خبرنامه تخصصی ایمن

۳

سال اول / شماره ۳ /تابستان ۱۳۷۹ / ۱۶ صفحه / ۱۰۰ تومان

- مصاحبه با Metabolis
- جلوگیری از آلودگی به ویروس‌ها
- آشنایی با ویروس Compusarcoma

و...

آزمایشگاه تحقیقات ویروسهای رایانه‌ای

آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co

بسمه‌تعالی

خبرنامهٔ تخصصی **ایمن ۳**

سال اول/شمارهٔ سوم
تابستان ۱۶/۱۳۷۹ صفحه

فهرست مطالب

سرمقاله.....صفحهٔ ۳
نامه‌های شما.....صفحهٔ ۵
دربارهٔ ویروس‌ها(قسمت دوم).....صفحهٔ ۶
جدول ویروس‌های گزارش شده در نقاط مختلف دنیا Wild list.....صفحهٔ ۸
آشنایی با یک ویروس ایرانی(ویروس Compusarcoma).....صفحهٔ ۹
بازیابی اطلاعات(قسمت سوم).....صفحهٔ ۱۰
مصاحبه با ویروس‌نویسان بزرگ.....صفحهٔ ۱۱
گزارش اولین گردهمایی سراسری نمایندگان ضدویروس ایمن.....صفحهٔ ۱۳
گزارش دومین همایش مدیران کامپیوتر شرکتهای مخابرات سراسر کشور.....صفحهٔ ۱۴
آشنایی با گروه‌های ویروس‌نویسی.....صفحهٔ ۱۵
جدول مراکز فروش ضدویروس ایمن.....صفحهٔ ۱۶

****

« 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

به نام یگانهٔ توانا

سرمقاله

لازمهٔ هر حرکتی دو چیز است: ۱- وجود راه و هدف ۲- وجود وسیلهٔ نقلیه و نیروی محرکه.

در شروع حرکتمان، ما راه و هدف را بالابردن سطح آگاهی کاربران نسبت به دنیای ویروس‌ها قرار دادیم تا بدینوسیله با آگاهی بیشتری نسبت به مبارزه با این بلای تکنولوژی اقدام کنند.

اما هر وسیلهٔ نقلیه‌ای احتیاج به نیروی محرکه‌ای دارد که باید بصورت مداوم به آن تزریق شود. نامه‌های گرم و صمیمی شما و تشویق‌ها، پیشنهادها و انتقادات شما خوبان مانند نیروی محرکه‌ای است که ما را در این راه یاری داده و در ادامه دادن این راه دلگرم می‌کند. لذا از شما می‌خواهیم که با کمک‌های فکری خود باز هم ما را یاری دهید تا نشریه‌ای پربارتر و مفیدتر را به تمامی علاقمندان و کاربران دنیای کامپیوتر عرضه کنیم. پیشاپیش متشکریم.

****

✂----------

علاقمندان می‌توانند جهت دریافت شماره‌های بعدی این خبرنامه، فرم مشخصات زیر یا کپی آنرا به دفتر مرکزی این شرکت به آدرس: تهران ـ خیابان جمهوری اسلامی ـ بین جمالزاده و کارگر ـ شمارهٔ ۳۷۱ ـ طبقهٔ سوم ـ شرکت مهندسی مهران رایانه ارسال نمایند.

حقوقی / نام سازمان یا شرکت: .....

حقیقی / نام و نام خانوادگی: .....

آدرس: .....

شمارهٔ تماس: .....

مهر و امضاء

۳

با نرم‌افزار ضدویروس

ایمن

اطلاعات خود را بیمه کنید .

Imen Anti Virus

NEW
Version 9.8

کاملترین ضدویروس برای بازار نرم‌افزار خاور میانه

با قابلیت شناسایی و پاکسازی صددرصد بیش از ۱۰۰۰ ویروس از جمله

ویروسهای ایرانی و خارجی شایع در بازار نرم‌افزار ایران

پشتیبانی جدیدترین ویروسهای ایرانی و خارجی از جمله:

W95/Mtx (I-Worm.Mtx)
VBS/KakWorm
Restive.707
Nice Fox 3.3f
Nice Fox 3.4f

محصولی از آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن

شرکت مهندسی مهران رایانه

✉ نامه‌های شما ✉

✉ یکی از خوانندگان خوب خبرنامه به نام آقای *حسین بهبودی* از تهران در مورد ویروس ایرانی Compusarcoma و عدم توانایی ضدویروسهای خارجی در شناسایی و پاکسازی این ویروس مطالبی را برای ما ارسال کرده‌اند و خواستار اختصاص بخشی از خبرنامه به این موضوع شده‌اند. ضمن تشکر از این خوانندهٔ گرامی به خاطر حسن نظری که به نشریهٔ خودشان دارند، به اطلاع این عزیز و سایر خوانندگان خبرنامه می‌رسانیم که در همین شماره و در بخش **آشنایی با یک ویروس ایرانی** به معرفی این ویروس پرداخته‌ایم.

