Cyber Risk Impacting PNG

Matt Dri – KPMG, Partner Cyber Response

My Background

MATT DRI
PARTNER

KPMG
Tower Two
Collins Square
727 Collins Street
DOCKLANDS VIC 3008

Tel +61 3 8620 9743
mattdri@kpmg.com.au

Function and Specialisation

- Cyber Incident Response
- Forensic Investigations
- Detection Engineering
- Threat Intelligence
- Compromise Assessments
- Threat Hunting
- Tabletop Exercises
- Incident Handling training
- Incident Response planning and playbook development

Education, Licenses & Certifications

- Bachelor of Applied Science, RMIT
- Advanced Diploma in Information Technology, RMIT

Professional and Industry Experience

Matt is a highly regarded, Digital Forensics and Incident Response professional, with over 19 years experience responding to security incidents around the world. Throughout his career, he has faced a multitude of attack types including ransomware, extortion, theft, fraud, espionage, denial of service and destructive attacks.

Matt's expertise extends beyond the realm of consulting. He has played a pivotal role as a security operations leader. In this capacity, he has been responsible for developing people, process, playbooks, automation and metrics.

Examples of Matt's recent experience include:

- High profile incident – Matt managed and led the response to a threat actor posting screenshots on Twitter of a large technology companies internal customer support systems. Matt was able to keep the investigation team calm and maintain focus on accurate and timely delivery. Matt's forensic analysis was crucial in changing the publics perception of the business and shutting down the media cycle. The engagement involved working closely with a third-party forensic provider, auditors, law enforcement, public relations, and multiple legal teams.
- [redacted] located in the Asia Pacific region. Matt found evidence of the threat actor using a zero-day vulnerability hosted on a popular news website which was used to strategically target the victim organization. Using custom malware, the threat actor achieved their objective, finding a backdoor into sensitive [redacted] continued attacks.
- Fact based decision making – Matt led the investigation in response to self-propagating malware rapidly spreading throughout a large government Health [redacted] to [redacted] This [redacted] have led to significant disruption to patient care. Matt was able to triage the malware and make the determination that the payload was benign. Working with the wider response team, a remediation plan was devised without impacting hospital operations. At the conclusion of the investigation, Matt presented on [redacted] IT service provider. He was able to effectively communicate, with evidence, that the source of the malware infection originated from the multinational IT service provider's internal network, a finding that multiple forensic teams failed to identify.
- Containment and recovery - Threat actors infiltrated a financial planning business and encrypted all client advice. The IT service provider recovered the client advise from a backup, however, the threat actors returned and re-encrypted the recovered data and the attached backup. Via a retainer service with a parent business, Matt was engaged for Incident Response. He first identified how the threat actor infiltrated the business and closed the vulnerable entry point He was then able to use forensics to recover a backup drive and restore critical client advice. The business was unlikely to have survived without Matt's support.
- Detection Engineering and Automation – Alert fatigue can lead to major business disruptions. Matt architected and led a team of security engineers in the development of a serverless infrastructure capable of detecting risks and notifying those responsible. The outcome being triage delegated to persons responsible and alerts escalated to security operations when warranted. With the integration of threat intelligence and automation, a small team was able to scale detection and response across for a global identity cloud, a major target for sophisticated adversaries.

Highly experienced, battle tested leader in incident response and detection engineering that's calm under pressure and a great mentor to those around him

Notable PNG Incidents

Oct 2021

Department of Finance

Ransomware attack locking access to hundreds of millions of dollars in foreign aid money

Ransomware Hackers Freeze Millions in Papua New Guinea

- The government's payment system has been locked by hackers
- Attackers demand payment from nation hard hit by Covid-19

December 2022

Telecommunications Provider

Port Moresby, Cobalt Strike beacon activity

August 2023

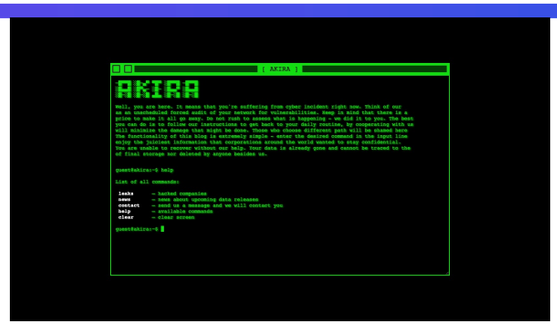
Spectra Industrial

Distribution of forklifts, generator sets, PPE, solar products and heavy equipment. Personal information of the company's clients, Personal correspondence, Financial statements, Documents containing confidential information

