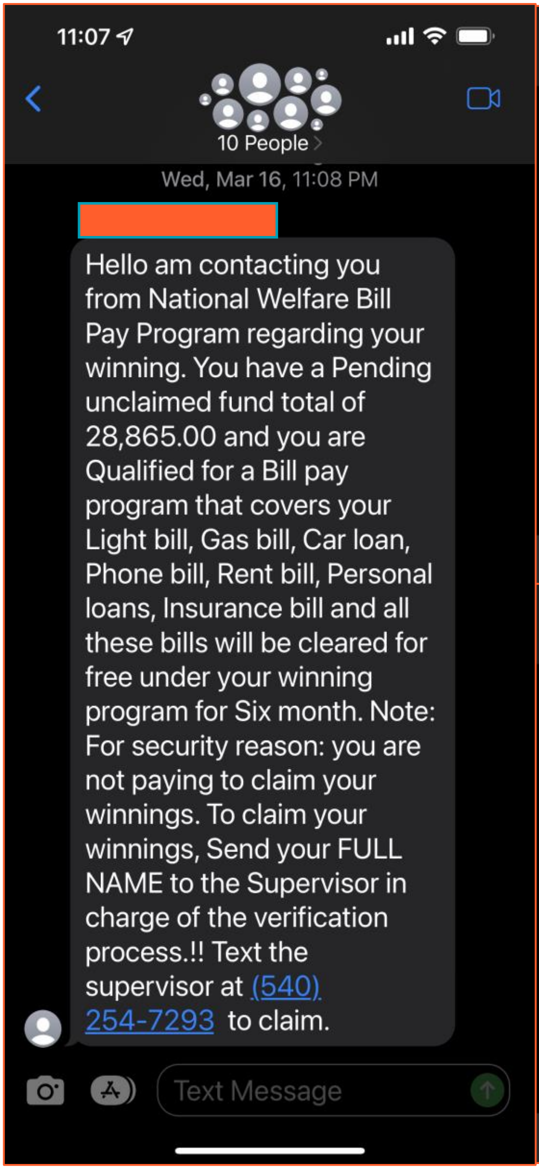
Text Message
Fri, Feb 25, 12:53 PM

Hi ~ Hello, my name is Sophia. I'm sorry to bother you rashly. I'm in a very bad mood because of something, so I randomly enter a set of numbers to talk to someone. I'm very sorry if I disturb you.



[redacted]

I'm MANUEL FRANCO,the Powerball winner of $768million in Powerball Jackpot,click here to see my winning interview https://www.Youtube.com/watch?v=sTm2y1G7zC0 . I'm donating to 200 random individuals. If you get this text then your number was selected after a spin ball.I have spread most of my wealth over a number of charities @ organizations.I have voluntarily decided to donate the sum of $20,000 to you as one of the selected 200, to verify your winnings. Send a text only to the agent in charge .Here's the Agent ROBERT MARTIN (319) 423-8175 . Just text him for confirmation & delivery of your wining.

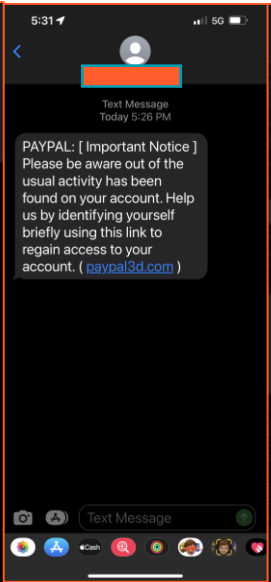


10 People

Wed, Mar 16, 11:08 PM

[redacted]

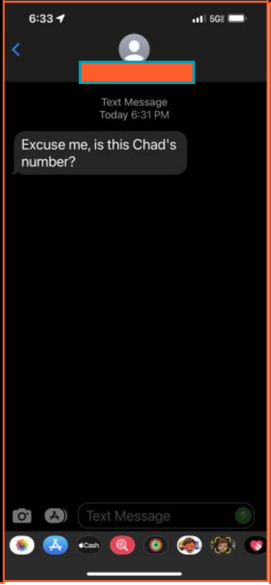
Hello am contacting you from National Welfare Bill Pay Program regarding your winning. You have a Pending unclaimed fund total of 28,865.00 and you are Qualified for a Bill pay program that covers your Light bill, Gas bill, Car loan, Phone bill, Rent bill, Personal loans, Insurance bill and all these bills will be cleared for free under your winning program for Six month. Note: For security reason: you are not paying to claim your winnings. To claim your winnings, Send your FULL NAME to the Supervisor in charge of the verification process.!! Text the supervisor at (540) 254-7293 to claim.



