Adaptive Trust Engine: Il concetto di fiducia applicato alla posta elettronica

Rodolfo Saccani, Security R&D Manager, Libraesva

11 novembre 2020, ore 15:00- 15:45 - StreamingEdition

#securitysummit #streamingedition

Rodolfo Saccani

SECURITY R&D MANAGER

Clusit SECURITY SUMMIT ASTREA

Streaming Edition

10-11-12 novembre 2020

/LIBRAESVA

LA FIDUCIA

LE RELAZIONI UMANE SONO BASATE SUL CONCETTO DI FIDUCIA.

LA MEDIAZIONE DELLA COMUNICAZIONE ELETTRONICA, IN PARTICOLARE DELL'EMAIL, FACILITA L'ABUSO DELLA FIDUCIA

VEDIAMO COME SUPERARE QUESTA LIMITAZIONE CON UN ADAPTIVE TRUST ENGINE

LO SCENARIO ATTUALE

L'EMAIL SECURITY È UN SETTORE IN CONTINUA EVOLUZIONE.

FACCIAMO UNA PANORAMICA SULLE SFIDE CHE CI VEDONO IMPEGNATI OGGI.

Clusit SECURITY SUMMIT ASTREA
Streaming Edition
10-11-12 novembre 2020

/LIBRAESVA

I SEGNALI

I SEGNALI "TRADIZIONALI" USATI PER DISTINGUERE MAIL LEGITTIME DA MAIL NON LEGITTIME VANNO SVANENDO.

IL TRAFFICO MALEVOLO OGGI È:

- **TECNICAMENTE INDISTINGUIBILE**
- **FORMALMENTE CORRETTO**
- **REPUTAZIONE NEUTRA O BUONA**
- **SEMANTICA COMUNE**

Clusit SECURITY SUMMIT ASTREA
Streaming Edition
10-11-12 novembre 2020
/LIBRAESVA

ACCOUNT COMPROMESSI

LE BOTNET GENERANO LA MAGGIOR PARTE DEL TRAFFICO.

C&C FORNISCE CREDENZIALI DI ACCOUNT LEGITTIMI.

ACCOUNT LEGITTIMI ABUSATI PER INVIARE MALWARE E PHISHING.

LE CREDENZIALI DERIVANO DA:
DATA BREACHES, CAMPAGNE DI PHISHING, ATTACCHI A FORZA BRUTA, SNIFFING DA DISPOSITIVI IOT COMPROMESSI, MERCATO NERO

TECNICAMENTE QUESTO TRAFFICO È INDISTINGUIBILE DA QUELLO LEGITTIMO

DOMINI AD-HOC USA-E-GETTA

DOMINI ACQUISTATI PER QUESTO SCOPO.

- CON UNA STORIA (SCADUTI O LASCIATI INVECCHIARE)
- DKIM, SPF, DMARC .. I PARAMETRI TECNICI SONO CORRETTI
- "PULITI" DAL PUNTO DI VISTA DELLA REPUTAZIONE

MIGLIAIA DI DOMINI UTILIZZATI PER QUESTO SCOPO CON NOMI CHE SPESSO RICHIAMANO BRAND LEGITTIMI.

I CONTROLLI TECNICI DI TRASPORTO SONO TUTTI OK, SPESSO ANCHE PIÙ DEL TRAFFICO LEGITTIMO MEDIO.

PHISHING E MALWARE

IL PHISHING USA LA STESSA SEMANTICA DEI MESSAGGI LEGITTIMI.

TRUFFA DEL CEO, IMPERSONIFICAZIONE DI PARTNER COMMERCIALI

L'ANALISI SEMANTICA NON AIUTA QUANDO LA SEMANTICA DEL MESSAGGIO RICALCA QUELLA DI MESSAGGI LEGITTIMI

L'APPROCCIO PATTERN/SIGNATURE NON FUNZIONA PIÙ CON IL MALWARE POLIMORFICO

/LIBRAESVA

IL RISULTATO

IL RISUTATO FINALE È CHE ABBIAMO SEMPRE MENO SEGNALI PER DISCRIMINARE TRAFFICO LEGITTIMO DA TRAFFICO NON LEGITTIMO.

