







*Keeping the pace with
attackers: storie di attacchi
e tendenze di phishing
emergenti*

Davide Canali

Sr Manager, Fraud and Theft Research @ Proofpoint

- 15 years of experience in cyber security
 - 8 years at Proofpoint
 - First as threat researcher
 - Currently leading a global team of researchers
 - Past: Network Threat Analyst at a cybersecurity startup 
- Education
 - Ph.D. in Computer Security from EURECOM (Telecom ParisTech) 
 - Visiting scholar at UCSB SecLab (UC Santa Barbara) 
 - Master in Computer Engineering from Università di Bologna 



Proofpoint Data Coverage

Where does our threat research data come from?

Email as well as Network (via Emerging Threats) are our primary source for data collection and intelligence; we also leverage cloud-focused data collections. Telemetry includes:

- ~3.1 billion email messages/day, 49 billion URLs, 1.9 billion attachments, and more.
- 300k+ unique malware samples per day.
- ~6k network sensors, globally.
- 85% of Fortune 100 are our customers.

Where does our threat research go?

- ~6500 campaigns published to customers in 2023.
- ~70 Differing Actor groups Tracked (including APT).
- Threat types: Malware, Phishing, BEC & Fraud
- 24 *Threat Insight* reports in 2023.
- 26 Episodes of *Discarded* podcast in 2023.
- And beyond!





Attack stories

Uno strano SMS...



Uno strano SMS...

Smishing attack



Hello, Incident Request
INC4259138 was created.
Review : [https://
www.eycrecruitmen
t.org](https://www.eycrecruitment.org) ServiceNow.

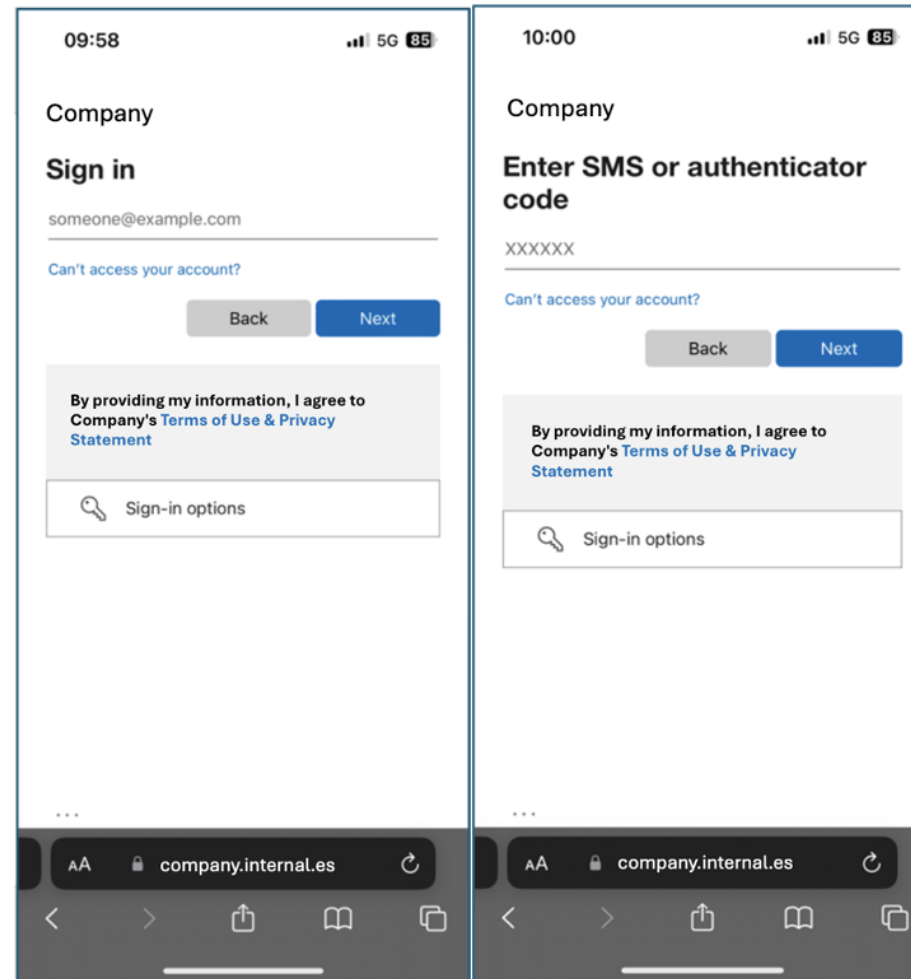


Hello, Incident Request
INC4259138 was created.
Review : [https://
www.renovationsric
hardbernier.com](https://www.renovationsrichardbernier.com) ServiceNow.

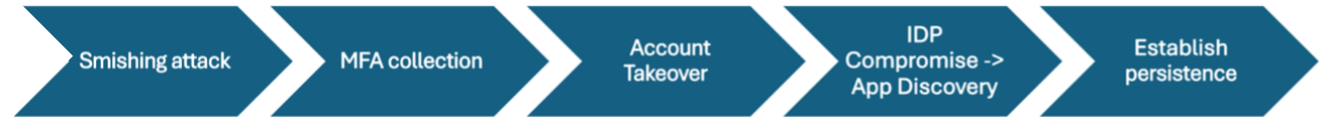
Uno strano SMS...



Portale di login
Microsoft
customizzato



E ora ?



