Cyber-Attack on Worldwide Nuclear Facilities

POSTED IN HACKING ON OCTOBER 12, 2015

SHARE

SKILLSET What's this?

Access Control

Incident Response

Malware

MITM Network Security

Critical infrastructure under attack

The protection of critical infrastructure is a pillar of the cyber security strategy of any government. Cybercriminal, hacktivists, state-sponsored hackers, and cyber terrorists can hit anyone, anytime, in any place.

Civil nuclear facilities across the world are privileged targets for cyber-attacks; an incident in this infrastructure could cause serious damage representing a major threat for the population.

The Stuxnet attack that targeted Iranian nuclear facility in Natanz demonstrated the risks for cyberattacks, for the first time the security industry observed the effects of a cyber weapon, for the first time military a threat from the cyberspace cause real damages in a real world scenario.

According to the report "Cyber Security at Civil Nuclear Facilities Understanding the Risks" recently published by the Chatham House and based on an 18-month study that focuses cybersecurity at civil nuclear facilities, the nuclear industry is falling behind other industries when facing cyber security.

"The nuclear industry is beginning – but struggling – to come to grips with this new, insidious threat," said Patricia Lewis, research director of Chatham House's international security programme.

The researchers at the Chatham House have interviewed 30 industry practitioners, academics and policymakers from the U.K., Canada, the U.S., Ukraine, Russia, France, Germany and Japan.

Cyber threats are becoming even more sophisticated and attackers can exploit new attack vectors, for this reason it is important to assume the proper security posture in order to mitigate the risk of exposure.

"Cyber criminals, state-sponsored hackers and terrorists were all increasing their online activity, it said, meaning that the risk of a significant net-based attack was "ever present". Such an attack on a nuclear plant, even if small-scale or unlikely, needed to be taken seriously because of the harm that would follow if radiation

were released," states the BBC.

Modern civil nuclear facilities make great use of technology, SCADA systems and industrial control systems (ICSs) represent the core of the critical infrastructure, but at same time, they could be the entry points for an attacker. Most of ICSs are affected by numerous vulnerabilities that could be exploited by threat actors to target the infrastructure causing serious damage.

Unfortunately, many experts consider the threat of a major cyber-attack a low risk because critical components in nuclear facilities are air gapped (i.e. isolated from the Internet), but the report published by the Chatham House confirmed that this is a wrong.

"However, it said, this so-called "air gap" between the public internet and nuclear systems was easy to breach with "nothing more than a flash drive". It noted that the destructive Stuxnet computer virus infected Iran's nuclear facilities via this route," continues the BBC.

The report highlights the gap between the physical and logical security of nuclear facilities, while nuclear plants worldwide have reached a high level of physical security and safety; they are still too exposed to the cyber-threats.

Internal staff is often not prepared to defend the assets in the nuclear facilities, its training is essential to repel cyber-attacks. At the first international conference organized by the International Atomic Energy Agency in June, Yukiya Amano, director of the IAEA, said both random and targeted attacks were being directed at nuclear plants.

"Staff responsible for nuclear security should know how to repel cyber-attacks and to limit the damage if systems are actually penetrated,"
Amano said in a keynote

The study has found that in many nuclear facilities, the systems are accessible via virtual private networks (VPN), but some cases operators might not be aware of their existence.

When dealing with technical challenges, the Chatham House study names the "insecurity by design" of industrial control systems, highlighting the difficulties in patching vulnerable systems.

A patch could cause serious compatibility issues and in the worst scenarios, the deployment could result in downtime and compromise the operation of the entire facility.

"The nuclear industry as a whole needs to develop a more robust ambition to take the initiative in cyberspace and to fund the promotion and fostering of a culture of cyber security, determining investment priorities and ensuring that sufficient and sustained funding is allocated to effective responses to the challenge. It also needs to establish an international cyber security risk management strategy and encourage the free flow of information between all stakeholders," Chatham House said in its report. *"This will require the industry to develop appropriate mechanisms and coordinated plans of action to address the technical shortfalls identified, as well as to find the right balance between regulation and personal responsibility."*

One of the principal challenges for any industry is the risk assessment that often may be inadequate. Underestimating the risks is a serious issue that could expose the infrastructure to major attacks; one of the principal effects is that a wrong perception of the cyber threat can induce a wrong evaluation of expenditure in defense measures against it. It is crucial to be able to accurately assess and measure the risks in order to have the requested funds and the commitment of executives.