L'ANALISI DEI PARAMETRI TECNICI DA SOLA NON BASTA.

L'ANALISI SEMANTICA DA SOLA NON BASTA.

ANCHE LA COMBINAZIONE DELLE DUE SEMPRE PIÙ SPESSO NON BASTA.

/LIBRAESVA

ANALISI

QUESTE PROBLEMATICHE DI CUI ABBIAMO PARLATO RIGUARDANO L'INTERO MERCATO DELLA EMAIL SECURITY.

COME SI È MOSSO IL MERCATO PER GESTIRE QUESTI PROBLEMI?

/LIBRAESVA

ML & AI

"MACHINE LEARNING" E "ARTIFICIAL INTELLIGENCE" SONO DIVENTATE BUZZWORD DI MARKETING.

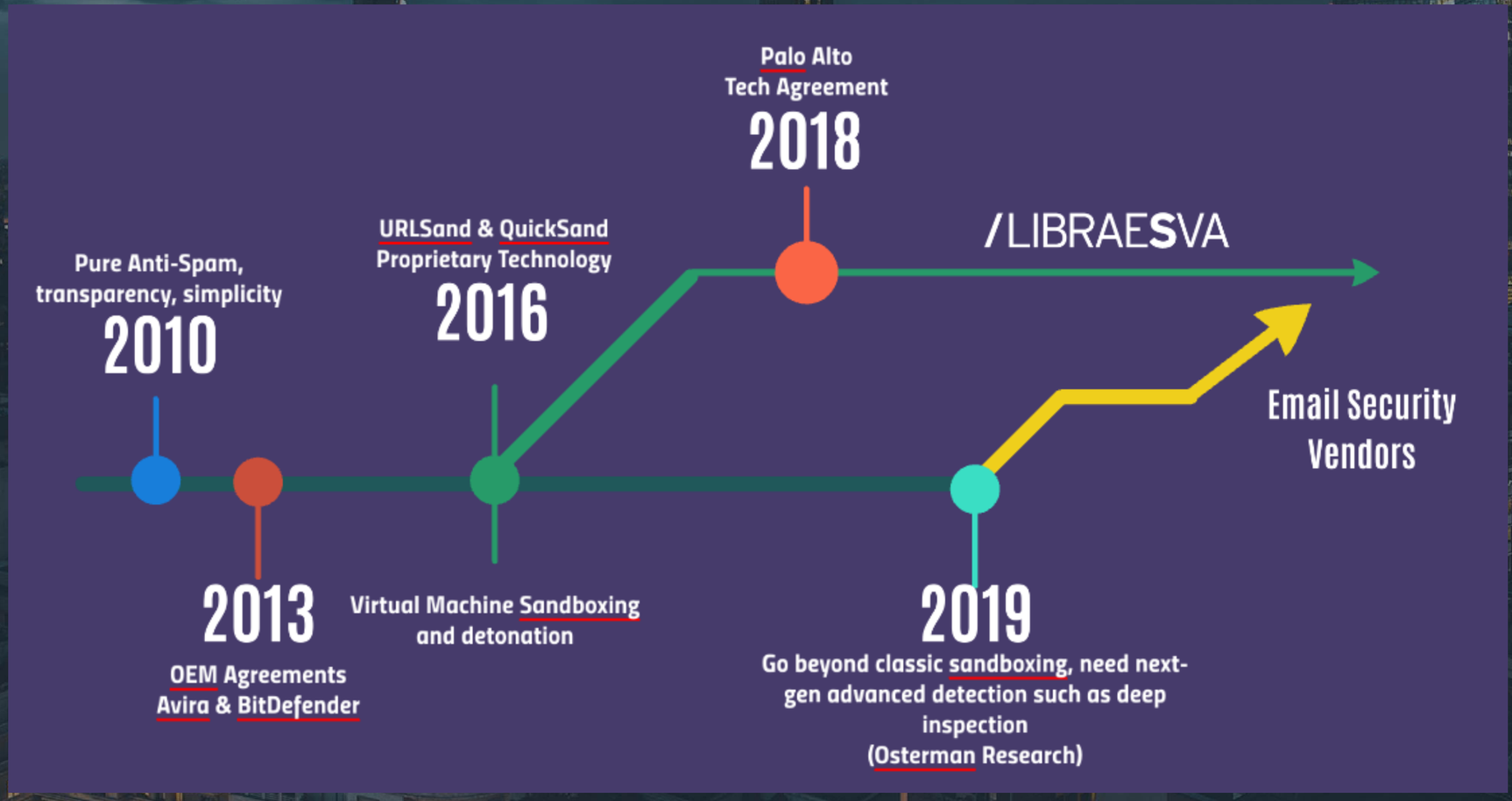
IN REALTÀ SONO STRUMENTI CHE UTILIZZIAMO DAL 1996.

