خبرنامه تخصصی ایمن

۱

سال اول / شماره ۱ /زمستان ۱۳۷۸ / ۱۲ صفحه / ۱۰۰۰ ریال

- تاریخچهٔ نرم‌افزار ضدویروس ایمن
- آشنایی با یک ویروس ایرانی
- مصاحبه با ویروس‌نویسان بزرگ

و...

آزمایشگاه تحقیقات ویروسهای رایانه‌ای

به نام یگانه هستی بخش

سرمقاله

همواره فکر انتشار خبرنامه‌ای تخصصی در مورد ویروسها و مسایل امنیتی شبکه‌ها در شرکت وجود داشت. نشریه‌ای که به دنیای ویروسها، ویروس‌نویسها، ضدویروسها و نفوذگران بپردازد و به صورت مستمر کار اطلاع‌رسانی را که برخود وظیفه می‌دانیم، انجام دهد. البته کماکان سلسله مقالات تخصصی و خبری برای نشریات جهت درج ارسال می‌گردد، ولی لزوم خبرنامه‌ای مستقل که به دور از مسایل جانبی بصورت علمی به مباحث فوق بپردازد، همواره احساس می‌شد. نتیجهٔ این تلاش اولین شمارهٔ این خبرنامه است که هم‌اکنون در پیش روی شماست. ممکن است برای شروع قابل قبول باشد ولی برای ادامهٔ این راه قطعاً کاستی‌هایی دارد که برای رفع آنها به کمک شما عزیزان نیازمندیم. لذا آمادهٔ پذیرش مقالات شما خوانندگان گرامی می‌باشیم تا بتوانیم نشریه‌ای پربار منتشر کنیم که ماحصل تلاش نه یک گروه، بلکه تمامی کسانی باشد که به این زمینه علاقمند هستند.

ما قصد داریم در این خبرنامه موضوعاتی را بصورت سلسله‌وار مطرح کنیم؛ از جمله:

- مصاحبه با ویروس‌نویسان بزرگ.
- آشنایی با گروه‌های ویروس‌نویسی.
- اخبار جدید از دنیای ویروسها، ویروس‌نویسها و نفوذگران.
- آشنایی با ویروسهای معروف و نحوهٔ عملکرد آنها.
- نکاتی از لایه‌های پنهان کامپیوتر.
- ویروسهای روز دنیا.

و بسیاری مطالب خواندنی دیگر...

در پایان امیدواریم که با نظرات و پیشنهادات شما خوانندگان عزیز، هرچه بیشتر در رفع نواقص کار خود موفق 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

تاریخچهٔ نرم‌افزار ضدویروس **ایمن**

در پاییز سال ۱۳۷۳ ویروسی به نام One Half بر روی کامپیوترها شیوع یافت که در نوع خود ویروس خطرناک و پیچیده‌ای بود. مشخصهٔ منحصر به فرد ویروس One Half این است که اطلاعات دیسک سخت سیستم آلوده شده را به تدریج کد کرده و تخریب می‌نماید. البته تا زمانی که ویروس در سیستم وجود داشته و کنترل عملیات خواندن و نوشتن بر روی دیسک سخت را در اختیار داشته باشد، نمی‌توان متوجه این تخریب شد ولی با پاک کردن ویروس، اطلاعاتی که به مرور کد شده و تخریب گردیده‌اند، نمایان می‌شوند.

در آن زمان هیچ یک از نرم‌افزارهای ضدویروس خارجی، قادر به شناسایی و پاکسازی ویروس One Half نبودند. بنابراین لزوم وجود یک نرم‌افزار ضدویروس که قابلیت شناسایی و پاکسازی این ویروس خطرناک و مخرب را داشته و ضمناً بتواند اطلاعات کد شده توسط ویروس را نیز بازسازی نماید، به شدت احساس می‌شد.

