



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 3, Issue 8

December 2004

MERRY CHRISTMAS



In this final issue of the year, we conclude the article on Radio Frequency Identification (RFID) technology, which pushes the newsletter to omnibus proportions. This could be useful when you are lying on the beach in the Coromandel or the Gold Coast and you need some extra sun protection.

The virus statistics for the year (see page 8) show an encouraging trend downwards. Does this mean that software is becoming more

robust and the world is taking information security more seriously? We would like to think so.

The web defacement statistics, courtesy of [Zone-H](#), are less obvious in their interpretation. Linux accounts for over 60% of NZ-related websites published, with Windows variants accounting for about 25% of targeted systems. These figures mirror the [world wide trend](#) reported by Zone-H.

Our lead article summarises Service Pack 1 for Microsoft Windows Server 2003, and in case you missed it, [Microsoft](#) have published a very recent update to the Windows Firewall in XP SP2. Details of which are on their website.

Finally, newsletters are now available on our [website](#).

All the staff at CCIP wish you a very merry Christmas and a happy and prosperous New Year.

WINDOWS SERVER 2003 SERVICE PACK 1

Following closely behind the release of Windows XP Service Pack 2, Microsoft is now preparing to release Service Pack 1 (SP1) for Windows Server 2003.

Many of the features between the two SPs will be similar (for example, IE updates, a more configurable firewall, wireless networking and a much stronger focus on security), however, SP1 for Windows Server 2003 also includes new functions in patch management and network security. New features also include a Security Configuration Wizard. This will allow administrators to quickly identify and disable unused services, which will ultimately reduce vulnerabilities.

Post-setup Security Updates allow the blocking of incoming traffic to newly installed servers until the latest updates are installed. Additional features include Data execution prevention (DEP), which comprises both DEP software and hardware to help mitigate malicious code execution in the

server, advanced monitoring and auditing of IIS, and improvements to firewall group policy management. Two key additions to this pack are the inclusion of IPv6 and Quarantine Control.

Microsoft Quarantine Control
Microsoft's new approach for improving security to a private network is the Network Access Quarantine Control.

This feature allows administrators to provide a script that will examine a computer in a quarantined environment before allowing it access to a private network. The key points will be checking that the latest security patches are installed, anti-virus software is up-to-date, routing is disabled, and the firewall is installed and active. A computer which fails these checks will then have the opportunity to update via Quarantine Resources.

The method of quarantine is the enforced use of packet filters, which are lifted once compliance with network policies is achieved. There are some limitations as this

feature uses Routing and Remote Access, wireless access and programs that require post-connection scripts that will attempt to connect in the quarantine zone. However there is the option of performing compliance scripts as part of the logon sequence or startup script.

Although Microsoft have allowed for the use multiple site Quarantine Resource Servers for the WAN environment, there are areas where this technology may encounter difficulties, such as remote sites where bandwidth for update deployment is limited. It is also worth noting that this function is not a security solution. It is purely to protect a private network from a poorly-configured computer.

SP1 is set to be released in the first half of 2005. A [Release Candidate](#) is available now.

CONTENTS

<i>Merry Christmas</i>	1
<i>Windows Server 2003 Service Pack One</i>	1
<i>Radio Frequency Identification (part two)</i>	2
<i>RFID References</i>	7
<i>Virus Activity for 2004</i>	8
<i>.nz Website Defacements for 2004</i>	8



Communication regarding this newsletter should be addressed to: newsletter@ccip.govt.nz



Government
Communications
Security Bureau

CONTACT DETAILS

Ph: +64 4 498 7654

Fax: +64 4 498 7655

E-mail: info@ccip.govt.nz

Web: www.ccip.govt.nz

Mail: P.O. Box 12-209
Wellington
New Zealand

Star City Casino in Sydney has placed RFID tags in 80,000 employee uniforms in an attempt to curb the theft of the uniforms.

RFID Part Two

Michelin is planning to build RFID tags into its tyres. The tag will store a unique number for each tyre, associated with the vehicle's identification number (VIN). The tag can also measure tyre wear.

RFID Part Two

RADIO FREQUENCY IDENTIFICATION (part two)

Part two of a two-part article on Radio Frequency Identification (RFID).

Part One provided a background to RFID. Part Two discusses RFID Usage Categories, typical applications and some security and privacy issues.

RFID Usage Categories

RFID devices can be classified into four categories:

- 1 EAS (Electronic Article Surveillance);
- 2 Portable Data Capture;
- 3 Networked systems; and
- 4 Positioning systems.