NON SONO STRUMENTI NUOVI MA SONO STATI OGGETTO DI MOLTE MIGLIORIE IN QUESTO PERCORSO ALLA RICERCA DI NUOVI SEGNALI DA SOSTITUIRE A QUELLI CHE ANDAVANO PERSI.

/LIBRAESVA

TIMELINE

L'APPROCCIO PRAGMATICO DI LIBRAESVA



/LIBRAESVA

ADAPTIVE TRUST ENGINE

"LEVERAGING KNOWLEDGE"

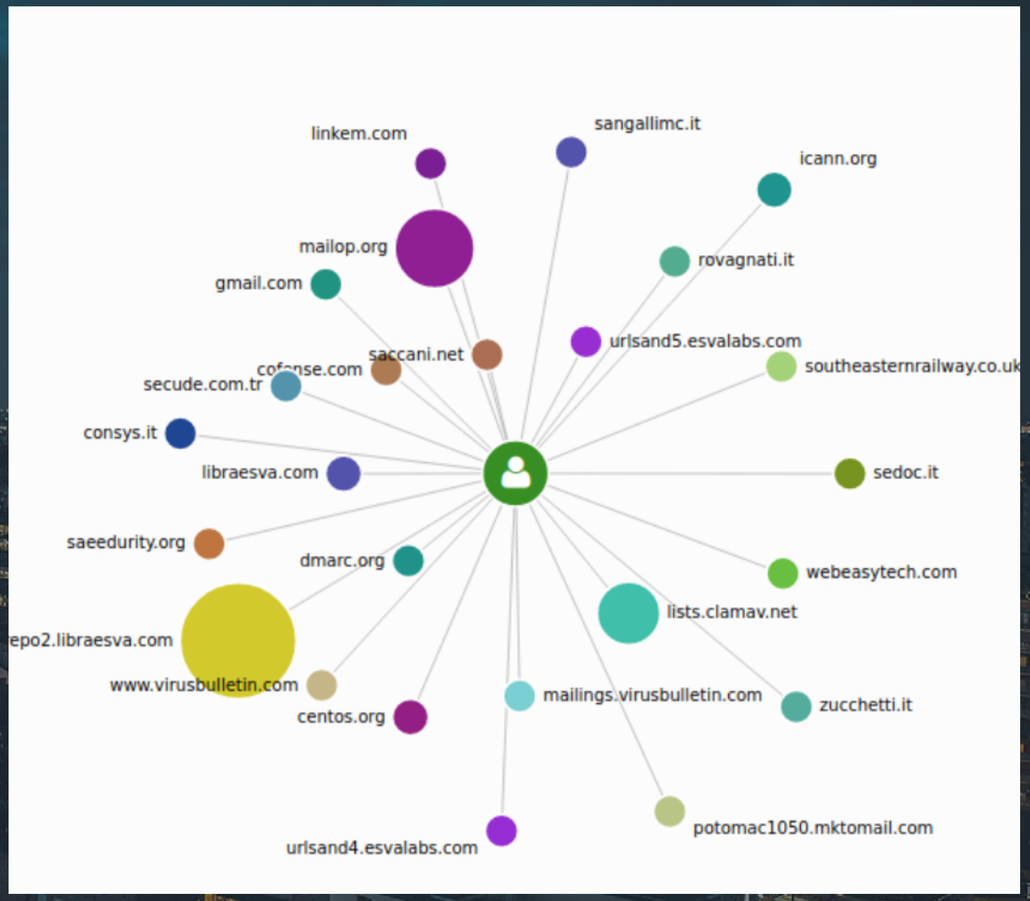
Clusit SECURITY SUMMIT ASTREA
Streaming Edition
10-11-12 novembre 2020

