خبرنامه تخصصی ایمن

۴

سال اول / شماره ۴ / پاییز ۱۳۷۹ / ۲۰ صفحه / ۱۰۰ تومان

- آشنایی با ساختار کلی ویروس‌ها
- مصاحبه با VicodinES
- مسابقه و جایزه !!
- آشنایی با ویروس W32/Mtx (I-Worm.Mtx)

و...

آزمایشگاه تحقیقات ویروسهای رایانه‌ای

آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن

شرکت مهندسی مهران رایانه
Mehran Rayaneh Co

بسمه تعالی

خبرنامهٔ تخصصی ایمن ۴

سال اول/شمارهٔ چهارم
پاییز ۲۰/۱۳۷۹ صفحه

فهرست مطالب

سرمقاله..... صفحهٔ ۳
آشنایی با یک ویروس خارجی (ویروس W95/Mtx)..... صفحهٔ ۴
دربارهٔ ویروس‌ها(قسمت سوم)..... صفحهٔ ۸
اندر حکایت رزم رستم و ویروس..... صفحهٔ ۱۰
مسابقه و جایزه!!!..... صفحهٔ ۱۱
مصاحبه با ویروس‌نویسان بزرگ..... صفحهٔ ۱۲
جدول ویروس‌های گزارش شده در نقاط مختلف دنیا Wild list..... صفحهٔ ۱۵
بازیابی اطلاعات(قسمت چهارم)..... صفحهٔ ۱۶
آشنایی با گروه‌های ویروس‌نویسی (گروه MATRiX)..... صفحهٔ ۱۸
جدول نمایندگی‌های فروش ضدویروس ایمن..... صفحهٔ ۱۹
What is a macro? (متن انگلیسی)..... صفحهٔ ۲۰

« 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 قادر متعال

سرمقاله

ویروسهای کامپیوتری معضل امروز دنیای کامپیوترهاست و با تمام اقدامات پیشگیرانه‌ای که در مقابل این بیماری تکنولوژی اتخاذ می‌شود، باز هم آنها در حال رشد و افزایش هستند و با از بین رفتن نسل یک ویروس یا ریشه‌کن شدن نوع خاصی از ویروسها، باز هم گونه‌های جدیدی متولد می‌شوند و در دنیای کامپیوترها پراکنده می‌شوند. در گذشته ویروسهای فایلی تحت DOS و نیز ویروسهای بوت‌سکتوری رواج فراوان داشت ولی امروزه انواع جدیدتری، از جمله ویروسهای ماکرو، ویروسهای اسکریپتی و کرمهای اینترنتی رواج بسیار دارند. علت این گسترش نیز سادگی نگارش اینگونه ویروسها می‌باشد.

هرساله با شروع سال نو میلادی، تعدادی ویروسهای جدید و معمولاً خطرناک در دنیای کامپیوترها رها می‌شوند که باعث دردسر، اتلاف وقت و هزینه برای کاربران می‌گردد. از آنجا که اغلب این ویروسها جدید و ناشناخته هستند، بهترین راه برای مقابله با آنها پیشگیری می‌باشد. لذا رعایت چند نکتهٔ سادهٔ زیر شما را تا درصد زیادی از آلوده شدن به ویروسهای جدید محافظت می‌کند:

۱ ـ در هنگام استفاده از نامه‌های الکترونیکی (e-mail) و خواندن ضمیمه‌های آنها بسیار مراقب باشید. چون امروزه بیشتر ویروسها از طریق نامه‌های الکترونیکی منتشر می‌شوند.

۲ ـ سیستم کامپیوتری خود را به طور مرتب با یک نرم‌افزار ضدویروس کارا و مطمئن، ویروس‌یابی کنید.

۳ ـ نرم‌افزار ضدویروس خود را همواره به‌روز نگاه دارید.

آزمایشگاه تحقیقات ویروسهای رایانه‌ای **ایمن** (ICVL) به علت دسترسی سریع به ویروسهای ایرانی و خارجی شایع در کشور (به خاطر طیف وسیع کاربرانی که با ما در ارتباط هستند) همواره آمادهٔ پاسخ‌گویی به شما عزیزان در رابطه با ویروس‌های کامپیوتری و ارائهٔ راه حل برای مبارزه با آنها می‌باشد. همچنین شما همواره می‌توانید آخرین نسخهٔ ویروس‌یاب **ایمن** را از طریق صفحهٔ خانگی **ایمن** بر روی شبکهٔ جهانی اینترنت بدست آورده و مورد استفاده قرار دهید.

آرزوی ما ارائهٔ بهترین خدمات برای حفظ سلامت اطلاعات شماست.

با تشکر،

آزمایشگاه تحقیقات ویروسهای رایانه‌ای **ایمن**

ICVL

آشنایی با یک ویروس خارجی

آشنایی با ویروس W95/Mtx یا I-Worm.Mtx :

اخیراً ویروسی به نام W95/Mtx (I-Worm.Mtx) در سطح بین‌المللی و از جمله در ایران شایع گردیده که از طریق پست الکترونیکی منتشر می‌شود. ما در این مقاله به معرفی این ویروس و نحوهٔ عملکرد آن می‌پردازیم.

اندازهٔ این ویروس ۹۴۲۵ بایت بوده و فایل‌های اجرایی از نوع PE را آلوده می‌کند. البته اندازهٔ فایل میزبان اصلی ویروس ۱۸۴۳۸ بایت است.