EAS

These are typically one-bit systems used to sense the presence or absence of an object. The most common use is in retail stores as an anti-theft device. Tags are attached to clothing or other items and trigger an alarm if the goods leave the store before being deactivated.

Portable Data Capture

Used in conjunction with portable readers where the data required from the tagged object may vary. Some devices are being combined with sensors to record, for example, temperature, movement (seismic) and radiation.

Networked Systems

Characterised by fixed position readers and used to track the movement of tagged objects. Usually directly connected to an enterprise system.

Positioning Systems

Where objects (vehicles) are tagged and the system provides automatic location and navigational support.

Applications

Used mainly in transportation, logistics, manufacturing, processing and security, typical applications include:

- Animal tagging;
- Animal husbandry;

- Toxic and medical waste management;
- Postal tracking;
- Airline baggage management;
- Paper money anti-counterfeiting;
- Anti-counterfeiting in the drug industry;
- Vehicle immobilisers and alarms;
- Road toll collection;
- EAS;
- Access control;
- Time and attendance;
- Manufacturing processes with robotics;
- Monitoring of offenders;
- Passports.

Advantages

The principal advantages of RFID system are the non-contact, non line-of-sight characteristics of the technology. Tags can be read through a variety of visually and environmentally challenging conditions such as snow, ice, fog, paint, grime, inside containers and vehicles and while in storage.

With a response time of less than 100 milliseconds, an RFID reader can read many (several hundred) tags virtually instantaneously. Tags coupled with sensors can provide important information on the state of the goods. For example, refrigerated goods can be monitored for temperature and problem areas identified and alarms raised.

Some Developments & Uses

The US Department of Defense and Wal-Mart require their major suppliers to implement RFID technology in their supply chains by 1 January 2005ⁱ. All cartons and pallets must be equipped with RFID tags. It is expected that this will provide a major impetus for the widespread adoption of the technology in the US.

UK's Tesco supermarket chain has begun work to roll out an RFID network that tracks shipments

from its central distribution centre to all 98 Tesco Extra Superstores by Christmas this yearⁱⁱ. This is the first stage of a plan to implement RFID across more than 2000 stores and distribution centres in the UK.

In January 2003, Gillette announced an order for 500 million RFID tags to be incorporated into razor and razor blade packagingⁱⁱⁱ.

In March 2003 Benetton announced similar plans to weave RFID tags into its designer clothes, although this was reversed in the face of an organised consumer boycott.

MasterCard and American Express have been testing RFID cards.

Mobil has been promoting its "Speedpass" since 1997.

Most high-end cars are now equipped with an RFID tag in the car keys.

Delta Airlines is testing RFID on some services, tagging 40,000 bags^{iv}.

The seaport operators, Hutchison-Whampoa Ltd, PSA Corporation Ltd and P&O Ports, who account for 70% of the world's port operations, have agreed to deploy RFID tags to track the 17,000 containers that arrive at US ports daily.

Star City Casino in Sydney has placed RFID tags in 80,000 employee uniforms in an attempt to curb the theft of the uniforms.

Michelin is planning to build RFID tags into its tyres. The tag will store a unique number for each tyre, associated with the vehicle's identification number (VIN). The tag can also measure tyre wear.

RFID Continued

The European Central Bank is planning to embed RFID tags into high-denomination bank notes as an anti-counterfeiting measure, by 2005. The bank notes already incorporate such measures as holograms, foil strips, special threads, microprinting, special inks and watermarks. At present, the US dollar is the world's most counterfeited currency. With the growth of the European Union and the growing use of the Euro. The Euro will become the most common currency in the world⁴.

These are examples of current usage of RFID tags. There are other applications under consideration. For example, the incorporation of RFID tags into important documents such as birth certificates, driver licences, educational certificates, manuscripts, medical registrations and so on. In fact any document where authenticity and veracity is key.

Security & Privacy Implications of RFID Technologies.

Radio Frequency Identification systems are emerging as a practical means of Auto-Identification in a wide variety of applications from access control to animal tracking. RFID systems are likely to supersede bar codes in some applications and complement bar codes in others. RFID is expected to help in reducing costs of supply chain management and inventory management in addition to the many other applications outlined in the first part of this article.

While RFID usage is limited at

present, Evans Data Corporation, an IT market research organisation, is predicting that RFID usage will increase by 450% in 2005 and a further 96% in 2006^{vi}.

