

THE BUILDING BLOCKS OF GOOD DETECTION AND RESPONSE SERVICES FOR THE ICS ENVIRONMENT

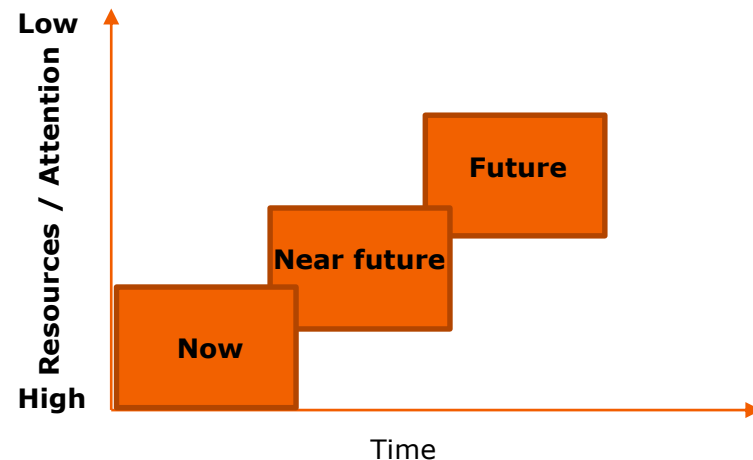


AGENDA

- **Building the right group & structure**
- **Threat intelligence and open source information**
- **Asset, network and collection**
- **Incident Response & Forensics**
- **Does it work?**

BUILDING THE RIGHT GROUP & STRUCTURE

- Build a strategy
 - Strategy: *"a plan of actions designed to achieve a long-term or overall aim"*
<https://en.oxforddictionaries.com/definition/strategy>
 - What is the business need and desirability?
 - What is your plan?
- It is important to know the objectives of the organization



BUILDING THE RIGHT GROUP & STRUCTURE

- Get the right people on the bus and in the correct seat
- Communication is key!
- SME (Subject matter expertise is very important
- A full group is around 7-10 people (to be able to work on a incident 24/7)
- Part of the work can be done by partners if needed
- The lack of understanding and communication between IT and ICS need to be eliminated!



THREAT AND THREAT INTELLIGENCE

Threat = Capability + Intent + Opportunity



THREAT AND THREAT INTELLIGENCE


Threat intelligence		
Type	Pro	Cons
Internal	Your data, full view	Costly, time, personal and skills is needed
External	Made by specialists (sometimes)	Made for a wide audience, marketing involved

Remember: People create intelligence not tools!

INFORMATION ATTACK SPACE & OPEN SOURCE INFORMATION

- OSINT is information public available
- Use OSINT to understanding your information attack space
 - PR documents, work descriptions etc.
 - Google site: and filetype:
 - Shodan.io
- It is important to understand what information is available

