الانترنت: النشأة ... والأخطار

شبكة أم شبكات؟

منذ الأيام الأولى لظهور أجهزة الحاسب الأولى كانت هناك حاجة لتشبيكها (Networking) والسبب إن تشبيك أجهزة الحاسب له مردودات كثيرة أقلها المشاركة بالمصادر (المادية الملموسة والبرمجية المحسوسة: (Hardware & Software Resources) بين تلك الأجهزة أولا، ورفع درجة الثقة والاعتمادية (Reliability) على المنظومة المحوسبة (بضم الميم) المستخدمة عند تسهيل إمكانية السيطرة على كامل الخزن الاحتياطي لكل البيانات المستخدمة في اية مؤسسة ثانيا، والأمان الممكن توفيره والحماية لحواسيب خدمية رئيسية (Severs) تلك التي تتكل عليها الحواسيب الوكيلة (Clients) والمشبوكة إليها ثالثا. كما إن تشبيك الحاسبات يوفر ويسهل عمليات الاتصال والنشر بأشكالها الإلكترونية المختلفة وما لكل ذلك من مردود مادي مرغوب وعال التبرير.

ولكن ابتداء ما تعريف شبكات الحاسب؟ ان التعريف لشبكة الحاسب هي توصيل لحواسيب كاملة الأهلية (Autonomous) وتشبيك لمصادرها الخدمية (Serving Resources) عبر وسائط اتصال تتراوح بين أسلاك موصلة وألياف ضوئية/ليزرية، و وصلات لاسلكية دقيقة الموجة قد تستخدم التوابع الفضائية، وتعمل تحت سيطرة مراسيم نظم وقواعد تراسل (Protocols).

والشبكات على أنواع تتدرج في مساحة الانتشار فمنها الشبكة المحلية (Local Area Network: LAN) التي تنتشر حاسباتها عبر موقع جغرافي صغير (مباني متقاربة في داخل مدينة)، والشبكة الإقليمية (Metropolitan Area Network: MAN) التي تنتشر حاسباتها ضمن اقليم معين يشمل مدن أو دول إقليمية، والشبكة العالمية أو الكونية الواسعة المواقع (Wide Area Network: WAN). أما الإنترنت فهي غير ذلك وهي ليست شبكة مفردة في هذا التصنيف حيث انها متكونة من تشبيك (Internetworking) أكثر من شبكة واحدة (أوقل انها شبكة الشبكات). ولتبين الفرق بين شبكة تشمل عدة شبكات خاصة ومملوكة من قبل مؤسسة ما عن شبكة الإنترنت العالمية، تعرف الأولى عادة بشبكة إنترنت (Intranet) لتميزها عن الشبكة العالمية الغير مملوكة لأحد والتي نعرفها في الوقت الحاضر بأسم الإنترنت (Internet). ولاهتمام

القارئ غير المتخصص لن نذهب في أغوار الشبكات الفنية بل سيكون الحديث مقتصرا عن الإنترنت.

البداية وتأريخ التطور:

ولشبكة الإنترنت تأريخ لا يبتعد عن صراع القوة والسلطة وحماية مرتكزاتها أيام هدوء السلم وخشية الحرب. فنشأة الإنترنت كانت من أجل حماية مراكز القوة والقواعد المعرفية التي إليهما تستند سنة الصراع في العصر الحديث. وحين تتصارع وتتقاتل الدول فأفضل الضربات تكون تلك التي تسدد إلى مراكز صنع القرار والقواعد المعرفية التي يعتمد عليها. وكذلك كان تفكير الاستراتيجيين في الولايات المتحدة حيث أبتدأت نشأة الإنترنت.

ان التمكن من خطوط الاتصالات والمواصلات وما ينتج عن ذلك من تواصل معلوماتي بين المركز وفروع التنفيذ ذو أهمية استراتيجية ولوجستية في صراع الدول وسيادة الأمم. كذلك كان حال الدولة الرومانية والدولة العربية الإسلامية على سبيل المثال وغيرها من الدول العظيمة الأخرى التي أهتمت للطرق والبريد في تواصلها المعلوماتي المهم بين مركزها وأذرعه الأخرى. وكان للسيطرة على البحار خاصية هامة للإمبراطورية البريطانية أيام مجدها وزهوها مثلا.

