KROLL

Business Email Compromises

An Evolving Attack

June 6, 2023

Courtney Dayter and Jamie Vendel

Table of Contents

1. Who We Are
2. Business Email Compromises
3. Trends
4. Proactive Solutions
5. Questions

Who We Are

Courtney Dayter

Associate Managing Director

- Been with Kroll for 8 years.
- Based out of Albany, NY.
- Specializing in leading Incident Response cases.
- GIAC Certified Forensic Examiner (GCFE), Certified Forensic Analyst (GCFA) and Network Forensic Analyst (GNFA).

Jamie Vendel

Vice President

- Been with Kroll for 5 years.
- Based out of Rochester, NY.
- Complete a variety of forensic investigations including Ransomware, Insider Threat, specializing in M365 and Business Email Compromises.
- GIAC Certified Forensic Examiner (GCFE) and Certified Forensic Analyst (GCFA).

Stay Ahead with KROLL

Risk and Financial Advisory Solutions

6,500 professionals worldwide
Continuing the firm's nearly 100-year history of trusted expertise

Unique insights, data and technology
Providing foresight clients need to create an enduring competitive advantage

1 **Valuation**

Valuation of businesses, assets and alternative investments for financial reporting, tax and other purposes.

2 **Compliance and Regulation**

End-to-end governance, advisory and monitorship solutions to detect, mitigate and remediate operational security, legal, compliance and regulatory risk.

3 **Corporate Finance and Restructuring**

Comprehensive corporate finance, investment banking and restructuring support to clients, investors and stakeholders.

4 **Cyber Risk**

Incident response, digital forensics, breach notification, managed detection services, penetration testing, cyber assessments and advisory.

5 **Environmental, Social and Governance**

Solutions include policies and procedures, screening and due diligence, disclosures and reporting and investigations, value creation and monitoring.

6 **Investigations and Disputes**

Worldwide expert services and tech-enabled advisory through all stages of diligence, forensic investigation, litigation and testimony.

7 **Business Services**

Technology-enabled legal and business solutions for corporate restructurings, settlement administrations, issuer services, agent and trustee services and other complex support needs.

By The Numbers

3,200+
ENGAGEMENTS IN 2021

550+ PRACTITIONERS
ACROSS 18 COUNTRIES

FORTUNE 100 TO MEDIUM-SIZED BUSINESSES

WORKING WITH **60+** CYBER INSURANCE CARRIERS

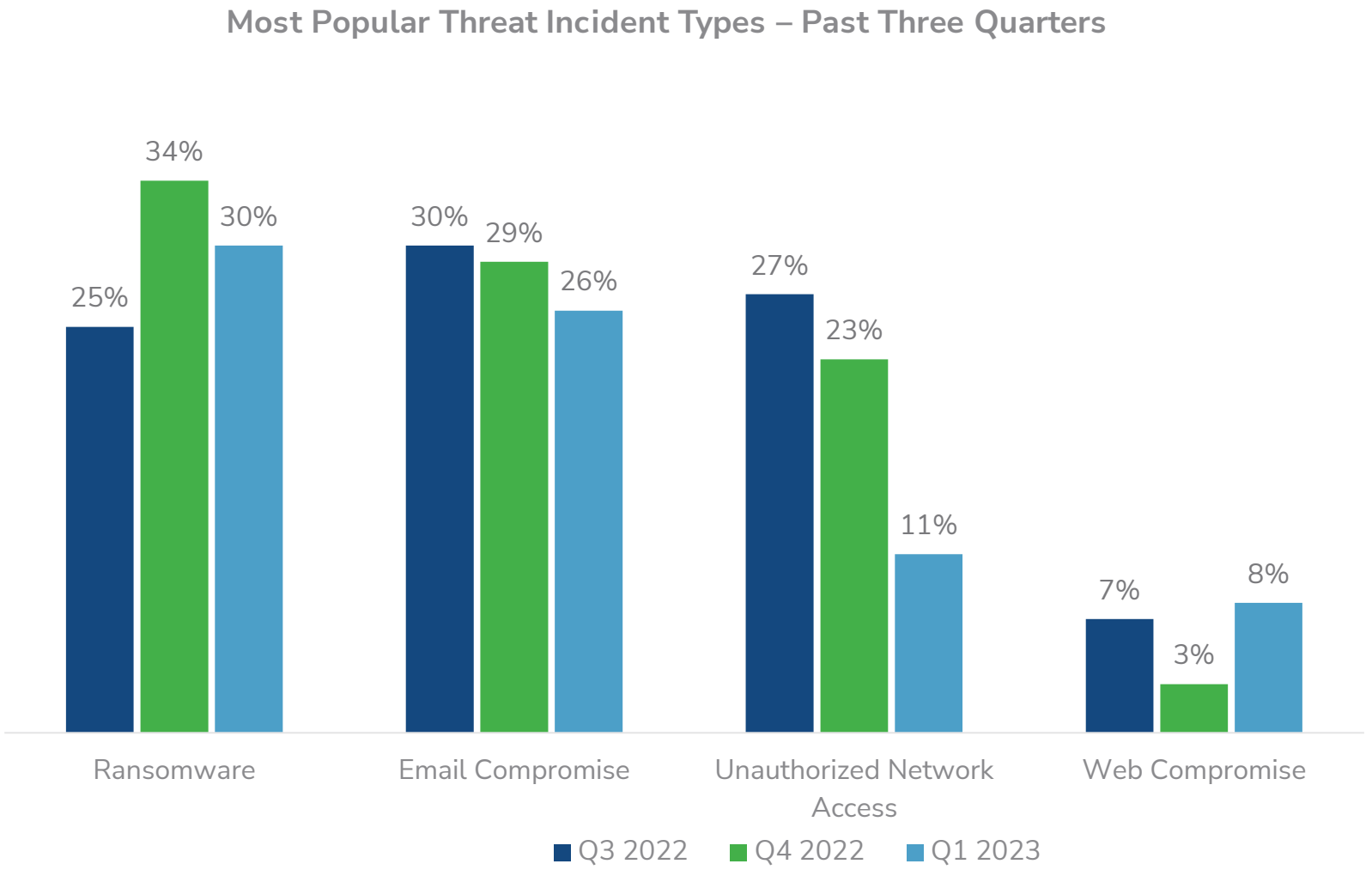
Reactive Services
- Incident Response

Managed Services
- 24/7 Managed Security Operations Center
- Endpoint Detection and Response

