شماره سی ام - تیر ۱۳۹۸

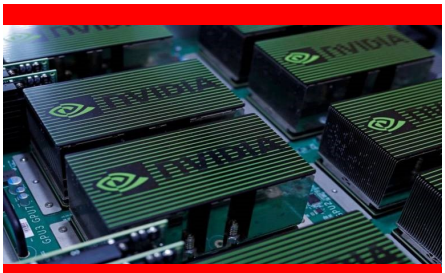
خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

کره شمالی و تخصیص میلیاردها دلار بـه حملات سایبری

شورای امنیت ایالات متحده آمریکا، کره شمالی را در سال ۲۰۰۶ به دلیل تلاش‌های خود برای تسلیح کردن خود با سلاح‌های کشتار جمعی، ممنوعیت یا محدود کردن دسترسی به فرصت‌های مختلف تجارت بین المللی، تحریم کرد. - صفحه ۲

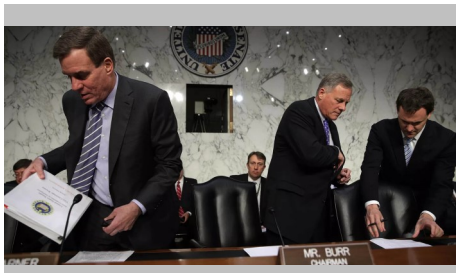


Nvidia پنج آسیب پذیری را پچ کرد!

در این ماه پنج آسیب پذیری جدی در محصولات Nvidia کشف گردید که دارای نمرات بسیار بالایی بودند. این آسیب پذیری‌ها جدی و درایورهای تحت تأثیر قرار گرفته عبارت اند از:

GeForce و Quadro و NVS و Tesla GPU

- صفحه ۳



روسیه سیستم‌های انتخاباتی ۵۰ ایالت را در سال ۲۰۱۶ هدف قرار داده

هکرهای روسی سعی در اخلال در سیستم انتخاباتی ایالات متحده سال ۲۰۱۶ داشتند، تلاش‌های آن‌ها بسیار مؤثر واقع شد و شاید بیشتر نگران کننده بود، زیرا بسیاری از کشورها آماده پاسخ به این حمله سایبری نبودند. - صفحه ۴

Windows Defender یکی از برترین آنتی ویروس‌ها

مدت زیادی نمی‌گذرد که Windows Defender یکی از ضعیف‌ترین آنتی ویوس‌ها برای محافظت از کامپیوتر شناخته شد. اما حالا با گذشت چند سال این آنتی ویروس توانسته است به یکی از بهترین آنتی ویروس‌های رایگان بر اساس رتبه بندی AV-test بدل شود. - صفحه ۵

PakCERT
Pakistan Computer Emergency Response Team

معرفی CERT پاکستان

The most trusted source of IT in Pakistan, Pakistan Computer Emergency Response Team (PakCERT), providing services for 19 years of excellence now, proves track record of delivering outstanding training to individuals as well as corporate firms for many years. PakCERT has been working with prestigious organizations from Government, Military Intelligence, Banking, Telecom, Education and Consultation etc.

