BIMANTARA Labs

2022

SECURITY REPORT

PHISING EMAIL ANALYSIS

Abdi Bimantara

CONTACT US:

abdibimantara91@gmail.com abdibimantara abdibimantara

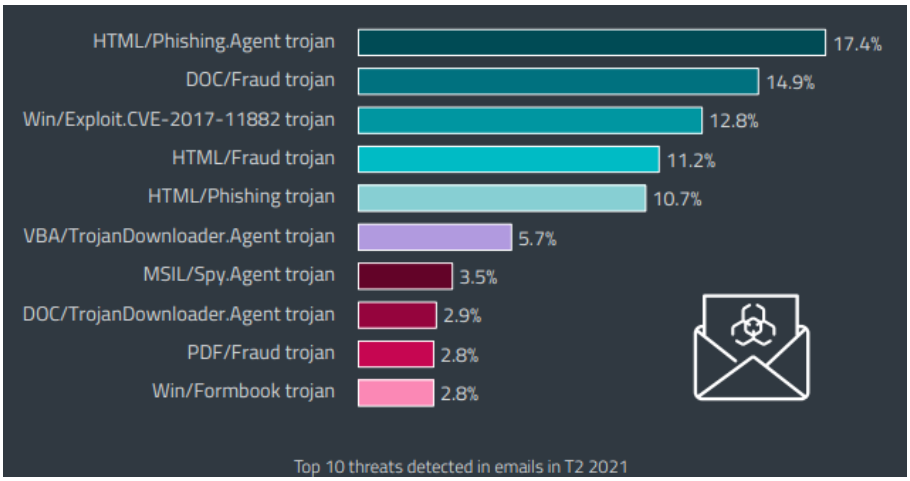
Daftar Isi

Halaman

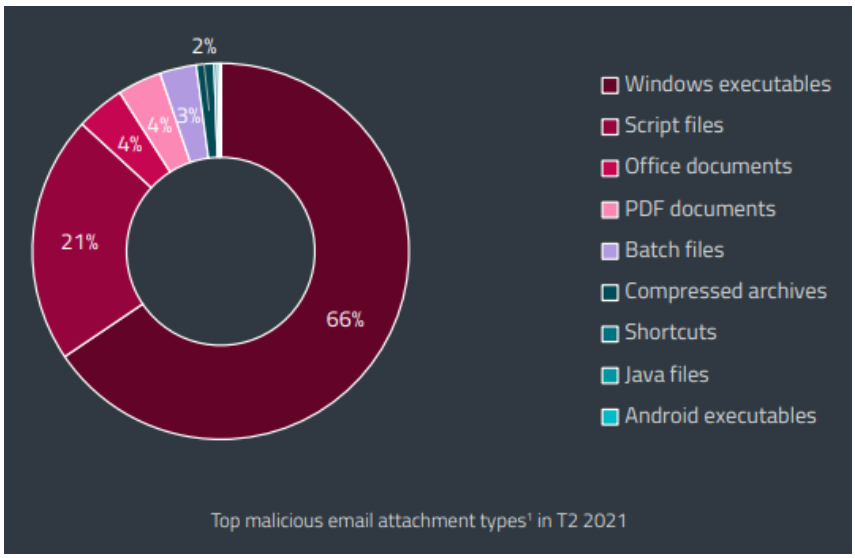
Email Phising

Phising adalah cara penyerang untuk mencuri informasi target, tanpa menimbulkan suatu kecurigaan. Cara yang umum di lakukan oleh penyerang melalui email atau pesan pribadi, pop up iklan dan lain segaianya. Penyerang akan berusaha meyankinan target bahwa payload yang dikirimkan tersebut tampak normal ataupun tidak berbahaya. Cara ini biasa disebut dengan **Sosial Engineering**.