[redacted]

Text Message
Today 5:26 PM

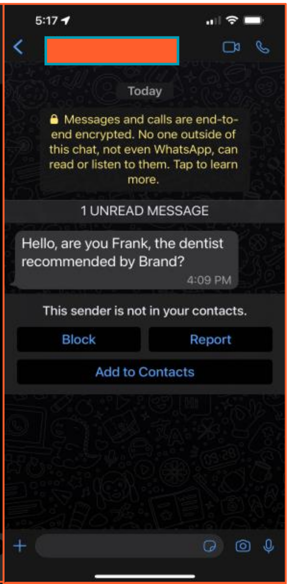
PAYPAL: [Important Notice] Please be aware out of the usual activity has been found on your account. Help us by identifying yourself briefly using this link to regain access to your account. (paypal3d.com)



[redacted]

Text Message
Today 6:31 PM

Excuse me, is this Chad's number?



[redacted]

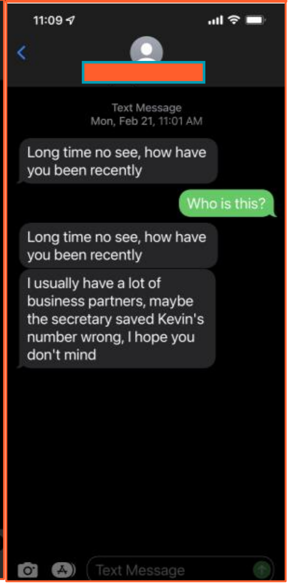
Today

🔒 Messages and calls are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Tap to learn more.

1 UNREAD MESSAGE

Hello, are you Frank, the dentist recommended by Brand? 4:09 PM

This sender is not in your contacts.



[redacted]

Text Message
Mon, Feb 21, 11:01 AM

Long time no see, how have you been recently

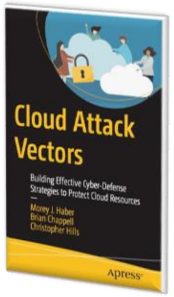
Who is this?

Long time no see, how have you been recently

I usually have a lot of business partners, maybe the secretary saved Kevin's number wrong, I hope you don't mind

* Yes, these are real and only a sampling of what we have personally received over the past few months

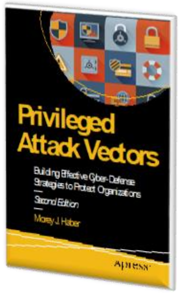
The more things change, the more they stay the same.