هكذا دار الجدل في دوائر القرار الأمريكية يوم أطلق الاتحاد السوفياتي أول قمر صناعي عام ١٩٥٧ الى الفضاء مفتتحا عصرا للسيطرة جديد تكون السماء ساحته بدل اليابسة والماء. واستجابة لفترة الحرب الباردة بين الشرق والغرب حينذاك وفي أوائل أعوام الستينات من القرن الماضي كانت طلبية الدفاع الأمريكية شبكة شبكات تحكّم أمرية لمراكز تلك القرارات والقواعد تصمد لأي هجوم سوفياتي محتمل وتكون ذات مواصفات تقنية عالية مقارنة بشبكة الهاتف التقليدية التي اعتبرت غير ملبية وبالتالي غير معول عليها في ساعات الأزمة، فضربة تقتل مقسما في تلك الشبكة يعني انقطاع خطوطه وتوصيلاته إلى باقي مقاسم الشبكة. واوكلت المهمة الى وكالة المشاريع للبحوث المتقدمة (Advanced Research Project Agency: ARPA). ولم يكن "لأربا" هذه مختبرات وعلماء بل ميزانية ومكتب للتعاقد مع مشاريع علمية في جامعات ومراكز بحثية يعتقد بجديتها. وكانت البداية من وكالة راند (RAND) التي اقترحت فكرة ثورية هامة عرفت بتسليك الحزم (Packets Switching) وهي طريقة تستخدم فيها تقنية ارسال البيانات التي هي نفسها عبارة عن سلسلة من الواحدات والأصفار (لغة تفاهم الحواسيب) على

شكل حزم رقمية (Packets). وتتولى عملية التوجيه لتلك المجموعات الرقمية حاسبات وسيطة عرفت بمعالجات الرسائل الموجهة (Interface Message Processors: IMPs) تتصل بالحاسبات الخدمية (Servers) التي تخدم بدورها الحاسبات الوكيلة (Clients). وبالتالي تكون البنية التحتية (Subnet) للشبكة تتكون من معالجات الرسائل الموجهة المشار لها أعلاه (IMPs) وخطوط التوصيلات بينها التي يمكن ان تكون بدورها سلكية أو لاسلكية وبتقنيات اتصالية مختلفة. وبأمكان المستخدمين بعد ذلك (وبواسطة حاسبات وكيلة Clients وحاسبات خدومة Servers) من الدخول الى الشبكة (والتي هي عبارة عن معالجات موجهة – كمقاسم الهاتف – وخطوط اتصال).

وهكذا بنيت شبكة أربا (ARPANet). بحيث لو دمر واحد من مراكز الشبكة (معالجات الرسائل الموجهة) فأنه لمن اليسير يكون ارسال حزم الرسائل الرقمية (Packets) عبر مراكز بديلة وبمسارات التفافية أخرى. ولقد كان من الضروري وضع قواعد وتعليمات تتفاهم وفقها مجموعات الحواسيب المتراسلة، ولقد عرفت مجموعة القواعد والتعليمات تلك بمراسيم العمل أو البروتوكولات (Protocols) وفي حالة أربا كان الاتفاق قد تم على بروتوكول عرف ببروتوكول التحكم بالنقل (Transmission Control Protocol: TCP) وآخر عرف ببرتوكول الإنترنت (Internet Protocol: IP) ولقد عرف هذين البرتوكولين اختصار ب TCP/IP. وبهذا تكون شبكة الأربا تلك أول إنترنت.

لقد تم تصميم عدد آخر من شبكات تولت تشبيك شبكات أخرى في الولايات المتحدة ودول أخرى، وتم انضمام تلك الشبكات بعد ذلك الى شبكة الإنترنت "أربا" الأم. الأ ان الانعطافة الهامة في عصر الإنترنت هي انتهاء فترة الحرب الباردة أوائل التسعينات من القرن الماضي وبالتالي برزت الحاجة الى الاستفادة من الإنترنت في التطبيقات المدنية التي شهدت بعد ذلك اكتساحا متسارعا للحياة في العالم وأولدت مصطلح العولمة بنصه الفاعل والمتواجد الآن. ولأدراك هذا التسارع تكون الارقام مفتاحا لذلك اللغز. ففي عام ١٩٩٠ كانت الإنترنت تضم ما يقارب ٣٠٠٠ شبكة توصل نحو مئتي ألف حاسب. وفي عام ١٩٩٢ قفز الرقم الى نحو مليوني حاسب. وفي عام ١٩٩٥ وصل الرقم الذي شمل عشرات الألوف من الشبكات تخدم ما يقارب عشرة ملايين حاسب. ومنذ ذلك الحين شهد الرقم الأخير من الحواسيب المشبوكة مع الأنترنت زيادة عالية حتى جعلته

يصل نحو ١٠٠ مليون حاسب قبل نهاية القرن الماضي. ولقد تشكلت جمعيات علمية عديدة ترعى التطور في تقنيات الإنترنت أمثال: IAB, IRTF, IETF, ICANN, ISOC.