اولین نسخهٔ نرم‌افزار **ایمن** که در آن زمان Hlf clean نام داشت، در پاییز سال ۱۳۷۳ به بازار عرضه شد که توانایی شناسایی و پاکسازی کامل ویروس One Half را داشت. مزیت عمدهٔ این نرم‌افزار آن بود که اطلاعات کد شده توسط این ویروس را نیز بازسازی می‌کرد. لازم به ذکر است که بعد از مدت زمان نسبتاً زیادی که از شیوع این ویروس گذشت، فقط تعداد اندکی از نرم‌افزارهای ضدویروس خارجی توانستند این ویروس را شناسایی و پاکسازی کنند ولی قادر به بازسازی اطلاعات کد شده نبودند و در صورتی که با استفاده از این نرم‌افزارها اقدام به پاکسازی ویروس مذکور می‌شد، تمامی و یا قسمتی از اطلاعات سیستم پاکسازی شده (بسته به مدت زمان عملکرد ویروس)، از بین می‌رفت که در بعضی موارد، از بین رفتن حتی قسمت کوچکی از اطلاعات ضررهای جبران‌ناپذیری به سازمان‌ها و یا اشخاص وارد می‌نمود.

بعد از موفقیت اولین نسخه از نرم‌افزار ضدویروس (با نام Hlf clean) تصمیم گرفتیم که قابلیت شناسایی و پاکسازی سایر ویروس‌های ایرانی و خارجی را به این نرم‌افزار اضافه کنیم. بنابراین نام آن به نرم‌افزار **ایمن** تغییر یافت. از آن زمان تاکنون همواره سعی‌مان بر این بوده است که ویروس‌های جدید و شایع در بازار نرم‌افزار داخلی را پشتیبانی کنیم تا خسارتهای احتمالی ناشی از شیوع این ویروس‌ها به حداقل برسد. البته با توجه به مشکلاتی که برای صنعت نرم‌افزار در ایران وجود دارد، پیمودن این راه بسیار سخت و دشوار است. لیکن ما با توکل به خدا و تکیه بر نیروها و استعدادهایی که در کشورمان وجود دارد و با یاری و مدد شما دوستان گرامی، تاکنون این راه را طی کرده‌ایم و امیدواریم در آینده نیز بتوانیم گام‌های بلندتری را در این زمینه برداریم.

مدیریت نرم‌افزار ضدویروس ایمن

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

بازیابی اطلاعات DATA RECOVERY

بازیابی اطلاعات عبارتست از روشهای مختلفی که بکار می‌رود تا بتوان فایلهای ذخیره شده روی رسانه‌های مختلف مانند دیسک سخت، دیسکت فلاپی، نوار و غیره را فراخوانی کرد. چون علت وجودی این روش ناشی از مشکلات سخت‌افزاری و نرم‌افزاری و یا ویروس می‌باشد، بنابراین حالات بوجود آمده در بازیابی اطلاعات متعدد و پیچیده می‌باشد. ممکن است در فکر بعضی از دوستان این مطلب تداعی شود که بتوان نرم‌افزاری برای بازیابی اطلاعات تولید کرد. باید گفت چند نمونه از این نرم‌افزارها تاکنون مشاهده شده است که در بدو برخورد با این نرم‌افزارها اینگونه به نظر می‌آید که مشکل حل شده است ولی با بررسی‌های انجام شده روی اینگونه نرم‌افزارها باید گفت مشکلات و نقاط ضعف بزرگی دارند. چراکه بهم ریختن اطلاعات توسط هر عنصری حتی ویروس خیلی کار ساده‌ای است ولی مرتب‌کردن و فراخوانی آن می‌تواند بسیار مشکل و بعضی مواقع ناممکن باشد. برای مثال می‌توان یک انفجار در چاپخانه‌ای را تصور کرد که در اثر آن صفحات هزاران کتاب بصورت پراکنده در فضائی پخش شود. حال مرتب کردن آنها ممکن است با هیچ قاعده و قانونی که بتوان بر اساس آن نرم افزار نوشت، امکان پذیر نباشد و تنها یک فکر می‌تواند از عهده آن برآید و صاحب فکر نیز فعلاً کامپیوتر نیست بلکه انسان است.
در اینجا ادامه بحث را به شماره بعدی موکول می‌کنیم و منتظر دریافت نظرات شما عزیزان در این رابطه هستیم.

****

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

جدول ویروسهای گزارش شده در نقاط مختلف دنیا WildList

این جداول که در اینترنت به WildList معروف می‌باشند، توسط سازمانهای مختلفی که دارای نمایندگیهایی در اکثر نقاط دنیا هستند، ارائه می‌شوند.

جداولی که ما از این به بعد منتشر خواهیم کرد، برگرفته از جداول سازمان جهانی WildList Organization International می‌باشد. لازم بذکر است که جدول زیر لیست ویروسهای گزارش شده تا نیمه اول سال ۱۹۹۹ را نشان می‌دهد. منتظر جداول جدیدتر ما در شماره‌های بعدی باشید.

