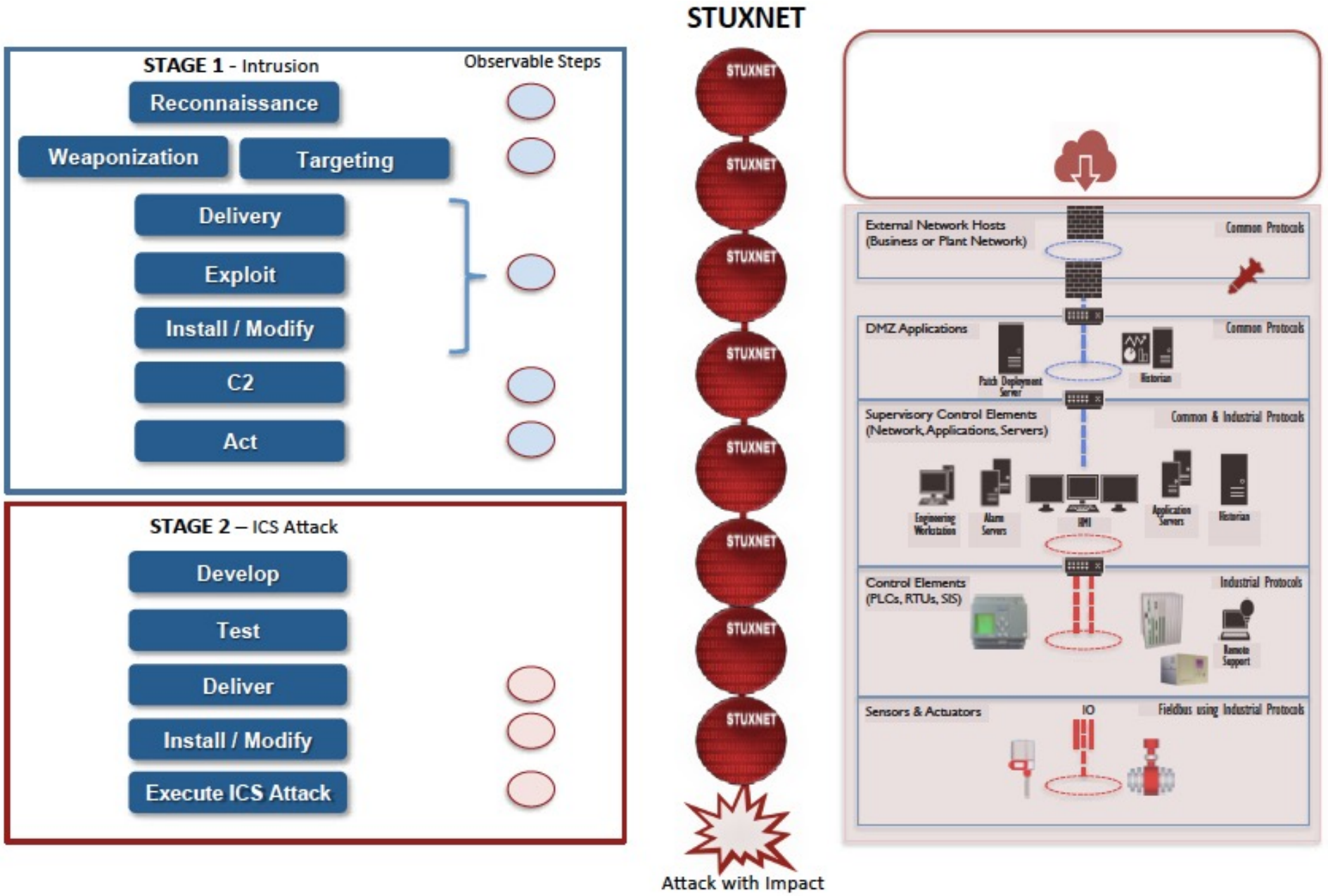
Case Studies

Chris Hankin

STUXNET

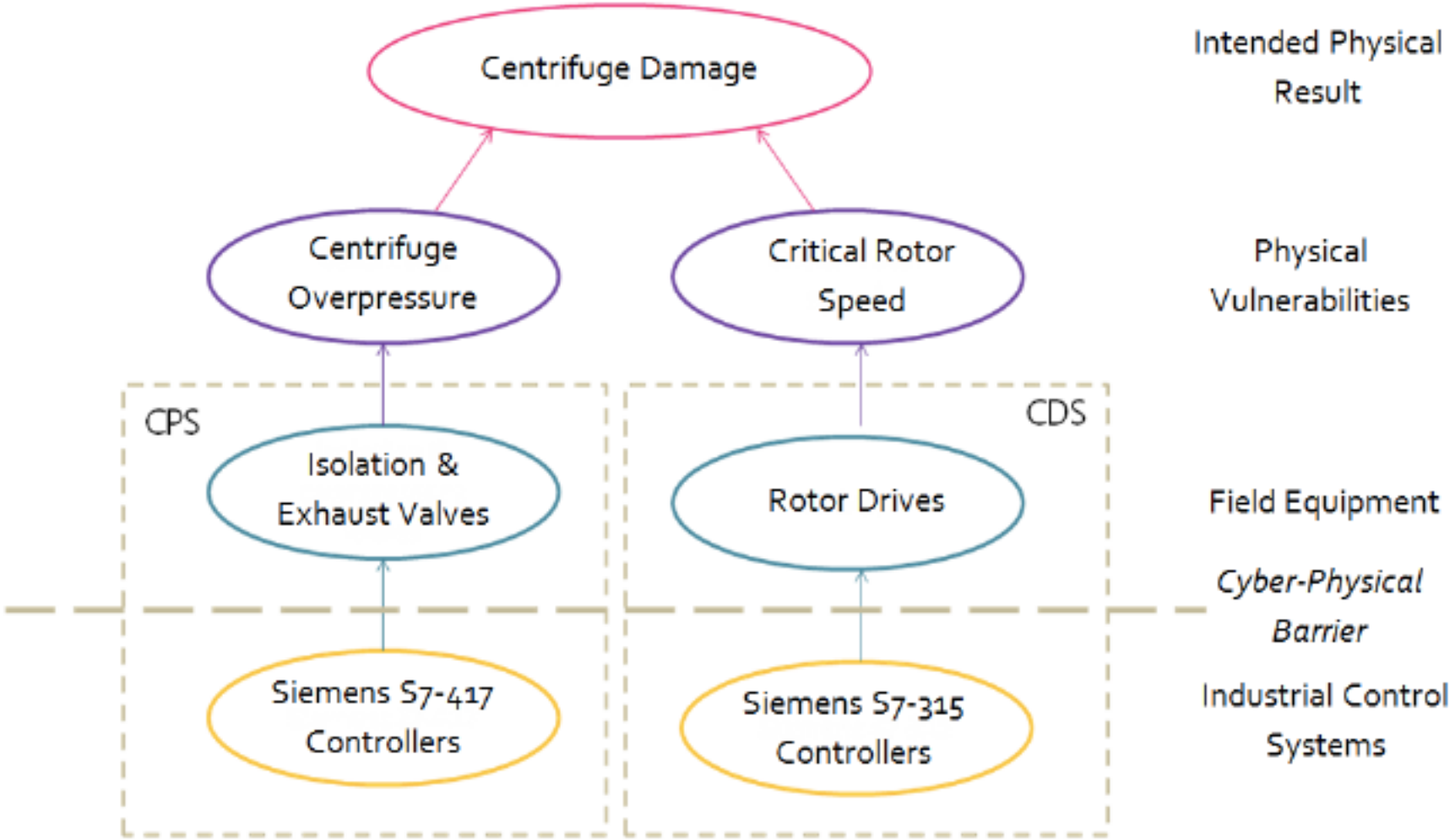


SANS Institute: The Industrial Control System Cyber Kill Chain

3 layers and their functions

- IT Layer – spread of malware
- Control system layer – manipulation of process control
- Physical layer – where the actual damage is created

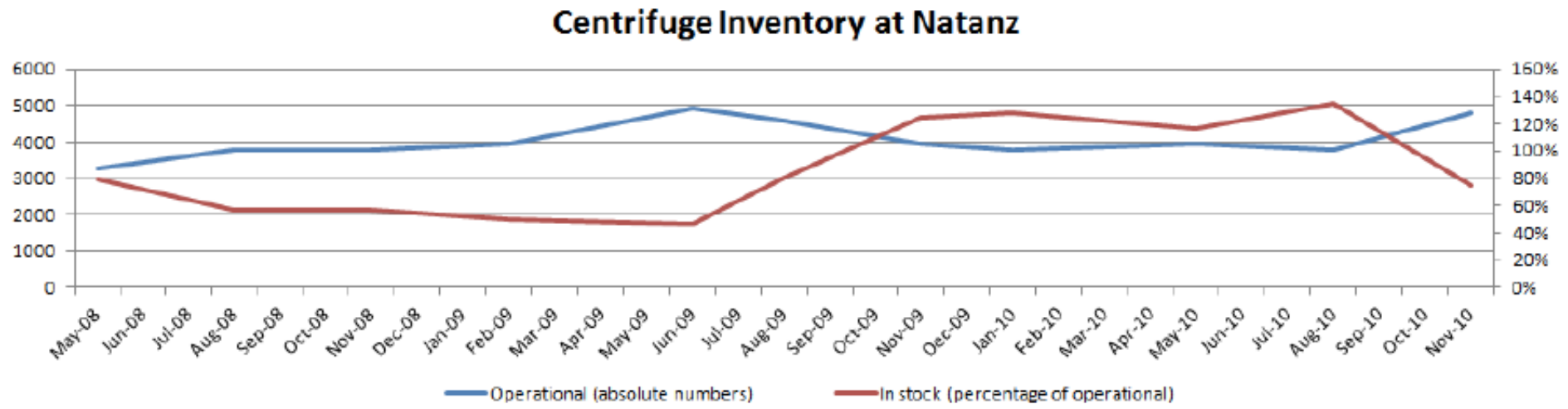
Two attack vectors (Langner)



Two attack vectors

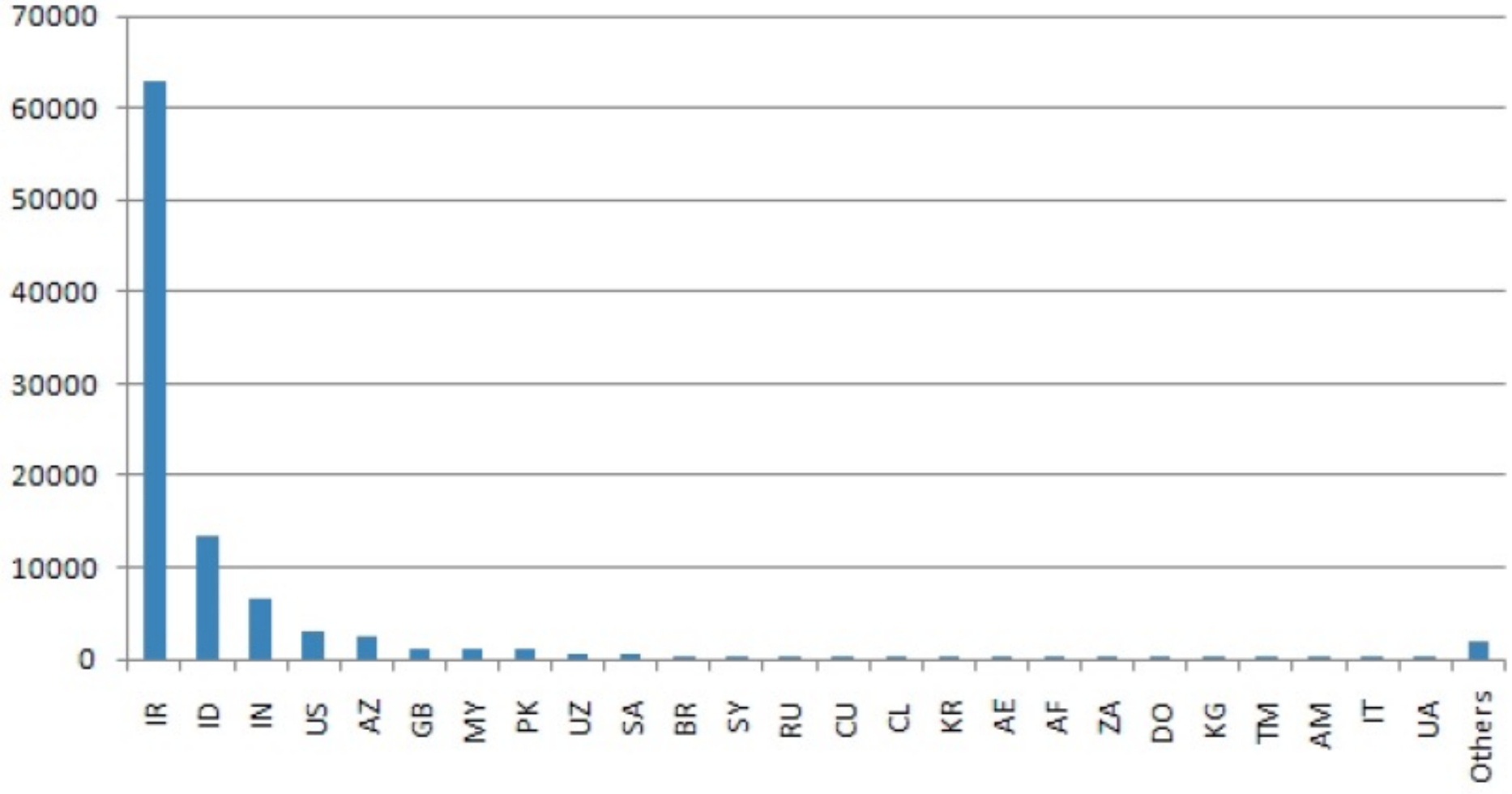
- CPS: cascade protection system – fault tolerance in cascades of centrifuges including pressure relief mechanisms.
- One Siemens S7-417 for 6 cascades (984 centrifuges)
- Man-in-the-middle attack
- CDS: centrifuge drive system – controls rotor speeds.
- Self-replication method
- One Siemens S7-315 for 164 drives

