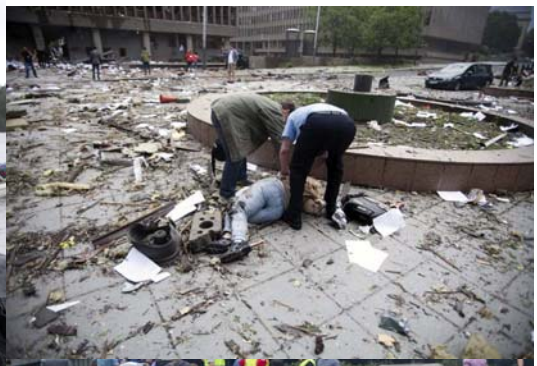
International Council For Industrial Security & Safety Management

Newsletter: August 2011

Let's professionalize the professionals…

http://www.wix.com/sbtyagi/iciss



Norway has suffered great loss! The trauma and agony of this peace loving country can not be described sufficiently! The all-together unfamiliar face of terrorism has started haunting the land which led a life full of tranquility and solitude!

A massive bomb blast recently hit government buildings in the Norwegian capital Oslo, killing at least seven people and injuring several others.

The bomb blast was followed by a fatal shooting incident near Oslo at a youth meeting of the Labour Party. The unprecedented shooting spree and bomb blast killed over 90 people in Norway Friday “shocked” and “saddened” the Norwegian citizens as much as the entire world.

One local commented that, “Norway would stand together as an open, peace-loving country also in the future” and for that, he said, “the Norwegian people and government needed the solidarity of the international society and the prayers worldwide. Now we know the reality of so many others in the world where violence pierces the lives of the innocent!” he said.

As the investigators and the national intelligence agency remain on their toes, one of the officials urged,

> ***“Let us all stay together for a world of justice and peace, without hate and revenge, but with the values of democracy, caring for the dignity and the human rights of every person”***

These are provably the words which aptly summarize the collective efforts of Security Professionals world-over…

Capt S B Tyagi
For ICISS

May 2011 issue of ICISS Newsletter carried article on security of Key Infrastructures and had discussed the cyberspace security and the treats to SCADA systems. In the newsletter there was reference of Stuxnet and as follow-up, following is worth reading….

SCADA worm a 'Nation State Search-and-Destroy Weapon'

With giant bulls eye on Iran nukes

A highly sophisticated computer worm that has burrowed into industrial systems worldwide over the past year may have been a “search-and-destroy weapon” built to take out Iran's Bushehr nuclear reactor, according to news reports published on Tuesday.

The Stuxnet worm was programmed to probe the hosts it infected for extremely specific settings. Unless it identified the hardware fingerprint it was looking for in industrial software systems made by Siemens, it remained largely dormant.

It was only after a unique configuration on a Programmable Logic Controller device was detected that Stuxnet took action. Under those circumstances, the worm made changes to a

piece of Siemens code called Operational Block 35, which monitors critical factory operations, according to IDG, which cited Eric Byres, CTO of a firm called Byres Security.

IDG reported: “By messing with Operational Block 35, Stuxnet could easily cause a refinery's centrifuge to malfunction, but it could be used to hit other targets too, Byres said.”

“Stuxnet is essentially a precision, military-grade cyber missile deployed early last year to seek out and destroy one real-world target of high importance – a target still unknown,” *The Christian Science Monitor* said. It went on to say that the digital fingerprinting capability “shows Stuxnet to be not spyware, but rather attack ware meant to destroy.”

http://www.theregister.co.uk/2010/09/22/stuxnet_worm_weapon/

Stuxnet clones may target critical US systems, DHS warns

Code samples raise concerns of variants

Officials with the US Department of Homeland Security warned that hackers could attack the country's power generation plants, water treatment facilities, and other critical infrastructure with clones of the Stuxnet computer worm, which was used to disrupt Iran's nuclear-enrichment operations.

Stuxnet was first detected last July as a self-replicating piece of malware that spread virally through SCADA, or supervisory control and data acquisition, systems used to control valves, gears, and other physical processes in industrial plants and factories. It was eventually identified as a highly sophisticated worm that exploited previously unknown vulnerabilities in Microsoft Windows and Siemens software that actively sought to sabotage several uranium enrichment facilities in Iran.