AntiCMOS	Quandary	W97M/ColdApe
AntiEXE	Ripper	W97M/Ethan.A
Boot-437	RP.A	W97M/Groov.A
Burglar	Sampo	W97M/Marker
Byway.A	Spanska.4250.A	W97M/Melissa.A
Cascade.1701	StealthBoot.C	W97M/Nono.A
Cascade.1704	Stoned	W97M/Nottice
Cruel.A	Stoned.Angelina	W97M/Pri
DelWin.1759	Stoned.June_4th.A	W97M/Proteced.A
Die Hard	Spirit	W97M/Walker
Eco.B	Stoned.Standard.B	WelcomB
Exebug.A	Tai-Pan.438	WM/CAP
Flip	Tequila.mp.2468.A	WM/Colors.A
Form	TMC_Level-69	WM/Concept
Happy99	TPVO.mp.3783.A	WM/CopyCap.A
J&M	Tremor.4000.A	WM/Demon.A
Jerusalem	V-Sign	WM/Divina.A
Jumper.B	VBS/Freelink	WM/Helper.B
Junkie	W32/Beast.A	WM/Johnny.A
Kampana.mp.A	W32/ExploreZip	WM/MDMA.A
Major.1644.A	W32/PrettyPark.A	WM/Niknat.A
Manzon.1426	W95/Anxiety.1358	WM/Npad.A
Michelangelo	W95/Anxiety.1823	WM/ShowOff.A
Monkey.A	W32/CIH.1003	WM/Wazzu
Monkey.B	W32/CIH.1019	X97M/Extras
Natas	W95/Fono	XM/Laroux
Night Fall	W95/K32.3030	X97M/VCX.A
NYB	W95/Kenston.1895	XF/Paix.A
O97M/Jerk.B	W95/Marburg.8590	XF/Sic.A
O97M/Tristate.C	W95/Padania	XM/Compat.A
One Half	WM/Appder	XM/Extras.A
Parity_Boot.b	W97M/Brenda.A	YD.2881
Pieck.mp.4444.A	W97M/Class	

آشنایی با یک ویروس ایرانی

ویروس Mortezania.2676

این ویروس ایرانی، فایل‌های com و Partition Table دیسک سخت را آلوده می‌کند. اندازهٔ آن در فایل‌های com ، ۲۶۷۶ بایت است. ضمناً برای اینکه کنترل وقفهٔ 21H را هنگام بوت شدن سیستم در اختیار بگیرد، یک روتین ۹۰ بایتی را به انتهای فایل command.com (یا هر command interpreter دیگری که توسط دستور SHELL در فایل config.sys مشخص شده باشد) اضافه می‌نماید.

هنگامی که فایل com آلوده به این ویروس اجرا می‌گردد، ویروس ابتدا به دنبال عبارت "COMSPEC=" در Environment Block گشته و روتین ۹۰ بایتی موردنظر خود را در انتهای فایلی که نامش در جلوی عبارت "COMSPEC=" است (معمولاً فایل C:\command.com) ، می‌نویسد. بعد از آن، سکتور شمارهٔ ۱ ، ساید شمارهٔ صفر از سیلندر صفر (سکتور Partition Table) دیسک سخت اول را خوانده و در صورتی که قبلاً آلوده نشده باشد، یک کپی از آن را در سکتور ۲ ، ساید صفر از سیلندر صفر همان دیسک سخت قرار داده و سپس Partition Table را آلوده می‌کند. ما بقی ویروس را نیز در سکتور ۳ به بعد می‌نویسد. بعد از آلوده کردن Partition Table ، تاریخ سیستم را برابر با روز ۵ ام از ماه ۱۰ ام (پنج اکتبر) سال ۱۹۹۸ میلادی قرار می‌دهد و سپس فایل com اصلی اجرا می‌شود.

