CIRED HRVATSKI OGRANAK

HRVATSKA KOMORA INŽENJERA ELEKTROTEHNIKE

Otpornost na kibernetičke prijetnje operativnoj tehnologiji u EES-u

dr.sc. Tamara Hadjina

14.03.2024.

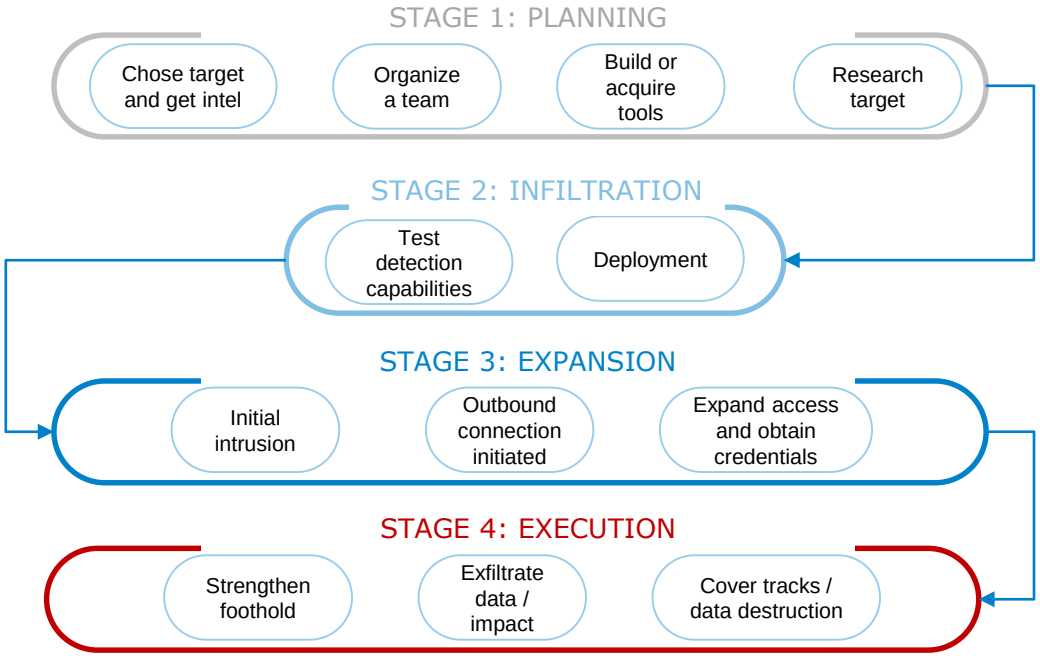
KONČAR Inspirirani izazovima

1. TKO I KAKO PRIJETI OPERATIVNOJ TEHNOLOGIJI?

2. KOJE SU POZNATE PRIJETNJE?

3. KAKO POSTATI OTPORAN?

APT napadi

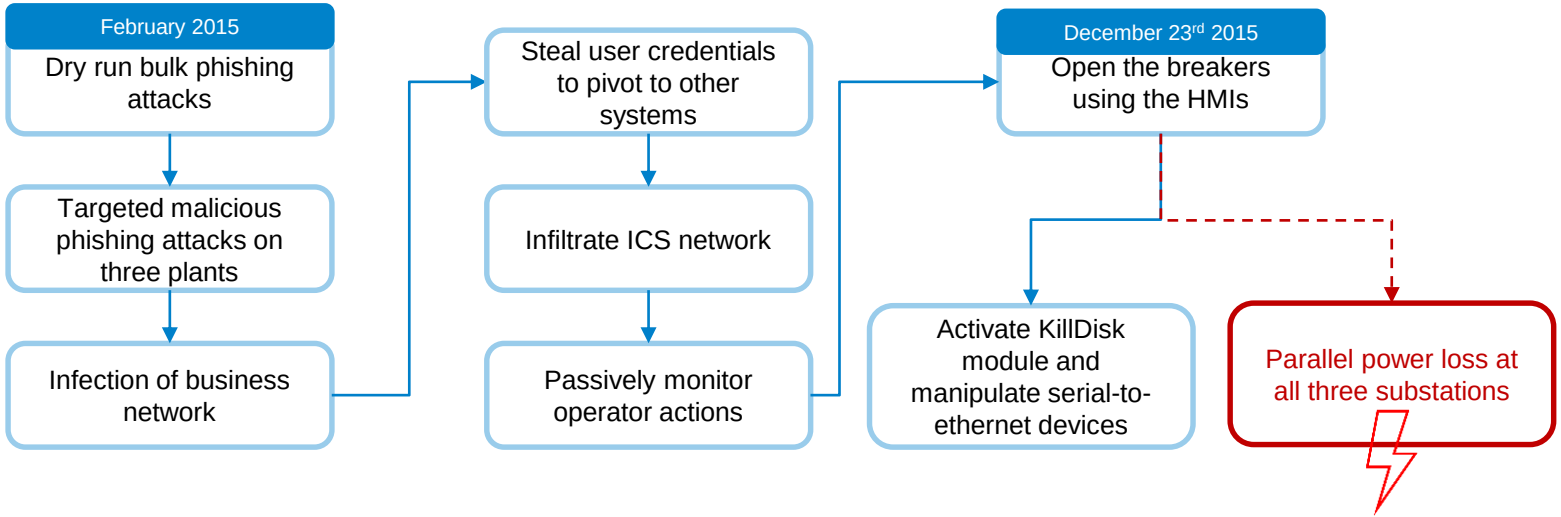

STAGE 1: PLANNING
Chose target and get intel
Organize a team
Build or acquire tools