Experts in the nuclear industry need to develop guidelines to measure cyber security risks taking into account security and safety measures. The process must involve CEOs and company boards to improve the action to mitigate the cyber threats.

The information presented in this post demonstrates the reluctance of the nuclear industry to disclose cyber incidents and share information.

It is not easy to disclose an incident; in many cases, the threats go undetected for a long period of time. In other cases, they will never be uncovered, for this reason, the perception of the risks related to a major cyber-attack is low and the hack of an ISC system is wrongly considered a rare event.

According to the study of Chatham House, the lack of cyber security policies, procedures and training makes the situation worse, the operators of nuclear facilities are not prepared to detect and respond to cyber-attacks.

Many operators in the industry do not believe that cyber security poses a real risk to the nuclear plants.

The development of guidelines could allow the measurement of cyber security risks in the nuclear industry, increasing the awareness of the cyber threats among the sector.

Risks must be calculated with a great accuracy based on metrics shared in the industry and globally accepted.

Another serious problem affecting the nuclear industry is the difficult communication between the nuclear plant personnel (OT engineers) and cyber security personnel (IT engineers). The report highlights the importance of cyber security personnel to garrison the nuclear facilities having on a regular basis meeting with OT engineers.

OT engineers have to report any activity has been conducted at the equipment and any suspicious activity they have noticed. Every modification to one of the components in the nuclear facility could potentially open the doors to cyber threats, so the IT engineers have to monitor carefully the “evolution” of the plant.

Face-to-face contact between IT engineers and IT personnel is a key factor to sustain mutual understanding between the two cultures so close, but so different.

Both categories of professionals might be involved in working together on joint vulnerability analyses or risk assessments.

Every component could be an open door for hackers

The increasing number of incidents occurring in the last years demonstrated that a cyber-attack could cause serious damage to industrial processes. Hackers can find and exploit any vulnerability in one of the numerous components of the targeted plant in order to paralyze any process with unpredictable consequences.

A research conducted a few months ago revealed some vulnerabilities in the Industrial Ethernet Switches (IES), which could be exploited by the hackers to gain an access to Nuclear Power Plants or the Hydroelectric Dams.

A team of security researchers presented the details of their study on the Industrial Ethernet Switches at the last Black Hat conference in Las Vegas.

The team of researchers conducted a study funded by the IOActive security firm, the work is a joint effort of Robert Lee, a security researcher and active-duty U.S. Air Force Cyber Warfare Operations Officer, risk researcher Eireann Leverett, and IOActive security consultant Colin Cassidy.

The group focused its analysis on the Industrial Ethernet Switches (IES) with the support of at least four industrial switch vendors, including Siemens, General

Electric, Opengear, and Garrettcom.

The existence of security vulnerabilities affecting industrial Ethernet switches can have serious consequences for the security of critical infrastructure.

Industrial Ethernet Switches are essential components of industrial processes, they are used to connect the various devices in civil nuclear plants, power plants, hydroelectric dams, refineries, ports, and other critical infrastructure.

The security researchers have proved the presence of numerous vulnerabilities in the Industrial Ethernet Switches; the flaws include the use of default passwords, hard-coded encryption keys and lack of proper authentication for firmware updates.

The hole discovered by the team of researchers together expose critical systems to serious threats and represent the "fundamental failures of security." *"Anything that the facility is capable of in its natural operating system, you're [an attacker] capable of doing—and doing damage with if you control the network,"* Robert Lee told the Daily Dot. *"With a power station, you can have major repercussions. With a hydroelectric dam, if you don't monitor processes in a normal situation, it'll spin out of control. Everything you have can be manipulated."*

"Compromising any switch allows the creation of malicious firmwares for further MITM manipulation of a live process. Such MITM manipulation can lead to the plant or process shutting down (think: nuclear reactor SCRAM) or getting into an unknown and hazardous state (think: damaging a blast furnace at a steel mill)," the researchers explained.

The security experts involved in the study explained that one of the major security problems for any industry is the lack of awareness of cyber threats and of a proper security posture, the presence of outdated technology demonstrates the low perception of cyber security risks.

Outdated systems don't allow operators for implementing reliable maintenance processes based on the distribution of validated and legitimate firmware updates.

"All these vulnerabilities are pervasive and endemic. Most vendors haven't done the basics." Mainly so because the equipment used in the facilities are all outdated because they were installed during the time when cyber-security had not advanced, on the contrary the threats posed today were not present in the list of cyber security," explained Leverett.