به محض اجرای فایل میزبان اصلی ویروس که توسط پست الکترونیکی دریافت گردیده است، ویروس تغییراتی را در روتین تابع Send موجود در فایل WSOCK32.DLL (که برای ارسال اطلاعات در شبکه و اینترنت از آن استفاده می‌شود) ایجاد می‌کند تا بتواند فایل میزبان ویروس را به نامه‌های پست الکترونیکی ضمیمه کرده و آن را به کامپیوترهای دیگر ارسال کند. ضمناً با این تغییرات اجازهٔ وصل شدن به سایت‌هایی که نامشان شامل یکی از حروف زیر باشد را نمی‌دهد:

NII.	nai.	avp.	AVP.	F-Se
f-se	mapl	pand	soph	ndmi
afee	yen	lywa	tbav	yman

همچنین اجازهٔ ارسال نامه‌های الکترونیکی را به آدرس‌هایی که نامشان شامل یکی از حروف زیر باشد، نمی‌دهد:

NII.	nai.	avp.
AVP.	F-Se	f-se
wildlist.o	il.esafe.c	perfectsup
complex.is	HiServ.com	hiserv.com
metro.ch>	beyond.com	mcafee.com
pandasoftw	earthlink.	inexar.com
comkom.co.	meditrade.	mabex.com>
cellco.com	symantec.c	successful
inforamp.n	newell.com	singnet.co
bmcd.com.a	bca.com.nz	trendmicro
sophos.com	maple.com.	netsales.n
f-secure.c	F-Secure.c	

این آدرس‌ها متعلق به چند شرکت تولیدکنندهٔ نرم‌افزارهای ضدویروس می‌باشند.

پس‌از اجرا شدن فایل‌های آلوده و یا فایل میزبان اصلی ویروس، سه فایل به نام‌های IE_PACK.EXE ، WIN32.DLL و MTX_.EXE در مسیر اصلی Windows ایجاد می‌شوند. دو فایل اول همان میزبان‌های اصلی ویروس و فایل سوم یک تروا است. فایل MTX_.EXE که بعد از ایجاد، توسط خود ویروس اجرا می‌گردد، به صورت مستقل از ویروس عمل کرده و قصد برقراری ارتباط با اینترنت و گرفتن

فایل از آن را دارد. بعد از اولین اجرای فایل MTX_.EXE ، نام و مسیر این فایل در Registry به صورت زیر ثبت می‌گردد تا هر بار که سیستم راه‌اندازی می‌شود، این فایل نیز اجرا گردد:

HKEY_LOCAL_MACHINE\Software\[MATRiX]

و

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
SystemBackup=" Windows نام و مسیر اصلی + MTX_.EXE "

این ویروس تمامی فایل‌های اجرایی از نوع PE را که اندازه‌شان بیش از ۸ کیلوبایت بوده و در عین حال مضربی از ۱۰۱ نباشد، در مسیر اصلی Windows ، مسیر Temp و مسیر فایل ویروسی در حال اجرا، آلوده می‌کند. اندازهٔ فایل‌های مقصد پس از آلوده‌سازی، مضربی از ۱۰۱ خواهد شد.

ارسال فایل میزبان اصلی ویروس توسط پست الکترونیکی و با استفاده از تابع Send فایل WSOCK32.DLL تغییریافته انجام خواهد شد. به این ترتیب که هر بار که کاربر، یک نامه الکترونیکی (e-mail) را برای آدرسی ارسال می‌کند، بعد از ارسال نامهٔ اصلی کاربر، یک نامهٔ دیگر بدون عنوان و متن توسط ویروس ایجاد شده و فایل WIN32.DLL (که میزبان اصلی ویروس بوده و قبلاً توسط ویروس در مسیر اصلی Windows ایجاد شده) با یکی از نام‌هایی که در ادامه فهرست شده است، به نامهٔ الکترونیکی ایجاد شده ضمیمه گردیده و توسط ویروس به همان آدرسی که نامهٔ اصلی کاربر ارسال شده است، فرستاده می‌شود.

این نام‌ها عبارتند از:

README.TXT.pif
I_wanna_see_YOU.TXT.pif
MATRiX_Screen_Saver.SCR
LOVE_LETTER_FOR_YOU.TXT.pif
NEW_playboy_Screen_saver.SCR
BILL_GATES_PIECE.JPG.pif
TIAZINHA.JPG.pif
FEITICEIRA_NUA.JPG.pif
Geocities_Free_sites.TXT.pif
NEW_NAPSTER_site.TXT.pif
METALLICA_SONG.MP3.pif
ANTI_CIH.EXE
INTERNET_SECURITY_FORUM.DOC.pif
ALANIS_Screen_Saver.SCR
READER_DIGEST_LETTER.TXT.pif
WIN_$100_NOW.DOC.pif
IS_LINUX_GOOD_ENOUGH!.TXT.pif
QI_TEST.EXE
AVP_Updates.EXE

SEICHO-NO-IE.EXE
YOU_are_FAT!.TXT.pif
FREE_xxx_sites.TXT.pif
I_am_sorry.DOC.pif
Me_nude.AVI.pif
Sorry_about_yesterday.DOC.pif
Protect_your_credit.HTML.pif
JIMI_HMNDRIX.MP3.pif
HANSON.SCR
F!!!ING_WITH_DOGS.SCR
MATRiX_2_is_OUT.SCR
zipped_files.EXE
BLINK_182.MP3.pif

در فایل میزبان اصلی ویروس عبارات زیر که نشان‌دهندهٔ نام گروه ویروس‌نویسی، نام اعضای آن و آدرس سایت این گروه می‌باشد، دیده می‌شود که هرگز نمایش داده نمی‌شوند:

Software provide by [MATRiX] VX team:
Ultras, Mort, Nbk, LOrd DArk, Del_Armg0, Anaktos
Greetz:
All VX guy on #virus channel and Vecna
Visit us: www.coderz.net/matrix

در آخر یادآور می‌شود که نرم‌افزار ضد ویروس ایمن قادر به شناسایی و پاکسازی صددرصد این ویروس و سایر ویروس‌های ایرانی و خارجی شایع در بازار نرم‌افزار ایران می‌باشد.