ویروس Mortezania ، توسط Partition Table آلوده، در حافظه مقیم می‌گردد. به این صورت که وقتی سیستم با Partition Table آلوده راه‌اندازی می‌شود، ویروس ابتدا اندازهٔ حافظهٔ Conventional را که Bios گزارش می‌کند، برابر با ۶۳۷ کیلوبایت قرار داده و سپس خود را از سکتور ۳، ساید صفر، سیلندر صفر دیسک‌سخت، در آدرس 9F40:0100 حافظه کپی می‌کند. سگمنت 9F40 در فضای آدرس‌دهی بالاتر از ۶۳۷ کیلوبایت قرار دارد و چون اندازهٔ حافظهٔ Conventional برابر با ۶۳۷ کیلوبایت قرار داده شده، بنابراین سیستم عامل و برنامه‌های دیگری که بعد از ویروس اجرا می‌شوند، از حافظهٔ اختصاص داده شده به ویروس استفاده نخواهند کرد. اکثر ویروس‌هایی که Partition Table یا Boot Sector را آلوده می‌کنند، از چنین تکنیک‌هایی برای در اختیار گرفتن حافظهٔ مورد نیاز خود استفاده می‌نمایند.

بعد از مقیم شدن ویروس در حافظه، آدرس وقفهٔ 13H به آدرس 9F40:0839 تغییر یافته و ویروس کنترل وقفهٔ 13H را در اختیار می‌گیرد. برای کنترل وقفهٔ 21H نیز از روتینی که در command.com آلوده قرار داده شده و هنگام بوت شدن سیستم اجرا می‌شود، استفاده می‌گردد. این روتین، آدرس وقفهٔ 21H را به آدرس 9F40:017D تغییر می‌دهد. البته چنانچه سیستم با Partition Table آلوده راه‌اندازی نشده و ویروس در حافظه مقیم نباشد، اجرای command.com آلوده و تغییر آدرس وقفهٔ 21H ، باعث قفل کردن سیستم خواهد شد.

بعد از آنکه ویروس در حافظه مقیم و فعال شد، کنترل توابع 2 (خواندن سکتور) و 3 (نوشتن بر روی سکتور) از وقفهٔ 13H و نیز توابع 3D (باز کردن فایل) و 4B (اجرای برنامه) از وقفهٔ 21H را در اختیار می‌گیرد. به این ترتیب، اجازهٔ نوشتن بر روی سکتور ۱، ساید صفر، سیلندر صفر از دیسک سخت اول (Partition Table آلوده) با استفاده از تابع 3 وقفهٔ 13H را نمی‌دهد. ضمناً هنگام خواندن سکتور فوق با استفاده از تابع 2 وقفهٔ 13H، چنانچه تاریخ سیستم، روز ۵ ام به بعد از ماه‌های ۱۱ و ۱۲ (نوامبر و دسامبر) سال‌های ۱۹۹۸ به بعد باشد، بر روی سکتور مذکور نوشته و اطلاعات آن را کلاً تخریب کرده و سیستم را Reset می‌کند. با از بین رفتن اطلاعات تقسیم‌بندی دیسک سخت، دیگر درایوهای منطقی قابل دسترس نخواهند بود.

این ویروس در دقایق فرد، اجازهٔ باز شدن فایل‌های با پسوند GIF، PCX، BMP و JPG با استفاده از تابع 3D وقفهٔ 21H را نمی‌دهد. همچنین هنگام اجرای فایل‌هایی با نام SCAN یا FINDVIRU با استفاده از تابع 4B وقفهٔ 21H، پیغام زیر را نمایش داده و فایل‌های مذکور را اجرا نمی‌کند:

This Program Is Too Big To Fit In Memory.

این ویروس هنگام اجرای فایل‌های با پسوند com توسط تابع 4B وقفهٔ 21H، آنها را آلوده می‌کند. درون فایل‌های آلوده به این ویروس، پیغام زیر را می‌توان مشاهده کرد:

A.Mortezania

این ویروس گونه‌های دیگری نیز دارد که توسط نرم‌افزار **ایمن** قابل شناسایی و پاکسازی می‌باشد.

مصاحبه با ویروس‌نویسان بزرگ

مصاحبه با **Vecna** نویسنده ویروس BabyLonia

- شما چگونه با کامپیوتر آشنا شدید ؟

در سال ۱۹۸۶ والدینم برای من یک کامپیوتر CP-400 خریدند. من همیشه آرزو داشتم که یک ویدئوگیم داشته باشم اما والدینم برای من یک کامپیوتر خریدند. من برنامه‌های کمی برای کامپیوترم پیدا کردم بنابراین شروع به نوشتن برنامه‌های خودم نمودم .