Cyber Threat Intelligence
- Dark Web Assessments
- Threat Landscape

Proactive Services
- Vulnerability Assessments
- Penetration Testing
- Governance and Risk Assessment
- Ransomware Preparedness

Overview – Cyber Crime Trends



Business Email Compromise

KROLL

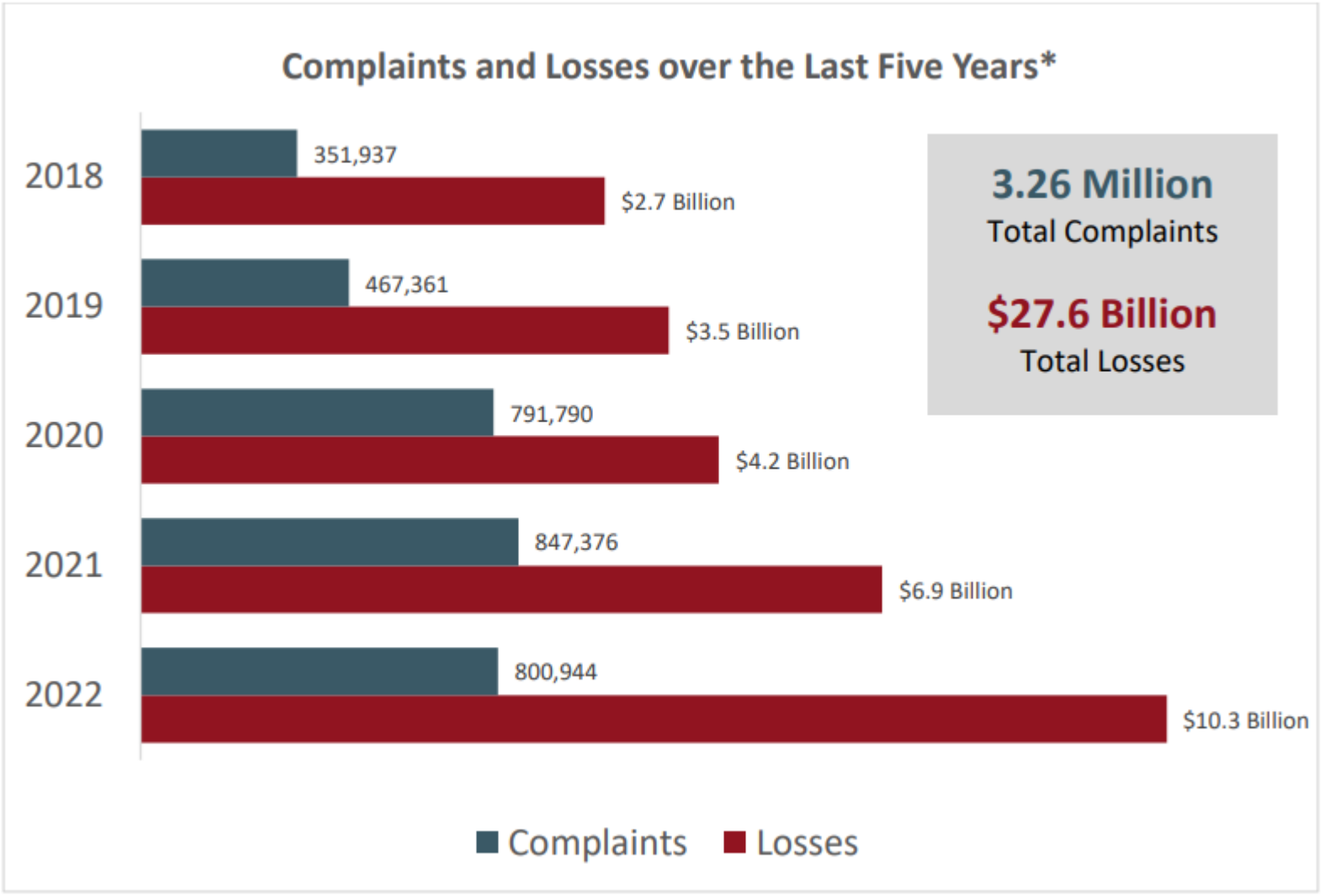
Business Email Compromise

Unauthorized access of email accounts for the purpose of collecting or exploiting sensitive information or access.

Typically gained via a phishing email that redirects to a site where credentials are stolen. May mirror a known log-in domain like Office 365, SharePoint, Google Drive.

Financially-motivated attacks
- redirect wire transfers to actor-controlled accounts or cryptocurrency wallets.