✉ آقای *محمد صادق صباغ کاشانی* از دیگر خوانندگان با لطف خبرنامه نیز طی نامه‌ای ضمن اظهار علاقه به مقالهٔ **دربارهٔ ویروسها** که در شمارهٔ دوم خبرنامه چاپ شد، خواستار ادامهٔ بحث‌هایی در این زمینه شده‌اند. با تشکر از این خوانندهٔ گرامی که با نامهٔ گرمشان موجب دلگرمی ما شدند، به اطلاع می‌رسانیم که در همین راستا در این شمارهٔ نشریه مقالهٔ **پیشگیری از آلودگی به ویروس** چاپ شده است و از شماره‌های بعد نیز به تفصیل به معرفی هر یک از انواع ویروسها خواهیم پرداخت. امیدواریم همچنان با نظرات سازندهٔ خود ما را در پربارتر کردن خبرنامه یاری فرمایید.

✍ ✍ ✍ ✍ ✍ ✍ ✍ ✍ ✍ ✍ ✍ ✍ ✍

توجه:

خبرنامهٔ تخصصی ایمن آمادهٔ دریافت انتقادات، پیشنهادها و مقالات شما خوانندهٔ گرامی جهت هرچه پربارتر نمودن این نشریه می‌باشد.

به طرق زیر می‌توانید با ما تماس بگیرید:

آدرس: تهران ـ خیابان جمهوری اسلامی ـ بین جمالزاده و کارگر ـ شمارهٔ ۳۷۱ ـ طبقهٔ سوم.

تلفن: ۶۴۲۳۵۷۷ (سه خط)

نمابر: ۶۴۲۳۴۰۸

آدرس e-mail:

imen_av@yahoo.com
mehran@irna.net

✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎ ✎

دربارهٔ ویروس‌ها (قسمت دوم)

پیشگیری از آلودگی به ویروس:

اگرچه ویروسها مشکل‌ساز هستند، ولی میزان این مشکلات باید در مقام مقایسه مورد توجه قرار بگیرد. عمومی‌ترین دلیل از دست دادن داده‌ها اشتباهات انسانی است. دومین دلیل ناشی از خرابی سخت‌افزارها و همچنین مشکلات نرم‌افزاری و باگها می‌باشد. دلیل بعدی ویروسها می‌باشند. به هر حال انجام یک سیاست درست ضدویروسی به شما در حفاظت از داده‌هایتان در مقابل هر نوع زیانی از جمله ویروسها، کمک خواهد کرد. در حالت خاص شما باید سه اصل زیر را در مورد حفاظت از داده‌ها انجام دهید:

۱ ـ پیشگیری: برای محدود کردن انتشار و شیوع ویروسها.

۲ ـ ردیابی: برای اطمینان از این مطلب که اگر ویروسی توانست از امکانات تدافعی و پیشگیرانهٔ ما عبور کند، در سریع‌ترین زمان ممکن کشف می‌شود.

۳ ـ بازیافت: برای اطمینان از این مطلب که اگر فایلی از دست رفته یا اینکه آسیب دیده است، در سریع‌ترین زمان ممکن بازسازی خواهد شد.

استفاده از ضدویروس **ایمن** آشکارا یک بخش قابل توجه و مهم از سیاست ردیابی و بازیافت است. در اینجا چند اصل عمومی از یک سیاست عاقلانهٔ ضدویروسی را برای شما شرح می‌دهیم:

۱ ـ نگهداری نسخه‌های پشتیبان.

۲ ـ بررسی منابع نرم‌افزارها.

۳ ـ نگهداری بوسیلهٔ دیسکتهای فلاپی و سایر رسانه‌ها.

۴ ـ اجتناب نمودن از کدکردن و حفاظت بویسلهٔ کلمهٔ رمز(Password).

حال به تفصیل هر یک از موارد فوق را تشریح می‌کنیم:

نسخه‌های پشتیبان:

مهمترین اقدام محتاطانه که شما می‌توانید در مقابل هرگونه از دست دادن اطلاعات انجام دهید، گرفتن نسخه‌های پشتیبان به صورت مرتب از سیستمتان می‌باشد. اگر شما از اطلاعات خود به صورت مرتب پشتیبان تهیه نکنید، احتمال ضرر و زیان بسیاری وجود دارد.

