السفير
الاربعاء 24-11-2010 العدد 11749

مؤتمر نحاس وفضل الله يكشف وقائع جديدة من محاولات توريط «حزب الله»: احتلال إسرائيلي كامل لقطاع الاتصالات... بالصور والوثائق والمعلومات

من انتظر المؤتمر الصحافي الطويل، الذي عقده وزير الاتصالات شربل نحاس ورئيس لجنة الإعلام والاتصالات النيابية حسن فضل الله، أمس، في وزارة الاتصالات، للتعرف الى حجم الاختراق الإسرائيلي لشبكات الاتصالات اللبنانية، لم يكن ليتوقع وصولها إلى حد الاستباحة التامة لكل القطاع.

اجتياح بالطول وبالعرض كان القطاع يشهده، كما ظهر في العرض الذي قدمه رئيس الهيئة المنظمة للاتصالات الدكتور عماد حب الله، بالتعاون مع المهندسين ديانا بو غانم ومحمد أيوب، بالصور والوثائق. اجتياح ربما لم يكن من الممكن معرفته لولا اعترافات «عملاء الاتصالات» الذين اكتشفوا مؤخراً. هؤلاء، ولا سيما منهم العميلان شربل قزي وطارق ربعة، فتحوا الباب على احتلال إسرائيلي منظم ومتكامل لكل نظام الاتصالات. بمكوناتها جميعها، فكانت شركتا الخلوي وشركة أوجيرو، وبالتالي الاتصالات الخلوية والأرضية، في متناول ايدي الإسرائيليين، من ألفها إلى يائها. وألفها هنا تبدأ من الشبكات وأعمدة الإرسال اللبنانية التي تبين أنها زرعت في أماكن تراعي الرغبة والتوجيهات الإسرائيلية، بما يضمن لها القدرة المثلى للوصول إلى كل ما تشاء التقاطه من البث الراديوي اللبناني وبوضوح تام، إلى يائها التي لا تقل عما نشاهده في أفلام الخيال العلمي. فقد تبين من خلال المعطيات التي عرضها حب الله، أن الاختراق الإسرائيلي وصل إلى حد التحكم الكامل بالهاتف الخلوي الذي نحمله بأيدينا، وكذلك بالشريحة التي في داخله، من خلال برنامج متطور يزرعه في الهاتف، ويستطيع الإسرائيلي من خلاله:

الاستماع إلى المكالمات، التنصّت على الحوارات الجارية في محيط الهاتف، الاطلاع على الرسائل النصية (SMS)، إرسال رسالة قصيرة (SMS) كإنذار في حال استقبال الهاتف المستهدف لاتصال، أو تغيير الشريحة SIM، أو إيقاف أو تشغيل الهاتف، إظهار سجل المكالمات الخاص بالهدف (المكالمات الصادرة والواردة والمدة والوقت)، التحكم بالخدمات (أي تشغيلها وتوقيفها) عبر إرسال رسائل غير مرئية إلى هاتف الهدف، التعقب عبر الـGPS أو الـCell ID في حال كانت خدمة الـGPS غير متوفرة في الهاتف، إظهار اسم المتصل أو المتصل به في حال وجوده على لائحة الأسماء الخاصة بهاتف الهدف، اعتراض الرسائل الالكترونية (e-mail).

وهذه التقنية غير المعروفة على نطاق واسع، والمستعملة من قبل عدد محدود من أجهزة المخابرات العالمية، ومنها إسرائيل، تبين بحسب ما كشفه النائب حسن فضل الله، رداً على سؤال في نهاية المؤتمر الصحافي عما يشاع عن اختراق حزب الله، أنها استعملت فعلاً في العام ٢٠٠٧، في محاولة لتوريط الحزب.

كيف؟ بدأت القصة حين طلب العقيد وسام الحسن لقاء رئيس شعبة الارتباط والتنسيق في حزب الله وفيق صفا، ليعلمه عن التوصل إلى معلومات عن اختراق حزب الله بثلاثة أشخاص، تبين أنهم يستعملون ثلاثة خطوط كان قد اشتراها العميل أديب العلم، لصالح الإسرائيليين. ويتابع فضل الله سرد القصة لينهي مؤكداً أن التحقيقات المكثفة والجدية التي أجرتها مخابرات الجيش اللبناني وحزب الله بالتعاون مع وزارة الاتصالات، أفضت بما لا يبقي مجالاً للشك أن هؤلاء الثلاثة كانوا يحملون هواتفهم التي تحمل خطوطهم المعروفة وكذلك الخطوط التي زرعها الإسرائيليون، والتي استطاعوا من خلالها القيام بكل ما تسمح به هذه التقنية وتم تفصيله خلال العرض الذي قدمه حب الله. وهو ما أكد أن الاختراق تم بالفعل، لكن ليس عبر تجنيد هؤلاء المقاومين الثلاثة، بل عبر اختراق هواتفهم.