June 2022

Government Department & Workforce Management Organisation

Carbanak RAT software operated by FIN7 who have been expanding into ransomware



May 2023

Harmony Gold

Gold mining and exploration company, has operations and assets in South Africa and Papua New Guinea. 3,5 TB of data

PNG Ranked 124th in the National Cyber Security Index (https://ncsi.ega.ee/ncsi-index/?order=rank)

RUSSIAN MARKET

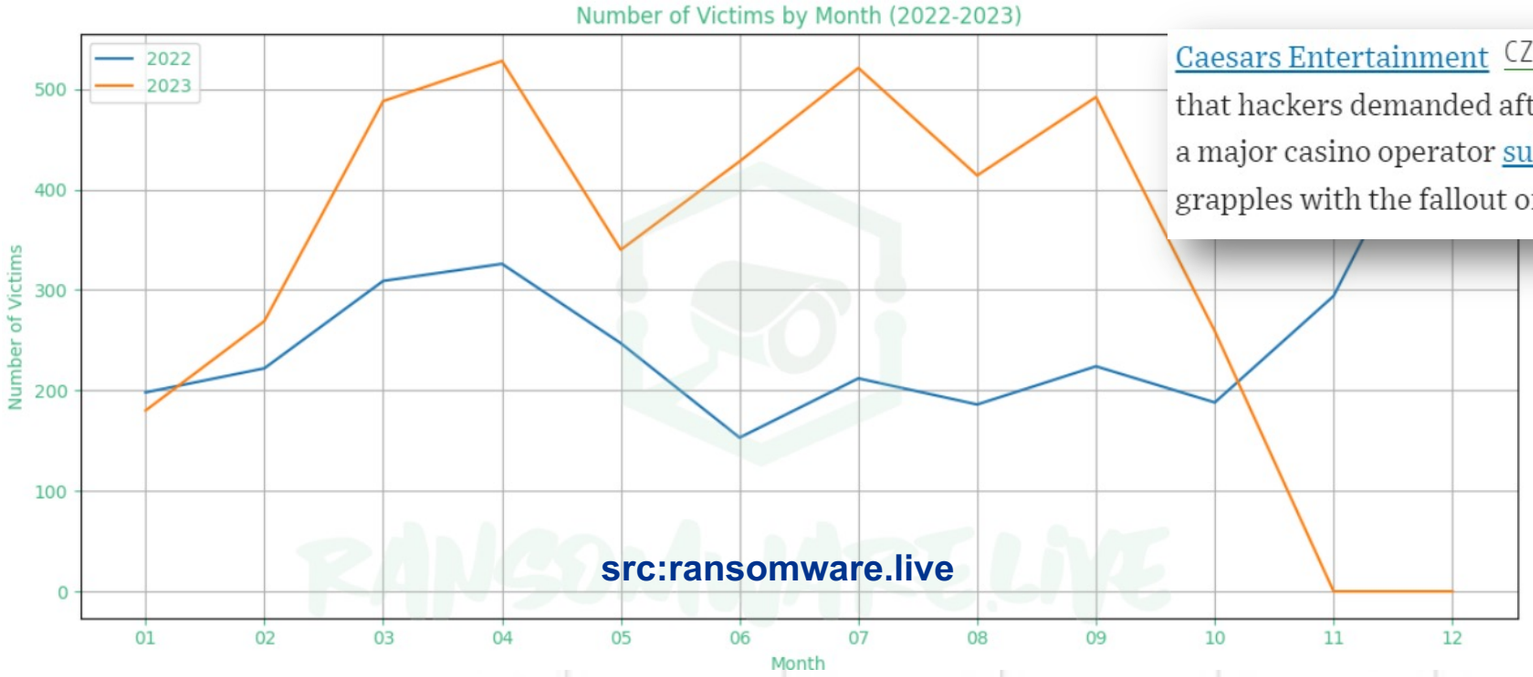
User

- News
- CVV
- Dumps
- RDP
- LOGS pre-order
  - Pre order
  - My orders
- PROs
- Checkers
- Tools
- My Purchases
- Support

