FRAMA
mail. message. managed.

Active Tracker™ Intelligence E-Mail-Lifecycle-Bericht

Mit Active Tracker™ Intelligence erhalten Absender umfangreiche Informationen und Statistiken über die manchmal erstaunlichen Weltreisen Ihrer E-Mails.

Daily Aggregate Domain Security Report

Active Threat Hunting Analytics: 03/14/2023

Domain: frama.com

Highest Risk Level:	**Yellow**
Activities Analyzed:	**44**
Locations Analyzed:	**18**

Risk Analysis: Percent of Total	Current Period	Previous Period	Delta
Green	95%	81%	+14%
Yellow	5%	19%	-14%
Red	0%	0%	0%

Sending Statistics	Current Period	Previous Period	Delta
Unique Originators	4	4	0
Aggregate Recipients	19	19	0
Total Activities Analyzed	44	43	+1
Total Unique Internet Locations	18	26	-8
Time to First Activity (Median)	30min	1hour 11min	-40min
Geographic Regions with Activities	4	3	+1

Primary Features: Percent of Total Encrypted	Current Period	Previous Period	Delta
Certified E-Delivery Proof	46%	55%	-9%
Electronic Signature	0%	0%	0%
File Share	8%	0%	+8%

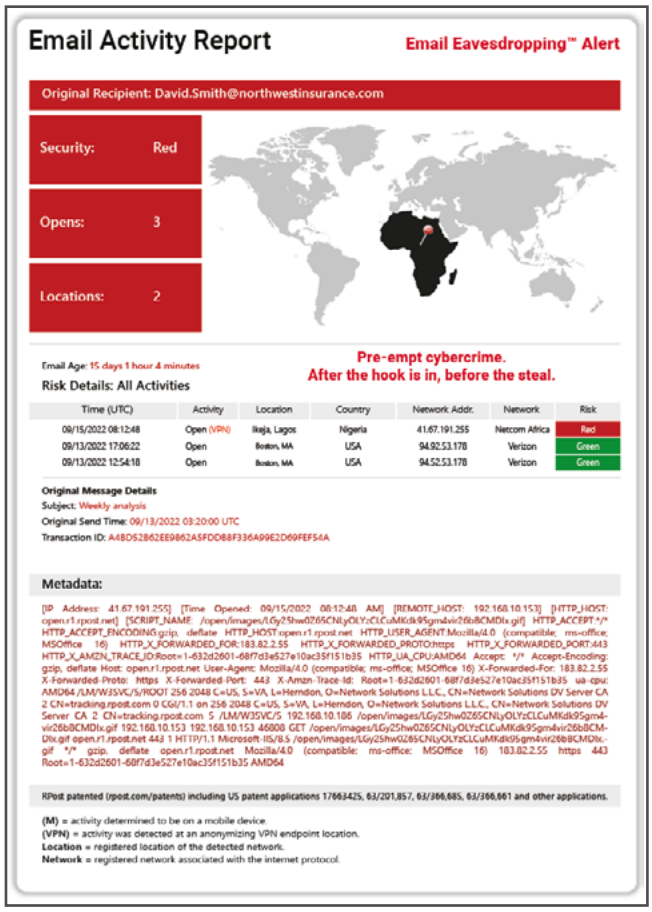
"Time to First Activity" includes only those messages sent in the period with an activity in the period.
"Highest Risk Level Map" displays the location that had the majority of the highest risk activities.
Total Potential Geographic Regions is 23.

FRAMA
mail. message. managed.

E-Mail Eavesdropping™ Alerts

Wenn die RMail **Active Threat Hunting-Technologie** ungewöhnliche Aktivitätsmuster identifiziert, generiert RMail eine E-Mail Eavesdropping™-Warnung und benachrichtigt in Echtzeit die IT-Administratoren (und optional den Absender) und liefert gleich forensische Daten dazu.

Bei typischen Angriffen nehmen Cyberkriminelle ihre Opfer ins Visier, indem sie sich in den E-Mail-Verkehr vom Absender bis zum Empfänger infiltrieren, um diesen abzufangen, zu analysieren, mit geringfügigen Änderungen zu kopieren (z. B. Zahlungsanweisungen) und um dann die Antworten so zu drehen, dass sie unbemerkt zurück zum Cyberkriminellen geleitet werden. Ähnliche Muster werden auch bei Spionage und anderen kriminellen Aktivitäten angewendet.


