www.tarfandestan.com

تاریخچه اولین ویروس های انفورماتیک و اولین آنتی ویروس ها

نویسنده و مترجم: ZzBb

تهیه و تنظیم:محمود ۸۰۸۰

انجمن های تخصصی ترفندستان

بسم الله الرحمن الرحیم

تاریخچه اولین ویروس های انفورماتیک و اولین آنتی ویروس ها

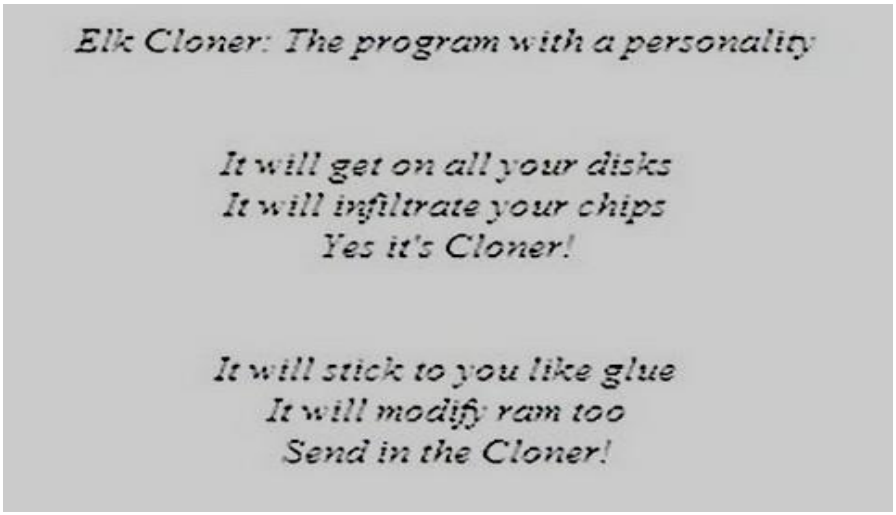
سی سال برای پیدایش اولین ویروسهای انفورماتیک لازم بود و پس از ان این امر شدت گرفته و در کمتر از ده سال یعنی از سال ۱۹۸۴ تا اوایل سال ۱۹۹۰ ویروسهای انفورماتیک از ازمایشگاه ها خارج گشته و الوده کردن اینترنت جوان را اغاز نمودند و مبارزه های ضد ویروس با اولین انتی ویروسها شروع شد .

یکی از وقایع مهم در ابتدای سالهای ۱۹۸۰ ظهور ویروس "In the Wild" بود .کانسپت پر اهمیت ان باعث شد تا انتی ویروسها هدف عملیاتی ای را تعیین نموده و در نتیجه معیارهای گواهی ها را نیز تعیین نمایند.

در سال ۱۹۹۲ رسما در کنفرانس Jeffrey Kephart و Steve White در مورد تکنیکهای پیشگیری از ویروسهای انفورماتیک, ویروس "In the Wild" برای تعیین معیار دو نوع ویروس اعلام شد. از یک طرف ویروسهائی که احتمال انتشار انها کم بوده و فقط در کلکسیون ها موجود بودند که به انها ویروس "zoo" گفته میشد و از طرفی دیگر ویروسهائی را میابیم که روی شبکه های شرکتها و یا روی کامپیوترهای افرادی یافت میشدند که ویروسهای "In the Wild" نامیده میشدند.

Elk Cloner-۱

"Elk Cloner"اولین ویروس "In the Wild" بود که در سال ۱۹۸۲ توسط یک جوان پانزده ساله دبیرستانی به نام Rich Skrenta2نوشته شده و سیستم عامل ذخیره شده روی فلاپی دیسکهای اپل دو را الوده کرده و انتشار یافت. زمانیکه کامپیوتر از روی این فلاپی دیسک الوده بوت میشد, ویروس بطور خودکار اجرا میشد اما به عملکرد کامپیوتر اسیب وارد نکرده و بار مخرب نداشت. ولی هنگامیکه فلاپی دیسک غیر الوده ای روی کامپیوتر استفاده میشد, این ویروس بطور خودکار خود را روی ان کپی میکرد. تنها عملی که برای کاربر قابل مشاهده بود, نمایش یک شعر در مورد عملیات ان بود که بعد از پنجاهمین بوت از روی فلاپی دیسک الوده نمایش داده میشد (تصویر زیر).