به یاد داشته باشید که نسخه‌های پشتیبان خود را بطور مکرر بررسی کنید و اطمینان حاصل نمایید که شما می‌توانید اطلاعاتتان را از آنها بازیابی کنید. مطمئن شوید که شما از تمامی فایل‌های اجرائیتان بر روی دیسکت یا هر رسانهٔ دیگری کپی‌های سالمی دارید. همهٔ دیسکت‌های پشتیبان و دیسکت‌های راه‌انداز شما باید در حالت Write Protect باشند.

بررسی منابع نرم‌افزاری:

مطمئن شوید که تمامی نرم‌افزارهای شما از یک منبع قابل اطمینان و مشهور بدست می‌آیند. بررسی کنید که نرم‌افزار در بسته‌بندی اصلی و دست‌نخوردهٔ خودش باشد.

هرگز از نرم‌افزارهای کپی‌شده و ثبت نشده استفاده نکنید. حتی اگر احساس می‌کنید که حق دارید از کپی دیگری بطور موقت استفاده کنید (برای مثال به خاطر اینکه نسخهٔ ثبت شدهٔ خود را در جای دیگری جا گذاشته‌اید) به یاد داشته باشید که کپی ممکن است شما را در معرض آلودگی ویروسی قرار دهد.

نرم‌افزارها می‌توانند از طریق پورتهای ارتباطاتی همانند رسانه‌های قابل حمل وارد کامپیوتر شما شوند. هنگامی که نرم‌افزاری را به کامپیوترهای قابل حمل و شبکه‌ها می‌فرستید یا دریافت می‌کنید و هنگامی که فایل‌ها را از صفحات بولتنی و اینترنت دریافت می‌کنید، بسیار مراقب باشید.

تهدید ویروسی از طریق دیسکتهای فلاپی:

احتمال آلودگی ویروسی بطور خاص از طریق دیسکتهای فلاپی بسیار زیاد است، اما شما می‌توانید چند مرحلهٔ سادهٔ زیر را برای افزایش ایمنی انجام دهید:

- دیسکتها را همواره در حالت Write-protect نگه دارید تا از کپی شدن ویروسها جلوگیری شود.
- هنگامی که کامپیوتر را خاموش می‌کنید، دیسکتهای فلاپی را درون درایوها باقی نگذارید. این مسأله شما را از آلودگی توسط یک ویروس بوت‌سکتوری وقتی که می‌خواهید تصادفاً سیستم را بوسیلهٔ یک دیسکت آلوده به این نوع ویروس راه‌اندازی کنید، مصون نگه خواهد داشت.
- درصورتیکه کامپیوتر را تصادفاً بوسیلهٔ یک دیسکت غیرسیستم راه‌اندازی کردید، کامپیوتر را مجدداً از طریق درایو :C راه‌اندازی کنید.
- Setup سیستمتان را طوری تغییر دهید که ابتدا از طریق درایو :C راه‌اندازی شود نه از طریق درایو :A .(این مورد معمولاً در درایوهای SCSI امکان‌پذیر نیست.)
- در صورت امکان از روشهای متناوب برای انتقال فایل‌ها استفاده کنید.
- به یاد داشته باشید که فایل‌های روی نوار(Tape) ممکن است هنگامیکه از آنها پشتیبان تهیه می‌شود، آلوده شوند.

اجتناب نمودن از کد کردن و حافظت بوسیلهٔ کلمهٔ رمز:

کد کردن و حفاظت بوسیلهٔ کلمهٔ رمز راه‌هایی برای حفاظت فایل‌ها از دستیابی بدون اجازه به آنها می‌باشند.

متأسفانه فایلهایی که به این روشها حفاظت می‌شوند، بوسیلهٔ برنامه‌های ویروس‌یاب قابل دسترسی نیستند که می‌تواند منجر به این مسأله شود که ویروسها کشف‌نشده باقی بمانند.

به عنوان مثال مستندات WORD می‌توانند شامل چند ماکرو باشند و این ماکروها ممکن است آلوده باشند. اگر یک مستند WORD بوسیلهٔ کلمهٔ رمز حفاظت نشده باشد، می‌تواند ویروس‌یابی شود و هر ویروسی که در آن است، شناسایی شود. اما درصورتیکه یک مستند WORD بوسیلهٔ کلمهٔ رمز حفاظت شده باشد، نمی‌تواند مورد ویروس‌یابی قرار گیرد. (ادامه دارد)

جدول ویروسهای گزارش شده در نقاط مختلف دنیا WildList

در این شماره، WildList مربوط به ماه‌های پنجم(می) تا نهم(سپتامبر) سال ۲۰۰۰ را برای شما تهیه کرده‌ایم. با مرور این جدول متوجه می‌شوید که اغلب ویروسها از نوع ماکرو بوده و تعدادی هم ویروس اسکریپت به چشم می‌خورد. از این ویروسها، ویروسهای W32/MTX وVBS/LoveLetter در ایران به دفعات گزارش شده که نرم‌افزار ضدویروس **ایمن** قادر به شناسایی و پاکسازی صددرصد این ویروسها می‌باشد.