The widespread adoption of RFID is a foregone conclusion, according to some industry commentators^{vii}. A major driving force being the adoption of the technology by such influential organisations as the US Department of Defense, Wal-Mart and Tesco.

Standards

The lack of standardisation and the lack of harmonisation of frequency allocation is hampering growth in this industry.

There is a proliferation of incompatible standards with major RFID vendors offering proprietary systems. ANSI and ISO have been working to develop RFID standards and some have been adopted for such applications as animal tracking (ISO 11784 and 11785) and supply chain goods tracking (ISO 18000-3 and ISO 18000-6).

The Electronic Product Code (EPC) system defines technical protocols and creates a data structure for the stored information. The EPC system was researched and developed at the Auto-ID Center at the Massachusetts Institute of Technology (MIT) and in November 2003 responsibility for the commercialisation and management of the EPC system was transferred to EPCglobal Inc.

This organisation is an affiliate of the Uniform Code Council (UCC) and EAN International (EAN). EAN and UCC created and maintain the EAN.UCC System, which covers global e-business communications standards, numbering schemes, uniqueness management, and bar code symbology standards, including the U.P.C. and EAN bar code symbols used on consumer goods around the world^{viii}. While there are some differences with the ISO standards, these organisations are now working together to rationalise standards.

EPC specifications have defined five tag classes, based on functionality, as shown in Figure 1 below^{ix}.

The current version of the Electronic Product Code (EPC) Tag Data Standard specifies the format for encoding and reading data from 64 and 96 bit RFID tags^x. See [Figures 2](#) and [3](#)^{xi}.

Privacy & Security

Simple RFID readers can cost as little as US\$20^{xii} and circuits and articles have been published in electronics and enthusiasts magazines^{xiii} to allow you to build your own readers. There are security and privacy concerns with this technology which fall broadly into the following areas:

- Location Privacy
- Customer information;
- Corporate espionage;
- Insecure operating environments;
- Denial of service;

Continued on page 4

The European Central Bank is planning to embed RFID tags into high-denomination bank notes as an anti-counterfeiting measure, by 2005.

RFID Part Two

The lack of standardisation and the lack of harmonisation of frequency allocation is hampering growth in this industry.

RFID Part Two

Figure 1

Class	Nickname	Memory	Power Source	Features
0	Anti-Shoplift Tags	None	Passive	Article Surveillance
1	EPC	Read-Only	Any	Identification Only
2	EPC	Read-Write	Any	Data Logging
3	Sensor Tags	Read-Write	Semi-Passive or Active	Environmental Sensors
4	Smart Dust	Read-Write	Active	Ad Hoc Networking

RFID must undergo a formal technology assessment, and RFID tags should not be affixed to individual consumer products until such assessment takes place.

RFID Part Two

Certain uses of RFID should be prohibited, for example tracking individuals with RFID tags in consumer purchases.

RFID Part Two

RFID Continued

- Spoofing;
- Technical attacks;
- Compromise of supporting systems.

Data can be extracted from tags and used to track individuals, thus violating location privacy. This is not unique to RFID systems as many Bluetooth and other wireless enabled devices may be subject to the same privacy issue.

Customer Information

Where a customer has made multiple purchases, buying patterns or the identification of high value items can result.

Corporate Espionage

If unprotected RFID tags are used, a retailer's stock may be monitored or tracked by competitors, marketing organisations, news media, private investigators or information brokers. This can yield sales, marketing, product mix and other valuable information.

Insecure Environments

RFID tags often operate in hostile environments and can be subject to intense electronic or physical attacks. Examples include container tracking, supply chains and manufacturing processes.

Denial of Service

Denial of service may be caused by "flooding" an area with RF energy, thus incapacitating the readers.

Spoofing

Spoofing occurs where tags are replicated from data transmitted by the tag. This is a particular risk with access control systems. It is

technically feasible that attackers may alter the contents of a tag to facilitate theft, disguise the identify of the tagged item or to remove items from the premises.

Technical Attacks

Because they are wireless; passive RFID tags may be susceptible to fault induction, timing attacks or power analysis attacks^{xiv}. Again all wireless devices may be susceptible to these types of attack. Lukas Grunwald, a consultant with a German technology organisation, has created a software tool, RFDump, that reads and can re-programme some RFID tags. This tool is available over the Internet.