- MFA manipulation
- Enrollment di nuovi dispositivi tramite app Microsoft native (e.g., Intune Enrollment)
- Uso della VPN aziendale a fini malevoli
- Accesso al portale SSO

Impatto



- Enumerazione delle app connesse all'IDP aziendale
- Ricerca di connessioni API da abusare
- Gli attaccanti identificano un'applicazione aziendale utilizzabile per creare carte regalo

Attribution

- Nome interno: TA4901
 - Aka Storm-0539 (Microsoft)
 - Aka Casablanca (AT&T)
- Gruppo probabilmente basato in Marocco
- Attivo e monitorato dal 2018
 - In passato:
 - sim swapping, altri tipi di frode
 - targeting (via email) di operatori telecom
 - Di recente:
 - principalmente attacchi di Smishing
 - furto/creazione di carte regalo
 - Attacchi mirati a poche compagnie dello stesso settore ad intervalli di tempo ravvicinati

Un bonifico
che tarda ad
arrivare...



Identità in gioco

**Azienda internazionale di macchinari
e servizi per la ristorazione**

**Riparatore di macchinari per
ristorazione e settore alberghiero:**

”fornitore.com”



”riparatore.info”

Il ”riparatore” deve pagare una fattura al ”fornitore”. L’attaccante ha già letto la conversazione ed è in possesso dei dettagli della fattura...

Impiegati:

- Alan
- Paola (?)

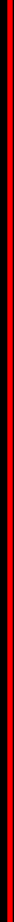
Impiegati:

- Julia <riparatore@riparatore.info>
 - account mail (webmail) compromesso
 - l’attaccante può leggere e inviare mail

fornitore.com



Alan



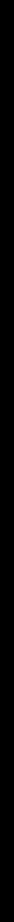
Alan



riparatore.info



Julia



Julia



fornitore.com



Alan



Alan

riparatore.info



Julia



Julia

From: Alan <asdafgdsf@gmail.com>
To: Julia <riparatore@riparatore.info>
Reply-to: "Alan <alan@fornitore.com>" <alan.fornitore@dr.com>
Subject: Re: Contabilità Dicembre

Buongiorno Julia,

se effettui il bonifico oggi, potresti per favore eseguire il pagamento verso il nostro conto secondario?

Non usare le vecchie coordinate bancarie, quel conto è stato chiuso.

Hai le coordinate dell'altro conto?

Grazie, saluti

Alan

fornitore.com



Alan



Alan

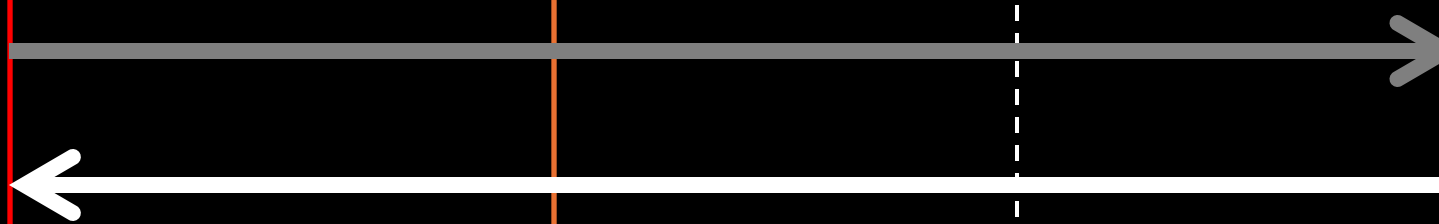
riparatore.info



Julia



Julia



From: Julia <riparatore@riparatore.info>
To: "Alan <alan@fornitore.com>" <alan.fornitore@dr.com>
Subject: Re: Contabilità Dicembre

Buongiorno Alan,

non ho i dettagli di nessun altro conto. Le uniche coordinate che ho sono quelle del conto verso il quale mandiamo sempre i pagamenti.

Indicami quali coordinate bancarie devo inserire.

Un saluto

Julia

fornitore.com



Alan



Alan

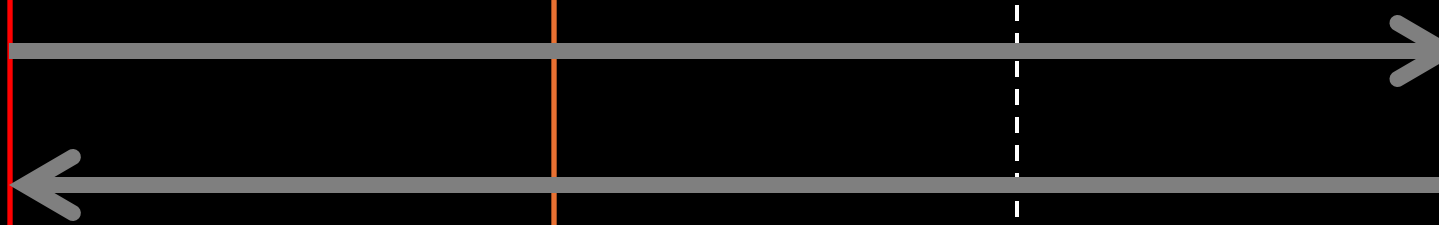
riparatore.info



Julia



Julia



From: Alan <asdafgdsf@gmail.com>
To: Julia <riparatore@riparatore.info>
Cc: "Paola <paola@fornitore.com>" <paola.fornitore@dr.com>
Reply-to: "Alan <alan@fornitore.com>" <alan.fornitore@dr.com>
Subject: Re: Contabilità Dicembre

Julia,

effettua il pagamento alle seguenti coordinate bancarie e mandami la ricevuta entro fine giornata.

