Email Analysis

LETSDEFEND

Sudenur MURATOĞULLARI

İçindekiler

Giriş(Introduction)

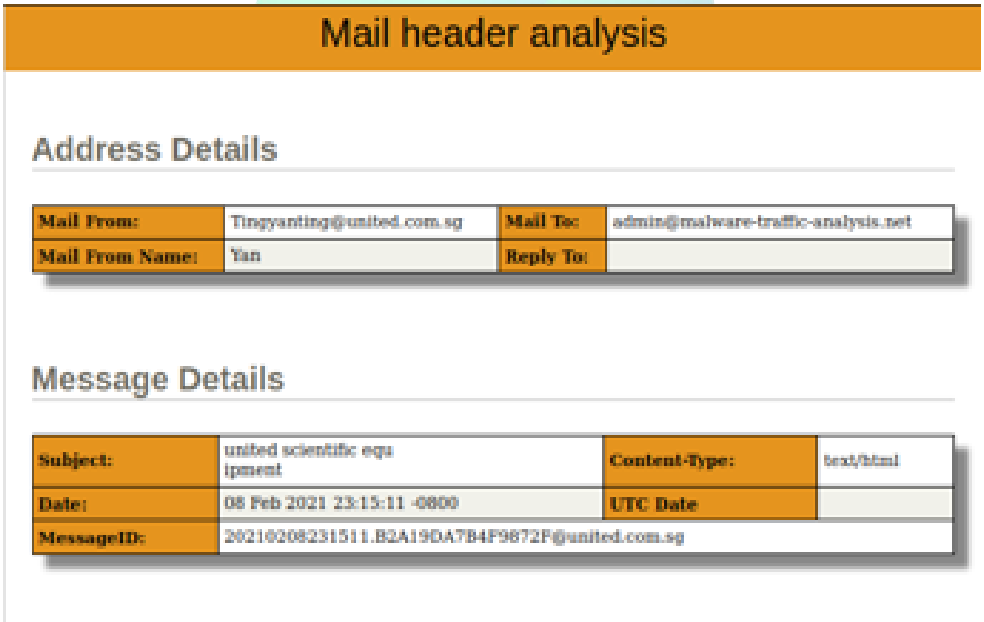
Yakın zamanda bir şirketi taklit etmeye çalışan birinden bir e-posta alındı, şüpheli olup olmadığını görmek için e-postayı analiz edeceğiz.

Metodoloji(Methodology)

Analizimiz için bize verilen EML ve EXE uzantılı iki dosyayı kullandık ve posta analizi için çevrimiçi araçlardan yararlandık.

Bulgular ve Analiz(Findings and Analysis)

Bir BusinessEmail.eml dosyamız var. Dosyamı Not Defteri'nde açıp tüm metni kopyalıyorum ve verileri daha okunabilir ve kategorize edilmiş olarak görmek için çevrimiçi Posta başlığı analiz sitesine atıyorum.



Yukarıda online analizimin çıktısı mevcut.

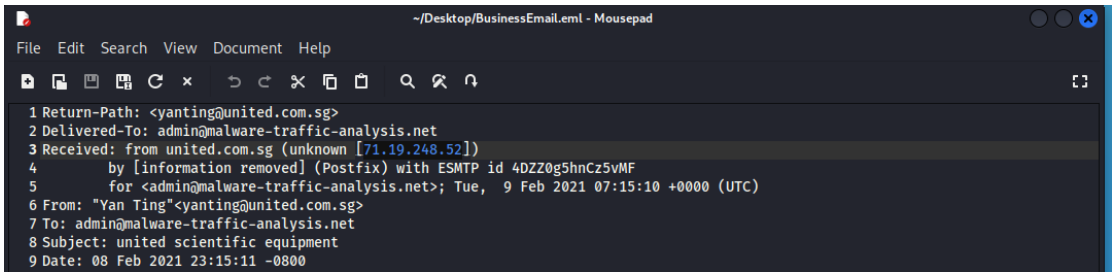
Bu analiz sonucunda gönderici e-posta adresinin yanting@united.com.sg, alıcı e-posta adresinin ise admin@malware-traffic-analysis.net olduğunu görebiliyorum.

Ayrıca e-postanın konusunda "united scientific equipment" yazdığını gözlemliyorum.

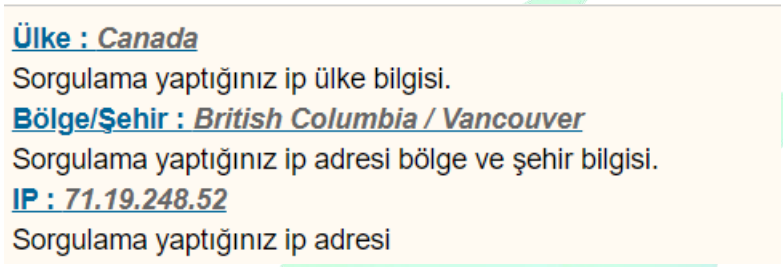
Ayrıca 02/08/2021 tarihinde gönderildiği bilgisi de mevcut.

Bu bilgiyi Notepad üzerinde metni inceleyerek doğruladım, kaynak IP adresine de eriştik.

➔ 71.19.248.52

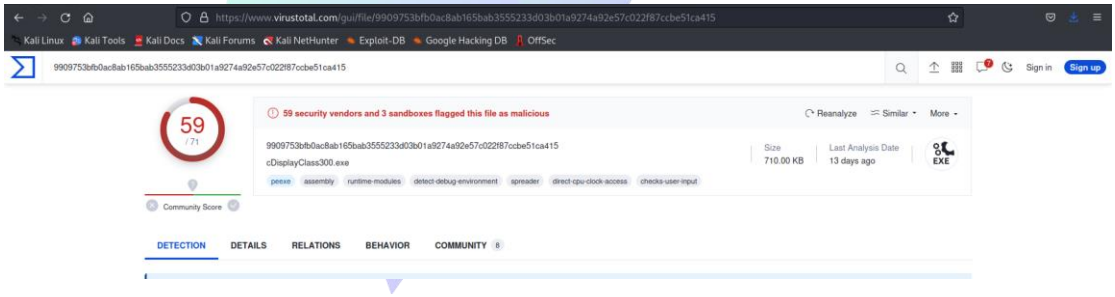


Bu IP adresi kullanılarak yapılan bir sorgulama, bunun Kanada'ya ait bir IP adresi olduğunu gösterdi.



Elimizdeki diğer dosya ise “united scientific equipent.exe”. Bu dosyayı virustotal'e atarak sha256 hash'ine ulaşıyorum.

➔ 9909753bfb0ac8ab165bab3555233d03b01a9274a92e57c022f87ccbe51ca415



Dosyanın kötü amaçlı yazılım olduğunu da doğruladık.

Olay Zaman Çizelgesi(Timeline of Events)

- 08 Feb 2021 23:15:11 :

  E-postayı aldık.

Sonuçlar(Conclusions)

Aldığımız e-postanın şüpheli olup olmadığını analiz ettikten sonra, bunun kötü niyetli bir e-posta olduğunu doğruladık.

Bilgili personel sayesinde zararlı dosya analiz edilmeden açılmamış ve olası bir siber saldırının önüne geçilmiştir.

HTTPS://APP.LETSDEFEND.İO/CHALLENGE/EMAİL-ANALYSİS