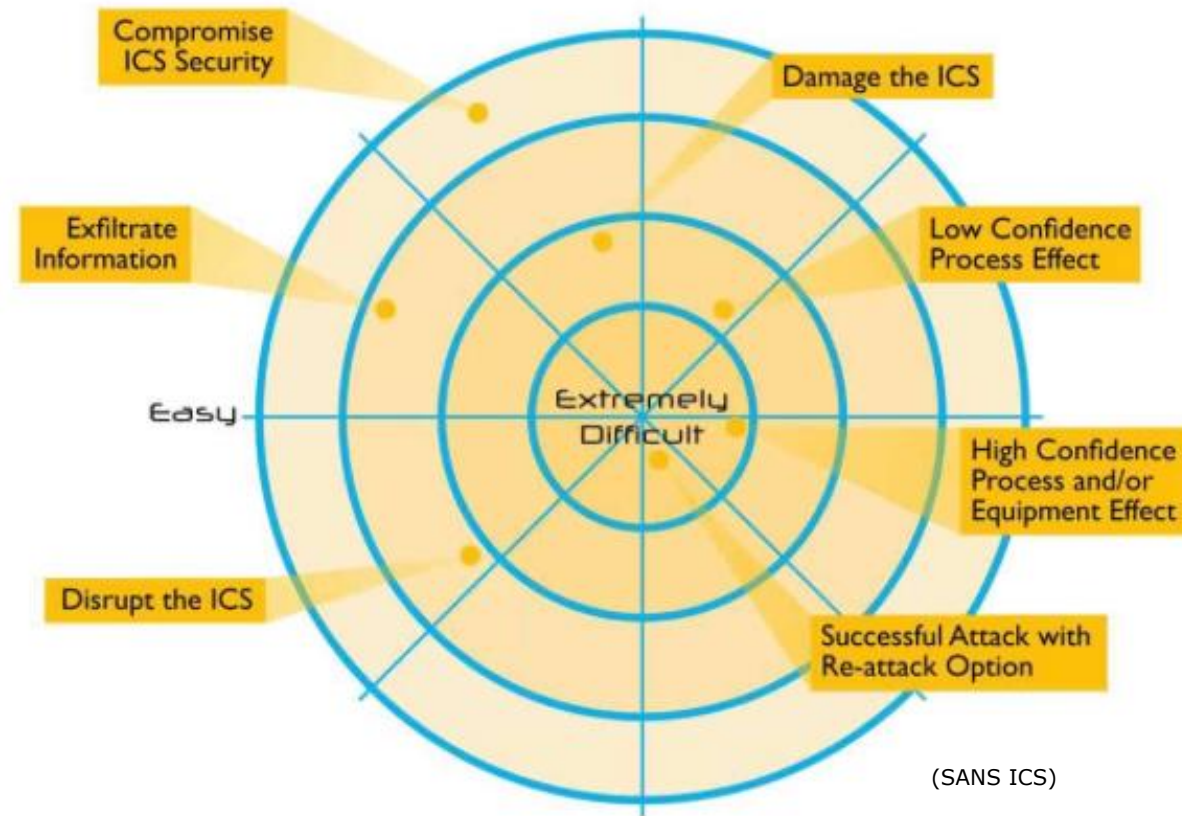


The local control system is based on ABB's S+ Operations combined with ABB AC800M controllers and I/O, and is the first such system to be delivered to  ABB commissioned the first plant at the end of 2015.

Responsibilities

5 to 7 years related experience to include experience with GE-D20, SEL-3530(RTAC), NovaTech, PLC and DCS programming and installation.