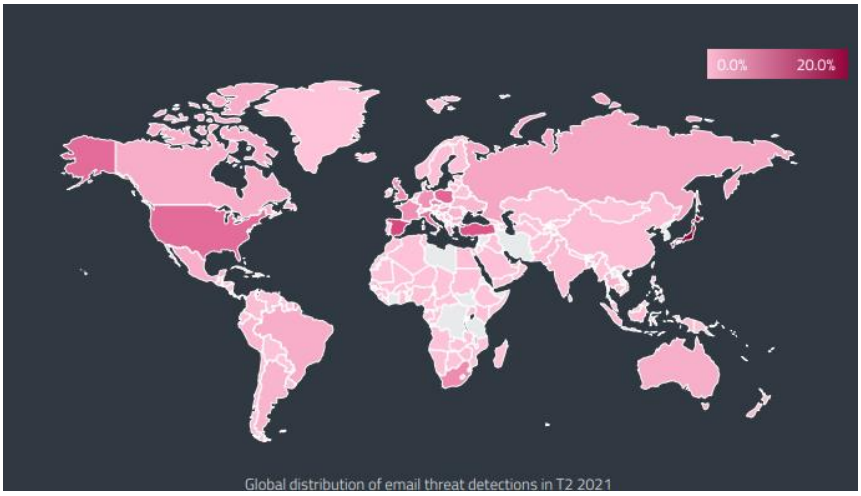
Umumnya serangan Email Phising ditargetkan untuk orang orang yang tidak terlalu peduli terhadap keamanan data personal, baik data pribadi maupun data instansi atau organisasi. Menurut penelitian yang dilakukan oleh tessian, umumnya seorang karyawan akan menerima rata rata sebanyak 14 email phising. Selain itu pada penelitian yang dilakukan oleh perusahaan Cyber Security internasioanal ESSET, mengklaim bahwa pada tahun 2021 mengalami peningkatan serangan phising berbasis email sebanyak 7,3%. Dimana peningkatan tersebut terjadi pada rentang bulan mei sampai agustus.



Data penelitian Esset pada tahun 2021 mengenai Email Threats



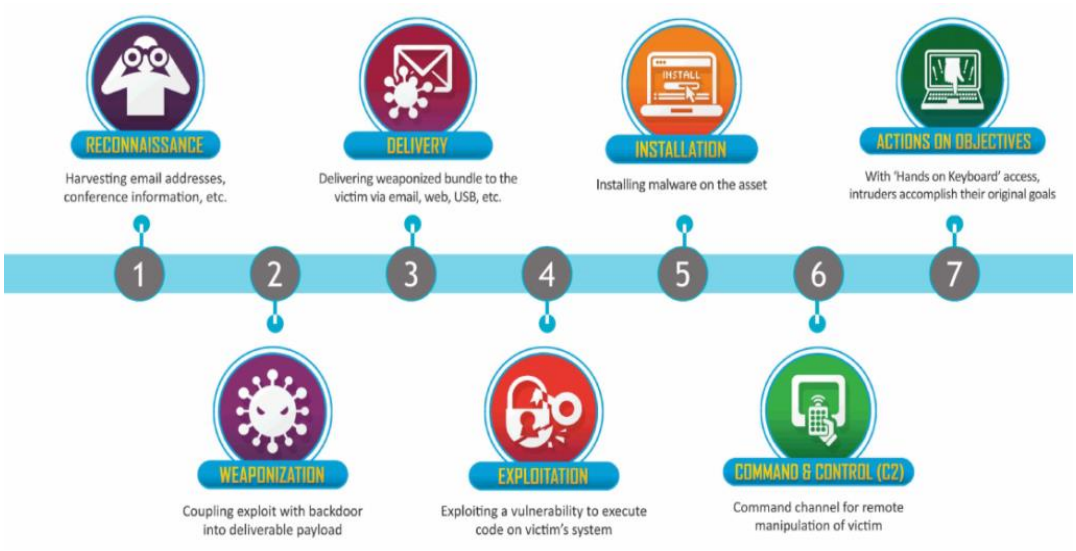
Data penelitian Esset pada tahun 2021email Attachments



Data penelitian Esset pada tahun 2021 Global distribution

Serangan Phising yang dilakukan melalui email menjadi trend saat ini. Melalui beberapa data yang kami dapatkan diatas, kami menyakini bahwa serangan email phising ini menjadi salah satu