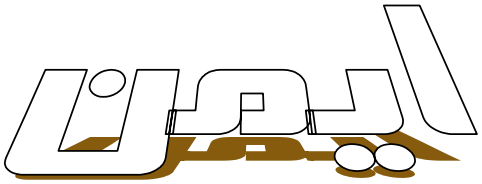
☺ ☺ ☺ ☺ ☺ ☺ ☺ ☺ ☺ ☺

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

imen_av@yahoo.com
mehran@irna.net
MehranCo@kosar.net

☺ ☺ ☺ ☺ ☺ ☺ ☺ ☺ ☺ ☺

با نرم‌افزار ضدویروس



دیگر نگران از دست دادن اطلاعات خود نباشید.

بهترین نرم‌افزار ضدویروس

برای بازار نرم‌افزار خاورمیانه

- با قابلیت شناسایی و پاکسازی صددرصد بیش از **۱۰۰۰** ویروس ایرانی و خارجی شایع در بازار نرم‌افزار ایران

- پشتیبانی جدیدترین ویروسهای ایرانی و خارجی از جمله:

W95/Mtx (I-Worm.Mtx)
VBS/KakWorm
W32/Kriz.4029
Restive.707
Nice Fox 3.3f
Nice Fox 3.4f
Ena.834

محصولی از آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن ICVL

شرکت مهندسی مهران رایانه

دربارهٔ ویروس‌ها (قسمت سوم)

آشنایی با ساختار کلی ویروسها

همانطور که در قسمت‌های گذشتهٔ این مقاله ذکر شد، ویروسها برنامه‌هایی هستند که می‌توانند تکثیر شوند یا به عبارت دیگر برنامه‌هایی هستند که می‌توانند خودشان را در فایل‌ها یا رسانه‌های دیگر کپی کنند. ما در این مقاله سعی می‌کنیم که شما را بطور دقیق‌تر با ساختار کلی ویروسها و نحوهٔ عملکرد آنها آشنا کنیم.

همانطور که ذکر شد، ویروسها می‌توانند تکثیر شوند. بطور کلی و خیلی خلاصه می‌توان گفت که برای تکثیر شدن لازم است که ابتدا ویروس یک میزبان داشته باشد. به عنوان مثال این میزبان می‌تواند یک فایل باشد که قرار است بوسیلهٔ ویروس مورد هجوم قرار گیرد.(بعضی از ویروسها می‌توانند Boot Sector و Partition Table را آلوده کنند، پس در مورد آنها میزبان Boot Sector یا Partition Table است.) پس از مشخص شدن میزبان، ویروس خود را درون آن کپی می‌کند و به این ترتیب آلوده‌سازی انجام می‌گیرد. پس می‌توان الگوریتم زیر را برای یک ویروس در نظر گرفت:

۱ ـ یک فایل میزبان خاص (مثلاً c:\command.com) را باز کن.

۲ ـ از ابتدای ویروس به اندازهٔ طول ویروس یا بیشتر را در آن فایل بنویس.

هر برنامه‌ای که اعمال فوق را بتواند انجام دهد، قطعاً یک ویروس است. یعنی انجام مراحل بالا شرط لازم و کافی برای ویروس بودن می‌باشد. اما به مراحل فوق می‌توان مراحل دیگری را نیز اضافه کرد تا هم قدرت انتشار ویروس افزایش یابد و هم احتمال شناسایی آن کمتر گردد. به عنوا ن مثال اگر ویروس فقط بخواهد یک فایل خاص را باز کند، اگر این فایل وجود نداشته باشد اولاً موفق به انجام این کار نشده و نمی‌تواند تکثیر شود و ثانیاً پیغام خطایی که سیستم عامل مبنی بر پیدا نشدن فایل مورد نظر نمایش می‌دهد احتمال کشف شدن ویروس را افزایش می‌دهد. پس بهتر است که ویروس به جای اینکه فرض کند آن فایل خاص وجود دارد، اولاً به دنبال آن فایل بگردد و در صورت وجود آن را آلوده کند و ثانیاً به جای یک فایل خاص دنبال دسته‌ای از فایل‌ها(مثلاً *.com) بگردد. همچنین می‌تواند در هر بار اجرا بیشتر از یک فایل را آلوده کند و برای اینکه اثرکمتری از خود بر جای گذارد قبل از آلوده‌سازی فایل میزبان، زمان(Time) ، تاریخ(Date) و صفات(Attrib) آن فایل را ذخیره کرده و پس از آلوده‌سازی دوباره همان مقادیر را برگرداند تا تغییر در این موارد باعث کشف شدن ویروس نگردد. در آخر بهتر است که پس از آلوده‌سازی، فایل میزبان را ببندد تا برای سیستم مشکل حافظه پیش نیاید. بعضی از ویروسها نیز برای اینکه یک فایل را چند بار آلوده نکنند، قبل از آلوده‌سازی آنرا چک می‌کنند و در صورت آلوده نبودن اقدام به آلوده‌سازی می‌نمایند. زیرا در مورد ویروسهایی که با اضافه شدن به فایل آنرا آلوده می‌کنند، چندین بار آلوده کردن یک فایل باعث افزایش بی‌رویهٔ طول فایل شده بطوریکه ممکن است دیگر فایل آلوده اجرا نگردد. بعضی از ویروسها علاوه بر موارد فوق سایز فایل میزبان را نیز چک

