جلسه نخست : تهدیدها در دنیای دیجیتال

تهیه کننده: نیما راشدان

جلسه نخست : تهدیدها در دنیای دیجیتال

رواج استفاده کامپیوترهای شخصی از دودهه پیش تا امروز، در عین مزایای بی شمار حامل خطرات و تهدیدهای جدی برای کاربران بوده است. کاربران کامپیوترهای شخصی، خصوصا پس از معرفی اینترنت و شبکه جهانی وب همواره در معرض خطراتی متفاوتی با هدف سرقت اطلاعات شخصی، هویت و داده های مالی قرار گرفته اند .گروههای جنایتکار اینترنتی متشکل از ماجراجویان ساده گرفته تا افراد و گروههای سازمانیافته، دولتهای سرکوبگر و سازمانهای تروریستی هر روز بر تنوع و پیچیدگی شیوه های خود در حمله علیه کاربران کامپیوترهای شخصی افزوده اند. در عین حال فن آوری حفاظت از کامپیوترهای شخصی در برابر این تهدیدات نیز دانشی در حال پیشرفت است. شرکتهای تولید کننده سخت افزار، نرم افزار و ارائه دهندگان سرویسهای آنلاین به مدد شبکه گسترده ای از کاربران و همچنین تجربه دو دهه دفاع در برابر حملات اینترنتی، هر روز فرآورده ها و سرویسهای مطمئن تری ارائه می دهند. دولتها در جهان آزاد نیز به یاری کاربران کامپیوترها آمده با وضع و اصلاح قوانین مربوط به جنایات سایبر، هرزه نگاری و دیگر حملات.
عرصه را بر انتشار دهندگان این تهدیدات تنگ تر کرده اند چنانکه بسیاری از جنایتکاران اینترنتی ناچار از فعالیت در مناطقی گردیده اند که از فقدان دولت منتخب و کارآمد رنج می برند.

تهدیدات کامپیوتری می توانند حاصل عملیات یک یا چند منبع ذیل باشند:(1)

هکرها و ماجراجویان کامپیوتری:
آپریل 2004 انتشار ویروس Sasser توسط نوجوان 17 ساله آلمانیSven Jaschan

باندهای جنایت سازمان یافته کامپیوتری
2007تا 2009، کشف باند صدنفره سرقت اطلاعات و وجوه بانکی در ایالات متحده و مصر

گروههای خرابکار مرتبط با دولتهای غیرآزاد
حملات اینترنتی گروههای مرتبط با روسیه علیه دولت استونی 2007 و گرجستان 2008

سازمانهای اطلاعاتی دولتهای سرکوبگر
حملات اینترنتی علیه سایتهای بالاترین، توییتر و هزاران حمله دیگر توسط سپاه پاسداران انقلاب اسلامی 2009، کشف شبکه ارواحGhost net ، جاسوسی اینترنتی احتمالا توسط دولت جمهوری خلق چین از دولت تبت در تبعید و صدها سفارتخانه، سازمان و شخص، راه اندازی سایت جاسوسی اینترنتی- گرداب توسط سپاه پاسداران انقلاب اسلامی ایران

طبقه بندی خرابکاران و جنایتکاران سایبر

کارشناسان روشهای مختلفی را برای طبقه بندی، افراد و یا گروههای تولید کننده تهدیدات سایبر به کار برده اند. یک روش نسبتا قدیمی خرابکاران را به سه گروه : مبتدی، نسبتا حرفه ای و الیت یا نخبه تقسیم بندی می کند. در طبقه بندی های جدیدتر نظیر طبقه بندیDonn Parker(2) ، افراد بر اساس انگیزه شان از خرابکاری، نفوذ و یا سرقت اینترنتی به هفت گروه افراز می شوند:

- خرابکاران با انگیزه شیطنت و بدجنسی
- گروهها یا افرد هکر با انگیزه کنجکاوی و یا شیطنت
- گروهها یا افراد هکر با انگیزه تخریب و نابودی، لذت از ویرانی و اخلال
- افرادی که به دلیل نومیدی از راهکارهای قانونی اطلاعات یا اعمال مورد نظر خود را با خرابکاری سایبری به دست می آورند
- خرابکاران حرفه ای سایبر، به صورت حرفه ای و مانند شغل دارای انگیزه مالی، به خرابکاری سایبری می نگرند

- فعالان تندرو و افراطی، که بدلیل تعلق به یک گروه یا عقیده سیاسی، مذهبی، اجتماعی اقدام به خرابکاری می کنند
- افراد نامتعادل و بیمار به لحاظ روانی ، که به دلیل مشکلات روحی – درونی اقدام به اعمال ضداجتماعی در حوزه سایبر می نمایند

علاوه بر افراد و گروههای تبهکار در سالهای گذشته، دولتهای سرکوبگر، حکومتهای حامی تروریسم و سازمانهای تروریستی نیز به صورت فزاینده ای وارد جنگهای سایبری شده اند. در ماه مارچ سال 2010، وزیر فرهنگ و ارشاد اسلامی ایران در کنفرانسی به نام « هم آیش 8 ماه جنگ اینترنتی»، رسما تعلق ارتش سایبری به سپاه پاسداران انقلاب اسلامی ایران را تایید کرد. سپاه پاسداران انقلاب اسلامی نیز به نوبه خود با تاسیس سایتی به نام گرداب خواستار همکاری کاربران اینترنت و جذب فعالان جوان برای مشارکت در پروژه های جنگ سایبری سپاه گردید. گرچه در جریان برخورد با سایتهای اینترنتی، تنها از شیوه های سایبری استفاده نشد و شیوه هایی چون شکنجه، حبس انفرادی طولانی مدت، تهدید به اعدام و قتل اعضای خانواده نیز علیه فعالان ایرانی سایتهای اینترنتی به کار گرفته شد.(3)