Email Activity Report

Email Eavesdropping™ Alert

Original Recipient: David.Smith@northwestinsurance.com

Security: Red

Opens: 3

Locations: 2

Email Age: 15 days 1 hour 4 minutes

Pre-empt cybercrime.
After the hook is in, before the steal.

Risk Details: All Activities

Time (UTC)	Activity	Location	Country	Network Addr.	Network	Risk
09/15/2022 08:12:48	Open (VPN)	Ikeja, Lagos	Nigeria	41.67.191.255	Netcom Africa	Red
09/13/2022 17:06:22	Open	Boston, MA	USA	94.92.53.178	Verizon	Green
09/13/2022 12:54:18	Open	Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details
Subject: Weekly analysis
Original Send Time: 09/13/2022 03:20:00 UTC
Transaction ID: A4BD52862EE9862A5FDD88F336A99E2D69FEF54A

Metadata:

[IP Address: 41.67.191.255] [Time Opened: 09/15/2022 08:12:48 AM] [REMOTE_HOST: 192.168.10.153] [HTTP_HOST: open.r1.rpost.net] [SCRIPT_NAME: /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26b8CMDlx.gif] HTTP_ACCEPT:*/* HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:open.r1.rpost.net HTTP_USER_AGENT:Mozilla/4.0 (compatible; ms-office; MSOffice 16) HTTP_X_FORWARDED_FOR:183.82.2.55 HTTP_X_FORWARDED_PROTO:https HTTP_X_FORWARDED_PORT:443 HTTP_X_AMZN_TRACE_ID:Root=1-632d2601-68f7d3e527e10ac35f151b35 HTTP_UA_CPU:AMD64 Accept: */* Accept-Encoding: gzip, deflate Host: open.r1.rpost.net User-Agent: Mozilla/4.0 (compatible; ms-office; MSOffice 16) X-Forwarded-For: 183.82.2.55 X-Forwarded-Proto: https X-Forwarded-Port: 443 X-Amzn-Trace-Id: Root=1-632d2601-68f7d3e527e10ac35f151b35 ua-cpu: AMD64 /LM/W3SVC/5/ROOT 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 0 CGI/1.1 on 256 2048 C=US, S=VA, L=Herndon, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA 2 CN=tracking.rpost.com 5 /LM/W3SVC/5 192.168.10.186 /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4-vir26b8CMDlx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNLyOLYzCLCuMKdk95gm4vir26b8CM-Dlx.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-IIS/8.5 /open/images/LGy25hw0Z65CNLyOLYzLLuMKdk95gm4vir26b8CMDlx.-gif */* gzip, deflate open.r1.rpost.net Mozilla/4.0 (compatible; ms-office; MSOffice 16) 183.82.2.55 https 443 Root=1-632d2601-68f7d3e527e10ac35f151b35 AMD64

RPost patented (rpost.com/patents) including US patent applications 17663425, 63/201,857, 63/366,685, 63/366,661 and other applications.

(M) = activity determined to be on a mobile device.
(VPN) = activity was detected at an anonymizing VPN endpoint location.
Location = registered location of the detected network.
Network = registered network associated with the internet protocol.

Mit Email Eavesdropping™-Warnungen wird jede versendete E-Mail und jede damit verbundene Aktivität über einen bestimmten Zeitraum forensisch analysiert.

Die generierten Warnungen enthalten alle faktenbasierten Daten zum E-Mail-Versand, damit diese von IT-Sicherheitsspezialisten sofort überprüft und entsprechende Sicherheits-Maßnahmen ergriffen werden können – **Noch bevor ein Schaden entsteht.**

Frama Communications AG, ein Unternehmen der Frama Gruppe . Dorfstrasse 6 . CH-3438 Lauperswil
Niederlassungen in: Österreich, Deutschland, Schweiz, Vereinigtes Königreich
www.frama.com . Kontakt: www.frama.com/de-de/kontakt/