می‌کنند و فایل‌های خیلی بزرگ و خیلی کوچک را آلوده نمی‌کنند. پس به طور دقیق‌تر می‌توان الگوریتم یک ویروس را بصورت زیر نوشت:

۱ ـ دنبال یک دسته از فایل‌ها (مثلاً com.*) بگرد.

۲ ـ اگر فایلی را پیدا نکردی برو به ۱۴، در غیر اینصورت ادامه بده.

۳ ـ صفات فایل یافت شده را بخوان و ذخیره کن.

۴ ـ فایل مذبور را باز کن.

۵ ـ اگر موفق به باز کردن فایل نشدی برو به ۱۲ در غیر اینصورت ادامه بده.

۶ ـ زمان و تاریخ فایل را بخوان و ذخیره کن.

۷ ـ فایل را از نظر آلوده بودن چک کن. اگر آلوده بود برو به ۱۰، در غیر اینصورت ادامه بده.

۸ ـ سایز فایل را چک کن. در صورتی که در محدودهٔ مورد نظر نبود برو به ۱۰، در غیر اینصورت ادامه بده.

۹ ـ از ابتدای ویروس و به اندازهٔ طول آن در فایل مقصد بنویس.

۱۰ ـ زمان و تاریخ اولیهٔ فایل را برگردان.

۱۱ ـ فایل را ببند.

۱۲ ـ صفات اولیهٔ فایل را برگردان.

۱۳ ـ دنبال فایل بعدی بگرد.اگر فایلی را پیدا نکردی برو به ۱۴، در غیر اینصورت برو به ۳.

۱۴ ـ پایان.

همانگونه که می‌بینیم ساختار اولیه حفظ شده و فقط قسمت‌هایی به آن اضافه شده است. در مورد بند ۹ لازم به تذکر است که نوشتن در فایل میزبان می‌تواند به روشهای متفاوتی انجام گیرد. به عنوان مثال بعضی از ویروسها خود را در ابتدای فایل رونویس یا Overwrite می‌کنند، بعضی از ویروسها خود را در انتهای فایل نوشته یا به عبارتی به انتهای فایل اضافه می‌شوند، بعضی به اول فایل اضافه می‌شوند و... . بنابر این الگوریتم فوق می‌تواند دارای جزئیات بیشتری باشد. همچنین علاوه بر تمام مراحل فوق ممکن است ویروس دارای اثر تخریبی نیز باشد و یا اینکه یک کار نمایشی را انجام دهد.

لازم به ذکر است که ساختار فوق در مورد ویروسهای غیر مقیم در حافظه یا ویروسهای با عملکرد مستقیم صادق است. در قسمت بعدی این مقاله با ساختار ویروسهای مقیم در حافظه آشنا خواهیم شد. (ادامه دارد)

خوانندهٔ گرامی:

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

1- www.geocities.com/imen_av
2- imen.homepage.com
3- imen_av.tripod.com
4- imen.cjb.net
5- www.MehranCo.com

