سال دوم / شماره ۷ / پاییز ۱۳۸۰ / ۲۴ صفحه / ۱۰۰ تومان

مسابقهٔ شمارهٔ ۷ ایمن

صفحهٔ ۱۲

دعوت به همکاری

صفحهٔ ۱۸

- مصاحبه با Stealth Warrior
- نرم‌افزار تولید ویروس DW97MVCK
- سرقت‌های هزارهٔ سوم
- آشنایی با گروه ویروس‌نویسی SLAM

آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن

بسمه تعالی

خبرنامهٔ تخصصی **ایمن** ۷

سال دوم/شمارهٔ هفتم
پاییز ۱۳۸۰/۲۴ صفحه

فهرست مطالب

سرمقاله ..... صفحهٔ ۳
مصاحبه با ویروس‌نویسان بزرگ (Stealth Warrior) ..... صفحهٔ ۵
جدول ویروس‌های گزارش شده در نقاط مختلف دنیا **WILD LIST** ..... صفحهٔ ۱۰
دستگیری دو قفل‌شکن توسط پلیس ۱۱۰ ..... صفحهٔ ۱۱
مسابقهٔ شمارهٔ ۲ **ایمن** ..... صفحهٔ ۱۲
آشنایی با نرم‌افزار تولید ویروس DW97MVCK ..... صفحهٔ ۱۳
آشنایی با گروه‌های ویروس‌نویسی (گروه SLAM) ..... صفحهٔ ۱۵
سرقت‌های هزارهٔ سوم ..... صفحهٔ ۱۶
متن انگلیسی ..... صفحهٔ ۲۲
جدول نمایندگی‌های فروش ضدویروس **ایمن** ..... صفحهٔ ۲۳

« تذکر »

- ✓ استفاده از مقالات این خبرنامه با ذکر منبع خبر بلامانع 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 ایمن
ICVL

تهران ـ خیابان جمهوری اسلامی ـ بین جمالزاده و کارگر ـ شماره ۳۷۱ ـ طبقه چهارم ـ شرکت مهندسی مهران رایانه

آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن

واحد خبرنامهٔ تخصصی ایمن

تلفن: ٦٤٢٣٥٧٧ (٦ خط) ـ نمابر: ٦٤٢٣٤٠٨

بسم الله الرحمن الرحیم

سرمقاله

هر بار که انتشار خبرنامه به تأخیر می‌افتد، این نگرانی را داریم که چگونه این مطلب را به خوانندگان عزیز بگوییم تا از طرف آنان مورد مؤاخذه قرار نگیریم. فکر می‌کنم بهترین راه گفتن دلیل این تأخیر به صورت صادقانه است. راستش مواجه شدن با ارائهٔ نسخهٔ جدید نرم‌افزار **ایمن** و همچنین پاره‌ای نقل و انتقالات در محل آزمایشگاه تحقیقات ویروس‌های رایانه‌ای **ایمن** باعث این تأخیر شد که بابت آن از تمامی خوانندگان معذرت‌خواهی می‌کنیم.

در چند ماهد اخیر اتفاقاتی افتاده است که لازم می‌دانیم به آنها اشاره کنیم. یکی از این اتفاقات حمله به برج‌های دوقلوی تجارت جهانی در آمریکا بود که تأثیر بسیاری در دنیا و نیز دنیای کامپیوتر داشت. بعد از این واقعه و تبلیغات زیادی که در ارتباط با آن بر علیه مسلمانان انجام گرفت موج حملات به مسلمانان از طریق اینترنت را افزایش داد. بسیاری از سایت‌های مربوط به مسلمانان توسط نفوذگرها، مورد حمله قرارگرفته و مختل شد و ویروس‌هایی نیز علیه آنان نوشته شد. لذا به تمامی کاربران توصیه می‌شود در هنگام استفاده از اینترنت بسیار مراقب باشند، e-mail هایی که منتظر آن نبوده‌اید و یا فرستندهٔ آنها را نمی‌شناسید به هیچ وجه باز نکرده و آنها را معدوم کنید. البته بهتر است قبل از معدوم نمودن آنها با ما تماس گرفته و یا آنها را برای ما ارسال نمایید.

خبردیگری که اخیراً همه جا شنیده می‌شود، خبر ورود Windows XP وتبی است که برای استفاده از آن در بین کاربران کامپیوتر شیوع پیدا کرده‌است. در این مورد هم لازم دیدیم که مطلبی را به عرض خوانندگان برسانیم و آن اینکه برای رجیستر شدن و برای اینکه شرکت ماکروسافت شما را به‌عنوان یک کاربر معتبر بشناسد، در سرویس رجیستر خود این امکان را قرار داده است که تمام اطلاعات کاربر، برای تشخیص معتبر بودن وی بر روی سرورهایش

Download شود. از طرف دیگر بعد از وقایع آمریکا، دولت این کشور به FBI رسماً اجازه داد که برای پیشگیری از اعمال مشابه تروریستی، از طریق اینترنت جاسوسی نماید. با کنار هم گذاشتن دو مطلب فوق به راحتی می‌توان خطر را احساس کرد. بنابراین به کاربران علی‌الخصوص مراکز دولتی، نظامی و بازرگانی توصیه می‌شود که نسخه‌های Windows خود را به هیچ وجه به Windows XP ارتقاء نداده و از همان Windows98 استفاده نمایند تا امکان خطرات فوق به حداقل برسد.

سخن آخر اینکه باز هم از تأخیر در انتشار خبرنامه پوزش می‌خواهیم و موفقیت تمامی شما عزیزان را از خداوند منان خواستاریم.

با سپاس

مسئول واحد خبرنامهٔ تخصصی **ایمن**

علاقمندان می‌توانند جهت دریافت شماره‌های بعدی این خبرنامه، کپی فرم مشخصات زیر را به دفتر خبرنامه به آدرس: تهران ـ خیابان جمهوری اسلامی ـ بین جمالزاده و کارگر ـ شمارهٔ ۳۷۱ ـ طبقهٔ چهارم ـ شرکت مهندسی مهران رایانه ـ **آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن ـ واحد خبرنامهٔ تخصصی ایمن** ارسال نمایند.