Speculation has abounded that it was the covert work of Israel, the US, or both.

At a hearing Tuesday before a subcommittee of the US House of Representatives Committee on Energy and Commerce, DHS officials said they are worried the wealth of technical details and code samples from Stuxnet could lead to clones that similarly target critical infrastructure in the US.

"Looking ahead, the Department is concerned that attackers could use the increasingly public information about the code to develop variants targeted at broader installations of programmable equipment in control systems," Roberta Stempfley and Sean P. McGurk warned in written comments posted on *Wired.com*, which reported on the warning earlier. "Copies of the Stuxnet code, in various different iterations, have been publicly available for some time now."

The ICS-CERT, short for the Industrial Control Systems Cyber Emergency Response Team, and the National Cybersecurity and Communications Integration Center "remain vigilant and continue analysis and mitigation efforts of any derivative malware," they added.

Stempfley and McGurk are the DHS assistant secretary for the DHS Office of Cybersecurity and Communications and director of the National Cybersecurity and Communications Integration Center Office, respectively. Their comments before the US House's Subcommittee on Oversight and Investigations warned that various nation states, terrorist networks, organized crime groups, and individuals on US soil "are capable of targeting elements of the US information infrastructure to disrupt, or destroy systems upon which we depend."

ICS-CERT recently warned that SCADA software originating from China and used by some customers in Europe, the Americas, and elsewhere contain security holes that could leave them open to Stuxnet-style attacks. The worm attacked five industrial plants inside Iran in 12,000 separate infections over a 10-month period, causing centrifuge arrays to malfunction.

http://www.theregister.co.uk/2011/07/27/beware_of_stuxnet_clones/print.html

Stuxnet code leak to cause Cyber-Apocalypse Now!

Source code for the sophisticated Stuxnet worm has reportedly made it onto underground forums where it is been offered up for sale at some unspecified price.

This not entirely unexpected development, first reported by Sky News, has prompted the satellite TV channel to get for broke with a loosely substantiated story sensationally headlined "Super Virus: A Target For Cyber Terrorists". Sky quotes unnamed senior IT security sources to report the "virus is in the hands of bad guys".

The malware could now be adapted and used to shut down power stations, "the transport network across the UK" and the 999 system, according to Will Gilpin, an IT security consultant to the UK government. Gilpin goes on to conclude, at the end of an accompanying video report that we're a generation behind and have already lost the war in cyberspace.

http://www.theregister.co.uk/2010/11/26/stuxnet_leak_hype_rot/

McAfee uncovers massive global cyber snoop

China masterminded 'Operation Shady RAT'

Courtesy: Captain Ian Lawrence Kerr, Ranbaxy

China masterminded 'Operation Shady RAT' targeting over 70 organizations, governments say analysts. Computer security company McAfee has said that it has discovered a massive global cyber spying operation targeting several US government departments, the UN and other governments across the world for five years or more.

Analysts say it is likely that China is behind the cyber espionage dubbed 'Operation Shady RAT' by McAfee. RAT stands for "remote access tool". The Guardian reported that security experts at McAfee had discovered a "command and control" server in 2009 that was used to control the operation. On revisiting the server this March, experts found logs which revealed all of the attacks.

Victims of snooping campaign include: governments of Canada, India, South Korea, Taiwan, the US and Vietnam; international bodies such as the UN, the Association of Southeast Asian Nations (ASEAN), the International Olympic Committee, the World Anti-Doping Agency; 12 US defense contractors, one UK defense contractor; and companies in construction, energy, steel, solar power, technology, satellite communications, accounting and media, said an AFP report. McAfee said there is evidence that security breaches date back to mid-2006.

McAfee vice-president of Threat Research Dmitri Alperovitch said the attacker was looking for information in military, diplomatic and economic domains. "If you look at an industry and think about what is most valuable in terms of intellectual property, that is what they were going after," Alperovitch said. He said that the loss represents a massive economic threat.

"This is the biggest transfer of wealth in terms of intellectual property in history," Alperovitch said.

"The scale at which this is occurring is really, really frightening." "Companies and government agencies are getting raped and pillaged every day. They are losing economic advantage and national secrets to unscrupulous competitors," he said.

Alperovitch said a nation state was behind the operation. Experts have blamed China for the snooping, though they say that it could be the work of Russia as well.