به نام خداوند ویروس گارد

اندر دیسکت گرفتن رستم از اسفندیار و به ویروس همی آلوده گشتن رایانهٔ وی

کنون رزم Virus و رستم شنو
دگرها شنیدستی این هم شنو

که اسفندیارش یکی Disk داد
بگفتا به رستم که ای نیکزاد

در این Disk باشد یکی File ناب
که بگرفتم از Site افراسیاب

چنین گفت رستم به اسفندیار
که من گشنمه نون سنگک بیار

جوابش چنین داد خندان طرف
که من نون سنگک ندارم به کف

برو حال می‌کن بدین Disk ، هان!
که هم نون و هم آب باشد در آن

تهمتن روان شد سوی خانه‌اش
شتابان به دیدار رایانه‌اش

چو آمد به نزد Mini Tower اَش
بزد ضربه بر دکمهٔ Power اَش

دگر صبر و آرام و طاقت نداشت
مر آن Disk را در Drive اَش گذاشت

نکرد هیچ صبر و نداد هیچ لفت
یکی List از Root دیسکت گرفت

در آن Disk دیدش یکی File بود
بزد Enter آنجا و اجرا نمود

کز آن یک Demo شد پس از آن عیان
همی فیلم و موزیک و شرح و بیان

به ناگه چنان سیستمش کرد Hang
که رستم در آن ماند مبهوت و منگ

چو رستم دگر باره Reset نمود
همی کرد Hang و همان شد که بود

تهمتن کلافه شد و داد زد
ز بخت بد خویش فریاد زد

چو تهمینه فریاد رستم شنود
بیامد که لیسانس رایانه بود

بدو گفت رستم همه مشکلش
وز آن Disk و برنامهٔ خوشگلش

چو رستم بدو داد قیچی و ریش
یکی دیسک Bootable آورد پیش

یکی فایل IMEN در آن دیسک بود
برآورد آنرا و اجرا نمود

همی گشت IMEN به Hard اندرش
چو کودک که گردد پی مادرش

به ناگه یکی رمز Virus یافت
پی حذف امضای ایشان شتافت

چو Virus را نیک بشناختش
مر از Boot Sector بر انداختش

یکی ضربه زد IMEN اندر سرش
که هر Byte آن گشت دور سرش

به خاک اندر افکند Virus را
تهمتن به IMEN بزد بوس را

چنین گفت تهمینه با شوهرش
که این بار بگذشت از پل خرش

دگر باره اما حماقت مکن
ز رایانه اصلاً تو صحبت مکن

قسم خورد رستم به پروردگار
نگیرد دگر Disk از اسفندیار

مسابقه ! . . . . . پاسخ دهید و جایزه 🏆 بگیرید !

خوانندهٔ گرامی، با پاسخ دادن به سؤالات زیر و ارسال فرم پاسخنامه یا کپی آن به دفتر نشریه، برندهٔ جوایز ما باشید. به 30 نفر از کسانی که بهترین پاسخ‌ها را داده باشند، جوایز زیر تعلق خواهد گرفت:

۱۰ عدد ساعت دیواری به ده نفر اول+ ویروس‌یاب **ایمن**

۱۰ عدد تی‌شرت به ده نفر دوم+ ویروس‌یاب **ایمن**

۱۰ عدد تقویم سالانه سال ۱۳۸۰ به ده نفر سوم+ ویروس‌یاب **ایمن**

مهلت ارسال : تا آخر اردیبهشت 1380

نشانی ما :

تهران - خیابان جمهوری اسلامی - بین جمالزاده و کارگر - شمارهٔ ۳۷۱ - طبقهٔ چهارم - شرکت مهندسی مهران‌رایانه

آزمایشگاه تحقیقات ویروسهای رایانه‌ای ایمن - واحد خبرنامهٔ تخصصی ایمن

سؤال ۱ : مزایای یک نرم‌افزار ضدویروس داخلی را نسبت به نرم‌افزارهای ضدویروس خارجی توضیح دهید.

. . . . . .

. . . . . .

. . . . . .

. . . . . .

. . . . . .

سؤال ۲ : نرم‌افزار ضدویروس **ایمن** را در یک جمله توصیف کنید.

. . . . . .

. . . . . .

نام و نام خانوادگی: . . . . . .

آدرس: . . . . . .

. . . . . .

شمارهٔ تماس: . . . . . مهر / امضاء

مصاحبه با ویروس‌نویسان بزرگ

مصاحبه با VicodinES

- شما چگونه با کامپیوترها آشنا شدید؟

من ۱۴ یا ۱۵ ساله بودم که پدرم برای من یک TI-99 4/A خرید و من شروع به یادگیری زبان BASIC نمودم. در آن زمان برنامه‌ها را روی نوار کاست ذخیره می‌کردیم. یکی از دوستانم نیز یک مودم داشت که بوسیلهٔ آن به شبکه‌های BBS وصل می‌شدیم. این در سال ۱۹۸۲ یا کمی بعد از آن بود.

- چطور و چه زمانی با دنیای ویروسها آشنا شدید؟

وقتی که تصمیم گرفتم برنامه‌هایی به زبان اسمبلی بنویسم.

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

بله من ویروس می‌نویسم و نمی‌خواهم در این زمینه اعتباری کسب کنم. من هنگامی اعتبار بدست خواهم آورد که چیزی سیستم شما را آلوده کند، حتی اگر من آن را ننوشته باشم. اگر شما را اذیت کند و بخواهید از شر آن خلاص شوید، در آن صورت من برای نجات دادن شما اعتبار می‌خواهم!!!

- شما چگونه ویروسهایتان را نامگذاری می‌کنید؟

همهٔ نام‌ها بصورت تصادفی به ذهن من خطور می‌کنند.

- با کدام زبانهای برنامه‌نویسی آشنا هستید؟

من زبان کوبول (COBOL) را در دبیرستان یاد گرفتم اما بیشتر آن را فراموش کرده‌ام. با زبانهای ماژولا (Modula) و پاسکال آشنایی دارم. همچنین زبانهای اسمبلی و C++ را نیز به خوبی بلد هستم. در حال حاضر هم روی مهارتهایم در Visual C++ کار می‌کنم، زیرا ایده‌های واقعاً خوبی برای ویروس بعدیم دارم.

- از کدام زبان برنامه‌نویسی دوست دارید بیشتر استفاده کنید؟

از همهٔ آنها!

- آیا شما عضو یکی از گروه‌های ویروس‌نویسی هستید؟

من یکی از اعضای The Narkotic Network یا TNN هستم. ما فقط سه نفر هستیم.

- شما در زمینهٔ ویروس‌نویسی چه هدفی را دنبال می‌کنید؟

دوست دارم کاربران بیشمار در سطح دنیا را اذیت کنم.

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

واقعاً چیز زیادی در این مورد نمی‌دانم.

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

در ایالات متحده VicodinES نام یک داروی ضددرد است. البته نام آن در حقیقت Vicodin Extra Strength است. من آن قرصهای کوچک را دوست دارم لذا این نام را برای خودم انتخاب کردم. این قرصها فقط از Hydrocodone و Tylanol تشکیل شده است. در هر صورت چون هنگامیکه تصمیم گرفتم شروع به ویروس‌نویسی کنم به این داروها علاقه داشتم، این نام را مناسب دانستم.