حقوقی/ نام سازمان یا شرکت: .....

حقیقی / نام و نام خانوادگی: .....

سمت: ..... میزان تحصیلات: .....

آدرس: .....

.....

شمارهٔ تماس: ..... نمابر(فاکس): .....

آدرس پست الکترونیکی(E-Mail): .....

آخرین شمارهٔ خبرنامه که در اختیار دارید: ..... مهر / امضاء

مصاحبه با ویروس‌نویسان بزرگ

مصاحبه با Stealth Warrior :

- *شما چگونه با کامپیوترها آشنا شدید؟*

من اولین کامپیوترم را وقتی که چهار ساله بودم، خریدم. کامپیوتر من یک کمودور ٦٤ بود و من در ابتدا با آن فقط بازی می‌کردم اما بعداً شروع به برنامه‌نویسی با زبان بیسیک نمودم. پنج سال بعد من اولین کامپیوتر شخصی‌ام را خریدم و به برنامه‌نویسی با زبان بیسیک ادامه دادم. سپس چیزهایی از زبان پاسکال و C و همچنین اسمبلی فرا گرفتم.

- *چطور و چه زمانی با دنیای ویروس‌ها آشنا شدید؟*

در سال ۱۹۹٦ وقتی که من به اینترنت دسترسی پیداکردم با دنیای ویروس‌ها آشنا شدم. در ابتدا تمام نرم‌افزارهای تولید ویروس را Download نموده و مدتی با آنها بازی کردم. سپس مطالبی را در مورد ویروس‌ها پیدا کردم و تصمیم گرفتم که چیزهایی در مورد ویروس‌نویسی یاد بگیرم. بنابراین این کار را انجام دادم. سپس به گروه Alliance (RIP) پیوستم و در حال حاضر در گروه SLAM می‌باشم. من دوست دارم دانشم را در اختیار دیگران بگذارم لذا مطالبی آموزشی در مورد ویروس‌ها می‌نویسم.

- *آیا شما ویروسی نوشته‌اید؟ اگر نوشته‌اید چه اعتباری می‌خواهید در این زمینه کسب کنید؟*

بله من ویروس‌هایی نوشتم. بیشتر به خاطر اینکه دانسته‌هایم را بعد از یاد گرفتن چیزهای جدید آزمایش کنم مانند ویروس‌های رونویس، ویروس‌های آلوده‌کنندهٔ فایل‌های COM ، ویروس‌های آلوده‌کنندهٔ فایل‌های EXE و .... بنابراین به جز مطالب آموزشی، چیز دیگری برای کسب اعتبار نیست.

- *شما چگونه ویروس‌هایتان را نام‌گذاری می‌کنید؟*

برای این کار قاعدهٔ خاصی وجود ندارد. ویروس‌های آزمایشی من دارای نام‌های مسخره‌ای هستند مانند COMmander (برای ویروس‌هایی که به فایل‌های COM اضافه می‌شوند)، EXEcutor (برای ویروس‌هایی که به فایل‌های EXE اضافه می‌شوند) و Shredder (برای ویروس‌های رونویس).

- *با کدامیک از زبانهای برنامه‌نویسی آشنا هستید؟*

من بیسیک را خیلی خوب می‌شناسم و مقداری هم پاسکال و C و البته اسمبلی.

- *از کدام زبان برنامه‌نویسی دوست دارید بیشتر استفاده کنید؟*

بستگی دارد. وقتی می‌خواهم یک برنامهٔ کمکی و یا برنامه‌هایی برای مدرسه بنویسم، از پاسکال یا C استفاده می‌کنم. اما برای ویروس‌نویسی صددرصد از اسمبلی استفاده می‌نمایم.

- *آیا شما عضو یکی از گروه‌های ویروس‌نویسی هستید؟*

بله. من یکی از اعضای گروه SLAM هستم.

- *شما در زمینهٔ ویروس‌نویسی چه هدفی را دنبال می‌کنید؟*

جواب دادن به این سئوال سخت است ! من دوست دارم بر تمام گستره‌های ویروس‌نویسی مانند مقیم شدن در حافظه، مخفی کاری، چند شکلی، کد کردن، آلوده‌سازی Partition Table و... تسلط پیدا کنم.

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

من به این مطلب اعتنایی نمی‌کنم. تا وقتی که مردم بتوانند نسخه‌های جدید نرم‌افزارهای ضدویروس را به طور رایگان Download کنند، برای من کافی است. مردم خواستار امنیت هستند اما به صورت رایگان ! اگر ما می‌توانیم به صورت رایگان ویروس بنویسیم، ضدویروس‌نویس‌ها هم می‌توانند برنامه‌های ضدویروس را به صورت رایگان بنویسند. بگذارید ببینیم چه کسی می‌تواند بیشتر دوام بیاورد.

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

من مطالب اندکی را در مورد هواپیماها می‌دانم و ایدهٔ هواپیماهای مخفی کار مانند B2 یا F117 را دوست دارم. وقتی من در زمینهٔ ویروس‌ها شروع به کار کردم، تعداد زیادی از ویروس‌ها را دیدم که دارای تکنیک‌های مخفی‌کاری بودند. بنابراین من برای خودم نام Stealth Fighter (جنگندهٔ مخفی‌کار) را فرض می‌کردم. اما از آنجایی که این نام توسط شخص دیگری (فکر می‌کنم یکی از اعضای گروه NuKE) برگزیده شده بود، لذا نام Stealth Warrior (جنگجوی مخفی‌کار) را برای خودم انتخاب کردم که معنی آن تقریباً همان می‌شود.