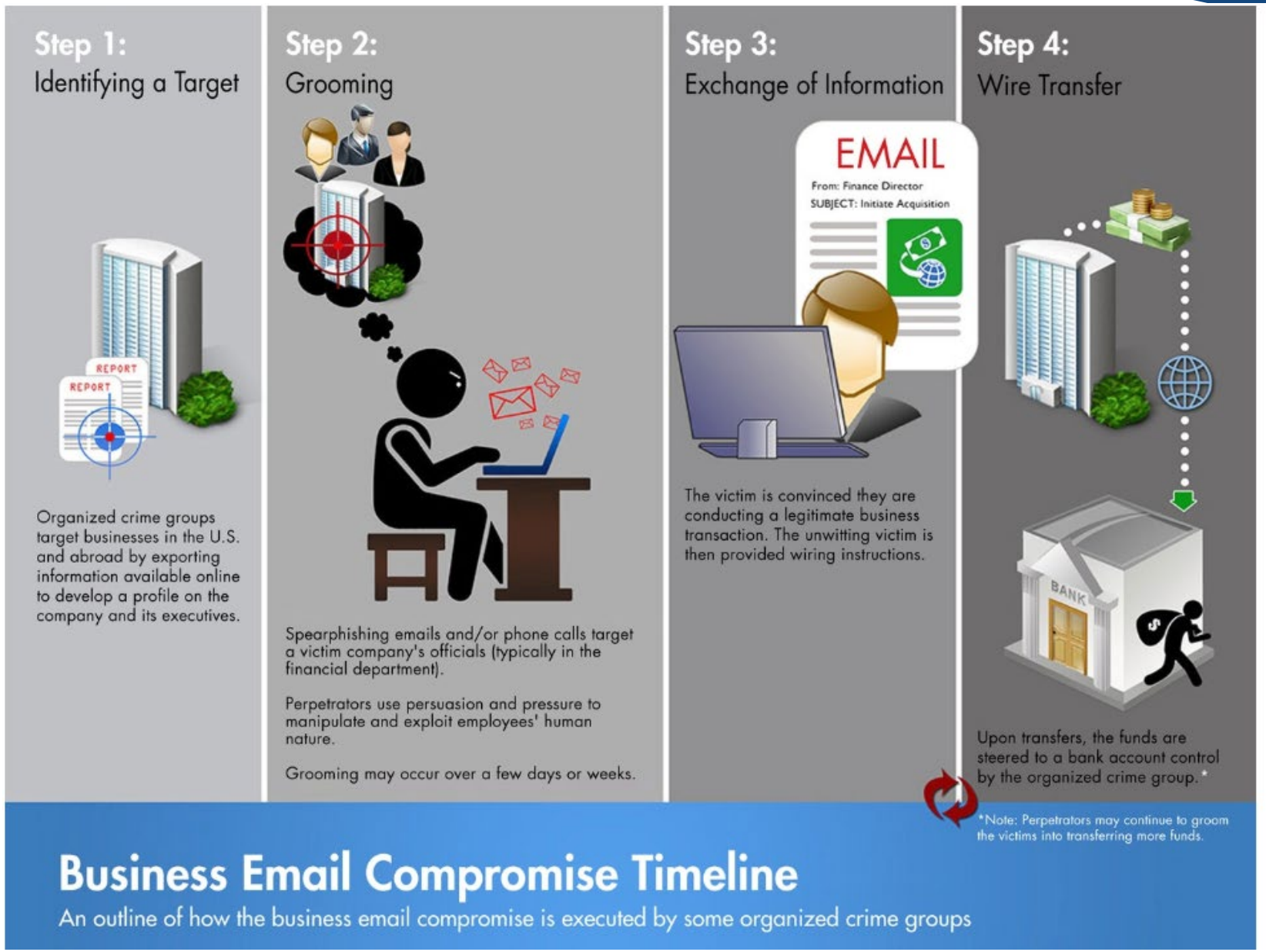
*Bad Actor has already arranged control of a named cryptocurrency wallet for the funds to be converted to



2022 BEC Losses:

$2.7 Billion

Image Source: IC3.gov



Source: FBI.Gov

5 Types of BEC

Bogus Invoice

CEO Fraud

Account Compromise

Attorney Impersonation

Data Theft

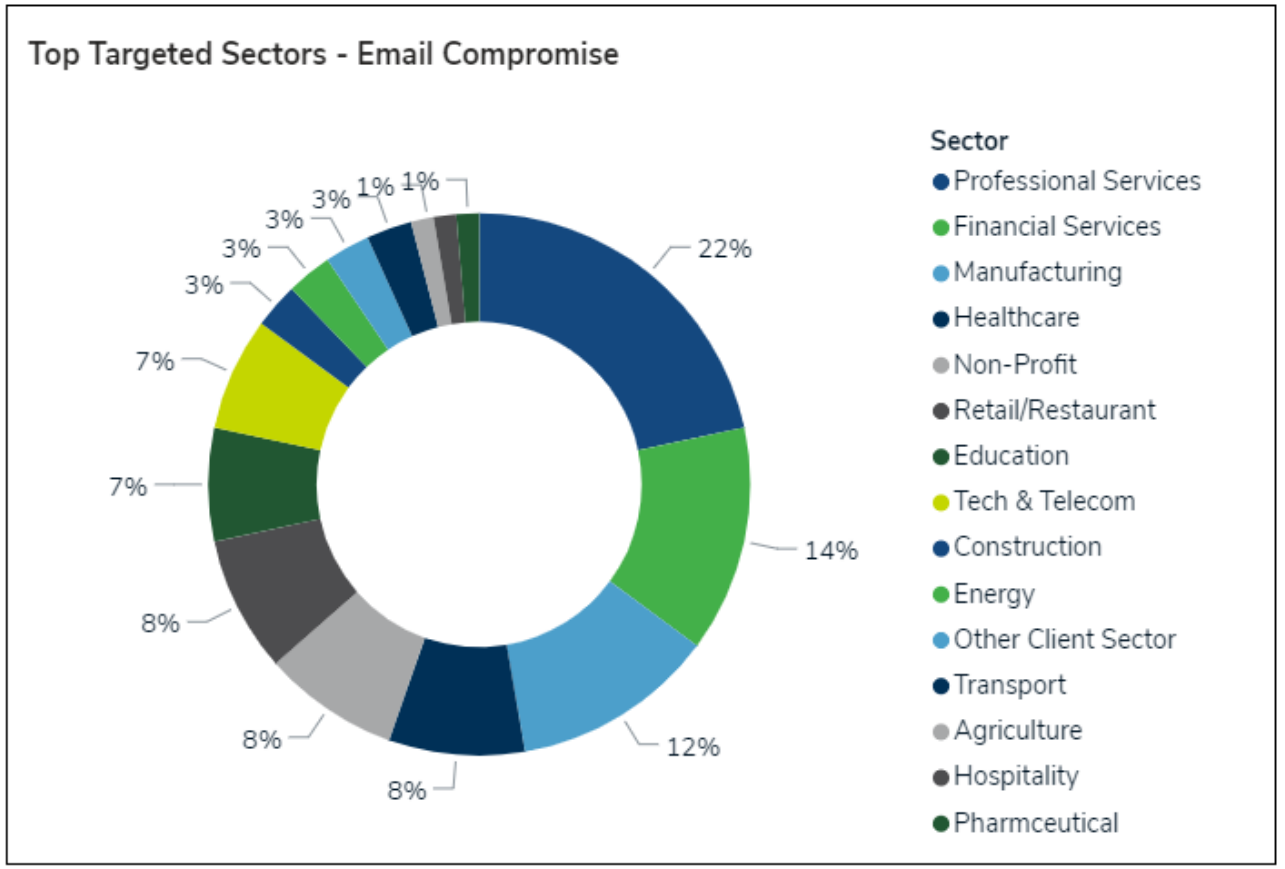
Why do actor(s) target BECs?