Earn money

Stealer	Country	Links	Outlook	Info	Struct	Date / Siz
Redline	National Capital ISP: Telikom PNG Limited	topup.digicelgroup.com | qantas.com | groups.itu.int | passport.alibaba.com | secure.agoda.com | agoda.com | itu.int | itu.int | 192.168.1.1 | 192.168.1.2 | 192.168.2.121 | home.mycloud.com | ucloudcam.com | ipa.gov.pg | 192.168.0.31 | qantasstore.com.au | confsynch.itu.int | 10.38.108.244 | watchnrl.com | japanesecartrade.com | japanesevehicles.com | mediaclient.netflix.com | nslonline.com.pg | account.hotspotshield.com | eyeplusiot.com | idmsa.apple.com | 192.168.0.53 | wdstorage | digicelid.digicelgroup.com | netflix.com | soeonline.info.gov.pg | sc.telikompng.com.pg | extranet.itu.int | shoppingcart.aliexpress.com | 192.168.0.252 | paypal.com | 192.168.0.252 | eyeplus.closeli.com | authentication.logmeininc.com | login.aliexpress.com | sals.nambawansuper.com.pg | account.samsung.com | sc.telikompng.com.pg | itu.int | 192.168.8.1 | 192.168.137.1 | selfcare.bmobile.com.pg | sc.telikompng.com.pg | 192.168.15.1 | 192.168.1.1 | sc.telikompng.com.pg | sc.telikompng.com.pg | aliexpresshd.alibaba.com | sc.telikompng.com.pg | adobeid.services.adobe.com | 192.168.0.119 | 192.168.0.119 | members.bet365.com | bet365.com | extra.bet365.com | members.bet365.com | signup.microsoft.com | bet365.com.au | 192.168.0.130 | sc.telikompng.com.pg | builder.zety.com | udemy.com | accounts.google.com | apt.int | login.itu.int | itu.int | extranet.itu.int | adfso.itu.int | 10.10.10.1 | adobeid.services.adobe.com | adobeid-na1.services.adobe.com | registration.apec2021nz.org | dx-flights.airniugini.com.pg | dx-flights.airniugini.com.pg | eventbrite.com | apply.dherst.gov.pg | myschoolappme.azurewebsites.net | idp.scu.edu.au | ssidm.scu.edu.au | idp.scu.edu.au | vastosoft.com | login.microsoftonline.com | account.live.com | 192.168.0.120 | cam.britannica.com | vodafone.com.pg | linkedin.com | login.live.com | login.live.com | learn.scu.edu.au | 192.168.15.1 | aws.ycc365plus.com | openstreetmap.org | sso.garmin.com | ibc.bsp.com.pg | tunnelbear.com | 192.168.15.2 | online-top-up.digicelgroup.com | 192.168.15.2 | digicelid.digicelgroup.com | selfcare.digicelpng.com | 192.168.15.2 | hitssite.com | expressvpn.com | auth0.accounts.westerndigital.com | 192.168.15.201 | 169.254.159.74 | 169.254.159.74 | 169.254.159.74 | login.microsoftonline.com | login3.id.hp.com | 192.168.2.252 |	-	-	archive.zip DomainDetects.txt ImportantAutofills.txt InstalledBrowsers.txt InstalledSoftware.txt Passwords.txt ProcessList.txt UserInformation.txt Autofills Google_[Chrome]_Default.txt Microsoft_[Edge]_Default.txt Cookies Google_[Chrome]_Default Extension.txt Google_[Chrome]_Default Network.txt Microsoft_[Edge]_Default Network.txt CreditCards Google_[Chrome]_Default.txt FileGrabber Users Kulu Alu	2023.09.1 *0.05Mb*

