دراسة تحليلية لهجمات ستاكس نت على المفاعلات النووية الإيرانية

Analytical Study of Stuxnet Attacks on Iranian nuclear reactors

BY ANWAR YOUSEF

Palestinian Computer Security Incident Response Team (PCSIRT)

MAKE PALESTINE GREAT AGAIN

"رخصة الكتاب"

مؤسسة المشاع الإبداعي نَسْبُ المُصنَّف، غير تجاري، منع الاشتقاق4.0 رخصة عمومية دولية

إنَّ ممارستك للحقوق المرخَّصة(المُعرَّفة أدناه)، تعني قبولك وموافقتك على أن تكون مُلْزَمًا بأحكام وشروط رخصة المشاع الإبداعي العمومية هذه، نَسْبُ المُصنَّف، غير تجاري، مَنْع الاشتقاق4.0 رخصة عمومية دولية "الرخصة العمومية". بالقدْر الذي يسمح بتفسير هذه الرخصة العمومية كعقد، فإنك تمنح الحقوق المرخَّصة لقاء قبولك هذه الأحكام والشروط، كما ويمنحك المرخِّص هذه الحقوق لقاء المنافع التي يتلقاها من خلال إتاحة استعمال المواد المرخَّصة بموجب هذه الأحكام والشروط

الإهداء

إلى المحبوب الذي أضاءت قلوب المؤمنين ببركات أنواره و تجلّت الأرواح في بديع أسراره

(نبي الرحمة محمد صلى الله عليه وسلم)

لها القلوب تهفو. ولها العقول تذهب. ولها الأرواح تفدى. ولها الأشعار تنظم. هي من أعشق

(فلسطين)

إلى من لوحت وجوههم شمس الصحاري في نفحة والنقب إلى الأمعاء الخاوية في عسقلان ومجدو وعوفر..إلى الأمهات التي ارضعن أبنائهن لبن الحرية في تلموند وهداريم وهشارون إلى الأشبال الذين بددت قضبان الحديد والأغلال براءة طفولتهم المسلوبة..من يطول الوعد ان شاء الله

(الأسرى)

إلى إبطال فلسطين الراسخين كشجر الزيتون الفلسطيني. إلى المرابطين على كل ثغر من فلسطين الحبيبة . واخص بالذكر أهلنا في غزة الحبيبة.أهديكم ضيا عيني....ودفء القلب أعطيكم

(المقاومين الفلسطينيين)

ليس هناك في الحياة امرأة واحدة تهب كل حياتها وكل حنانها وكل حبّها دون أن تسأل عن مقابل أنت حياة الروح.. أنت الأغلى من عيني....

(أمي)

إلى النور الذي ينير لي درب النجاح

(أبي الغالي)

إلى نبض وجداني؛ فالنبض لهما يسري، والروح لهما تنساق، في بعدهن تكثر جروحي، و بقربهن تبعد أحزاني. هن فاكهة الحياة، والحب المملوء بالشغب الجميل ربّي أسعدهم ولا تحرمني وجودهم أحبكم

(أخواتي)

وإن كنت سأتحدث عن نعيم الحياةسأبدأبه . إلى من عشت معه طيلةأيام طفولتي وقاسمته حلوها ومرها.. إلى سندي وقوتي وملاذي بعد اللّه... إلى من آثرني على نفسه

(أخي)

إلى الذين تسكن صورهم وأصواتهم أجمل اللحظات والأيام التي عشتها

(أصدقائي وأحبائي)

إلى الأحبة والأعزاء على القلب

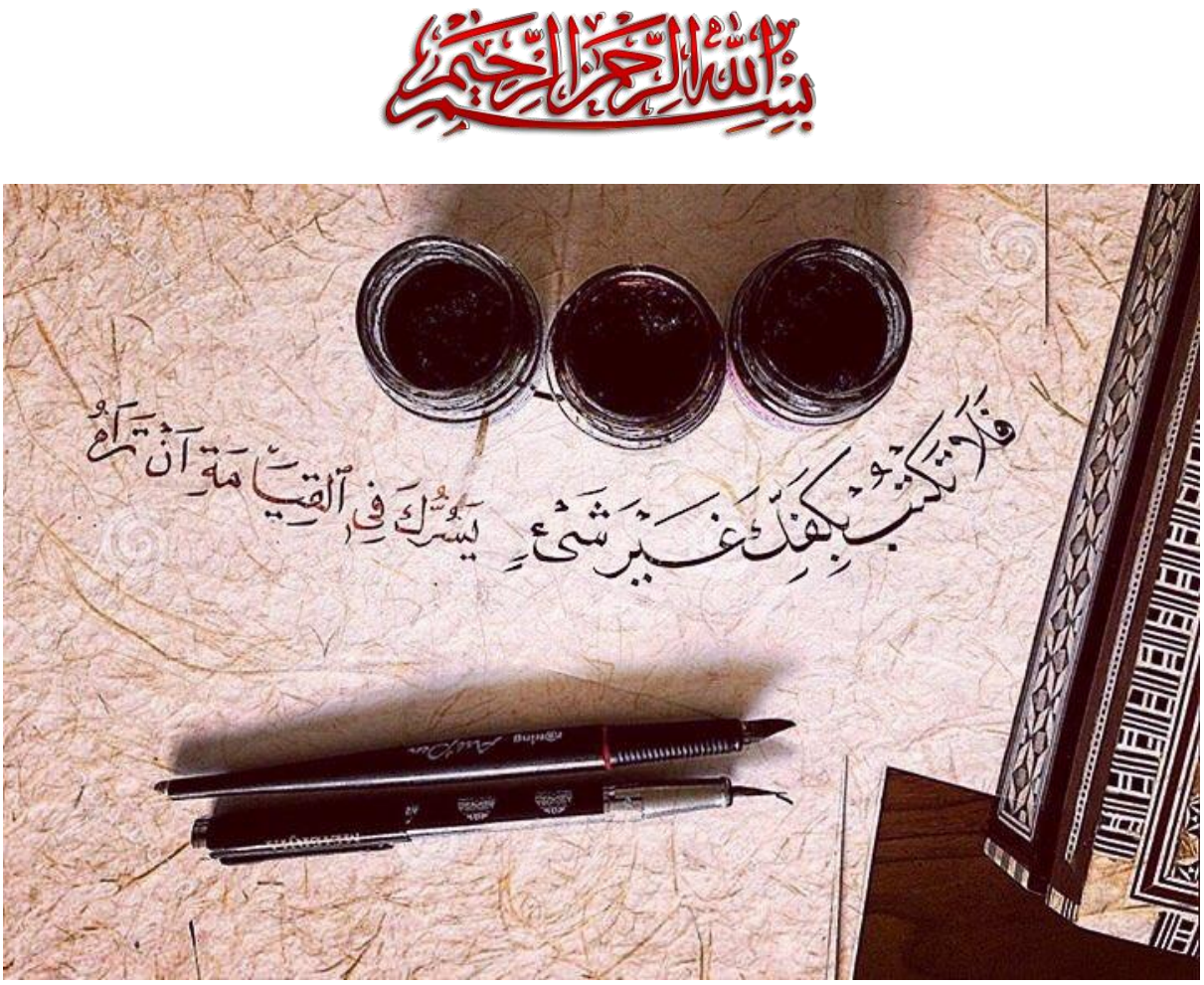
أيمن قاسم (أبو عمر)

باسل الشيخ قاسم (أبو زاهر)

وإلى جميع أعضاء فريق الأستجابة لحوادث أمن الحاسوب الخاص بدولة فلسطين

(PCSIRT)

مقدمة الكاتب



بحمد الله ومنته علي فقد أتممتالدراسة التحليلية لهجماتستاكس نت على المفاعلات النووية الايرانية, ونظراً لأنه موضوع هام جدًيتناول إنطلاق شراراة بدء الحروب السيبرانية وتأثيرها الضخم على منشآت هامة في أي دولة صاعدة فكان لزاماً تسليطالضوء عليه بصورة شاملة بدء من خلل ما قبل الهجمة انتهاء بالهندسة العكسية له. وهذا الجهد كله أدين به لله عز وجل الذي منحني الصبر وبعض من العلم فله الحمد والمنة . هذا ما عندي فأن أحسنت فمن الله , وإن أسأت أو أخطت فمن نفسي والشيطان .

أنور يوسف

التاسع من ذو القعدة ألف وأربعمائةوأربعون هجري .

تتضمن الدراسة ما يلي :

1 - نقاط الضعف التي أدت إلى استغلال الثغرات المادية للوصول للمفاعلات النووية الإيرانية .

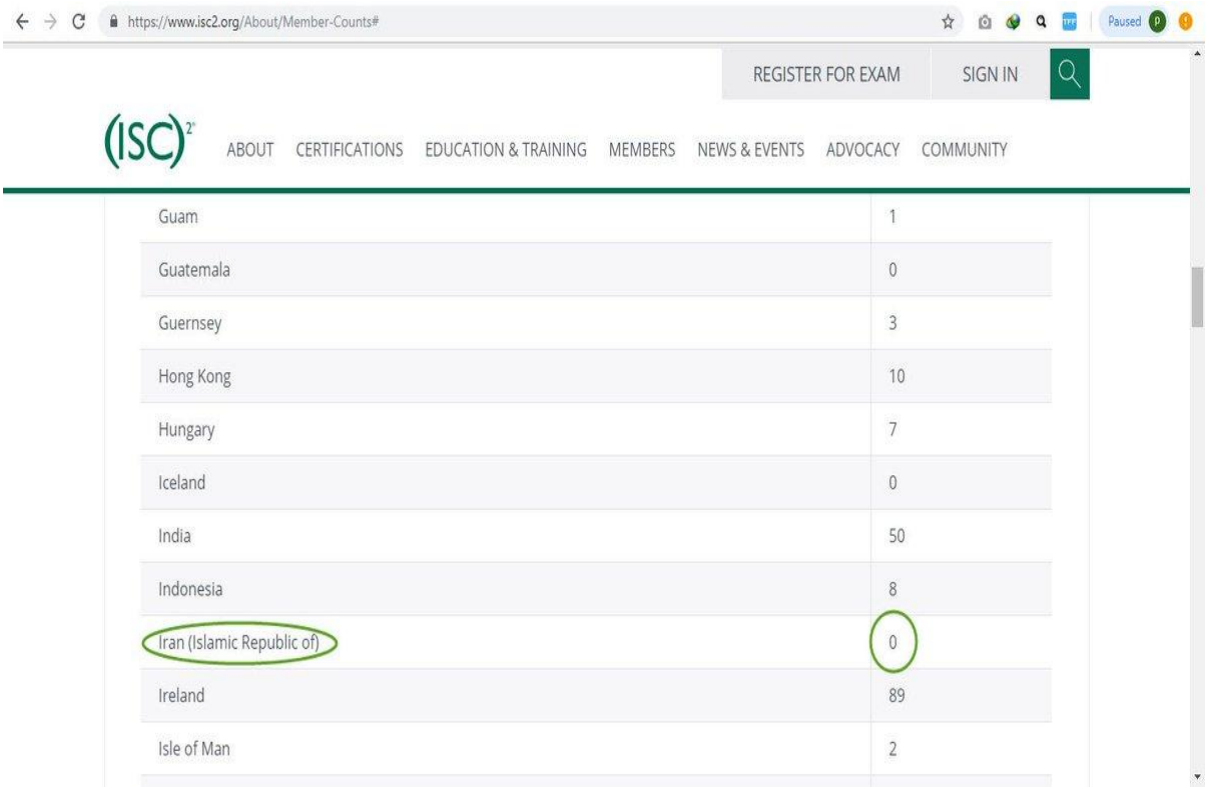
2 - نقاط الضعف التي أدت إلى استغلال ثغرات الأنظمة الخاصة بتنظيم عملية تخصيب اليورانيوم.

3 - ماهية البرمجية الخبيثة ستاكس نت .

4 - الهندسة العكسية الكاملة لستاكس نت المخصصة بالتحديد لضرب منشأة نطنز النووية .

في البداية من الملاحظ بأنه كان هناك خلل كبير للغاية من الناحية الفيزيائية في تأمين منشأة نظنز النووية . فلا كاميرات مراقبة في كل اتجاه ولا أجهزة بيومترية إضافة إلى غياب التوعية الأمنية وهذا ما تم مناقشته وتأكيده من الباحثين الإيرانيين.

الصورة التي في الأسفل توضح بأنه لم يحصل أي شخص إيراني على شهادة Systems Security Certified Practitioner (SSCP) والتي تبحث في تأمين المنشآت بصورة عملية .



إضافة إلى ذلك غرد أحد الباحثين الأمنيين في مجال الحماية الأمنية لأنظمة السكادا بأن إيران تعتمد على كوادر من دول أجنبية وبالتحديد كوريا الجنوبية ليقوموا بعمليات تأمين وحماية لتلك الأنظمة بدلاً من الخبراء الإيرانيين , الأمر الذي يدعو إلى الحيرة حسب تعبيره خصوصاً بأن إيران تملك من الخبراء المحليين مايكفي لذلك.

ولكن على صعيد أخر غرد وزير الإتصالات الإيراني مؤخراً بأن الخبراء المحليين نجحوا في تصميم أنظمة محلية قادرة على حماية المنشآت الصناعية وأنظمة السكادا من أي تهديد وهجوم إلكتروني وكان ذلك بأيدي محلية خالصة.