نام ویروس	نوع	نام ویروس	نوع
Dodgy	فایل	W97M/Ethan.D	ماکرو
VBS/Fireburn.A	اسکریپت	W97M/IIS.E	ماکرو
VBS/LoveLetter	اسکریپت	W97M/Marker	ماکرو
VBS/Netlog.D	اسکریپت	W97M/Melissa.AL	ماکرو
VBS/NewLove.A	اسکریپت	W97M/NSI.B	ماکرو
VBS/Stages.A	اسکریپت	W97M/Proverb	ماکرو
VBS/Timofonica.A	اسکریپت	W97M/Resume.A	ماکرو
VBS/Tune.B	اسکریپت	W97M/Service.A	ماکرو
W32/MTX	فایل	W97M/Smac.D	ماکرو
W32/Qaz	فایل	W97M/Surround.A	ماکرو
W95/Plage	فایل	W97M/Thus	ماکرو
W95/Weird.10240	فایل	W97M/Titch.D	ماکرو
W97M/Assilem.G	ماکرو	W97M/Wrench.E	ماکرو
W97M/Bobo	ماکرو	X97M/Barisada	ماکرو
W97M/Bridge.A	ماکرو	X97M/Divi	ماکرو
W97M/Dariem.A	ماکرو	X97M/Laroux	ماکرو
W97M/DB.A	ماکرو	X97M/Yawn.A	ماکرو
W97M/Eight941.D	ماکرو	————	———

☠ آشنایی با یک ویروس ایرانی ☠

ویروس Compusarcoma :

عبارت Sarcoma به معنای تومور سرطانی است و Compusarcoma تلویحاً به معنای سرطان کامپیوتر می‌باشد. ویروس ایرانی Compusarcoma در سال ۱۳۷۷ متولد شد و در بازار نرم‌افزار ایران به شدت شایع گردید. اندازهٔ این ویروس ۱۳۲۸ بایت است و فقط فایل‌های اجرایی اعم از فایل‌های COM ، EXE و . . . را آلوده می‌کند و هیچگونه عملیات تخریبی دیگری ندارد. از آنجایی که این ویروس در سطح کشور بصورت گسترده‌ای شیوع یافت، قسمتهایی از آن توسط افراد مختلف دستکاری شده و به عنوان گونهٔ جدید تکثیر و منتشر گردیده‌اند.

در گونهٔ اولیهٔ آن عبارت 'COMPUSARCOMA' virus by M.S.S. در فایل‌های آلوده دیده می‌شود. در نوع Jamal و Amir ویروس، عبارت فوق دستکاری شده و بصورت زیر تغییر یافته‌اند:

'LAHIJAN UNIT' JAMAL PENTIUM Vir

و

(AMIR MOHEIMANI) TEL:0171-30297 !

هنگام اجرای یک فایل آلوده، ویروس در حافظه مقیم شده (در صورتیکه قبلاً مقیم نشده باشد) و کنترل چند تابع از توابع وقفهٔ 21h را در اختیار می‌گیرد. سپس فایل command.com را آلوده می‌کند. این ویروس با در اختیار گرفتن توابع (Close File)3E ، (Create or Truncate File)3C ، (Create New File)5B ، (Extended Open/Create)6C و نیز (Load & Execute File)4B00 ، فایل‌های اجرایی را آلوده می‌کند. همچنین با در اختیار گرفتن توابع 11 ، 12 ، 4E و 4F ، سعی در مخفی نمودن سایز واقعی فایل‌های آلوده می‌کند. فایل‌های COM بیش از ۶۳۹۵۱ بایت و یا کمتر از ۱۰۰۰ بایت توسط این ویروس آلوده نمی‌گردند.

لازم به تذکر است که تاکنون چند گونه از این ویروس مشاهده شده که هر کدام از آنها با دستکاری بر روی گونهٔ اولیه ایجاد گردیده‌اند و چون این ویروس ایرانی می‌باشد، اغلب نرم‌افزارهای ضدویروس خارجی از شناسایی و پاکسازی این ویروس ناتوان هستند و نرم‌افزارهایی هم که این ویروس را شناسایی می‌کنند، فقط گونه‌های قدیمی این ویروس را می‌شناسند درحالیکه در حال حاضر گونه‌های جدید این ویروس در بازار نرم‌افزار ایران بسیار شایع می‌باشند.

