جلد سوم

آشنایی با جاسوسی صنعتی

ایمن گستر حصین

مقدمه:

هر چند تاریخ دقیق شروع جاسوسی صنعتی دقیقاً مشخص نیست، اما شواهد و مدارک نشانگر آن است که سابقه این نوع جاسوسی به قبل از میلاد مسیح برگشته و اعزام راهبه‌ها از بیزانس به رم، اولین جاسوسی صنعتی شمرده شده است.

جاسوسی صنعتی به شکل رسمی و دولتی آن از سال ۱۷۸۹ با قانون ثبت اختراع در فرانسه به تصویب رسید؛ بر اساس این قانون، هر فرد فرانسوی که هر نوع دانشی را از خارج فرانسه وارد آن کشور می‌نمود، دارای همان حقوقی می‌شد که مخترع آن داشت.

این کار در واقع، نوعی تشویق برای انجام جاسوسی صنعتی بود که از خصوصیات بارز دولت‌ها و حکومت‌های گذشته بوده و هم اکنون نیز در پوشش‌هایی دیگر مانند تعامل و همکاری صنعتی و فن‌آورانه، بازرسی‌های بین‌المللی و بعضاً زور و تهدید دنبال می‌گردد.

با افزایش روزافزون ارتباطات، تبادل اطلاعات نیز به مراتب بیشتر و بیشتر می شود؛ تبادل اطلاعات یعنی ارسال یک سری اطلاعات از یک مبدأ مشخص به مقصدی مشخص؛ حال هر چه اهمیت و ارزش اطلاعات مبادله‌شده بیشتر باشد، بالطبع امنیت ارسال این اطلاعات هم حیاتی‌تر خواهد شد و در این میان اگر اطلاعات و اسرار مهم یک شرکت یا سازمان چه به‌شکل عمدی و چه به‌شکل غیرعمدی لو برود، آن شرکت یا سازمان به‌نوعی دچار یک حمله جاسوسی شده است؛ چون ماهیت اطلاعاتی که مورد هجوم این نوع حمله‌ها قرار می‌گیرد، نوعا صنعتی است که مهندسان، این پدیده را جاسوسی صنعتی نام نهاده‌اند.

مطالعات اخیر نشان داده که افراد داخل یک شرکت، مسئول بیش از ۷۰ ٪ از موارد جاسوسی صنعتی یا دزدی‌های اطلاعاتی از شرکت‌ها بوده‌اند.

تعاریف:

جاسوسی صنعتی:

جاسوسی صنعتی عبارت است از سرقت اسرار تجاری (شامل اطلاعات مالی، تجاری، علمی، فنی، اقتصادی و مهندسی) از طریق ربایش، کپی‌کردن یا ضبط اطلاعات محرمانه یک شرکت برای استفاده رقیب و یا کشور دیگر.

امنیت:

وجود شرایطی که کشور را از اعمال نفوذ دشمن مصون نگه می‌دارد.

امنیت ملی:

وضعیتی که در آن، یک کشور نسبت به منافع و ارزش‌های حیاتی خود، تهدیدی جدی احساس نکند .

اطلاعات اقتصادی:

سیاست، خط مشی و اخبار اقتصادی که شامل داده‌های فناورانه مالی، اولویت‌های تجاری و... می‌شود.

دلایل انجام فعالیت‌های جاسوسی در بخش‌های صنعتی:

جاسوسی صنعتی صرفا به معنای از دست دادن اطلاعات حفاظت‌شده که ممکن است توسط یک سازمان و یا دولت خارجی مورد استفاده قرار گیرد، نیست (گرچه این اطلاعات، جزئی از دارایی فیزیکی شرکت مانند یک وسیله نقلیه یا ساختمان نیست) بلکه اطلاعاتی است که به‌ویژه در

بخش صنعت دارای ارزش پولی است و اطلاعات یا اسناد یا از دست رفتن در آمد یک شرکت را در صورتی که یک رقیب بتواند به واسطه جاسوسی صنعتی، محصول جدیدی را وارد بازار کند، نشان می‌دهد.

