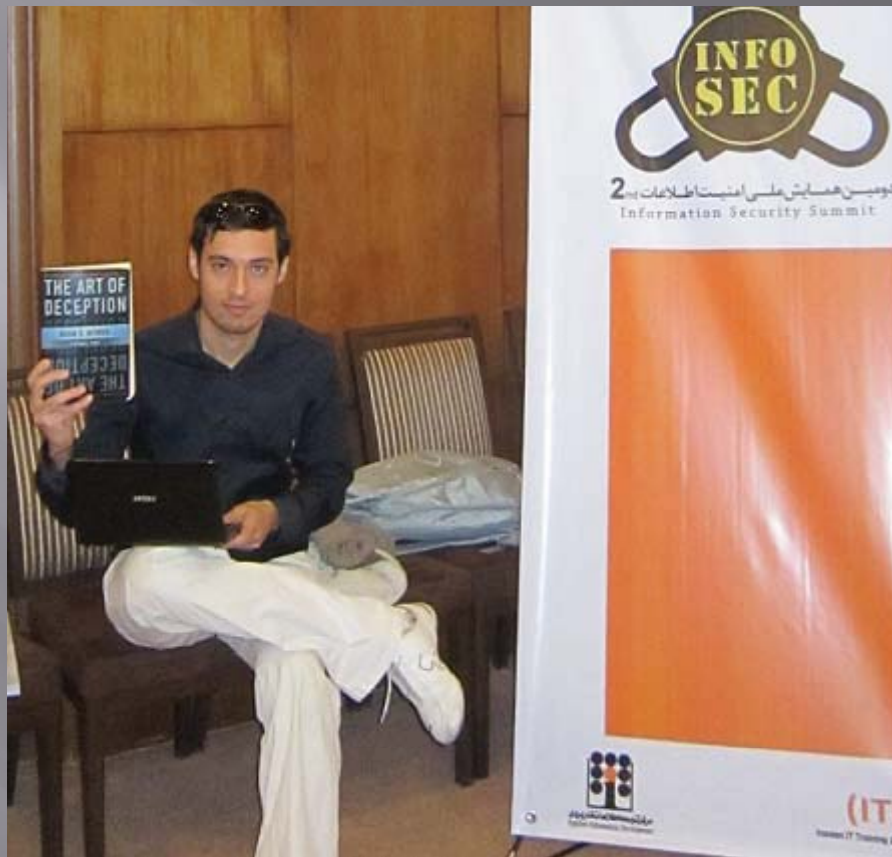


The Art of Deception for Stuxnet in IRAN

A Report about Stuxnet Activity In IRAN

U0VD SECURITY INC

www.u0vd.org



I'm sure persons who wrote the Stuxnet worm, Right now reading this note!

We know this is nature of the Cyber war

But, we are peace, Always

Nima Bagheri, Security Researcher

Contact: www.nima.tel

U0VD SECURITY INC

www.u0vd.org

Who Am I ?

- ▣ CEO of the U0vd Security web Site www.u0vd.org
- ▣ Security Developer ,Security Researcher
- ▣ MCSD , MCSE , CEH , CSISSP , A+ ,CCNA
- ▣ 7 years experience in Computer Security Programming and 4 years in Anti Malware Technologies
- ▣ Experience in Maintenance for Iranian Power Plants
- ▣ First person in IRAN who Released Security Solution for Stuxnet worm for Iranian CERT
- ▣ Author of the Venak and Avenak Detection Malware Scanner MPS Edition

The Story of Stuxnet

Stuxnet was first developed more than a year ago; Stuxnet was discovered in July 2010, when a Belarus-based security company discovered the worm on computers belonging to an Iranian client.

Symantec researchers said in July that nearly 60% of all infected PCs were located in IRAN.

It is the first discovered worm that spies on and reprograms industrial systems. The first to include a PLC Rootkit, the first to target critical industrial infrastructure.

The worm's probable target has been said to have been high value infrastructures in Iran using Siemens control systems. According to news reports the infestation by this worm might have damaged Iran's nuclear facilities in Natanz and eventually delayed the start up of Iran's Bushehr Nuclear Power Plant.

Stuxnet attacks Windows systems using four zero-day attacks (plus the CPLINK vulnerability and a vulnerability used by the Conficker worm) and targets systems using Siemens' WinCC/PCS 7 SCADA software.

It is initially spread using infected USB flash drives and then uses other exploits to infect other WinCC computers in the network. Once inside the system it uses the default passwords to command the software.

The Stuxnet Technical

The complexity of the software is very unusual for malware. The attack requires knowledge of industrial processes and an interest in attacking industrial infrastructure.

The number of used zero-day Windows exploits is also unusual, as zero-day Windows exploits are valued, and hackers do not normally waste the use of four different ones in the same worm.

Stuxnet is unusually large at half a megabyte in size and written in different programming languages (including C and C++) which are also irregular for malware.

It is digitally signed with two authentic certificates which were stolen from two certification authorities (JMicron and Realtek) which helped it remain undetected for a relatively long period of time.

It also has the capability to upgrade via peer to peer, allowing it to be updated after the initial command and control server was disabled.

Stuxnet requires specific variable-frequency drives (frequency converter drives) on the system.

It only attacks systems with variable-frequency drives from two specific vendors: one headquartered in Finland and the other in Tehran, “Fararo Paya” located in Iran ex web www.fararo.com or now <http://fararopaya.com>

What was the IRAN's Reaction to Stuxnet?

In 29th July Computer Emergency Response Team in Iran (IrCERT or APA) Reported Iran's Stuxnet Attack and Removal tool.

APA reported "Virus writers attack the Windows operating system, which recently intensified by an Internet worm was getting some action with a new virus writers have entered a new level."

APA also reported an advisory for all Iranian users to use a removal tool "Iranian users could use the Venak and Avenak Anti malware".