Research target
STAGE 2: INFILTRATION
Test detection capabilities
Deployment
STAGE 3: EXPANSION
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
STAGE 4: EXECUTION
Strengthen foothold
Exfiltrate data / impact
Cover tracks / data destruction

Napadi na operativnu tehnologiju u EES-u

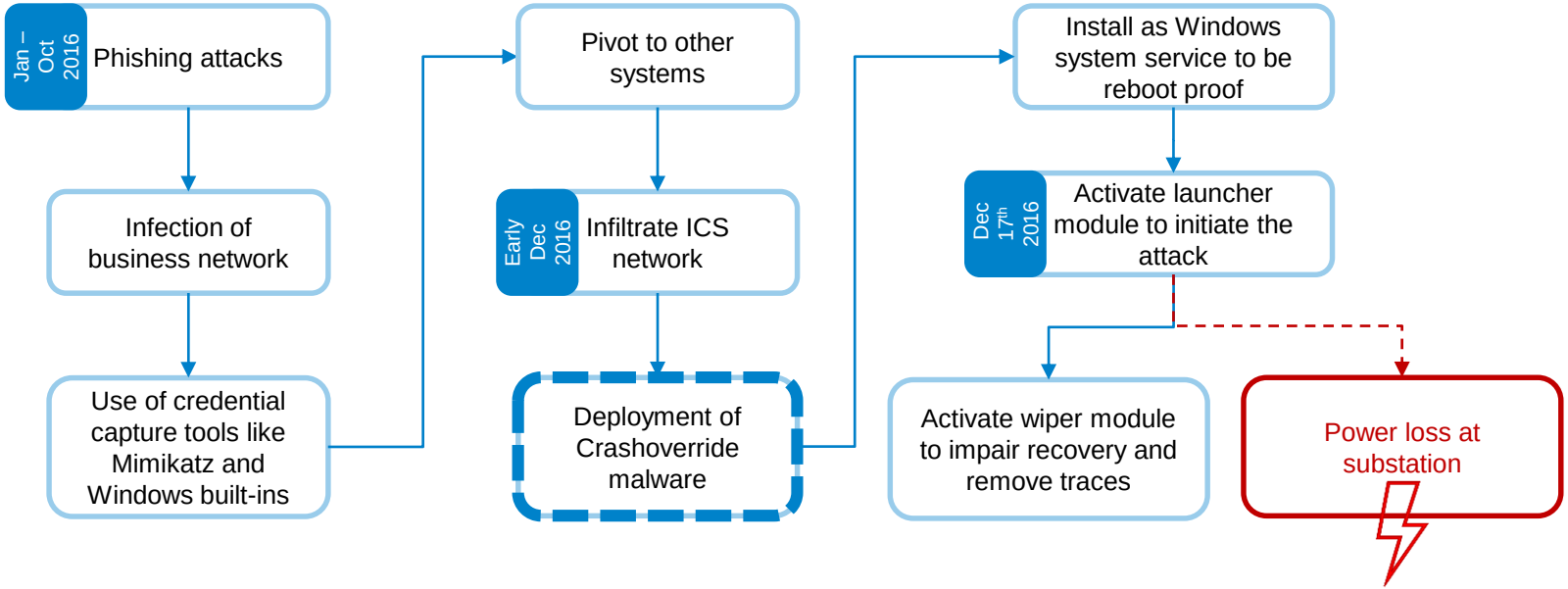
Blackenergy
• Blackenergy1 iz 2007. • Blackenergy3 iz 2015. • Simultani napad na 3 distribucijske stanice • 200 000 ljudi bez električne energije nekoliko sati