نرم‌افزار ضدویروس **ایمن** با قابلیت شناسایی و پاکسازی این ویروس و گونه‌های مختلف آن و همچنین دیگر ویروس‌های شایع در ایران، بهترین نرم‌افزار برای مبارزه با این ویروس می‌باشد.

☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎ ☎

در صورت یافتن هر گونه ویروس جدید و یا وجود هر نوع فایل مشکوک با شرکت مهندسی مهران رایانه و یا با آدرس الکترونیکی زیر تماس بگیرید:

imen_av@yahoo.com
mehran@irna.net

بازیابی اطلاعات (قسمت سوم)

همواره کاربران اینگونه تصور می‌کنند که بازیابی اطلاعات به معنی برگردانیدن کلیهٔ فایلها و فهرستها می‌باشد. درحالیکه طبق تجربهٔ بدست آمده تا کنون، ممکن است بازیابی اطلاعات همواره بطور کامل انجام نشود و فقط درصدی از اطلاعات قابل بازیابی باشد. با نگاهی به جدول زیر تا حدودی می‌توان درصد میزان بازگشت اطلاعات را در حالتهای مختلف تخمین زد:

	محدودهٔ خرابی	میزان بازگشت اطلاعات
۱	از بین رفتن جدول قسمت‌بندی **Partition Table**	۱۰۰٪
۲	از بین رفتن سکتور راه‌انداز **Boot Sector**	۱۰۰٪
۳	از بین رفتن جدول تخصیص فایل **FAT**	۱۰۰٪ = برای فایلهای کوچکتر از یک کلاستر (میزان پراکندگی فایل* ظرفیت فایل) / ۱۰۰٪ = برای فایلهای بزرگتر از یک کلاستر
۴	ازبین رفتن فهرست اصلی **Root Directory**	۱۰۰٪ = فایلهای داخل زیرشاخه‌ها (میزان پراکندگی فایل* ظرفیت فایل) / ۱۰۰٪ = فایلهای ریشهٔ اصلی
۵	فرمت کردن پارتیشن	مانند مورد ۴
۶	حذف کردن فایل‌ها	۱۰۰٪ ، در صورت پیوسته بودن فایل در غیر اینصورت مانند مورد ۳
۷	گم شدن پارتیشن	۱۰۰٪
۸	از بین رفتن ناحیهٔ کلاسترها (محدودهٔ داده‌ها)	غیر قابل بازیابی

حال ممکن است هر ترکیبی از موارد فوق با یکدیگر بوجود آید. در نتیجه درصد بازگشت اطلاعات کمتر هم می‌شود. در ضمن ممکن است قسمتی از محدوده‌های ذکر شده آسیب دیده باشند که در آنصورت تنها قسمتهای سالم آن قابل بازیابی هستند.

درصد بازیابی برای رسانه‌های مختلف زیر، بترتیب کم‌تر و بازیابی آن مشکل‌تر می‌گردد:

۱- فلاپی دیسک ۲- هارددیسک FAT 12 ۳- هارددیسک FAT 16 ۴- هارددیسک FAT 32

۵- NFS ناول ۶- NTFS ، NT ۷- CD-ROM ۸- ZIP Drive

۹- DRV Space ۱۰- Zip File ۱۱- Tape

مصاحبه با ویروس‌نویسان بزرگ

مصاحبه با Metabolis

- شما چگونه با کامپیوترها آشنا شدید؟

در سال ۱۹۸۲ من بدلایلی یک کامپیوتر می‌خواستم و آنقدر پدر و مادرم را اذیت کردم تا آنها برای من یک کامپیوتر خریدند. آنها برای من یک Sinclar ZX81 خریدند.

- چطور و چه زمانی با دنیای ویروسها آشنا شدید؟

فکر می‌کنم اواخر سال ۱۹۹۳ بود که تصمیم گرفتم به منظور سرگرمی یک گروه ویروس‌نویسی تأسیس کنم. من با Qark بوسیلهٔ یک شبکهٔ BBS محلی ملاقات داشتم و باقی قضایا.

- آیا شما ویروسی نوشته‌اید؟ اگر نوشته‌اید چه اعتباری دوست دارید در این زمینه کسب کنید؟

من تعدادی ویروس نوشته‌ام. اما هیچکدام از آنها را شایستهٔ ذکر کردن نمی‌دانم.

- شما چگونه ویروسهایتان را نامگذاری می‌کنید؟

روش خاصی نیست. نامها بسادگی به ذهنم خطور می‌کنند.

- کدام زبانهای برنامه‌نویسی را بلد هستید؟

اسمبلی ۸۰۸۶، بیسیک و پاسکال.