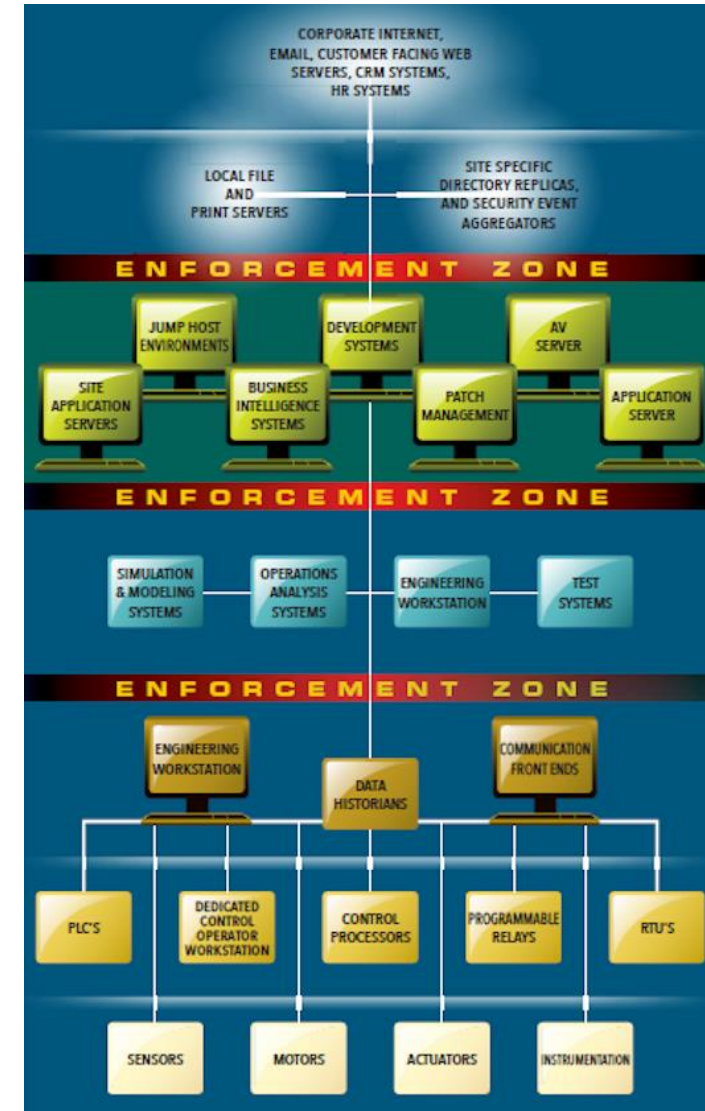
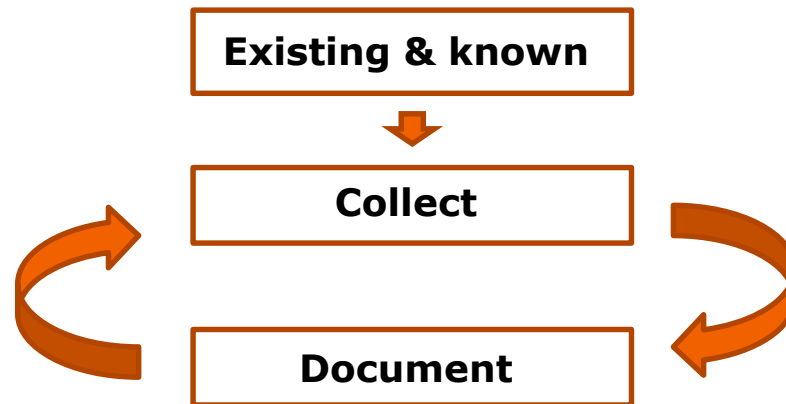
USE THE ICS ATTACK DIFFICULTY TO YOUR BENEFIT



Advanced ICS attack requires knowledge of ICS, IT, SIS and more. It is not easy.

ASSETS AND NETWORK

- Know your area of responsibility
- Separation is key (choke points)
- Know your assets and network
 - What assets do you use?
 - What protocols are in use?



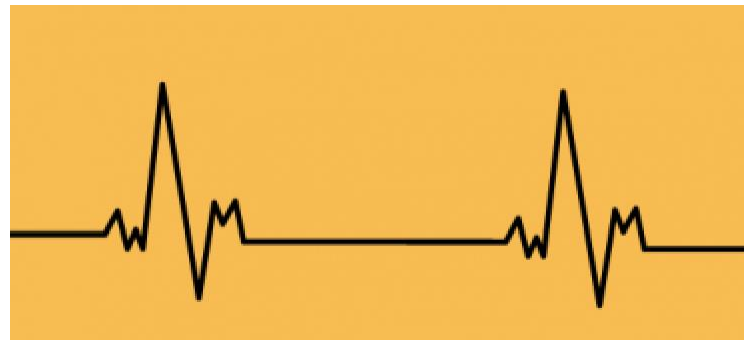
Remember active scanning is dangerous in ICS

(SANS)

WHAT TO COLLECT

Assets	Network
Type / Brand / Role	East – West flow
Protocols	North – South flow
Log / services	PCAP / IPFIX (5-Tuples)