Compromise of Supporting Systems

Microsoft is writing code to accommodate RFID for its Axapta, Great Plains and Navision systems and is expected to have the software RFID-ready by the middle of next year. SAP is embracing RFID^{xv} and Oracle announced recently that its 10g database and application server are able to interface with RFID data streams^{xvi}.

The passive (classes 0 and 1) tags we can expect to find in general retail use can store very little information and generally have no writable memory. They do, however, contain unique identifiers which, when linked to a supporting application or system (database), can store additional information on the tagged item and a read history and lifecycle of that item. They also store tag "kill" codes to deactivate tags. Clearly, the

valuable data is in the database, not in the tag.

The rules on protecting the confidentiality of this information do not change when the collection mechanism changes (RFID tags and readers). The question of liability can also arise. This applies whether the information is commercially sensitive or deals with and individual's privacy.

Supporting systems constitute the greatest risk, but one which is relatively well understood.

Legislation

Several privacy advocate groups have proposed frameworks to manage consumer privacy. These frameworks emphasise individuals' rights to location privacy and have three basic elements:

- RFID must undergo a formal technology assessment, and RFID tags should not be affixed to individual consumer products until such assessment takes place. This may be accompanied by a "seal of approval" to provide a visual guide that the tags in use conform with approved guidelines; as shown in [Figure 4](#).
- RFID implementation must be guided by existing privacy legislation and good privacy practice. This may include clear notice, consumer education and consumer choice; and
- Certain uses of RFID should

Continued on page 5

Figure 2

EPC Type	Header Size	First Bits	Domain Manager	Object Class	Serial Number	Total
64 bit type I	2	01	21	17	24	64
64 bit type II	2	10	15	13	34	64
64 bit type III	2	11	26	13	23	64
96 bit and more	8	00	28	24	36	96

RFID Continued

be prohibited, for example tracking individuals with RFID tags in consumer purchases.

However, another aspect is an organisation's ability to track products in the supply chain in the most cost-effective and efficient manner without excessive compliance costs. This could be viewed as a fundamental part of doing business.

While there is considerable debate on RFID and privacy concerns, no specific legislation to deal with RFID has yet been passed. In the US, bills have been proposed in California and Massachusetts and legislators from the Virginia General Assembly intend to study RFID as an "invasive technology, along with facial recognition, hidden cameras, spyware and Internet wiretaps^{xviii}. The need to legislate or regulate to manage public policy aspects is gaining momentum.

Costs

A major constraint on the widespread use of RFID technologies is the cost of the tags. The most widely used tags are Electronic Article Surveillance (EAS, class 0) tags which cost between 1 and 6 US cents. Over 6 billion of them are used annually^{xix}. These EAS tags are a

one-bit tag and contain no information, merely indicating presence or absence.

Passive tags (class 1) with some data storage, cost between five and ten US cents each in large quantities (several million). High value items, cartons and pallets are being tagged (class 2-4) and here costs may be up to US\$100 per tag. At current prices it is not economic to incorporate tags into every retail item. Prices will fall as manufacturing technologies improve and there is a prediction that 10 billion tags will be used annually by 2007^{xx} with 1 trillion being delivered in 2015. In the last 50 years only one billion RFID passive tags (other than EAS tags) and 500 million active tags have been sold. While the use of RFID technologies is predicted to grow significantly, it may take several years to get to the point where the majority of retail items are tagged.

Countermeasures

RFID tag standards incorporate a 64-bit region that cannot be modified and remains unique to the tag itself. This can be used to authenticate the tag and defends against tag spoofing^{xxi}. Where class 2,3 or 4 RFID tags are used in access cards, a new bitstream (possibly cryptographically signed) can be uploaded each

time the card is used. This reduces the opportunity for a spoofed card to be used and significantly increases the risk of discovery as legitimate cards not accepted by the system will soon be reported.

Replay attacks can be protected against through the use of a "hidden" authentication bitstream or serial number on the tag and use a challenge/response mechanism using the hidden number to establish the tag's credentials. The hidden number is never transmitted.

To successfully replace barcodes, RFID devices must be very low cost. To keep the cost down, these are generally passive devices with limited functionality. At present, affordable tags cannot perform standard cryptographic operations necessary for privacy and security having only 500-5000 gates. By contrast, the Advanced Encryption Standard (AES) requires some 20,000 - 30,000 gates to manage cryptographic security^{xxii}. Security for passive RFID tags therefore represents a considerable challenge^{xxiii}.

