October 2011 / Issue 01

The Cyber Advisor

Invensys Critical Infrastructure & Security Practice

this issue

This Virus Will Bug You

NERC Stats
For September 2011:

Total Fines
$1,259,000

Average Fine per Violation
$419,667

Fines Increased
183%

NERC-CIP Violations as % of Total Violations
33%

Critical Cyber Security News

This month, everyone's fears were realized with a follow up to Stuxnet when the new "Son of Stuxnet" bug, called Duqu, was confirmed on October 14, 2011. The confirmation validates a recent report from the CIA that Cyber Security is now a Top -3 concern for the US government.

NERC News

In September, the average fines skyrocketed to $419,667 from a year-to-date average of only $29, 258. NERC Notice of Penalties (NOP) fines were up significantly going into October.

YTD Total Fines

$6,663,293

YTD Total Fines

195 companies

YTD Total NERC-CIP Fines

77 companies

Duqu and You

On October 18, 2011, Symantec re-leased a Se describing W32. Duqu, an information-gathering threat targeting specific organizations including industrial control system manufacturers. According to Symantec, W32. Duqu does not contain any code related to industrial control systems (ICS) and is primarily a remote access Trojan.

Symantec reports that the original sample of W32. Duqu was gathered from a research organization based in Europe, and that additional variants have been recovered from an additional organization in Europe. According to Symantec, the attackers are looking for information such as design documents that could potentially be used in a future attack on an industrial control facility.

Industry News

Son of Stuxnet? Researchers Warn of Impending Cyber Attack - *From abcNews.com 10/18/2011*

A new computer virus using "nearly identical" parts of the cyber super weapon Stuxnet has been detected on computer systems in Europe and is believed to be a precursor to a new Stuxnet-like attack, a major U.S.-based cyber security company said today.

The Day of the Golden Jackal–The Next Tale in the Stuxnet Files: Duqu - *From McAfee 10/18/2011*

Stuxnet was possibly the most complex attack of this decade, and we expected that similar attacks would appear in the near future. One thing for sure is that the Stuxnet team is still active–as recent evidence has revealed. McAfee Labs received a kit from an independent team of researchers that is closely related to the original Stuxnet worm, but with a different goal—to be used for espionage and targeted attacks against sites such as Certificate Authorities (CAs).

Stuxnet Clone 'Duqu': The Hydrogen Bomb of Cyberwarfare? - *From FoxNews.com 10/19/2011*

If the Stuxnet virus was the atom bomb of cyberwarfare, then the discovery this week of the "Duqu" virus is the hydrogen bomb, security experts are warning. It is the second major weaponized virus to turn computers into lethal weapons with devastating destructive power.

U.S. Strategic Drone Fleet Infected by Stealthy Keylogger Malware - *From eWeek.com 10/8/2011*

An unknown type of malware has been detected on the computers that control the Predator and Reaper drones in the US Air Force's fleet of unmanned aircraft. Computers used to control the drone unmanned aircraft used by the military to carry out military operations have been reportedly infected with malware, ac-cording to a report.

Smartphones Will Become a Way to Attack Otherwise Protected Devices - *From InfoWorld.com 10/11/2011*

Compromised smartphones will infect computers when they dock in much the same way malware gets onto laptops via thumb drives. Smartphones will become an increasing menace to network security that could drop malware onto protected devices when they dock to sync or plug into USB ports to charge, security experts say in a Georgia Tech report.

Nuclear and Military Data Taken in Mitsubishi Hack - From eWeek.com Europe 10/25/2011

Highly sensitive military and industrial data was stolen from Mitsubishi when it was hacked in the summer. The perils of a well-organized cyber-attack have been underlined once again, after highly sensitive data relating to Japan's military and critical infrastructure was reportedly stolen.