/LIBRAESVA

CONOSCERE

LA STORIA DELLE COMUNICAZIONI AZIENDALI.
(NON PUOI FALSIFICARE LA TUA STORIA)

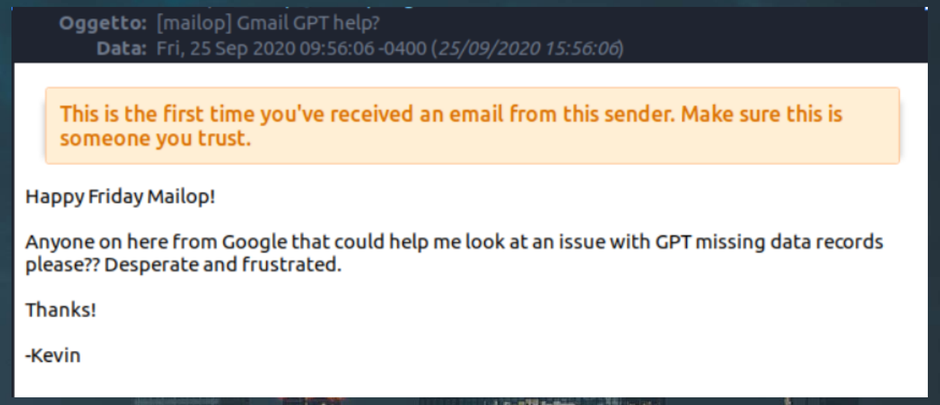
IL GATEWAY APPRENDE IL GRAFICO SOCIALE DELLE INTERAZIONI E L'INTENSITÀ DELLE RELAZIONI TRA INDIVIDUI E ORGANIZZAZIONI.

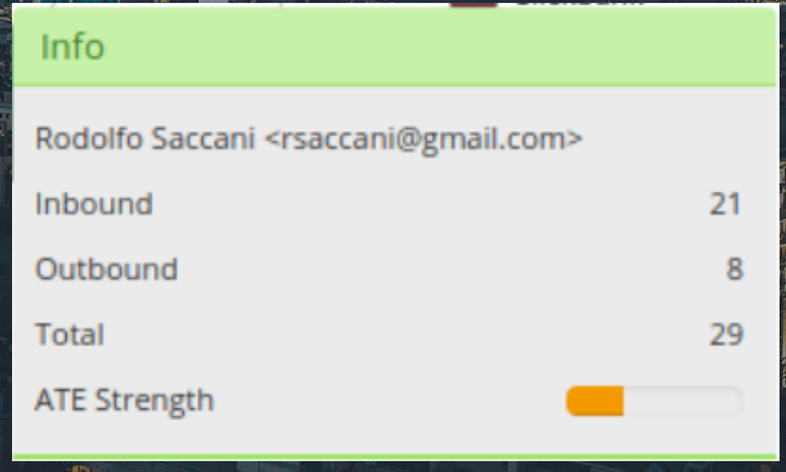


RI-CONOSCERE

INDIVIDUARE I FIRT-TIME-SENDERS (SIA PER GLI INDIVIDUI CHE PER LE ORGANIZZAZIONI)