پدیده دیگر قابل مشاهده تبدیل فعالان اینترنتی تحت فشار به بازجویان و تبهکاران اینترنتی است. در سال 2003 میلادی روزنامه نگار و فعال اینترنتی به نام « پیام فضلی نژاد » با ارسال ایمیلی با من تماس گرفته و خواستار گفتگوی تلفنی شد. پس از رد این درخواست، اخبار منتشره در رسانه های ایران نشان داد. فضلی نژاد پس از بازداشت، روند همکاری با بازجویان را آغاز کرده بیش از 6 سال است در یک مجموعه نبرد علیه وبلاگها، رسانه های و چهره های سیاسی منتقد فعالیت می نماید. او همچنین عملیات تخریب فعالان اینترنتی را در قالب انتشار یادداشتهایی در روزنامه کیهان و کتبی چون : شوالیه های ناتوی فرهنگی پی گرفته است.

روشهای غیرتکنیکی نفوذ و اخذ اطلاعات

جنایتکاران عموما برای کسب اطلاعات و یا نشر اطلاعات آلوده خود، از روشهای تماما تکنیکی و سایبر استفاده نمی کنند. در بسیاری از موارد فرد یا افراد هرچند درستکاری از داخل مجموعه شما، نردبان دستیابی جنایتکاران به اطلاعات و داده ها می شوند.در سال 2010 خرابکاران ارتش سایبری سپاه، عملیات هک رادیو زمانه – رادیوی فارسی زبان مستقر در هلند – را همزمان با چت Gmail با یکی از کارمندان آن رادیو جلو می بردند.

در اینجا برخی از روشهای معمول مورد استفاده خرابکاران برای دسترسی به اطلاعات شما را توضیح می دهیم.

مهندسی اجتماعی

مهندسی اجتماعی مبتنی بر دروغ و تقلب است. مهندسی اجتماعی طراحی و اجرای روشهایی است که شما و یا فعالان همکار شما را وا دارد تا داوطلبانه تمام و یا بخشی از اطلاعات مورد نیاز جنایتکاران را در اختیار ایشان قرار دهند.

کاربرد مهندسی اجتماعی برای اخذ اطلاعات و نفوذ داخل سیستم توسط شیوه هایی نظیر فهرست ذیل اعمال می گردد(4) :

1– دروغگویی :

در بسیاری از موارد با می توان افراد را با چند دروغ ساده فریفت و زمینه دسترسی به اطلاعات ایشان را فراهم آورد. یک مثال بسیار ساده به دست آوردن رمز عبور ایمیل شماست. بسیاری از افراد به سادگی، تاریخ تولد، شهر تولد و دیگر اطلاعات به ظاهر غیرحساس را در صفحات فیس بوک خود منتشر کرده یا در هنگام چت در اختیار افراد ناشناس قرار می دهند. بدون آنکه تصور کنند با در دست داشتن این اطلاعات، خرابکار سایبری می تواند به سرویس ایمیل شما مراجعه کرده و با ادعای گم کردن رمز عبور، رمز عبور جدیدی دریافت دارد.

الف : دروغگویی به شیوه مقام مسئول

در این روش جنایتکار خود را به جای یکی از مسئولین موسسه یا گروه شما جا می زند و خواستار دسترسی به اطلاعات موسسه می شود. بطور مثال در چت با شناسه رئیس یک روزنامه اینترنتی وارد شده و از مسئول فنی می خواهد، رمز عبور Passwordروزنامه راتغییر و رمز جدید را جهت اطمینان و حفظ برای او ایمیل نمایند.

ب : دروغ گویی به شیوه شخص ثالث

در این روش جنایتکاران سایبری، خود را به عنوان کارمندان یک موسسه ثالث جا می زنند، مثلا اگر دومین و هاست شما را دو شرکت مختلف سرویس دهی می کنند به عنوان کارمندان شرکت دومین از شما خواستار ارائه اطلاعات مربوط به هاست می شوند و یا بالعکس. نمونه ساده آن، روشهایی است که سارقان برای ورود به ساختمان شرکتها استفاده می کنند : پوشیدن لباس شبیه ماموران، برق، تلفن و یا نظافتچیها.

خرابکاری درونی :

جنایتکاران برای دستیابی به اطلاعات مورد نیاز خود، قربانی و یا نزدیکان وی را به شیوه هایی اینچنینی تحت فشار قرار می دهند تا زمینه همکاری و نفوذ فراهم گردد.

الف : رشوه

به سادگی فرد مورد نظر یا یکی از همکاران او با پرداخت رشوه تطمیع می شود تا اطلاعات مورد نیاز را در اختیار آنان قرار دهد، شایان توجه است که پرداخت رشوه غالبا به صورت مستقیم برای دریافت اطلاعات صورت نمی گیرد. رشوه به صورت هدیه ای غیرمعمول در ازای دریافت کمکی بسیار جزئی و بی خطر پیشنهاد می شود. آن کمک کوچک زمینه دسترسی جنایتکاران به اطلاعات بعدی را فراهم خواهد آورد.

ب : فریب و اغواء

از روشهای بسیار معمول جنایتکاران، ظاهر شدن در قالبی دروغین، مثلا دختران و زنان جذاب، استفاده از پروفایل جذاب در شبکه های اجتماعی و ریختن طرح دوستی و سوء استفاده از احساسات درونی انسانی قربانیان است.

ج : تهدید

تهدید خانواده یا شخص قربانی، به خشونت فیزیکی یا از بین بردن اموال ایشان از روشهای معمول تبهکاران است. این روش در حکومتهای سرکوبگر به صورت گسترده به کار گرفته می شود. در سال 2004 گروهی از وبلاگ نویسان ایرانی بازداشت شدند. بازجویان با حبس آنان در سلولهای انفرادی، شکنجه و ضرب و شتم ایشان، تهدید به تجاوز و شکنجه خانواده ازآنان خواستار اطلاعات فنی، رمزهای عبور و دیگر مشخصات سایتهای اینترنتی منتقد گردیدند.