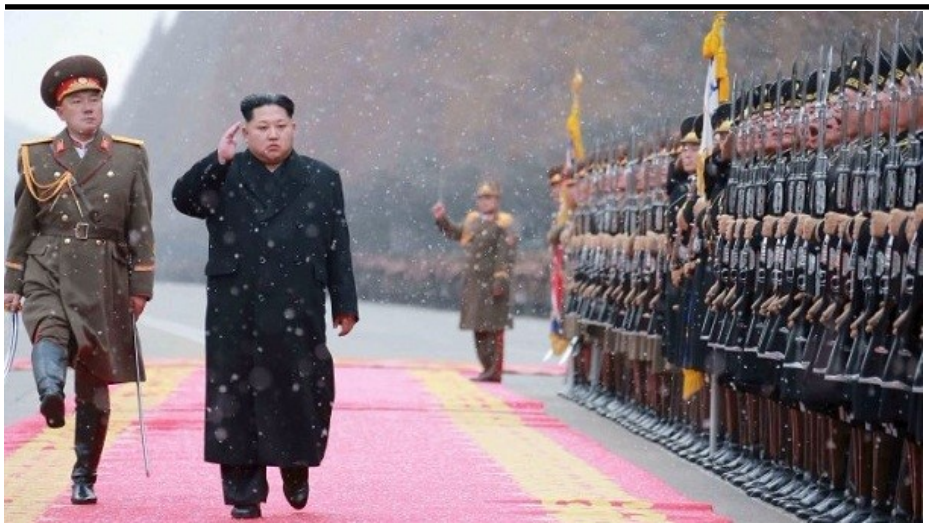
Armed with the latest exploit codes and techniques the underground is using for years to compromise the networks, it uses the same techniques to harden the network from such intruder attacks. PakCERT experts have leading industry recognized security certifications like CISSP, CEH, CPTS, ITIL, COBIT, MBCI, etc and are frequently interviewed and invited to speak at national and international security programs and conferences.

صفحه ۶ و ۷

کره شمالی و تخصیص میلیاردها دلار به حملات سایبری

شورای امنیت ایالات متحده آمریکا، کره شمالی را در سال ۲۰۰۶ به دلیل تلاش های خود برای تسلیح کردن خود با سلاح‌های کشتار جمعی، ممنوعیت یا محدود کردن دسترسی به فرصت‌های مختلف تجارت بین المللی، تحریم کرد. هدف این بود که کشور کوچک آسیا را ترغیب کند تا از برنامه تسلیحات هسته‌ای خود دست بکشد، اما تاکنون چنین نبوده است. اکنون که تنظیم کننده‌ها توجه خود را به سمت توسعه ارزهای غیرمتمرکز سوق می‌دهند، جزئیات جدیدی در مورد استفاده کره شمالی از تیم‌های جنگ سایبری برای تأمین اعتبار اهداف نظامی این کشور آشکار شده است.

کره شمالی مرکز اختلافات بسیاری بوده است که آخرین آن‌ها در تقاطع سیاست، فناوری و ارتش است. براساس گزارشی از رویترز، این کشور توانسته است حدود ۲ میلیارد دلار با هزینه کمتر از راه‌های قانونی برنامه تسلیحات کشتار جمعی، تولید کند.