واستنادا الى تعريف الإنترنت السابق ذكره مع شبكة أربا الذي قيل فيه ان الإنترنت عبارة عن بنية تحتية تتكون من معالجات حاسوبية (IMPs) ذات وظيفة توجيهية للمجموعات الرقمية وخطوط اتصال سلكية ولاسلكية تنتشر بمواقع جغرافية عديدة في العالم حيث تتولى تلك المراكز وظيفة تجهيز خدمة الإنترنت (Internet Server Provider: ISP). ويمكن لأي شبكة أو شخص ان يتصل بالإنترنت عبر تلك المراكز. وبهذا تكون الإنترنت غير مملوكة لدولة معينة أو جهة خاصة. الا ان من يملك الإنترنت فعلا هو من يتواجد بشكل فاعل عبر النشر والتراسل والخدمة وغير ذلك من فعاليات التواجد والأهمية.

الأخطار:

ان مشاركة المصادر وعلو الاعتمادية وحسن الأداء في الاتصال ميزات للشبكات بشكل عام. الا ان هذه الميزات تصحبها أيضا عوائق أخرى مثل الكلفة والتعقيد في الماديات الملموسة (Hardware) والبرمجيات المحسوسة (Software) ومشاكل اجتماعية ناتجة وتهديدات أمنية. وفي هذه المقالة سنركز فقط على تلك التهديدات الأمنية والتي تكون في العادة من أشكال ثلاثة نوجزها كما يلي:

١- الاستخدام الغير الشرعي (Access Violation) للمصادر: ففي تقرير المكتب الفدرالي الأمريكي (FBI) ومعهد أمن الحاسبات (CSI) لعام ٢٠٠٠ يذكر ان ٨٠% من المخالفات الأمنية التي حصلت في مؤسسات وشركات شملتها إحصائيات التقرير كانت من أفراد ومجموعات منتسبين لتلك المؤسسات والشركات. ان هذا الرقم يرفع أهمية الاستراتيجية الواجب اتباعها لامن الشبكة بشكل خاص.
٢- الدخلاء (Hackers): ان تعبير الدخلاء يعني في العادة واحد من ثلاثة: أناس يخترقون أمنية الشبكة، أو أناس يلغون أمنية برامج تطبيقية من أجل أغراض ذات طابع قرصني، أو أناس يهتمون بكتابة برامج مؤذية أمثال الفيروسات (موضوع الفقرة القادمة). وفي العادة يقوم هؤلاء الدخلاء بأعمال ذات فعاليات متعددة الأشكال متحدة الهدف في القصد من الأذى والتشويش على العمل. فعلى سبيل المثال وفي اليوم السابع من الشهر الثاني من

عام ٢٠٠٠ قام ٧٢٠٠ من محترفي هذا التصرف (كـدخلاء) بـالهجوم المنـضم ذو الطبيعة الموزعة (Distributed Denial of Services) بأعمال غير مصرح لها على عدد من مواقع الإنترنـت المـشهورة أمثـال: Yahoo, E*Trade, Amazon.com, eBay. وفي العمليات الغير مصرح لها من هذا النوع تمطر (برفع التـاء) أعـداد مـن الحاسبات الخادمة لمواقع الشبكة ببيانات لا معنى، الا ان الهدف من ذلك شل حركة تلـك المواقع وجعلها مشغولة عن خدمة مستفيدها الحقيقيين كونها غارقة في خدمة عمليـات لا نهاية لها وبعيدة عن أعمال قانونية مرخص بها. وأنماط الهجوم الذي يقوم بـه الـدخلاء عموما ذو أشكال عدة فمنها التعرف على هيكلية الشبكة المعنية لإدخال الأذى في وقـت لاحق أو بأخذ عينات (Scanning) عن معلومات صادرة من حاسبة معينة في الـشبكة لأغراض غير مصرح بها. كما ان الأنماط غير القانونية تلك قد تشمل خطـف وصـلة معينة بالاستيلاء على أحـد أطرافهـا (Hijacking)، أو التـصنت (Sniffing) علـى اتصالات تجري، أو الدخول عنوة الى احدى حاسبات الشبكة واستخدامها دون تـصريح مشروع، أو سرقة كلمة سر لأحد مستخدمي الشبكة الشرعيين غفل عن حفظهـا بـشكل حذر، أو التمازج الاجتماعي (أو ما يعرف في أدب الدخلاء بالهندسة الإجتماعية: Social Engineering) مع مستخدمي شبكة للحصول على معلومات تخدم هدف غير مشروع أو مصرح به.