د : باجگیری

باجگیری با تهدید قربانیان به افشای عمومی اطلاعات خصوصی و اسرار ایشان صورت می پذیرد. به طور مثال تبهکاران با دستیابی به فیلم یا تصاویر بسیار خصوصی افراد، آنان را تهدید می کنند در صورت عدم همکاری این تصاویر در اختیار نزدیکان، اعضای خانواده و یا افکار عمومی قرار خواهد گرفت.

علاوه بر تهدیدهای ذکر شده در بالا، نفوذ به سازمان و یا نهاد شما می تواند به سادگی با نفوذ شخصی تبهکاران به عنوان عضو، هوادار، داوطلب و غیره صورت پذیرد.خصوصا در مواردی که افراد ناشناس بدون استفاده از نام حقیقی و با شناسه مجازی فعالیت می کنند. در سال 2010 جمعی از فعالان اینترنتی ایران در جلسه ای خصوصی تصمیم گرفتند سایت اینترنتی با نام « ایران رسا » تاسیس کنند. ساعتی پس از این جلسه تمام دامنه های ایران رسا توسط سازمانهای

اطلاعاتی ایران رجیستر شده بود. نمونه فوق نفوذ بسیار ساده تبهکاران به گروههای فعال را در قالب داوطلب و هوادار به نمایش می گذارد.

مقابله با روشهای مبتنی بر مهندسی اجتماعی

مقابله با روشهای مبتنی بر مهندسی اجتماعی ، نیازمند پیش بینی، مصون سازی و آموزش است. در این بخش می کوشم تا با ذکر مثالهایی واقعی به ایجاد نوعی « درک مقابله با تهدیدهای مبتنی بر مهندسی اجتماعی» کمک کنم.

توصیه اول : این سوال را چند بار از خود بپرسید : آیا او همان کسی که ادعا می کند؟

در هنگام مواجهه با یک دوست جدید اینترنتی، یک پیام، یک ایمیل حاوی درخواست دوستی، یک تصویر و یا ارتباط اتفاقی اسکایپ، بدون هیچ رودربایستی سوالات زیر باید پرسیده شود؟ آیا شما را می شناسم؟ قبلا شما را دیده ام؟ از کجا شناسه و تماس مرا یافتید؟ سوالات بالا نیازمند جواب روشن و بدون ابهام هستند.

پاسخ اول : مثلا: بله؛ من محمد امیری همکلاسی شما در دانشکده کامپیوتر دانشگاه علم و صنعت ایران ورودی 1380 هستم! این پاسخ نوعی پاسخ قابل قبول تلقی شده و وظیفه بعدی تحقیق درباره صحت این ادعا خواهد بود.

پاسخ دوم : چطور منو نمی شناسی؟ چه اهمیتی داره کی هستم؟ حالا یک کم گپ بزنیم خودت می فهمی من کی هستم! این نوع پاسخها، پاسخ غیرقابل قبولند. تنها واکنش به این نوع درخواست : قطع ارتباط است بدون هیچ توضیح اضافی.

موضوع بسیار حائز اهمیت در مقابله با این روشها توجه به دو نکته در شیوه های حرفه ای کسب اطلاعات توسط تبهکاران و یا عوامل دولتهای سرکوبگر است:

نکته اول : آنان همه اطلاعات را به یکباره نمی گیرند، با شما طرح دوستی می ریزند و در طی زمان گام به گام پازل اطلاعاتی خود را کامل می کنند. اگر برای دسترسی به سیستم شما نیازمند 8 قلم داده، از قبیل تاریخ تولد، محل تولد، نام مادر و غیره باشند. به صورت زمانبندی شده و مثلا با ارتباط چت در طول زمانی طولانی این داده ها را یک به یک از شما اخذ می کنند.حتی ممکن است افراد مختلفی مامور ارتباط با شما شده، هر یک به دنبال قطعه ای از این پازل باشد.

نکته دوم : تخلیه اطلاعاتی با سوء استفاده از سهل انگاری شما. فرض کنید تبهکار شماره تلفن موبایل شما را در اختیار داشته، قصد دسترسی به اطلاعات پرسنلی شما نظیر آدرس، محل تولد، تاریخ تولد، شماره شناسنامه و غیره را دارد، مکالمه احتمالی به شکل زیر خواهد بود: الو سلام ...از دانشگاه آزاد واحد تهران مرکز تماس می گیرم، من نجفی هستم، همکار آقای سعیدلو مسئول بایگانی اداره آموزش(سعید لو فردی است که واقعا وجود دارد و برای بالابردن اعتبار مکالمه از او یاد می شود)، پرونده شما مقداری اطلاعات کسر دارد، محبت می کنید سوالهای منو جواب بدهید؟ مقابله با تهدید مکالمه بالا نیازمند قدری آموزش است، کافیست شما سوال فوق را اینچنین جواب دهید: بله خواهش می کنم، لطف کنید شماره تلفن و داخلی تان را بدهید. من با شما تماس می گیرم.

مقابله با اخذ اطلاعات به شیوه هایی نظیر تهدید، ارعاب و شکنجه

در مناطقی از جهان که پلیس و نیروهای امنیتی، ضابطین قانونی و مدافع حقوق شهروندان آزاد اند. بهترین راه حل مراجعه به پلیس و استفاده از ظرفیتهای حرفه ای سازمانهای امنیتی در مقابله با جنایت سازمان یافته سایبری است. اما متاسفانه در برخی مناطق جهان نیروی پلیس، خصوصا پلیس سیاسی و امنیت، خود بخشی از جنایت سازمان یافته سایبری است.