IBAN: ES92 1234 5678 4321 8765 1337

Grazie, saluti

Alan



fornitore.com



Alan



Alan

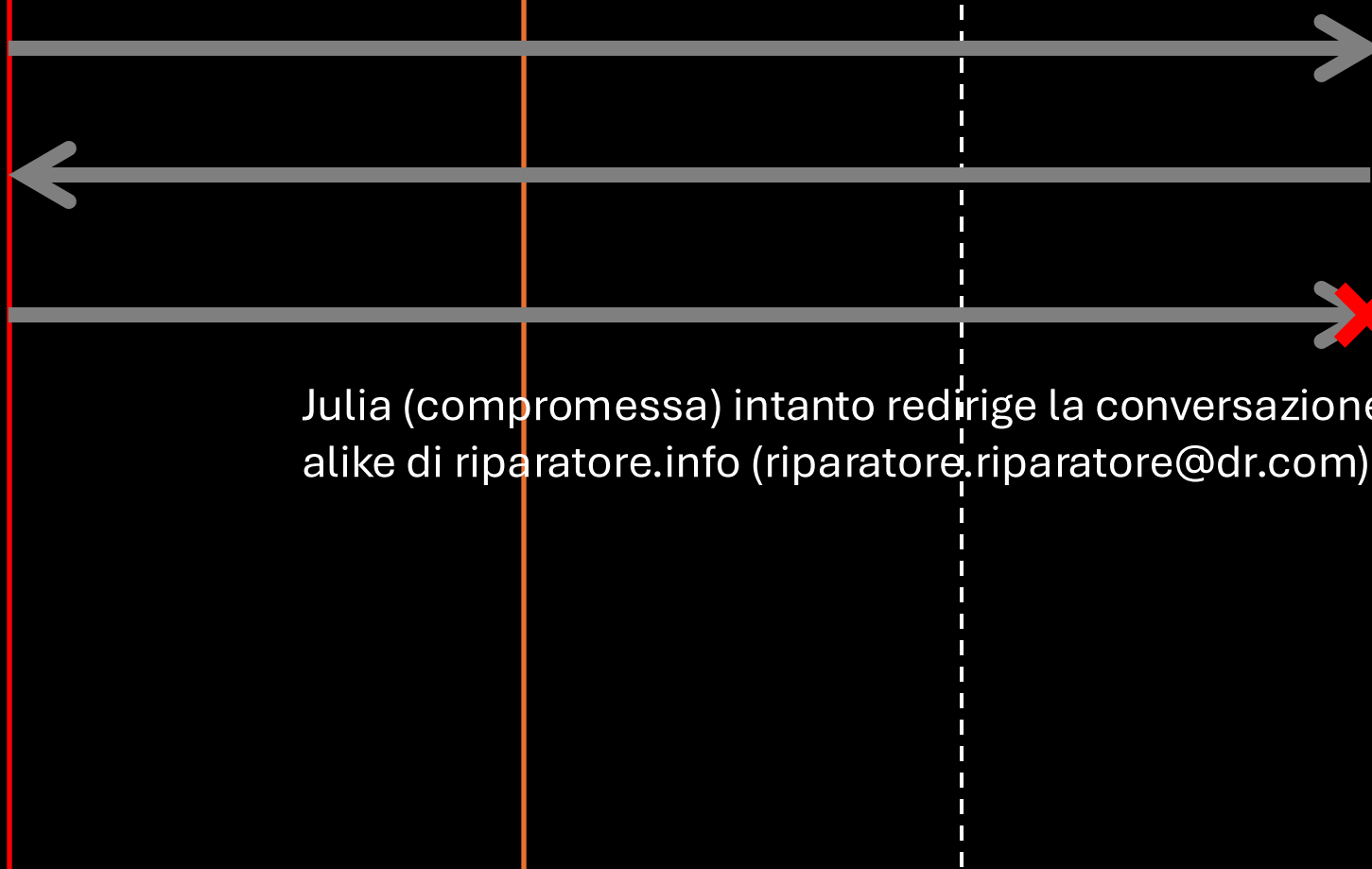
riparatore.info



Julia



Julia



Julia (compromessa) intanto redirige la conversazione del vero Alan verso un look-alike di riparatore.info (riparatore.riparatore@dr.com) sotto il suo controllo...

fornitore.com



Alan



Alan

riparatore.info



Julia



Julia

From: Alan <Alan@fornitore.com>
To: Julia <riparatore.riparatore@dr.com>
Subject: Re: Contabilità Dicembre

Buongiorno Julia,
non abbiamo ricevuto il pagamento, puoi mandarmene la ricevuta?
Grazie, saluti
Alan

...azione del vero Alan verso un look-
(com) sotto il suo controllo...



Ready when you are
Transfer expires in 6 days

Hello, Trust you had a nice day

- Price List.pdf
- Invoice.pdf
- Offer.pdf

Download

Welcome to WeTransfer

- ✓ Simple file-sharing
- ✓ No registration
- ✓ It's free

To continue, please agree to our [Terms of Service](#) and [Cookie Policy](#). We use cookies for functional and analytical purposes and third party cookies for advertising purposes.

I agree

riparatore.info



Julia

info>
[redacted]
[redacted]



Ready when you are
Transfer expires in 6 days

Hello, Trust you had a nice day

- Price List.pdf
- Invoice.pdf
- Offer.pdf

Download

Welcome to WeTransfer

- ✓ Simple
- ✓ No re
- ✓ It's fre

To continue, please agree to our [Terms of Service](#) and [Cookie Policy](#). We use cookies for functional and analytical purposes and third party cookies for advertising purposes.