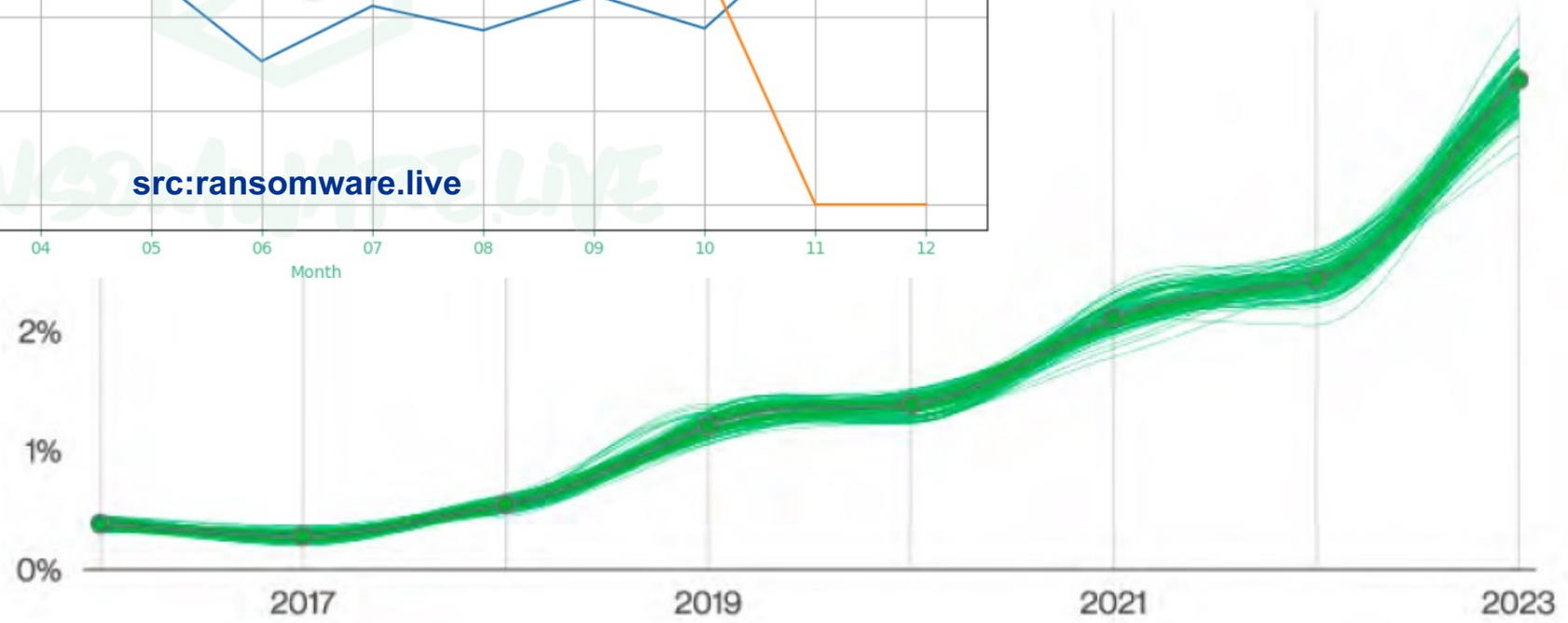
The Two Largest Risks: BEC & Ransomware



src:ransomware.live

> [Caesars Entertainment](#) CZR 2.43% ▲ paid roughly half of a $30 million ransom that hackers demanded after a cyberattack late this summer, another example of a major casino operator [suffering from an attack](#) as [MGM Resorts](#) MGM 1.75% ▲ grapples with the fallout of a recent incident.