The only way to prevent further attacks is to share information on cyber-threats and assess computer systems searching for vulnerabilities exploitable by threat actors.

Hackers targeting nuclear facilities

It is not difficult to collect information publicly available online related the activities of a group of hackers that with different motivations tried to hack ISCs systems in nuclear plants of target organizations managing sensitive data of the nuclear industry.

Last year, the U.S. Nuclear Regulatory Commission (NRC) revealed to have suffered cyber-attacks three times during the past three years, threat actors targeted the personnel of the organization with spear phishing attacks to compromise the internal network of the organization and to harvest log-in credentials.

The Nuclear Regulatory Commission (NRC) is a critical organization for the US nuclear industry because it maintains detailed information about nuclear reactors, waste storage facilities and uranium processing plants across the United States. It is considered by state-sponsored hackers a privileged target, and the attacks discovered by the IT personnel of the organization for foreign hackers demonstrate it.

According to the NextGov in all the attacks were involved state-sponsored hackers, but the agency hasn't provided the name of the Government behind the cyber operations.

Two hundred fifteen employees of the Nuclear Regulatory Commission were targeted by cyber-attacks; victims were infected by clicking on a malicious link included in phishing emails. The malicious emails baited the U.S. Nuclear Regulatory Commission by requesting them to verify their user accounts by clicking a link and logging in, the link really took the victims to a Google Docs spreadsheet.

The report accessed by Nextgov reveals that the IG Cyber Crime Unit was able to "track the person who set up the spreadsheet to a foreign country," without providing further info on its country.

In a second attack, state sponsored hackers served a malware in a spear phishing attack, this time the malicious link embedded in the emails linked back to a Microsoft OneDrive storage folder that hosted a malware.

"Hackers also attacked commission employees with targeted spear

phishing emails that linked to malicious software. A URL embedded in the emails connected to "a cloud-based Microsoft Skydrive storage site," which housed the malware," investigators wrote. *"There was one incident of compromise and the investigation tracked the sender to a foreign country." Again, the country is not named.* "states the post published by the NextGov.

The third attack was quite different because the bad actors have compromised the personal email account of an employee at the Nuclear Regulatory Commission to serve the malware to 16 people in the victim' contact list. The malware was injected through a PDF attachment that contained a JavaScript exploits.

Unfortunately, it's not the first time that state-sponsored hackers target the Nuclear Regulatory Commission, in the past Sen. Tom Coburn, M.D. (R-Okla.) reported that the NRC has stored sensitive details about nuclear plants without implementing proper defensive measures.

Curious that a report on cyber security on the Nuclear Regulatory Commission issued by the OIG considered the agency suitable for securing nuclear power plants in the case of a major cyberattack avoiding to make any recommendations to the agency.

In March 2015, the Government of Seoul has issued a report blaming North Korea for cyber-attacks against computers at Korea Hydro and Nuclear Power (KHNP), a subsidiary of the Korea Electric Power Corporation (KEPCO) that operates 23 nuclear reactors and many hydroelectric plants in South Korea.

South Korean authorities reported that hackers compromised the internal network of the company and have stolen data from its systems, but according to the government only "non-critical" networks were affected. Stolen data also included set of technical data and documents on reactor design.

In this case, the attacks had serious consequences on the operation of plants, the company shutdown three reactors after the hack.

Figure 1 – South Korean critical infrastructure

The report published by the Chatham House includes also a list of "known cyber security incidents at nuclear facilities" occurred between 1992 and 2014:

- **At Ignalina nuclear power plant (1992)** in Lithuania, a technician intentionally introduced a virus into the industrial control system, which he claimed was "to highlight cyber security vulnerabilities".
- The **Davis-Besse nuclear power plant (2003)** in Ohio was infected by the Slammer worm, which disabled a safety monitoring system for almost five hours.
- The **Browns Ferry nuclear power plant (2006)** in Alabama experienced a malfunction of both the reactor recirculation pumps and the condensate deminerliser controller (a type of PLC).
- The **Hatch nuclear power plant (2008)** was shut down as an unintended consequence of a contractor's software update.
- An **Unnamed Russian nuclear power plant (circa 2010)** was revealed by Eugene Kaspersky to have been "badly infected by Stuxnet".
- **South Korea's Korea Hydro and Nuclear Power Co. commercial network (2014)** was breached, and information was stolen. The attack was subsequently attributed to North Korea.