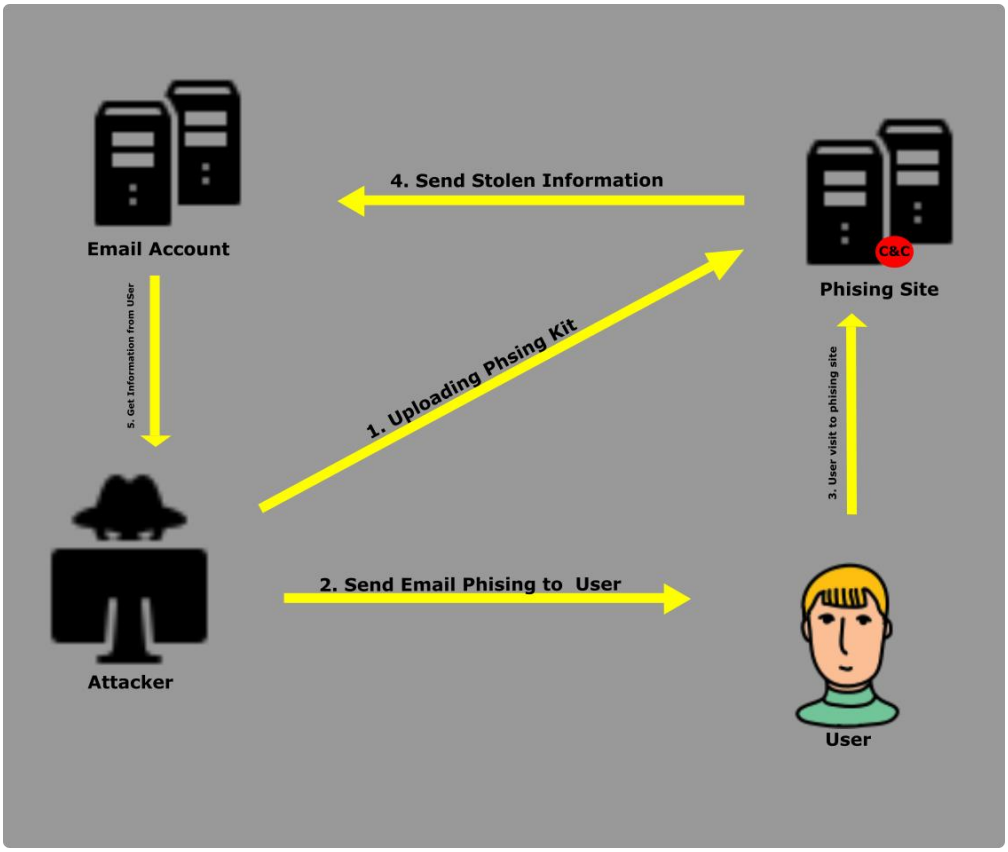
Langkah penting untuk meneruskan fase lain dalam kegiatan pentesting.



Gambar Killchain tim Lockheedmartin

Melihat dari Kill Chain yang dibuat oleh tim **Lockheedmartin,** Serangan Email Phising termasuk kedalam fase **Delivery**. Dimana pada fase tersebut penyerang akan berusaha mengirimkan payload phising melalui perantara email, web, USB dan lain sebagainya. Jika melalui fase ini penyerang berhasil mengirimkan payload tersebut, maka akan membuka peluang menuju fase lainnya baik tu fase Exploitation, Installation, Command and Control ataupun yang peling berbahaya yaitu Actions on Objectives. Berikut adalah contoh umum pada email phising.

Flow Email Phising



Flow Serangan email phising

Terdapat beberapa metode atau cara yang sering diterapkan penyerang dalam menjalankan serangan email phising. Umumnya, penyerang akan menggunakan cara seperti pada gambar diatas. Serangan email phising dimulai dengan si penyerangan mengupload phising kit kedalam phising site. phsing kit adalah segala sesuatu baik itu berupa gambar, link ataupun utilitas lainnya yang dapat menyebakan phising namun tidak membuat curiga dari sitarget. setelah berhasil mengupload phising kit, penyerang akan mencoba mengirimkan email, biasanya akan memuat konten yang menarik atau