دلایل جاسوسی صنعتی:

- کسب برتری در مقابل رقیب
- کسب اطلاعات مربوط به تحقیقات موردنظر با کم‌ترین هزینه
- کسب اطلاعات مربوط به فن‌آوری‌های جدید صنعتی و نظامی با حداقل هزینه
- کاهش هزینه‌های پژوهش از طریق کسب اطلاعات دستارودهای دیگران
- کسب اطلاعات درخصوص تحلیل رقبا
- ایجاد سیستم پدافندی برای مقابله با خطرات احتمالی

شروط موفقیت‌آمیز بودن جاسوسی صنعتی:

انگیزه:

برای موفقیت در مقابله با جاسوسی صنعتی بسیار مهم است که از انگیزه‌های افرادی که در چنین فعالیت فریبنده و مجرمانه‌ای شرکت می‌کنند، شناخت داشته باشیم؛ اگرچه انگیزه‌های فردی ممکن است متفاوت باشند اما معمولا یک وجه اشتراکی وجود دارد که اقدام به جاسوسی صنعتی را محقق می‌کند؛ این انگیزه ممکن است پول، انتقام‌جویی یا دیدگاه‌های دینی، سیاسی یا اجتماعی باشد؛ البته گاهی هم ممکن است صرفاً به‌خاطر هیجان باشد؛ ولی در هر صورت، شایع‌ترین انگیزه، پول است.

فرصت:

منظور از فرصت، شرایطی است که فرد به اطلاعات حفاظت‌شده دسترسی پیدا و احساس می‌کند که می‌تواند آنها را بدون شناسایی یا هرگونه عواقبی سرقت یا تکثیر کند؛ اساساً اگر فرصتی برای جاسوسی صنعتی وجود داشته باشد، نشان‌دهنده تدابیر امنیتی ناکافی است. کافی نبودن تدابیر امنیتی ممکن است در نتیجه امنیت فیزیکی ناکافی باشد (مانند نبودن موانع کنترل دسترسی، سیستم‌های تشخیص نفوذ، دوربین‌های امنیتی و فقدان نیروهای حراستی).

چنانچه فرصتی برای جاسوسی صنعتی وجود داشته باشد، غالبا وجود یک مسئله سیستماتیک مطرح است، نه صرفاً کمبود امنیت فیزیکی؛ نبود سیاست کنترل داخلی نظارت، آموزش و بازرسی، فضایی ایجاد می‌کند که افراد به اطلاعات حفاظت‌شده دسترسی پیدا خواهند کرد؛ این موضوع باعث می‌شود که افراد احساس کنند می‌توانند بدون شناسایی و هرگونه عواقبی دست به سرقت بزنند.

هنگامی که نقصی امنیتی رخ می‌دهد و به دنبال آن تحقیق کافی و اقدام انضباطی علیه مجرم انجام نمی‌گیرد، کسانی که می‌خواهند در جاسوسی شرکت کنند، جرأت این کار را پیدا خواهند کرد.

توجیه منطقی:

جاسوسان با این توجیه که جاسوسی صنعتی واقعاً کار غلطی نیست، کار خود را موجه می‌دانند و در واقع این استدلال که این کار پشتوانه سیاسی یا ایدئولوژیکی دارد، می‌تواند برای آنها بهانه خوبی باشد؛ توجیهات دیگر شاید این باشد که هر شخص دیگری هم ممکن است این کار را انجام دهد یا این‌که مجرم مشمول افزایش حقوق نشده است؛ اگر جاسوسی برای دریافت پول انجام شود، ممکن است این توجیه مطرح شود که شرکت می‌تواند خسارت وارده را جبران کند.

توانایی:

توانایی در این‌جا بدین معناست که فرد برای انجام رفتارهای مجرمانه مانند جاسوسی صنعتی توانسته است بر بازدارنده‌های ذاتی غلبه کند؛ چنین شخصی باید ارزش‌های اخلاقی و وفاداری به کشور یا کارفرما و بیش از همه، ترس از شناسایی شدن را زیر پا بگذارد.