رعایت مواردی از این دست می تواند، بسیاری از تهدیدهای جدی از ناحیه نیروهای سیاسی سرکوبگر را خنثی نماید.

- هنگامی که چت می کنید، لحظاتی را در نظر آورید که یک بازجو، متن کامل لغاتی را که در حال تایپ کردنش هستید، به صورت پرینت جلویتان می گذارد. این بازجو می تواند فردی باشد که همین حالا مشغول چت کردن با او هستید. این بازجو می تواند بالای سر دوستی که در حال حاضر با او چت می کنید ایستاده باشد و این بازجو می تواند به راحتی شیشه اتومبیل دوست شما را شکسته، کامپیوتر نوت بوک او را دزیده و از قسمت آرشیو چت ایمیل دوستتان تمام متن چت شما را پرینت کند.چت متنی از ناامن ترین ارتباطات موجود است. اگر از سرویس چت شبیه Gmail استفاده می کنید، حتما آرشیو چت را غیرفعال کنید و با افرادی که احتمال می دهید، متن چت را جایی ذخیره می کنند و یا امکان آرشیو را غیرفعال نکرده اند، چت نکنید.
- اگر در ایران زندگی می کنید باید بدانید و کاملا درک کنید که در یکی از خطرناکترین مناطق کره زمین به دنیا آمده و درحال زندگی هستید، اکثریت ساکنان کره زمین حتی در مناطق کمتر توسعه یافته نظیر آفریقا، باور نخواهند کرد که در کشور شما، افراد به دلیل نوشیدن یک قوطی آبجو یا نشستن کنار دوست دخترشان در پارک مجازات، حبس و حتی محکوم به تحمل شلاق خواهند شد. همچنین بسیاری از ایرانیان نمی دانند که بر اساس قوانین جاری ایران، مجازات سه بار نوشیدن مشروبات الکلی اعدام است. به عنوان یک کاربر اینترنت متاسفانه شما نمی توانید در قلمرو جمهوری اسلامی ایران زندگی کنید و تصاویر میهمانی جشن تولد خود را مانند یک جوان ساکن آنگولا، اردن و یا ترکیه روی فیس بوک و یا وبلاگتان قرار دهید. شما را با این تصاویر مورد فشار و شکنجه قرار خواهند داد. سیستمهای امنیتی جمهوری اسلامی ایران از نوعی پارادوکس انسانی - غیرعقلانی نهایت استفاده را می کنند. آنان می دانند بسیاری از فعالان اینترنتی، دانشجویی، روزنامه نگاران و منتقدان سیاسی، شیوه زندگی مدرنی دارند. آنان می دانند که برخی از این افراد مانند آدمیان دیگر، از مشروبات الکلی استفاده می کنند و یا روابط جنسی خارج از ازدواج دارند. در کشور ایران از این اطلاعات برای تحت فشار قرار دادن منتقدان استفاده می شود. لذا اکیدا از فیلمبرداری، تصویربرداری، خاطره نویسی و شرح این نوع روابط برای دیگران بپرهیزید. در شرایط کنونی اکثر تلفنهای همراه قابلیت ضبط فیلم را دارند. هنگامی که مشغول ضبط فیلم با تلفن همراهتان و یا روشن کردن وب کم کامپیوترتان هستید بایستی بدانید که دو نفر موتورسوار به راحتی قادرند تلفن همراه شما را در هنگام صحبت در خیابان، قاپ زده و از دست شما احتمالا هیچ کاری ساخته نیست. باز تاکید می کنم، فیلم، صدا، مکالمات تلفنی آخر شب با شریک عاطفی تان، شرح پارتی و دخیره و انتشار عکسهای خصوصی، طلایی ترین فرصتها را برای تحت فشار قراردادن شما در اختیار بازجو و پلیس سیاسی قرار می دهد.
- یک شیوه موثر اگر احتمال بازداشت خود را می دهید، ذخیره داده های مهم و حساس در یک سرویس اینترنتی آنلاین نظیر گوگل و یا فضاهای ذخیره مطمئن آنلاین است. رمز عبور این داده ها را به همراه سوالهای امنیتی برای تغییر رمزSecurity Questions and Password hint، می توانید در اختیار فرد مورد اعتماد خود در خارج از ایران قرار دهید تا بلافاصله پس از بازداشت شما همه رمزهای عبور را تعویض نماید.
سرعت عمل این فرد بسیار مهم و حیاتی است. چرا که شما غالبا می توانید در مقابل بازجویان برای یک یا چند روز نخست مقاومت نمایید. در این باره در بخشهای بعدی به تفصیل توضیح خواهم داد.

روشهای تکنیکی نفوذ : بدافزارهاMalwares

بدافزارها مجموعه گسترده ای از نرم افزارهای آلوده و مخرب هستند که بدون اجازه شما، وارد سیستم شده و با اهداف متفاوتی موجب زیان، از بین رفتن داده ها و یا نرم افزارهای شما می شوند. بدافزارهای را می توان به گروههای مختلفی تقسیم کرد:(5)

- بمبهای منطقیLogic Bombs
- اسبهای تروایTrojan Horse
- درب پشتیBack Door
- ویروسVirus
- کرمWorm
- خرگوشRabbit
- جاسوس افزارSpyware
- تبلیغ افزارAdware

- بدافزارهای ترکیبی، قطره چکان، تهدیدات مخلوطHybrid, Dropper and Blended threats
- زامبی هاZombies

بمبهای منطقی - شرطی

هر بمب منطقی، وقوع یک شرط یا گزاره منطقی را بر روی سیستم میزبان بررسی می کند، مثلا آیا امروز پنجشنبه 24 جون 2010 است یا نه؟ به مجرد تحقق این شرط بمب فعال می شود و به سیستم شما آسیب می رساند.