- Some are short-term, looking to redirect wire transfers or employee paychecks, send outbound spam, target bigger fish, collect as many credentials as they can, or to harm reputation.
- CVE/RCE/Zero Day – Exchange Servers
- Some are long-term, leading to Intrusion Lifecycles and Ransomware focused operations for larger payouts.

- Kroll conducts approximately 3,200 engagements per/year. Approximately 30% of the IRs Kroll Cyber works annually are BEC's and are about tied with Ransomware in volume.
- All have the same end goal of stealing money or critical information.

Targeted Sector(s) for BEC's

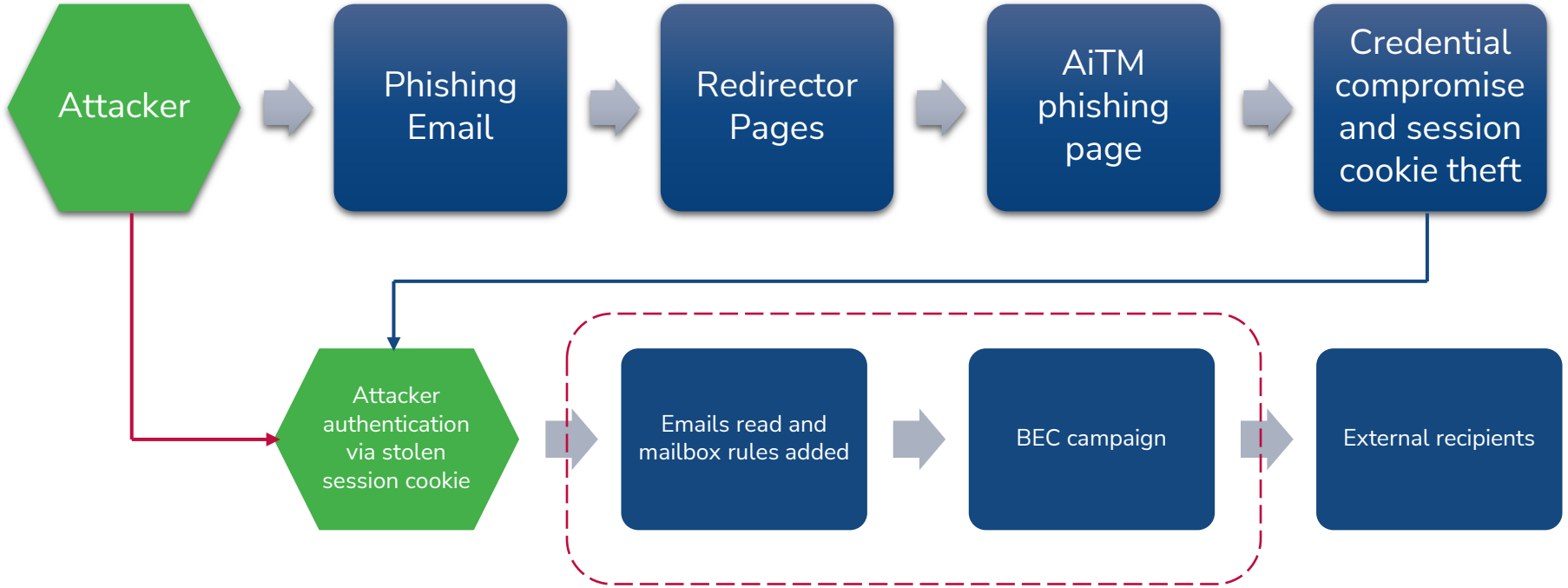
- Business email compromises affect a wide variety of industries and businesses.
- As of May 2023, Kroll has seen the Professional Services sector as the top targeted sector.
- Followed by Financial Services/Banking, Manufacturing and Healthcare.
- However, any individual who handles finances and executive decision-making roles can be a target.
- Threat actors perform reconnaissance on who approves payments within an organization and target those individuals with phishing campaigns.



