

National University of Ireland Galway

Social networking sites proved rich pickings for spammers and a headache for IT

IronPort case study

October 2006

The Challenge:

- Tackle email SPAM growth (1.2 million messages per day)
- Improve overall email performance
- Stamp out problem of URL based threats
- Reduce false positives for each spam outbreak; estimated 30,000 emails per outbreak.
- Reduce time and administration spent managing email

The Solution:

- Implement IronPort C300 email security and management appliances to protect 17,000 mailboxes

The Benefits:

- Continuity of email service to the university
- Ability to refocus IT resource away from day-to-day management of email
- Reduced hardware and support costs by replacing legacy email system;
- Protection against viruses, SPAM and unauthorised activity;

Introduction

Established in 1845 as Queen's College Galway, today the National University of Ireland Galway is one of Ireland's foremost centres of academic excellence.

With over 15,000 students, it has a long established reputation of teaching and research excellence in each of its seven faculties - Arts, Science, Commerce, Engineering, Celtic Studies, Medicine & Health Sciences, and Law.

Technological development and academic institutions have for sometime been happy bedfellows, the very DNA of some technologies we all use today are direct descendents from applications developed for academic use. From the early days of the web to even earlier programming languages used to solve complex problems in scientific research, these organisations have always been at the forefront of technology development and NUI Galway is no exception.

Like many modern universities, National University of Ireland Galway (NUI) had become heavily reliant upon its email service. It was used as a means of providing communication access within the university and a vital link to other research establishments and academic groups on the outside. Email was not only an important communications tool it was also the system costing the university the most to maintain both physically and in terms of resources.

Like any modern enterprise, the NUI Galway has a 30 strong team in its computer services team, a team responsible for all Information Communication Technology (ICT) across the campus and beyond. Their role is twofold: deliver the right services and technology to the right people, at the right cost and overseen in the right way. The bulk of the team's work is operational development and delivery of defined ICT services. However, they also have a wider concern with the strategic position of ICT within the University, working to ensure that the ICT environment supports change in NUI Galway and tracks changes in the external environment, both academic and technological. The ICT infrastructure must serve around 15,000 students, approximately 1,200 staff a total of 11,000 network nodes and 17,000 mail boxes which generates 120,000

outbound emails per day. Where NUI Galway's situation does differ from traditional enterprises is in the usage patterns of its internal customers, 'the students'. While the majority of technology use is educational and research based, the proliferation and popularity amongst students of community networking sites such as YouTube.com, craigslist.com and Bebo.com increase the risk of greater levels of SPAM targeted at this class of users.

The problem

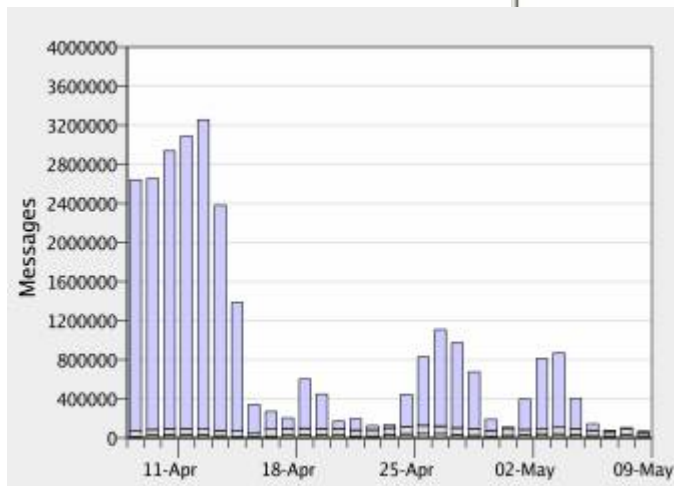
The university was coming under increasingly high levels of spam, with each attack resulting in around 30,000 messages hitting the universities network. The result was 'Denial of Service' attacks which had a detrimental effect on delivery times of legitimate email communication while the situation was resolved by the computer service team.