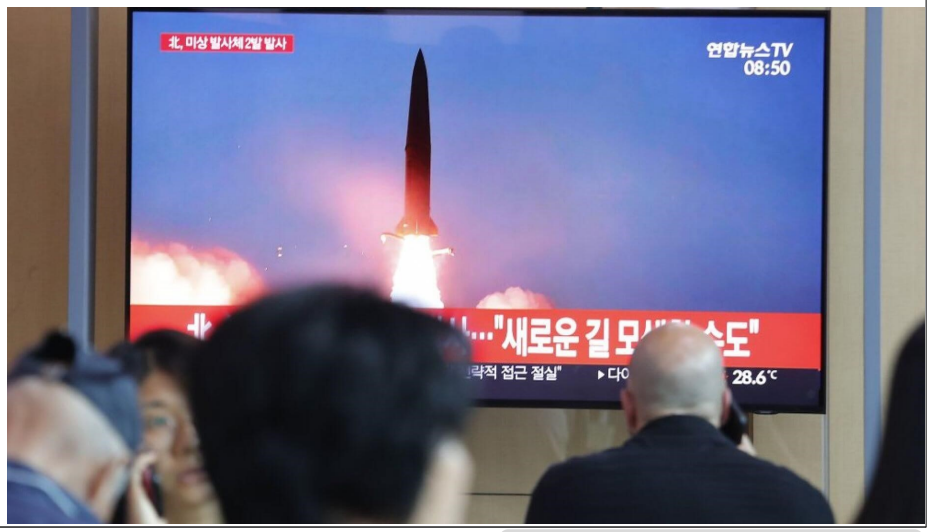


بدون شک می‌دانید که کره شمالی تقریباً در تمام تاریخ حمله اخیر یک مظنون اصلی است. باج افزار مشهور WannaCry یک نمونه برجسته است گروهی که در پشت این حمله قرار داشتند می‌توانستند به ازای هر شخصی که بخواهند در ازای دریافت پرونده های مهم، پول زیادی را جمع کند.

به گزارش رویترز، "این حملات برای سرقت وجوه از موسسات مالی و مبادلات رمزنگاری برای تولید درآمد" مورد استفاده قرار می گیرد، همچنین طرح‌های پولشویی برای پول های دزدیده شده را مشاهده می‌کنند.

حداقل ۳۵ حمله به ۱۷ کشور را هدف قرار داده، اما گفته شده که تعداد بیشتری از این حمله را می‌توانند انجام دهد. همچنین به نظر می‌رسد این کار همان گروه‌های هکر است که طی دو دهه گذشته زیر دفتر عمومی بازآفرینی کره شمالی مشغول به کار بوده‌اند.

نتیجه واضح این است که کره شمالی با چند روش جدید تحریم خواهد شد تا این کشور از استفاده از هکرها برای تأمین بودجه برنامه های نظامی خود منصرف کند، اما این کشور روش‌های جدیدی برای در امان ماندن پیدا خواهد کرد. در مورد پروژه هسته‌ای، ایالات متحده می‌گوید پیونگ یانگ برنامه‌های هسته ای و موشکی خود را افزایش خواهد داد.



گردآورنده: امیرحسین ضرغامی

Nvidia پنج آسیب پذیری را پچ کرد!

در این ماه پنج آسیب پذیری جدی در محصولات Nvidia کشف گردید که دارای نمرات بسیار بالایی بودند. این آسیب پذیری-ها جدی و درایورهای تحت تأثیر قرار گرفته عبارت اند از:

- GeForce
- Quadro
- NVS
- Tesla GPU

سه مورد از آسیب پذیری‌ها - CVE-2019-5683، CVE-2019-5684 و CVE-2019-5685 - به ترتیب با نمرات ۸.۸ ، ۷.۸ و ۷.۸ به ترتیب در معرض خطر بالا قرار گرفته اند، در حالی که دو آسیب پذیری دیگر - CVE-2019-۵۶۸۶ و CVE-2019-5687 - به ترتیب با نمرات ۵.۶ و ۵.۲ با خطر متوسط در نظر گرفته می‌شوند. امتیاز دهی مبتنی بر استاندارد رایج امتیاز دهی آسیب پذیری (CVSS) استاندارد V3 است.

Nvidia از این پنج آسیب پذیری تحت تأثیر قرار خواهد گرفت و این آسیب پذیری‌ها برروی درایورهای نمایش داده شده GeForce، Quadro، NVS و Tesla GPU و برروی نسخه‌های سیستم عامل ویندوز از ۷ تا ۱۰ تأثیر می‌گذارند. در صورت عدم رعایت، این نقص‌ها می‌توانند منجر به خطراتی همچون انکار سرویس (DoS)، افزایش سطح دسترسی و اجرای کد روی کامپیوتر شود.

دو مورد از این نقص‌ها توسط پیوتر بانیا از سیسکو تالوس کشف شد. بانیا قبلاً آسیب پذیری‌های متعددی را در مناطقی از درایورهای انویدیا کشف کرده است، هیچ یک از آسیب پذیری‌ها نمی‌توانند از راه دور مورد سوء استفاده هکرها قرار بگیرند، بنابراین نیاز است تا از نزدیک به آن سیستم آلوده دسترسی فیزیک داشت. هرچند این امر نگرانی‌ها را کم خواهد کرد اما این امر نیز باید هرچه سریع‌تر از سوی مصرف کنندگان این نوع از کارت‌های گرافیک رفع گردد تا خطرات آتی به بار نیایند.