- از کدام زبان برنامه‌نویسی دوست دارید بیشتر استفاده کنید؟

من تا ۱۵ سالگی از برنامه‌نویسی واقعاً لذت نمی‌بردم.

- آیا شما عضو یکی از گروه‌های ویروس‌نویسی هستید؟

ممکن است.

- شما در زمینهٔ ویروس‌نویسی چه هدفی را دنبال می‌کنید؟

من به تمام چیزهایی که در این زمینه مد نظر داشتم رسیده‌ام.

- شما نام مستعار خود را از کجا بدست آورده‌اید و معنی آن چیست؟

از یک بازی کامپیوتری برای کامپیوترهای Sinclair ZX Spectrum 48k که آن را همراه یک مجله در سال ۱۹۸۹ خریدم.

- نظر شما دربارهٔ نرم‌افزارهای تولید ویروس چیست؟

من هرگز واقعاً با آنها موافق نبوده‌ام. تمام کاری که آنها انجام می‌دهند اینست که توجه بیشتری را به نویسندهٔ این نرم‌افزارها جلب می‌کنند و تعداد زیادی ویروس ناتوان را وارد دنیای کامپیوترها می‌کنند.

 نظر شما در مورد ویروسهای ماکرو در مقابل ویروسهای نوشته شده به زبان اسمبلی و زبانهای سطح یالا چیست؟
اگرچه این روزها ماکرو ویروسها درصد بیشتری از آلودگی را ایجاد می‌کنند، ولی من آنها را ویروسهای ناچیز و پیش‌پا افتاده‌ای می‌دانم.

 آیا تا بحال یکی از ویروسهایتان را در دنیای کامپیوترها تثبیت کرده‌اید؟
من هرگز نشنیده‌ام که کسی با یکی از ویروسهای من آلوده شده باشد. البته برای این موضوع دلیل خوبی هم وجود دارد.

 نظر شما در مورد اثرات مخرب در ویروسها چیست؟
من هرگز با اثرات مخرب موافق نیستم. اطلاعاتی که تخریب می‌گردند ممکن است مال خودتان باشد.

 آیا به نظر شما چیزی بعنوان ویروس « خوب » وجود دارد؟
من فکر نمی‌کنم در آلوده شدن چیز سودمندی وجود داشته باشد.

 شما در زندگی حقیقیتان چکار می‌کنید؟
در این لحظه از زمان در کل کار زیادی انجام نمی‌دهم.

 آیا افرادی که خارج از دنیای ویروسها هستند(مانند والدین، دوستان و ...) می‌دانند که شما چکار می‌کنید؟
بله، والدینم معمولاً از فعالیتهای زیرزمینی من پشتیبانی می‌کنند. دوستانم نیز گروه VLAD را می‌شناسند و کسی با کارهای من مشکلی ندارد.

 آیا شما در زمینهٔ کامپیوتر بجز فعالیت در مورد ویروسها کار دیگری نیز انجام می‌دهید؟
این روزها خیر. قبلاً بیشتر وقتم را صرف نوشتن موسیقی و برنامه‌های کمکی می‌کردم.

 آیا ویروسها باید غیرقانونی باشند؟ آیا فرقی بین تولید ویروس و انتشار آن وجود دارد؟
خیر، ویروسها نباید غیرقانونی باشند. هرکسی حق دارد که هرچه را می‌خواهد روی کامپیوتر خودش بنویسد.
در واقع یک تفاوت بین ایجاد و انتشار ویروس وجود دارد. هرکسی بوسیلهٔ یک اسمبلر و سورس یک ویروس می‌تواند آن را پخش کند.

 ویروس کامل را تعریف کنید.
یک ویروس کامل نمی‌تواند وجود داشته باشد. هنگامیکه سیستم عامل و معماری سیستم تغییر می‌کند، معمولاً مشکلات جدیدی با ویروسهای قدیمی بوجود می‌آید.

 در پایان آیا صحبت دیگری دارید؟
خیر.

گزارش اولین گردهمایی سراسری نمایندگان ضدویروس **ایمن**

در حاشیهٔ ششمین نمایشگاه بین‌المللی برق، الکترونیک و کامپیوتر، مدیریت شرکت تصمیم به برگزاری اولین گردهمایی سراسری نمایندگان ضدویروس **ایمن** با اهداف زیر گرفت:

۱ـ ارتباط هرچه نزدیکتر با نمایندگان فروش **ایمن**.

۲ـ دریافت نقطه نظرات نمایندگان در ارتباط با مشکلات مشتریان **ایمن**.

۳ـ ارائهٔ روشهای بهتر در جوابگویی به مشتریان **ایمن**.