<http://www.ircert.ir/fa/42/-1/ta/show/3092>



Figure 1, The APA (Iranian Cert) Guide Article for defeat with W32.Stuxnet.B worm

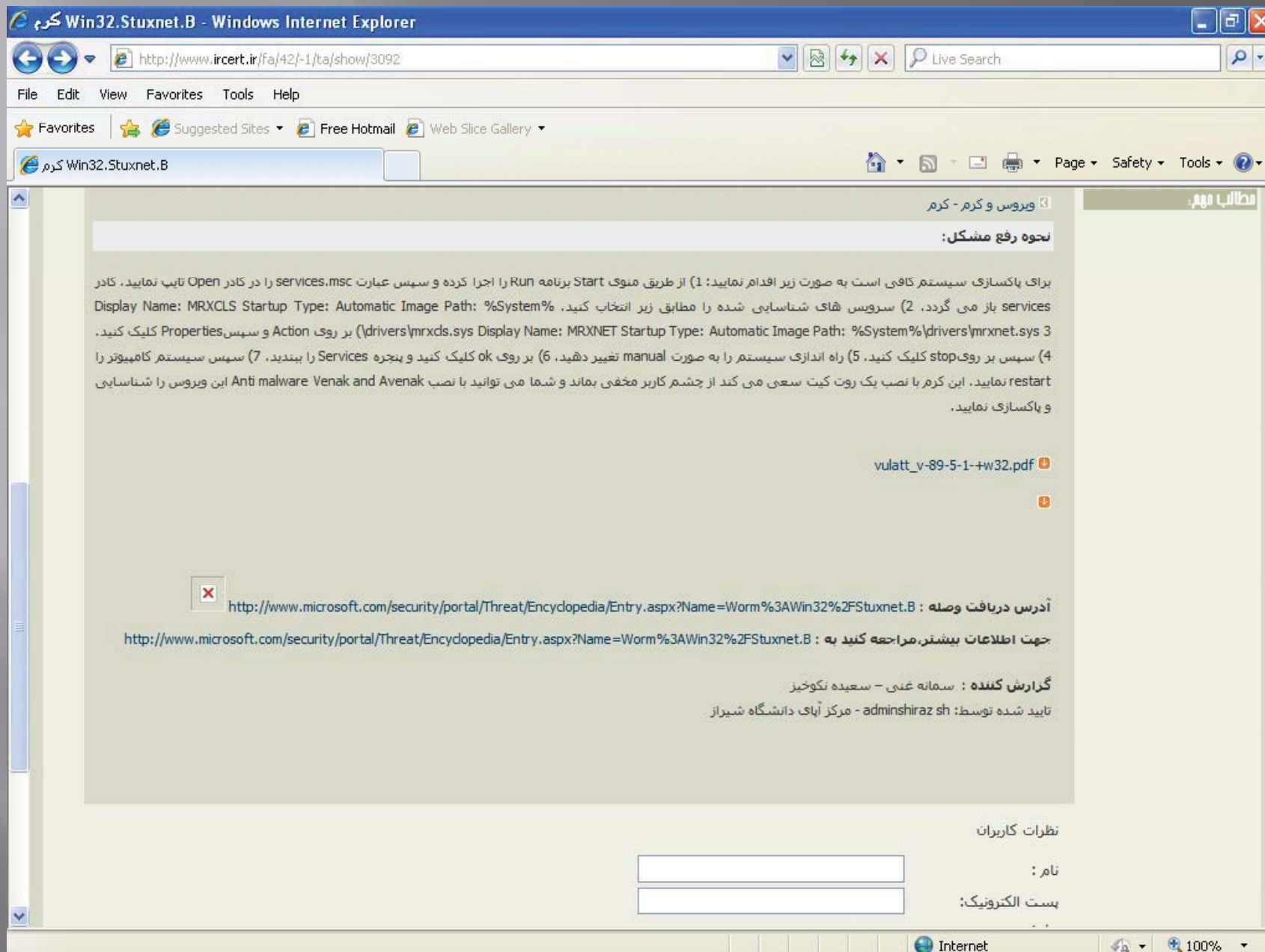
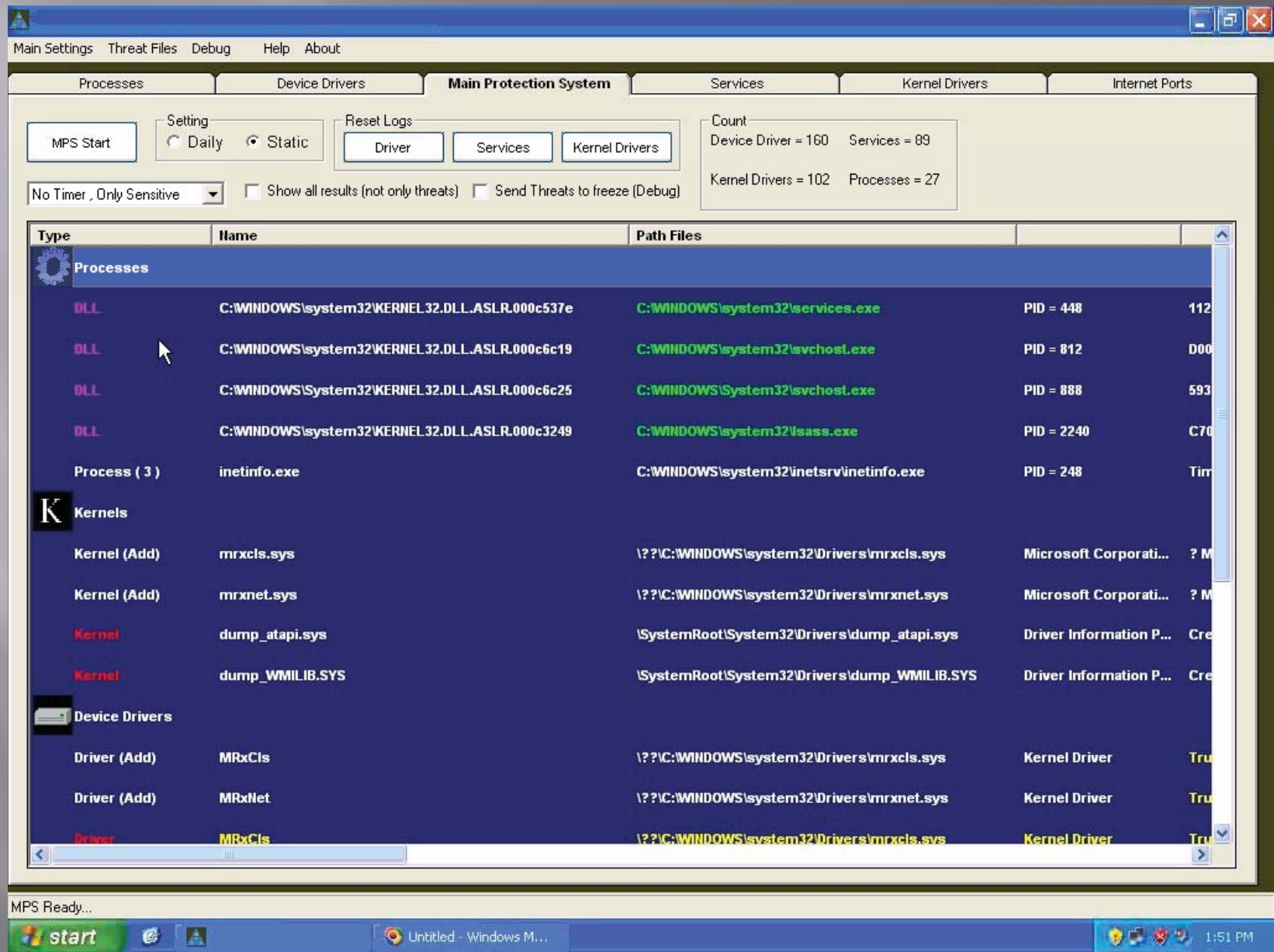