- *نظر شما دربارهٔ نرم‌افزارهای تولید ویروس مانند (VCL، PS-MPC و...) چیست؟*

آنها می‌توانند مفید باشند، اما بدون دانشی از اسمبلی شما نمی‌توانید خیلی پیشرفت کنید و بدتر اینکه شما نمی‌توانید برنامهٔ ایجاد شده را بفهمید. هیچ چیز بدتر از این نیست که چیزی را کامپایل کنید که آن را نمی‌فهمید.

- *نظر شما دربارهٔ ویروس‌های ماکرو در مقابل ویروس‌های نوشته شده به زبان اسمبلی یا زبانهای سطح بالا چیست؟*

من چیزی در مورد ویروس‌های ماکرو نمی‌دانم. تا به حال نیز ویروس ماکرویی ننوشته‌ام. اما ویروس‌های تمیزی با ایده‌های خوب در این زمینه دیده‌ام و آنها بسیار سریع تکثیر می‌شوند. اما در مورد ویروس‌های نوشته شده به زبانهای سطح بالا (پاسکال/C /...) : من فکر می‌کنم که کار بر روی آنها تلف کردن زمان می‌باشد. اسمبلی یاد بگیرید!

- *آیا تا به حال یکی از ویروس‌هایتان را در دنیای کامپیوترها منتشر کرده‌اید؟*

خیر. من ویروس‌هایم را پخش نمی‌کنم و آنهایی را که در مطالب آموزشیم قرار می‌دهم بسیار ساده هستند تا برای هر کسی کاملاً مشخص باشد. من می‌دانم که تکثیر ویروس‌ها ممنوع است و من به قانون احترام می‌گذارم. من ویروس‌ها را برای آزمایش مهارت خودم می‌نویسم نه برای آلوده کردن انسان‌های بیگناه.

- *نظر شما در مورد اثرات مخرب در ویروس‌ها چیست؟*

من با اثرات مخرب تا وقتی که منتشر نشوند، مشکلی ندارم. ویروس‌هایی که از این روش‌ها استفاده می‌کنند خیلی دوام نمی‌آورند.

- *آیا به نظر شما چیزی بعنوان ویروس « خوب » وجود دارد؟*

فکر نمی‌کنم چنین چیزی وجود داشته باشد. باید دلیل خوبی برای افزایش طول فایل وجود داشته باشد و من تا به حال چنین دلیلی را نیافته‌ام.

- *شما در زندگی حقیقیتان چکار می‌کنید؟*

برای درس خواندن به مدرسه می‌روم، تنیس و بسکتبال بازی می‌کنم، با کامپیوتر کار می‌کنم... یک شخص کاملاً عادی و بر خلاف چیزی که ضدویروس‌نویسان دربارهٔ ویروس‌نویسان می‌گویند، من کند ذهن و غیر اجتماعی نیستم. من یک دانش‌آموز ممتاز هستم.

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

بله. آنها تا وقتی که من کامپیوترهایشان را آلوده نکنم به این موضوع اهمیتی نمی‌دهند.

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

من کارهایی مانند نفوذگری، قفل‌شکنی یا کپی‌برداری از نرم‌افزارها را انجام نمی‌دهم چون این کارها غیرقانونی هستند. من بازی‌های کامپیوتری را برای استراحت انجام می‌دهم و برنامه‌نویسی می‌کنم.

- *آیا ویروس‌ها باید غیرقانونی باشند؟ آیا فرقی بین تولید ویروس و انتشار آن وجود دارد؟*

نوشتن یک ویروس نباید غیرقانونی باشد. بین تولید ویروس و انتشار آن تفاوت وجود دارد همانطور که بین دادن ویروس به فردی که آن را برای یادگیری می‌خواهد و کسی که آنها

را نمی‌خواهد تفاوت وجود دارد. دومین مورد باید ممنوع باشد ولی بقیهٔ موارد خیر.

- *ویروس کامل را تعریف کنید.*

ویروس کامل اینچنین است: آلوده کنندهٔ Partition Table ، فایل‌های COM ، فایل‌های EXE ، فایل‌های SYS ، فایل‌های EXE ی Win3.x و Win9x ، فایل‌های DOC با قابلیت‌های مخفی‌کاری، چندشکلی، ضد نرم‌افزارهای ضدویروس با روتین‌های فعال‌سازی قوی و قابلیت پاکسازی مشکل.

- *نظر شما در مورد Windows(95/98) چیست؟*

من از آنها نفرت دارم و از آنها استفاده نمی‌کنم. من از DOS ، OS/2 و لینوکس استفاده می‌کنم. شما باید حتماً لینوکس را امتحان کنید. شما عاشق آن خواهید شد! از بین سیستم عامل‌های تجاری OS/2 نسبت به بقیه (البته به جز Unix تجاری) از جمله Windows 95 و Windows NT برتری دارد.

- *نصیحت شما به کسانی‌که در این زمینه تازه شروع به کار کرده‌اند چیست؟*

یک کتاب خوب در مورد اسمبلی تهیه کنید و آن را یاد بگیرید. از هر مطلب آموزشی که می‌توانید کمک بگیرید. ابتدا در زمینه‌های ابتدایی (رونویسی، ویروس‌های اضافه شونده به فایل‌های COM و EXE) و سپس در زمینه‌های پیشرفته (ویروس‌های مقیم در حافظه، کد کردن و ...) کار کنید.

- *چگونه می‌توان به شما دسترسی پیدا کرد؟*

من از طریق e-mail با آدرس stealthwarrior@hotmail.com در دسترس خواهم بود.

- *در پایان آیا صحبت دیگری دارید؟*

مطلب دیگری نیست.

جدول ویروس‌های گزارش شده در نقاط مختلف دنیا WILDLIST

WildList تهیه شده در این شماره مربوط به ماه‌های ژوئن تا اکتبر می‌باشد. با بررسی این جدول مشاهد می‌شود که ویروس‌های اسکریپتی روز به روز کمتر می‌شوند. ذکر این نکته نیز لازم است که بر خلاف تعداد بیشتر ویروس‌های ماکرو نسبت به ویروس‌های فایلی، شیوع ویروس‌های فایلی که اغلب از طریق اینترنت منتشر می‌شوند به مراتب نسبت به ویروس‌های ماکرو بیشتر است.