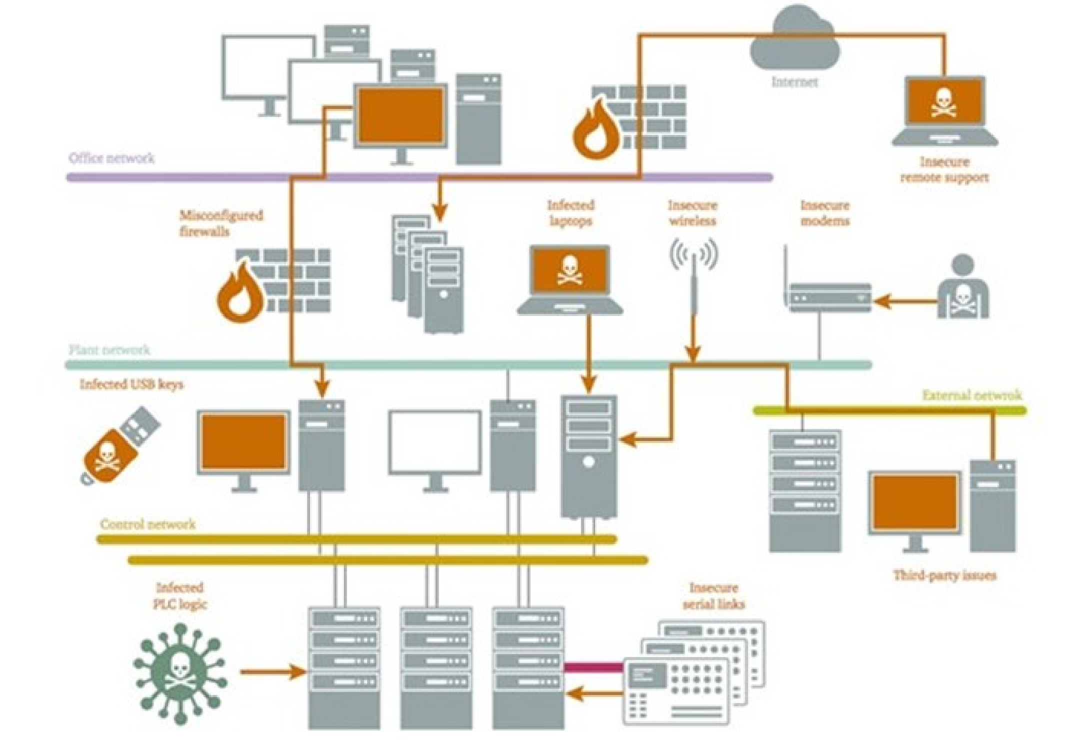
Exception or false sense of security?

While the study from Chatham House states that underestimating the risk of cyber-attacks against civil nuclear facilities could be a serious error, some organizations in industry replied that they are making significant investment in cyber security.

The UK's nuclear industry, for example, has already made significant moves to protect its infrastructure to cyber-attacks.

"This threat has already been considered in many of the stations in the UK," Ian Bonnett, director of Davies Nuclear Associates — an energy consultancy firm — told WIRED.

"I don't see this as a serious threat for the UK nuclear industry."



Source: Eric Byres, Byres Security.

Figure 2 – Diagram from the report showing potential control system vulnerabilities

The combination of a "very good" Office of Nuclear Regulation, a "continuous self-questioning," and a "goal-setting approach to regulation," makes the UK nuclear industry a global leader in terms of cybersecurity defense,

Bonnett explained that the effort of the Office of Nuclear Regulation in continuously improving cyber security of civil nuclear facilities and a "goal-setting approach to regulation," are making the UK nuclear industry one of the most active in approaching cyber security.

Bonnett added that British nuclear facilities are not so easy to hack because the adoption of hard-wired, independent control systems.

"There are easier industries to go after than the nuclear industry," said Bonnett.

"There are a lot more attacks on the finance sector and retail sector than the more industrial sectors."

In response to the study conducted by the Chatham House, the Department of Energy and Climate Change (DECC) said it takes cyber threats seriously and is taking all the necessary countermeasures to improve cyber security of the UK's nuclear facilities.

"We take the security of the UK's nuclear sites extremely seriously, which is why the government has a National Cyber Security Programme in place to keep our national infrastructure sites secure," a spokesperson from the DECC told WIRED. *"The UK's independent regulator also has strict regulations in place that protect our nuclear sites."*

"Cyber risks are always developing and no one can afford to be complacent," a spokesperson for the regulator explained. *"In addition to our robust inspection regime, the Office of Nuclear Regulation is constantly reinforcing the importance of cyber security to senior figures across the UK nuclear industry."*

"We agree with the Chatham House report that significant attention must be paid to these issues now and in future," the spokesperson added.