Cloud Attack Vectors

Building Effective Cyber-Defense Strategies to Protect Cloud Resources

Morey J. Haber
Brian Chappell
Christopher Hills

Apress

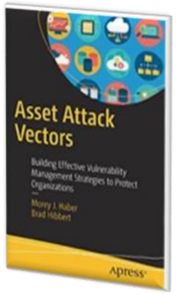

Privileged Attack Vectors

Building Effective Cyber-Defense Strategies to Protect Organizations

Second Edition

Morey J. Haber

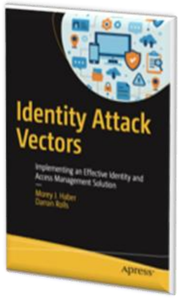
Apress


Asset Attack Vectors

Building Effective Vulnerability Management Strategies to Protect Organizations

Morey J. Haber
Brad Hibbert

Apress


Identity Attack Vectors

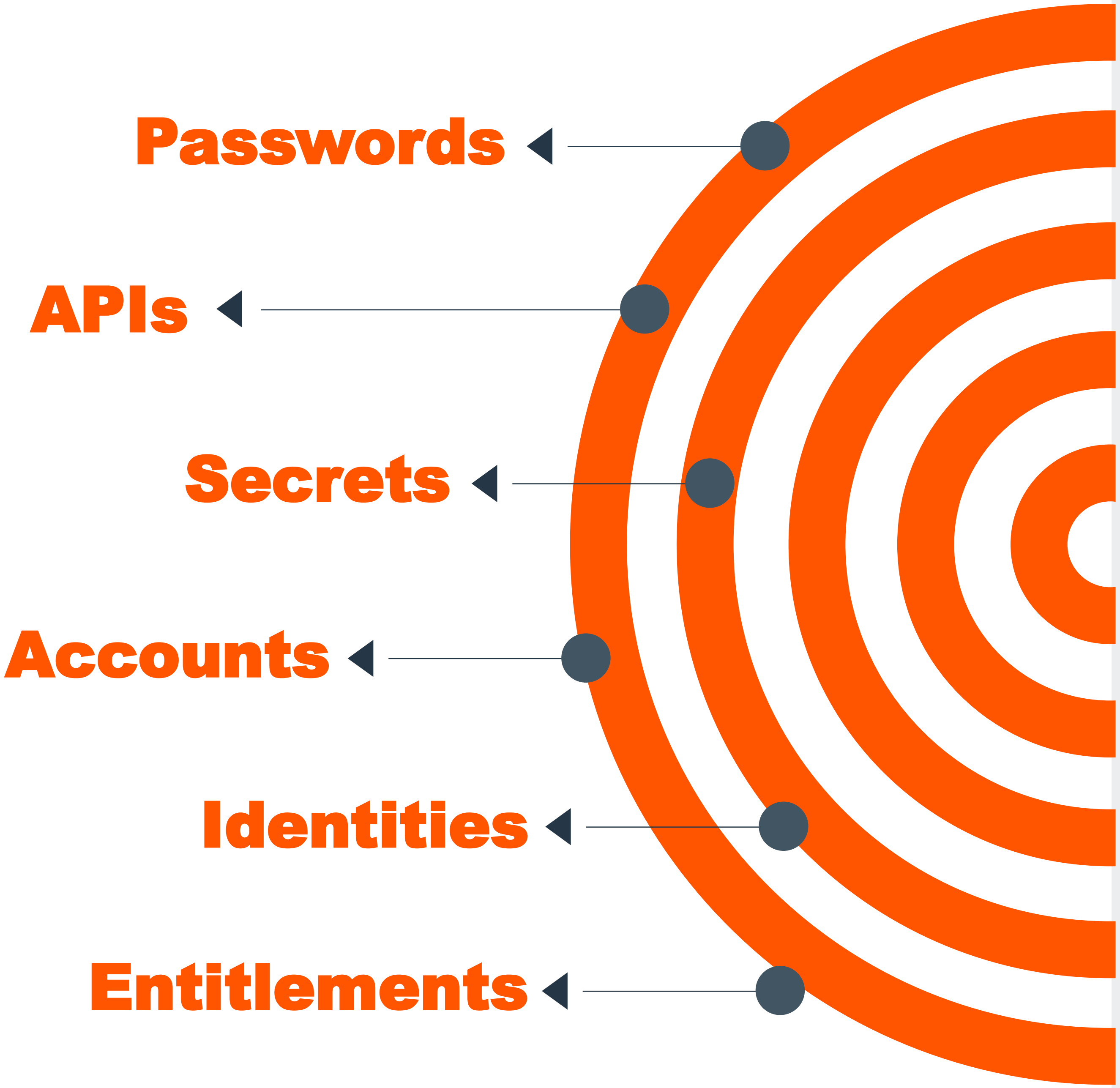
Implementing an Effective Identity and Access Management Solution

Morey J. Haber
Darran Rolls

Apress

The Cloud is no different…

Threat actors are targeting broader identity attack vectors due to inadequate protection



Passwords

APIs

Secrets

Accounts

Identities

Entitlements

#identiverse

So, how do we adapt our strategy for risk mitigation in the cloud?

Beware of Vendor Buzzword Bingo

B	I	N	G	O
Zero Trust	Cloud Washing	Future Proof	Infinitely Scalable	Unhackable
Imposter Syndrome	CI/CD Pipeline Protection	API Protection	Data Security	Serverless
Attack Monitoring	Continuous Monitoring	FREE	Codeless Integration	Vendor Agnostic
Data Privacy	Regulatory Compliant	Five Nine’s	Digital Transformation	Just in Time
Shadow IT	Cloud Agnostic	Identity Based Segmentation	XaaS	Artificial Intelligence

Relevant…

However, not clearly defined for the problem

Get Your Definitions Right... and Educate

Next, Think of The Cloud Regarding…

- ✓ The Benefits of the Cloud
- ✓ Do Not Repeat the Mistakes of the Past
- ✓ Scanning vs. Agents vs. API's – *Oh My!*
- ✓ Asset, Identity, and Privilege Management as Priorities
- ✓ Vulnerability and Patch Management Must be Perfect
- ✓ It is Not Your Infrastructure
- ✓ Accountability is Your Responsibility!