You Can Help Prevent Card Fraud

Since the late 1990s, merchants have been known to be targets of card fraud perpetrators who recruit staff to record magnetic stripe data of the credit cards used at the establishments. This is termed as "Skimming Counterfeit" and it is costing the financial institution astronomical fraud losses globally.

The equipments illustrated below are some data capture devices ("skimmers") recovered in various criminal cases around the world. Each of these skimming devices can be used to copy and store data from the magnetic stripes of credit, debit, ATM and other cards. Please note that other models of these devices may also be in circulation.

Definition of Skimming

"The illegal copying (stealing) of the magnetic stripe data of a genuine card, including the encryption value, and subsequently transferring the data onto a counterfeit magnetic stripe for illegal usage."

- Skimming involved the solicitation of merchants' owner and/or staff by the counterfeiting groups in stealing of the magnetic stripe data from a customer.
- Most of these merchants identified for skimming activity are those that process the credit card 'out-of-sight' of the cardholder, i.e. restaurants, nightclubs, pubs, discotheques and hotel front offices, etc.

Most of the credit cards data are skimmed using these devices. Please take note that a skimmer on average is only 10 cm in length and can be easily concealed from view. To avoid detection, the perpetrators have also cleverly disguised these skimmers as a Y2K checker and pager (refer to exhibits B and D).

Exhibit A: Top View

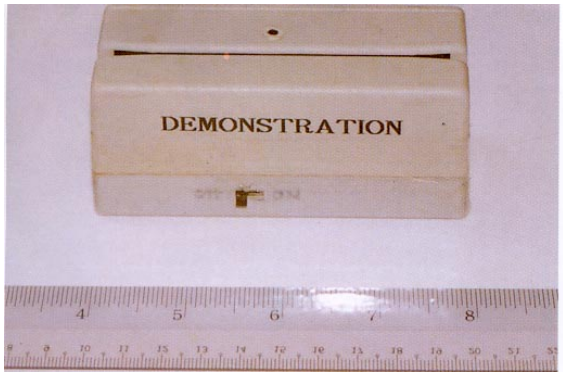


Exhibit A : Front View

Exhibit B : Front View

Exhibit C: Top View

Exhibit D : On belt

Exhibit D : Side View

Modus Operandi:

When the cardholder presents the card for payment, the 'collusive' waiter/waitress or attendant at the establishment swipes the credit card across a skimming device. This

device basically reads and stores the magnetic stripe data. The physical card is then delivered to the cashier counter for normal processing of the card transaction. All this while, the cardholder does not know that his credit card magnetic stripe data has been compromised. The cardholder only knows about it upon notification by the bank or upon receipt of the monthly statement of account that will reflect a string of 'disputed' transactions.

To assist the bank to mitigate the risk of skimming and to help the card-holders, append below are guidance pointers for reference.

- **Treat all credit cards like cash.**
- **During check-in or out from a hotel, be aware on the movement of credit card, and ensure that the staff is swiping the card over a POS/EDC terminal only**
- **Beware and question the personnel handling the credit card when it is swiped in a device other then a POS/EDC terminal.**
- **Inform the concerned bank, should you notice the personnel handling the card swipes it through a device similar to those reflected above.**
- **Do not allow anyone to take the card to another area to process transaction.**
- **Speak to and recognize the waiter/waitress that handles the credit card during payment. This transmits a 'deterrent' message to the personnel handling the card who may have intention to 'skim' credit card magnetic stripe data.**

Should anyone come across any suspicious practices or noted similar-looking devices being applied at the merchant outlets, do contact the concerned bank / credit card provider or Authorization Center immediately. Their contact numbers are appended below.

TELEPHONE HOTLINE			
COUNTRY	FRAUD CONTROL UNIT		24-HRS AUTHORISATION CENTER
	Office	Hand-phone	
Hong Kong	2282 1118	909 92326	2282 1115
Taiwan	2715 9087	920 782154	271 56100
Malaysia	7720 4620	012 7032828	772 04611
Singapore	780 7666	973 72966	780 7629
Philippines	830 1231	091 78381026	830 1222
Thailand	232 6549	01 8355569	636 1144/5
India	(80) 532 1392	984 5044005	(80) 558 6600
Indonesia	5739618 x2830	08 11991195	573 9618 x2820/28/27
Brunei	223 4401	N/A	(65) 780 7629
Grindlay	(44) 8219 535	984 1026942	(44) 821 2255
SCB Manhattan	265 53682	N/A	265 53128

Security of your children

Courtesy: Col D R Semwal (callsamydr@yahoo.com)

It has been said "children are our most valuable resource". It is absolutely necessary we take positive measures to insure their safety and prevent them from becoming a victim of crime. Whether they're your own child, your brother or sister, neighbor, or child you frequently baby sit.