تروجانها Trojans یا اسب های تروا

غالبا در شکل برنامه های سودمند توسط کاربران بر روی سیستمها نصب می شوند .بلافاصله و یا پس از مدتی کد آلوده تروجان فعال می شود، برخی از فایلها و یا تنظیمات شما را از بین می برد. در بسیاری از موارد تنظیم بندی های ایمنی کامپیوتر شما را هدف قرار می دهد و زمینه دسترسی تبهکاران به داده های شما را فراهم می آورد.استفاده از نرم افزارهای اشتراک داده هایی مثل فیلم و موزیک و همچنین استفاده از نرم افزارهای کرک crack شده و غیرقانونی از ساده ترین راههای نصب تروجان Trojan ها روی کامپیوتر شماست. بسیاری از این برنامه های مجانی کرک و یا قفل شکسته به منظور صرف، ورود تبهکاران به کامپیوترهای شخصی قربانیان و سرقت اطلاعات، در سطح وسیعی منتشر می شوند.

درب پشتی، Back Door

با مکانیسمی نظیر بمبهای منطقی، قطعه ای از برنامه به ظاهر سالم و پاکیزه است که در صورت وقوع شرط یا شروطی خاص زمینه دسترسی مهاجمین به داده های شما را فراهم می آورد. مثال بسیار ساده به شکل زیر است، یک برنامه نویس می تواند برنامه ای برای امنیت کامپیوتر شما تولید کند که مانع ورود مهاجمان شود، اما او در داخل برنامه راهی برای ورود خود به کامپیوتر شما باز گذاشته و می تواند از آن درب وارد سیستم شما شود.

ویروسها

ویروس ها از پایان دهه 1980 میلادی از عمده ترین خطرات و تهدیدها علیه امنیت سایبری به شماره می روند. ویروسها را بر اساس مکانیسم تخریب و انتشارشان می توان به گروههای متفاوتی تقسیم کرد، نظیر:

- ویروسهای بوت سکتور یا ویروسهایی که سکتور صفر دیسکهای حاوی اطلاعات را نشانه رفته، سعی در تکثیر از طریق آلوده کردن دیسک های دیگر دارند.
- ویروسهای آلوده کننده فایلهای اجرایی نظیر .com .exe .bat .bin: که از طریق تغییر فایلهای اجرایی سیستم و تکثیر در زیرشاخه ها، برنامه ها و داده های شما را تخریب و در انتظار انتقال به رایانه قربانی دیگری می نشینند.
- ویروسهای ترکیبی از بوت سکتور و فایلهای اجرایی

ویروسهای زیر موجب وارد آوردن خسارات بسیار گزاف در سطح جهانی شدند:

Sircam-2001, , Nimda-2001, Magistr 2001, Melissa 1999, Mydoom 2004 , CIH Chernobyl 2001 .

همزمان با تولید و انتشار ویروسها، شرکتهای امنیت کامپیوتری نیز نرم افزارهای ضدویروس بسیاری ارائه کرده اند. ویژگی مشترک همه این نرم افزارها؛ ضرورت به روزرسانی Update کردن بانک اطلاعات ویروسهای هر ویروس کش است. اگر کامپیوتر شما به شبکه اینترنت وصل باشد این عمل عموما به صورت اتوماتیک انجام می شود.

برای کاربرانی که به شبکه اینترنت متصل می باشند، امکان فراخوانی Load نرم افزارهای آنلاین ضد ویروس وجود دارد به اینصورت که با دانلود موتور جستجوی ویروس، نرم افزار ویروس یاب آنلاین، حافظه کامپیوتر شما را به دنبال ویروسها جستجو می کند. در سالهای گذشته شرکت های نرم افزاری معتبری، بسته های ویروس یاب و ویروس کش مجانی را در اختیار کاربران کامپیوترهای شخصی قرارداده اند. بسته هایی که به سادگی از شبکه جهانی اینترنت قابل دانلود هستند.در بخشهای بعدی درخصوص نحوه مقابله با ویروسها و نصب و استفاده از آنتی ویروسها بیشتر صحبت خواهیم کرد.

کرمهاWorms

تفاوت عمده کرمها worms با ویروسها به انتشار اتوماتیک و خودکار کرمها باز می گردد. کرمها با شناسایی حفره های امنیتی یک سیستم عامل، یک شبکه و یا یک پروتکل انتقال داده معین، خود را تکثیر و وارد کامپیتوتر شخصی شما می کنند.

برخی از مخرب ترین کرمهای کامپیوتری که سرورها و شبکه های کامپیوتری را با اختلالات جدی مواجه کردند عبارتند از:

Anna Kournikova worm 2001, Klez worm 2001 , Explorer worm 1999, Bad Benjamin worm 2002, Loveletter worm 2000, Sasser worm 2004, Blaster worm 2003, Sobig worm 2003.

خرگوش ، Rabbit

برنامه های کمیابی هستند که مانند خرگوش و یا باکتری با سرعت بسیار زیادی خود را تکثیر می کنند. بسیاری از آنان با افزایش سریع تمام منابع سیستم شما را به خود اختصاص داده عملا کامپیوتر شما را فلج می کنند. نمونه ساده آن قطعه برنامه ای است که در هر ثانیه چند پنجره جدید را می گشاید. این عمل بسیاری از توان سی پی یو و حافظه شما را به خود اختصاص داده کامپیوتر را عملا قفل می کند .حالت دیگر خرگوشها برنامه ای است که بلافاصله پس از تولد مادر خود را پاک می کند. مثلا در شکلی از یک کرم که میان کامپیوترهای مختلف شبکه در حال جست و خیز است و هر بار قطعه و یا برنامه مولد خود را پاک کرده با شکل جدیدی در کامپیوتر دیگری ظاهر می شود.