Disruption



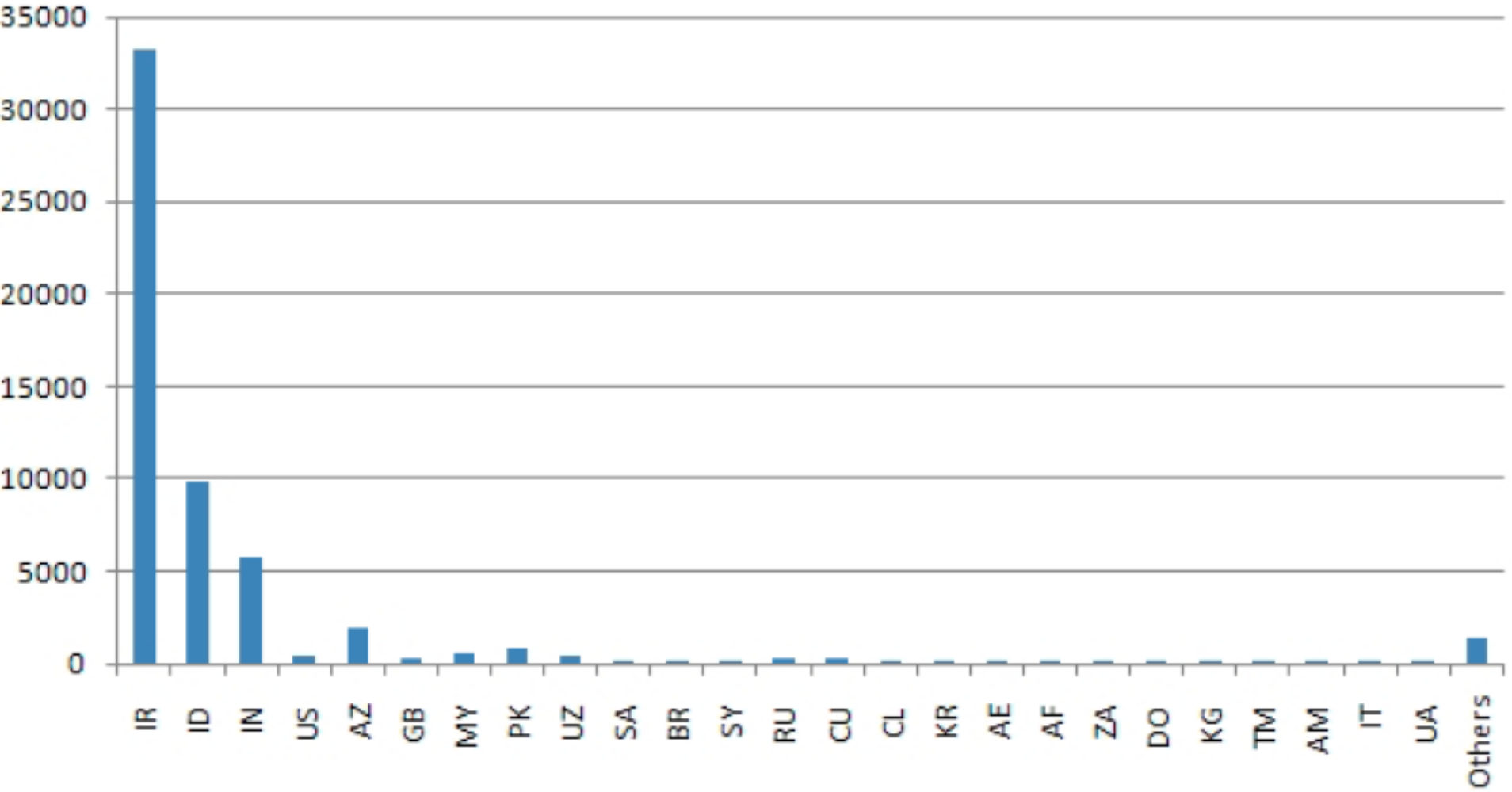
From *To kill a centrifuge,* white paper by Ralph Langner

Unique infected hosts (29.09.2010)