Take memory dump of critical assets yearly



Create a baseline of Asset and Network information

Good

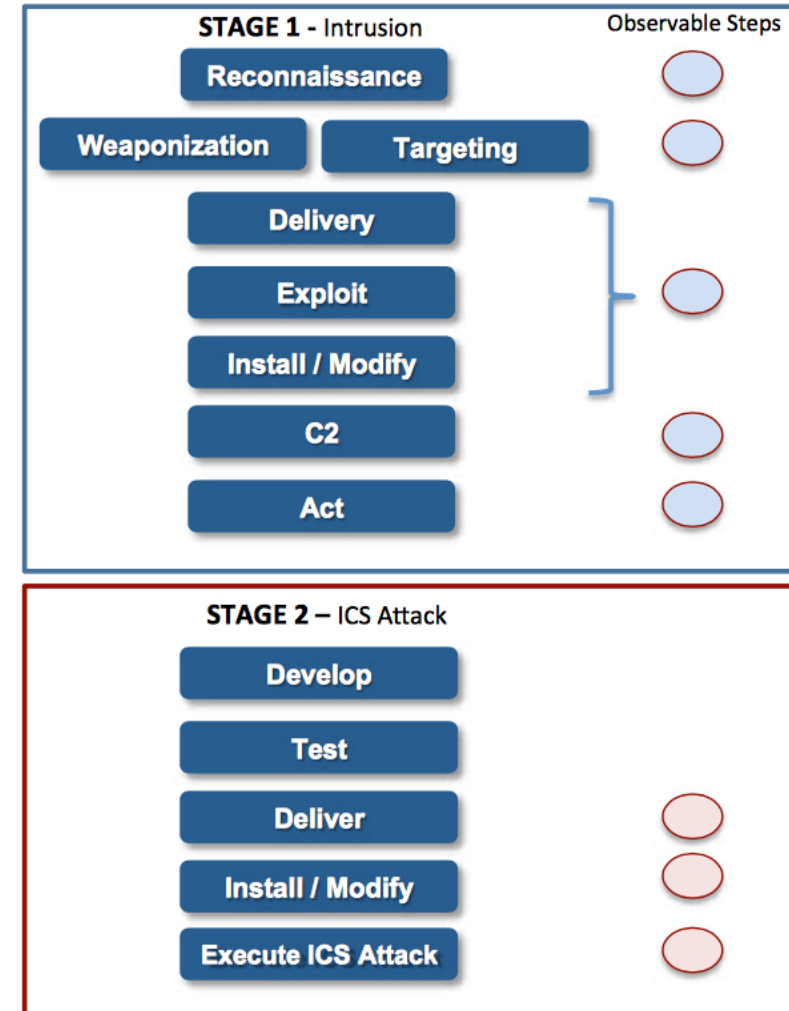
Team + Architecture + baseline (asset and network) =



Then we are ready for the incident – lets look a bit deeper

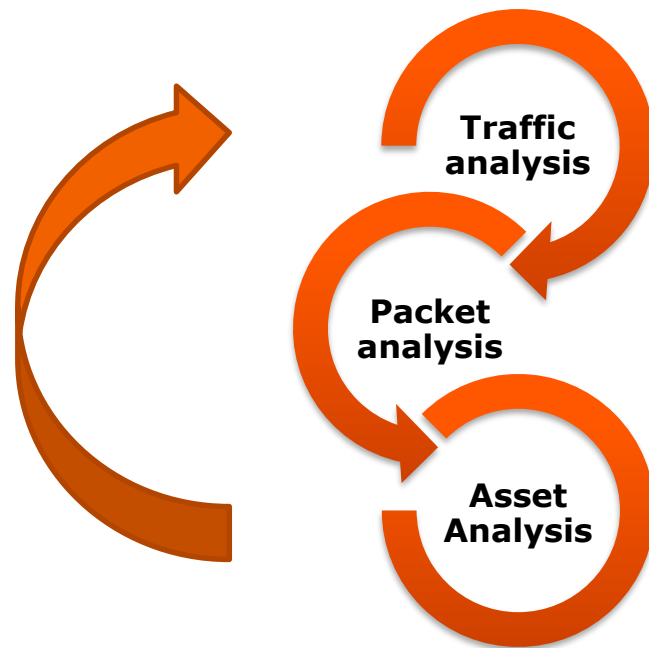
ICS CYBER KILL CHAIN

- ICS kill chain has 2 stages
- If we stop the adversary one place we stop the attack
- We need to detect and stop it before the attack is finalised



