

R A N S O M W A R E :  
P R E V E N T ,  
D E T E C T F R O M  
O V E R T R U S T  
B E H A V I O R

D R R I C C I I E O N G

V I C E C H A I R M A N - P R O F E S S I O N A L  
D E V E L O P M E N T

C S A H O N G K O N G C H A P T E R



# WHOAMI (RICCI IEONG)

## Working Experience

- Adjunct Assistant Professor in the Hong Kong University of Science & Technology (2015 - )
- Adjunct Assistant Professor in the Chinese University of Hong Kong (2023 - )
- Part-time lecturer in Tung Wah College (2019 - 2021)
- Principal Consultant and Founder of eWalker Consulting Limited (2005 - )
- Authorized Trainer for CCAK (2021 - )
- Authorized Trainer for ISC2 CCSP (2016 - )
- Authorized Trainer for CSA CCSK (2013 - )
- Consultant of Hewlett Packard HKSAR (2000 – 2005)
- Senior Consultant of PrivyLink HKSAR (2000)
- ACO of Cyberspace Center, HKUST (1997 – 2000)
- Demonstrator, COMP, HKUST (1996 – 1997)

## Education

- PhD (2013), HKU HK
- MA Arb (2006), City University HK
- M.Phil (1996), HKUST
- B.Sc (1994), CUHK

## Others

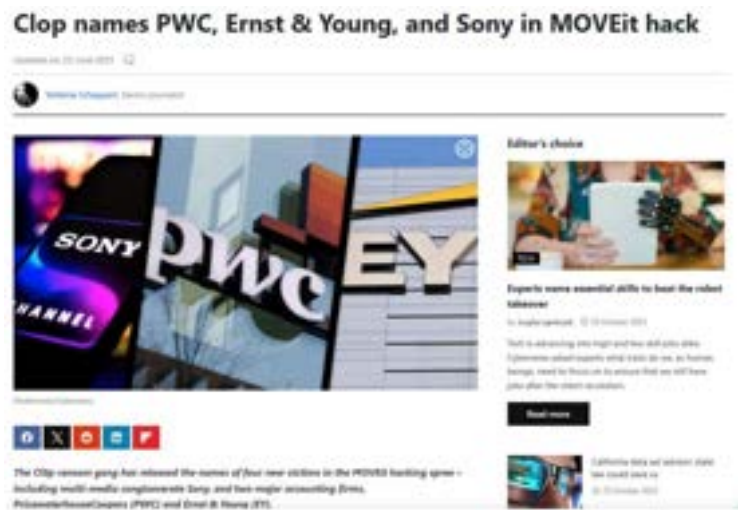
- Active speaker in HK IT security industry
- Team member of Foreigner Team Champion in a Korean based Digital Forensics Challenge (2018, 2020)
- ISC2 Asia-Pacific Information Security Leadership Achievements (ISLA) – Senior Information Security Professional (2017) Award
- HKSAR Government Cyber Security Professionals Awards (2017)
- HKMA PDP Committee
- Council Member of Information Security and Forensics Society
- Vice Chairman of Cloud Security Alliance (HK&M) Chapter



# RECENT INCIDENTS

# RECENT DATA BREACH HEADLINES (SEP - OCT 2023)

- Cl0p ransom gang attack through MOVEit hack in Sep 2023



- On October 6, 23andMe announced that hackers had obtained some user data, claiming that to amass the stolen data the hackers used credential stuffing — a common technique where hackers try combinations of usernames or emails and corresponding passwords that are already public from other data breaches

## Hacker leaks millions more 23andMe user records on cybercrime forum

Lorenzo Franceschi-Bicchieri (@lorenzofb) · October 11, 2023



# RECENT DATA BREACH HEADLINES (OCT 2023)

## 200 million Twitter users' email addresses allegedly leaked online

By Lawrence Abrams

January 4, 2023 10:14 PM



Image AI generated by Dall-E

A data leak described as containing email addresses for over 200 million Twitter users has been published on a popular hacker forum for about \$2. SleepingComputer has confirmed the validity of many of the email addresses listed in the leak.

Since July 22nd, 2022, threat actors and data breach collectors have been selling and circulating large data sets of scraped Twitter user profiles containing both private (phone numbers and email addresses) and public data on various online hacker forums and cybercrime marketplaces.



12/27/2023

## Cyberattack on health services provider impacts 5 Canadian hospitals

By Bill Toulas

October 24, 2022 10:18 AM



A cyberattack on shared service provider Transform has impacted operations in five hospitals in Ontario, Canada, impacting patient care and causing appointments to be rescheduled.