- چطور و چه زمان با دنیای ویروسها آشنا شدید ؟

من در سال ۱۹۸۸ سعی کردم تا یک ویروس بنویسم. اما در آن زمان نوشتن یک ویروس که بتواند نوارخوانهای K7 یک CP-400 را آلوده نماید، بنظر غیرممکن می‌آمد . در سال ۱۹۹۲ یک کامپیوتر ۳۸۶ خریدم و دو ماه بعد اولین کار ویروسیم را منتشر نمودم. آن ویروس (به نام GoldBug ‘ala’) یک ویروس غیرمقیم در حافظه به زبان توربو پاسکال بود و من آنرا در تمام شبکه‌های BBS که پیدا نمودم پخش کردم که آنرا هنوز هم می‌توان در بعضی از شبکه‌های BBS پیدا نمود.

- چطور شما ویروس می‌نویسید ؟ آیا شما دوست دارید در این رابطه اعتبار کسب نمایید ؟

من از اولین ویروسم به زبان پاسکال و همچنین اولین ویروسم به زبان اسمبلی چندان خرسند نیستم اما آنها را قدمی برای بهبود دادن مهارتهایم در زمینه برنامه‌نویسی واقعی می‌دانم. من آخرین ویروسهایم را بسیار خوب می‌دانم هرچند که آنها نشان دهنده تمام توانایی من نمی‌باشند، با اینحال من با آنها احساس سربلندی می‌نمایم.

- شما چگونه ویروسهایتان را نامگذاری می‌نمائید ؟

نمی‌دانم... من اسامی ویروسها را از چیزهایی که گاهی اوقات به ذهنم میرسند انتخاب می‌نمایم .

- شما کدام زبانهای برنامه نویسی را بلد هستید ؟

بیسیک، C ، C++ ،پاسکال، دلفی و اسمبلی 80x86 و 6908e و بعضی زبانها را نیز به مقدار کم مثل Pearl , lisp , Forth , Fortran , Cobol و غیره...

- شما دوست دارید از کدام زبان برنامه‌نویسی بیشتر استفاده نمائید ؟

من اخیراً بطور کامل در اسمبلی برنامه‌نویسی می‌کنم حتی اغلب برنامه‌های غیر ویروسیم را نیز به زبان اسمبلی می‌نویسم. همچنین بعضی اوقات در پاسکال و دلفی نیز برنامه‌نویسی می‌کنم.

- آیا شما عضو یکی از گروه‌های ویروس‌نویسی هم هستید ؟

من عضو گروه SGWW (Stealth Group World Wide) هستم.

- شما در زمینه ویروس‌نویسی چه هدفی را دنبال می‌نمائید ؟

کار من در مورد ویروس‌نویسی بیشتر شبیه کارهای روزمرهٔ زندگی است. دانستن اینکه وسایل چگونه کار می‌کنند، انجام کارهای جالب، شناخت مردم و علی‌الخصوص عوض کردن چیزهایی که فکر می‌کنم اشتباه هستند.

من می‌دانم که نوشتن و انتشار ویروسها علی‌الخصوص ویروسهای خطرناکی مانند ویروسهای خودم ، یک نوع تروریسم است ... من نمی‌توانم در مورد افرادی که اطلاعاتشان را بخاطر یکی از ویروسهای من از دست داده‌اند ، فکر نکنم و من بخاطر این موضوع بسیار متأسفم. اما این نوع تروریسم تنها راهی است که یک انسان اهل آمریکای جنوبی می‌تواند بوسیله آن به نابودی امپریالیسم که بر دنیای ما حکومت می‌کند، کمک نماید . من می‌دانم که این حرکت بسیار کوچکی است، ولی این وظیفه هر انسان شریفی است که با بدی مبارزه کند حتی اگر سلاح او به بی خطری یک ویروس کامپیوتری باشد .

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

من این اسم مستعار را از بازی AD&D rpg گرفته‌ام ، البته من اسم مستعار دیگری نیز دارم که فقط در زبان پرتغالی از آن استفاده می‌نمایم . ویروسی که من در مجله الکترونیکی VLAD#7 منتشر کردم تحت نام مستعارVecna بود لذا مردم مرا به این اسم شناختند .

من نام مستعار Vecna را خیلی دوست ندارم و هنوز نام مستعار Sangue Sujo را ترجیح می‌دهم .