- Never leave children alone; not at home, in a vehicle, in the yard or anywhere.
- Define what a STRANGER is. Let the child know just because they have seen someone before (i.e. mailman, paperboy, neighbor, waitress, etc.) it does not mean these people are not strangers. They are still people they don't know.
- Teach the children their full name, your name, address and phone number, including area pin codes. Teach them how to use a phone and cell phone.
- Teach your child the "What If...?" Making up different dangerous situations they might encounter and helping them role play what they would do in that situation.
- Take the time to talk with your children and be alert to any noticeable change in their behavior or attitude toward an adult or teenager; it might be a sign of sexual abuse or harassment.
- Set up procedures with your child's school or day care center as to whom the child will be released to other than yourself, and what notification procedures they are to follow if the child does not show up on time.

He changed the face of Delhi in Bhati Mines Area!

He was successful in restoration of mining land by afforestation activities in coordination with Deptt of Environment, Government of Delhi.

His restoration efforts resulted in ecological balance of this large mining area to create a Wild Life Sanctuary.

Teach your children their body is private and no one has the right to touch them in a way that makes them feel uncomfortable. (Anywhere their bathing suit would be). If anyone touches them in a wrong way they should "SAY NO, GET AWAY", and TELL SOMEONE they trust as soon as possible, no matter what the other person might say to scare them or threaten them.

Scam targeting females in particular

Courtesy: Col D R Semwal (callsamydr@yahoo.com)

Here is a serious issue that has been spreading through-out all cosmopolitan and metropolitan cities. Currently this is happening in Bombay. We may not even know when this kind of crime has reached to you. So, this is to make you aware of the situation. Also pass on the same to all known near and dear to make them aware and be alert.

We have been informed of the following scam, which is targeting females in particular. They receive a phone call from the Post Office asking them to confirm their company postcode. When this is given, they are told that they have become eligible for some gift vouchers for their co-operation and are asked to provide their home address and postcode in order to receive the vouchers. So far 90% of the women who have provided this information have been burgled as it is assumed that their homes are empty during office hours. The police are aware of this scam and the Post Office has confirmed that they are NOT conducting postcode surveys.

Also, it has been reported if you receive a telephone call from an individual who identifies himself/herself as being an AT & T Service technician who is conducting a test on that telephone line, or anyone else who asks you to do the following, don't. They will state that to complete the test the recipient should touch nine, zero, the hash (90#) and then hang up. To do this gives full access to your phone line, which allows them to place a long distance international or chat-line calls billed to your account. The information, which the police have, suggests that many of these calls are emanating from local jails. The information has been checked out by the police and is correct: DO NOT PRESS 90# FOR ANYONE.

Would anyone reading this please pass the information on to colleagues, friends, etc. otherwise it could cost someone a lot of money.

Flying robot in sky to keep vigilance

Scientists have developed a new flying robot equipped with the world's most advanced intelligence systems which could help spy on and track down criminals easily.

Users simply need to point to a place on Google Maps on its touch screen controller and the robot flies there at 48kmph to record high quality video that can be beamed to an iPhone in real-time.

The robot, called the Scout, can go up to 500ft above the ground and can zoom in to a close-up from 300 meters away, meaning it may not even be seen while on a mission. Developed by Canada based Aeryon Labs, the miniature unmanned aerial vehicle contains four rotor blades that also ensure it is practically silent when hovering.