Transform is a not-for-profit, shared service organization founded by five hospitals in Erie St. Clair, Ontario, to manage their IT, supply chain, and accounts payable.

Yesterday, the service provider released a statement stating that their IT systems are experiencing an outage due to a cyberattack.

## University of Michigan employee, student data stolen in cyberattack

By David Siders

October 27, 2022 10:14 PM



The University of Michigan says in a statement today that they suffered a data breach after hackers broke into its network in August and accessed systems with information belonging to students, applicants, alumni, donors, employees, patients, and research study participants.

Unauthorized access to the servers lasted between August 23-27, the university says, and the data exposed included personal, financial, and medical details.

Copyright © Ricci IEONG for CSA HKM in CTF 2023

# RECENT DATA BREACH HEADLINES (OCT 2023)

## City of Philadelphia discloses data breach after five months

By Sergio Gattin

October 23, 2023 08:25 AM




The City of Philadelphia is investigating a data breach after attackers "may have gained access" to City email accounts containing personal and protected health information five months ago, in May.

While officials discovered the incident on May 24 following suspicious activity in the City's email environment, the investigation found that the threat actors may have accessed emails in the compromised email accounts for at least two months after the City became aware of the incident.


## Okta's Latest Security Breach Is Haunted by the Ghost of Incidents Past

A recent breach of authentication giant Okta has impacted nearly 200 of its clients. But repeated incidents and the company's delayed disclosure have security experts calling foul.



ON FRIDAY, October 20, the identity management platform Okta said it suffered an intrusion in its customer support system. As an access and authentication service, a breach of Okta always comes with risks to other organizations, and the company confirmed that "certain Okta customers" were affected. Okta tells WIREX that it notified "around 1 percent" of its 58,000 customers that they were impacted.

The password manager (Paycom), an Okta customer, said that it had notified the company on September 29 of suspicious activity that ultimately was tied to the support system incident. BeyondTrust, another identity and access management firm and also an Okta customer, said last week that it had



Stacked Assets: Penetration Test

# CYBERPORT HACK (SEP 2023)



7th September 2023 – (Hong Kong) A notorious international hacker group is suspected of infiltrating the network systems of Hong Kong's Cyberport digital hub, stealing a trove of confidential data on startup tenants and sensitive internal documents. The hackers are auctioning off the 400GB cache of files on the dark web for a base price of US\$300,000 (HK\$2.34 million).

- The data was released recently after international hackers demanded a ransom of US\$300,000 - approximately HK\$2.35 million - for the leaked 400 gigabytes of information.
- Apart from the personal data of staff, the hacked files also included lease agreements, receipts, audit reports, and a large number of documents involving HSBC, CLP Power, and the government.
- The hacker organization, Trigona, put up the data for bid online.
- Cyberport on Tuesday strongly condemned the hackers and expressed regret over the concerns and inconvenience caused by the incident.

# CONSUMER COUNCIL HACK (SEP 2023)

Hong Kong's consumer watchdog has fallen victim to hackers and has warned the public of a suspected data breach, [just two weeks after it emerged that Cyberport tech hub](#) suffered a data leak.

The Consumer Council said on Friday that a cyberattack against its computer system had been identified on Wednesday, causing damage to about 80 per cent of their systems and disruption to their hotline services and price comparison tools. Whether a personal data breach was involved, and the scope of the data leak, remains to be confirmed.



The consumer council's website displays a warning message about a "system disruption" on Wednesday, September 20, 2023. Photo: Screenshot.

The council was not able to determine the scope of the data leak. It urged possibly affected individuals to be extra cautious about potential scams and take precautionary measures to ensure cybersecurity.

A ransomware note claimed to have obtained employee and client data during the attack, Chan said. It had demanded US\$500,000 (HK\$3.9 million) be paid by Saturday night, and up to US\$700,000 (HK\$5.5 million) if the deadline was not met.

"The council strongly condemns the unlawful cyber activity of hackers, and will not succumb to ransomware extortion," Chan said, adding that the watchdog will support police investigations and expresses apologies to the public.