وما ملكته إسرائيل من قدرات للتحكم في قطاع الاتصالات، استفادت منه على أكمل وجه في عدوانها في العام ٢٠٠٦. كان الطيران الإسرائيلي جاهزاً لقصف أي منزل في الضاحية الجنوبية ترفع فيه سماعة الهاتف، بثوان معدودة.

عناصر عديدة حملها المؤتمر إذاً، كلها تقود إلى عنوان واحد: المطلوب حالة طوارئ وطنية لمواجهة الحرب المستمرة على لبنان. وهو ما أكده النائب فضل الله، الذي أشار في بداية المؤتمر الى «اننا اليوم أمام قضية وطنية تتعلق بالأمن القومي الذي من المفترض أن يكون فوق كل الحسابات السياسية، والانقسامات والخلافات. وأضاف: هذه قضية تتعلق بأمن الدولة ومؤسساتها وأجهزتها، وبأمن كل القوى السياسية على اختلاف انتماءاتها، وبكل مواطن أو مقيم على الارض اللبنانية من عرب وأجانب وهيئات ومنظمات دولية وسفارات.

كما دعا فضل الله «جميع اللبنانيين على اختلاف انتماءاتهم الى العمل معاً لمواجهة هذا الخطر على امنهم وحريتهم». وأكد أن الحد الأدنى المطلوب من الدولة اللبنانية هو رفع دعوى قضائية دولية ضد اسرائيل.

الوزير نحاس بدوره، حملت كلمته إشارات عدة في كل الاتجاهات، أولاها أننا في لبنان لا يمكن أن نتعامل مع قطاع الاتصالات بصفته قطاعاً تجارياً ومصدراً للدخل فقط، هو قطاع أمني بامتياز ومرتبط بأمن الوطن والمواطنين، مشيراً إلى أن «الاتصالات قائمة على أقانيم ثلاثة: تجاري واقتصادي اولا، ضريبي واحتكاري ثانيا، وتقني وامني ثالثا».

وبالرغم من أنه تقرر تأجيل الحديث عن الحلول إلى مؤتمر ثان يعقد في المجلس النيابي قريباً جداً، كما قال فضل الله، اختصاراً لوقت مؤتمر، الذي استغرق نحو ساعتين، إلا أن الوزير نحاس بدا متخوفاً من المحاولات السياسية الرامية إلى تعطيل مشروع الألياف الضوئية لأهداف سياسية بحتة وبعيدة عن المصلحة العامة. وأعاد التأكيد أن «إحدى غايات المشروع أن يتمكن من نقل المعلومات من شبكة الراديو الى منظومة أكثر أماناً. من هنا أهمية أن تتمكن الوزارة، بوصفها مسؤولة عن هذا القطاع لناحية حريات المواطنين والأمن الوطني، من الاشراف والرقابة الفعلية على مكونات هذه الشبكة». وأكد أن الوزارة بدأت الخطوات العملية الممكنة في الوقت الحالي للحد من الاختراق الإسرائيلي.

إيلي الفرزلي

نحاس: الاتصالات ليست قطاعاً تجارياً فقط

بدأ وزير الاتصالات د.شربل نحاس المؤتمر الصحافي، الذي عقد في قاعة المؤتمرات في وزارة الاتصالات، وحضره النائبان نبيل نقولا وعباس هاشم، وحشد اعلامي بالاشارة إلى مؤتمر المندوبين المفوضين للاتحاد الدولي للاتصالات، الذي عقد في المكسيك، والذي تقدمت خلاله المجموعة العربية نيابة عن لبنان باقتراح قرار يدين القرصنة والتعديات والخروق الإسرائيلية على شبكات الاتصالات في لبنان، واستطاعت الحصول على قرار يدين اسرائيل بالاسم وينص على ان «مرافق الاتصالات في لبنان قد تعرضت ولا تزال تتعرض للقرصنة والتداخل والتعطيل وبث الفتنة من قبل إسرائيل على الشبكات الثابتة والخلوية اللبنانية للاتصالات».

وقال نحاس إنه «خلال المرحلة التي سبقت انعقاد المؤتمر، وبعد انتهائه، قامت الوزارة بالتعاون الوثيق مع رئيس الهيئة المنظمة للاتصالات بالانابة الدكتور عماد حب الله، الذي كلّفتُه بنيابة رئاسة الوفد اللبناني الى المؤتمر الدولي للاتصالات، ومع عدد من الفنيين المتخصصين في الوزارة منهم المهندسين ديانا بوغانم ومحمد أيوب، بأعمال ميدانية سمحت بجمع معلومات مفصلة عن واقع الاختراقات. كما استند الفريق الى معطيات متوافرة لدى الجهات المشغلة للشبكات اللبنانية، واجرت الاتصالات اللازمة بالوزارات المعنية، ولا سيما وزارتا الدفاع والداخلية. وقام الفريق بتحليل هذه المعطيات مستعينا بأحدث المراجع الفنية المتوافرة، وخلص الى صورة دقيقة عن واقع هذه الاختراقات.