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

من با نرم‌افزار NuKE NRLG و PS G2 کار می‌کردم. من فکر می‌کردم که آنها تاحدی خوب هستند. من ایدهٔ اولیهٔ نرم‌افزار DREG را دوست داشتم. من هرگز یک کپی از این نرم‌افزارها را نداشته‌ام(البته در اصل زحمت Download کردن آنها را به خودم نداده‌ام) اما فلسفه‌ای را که پشت همهٔ این نرم‌افزارها بود، دوست داشتم.

- نظر شما در مورد ویروسهای ماکرو در مقابل ویروسهای نوشته شده به زبان اسمبلی و زبانهای سطح یالا چیست؟

به نظر من ماکروها خیلی خوب هستند. من گاهی اوقات فکر می‌کنم که آنها راه آسانی برای ایجاد یک گونهٔ جدید از یک ویروس باشند. اما بعضی از آنها را دیده‌ام که مرا واقعاً تحت تأثیر قرار داده‌اند. من تا به حال ویروس ماکرویی ننوشته‌ام اما این کار یکی از اولویت‌های من است. ویروسهای نوشته شده با زبانهای سطح بالا راهی برای حرکت هستند. شما می‌توانید با یک ویروس نوشته شده با زبان C++ تحت ویندوز کارهای جالبی انجام بدهید. فقط صبر کنید، خواهید دید.

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

گفتن این حرف برای من هنوز زود است. هرچند من این کار را وقتی انجام دادم که بیش از ۳۰۰ نفر، یک فایل آلودهٔ WinZip مرا Download کردند. این فایل حامل ویروس Skim.Poppy بود. به هر حال فکر می‌کنم که روزی یکی از ویروسهایم مرا به این امر مفتخر کند.

- نظر شما در مورد اثرات مخرب در ویروسها چیست؟

یک عکس‌العمل مؤثر!

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

ویروسهای من که همه خوب هستند! من منظور سؤال را نمی‌فهمم!!

- شما در زندگی حقیقیتان چکار می‌کنید؟

من برای یک شرکت بزرگ مهندسی کار می‌کنم و همچنین در کنار این کار، یک هنرمند دنیای موسیقی نیز هستم. ممکن است شما روزی یکی از CDهای مرا داشته باشید.

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

نه خیلی. زیرا من از مردم نمی‌خواهم که در مورد فعالیت‌هایم قضاوت بکنند.

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

من بصورت تفریحی در مورد کپی برداری از نرم‌افزارها کار می‌کنم.

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

من اینگونه فکر نمی‌کنم. من بوسیلهٔ اخلاقیات مردم دیگر تحت کنترل قرار نگرفته‌ام. من هیچ قانونی را واقعاً مراعات نمی‌کنم. من وقتی تحت قانونی قرار خواهم گرفت که آن قانون مستقیماً بر من تأثیر داشته باشد ولی تا آن موقع من وقتم را بیهوده صرف بحث کردن در این موارد نمی‌کنم.

- در پایان آیا صحبت دیگری دارید؟

خیر.

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 چهارم ـ شرکت مهندسی مهران‌رایانه ـ **آزمایشگاه تحقیقات ویروسهای رایانه‌ای** ایمن **ـ واحد خبرنامهٔ تخصصی** ایمن.

تلفن: ۶۴۲۳۵۷۷ (سه خط)

نمابر: ۶۴۲۳۴۰۸

آدرس e-mail:

imen_av@yahoo.com
mehran@irna.net
MehranCo@kosar.net

جدول ویروسهای گزارش شده در نقاط مختلف دنیا WildList

در این شماره، WildList مربوط به ماه‌های دهم(اکتبر) و یازدهم(نوامبر) سال ۲۰۰۰ را مشاهده می‌کنید. با نگاهی به این جدول متوجه می‌شوید که اغلب ویروسها از نوع ماکرو بوده و تعدادی هم ویروس اسکریپت و فایلی وجود دارد.

از این ویروسها فقط گونه‌های ویروس VBS/LoveLetter و همچنین ویروس W32/Kriz در ایران گزارش شده که نرم‌افزار ضدویروس **ایمن** قادر به شناسایی و پاکسازی صددرصد این ویروس‌ها می‌باشد.

نوع	نام ویروس	نوع	نام ویروس
ماکرو	W97M/Murke.A	اسکریپت	VBS/LoveLetter
ماکرو	W97M/Opey.M	اسکریپت	VBS/LoveLetter.C
ماکرو	W97M/Replog.A	اسکریپت	VBS/LoveLetter.VeryFunny
ماکرو	W97M/Seliuq.A	فایل	W32/Kriz
ماکرو	W97M/Shore.D	فایل	W32/MSInit
ماکرو	WM/Demon.A	فایل	W32/Navidad-m
ماکرو	X97M/Barisada.G	ماکرو	W97M/Assilem.C
ماکرو	X97M/Jini.A1	ماکرو	W97M/FF.E

علاقمندان می‌توانند جهت دریافت شماره‌های بعدی این خبرنامه، فرم مشخصات زیر یا کپی آنرا 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: .....

آدرس: .....

.....