# CONSUMER COUNCIL HACK (SEP 2023)

## Cyberattack on the Consumer Council's Computer System

2023.09.22

The Consumer Council confirmed today (22 September 2023) that a malicious ransomware attack against its computer system was identified on Wednesday morning (20 September 2023). The attack has resulted in almost 80% damage of the computer system, causing disruption to its hotline services and update of price comparison tools. The Council has taken immediate action to strengthen the security measures of the system to prevent further attack by the hacker, whilst appointing a forensic expert immediately to conduct investigations. Hotline services have currently resumed after emergency repairs. The case was reported to the Police yesterday morning (21 September 2023), and the Council has also proactively notified the Office of the Privacy Commissioner for Personal Data of the incident.



# NO DATA LEAKED ON DARK WEB

## Consumer Council says no data leaked on 'dark web' following hack

Local | 10 Oct 2023 3:01 pm



The Consumer Council said on Monday that its data compromised in a recent computer server hack was not leaked on the "dark web", adding that an investigation is ongoing.

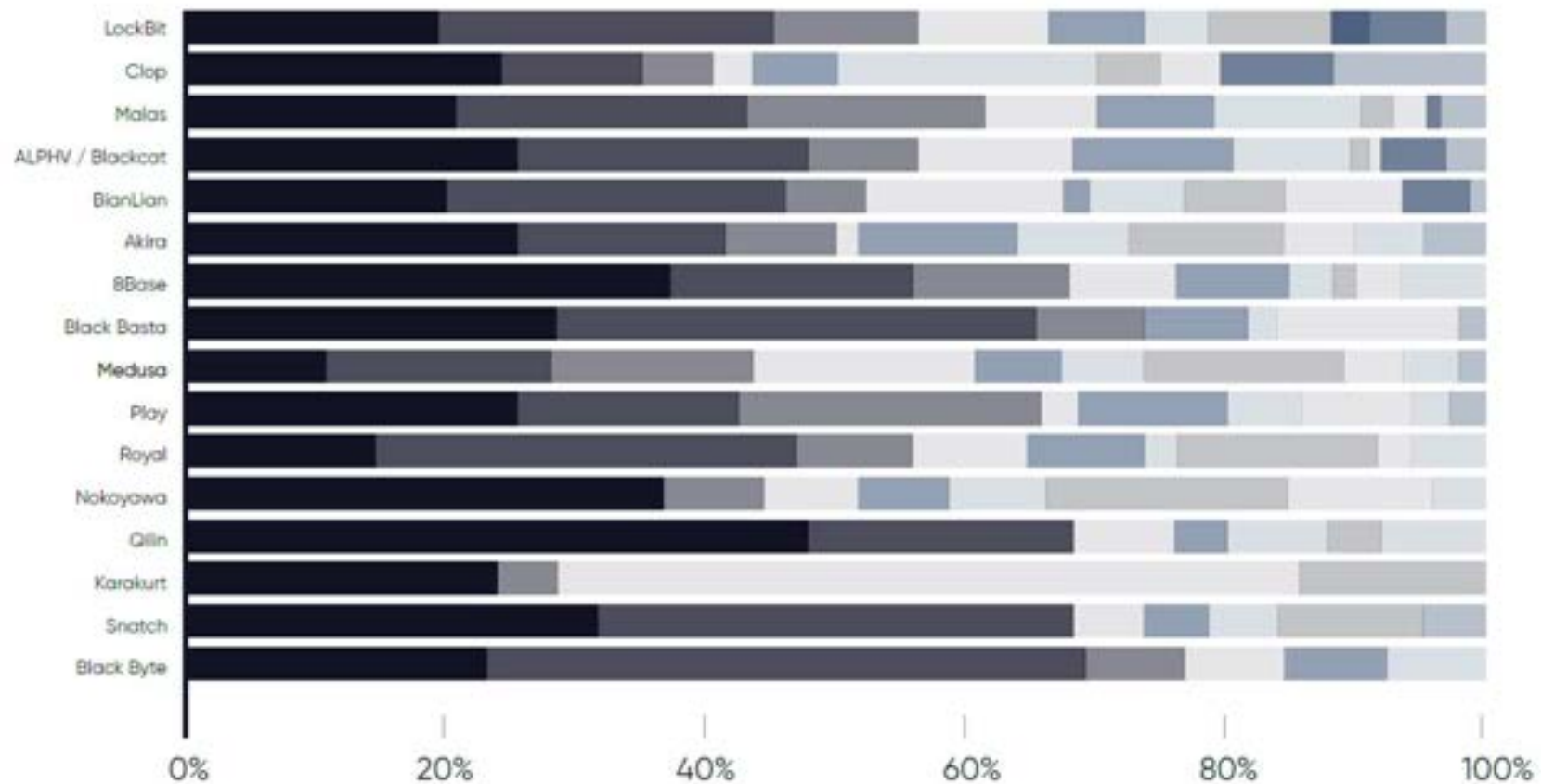
- “The Standard HK”
  - The Consumer Council previously sent out 25,000 data breach notifications to complainants, staff, and its magazine subscribers and received 106 inquiries after the watchdog discovered its computer server was hacked on September 20 and a US\$500,000 (HK\$3.9 million) ransom demanded.
  - The watchdog’s chief executive, Gilly Wong Fung-han, said earlier that the Council would not pay the ransom - which the hackers demanded to be paid before September 23.
  - The watchdog’s investigation found that the data of approximately 8,000 individuals was suspected to have been compromised.