مفاعل نطنز النووي كان مصمم بصورة Air–Gap أي أنه لا يحدث أي اتصال بينه وبين أي شبكة ولكن إشارة إلى هذه الثغرات فقد تمكن باحثين في قسم السايبر بجامعة بن غوريون من اكتشاف عدة تقنيات لتجاوز ال Air–Gap أو ما يعرف بثغرات الفجوات الهوائية ولكن الاختراق حدث عن طريق جاسوس روسي قام بزرع قرص قابل للإزالة يحوي على ستاكس نت بحسب مصادر وباحثين إيرانيين مستقلين .

في الثامن عشر من شهر مايو سنة 2018 كنت قد دونت في الفيس بوك حول ثغرات الفجوات الهوائية وذهبت لتحليل بعض أبحاث قسم السايبر في جامعة بن غورين ونص التدوينة كان

ثغرات الفجوات الهوائية المثيرة للجدل

بعد ما نشر قسم السايبر الخاص بجامعة بن غوريون أبحاث حول موضوع ثغرات Air Gap , وبعد متابعتي لكافة الأبحاث المنشورة والتي عددها 22 .. نلاحظ موضوع هام يجب الحذر منه وهو الحيطة عند اقتناء جهاز الهاردوير المشغل لأي سوفت وير

تعريف بسيط بثغرات Air Gap

هي مقياس أمان للشبكة يتم استخدامه على كمبيوتر واحد أو أكثر للتأكد من أن شبكة الكمبيوتر الآمنة قد عزلت فعلياً عن الشبكات الغير أمنة

أي اختراق الجهاز ولو كان مفصول تماما عن الاتصال بالشبكة سواء عن طريق انترنت – بلوتوث أو أي مصدر للاتصال ولو كان داخلي.

غالبية الشركات العسكرية والتقنية تنتهج وضع ثغرات

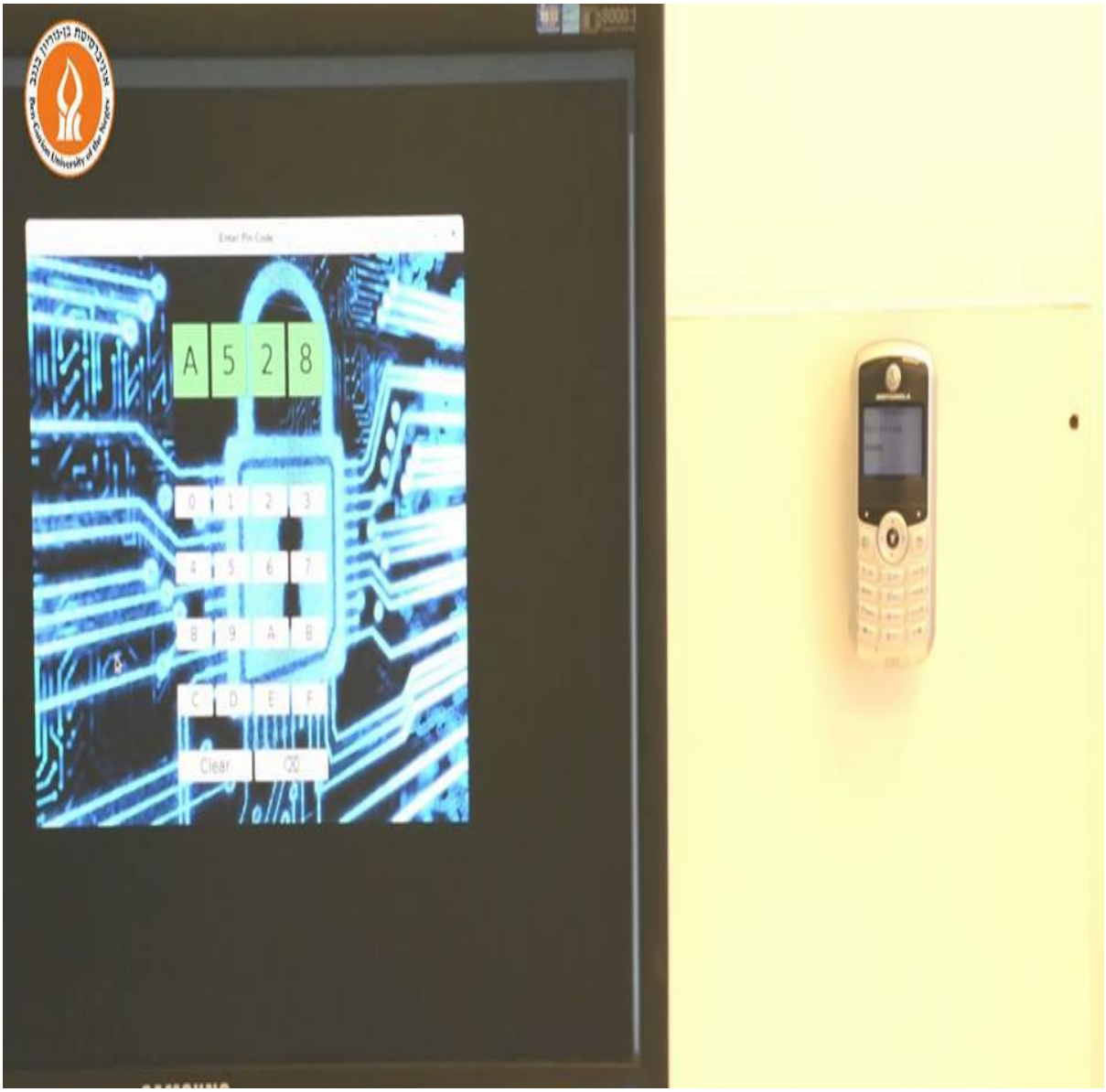
الهاردوير في أجهزتها لاستغلالها بالملايين عن طريق إغراق الأسواق منها وخير دليل الكيلوجر الصيني بالكيبوردات الذي اكتشف مؤخرا .

هنا قاموا بتجربة مالوير يعمل بتطابق خاص عن طريق ثغرات الفجوات الهوائية على أجهزة موتورولا المصنعة داخل الكيان الصهيوني وقاموا بعمل Sniffing على جهاز Motorola c 123

مصدر المعلومة بأن شركة المتورولا أسست في الكيان الصهيوني ومقرها تل أبيب

#Motorola Communications Israel Ltd. develops and manufactures radio communications and electronics equipment. The company's main activities are the design and development of products for worldwide marketing and manufacture, and the sale and maintenance of Motorola's communications products and systems. The company was founded in 1985 and is based in Tel Aviv, Israel. Motorola Communications Israel Ltd. operates as a subsidiary of Motorola Israel, Ltd.

في الصورة المرفقة تجربة لقسم السايبر بجامعة بن غوريون توضح عمل Sniffing لجهاز موتورولا والتجسس على بيانته بدون اتصال بالانترنت.



ستاكس نت Stuxnet

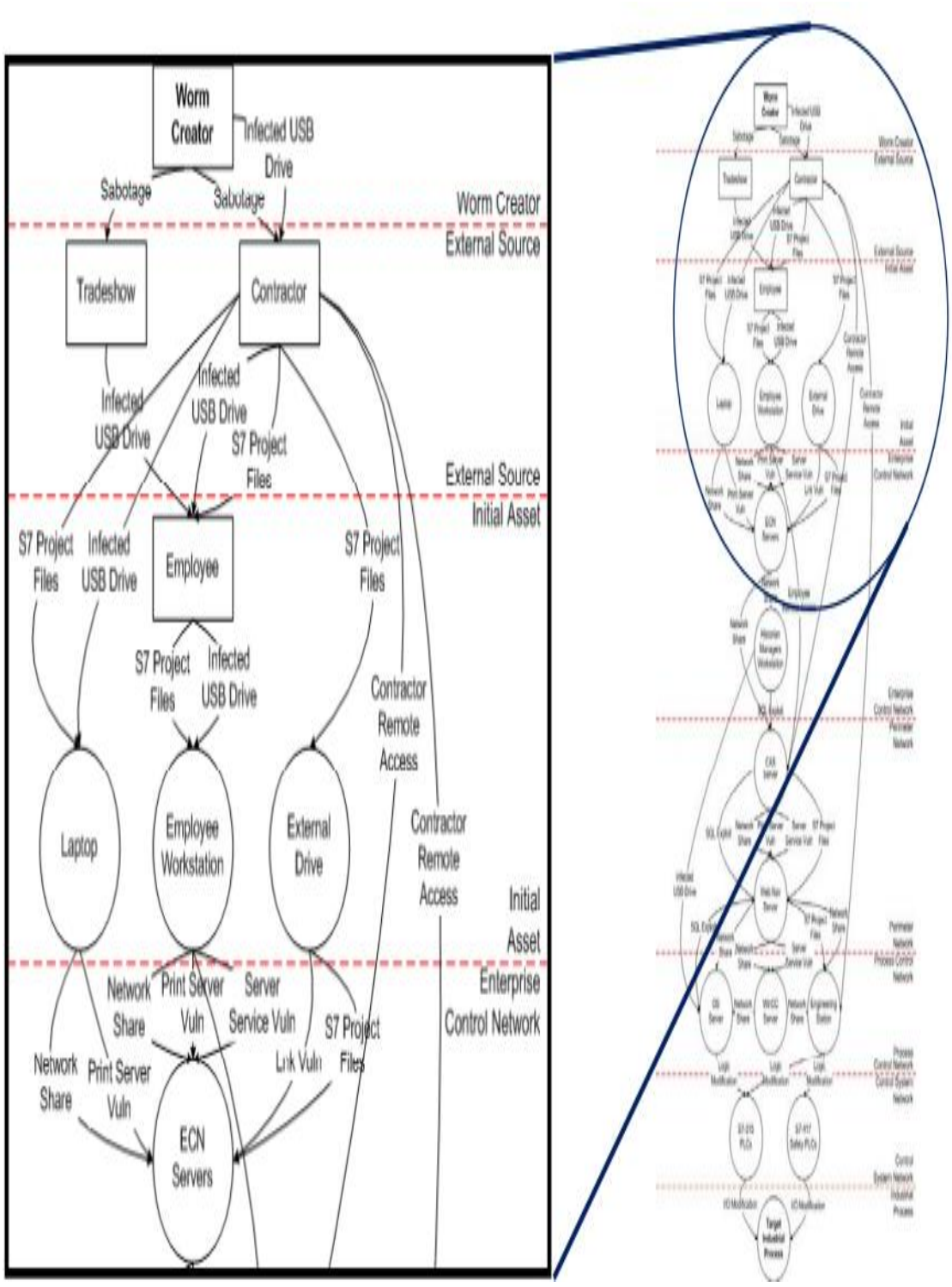
انتشرت البرمجية الخبيثة التي تعرف باسم ستاكس نت في وسط عام 2010 والتي شكلت بلورة واضحة لحقيقة الحروب السيبرانية , ولكن في الحقيقة طبق تحليلات عديدة كان ستاكس نت منتشر قبل أعوام في الأنظمة الإيرانية التي تساعد على تنظيم عمليات تخصيب اليورانيوم . الكشف الأول لستاكس نت كان عند نقل حاسوب إيراني إلى بيلاروسيا وتم الكشف عنه هناك عن طريق أحد الشركات العاملة في مجال مكافحة البرمجيات الخبيثة لتقوم بعدها شركة Symantec بتحليل أوسع لستاكس نت. وبصورة بسيطة تنتشر تلك البرمجية الخبيثة إما عن طريق المرفقات البريدية أو بواسطة الأقراص القابلة للإزالة (USB) وتقوم بنسخ نفسها كدودة في الأنظمة وسرعان ما تنتشر بصورة مخفية مستغلة ثغرات 0day في أنظمة ويندوز إضافة إلى ثغرات في برامج SCADA WinCC الخاصة بأنظمة التحكم الصناعي لدى شركة Siemens لتحدث أضرار في أجهزة التحكم الصناعي (SCADA) التي تعمل في حالتنا

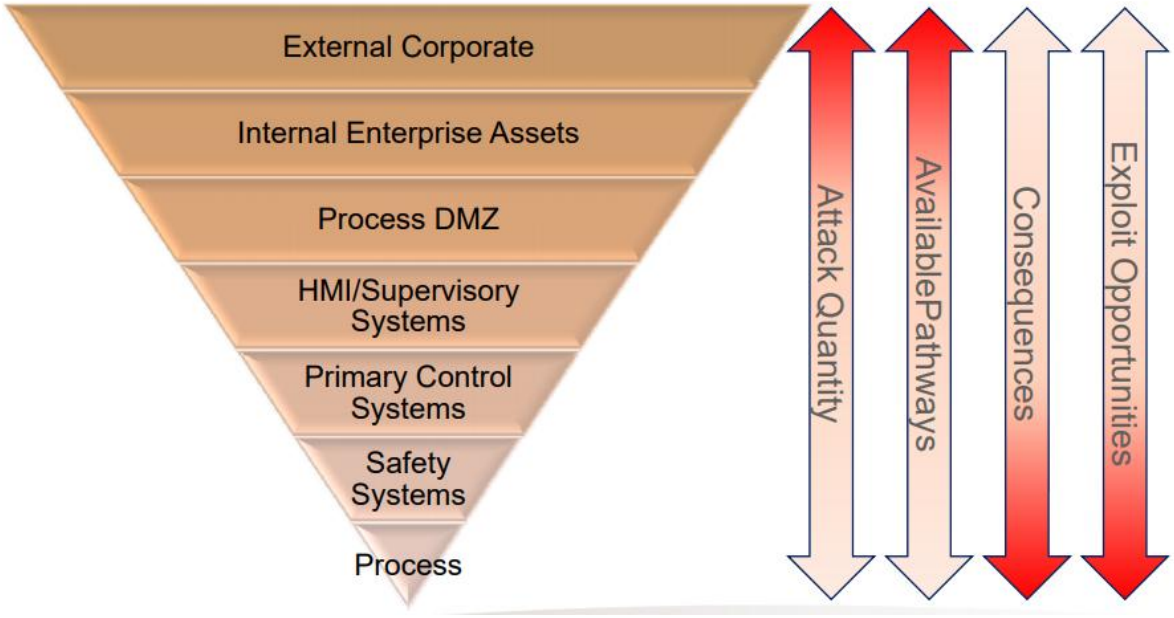
هنا على تنظيم ومراقبة عمليات تخصيب اليورانيوم في المنشآت النووية .