Figure 2, The APA Article for defeat with W32.Stuxnet.B, they Reported to users to use Venak and Avenak anti malware to remove the Stuxnet worm.



The Venak and Avenak Detection Malware Scanner MPS Edition Detect Stuxnet as unknown Malware Simply (without any Update)

The Iranian News Reporters

The Iranian News Reporters

The head Manager of the Bushehr Nuclear Power Plant told Reuters that only the personal computers of staff at the plant had been infected by Stuxnet and the state-run newspaper Iran Daily quoted “Reza Taghipour”, Iran's telecommunications minister, as saying that it had not caused "serious damage to government systems” reported by “Fars news”.

<http://www.farsnews.com/newstext.php?nn=8908061031>



Figure 3, The Farsnews Report about Stuxnet.

Maher (Computer Rescue and Coordination Center)

The Iranian Computer Rescue and Coordination Center Portal (Maher) presented more than 3 times Workshop and security conference to Defeat with Stuxnet. <http://www.certcc.ir>

The screenshot shows the Maher (CERTCC) website in a Windows Internet Explorer browser window. The browser's address bar displays <http://www.certcc.ir/#>. The website's header features the Maher logo and the text "مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای" (Maher Center for Computer Incident Response and Coordination of Computer Incident Operations). The main content area is divided into several sections:

- تهدیدات جاری** (Current Threats): A section listing current threats, including "آسیب پذیری فراخوانی فایل های DLL" (DLL Calling Vulnerability) and "بدافزار Stuxnet" (Stuxnet malware).
- آزمایشگاه بدافزار ماهر** (Maher Malware Lab): A section for malware analysis, featuring a list of reports and a "گزارش سازمان های آلوده به بدافزار" (Report of organizations infected with malware) link.
- امنیت در رایانه شما** (Security on your computer): A section providing security tips, including "پنج نکته امنیتی برای کاهش خطرات مدرن وب" (Five security tips for reducing modern web risks).
- معرفی ماهر** (Maher Introduction): A section providing information about the center, including "اهداف و مأموریت" (Goals and Mission), "ساختار" (Structure), "نقشها و وظایف" (Roles and Responsibilities), "کمیته مشورتی" (Advisory Committee), "دانلود بروشور" (Download Brochure), and "تماس با ما" (Contact Us).
- خدمات** (Services): A section listing services, including "گزارش حادثه" (Incident Report), "گزارش آسیب پذیری" (Vulnerability Report), and "مشاوره" (Consulting).

The website also includes a search bar, a navigation menu, and a footer with contact information.

Stuxnet: A Breakthrough Maher's Reported

At 16th November 2010 "Zahra Neekdel" the news reporter of The Iranian Computer Rescue and Coordination Center (Maher) reported new documents about Iranian Stuxnet.

That reported has been based on Eric Chien's article "Stuxnet: A Breakthrough".

Reporter Said: Eric Chien's "We can now confirm that Stuxnet requires the industrial control system to have frequency converter drives from at least one of two specific vendors, one headquartered in Finland and the other in Tehran, Iran (Industrial automation Fararo Paya Company)."

"Stuxnet monitors the current operating frequency of these motors, which must be between 807 Hz and 1210 Hz, before Stuxnet modifies their behavior. Relative to the typical uses of frequency converter drives; these frequencies are considered very high-speed and now limit the potential speculated targets of Stuxnet. We are not experts in industrial control systems and do not know all the possible applications at these speeds, but for example, a conveyor belt in a retail packaging facility is unlikely to be the target".

"Also, efficient low-harmonic frequency converter drives that output over 600Hz are regulated for export in the United States by the Nuclear Regulatory Commission as they can be used for uranium enrichment."

"According to his words, suspicion, and think about the fact that nuclear power plants Stuxnet target was there, but nuclear power plants use enriched uranium, and therefore require frequency converters Stuxnet notes that they are looking for is not."

<http://www.certcc.ir/index.php?name=news&file=article&sid=905>

<http://www.symantec.com/connect/blogs/stuxnet-breakthrough>

Information technology news agency (ITNA)

In 21th October 2010 Information technology news agency (ITNA) reported Reza Taghipour" Iran's telecommunications minister said they identify persons who transfer Stuxnet to IRAN.