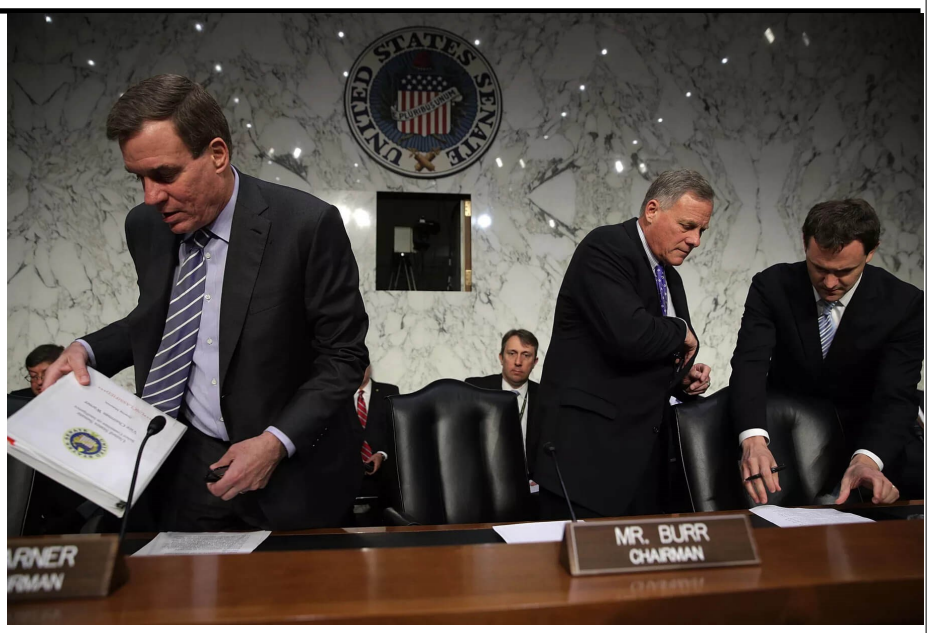
انویدیا توصیه می‌کند آخرین نسخه بروزرسانی نرم افزار را بارگیری و نصب کنید.

آخرین نسخه از درایورهای Nvidia را می-توان از آدرس زیر دریافت نمود.

https://www.nvidia.com/Download/index.aspx

گردآورنده: امیرحسین ضرغامی

روسیه سیستم‌های انتخاباتی ۵۰ ایالت را در سال ۲۰۱۶ هدف قرار داده



هکرهای روسی سعی در اخلال در سیستم انتخاباتی ایالات متحده سال ۲۰۱۶ داشتند، تلاش‌های آن‌ها بسیار مؤثر واقع شد و شاید بیشتر نگران کننده بود، زیرا بسیاری از کشورها آماده پاسخ به این حمله سایبری نبودند.

کمیته‌ی اطلاعاتی مجلس سنا اخیرا نخستین جلد تحقیقات خود را در مورد دخالت روسیه در انتخابات ۲۰۱۶ در ایالات متحده منتشر کرد. این گزارش نشان می‌دهد که مقامات به این نتیجه رسیده‌اند که همه‌ی ۵۰ ایالت توسط هکرهایی با روابط دولت روسیه هدف قرار گرفته‌اند لذا توصیه‌هایی را برای سال ۲۰۲۰ ارائه نمودند.

در سال ۲۰۱۷، خبرها حاکی از آن بود که این حملات محدود به ۳۹ ایالت بود و در همان سال، وزارت امنیت داخلی تنها اعتراف کرد که ۲۱ کشور تحت تاثیر این نقض قرار گرفته‌اند. در اوایل سال جاری DHS و FBI نشان دادند که برخی از اطلاعات جمع آوری شده در سال ۲۰۱۸ نشان می‌دهد که هکرها در واقع تلاش کردند تا زیرساخت‌های انتخاباتی دولت ایالات متحده را مورد هدف قرار دهند.

