ماژول 2

امنیت در سیستم عامل

C|SCU
Certified Secure Computer User

Certified Secure Computer User

Honors & Awards

- MCSA2003-MCSA2003Security
- MCSE2003-MCSE2003Security
- Windows Server 2008 Network Infrastructure Configuration
- Windows Server 2008 Application Infrastructure Configuration
- Windows Server 2008 Active Directory Configuration
- MCITP Server Administrator
- MCITP Enterprise Administrator
- Microsoft Certified Information Technology Professional
- Installing and Configuring Windows Server 2012
- Administering Windows Server 2012
- Configuring Advanced Windows Server 2012 Services
- Microsoft Certified Solutions Associate 2008, 2012
- Microsoft Certified Solutions Expert 2012 - Server Infrastructure
- IT professional - Cyber Security Org – SANS – Cloud Security Org – Network Security Org
- Comptia A+ - Comptia Network + - Comptia Security + - Comptia Master Level Security (CASP)
- Mcp V1, 2- MCTS
- Microsoft Certified Solutions Expert 2012 - Cloud & Security
- Microsoft Certified Solutions Expert 2012 – MSG

Best Regards,

Alireza Ghahrood

Pm: Security Products Manager

(Security Solution Provider : Cyber Space |BigData |Cloud |Virtualization

Sarv Co

Email: Ghahrood.A@Sarvrayaneh.com

Tel : +98 (21) 88027364 Ext.136 | Cell :+98 (912) 1964383 |

امنیت سیستم

توسعه دهندگان نرم افزارو سیستم عامل، معمولا برای این نقص ها وصله های امنیتی تولید می کنند

هر سیستم عامل و برنامه ای ممکن است نقص امنیتی داشته باشد

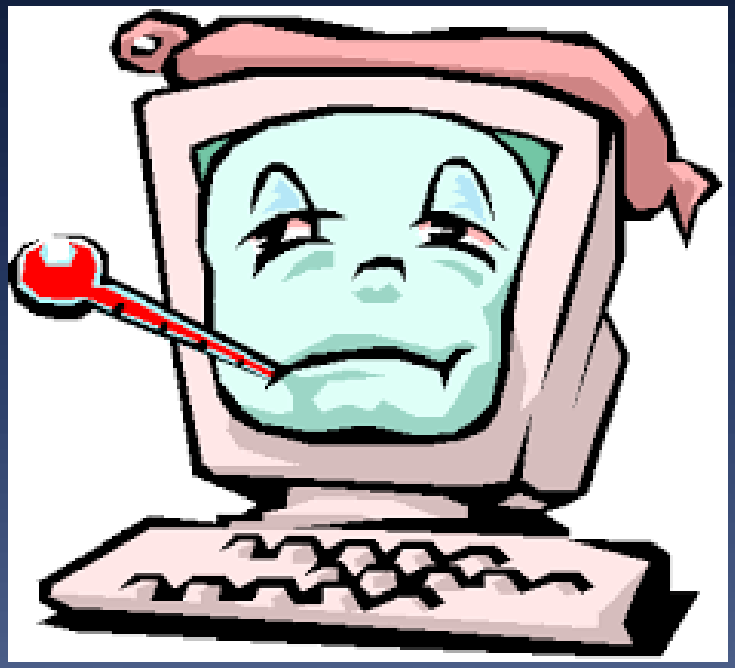
بوسیله نصب وصله های امنیتی از به خطرافتادن سیستم می توان جلوگیری نمود.