عمال محرک:

فرد ممکن است برای دریافت پول بیشتر اقدام به جاسوسی کند؛ فرد ممکن است برای حفظ سبک زندگی پرخرج خود یا اعتیاد به مواد مخدر، الکل یا قمار به پول نیاز داشته باشد؛ محرک دیگر مربوط به تمایلات جنسی است که در آن از احساسات فرد، سوءاستفاده می‌شود و او به‌خاطر معشوقش اقدام به جاسوسی می‌کند. گاهی اوقات هم ممکن است فرد مورد تهدید و اخاذی قرار بگیرد و یا شخصی به‌خاطر عضویت در گروه‌های تبهکار تروریستی یا ایدئولوژیکی که به دنبال اطلاعات حفاظت‌شده‌ای هستند و وی احتمالاً به آنها دسترسی دارد، تحت فشار باشد؛ این شرایط در سازمان‌هایی که هدف دولت‌های خارجی و رقبا هستند، مبنای استخدام افراد قرار می‌گیرد.

جاسوسان صنعتی در کار خود چگونه عمل می‌کنند؟

دست‌یابی به روش‌های مدیریتی در صنایع از عرصه‌های خاص فعالیت سرویس‌های جاسوسی در سراسر جهان محسوب می شود. در این زمینه، جاسوسان صنعتی معمولاً به موارد ذیل توجه بیشتری نشان می‌دهند:

۱. اسناد و اطلاعات مربوط به ساختار سازمان‌ها

۲. اطلاعات مربوط به برآورد هزینه‌ها، اعتبارات و طرح‌های سرمایه‌گذاری

۳. ایده‌های جدید در نحوه و نوع تولیدات

۴. نتایج حاصله از تحقیقات

۵. مطالعات مربوط به طراحی محصولات نوین

۶. تدابیر سنجش کیفیت مؤسسات

۷. روش‌های مورداستفاده در تأمین نیازهای مشتریان

۸. راهبرد فروش، بازاریابی و خرید

۹. اطلاعات مربوط به اعطای امتیاز و آدرس مشتریان

۱۰. مشخصات و آدرس‌های محققین، صاحبان تخصص و ...

کدام شرکت‌ها موردتوجه جاسوسان صنعتی می‌باشند؟

این نکته را باید در نظر گرفت که بزرگی و یا کوچکی یک مؤسسه علمی و یا صنعتی، تعیین‌کننده هجوم جاسوس‌ها به آن محل نیست؛ بلکه در این زمینه، جایگاه آن مرکز در عرصه‌های علمی، تحقیقات و فن‌آوری اهمیت بسیاری دارد. از این رو باید صنایع و شرکت‌های کوچک و متوسط نیز که در زمینه نوآوری و تحقیقات پیشتاز هستند، مراقب عملیات جاسوسی سرویس‌های اطلاعاتی باشند.

مجاری نشت اطلاعات صنعتی کدامند؟

منابع آشکار:

اینترنت، بولتن‌های داخلی صنایع و سازمان‌ها و ... توسط عوامل سرویس‌ها استخراج و با تجزیه و تحلیل روی اخبار آنها نشر پیدا کرده و به نتیجه دلخواه و موردنظر منتهی می‌گردند.

منابع پنهان:

یکی دیگر از راه‌های کسب اطلاعات، شناسایی و سرمایه‌گذاری روی افرادی است که از نظر شخصیتی دارای ضعف بوده و قادر به حفظ زبان خود و رعایت حفاظت گفتار نمی‌باشند؛ این‌گونه انسان‌ها بازگویی کارها و اقدامات خود را آن هم با آب و تاب بیش از حد برای خود مایه افتخار و غرور می‌دانند. لذا اگر این دسته از افراد به پست و مقامی برسند، می‌توانند برای نظام و صنایع دفاعی مشکلاتی ایجاد نمایند؛ زیرا جاسوسان به طرق مختلف سعی در برقراری رابطه با این اشخاص و یا خانواده و اطرافیان آنها می‌کنند تا اطلاعاتی را که این افراد در محافل و مجالس مختلف انتشار می‌دهند، به‌راحتی جمع‌آوری نمایند.

آسیب‌های ناشی از جاسوسی صنعتی؟

- آسیب مالی
- آسیب روانی
- ضربه به شهرت و آبروی شرکت‌ها

روش‌های جاسوسی صنعتی:

روش‌های جاسوسی صنعتی بر دو دسته است:

- **روش‌های قانونی (غیرپنهان)**
- **روش‌های غیرقانونی (پنهان)**

روش‌های قانونی:

۱- خرید شرکت‌ها یا محصولات‌شان که سبب انتقال فناوری و دانش به رقبای سابق شرکت خریداری‌شده می‌شود.