Symantec: W.32 Stuxnet Dossier

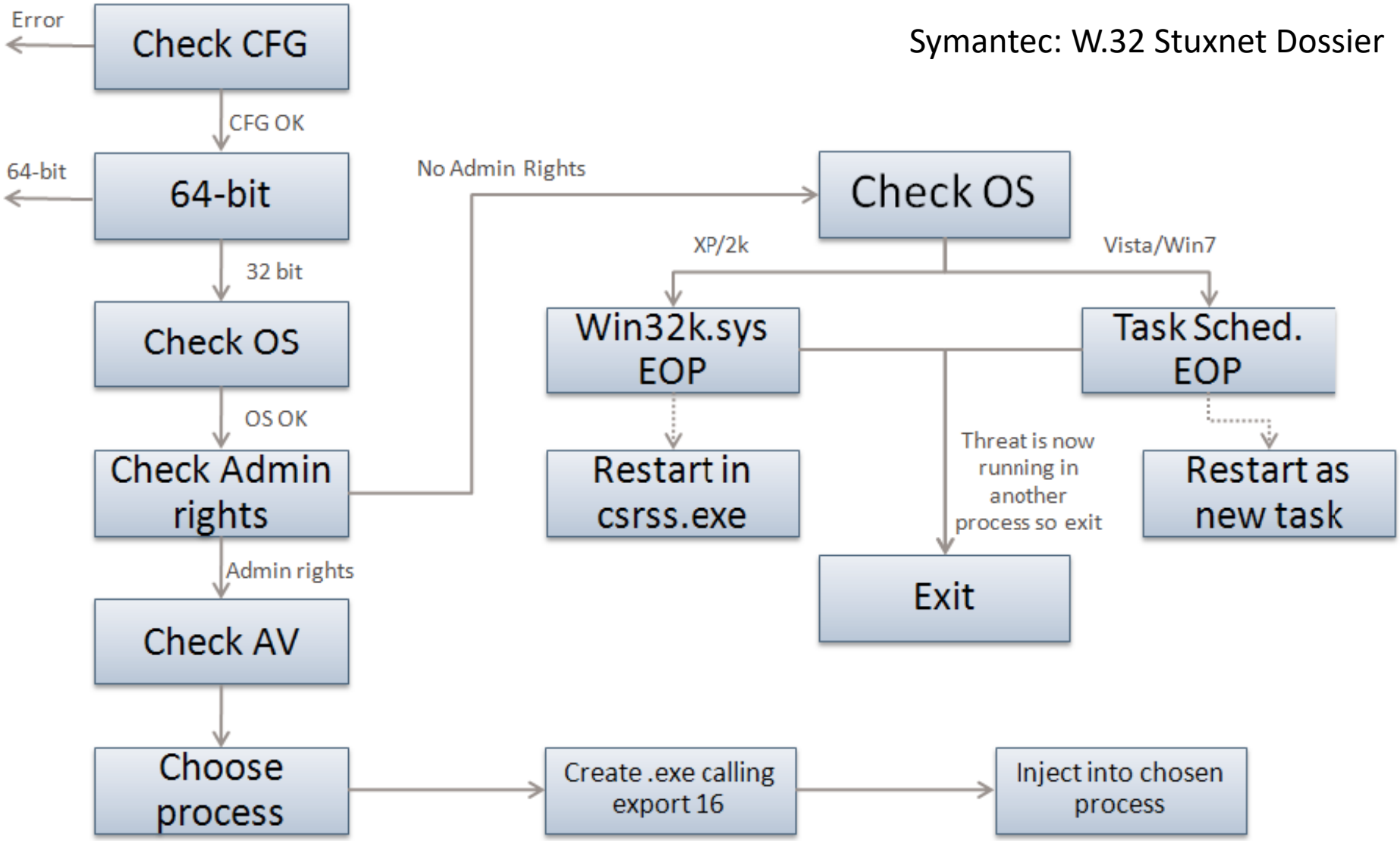
Infected Organizations



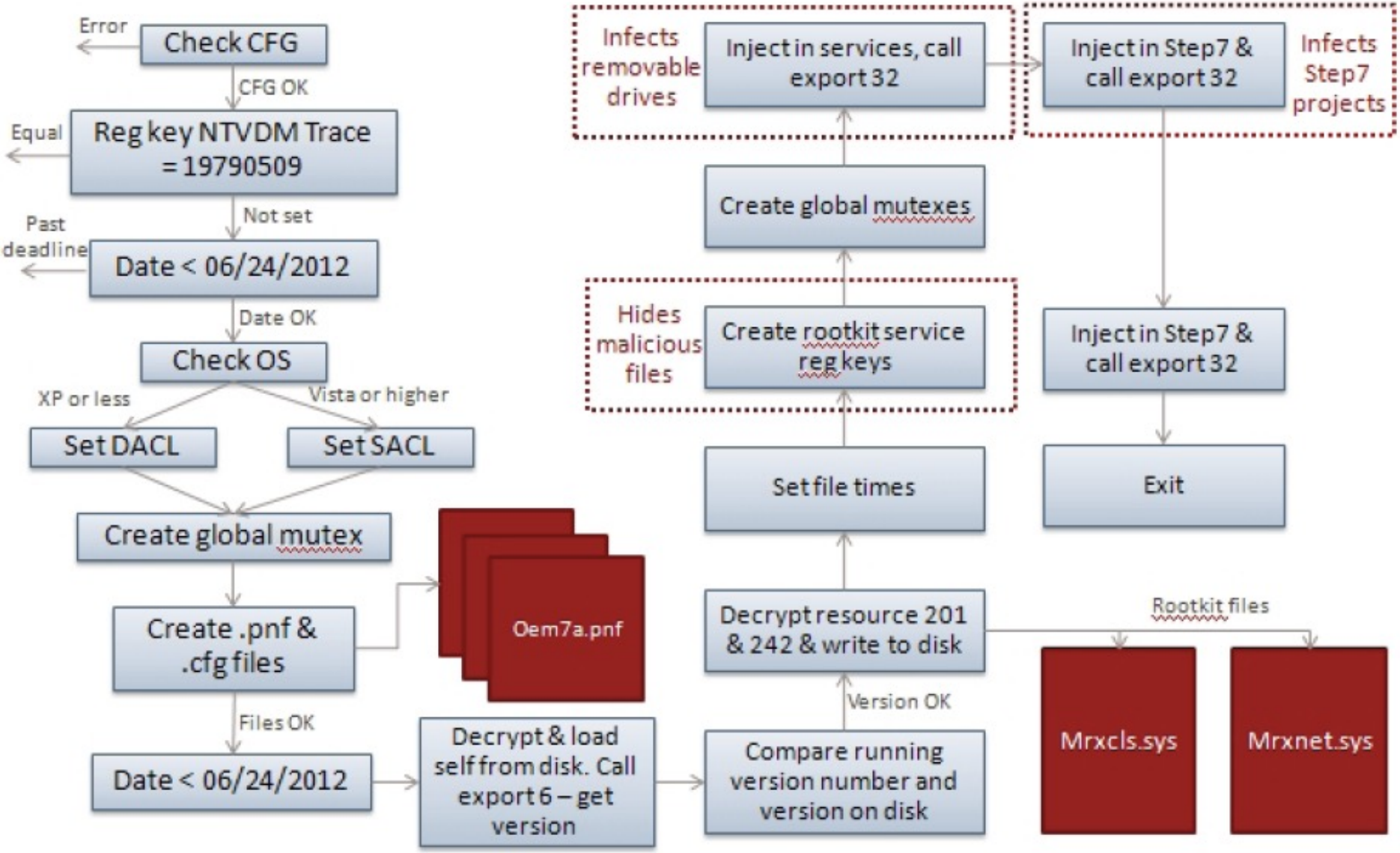
Symantec: W.32 Stuxnet Dossier

Installation

Symantec: W.32 Stuxnet Dossier

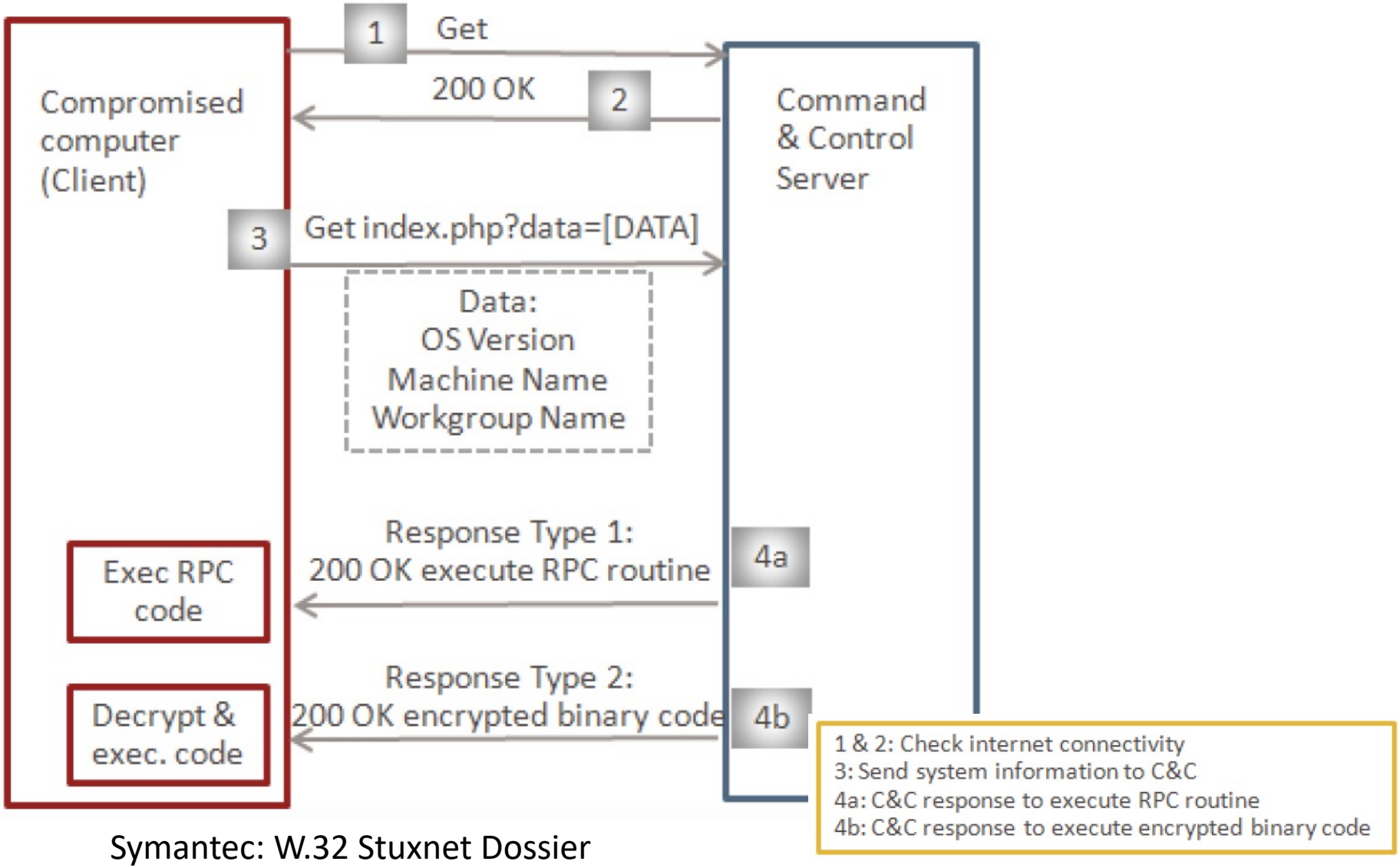


Export 16



Symantec: W.32 Stuxnet Dossier

Command and Control

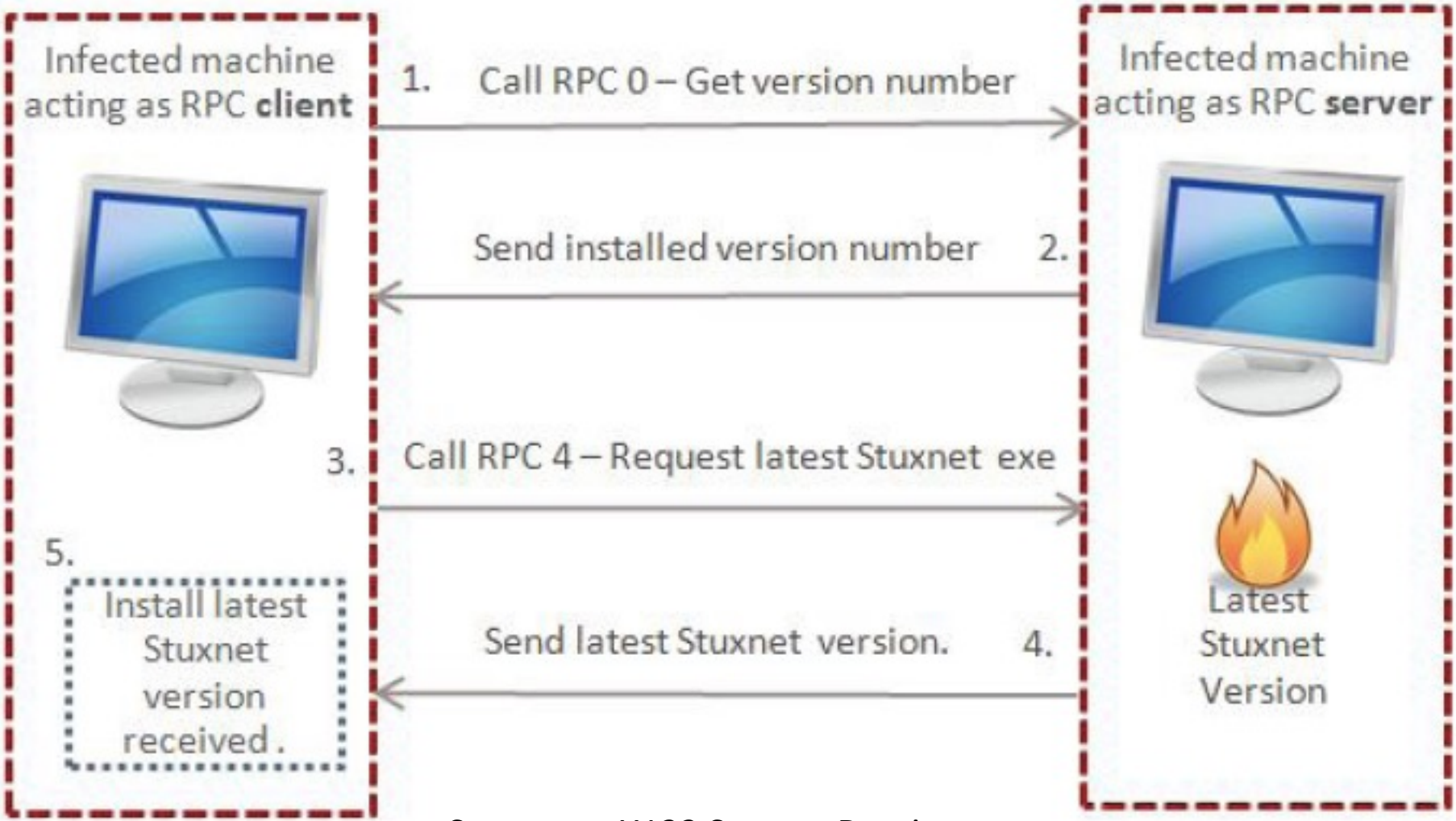


Symantec: W.32 Stuxnet Dossier

Network Propagation

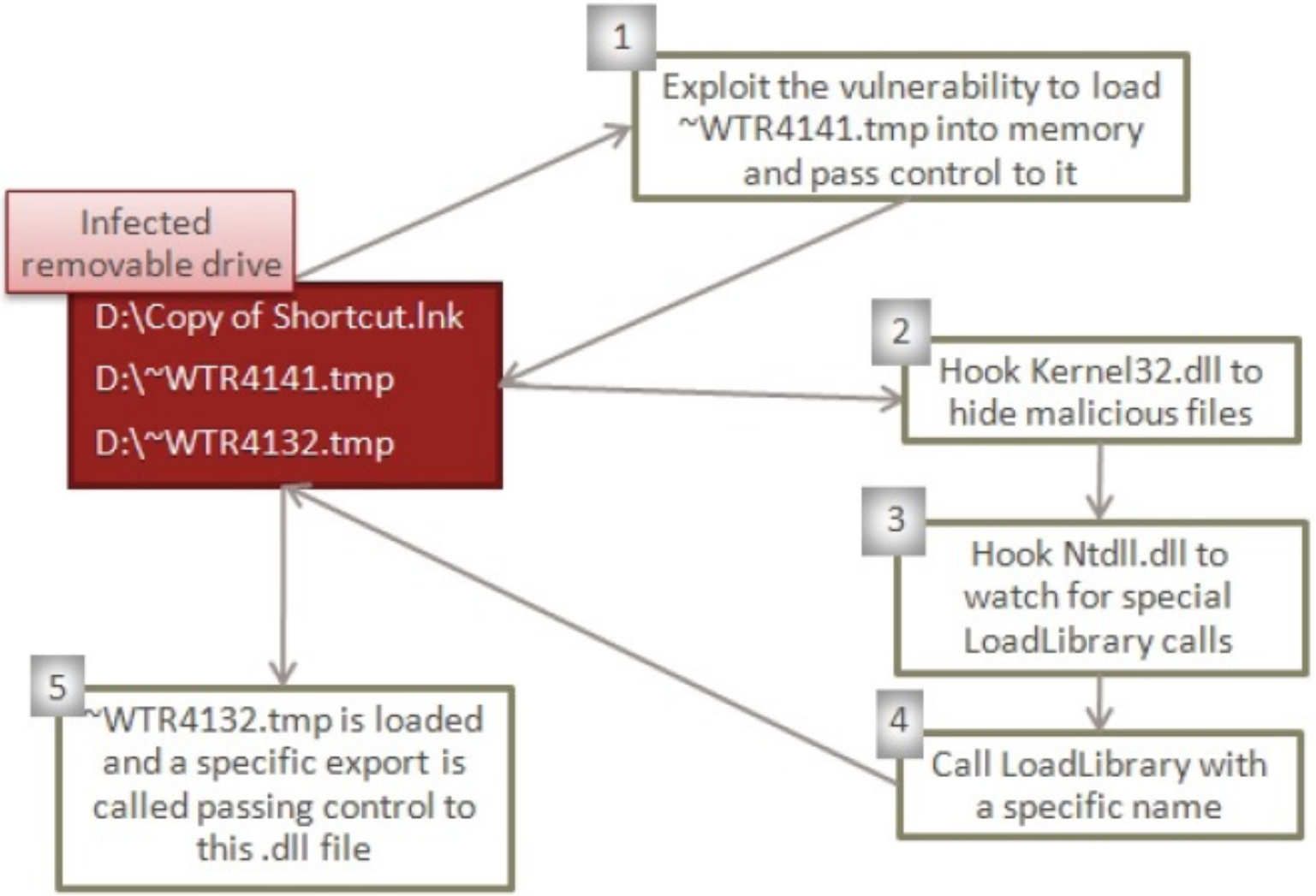
- Peer-to-peer communications and updates
- Infecting WinCC machines via a hardcoded database server password
- Propagating through network shares
- Propagating through the MS10-061 Print Spooler 0-day vulnerability
- Propagating through the MS08-067 Windows Server Service vulnerability

P2P



Symantec: W.32 Stuxnet Dossier

Removable Drive Propagation



Symantec: W.32 Stuxnet Dossier

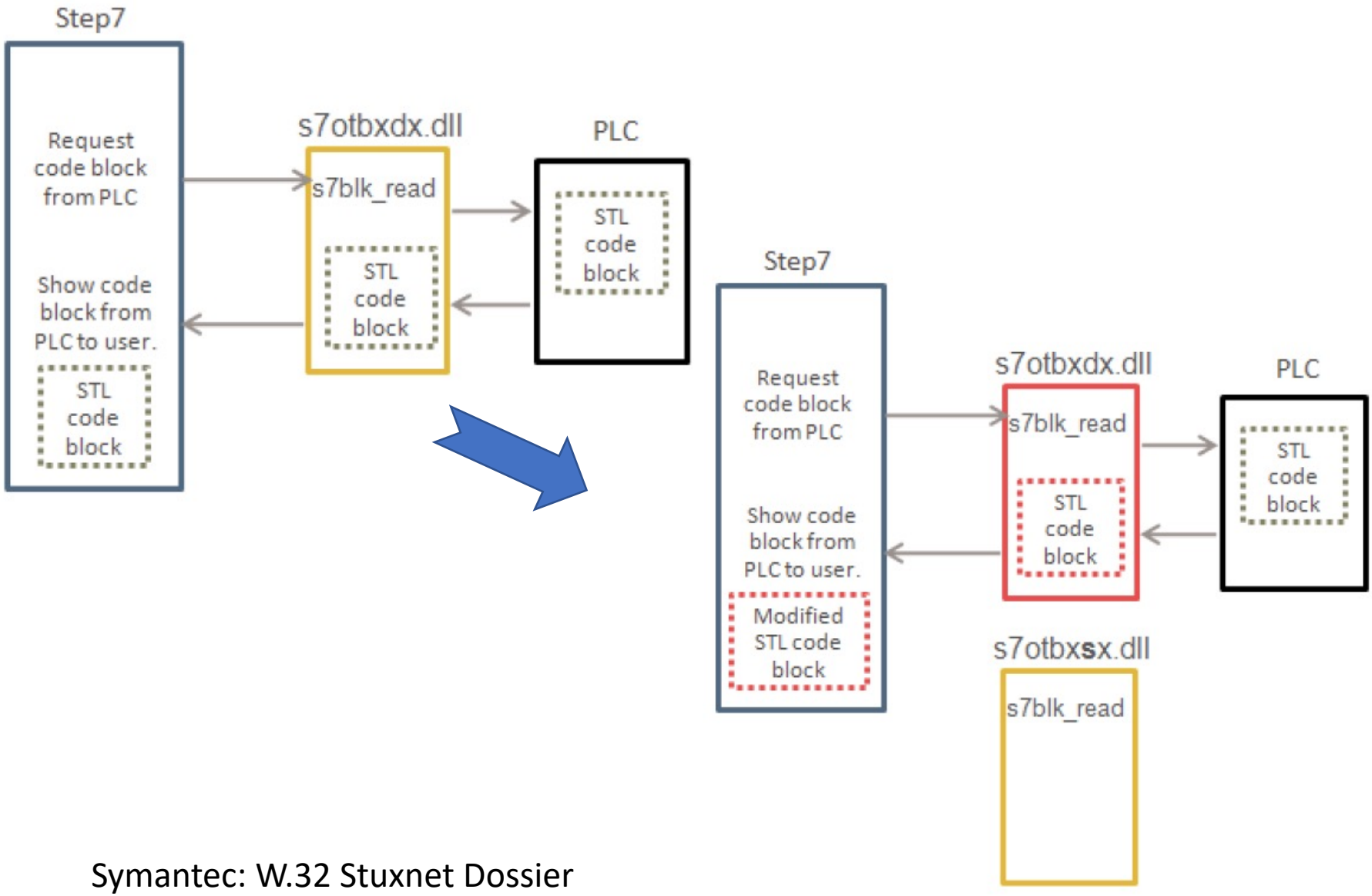
Step 7 Project File Infections

- S7P files – when an infected project is opened by the Simatic manager it performs some checks and then loads the malicious code
- MCP files – may be in a Step7 folder but usually created by WinCC; opening such a file may infect the WinCC database as well
- TMP files – are used by Stuxnet to copy infected files