انگیزه Rich Skrenta غیر منتظره و عجیب بود. در واقع سازنده این ویروس عادت کرده بود که کپی بازیهای هک شده را بین دوستانش توزیع کند. بازیهائی که وی قبلا انها را تغییر داده و بگونه ای تنظیم میکرد که بعد از بازی تعدادی از قسمتها دیگر کار نکنند .او همه اینکار ها را برای ازار رفقایش میکرد. بعد از مدتی این رفیقان متوجه عملیات وی گشته و تصمیم گرفتند دسترسی به فلاپی دیسکها و کامپیوترهای خود را برای او ممنوع کنند. اینجا بود که وی تصمیم گرفت با "Elk Cloner" حتی در زمان غیبت خود انها را اذیت کند .

Rich Skrentaمیگوید که خود از انتشار سریع ویروسش غافلگیر شده بوده و عملش از نظر خود او اهمیت چندانی نداشته اما ناگهان متوجه میشود که حتی خود قادر نیست از شر ویروس خود ساخته اش که تمام دیسکهای او و دوستانش را الوده کرده بود خلاص شود

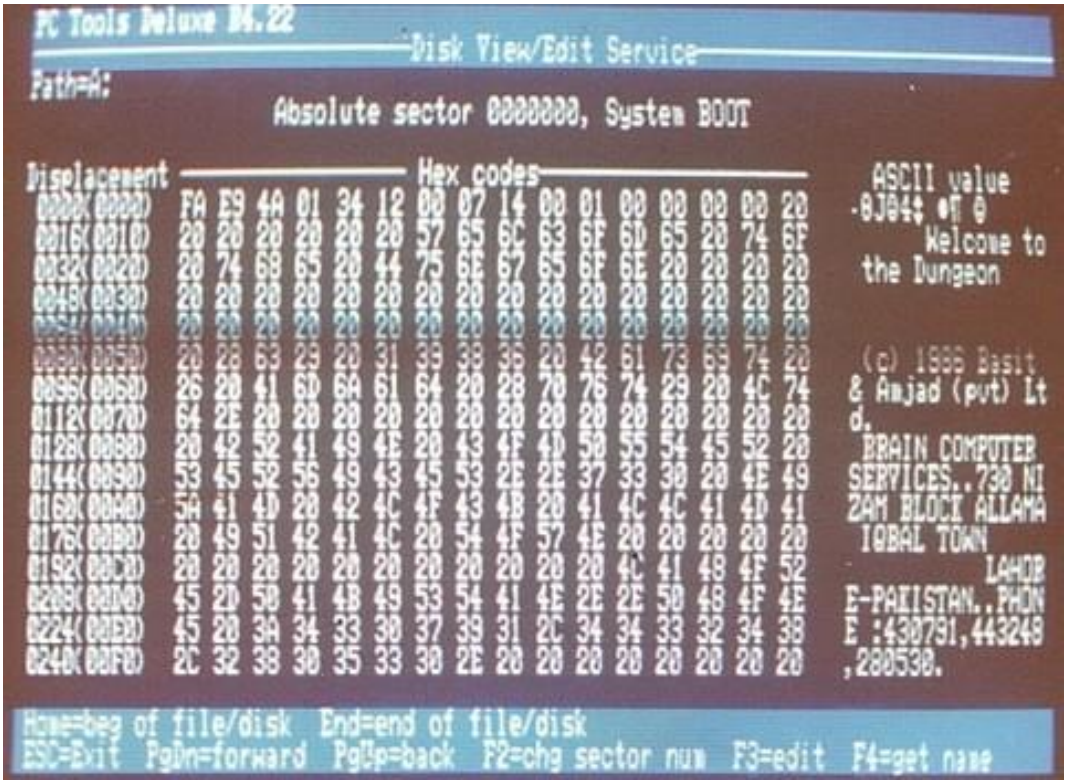
Brain-۲

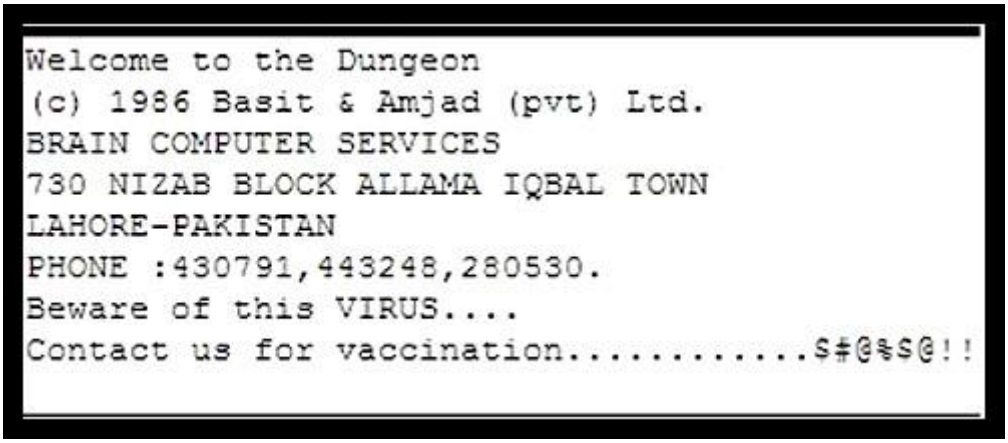
اما در سال ۱۹۸۶ بود که رهائی از ویروسی که به سرعت انتشار میافت به معنای واقعی همه را دچار دردسر کرد.