۲- انتقال فناوری به کشورهای دیگر از راه انجام تجارت در آنها که ضمن آن شرکت مذکور مجبور می‌شود ابتدا نیروی انسانی خارجی را آموزش دهد.

۳- انجام کار مشترک با سایر رقبا (مثلا چند شرکت باهم تصمیم به ساخت محصولی جدید می‌گیرند که در این روند، اطلاعات شرکت‌ها به اشتراک گذاشته می‌شود).

۴- اطلاعات منبع باز؛ مانند مقالات روزنامه‌ها، گزارش‌های سالانه شرکت‌ها، اطلاعاتی که شرکت مجبور شده در یک دادگاه برای دفاع از اتهام وارده به خود ارائه کند و ...

۵- استخدام کارمندان توسط شرکت‌های دیگر و رقبا که هرچند در بسیاری از موارد ناخواسته و غیرمغرضانه است، اما به هر حال سبب انتقال دانش توسط این کارمندان می‌شود. (مثال

بارز آن استخدام بیشتر نیروهای متخصص شرکت اپل توسط شرکت ماکروسافت بود که به‌دلیل ضربه‌ای که به شرکت اپل خورد، لوگوی آن از یک سیب کامل تبدیل به یک سیب گاززده شد.)

۶- کنفرانس‌ها و برنامه‌های تبلیغاتی: به‌عنوان مثال یک دانشمند برجسته غربی که در حوزه قدرت شتاب‌دهنده نبض کار می‌کرد، در سال ۱۹۷۳ در یک نشست بین‌المللی در مورد فیزیک پلاسما در مراسمی که برای معارفه برگزار شده بود، با یکی از دانشمندان روسیه که در همان زمینه کار می‌کرد، وارد یک بحث طولانی شد که طی آن بعضی از پیشرفت‌های مهم روسیه لو رفت.

روش‌های غیر قانونی:

۱- سوءاستفاده از افراد داخلی برای سرقت اطلاعات، چه به صورت آگاهانه (تطمیع کارمندان) باشد و چه به صورت ناآگاهانه (مانند جاسوسی تلفنی و زیر پاکشی)

۲- فرستادن جاسوس‌هایی به شرکت در قالب افراد واجد شرایط و متخصص و جویای کار

۳- حمله فیزیکی به شرکت و سرقت اسناد و مدارک و یا نمونه‌های تحقیقاتی و آزمایشگاهی (این عمل معمولا وقتی موفق است که حمله‌کنندگان دقیقا بدانند دنبال چه هستند و آن را کجا باید بیابند.)

۴- گشتن اتاق‌های هتل، زمانی که نمایندگان شرکت‌ها در خارج از کشور مستقر هستند.

علاوه‌بر روش‌های بالا گاهی از روش فنی نیز برای جاسوسی صنعتی استفاده می‌شود که شامل موارد زیر است:

رایانه:

سرقت اطلاعات دیجیتال ازطریق فلش‌های آلوده و نرم‌افزارهای جاسوسی

سرقت اطلاعات و یا خرابکاری ازطریق هک و نفوذ به سیستم‌ها در بستر اینترنت

وسایل و تجهیزات الکترونیکی:

دوربین‌های مخفی با کارایی بالا

میکروفن‌های شنود با امکان ارسال صوت به‌صورت وایرلس

جاسازی ابزارهای جاسوسی مختلف در وسایل مورد استفاده افراد مانند عینک، فندک، ساعت، کفش، کراوات و ...

ماهواره‌ها:

امروزه ماهواره‌ها یکی از ابزارهای پرکاربرد در بحث جاسوسی هستند که بدون محدودیت‌های معمول از اهداف مورد نظر (بنادر، کارخانجات، پالایشگاه‌ها، شرکت‌ها و ...) جاسوسی می‌نمایند.

جاسوسی صنعتی، اقتصادی و تجاری از دید قانون:

جاسوسی به‌طور کلی عمل خائنانه‌ای است که در قوانین تمام کشورها جرم محسوب و مجازات سنگینی تا حد اعدام برای آن پیش‌بینی شده است.