I agree

Verify E-mail account to start download



Password

☐ Keep me signed in

Download File

[Can't access your account?](#)

Recap sulle tecniche usate

- “Social Engineering”
- Abuso di relazioni esistenti tra fornitore e cliente
- Abuso di brand/servizi noti: WeTransfer
- Impersonificazione & compromissione
 - Display name spoofing + Reply-to manipulation
 - Multi-persona impersonation
 - Uso di un account compromesso



*Le perdite causate da attacchi
BEC nel 2023 hanno superato i
2,9 miliardi di dollari.*

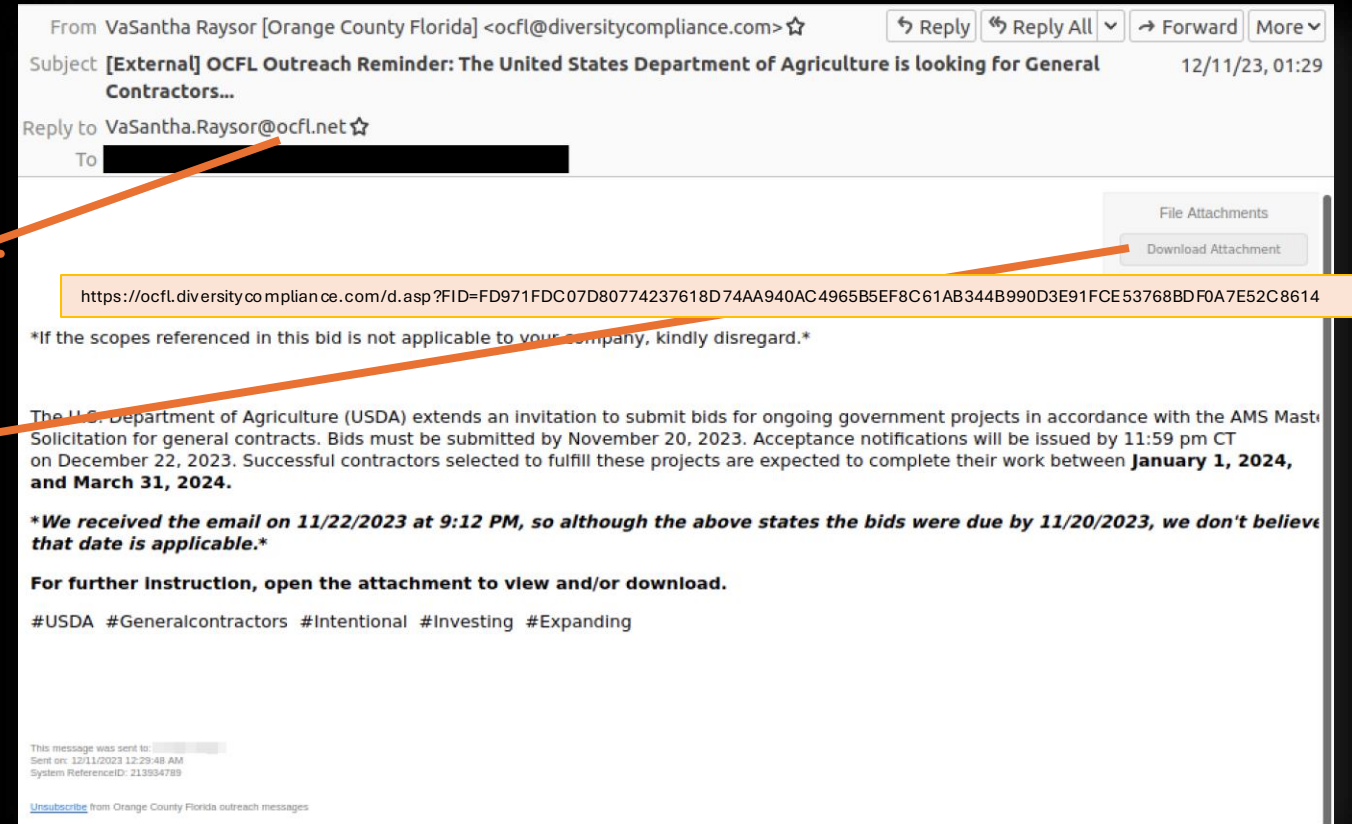
Source: IC3 2023 Internet Crime Report

Gare
d'appalto
pericolose...