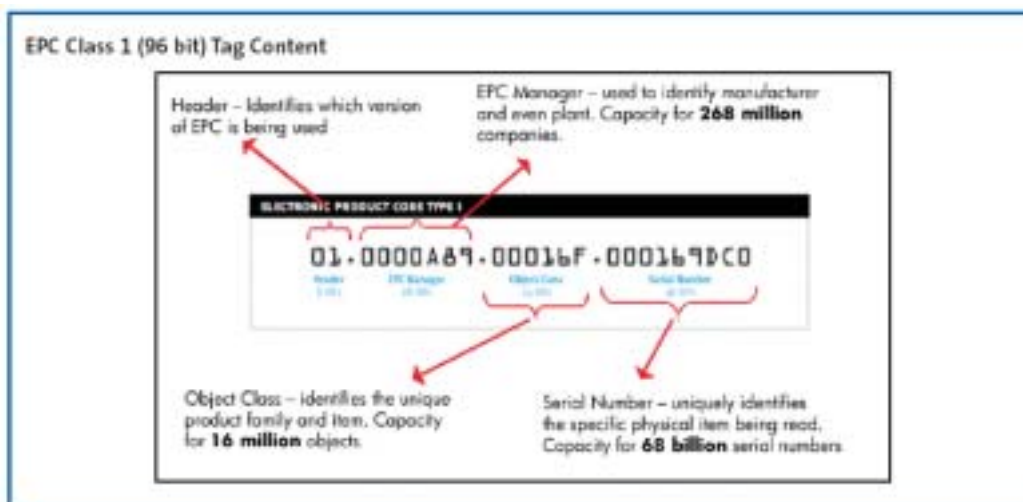
Two techniques have been proposed to address eavesdropping of RFID devices.

While there is considerable debate on RFID and privacy concerns, no specific legislation to deal with RFID has yet been passed.

RFID Part Two

Continued on page 6

Figure 3ⁱⁱⁱ



To successfully replace barcodes, RFID devices must be very low cost. To keep the cost down, these are generally passive devices with limited functionality.

RFID Part Two

RSA have also designed a “blocker tag” technology that prevents RFID devices being read.

RFID Part Two

There is some use of RFID in New Zealand, mainly EAS, access cards and similar access control applications and some dairy applications for animal tracking and husbandry.

RFID Part Two

RFID Continued

One, proposed by MIT, is known as “silent tree walking”. If two or more tags respond to a reader at the same time, a collision occurs. When this happens, the read performs a binary tree walk—though the address space, one bit at a time, until a unique response can be determined.

The other technique, proposed by RSA Laboratories, involves the use of pseudonyms with tags having multiple identifiers which are rotated. Legitimate systems will recognise all identifiers associated with a particular tag. So while eavesdroppers will be able to read the tags, they will need to know all identifiers associated with a tag to make sense of the data or successfully track a tag.

RSA have also designed a “blocker tag” technology that prevents RFID devices being read. This system is software based and prevents readers from gathering data from other tags in their immediate vicinity^{xxiv}. RFID readers are unable to read multiple tags simultaneously. Anti-collision protocols allow multiple tags to be read within a very short timeframe. However, “blocker tags” confuse the reader by always responding and thereby prevent any tags being read^{xxv}. Blocker tags could, for example, be incorporated into shopping bags at provided at the checkout. Without this technology, readers could read any tag within range.

The Auto-ID Center specification includes a kill command to permanently deactivate a tag. Earlier kill codes were 8 (Class 1) and 24 (Class 0) bit codes, which are relatively trivial to a brute force or DOS attack. The new specification for Class 1 tags

incorporates a 32-bit kill code. Separate and random “kill code” for each RFID tag, would then have to be retrieved from a secure database, and activated at the checkout. A variation is to disable the tag’s unique identifier. Keeping other identifiers in the chip, such as what the item is, could be useful, for example, for sight impaired people who can use a reader to identify medicines and dosages.

One further technique proposed is using antenna energy analysis to enhance security^{xxvi}. There are two variations in this technique. In the first, signal analysis estimates the reader distance, distance implying degrees of trust with greater distance equating to less trust. In the second, antenna energy is used to power a tiered authentication scheme in which tags provide more information to more trusted readers.

In New Zealand

There is some use of RFID in New Zealand, mainly EAS, access cards and similar access control applications and some dairy applications for animal tracking and husbandry. Indications are, however, that increasing use can be expected over the next few years.