INCIDENT RESPONSE AND FORENSICS

- **Baseline and abnormality is your friend**
- **Most attacks will use C2 server (not all)**
- **Remember lateral movement**



Who

What

Where

When

How

TRAFFIC AND PACKET ANALYSIS

Traffic analysis (5-Tuples)

Source IP	Destination IP	Source port	Destination port	IP protocol	Packet count	Byte count	TCP flags	Starting time	Duration	End time
50.116.29.253	54.205.251.140	80	38869	6	1	40	RA	2014/10/13 00:02:33.513	0.000	2014/10/13 00:02:33.513
50.116.29.253	63.131.206.19	80	58854	6	1	40	RA	2014/10/13 01:09:42.456	0.000	2014/10/13 01:09:42.456
50.116.29.253	63.131.206.19	80	58855	6	1	40	RA	2014/10/13 01:09:42.504	0.000	2014/10/13 01:09:42.504
50.116.29.253	185.4.227.195	80	4355	6	1	40	RA	2014/10/13 04:19:30.391	0.000	2014/10/13 04:19:30.391
50.116.29.253	190.144.2.10	80	2278	6	1	40	RA	2014/10/13 04:23:36.297	0.000	2014/10/13 04:23:36.297

Packet analysis (PCAP)

104	2017-06-30 10:27:09.750265	172.20.0.126	172.20.0.128	S7COMM	90	R0SCTR: [Job] Function: [Write Var]
122	2017-06-30 10:27:09.756725	172.20.0.128	172.20.0.126	S7COMM	76	R0SCTR: [Ack_Data] Function: [Write Var]

▶ Frame 104: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
 ▶ Ethernet II, Src: HewlettP_00:34:40 (08:2e:5f:00:34:40), Dst: SystemeH_01:27:82 (24:ea:40:01:27:82)
 ▶ Internet Protocol Version 4, Src: 172.20.0.126, Dst: 172.20.0.128
 ▶ Transmission Control Protocol, Src Port: 58660 (58660), Dst Port: 102 (102), Seq: 1, Ack: 1, Len: 36
 ▶ TPCKT, Version: 3, Length: 36
 ▶ ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
 ▼ S7 Communication
 ▶ Header: (Job)
 ▼ Parameter: (Write Var)
 Function: Write Var (0x05)
 Item count: 1
 ▼ Item [1]: (DB32.DBX 2.1 BIT 1)
 Variable specification: 0x12
 Length of following address specification: 10
 Syntax Id: S7ANY (0x10)
 Transport size: BIT (1)
 Length: 1
 DB number: 32
 Area: Data blocks (DB) (0x84)
 ▶ Address: 0x000011

What to Look for

External communication

Encrypted communication

Top takers

Low talkers

Abnormalities in communication

DNS names

Commercial tools like KICS makes it more easy

ASSET ANALYSIS

- Highly volatile data
- Take the memory dump fast (no reboot)
- Read it with e.g. Volatility or Redline
- Memory analysis