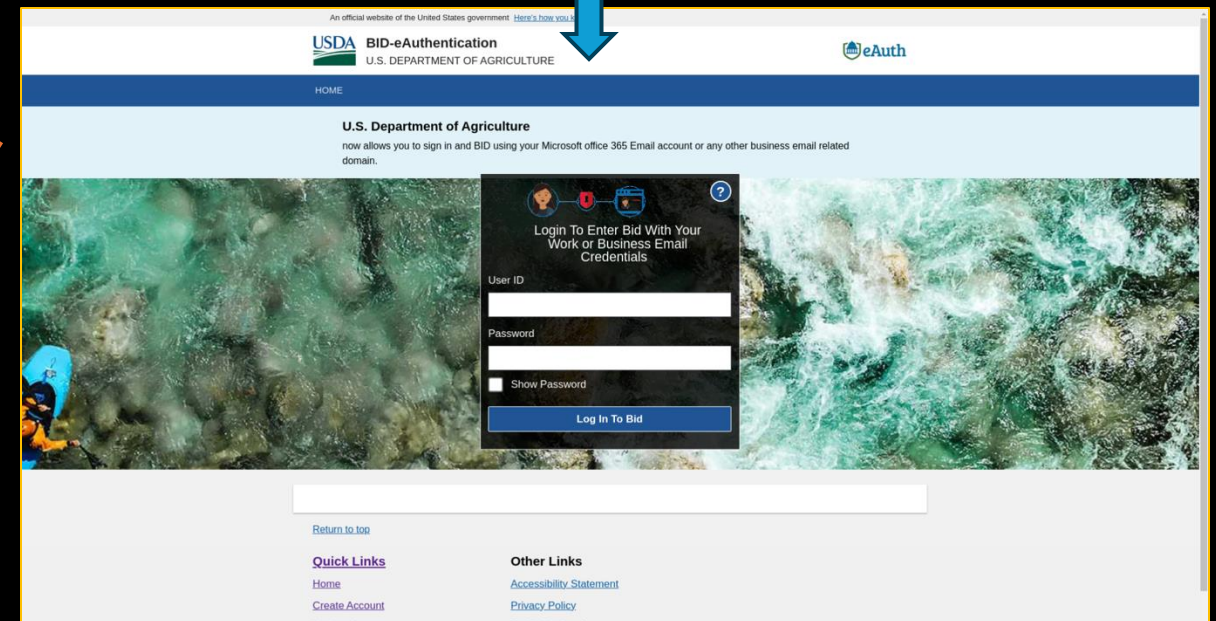
USDA in cerca di costruttori

- Richiesta di partecipare a gare di appalto per il Dipartimento di Agricoltura degli Stati Uniti (USDA)
- Account compromesso su ocfl.net (Orange County Florida)
- Link a un file sul portale di diversità di OCFL
 - Attaccante ha controllo del conto di OCFL su diversitycompliance.com



USDA in cerca di costruttori

- Il link nella mail invia a un PDF su docusharesync.com (actor-controlled) ←
- Link e QR code nel PDF inviano a una pagina di phishing ←
 - Copia del vero portale di autenticazione dell'USDA



TA4903 - Profilo

- TA4903 è un gruppo di attaccanti avanzato e specializzato in due obiettivi distinti:
 - Credential phishing
 - Business email compromise (BEC)
- Operativo almeno dal 2021
- Impersonificazione di vari enti governativi degli Stati Uniti al fine rubare credenziali aziendali
- Obiettivo finale: furto di denaro (tramite redirectione di pagamenti)

- Targeting:
 - da centinaia di messaggi a decine di migliaia di messaggi per campaign
 - Messaggi in genere destinati a
 - Settori e imprese che lavorano col governo Statunitense
 - Più raramente, targeting globale
- Infrastruttura:
 - Nomi di dominio e indirizzi email appositamente registrati (lookalikes)
 - Infrastruttura compromessa

TA4903 / 2021-2022

- Campagne di phishing con spoofing di
 - U.S. Department of Labor
 - U.S. Departments of Housing and Urban Development
 - U.S. Department of Transportation
 - U.S. Department of Commerce
- attacchi BEC mirati con informazioni e accesso ottenuti dagli account compromessi

The United States Department of Transportation in accordance with directives from the U.S Government is seeking bid proposals for ongoing commercial projects. The bids solicited under this Invite will not be publicly opened nor read. Bids should not be double sided.

Kindly, follow the instructions:

- Click on the button below to access our website to bid.
- This registration is maintained by you, and you may update your information at any time after registration.
- Our tracing system will generate a bid identification number BIN for reference to the project documents and bid submitting. You must not submit a bid twice as this may lead to disqualification.