While EAS tags have been used in New Zealand by retailers for many years, one of the early adopters of new developments in RFID technologies is the Manukau City Council’s library in Botany Downs. The library is the first in New Zealand to use RFID tags to track and manage its book collection. Wellington Libraries are expected to follow suit in two to three years^{xxvii}. Libraries in the US and UK are deploying the technology with about 250 libraries in the US already using

the technology. Singapore implemented the technology in 1998 under the leadership of the National Library Board^{xxviii}.

Supermarket group Progressive Enterprises which includes Woolworths, Foodtown and Countdown, is trialling RFID to track meat from processing plants to its butcheries^{xxx}. RFID tags will be incorporated into specialised meat containers to assist in supply chain management.

Hastings based Richmond Meats has been evaluating RFID for animal tracking. This will allow shipments to be traced through processing plants back to the livestock^{xxxi}.

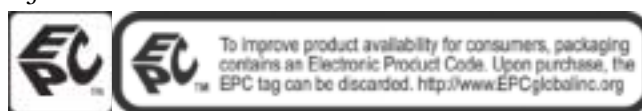
Preliminary discussions between a Canadian RFID vendor, AdvancedID and New Zealand sheep industry officials are underway to establish field demonstrations of RFID technology^{xxxii}.

A practical view

At present, RFID systems do not have high reliability, particularly in a retail environment. UHF tags are virtually unreadable near the human body because of its high water content^{xxxiii}. Many retailers have difficulty in getting an accurate, consistent reading when the tag is any distance (more than a few centimetres) from the reader. With low-cost, RFID technologies in passive tags, readers have to be in close proximity to the tag.

Many Customer Relations Management (CRM) systems today, store more data than organisations can use which raises the question why they would want to go to the expense and trouble of collecting more data? The technology does not yet exist for a retailer to drive

Figure 4^{xviii}



RFID Continued

through a suburb collecting information from the roadside and again there is, perhaps, little desire for retailers so to do.

RFID Technologies have been in use for many years (for example access control, toll collection and animal tracking systems) without any significant privacy or security violations. A greater privacy concern is, for example, the cell-phone, particularly the latest feature-rich devices with cameras and location tracking. Loosely

speaking, your cell-phone is a sophisticated, active RFID tag^{xxxiv}! These concerns are unlikely to constrain the use of cell-phones.

Using RFID tags in pallets and cartons to facilitate consignment, distribution and inventory management does not raise major privacy issues^{xxxv}. However, where tags are related to individual products, there are legitimate privacy and security concerns. These will have to be addressed if RFID is going to find

the same widespread acceptance as bar codes.

As with many new technologies there is potential for great benefit and misuse. But before we see widespread adoption of RFID, tag prices will have to fall significantly, clear benefits will have to be demonstrated and consumers will have to embrace the technology.

Loosely speaking, your cell-phone is a sophisticated, active RFID tag^{xxxiv}!