جاسوس افزارهاSpyware

برنامه های جاسوس، پس از ورود و استقرار بر روی سیستم شما سعی در جمع آوری اطلاعات غیرمجاز و ارسال آن برای فرستندگان خود دارند. مثلا شناسه ها و یا رمزهای ورود، آدرس ایمیل دوستان شما و یا مشخصات مالی، فایلهای متن و غیره .بسیاری از صفحات اینترنتی به محض باز شدن و مرور، برنامه های جاسوس را به حافظه کامپیوتر شما منتقل می کنند. تفاوت اساسی برنامه های جاسوس و ویروسها یا کرمها، عدم توانایی برنامه های جاسوس در تکثیر کردن خود و یا انتقال به کامپیوترهای مختلف است. یکی از متداولترین و رایج ترین برنامه های جاسوس کامپیوتری، برنامه های ضبط کننده صفحه کلید یا Keylogger ها هستند، این برنامه ها هر کلیدی را که روی صفحه کلید شما فشرده شود ضبط کرده و سپس همه این مجموعه را برای دریافت کننده اطلاعات جاسوسی ارسال می دارند. این کلیدها می تواند مجموعه کامل گفتگوی چت نوشتاری شما، رمزهای ورود به ایمیل و یا نگارش متن یک گزارش و یا ایمیل بر روی کامپیوتر شما باشد. برنامه های جاسوس دیگری برای جاسوسی از وب کم شما، میکروفن لپ تاپ و یا ضبط صفحه نمایش وجود دارند. به این معنی که پس از فعال شدن همه رویدادهای صفحه نمایش شما را ضبط و به مرور به خارج از کامپیوتر شما قاچاق می کنند.

تبلیغ افزار، برنامه های آگهیAdware

همه شما برنامه های آگهی را تجربه کرده اید، برنامه هایی که با بازکردن صفحات خاص یا ظاهر کردن بنرهای متعددی شما را به خرید محصولات و یا استفاده از سرویسهای خود توصیه می کنند. برنامه های تبلیغی نیز مانند Spyware ها فاقد توان تکثیر خود هستند. این برنامه ها می توانند داده های شما را دستخوش تغییر کنند و در برخی موارد تنظیمات کامپیوتر شما را تغییر دهند. مثلا صفحه جستجوی پیش فرض شما را به سایت خود تغییر داده و یا به هنگام جستجوی محصولات برای خرید، شما رابه صورت خودکار به محصولات مورد نظر خویش، هدایت نمایند.

بدافزارهای ترکیبی، قطره چکانها، تهدیدات مخلوط

هیبرید ها به ترکیبی از تهدیدهای ذکر شده در موارد قبل اطلاق می شود، برنامه جاسوسی که در عین حال یک اسب تراوا و یا یک ویروس را نیز در کامپیوتر قربانی نصب می کند. یا به طور مثال قطعه برنامه ای که اولا یک «درب پشتی «Back Doorرا ایجاد کرده و ثانیا این عمل شبیه یک ویروس را بر فایلهای دیگر آن سیستم تکرار می کند . Dropperها نیز می توانند با روشهای ترکیبی از خود حفره هایی در کامپیوتر قربانی بر جای گذارند، مثلا ویروسی که علاوه بر بازنشر خود، یک «درب پشتی » Back Door هم روی کامپیوتر میزبان بر جای می گذارد. تهدید مخلوط یا Blanded Threatبه ویروسی اطلاق می شود که از روشی مشابه کرمها یا Worms برای کشف آسیب پذیریهای تکنیکی شبکه یا پروتکل استفاده کرده و در عین حال بر خلاف کرم توان تکثیر دارد.

زامبی ها ، Zombies

بسیاری از بد افزارها مثلا اسبهای تراوا پس از در اختیار گرفتن کامپیوتر قربانی از آن برای مقاصد غیرقانونی خود استفاده می نمایند. این مقاصد می تواند ارسال هرزنامه Spam و یا حملاتی چون حمله توزیع شده به منظور توقف سرویس distributed denial-of-service attack -DDoS attackباشد. در این مرحله قربانی بدون آنکه خود بداند. بخشی از شبکه بزرگ حمله و اقدامات غیرقانونی تبهکاران است. به طور مثال در جریان حملات سایبر علیه دولت استونی در سال 2007سازماندهندگان حملات از شبکه های بات نت و کامپیوترهای زامبی ارسال کننده هرزنامه برای اجرای یک حمله بزرگ DDoS استفاده کردند.

شناخت تهدیدها در قالب پاسخ به چند سوال

سوال : کدام دسته از تهدیدها خطرناک ترند؟

پاسخ به این سوال واقعا به شیوه استفاده شما از دنیای دیجیتال بستگی دارد .خیلی ساده به چند سناریوی پایین بیاندیشید :

- فرزندان شما از کامپیوتر و اینترنت خانه استفاده می کنند.
- شما برای کارهای بانکی تان از اینترنت استفاده می کنید.
- کارهای اداری و نامه نگاریهای محل کار خود را در منزل از طریق اینترنت انجام می دهید.
- فعال سیاسی - مدنی بوده از طریق اینترنت با دوستان خود در تماس اید.
- از طریق اینترنت و سایتهای خرید و فروش آنلاین، مثلا لوازم الکترونیکی می خرید.

در مورد اول یعنی استفاده فرزندان، خطرات متعددی در کمین کاربران کم سن و سال شبکه اینترنت است .کودکان و نوجوانان می توانند در شبکه های اجتماعی و چت رومها مورد سوء استفاده تبهکاران قرار گیرند .آنان به دلیل تجربه پایین در برخوردهای اجتماعی، سخن و ادعای افراد ناشناس را باور کرده حتی ممکن است شماره تماس، آدرس ایمیل، آدرس خود را در اختیار آنان قرار داده یا درخواست ایشان برای ملاقات در سطح شهر را بدون درنظر گرفتن خطرات احتمالی آن بپذیرند.