کاربران مجبور به نصب وصله امنیتی و پیکربندی نرم افزار هستند

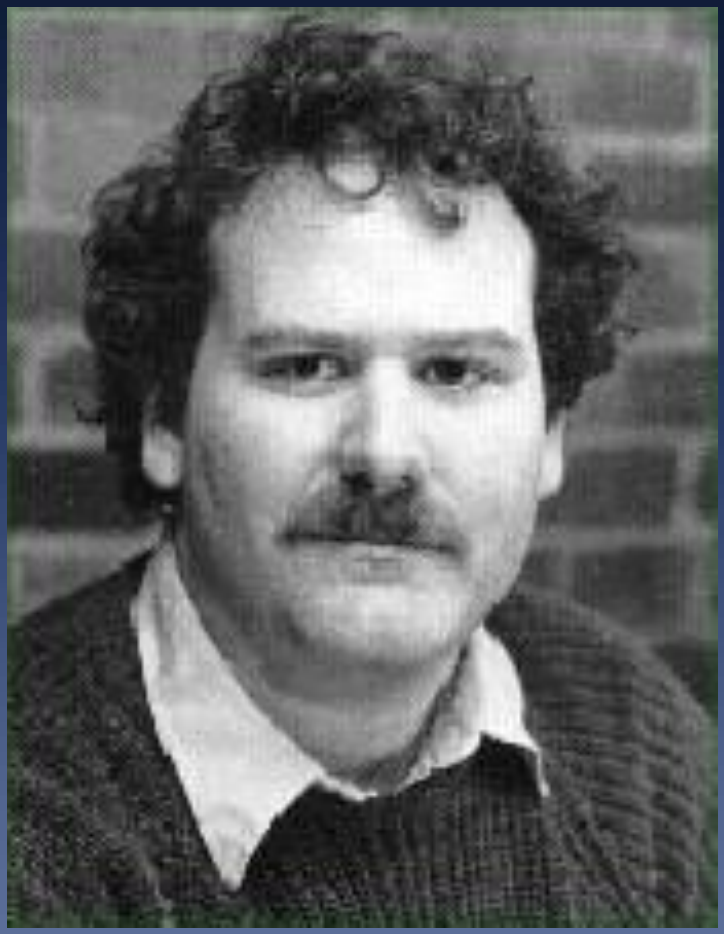
تهدیدات سیستم؟؟؟؟

بدافزار
ویروس
کرم
بک دور
روت کیت
تروجان
بمب منطقی
بات و بات نت
گروگان گیر
جاسوس
تبلیغات چی
.....

