sysnet TELEMATICA

NEL FUTURO DELLE TELECOMUNICAZIONI

PROTEZIONE E-MAIL TOTALE - MINACCE E SOLUZIONI

TECNOLOGIE PER LE **TELECOMUNICAZIONI** E IL **NETWORKING**

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

93% of phishing emails are now ransomware

FBI: $2.3 Billion Lost to CEO Email Scams

Advocate Health to pay largest HIPAA settlement

FBI Report: Ransomware and Phishing Scams Increasing

Of course, the number one cause of data loss, according to the FBI report, continues to be social engineering and email compromises. The reported losses associated with business email compromises in 2015 was $246,226,016.

Netflix Email Scam Targets Millions Of Subscribers

Russian Hackers Faked Gmail Password Form To Invade DNC Email System

New online financial scam costs victims $130K per attack

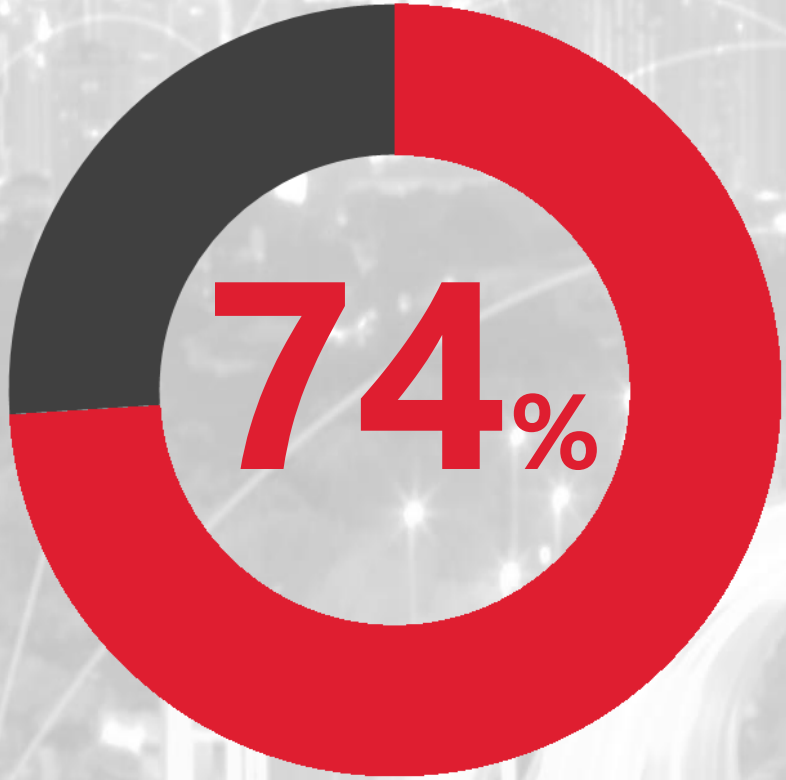
- "Business-email compromise" scams target financial services firms and their clients through phishing.
- A successful attack nets an average $130,000 loss per scheme.
- Between 2013 and 2016, these schemes have resulted in a total dollar loss of $5.2 billion.

North Korean hackers target US electric companies with malicious email attack

Attackers Exploit 17-Year-Old Bug to Deliver Malware via Cobalt Strike

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Il problema: la maggior parte degli attacchi è originata da e-mail



- *"Circa **tre quarti di tutti gli attacchi** partono da un allegato o un link."*