مورد دوم : رمز عبور حسابهای بانکی شما ممکن است توسط برنامه های آلوده ای که از قبل روی کامپیوتر شما ارسال شده، به سرقت رفته، حساب شما توسط تبهکاران مورد سوء استفاده قرارگیرد.

مورد سوم : اطلاعات حساس و محرمانه، تجارت یا محل کار شما ممکن است مورد سوء استفاده فرد یا افرادی قرار گیرد که از طریق بدافزارهای Backdoor یا Trojan وارد کامپیوتر شما شده اند.

مورد چهارم : امنیت شما، همکاران و دوستانتان می تواند از طریق رخنه و نفوذ دستگاههای سرکوب به خطر افتد.

مورد آخر : شما صورتحساب آنلاین را پرداخت کنید اما جنس مورد نظر هیچگاه برای شما ارسال نشود یا جنسی متفاوت از آنچه در صفحه فروشنده درج شده است برای شما ارسال گردد.

سوال : چند شیوه متداول کلاهبرداری مهندسی اجتماعی را می شناسید؟

شیوه های عمومی زیر از متداول ترین و قدیمی ترین شیوه های مهندسی اجتماعی اند که به هزاران شکل مختلف مورد سوءاستفاده تبهکاران و یا دستگاههای سرکوبگر قرار می گیرند.

- ایمیلهای نیجریه ای419، چند میلیون دلار در سوئیس
- گمراه سازی عاطفی : به این کودک سرطانی کمک کنید
- پیشنهاد تجارتی پر سود، درآمد سرشار با کار در منزل
- سلامت - بدن ایده آل، در عرض دوهفته سی کیلو لاغر شویدsix pack .
- آی پد مجانی، گرین کارد آمریکا، خودروی با اقساط بسیار ناچیز بدون بهره.
- و .....

در موارد بالا از روشهای متعددی برای کلاهبرداری استفاده شده است .در روش ایمیلهای نیجریه ای مثلا ایمیلی دریافت می کنید که در آن نوشته است شما لاتاری برنده شده اید، گرین کارد ایالات متحده برنده شده اید و .... ولی بهرحال برای دریافت مدارک باید 500دلار پرداخت کنید.

در آخرین نمونه از این نوع کلاهبرداری ها فردی با افتتاح حسابی در سوئیس از خبرنگاران ایرانی متقاضی آموزش در لندن خواست 500 یورو به حساب او واریز نمایند تا ترتیب شرکتشان در کلاسهای رویترز داده شود.

گمراه سازی عاطفی به کرات در مواردی نظیر سیل، زلزله، بلایای طبیعی و ... اتفاق می افتد .حتی در وضعیت عادی نیز ممکن است تبهکاران با انتشار تصویر کودکی سرطانی حتی از طریق ترغیب شما به کلیک یا لایک کردن تصویر برای خود از طریق آگهی کسب درآمد کنند .در موارد جدی تر از شما می خواهند برای جلوگیری از مرگ کودک مقادیری پول را برای شماره حسابی شخصی ارسال نمایید.

در سالهای گذشته صدها هزار محصول بی تاثیر با استفاده از حساسیت انسانها به زیبایی و بدن زیبا و سالم به فروش رسیده است محصولاتی که اگر برای سلامت افراد ضرر نداشته باشند حداقل تاثیر دلخواه فرد را به هیچ وجه به ارمغان نمی آورند.

ایمیلهای شما آی پد برنده شده اید، برای یک پلی استیشن مجانی اینجا را کلیک کنید، سفر مجانی و ... همه و همه از یک شیوه ساده تطمیع افراد برای کسب و دریافت اطلاعاتی نظیر تلفن، ایمیل، مشخصات واقعی و آدرس بهره می گیرند .توجه داشته باشید که اکثر افراد احتمال می دهند حتی اگر یکدرصد هم موضوع ایمیل درست باشد چرا که نه؟ و مشخصات واقعی خود را وارد می کنند .این مشخصات بعدا برای ارسال هرزنامه و یا کلاهبرداری های جدی تر مورد سوء استفاده قرار می گیرد.

سوال: مهندسی اجتماعی - فریب شخصیتی به چه معناست؟

سه شیوه عمومی فریب شخصیتی مورد استفاده گسترده قرار می گیرد :

- EGO ATTACKS
- SYMPATHY ATTACKS
- INTIMIDATION ATTACKS

EGO ATTACKS

در شکل نخست ضعفهای شخصیتی افراد و عزت نفس ایشان اصلی ترین دستاویزفریب است .افراد عموما از تعریف و تمجید از خود خوشحال می شوند و شک و تردید نسبت به گوینده را فراموش می کنند .کافیست به افراد بگویید شما متفاوت ترین فردی هستید که من در تمام زندگی خود دیده ام .همین جمله ساده اعتماد قابل توجهی را در اکثریت اعضای جوامع برای شما فراهم آورده، دربهای اطمینان گشوده خواهند شد .تبهکاران از این ویژگی شخصیتی برای تماس نخست با قربانی نهایت استفاده را می برند .روش دیگر درک موقعیت فردی است که در شرایط دشواری قرار دارد .از زندان آزاد شده،رابطه خوبی با خانواده نداشته، نزدیکان خود را از دست داده است و یا دوستانش او را طرد کرده اند .نزدیکی با وی و این ادعا که من موقعیت تو را کاملا درک می کنم . دوستان و خانواده ات تو را نمی فهمند .آنها توان درک شخصیت والا و زیبایی های انسانی تو را ندارند .فرد آسیب دیده را کاملا متکی به گوینده می کند .مثال بسیار آسیب پذیر این نوع حملات نوجوانان در سنین آغاز نوجوانی می باشند که به دلیل ویژگیهای روانی دوران بلوغ کاملا در معرض آسیبهای جدی از این ناحیه قرار دارند.