For the university, both students and faculty, email was a critical tool. Applications, research papers and other time sensitive material were all submitted via email. Soon the unreliability of the system began to have a major impact on the users and the stability of the email infrastructure.

A potential risk factor with regards SPAM would be the use of University PCs and student email addresses to register on social networking sites. This means the address can very quickly be passed into the hands or spoofed by spammers for illegitimate gain.

Having been appointed as director of computer services at NUI Galway, Kieran Loftus knew that immediate action needed to be taken. Speaking about the implementation, he said: "The implications, had we not taken the evasive action we did, would have been immeasurable, our email infrastructure would have become redundant very quickly. Email is a service architecture. People just expect it to work and when they hit send, they assume the email has been sent immediately. This is simply not the case when your infrastructure has to deal with denial of service attacks on a daily basis. The time and cost to manage this situation was quickly becoming prohibitive."

Message volumes

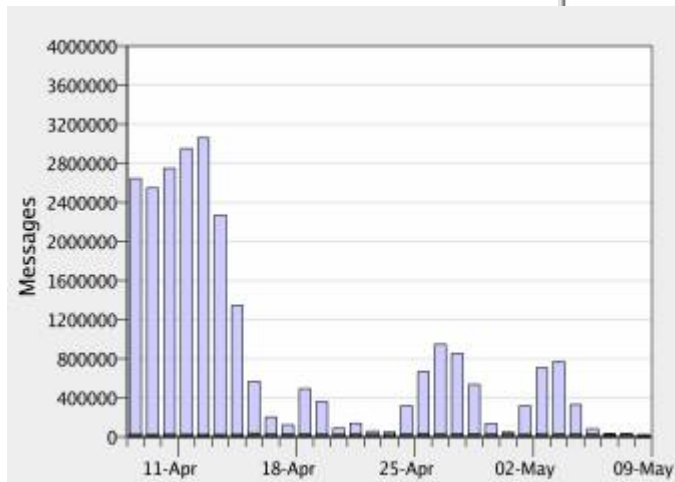


IronPort C30 (mx1.vlan.nuigalway.ie) - Monitor > Overview - Microsoft Internet Explorer

Address: https://mx1.vlan.nuigalway.ie/monitor/overview

Sender	Messages						
	Domain	Attempted	Stopped By Reputation Filtering	Invalid Recipients	Spam Detected	Virus Detected	Accepted (Clean)
Total (All Senders)		28014920	25238357	9565	1877210	34621	855167
<input type="checkbox"/> bebo.com		17032831	16916615	0	601	0	115615
<input type="checkbox"/> birthdayalarm.com		3422685	3399513	0	0	0	23172
<input type="checkbox"/> No Domain Information		3191928	2181776	4669	877444	17962	110077
<input type="checkbox"/> comcast.net		686300	581370	318	84484	1139	18989
<input type="checkbox"/> rr.com		334003	266151	214	57126	391	10121
<input type="checkbox"/> mchsi.com		287846	252929	182	25897	390	8448
<input type="checkbox"/> apple.com		240548	216435	83	14403	270	9357
<input type="checkbox"/> insightbb.com		183950	162854	107	16151	236	4602
<input type="checkbox"/> att.net		183117	175323	46	5446	133	2169
<input type="checkbox"/> shawcable.net		141611	121036	75	16965	157	3378
<input type="checkbox"/> charter.com		119850	87310	136	29444	118	2842
<input type="checkbox"/> mindspring.com		100824	85371	43	12535	95	2780
<input type="checkbox"/> fiber.net		83006	1092	0	1	0	81913
<input type="checkbox"/> hp.net		63919	55493	16	4357	106	3947
<input type="checkbox"/> processrequest.com		59175	51588	21	3420	109	4037
<input type="checkbox"/> c gocable.net		38633	34863	4	3087	29	650
<input type="checkbox"/> rima-tde.net		37862	1795	258	34165	832	812
<input type="checkbox"/> msu.edu		36930	30780	13	2705	45	3387
<input type="checkbox"/> eircom.net		36359	0	84	12657	5007	18611
<input type="checkbox"/> adelphia.net		35444	25264	7	8637	63	1473

Add to Sender Group...