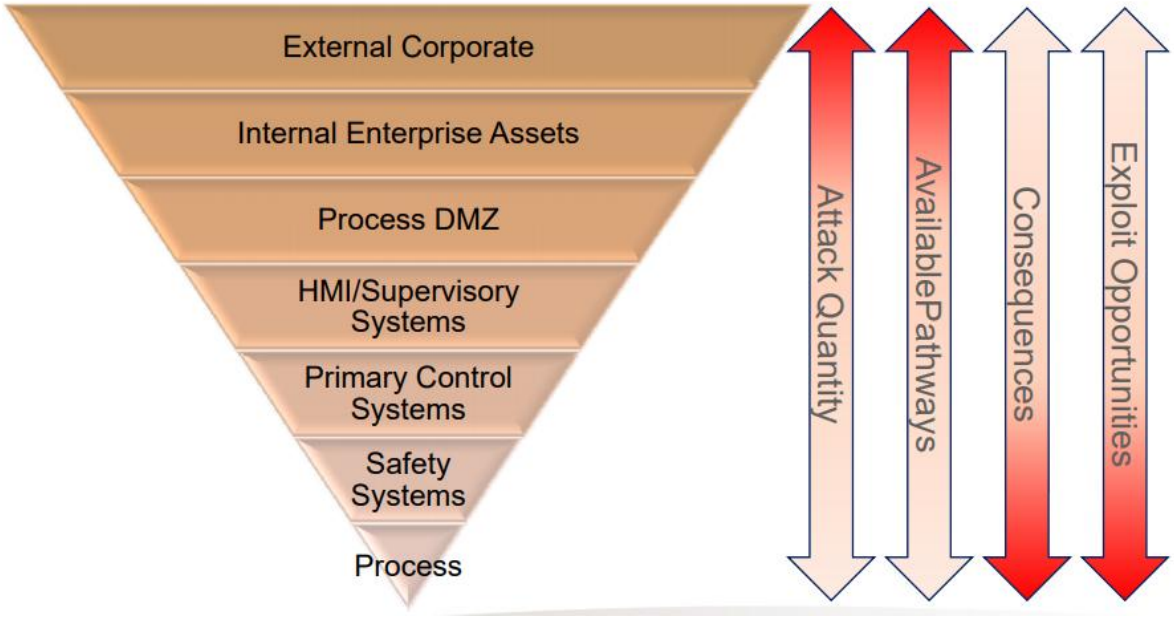
يستخدم ستاكس نت 4 ثغرات و7 طرق للوصول إلى المبتغى الذي صمم من أجله ويعتبر من اعقد البرمجيات الخبيثة التي مرت على تاريخ الحروب السيبرانية ويعتقد بأن جمع هائل من الخبراء في كافة المجالات قد أسهموا بالمشاركة في صناعة هذه البرمجية الخبيثة .

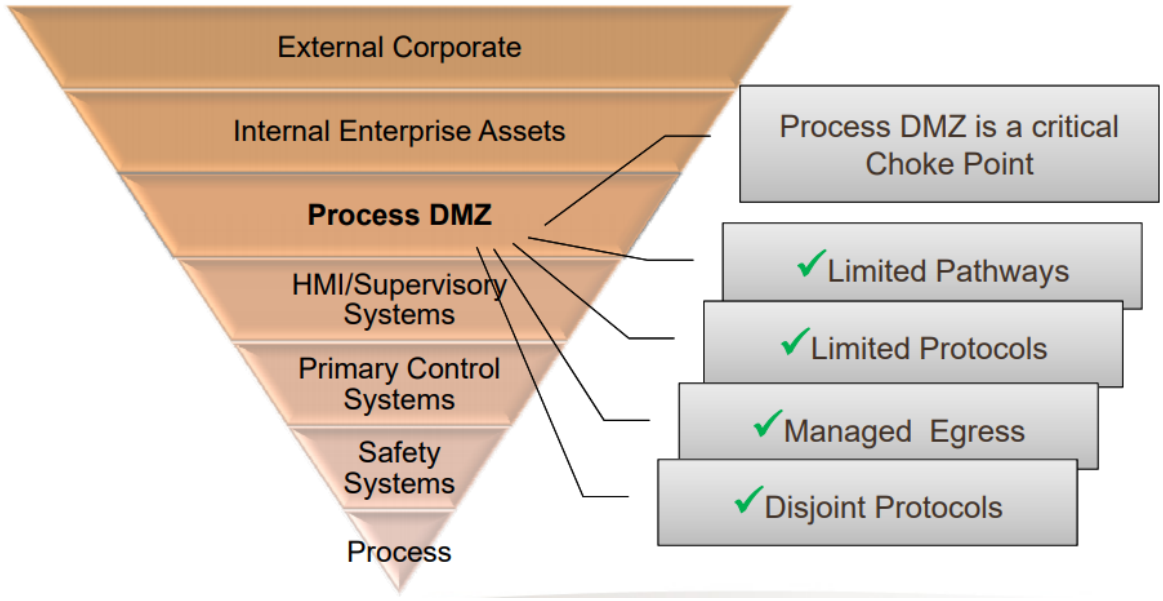
الهدف الرئيسي لستاكس نت كان إيران وبرنامجها النووي والبنية التحتية للمنشأت النووية وقد نجح بتأخير البرنامج في مفاعل نطنز ما يقارب السنتين . وقد حللت الشركات الأمنية ستاكس نت بعبارة Welcome to Cyberwar نظراً لخطورة ما أحدثه وما قد يكون باب أولي لنزاعات الحروب السيبرانية .

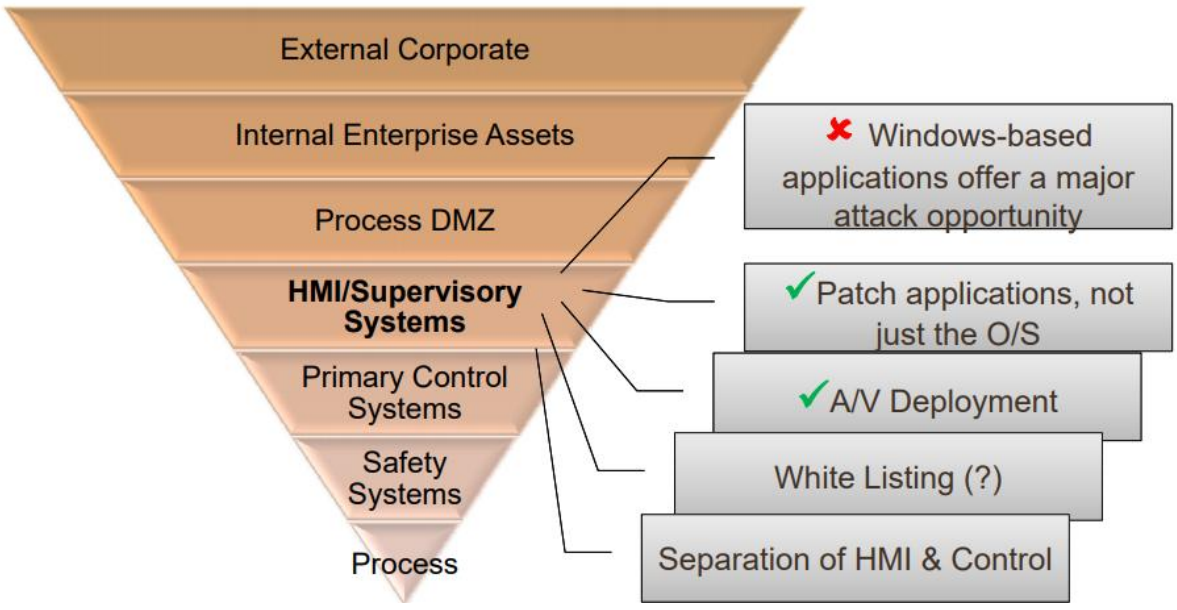
دورة حياة ستاكس نت

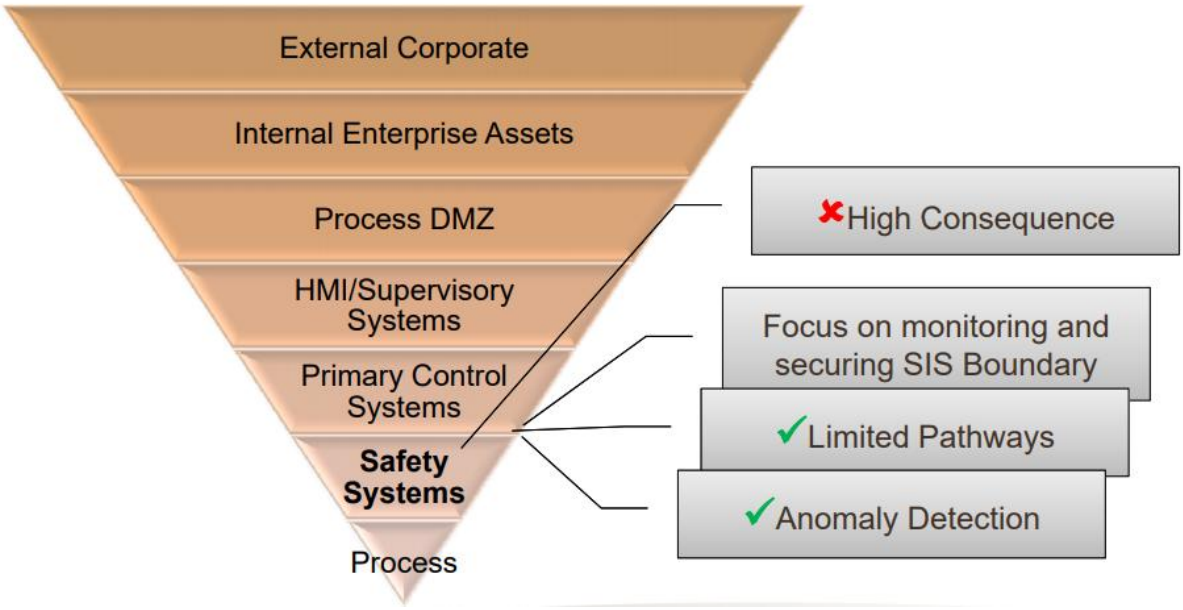


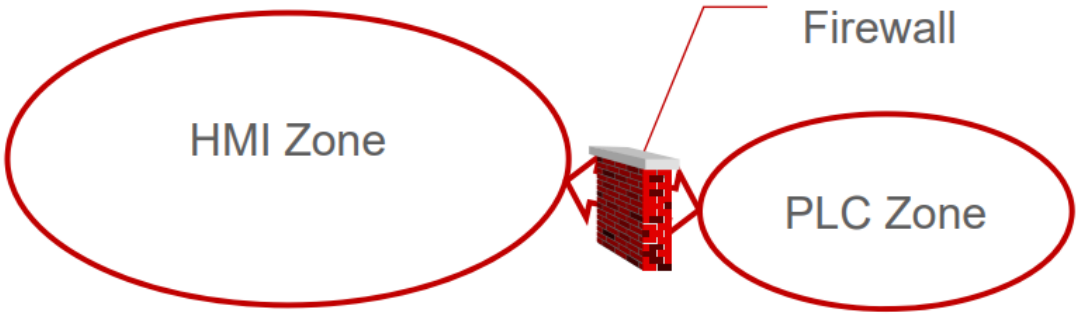

External Corporate
Internal Enterprise Assets
Process DMZ
HMI/Supervisory Systems
Primary Control Systems
Safety Systems
Process
Attack Quantity
AvailablePathways
Consequences
Exploit Opportunities