Modifying PLCs

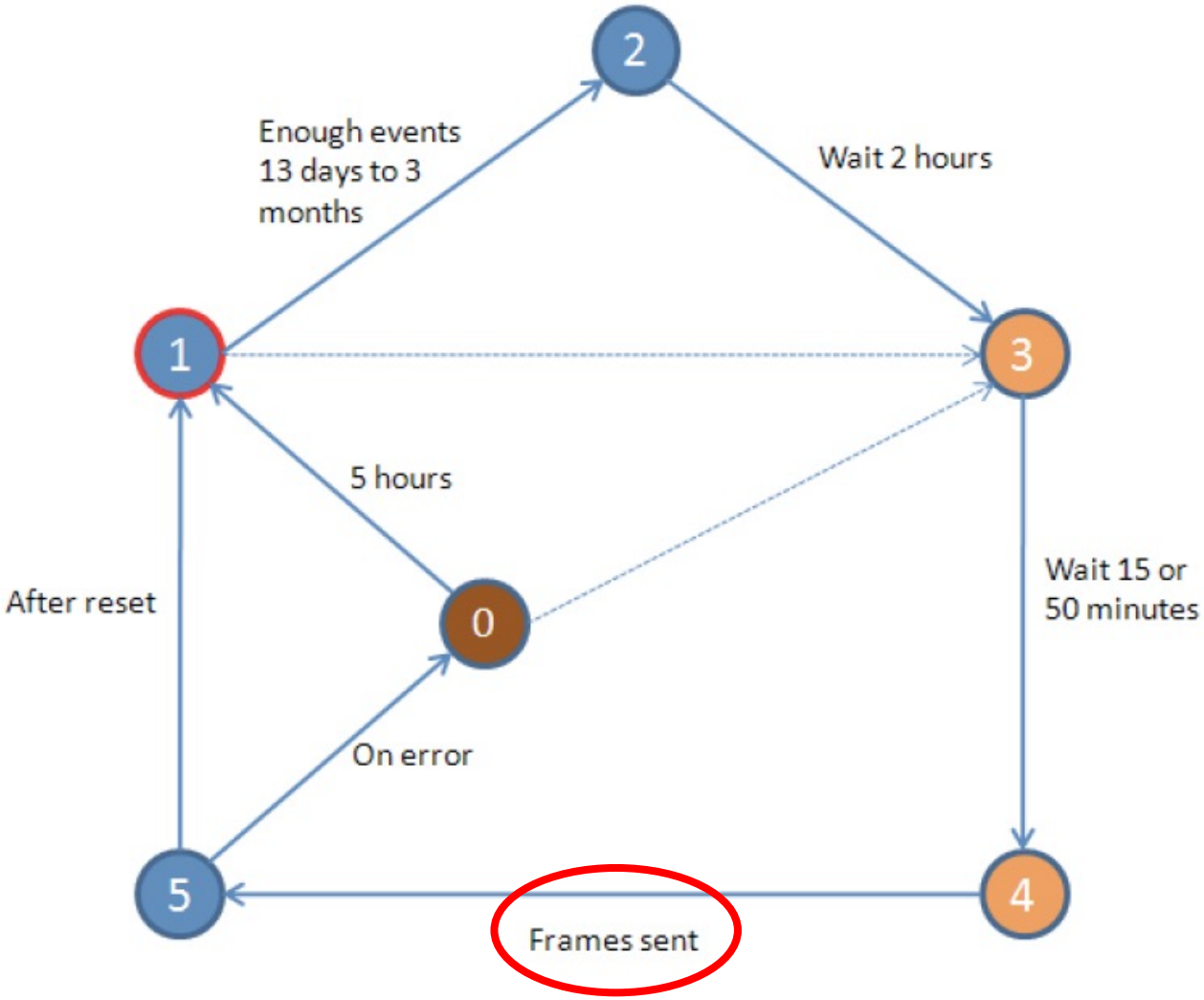
Symantec: W.32 Stuxnet Dossier

Man-in-the-middle



Symantec: W.32 Stuxnet Dossier

Infected PLC (S7-315)



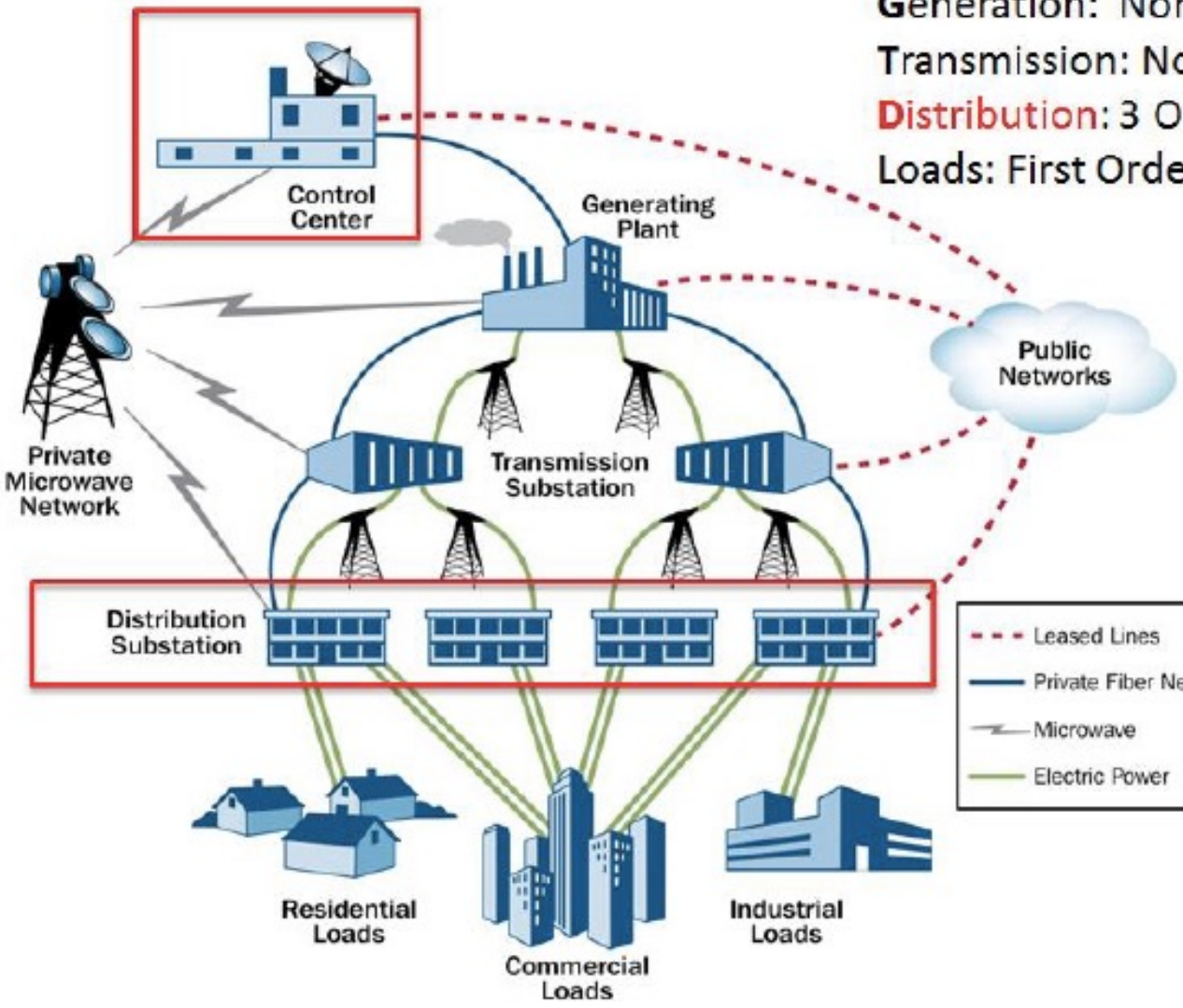
Symantec: W.32 Stuxnet Dossier

UKRAINE 2015

Timeline

- 23 December 2015, Ukrainian Kyivoblenergo reported outages to customers
- Starting at around 3.35pm, 7 110kV and 23 35kV substations were disconnected for 3 hours
- 80,000 customers affected
- It later emerged that 3 different oblenergos were attacked
- In total 225,000 customers were affected
- The cyber attacks were launched within 30 minutes of each other

Generation: None
Transmission: None
Distribution: 3 Oblenergos
Loads: First Order Impacts



110 kV & below

Attacker capability

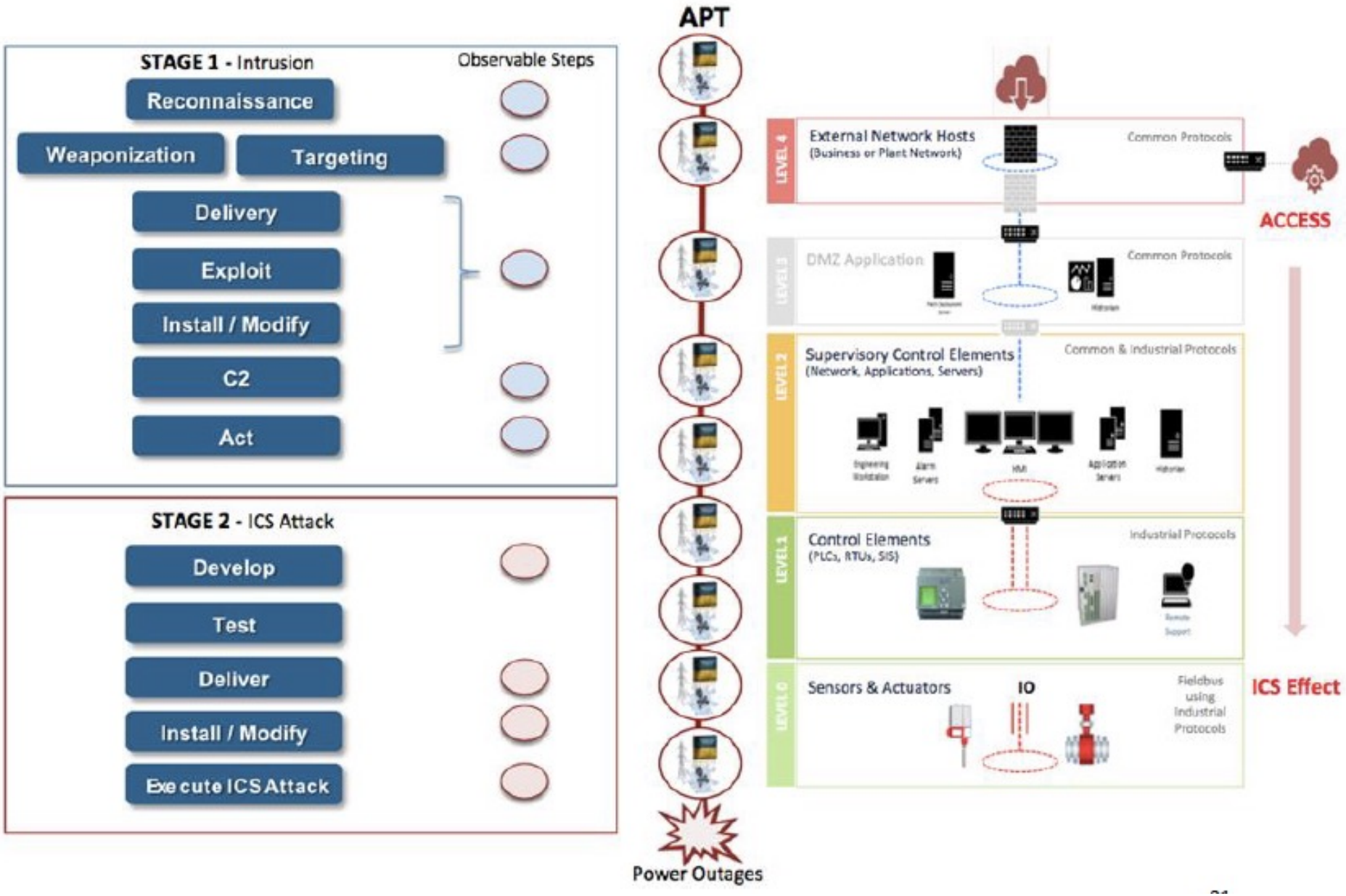
- Spear phishing emails
- BlackEnergy 3 malware
- Manipulation of Microsoft Office documents to deliver malware
- Ability to harvest information and credentials to gain access to ICS system
- Expertise in Uninterruptable Power Supplies (UPS), SCADA and HMI
- Ability to target field devices at substations
- Denial of service on telephone system