IronPort C30 (mx2.vlan.nuigalway.ie) - Monitor > Overview - Microsoft Internet Explorer

Address: https://mx2.vlan.nuigalway.ie/monitor/overview

Links: PDX PDM, IronPort C30 (mx1.srv.nuigalway.ie), Microsoft Outlook Web Access, BBC - homepage - Home of the BBC on the Internet, USC

Sender	Messages						
	Domain	Attempted	Stopped By Reputation Filtering	Invalid Recipients	Spam Detected	Virus Detected	Accepted (Clean)
Total (All Senders)		25445357	24611791	4631	626486	17689	184760
<input type="checkbox"/>	bebo.com	16587047	16480928	0	475	0	105644
<input type="checkbox"/>	birthdayalarm.com	3381432	3361429	0	0	0	20003
	No Domain Information	3351122	2903349	3316	395614	12382	36461
<input type="checkbox"/>	comcast.net	556512	527068	115	25580	386	3363
<input type="checkbox"/>	rr.com	326855	306619	107	17985	252	1892
<input type="checkbox"/>	att.net	202099	199571	9	1635	108	776
<input type="checkbox"/>	mchsi.com	177484	168905	68	6553	145	1813
<input type="checkbox"/>	insightbb.com	147956	141962	20	4478	126	1370
<input type="checkbox"/>	shawcable.net	93636	88838	14	4250	59	475
<input type="checkbox"/>	charter.com	67154	58627	29	7704	65	729
<input type="checkbox"/>	mindspring.com	64026	60465	18	3227	27	289
<input type="checkbox"/>	adelphia.net	62590	59789	23	2382	29	367
<input type="checkbox"/>	verizon.net	22043	13911	28	7809	25	270
<input type="checkbox"/>	chello.nl	16809	15149	16	1572	24	48
<input type="checkbox"/>	nanotechcongress.net	15314	15232	0	29	2	51
<input type="checkbox"/>	fibertel.com.ar	13252	11842	3	1371	4	32
<input type="checkbox"/>	cgocable.net	13007	12081	0	738	19	169
<input type="checkbox"/>	rma-tde.net	11890	1885	55	9673	89	188
<input type="checkbox"/>	galway.net	10077	8720	0	30	1	1326
<input type="checkbox"/>	nctv.com	9866	9767	0	88	3	8

Add to Sender Group

Internet

The Solution

An IronPort C300 was installed in a test environment. The C300 is the entry level enterprise model; it can process 180,000 messages per hour and features hardware redundancy for power, network and discs. The installation, configuration and product training was straightforward, so within a day NUI Galway were ready to start testing.

Kieran added: “We contacted three vendors who we felt could provide us with a solution which worked today and as our IT environment grew. All three vendors’ technology was fully evaluated and it very quickly became clear that IronPort’s technology was the superior. The C300 was very simple and quick to deploy but perhaps more importantly, IronPort’s reputation filters meant that the denial of service attacks almost over night became history. We implemented the C300 in conjunction with MS Exchange which allowed us to provide our internal customers with an email service which ensures continuity of service which from a SPAM management perspective, requires very little, if any maintenance.”

Matt Peachey, regional director, IronPort Systems said: “The work we carried out with NUI Galway is a great example of how all organisations need to evolve the way they protect themselves from email and web threats. Too many businesses think they have the situation under control. The reality is that IT departments have to spend increasing amounts of time administering email systems which are simply not dealing with the problem. This costs time and money and is a distraction and drain on resources which could be better deployed in other areas of greater benefit to the organisation. This stands as a testament to the organisations proactive approach to stopping spam becoming a major organisational headache.”