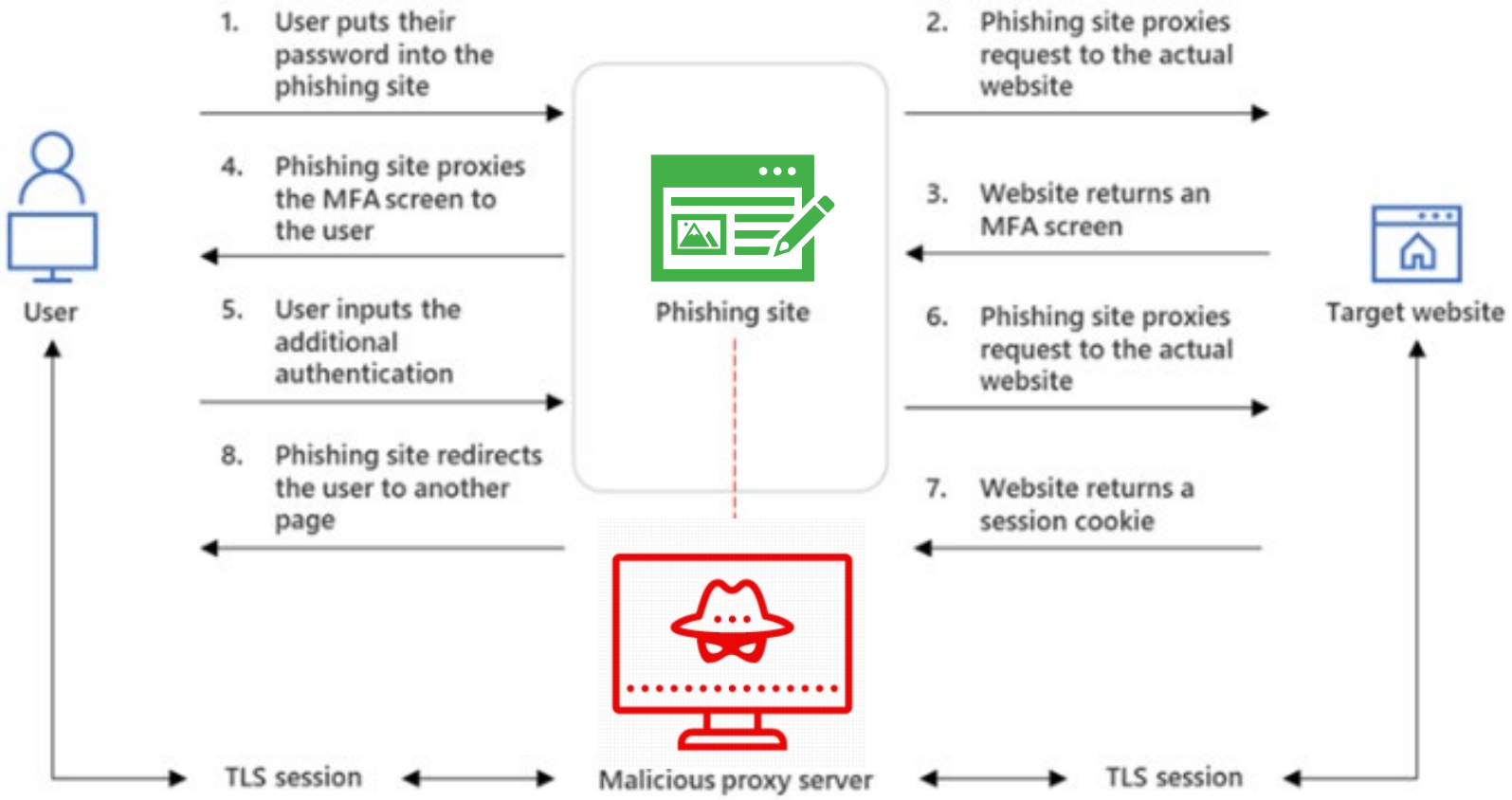
Trends

Adversary in the Middle (AiTM)

- **What is AiTM?**
- A bad actor intercepts and modifies communications between two parties, typically a user and a website or service, to steal sensitive or financial information, such as login credentials and credit card data



Adversary in the Middle (AiTM)



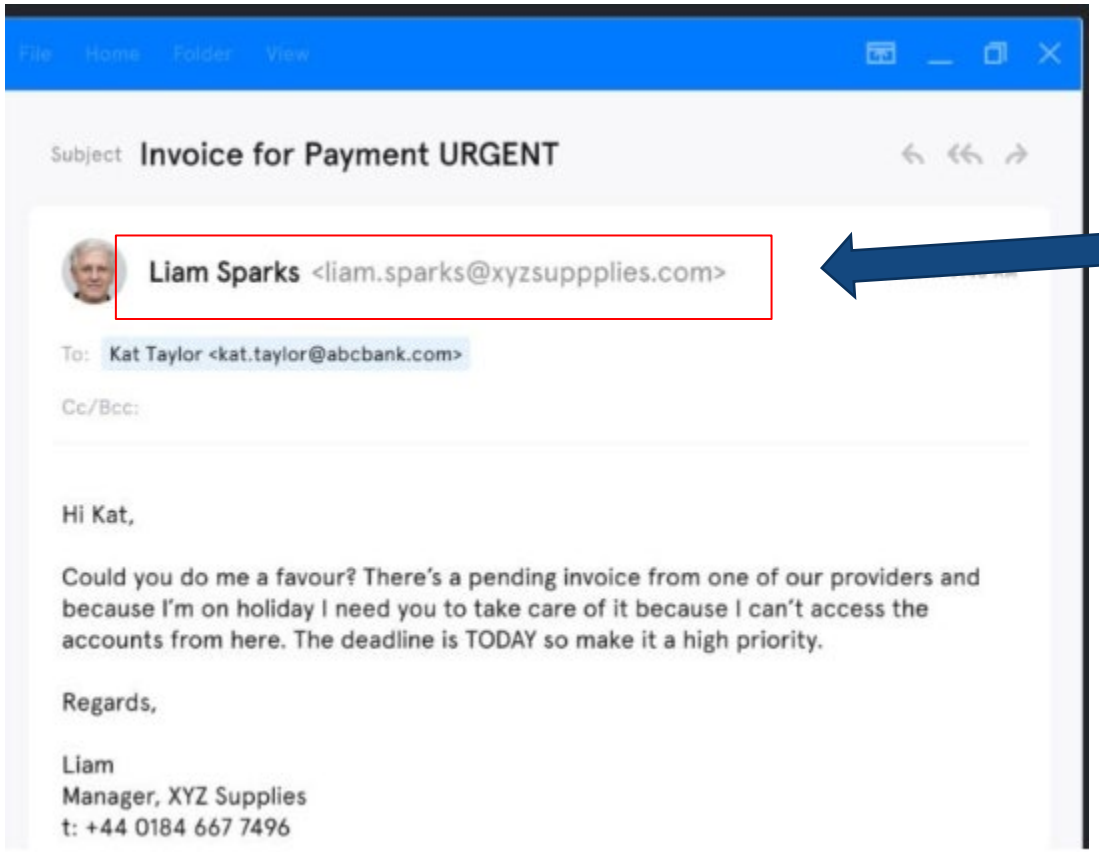
Adversary in the Middle (AiTM)