همچنین لازم به ذکر است که مقامات ایالات متحده هنوز مطمئن نیستند که اطلاعات رأی دهندگان اصلاح شده است یا اگر هکرها هر ماشین رای گیری واقعی را دستکاری کرده‌اند. در بیانیه‌ای، هر دو طرف از ایده ارائه دولت به هزینه‌های بیشتر برای امنیت انتخابات و تنظیم سیاست‌های انتخاباتی حمایت کردند تا هکرها دیگر نتوانند از شکاف بین مقامات فدرال و ایالت استفاده کنند.

توصیه‌های کمیته عبارتند از:

- ایجاد یک پیش نویس مقاله برای تکنولوژی رای گیری
- اجرای ممیزی‌های پس از انتخابات
- تهیه نسخه پشتیبان برای سیستم‌های ثبت نام و همچنین پذیرش صورتحساب‌های امنیتی انتخاباتی (ایده ای که اغلب توسط میچ مک کانل، رهبر اکثریت مجلس سنا، رد شد.)

در پاسخ، سناتور رون ویدن گفت: "ما نباید از کارکنان فناوری اطلاعات در انتخابات بخواهیم جنگ بر علیه توانایی‌های کامل و منابع گسترده ارتش سایبری روسیه را ببرند. این رویکرد در سال ۲۰۱۶ ناکام ماند و دوباره هم شکست خواهد خورد."

گردآورنده: امیرحسین ضرغامی

Windows Defender یکی از برترین آنتی ویروس‌ها

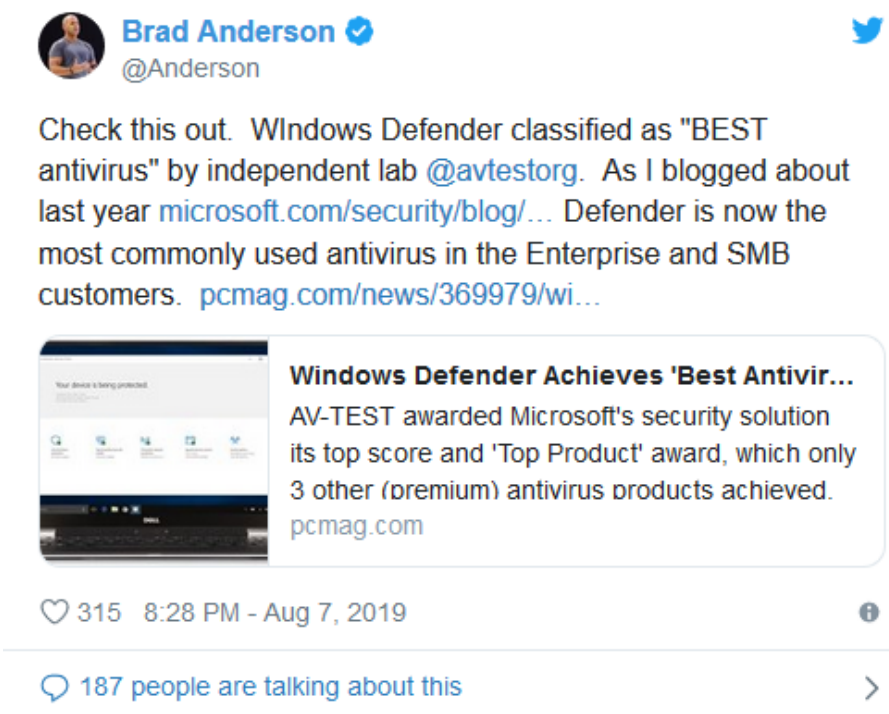
مدت زیادی نمی‌گذرد که Windows Defender یکی از ضعیف‌ترین آنتی ویوس-ها برای محافظت از کامپیوتر شناخته شد. اما حالا با گذشت چند سال این آنتی ویروس توانسته است به یکی از بهترین آنتی ویروس-های رایگان بر اساس رتبه بندی AV-test بدل شود.