در حال حاضر آخرین نسخهٔ نرم‌افزار ضدویروس **ایمن** (نسخهٔ ۸۰/۷) از ویروس‌های موجود در این جدول توانایی شناسایی و پاکسازی ویروس‌های VBS/Happytime ، VBS/LoveLetter ، VBS/AnnaKournikova ، W32/Magister.B ، W32/Nimda و W32/SirCam را که در ایران شیوع یافته‌اند دارا می‌باشد.

نوع	نام ویروس	نوع	نام ویروس
ماکرو	W97M/Ethan.AW	اسکریپت	VBS/AnnaKournikova
ماکرو	W97M/Flop.A	اسکریپت	VBS/Happytime
ماکرو	W97M/Hope.A	اسکریپت	VBS/LoveLetter
ماکرو	W97M/Marker	فایل	W32/Apost.A
ماکرو	W97M/Melissa.U	فایل	W32/Choke
ماکرو	W97M/Nottice.AU	فایل	W32/Hai.A
ماکرو	W97M/Ostirch.B	فایل	W32/Magistr.B
ماکرو	W97M/Pecas.B	فایل	W32/Nimda
ماکرو	W97M/Shepmah.A	فایل	W32/SirCam
ماکرو	W97M/Thus	فایل	W95/Linong.A
ماکرو	X97M/AND.B	ماکرو	W97M/Bottra.A
ماکرو	X97M/Squared.B	ماکرو	W97M/Class.BT

دستگیری دو قفل‌شکن توسط پلیس ۱۱۰

متأسفانه در روز یکشنبه مورخ ۷۹/۱۲/۱٤ دو نفر به عنوان ویزیتور با ارایهٔ یک لیست ٦۳ ردیفه و قیمت‌های بسیار پایین، اقدام به نشر و عرضهٔ نرم‌افزارهای تولید داخل کشور به صورت قفل شکسته کردند.

خوشبختانه فروشندگان متعهد بازار رضا با اطلاع‌رسانی به موقع به پلیس ۱۱۰ نیروی انتظامی توانستند افراد مذکور را دستگیر کرده و به کلانتری ۱۰۷ میدان فلسطین منتقل کنند و متهمین شب را در بازداشت بسر بردند و پرونده‌ای نیز با شمارهٔ ٤۰۸-۳٦ تشکیل شده و به شعبهٔ ۳ مجتمع قضایی امام خمینی (ره) ارجاع داده شد.

در حال حاضر ٥ شرکت اقدام به شکایت کرده‌اند که عبارتند از مهران رایانه، CD Center، پژوهش نوین، مهر ارقام رایانه و پایا سیستم مرو و پروندهٔ مذکور در جریان می‌باشد.

➢ ⅄ ≺ ⅄ ➢ ≺ ⅄ ➢ ⅄ ≺

در صورت یافتن هرگونه ویروس جدید و یا وجود هر نوع فایل مشکوک، با آزمایشگاه تحقیقات ویروس‌های رایانه‌ای **ایمن** (ICVL) و یا با آدرس‌های الکترونیکی زیر تماس بگیرید:

info@ImenAntiVirus.com
imen_av@yahoo.com

خوانندهٔ گرامی:

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

www.ImenAntiVirus.com
www.geocities.com/imen_av

مسابقهٔ شمارهٔ ۲ ایمن

دوستان عزیز! پاسخ دهید و جایزه بگیرید!

به نظر شما یک نرم‌افزار ضدویروس خوب باید دارای چه خصوصیاتی باشد؟

پاسخ سؤال فوق را در فرم زیر نوشته و پس از تکمیل آن برای ما بفرستید تا از جوایز ما برخوردار شوید.

(در صورت طولانی بودن پاسخ، لطفاً آن را در یک برگهٔ مجزا نوشته و به فرم پاسخنامه ضمیمه نمایید.)

☆ یک عدد ساعت دیواری + یک سال اشتراک رایگان ماهنامهٔ کامپیوتر و ارتباطات + ☆

یک سال اشتراک رایگان ویروس‌یاب **ایمن** + اشتراک رایگان خبرنامهٔ تخصصی **ایمن** برای نفر اول

☆ ۹ عدد ساعت دیواری + یک سال اشتراک رایگان ویروس‌یاب **ایمن** + ☆

اشتراک رایگان خبرنامهٔ تخصصی **ایمن** برای ۹ نفر

☆ ۲۰ عدد تی‌شرت + یک سال اشتراک رایگان ویروس‌یاب **ایمن** + ☆

اشتراک رایگان خبرنامهٔ تخصصی **ایمن** برای ۲۰ نفر

مهلت ارسال : انتهای ماه تیر سال ۱۳۸۱

نشانی ما :

تهران ـ خیابان جمهوری اسلامی ـ بین جمالزاده و کارگر ـ شمارهٔ ۳۷۱ ـ طبقهٔ اول ـ شرکت مهندسی مهران رایانه

آزمایشگاه تحقیقات ویروس‌های رایانه‌ای ایمن ـ واحد خبرنامهٔ تخصصی ایمن

✂ -

پاسخ مسابقهٔ شماره ۲ : .....

.....

.....

.....

.....

.....

نام و نام خانوادگی : .....

میزان تحصیلات : .....

آدرس : .....

.....