2017 Threat Landscape Survey: Users on the Front Line - SANS Analyst Program

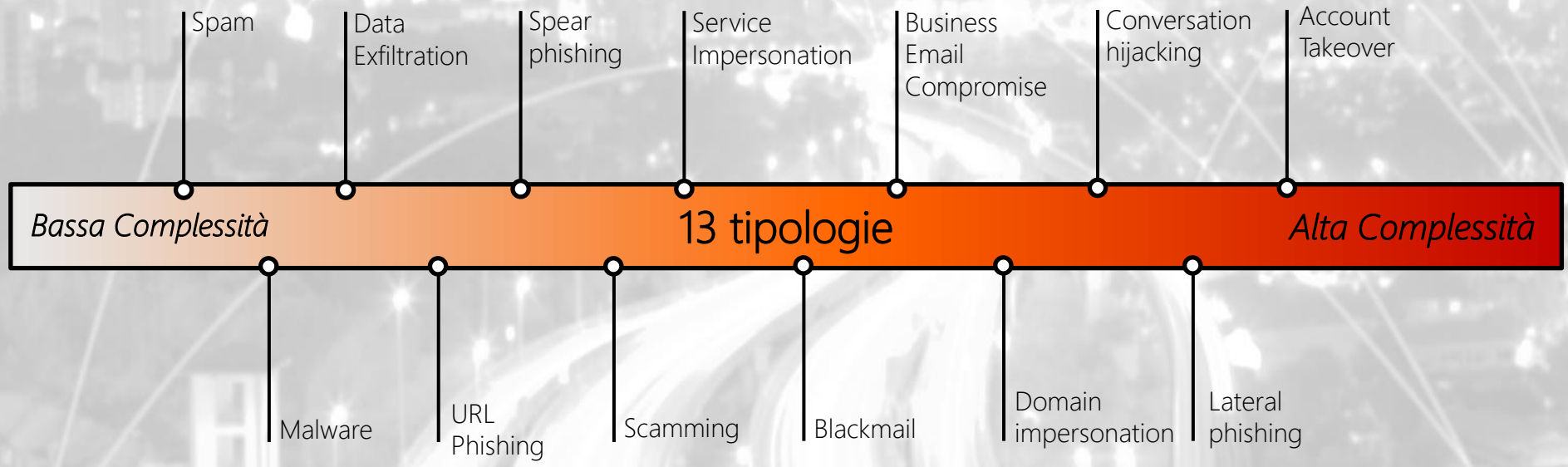
Classificazione minacce

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

13 tipologie di attacco / 2 tipologie di difesa

	Gateway E-mail tradizionale		Sicurezza E-mail con API basate su AI (Intelligenza Artificiale)	
Spam		Il controllo in linea riconosce e blocca lo spam prima che raggiunga le caselle.		Essendo attacchi su vasta scala l'approccio API non è efficiente.
Malware		Il controllo in linea riconosce e blocca lo spam prima che raggiunga le caselle.		Essendo attacchi su vasta scala l'approccio API non è efficiente.
Data Exfiltration		I gateway sono progettati per impedire l'inline exfiltration.		Le API non possono bloccare questa minaccia.
URL Phishing		I gateway hanno a disposizione informazioni storiche limitate e visibilità limitata, bloccano solo attacchi molto popolari.		Le API conoscono lo storico degli URL utilizzati e possono bloccare questa minaccia in modo efficiente.
Lateral Phishing		I Gateway non possono bloccare attacchi interni.		Le API conoscono lo storico delle comunicazioni e possono bloccare questa minaccia in modo efficiente.
Spear Phishing		I Gateway non possono individuare comunicazioni atipiche non avendo a dispositizioni uno storico comunicazioni.		Le API conoscono lo storico delle comunicazioni e possono bloccare questa minaccia in modo efficiente.
Service Impersonation		I Gateway non possono individuare anormalità nei servizi poichè non possiedono uno storico dei servizi attivi.		Le API conoscono lo storico dei servizi in uso e possono bloccare questa minaccia in modo efficiente.
Domain Impersonation		I Gateway non possono individuare una sostituzione di dominio poichè non possiedono uno storico delle caratteristiche dei domini.		Le API conoscono lo storico dei domini con le relative caratteristiche e possono bloccare questa minaccia in modo efficiente.
Business Email Compromise		I Gateway non possono bloccare attacchi interni.		Le API conoscono lo storico delle comunicazioni e possono bloccare questa minaccia in modo efficiente.
Scamming		I Gateway conoscono e bloccano solo attacchi molto popolari.		Le API conoscono lo storico dei domini con le relative caratteristiche e possono bloccare questa minaccia in modo efficiente.
Blackmail		I Gateway conoscono e bloccano solo attacchi molto popolari.		Le API gestiscono queste minacce con la maggiore efficacia rispetto ai gateway.
Account Takeover		I Gateway non hanno visibilità sugli account quindi non possono identificare operazioni fraudolente.		Le API hanno visibiità su policy e attività degli account e possono intervenire con efficacia in caso di comportamento sospetto.
Conversation Hijacking		I Gateway non possono identificare questa minaccia poichè non hanno uno storico delle conversazioni.		Le API conoscono lo storico delle comunicazioni e possono bloccare questa minaccia in modo efficiente.