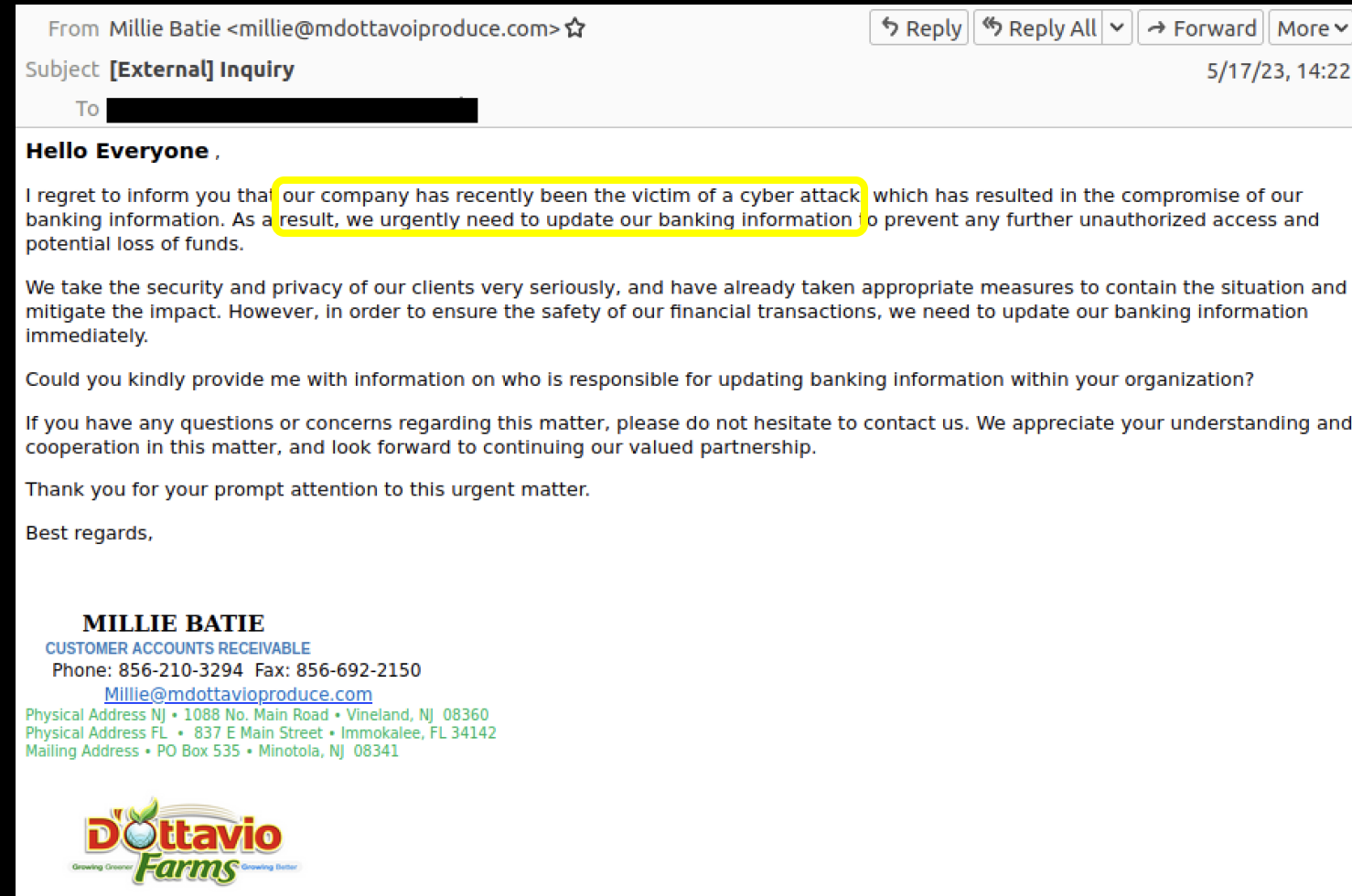


Notice: The above "BID" button/link to the bid website might not be clickable for some email providers, bidders are advised to download this pdf before clicking the "BID" button above

The information below is a checklist to assist you in preparing a responsive bid. Please note that these instructions may not contain all applicable requirements, and careful reading of the Invitation for Bid is critical. It is not necessary to return this page with your bid response.

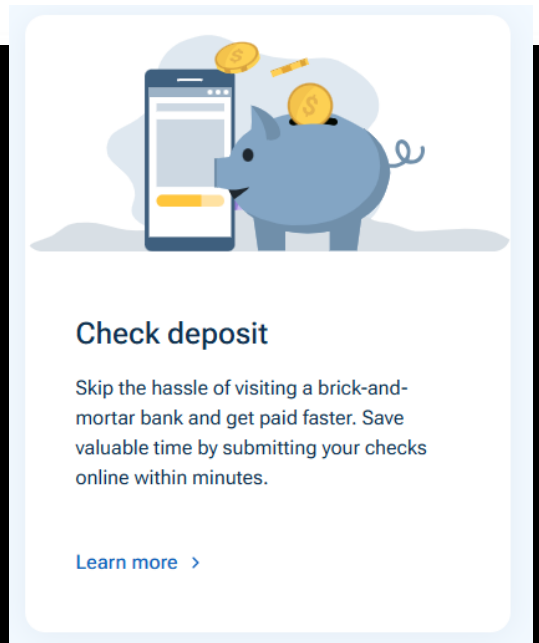
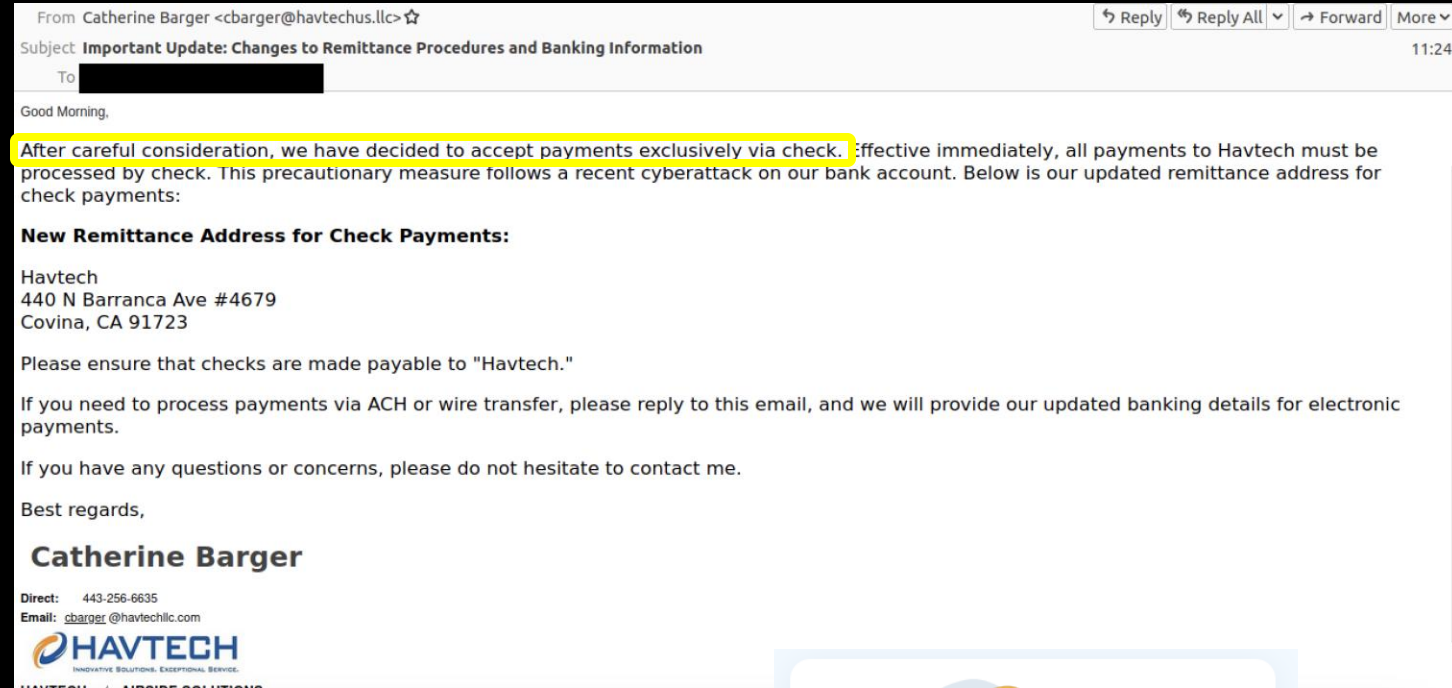
TA4903 / 2023

- aumento delle campagne di phishing
- temi diversi (non più esclusivamente governativi)
 - Spoofing di PMI in settori quali edilizia, produzione, energia, finanza.
- utilizzo di EvilProxy (PhaaS)
- Aumento delle attività di BEC
 - campagne con temi quali “cyber attack”



TA4903 / 2024

- Temi di phishing
 - enti governativi
 - servizi di condivisione documenti
 - “Proofpoint secure message”
- BEC
 - Da fine Aprile 2024, le vittime sono invitate a pagare con assegni!