وأوضح أن «الاختراقات الإسرائيلية أمر مثبت وأكيد ومداها واسع جدا. ولا مجال للنظر إلى قطاع الاتصالات في بلد يواجه عدوانية دولة لعلها الأكثر تقدما في العالم في مجال تقنيات الاتصالات والتشفير وحماية الأنظمة، على انه مجرد قطاع تجاري. فالاتصالات قائمة على اقانيم ثلاثة: تجاري واقتصادي أولا، وإنما ضريبي واحتكاري ثانيا، ونضيف تقني وامني ثالثا. ومن الواجب الوطني أن نتعامل مع قطاع الاتصالات على اساس هذه الاقانيم الثلاثة مجتمعة في كل خطوة إجرائية أو إدارية أو فنية نتخذها».

وأشار إلى أن المسؤولية العامة أكيدة في هذا المجال، لاسيما من خلال: وضع شروط تسمح بتوفير الخدمات التي يطمح اليها اللبنانيون، افرادا واسرا ومؤسسات، حسن إدارة العبء الضريبي والريعي الذي أرهق به هذا القطاع لناحية خفض وطأته او توزيعه على الشرائح الاجتماعية والقطاعات، تحصين أمان الشبكات والاتصالات لحماية الحريات لشخصية والمعلومات التجارية والادارية، وبشكل اخص الأمن الوطني.

وقال نحاس «إن احدى غايات تمديد شبكة الالياف الضوئية ان تتمكن من نقل المعلومات من شبكة الراديو الى منظومة اكثر امانا». وأكد على أهمية ان تتمكن الوزارة، بوصفها مسؤولة عن هذا القطاع لناحية حريات المواطنين والامن الوطني، من الاشراف والرقابة الفعلية على مكونات هذه الشبكة.

من اليمين: بو غانم، انطوان البستاني، فضل الله، نحاس، حب الله وايوب (عباس سلمان)

تضمن العرض الذي تناوب على تقديمه رئيس الهيئة المنظمة للاتصالات بالإنابة الدكتور عماد حب الله، والمهندسان محمد أيوب وديانا بو غانم، تقديم صورة واضحة عن واقع الإتصالات في لبنان والمشاكل التقنية التي تعتريها والخروقات الإسرائيلية التي تعرضت وتتعرض لها والتي أدت لإدانة إسرائيل والتوصيات الواجب اتباعها لسد الثغرات. وقسم العرض إلى ثلاثة محاور.

وتناول المحور الاول واقع الاتصالات وخلاصة أعمال القرصنة والاختراقات الإسرائيلية

أ ـ واقع التجهيزات التقنية والشركات المصنّعة:

١) التجهيزات والمعدّات والتطبيقات مستوردة بمجملها من شركات اجنبية وغير خاضعة لأي معايير اختبار واختبار ولا قدرات مؤسسية للتحقّق الفنّي.

٢) الأجهزة والأنظمة الإدارية والفنّية للمشغّلين لا تستوفي أبسط الشروط المهنية للسلامة والأمان مثل: دمج مهام يفترض فصلها، غياب معايير واضحة لأصول وسبل تعامل العاملين والمصنّعين والمشغّلين مع بيانات الشبكات وكلمات السر، قنوات الإخطار والرقابة والتدخّل والتصحيح معطلة.

ب ـ صلاحيات واختبار العاملين في القطاع، ولا سيّما الأجانب، إذ انهم لا يخضعون لأي تدقيق أمني (كعلاقاتهم أو تاريخهم أو ارتباطاتهم بالعدو مثلا)، كما أن بعض أنظمة الأمان في شبكات الاتصالات معروفة بتخصص العدو الإسرائيلي بتصنيعها ما يؤمن بوابات عبور خلفيّة تُتيح النفاذ إلى أنظمة تلك الشبكات. بالنتيجة فإن «القطاع محكوم بمعايير تجارية دون اعتبار للأمن الوطني».

ج ـ وضع الشبكات الاتصالات:

١) غياب الفاعلية والترابط بين أنظمة المراقبة والتحكم:

- غياب التنسيق بين أقسام الشبكة المختلفة.
- أعطال متكرّرة على الكوابل والإنترنت.

٢) انتشار معيدات البث (Repeaters) غير الشرعية بشكل عشوائي.

٣) هناك اعتماد أساسي على شبكة الاتصال الميكروويو الراديوية في وصل البنية التحتية بعضها ببعض، وهي شبكة أكثر عرضة للتشويش والتنصت والاختراق.