Aumento della complessità degli attacchi

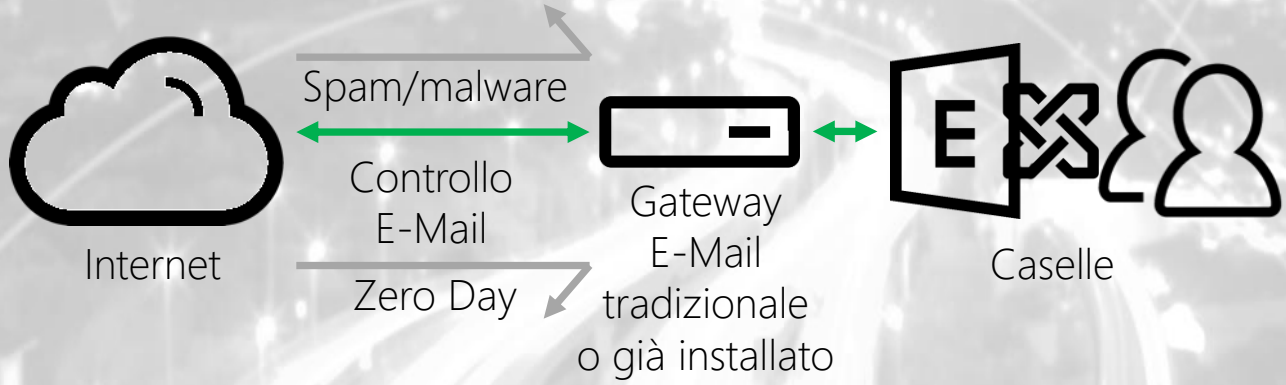


Cos'è un Gateway di Sicurezza E-Mail tradizionale?

- È un sistema di sicurezza **infrapposto fra la rete interna e la rete esterna**
- Filtra **spam e malware**
- Lavora basandosi su **schemi di attacco noti**

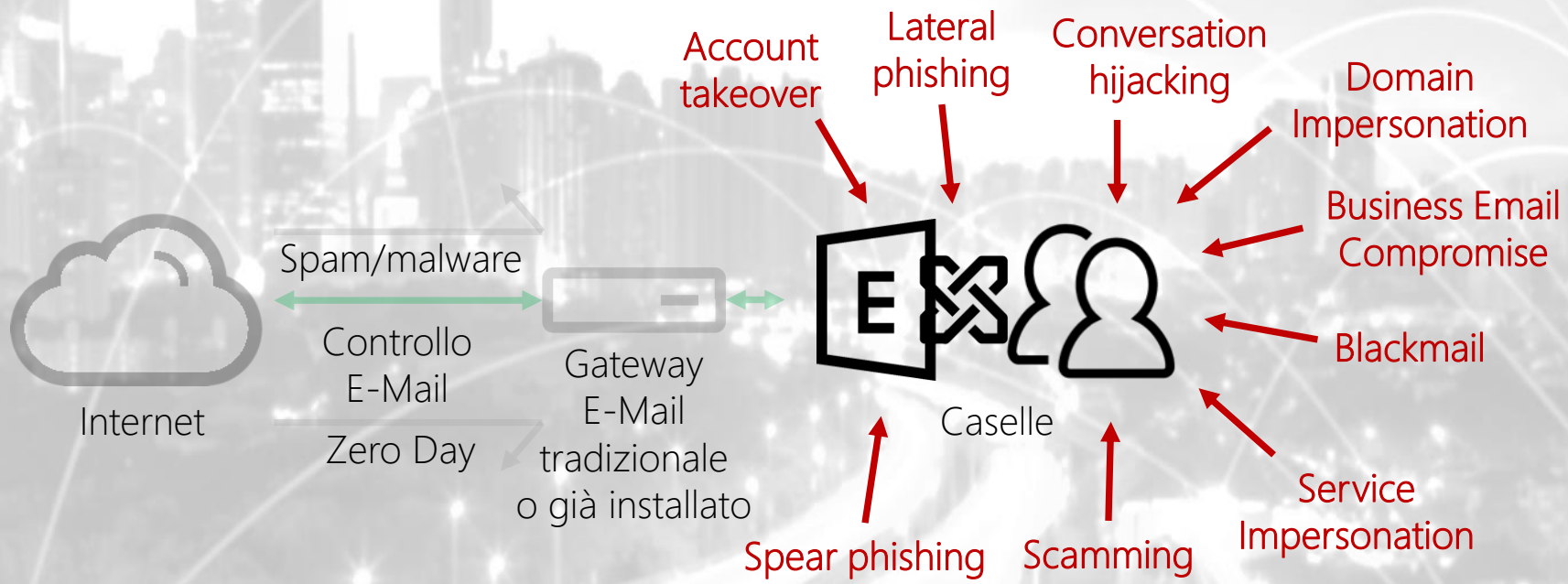
sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Protezione Gateway E-mail tradizionale



sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Sicurezza E-mail con API basate su IA



La **protezione E-mail con API basate su IA (Intelligenza Artificiale)**, avendo accesso a molti più dati inerenti l'infrastruttura e gli utenti rispetto a una protezione tradizionale, **è in grado di bloccare anche le tipologie di attacco più sofisticate**.

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Contenuti malevoli

Spam, Malware, Data Exfiltration

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Cosa blocca la Protezione Gateway standard?

Spam

Gateway

Blocca lo spam prima che raggiunga le caselle

Malware

Gateway

Riconosce i malware noti e li blocca (sandboxing)

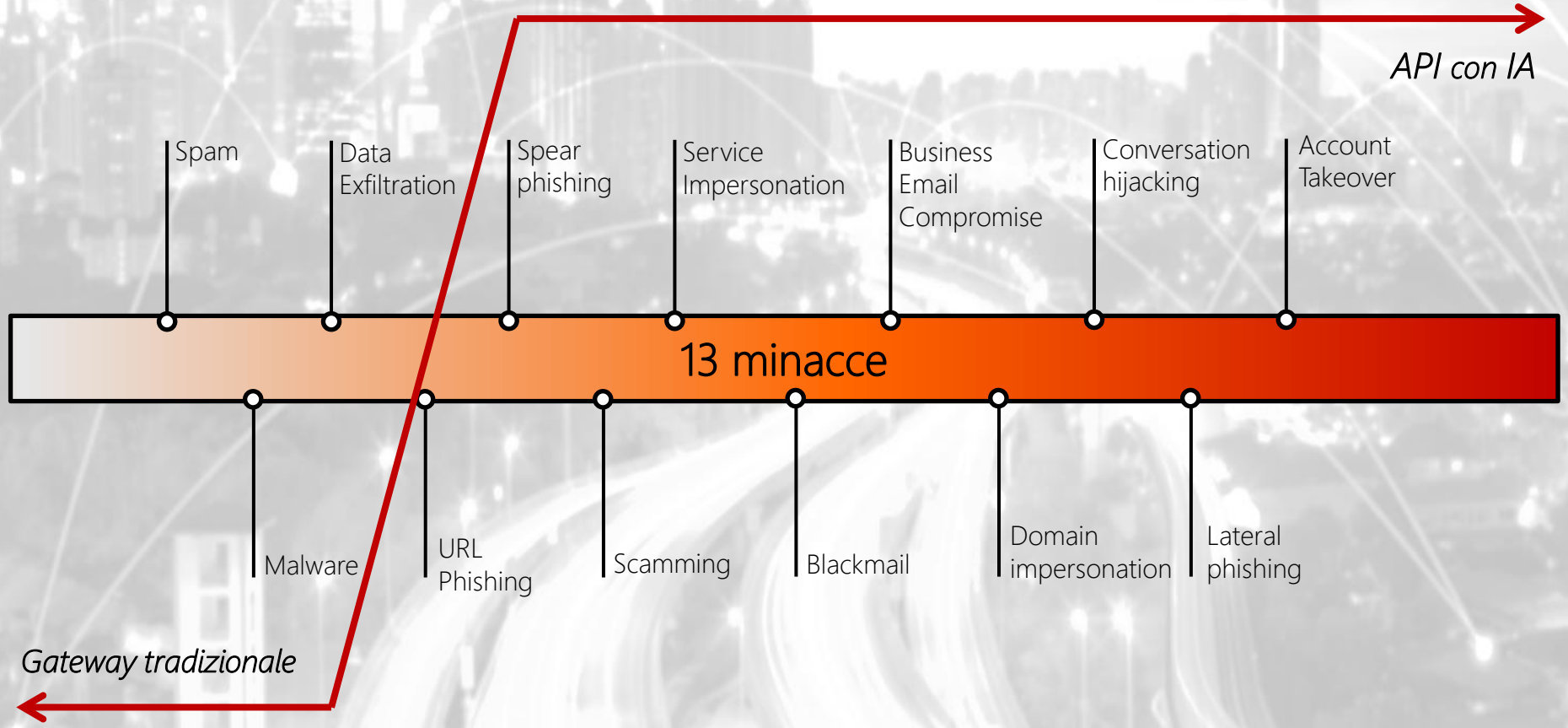
Furto informazioni

Gateway

Crittografa I dati sensibili

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Come bloccare le minacce più recenti?



sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Azioni malevole

Phishing & Impersonificazione

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

BEC (Business E-mail Compromise)
E-mail fraudolente

PASSO 1

Identificazione **bersaglio**

PASSO 2

Guadagno **fiducia**

PASSO 3