Make the Best Security & Business Decision

Implement the latest shiny tool?

OR

Implement Security Best Practices!

Mitigating Risks

- Entitlements
- Vulnerabilities
- Remediation
- Hardening
- Default Configuration
- Configuration Management
- Privileges (Access, Monitoring)
- Asset Management
- Web Services
- API Protection
- Ransomware Mitigations
- Crypto Mining Protection
- Phishing (email, SMS, voice)
- Lateral Movement Detection
- Remote Access (RDP, SSH, Other)
- Social Engineering
- Supply Chain Attacks
- Insider Threats

New Categories of Solutions,

Same Security Disciplines

- Vendor Privileged Access Management (VPAM)
- Cloud Security Management (CSM)
- Cloud Infrastructure Entitlement Management (CIEM)
- Customer Identity and Access Management (CIAM)
- Cloud Security Posture Management (CSPM)
- Cloud Workload Protection Platform (CWPP)
- Cloud Native Application Protection Platform (CNAPP)
- Cloud Access Service Broker (CASB)
- Vulnerability, Patch, Configuration, Compliance, Log, etc…

Choosing a Cloud Provider

- Certifications and standards
- Technology and strategic roadmap
- Data security, privacy, protection, compliance, & governance
- Operational dependencies
- Technology and business partners
- Contractual terms and pricing
- Service level agreements
- Reliability and performance
- Backup, recovery, high availability, and disaster recovery
- Technology stickiness and vendor lock-in
- Business viability
- Company and culture compatibility

Key Takeaways

Ask the business, 'what are you doing for these disciplines?'

- Password and Secrets Management
- Endpoint Privilege Management
- Identity Management
- Asset Management
- Vulnerability Management
- Configuration Management
- Patch Management
- Penetration Testing
- Regulatory Compliance
- Architecture Reviews
- Standard User Accounts
- Password Reuse
- Complex and Hardened Secrets
- Break Glass
- Audit and Logging
- Multi-Factor Authentication
- Principle of Least Privilege
- Behavioral Monitoring
- Education and Training

Company Overview

BeyondTrust

1,500+ Employees

20 Countries

2003 Founded

Market Leader

Recognized as a PAM leader by key Market Analysts

Global Presence

~20k customers in 100+ countries and extensive partner network

Integrated Platform

Unified platform with seamless third-party integrations

Broadest Portfolio

Best-in-class identity and privileged access solutions

Customer Driven

90%+ gross retention and exceptional customer support and success

Technology Pioneers

Heritage of innovation with 75+ patents and commitment to R&D

Headquarters	**Atlanta, GA | USA**
Global Offices	**Americas, EMEIA, APJ**
Privately Held	**Francisco Partners & Clearlake Capital**

Recognition

Gartner
Peer Insights
Customers'
Choice 2022
™

Chosen by Customers

- A **Customers' Choice** in the 2022 Gartner® Peer Insights™ "Voice of the Customer: Privileged Access Management", 2nd year running
- 4.5/5 overall rating out of 278 reviews, as of October 2022

Recognized by Analysts

- Named a Leader in the **Gartner® Magic Quadrant™** for Privileged Access Management – again