وبعد استعراض وسائل القرصنة والاختراقات الاسرائيلية، ونتائجها، انتقل حب الله إلى المحور الثاني من العرض الذي تضمن «المكوّنات الرئيسية للشبكة الخلوية وعوامل الأمان فيها والتي قد تكون هي نفسها سببا للخرق. فالثالث الذي تحدث عن «القرصنة واختراق شبكات الاتصالات»، مشيراً إلى أن الانتشار التقني الإسرائيلي على الحدود اللبنانية ـ الفلسطينية يتيح:

- التجسس على كامل الاتصالات الخلوية واللاسلكية (والثابتة).
- تحديد مواقع الاتصالات ولا سيّما اللاسلكية وتعقّب حركة المتصلين.
- الإطلاع على بيانات المتصلين.
- التشويش وعزل وتعطيل جزئي أو كلي لشبكات الاتصالات.
- السيطرة على شبكة الربط الميكروويو الراديوية والتحكم بها والتحكم بشبكات الخلوي.
- اختلاق اتصالات ورسائل.
- توسعة تغطية الشبكة لداخل الأراضي الفلسطينية المحتلة باستخدام معيدات البث لتأمين اتصالات مع العملاء من الأراضي المحتلة باستخدام شرائح لبنانية.
- توسعة تغطية الشبكة الإسرائيلية للأراضي اللبنانية لتأمين اتصالات مع العملاء (شرائح إسرائيلية).
- كشف وجود وتحركات حملة الشرائح اللبنانية وتوفير خدمة التجوال لحملة الشرائح غير اللبنانية وطواقم الأمم المتحدة وتأمين وصلات ربط لاسلكية مباشرة عند الحاجة مع العملاء.
- التجسس على اتصالات قوات الطوارئ الدولية.

ثم اورد حب الله أمثلة عدة على الخروقات التي قامت بها اسرائيل، كما عرض صوراً وبيانات تظهر كيفية حصول هذه الخروقات بشكل دقيق، بالاضافة إلى خرائط تبين اختراق الوصلات الميكروويو الراديوية ما بين محطات الإرسال الخلوية وبقية بنية الشبكة عبر تقاطعاتها مع المواقع الإسرائيلية.

كذلك عرضت صور الهوائيات الاسرائيلية الموجهة إلى الاراضي اللبنانية، كما تم تصويرها عبر الفيديو. ومن أمثلة الاختراقات ما يتم عبر استخدام عدة أنواع من معيدات البث (Repeaters) التي تهدف إلى زيادة تغطية محطات الإرسال التابعة لشبكتي الهاتف الخلوي (أم تي سي، ألفا) إلى داخل الأراضي الفلسطينية المحتلة وبالتالي يصبح بإمكان الجيش الإسرائيلي وأجهزة مخابراته إجراء مكالمات هاتفية من داخل الأراضي الفلسطينية المحتلة باستخدام خطوط خلوية لبنانية، حيث تظهر جميع الاتصالات كأنها أجريت من داخل الأراضي اللبنانية.

حرب تموز

وبالنسبة للاختراقات في حرب تموز ٢٠٠٦، أوضح حب الله أنه تبين أنها تمت عن طريق تنفيذ أوامر بطريقة مشبوهة وغريبة على عدد من السنترالات المسؤولة عن إدارة اتصالات الجنوب والبقاع وبيروت وقضاء بعبدا والضاحية الجنوبية ضمناً. وقال إن ما رُصد يُمكن من خلاله الدخول إلى مجموعة دعم نظام المُقسَم (السنترال). وقد تلى الأمر الأول أمر تحويل الأوامر إلى منفذ معين، فقد حوّلت الجهة المخترقة الأوامر إلى منفذ وهمي Dummy Terminal، وذلك كي لا يتم تسجيلها في نظام تسجيل الأوامر (Events Log) وهي طريقة محترفة لتنفيذ الأوامر والتعديلات دون أن يتم تسجيلها ودون إصدار أي إنذار خطير للمراقبين. وحاول المسؤولون والشركة المشغّلة معرفة طريقة الخرق ولم يتبين أي أثر عبر الوسائل التقليدية، كما قام تقنيو الشركة بفصل نظام التحكم الذي تستخدمه الشركة المشغّلة للدخول إلى المُقسَمات من خارج الشركة، وكذلك قاموا بمراجعة الأقسام المسؤولة عن نظام الحماية على الإنترنت وتمّ بفصل الاتصال مع وزارة الاتصالات. وبالرغم من كل هذه التدابير تبين أن المُقسَمات تعرضت للاختراق عدة مرات في الأيام التالية، وكان التفسير الوحيد المتبقي أن الاختراق يأتي من جهة شبكة النقل والوصل (وصلات ميكروويو مخصصة للاختراق). وأوضح حب الله أنه بالمحصلة لم يتمكن التقنيون من وقف الاختراق الذي استمر لأيام. وذكّر بمشاكل قصف أقسام من الضاحية بناءً على استعمال بعض الهواتف الثابتة، كما ذكّر ببعض القصف الذي أدى للابقاء على بعض الوصلات في شبكات التواصل.

اختراقات بكل الاشكال

من جهة أخرى، أوضح أن الدخول إلى الأنظمة المعلوماتية يُتيح بالتالي التلاعب بسجلات الاتصالات، إظهار اتصالات و... إصدار سجلات لاتصالات لم يقم بها المشترك. وأشار إلى أن «هذا ممكن بشكل مباشر (من داخل الشركة)، وعن بعد (من خلال الاستفادة من خدمة VPN التي تُتيح الدخول عبر الإنترنت وتنفيذ مختلف الأوامر والتطبيقات المتاحة من داخل الشركة)، وعبر اختراق الوصلات الرئيسية لشبكة GPRS أو الوصلات الانتهائية (Last mile)، وكذلك عبر زرع تجهيزات ملوّثة.