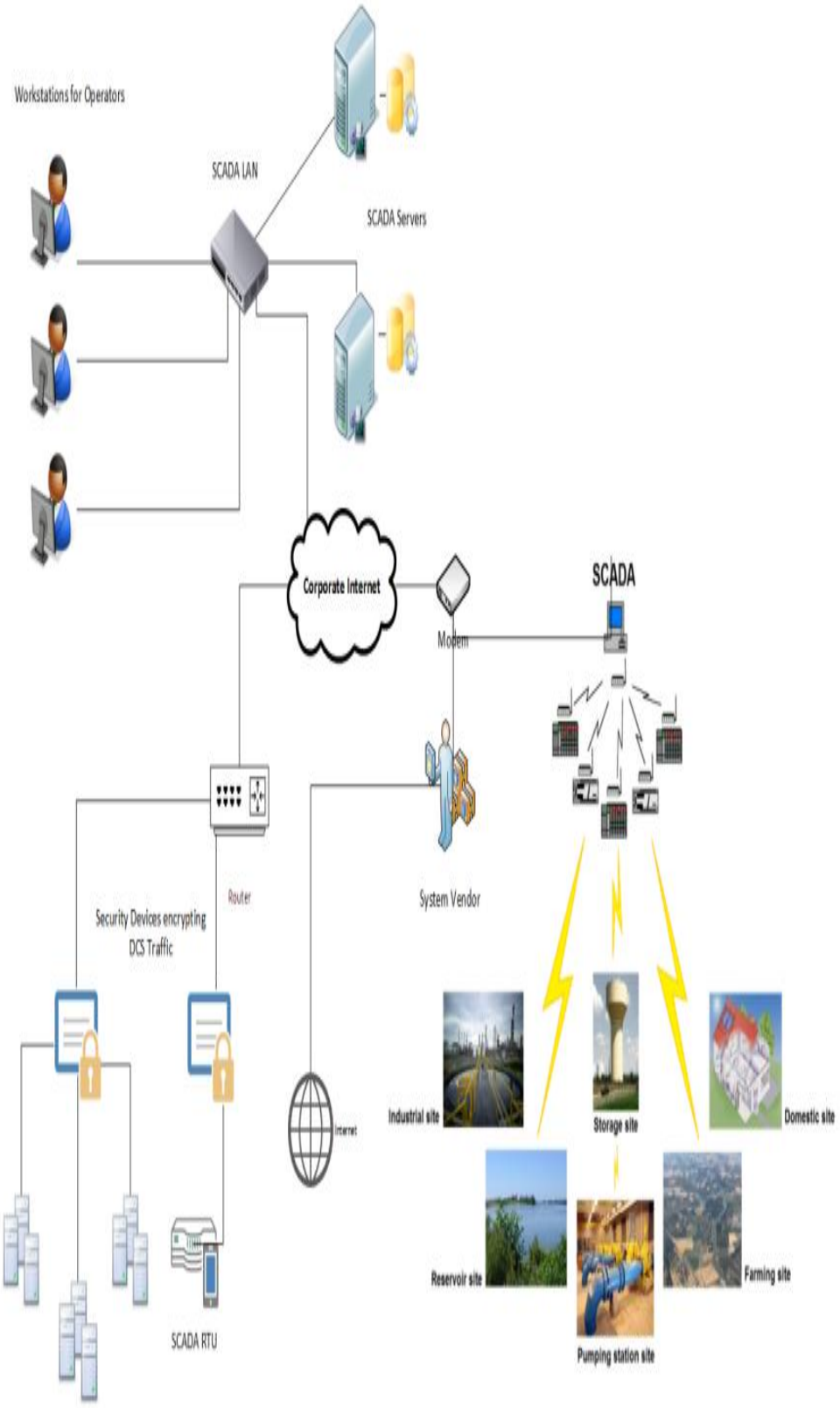

External Corporate
Internal Enterprise Assets
Process DMZ
HMI/Supervisory Systems
Primary Control Systems
Safety Systems
Process
Attack Quantity
AvailablePathways
Consequences
Exploit Opportunities


External Corporate
Internal Enterprise Assets
Process DMZ
HMI/Supervisory Systems
Primary Control Systems
Safety Systems
Process
Process DMZ is a critical Choke Point
✓Limited Pathways
✓Limited Protocols
✓Managed Egress
✓Disjoint Protocols

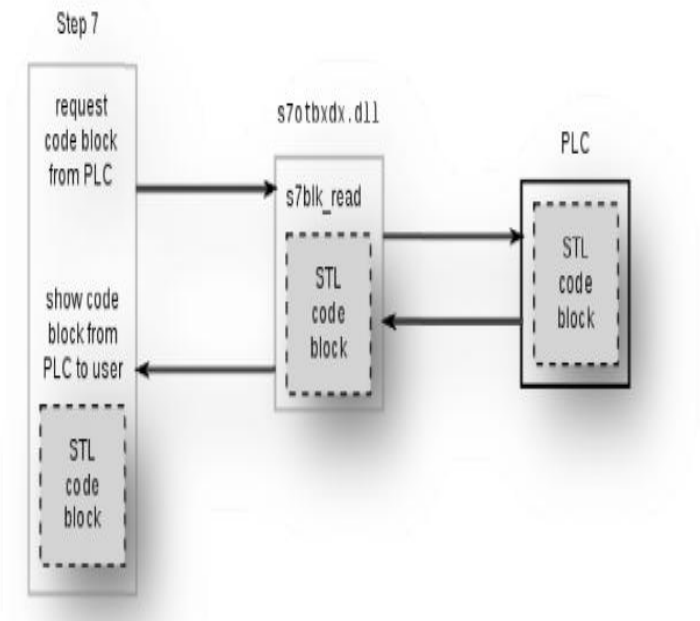

External Corporate
Internal Enterprise Assets
Process DMZ
HMI/Supervisory Systems
Primary Control Systems
Safety Systems
Process
✘ Windows-based applications offer a major attack opportunity
✓Patch applications, not just the O/S
✓A/V Deployment
White Listing (?)
Separation of HMI & Control

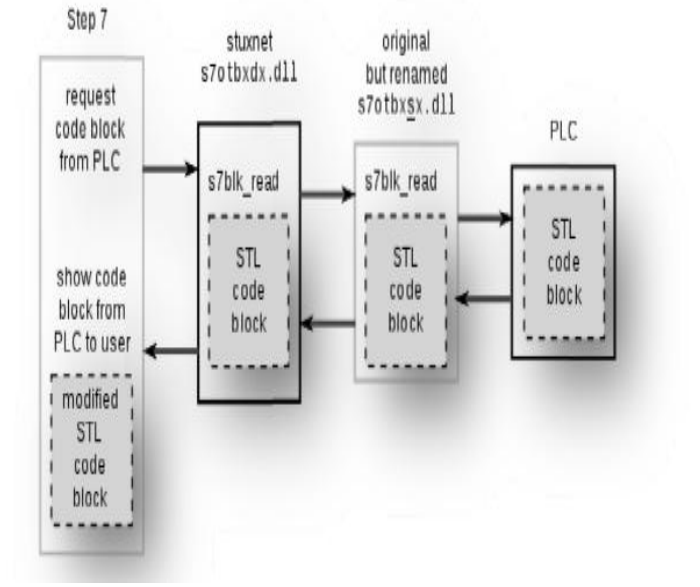

External Corporate
Internal Enterprise Assets
Process DMZ
HMI/Supervisory Systems
Primary Control Systems
Safety Systems
Process
High Consequence
Focus on monitoring and securing SIS Boundary
Limited Pathways
Anomaly Detection

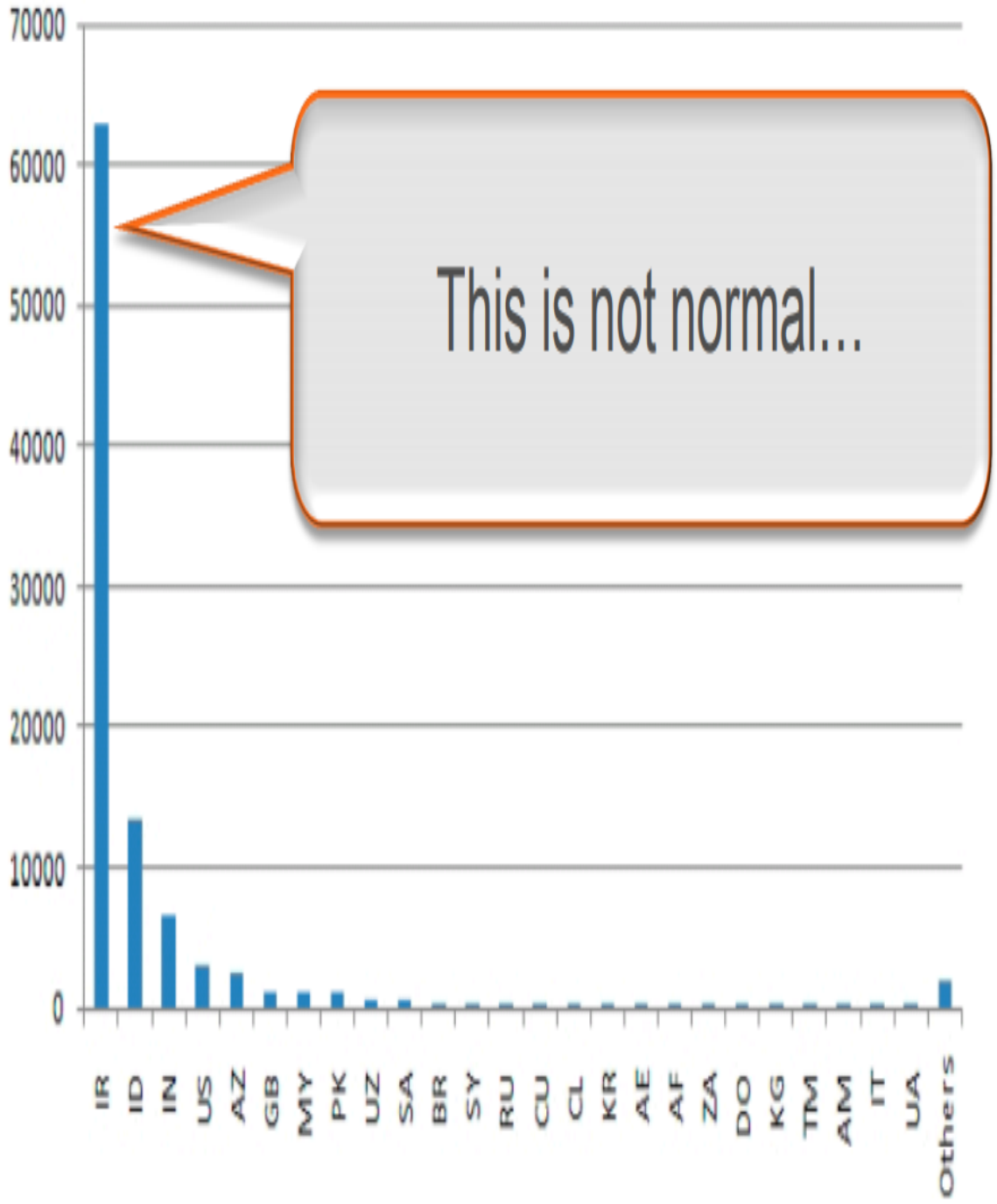

Firewall
HMI Zone
PLC Zone


Workstations for Operators
SCADA LAN
SCADA Servers
Corporate Internet
Modem
SCADA
Router
System Vendor
Security Devices encrypting
DCS Traffic
Internet
SCADA RTU
Industrial site
Storage site
Domestic site
Reservoir site
Farming site
Pumping station site

* مبدأ عمل ستاكس نت كان يتجلي بشكل أساسي بتغير أحد ملفات المكاتب للبرمجيات القائمة على نظام سكادا بملف مكاتب محقون بأكواد خبيثة .






70000
60000
50000
40000
30000
20000
10000
0
This is not normal...
IR
ID
IN
US
AZ
GB
MY
PK
UZ
SA
BR
SY
RU
CU
CL
KR
AE
AF
ZA
DO
KG
TM
AM
IT
UA
Others

الهندسة العكسية الكاملة لستاكس نت

من خلال التحليل بالهندسة العكسية تمت الملاحظة بأن إحدى ملفات المكاتب تم استبداله بالملف s7otbxdx

الملف السابق من نوع DLL واستغرق خمس مراحل إلى أن تم تحليله عن طريق الهندسة العكسية .

المرحلة الأولى : عزل الملف .

المرحلة الثانية : فك تشفير الملف .

المرحلة الثالثة : تنقيح الملف .

المرحلة الرابعة : تبديل الملف بأكواد تشبه إلى حد ما لغة السي لأنها هي اللغة المستخدمة في أنظمة سكادا بصورة كبيرة .

المرحلة الخامسة : عرض الكود في طبقة المستخدم للعمل عليها .

نتائج الهندسة العكسية لستاكس نت تظهر بصورة لا ريب بها بأنه صمم في المقام الأول لضرب أجهزة تخصيب اليورانيوم في مفاعل نطنز الواقع في مدينة أصفهان الإيرانية .

Array [0..16383]: BYTE

معطيات المقادير الأولية المسؤولة عن تسجيل دخول ستاكس نت إلى النظام.

