received 1960 leads, on companies using pirated software.

Ex-employees suspected in hack

US software company, LapLink, was compromised using passwords belonging to ex-employees.

The intruders were traced to a company called Classmates Online, where two former Laplink system administrators moved to new positions.

The attack caused the email systems to go down and important files disappeared according to the *Seattle Times.*

Classmates Online are currently investigating the incident and the suspects have been placed on paid leave.

This attack highlights the importance of deactivating ex-employee passwords.

US accountant pleads guilty in insurance fraud

A US accountant has pleaded guilty to charges of computer fraud for helping to divert millions of dollars in what is thought to be the largest insurance fraud in the US.

Gary Atnip, CFO of several insurance companies owned by financier, Martin Frankel, assisted in the diversion of funds to steal $200 million.

Mr Atnip pleaded guilty to transferring money from Franklin American Life Insurance Company to a securities company, allowing Frankel to transfer the money into a Swiss bank account.

Atnip was the CFO of several of the insurance companies owned by Frankel.

Frankel has pleaded guilty to stealing millions across insurance companies in five US states.

Another accomplice, Philp Miller, has been sentenced for his role in withdrawing money from the Swiss bank accounts to deliver to Frankel.

Anti-war hacking hits businesses

The start of the war in Iraq has been accompanied by a separate hacking war against websites by hacktivists.

Victims include Al-Jazeera, a US Navy website, the UK Prime Minister's site and the homepage of a UK industrial products distributor, Routeco.

The British Prime Minister, Tony Blair's site at www.number-10.gov.uk was apparently attacked using DDoS. The site was inaccessible for a short time, according to F-Secure, a provider of managed security.

The website of Al-Jazeera, which showed pictures of US Prisoners of War, has been overloaded with traffic due to a possible denial-of-service attack.

US, UK, Australian and South Korean organizations have been coming under heavy digital attack according to digital risk specialists, Mi2g.

The attacks are originating from the Middle East, France, Eastern Europe and a number of Latin American countries.

The number of attacks in March has exceeded 5646 against US online victims compared to 4365, which is what the rest of the globe has experienced.

So far the attacks have come from disparate hacking groups without a coordinated effort.

F-Secure say the actual number of defacements is much higher than the reported figures. The slow reporting system and the fact that many sites are restored before the defacement can be verified means that not all of the activity can be recorded.

The hacking groups select targets using systematic methods. Whole domains are scanned and several vulnerable hosts in the domain tend to be hacked at once say F-Secure.

The cost from anti-war attacks is thought to be $2.1-2.6 billion for March, Mi2G predicts.

Gov. Agencies join Liberty Alliance

The US General Services Administration and the Department of Defense (DOD) have joined the Liberty Alliance, a project dedicated to authentication standards.

The move will support the fact that authentication is one of the Bush Administration's 24 eGovernment initiatives.

"We are involved in a number of projects where there is a need for secure digital identity," said Bill Boggess, Chief of Access and Authentication Division at the DOD.

In Brief

COMMONWEALTH BANK VICTIM OF SCAM

Some Commonwealth Bank of Australia customers have been tricked into releasing their account numbers and passwords through a fake email scam. The bank is insisting that security has not been breached. The fake email asks users to reactivate their bank accounts and contains the Commonwealth Bank logo.

VISA FINE OVER RECENT CREDIT CARD BREACH

VISA USA has fined the Provident Bank of Cincinnati, the acquiring bank for Data Processors International (DPI) in response to the recent eight million credit card compromise.

ABBEY NATIONAL END FRAUD INVESTIGATION

Abbey National, a UK bank has completed an internal fraud investigation and failed to find evidence against staff suspected of taking back-handers from overpriced IT suppliers. A former member of the IT staff, Leslie Roberts made allegations stating that cheaper IT suppliers could have been used. The investigation involved Abbey National's First National subsidiary, which is in the process of being sold.

UK COMPANIES REPORTING MORE CYBERCRIME

There has been a noticeable increase in the number of cybercrimes that have been reported to the UK Hi-Tech Crime Unit since the launch of the Confidentiality Charter in December. This charter allows companies who report crime to the Unit to refuse legal proceedings to avoid negative publicity.