Consolidated Technical Components

Opportunities

- Detailed list of infrastructure (such as RTU vendors and versions) posted online by vendors
- VPNs into business and ICS networks lack 2-factor authentication
- Firewall allowed remote access facility
- No continuous monitoring of ICS network

- Result: adversary could have been resident in system for 6 months or more to conduct reconnaissance

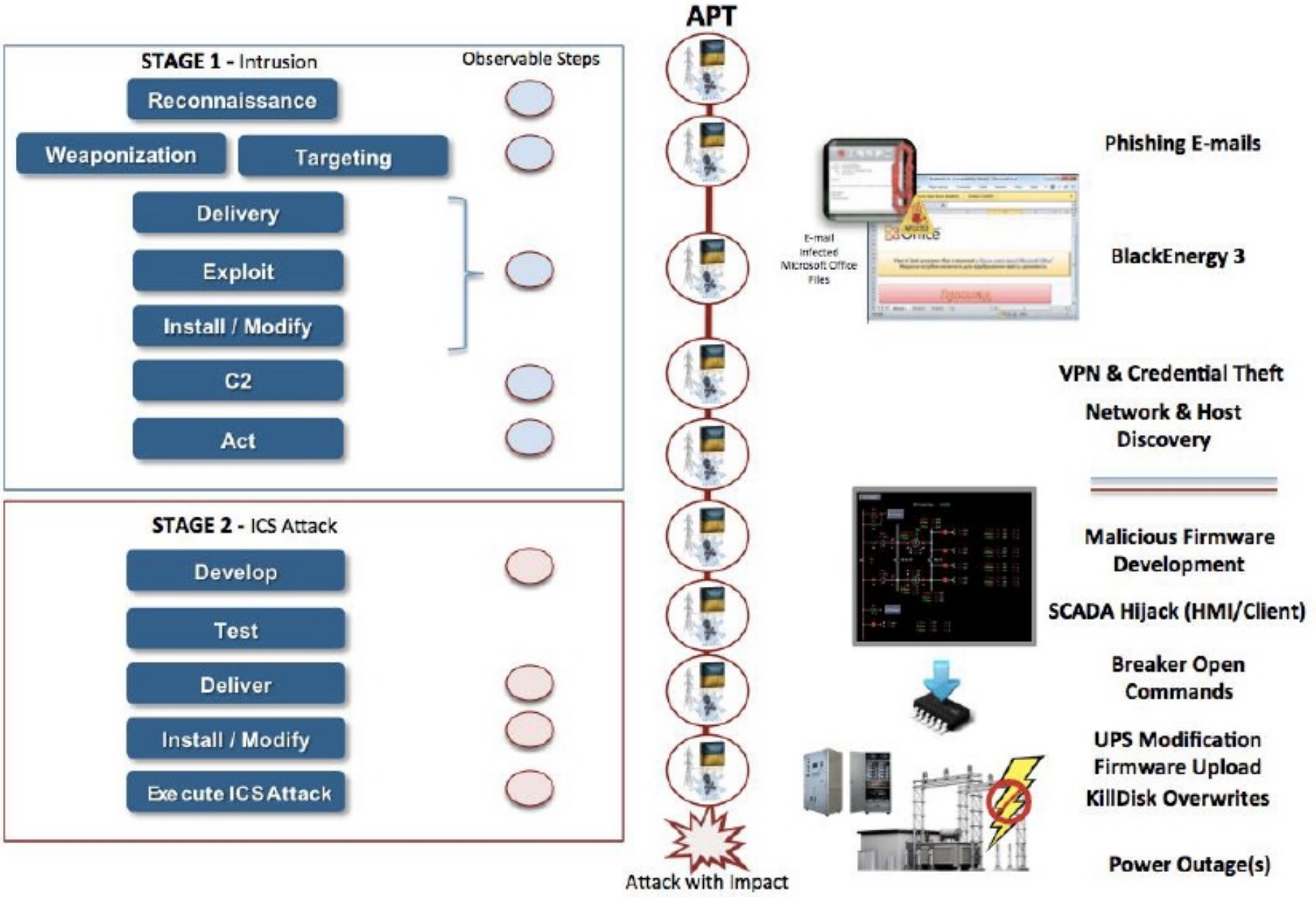

STAGE 1 - Intrusion
Observable Steps
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
STAGE 2 - ICS Attack
Develop
Test
Deliver
Install / Modify
Execute ICS Attack
APT
Power Outages
LEVEL 4
External Network Hosts
(Business or Plant Network)
Common Protocols
ACCESS
LEVEL 3
DMZ Application
Common Protocols
LEVEL 2
Supervisory Control Elements
(Network, Applications, Servers)
Common & Industrial Protocols
LEVEL 1
Control Elements
(PLCs, RTUs, SIS)
Industrial Protocols
LEVEL 0
Sensors & Actuators
IO
Fieldbus using Industrial Protocols
ICS Effect

Some details

- BlackEnergy 3 embedded in Microsoft Windows files – Word and Excel
- Enabling macros allowed the installation of the malware
- BlackEnergy3 connects to a C2 server – this appears to have happened 6 months before the outages
- Attackers gathered intelligence about the Distribution Management Systems (DMSs) used by the companies

Stage 2 Details

- Attackers learnt how to interact with the 3 different DMSs
- Developed malicious firmware for the serial-to-ethernet devices (“blowing the bridges”)
- There is evidence that the attacker capabilities were tested
- Use of remote admin tools on operator workstations
- Installed modified KillDisk across the environment
- Use HMIs to open breakers


APT
STAGE 1 - Intrusion
Observable Steps
Reconnaissance
Weaponization
Targeting
Delivery
Exploit
Install / Modify
C2
Act
STAGE 2 - ICS Attack
Develop
Test
Deliver
Install / Modify
Execute ICS Attack
Attack with Impact
E-mail Infected Microsoft Office Files
Phishing E-mails
BlackEnergy 3
VPN & Credential Theft
Network & Host Discovery
Malicious Firmware Development
SCADA Hijack (HMI/Client)
Breaker Open Commands
UPS Modification
Firmware Upload
KillDisk Overwrites
Power Outage(s)

Stage 2 Attack elements

- Supporting elements
  - Schedule disconnects for UPS systems
  - Telephone system attack for at least one oblenergo
- Primary attack: SCADA hijack with malicious operation to open breakers
- Amplifying attacks
  - KillDisk wiping of workstations, servers and an HMI
  - Firmware attacks against serial-to-ethernet devices at substations

Disrupting Spear Phishing

- Communication with untrusted areas should be segmented, monitored and controlled
- Consider using sandboxing to evaluate emails and documents coming into the system
- Use proxy systems to control outbound and inbound communication paths
- Limit workstations to communicate only through the proxy devices by implementing perimeter egress access control

Credential Theft

- Performed by keystroke loggers – could be detected by forensic tools
- Change user and shared passwords – if permitted by vendor
- Monitor account behavior
- Implement a multi-level alarm capability

Data exfiltration

- Understand where relevant data exists in the system
- Maintain a vaulted copy of known good project files, control and safety logic and firmware
- Use file integrity checkers
- Network Security Monitoring is an active cyber defense method that detects data exfiltration

VPN Access

- Recommend use of 2-factor authentication
- Know which trusted communication paths exist
- Consider implementing time of use access
- Time-outs and manual disconnection
- Force choke points – such as all access through a DMZ. This allows monitoring by active defenders

Workstation Remote Access

- Disable remote access at host and at perimeter firewall
- Host-based application aware firewalls, application whitelisting and configuration management
- Good architecture to segment or disable remote connections
- Incident response capability

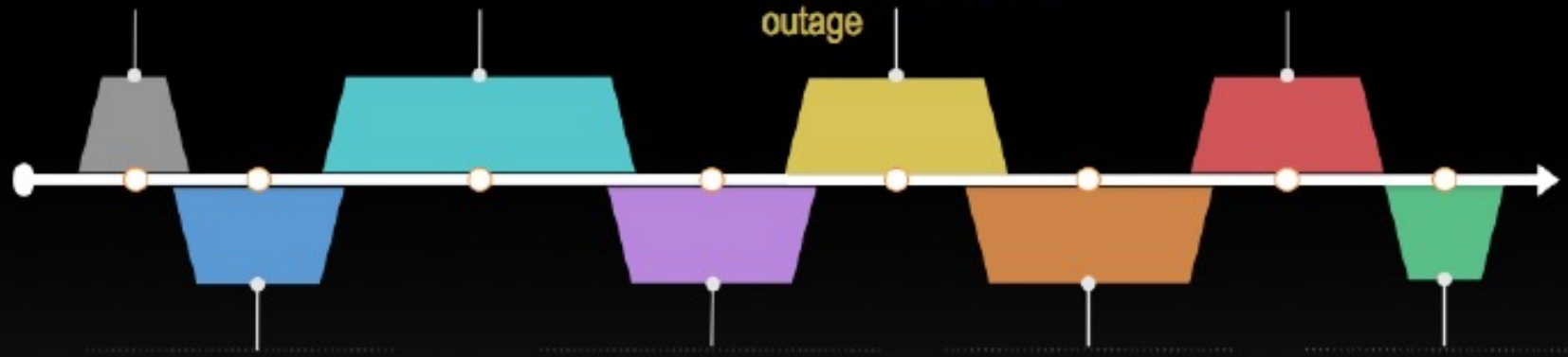
Control and Operate

- Areas of responsibility (AoRs) to restrict capabilities of operators – determined by username, workstation or hybrid
- Communication path or protocol authentication to require commands issued from an authorized asset
- Collect logs not only from hosts but from SCADA applications to – use active defenders to analyse logs

Respond and Restore

- Contingency analysis
- Failure planning
- Conservative operations
- Cyber load shed
- Root Cause Analysis
- Blackstart
- Information Sharing

Opportunities to Disrupt



IT Preparation
- Target selection
- Unobservable target mapping
- Malware development and testing

Hunting and Gathering
- Lateral Movement and Discovery
- Credential Theft and VPN access
- Control system network and host mapping

Sequence Pre Work
- Upload additional attack modules - KillDisk
- Schedule KillDisk wipe
- Schedule UPS load outage

Attack Launch
- Issue breaker open commands
- Modify field device firmware
- Perform TDoS
- Scheduled UPS and KillDisk

Spear phishing
- Delivery of phishing email
- Malware launch from infected office documents
- Establish foothold

ICS Preparation
- Unobservable malicious firmware development
- Unobservable DMS environment research and familiarization
- Unobservable attack testing and tuning

Attack Position
- Establish Remote connections to operator HMI's at target locations
- Prepare TDoS dialers

Target Response
- Connection sever
- Manual mode / control inhibit
- Cyber asset restoration
- Electric system restoration
- Constrained operations
- Forensics
- Information sharing
- System hardening and prep

BlackEnergy 3

- F-Secure White Paper
- BlackEnergy originally a toolkit for DDoS attacks
- Quedagh variant of BlackEnergy
- Customisations include support for proxy servers, bypass of User Access Control and driver signing in 64-bit Windows systems
- Used by multiple groups – plausible deniability