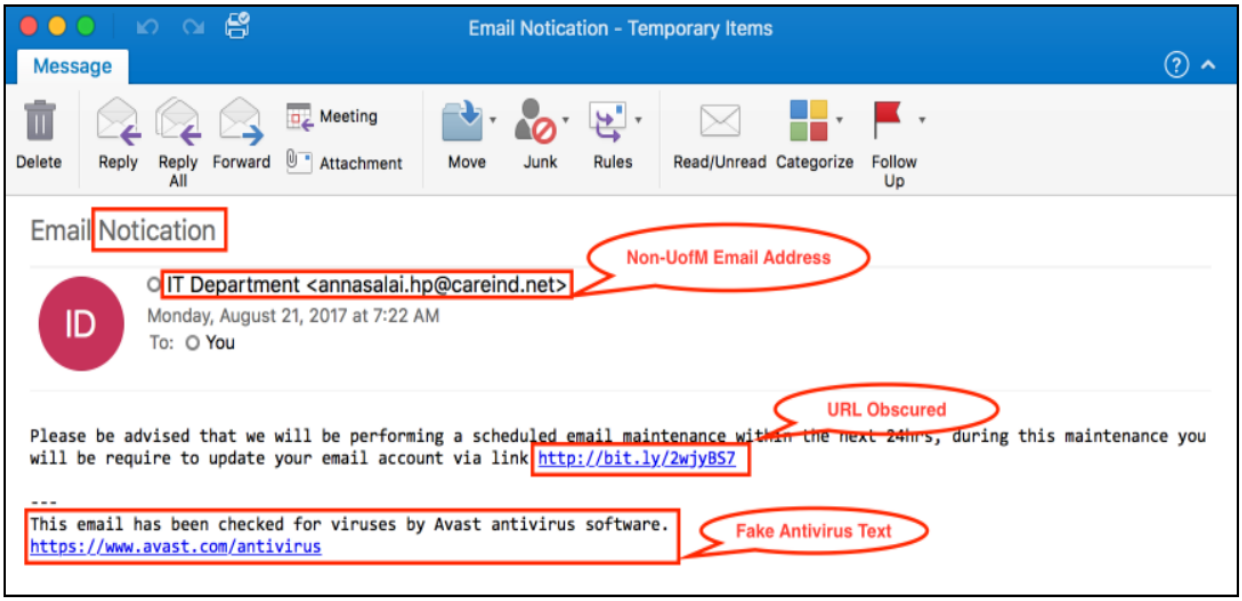
menakutkan. hal ini menyebabkan target akan segera membuka dan membaca email tersebut. saat target membuka email dan mengklik link yang diberikan, target akan secara otomatis mengunjungi phising site. pada phising site, target akan diminta untuk mengisi beberapa data baik itu data receh maupun data sensitif. dan data tersebut akan dikirimkan langsung oleh phising site ke penyerang melalui email acccount si penyerang tersebut.

Ciri Ciri Email Phising

Umumnya email phising akan dibuat semenarik mungkin oleh si penyerang. Baik menggunakan topik pembahasan finansial, doorprize ataupun lain sebagainya. Ada beberapa point yang setidaknya akan selalu ada dalam email phising yaitu

- Attachment file ataupun program
- Hyperlink yang dimasukkan pada pesan
- Email yang digunakan tidak professional atau tidak jelas

Ketiga point tersebut akan selalu ada dalam beberapa contoh kasus email phising



Contoh email phising

Pada gambar diatas, kita dapat mengetahui bahwa :

1. Email yang digunakan tidak jelas
2. Melampirkan URL yang sudah dibungkus menggunakan url lainnya yaitu bit.ly
3. Berusaha meyakinkan korban, dengan cara seolah olah isi pesan telah dikonfirmasi aman oleh salah satu vendor security.
4. Terdapat beberapa kosa kata yang sedikit membingungkan

Information Gathering

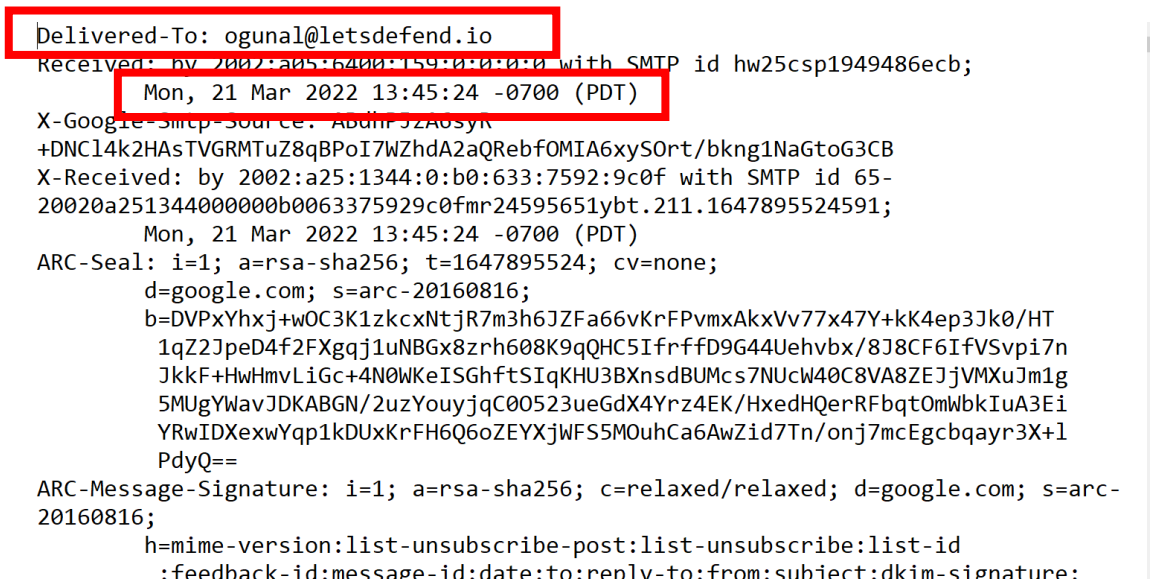
Sebelum melakukan penyerangan ataupun pengiriman email phsiing, tentunya attacker membutuhkan email dari target tersebut. Baik email perushaan ataupun email pribadi. Namun pada umumnya, attacker lebih menyukai email perusahaan dengan user yang lebih banyak. Untuk menemukan atau mengetahui information email tersebut, attacker akan terlebih dahulu mencarinya di darkweb jika data tersebut telah bocor atau melakukan proses reconnaissance secara mandiri. Proses reconnaissance ataupun information gathering tersebut umunya dapat menggunakan tools **theHarvester** yang dapat ditemukan dengan mudah di kali linux ataupun github.