<http://www.itna.ir/archives/news/014900.php>

The Original article was translated with Google translate

Minister of Communications and Information Technology: people who willingly or not the virus has been transported into the country.

Minister of Communications and Information Technology to identify the perpetrators of spyware virus release, called Stuxnet said. Reza Tqypvr after the Cabinet meeting yesterday in an interview with the Central News release about the cause of the virus, said: diffusion path through which the virus Stuxnet portable flash memory had been identified.

He added: "People willingly or not the virus has been transported into the country. Tqypvr about identifying these people said: currents were detected and whether it was deliberate or without notice to the approximately Sahvy (sinless and without purpose of attack) been identified.

Communications Minister stating that this issue has followed the necessary directions, added: "Thus we could repeat these things to avoid in the future.

Tqypvr currents in response to a question about viruses Stuxnet publisher said: some foreign experts who have studied industrial traffic and also some people were unaware that if Sahvy (sinless) through portable memory have transferred the virus.

He added: "The working groups in coordination with the Ministry of Communications has been formed in all ministries, we have found a good structure and containment in this topic.

The Points of View

The Points of View

▣ **Symantec Report about 60% of infected system located Iran.**

On July 20, 2010 Symantec set up a system to monitor traffic to the Stuxnet command and control (C&C) servers.

This allowed us to observe rates of infection and identify the locations of infected computers, ultimately working with CERT and other organizations to help inform infected parties. The system only identified command and control traffic from computers that were able to connect to the C&C servers. The data sent back to the C&C servers is encrypted and includes data such as the internal and external IP address, computer name, OS version, and if it's running the Siemens SIMATIC Step 7 industrial control software.

▣ **The Problem and Limits.**

There is rule exist in Iran which will blocked any trade between a company which belongs to Iran's government and a US Companies to buying Security Product likes Symantec. Let's check this out!

The Government's Rules in Iran for Companies.

That is not possible for any power plant in Iran to install Symantec products on their systems.

Why not?

First because we have no any reseller located in Iran to sold American products to power plants.

So, are you trying to say Symantec is lair? Oh No

That systems checked by Symantec belong to Iranian users or persons who used cracked version of the Symantec for their networks, well anyone can download and install.

Second, 100% of Iranian power plants use the original anti viruses for their networks based that law.

Third, we have only 11 PAP (Private Access Provider) companies in Iran and Iranian power plants had to receive internet service form or the ICP (Internet Connection Provider) who get certificated form.

Well, I'm not sure but I don't think so Symantec could identify and detect those industrial systems infected by Stuxnet technically (Because for nature of the privacies exist in Iran) .

The Bushehr Nuclear Plant

As we know the Stuxnet could attack to centrifuges, Bushehr is just a power plant and it's not place for uranium enrichment, so technically I can't believe Stuxnet could attack to Bushehr Power plant systems.

Maybe we have Scada Siemens in Bushehr Nuclear plant but we have not any Drive or Centrifuges there.

The Bushehr Nuclear Plant project is considered unique in terms of technology, Security Defenses and Safe guards and Please remember Most of important Iranian power plants even have not access to internet directly for example likes Bushehr power plant.

Also Bushehr power plant even have not any web site for.

The Proactive law

We have a proactive law in most of Iran's power plants which restricted access to any USB devices for their employees in important part of a network for security reasons.

Most of these systems even are not connected to their local networks and will be updated by Read-only Devices.

I have a report from some engineers which told me they had Some infected systems in their networks, but those systems belongs to Maintenance systems and did not connected to local network.

The Part Time Jobs!

As you know most Maintenance employees have part time jobs (in fact in Iran it is), so they are not part of a power plant systems and could break any rules! These persons could transfer their laptops in to the power plants and infect the systems. Plus, these employees could have any version of the anti viruses in their own systems likes Symantec or anything.

Maybe Symantec trace those persons, we don't know!

Maybe Symantec had access to internet Backbone and could trace the infected systems but how when these networks are not connected to the internet ?

At last we believe anyone could break the law and that is fact!
We can't have documented results for some security reasons.

Interview with Fararo Paya's CEO

Interview with Fararo Paya's CEO

We received an information from Farao Paya's CEO.

For privacy and security reasons we can't release the CEO name and that engineer, but we can grantee these information is 100% truth.

For more information you can see the new website of Fararo Paya's Corporation find out here

<http://fararopaya.com>

So here it is

The Interview

Engineer:

Can you introduce yourself?

CEO:

I'm Mr. *****, CEO of Fararo Paya Corporation

Engineer:

So, your company is very famous right now , isn't ?

CEO:

Yes, out of believe!

Engineer:

So tell me more about your Drives My mean the Famous "KFC750"

What mechanisms are exists on this product which permission to Stuxnet worm to attack the centrifuges ?

CEO:

Technically , nothing

Engineer:

Why ? We know Stuxnet writers try to attack your product in that range

CEO:

Yes, I seen some research about Stuxnet and our KFC750 product

The Interview

Engineer:

Well , all of us know Stuxnet monitors the current operating frequency of these motors which must be between 807 Hz and 1210 Hz , did you set that range for your Company Drives ?

CEO:

No

Engineer:

Can you tell me what is that range ?

CEO:

For security reasons nope

Engineer:

Oh sorry, I forgot!

CEO:

Look, technically our product will support ranges between 0 to 2400 and Stuxnet could attack KFC750 if we set that rang on it but I don't know how Stuxnet could attack our drives ?

Can you tell me how ?

Engineer:

Well, have you any Serial port on it , isn't ? For example RS232 Or something like that ?

CEO:

Yes , but it's not necessary when you Decided to use our Drive

The Interview

Engineer:

Why ?

CEO:

Because our drives capable to set that range without any PLC or “Motion Card”

In fact our drives are” Stand Alone”

You can find out in our website here

<http://www.fararopaya.com/ProductItem-48.html>

Engineer:

So if an employee connects an infected computer with RS232 to your drives, could Stuxnet attack to it?