شمارهٔ تماس: ..... مهر و امضاء

۴

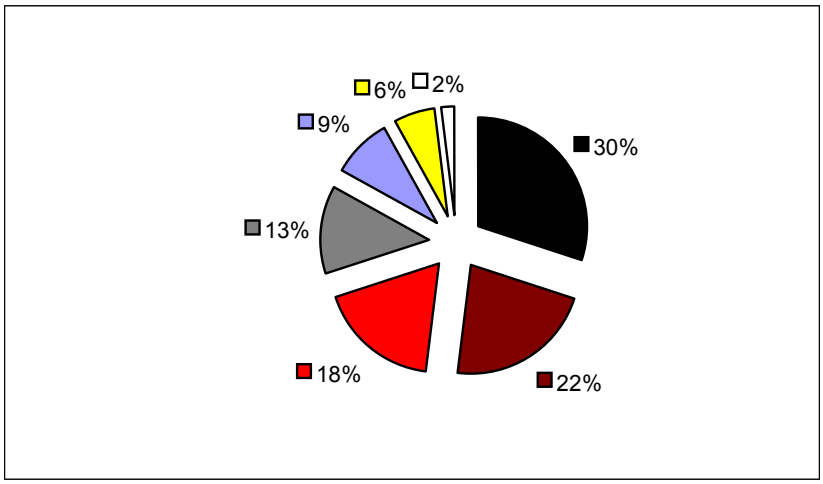
بازیابی اطلاعات (قسمت چهارم)

دلایل از کار افتادن دیسک سخت :

دلایل از کار افتادن دیسک سخت را می‌توان بصورت جدول زیر دسته‌بندی کرد:

نوع خطا	احتمال رویداد خطا
خطاهای انسانی	٪۳۰
ایرادات نرم افزاری	٪۲۲
درست عمل نکردن سیستم	٪۱۸
ایرادات سخت افزاری	٪۱۳
تخریب توسط ویروس	٪۹
خرابکاری عمدی	٪۶
حوادث طبیعی	٪۲
جمع کل	**٪۱۰۰**

و نمایش نموداری آن به شکل زیر می‌باشد:



نکات قابل توجه :

- خطاهای انسانی بزرگترین درصد از دست رفتن اطلاعات را شامل می‌شود که عبارتند از: حذف تصادفی فایلها، استفادهٔ اشتباه از دستورات و بعضی اوقات فرمت کردن دیسک‌سخت.

- هنوز از تهدیدات ویروس‌ها کاسته نشده و صدمه به اطلاعات همچنان ادامه دارد.

- از دلایل اجتناب ناپذیر از بین رفتن اطلاعات می‌توان طوفان، آتش سوزی، رعدوبرق و زمین‌لرزه را نام برد.

چند توصیه ایمنی:

با توجه به ارقام و اطلاعات ذکر شده باید نکات زیر را در نگهداری اطلاعات رایانه‌ای مد نظر داشت:

- آخرین و بهترین روش برای حفظ اطلاعات، گرفتن نسخه پشتیبان بصورت مستمر و دوره‌ای (روزانه - هفتگی - ماهانه) می‌باشد.

- در صورت عدم دسترسی به اطلاعات و یا بهم‌ریختگی آنها، از فرمت کردن و یا دوباره پارتیشن بندی کردن دیسک‌سخت خودداری کنید. زیرا این کار باعث می‌شود احتمال بازگشت اطلاعات کمتر شده و یا غیرقابل بازیابی شود.

- از نصب برنامهٔ جدید (و یا مجدد) و حذف برنامه‌های موجود بشدت بپرهیزید.

- به هیچ عنوان از برنامه‌هائی نظیر NDD ، SCANDISK ، FDISK و مشابه آنها استفاده نکنید. زیرا اینگونه برنامه‌ها از مدیریت بالای فایل سیستم به دیسک‌سخت نگاه می‌کنند و چنانچه مثلاً اطلاعات بوت سکتور تغییری کند، این برنامه‌ها کلیه داده‌ها را بر اساس اطلاعات غلط بوت سکتور مرتب می‌کنند و در نتیجه بهم‌ریختگی افزایش می‌یابد.

در پایان امیدواریم راهنمائی‌های ارائه شده بتواند در جهت بالاتر بردن ایمنی سیستمهای شما مؤثر بوده باشد. در هر صورت چنانچه برای دیسک‌سخت شما مشکلی بوجود آمد، این شرکت آمادگی دارد تا نسبت به بازیابی اطلاعات شما اقدام لازم را انجام دهد.

Dear reader,
You can visit our homepage in:
www.geocities.com/imen_av
imen_av.tripod.com
imen.homepage.com
imen.cjb.net
www.MehranCo.com

آشنایی با گروه‌های ویروس‌نویسی

آشنایی با گروه MATRiX

نام گروه: Matrix

منشأ: روسیه

وضعیت: جدید

اطلاعات زیادی از این گروه در دست نیست جز اینکه این گروه در اواخر سال ۱۹۹۹ بوجود آمد. اعضای شناخته شدهٔ گذشته و حال این گروه عبارتند از:

1.Ultras	2.NBK	3.Mort	4.LOrd Dark
5.DelArmg0	6.Anaktos	7.HenKey	8.tgr

یکی از اعضای این گروه به نام Ultras به خاطر کارهایی که در زمینهٔ ویروسهای ماکرو انجام داده، شناخته شده است. نتیجهٔ این فعالیت‌ها نرم‌افزارهای تولید ویروس‌های ماکرو به نام‌های زیر است:

1.UCK (Ultras Construction Kit)
2.UAMP(Ultras Access Macro Polymorphic)
3.UMPE (Ultras Macro Polymorphic Engine)
4.UMP (Ultras Macro Polymorphic)
5.UHE (Ultras HTML Encryptor)
6.ME (Macro Encryptor)
7.MUCK(Mini Ultras Construction Kit)
8.AMG (Access Macro Generator)

این گروه دارای یک مجلهٔ الکترونیکی به نام MATRIX E-ZINE است که پس از انتشار اولین شمارهٔ آن، تعطیل شد. ویروس W95/Mtx یا I-Worm.Mtx که در حال حاضر در بازار نرم‌افزار ایران شایع شده است، از محصولات این گروه می‌باشد.