یک موسسه‌ی خصوصی آلمانی در ماه می سال ۲۰۱۹ در گزارشی به عنوان "بهترین آنتی ویروس برای کاربران خانگی ویندوز"، Windows Defender مایکروسافت را جزو یکی از محصولاتی معرفی نمود که امتیاز ۶ از ۶ را به خود اختصاص داد. در این گزارش سه آنتی ویروس دیگر نیز توانستند امتیاز کامل را کسب نمایند.

این گزارش آنتی ویروس‌ها را براساس سه معیار محافظتی، کارایی و قابلیت استفاده پذیری رده بندی کرده است.

آنتی ویروس Windows Defender توانست با سه آنتی ویروس F-Secure SAFE، Kaspersky Internet Security و Norton Security در جایگاه نخست قرار گیرد.

اما آنتی ویروس Windows Defender یک مزیت بسیار بالا به نسبت تمامی این آنتی ویروس‌ها داشت و آن چیزی نبود جز رایگان بودن آن.



گزارش AV نشان می‌دهد که آنتی ویروس Windows Defnder توانایی جلوگیری از ۱۰۰ درصد از ۳۰۷ نمونه بدافزار Zero Day و ۱۰۰ درصد از ۲۴۲۸ نمونه در تست عمومی را دارا می‌باشد.

دو آنتی ویروس رایگان دیگر نتوانستند امتیازی مناسبی بگیرند. همچنین Avast و AVG توانستند امتیاز ۱۷.۵ از ۱۸ را کسب نمایند. پایین ترین امتیاز نیز متعلق به آنتی ویروس Webroot Secure Anywhere بود که تنها توانست امتیاز ۱۱.۵ را کسب نماید.

آنتی ویروس Windows Defender راه زیادی را برای رسیدن به این مرحله از Microsoft Security Essential طی نموده است. در تمامی این سال‌ها این آنتی ویروس در انتهای لیست AV قرار داشت. اما با گذر زمان مایکروسافت ثابت کرده است که در دنیای آنتی ویروس‌ها هم می‌تواند حرفی برای گفتن داشته باشد.

معاون شرکت مایکروسافت نتایج مربوط به این تست را در توییتر خود نشر داده است و بیان نموده است که این آنتی ویروس در سطح‌های بزرگتر از خانگی و Enterprise نیز جای خود را مستحکم نموده است.

شما نیز می‌توانید این آنتی ویروس را از سایت زیر دانلود و نصب نمایید.

https://www.techspot.com/downloads/4733-windows-defender-definition-update.html

گردآورنده: محمد مرتضوی

PakCERT: The Top Cyber Security Company in Pakistan

About and Objectives:

The most trusted source of IT in Pakistan, Pakistan Computer Emergency Response Team (PakCERT), providing services for 19 years of excellence now, proves track record of delivering outstanding training to individuals as well as corporate firms for many years. PakCERT has been working with prestigious organizations from Government, Military Intelligence, Banking, Telecom, Education and Consultation etc.

Armed with the latest exploit codes and techniques the underground is using for years to compromise the networks, it uses the same techniques to harden the network from such intruder attacks. PakCERT experts have leading industry recognized security certifications like CISSP, CEH, CPTS, ITIL, COBIT, MBCI, etc and are frequently interviewed and invited to speak at national and international security programs and conferences.

It has been also credited for finding the most severe security vulnerability ever in Microsoft .NET Passport services affecting millions of people worldwide.