- **How to detect it in the Unified Audit Logs:**

Event Date/Time UTC 24hr	Source IP	City	State	Country	ISP	Assessment	Operation (or) Status Message	Session Token
02/10/2023 13:06:27	45.92.142.7	Los Angeles	California	United States	DediPath	Context	User Logged In	SessionId"","Value"":"ef038dfa-dfee-4382-aa86-25e76de2d364
02/10/2023 13:06:44	45.92.142.7	Los Angeles	California	United States	DediPath	Context	User Logged In	SessionId"","Value"":"ef038dfa-dfee-4382-aa86-25e76de2d364
02/10/2023 13:06:47	45.92.142.7	Los Angeles	California	United States	DediPath	Context	User Logged In	SessionId"","Value"":"ef038dfa-dfee-4382-aa86-25e76de2d364
02/11/2023 22:56:14	91.193.232.131	Atlanta	Georgia	United States	Clouvider Limited	Malicious	User Logged In	SessionId"","Value"":"ef038dfa-dfee-4382-aa86-25e76de2d364
02/11/2023 22:56:21	91.193.232.112	Atlanta	Georgia	United States	Clouvider Limited	Malicious	User Logged In	SessionId"","Value"":"ef038dfa-dfee-4382-aa86-25e76de2d364
02/11/2023 22:56:21	91.193.232.131	Atlanta	Georgia	United States	Clouvider Limited	Malicious	User Logged In	SessionId"","Value"":"ef038dfa-dfee-4382-aa86-25e76de2d364

- **How to prevent it:** Create a CAC policy to only allow access from managed devices.
- There is a new CAC policy from Microsoft released 3/14/23 that is finer tuning, but has caveats.

Domain Name Spoofing



TACTIC: Domain Spoofing

Legitimate Domain:
xyzsupplies.com

Spoofed Domain:
Xyzsuppplies.com

Other Iterations:
Xyzsupplies.com
Xyzsuuplies.com

- Be aware of letter lookalikes:
  - rn < RN
  - l < capital I not lower L
- Be cautious of spoofed phone numbers as well.

Smishing Trends

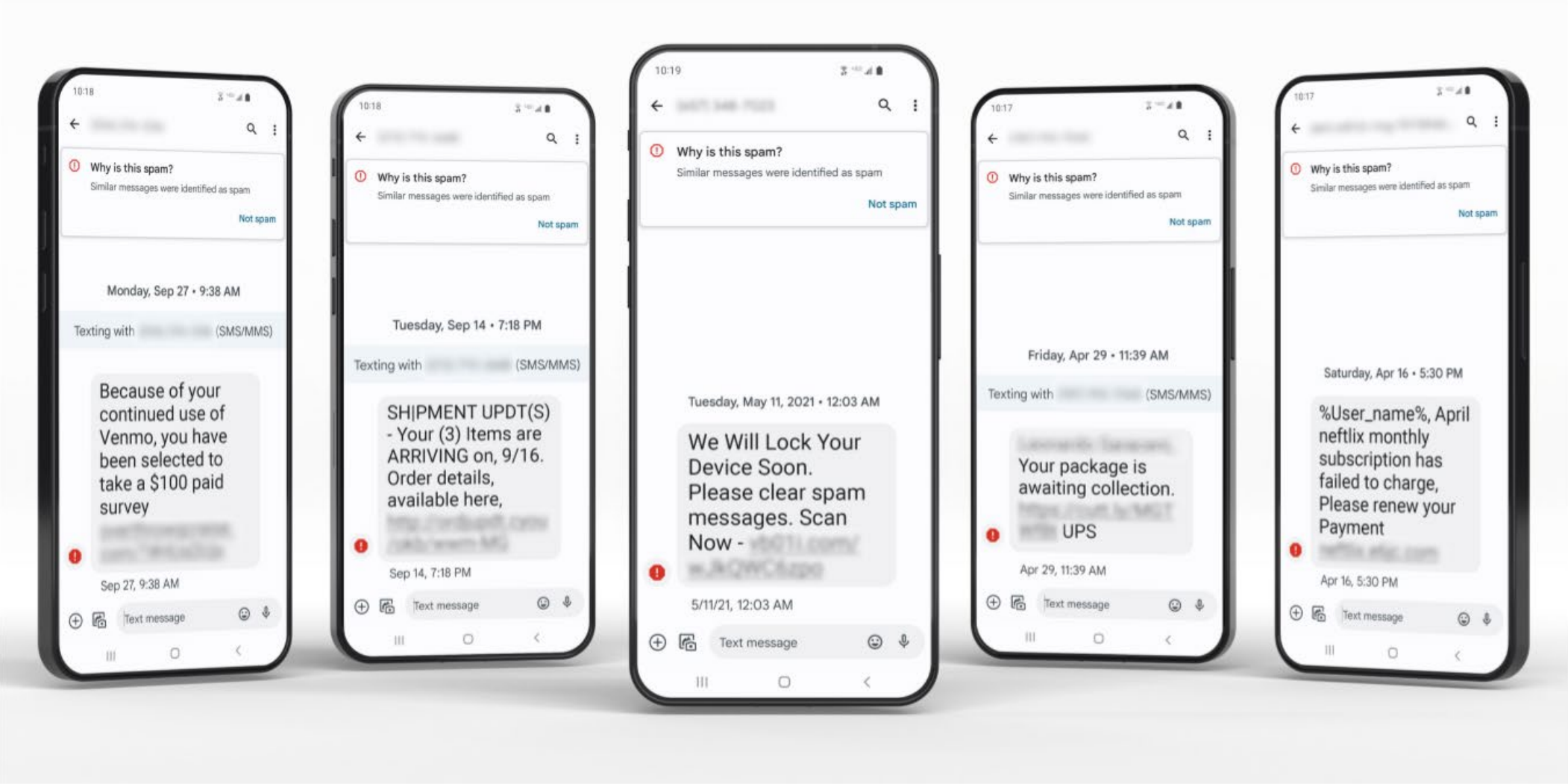


Figure 1: Examples of Smishing

Actor(s) Adding MFA Devices

- Kroll is seeing more and more cases where actor(s) are adding their own device to MFA.
- User gets phished, provides credentials, actor(s) login, user approves MFA push request\phone call, actor(s) login and add their own device to MFA to maintain persistence.