- نظر شما در مورد نرم‌افزارهای تولید ویروس چیست ؟

آنها عموماً توسط اشخاصی استفاده می‌شوند که هیچ هدفی جز ویرانگری و خرابکاری ندارند . هرچند ایجاد خرابی مرا در اصلاح اشکالات پروژه‌هایم کمک می‌کند، ولی من بعنوان ویروس‌نویس برای افرادیکه از این نرم‌افزارها استفاده می‌کنند، ارزش زیادی قائل نیستم .

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

من ویروسهای ماکرو را زیاد دوست ندارم، بخاطر اینکه من چیز پیشرفته‌ای را در آنها مشاهده نمی‌کنم. اما به تازگی گروه SLAM در این زمینه کارهای خوبی را آغاز نموده است . اسمبلی اثاثاً زبان خوبی است زیرا اسمبلی زبان بسیار سریعی می‌باشد و بسیارکوچک است و می‌تواند مستقیما به سخت‌افزار دسترسی پیدا کند . ویروسهای زبانهای سطح بالا بسیار عالی هستند اما باید پیشرفته باشند . در جهان امروز ویروسهای Overwriting و غیرمقیم حتی اگر به زبان اسمبلی یا زبان سطح بالا باشند ، بسیار بی‌ارزش هستند. من فکر می‌کنم یک ویروس چه به زبان WordBasic ، زبان سطح بالا یا اسمبلی باشد، مانند یک کتاب است و برای گسترش ایده‌ها بکار می‌رود. اگر شما یک ایده خوب داشته باشید جنس کاغذی که در کتاب به کار می‌برید مهم نیست و در مورد ویروسها نیز اینچنین است.

- دیدگاه شما در مورد ویروسهایی که اثرات مخربی دارند چیست ؟

ما در دنیای ناسالمی زندگی می‌کنیم و گاهی اوقات مجبوریم از اسلحه‌های ناسالمی استفاده کنیم. من شخصاً از اثرات مخرب در ویروسهایم استفاده می‌کنم.

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

البته، یک ویروس، یا کتاب یا عکسی که به عوض شدن فکر مردم در جهت مثبت کمک کند، یک چیز خوب است .

- شما در زندگی حقیقیتان چکار می‌کنید ؟

من در دانشگاه درس می‌خوانم و کار می‌کنم. من در رشته Fonoaudiologia تحصیل می‌نمایم. این رشته شاخه‌ای از پزشکی و روانشناسی است که ارتباطات انسانی را مطالعه می‌کند. کار کسی که در این رشته درس می‌خواند این است که به افراد کر و لال و همچنین کسانیکه مشکلات عصبی دارند کمک کند تا با دیگران ارتباط برقرار نمایند و زندگی بهتری داشته باشند .

- آیا در پایان صحبت دیگری نیز دارید ؟

من فکر می‌کنم از تمام افرادیکه در زندگیم با آنها صحبت کرده‌ام ، نکته کوچکی آموخته‌ام .
من از دنیا متشکرم .

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

Interview with VECNA about "BABYLONIA"

This is an interview with Vecna, about his "Babylonia" virus. Enjoy.

- **Is the idea of making a virus that can be upgraded new, or based on anything else?**

The idea of a virus using plugins was floating around at some time between the w32 coders... This technology also is used in AV updaters

- **Do you think this is your best virus, or do you consider any of your previous viruses better?**

Several virus from mine are better... Lexotan, cocaine, fono...

- **How long did it take to code?**

More or less 3 months... But some parts, as the ring3-ring0 jump routine, where ready at more time(and it use the GDT, not IDT, as silly AVPVE say)

- **What was the most difficult part of the virus to code?**

The virus code residing in the wosck32.dll must get a pointer to a resident part in ring0 memory... I use a file attributes call with a special named filename, that contains, in A-Z letters, the converted address to patch... This ring3-ring0 communication scheme was somewhat difficult to code

- **The virus uses several ways of spreading, but which one do you think is the most effective?**

Sending itself as attachment in outgoing emails... Altought AVPVE say that this part of virus dont work, i still believe that the new icons and filenames that will appear in the comming months will boast spreading again

- **Do you think this virus is an important example for the future?**

Hmm... Yep... But was a natural step... Happy99 was a better example :)

- **How did you choose the name for the virus?**

Babylonia is, for the rastafaris, the place of evil and home of satan...