ویروس



فرد کوهن

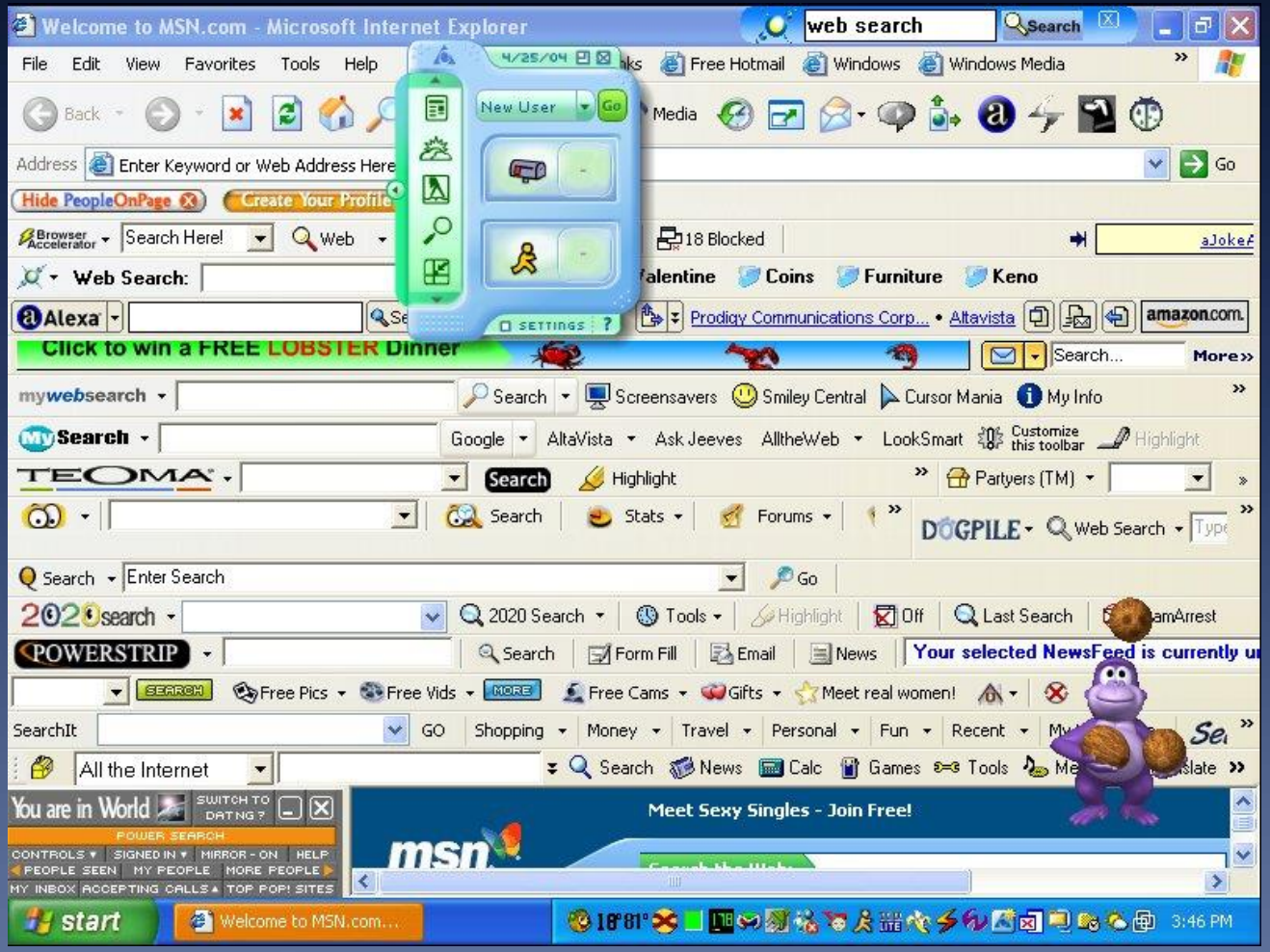


کرم

تروجان

جاسوسی

تبلیغات چی


Welcome to MSN.com - Microsoft Internet Explorer
web search
Search
File Edit View Favorites Tools Help
Free Hotmail
Windows
Windows Media
Back
Media
Address
Enter Keyword or Web Address Here
Go
Hide PeopleOnPage
Create Your Profile
New User
Browser Accelerator
Search Here!
Web
18 Blocked
Web Search:
Valentine
Coins
Furniture
Keno
Alexa
Prodigy Communications Corp...
Altavista
amazon.com
Click to win a FREE LOBSTER Dinner
Search...
More
mywebsearch
Search
Screensavers
Smiley Central
Cursor Mania
My Info
MySearch
Google
AltaVista
Ask Jeeves
AlltheWeb
LookSmart
Customize this toolbar
Highlight
TEOMA
Search
Highlight
Partyers (TM)
Search
Stats
Forums
DOGPILE
Web Search
Search
Enter Search
Go
2020search
2020 Search
Tools
Highlight
Off
Last Search
POWERSTRIP
Search
Form Fill
Email
News
Your selected NewsFeed is currently u
SEARCH
Free Pics
Free Vids
MORE
Free Cams
Gifts
Meet real women!
SearchIt
GO
Shopping
Money
Travel
Personal
Fun
Recent
All the Internet
Search
News
Calc
Games
Tools
You are in World
SWITCH TO DATING
POWER SEARCH
CONTROLS
SIGNED IN
MIRROR - ON
HELP
PEOPLE SEEN
MY PEOPLE
MORE PEOPLE
MY INBOX
ACCEPTING CALLS
TOP POP! SITES
Meet Sexy Singles - Join Free!
msn
start
Welcome to MSN.com...
3:46 PM