# ANOTHER VICTIM – HONG KONG BALLET



- SCMP 16 Oct 2023
  - The Hong Kong Ballet has reported a data breach caused by a ransomware attack on its computer systems, becoming the third well-established organisation in the city to be hacked in two months.
  - In an official statement released on Monday night, the renowned cultural institution said it had recently discovered its network systems had been infected with ransomware, allowing intruders to illegally access files stored on computers.
  - Data including personal user details and the organisation's internal information had been viewed by the intruders, the company said, adding it was still working to determine the full scope of the attack.

# PROPORTION OF RANSOMWARE GROUPS IN Q2/2023



# RANSOMWARE ATTACKS DISTRIBUTION FROM MICROSOFT



Figure 1: Percentage Distribution of Key Sectors Targeted in Recent Ransomware Attacks

# ATTACK TIME DURATIONS



# HOW DO THOSE ATTACK WORK (PATH 1)?

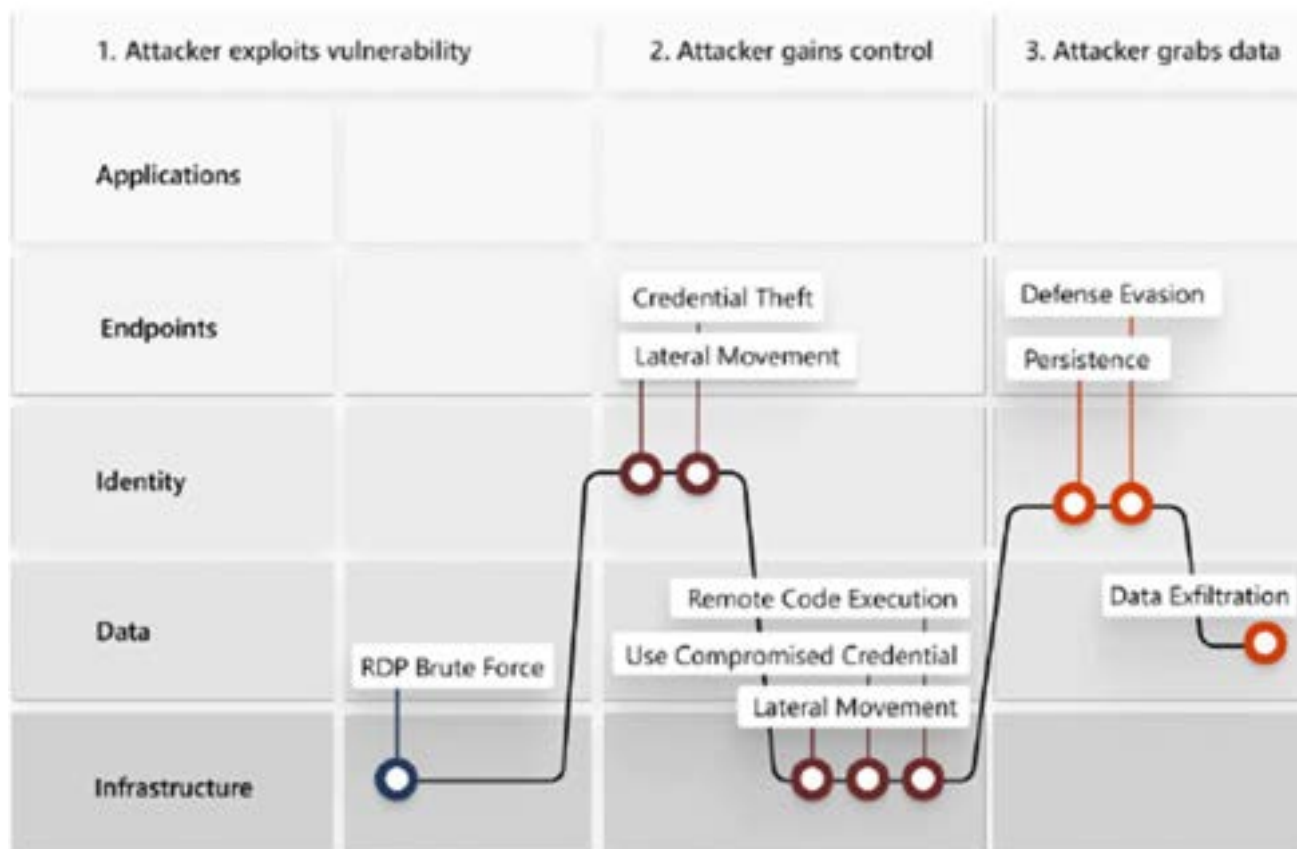
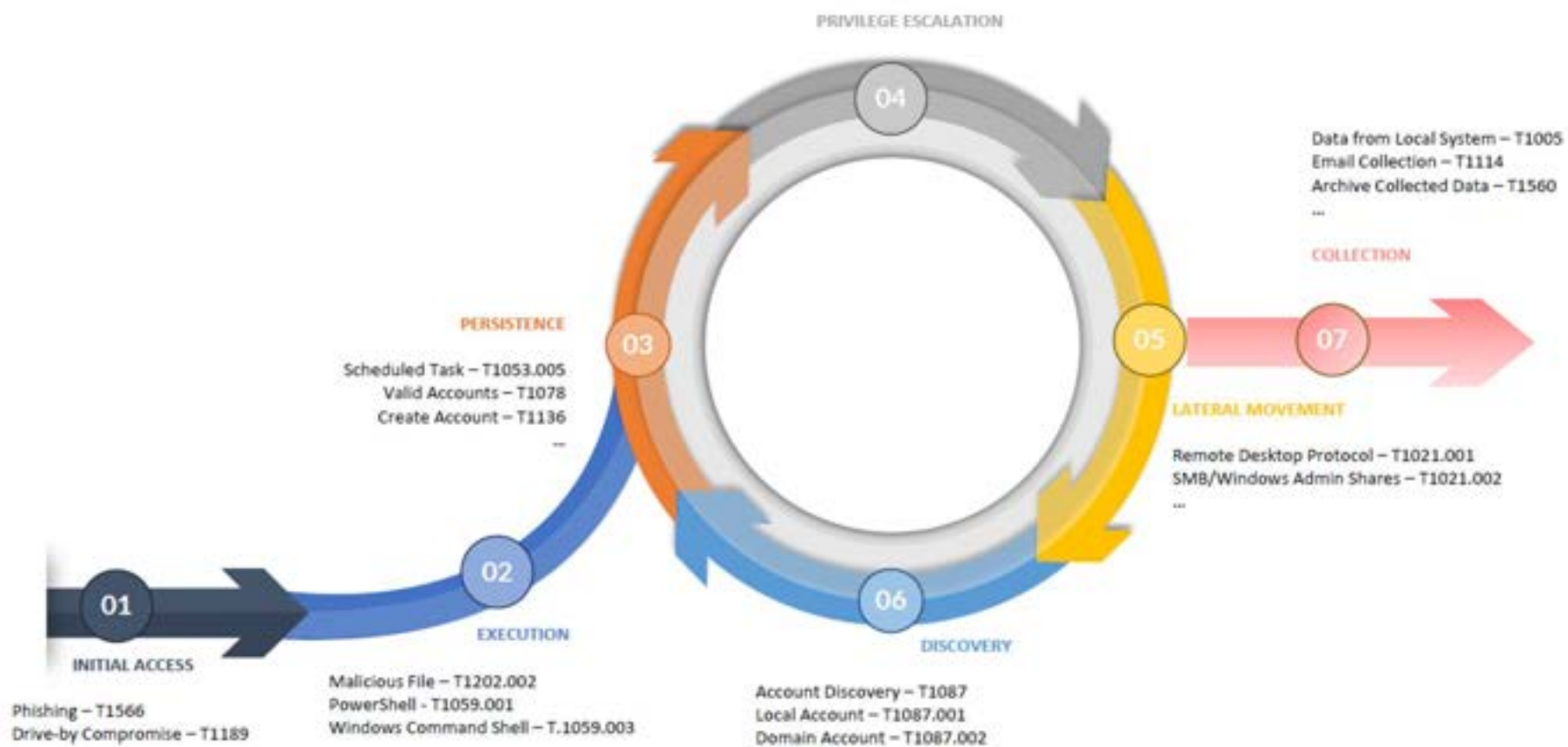