شمارهٔ تماس : ..... مهر/امضاء

آشنایی با یک نرم‌افزار تولید ویروس

نام : DarkChasm's Word 97 Macro Virus Construction Kit

تولیدکننده/ ملیت : DarkChasm / آمریکا

نام اختصاری : DW97MVCK

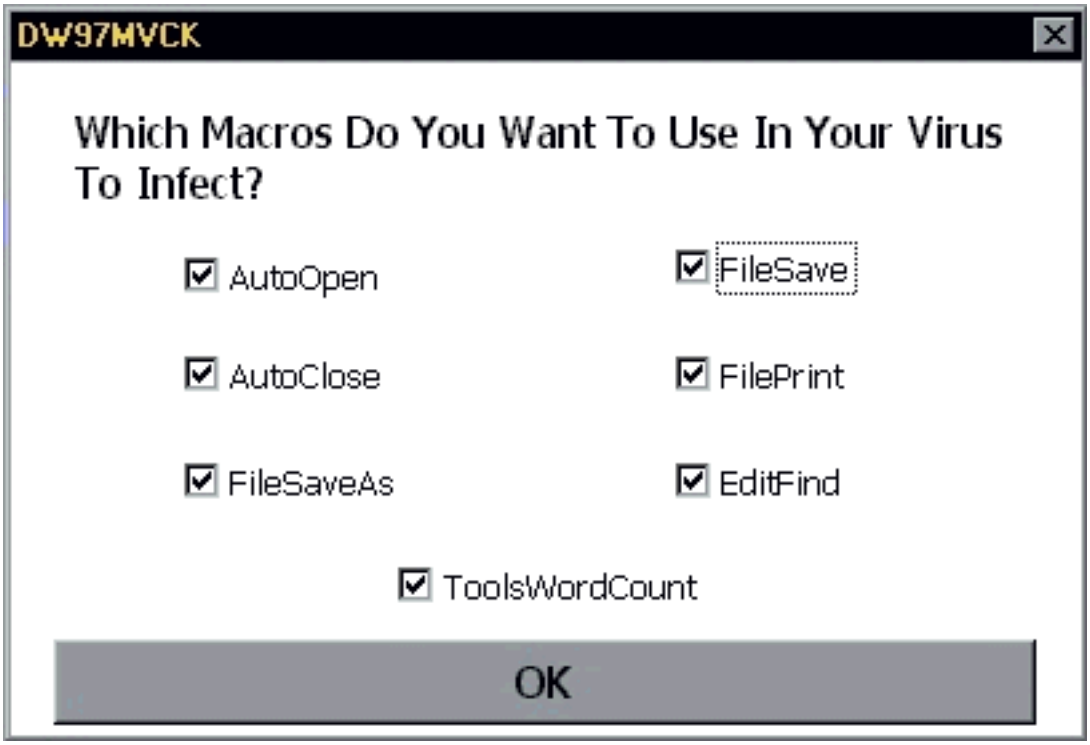
نوع : نرم‌افزار تولید ویروس

نسخه‌های شناخته شده : DW97MVCK 1.0 ـ ژوئن ۱۹۹۷

خصوصیات:

این نرم‌افزار گونهٔ دیگری از تولید کنندهٔ ویروس‌های ماکرو است که به طور خاص برای تولید ویروس‌های ماکرو Word 97 (VBA) نوشته شده است. خود این نرم‌افزار مانند بیشتر دیگر نرم‌افزارهای تولید کنندهٔ ویروس ماکرو، یک ماکروی بزرگ است.

صفحهٔ اصلی این نرم‌افزار به شکل زیر می‌باشد:



چندین گزینهٔ مختلف ازجمله قابلیت مخفی‌کاری، اثرات تخریبی و نمایشی، ماکروهای مورد استفاده و... توسط کاربر قابل انتخاب می‌باشند. برای پشتیبانی یک تابع چندشکلی (Polymorphic) ، امکان استفاده از موتور چندشکلی APMRS که توسط Pyro (یک ویروس‌نویس عضوگروه VBB) نوشته شده است، گنجانده شده و توسط کاربر قابل انتخاب می‌باشد.

خصوصیات فراوانی وجود دارد که برنامهٔ DW97MVCK می‌تواند برای ساخت ویروس‌ها از آنها استفاده نماید که عبارتند از:

- ٤ عدد ماکرو مخصوص مخفی‌کاری
- در حال حاضر یک موتور چندشکلی
- ۷ اثر تخریبی یا نمایشی
- ۷ ماکروی آلوده‌سازی

البته شما می‌توانید هر ترکیبی را با هم ادغام کنید، که در کل می‌توان ۱۰۰ ترکیب مختلف را بدست آورد.

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 اول ـ شرکت مهندسی مهران‌رایانه ـ **آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن**

واحد خبرنامهٔ تخصصی ایمن

تلفن: ٦٤٢٣٥٧٧ (شش خط)

نمابر: ٦٤٢٣٤٠٨

آدرس e-mail :

info@ImenAntiVirus.com
imen_av@yahoo.com

آشنایی با گروه‌های ویروس‌نویسی

آشنایی با گروه SLAM

نام: SLAM

منشأ: بین‌المللی

وضعیت: منحل شده

یک گروه با بنیان اینترنتی که در اواخر سال ۱۹۹۶ از بین چندین گروه دیگر ظهور کرد. اعضای خارج شده از گروه VBB در این گروه یک خانهٔ جدید برای خود یافتند. هرچند که این گروه در ابتدا با تأکید بر ویروس‌های ماکرو شروع به کار کرد، ولی نشریهٔ شمارهٔ ۳ این گروه به نام SLAM نشان داد که این گروه ویروس‌های متداول بسیاری را در برمی‌گیرد. اطلاعات بیشتر در مورد این گروه محدود است.

آرم این گروه به شکل زیر می‌باشد:

اعضای شناخته شدهٔ حال و گذشتهٔ این گروه عبارتند از:

Neophyte	Nightmare Joker	Underground Prophet
Cyborg	Aurodreph	Phardera
DarkChasm	Cursor Luxor	CyberYoda
Lone Rider	Casio / Raid	Dark Chakal
Darkside1	Virtual Daemon	Lord Of Navan
Sir Death Knight	Hyperlock	Stealth Warrior
Kid Chaos	Trigger	Darx Kies
Forms	Shaitan	Yesna
Blue Skull	Lord Julus	

این گروه دارای نشریه‌ای به نام SLAM می‌باشد.