Array [1..984]: DWORD

Array [1..984]: BOOL

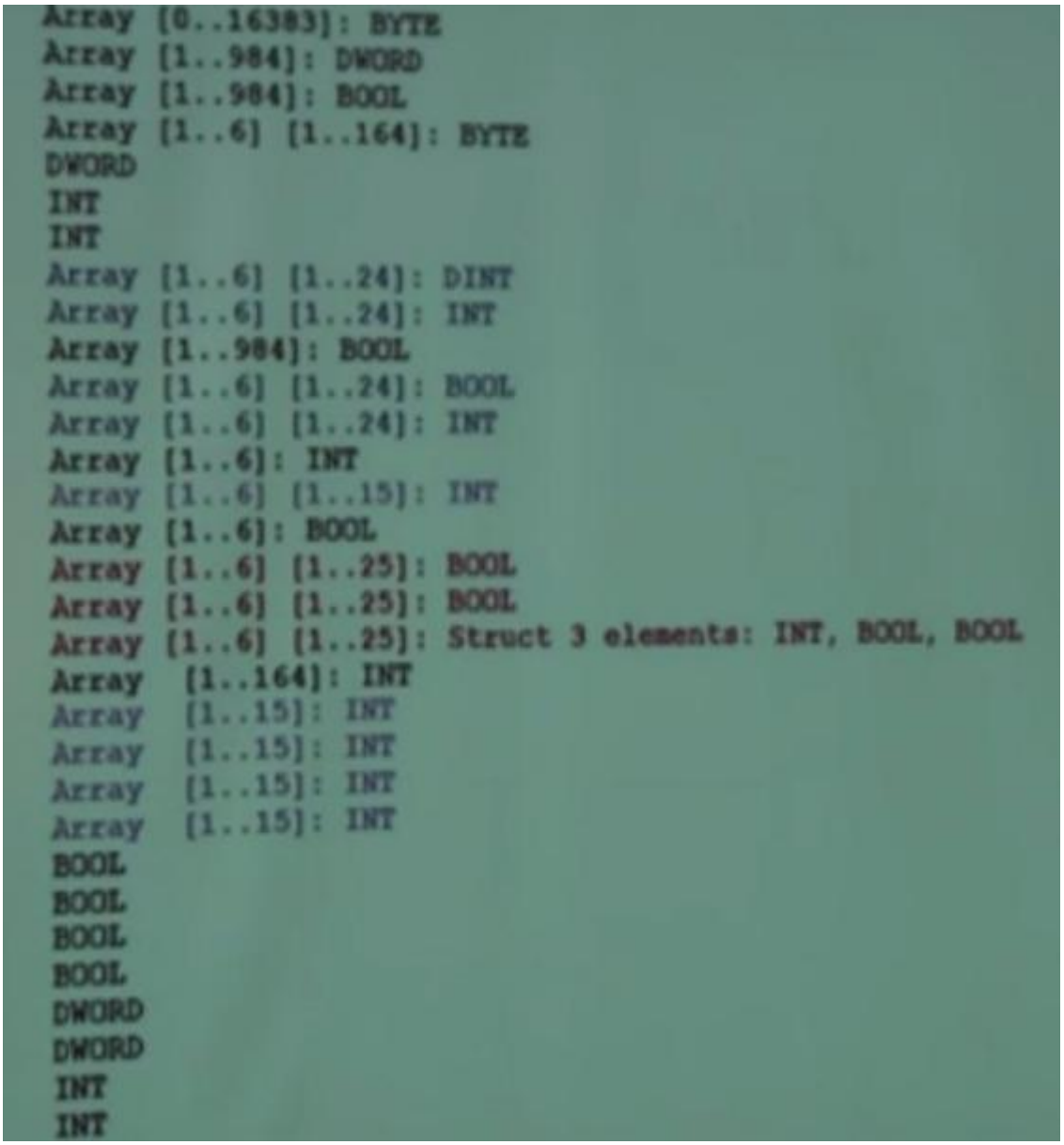
Array [1..6][1..164]:BYTE

في إشارة بأن مفاعل نطنز في تاريخ 17.4.2009 كان يحوي 164 جهاز طرد مركزي وه ذا ما بينته المقادير الأولية لعملية تسجيل الدخول .

Array [1..6][1..164]:BYTE

146 * 6 = 984

وكان ستاكس نت معني بالهجوم على 6 أجهزة من مفاعلات الطرد المركزي التي تقوم بتخصيب اليورانيوم .



بنية ملف " DB 8063 " الخاص ببرمجية بستاكس نت

Array [1..6][1..24]: DINT

Array [1..6][1..24]: INT

Array [1..984]: BOOL

Array [1..6][1..24]: BOOL

Array [1..6][1..24]: INT

المقادير المذكورة لا ترتبط بالتأسيسات الفيزيائية وهي فقط مسؤولة عن فهرسة عناوين الجداول :

Array [1..6]:INT

Array [1..6][1..15]: BOOL

Array [1..6]: BOOL

Array [1..6][1..25]: BOOL

Array [1..6][1..25]: BOOL

Array [1..6][1..25]: Struct 3 elements : INT ,BOOL , BOOL

المقادير المذكورة تبين بأن الهجوم لم يكن على مستوى أجهزة الطرد فحسب بل كان يستهدف أجهزة التخصيب واحد تلو الأخر وهذا ملاحظ عند القيمة 25

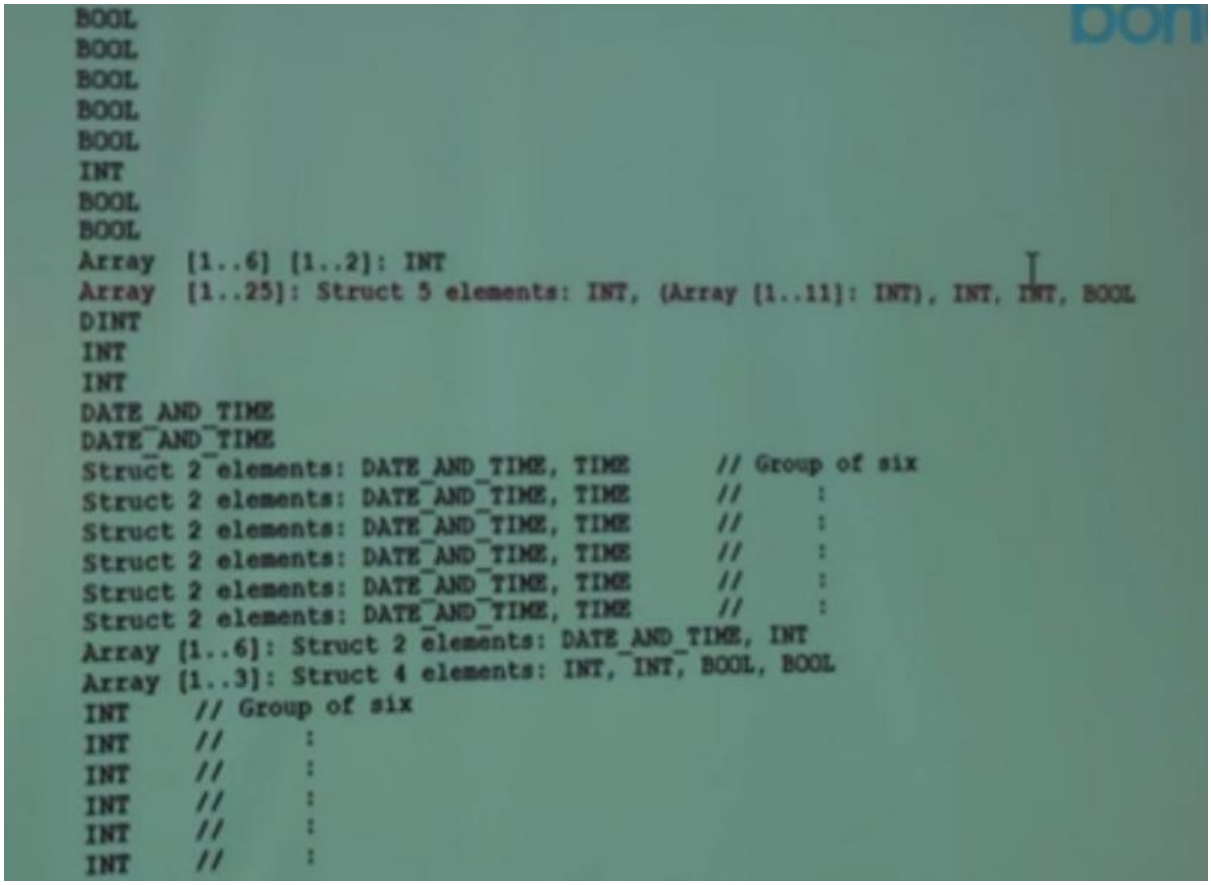
Array [1..15]: INT

Array [1..15]: INT

Array [1..15]: INT

Array [1..15]: INT

مدخلات البلوك رقم15



صورة عن البلوك DB 8063

Array [1..25]: Struct 5 elements :INT , (Array [1..11]: INT),INT,INT, BOOL

- أحد أسرار ستاكس نت هي بأنه بدون رفع معلومات البلوك رقم 8061 في الملف DLL لن يكون بمقدوره تنفيذ هجمته المرجوة.

- يتسم بلوك الستاكس نت بعملية دخول تتكون من 10 مراحل وخروجه بمراحل أكبر من ذلك . نظم المصفوفات التالية تبين 6 مراحل معادلة ل 6 أجهزة طرد مركزي كانت مصممة خصيصاً لمفاعل نطنز. الست أجهزة تحوي 146 هياكل لعملية الدخول. الأرقام 25-3-30 الواردة في المصفوفات في الأسفل أيضا تدخل في عملية بنية تسجيل الدخول لستاكس نت على النظام.

Array [0..16383]: BYTE

Array [1..984]: DWORD

Array [1..984]: BOOL

Array [1..6][1..164]: BYTE

Array [1..6][1..24]: DINT

Array [1..6][1..24]: INT

Array [1..984]: BOOL

Array [1..6][1..24]: BOOL

Array [1..6][1..24]: INT

Array [1..6]: INT

Array [1..6][1..15]: BOOL

Array [1..6]: BOOL

Array [1..6][1..25]: BOOL

Array [1..6][1..25]: BOOL

Array [1..6][1..25]: Struct 3 elements

Array [1..15]: INT

Array [1..15]: INT

Array [1..15]: INT

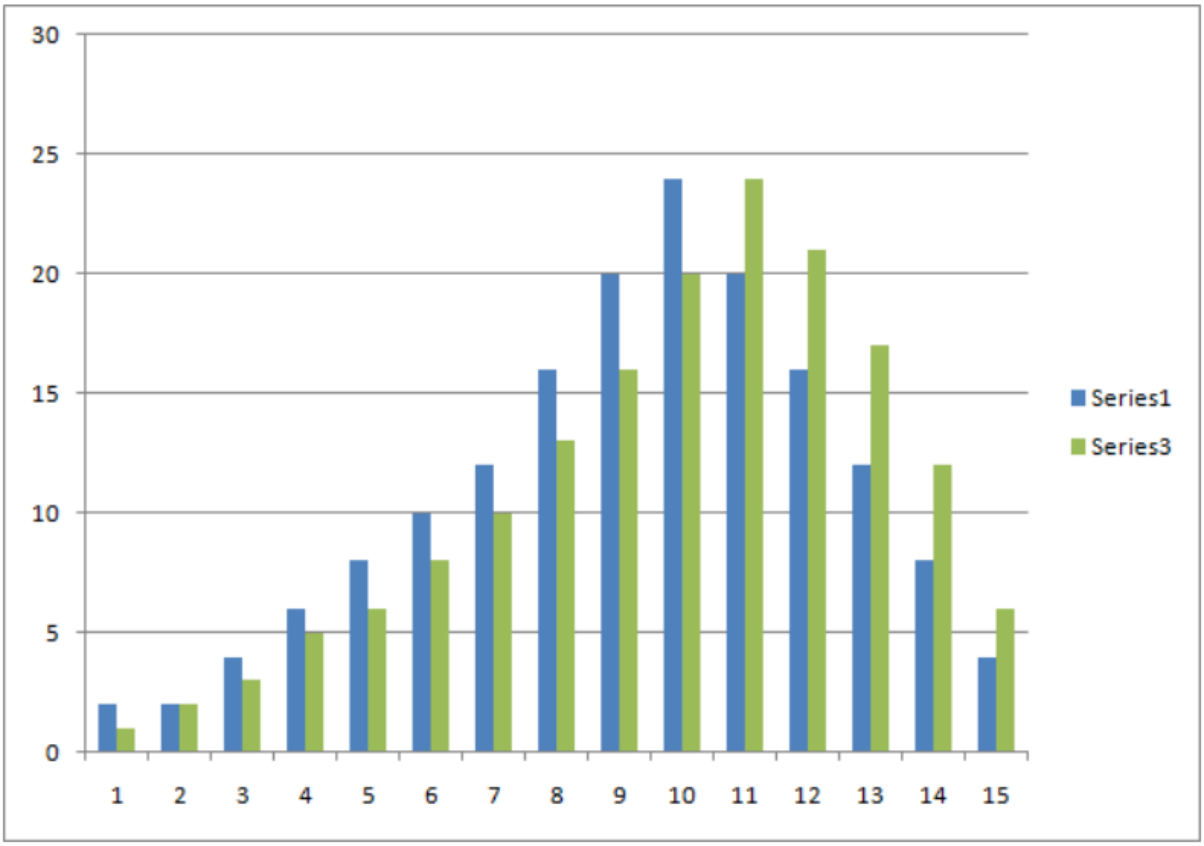
Array [1..15]: INT

حسب التحليلات التي أجريت أتضح بأن مفاعل نطنز كما ذكرنا سابقاً يحوي 146 جهاز طرد مركزي مرتب على 15 مرحلة.أي أن سداسي فلوريد اليورانيوم ينتقل إلى أجهزة الطرد المركزي في المرحلة الخامسة وفي نهاية المرحلة الخامسة عشر يتشكل اليورانيوم بنسبة 3.5% .