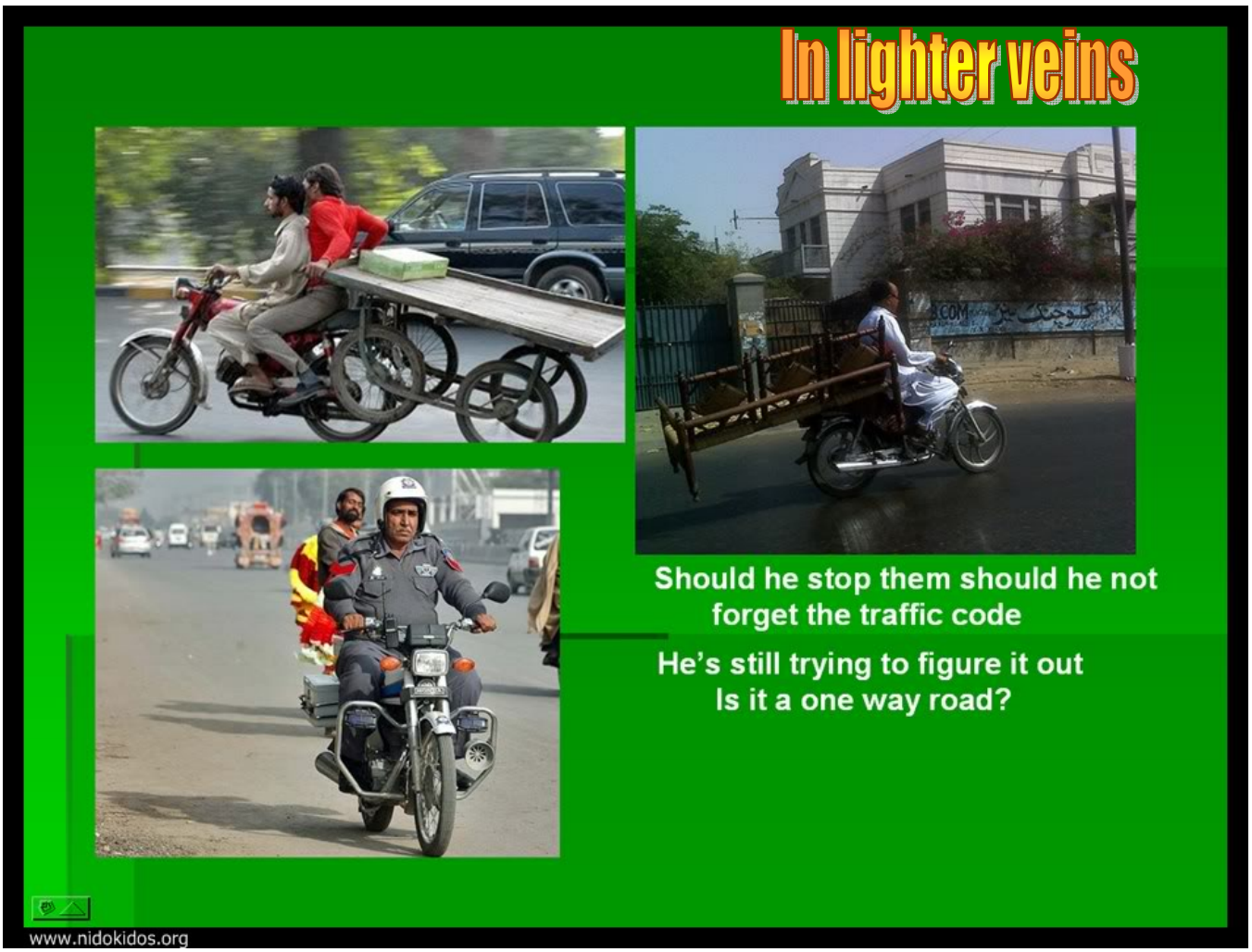
According to Aeryon, the Scout has the most sophisticated and highest quality aerial intelligence available today and it beams its pictures to any electronic device, be it a remote computer or even an iPhone. The $50,000 robot and its laptop style control panel fits into a suitcase so it can be deployed easily over any crowd and carried away covertly, the company said.

One of the most ingenious features is that the camera is self-correcting, so even if you are flying along at speed it will stay locked on the target.

In a video posted on the Aeryon website, the robot hovers at a great distance from a car thief who is being caught in the act. When the camera zooms in, the suspects face can be seen clearly, enabling police to get a better idea of his identity.

The Scout also has potential uses for the military and general surveillance missions.

Capt S B Tyagi, COAS' CC*,
FISM, CSC, CSP
2011.08.12 12:37:18 +05'30'



P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!

Security is thankless job, but someone got to do it!

Suggestions & feedback may be sent to us on e-mail: sbtyagi1958@gmail.com