Figure 3: Ransomware Compromise Techniques

# HOW DO THOSE ATTACK WORK (PATH 2)?



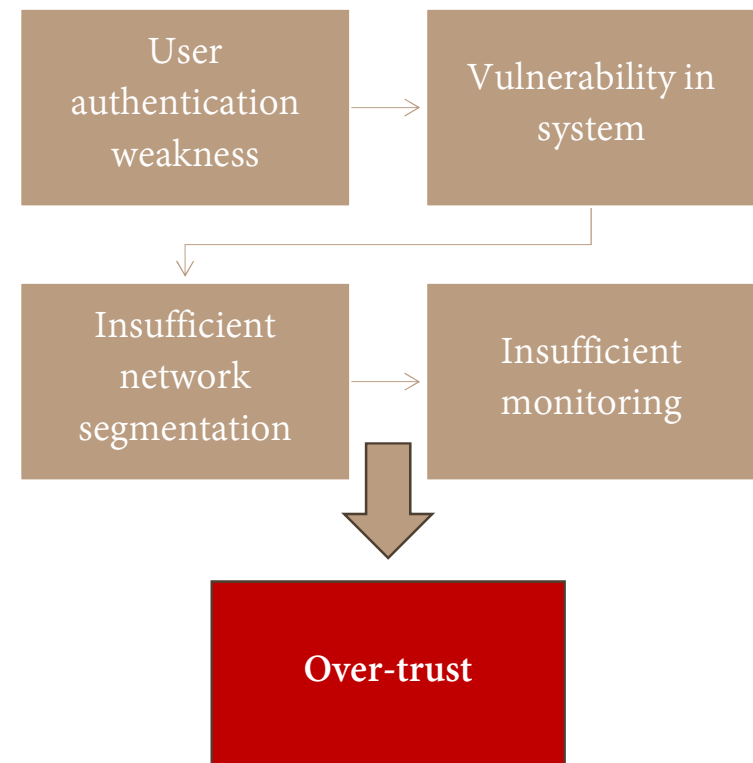


# DEEP DIVE IN TTP

Tactics, Techniques and Procedures	CVE
1. Bypassing Security Measures and Tampering with Security Mechanisms	CVE-2021-27065, CVE-2021-26857, CVE-2021-26855
2. Exploiting Vulnerabilities in Backup and Recovery Solutions	CVE-2023-34362
3. Exploiting Remote Code Execution Vulnerabilities	CVE-2023-28252
4. Bypassing Authentication and Exploiting Pre-Authentication Vulnerabilities	CVE-2023-0669, CVE-2023-27350

# COMMON ROOT CAUSES

- 1) Phishing and Business Email Compromise (BEC) attack
- 2) User/password brute force attempt
- 3) Weak password used in privilege accounts
- 4) Local privilege account obtained followed by use of lateral movement tools
- 5) Known vulnerabilities in the system
- 6) Implant of tools to critical systems
- 7) Insufficient network segmentation to prevent further compromise
- 8) Insufficient monitoring and logging