داستان از این قرار بود که دو برادر به اسامی Basitو Amjad Farooq Alvi که تجارت انفورماتیک در لاهور در پاکستان داشتند, بعد از اینکه نرم افزارشان که برای انالیز پزشکی بود بسیار هک شده و استفاده میشد, تصمیم به ساختن ویروسی گرفتند.

انها ویروسی ساختند تا هر کسی که از یک کپی غیر قانونی این نرم افزار پزشکی انها استفاده میکند را الوده کند. نام این ویروس "Brain"بود.

نتیجه الودگی با این ویروس وحشتناک بود. هر کامپیوتری که الوده "Brain" میگشت, به هنگام بوت ,انچه را که در تصویراول زیر مشاهده میشود نمایش داده شده و به هیچ گونه نمیشد از سد ان گذشت و یا کاری کرد و در عمل استفاده از کامپیوتر غیر ممکن میشد. در سمت راست ان نیز انچه که در تصویر دوم زیر است مشاهده میشد.





انها ادرس و شماره تلفن خود را برای قربانیان ویروس "Brain" نمایش میدادند تا برای حذف ان و یا واکسینه کردن کامپیوتر انان انها را یاری کنند چون در واقع هدف انها الوده کردن کاربرانی که از نسخه های هک شده نرم افزار انها استفاده میکردند نبوده بلکه مایل بودند بدینگونه اماری از تعداد نسخه های هک شده که استفاده میشدند تهیه نمایند .

اما انچه که هرگز تصورش را نمیکردند این بود که هزاران نفر به دام این ویروس افتاده و با انها تماس بگیرند. این تماسها باعث اشباع خط تلفن انها شده و این داستان خبر مهمی برای رسانه ها گشت.

"Brain"یک ویروس بوت و همچنین اولین ویروس فرار یا مخفی است که روی سکتور ۰ دیسکت نصب شده و سکتور اصلی را در سکتوری خالی کپی میکند. هر تلاش برای خواندن سکتور ۰ یک دیسکت الوده شده با کامپیوتری که حافظه اش حاوی این ویروس است, به سمت سکتور بوت هدایت میشود. این ویروس کاری بجز الوده کردن سکتور بوت انجام نداده و بار مخرب ندارد ., ویروس "Brain" در سکتور بوت دیکست هر برنامه ای که به کشورهای خارجی فروخته میشود نصب شده و لابل این دیسکتها با Brain (c)جایگزین میشود .

بعدها در ۲۲ اکتبر ۱۹۸۷ نسخه های متفاوتی از ویروس "Brain" متولد شده و در دانشگاه Delaware نیز این وبروس کشف شد. در ژوئیه سال ۱۹۸۹ Brain ,یکی از ده ویروسی بود که مک افی انرا عامل نود درصد الودگیها در جهان اعلام کرده بود .

و اما ایندو بردار سازنده Brain همچنان در پاکستان در زمینه انفورماتیک فعالیت داشته و شرکت خدماتی اینترنت به نام Limited5را دارند که یکی از معروفترین شرکتهای خدماتی اینترنت در پاکستان است .

Lehigh-۳

با اولین میکرو کامپیوترهای سازگار با IBM PC تعداد ویروسها بطور محسوسی افزایش یافت .

این پلاتفرم جدید انفورماتیک با Apple II مکینتاش بطور انبوه به شرکتها و دانشگاه ها و خانه ها راه یافته و در این راستا توسعه دهندگان برنامه ها نیز الدورادوی جدید خود را یافته و سالهای ۱۹۸۷ و ۱۹۸۸ و ۱۹۸۹ از نظر ویروسهای جدید غنی شد.

بدینگونه ویروس "Lehigh" در نوامبر ۱۹۸۷ در دانشگاهی به همین نام در ایالات متحده امریکا کشف شد. ا

این ویروس فقط فایل Command.com را الوده کرده و قسمتی از چهارمین نسل FAT را تخریب میکرد. از این نظر این ویروس اولین ویروسی بود که به صورت موثری به داده ها اسیب میزد.
اما ویروس Lehigh از دانشگاه Lehigh خارج نشده و انتشار نیافت ولی باعث تحقیقات بسیاری شد .

Lehighتوسط دانشجوئی یا یکی از همکاران دکتر Fred Cohen ساخته شده بود.