أما بالنسبة لإمكانية الدخول عبر الـ VPN، فأشار إلى أنه «من المؤكد أنه يمكن لأي موظف / مخترق في شبكة اتصالات مع صلاحيات واسعة أن يفعل الأمور التالية:

١. تعريف مجموعة من الأرقام وإلغاء إصدار سجلات الاتصالات (CDR) التابعة لها، عبر:

- تعريف مجموعة من IMSI MSISDN، وKi في الـHLR وAUC.
- وضع مجموعة الأرقام في جدول يبين الأرقام المتّصلة والأرقام المتصل بها.
- إزالة Charging Case للمجموعة المعرفة.

٢. القيام باتصالات بأرقام متعددة باسم مشترك ما وبالتالي إمكانية إصدار سجلات الاتصالات لمكالمات لم يقم بها هذا المشترك، عبر:

- إجراء الاتصالات من النوع التجريبي Test Calls

وهذا ممكن بشكل مباشر (أي من داخل الشركة) أو عن بعد (من خلال الاستفادة من خدمة VPN التي تُتيح الدخول عبر الإنترنت وتنفيذ مختلف الأوامر والتطبيقات المتاحة داخل الشركة).

اختراق الأجهزة والشرائح

وقال إن القسم الأكبر مما تبقّى يتعلق بالأجهزة والشرائح (SIM) التي هي مع الجميع، ملخصاً ما يحصل بالنسبة لـ: نسخ شريحة الهاتف الخلوي SIM Card، تعديل الرقم التسلسلي للهاتف الخلوي IMEI. إنزال برمجيات على الهاتف الخلوي، برمجة هاتف خلوي كامل (IMSI + IMEI)، زرع هاتف خلوي كامل (IMSI + IMEI).

اما المخاطر الناجمة عن الاختراق، فهي:

- الاستحصال على الأرقام السرّية التي تعرّف بالمشترك عبر شريحته (IMSI, KI) وعبر جهاز الهاتف خاصته (IMEI).
- يمكن للاختراق أن يحصل عبر هاتف ملوّث، أو برمجيات، أو عن بعد أو عبر رسائل صامتة، أو عبر مصنّع، أو مشغّل، أو مصنّع الشرائح، أو عبر محطة وهمية، أو عبر البث الهوائي.
- هذه الاختراقات تؤدّي إلى معرفة الرموز السرّية، أو مسح الشريحة الذكية الخاصّةSIM بمشترك معيّن، أو تعديل الرقم التسلسلي لجهاز الهاتف الخاص وحتّى زرع هاتف خلوي كامل أو برمجة هاتف خلوي كامل.
- الأوضاع الخطيرة تؤدي بما لا شك فيه إلى تقمّص شخصيّة المشترك، واختلاق اتصالات ورسائل، والتحكّم بالخدمات (كتشغيلها وتوقيفها) والتنصّت على المكالمات والإطلاع على الرسائل والبريد الإلكتروني وبالطبع تحديد المكان والتتبّع كما التنصّت المحيطي.
- على صعيد المثال، فإن زرع المحطة الوهمية يمكّن من كل ما ذكرناه.
- معرفة الرموز السرّية يمكن أن يوصل إلى نفس النتيجة.
- الإصدارات المختلفة للشرائح تواجهها درجات عدة من الخروقات وإمكانياتها.

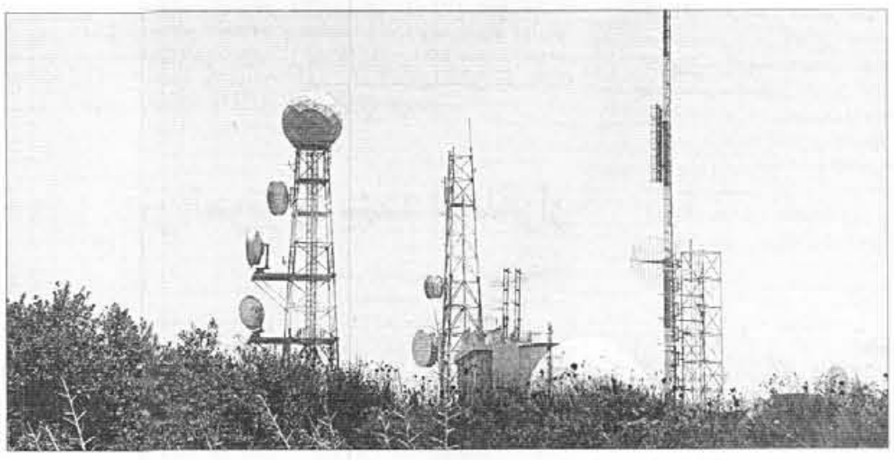
وخلص إلى أن نسخ نفس البطاقة SIM ما يسمح باختلاق اتصالات باسم المستخدم الأصلي، تعديل الرقم المتسلسل لجهاز الهاتف الخلوي IMEI ليُماثل الرقم المتسلسل لهاتف مشترك ما يسمح بنسب اتصالات مفبركة لصاحب الجهاز الأول، التنصّت والاستماع إلى المكالمات والرسائل القصيرة، التحكّم بالخدمات (أي تشغيلها وتوقيفها)، التعقّب والتتبّع، التنصّت المحيطي، تقمّص شخصية مشترك من خلال برمجة هاتف خلوي كامل (IMSI + IMEI) فلا يُمكن الفصل بين نشاط هاتف الهدف ونشاط الهاتف المبرمج (يُنسب النشاطان لشخصية الهدف)، زرع هاتف خلوي كامل (IMSI + IMEI) في هاتف الهدف بحيث يظهر الهاتفان متلازمين في الحركة!