٣- الفيروسات (Viruses): ان الفيروس هو برنامج صغير قد يلحق نفسه مختبئا بملف أو قد يكون مستقلا بذاته. وقد يلحق الفيروس الضرر بالبيانات التي يهاجمها أيضا. والفيروسات بشكل عام تسبب تلفـا برمجيـا بالـذاكرة الحيـة أو الافتراظيـة (Real or Virtual Memory) للحاسب، أو قد تبطيء عمليات الحاسب، أو ان تسبب توقفا كاملا للجهـاز. ولقد مر تطور الفيروسات بأجيال ثلاثة:

أ) الجيل الأول المعروف بفيروس قـاطع الاسـتنهاض (Boot Sector Virus): ولا يشكل الفيروس من هذا النوع أي تهديد للشبكة وذلـك لانـه يـستقر فـي قـاطع الاستنهاض الخاص بالقرص وينتقل من القاطع عند استخدام القرص الموبوء الـى الذاكرة الحية للحاسب لينسخ نفسه وعدواه بعد ذلك لأي قرص يستخدم في مـسوقة الأقراص لتلك الحاسبة المصابة. وبالتالي تكون وسيلة انتشاره وعدواه محدودة مـن حاسبة الى أخرى.

ب) الجيل الثاني المعروف بمعدي الملفات (File Infector Virus): ويمتاز هذا النوع من الفيروسات بقابليته على ان ينقل العدوى الى الملفات الفاعلة في البرنامج والتي تكون في العادة تمدداتها (extension) من النوع (.com, .bat, .exe, etc.). وهذا النوع من الفيروسات يشكل خطرا على الشبكات المحلية (LAN) بشكل خاص والتي يشيع فيها المشاركة بالمصادر البرمجية ذات الفاعلية المحلية وذلك لان أي مستخدم (على حاسب معين) يطلب خدمة برنامج (مستقر على حاسب آخر) مصابة ملفاته الفاعلة بعدوى الفيروس يحكم على ملفاته الفاعلة بالعدوى أيضا بذلك الفيروس.

ت) الجيل الثالث المعروف بفيروس البرنامج الملحق (Macro Virus): وهو عبارة عن شفرة برمجية تلحق نفسها (Attachment) بملف آخر. ان هذا النوع من الفيروسات هو الخطر الحقيقي على الشبكات بشكل عام وعلى الإنترنت بشكل خاص وتطبيقاتها العديدة.

ولأهمية الجيل الثالث من الفيروسات وتأثيره على شبكة الإنترنت واستخداماتها فأن أنواع هذا الفيروس من الأهمية التي تستحق إدراجها وذكر خطر كل نوع منها. ان أنواع هذا الفيروس هي كالآتي:

١- الخدعة (Internet Hoaxes): وهذا النوع من الفيروسات له قابلية الاستيلاء على برنامج البريد الإلكتروني ودفتر العناوين الخاص بالبريد الإلكتروني حال استيطانه في الحاسب المصاب وإرسال جميع العناوين المتوفرة رسائل وهمية هدفها انتقال الفيروس الى حاسبات الآخرين حال قراءتهم لتلك الرسائل الإلكترونية واطلاعهم على البريمج (الفيروس) الملحق. إضافة الى الضرر المحتمل المبرمج له هذا النوع من الفيروسات فأن إرسال كم كبير من الرسائل يشغل الأجهزة المكلفة للتعامل مع عمليات البريد مما يسبب تأخيرا واعاقة للعمليات الصحيحة نتيجة الاختناق الحاصل.

٢- القنبلة الموقوتة (Logic Bomb): عند وصول هذا الفيروس الى الحاسبة الضحية يستقر فيها منتظرا حدثا معينا (كتأريخ أو وقت معين أو عمل إجراءي آخر كقراءة أو نسخ أو حذف ملف ... الخ) للبدء بعمله المؤذي في أغلب الأحوال.

٣- حصان طروادة (Trojan Horse): تقول الأسطورة ان طروادة كانت مدينة عظيمة ومنيعة الحصون لم يستطع الغزاة من مقاتلي إسبارطة دخولها رغم شجاعتهم وصبرهم على حصارها الذي طال عشرة سنوات. وفي الأخير لجأوا الى حيلة ادعاء الانسحاب مع إهداء أهالي طروادة حصان خشبي كبير كان قد اختبأ فيه ثلة جنود إسبارطيين. وبعد ان قبل أهالي طروادة الهدية وادخلوها إلى مدينتهم. خرج المختبئون ليلا ليفتحوا أبواب المدينة الحصينة لجيش إسبارطة المنتظر كي يدخل ويفتك بأهالي طروادة شر فتك. كذلك هو الفيروس المسمى بهذا الاسم الذي يبدو بريئا لكنه في الحقيقة يستخدم لإدخال برنامج آخر ضار.