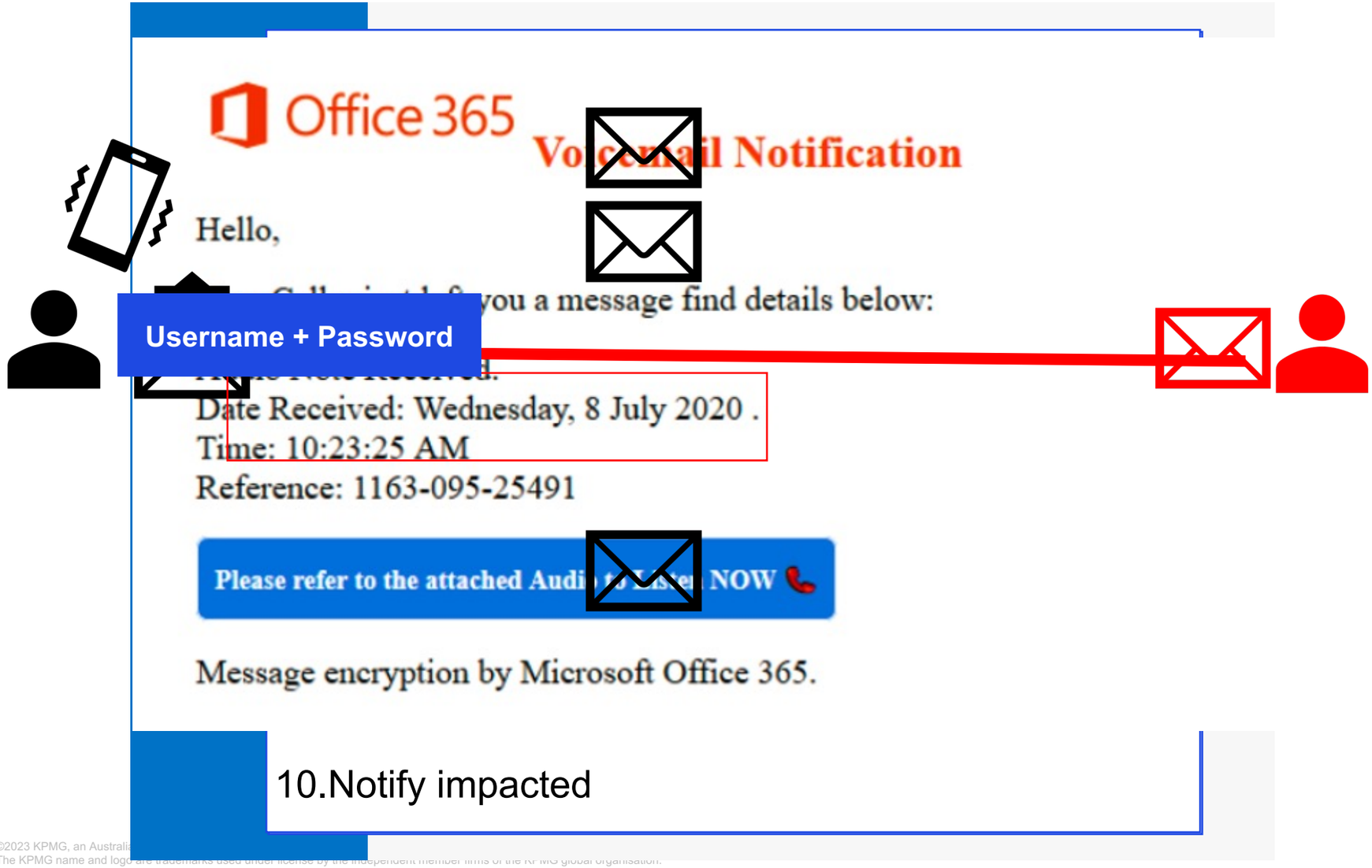
BEC **$98 million** *an average loss of* **$64,000** *per report.*
src: ACSC 2022 Threat Report



src: https://www.verizon.com/business/en-au/resources/reports/dbir/

Business Email Compromise (BEC)