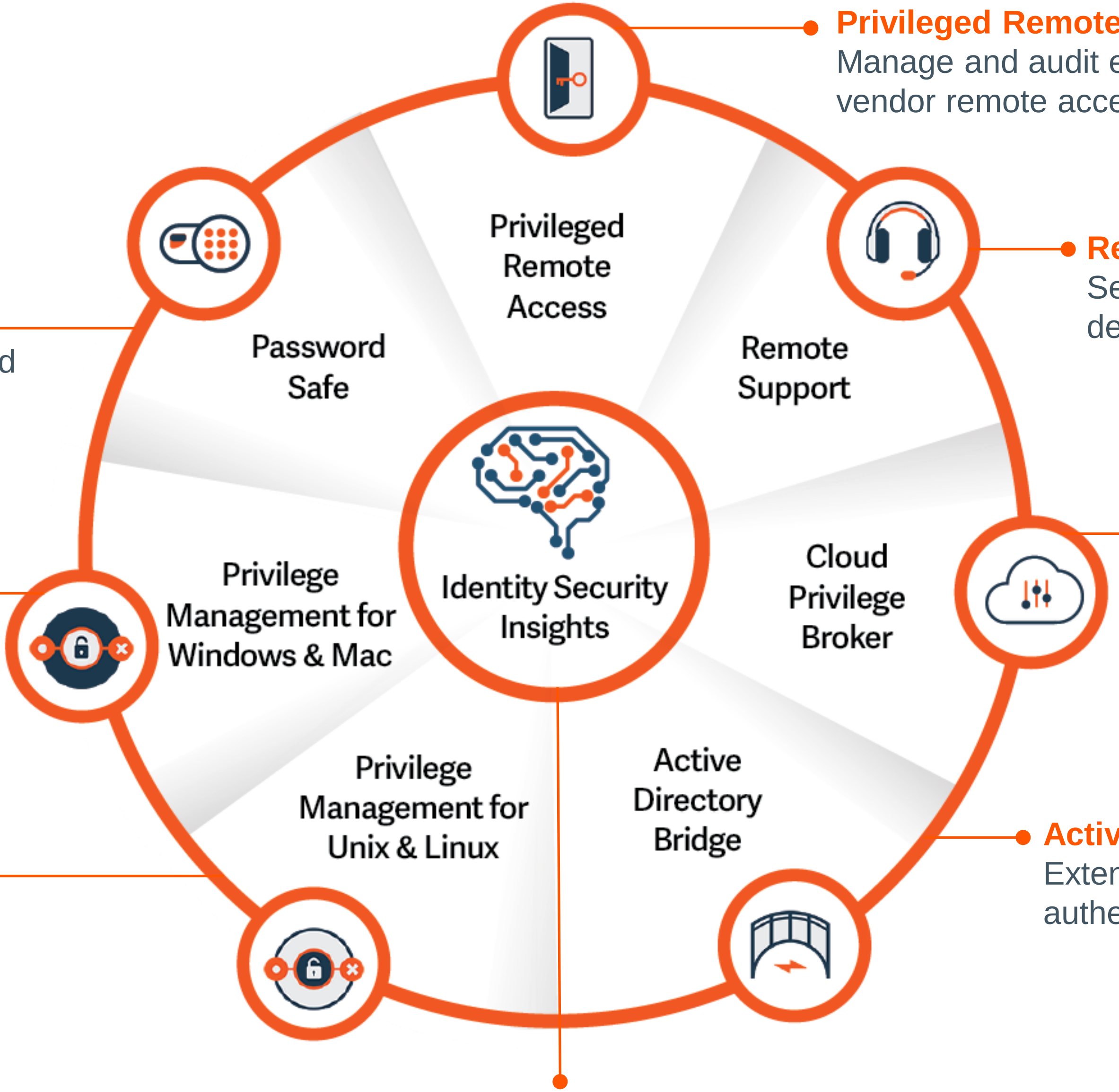
GARTNER, PEER INSIGHTS and MAGIC QUADRANT are trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and 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, etc., 19 July 2022.

Gartner, Gartner Peer Insights 'Voice of the Customer': Privileged Access Management, Peer Contributors, 21 December 2022
Gartner® Peer Insights™ content consists of the opinions of individual end users based on their own experiences, and should not be construed as statements of fact, nor do they represent the views of Gartner or its affiliates. Gartner does not endorse any vendor, product or service depicted in this content nor makes any warranties, expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.

The GARTNER PEER INSIGHTS CUSTOMERS' CHOICE badge is a trademark and service mark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.

BeyondTrust

Platform



Privileged Remote Access
Password Safe
Remote Support
Identity Security Insights
Privilege Management for Windows & Mac
Cloud Privilege Broker
Privilege Management for Unix & Linux
Active Directory Bridge

Privileged Remote Access
Manage and audit employee and vendor remote access

Remote Support
Securely access and support any device or system in the world

Password Safe
Gain visibility and control of privileged credentials and secrets

Cloud Privilege Broker
Visualize and right-size entitlements across clouds

Privilege Management for Windows & Mac
Enforce least privilege and control applications

Active Directory Bridge
Extend and manage Unix/Linux authentication and group policies

Privilege Management for Unix & Linux
Implement unmatched privilege access security

Identity Security Insights
Gain one holistic view of identities and access across your IT estate from a single interface

THANK YOU!

Available to chat at the BeyondTrust booth #1209

Morey Haber, CSO, BeyondTrust

mhaber@beyondtrust.com