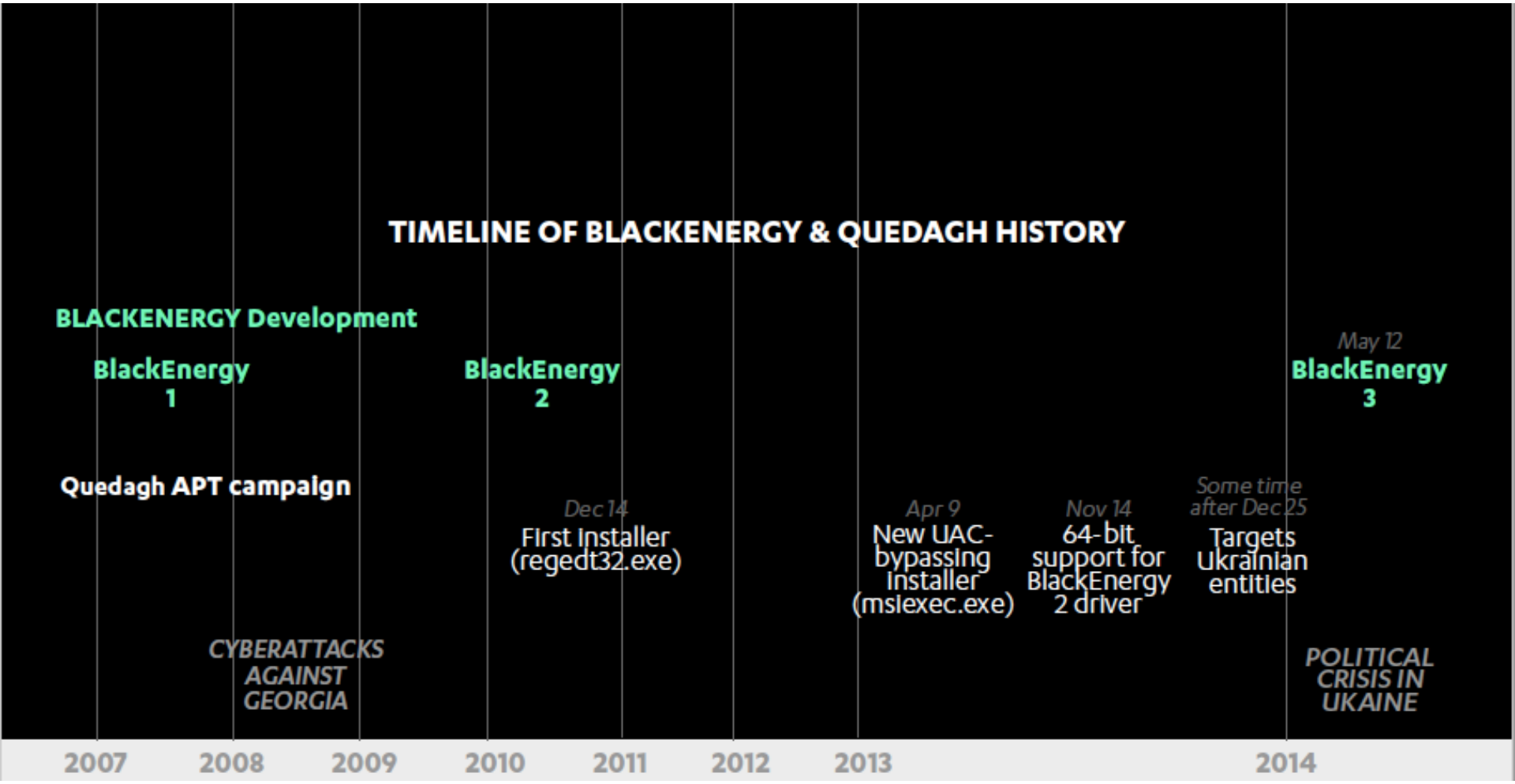
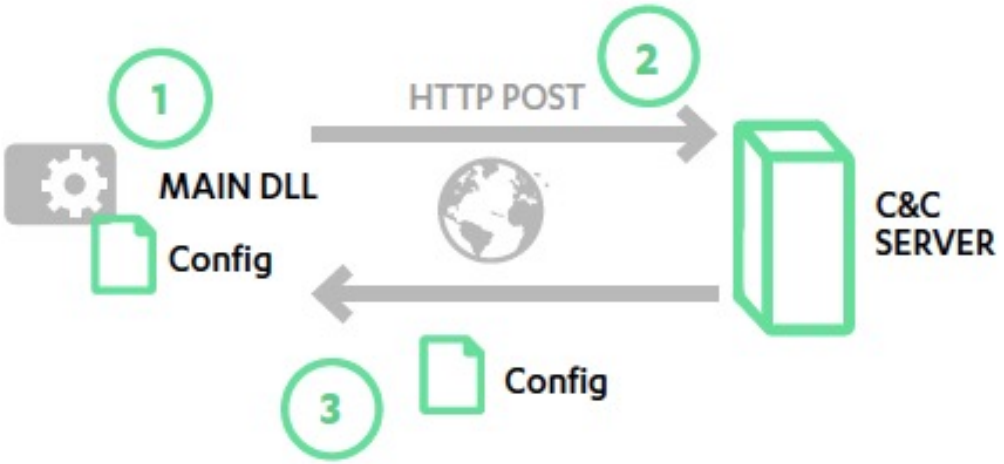

TIMELINE OF BLACKENERGY & QUEDAGH HISTORY
BLACKENERGY Development
BlackEnergy 1
BlackEnergy 2
May 12
BlackEnergy 3
Quedagh APT campaign
Dec 14
First Installer (regedt32.exe)
Apr 9
New UAC-bypassing installer (msiexec.exe)
Nov 14
64-bit support for BlackEnergy 2 driver
Some time after Dec 25
Targets Ukrainian entities
CYBERATTACKS AGAINST GEORGIA
POLITICAL CRISIS IN UKAINE
2007
2008
2009
2010
2011
2012
2013
2014

DIAGRAM 3: CONFIGURATION DATA HANDLING



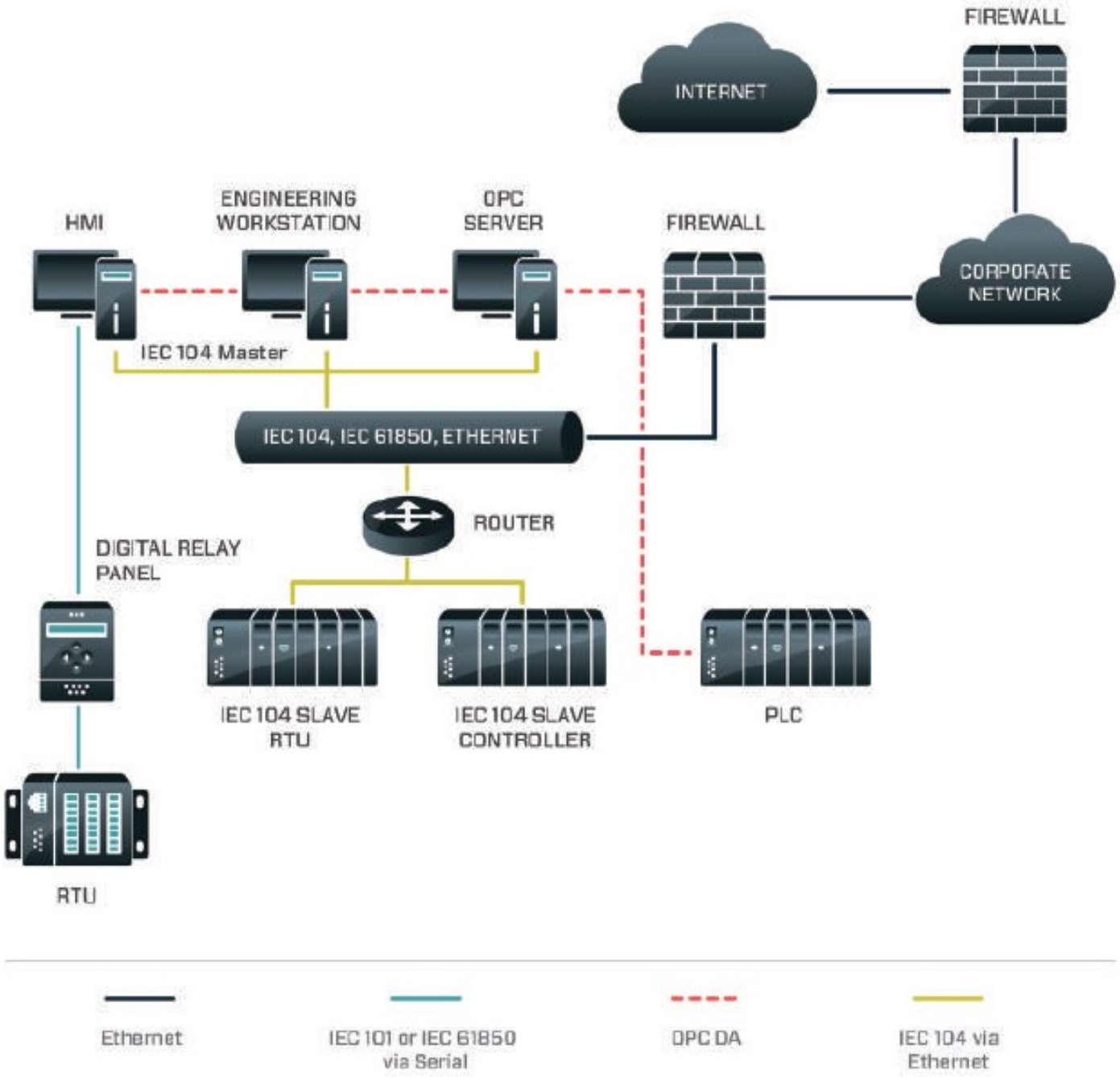
1. Main DLL process configuration data embedded in its body; will only process fields related to C&C communication. BlackEnergy 2 configuration may also contain initial commands to execute.
2. Main DLL reports to C&C.
3. Main DLL processes the configuration data returned by the C&C. This time, it processes fields related to plugins and commands.

TABLE 6: MAIN DLL'S ADDITIONAL COMMANDS DURING DOWNLOAD OF ADDITIONAL FILES

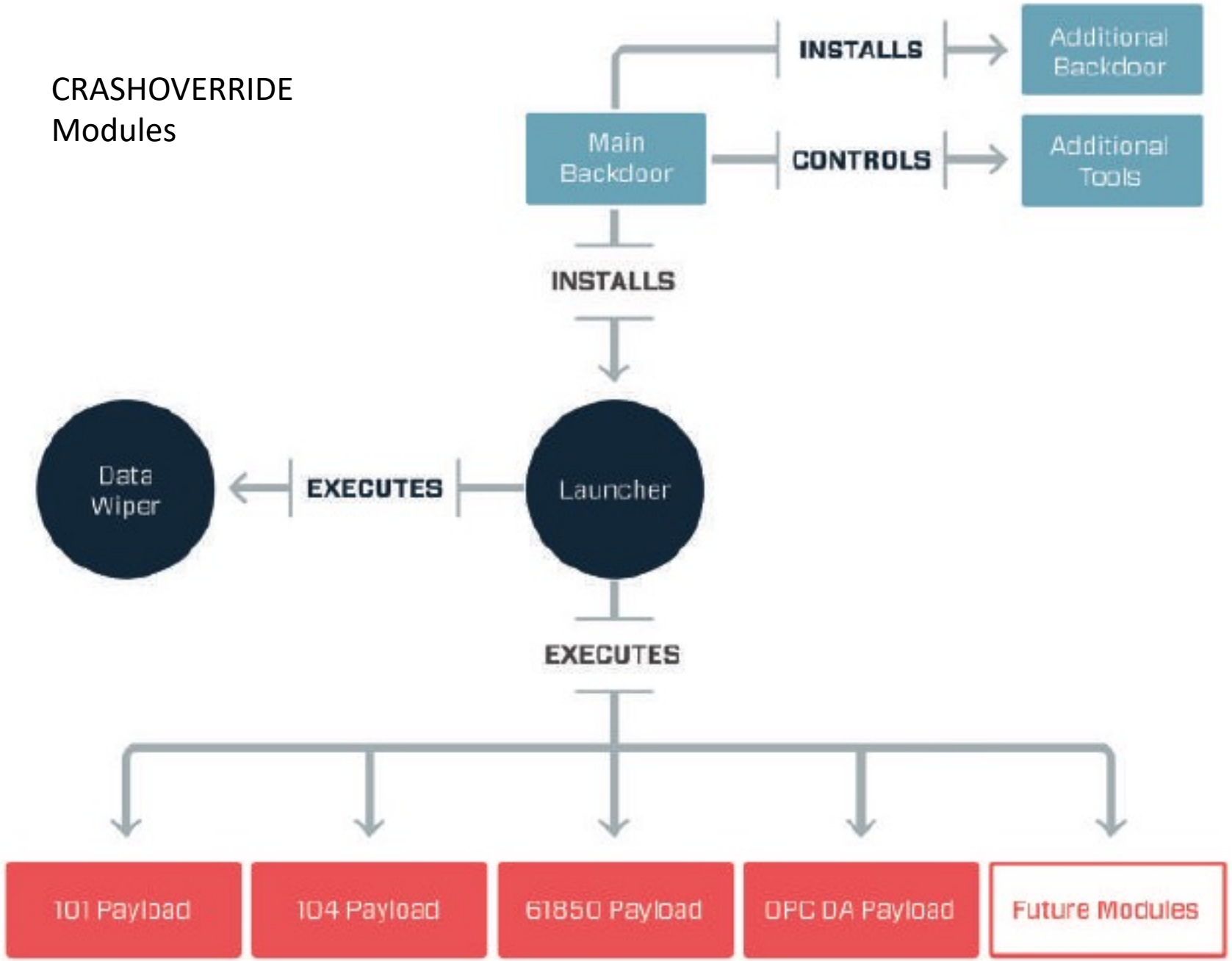
HTTP POST Field	Description of Values
getp	The plugin name to be downloaded
plv	Some variants specify the version of the plugin to be downloaded
getpd	The binary name to be downloaded

UKRAINE 2016

www.dragos.com


FIREWALL
INTERNET
HMI
ENGINEERING WORKSTATION
OPC SERVER
FIREWALL
CORPORATE NETWORK
IEC 104 Master
IEC 104, IEC 61850, ETHERNET
ROUTER
DIGITAL RELAY PANEL
IEC 104 SLAVE RTU
IEC 104 SLAVE CONTROLLER
PLC
RTU
Ethernet
IEC 101 or IEC 61850 via Serial
OPC DA
IEC 104 via Ethernet