RFID Part Two

RFID References

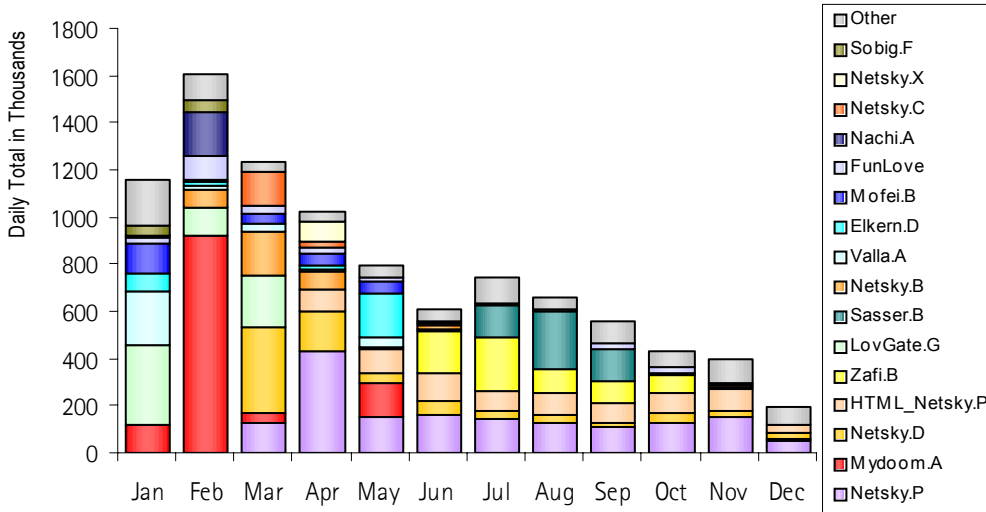
- i [RFID Gazette](#) June 28 2004 <http://www.rfidgazette.org/>
- ii [RFID Journal](#) Sept 28 2004 <http://www.rfidjournal.com/>
- iii [The Nation](#), 3 February 2004 <http://www.thenation.com/>
- iv [The Register](#), 27 June 2003 <http://www.theregister.co.uk/>
- v Supply Chain Security, [Are you Ready?](#), Hau L. Lee, Stanford Global Supply Chain Management Forum, September 3, 2004 <http://www.stanford.edu/group/>
- vi [Euro Bank Notes to Embed RFID Chips by 2005](#), EETimes, December 19 2001 <http://www.eetimes.com/>
- vii San Francisco Business Times, March 24 2004, Surging Market for RFID security predicted.
- viii [RFID: Robot for Infinite Decluttering](#), Kevin Maney, USA Today, 5 October 2004. <http://usatoday.com/>
- ix RFID: The Next Generation of AIDC, Application White Paper, Zebra Technologies
- x Security and Privacy in Radio-Frequency Identification Devices by Stephen August Weis; Massachusetts Institute Of Technology, May 2003
- xi Auto-ID Center, Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag, 23 February 2003
- xii RFID in the Supply Chain, A Balanced View A Business Briefing Paper, Amcor Australasia and Hewlett Packard, 2004
- xiii [RFID Devices & Privacy](#), Junkbusters <http://www.junkbusters.com/>
- xiv [An RFID Security Module](#) <http://www.siliconchip.com.au/>
- xv Radio Frequency Identification: Security Risks and Challenges, Sarma, Weis and Engels, RSA Laboratories Cryptobytes Volume 6 No.1 Spring 2003
- xvi [Radio tags set to short circuit supply chains](#), Peter Griffin, The New Zealand Herald, 07.09.2004 <http://www.nzherald.co.nz/>
- xvii [RFID: Is that a radio in your toothpaste?](#), Francis Till, The National Business Review, 20 January 2004 <http://www.nbr.co.nz/>
- xviii [EPCglobal Consumer Information](#) <http://www.epcglobalinc.org/>
- xix [States Move on RFID Privacy Issue](#), Claire Swedberg, RFID Journal, 30 April 2004 <http://www.rfidjournal.com/>
- xx RFID Explained, IDTechEx White Paper, IDTechEx Limited, 2004
- xxi Ibid
- xxii [RFID Security](#), Dan Kaminsky, Doxpara Research, November 2002 <http://www.doxpara.com/>
- xxiii RSA Laboratories, [Technical Characteristics of RFID](#) <http://www.rsasecurity.com/>
- xxiv RSA Laboratories, [A Primer on RFID](#) <http://www.rsasecurity.com/>
- xxv [RSA Keeps RFID Private](#), Dennis Fisher, eWeek, 23 February 2004 <http://www.eweek.com/>
- xxvi [RSA Security Designs RFID Blocker](#), RFID Journal, 28 August 2003, <http://www.rfidjournal.com/>
- xxvii Enhancing RFID Privacy via Antenna Energy Analysis, Kenneth P. Fishkin and Sumi Roy, MIT RFID Privacy Workshop, Boston, November 2003
- xxviii RFID Library Opens Tomorrow, The Dominion Post, 4 October 2004.
- xxix [Are Book Tags a Threat?](#), Andrew Heining and Christa Case, The Christian Science Monitor, October 5 2004 <http://www.csmonitor.com/>
- xxx [Singapore Seeks Leading RFID Role](#), RFID Journal, 12 July 2004, <http://www.rfidjournal.com/>
- xxxi Progressive Tags Meat, Tom Pullar-Strecker, The Dominion Post, 4 October 2004
- xxxii [RFID - Tracking Every Step You Take](#), iStart, April 2004 <http://www.istart.co.nz/index/>
- xxxiii [Globalisation of RFID boots AdvancedID sales](#), Food Production Daily, 5 October 2004 <http://www.foodproductiondaily.com/>
- xxxiv RSA Laboratories; [FAQ on RFID and RFID Privacy](#) <http://www.rsasecurity.com/>
- xxxv RSA Laboratories; [Technical Characteristics of RFID](#) <http://www.rsasecurity.com/>
- xxxvi [Privacy Groups Tag RFID](#), Roy mark, July 14 2004, Internet News <http://www.internetnews.com/>

Certain uses of RFID should be prohibited, for example tracking individuals with RFID tags in consumer purchases.