Azure Audit Example

Activity	IPAddress	Target1UserPr	ResultReason	ModifiedProperty
Update user	XX.XXX.XXX.XXX	test@test.com	Azure MFA StrongAuthenticationService	DeviceName:Test Device,AuthenticationType:3,
Add registered owner to device	XX.XXX.XXX.XXX	test@test.com	Device Registration Service	"Test Device"
Add registered users to device	XX.XXX.XXX.XXX	test@test.com	Device Registration Service	"Test Device"
Register device	XX.XXX.XXX.XXX	test@test.com	DeviceRegistrationClient	
User started security info registration	XX.XXX.XXX.XXX	test@test.com	User started the registration for Office Phone Call	
Update user	XX.XXX.XXX.XXX	test@test.com		PhoneNumber:"+1 XXXXXXXXXX","AlternativePhoneNumber":null, VoiceOnlyPhoneNumber":"+1 XXXXXXXXXX"
Update user	XX.XXX.XXX.XXX	test@test.com		MethodType:6:true
User registered security info	XX.XXX.XXX.XXX	test@test.com	User registered Office Phone Call	
Update user	XX.XXX.XXX.XXX	test@test.com	Azure MFA StrongAuthenticationService	DeviceName":"Test iPad"
Update user	XX.XXX.XXX.XXX	test@test.com	Azure MFA StrongAuthenticationService	DeviceName":"Test"

UAL Example

CreationTime	CombinedIP	UserId	Operation	ResultStat	_raw
XX/XX/XX XX:XX	XX.XXX.XXX.XXX	test@test.com	Update user	Success	StrongAuthenticationMethod, NewValue:[XXX], OldValue: [XXX]

Where can your team find this?

- **Azure Audit Log**
- Review add registered owner\users to device, user started security info registration, user registered security info, register device, update user events.
- Also check if an alternate phone number was added.
- **Unified Audit Log (UAL)** as an "Update User" event, check raw data.

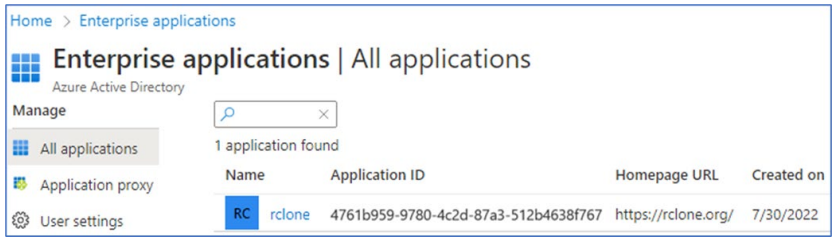
Actor(s) Adding Enterprise Applications

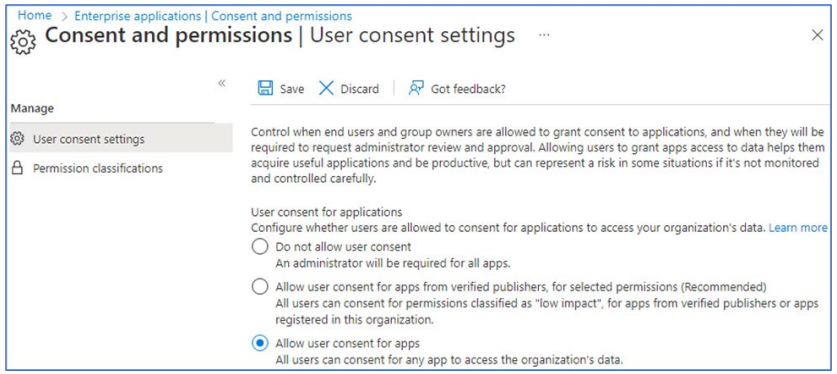
New tactic actor(s) are using to exfiltrate data from M365

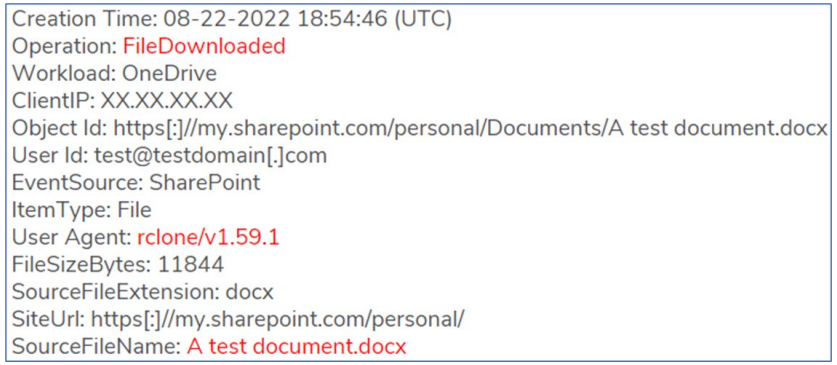
- Kroll has seen actor(s) adding Enterprise Applications like Rclone and PerfectData.
- Both applications allow users to collect different types of data from various data sources.
- In ***most*** cases, this will require a Global Admin account.
- The account only needs permissions to create and consent to enterprise applications; and access to the SharePoint site that the threat actor is targeting.
- In the case of overly permissive configurations; applications may be used with any level user account.
- Actor(s) created an Azure Enterprise Application, rclone on 7/30/22 using a compromised M365 global admin account.
- Actor(s) then used rclone to exfiltrate SharePoint\One drive data.
- Actor(s) were able to download 8,426 SharePoint\OneDrive files with Rclone via M365 within ~1 hour.
- Seen in UAL as "**FileDownloaded**" events

Link to article:

❖ New M365 Business Email Compromise Attacks with Rclone | Kroll







Actor(s) Adding Enterprise Applications Continued

Where can you find this?