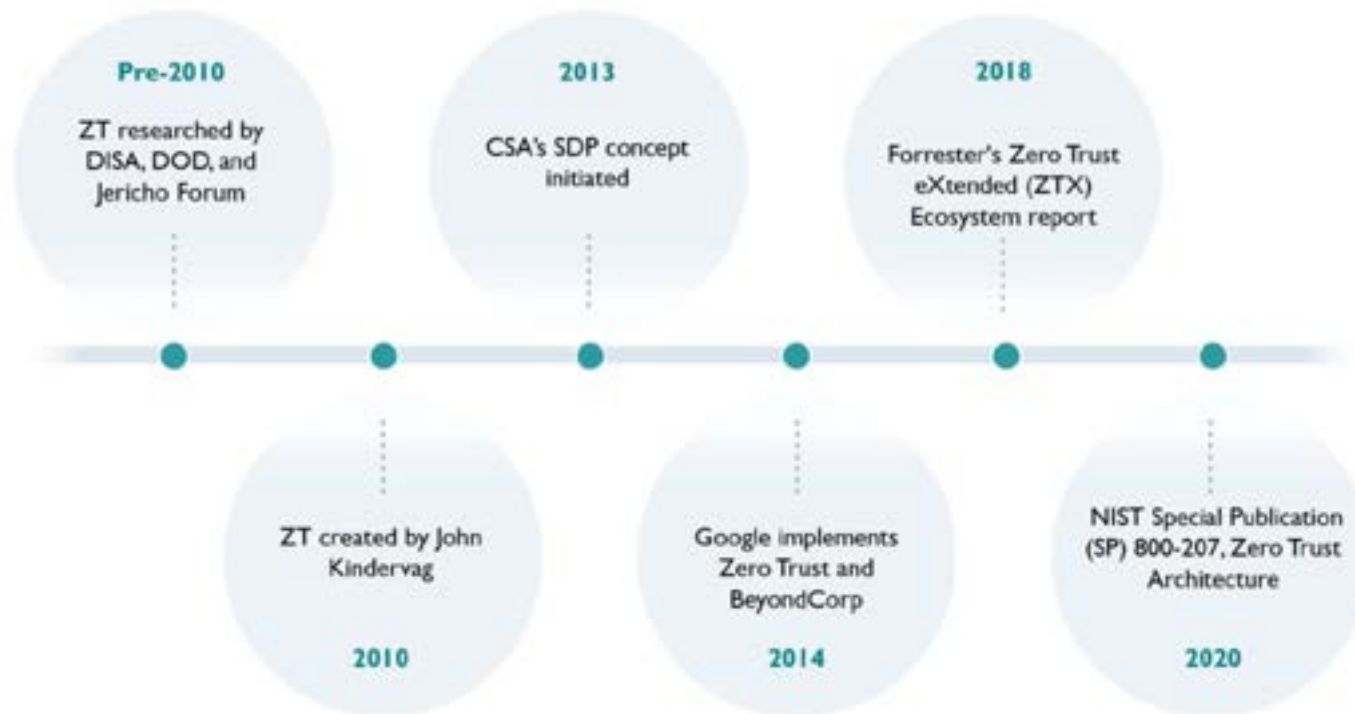
# 8 STEPS TO PREVENT RANSOMWARE





# ZERO TRUST ARCHITECTURE

# ZERO TRUST HISTORY



# CONCEPT OF ZT

- A key aspect of ZT networks is that authentication and explicit authorization must occur prior to network access being granted (e.g., the communication between a requesting entity and the target resource).
- ZT concepts from Cloud Security Alliance
  - Making no assumptions about an entity's trustworthiness when it requests access to a resource
  - Starting with no pre-established entitlements, then relying on a construct that adds entitlements, as needed
  - Verifying all users, devices, workloads, network and data access, regardless of where, who, or to what resource, with the assumption that breaches are impending or have already occurred