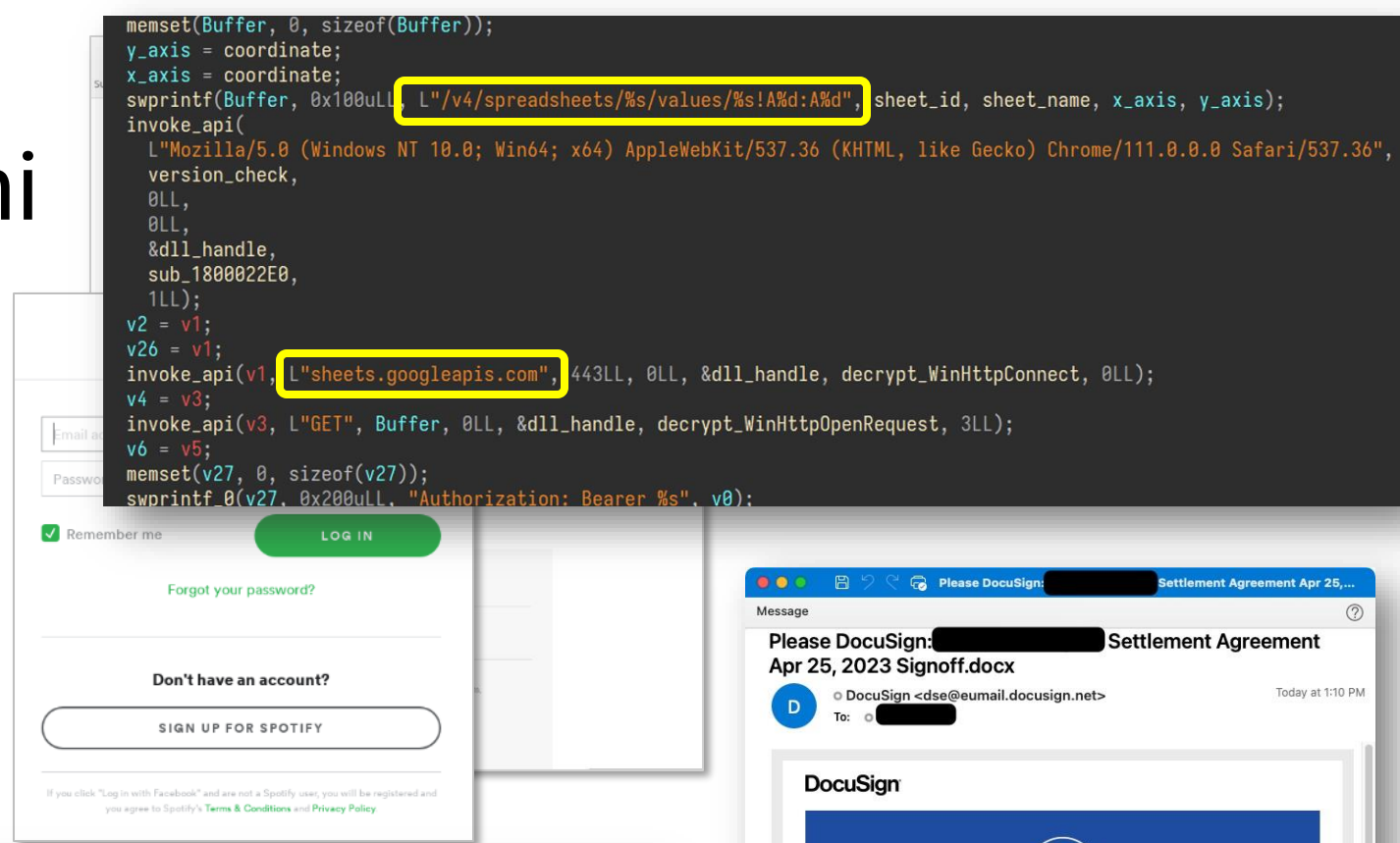




Tendenze globali ed emergenti

Abuso di servizi legittimi

- Messaggi “esca” che fanno uso di marchi e servizi noti:
 - Di cui la vittima si fida
 - Che la vittima è abituata ad usare
- Consolidamento dei servizi “Cloud” verso pochi leader di mercato*
 - Facile indovinare chi usa un certo servizio



Phishing: minaccia globale #1

- ... per volume di email
- ... e preoccupazione #1 per gli addetti ai lavori

“what’s your top cyber security concern this year?”