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	ساوه	شهر صنعت	۲۲۹۲۶۱
اهواز	پارس رایانه‌جنوب	۲۱۸۶۶۲	سلماس	مرکز توسعهٔ کامپیوتر	۳۱۰۷۹
ایلام	آروین رایانه	۳۳۷۷۳	سمنان	سینانگار	۲۲۱۶۱
بابل	کامپیوتر پویا	۲۲۲۲۵۸۹	سنندج	داده‌پردازان کردستان	۶۶۱۲۹۵
بجنورد	دنیای رایانه	۲۲۳۲۵۲۱	سیرجان	در رایانه	۳۲۵۷۴
بروجرد	خدمات‌کامپیوتررهاورد	۲۶۴۷۲	شوش	الکترونیک داریوش	۴۷۱۵
بندرعباس	ساحل داهیر	۵۵۵۲۸۹	شوشتر	همایش رایانه جنوب	۲۷۶۵۳
بوشهر	بوشهر سیستم	۳۴۴۵۶	شهرکرد	کامپیوتر آرایه	۳۳۳۶۶۵
تبریز	نداپرداز آذر	۵۵۵۱۴۲۴	شیراز	صبا کامپیوتر	۶۷۷۷۴۴
تهران	پانیران	۸۷۷۸۶۵۷	قائم شهر	کپی کامپیوتر	۴۲۵۸۴
تهران	پردازش انفورماتیک	۶۴۱۴۰۶۶	قزوین	مرکز کامپیوتر پگاه	۴۸۷۲۷
تهران	تدارک نرم‌افزار	۶۴۶۰۳۰۳	قم	متین پردازش	۹۳۷۸۸۱
تهران	تکنو ۲۰۰۰ صبا	۶۴۹۸۵۲۳	کرج	صنایع رایانه کرج	۴۳۸۶۳۶
تهران	خانه نرم‌افزار سپاه	۸۳۰۳۱۴۱	کرمان	باور الکترونیک	۲۶۴۰۱۲
تهران	سرزمین رایانه	۲۰۰۰۱۸۷	گنبد	کامپیوتر شیما	۲۲۲۶۱
تهران	کامپیوتر گویا	۸۸۲۷۴۱۷	مشهد	حساب رایانه	۹۸۹۸۹
تهران	مهران کامپیوتر	۸۹۰۷۵۳۳	هشتگرد	پژوهش رایانه هوشمند	۴۴۰۴
خرم‌آباد	تکنوشارپ	۴۴۳۳۰۱	همدان	نوین رایانه	۸۲۶۴۵۳۵
خوی	نیک افزار	۲۲۲۰۶۱۰	یاسوج	بهینه یاسوج	۲۵۳۵۴
دامغان	کیهان کامپیوتر	۸۱۸۲	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

What is a macro?

Many applications provide the functionality to create macros. A macro is a series of commands to perform some application-specific task. Macros are designed to make life easier; for example, to perform some everyday tasks like text-formatting or spreadsheet calculations.

Macros can be saved as a series of keystrokes (the application records what keys you press); or they can be written in special macro languages (usually based on real programming languages like C and BASIC). Modern applications combine both approaches; and their advanced macro languages are as complex as general purpose programming languages. When the macro language allows files to be modified, it becomes possible to create macros which copy themselves from one file to another. Such self-replicating macros are called macro viruses.

History

Many software packages have a macro language. Perhaps the very first well- known and widespread was Lotus 123. It was proved long ago that for Lotus 123 it is possible to write a self-replicating macro (a virus macro) which would be capable of spreading from one file to another. However, viruses have never been a problem for Lotus 123; its macro language is rather simple; and access to files can be done only via menus. So, a virus for Lotus 123 would be extremely obvious - you would literally see the infection process right on your screen.

In December 1994, the researcher Joel McNamara wrote the first real macro virus . . . for demonstration purposes. It was called DMV (Document Macro Virus). In fact, there were two viruses written, DMV for Word for Windows and DMV for Excel for Windows. The samples were used to demonstrate the possibility of macro viruses under these platforms.

The first "in the wild" macro virus appeared in the summer of 1995. This virus (perhaps written by one of Microsoft's employees) was the infamous WM/Concept. This soon became the most widespread virus ever. The comment within the body of the virus says "That's enough to prove my point". After the appearance of WM/Concept we saw other macro viruses within a couple of months - WM/Nuclear, WM/Hot, WM/Colors and WM/Atom.

By the end of May 1997 the total number of macro viruses had reached many hundreds. If we count every single-bit difference as a virus variant, the total number will be above 1,800. This figure is growing fast; currently we see more than five new macro viruses every day!

IMEN Anti-Virus