٤- الديدان (Worms): وهي نوع من الفيروسات ذات القابلية على التكاثر والاستنساخ الذاتي حتى اختناق منظومة العمل بزحمة امتلاء الذاكرة بشكليها الحقيقي والأفتراظي وتوقف سعتها عن فسحة العمل اللازمة.

٥- ذو الفعل المستتر (Stealth): يؤدي هذا الفيروس عمله بتستر خادع كأن يحذف الملفات المستهدفة ويؤدي دور أخبار المنظومة عن وجودها، أو يصيبها بوبائه ويخبر المنظومة انها صحيحة لا عيب فيها مما يجعل الخديعة أو الكذبة مزدوجة على الضحية صاحب الجهاز الذي لا يكتشف الضرر الا ساعة الحاجة.

٦- المتغير (Variant): يتخلق هذا النوع من الفيروسات بمهاجمة فيروسات معروفة وبالتالي يتقمصها لكن مع فارق التعديل والتغير الذي يدخله على تكون الفيروس الضحية. ان لهذا النوع من الفيروسات قابلية التميز بين الفيروس المعدل كضحية له وبين الفيروس غير المعدل من أجل مهاجمته نحو تعديله حسب توجهات هذا الفيروس. ان قابلية التميز هذه تعرف بالتميز الذاتي (Self Recognition).

٧- المشفر (Encrypted): وهذا أحدث أنواع الفيروسات وأخطرها درجة. ان هذا النوع من الفيروسات يتكون من جزئين. الجزء الأول مكلف بتشفير بريمج الفيروس (الجزء الثاني) الفاعل لتعقيد اكتشاف الفيروس. وعند بدء تنفيذ الفيروس عمله يبدأ الجزء الأول الذي يزيل شفرة بريمج الفيروس الذي بدوره يبدأ العمل بعد ذلك بحيث يستطيع نسخ نفسه أو التمسكن في الجهاز الموبوء. كما ان لهذا النوع من الفيروسات نوع يتغير تشفيره كل مرة باستخدام خوارزمية معينة ومفتاح متغير (Certain Algorithm and a Variable Key). ولأن البرامج الكاشفة للفيروسات تبحث في العادة عن شفرة تشغيل معينة، فأن هذا النوع من الفيروسات يجعل عمل تلك البرامج الكاشفة عسيرا و صعبا.

٨- الفيروس تحت البحث (Research Virus) أو التجريب: وهذا النوع من الفيروسات غير معرف حتى هذه التسمية (أو المرحلة) وهو لا يزال في مختبرات البحث والتجريب قبل اطلاقه على الشبكة نحو عمله الفيروسي. وقد تظهر نسخ قليلة من هذه الفيروسات للتجريب وملاحظة تأثيراتها.

الخاتمة:

لقد أصبح استخدام أجهزة الحاسب دليلا على التطور والرقي ومن أسباب التقدم. والحاسب جهاز يعتمد في واحد من جوانب تطوره على إنتاجه وتحديات ذلك الإنتاج بتغذية مرتدة الى جهاز الحاسب نفسه، وهذا أمر غير مسبوق في التأريخ. فهذا الجهاز الجديد والمولود في أواسط القرن الماضي لم تمض على ظهوره الأول سوى عشرات من السنين، ورغم ذلك فأن تطوره السريع وقفزاته العلمية جعلت حضوره الفاعل ضرورة وحاجة في كل مجالات الحياة. ان تعاون وتواصل تلك الأجهزة في قفزة الإنترنت سلب البعض هدوءهم وقلل طمأنينتهم، فكانوا صنفين، صنف منكر ينقرض وصنف مدرك يتفاعل. ويبقى السؤال في كيف يمكن الاستفادة من شبكة الإنترنت التي نشأت ملك لمؤسسة في دولة وأصبحت في تطورها الحالي غير مملوكة لأحد. ورغم ان شبكة الإنترنت لا زالت تحبو في عصرها البرونزي الحالي فأنها ستصنع إرهاصاتها المستقبلية التطورات الموعودة في مجال تقنيات الذكاء الاصطناعي على وجه الخصوص والاتصالات على وجه العموم، بالإضافة الى تسارع التطور في ماديات وبرمجيات الحاسب وجوانب تطبيقاته الأخرى. وكما هو الحال دائما حين يزيد اعتمادنا على شيء ما فأنه يصبح مهما، وحين يصبح مهما تستهدفه الهواجس والأخطار. والأخطار عموما تتطلب وسائل حماية وتصدي.