وبالنسبة للشبكة الثابتة، فقد أشارت بو غانم إلى:

- امكانية خرقها من خلال اعتراض شبكة الربط الميكروويو الراديوية.
- امكانية الدخول الى مكونات مركز التحكم (NOC) عبر الإنترنت ـ الوصلة الافتراضية (VPN) بمعرفة اسم المستخدم (User Name) وكلمة السر (Password).
- تغيير / خلق وصلات مبرمجة فرعية لأرقام هواتف مستخدمة بنفس مواصفات الرقم الأساسي تسمح باستعمال الرقم والتنصّت عليه.
- تغيير / خلق وصلات مباشرة (Physical Connection) من الموزع الرئيسي (MDF) تسمح باستعمال الرقم والتنصّت عليه.
- امكانية خرق عناصر وأنظمة إدارة مختلف عناصر الشبكة (NMS) بما فيها نظام الفوترة.
- امكانية الخرق باستغلال خاصّية التحكّم عن بعد المتوفرة لصيانة الأجهزة والشبكة للموردين وذلك بتغيير خصائص الشبكة.
- امكانية الخرق الناتج عن عدم وجود ضوابط ادارية تحدد أصول الولوج الى مكونات الشبكة وتغيير اعداد وتشكيل الشبكة من تعدد مستعملي اسم المستخدم وكلمة السر والمشاركة في استخدام نفس اسم المستخدم وكلمة السر.
- شبكات الإنترنت غير آمنة تتعرض لمشاكل مشابهة ولمعدومية السرية وأمن المعلومات الخاصة والإدارية والرسمية.

حماية اسرائيلية!

وبالاضافة إلى كل ما سبق، فقد حذر الفريق التقني من أن بعض أنظمة الحماية مُصمّمة أصلاً لتسهيل عمليات الاختراق عبر ما يسمى بالباب الخلفي (back door)، وهو عبارة عن باب برمجي يسمح لواضعه التسلل إلى البرنامج والأنظمة المعلوماتية بهدف التحكم بها وأخذ ما يلزمه من داتا بداخلها. وهذا الأمر يتعزز عند معرفة أن الشركات الموردة الأساسية، وكذلك برنامج الحماية الشهير ماكافي (McAfee) في معظمها شركات شريكة لشركة Check Point الإسرائيلية المتخصصة في تكنولوجيا المعلومات.



هوائيات اسرائيلية قبالة الناقورة

وسائل القرصنة ونتائجها

أوضح رئيس الهيئة الناظمة للاتصالات بالانابة الدكتور عماد حب الله خلال العرض الذي قدمه أن وسائل القرصنة والاختراقات الاسرائيلية تتم عبر:

- انتشار المراكز والأبراج والبوارج والطائرات الإسرائيلية
- تخطيط وتنفيذ إصطفاف المواقع ـ إختراق عن طريق الوصلات الميكروويو الراديوية
- تركيب المعيدات ومحطات الإرسال (الخلايا) الوهمية
- الحصول على كلمات السر
- الولوج عبر الشبكات الخاصة الافتراضية VPN
- زرع المعدّات وإدخال المعدات الملوّثة ضمن الشبكة
- الوصول إلى الوصلات الرئيسية لشبكة GPRS أوالوصلات الانتهائية
- استنساخها للشرائح الذكية (V1, V2, V3)
- الهواتف الخلوية الملوّثة
- فك شيفرة المفاتيح الخوارزمية واختراق الوصلة بين الهاتف والمحطة
- إمكانية الولوج عبر الأبواب الخلفية لشبكات الأمان

وهذه العمليات تتم اما عبر دخول مباشر أو عبر العملاء أو عبر اختراق الشركات الموردة أو عبر شبكات المشغّلين لا سيّما غير الشرعيّين.

أما أبرز نتائج هذه القرصنة والاختراقات فهي:

١) السيطرة على الشبكة (الخلوية أو الأرضية) والتحكم بمكوناتها الرئيسية.