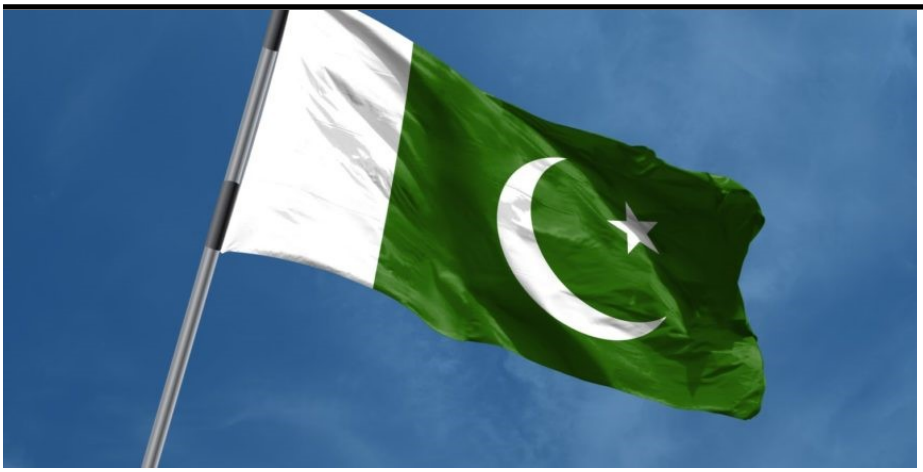
Services: Offering a range of facilities, PakCERT's main focus includes:

- Cost-effective Cyber Security Operations Center (CSOC), supporting services, scale and deploy rapidly to ensure information systems and critical infrastructure remain operational.
- Cyber Threat Intelligence provides information on potential threats based on security trends from around the world. This data would allow your organization to proactively defend against possible attacks. It has information on high-risk web pages, hosts, domains, and IP addresses, and can detect exact targeted aspects.
- Digital Forensic Analysis, in relation to the investigation and handling of computer related fraud, abuse and compromise, has made a proven track record of recovering vital evidence which could not have been found using conventional techniques.
- Managing compliance with ISO 27001 is a complex task but PakCERT is well-informed about the security practices, thus focuses on the Security Audit Process to ensure business outcomes.
- Development of Security policies: Fortunately, PakCERT's security policy framework provide standard solutions to typical environments thereby lowering the cost and complexity of policy deployment and business operations.
- PakCERT believes in data disaster recovery plans as a service, because users need experienced experts to help them create a plan. Through their time-tested processes and procedures, they can guide the users in implementing an ongoing, sensible, and cost-effective continuity plan.
- When discuss about the Malware reverse engineering, the Code analysis is performed on the malware using disassembler and debugger programs. The end result is to determine how the malware operates, take precautions to prevent further contamination, and employ techniques to safely remove the malware.

Continued on the next page...

گردآورنده: فاطمه علی نجفی

PakCERT: The Top Cyber Security Company in Pakistan



Information Security Trainings:

PakCERT has designed and delivered hundreds of trainings, seminars, workshops; spoken at various conferences related to information security. They firmly believe that knowledge only grows by sharing and frequently associate ourselves with active security communities.

Currently we are offering the following courses on client's site for corporate customers or individuals in groups.

- Certified Information Systems Security Professional (CISSP)
- Penetration Testing and Ethical Hacking
- Digital Forensic Analysis and Evidence Gathering
- Information Security Management System (ISMS/ ISO27001) Implementation
- Cyber Security Risk Management
- Incident Response
- General Data Protection Regulation (GDPR)
- Business Continuity and Disaster Recovery Planning
- Security Awareness (Management/Technical/End User)

PakCERT regularly runs training courses covering different areas of information security. Visit www.pakcert.org/ trainings.html for events calendar and to find out more about PakCERT's on-demand training curriculum.

گردآورنده: فاطمه علی نجفی

KHARAZMI CERT COORDINATOR CENTER

مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

امیرحسین ضرغامی

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

https://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.