ستاكس نت كان ينتهج أيضا تقنية تقسيم مراحل الهجوم على كل جهاز طرد مركزي بصورة مستقلة لكي إن تم الكشف عنه في جهاز يتضح للخبراء بأن هناك خلل ما فقط في جهاز الطرد المركزي المستهدف . تم تقسيم الهجمات على 15 مرحلة وكل مرحلة كما ذكرنا تمت بصورة منفردة .

مثال : في المرحلة 15 تم الهجوم على الأجهزة رقم 164 و 161

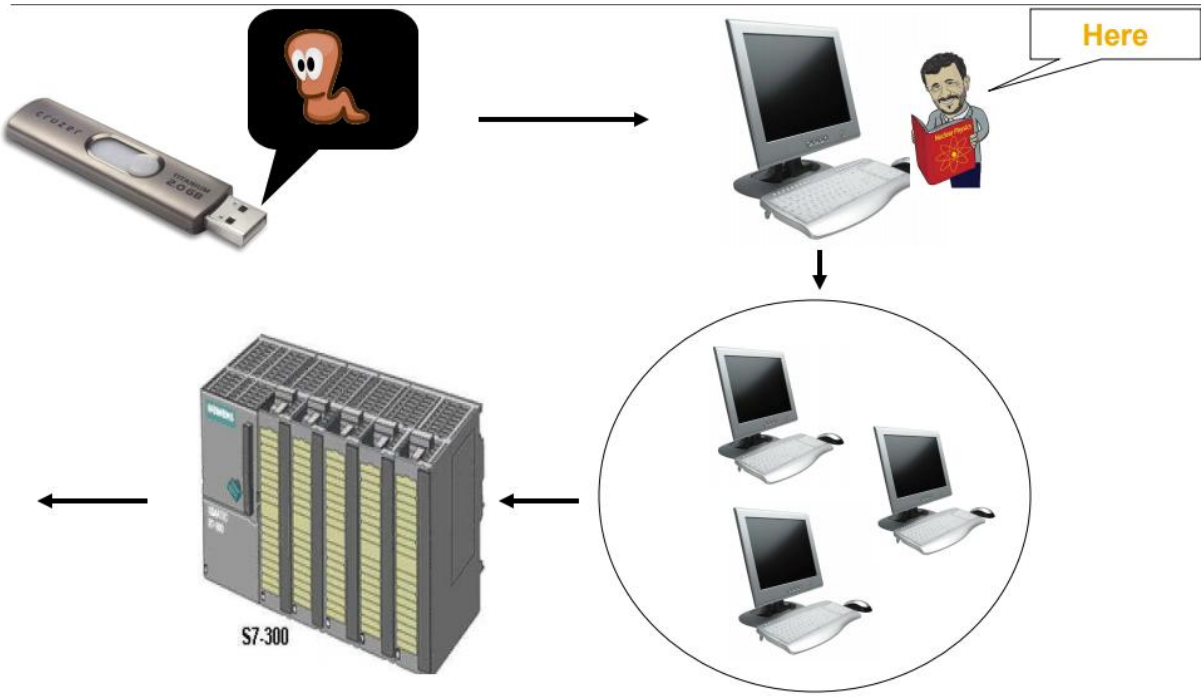
* الرسم البياني في الأسفل يوضح العلاقة بين ستاكس نت وتأسيسات مفاعل نطنز النووي



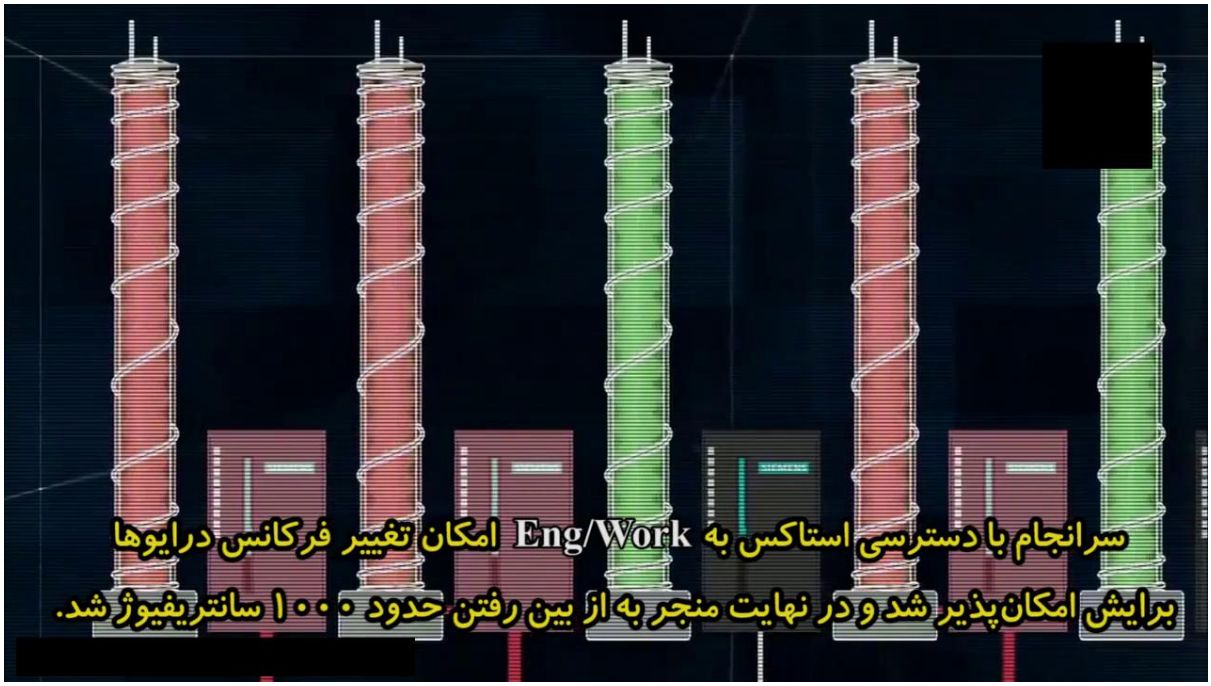
اللون الأزرق : تعداد أجهزة الطرد المركزي في مفاعل نطنز النووي .

اللون الأخضر : تعداد الأجهزة المفروضة من قبل ستاكس نت التي تخصب اليورانيوم أي الأجهزة الوهمية.

ولكن النقطة الأهم هنا هي مرحلة تغذية اليورانيوم المخصب في أجهزة الطرد المركزي. فحسب تصريحات رئيس الوكالة الذرية في إيران : في مفاعل نطنز النووي المرحلة الخامسة هي المسؤولة عن التغذية. هذا يعني أن ستاكس نت سيفرض المرحلة السادسة للتغذية.



الخلل في أجهزة الطرد المركزيالتي أدت إلى عدم إنتاج اليورانيوم المخصب

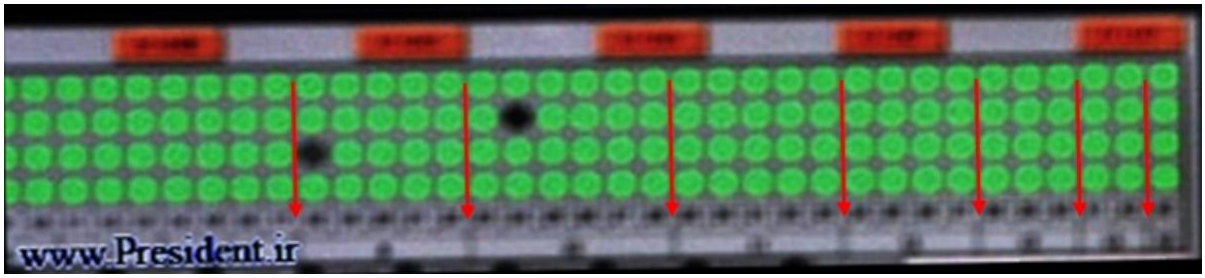


Before Attack

المنشأة الصناعية قبل الهجوم الالكتروني

المنشأة الصناعيةخلال التعرض لهجمات إلكترونية During Attack

هذا التصوير يبين فرز الفقرات بالخط الأحمر لتشكل صفوف متتالية من اليمين 4 ثم 12 , 16 , 20 ,24 وهي نفس المقادير التي شوهدت بالمخطط البياني السابق .



أما هنا المخطط القياسي لأجهزة الطرد المركزي في مفاعل نطنز النووي

IR-1 cascade model

RCG	1							2							3							4							5							6						
Line 1			⊕		⊕	⊕	⊕		⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Line 2	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Line 2	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Line 4			⊕		⊕	⊕	⊕		⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Row	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Stage	1	2	3	4	5	6		7		8		9				10							11						12							13				14			15	

RCG: Rotor Control Group, a group of up to 28 centrifuges Stage: Enrichment stage, with the general flow direction from right to left

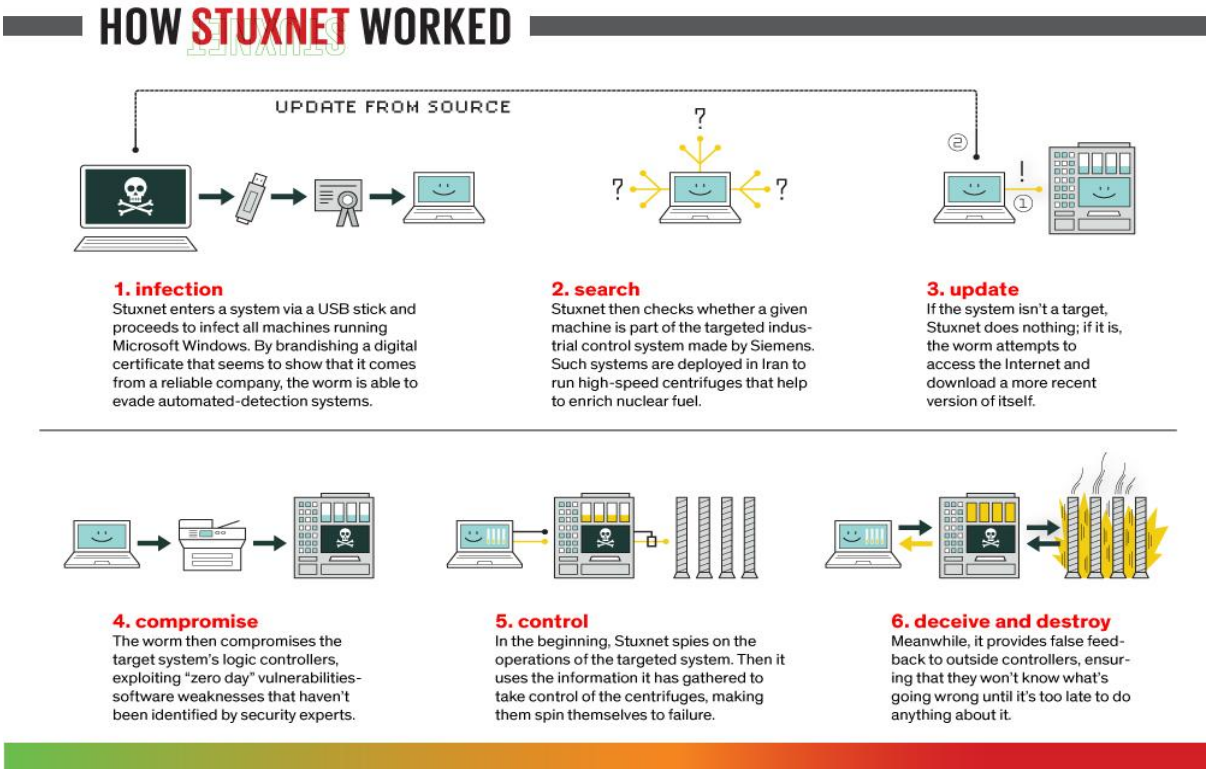
Row: Row number of a centrifuge quadruple, corresponding to the floor markings

أوجه الشبه في جميع المقاييس الرسمية للمفاعل تتضح بمجال لا يدعى للشك بأن ستاكس نت صُمم بصورة خاصة لمفاعل نطنز.

تحليل إستراتيجيةستاكس نت.

ما بعد الهندسة العكسية لأي برمجية خبيثة أو حتى تطبيق تتضح إستراتيجية المبرمج وما كان يريديه ويفهم نمطه وأسلوبه

بعد الهندسة العكسية الكاملة لستاكس نت ومقارنته بالتأسيسات المبينة في المفاعل النووي نطنز أتضح بأن الهدف الرئيسي له ليس التخريب وإنما التحكم المخفي على أساس التلاعب في أجهزة الطرد المركزي. أي أشبه بفخ مزروع يستفيد من الحفرات لإيقاع خسائر غير مرئية للعين المجردة .