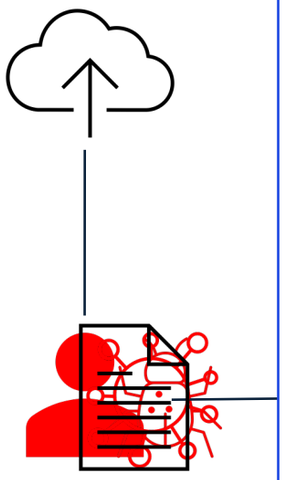
Business Email Compromise & Phishing



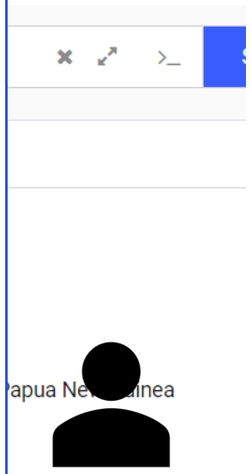
10.Notify impacted

Ransomware

Ransomware



1. Invoke Incident Response Plan
2. Engage retained breach lawyers and IR investigators
    1. Preserve evidence and contain the incident
    2. Draft initial breach communications
    3. Consider Threat Actor negotiation
    4. Contact insurer
3. Perform mandatory notifications
4. Determine root cause, extent of breach and confirm no backdoors have been deployed
5. Review at risk data
6. Develop public relations plan: call centres, customer support..
7. Notify impacted parties and manage customer queries
8. Conduct Post Incident Review
9. Build and action remediation plan taking input from Investigation report and PIR