CRASHOVERRIDE
Modules



Backdoor/RAT Module

- Authenticates with a local proxy via the internal network established before the backdoor installation
- Opens HTTP channel to external C2 server through internal proxy
- Receives commands from external C2 server
- Creates a file on the local system
- Overwrites an existing service to point to the backdoor so the malware persists between reboots

Launcher module

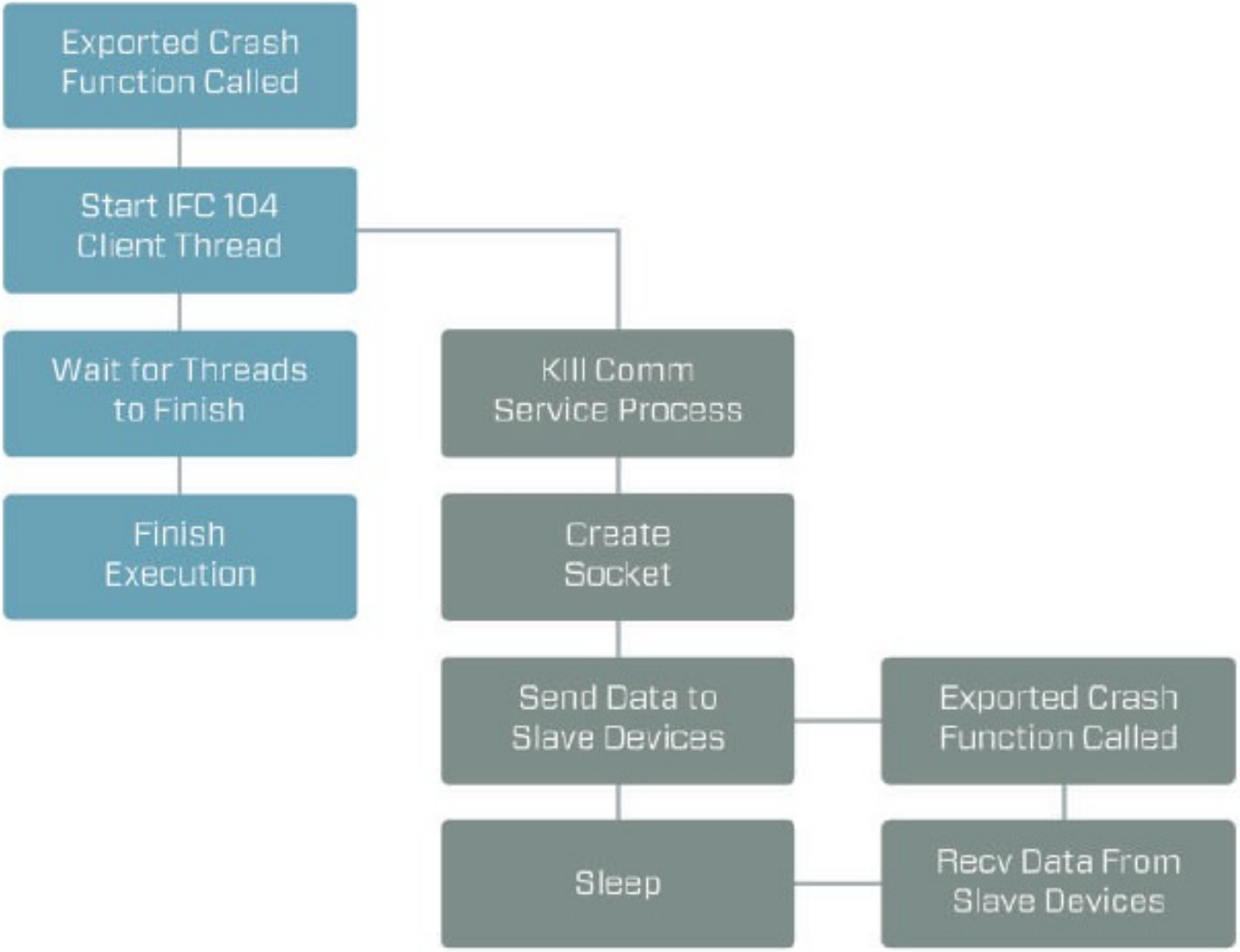
- Loads payload modules and causes destruction via the wiper
- Starts itself as a service likely to hide better
- Loads the payload modules defined on the command line during execution
- Launches the payload and waits 1 or 2 hours before launching the data wiper

Data wiper

- Clears all the registry keys associated with system services
- Overwrites all ICS configuration files across the hard drives and mapped network drives
- Overwrites generic Windows files
- Renders the system unusable

IEC 104 module

- Reads a configuration file defining the target (likely an RTU) and the action to take
- Kills the legitimate master process on the victim host
- Masquerades as the new master
- Manipulates the RTU in one of four modes (not all analysed)


Exported Crash Function Called
Start IFC 104 Client Thread
Wait for Threads to Finish
Finish Execution
KIll Comm Service Process
Create Socket
Send Data to Slave Devices
Sleep
Exported Crash Function Called
Recv Data From Slave Devices

Attack options

- De-energize substation by an infinite loop opening closed breakers – a few hours of outages
- Force an islanding event by toggling breakers between open and closed – a few days of outages
- Amplification attacks
  - Denial of visibility
  - Denial of service against protective relays

Defense

- Develop clear understanding of where vulnerable protocols are used
- Understand OPC implementations and how the protocol is being used
- Robust backups of engineering files such as project logic, IED config files and ICS application installers
- Incident response plans
- Use forensic tools (YARA) to search for infections
- Air-gapped networks, uni-directional firewalls, antivirus etc are not appropriate. Human defenders are needed against a determined human adversary