تحليل عمل كود FC6082

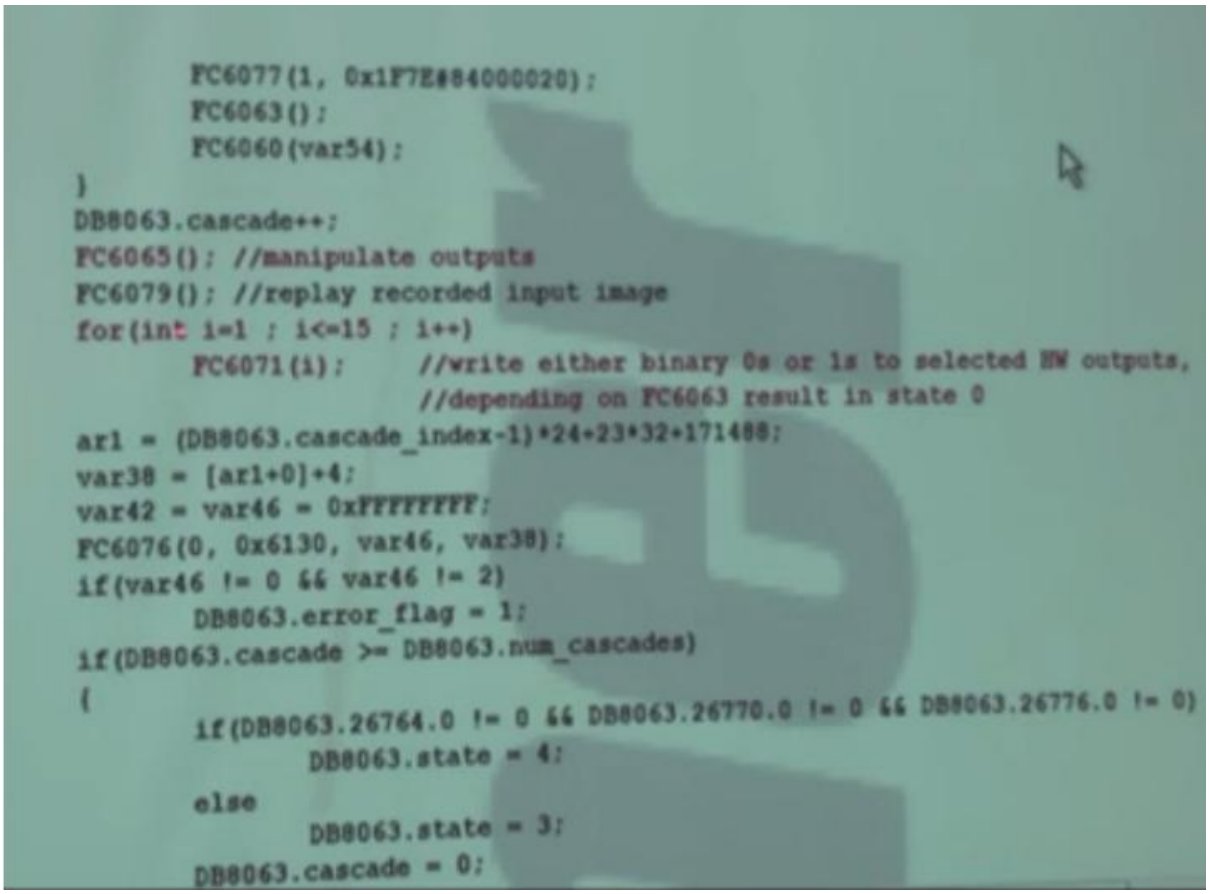
يتكون الكود المذكور من 8 مراحل مجزأة وتتم المهاجمة لستاكس من من المرحلة الثانية إلى السادسة .تبدأ المرحلة رقم صفر بمقادير أولية وتكون عبارة عن عملية رصد بحتة . في هذه المرحلة يجب تحقيق شرطين :

1- تثبيت process image Inter خلال 20 ثانية .

مهمة هذه العملية هي خداع النظام في تسجيل الدخول .

2- تنفيذ مخطط الحملة الحقيقية لستاكس نت حسب ما كتب في السورس كود .

وتلك المراحل تتم من بشكل متتالي وسريع .



```
        FC6077(1, 0x1F7E#84000020);
        FC6063();
        FC6060(var54);
}
DB8063.cascade++;
FC6065(); //manipulate outputs
FC6079(); //replay recorded input image
for(int i=1 ; i<=15 ; i++)
        FC6071(i);      //write either binary 0s or 1s to selected HW outputs,
                        //depending on FC6063 result in state 0
ar1 = (DB8063.cascade_index-1)*24+23*32+171488;
var38 = [ar1+0]+4;
var42 = var46 = 0xFFFFFFFF;
FC6076(0, 0x6130, var46, var38);
if(var46 != 0 && var46 != 2)
        DB8063.error_flag = 1;
if(DB8063.cascade >= DB8063.num_cascades)
{
        if(DB8063.26764.0 != 0 && DB8063.26770.0 != 0 && DB8063.26776.0 != 0)
                DB8063.state = 4;
        else
                DB8063.state = 3;
        DB8063.cascade = 0;
```

FC 6065 () ; //manipulate outputs

الخروج الأولي بشكل متلاعب .

FC 6079 () ; //replay recorded input image

وبشكل متزامن تصوير العمليات يُرسل على شاشات التحكم وفي هذه الحالة لا يمكن للكوادر البشرية المراقبة لأجهزة التحكم الصنا عي .

ملاحظة الخلل الذي يسببه ستاكس نت على أجهزة الطرد المركزي.

ويتم تكرار هذه العملية في الخروج .

تحليل عمل كود FC6064

قبل تنفيذ هجمة ستاكس نت يجب تنفيذ عدة شروط لعمله .
وهناك 3 شروط يجب أن تتحقق قبل عمل ستاكس نت وهي كالتالي

الشرط الأول : يجب أن تكون عدد الأيام التي يجب أن يقضيها ستاكس نت هي 297 يوم أو أكثر .

الشرط الثاني : في حال تحققت الشروط التالية :

1- جميع أجهزة التخصيب يجب أن يكون مدة عملها 3 أيام أو أكثر .

2- على أقل شرط يجب أن يكون جهاز واحد من أجهزة التخصيب قد دخل في الخدمة لأكثر من 35 يوم.

3- على الأقل تنظيم علم في جهاز التخصيب حسب البلوك 8063

4- البلوك DB8062.w12 < =5 أو FC6057 == صحيح .

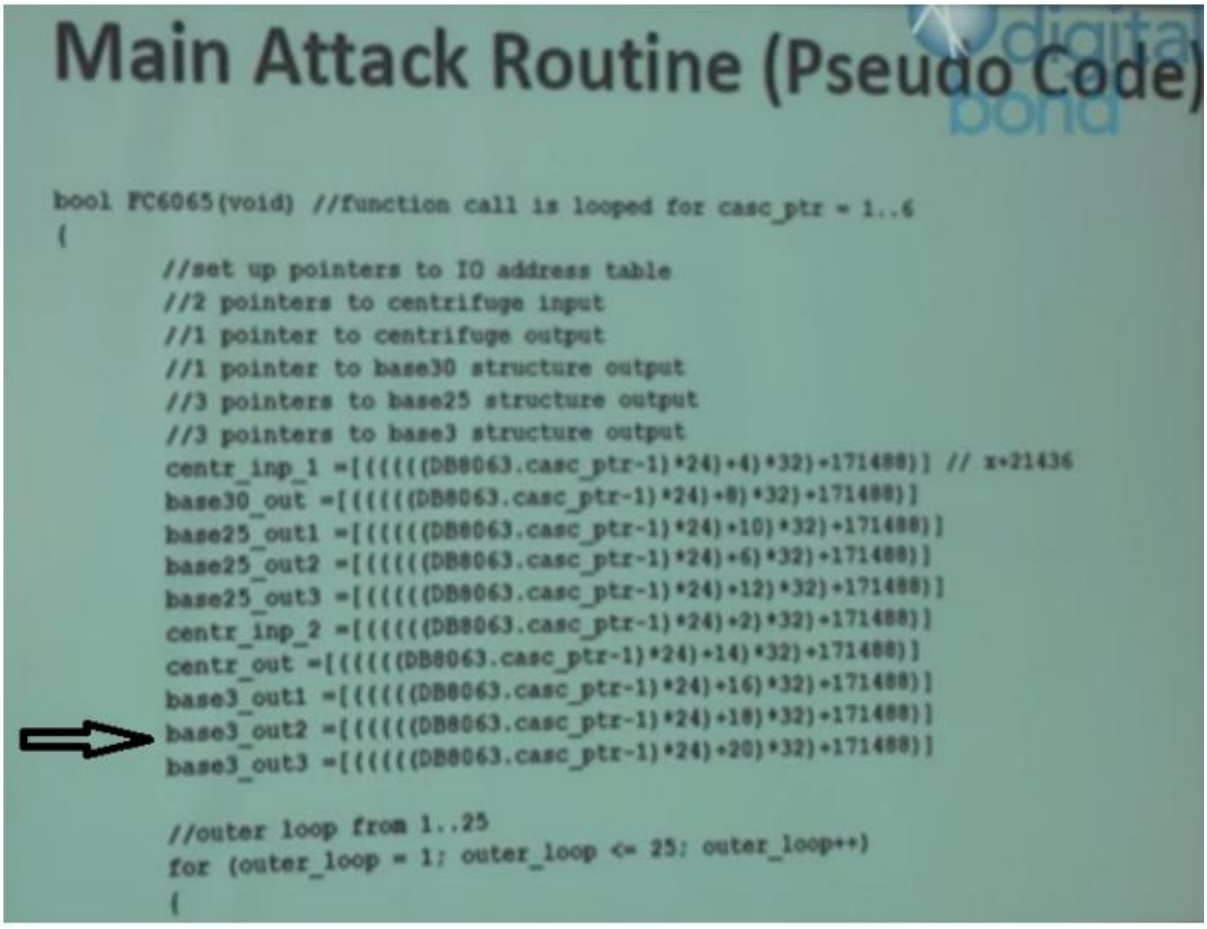
5- يجب على أقل تقدير تشغيل أحد أجهزة التخصيب بين 17 إلى 18 ساعة .

الشرط الثالث : D28 يجب أن تكون منظمة في البلوك DB8061 .

تحليل عمل كود FC6065

يتمثل عمل هذا الكود بعملية الخروج الرئيسية لستاكس نت ,وأيضا له الوظيفة الرئيسية للبرمجية الخبيثة .

القسم الأول للكود التخريبي لستاكس نت لحظة الخروج والمربوط بالبلوك FC6065

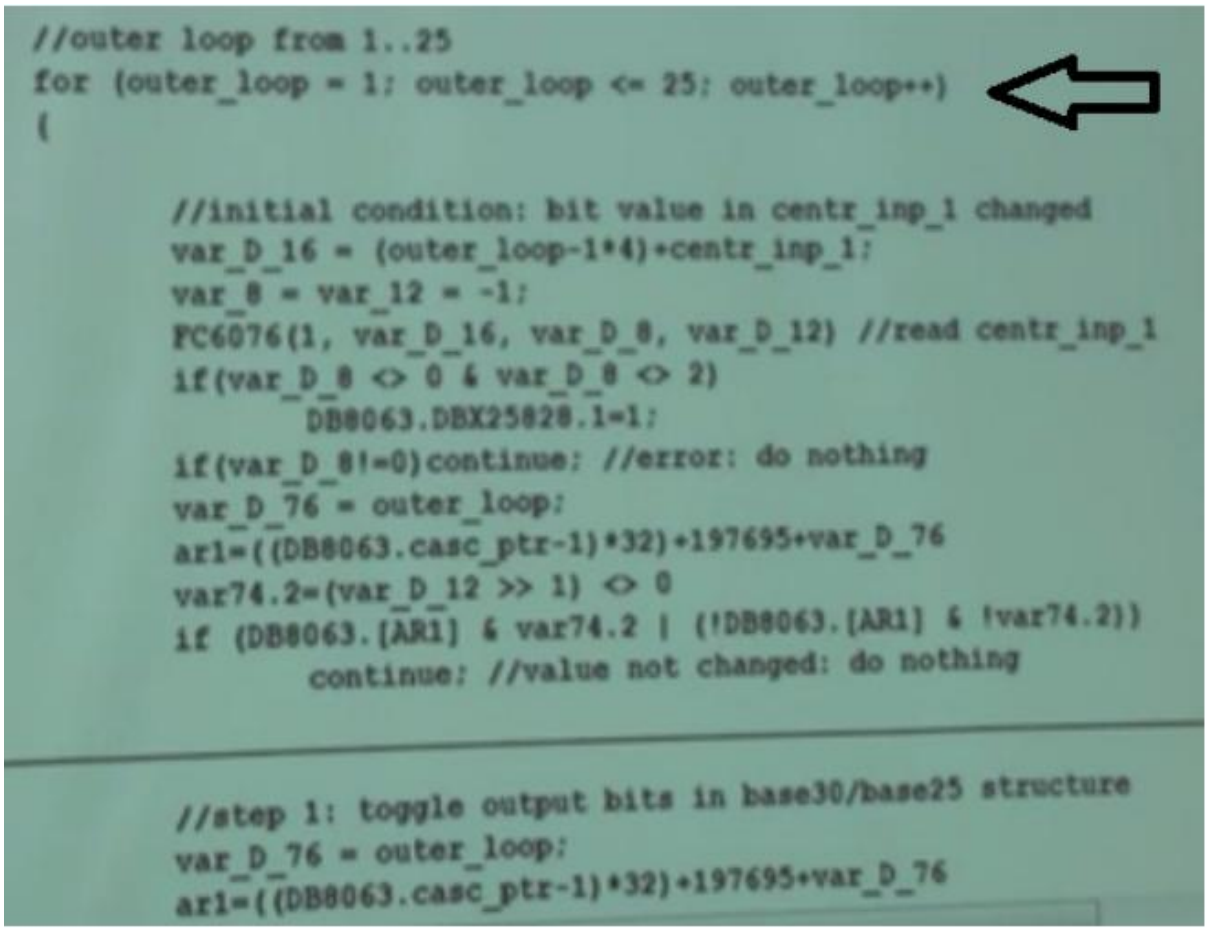


نلاحظ من التحليل العكسي للكود السابق بأنه كما هو معروف بأن مفاعل نطنز النووي هو كأي مفاعل نووي تعتبر المعلومات

حول أجهزة تخصيب اليورانيوم وأجهزة الطرد المركزي أيضاً مقادير الدخول والخروج معلومات سرية للغاية .