در کشور ما نیز در ماده ۵۰۱ قانون مجازات اسلامی، جاسوسی جرم محسوب شده و برای آن مجازات‌هایی پیش‌بینی شده که به‌شرح زیر است:

ماده ۵۰۱ قانون مجازات اسلامی: هر کسی نقشه‌ها یا اسرار، اسناد و تعلیمات راجع به سیاست داخلی یا خارجی کشور را عالما و عامدا دراختیار افرادی که صلاحیت دسترسی به آنها را ندارند، قرار دهد یا آنها را از مفاد آن مطلع کند به‌نحوی که متضمن نوعی جاسوسی باشد، نظر به کیفیت و مراتب جرم به یک تا ده سال حبس محکوم می‌شود.

در ماده قانونی فوق، موضوع جرم، نقشه‌ها، اسناد و همچنین اسرار و تصمیمات دارای طبقه‌بندی است که کلیه موضوعات سیاسی، نظامی، اجتماعی، فرهنگی، اقتصادی و صنعتی را شامل می‌شود.

راه‌های مقابله با جاسوسی صنعتی:

وجود امنیت در صنعت از ابعاد مختلف (اقتصادی، امنیتی و سیاسی) موجب تقویت و ارتقای توان و موقعیت کشورها در عرصه‌های مختلف شده و از خطرات ناشی از فعالیت‌های جاسوسی می‌کاهد. مدیران باید به این نکته توجه داشته باشند که در عرصه روابط خود با شرکت‌ها و مؤسسات و سایر مراکز وابسته به بیگانه، خطر بیشتری آنها را تهدید می‌کند و از این رو باید با تمهیدات بازدارنده در برابر حملات جاسوسان و تهیه طرح‌های مناسب و یک‌پارچه، اقدامات جامعی را براساس تهدیدات و با تحلیل لازم اجرا نمایند.

هدف نهایی از بررسی تهدیدات و تحلیل آن، تدوین یک طرح امنیتی بازدارنده برای سازمان صنعت و یا پروژه موردنظر است که برخی از آنها به شرح ذیل است:

تعریف و مشخص کردن بخش‌های حساس

تعیین اطلاعاتی که نیازمند مراقبت گسترده هستند.

مشخص کردن افرادی که اجازه دسترسی به اطلاعات محرمانه را دارند.

تعیین وظایف بخش‌های مختلف سازمان در ارتباط با حفاظت از داده‌ها

ارائه تعریفی یکسان از روش‌های کاری ایمن در برابر جاسوسی

اجرای اصول مربوط به کنترل‌های منظم امنیتی براساس آیین‌نامه حفاظت از اسناد و مدارک

تعیین صلاحیت کارکنان و ارائه تحلیل‌های منظم درباره نقاط ضعف کارکنان

حفاظت از اسناد و مدارک و اتخاذ تدابیر امنیتی فنی و سازمانی به‌منظور مراقبت از اطلاعات ارزشمند و محرمانه

حفاظت از رایانه‌ها، اتاق‌های سرور و لوازم ذخیره‌ساز اطلاعات

آموزش کارکنان در بدو استخدام و حین خدمت

امنیت برای کارکنان:

هرگونه طرح در مؤسسات باید در وهله نخست، تدابیر امنیتی مربوط به کارکنان آن مجموعه را مدنظر داشته باشد؛ زیرا کارکنان باتوجه به جایگاه و نوع شغل خود می‌توانند حجم گسترده‌ای از اطلاعات دارای طبقه‌بندی را افشا کنند؛ به‌طوری که سرویس‌های مخفی یا رقبا به‌هیچ وجه بااستفاده از سایر روش‌ها نمی‌توانند به اطلاعات دست یابند. تدابیر امنیتی کارکنان با گزینش و استخدام آغاز و با آموزش‌های بدوی و ضمن‌خدمت ادامه پیدا می‌کند.

اگر کارکنان شرکت‌ها به ضرورت حفظ اطلاعات حساس شوند، در آن‌صورت خواهند توانست فلسفه امنیتی موردنظر رؤسای مراکز را درک کنند؛ چنین کارکنانی سعی می‌کنند از ارتکاب اشتباهاتی‌که باعث لورفتن اطلاعات محرمانه می‌شود، خودداری کرده و سهم خود را در امنیت مجموعه بالا ببرند.

امنیت مادی یا سخت‌افزاری:

استفاده از سیستم‌ها و ابزارهای امنیتی، مانند دستگاه‌های کنترل مراجعین (ایکس‌ری)، دوربین‌های مداربسته، سامانه‌های هشداردهنده و اعلام‌خطر باتوجه به موقعیت و اهمیت هر صنعت، کاربرد دارد.