بدین منظور در تاریخ ۷۹/۳/۲۶ در مجموعهٔ فرهنگی، ورزشی انقلاب بعد از اتمام نمایشگاه، این گردهمایی برگزار گردید و بعد از قرائت قرآن مجید و خوش‌آمدگویی مدیریت عامل شرکت به میهمانان، آقای مهندس محمدرضازارع در رابطه با مسایل طراحی و برنامه‌نویسی ضدویروس **ایمن** و آقای مهندس حمیدرضا سعدی نیز در مورد تشریح نحوهٔ همکاری و اطلاع‌رسانی به مشتریان صحبتهایی را ارائه کردند. در پایان نیز پس از مراسم اهداء جوایز و صرف شام، تعدادی عکس نیز به یادگار گرفته شد.

انشاءالله بتوانیم همه ساله این گردهمایی را با حضور تعداد بیشتری از نمایندگان داشته باشیم.

📖 📖 📖 📖 📖 📖 📖 📖 📖 📖 📖

خوانندهٔ گرامی:

برای دیدن صفحهٔ ایمن بر روی شبکهٔ جهانی اینترنت به آدرسهای زیر مراجعه نمایید:

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

Imen Anti-Virus

گزارش دومین همایش مدیران کامپیوتر شرکتهای مخابرات سراسر کشور

این همایش در روزهای ۲۹ و ۳۰ شهریورماه ۱۳۷۹ در جزیرهٔ کیش برگزار گردید که از این شرکت نیز در زمینهٔ ویروس ـ ضدویروس ـ بازیابی اطلاعات و امنیت اطلاعات درخواست ارائهٔ مقاله شده بود.

در این همایش که مدیران کامپیوتر شرکتهای مخابرات سراسر کشور و نیز تعدادی از مدیران کل مخابرات حضور داشتند، مقالاتی در زمینه‌های مختلف ارائهٔ گردید.

ارائهٔ دو مقاله از طرف آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن (ICVL) توانست اطلاع‌رسانی کاملتری برای مدیران کامپیوتر شرکتهای مخابرات فراهم آورد و انواع خطراتی که برای اطلاعات می‌تواند بوجود آید و نحوهٔ پیش‌گیری و احتمالاً بازیابی اطلاعات را تشریح کند.

در پایان از دبیر انجمن، جناب آقای مهندس منصور عطایی و سایر دست‌اندرکاران برگزاری همایش کمال تشکر و قدردانی را نموده و امیدواریم در سایر همایش‌های شرکت مخابرات نیز حضور فعالتری داشته باشیم.

ضمناً به کلیهٔ مراکز دولتی که جهت ارتقاء سطح دانش علمی مدیران خود و آشنایی آنان با توانایی‌های موجود در داخل کشور اقدام به برگزاری چنین همایش‌هایی می‌نمایند، آمادگی خود را جهت ارائهٔ مقاله اعلام می‌داریم.

❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖ ❖

DATA Recovery

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

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

شرکت مهندسی مهران رایانه

تلفن: ۶۴۲۳۵۷۷ (سه خط) - نمابر: ۶۴۲۳۴۰۸

بازیابی اطلاعات

آشنایی با گروه‌های ویروس‌نویسی

نام گروه: VLAD

منشأ: استرالیا

وضعیت: منحل شده است

گروهی است که در زمینهٔ تألیف و نویسندگی ویروس فعالیت داشته و حدود ۴۰ ویروس مختلف محصول این گروه می‌باشد. گروهی است با اعضای بین‌المللی، ولی در استرالیا بنیان‌گذاری شده است. در آخرین سال موجودیت این گروه، لیست عضویت آن بارها تغییر کرد. با وجود تعداد زیاد اعضایی که از این گروه کناره‌گیری کردند، چنین به نظر می‌آمد که آخر سال ۱۹۹۶ ، آخر عمر این گروه نیرومند ویروس‌نویسی باشد. بقایای این گروه را می‌توان به صورت مجلهٔ الکترونیکی در سایت این گروه مشاهده کرد. VLAD یعنی Virus Laboratory And Distribution .