سرقت‌های هزارهٔ سوم

در چند قرن پیش معمول بود که راهزن‌ها سر گردنه‌ها به کمین کاروان‌ها می‌نشستند تا بتوانند بدین وسیله برای خود درآمدی کسب کنند که البته هیچگاه با یکبار لخت کردن کاروانی زندگیشان از این رو به آن رو نمی‌شد و در نتیجه راهزن‌ها همواره افرادی با سابقه‌کار بالا (حتی بیش از ۳۰ سال که مصادف با شروع بازنشستگی است) بودند. در قرن گذشته اینگونه سرقت‌ها به تناسب بزرگ شدن شهرها و عدم شناخت همهٔ شهروندان توسط یکدیگر، به داخل شهرها گسترش پیدا کرد و حتی راحتی کار راهزن‌ها را نیز به همراه داشت چراکه راهزن‌های سرگردنه به نوعی باید از جان شیرین خود در سرما وگرما می‌گذشتند تا شاید یک درهم و یا دیناری بدست آورند و اگر به دام می‌افتادند نیز به خاطر آن یک درهم و دینار سر خود را از دست می‌دادند. ولی در شهرها اینگونه نبود و بسته به میزان سرقت، خاطی گوشمالی داده می‌شد.

حال هزارهٔ سوم با تمام وسایل IT خود به جوامع عرضه شده است و در نتیجه جهت سرقت ابزاری یافت می‌شود که حتی به راه رفتن نیز نیاز ندارد و به راحتی با زدن چند کلید و شماره می‌توان ثروتی افسانه‌ای را به چنگ آورد و تازه نیاز به سابقه کار بالا نیز نمی‌باشد. ولی در کنار این مسأله قانون نیز ظهور پیدا کرده است تا جوامعی که در محدودهٔ قانون زندگی می‌کنند به نوعی از حرکت‌هایی از این دست در امان باشند و اینکه قانون تا چه اندازه برای مجرمین دندان تیز کرده است خود برمی‌گردد به اهمیتی که قانون به روابط اجتماعی و اقتصادی سالم می‌دهد.

حال چه شده است؟ از قرار معلوم دو نفر از همین سارقین هزارهٔ سوم که احتمالاً سنوات خدمتی‌شان نزدیک به صفر بوده است، خواسته‌اند عنوان اول را در ایران به خود اختصاص دهند و در نتیجه در اسفند سال ۱۳۷۹ با یک چمدان پر از لیست قیمت نرم‌افزارهای تولید داخلی (۶۳ عنوان نرم‌افزار) از پایانهٔ مسافربری شهر خود بلیط تهیه کرده‌اند و با هزاران

فکر بکر وامید و آرزو قبول زحمت کرده و به مهد تولید نرم‌افزارهای فارسی که همان تهران خودمان است آمده‌اند و چون از سوابق خدمتی در این حرفه محروم بوده‌اند، یک راست رفته‌اند سراغ بازار با سابقهٔ رضا و شروع به معرفی خود و محصولات تکثیری (غیر مجاز) خود با قیمت‌های باورنکردنی (تا ۹۵٪ زیر قیمت نسخهٔ اصلی) کرده‌اند.

یکی از بزرگان تجار این بازار آنان را نصیحت پدرانه کرده که اگر می‌خواهید در جا همه را بفروشید بروید سراغ فلان مفاخرالتجار بازار، که از قضا ایشان نیز خود تولید کنندهٔ ۷ قلم از ۶۳ قلم لیست مربوطه بود!!!

جالب است بدانید که این دو عزیز بی‌خبر از همه جا مجبور شدند کل بروشورهای خود را یک راست تقدیم پلیس ۱۱۰ که از بدو تولد همواره اخبار خوشحال کننده‌ای برای جامعهٔ ما به ارمغان آورده‌است، بکنند.

حال یک سؤال باقی می‌ماند و آن اینکه در هزارهٔسوم سارقین در مطالبات خود از پول نقد دست دوم نام می‌برند و از پول‌های نو وتا نشده و همینطور چک و سایر ابزارهای الکترونیکی پرداخت پول به شدت اجتناب می‌کنند و سعی می‌کنند هیچگونه ردپایی از خود بر جای نگذارند. ولی این آقایان گرفتار شده با لیستی به بازار آمده که شمارهٔ تماس تلفن نیز دارد و اعلام آمادگی برای سایر جرایم را نیز در آن اظهار کرده‌اند. نتیجه اینکه اینان حداقل مسائل هزارهٔ سوم را درک نکرده‌اند و از روابط اجتماعی هزارهٔ سوم به دور بوده‌اند و قطعاً باید در مراکز تربیت بزه‌کاران کلاس‌هایی برای اینان ترتیب داد.

حال ما چه آشی برایشان پخته‌ایم. پرونده تشکیل شد و یک وکیل مجرب نیز در این امور بکار گرفته شد که متعاقباً اعلام انزجار عمومی نسبت به این عمل متخلفین را نیز توسط کلیهٔ دست‌اندرکاران مربوطه را به همراه داشت. همچنین متهمین از این عمل خود اظهار ندامت کردند که امیدواریم عبرتی شود برای سایرین تا بدانند که قانون حمایت از پدیدآورندگان نرم‌افزار که در دی ماه ۱۳۷۹ به تصویب رسیده است، از این به بعد پشتوانهٔ محکمی است برای کلیهٔ متخصصان این صنعت تا بتوانند با فراق خاطر نسبت به تولید نرم‌افزار در داخل کشور همت بگمارند.

در پایان امیدواریم که قانون جدید بتواند جلوی فرار مغزها را به خارج از کشور تا حدودی بگیرد و کسانی که تاکنون با توان فکری خود در جهت مخالف این قانون قدم برمی‌داشتند به سر عقل آمده و سعی کنند در جهت مصالح کشور، به جای جرم IT تولید IT داشته باشند.