نشاهد في الصورة بأن الهيكل base3_out2 مرتبط بجهاز التخصيب الثالث.

ونلاحظ أيضاً تكرار الهجمة في الحلقة 25 به عبارة أخرى كان الهجوم يتركز في المرحلة25



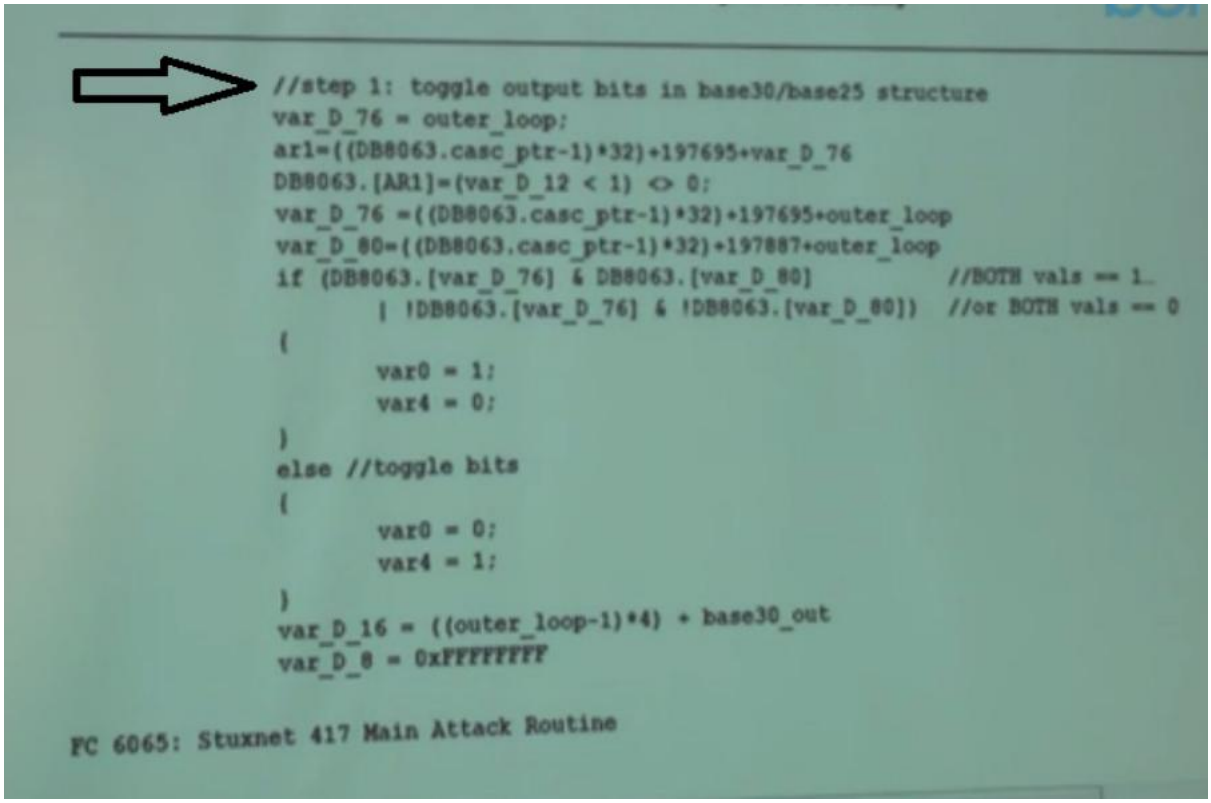
```
//outer loop from 1..25
for (outer_loop = 1; outer_loop <= 25; outer_loop++)
{

        //initial condition: bit value in centr_inp_1 changed
        var_D_16 = (outer_loop-1*4)+centr_inp_1;
        var_8 = var_12 = -1;
        FC6076(1, var_D_16, var_D_8, var_D_12) //read centr_inp_1
        if(var_D_8 <> 0 & var_D_8 <> 2)
                DB8063.DBX25828.1=1;
        if(var_D_8!=0)continue; //error: do nothing
        var_D_76 = outer_loop;
        ar1=((DB8063.casc_ptr-1)*32)+197695+var_D_76
        var74.2=(var_D_12 >> 1) <> 0
        if (DB8063.[AR1] & var74.2 | (!DB8063.[AR1] & !var74.2))
                continue; //value not changed: do nothing


        //step 1: toggle output bits in base30/base25 structure
        var_D_76 = outer_loop;
        ar1=((DB8063.casc_ptr-1)*32)+197695+var_D_76
```

القسم الثالث للبلوك السابق الخاص بستاكس نت عند مرحلة الخروج.

في هذا القسم يتضح أيضاً بأن من قام بكتابة أكواد البرمجية الخبيثة ستاكس نت كان على علم كامل بتأسيسات المفاعل النووي نطنز وأيضاً على معرفة بألية الدخول والخروج وعملية التخصيب .



```
//step 1: toggle output bits in base30/base25 structure
var_D_76 = outer_loop;
ar1=((DB8063.casc_ptr-1)*32)+197695+var_D_76
DB8063.[AR1]=(var_D_12 < 1) <> 0;
var_D_76 =((DB8063.casc_ptr-1)*32)+197695+outer_loop
var_D_80=((DB8063.casc_ptr-1)*32)+197887+outer_loop
if (DB8063.[var_D_76] & DB8063.[var_D_80]          //BOTH vals == 1
      | !DB8063.[var_D_76] & !DB8063.[var_D_80])   //or BOTH vals == 0
{
      var0 = 1;
      var4 = 0;
}
else //toggle bits
{
      var0 = 0;
      var4 = 1;
}
var_D_16 = ((outer_loop-1)*4) + base30_out
var_D_8 = 0xFFFFFFFF

FC 6065: Stuxnet 417 Main Attack Routine
```

في القسم الرابع من الكود السابق يتضح بأن المبرمجين لستاكس نت حاولو جاهدين بإطالة المدة الزمنية لستاكس نت في الأنظمة وعدم التخريب سعياً لعدم كشفه.

```
var=8 = FC6076(0,var0,var_D_16);     //write var0 to base30_out
if  (var_8 <> 0 && var_8 <> 2)
       DB8063.DBX25828.1=1;
var_D_16=((outer_loop-1)*4) +base25_out1
var=8 = FC6076(0,var4,var_D_16);     //write var4 to base25_out

if  (var_8 <> 0 && var_8 <> 2)
       DB8063.DBX25828.1=1;
ar1=((outer_loop-1*240)+207056)                    //25882
L74.2=!DB8063.[ar1]
var_D_76=((DB8063.casc_ptr-1)*32)+197695+outer_loop // 24711
var_D_80=((DB8063.casc_ptr-1)*32)+197887+outer_loop // 24735
L74.2 = ((DB8063.[var_D_76]&DB8063.[var_D_80]
       | !DB8063.[var_D_76] & !DB8063.[var_D_80]) & L74.2)
var_D_76=outer_loop-1*240+207056
var_D_80=((DB8063.casc_ptr-1)*32))+197695+outer_loop
ar1=((DB8063.casc_ptr-1)*32)+197887+outer_loop // 24735
L74.3 = !DB8063.[ar1]
if ((DB8063.[var_D_80] & L74.3 | !DB8063.[var_D_80] & !L74.3)
       & DB8063.[var_D_76] | L74.2)
       continue //check next condition; if not met, continue outer loop
```

تحليل عملية تزوير تسجيل الدخول في الأكواد FC6084 , FC6079

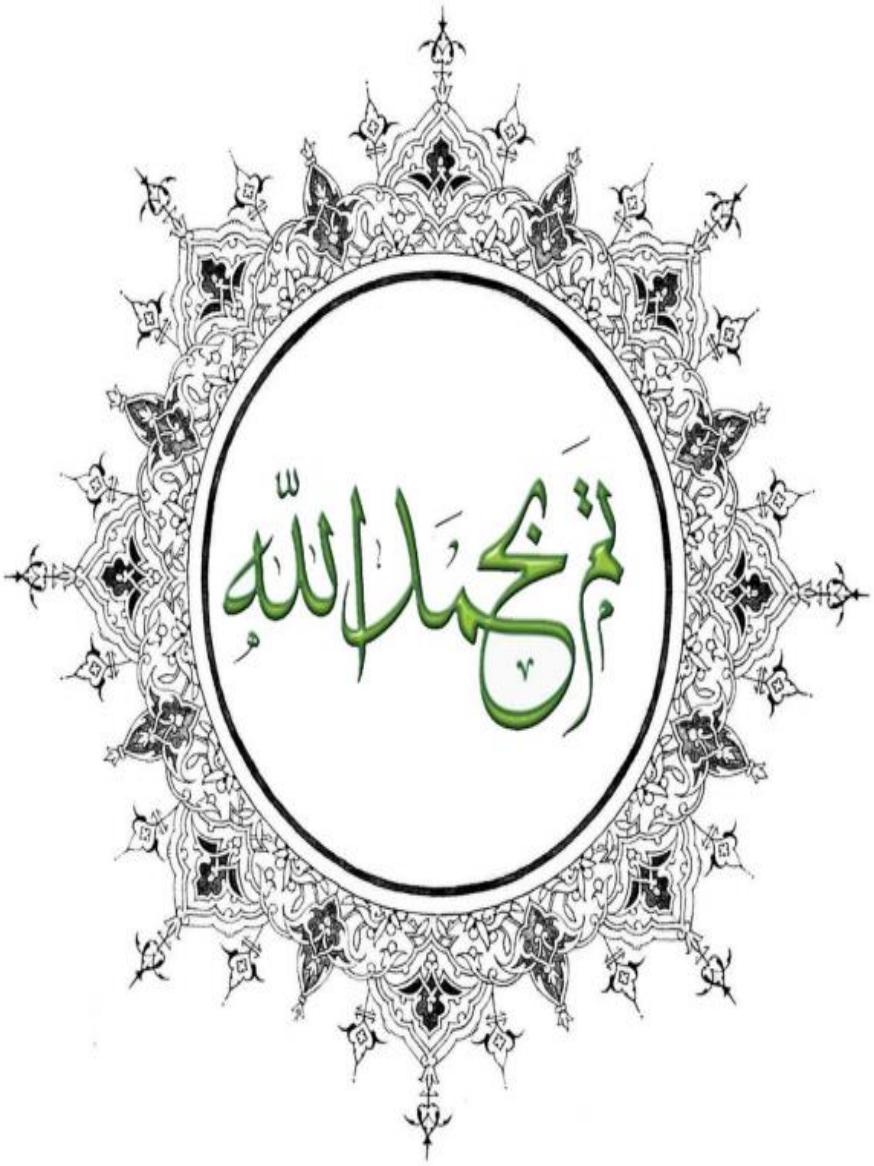
المسؤول عن خداع نظام التحكم الصناعي وإظهار معلومات مزيفة بلوك الكود FC6079 عند الدخول.

يتم من المرحلة الثانية إلى السادسة في الروتين الأصلي لستاكس البلوك FC6079 نت .

وكما ذكر بأن هذا البلوك مسؤول عن خداع النظام وإظهار معلومات مغلوطة فوظيفته الأساسية تصبح الفصل عن المراحل المنطقية للنظام وإرسال معلومات خاطئة .

النتيجة النهائية

ستاكس نت بالاستفادة من ثغرة في أنظمة التحكم الصناعي وأنظمة الويندز العاملة عليها استطاع ببساطة التحكم بعملية الدخول والخروج في أنظمة أجهزة الطرد المركزية لمفاعل نطنز النووي ا لواقع في مدينة أصفهان الإيرانية .البرمجية الخبيثة ستاكس نت استطاعت عن طريق رفع وخفض السرعة في أجهزة تخصيب اليورانيوم بأن تسبب ضرر حقيقي لمنشأة نطنز .وبناء على عدة تقارير اتضح بأن ستاكس نت استطاع تخريب ما يقارب 1000 جهاز طرد مركزي في مدة قصيرة.


تم بحمد الله