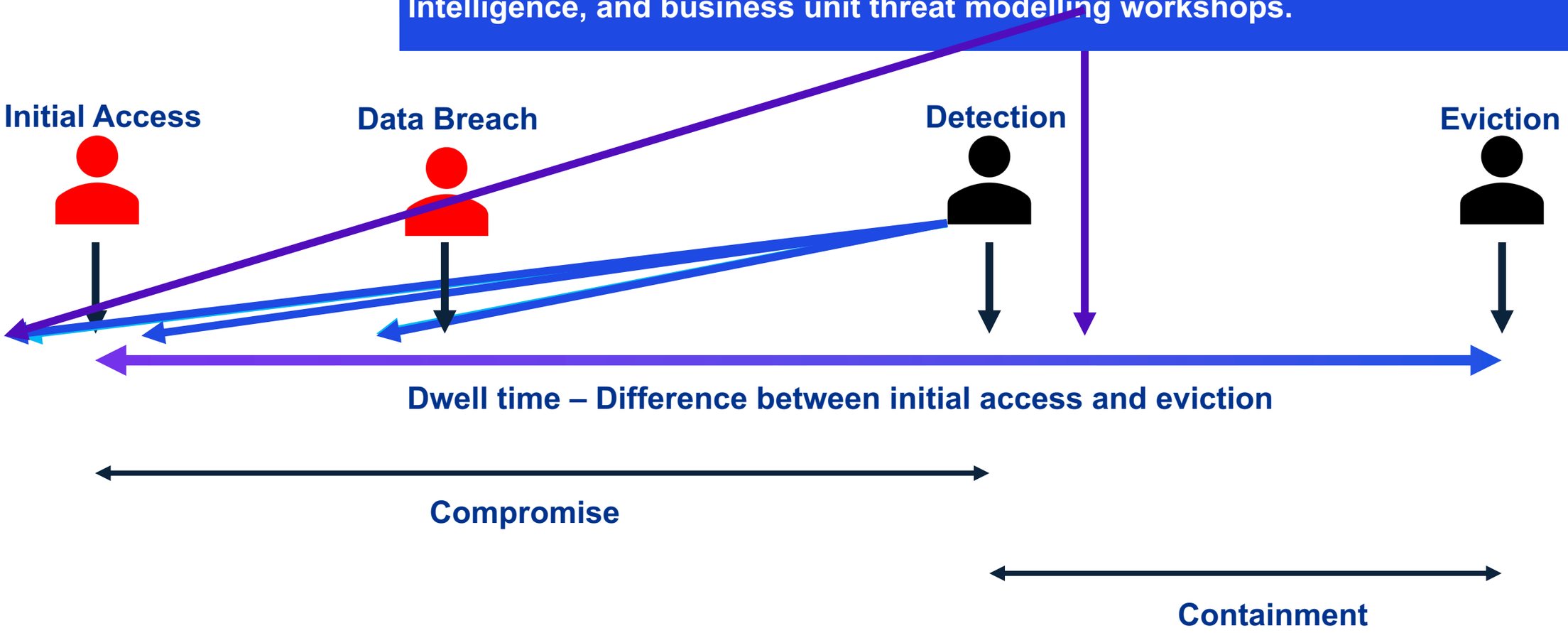


Reducing Dwell Time

Dwell Time

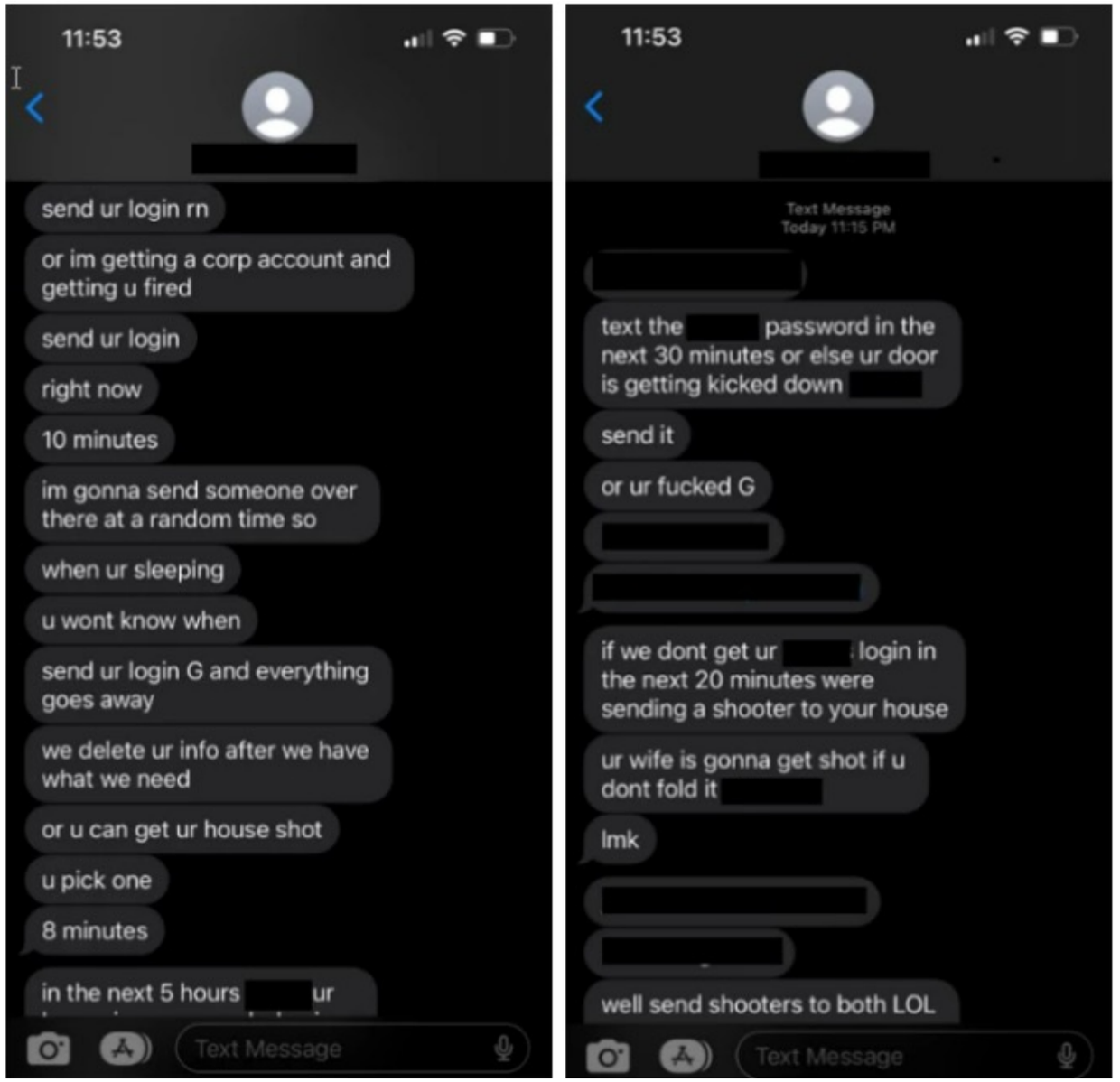
Detection Engineering

Continuous improvement in detection coverage, quality assurance and response automation. Taking input from intrusion analysis, attack simulation, Threat Intelligence, and business unit threat modelling workshops.