کیلاگر


DRPU PC Data Manager
DRPU
PC Data Manager
(Advanced Edition)
System Activities
Keystrokes
Clipboard
Screenshots
Application
System
Time
Sound
Date
Window Caption
Application Path
Input Keystrokes
Computer\User
3/14/2009 11... nick.wilss@gmail.com C:\Program Files\Googl... [Caps]N[Caps]obody[S... SYST02\Smith
3/14/2009 11... Microsoft Excel - Book1 C:\Program Files\Micros... tools[TAB]sales SYST02\Smith
3/14/2009 11... Document3 - Microsoft ... C:\Program Files\Micros... [Enter]employess[Spac... SYST02\Smith
3/14/2009 11... Untitled - Notepad C:\Windows\System32\... [Enter]records SYST02\Smith
3/14/2009 11... Untitled - Notepad C:\Windows\System32\... [Enter]times SYST02\Smith
3/14/2009 11... Microsoft Excel - Book1 C:\Program Files\Micros... date SYST02\Smith
3/14/2009 11... Document4 - Microsoft ... C:\Program Files\Micros... hi[Space]sir[Space][Ent... SYST02\Smith
3/14/2009 11... Document3 - Microsoft ... C:\Program Files\Micros... hi[Space]julia[Space]ho... SYST02\Smith
3/14/2009 11... Untitled - Notepad C:\Windows\System32\... hi[Space]sir[Space]y[B... SYST02\Smith
3/14/2009 11... Untitled - Notepad C:\Windows\System32\... free[Space]download[S... SYST02\Smith
Date : 3/14/2009 11:33:08 AM
Window Caption : nick.wilss@gmail.com
Application Path : C:\Program Files\Google\Google Talk\googletalk.exe
Computer\User : SYST02\Smith
Input Keystrokes : Nobody can even know that we are meeting since last 6 months, even your wife
System Activities
Internet Activities
Reports
Settings
Show Only Printing Keystrokes
View Keystrokes Activities
Delete All
Recording Status : Running
Time : 3/14/2009 11:34:20 AM
Start
Stop
Hide
Clear Log
Uninstall
About us
Help
Exit

بات نت

روت کیت

گروگان گیر


Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 100 USD / 100 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
9/8/2013
5:52 PM
Time left
56 : 16 : 12
Next >>


YOUR FILES HAVE BEEN ENCRYPTED!
CoinVault®

کرک پسورد (تهدید دیگر؟)

فرایندی برای شناسایی و یا بازیابی پسورد هاست

مهندسی اجتماعی　حدس زدن　برات فورس　دیکشنری　نگاه کردن　شنود

بدافزار چگونه انتشار می یابد؟




از طریق پیوست های ایمیل
از طریق فلش
از طریق وب سایت های الوده
از طریق کدک های جعلی
از طریق share folder
از طریق آنتی ویروس جعلی
از طریق دانلودهای رایگان
از طریق ارتباط p2p

راهنمایی برای امنیت ویندوز

- فرایندهای غیرضروری را پایان دهید
- پالیسی ویندوز را پیکربندی کنید
- در صورت لزوم فایلهای مهم را پنهان کنید
- سیستم اشتراک فایل پیش فرض را غیر فعال کنید
- از UAC استفاده کنید
- روال پیشگیری از بدافزارها را پیاده سازی کنید

- وصله های امنیتی را نصب کنید
- از فایروال ویندوز استفاده کنید
- از ntfs استفاده کنید
- از رمزگذاری ویندوز استفاده کنید
- از bitlocker استفاده کنید
- سرویس های غیر ضروری را غیر فعال کنید

- زمانیکه سیستم استفاده نمی شود، آنرا قفل کنید
- پسوردی قوی برای ویندوز انتخاب کنید
- حساب کاربری مهمان راغیر فعال کنید
- حساب های کاربری ناشناس را قفل کنید
- حساب کاربری مدیر را تغییر نام دهید
- منوی استارتاپ را غیر فعال کنید

ابزارهای امنیتی رایگان ویندوز

KeePass Password Safe
http://www.keepass.info

Eraser Portable
http://www.portableapps.com

PWGen Portable
http://www.portableapps.com

WSUS
http://www.pcdownload.com

Registry Mechanic
http://www.pctools.com

Wise Disk Cleaner
http://www.pcdownload.com