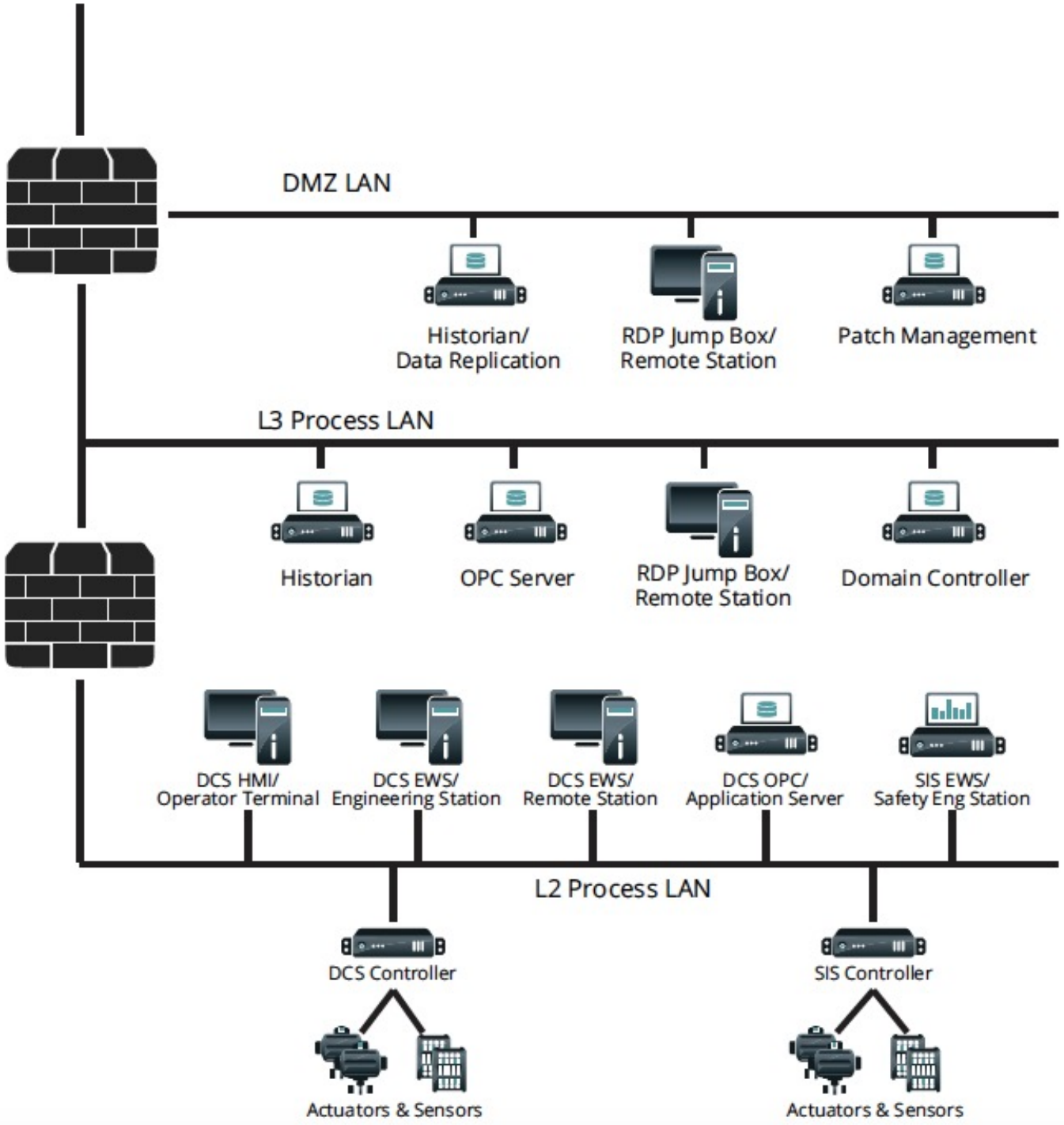
TRITON

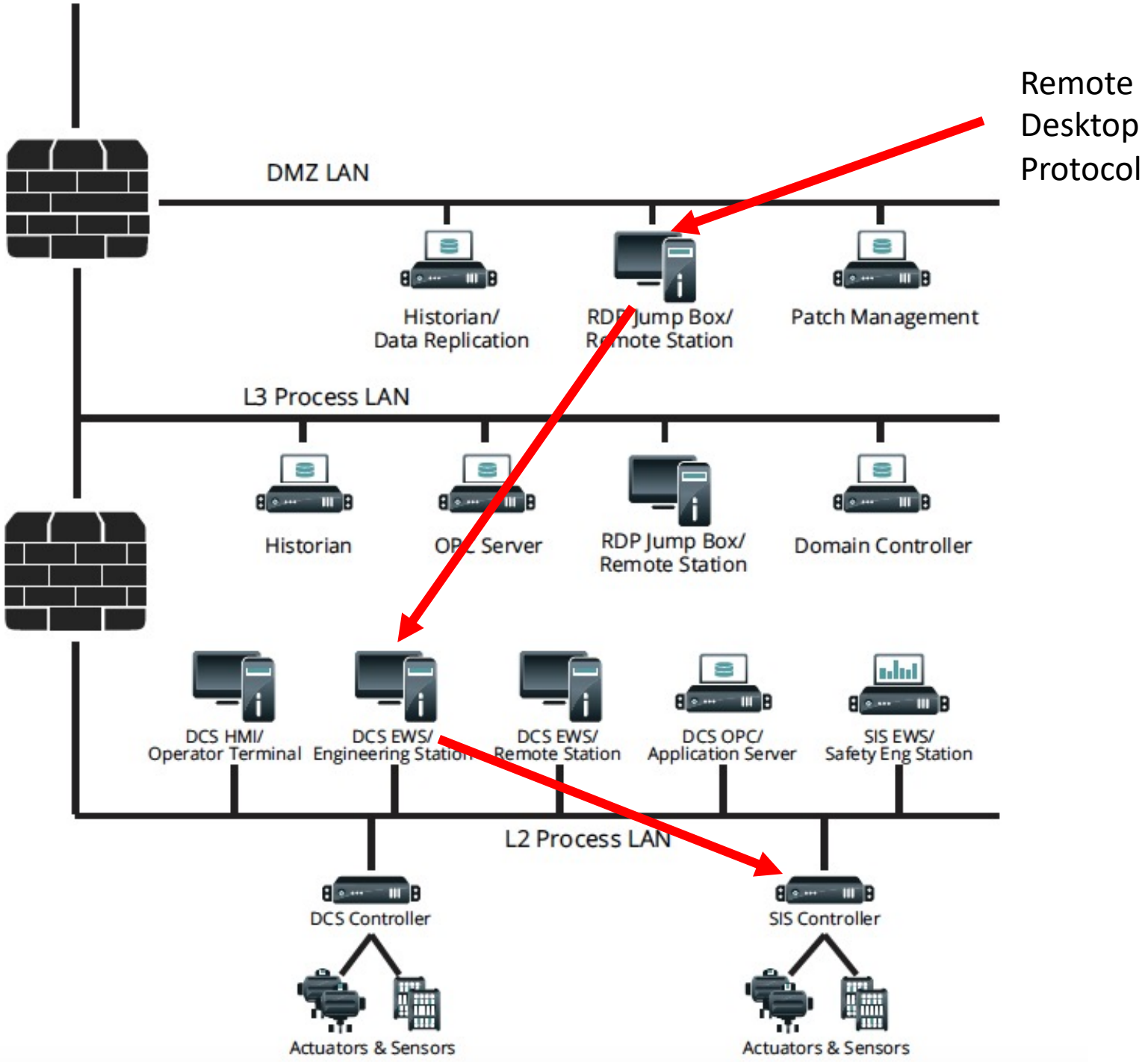
Summary

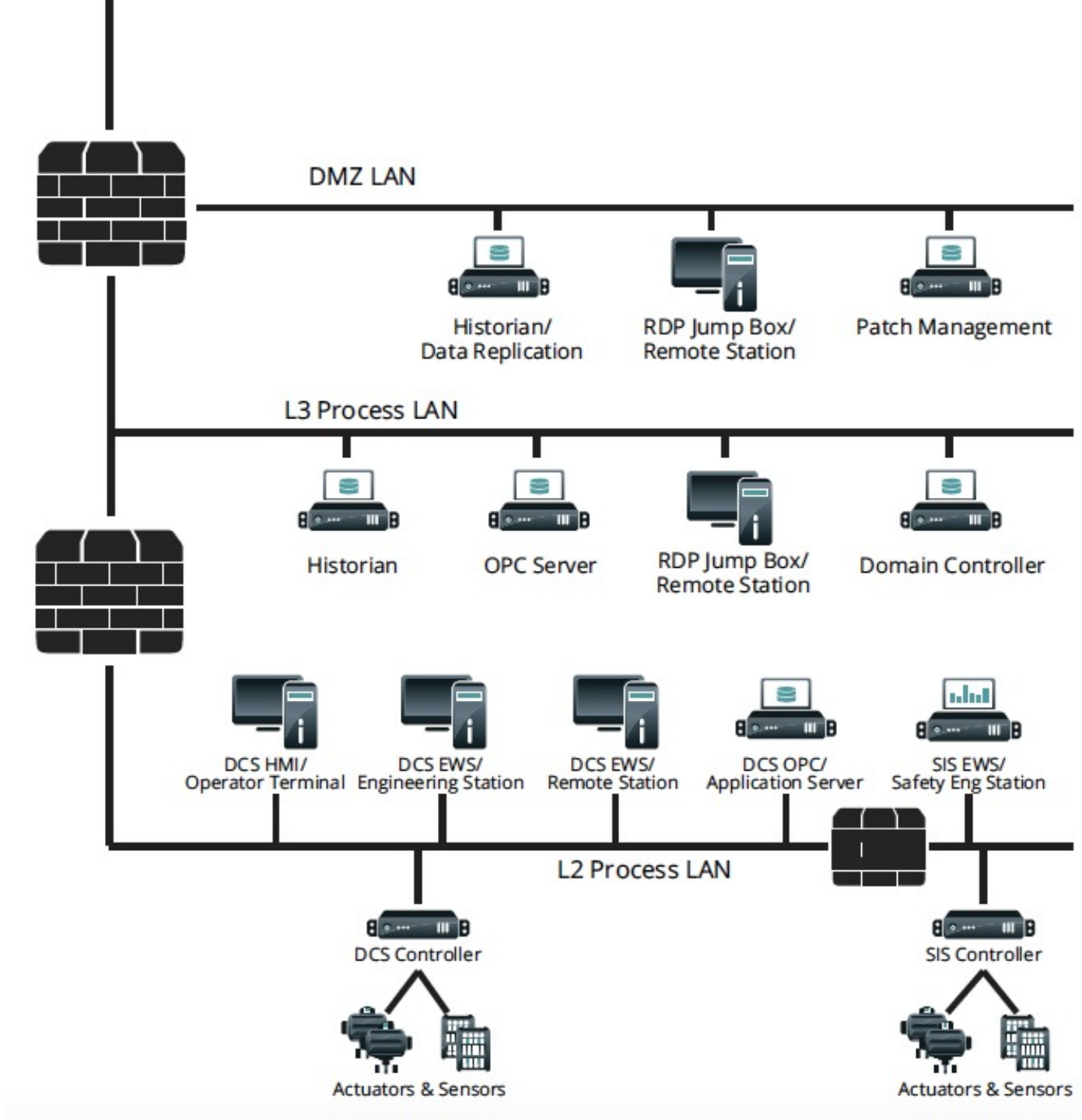
- Malware targeting Schneider Triconex safety controllers
- Single user of Tricon safety shutdown system
- Campaign of intelligence gathering likely to have lasted for weeks/months
- Triton malware has the ability to reprogram Triconex controllers
- Malware deployed via compromised Safety Instrumented System (SIS) engineering workstation
- System entered failed safe state and shutdown

TRISIS/Triton (www.dragos.com)

- Each SIS is unique – attackers need specific knowledge about the target system
- Therefore the attack is not highly scalable
- Compromise of the SIS does not necessarily impact on the safety of the system because the SIS should fail safe
- However changes to the control elements could change the points at which the safety system would take control of the process in an unsafe condition


DMZ LAN
Historian/
Data Replication
RDP Jump Box/
Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/
Remote Station
Domain Controller
DCS HMI/
Operator Terminal
DCS EWS/
Engineering Station
DCS EWS/
Remote Station
DCS OPC/
Application Server
SIS EWS/
Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensors


Remote
Desktop
Protocol
DMZ LAN
Historian/
Data Replication
RDP Jump Box/
Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/
Remote Station
Domain Controller
DCS HMI/
Operator Terminal
DCS EWS/
Engineering Station
DCS EWS/
Remote Station
DCS OPC/
Application Server
SIS EWS/
Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensors


DMZ LAN
Historian/
Data Replication
RDP Jump Box/
Remote Station
Patch Management
L3 Process LAN
Historian
OPC Server
RDP Jump Box/
Remote Station
Domain Controller
DCS HMI/
Operator Terminal
DCS EWS/
Engineering Station
DCS EWS/
Remote Station
DCS OPC/
Application Server
SIS EWS/
Safety Eng Station
L2 Process LAN
DCS Controller
SIS Controller
Actuators & Sensors
Actuators & Sensors

Possible Attack Scenarios

- Plant shutdown
  - Create operational uncertainty
  - Trip safety fail-safes to halt operation
- Unsafe physical state
  - Typical operations safety layering should mitigate
- TRISIS is a Stage 2 attack – so an adversary must have already achieved success in Stage 1

Completion of Stage 1 of the ICS Cyber Kill Chain:

Identify and gain access to a system able to communicate with target SIS.

Stage 2 Develop:

Identify target SIS type and develop TRISIS with replacement logic and loader

Stage 2 Test:

Ensure TRISIS works as intended, likely off network in the adversary environment

Stage 2 Deliver:

Transfer TRISIS to the SIS which contains the 'loader' module for the new logic and support binaries that provide the new logic

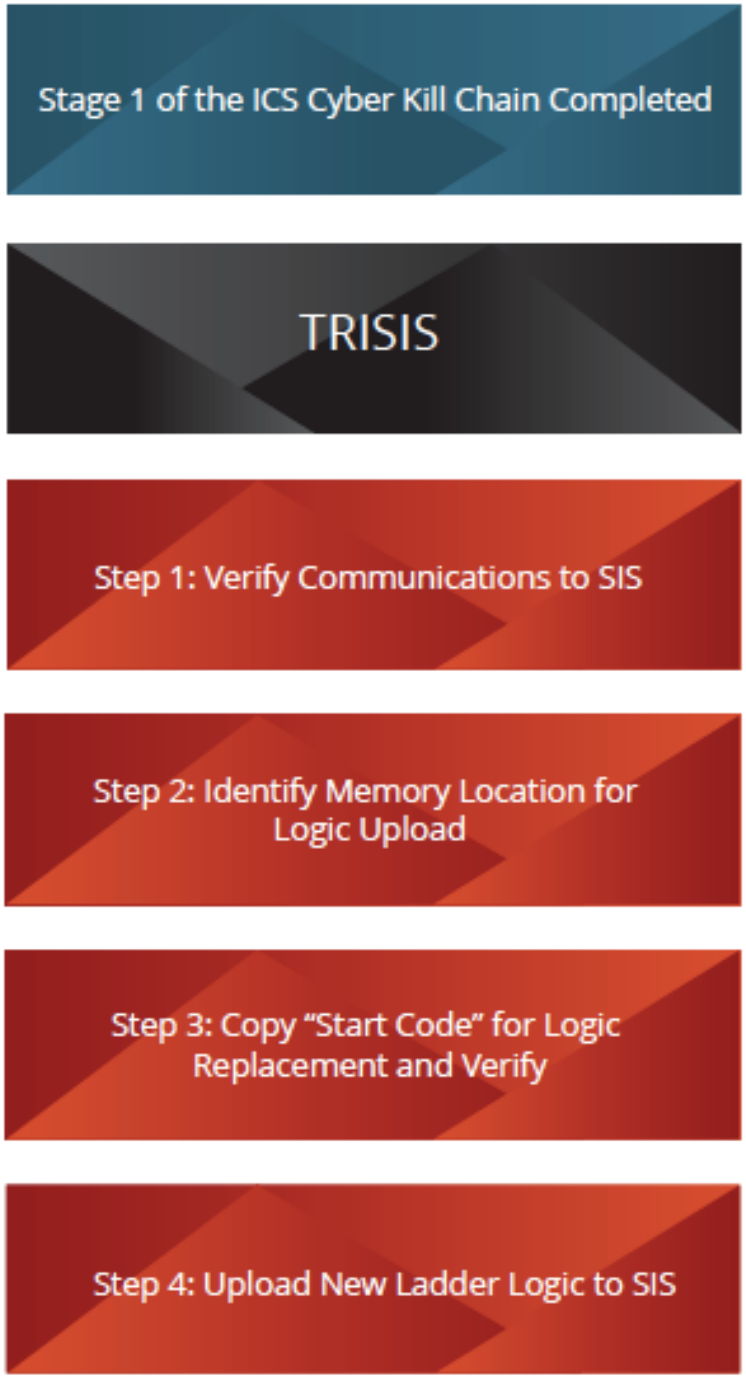
Stage 2 Install/Modify:

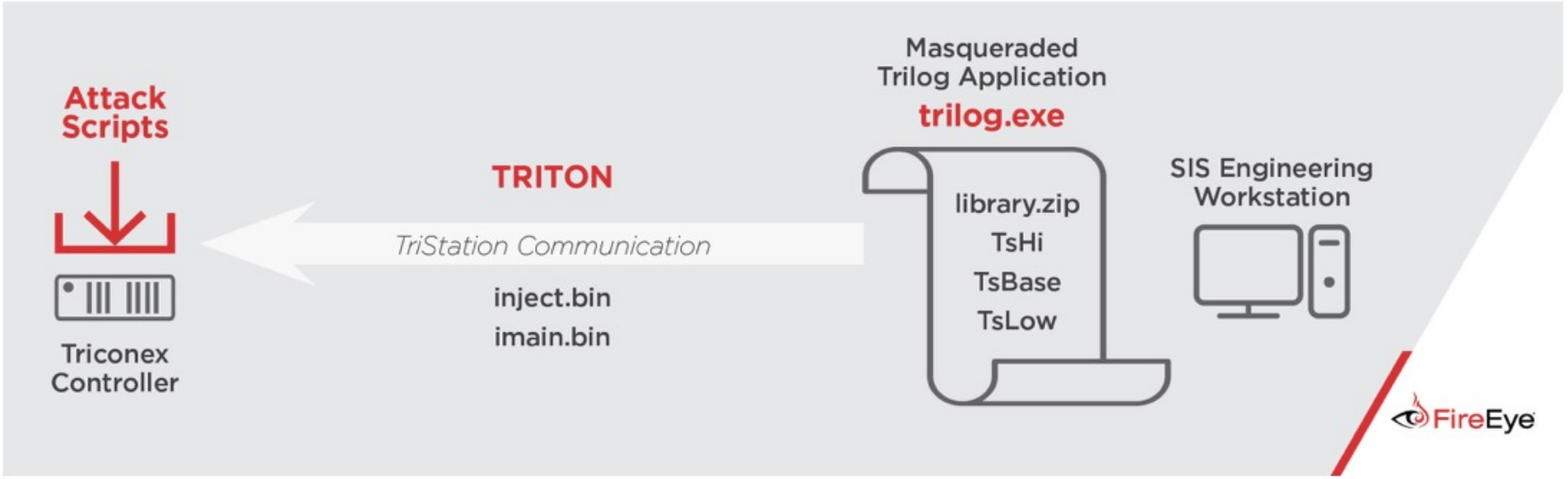
Upon running the TRISIS executable, disguised as Triconex software for analyzing SIS logs, the malicious software utilizes the embedded binary files to identify the appropriate location in memory on the controller for logic replacement and uploads the 'initializing code' (4-byte sequence)

Stage 2 Execute ICS Attack:

TRISIS verifies the success of the previous step and then uploads new ladder logic to SIS

Figure 4: TRISIS Attack Flow




Attack Scripts
Triconex Controller
TRITON
TriStation Communication
inject.bin
imain.bin
Masqueraded Trilog Application
trilog.exe
library.zip
TsHi
TsBase
TsLow
SIS Engineering Workstation
FireEye

Details

- Compiled Python Py2EXE script plus:
  - inject.bin – malicious function code
  - imain.bin – malicious control logic
- TsHI is the high level interface that allows adversary's operators to implement attack scripts
- TsBase translates the attacker's intended operation to the TriStation protocol function code
- TsLow implements the TriStation UDP wire protocol

Defending against Triton

- Safety systems on isolated networks
- Physical access control
- Controllers in locked cabinets
- TriStation terminals in locked cabinets and only ever connected to the safety system
- Mobile data devices scanned before connection
- Proper sanitation for laptops that are connected to the safety system
- Operator stations should be configured to display an alarm when the Tricon key switch is in Program mode


REMOTE
RUN
1
PROGRAM
STOP
TRICONEX
-LOCAL-
11290849