آگهی دعوت به همکاری

بدینوسیله از تمامی کسانی که در زمینهٔ ویروس‌های کامپیوتری علاقمند بوده و به System Programming و Windows Programming تسلط دارند، دعوت به همکاری می‌گردد. لذا از کلیهٔ علاقمندان تقاضا می‌شود در یک صفحه به موارد زیر پاسخ گفته و به آدرس ما ارسال نمایند. پس از بررسی تقاضاهای رسیده در آزمایشگاه تحقیقات ویروس‌های رایانه‌ای ایمن، هماهنگی‌های بعدی از سوی این آزمایشگاه انجام خواهد گرفت.

- نام و نام خانوادگی.....
- رشتهٔ تحصیلی و میزان تحصیلات.....
- محل اخذ مدرک تحصیلی.....
- سن - وضعیت تأهل.....
- سوابق کاری.....
- آدرس محل سکونت.....
- شماره تماس (الزامی).....

means that anti-virus products have more problems detecting and removing these viruses.

Visual Basic macros are represented by two different entities - by a compiled macro body and compressed macro text (both are usually present in OLE2 files containing macros). When the macro text is modified, the macro body is re-compiled from it. Usually both instances of a macro contain the same information (but one is used by the Visual Basic editor, another by the Visual Basic interpreter). If there is corruption, however, this may not be true. For example, even if the macro text is missing, the compiled macro body could still be executed. Scanners should (and most of them do) rely on the compiled body, as this is the real executable macro code. Poor scanners use the macro text to detect viruses. This is easier, but it is less reliable (it is prone to miss the viable viruses if corruption to the macro text occurs).

Under Office 97, all major applications use the same macro language. This means that cross-application viruses are possible. Moreover, PowerPoint 97 (these files have the extension PPT) can now contain macros (this was not the case in previous versions of PowerPoint).

The Office 97 version of Excel for Windows is able to save spreadsheets in the old VBA3 format. This means that macro viruses in VBA5 format can be 'down-converted' back to VBA3 format. It is even possible to have both VBA3 and VBA5 incarnations of the macros in a single spreadsheet file. Such a file is readable by both old and new versions of Excel and contains two viruses. 'Down-converted' viruses can be 'up-converted' again; and this process (VBA5->VBA3->VBA5) does not necessarily result in exactly the same virus body - it is known that the formatting (spaces, tabulation, etc.) of the virus may change. That is why, if VBA5 viruses are to be identified properly, these variable parts of the macro code should be ignored.

In Office 97, all applications use the same macro language - VBA5 (Visual Basic for Applications, version 5). Word for Windows 8.0 (the version included in Office 97) has the ability to convert (re-compile) old macros into this new language. Many viruses can be re-compiled in this way, resulting in completely different viruses. However, sometimes these viruses are not viable, as the converter's success rate has been estimated by Microsoft at about 90%. Moreover, Microsoft included within the converter some sort of detection of the most common macro viruses, to prevent their re-compilation (so that, for example, some of the most common macro viruses like WM/Concept.a, WM/Wazzu.a and WM/Npad.a are not converted). Unfortunately, this feature was not included in the beta release of Office 97; and several macro viruses were 'up-converted' to the new format.

Another feature of Word for Windows 8.0 is that it produces a warning if the user tries to load a document which contains macros. It displays a dialog-box which says, 'The document you are opening contains macros or customizations. Some macros may contain viruses that could harm your computer. '. It then offers three options:

1. Disable Macros [default]
2. Enable Macros
3. Do Not Open

This warning can be turned off, so that it will never appear again.

VBA5 is a much more complex language than WordBasic (in fact, it includes WordBasic as a subset of its commands) and its data is stored within a file in much more complex way (as many multi-level streams, containing lots of cross-references). This means that more complex macro viruses can be written (all existent Office 97 viruses are still similar to their WordBasic predecessors; even those which are not simply 'up-converted' from their WordBasic counterparts). This also

'mated' viruses do exist and they replicate without problem, using macros taken from other macro viruses.

Macro viruses can also take macros from a set of legitimate macros in NORMAL.DOT. For example, many known macro viruses are the result of 'mating' between the ScanProt macro (an anti-WM/Concept macro released by Microsoft) and a macro virus.

Devolving

Some viruses are badly-written and 'lose' their own macros. For example, the original virus may consist of the set: {AutoOpen, FileSave, FileSaveAs}. If it replicates via AutoOpen, the complete macro set will be preserved. However, if the user invokes File | SaveAs, the virus will fail to copy the FileSave macro. The resulting virus (set: {AutoOpen, FileSaveAs}) is known as a devolved macro and original virus is devolving. Devolving macro viruses may be multi-level (that is, they lose different macros), resulting in many different variants. WM/Rapi is the best-known example of this.

VBA3 and VBA5

Excel for Windows 3.1 (Excel for Windows 5.0) includes the macro language VBA3 (Visual Basic for Applications, version 3). VBA3 was used as a prototype for VBA5 - the macro language used in Microsoft's Office 97 applications.

Visual Basic, up-converting and down-converting

In January 1997, Microsoft unveiled Office 97. This is a result of a complete re-write of the 'old' Microsoft Office suite (by " 'old' Microsoft Office" I mean Office 95, which includes Word for Windows 7.0 or 7.0a).

The template bit in DOC/DOT files

Word for Windows OLE2 files (documents) contain a special bit which indicates whether or not the current document contains anything but text. In DOC files, this bit is reset (zero) and in templates (DOT files) the bit is set (one). However the template bit itself is not linked to the file extension (and on the Macintosh there are no fixed extensions for files). So the following are all possible:

1. a DOC file containing no macros, in which the template bit is set (this does not normally happen, but it is possible if all macros have been removed from the DOC file)
2. a DOC file containing macros (virus macros, for example), in which the template bit is set (this occurs normally if the file is infected)
3. a DOC file containing macros (virus macros, for example), in which the template bit is reset (this means that the virus is inactive, or 'dormant' - the virus will not infect unless somebody 'flips' the template bit)

The first situation often causes confusion for users. Even when a file is clean, Word for Windows insists on saving it as a template (File | SaveAs offers only 'Document Template' as the available file type). Furthermore, there is no functionality built in to Word for Windows to clear the template bit. The easiest way to overcome this problem is to select the whole text (Ctrl-5), paste it to the clipboard (Ctrl-C), close the file (Ctrl-W), create a new file (File | New) and paste the text into the new file (Ctrl+V). File | SaveAs will then work normally.