therHarvester Tool Osint

Email's Header

Emails Header adalah bagian dari suatu email yang terletak pada paling atas. dimana Email header membuat beberapa informasi penting sepertin nama pengirim, Penerima, serta tanggal pengiriman email tersebut. Selain informasi tersebut kita juga dapat menjumpai informasi tambahan seperti "Return Path", "Reply To", dan "Received".

Bila email yang digunakan adalah Gmail. Maka file tersebut dapat dengan mudah mendownload email tersebut. Dan email tersebut secara otomatis akan tersimpan menggunakan format .eml. File tersebut akan dengan mudah kita buka menggunakan notepad.



```
Delivered-To: ogunal@letsdefend.io
Received: by 2002:a05:6400:159:0:0:0:0 with SMTP id hw25csp1949486ecb;
        Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
X-Google-Smtp-Source: ABdhPJzA6syR
+DNCl4k2HAsTVGRMTuZ8qBPoI7WZhdA2aQRebfOMIA6xySOrt/bkng1NaGtoG3CB
X-Received: by 2002:a25:1344:0:b0:633:7592:9c0f with SMTP id 65-
20020a251344000000b0063375929c0fmr24595651ybt.211.1647895524591;
        Mon, 21 Mar 2022 13:45:24 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1647895524; cv=none;
        d=google.com; s=arc-20160816;
        b=DVPxYhxj+wOC3K1zkcxNtjR7m3h6JZFa66vKrFPvmxAkxVv77x47Y+kK4ep3Jk0/HT
         1qZ2JpeD4f2FXgqj1uNBGx8zrh608K9qQHC5IfrffD9G44Uehvbx/8J8CF6IfVSvpi7n
         JkkF+HwHmvLiGc+4N0WKeISGhftSIqKHU3BXnsdBUMcs7NUcW40C8VA8ZEJjVMXuJm1g
         5MUgYWavJDKABGN/2uzYouyjqC0O523ueGdX4Yrz4EK/HxedHQerRFbqtOmWbkIuA3Ei
         YRwIDXexwYqp1kDUxKrFH6Q6oZEYXjWFS5MOuhCa6AwZid7Tn/onj7mcEgcbqayr3X+l
         PdyQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
        h=mime-version:list-unsubscribe-post:list-unsubscribe:list-id
         :feedback-id:message-id:date:to:reply-to:from:subject:dkim-signature;
```

File Emails Header tersebut dapat didownload pada link **6**.

Berdasarkan email header tersebut, terdapat beberapa informasi penting seperti

- Jika pesan tersebut anda balas, pesan tersebut akan dikirim untuk siapa ?
- Tahun berapa email tersebut dikirim
- Sebutkan nilai dari message IDnya

Sumber :

1. https://www.securitymagazine.com/articles/96430-mobile-phishing-threats-surged-161-in-2021
2. https://www.tessian.com/blog/phishing-statistics-2020/
3. https://cybersecnerds.com/lockheed-martin-cyber-kill-chain-illustrated/
4. https://lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
5. https://www.memphis.edu/its/security/phishing-examples.php
6. https://app.letsdefend.io/accounts/login/?next=/download/downloadfile/Challenge%2520Mail.zip/