اعضای شناخته شدهٔ گذشته و حال این گروه عبارتند از:

1-Metabolis	2-Automag	3-Qark	4-Antigen
5-Darkman	6-Quantum	7- Rhincewind	8-Absolute Overlord
9-Coke	10-Sepultura		

این گروه دارای مجله‌ای الکترونیکی به نام VLAD Magazine است که در تاریخهای زیر منتشر شده‌اند:

۱ ـ جولای ۱۹۹۴

۲ ـ اکتبر ۱۹۹۴

۳ ـ فوریهٔ ۱۹۹۵

۴ ـ آوریل ۱۹۹۵

۵ ـ آگوست ۱۹۹۵

۶ ـ فوریهٔ ۱۹۹۶

۷ ـ AF آوریل ۱۹۹۶

۸ ـ اکتبر ۱۹۹۶

این مجلات شامل مقالات، سورس ویروسها، فوت و فن ویروسها و مصاحبه‌ها می‌باشند. شمارهٔ ششم این مجلات شامل سورس اولین ویروس Windows95 بود که نشریات و ضدویروسها آنرا Boza نامیدند ولی نویسندهٔ این ویروس یعنی Quantum آنرا Biztach می‌نامید. شمارهٔ AF این مجلات در آوریل ۱۹۹۶ نشریه‌ایست فریب‌آمیز که مملو از مطالب ویروسی مرموز است و اولین نشریهٔ این گروه بعد از تغییر ریاست آن از Metabolis به Qark می‌باشد. در اکتبر ۱۹۹۶ نشریهٔ بازنشستگی VLAD Mgazine منتشر شد.

مراکز فروش نرم‌افزار ایمن در داخل کشور

شهرستان	نام نماینده	تلفن	شهرستان	نام نماینده	تلفن
آبادان	اسوه‌پردازش‌اروند	۲۶۹۲۹	دزفول	کامپیوتر خوزستان	۲۳۵۲۹
اراک	آریاسیستم	۴۶۵۲۰	رشت	رایانهٔ سپید رود	۴۸۶۳۲
اردبیل	افق کامپیوتر	۲۲۲۴۴۸۹	زنجان	زنجان پرداز	۴۴۷۳۱۶
اردکان	نوین رایانه	۷۲۲۹۰۸۰	زاهدان	پردازش جنوب	۲۲۵۶۳۰
ارومیه	عصر کامپیوتر	۲۲۴۹۸۹	ساری	کامپیوتر ندا	۲۰۸۶۳
اصفهان	فاراد رایانه پرداز	۶۳۲۳۶۲	سلماس	مرکز توسعهٔ کامپیوتر	۳۱۰۷۹
اهواز	پارس رایانه‌جنوب	۲۱۸۶۶۲	سمنان	سینانگار	۲۲۱۶۱
ایلام	آروین رایانه	۳۳۷۷۳	سنندج	داده‌پردازان کردستان	۶۶۱۲۹۵
بابل	کامپیوتر پویا	۲۲۵۸۹	سیرجان	در رایانه	۳۲۵۷۴
بجنورد	دنیای رایانه	۲۲۳۲۵۲۱	شوش	الکترونیک داریوش	۴۷۱۵
بروجرد	خدمات‌کامپیوتررهاورد	۲۶۴۷۲	شوشتر	همایش رایانه جنوب	۲۷۶۵۳
بندرعباس	ساحل داهیر	۵۵۵۲۸۹	شهرکرد	کامپیوتر آرایه	۳۳۳۶۶۵
بوشهر	بوشهر سیستم	۳۴۴۵۶	شیراز	صبا کامپیوتر	۶۷۷۷۴۴
تبریز	نداپرداز آذر	۵۵۵۱۴۲۴	قائم شهر	کپی کامپیوتر	۴۲۵۸۴
تهران	پانیران	۸۷۷۸۶۵۷	قزوین	مرکز کامپیوتر پگاه	۴۸۷۲۷
تهران	پردازش انفورماتیک	۶۴۱۴۰۶۶	قم	متین پردازش	۹۳۷۸۸۱
تهران	تدارک نرم‌افزار	۶۴۶۰۳۰۳	کرج	صنایع رایانه کرج	۴۳۸۶۳۶
تهران	تکنو ۲۰۰۰ صبا	۶۴۹۸۵۲۳	کرمان	باور الکترونیک	۲۶۴۰۱۲
تهران	خانه نرم‌افزار سپاه	۸۳۰۳۱۴۱	گنبد	کامپیوتر شیما	۲۲۲۶۱
تهران	سرزمین رایانه	۲۰۰۰۱۸۷	مشهد	حساب رایانه	۹۸۹۸۹
تهران	کامپیوتر گویا	۸۸۲۷۴۱۷	هشتگرد	پژوهش رایانه هوشمند	۴۴۰۴
تهران	مهران کامپیوتر	۸۹۰۷۵۳۳	همدان	نوین رایانه	۸۲۶۴۵۳۵
خرم‌آباد	تکنوشارپ	۴۴۳۳۰۱	یاسوج	بهینه یاسوج	۲۵۳۵۴
خوی	نیک افزار	۲۲۲۰۶۱۰	یزد	خدمات‌کامپیوتری ارس	۶۶۴۶۴۶
دامغان	کیهان کامپیوتر	۸۱۸۲			

نمایندگیهای خارج از کشور

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