Preparing for what's next

- Generative AI being used to bypass KYC verification
- Continued external management interface compromise
- Aggressive social engineering
- Threat Actors leveraging DevOps
- Data lake compromise
- Continued supply chain attacks, BPO's and software
- Disinformation and misinformation

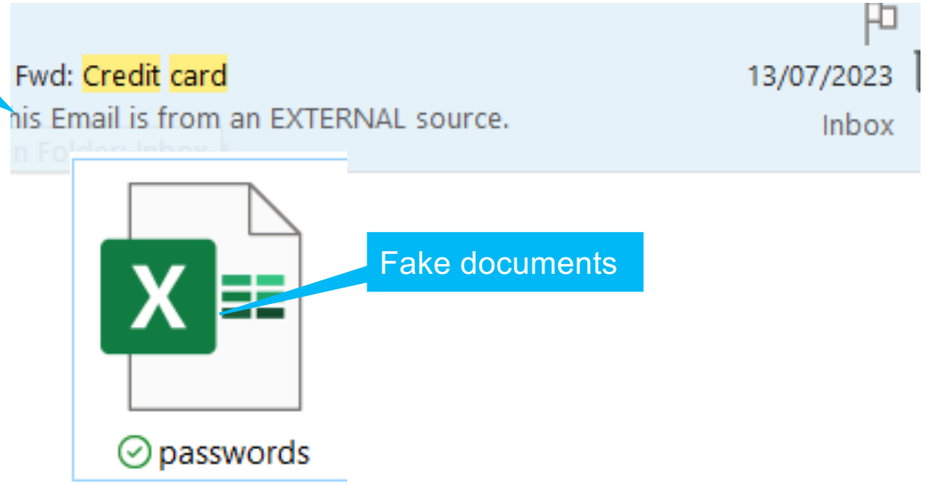


src: Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction | Microsoft Security Blog

Detection using Deception

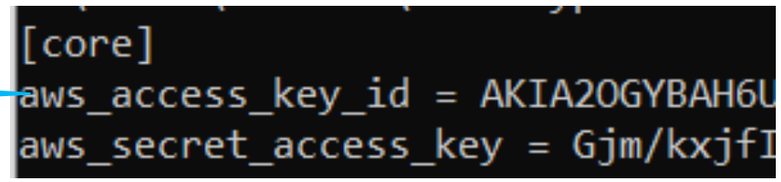
High fidelity detection	Low to no cost	Easy to deploy	Building blocks for automation	Early detection	Deception may lead to adversary mistrust and paranoia

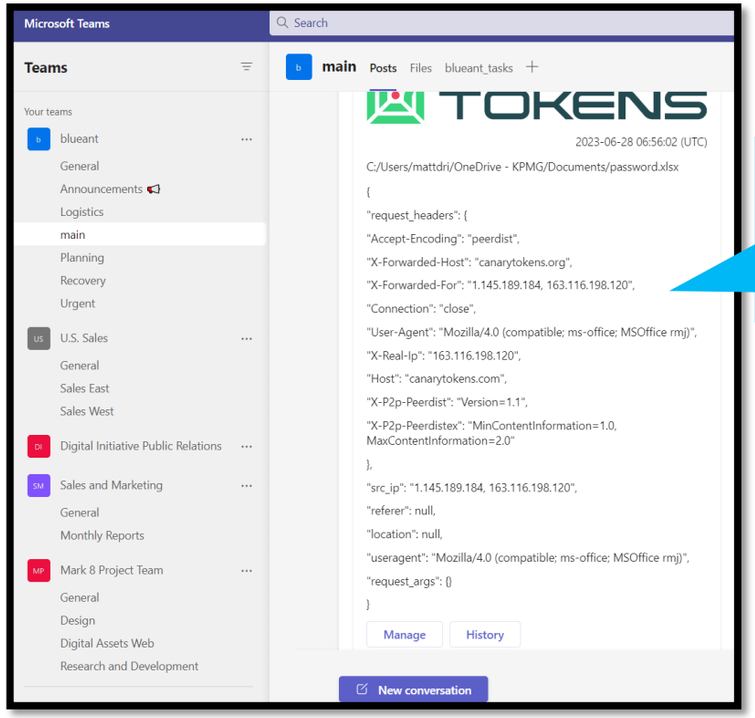
Fake credit card in mailbox



Fake documents

Fake credentials





Alert delivered to monitoring systems