Mating

When different macro viruses meet on one system, they may 'mate'. WordBasic copies macros by name; and if the virus macro has been substituted by another virus, the new macro will be copied instead of the original. Such

نمایندگی‌های فروش نرم‌افزار ضدویروس ایمن در داخل کشور

شهرستان	نام نماینده	تلفن	شهرستان	نام نماینده	تلفن
آبادان	اسوه‌پردازش‌اروند	۲۶۹۲۹	رشت	رایانه سپید رود	۲۲۳۸۶۳۲
ابهر	ابهر رایانه عصر نوین	۷۸۲۶۸	زنجان	زنجان پرداز	۴۲۴۷۳۱۶
اراک	آریاسیستم	۲۲۴۶۵۲۰	زاهدان	پردازش جنوب	۲۲۵۶۳۰
اردبیل	افق کامپیوتر	۲۲۴۶۳۵۸	ساری	کامپیوتر ندا	۲۲۲۰۸۶۳
اردکان	نوین رایانه	۷۲۲۹۰۸۰	ساوه	مرکز کامپیوتر شهر صنعت	۲۲۹۲۶۱
ارومیه	عصر کامپیوتر	۲۲۲۴۹۸۹	سلماس	مرکز توسعهٔ کامپیوتر	۳۱۰۷۹
اصفهان	فاراد رایانه پرداز	۶۲۵۱۳۱۱	سمنان	سینا نگار	۳۳۸۰۳
اهواز	پارس رایانه‌جنوب	۲۲۲۴۳۱۵	سنندج	داده‌پردازان کردستان	۶۶۶۱۲۹۵
ایلام	آروین رایانه	۳۳۴۷۳۲۰	سیرجان	در رایانه	۲۴۸۰۳
بابل	سرو سبز	۲۲۵۵۵۰۶	شوش	الکترونیک داریوش	۴۷۱۵
بجنورد	دنیای رایانه	۲۲۳۲۵۲۱	شوشتر	همایش رایانه جنوب	۲۷۶۵۳
بروجرد	خدمات کامپیوتر رهاورد	۲۶۴۷۲	شهرکرد	کامپیوتر آرایه	۳۳۳۶۶۵
بندرعباس	ساحل داهیر	۵۵۵۲۸۹	شیراز	صبا کامپیوتر	۶۲۷۷۷۴۴
بوشهر	بوشهر سیستم	۳۴۴۵۶	قائم شهر	کپی کامپیوتر	۲۲۴۲۵۸۴
تبریز	ندا پرداز آذر	۵۵۵۱۴۲۴	قزوین	مرکز کامپیوتر پگاه	۳۳۴۸۷۲۷
تهران	پاکچین ۲	۸۷۹۱۷۷۱	قم	متین پردازش	۹۳۷۸۸۱
تهران	پردازش انفورماتیک	۶۴۱۴۰۶۶	کاشان	صنایع دفتری زمان	۲۳۰۳۹
تهران	تدارک نرم‌افزار	۶۴۶۰۳۰۳	کرج	صنایع رایانه کرج	۴۳۸۶۳۶
تهران	تکنو ۲۰۰۰ صبا	۶۴۹۸۵۲۳	کرمان	باور الکترونیک	۲۶۴۰۱۲
تهران	خانه نرم‌افزار سپاه	۸۳۰۳۱۴۱	کرمانشاه	داده‌پردازی غرب	۷۹۲۳۳۰
تهران	صنایع رایانه ایران	۶۷۲۱۳۸۰	گنبد	کامپیوتر شیما	۲۲۲۶۱
تهران	مهران کامپیوتر	۸۹۰۷۵۳۳	مشهد	حساب رایانه	۹۸۹۸۹
خرم‌آباد	تکنوشارپ	۴۴۳۳۰۱	هشتگرد	پژوهش رایانه هوشمند	۴۴۰۴
خوی	نیک افزار	۲۲۲۰۶۱۰	همدان	نوین رایانه	۸۲۶۴۵۳۵
دامغان	کیهان کامپیوتر	۸۱۸۲	یاسوج	بهینه یاسوج	۲۲۲۵۳۵۴
دزفول	کامپیوتر خوزستان	۲۳۵۲۹	یزد	خدمات‌کامپیوتری ارس	۶۲۶۴۶۴۶

نمایندگیهای فروش در خارج از کشور

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

نرم‌افزار ضدویروس

ایمن

هر کسی می‌تواند

بهترین

را انتخاب کند!

جدید
نسخهٔ ۸۰/۷

- پشتیبانی جدیدترین ویروس‌های شایع ایرانی و خارجی از جمله :

W32/Nimda
W32/Magistr
W32/SirCam
VBS/HappyTime
W32/Badtrans
W32/BleBla
Baba-Caca.581

- افزایش تعداد ویروس‌ها به بیش از ۱۵۰۰ عدد
- اجرای تحت شبکه و دارای امکانات دیسکت نجات
- خدمات مشاوره و راه حل برای ویروس‌های جدید
- قابلیت غیرفعال‌سازی ویروس در حافظه (نیاز به راه‌اندازی مجدد از فلاپی دیسک نمی‌باشد)
- ارسال خبرنامهٔ تخصصی برای تمامی کاربران

برای Download کردن ویروس‌یاب ایمن، به سایت آن در آدرس زیر مراجعه نمایید

Web : www.ImenAntiVirus.com

E-Mail : info@ImenAntiVirus.com

Design : H.Sarikhani

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co

تهران - خیابان جمهوری اسلامی - بین جمالزاده و کارگر - شماره ۳۷۱
طبقه سوم - تلفن : ۷۴۲۳۵۷۷ (۷ خط) نمابر : ۷۴۲۳۴۰۸