- **1. Unified Audit Log (UAL)**
  - Check **User Agent String** (UAS) for application name
  - Review **File Downloaded** events
  - Review **Consent to Application** events (check for possibly compromised accounts and unfamiliar applications)

- **2. Azure Non-Interactive Sign-Ins**
  - Check UAS & Application
  - All of the users utilizing the application will appear here

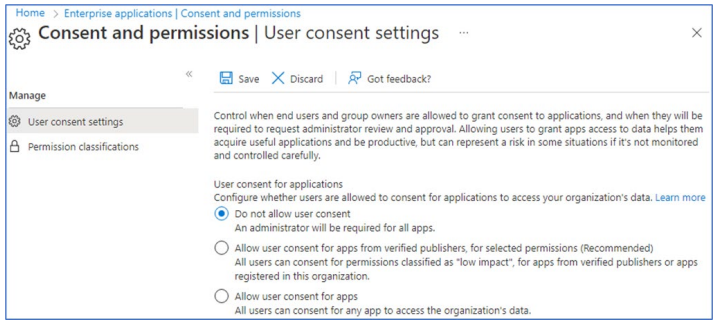
- **3. Azure Application Sign-Ins**
  - User, Application, IP Address
  - Enterprise Application > Activity > Sign-In Logs

- **4. Azure Enterprise Applications**
  - Any newly created apps?
  - Check "Created Date" (Only detail that cannot be changed)

Recommendations:

• Review Azure Enterprise Applications regularly; remove third-party applications that are not needed for business purposes.

• Do not allow non-privileged accounts to consent for applications.



• Only grant the Global Administrator role to dedicated administrative accounts.

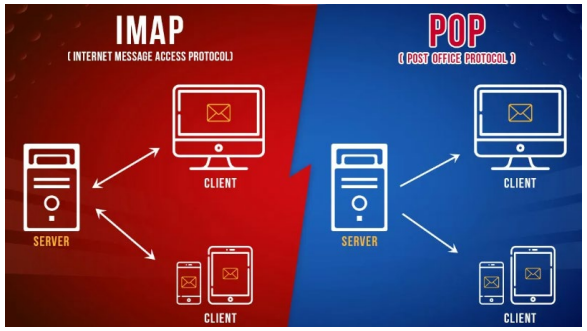
• Administrators should use non-privileged accounts for email and other everyday purposes and have separate named accounts with administrator roles.

• Any Consent to Application UAL event should be reviewed - this event should be uncommon.

• If your organization uses a SIEM to alert on sensitive events, include this event and confirm that all applications are authorized.

Types of Access

- **Mail Client**
- Examples: Outlook, Thunderbird, eM Client.
- Or related IMAP4, POP3, EWS protocols.
- Method which can provide acquisition capabilities in addition to being able to view or access the contents of email messages and their attachments.
- The contents of the account-holder email account could have been downloaded by the actor(s) onto their local device.



- **Web Browser**
- Examples: Edge, Firefox, Chrome, Opera.
- Does not provide the unauthorized actor(s) the ability to download or sync a copy of the impacted user's mailbox.

How to Handle an Email Account with Suspected Unauthorized Access

1. Force a password reset on the impacted user account(s).
   - Ensure that the user is not recycling passwords and creates a strong, complex password.
   - **A password reset should be conducted first**, as this action will eject threat actors from the email account.
2. Terminate all active sessions.
   - Via the Microsoft Azure portal (https://portal.azure.com), revoke all active sessions for the impacted user account(s).
3. Enable and enforce Multifactor Authentication (MFA).
4. If MFA is already enforced, review and verify all registered devices.
5. Review inbox and forwarding rules for any signs of malicious rules.

Common Mistakes

- In Kroll's experience, an immediate reaction to unauthorized access to an email account is to disable the account.
- However, Kroll does not recommend disabling the impacted user account first, as disabling the impacted user account does not terminate all active sessions.
- Active sessions may continue for up to six (6) hours.

Proactive Solutions

Logging

- Not all tenants have Unified Audit Logging enabled.
- Newer tenants have this enabled by default however, not all older tenants do.
- Ensure your tenant has all necessary logging enabled.
- There are a few logs enabled by default most teams don't know to review: Mailbox Audit Log (MAL), Admin Audit Log, Search Terms.
- Some tenants with E5 Licensing UAL logs go back 180 days or a full year.
- If possible, offload M365 logs to an offsite server or SIEM to see more than 90 days.

M365 Logs Kroll Reviews:

1. Unified Audit Log (UAL)
2. Mailbox Audit Log (MAL)
3. Admin Audit Log
4. Azure Sign-Ins
5. Azure Audit Log
6. Message Traces (Inbound\Outbound)
7. Search Terms

- Message Traces, UAL, MAL, Admin Audit Log = 90 days by default.
- Azure Sign-Ins & Azure Audit Log = 1 Month or 7 Days, depending on AAD license level

Kroll Recommendations

- Long and complex password requirements for all accounts.
- Require password changes every 90 days.
- Do not allow password reuse.
- Ensure all users have MFA enabled and enforced.
- Kroll recommends MFA texted code method (Disable push approve\deny & phone call methods).
- Far too many users approve MFA prompts when they are not attempting to login (muscle memory).
- End user awareness training on Phishing and MFA.
- Show them how to carefully examine the email address, what to watch for, spelling errors, unknown sender, urgent requests, update\verify account information.
- Monthly phishing testing, more training for those clicking.

- Have procedures in place to verify payments and purchases **outside of just email communication.**
- May include direct phone calls, however this should only be to a known phone number.
- **Do not rely on the phone numbers included in emails.**
- Add geofencing if possible.
- Restrict logins from Non-US locations like Nigeria, South Africa, Netherlands, Russia.
- Disable SMTP – Abused by spammers.
- Disable POP\IMAP – does now include MFA – however to ensure that threat actors are not able to download a full copy of the victim's mailbox, it is recommended to disable these if they are not needed.
- Internally test to verify all of Microsoft's updates and patches are working correctly for your tenant.

Summary

If in doubt – Report or Ask

All employees – not just IT – play an active role in identifying and stopping cyber threats before they harm your organization!

Questions?

For more information, please contact:

Kroll.com

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

© 2021 Duff & Phelps, LLC. All rights reserved. Kroll is a trade name for Duff & Phelps, LLC and its affiliates.