CEO:

Why an employee must do something like this?

Engineer:

For example for Update Reasons

CEO:

No ,Only Fararo paya’s Engineers could update our Drives

Anyone who use our products have to use our user interface for changing settings

In fact KFC750 no need to any external device for working with centrifuges, Keep it in your mind.

The Interview

Engineer:

Fine !

Do you think Busher was target of the Stuxnet ?

CEO:

Technically No

Engineer:

Why Not ?

CEO:

Because busher is just a Nuclear plant, I know there is no Drive or centrifuges there so technically I can't accept this

Engineer:

Oh , thanks

Can I ask you something ?

CEO:

Yes

The Interview

Engineer:

Have you any hidden activity from IAEA ?

CEO:

Who told you this?

Engineer:

I read it form Fox news find out here

<http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/>

News reporter wrote

“What surprises experts at this step is that the Iranian company was so secret that not even the IAEA knew about it”

Is this true ?

CEO:

Look we always registered our products to Ni.com

Engineer:

What is Ni.com?

CEO:

The National Instruments web site. We have even some certification from!
Any corporation have to register own product there.

The Interview

Engineer:

Really?

CEO:

Yes of course, any corporation needs to had activity in power plants must submit their product there. It is something like a computer certification and it is proved the capability of the Device Producer or Factory.

Engineer:

Well, thank you for all questions and answers and Thanks for your time

CEO:

Thanks for having me

Note: all of information we said here is available on Fararo Paya's web site anyone can find out there

<http://www.fararopaya.com>

The International Conferences

The International Conferences

I went to Security Conferences for Stuxnet, Black hat 2010 Abu Dhabi and Info sec event in Iran, one for a normal person and the other as Security Speaker about Stuxnet.

The Black hat Abu Dhabi Conference was Great, I had some conversation with technology Professionals and information Security Researcher about Stuxnet for example with Tom Parker Stuxnet's Security Researcher and Dan Kaminsky in black hat Abu Dhabi. In fact Mr. Parker and "Jonathan Pollet" had Briefing on Black hat Abu Dhabi 2010

<http://www.blackhat.com/html/bh-ad-10/bh-ad-10-archives.html>

http://www.blackhat.com/html/bh-ad-10/bh-ad-10-speaker_bios.html#Parker

Also during his presentation Mr. Parker said that whoever did write it failed in one respect because Stuxnet has not stayed live for as long as its creators hoped.

After presentation Tom asked me about his Conference Quality and I told him it was impressive.

<http://www.glasgowwired.co.uk/news.php/109371-Code-clues-point-to-Stuxnet-maker>

That conference it was very good for me because I received cool review from the top.

The International Conferences



Jeff Moss CEO of the Black hat, me - Tom Parker in Black Hat Abu Dhabi 2010

The International Conferences

The Info Sec event Conference in Iran

<http://www.infosecevent.com>

In this Security conference I had article about Stuxnet Activity in Iran for many Iranian technology leaders.

We have many people who came for power plants. Only one administrator from one power plant admit Stuxnet infection on their network.

In this conference I demonstrate my tool “Venak and Avenak” to defeat with Stuxnet and how Venak could detect and Remove Stuxnet Simply. Also we released the New Version of the Venak and Avenak Seven Edition and Demonstrate the Future of the Next Stuxnet. www.u0vd.org



آشنایی با سخنران

نیمه باقری

دانش آموخته MCSD ، MCSE ، CEH ، CSISSP ، A+ ، CCNA

- طراح سیستم های امنیتی آنتی ویروس ، مشاوره امنیتی شبکه ها ، مدرس امنیتی
- ۷ سال تجربه برنامه نویسی ، ۵ سال مشاوره امنیتی ، طراح محصولات امنیتی

عنوان سخنرانی

تجارت سیاه استاکس نت

The black business of Stuxnet

شرح کوتاهی از موضوع سخنرانی

در این مقاله بررسی کاملی نسبت به فعالیت ویروس استاکس نت خواهیم داشت

تاریخچه فعالیت استاکس نت / بررسی تاریخ فعالیت این کرم اینترنتی و اینکه چه زمانی طراحی و تولید شده و چه اهدافی را برای فعالیت خود دنبال می کرده. نحوه فعالیت استاکس نت/ بررسی تکنیک های این ویروس شامل: نحوه انتشار و انتقال بررسی تکنیک های روتکیت این ویروس/ بررسی استفاده این ویروس از ابراد های امنیتی بچ نشده استاکس نت/ بررسی کد های پنهان در استاکس نت/ چگونگی کشف و پاکسازی/ تشریح روش های کشف و پاکسازی با استفاده از وناک و آوناک/ تشریح روش های کشف روتکیت ها به واسطه وناک و آوناک/ استاکس نت ها آینده/ تهدیدات آینده چگونه خواهند بود/ راه کارهای ما برای مقابله/ بررسی تجارت سیاه رایانه ای

The International Conferences



The International Conferences




The International Conferences



Review The International News

Review The International News

So we want review some International News about Stuxnet Activity in Iran.



Stuxnet worm hits the black market

Oh my God... the terrorists have it!

25 November, 2010


[comment](#) [print](#) [favourite](#)

News that the source code of the Stuxnet worm has been traded on the black market has some of the UK's biggest news outlets in a bit of a lather.

The malware, which is widely suspected to have been developed by a nation state, and was almost certainly deliberately targeted at Iran's fledgeling nuclear industry, has fallen into the hands of criminal gangs, according to a characteristically shrill new report on Sky News.

The report quotes 'senior security figures' who warn that the virus could be used to "attack any physical target which relies on computers."

Adding to the hysteria, Will Gilpin who apparently advises the Government on security matters, adds, "You could shut down the police 999 system. You could shut down hospital systems and equipment. You could shut down power stations, you could shut down the transport network across the United Kingdom."