Source: PROTECT 2024 London

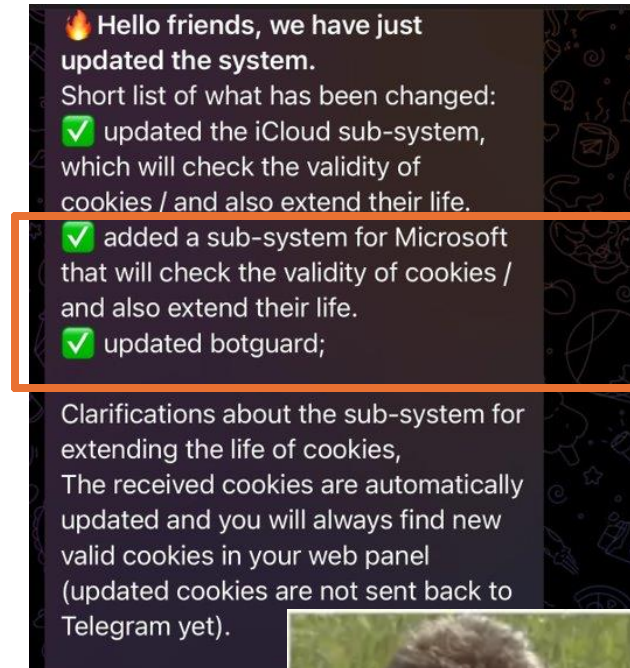


*L'89% dei professionisti IT
crede che l'MFA sia la
protezione perfetta contro la
compromissione di account*

Source: 2024 State of the Phish

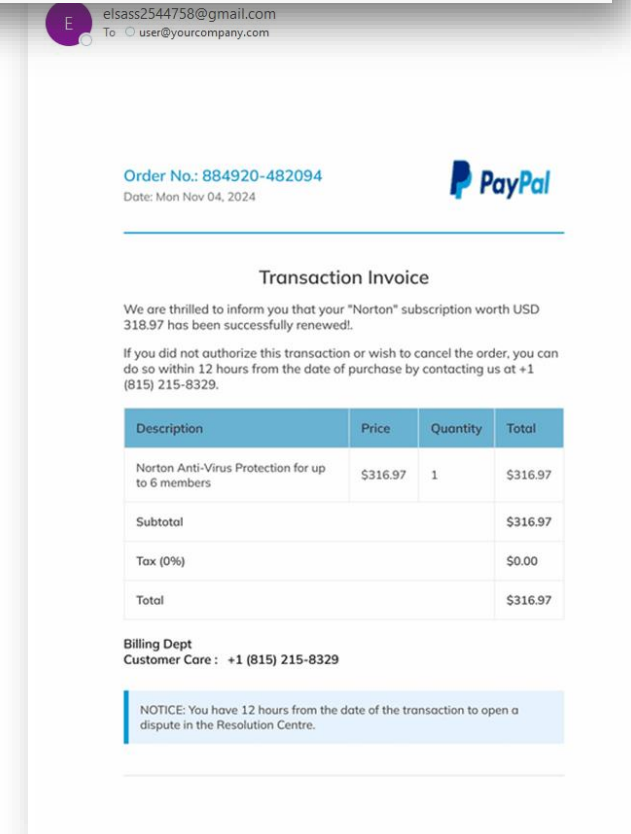
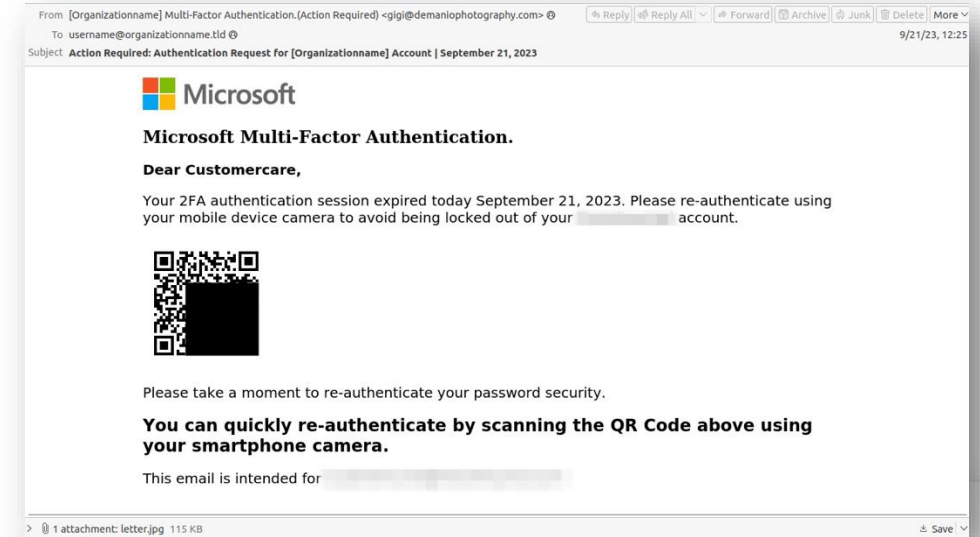
MFA-capable phishing is the new norm

- Boom dell'AitM (Adversary-in-the-Middle)
- Offerte open source e a pagamento (criminali); diverse piattaforme PhaaS
 - Barriere all'ingresso per il "phishing avanzato" considerevolmente abbassate
 - Permettono di bypassare protezioni MFA
 - ...e stabilire persistenza (resistenza a password-reset)
- Uso di servizi cloud legittimi, protezioni anti-bot rendono difficile l'analisi



Attacchi multi canale

- Sicurezza tradizionalmente basata su protezione del posto di lavoro e della rete aziendale
- Shift verso il cloud e il mobile working
 - Gli impiegati accedono da ovunque, anche via smartphone
 - Smartphone molto meno protetti dei posti di lavoro aziendali
 - Dispositivi personali, non-managed
- Gli attaccanti spingono le vittime fuori dal “perimetro di sicurezza” tradizionale
 - Mail → Telefonate (TOAD)
 - SMS (Smishing)
 - QR codes → phishing



Riassumendo

- Il paesaggio delle minacce odierno è al 99%+ basato su Social Engineering
- L'attaccante deve convincere la vittima a eseguire una o più azioni
 - Creare uno scenario “credibile”, “familiare” o “fidato” è essenziale
 - Interlocutori conosciuti o fidati
 - Uso di servizi legittimi
 - Uso di temi e brand conosciuti
- Il phishing è di nuovo un problema critico



Grazie