

Email Lifecycle & Popularity Report

Senders can now gain insights into the popularity of their email and the sometimes astonishing journey their message takes as it is forwarded along...


Email Activity Report Active Tracker™ Intelligence

Original Recipient: jim@insurancegrp.com

Security: Green

Opens: 3

Locations: 2



Risk Details

Time	Activity	Detail	Locale	Location: Country	Location (IP)	Network	Risk
09/15/2022 08:12:46 UTC	Open	M	Frankfurt, Hesse	Germany	52.72.5.168	T-Mobile	Green
09/13/2022 12:54:18 UTC	Open		Boston, MA	USA	94.92.53.178	Verizon	Green
09/12/2022 02:15:17 UTC	Open		Boston, MA	USA	94.52.53.178	Verizon	Green

Original Message Details

Original Send Time: 09/12/2022 1:33:52 UTC
Transaction ID: E64B9039C2CE5914F42EE618CADAB09C55894832

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/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDlx.gif 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDlx.gif open.r1.rpost.net 443 1 HTTP/1.1 Microsoft-IIS/8.5 /open/images/LGy25hw0Z65CNlyOLyZCLCuMKdk95gm4vir26b8CMDlx.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.

Email Eavesdropping™ Alerts for Wire-Fraud Prevention

If the Frama RMail **active threat hunting** technology identifies unusual activity patterns, RMail generates an Email Eavesdropping™ instant alert, and notifies in real-time IT admins (and optionally senders) with forensic details.

Typical business attack lures start with cybercriminals targeting their victims by eavesdropping on email from sender to recipient, to siphon off email, analyse it, copy it with slight modifications (e.g. payment instructions), and then pivot replies so they route in a loop back to the cybercriminal.

Email Activity Report Email Eavesdropping™ Alert

Original Recipient: David.Smith@northwestinsurance.com

Security: Red

Opens: 3

Locations: 2



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)	Ibeja, Lagos	Nigeria	41.67.191.255	Neccom Africa	Red
09/13/2022 17:06:22	Open	Roson, MA	USA	94.52.53.178	Verizon	Green
09/13/2022 12:54:18	Open	Roson, 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: A48D528Q2E199K2ASF0D88F336A99E2D99FF54A

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.post.net] [SCRIPT_NAME: /open/images/LGy25hwOZ65CNlyOlyZCLCuMKd95gm4vr26bBCMDic.gif] HTTP_ACCEPT: */*
HTTP_ACCEPT_ENCODING:gzip, deflate HTTP_HOST:open.r1.post.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.post.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=1-632d2001-68f7d3e527e10ac35f151b35 ua-cpu:
AMD64 UA:W35VC/S/ROOT 256 2048 C=US, S=VA, L=Henriksen, O=Network Solutions L.L.C., CN=Network Solutions DV Server CA
2 CN=tracking.post.com 0 CGU/1.1 on 256 2048 C=US, S=VA, L=Henriksen, O=Network Solutions L.L.C., CN=Network Solutions DV
Server CA 2 CN=tracking.post.com 5 UA:W35VC/S 192.168.10.153 /open/images/LGy25hwOZ65CNlyOlyZCLCuMKd95gm4vr26bBCMDic-
gif?1 192.168.10.153 192.168.10.153 46808 GET /open/images/LGy25hwOZ65CNlyOlyZCLCuMKd95gm4vr26bBCMDic-
gif */* gzip, deflate open.r1.post.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, 63/366,665, 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.

With Email Eavesdropping™ alerts, every email sent out of the organisation has every activity associated with it analysed forensically, for a period of time.

These alerts include all the email data so that IT security specialists can validate and take immediate action, **before the cybercriminal lures users into mis-wiring money to the criminal's bank.**