Stoned-۴

در سال ۱۹۸۷ ویروسهای دیگری ظهور کردند که از ان میان میتوان از "Stoned " ملقب به "Marijuana" نام برد که ویروسی نیوزلندی بوده و MBR را الوده میکرد.
به هنگام استارت کامپیوتر پیام "Your PC is now Stoned" نمایش داده میشد.
Stonedویروس کوچک چند اکتت (octet) بود که سریعا یکی از ویروسهائی گشت که در همه جهان بسیار منتشر شده بود.

ping-pong-۵

در سال ۱۹۸۷ ویروس دیگری که یک ویروس سکتور بود در دانشگاه تورین در ایتالیا کشف شد.

این ویروس یک توپ کوچک که روی لبه های صفحه نمایش به هوا میرفت را نشان میداد و به همین دلیل "Ping-Pong" نامیده شده بود.

۶-Vienna

ویروس "Vienna" نیز در سال ۱۹۸۷ ظاهر شده و بسیار معروف شد.

راز منشاء این ویروس باعث شد تا بسیار در رسانه ها از ان صحبت شود. اما فقط از این نظر جالب بود که اولین ویروسی بود که برای مقابله با ان ابزاری ساخته شد.
Bernt Fixسازنده ابزار مقابله با ویروس "Vienna" را میتوان پدر متخصصین جدید مقابله با ویروسها دانست.
کد "Vienna" در کتابی از Ralph Burger به نام "Computer Virus: The Disease of High Technology6" منتشر شد.

۷- Suriv و Jerusalem

ویروس "Suriv"و انواع ان توسط ناشناسی در اسرائیل و در سال ۱۹۸۷ ساخته شده بود .هدف از ساخت ان مبهم بود اما به نظر میرسد که این ویروس حاصل تجربیاتی بوده است.
اولین نوع این ویروس که "Suriv-1" نام داشت میتوانست فایلهای COM را الوده کند.

"Suriv-2"فایلهای اجرائی EXE را الوده میکرد.
"Suriv-3"ترکیبی از دو نسخه اولیه این ویروس یعنی "Suriv-1" و "Suriv-2" بوده و بدینگونه میتوانست هم فایلهای COMو هم EXE را الوده کند.
"Suriv-4"هم بعد از سه نسخه اولیه ویروس Suriv کشف شده و بیشتر با نام "Jerusalem" شناخته میشد.

"Jerusalem"یک ویروس DOSبود که در اکتبر ۱۹۸۷ و در اورشلیم کشف شد. این ویروس بعد از الوده کردن کامپیوتردر حافظه باقی مانده و هر یک از فایلهای برنامه هائی که اجرا میشدند را الوده میکرد. اما در واقع برای تخریب این فایلها تاریخ بخصوصی داشت و فایلهای هر برنامه ای که یک روز جمعه که به تاریخ ۱۳ ماه بود انجام میشد را الوده میساخت.

"Jerusalem"هم انواع مختلفی داشت و همه نسخه های متفاوت ان سریعا در تمام جهان منتشر شدند و سالها بعنوان یکی از ویروسهای بسیار رایج باقی ماند

۸-Cascade

ویروس "Cascade" یکی از وقایع مهم سال ۱۹۸۷ بود.
ویروس "Cascade" به دلیل اینکه بعد از فعال شدن حروف را به پائین صفحه نمایش میراند بدینگونه نامیده شد.
این ویروس از دو قسمت تشکیل شده بود که بدنه ان برنامه رمزنگاری ۳۵ اکتت بود تا ظاهری متفاوت به هر فایلی که الوده میکرد

بدهد. بدینگونه "Cascade" اولین ویروس پلیمورف بود چون شکل ظاهری متفاوتی به فایلهای الوده میداد. بعد از اجرا, برنامه رمزنگاری بدنه ویروس را دیکد کرده و سپس فرمانها را به ان میداد.
نتایج حاصل از الودگی با این ویروس, ای بی ام را ناچار ساخت تا انتی ویروسی برای عموم بسازد.

هجوم کرم های انفورماتیک

در سال ۱۹۸۷ اینترنت یک شبکه انفورماتیک با حدود شصت هزار کامپیوتر و صد هزار کاربر بود.
شبکه های بزرگ به یکدیگر کانکت میشدند و استفاده از ایمیل و یوزنت (مجموعه پروتکل هائی برای تولید و ذخیره و دسترسی به مقالات و پیامهائی که از نظر ساختاری شبیه هستند و تبادل انها بین اعضای گروه ها) عمومیت یافت.
در همین زمان و وضعیت مناسب بود که کرمهای بسیاری ظهور کردند