Invio **richiesta**

PASSO 4

Pagamento

BEC (Business E-mail Compromise)
E-mail fraudolente

To: Daniel Diamond <daniel_diamond@acme.org>
From: John McDonald <ceo.mail@acrne.net>
Reply to: John McDonald <ceo.mail@acrne.net>
Date: Dec 03, 2018

Subject: Wire Transfer Request

Hi Daniel,

Are you in the office today? I need you to process a wire transfer for me. Get back to me as soon as you get this.

Regards,
John

Sent from my iPad.

Simulazione invio da mittente noto

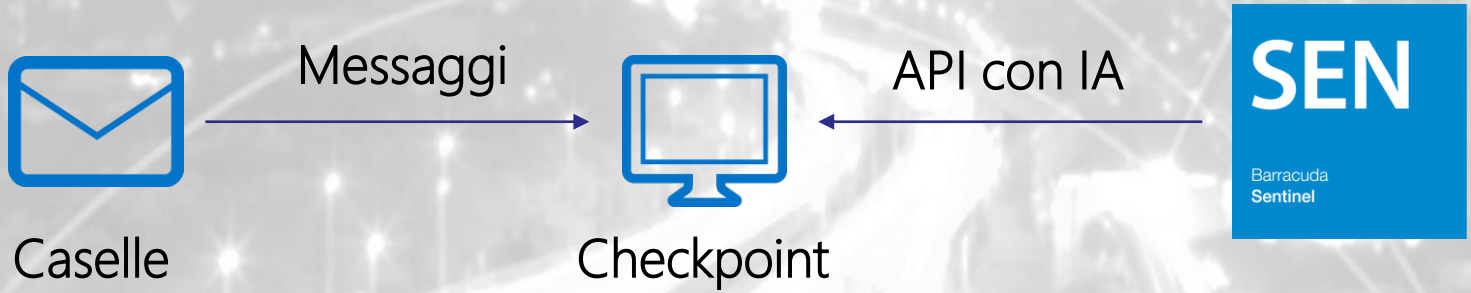
Urgenza

Autorità riconosciuta

(direttore, responsabile, ecc.)

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Cosa può fare una difesa basata su API con IA (Intelligenza Artificiale)?



Accesso a molteplici informazioni

Classificazione secondo parametri multipli

Perchè le API con IA Barracuda sono superiori?

L'IA (Intelligenza Artificiale) rileva il comportamento anomalo basandosi su molte informazioni ed assume un comportamento dinamico.

Sarebbe impossibile ottenere un risultato simile con una protezione tradizionale, occorrerebbe un infinito numero di regole statiche.

Le API con IA offrono protezione dalle più avanzate minacce.