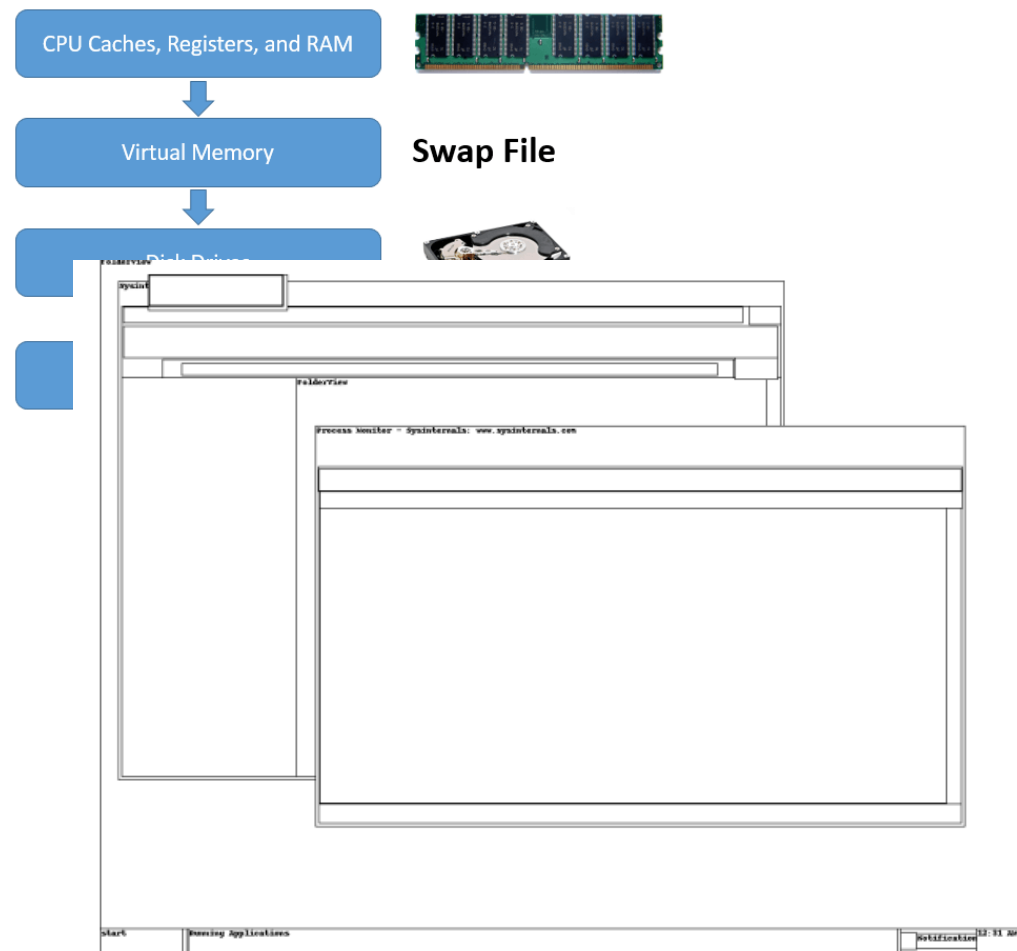
```
remnux@remnux:~/Desktop/ICS2017$ volatility -f stuxnet.vmem --profile=Win7SP1x64 imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86
AS Layer1 : IA32PagedMemoryPae (Kernel AS)
AS Layer2 : FileAddressSpace (/home/remnux/Desktop/ICS2017/stuxnet.vmem)
PAE type : PAE
DTB : 0x319000L
KDBG : 0x80545ae0

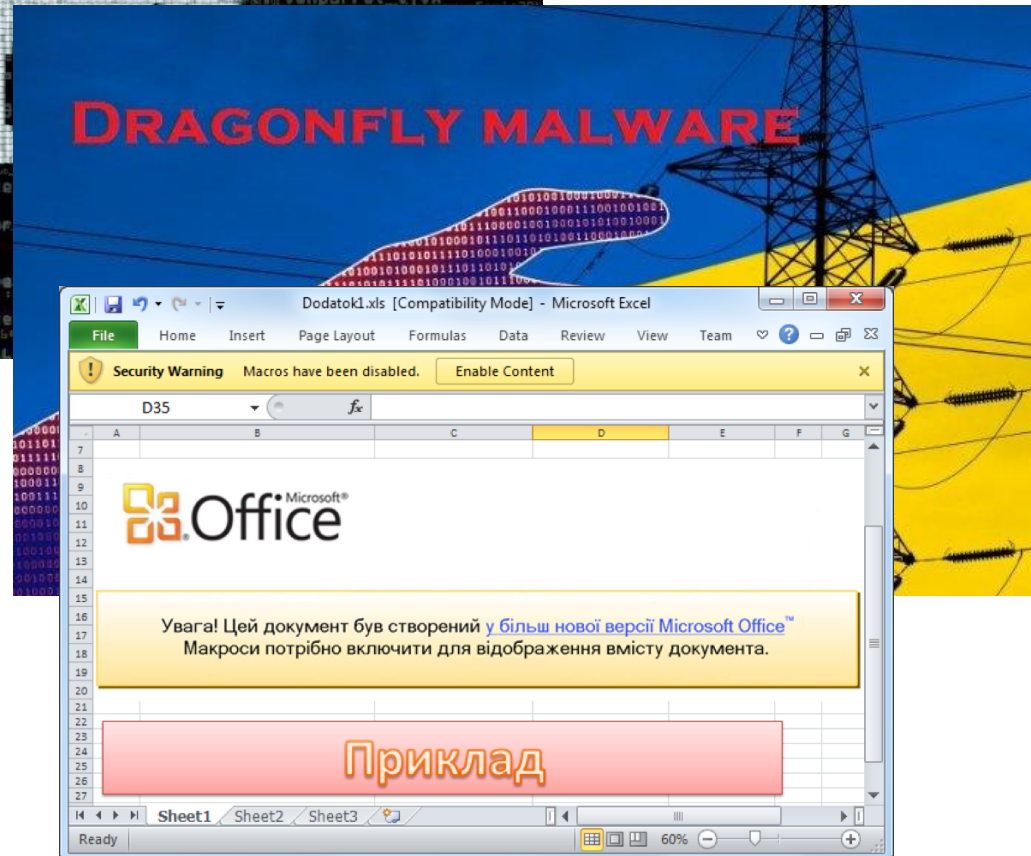
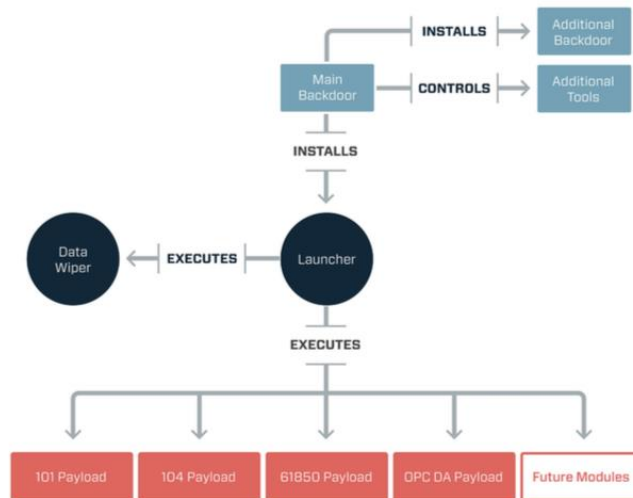
Number of Processes: 1
remnux@remnux:~/Desktop/ICS2017$ volatility -f stuxnet.vmem malfind
Image Type (Service Process) : Volatility Foundation Volatility Framework 2.4
KPCR for Process: csrss.exe Pid: 600 Address: 0x7f6f0000
KUSER_SHARED Va Tag: Vad Protection: PAGE_EXECUTE_READWRITE
Image date and time: 0x7f6f0000
Image local date and time: 0x7f6f0000

0x7f6f0000 c8 00 00 00 1f 01 00 00 ff ee ff ee 08 70 00 00 .....p..
0x7f6f0010 08 00 00 00 00 fe 00 00 00 00 10 00 00 20 00 00 .....
0x7f6f0020 00 02 00 00 00 20 00 00 8d 01 00 00 ff ef fd 7f .....
0x7f6f0030 03 00 08 06 00 00 00 00 00 00 00 00 00 00 00 00 .....

0x7f6f0000 c8000000 ENTER 0x0, 0x0
0x7f6f0004 1f POP DS
0x7f6f0005 0100 ADD [EAX], EAX
0x7f6f0007 00ff ADD BH, BH
0x7f6f0009 ee OUT DX, AL
0x7f6f000a ff DB 0xff
0x7f6f000b ee OUT DX, AL
```



DOES IT WORK?



QUESTIONS



THANK YOU FOR LISTENING