IBM Christmas Tree (a

نام اولین کرم انفورماتیک "IBM Christmas Tree" بود که در نهم دسامبر سال ۱۹۸۷ روی شبکه EARNetیا European Academic Research Networkمنتشر شد.
سازنده ان یک دانشجوی المانی بود که گفته بود هدف از ان ارزوی کرسمسی شاد برای رفقای دانشگاهیش بوده است.
اما متاسفانه در کمتر از یک هفته یعنی در ۱۵ دسامبر ۱۹۸۷ این کرم روی شبکه EARNet منتشر شده و به مدت دو روز شبکه پیام رسانی خصوصی VNET ای بی ام را فلج کرد.
IBM Christmas Treeبصورت ایمیلی که فایل پیوستی به نام "Christma Exec" داشت بود. با اجرای ان, تبریک کریسمس نمایش داده شده و سپس یک کپی از خود را برای همه ادرسهائی که در دفترچه ادرس کاربر بودند ارسال میکرد.
موضوع ایمیل ارسالی "Let this exec run and enjoy yourself!" بود.

```
                *
               ***
              *****
             *******
            *********
           ***********                A
          *************
         ***************             VERY
        *****************
       *******************           HAPPY
      *********************
     ***********************         CHRISTMAS
    *************************
   ***************************       AND MY
  *****************************
 *******************************     BEST WISHES
*********************************
               ***                   FOR THE NEXT
              *****
             *******                  YEAR
            *********
           ***********
```

RTM Worm (b

در شب 2نوامبر ۱۹۸۸ حدود ساعت ۱۸ برنامه ای که بطور خودکار خود را تولید میکرد توسط کامپیوترهای prep.ai.mit.edu,لابراتوار هوش مصنوعی ام ای, تی روی نت منتشر شد.
یکساعت بعد, یک روتر دانشگاه برکلی نیز به نوبه خود الوده گشت.

حدود ساعت ۲۰ به سرور فینگر دانشگاه مریلند نیز حمله شد.
ساعت ۲۳ Peter Yee ,از مرکز تحقیقات ناسا ایمیل هشداری که در ان از حمله ای الوده کننده خبر میداد ارسال کرد و توصیه نمود که سرویسهای telnet, ftp, finger, rsh و SMTP روی کامپیوترها مسدود گردند .

سراسر روز سوم نوامبر این سال سیستمهای انفورماتیک چندین دانشگاه و مراکز تحقیقاتی امریکائی از کار افتادند.
چهارم نوامبر حدود ساعت ۶ یک گروه از پژوهشگران دانشگا برکلی دیکماپیل و انالیز این کرم را تمام کرد. بیلان سنگین بود. حدود ۶۰۰۰ کامپیوتر الوده شده و خسارات وارده بین ۱۰ و ۱۰۰ میلیون دلار تخمین زده شدند .

کرم عامل این خرابیها "RTM Worm"بود که توسط یک دانشجوی ۲۳ ساله دانشگاه کرنل به نام Robert Tappan Morrisبه زبان C نوشته شده بود. این کرم به کامپیوترهای VAX و SUN-3با سیستمهای UNIX BSD یا SunOS حمله میکرد.
Robert Tappan Morrisپسر Robert Morrisو یکی از مخترعین بازی داروین است که در اینزمان رئیس بخش National Computer Security Centerکه یکی از بخشهای سازمان امنیت ملی امریکا است بود.

"RTM Worm"برای انتشار خود روی شبکه ها از اسیب پذیری سیستمهای UNIX BSDو SunOS استفاده میکرد و عملکردی سه مرحله ای داشت:

-یافتن شبکه و کامپیوترهای کانکت
-استفاده از اسیب پذیری سیستمها
-کانکشن به کامپیوتر هدف و ارسال یک کپی از کرم
-کمپایل و اجرای کپی کرم روی کامپیوتر هدف

"RTM Worm"لیست کامپیوترهای قابل دسترس توسط شبکه را با جستجوی فایلهای تنظیمات سیستم چون etc/hosts.equivیا با استفاده از اطلاعات روتاژ داینامیک توسط netstat بدست اورده و برای رخنه در یک کامپیوتر و خود را روی ان کپی کردن سه راه داشت که استفاده از اسیب پذیری سرویس فینگر و یا استفاده از قابلیتی مخفی در سرور sendmail و یا اگر موفق به یافتن رمز عبور یک اکانت محلی و رخنه به کامپیوتری میشد از سرویسهای rexec و rsh استفاده میکرد.
"RTM Worm"بعد از کپی شدن روی یک کامپیوتر جدید خود را کمپایل و اجرا میکرد .

ضربه مهم این کرم بیشتر به این خاطر بود که ادمینیستراتورهای کمی از خطرات مربوط به برنامه هائی که بطور خودکار خود را تولید یا کپی میکردند اگاه بودند.