٢) القدرة على تعطيل أجزاء من (أو كل) الشبكة أوعزل مشتركين عن الشبكة.

٣) تحديد مواقع الأشخاص وتعقب تحركاتهم ونمط تواجدهم واتصالاتهم.

٤) التنصّت على المكالمات الصوتية والاطلاع على محتوى الرسائل والتنصّت المحيطي.

٥) اختلاق اتصالات ورسائل.

٦) الإطلاع على بيانات خصائص الإتصال (المتّصل، المتّصل به، موقعيهما، أجهزتهما، زمان ومدة الاتصال).

٧) إجراء إضافة أو إلغاء أو تعديل في قاعدة بيانات خصائص الإتصال وغيرها.

٨) التلاعب بالعناصر الأساسية للهاتف الخلوي الشريحة (SIM) والجهاز (Phone).

٩) بث الرسائل الصوتية والمكتوبة.

فضل الله: إسرائيل زرعت خطوطاً في هواتف مقاومين واستخدمتها بالتزامن

كشف رئيس لجنة الاعلام والاتصالات النيابية حسن فضل الله ردا على سؤال حول الكلام على اختراق «حزب الله» بثلاثة من عناصره «عن احد الاسرار الذي تم من خلال تعاون وثيق مع اجهزة الدولة الرسمية، سواء من خلال وزارة الاتصالات او من مديرية المخابرات في الجيش اللبناني».

وأكد فضل الله أن «لقاءً حصل بين رئيس فرع المعلومات العقيد وسام الحسن ورئيس لجنة الارتباط والتنسيق في «حزب الله» الحاج وفيق صفا. حينها استوضح العقيد الحسن من المقاومة حول شخصية مواطن لبناني هو عميل للعدو الإسرائيلي اسمه أديب العلم. وسأله هل للحزب علاقة به؟ وهل هو عميل مزدوج؟ وتبين ان فرع المعلومات اكتشف عمالة العلم من خلال شبكة الاتصالات. فكان الجواب ان لا علاقة للمقاومة به وهو في دائرة العملاء وزوجته هي مشبوهة وهي عميلة».

ثم التقى القبض على هذين العميلين واجري معهما تحقيق. بعد ايام عدة، طلب الحسن من صفا لقاء، واعلمه ان ثمة مجموعة من الأرقام الهاتفية تبين ان العميل العلم اشتراها من السوق اللبنانية وزودها للعدو الاسرائيلي. وان ارقاما من هذه المجموعة يستخدمها ٣ من المقاومين.

وأوضح فضل الله أن «هذه هي الوصلة التي ادت الى القول ان هؤلاء المقاومين يتعاملون مع العدو»، مشيراً إلى أنه جرت العادة عند العدو الاسرائيلي ان يأخذ ارقاما من السوق اللبنانية ويستخدمها مع عملائه، فجاءت الشبهة من خلال هذا الباب.

وقال: الجميع يعلمون ان المقاومة حساسة جدا تجاه هذا العمل ولكل ما يتعلق بالمواجهة مع العدو وبأمن المقاومة. والعقيد الحسن خلص الى ان هؤلاء الثلاثة عملاء اخترقوا المقاومة لانهم استخدموا هذه الهواتف. تعاطينا مع هذا الموضوع بجدية عالية وبدأت المقاومة تحقيقا مفصلا ومعقدا الى حد انها لم تترك شيئا يتعلق بهؤلاء الثلاثة، لا في منازلهم ولا في محيطهم ولا في علاقاتهم الا دققت فيه وعاشت حال استنفار. ولا انكر انها كانت لفترة معينة في حيرة حيال هذا الامر، ومن ثم في مرحلة لاحقة رفع هذا الامر الى مديرية المخابرات في الجيش وتم التعاون مع وزارة الاتصالات للوصول الى نتيجة، لان الفكرة الاساسية لدى فرع المعلومات ان المقاومين الثلاثة يستخدمون هواتف شخصية ومعهم ايضا هواتف اخرى يستخدمونها من خلال تواصلهم مع العدو الاسرائيلي. بعد كل التدقيق والتفتيش وهذا الاستنفار الكبير تبين لنا ان كلا منهم يستخدم هاتفا واحدا. فمن اين اتى الهاتف الآخر؟ استمر التحقيق لفترة من الزمن وكان المحققون في حيرة، سواء فنيي المقاومة او فنيي مخابرات الجيش اللبناني الذين عملوا على هذا الامر.

وتابع فضل الله: بدأ العمل للتوصل الى نتيجة. هل المقاومة مخترقة فعلا بهؤلاء الثلاثة؟ ما الذي حصل؟ وما هو السر؟

وتبين بعد التحقيق ان هناك سرا كبيرا تمكن فنيو مخابرات الجيش وفنيو المقاومة من كشفه، وهو يتعلق بالاستخبارات الاسرائيلية وبما توصلت اليه التقنيات الإسرائيلية العالية جدا لجهة امكانية زرع خطوط هاتفية في خطوط اخرى.