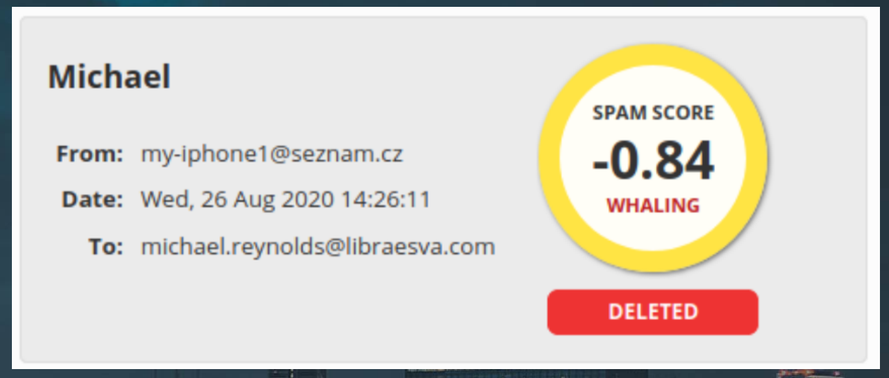
DAI PATTERN DI COMUNICAZIONE:
- RICONOSCERE L'AFFINITÀ
- STIMARE IL GRADO DI FIDUCIA

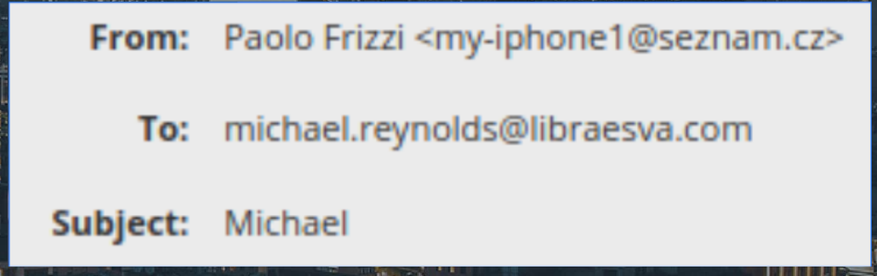


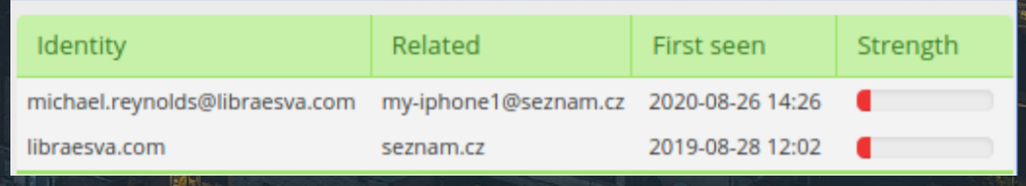


RILEVARE

- TENTATIVI DI IMPERSONIFICAZIONE
- CORRISPONDENTI FIDATI
- SPAMMING
- INDICE DI FIDUCIA ED AFFINITÀ
- ACCOUNT TAKEOVER







Identity	Related	First seen	Strength
michael.reynolds@libraesva.com	my-iphone1@seznam.cz	2020-08-26 14:26	
libraesva.com	seznam.cz	2019-08-28 12:02	

Clusit SECURITY SUMMIT ASTREA
Streaming Edition
10-11-12 novembre 2020

/LIBRAESVA

PER CONCLUDERE

ADAPTIVE TRUST ENGINE È UN MOTORE DI REPUTAZIONE.

LA CONOSCENZA DELLA STORIA E DELLE RELAZIONI FORNISCE SEGNALI ESTREMAMENTE UTILI PER DISCRIMINARE TRAFFICO LEGITTIMO DA TRAFFICO NON LEGITTIMO.

LA PROPRIA STORIA È UNA COSA CHE NON SI PUÒ FALSIFICARE, QUESTO RENDE ATE UNO STRUMENTO MOLTO EFFICACE

Clusit SECURITY SUMMIT ASTREA
Streaming Edition
10-11-12 novembre 2020

/LIBRAESVA

Q&A

Streaming Edition

Rodolfo Saccani: rodolfo.saccani@libraesva.com

Vieni a trovarci al nostro virtual desk!