SYMPATHY ATTACKS

در این شکل این فرد فریب دهنده است که خود را به شکل قربانی می نماید .فردی که نزدیکانش را از دست داده است .فرزندش بیمار است .پولش را دزدیده اند .به خاطر دلیلی انسانی و شرافتمندانه زندانی بوده است .همسرش به او خیانت کرده و یا از بازماندگان بلایای طبیعی مثل زلزله، سیل، سونامی و حوادث تروریستی است .در یک مورد مشهور مادری در ایالات متحده آمریکا برای موفقیت فرزندش در یک مسابقه موسیقی ادعا کرده بود که همسرش را در جنگ از دست داده است و جالب اینجاست که این ادعای نادرست سمپاتی و همدردی شمار قابل توجهی از داوران و رای دهندگان را برانگیخته بود .

INTIMIDATION ATTACKS

در شکل آخرکلاهبردار خود را نوعی مقام مسئول معرفی می کند، مسئول بخش ایران در سازمان ملل، سفیر کانادا در تهران، نماینده اتحادیه اروپا و .... این شیوه که به کرات برای فریب ناراضیان سیاسی، روزنامه نگاران و فعالان مدنی مورد استفاده قرار می گیرد به این شکل است که مثلا فردی تماس گرفته خود را نماینده دفتر اتحادیه اروپا معرفی می کند قربانی به جای ملاقات در دفتر واقعی اروپا در تهران حاضر می شود در رستوران یا ... با او ملاقات کند، این فرد می تواند یک کلاهبردار معمولی و یا یک افسر امنیتی نظام سرکوبگر باشد.

سوال : چند نمونه از پیشینگ یا فیشینگ را می شناسید؟

دهها و صدها نمونه پیشینگ وجود دارد، مثالهای زیر برای فهم بهتر این تهدید کمک می کند :

- در ایمیل دریافتی گوگل برای نوشته است : اکانت جمیل شما هک شده به این آدرس بروید.
- در ایمیل دریافتی بانک شما نوشته است :حساب شما مورد تهدید قرار گرفته به این آدرس بروید.
- در ایمیل دریافتی نوشته : پسورد عابربانک یا کارت بانک خود را در آدرس زیر عوض کنید.
- در ایمیل نوشته برای دریافت 100 دلار اعتبار Skype یا Paypal به آدرس زیر روید.

نکته مشترک همه حملات بالا این است که پس از کلیک کردن بر آن لینک شما وارد گوگل، سایت بانک، Paypal یا Skype خود نخواهید شد و تنها سر از سایت آلوده ای درخواهید آورد که شناسه و پسورد شما را سرقت خواهد کرد .اصلی ترین ویژگی سایتهای پیشینگ این است که ظاهر سایت آلوده شان شباهت بسیاری مثلا به سایت جیمیل، یاهو، بانک شما و ... دارد به شکلی که شما متعجب نشده و با اطمینان اطلاعات حساس خود را وارد خواهید نمود.

سوال : دیگر تهدیدهای مهندسی اجتماعی ؟

هیچ فهرستی که همه تهدیدهای مهندسی اجتماعی را شامل شود، وجود ندارد .هر روز با ظهور و نوآوری تکنولوژیک تهدیدهای جدیدی ابداع و آزموده می شوند .امام خطوط اصلی شکل دهنده تهدیدها همچنان ثابت باقی مانده اند .یکی از تهدیدهای متداول به شکل زیر است:

دستور از ناحیه مقام مسئول

در این شکل مثلا فردی با شما که کارمند دفتری یک موسسه هستید، تماس می گیرد و خود را رئیس کل موسسه شما، یا یک نماینده مجلس یا وزیر و ... معرفی می کند و از شما خواستار اطلاعات خاصی می شود .او مثلا از شما می خواهد شماره تلفن مسئول حسابداری شرکت را برای او پشت تلفن بخوانید .اگر از وی خواستار توضیح بیشتر شوید با فریاد و هیاهو به شما دستور می دهد .فورا شماره را برایش بخوانید والا برایتان عواقب بدی خواهد داشت ...او در یک جلسه فوق العاده مهم است و فرصت توضیح بیشتر ندارد و....

بررسی ها نشان داده است جمع کثیری از قربانیان درخواست فرد فوق را پاسخ مثبت می دهند.

تلفنهایی مثلا : ما از وزارت کشور تماس می گیریم، از سازمان آب تماس می گیریم، از سرشماری سازمان آمار تماس می گیریم و غیره نیز می توانند نمونه هایی برای روش بالا باشند.

پیشنهاد کمک به شما

در این روش فردی با شما تماس می گیرد و ادعا می کند مثلا از قسمت امنیتی بانک شما و یا شرکت کامپیوتری معتبری است وی اعلام می کند که کامپیوتر شما آلوده شده، یا فرد دیگری از اکانت شما استفاده می کند .سپس از شما خواستار اطلاعات می شود مثلا نام، نام خانوادگی، شناسه و رمز عبور شما را می پرسد .این اطلاعات توسط فرد مهاجم برای سوء استفاده از داده های شما مورد استفاده قرار خواهد گرفت.

درخواست کمک از شما

در این روش بر خلاف شیوه بالا، فردی با شما تماس می گیرد و از شما درخواست کمک می کند .مثلا تلفنش گم شده، دسترسی به دفتر تلفن ندارد، جانش در خطر است و ... اغلب افراد به دلیل حسن نیت و خوش قلبی ذاتی آدمها به درخواست فوق پاسخ مثبت می دهند و برای کمک اعلام آمادگی می کنند او مثلا از شما می خواهد یک آدرس اینترنتی را برایش چک کنید .ورود شما به سایت مورد ادعای فرد منجر به آلوده شدن کامپیوتر شما خواهد شد.