همین واقعه باعث ایجاد CERT یا Computer Emergency Response Team گشت .

گزارش کمیسیون تحقیقات روی حادثه کرم اینترنت که توسط مدیر دانشگاه پراوست تهیه شده بود اینطور نتیجه گیری کرده بود که واقعا Robert Tappan Morrisاین کرم را ساخته و قانون استفاده های خوب از انفورماتیک دانشگاه را نقض نموده و هدف وی تحریب داده ها نبوده است .

از نظر قانونی نیز اینطور رای داده شد که وی) Computer Fraud and Abuse Act این قانون در سال 1986و با هدف کاهش هک سیستمهای اطلاعات توسط کنگره امریکا تصویب شده و در سالهای ۱۹۹۴ و ۱۹۹۶ و ۲۰۰۱ با قانون USA PATRIOT Actاصلاح شد) را نقض نموده و به چهارصد ساعت کار برای منافع عمومی و یک دوره سه ساله مشروط و ده هزار دلار جریمه محکوم شد.

Father Christmas Worm (C

یکماه بعد از ,RTM Worm در بیست و سوم دسامبر سال ۱۹۹۸, شبکه SPAN یعنی Space Physics Analysis Networkناسا نیز به نوبه خود توسط کرمی فتح شد .

این کرم "Father Christmas Worm" نام داشت و همانند IBM Christmas Treeبرای تبریک کریسمس و همراه با پیامی کوتاه بود.

```
HI,
How are you? I had a hard time preparing ale the presents.
It isn't quite an easy job. I'm getting more and more letters...
Now stop computing and have a good time at home!!
Merry Christmas and a Happy New Year
Your Father Chritmas
```

"Father Christmas Worm"سیستمهای VMS شرکت DEC را توسط پروتکل DECnet هدف خود کرده بود.

روش انتشار ان ساده بود .این کرم از حساب کاربری پیشفرض DECnet برای کپی اسکریپت کرم روی سیستم هدف استفاده کرده و با یکی از قابلیتهای DECnetیعنی ,TASK 0 از راه دور این اسکریپت را اجرا میکرد و سپس منتظر ۲۴ دسامبر برای ارسال ایمیل تبریک میماند.

WANK (d

بعد از کرمهای انفورماتیکی که تبریک کریسمس سازنده خود را منتشر میکردند, کرمهائی برای انتشار ایدئولوژیها ظهور کردند.

در ۱۶ اکتبر ۱۹۸۹ CERT ,پیامی از گره کنترل شبکه SPAN دریافت کرد که در ان گفته شده بود که کرمی به پلاتفرمهای DEC VMSحمله کرده است. این کرم شبیه "Father Christmas Worm" بود و "WANK" نام داشت.

"WANK"توسط پروتکل DECnet انتشار میافت و چندین عمل روی سیستمی که الوده میکرد انجام میداد:

-از اینکه در دایرکتوری ای که در ان دسترسی برای خواندن و نوشتن و اجرا داشت اطمینان یافته و این موضوع را کنترل میکرد

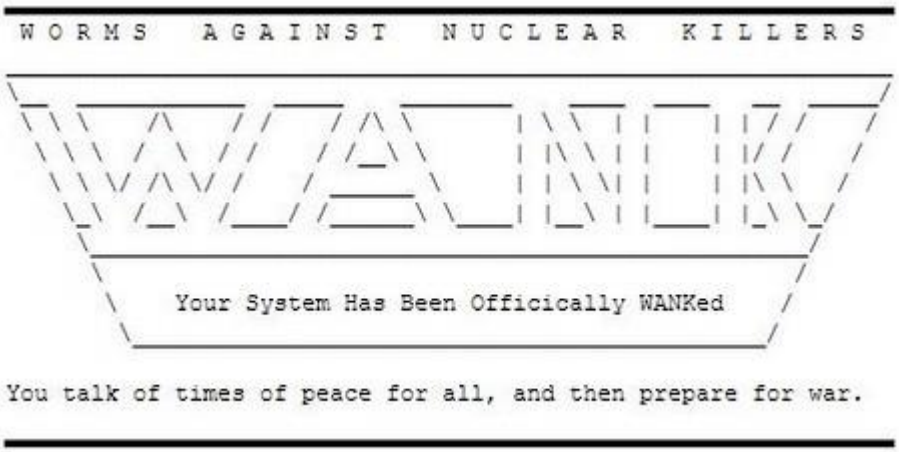
-وجود احتمالی یک کپی از خود را روی سیستم تست میکرد

-رمز عبور پیشفرض را با حداقل ۱۲ کاراکتر تصادفی تغییر میداد

-رمز عبور جدید را با ایمیل برای کاربر GEMPAK روی کامپیوتر ارسال مینمود

-نام پروسس خود را به _NETW و یک عدد تصادفی در اخر ان تغییر میداد

-بنر استقبال سیستم را در صورتیکه اجازه ها یا امتیازات SYSNAM را داشت را عوض میکرد و انچه را که در تصویر زیر مشاهده میشود را نمایش میداد



-اگر سیستم اجازه های SYSPRIV را داشت, قابلیت ایمیل برای ارسال به اکانت سیستم را غیر فعال نموده و فرمان لاگین سیستم را تغییر میداد تا به هنگام کانکشن به کاربر اینطور وانمود کند که در حال تخریب فایلها است .