# KEY LOGICAL COMPONENTS OF A ZTA

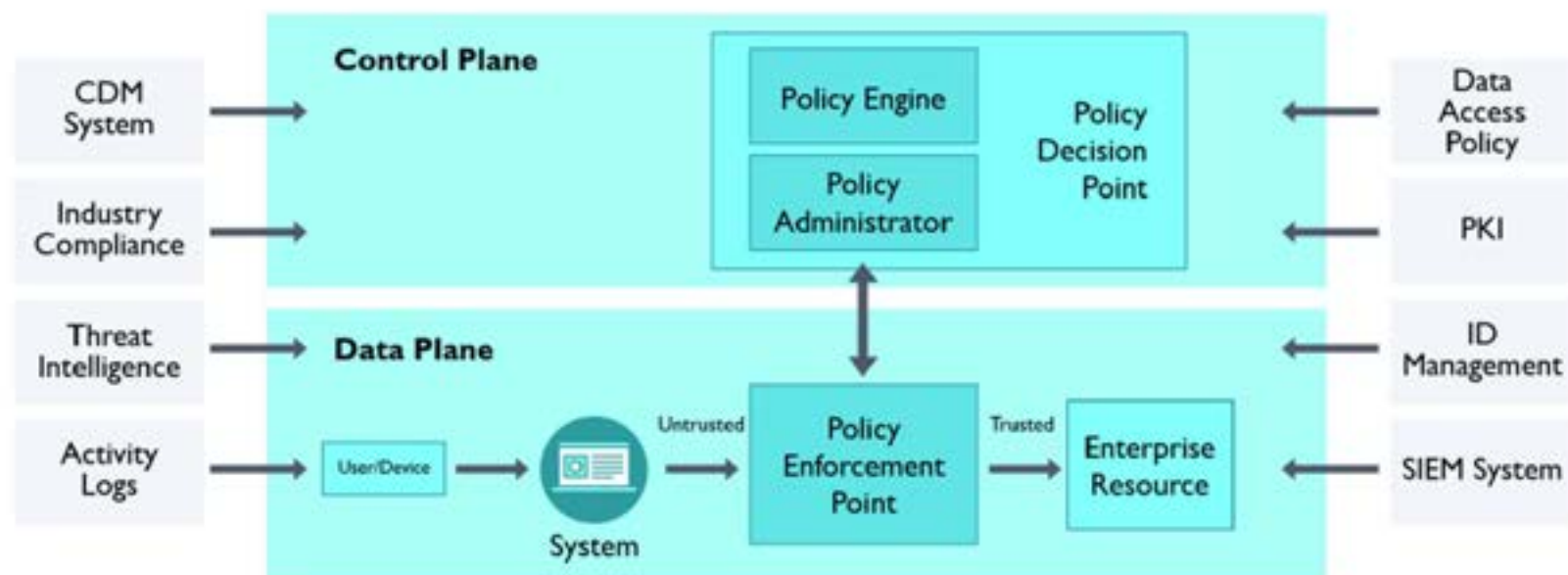


Figure 2: Key Logical Components of a ZTA<sup>11</sup>



# Z T A

# IMPLEMENTATION

- Various ZTA implementation approaches defined by NIST SP 800-207
  - ZTA using Enhanced Identity Governance
  - ZTA using Micro-Segmentation
  - ZTA using Network Infrastructure and Software Defined Perimeters



# ZERO TRUST NETWORK ACCESS (ZTNA) IMPLEMENTATION

- ZTNA supports a paradigm
  - where neither users nor the applications they access are sitting behind the perimeter.
  - Considered a VPN replacement, ZTNA allows users to access services from anywhere, anytime, from any device.
  - ZTNA consists of two distinct architectures:
    - endpoint-initiated ZTNA (on managed devices)
    - service-initiated ZTNA (for unmanaged devices)

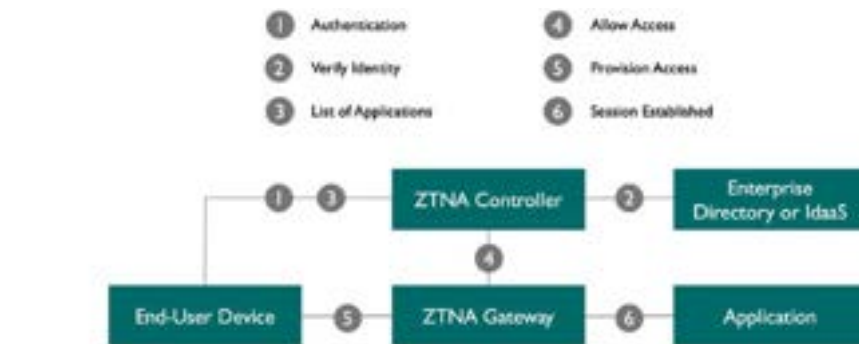


Figure 9: Endpoint-Initiated ZTNA Communication Flow<sup>12</sup>

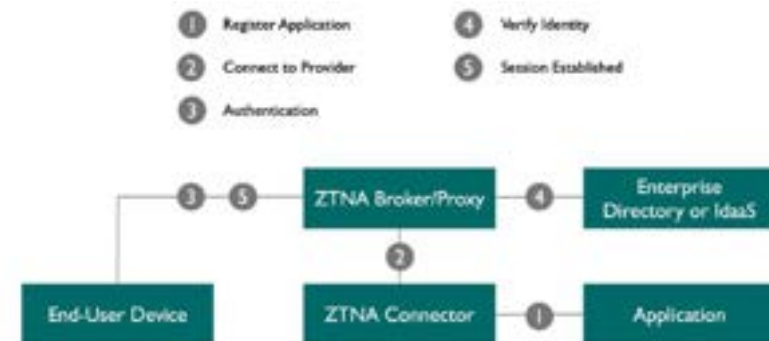


Figure 10: Service-Initiated ZTNA Communication Flow<sup>12</sup>

# CSA – CCZT CERTIFICATE

cloud security alliance®

Membership ▾ STAR Program ▾ Certificates & Training ▾ Research ▾

## Certificate of Competence in Zero Trust (CCZT)

The industry's first authoritative Zero Trust training and certificate.

Take the Exam View Training

CCZT

<https://cloudsecurityalliance.org/education/cczt/>