Written by
Stewart Meagher

Stewart had over 20 years of experience in the print publishing industry working at the bleeding edge of technology before deciding that this new-fangled interweb thingummybob was the way forward for a jaded middle-aged hack ...

[view bio](#) [follow](#)

[Would you like to write for us?](#)

Subscribe to THINQ Newsletter

☒ Subscribe and accept [Terms and Conditions](#)

Editor's Choice

- [Segway boss dies in cliff-top fall... on a Segway](#)
- [UK music calls for truce with technology](#)
- [Facebook worm attacks Windows, Mac and Linux](#)
- [Microsoft predicts Blu-ray's demise](#)
- [US demands tougher internet spying powers](#)

Breaking News

Google-branded Chrome netbooks coming in weeks

1 hour ago, 26 Nov 2010

Mario Andretti gets a name-check

High Court rules newspapers can charge for links

1 hour ago, 26 Nov 2010

Bad news for aggregators

Review The International News

TECHNOLOGY

Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions

By Ed Barnes

Published November 26, 2010 | FoxNews.com

Print Email Share Comments (817) Recommend 33K Text Size



AP

An aerial view of Iran's nuclear facility in Natanz.

In the 20th century, this would have been a job for James Bond.

The mission: Infiltrate the highly advanced, securely guarded enemy headquarters where scientists in the clutches of an evil master are secretly building a weapon that can destroy the world. Then render that weapon harmless and escape undetected.

But in the 21st century, Bond doesn't get the call. Instead, the job is handled by a suave and very sophisticated secret computer worm, a jumble of code called Stuxnet, which in the last year

Ads by Adblade™



50% OFF

\$49 Air From Chicago?

It's true: Airfare from only \$49. Get the Top 25 weekly deals email & Save up to 70% on travel! [Learn more](#)



SHOCKING: iPads for \$109?

Special Report: we discover how iPads are being sold for an amazing 80% off retail! [Learn more](#)



Illinois Job Scam?

We investigated work at home job opportunities and what we found may shock you... [Learn more](#)



Strange Fruit Burns Fat

Lose 12.3 pounds and 2 inches of belly fat every 28 days - without diet or exercise. [Learn more](#)



Chicago: Job Scam Report

We investigated work at home jobs and what we found will shock you... [Learn more](#)

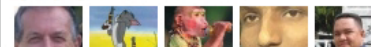
[Add Your Link Here!](#)



Fox News SciTech on Facebook



4,371 people like Fox News SciTech



But as the extent of the worm's capabilities is being understood, its genius and complexity has created another perplexing question: Who did it?

Speculation on the worm's origin initially focused on hackers or even companies trying to disrupt competitors. But as engineers tore apart the virus they learned not only the depth of the code, its complex targeting mechanism, (despite infecting more than 100,000 computers it has only done damage at Natanz,) the enormous amount of work that went into it—Microsoft estimated that it consumed 10,000 man days of labor-- and about what the worm knew, the clues narrowed the number of players that have the capabilities to create it to a handful.

Sponsored Links Buy a link here

TODAY: 97% Off iPads

Auction Site Is Selling 1,000 Brand New iPads For \$17.87
www.DailyDigestReports.com

Bonati Spine Institute

Where Laser Spine Surgery Began

"This is what nation-states build, if their only other option would be to go to war," Joseph Wouk, an Israeli security expert wrote.

Byres is more certain. "It is a military weapon," he said.

And much of what the worm "knew" could only have come from a consortium of Western intelligence agencies, experts who have examined the code now believe.

100,000 Computers?

False, First because Stuxnet can't damage any computer, Stuxnet could infect a computer and could Damage the Drive and in best timing could damage centrifuges. (In fact if the drive connected to PC with Rs232 port)

False, the biggest Power plant in Iran has under 1000 computers or their network!

False, we have not even 50,000 IT Professional in Iran as administrator or network scientist!

100,000 computers at lease needs a 30Megawatt power plant for it, how Natanz engineer want prepare this energy for their network?

—Once allowed entry, the worm contained four “Zero Day” elements in its first target, the Windows 7 operating system that controlled the overall operation of the plant. Zero Day elements are rare and extremely valuable vulnerabilities in a computer system that can be exploited only once. Two of the vulnerabilities were known, but the other two had never been discovered. Experts say no hacker would waste Zero Days in that manner.

—After penetrating the Windows operating system, the code then targeted the Siemens operating system that controlled the plant. Once that was in its grip it then took over the “frequency converters” that ran the centrifuges. To do that it used specifications from the manufacturers of the converters. One was Vacon, a Finnish Company, and the other Fararo Paya, an Iranian company. What surprises experts at this step is that the Iranian company was so secret that not even the IAEA knew about it.

—The worm also knew that the complex control system that ran the centrifuges was built by Siemens, the German manufacturer, and — remarkably — how that system worked as well and how to mask its activities from it.

Ancient 8
Pussycat

get th
AT&T U-V

Fararo Paya’s CEO confirm he had Submit his Devices in “The National Instruments” web site and also he received some certificate form that website for his company.

Is this hidden activity form someone or somewhere ?

Internet Archive Wayback Machine - Windows Internet Explorer

http://web.archive.org/web/*/http://www.fararo.com

File Edit View Favorites Tools Help

Internet Archive Wayback Machine

WayBackMachine

Enter Web Address: All [Adv. Search](#) [Compare Archive Pages](#)

Searched for <http://www.fararo.com> 29 Results

Note some duplicates are not shown. [See all](#).
 * denotes when site was updated.
 Material typically becomes available here 6 months or more after collection, with some exceptions [See FAQ](#).