-لیست اکانتها را اسکن کرده و تلاش میکرد تا رمز عبورها را تغییر دهد

-تلاش میکرد تا با استفاده از یک شماره گره تصادفی و لیستی از رمز عبورهای پیشفرض به سایر کامپیوترها دسترسی پیدا کند

در ۱۷ اکتبر CERT, اطلاعیه CA-89:04 که این کرم را توصیف میکرد و روش حذف انرا منتشر کرد و در عین حال توصیه های احتیاطی و برای هوشیاری به هنگام حمله کرم در مورد ایمن ساختن رمز عبورها میکرد.

اولین آنتی ویروس ها

در اواخر سالهای ۸۰ ,چندین سال از ویروس شناسی انفورماتیک میگذشت اما مجمع متخصصین امنیت انفورماتیک در مورد خطرناک بودن انها بطور جدی, به دو دسته تقسیم میشدند.

دکتر Alan Solomon در تاریخ ویروسهای انفورماتیک خود تعریف کرده است که چگونه در سال ۱۹۸۸ ,Peter Norton , توسعه دهنده نرم افزار Norton Utilities در مصاحبه ای گفته بود که ویروسهای انفورماتیک افسانه ای شبیه تمساح هائی است که در فاضلاب های نیویورک زندگی میکنند!

سال ۱۹۸۸ سالی بود که بسیاری از شرکتهائی که نرم افزارهای انتی ویروس میفروختند ظهور کردند. این شرکتها معمولا متشکل از دو یا سه نفر بودند و نرم افزارهای انها یک اسکنر ساده بود که جستجوی متنی میکرد تا سکانسهائی مخصوص از کد ویروسی را بیابد.
این محصولات به مبالغی بسیار ارزان و بین پنج تا ده دلار بفروش میرسیدد و اغلب همراه با برنامه ای برای ایمن سازی همراه بودند که برای مقابله با ویروس ها به ویروس وانمود میکرد که کامپیوتر پیشتر الوده شده است .
اما متاسفانه برای هر ویروس, برنامه ایمن سازی یا مقابله با فقط همان ویروس بود و بدینگونه این ابزار با افزایش فوق العاده ویروسهای انفورماتیک, برای مقابله با سرایت ویروسها کافی نبودند. از طرفی همانطور که بالاتر توضیح داده شد, بعضی حرفه ای ها و متخصصین از نیاز به محافظت در مقابل ویروسها اگاه نبودند و بدینگونه با انتشار ویروسهائی چون ,Jerusalem Cascade, Stonedیا ,Vienna نتیجه اسفناک بود.

اولین سلاح های جدی تر برای مقابله با ویروسهای انفورماتیک

به تدریج مبارزه با ویروسهای انفورماتیک سازماندهی شد.

در ۲۲ اوریل ۱۹۹۸ ,Ken Van Wyk, یکی از شرکای) Fred Cohen انفورماتیسینی که بیشتر بعنوان مخترع تکنیکهای دفاعی در مقابل ویروس معروفیت دارد), اولین فروم الکترونیک برای مبارزه با ویروس را ایجاد کرد. این فروم "Virus-L" و روی شبکه یوزرنت بود.

در ژوئیه ۱۹۸۹ Virus Bulletin Ltd ,با حمایت Sophos راه اندازی شد.

Virus Bulletinمجله ای ماهیانه بود که خیلی زود در جهان معروف گشت و اطلاعاتی تکنیکی در مورد ویروس ها و انتی ویروسها و کمی دیرتر نیز مقایسه مستقل محصولات ضد ویروس را ارائه میکرد. اولین شماره ان در ژوئیه ۱۹۸۹ منتشر شده و چهارده ویروس برای IBM PC و ده ویروس برای Macintosh را قید کرده بود .

اولین انتی ویروس در سال ۱۹۸۸ متولد گشته و "Anti-Virus Toolkit" نام داشت. این برنامه بسیار محبوب بوده و بصورت گسترده ای در جهان استفاده میشد.