Resuming the operators of the UK nuclear industry are confident about the good cyber security level implemented by the operators of the facilities in the plant.

What about the US?

Let me share with you an excerpt of an interview that Bruce McConnell, co-authored of the "A Measure of Restraint in Cyberspace: Reducing Risk to Civilian Nuclear Assets" for the EastWest Institute, released to the Global Security Newswire.

McConnell confirmed that there are plausible indications that terrorists seek to hack nuclear facilities.

GSN: How vulnerable are U.S. nuclear power plants to cyber-attacks? And what about facilities worldwide?

McConnell: The answer is somewhat counterintuitive. In general, what we find is that the United States tends to be an early adopter in terms of using information technology in industrial control systems and industrial applications. … The source of vulnerability is related to how much of the nuclear operation is connected and dependent upon IT. So, if you have older facilities that are less connected and … located somewhere where there is less aggressive use of IT in industrial spaces … they may be less vulnerable.

The probability of release of radioactive material through a combined physical cyber-attack is relatively low. Therefore, we try not to join the chorus of hype here and say, "The sky is falling," because it's actually pretty hard to have a release of radioactive material. Therefore, it's a low-probability event. It's almost impossible, I think, just through cyber; you'd have to add some physical aspect to it.

I would say that neither U.S. nor European [nor] other foreign nuclear facilities are particularly vulnerable from the standpoint of a dire release of radioactivity. However, if you think about the risk — a function of threat, vulnerability and consequences — in this case it's the consequences that make the risk higher, not so much the vulnerability. Although vulnerabilities exist, and there are people, obviously, and threats who would like to take advantage of them.

GSN: What determines the degree to which nuclear facilities are at risk of cyber-attacks?

McConnell: There are two ways of attack. One way is through the business systems, which are generally connected to the Internet. Therefore, the example here would be the Saudi Aramco attack. It was a scare. We've seen other cases where business systems have been used to get into operational systems, which have been less well publicized.

In the old days, there was a rule in the utility industry never to connect your business systems to your control systems, because of just that problem. Moreover, this was even before the Internet. However, economics has [changed] that, and now you can do maintenance remotely … and save a lot of money and be more efficient. Nevertheless, you also introduce more vulnerability. It's the connection to the business system, in general, that opens up a whole host of generic vulnerabilities that create the potential for havoc.

The other way is what we saw in Stuxnet, which is where the control systems were not connected to the outside world. So, there the malware was introduced through — and we don't know the details — a combination of physical means, maybe a thumb drive, and very sophisticated … techniques that allow you to get in that way. …

That was a more cumbersome process. The kind of physical way of doing it, whether it's through a thumb drive or somebody on the inside, takes more art form, a more sophisticated, better-resourced attacker. However, it's also a possibility.

Which are the security measures in place in US?

According to the Nuclear Energy Institute, nuclear power plants in the US share the adoption of the following measures to ensure the protection against cyber-attacks:

- Isolation of the key control systems in the facility deploying them in air gapped network or installing robust hardware-based isolation devices that are able to ensure the separation of front-office computers from the control system. This measure will ensure that key components in the plants are protected from any network-based cyber-attacks from outside sources.

- Enhancement and implementation of a capillary control over portable media and equipment. Security policies in place to restrict the use of portable assets to the performance of a specific task in order to ensure the protection of air-gapped networks.
- Monitoring of internal personnel with an accurate screening and behavioral observation in order to mitigate insider threats. Training of the internal personnel.
- Implementations of cyber security controls to protect critical components.
- Adoption of measures to maintain effective cyber protection, including the implementation of a plant configuration management program.

t in a

Conclusions

Cyber-attacks represent a serious threat for the physical and logical security of a nuclear facility, information gathered by attackers could allow them to breach systems in a nuclear plant or bypass physical security measures in place to protect the critical infrastructure.

As highlighted by McConnell it is crucial the support of a national regulator and huge investment by governments in order to protect critical infrastructure.

Firms in the nuclear industry are proactive and are operating responsibly to mitigate cyber threats, but it is necessary a joint effort to avoid incidents.