Industry News

RSA Hackers Knock Off 760 Other Businesses

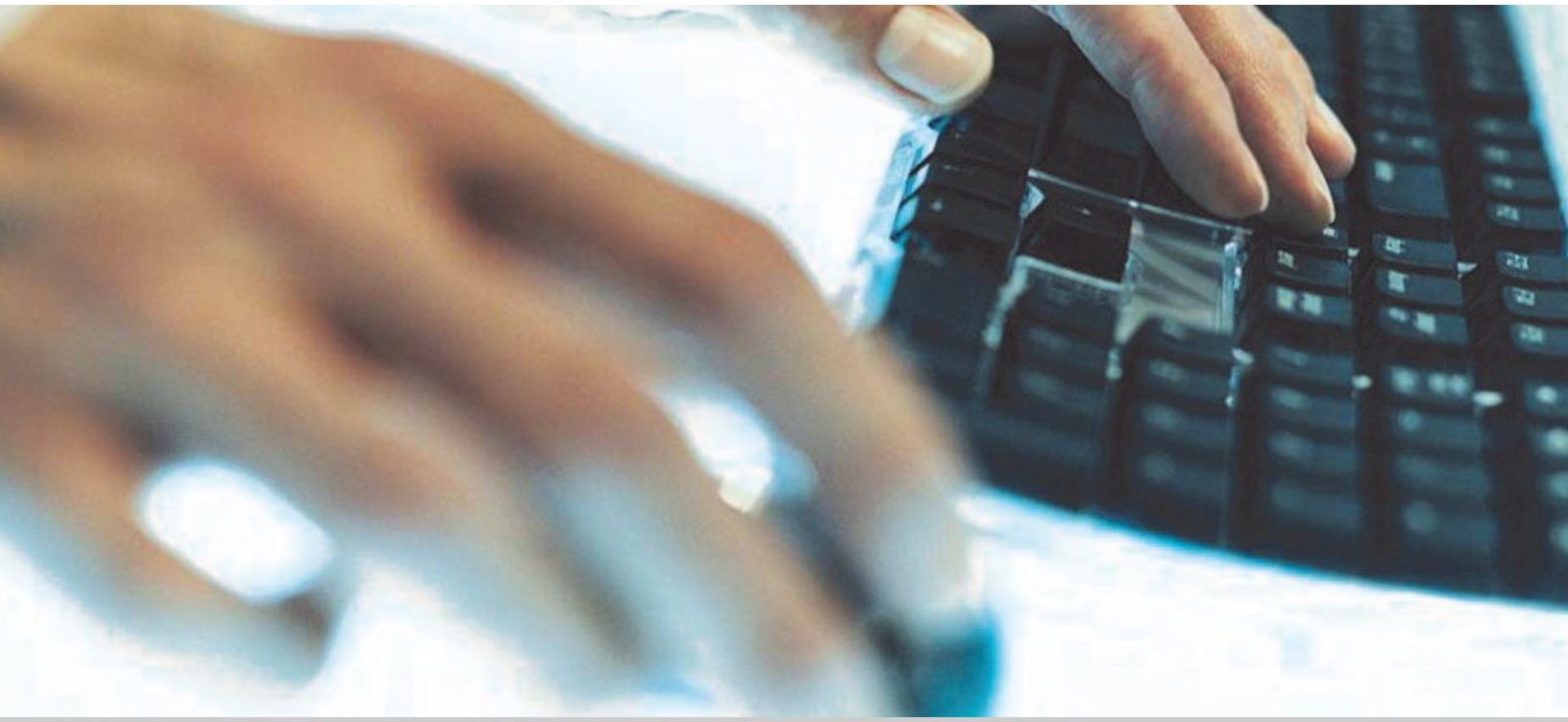
- From SC Magazine 10/25/2011

At least 760 organizations appear to have fallen victim to the same attacks that compromised RSA's SecurID authentication system earlier this year. The names appear on a list of targeted machines that had phoned home to the same command-and-control (C&C) servers used in the March attacks on RSA. The list was shared by information professionals to Congress and subsequently published by blog "Krebs on Security."

SEC Says Companies Should Disclose Cyber-Incidents, Risks to Investors

- From eWeek.com 10/15/2011

The latest guidance from the SEC explicitly states that companies should discuss their cyber-security measures to investors and disclose "material" security incidents. The Securities and Exchange Commission issued some guidelines suggesting that companies should report cyber-incidents that may affect the bottom line.



The Cyber Advisor
Invensys Critical Infrastructure & Security Practice
October 2011 / Issue 01

Invensys Critical Infrastructure and Security Practice (CISP)

Invensys CISP has capability in establishing, implementing and maintaining industry best practices to meet the demands for government regulations (NERC-CIP, NEI 08-09, CFATS), industry requirements and company compliance requirements. Attributes of Invensys CISP Critical Infrastructure Consulting include:

Hardware Independence

CISP can work with any type of control system or type of technology a customer prefers for the security environment.

Industry Knowledge

CISP has a number of resources that understand the demands of Controls Networks and the requirements for continued uptime.

Regulation Knowledge

CISP has a number of subject matter experts who understand a whole host of regulatory requirements as well as active participation in a number of industry and government groups.

Proven Methodology

CISP follows a proven life cycle methodology to support the implementation of a comprehensive successful cyber security program. Attributes of the life cycle approach are Assessments, Development, Implement and Management.

Technical Knowledge

The same CISP personnel who have regulatory knowledge are also well versed in the latest security policies, procedures, and technologies for intrusion detection and prevention, firewalls, DCS, and network architecture.

invensys™

For additional information, please visit us at
http://iom.invensys.com/CyberSecurity

5601 Granite Pkwy. Suite 1000 Plano, TX 75024 ▪ P 214.295.6365 ▪ F 888.758.7675 ▪ **iom.invensys.com**