Archived Results from Jan 01, 1996 - latest

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
0 pages	0 pages	0 pages	0 pages	0 pages	0 pages	4 pages	16 pages	0 pages	0 pages	0 pages	3 pages	5 pages	0 pages	0 pages
						Mar 28, 2002 * May 27, 2002 Jun 05, 2002 Dec 17, 2002	Feb 10, 2003 * Feb 11, 2003 Feb 16, 2003 Apr 19, 2003 * Apr 24, 2003 Jun 01, 2003 Jun 19, 2003 Jul 17, 2003 Aug 02, 2003 Sep 21, 2003 Oct 09, 2003 Oct 13, 2003 Oct 19, 2003 Nov 22, 2003 Nov 28, 2003 Nov 30, 2003			May 05, 2007 * Aug 26, 2007 Oct 19, 2007	Feb 22, 2008 Mar 10, 2008 Apr 09, 2008 Apr 30, 2008 May 30, 2008			

[Home](#) | [Help](#)

The Fararo Paya's web Archive ,for more Please visit
www.archive.org

Review The International News

[Home](#) [US & Canada](#) [Latin America](#) [UK](#) [Africa](#) [Asia-Pac](#) [Europe](#) [Mid-East](#) [South Asia](#) [Business](#) [Health](#) [Sci/Environment](#) [Tech](#) [Entertainment](#) [Video](#)

19 November 2010 Last updated at 07:07 ET

Code clues point to Stuxnet maker

By Mark Ward

Technology correspondent, BBC News

Detailed analysis of the code in the Stuxnet worm has narrowed the list of suspects who could have created it.

The sophisticated malware is among the first to target the industrial equipment used in power plants and other large scale installations.

New research suggests it was designed to disrupt centrifuges often used to enrich uranium.

Detailed analysis of the worm has revealed more about the team behind it and what it was supposed to do.

Code secrets

The close look at the code inside Stuxnet was carried out by [Tom Parker](#) from security firm Securicon who specialises in picking out the digital fingerprints hackers leave behind in malware.

His analysis of Stuxnet shows it is made of several distinct blocks. One part targets industrial control systems, another handles the worm's methods of spreading itself and another concerns the way its creators planned to communicate with and control it.

The most sophisticated part of Stuxnet targeted the Programmable Logic Controllers used in industrial plants to automate the operation of components such as motors or pumps.

Subverting PLCs required detailed knowledge of one manufacturer's



Stuxnet seems to have been designed to target uranium enrichment systems

Related stories

[Iran makes 'nuclear spy' arrests](#)

['Virus targeted Iranian assets'](#)

[Two million US PCs hijacked](#)

Top Stories



[N Korea warns South on war drills](#)

[Passive smoking 'kills 600,000'](#)

[Black Friday bargains go on sale](#)

[UK blamed over Taliban impostor](#)

[Year reaches record temperatures](#)

Features & Analysis



Trump card

The man and the brand - the secret of Donald Trump's success



Gherkin, Shard, Armadillo

Why do tall buildings have such silly names?



'Don't divide us'

The gay newlyweds fighting deportation from the US



It's quiz time!

And just who has been feted as the 'real man'?

Most Popular

[Shared](#) [Read](#) [Watched/Listened](#)

[N Korea warns South on war drills](#)

Research by security firm Symantec has shown that the likely target were frequency controllers that many PLCs are hooked up to in order to regulate a motor.

In particular, said Symantec, Stuxnet targeted those operating at frequencies between 807 and 1210Hz.

"There's a limited amount of equipment operating at that speed," said Orla Cox, security operations manager at Symantec. "It knew exactly what it was going after."

"Those operating at 600hz or above are regulated for export by the US because they can be used to control centrifuges for uranium enrichment," she said.

If Stuxnet did manage to infect a PLC connected to a centrifuge, it would seriously disrupt its working, said Ms Cox.

What is not clear, said Ms Cox, is whether Stuxnet hit its target. If it did not, she said, then the fact that the command and control system has been taken over by security firms has ended any chance of it being used again.

"Our expectation is that the attack is done at this point," she said. "We've not seen any more variants out there and I don't suspect we will."

Mr Parker said that whoever did write it failed in one respect because Stuxnet has not stayed live for as long as its creators hoped.

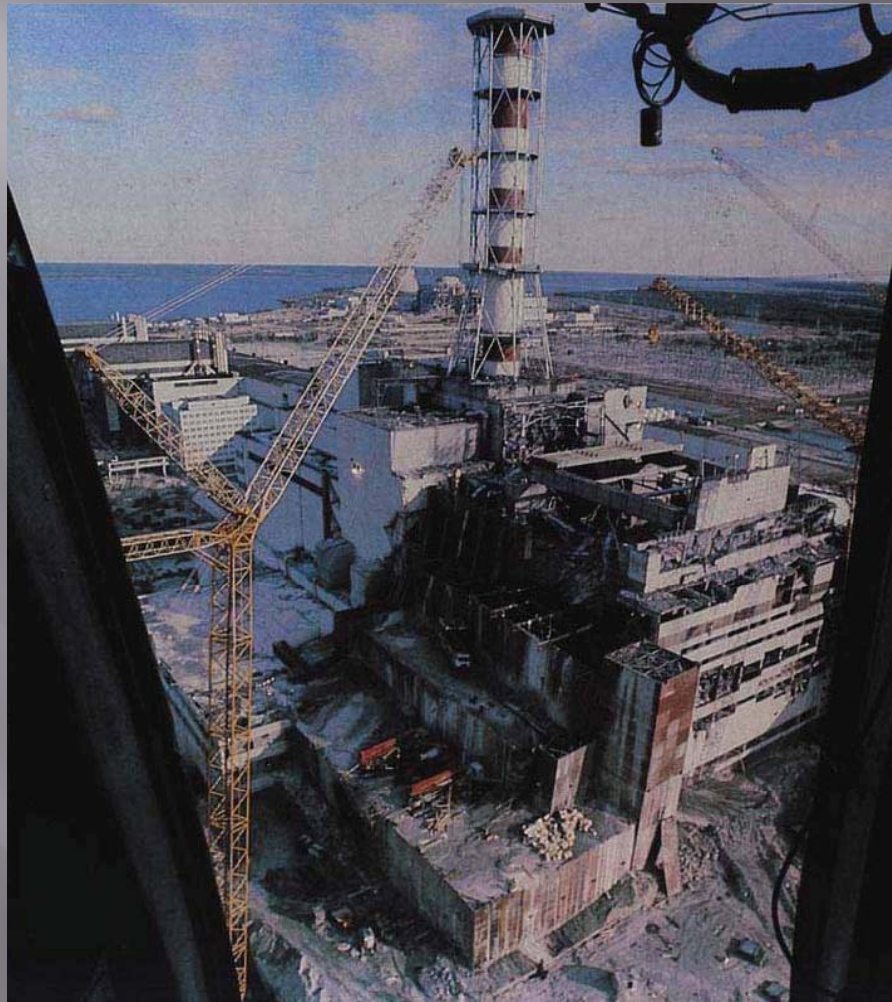
The control system set up needed to have been in place for years to have a seriously disruptive effect on its intended targets, he said.