"No individual firm can afford to make the investments to protect against a seriously well-funded attacker." States McConnell. *"In general, investment among companies in cybersecurity is not what it should be."*

References

http://securityaffairs.co/wordpress/40773/cyber-crime/civil-nuclear-facilities-security.html

http://www.bbc.com/news/technology-34423419 http://securityaffairs.co/wordpress/39038/hacking/hacking-industrial-ethernet-switches.html

http://securityaffairs.co/wordpress/12616/malware/stuxnet-was-dated-2005-symantec-discovered-earlier-version-05.html

http://www.wired.co.uk/news/archive/2015-10/05/uk-nuclear-cybersecurity-risk

https://www.blackhat.com/docs/us-15/materials/us-15-Cassidy-Switches-Get-Stitches.pdf

http://securityaffairs.co/wordpress/31416/cyber-warfare-2/nuclear-plant-south-korea-hacked.html

http://www.eastwest.ngo/idea/measure-restraint-cyberspace

http://securityaffairs.co/wordpress/27657/cyber-crime/nuclear-regulatory-commission-hacked.html

http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit

http://www.theregister.co.uk/2015/10/05/nuclear_plants_cyber_denial_man_in_the_middle/

http://securityaffairs.co/wordpress/35013/cyber-crime/hacker-south-korean-nuclear-plants.html

http://www.nei.org/Master-Document-Folder/Backgrounders/Policy-Briefs/Cyber-Security-Strictly-Regulated-by-NRC;-No-Addit

http://www.nti.org/gsn/article/q-expert-wants-nuclear-plants-taken-table-cyber-warfare/

59 Tweet 7 G+ Share 96 in Share 1 reddit 167 Like

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist,

AUTHOR

Pierluigi Paganini

Security Analyst and Freelance Writer. Editor-in-Chief at Cyber Defense magazine, Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to create the blog "Security Affairs," recently named a Top National Security Resource for US. Pierluigi is a member of the The Hacker News team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News magazine and for many other security magazines. He is the author of the books The Deep Dark Web and Digital Virtual Currency and Bitcoin.

FREE PRACTICE EXAMS

- CCNA Practice Exam
- Network + Practice Exam
- PMP Practice Exam
- Security+ Practice Exam
- CEH Practice Exam
- CISSP Practice Exam

EDITORS CHOICE

- Career Opportunities at Stroz Freidberg
- Ashley Madison Revisited: Legal, Business and Security Repercussions
- Cyber-Attack on Worldwide Nuclear Facilities

RELATED BOOT CAMPS

- Information Security
- Security Awareness
- CCNA
- PMP
- Microsoft
- Incident Response
- Information Assurance
- 8570

MORE POSTS BY AUTHOR

Vigilante Malware: Do We Need a Cyber Vigilante?

Modern Physical Security Awareness Is More Than Dumpster Diving

How Hackers Violate Privacy and Security of the Smart Home

Career Opportunities at Stroz Freidberg

Ashley Madison Revisited: Legal, Business and…

Antivirus Evasion Tools

Evaluating the Security of Potential Partners...

0 Comments InfoSec Institute Resources Исследовательс...

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

ALSO ON **INFOSEC INSTITUTE RESOURCES** WHAT'S THIS?

Andromeda Bot Analysis part 2

1 comment • 15 days ago

Avat Mohamed — How did you identify the encryption algorithm as RC4

The Top Five Cyber Security Vulnerabilities

1 comment • 3 months ago

Avat MailShark Corporation — Great article but would patching the vulnerabilities solve the problems? many vendors of the …

15 Must Have Books for InfoSec Enthusiasts and IT Security

1 comment • 3 months ago

Avat hackingalldaylong — Great list! I'd also recommend The Hacker Playbook 2: Practical Guide to Penetration Testing. It …

Top 7 Types of Hacking Tutorials on YouTube

1 comment • 8 days ago

Avat Patricia Brook — I can't say how amazed I am, I wanted a remote password hacking software but I got a hacker instead. If you

Subscribe Add Disqus to your site Privacy DISQUS

About InfoSec

InfoSec Institute is the best source for high quality information security training. We have been training Information Security and IT Professionals since 1998 with a diverse lineup of relevant training courses. In the past 16 years, over 50,000 individuals have trusted InfoSec Institute for their professional development needs!

Connect with us

Stay up to date with InfoSec Institute and Intense School - at info@infosecinstitute.com

Like 506

Follow @infosecedu

Join our newsletter

Get the latest news, updates & offers straight to your inbox.

ENTER YC SUBSCRIBE