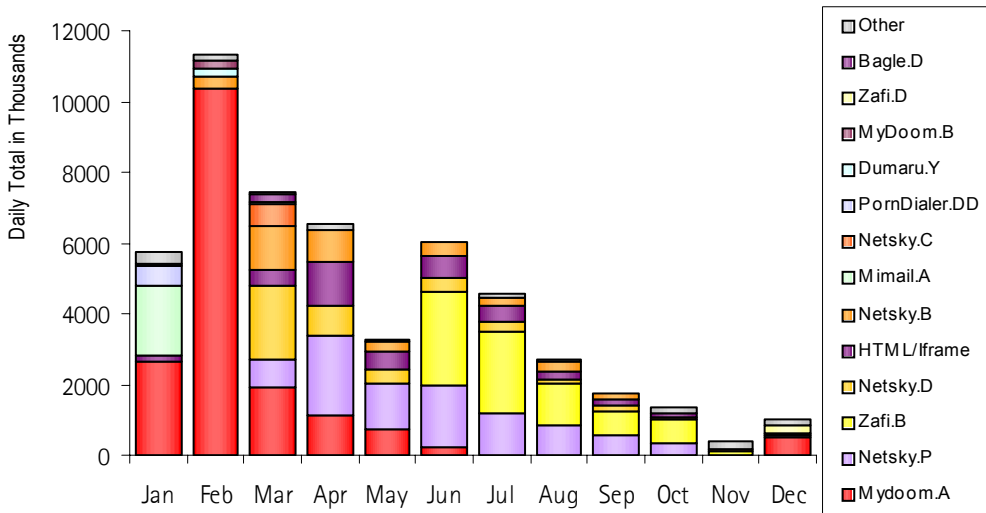
RFID Part Two

VIRUS ACTIVITY FOR 2004

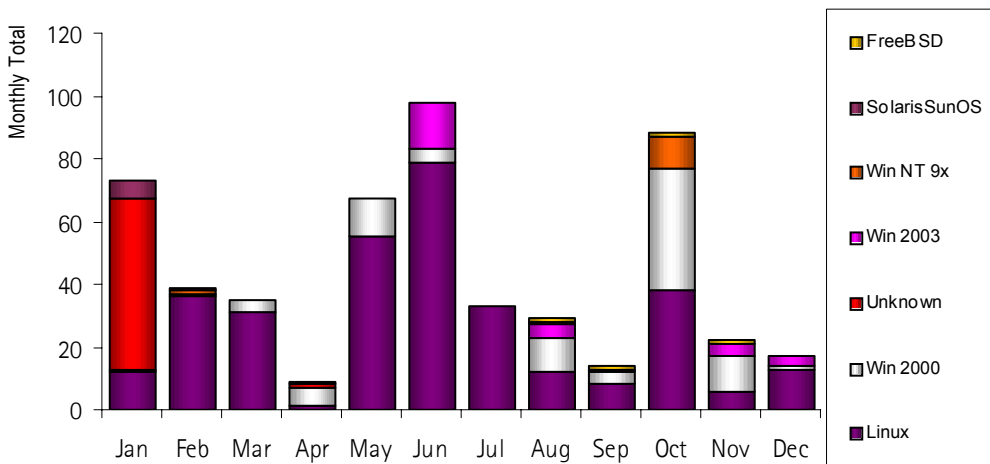
Daily Top Five: viruses captured worldwide by [TrendMicro](#) for 2004.



Daily Top Five: viruses captured worldwide by [RAV](#) for 2004.



.NZ WEBSITE DEFACEMENTS FOR 2004



Note: Each defacement by OS does not necessarily constitute a different machine per break-in – as multiple websites may be hosted on the same server. Data sourced from Zone-H.

DISCLAIMER

While this newsletter is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this newsletter.

CCIP only issues those external alerts that we assess as serious and would affect a large number of New Zealand users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.

Reference in this newsletter in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions stressed herein may not be used for advertising or product endorsement purposes.

Please refer to the CCIP website for a list of recent alerts and advisories.



CONTACT DETAILS

Ph: +64 4 498 7654

Fax: +64 4 498 7655

E-mail: info@ccip.govt.nz

Web: www.ccip.govt.nz

Mail: P.O. Box 12-209
Wellington
New Zealand