Fararo Paya's CEO confirm
their engineers never set
that rang for their
drives.

Also Tom Parker confirm
the Stuxnet writers
failed.

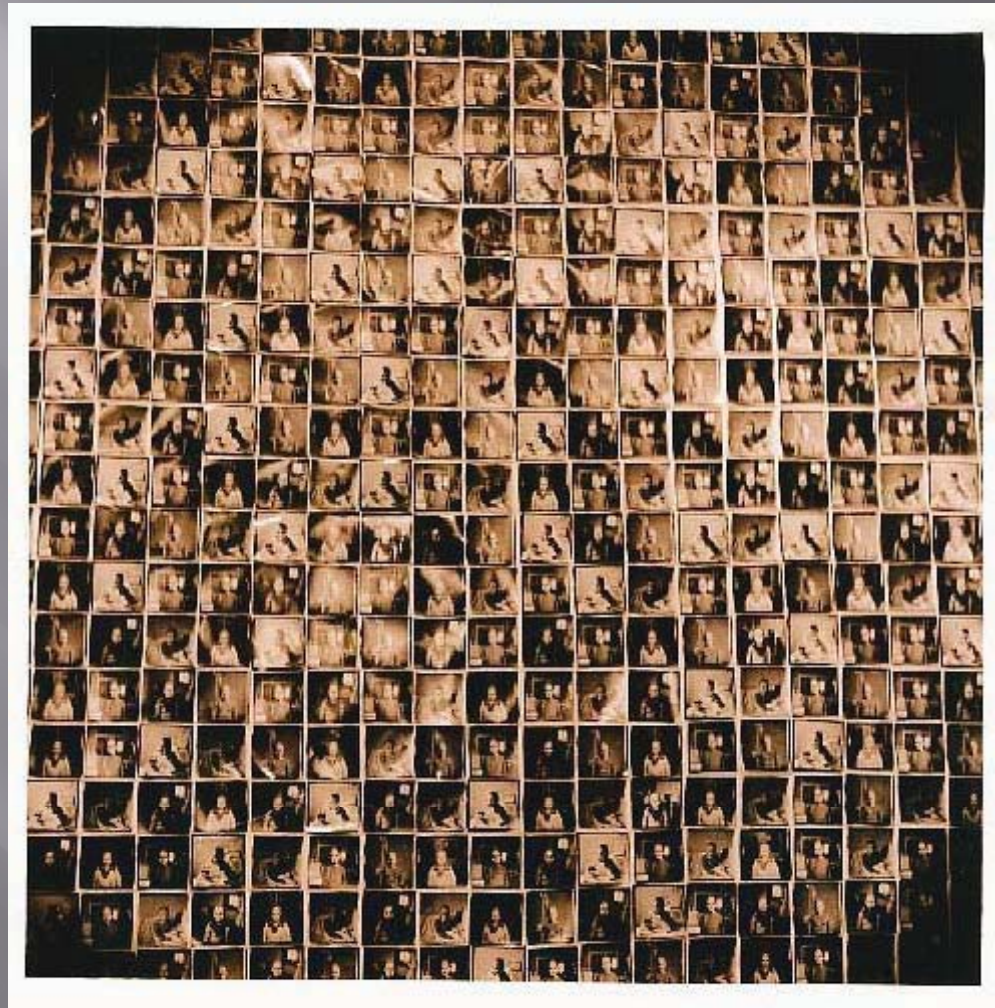
Stuxnet Goals (if had Success)

Stuxnet Goals (if had Success)



The Chernobyl disaster was a well-known nuclear accident of catastrophic proportions that occurred on 26 April 1986

Stuxnet Goals (if had Success)



this is a wall of over 600 images of children suffering from thyroid cancer , they were taken in hospitals in belarus which was hit the hardest after the chernobyl disaster

The Final Results of this Article

- ▣ I have been following the story of the Stuxnet worm in whole past months. As you know, Stuxnet worm was designed to attack Iranian nuclear operations to create problems for it but as a security researcher in Iran I'm sure the Stuxnet had failed to do it's own operation.
- ▣ I think the News and Internet Media's try to release about Stuxnet's success attack on IRAN's Peace Atomic Program, but something did not happened any way.
- ▣ This is my Final Research about Stuxnet Activity in IRAN.

My Advice

My Advice

- ▣ Living with No Drinks , No Hack and No \$ex.
- ▣ Using Internet for spreading peace purposes and always respect to any human with any skin color and any nation.
- ▣ Using technology to upgrade people education because I believe it is only thing could help the world.
- ▣ At last I want confirm the person of the year (2010) in technology ,
- ▣ Yes Mr. "Steve Jobs".
- ▣ Sorry mark but when you did figure that capability on your facebook as we called "Download patch for your stupidity" (in fact Kevin Mitnick is Author of it not me) you're lost the person of the year Honor!
Please change that shame privacy on your facebook. It's real Security leak for all facebook users and whole world. Mark ,I love you as a normal person but with Maximum of Respect I have to tell you, you're a Great Villain !

The New facebook's Capability "Facebook Internet IDs" !! Mark Did you sold user's information to any Company ? , Answer is Yes , ohhhh too Bad !

We Are Peace, Always