مسلم است که شرکت‌های متعامل با نیروهای مسلح و مراکز امنیتی باتوجه به حساسیت بالا که خطری از سوی دشمن محسوب می شود، باید در ایمن‌ترین نقطه قرار داشته باشند.

باتوجه به مطالب فوق‌الذکر می‌توان نتیجه گرفت که حفاظت از فن‌آوری، یکی ازفرایندهای اصلی و دغدغه‌های مدیران صنایع و در سطح پایین‌تر مسؤلان واحدهای تحقیق و توسعه می‌باشد.

زیرا بی‌شک فن‌آوری، یکی از ارکان اقتدار دفاعی است و حفاظت از آن به‌معنای حفظ شالوده دانشی و کاهش خطر انتقال ناخواسته اطلاعات مربوط به آن به خارج از سازمان و همچنین جلوگیری از افشای برنامه‌های حیاتی و قابلیت‌های آن است.

داستان دستمال:

تیم خارجی مشغول بازدید از پروژه بود تا درصورت تایید، برای عقد قرارداد تولید و خرید محصول با صنعت وارد مذاکره شود. هنگام ورود به صنعت، به وسیله ی دستگاه دقیقاً چک شده بودند و با علم به این که هیچ وسیله ای برای ثبت اطلاعات در اختیار ندارند، به محل پروژه هدایت شده بودند. با توجه به این که در این گونه بازدیدها نفر یا نفراتی نیز باید از حفاظت در راستای وظایف امنیتی و حفاظتی، حضور داشته باشند. این بار نوبت من بود که این تیم را در کنار کارشناسان و مدیران پروژه همراهی نمایم. در حین بازدید تیم خارجی که شامل ۳ نفر بودند، یکی از آنها ظاهراً دچار سرماخوردگی شده بود و هر از گاهی عطسه می‌کرد و به ظاهر برای رعایت ادب از ما کمی فاصله می‌گرفت و دستمال پارچه‌ای را که همراه داشت، جلوی صورت خود می گرفت. در مدت بازدید که تقریباً ۴۵ دقیقه به طول انجامید، او ۷ یا ۸ بار عطسه نمود که در نهایت تعجب وقتی که وی را زیر نظر داشتم، متوجه شدم دستمالی را که همراه دارد، ۵ بار در نقاط مختلف کارگاه به زمین انداخت و وقتی هم که قصد برداشتن آن را از زمین داشت، به طوری که توجه کسی را جلب نکند، دستمال را کمی به زمین کشیده و بعد بر می داشت. بازدید به پایان رسید و من این موضوع را به مسؤلان خود گزارش نمودم. ظواهر امر مؤید اقدام بیگانه به انجام کار اطلاعاتی و جمع آوری محیطی بود که چون اقدام خاص و یا غیر اصولی در محیط انجام نمی‌شد، اقدامی در خصوص برخورد با بیگانه صورت نگرفت. وقتی موضوع را به رئیس خود منتقل کردم، او بسیار متعجب بود که جاسوسان برای به دست آوردن اطلاعاتی که مربوط به صنعت ما و به ویژه صنایع نظامی است، چگونه از هر راهی وارد می‌شوند.

ایمن گستر حصین

با افزایش روزافزون ارتباطات، تبادل اطلاعات نیز به مراتب بیشتر و بیشتر می شود؛ تبادل اطلاعات یعنی ارسال یک سری اطلاعات از یک مبدأ مشخص به مقصدی مشخص؛ حال هر چه اهمیت و ارزش اطلاعات مبادله‌شده بیشتر باشد، بالطبع امنیت ارسال این اطلاعات هم حیاتی‌تر خواهد شد و در این میان اگر اطلاعات و اسرار مهم یک شرکت یا سازمان چه به شکل عمدی و چه به شکل غیر عمدی لو برود، آن شرکت یا سازمان به نوعی دچار یک حمله جاسوسی شده است؛ چون ماهیت اطلاعاتی که مورد هجوم این نوع حمله‌ها قرار می‌گیرد، نوعا صنعتی است که مهندسان، این پدیده را جاسوسی صنعتی نام نهاده‌اند.

ایمن گستر حصین
www.ig-hassin.com