"Anti-Virus Toolkit"حاصل کار و تلاش یک انفورماتیسین انگلیسی به نام دکتر Alan Solomon بود .همزمان وی شرکت خود به نام Virus Fax International را که بعدها نام ان به Secure Computingتغییر یافت را تاسیس نمود .

امروز هنوز Secure Computing یکی از منابع اطلاعاتی در مورد پرسشهای امنیت انفورماتیک محسوب شده و بسیار محبوبیت دارد.

Secure Computingهر ساله مسابقه ای با عنوان "Secure Computing Awards" بر پا میکند که به بهترین توسعه دهندگان در بخشهای گوناگون که یکی از انها امنیت انتی ویروس است جایزه میدهد.

در همین سال, ای بی ام که سایت Lehulpe ان بطور جدی توسط ویروس cascade الوده شده بود, تصمیم گرفت تا ابزار و وسایلی برای مبارزه با ویروس ها تهیه کند. در این راستا ای بی ام ازمایشگاه خود High Integrity Computing" ,

"Laboratory"واقع در Yorktown که Steve White انرا اداره میکرد را برای ماموریت تخصص و تحقیق در این زمینه مامور کرد .

خیلی سریع ای بی ام صاحب یک برنامه انتی ویروس برای استفاده داخلی شد. اما با اصرار شرکتهای بزرگ و مهم مشتری و در رابطه با خطرات ویروسهای Jerusalemو ,Datacrime ای بی ام این انتی ویروس خود "IBM V SCAN" ,را در چهارم اکتبر ۱۹۸۹ و به مبلغ ۳۵ دلار تجاری کرد.

اولین نسخه IBM V SCAN بیست و هشت ویروس را شناسائی میکرد و شامل سه فایل میشد:
.

- VIRSCAN.EXE - برنامه انتی ویروس - ۴۴ ۹۸۳octets

- SIGFILE.LST - پایگاه امضای ویروس های فایلها - ۲ ۸۷۳octets

- VIRSCAN.EXE - پایگاه امضای ویروسهای سیستم - ۹۸۰octets

در اکتبر سال ۱۹۸۹ ,Eugene Kaspersky, مهندس روسی, متوجه شد که کامپیوترش با ویروس Cascade الوده شده است. این حادثه باعث شد تا در صدد ساختن برنامه ای برای از بین بردن ان براید. انتی ویروس وی به نام "V-" کاملتر گشته و یکماه بعد میتوانست ویروس "Vacsina" را بیابد.

چند سال بعد "V-" به "AVP Antiviral Toolkit Pro"تبدیل شد و کسپرسکی شرکت خود که در مبارزه با ویروسها تخصص دارد را با نام "Kaspersky Lab" تاسیس کرد.
در سال ۱۹۸۹ انتی ویروسهای دیگری نیز متولد شدند که میتوان از F-Prot, ThunderBYTE و یا VirusScanکه توسط مک افی بصورت) shareware نرم افزاری غیر رایگان که برای مدتی محدود بصورت رایگان و معمولا با قابلیتهائی محدود برای ازمایش ان در دسترس کاربران قرار داده میشود) توزیع شد نام برد.

ویروس بر علیه ویروس

نمونه ویروسهائی برای از بین بردن ویروسهای دیگر زیاد نیستند اما با اینهمه میتوان از یکی از انها به نام "Den Zuk" نام برد.

"Den Zuk"در باندونگ واقع در اندونزی و توسط Denny Yanuar Ramdhani توسعه یافته و یک ویروس بوت برای سلام دادن از جانب سازنده خود بود.
زمانیکه کاربر کامپیوتر الوده همزمان روی دکمه های CTRL+ALT+DEL کلیک میکرد, پیامی به مدت چند ثانیه نمایش داده شده و سپس کامپیوتر ریستارت میکرد.

گوئیا که در زبان اندونزی den zuk به معنای محقق است .

"Den Zuk"توانائی حذف ویروس "Brain" را داشت و علاوه بر این میتوانست دیسکت ها را در قبال حمله مجدد ویروس Brainواکسینه کند. برای اینکار لابل Brainدیسکتهای الوده به "YC1ERP23"تغییر میافت.
در عین حال ویروس "Den Zuk" نسخه قبلی خود که به نامهای Ohio و Hacker بودند را نیز حذف میکرد.
ویروس Den Zucko در ایالات متحده امریکا و ونزوئلا یافت شده بود.

منابع مورد استفاده

کتاب ویروسهای انفورماتیک : تاریخچه, ویروس بیولوژیک و انفورماتیک, تئوری و توسعه یک کرم مفید, نوشته میشل دوبوا

با تشکر از مدیر وب سایت ترفندستان : مهندس کسری مقبلی

نویسنده و مترجم: ZzBb

تهیه و تنظیم:محمود ۸۰۸۰

بهمن ماه ۹۷