Service Impersonation

From Amazon <support@amazon.com>
Subject **Verifica i dettagli del tuo account**

Impersonificazione mittente noto, ad esempio *support@amazon.it*

amazon

ALLARME DI SICUREZZA

Condizione allarmante

Caro cliente,

Abbiamo bisogno del tuo aiuto per risolvere un problema con il tuo account. Per proteggere le tue informazioni da abusi, l'accesso al tuo account rimarrà limitato fino alla risoluzione del problema. Comprendiamo che potrebbe essere frustrante non avere pieno accesso al tuo account Amazon. Pertanto abbiamo bisogno della tua collaborazione affinché possiamo riportare il tuo account alla normalità il più rapidamente possibile.

Conferma Il Tuo Account

Link fraudolento a un sito contraffatto, spesso clone dell'originale ma con **URL differente**, ad esempio *http://www.amazom.com*

Furto di account

Furto di credenziali mediante phishing o altre vulnerabilità

Furto di informazioni e di altri account

Infiltrazione → Ricognizione → Ottenimento credenziali → Monetizzazione

Ottenuto l'accesso a un qualsiasi account è facile attaccare dall'interno altri account o utenti, utilizzando malware o richieste fraudolente **percepiti dal destinatario come sicure, poichè provenienti da un collega o da un superiore**.

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Conversation hijacking rilevata da IA

Giorno 1

Il fornitore invia una fattura

Giorno 3

La fattura viene saldata

Giorno 32

Il fornitore invia una nuova fattura

Giorno 33

Comunicazione fraudolenta di cambio coordinate bancarie per rubare il pagamento

Un fornitore abituale manda mensilmente le sue fatture che vengono regolarmente saldate secondo le istruzioni ricevute.
L'hacker, rilevando l'invio di una nuova fattura, **si sostituisce alla persona nota** del fornitore **per dare istruzioni di pagamento fraudolente**.

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

La soluzione Barracuda con API basate su IA protegge da tutte le 13 tipologie di minaccia

PL
Barracuda
PhishLine

SEN
Barracuda
Sentinel

ESS
Barracuda
Essentials

Tipo minaccia	Barracuda
Spam	Essentials
Malware	Essentials
URL Phishing	Sentinel
Lateral Phishing	Sentinel
Spear Phishing	Sentinel
Service Impersonation	Sentinel
Domain Impersonation	Sentinel
Business Email Compromise	Sentinel
Scamming	Sentinel
Data Exfiltration	Essentials
Blackmail	Sentinel
Account Takeover	Sentinel
Conversation Hijacking	Sentinel

FIR

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Barracuda Total E-mail Protection

PL Barracuda **PhishLine**

SEN Barracuda **Sentinel**

ESS Barracuda **Essentials**

Consapevolezza e training

Difesa avanzata caselle e account

Cloud to Cloud Service

Cloud Archiving Service

Difesa Gateway tradizionale

FIR

Forensics and Incident Response

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Automate incident response

FIR

IDENTIFICAZIONE

Segnalazione dallo staff

Identificazione Forensics & Insights

INVESTIGAZIONE

Ricerca altri destinatari

Creazione incident

Ricerca utenti attaccati

REAZIONE

Rimozione e-mail fraudolente e invio avvisi agli utenti

Protezione da attacchi futuri

2 – 11 min

sysnet TELEMATICA
NEL FUTURO DELLE TELECOMUNICAZIONI

Scansione di prova gratuita

PL
Barracuda
PhishLine

SEN
Barracuda
Sentinel

ESS
Barracuda
Essentials

Contatta sysnet per richiedere una **scansione di prova gratuita** e non invasiva delle tue caselle o per attivare una soluzione, su misura per le tue esigenze, in **prova gratuita**.

Potrai decidere se **acquistarla o restituirla** senza alcun impegno.

sysnet TELEMATICA

NEL FUTURO DELLE TELECOMUNICAZIONI

GRAZIE

SYSNET TELEMATICA SRL

Via Berbera, 49
20162 Milano, Italia
Tel. +39 02.64.73.021
www.sysnettelematica.it
E-mail: sales@sysnettelematica.it

TELECOMUNICAZIONI E NETWORKING

NETWORKING INDUSTRIALE

SMART IIOT E SOLUZIONI CUSTOM

SICUREZZA INFORMATICA

© Sysnet Telematica Srl 2020 -Tutti i diritti riservati