فأثناء حركة الهاتف الخليوي للمقاومين الثلاثة، كان يتزامن معه باستمرار وبشكل يومي خط آخر، بينما كان كل من الثلاثة يستخدم هاتفا واحدا. اجريت اختبارات وتجارب على عملية التزامن هذه حتى تبين ان الاستخبارات الاسرائيلية تمكنت من زرع خط ثان داخل جهاز الهاتف، من خلال برمجيات متطورة وامطار الهاتف برسائل مكثفة، اكثر من ١٠٠٠ رسالة غير مرئية.

كيف تمت هذا العملية المعقدة؟ وكيف تم تفكيك اسرارها؟

عمد العدو الى زرع رقم في جهاز احد المقاومين الثلاثة هو من الارقام التي اشتراها العميل العلم وزود العدو بها، الذي قام ببرمجته وعاد الى زرعه داخل هاتف هذا المقاوم. اما الخطان الآخران للمقاومين الباقيين فأدارهما العدو عبر احد الخطوط التي اشتراها العميل العلم. وبالتالي اصبح لكل من المقاومين الثلاثة خطان، واحد حقيقي وآخر مخفي زرعه العدو من دون معرفة المقاوم.

وصار بإمكان العدو ان يتصل بالرقم المخفي من دون ان يعرف صاحب الخط، وان يستمع الى كل ما يجري في محيط المقاوم. ووصل فرع المعلومات في معطياته الى القول ان هذا الخط موجود في غرفة نوم المقاوم وينقل ما يجري فيها من كلام الى المشغلين الاسرائيليين. فهل يعقل مثلا ان يقبل أي عميل ان يسمّع مشغليه انه في غرفة النوم؟

في الخلاصة، كان هذا كشفا نوعيا لبنانيا يسجل لاستخبارات الجيش وللمقاومة.

وتحدث فضل الله ردا على سؤال، عن الادوار التي قام بها العملاء في شبكة الاتصالات، «وهي اعترافات رسمية بعضها موثق في الامم المتحدة لان لبنان تقدم بشكوى في هذا الصدد». وقال: العميل طارق ربعة قدم دراسة دقيقة عن كل تصاميم شركة «الفا» وشبكة اتصالاتها ومن ضمنها الاجهزة المستعملة والهوائيات والترددات. وابلغ العدو الاسرائيلي بالمخطط الذي ستعتمده شركة «الفا» بعد عدوان تموز ٢٠٠٦، بغية اعادة العمل في المحطات. وهذا المخطط نال اعجاب «الموساد»، بحسب الاعترافات، لانه يؤمن للعدو اتصالات جيدة وعدم تشويش. ووضع العميل ربعة دراسة فنية حول محطة الاتصالات في ضهر البيدر التي تصل البقاع بمحطة الحازمية، وحاول بطلب من «الموساد» وضع المحطة في الحازمية على احد الابنية دون غيرها، لتسهيل عملية التنصت والاختراق لكل اتصالات منطقة البقاع. واعترف العميل ربعة ان النشاط الذي قام به غاية في التطور والتعقيد وقلة من الخبراء لديهم القدرة على فهم هذه الامور. وكان العدو، وفق اعترافات العميل ربعة الموثقة رسميا، مهتما بمعرفة تفاصيل التحكم عن بعد وبتقديم تفاصيل هذا النظام، وكذلك نظام الفوترة، الى مشغليه الإسرائيليين.

اما العميل شربل قزي فهو المسؤول عن الربط الهوائي بين الخلايا والمقسمات. وقدم الى العدو مواقع الهوائيات ومواصفاتها وهي العناصر الاساسية لتسهيل عمليات الاختراق المتعلقة بالوصلات الرديوية. وقدم العميل قزي كلمات السر الى العدو، وهو المسؤول عن حسابات تقنية تزود المستخدمين باسم الحساب وكلمات السر.

في العام ١٩٩٧، عرض العدو الإسرائيلي على العميل قزي ٥٠ الف دولار مقابل زرع معدات للتنصت للولوج الى الشبكة في عدد من المحطات. وعارض الاسرائيلي من خلال عملائه الذين احتلوا مواقع نافذة، استفادة شركة «الفا» من تجهيزات شركة هواوي وطلب من العميل الربعة بحدة وبإصرار ان يعمل لان تبقى الاجهزة من نوع «الكاتيل» على حالها، لان العدو قادر على التحكم بها.

الفضائيات اللبنانية تتعرض للتشويش في الجنوب

بنت جبيل ـ «السفير»

تعرضت المحطات الفضائية اللبنانية التي كانت تنقل بعد ظهر أمس، وقائع المؤتمر الصحافي المتعلق بالخروقات الإسرائيلية لقطاع الاتصالات في لبنان، لتشويش إسرائيلي حاد ما أدى الى تقطع استقبال إشارات تلك المحطات وصعوبة متابعة المؤتمر في الكثير من القرى الجنوبية لا سيما الحدودية.