Crashoverride / Industroyer
• 2016. godina • 1 distribucijska stanica • dio Kijeva bez energije 1 sat • Industroyer2 neuspješan pokušaj u 2022.

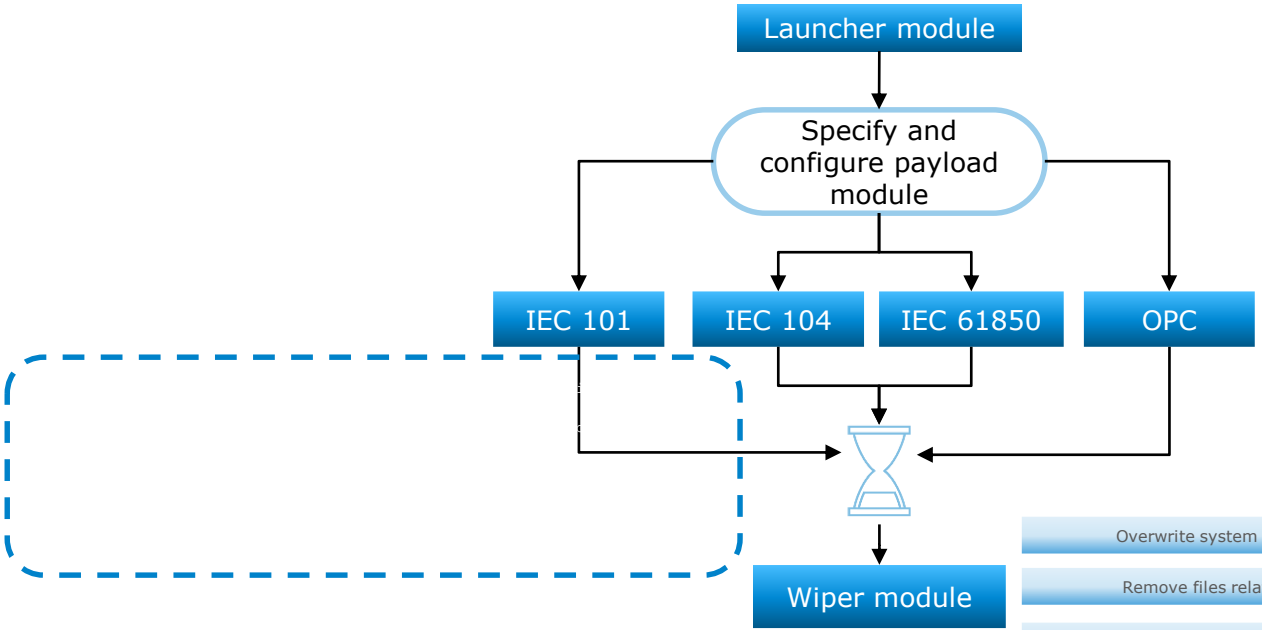
Blackenergy 3



Crashoverride
(Industroyer)



Crashoverride malware



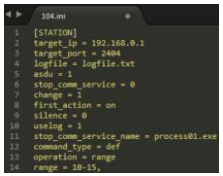
Overwrite system service registry entries to null values to render system unbootable.

Remove files relating to ICS operations to impede recovery and system restoration.

Terminate system processes to cause a crash and system shutdown.

104.dll

Configurable nature – customized by the attackers for different infrastructures



Stop the process responsible for IEC 104 communication with the target device

Connect module to the specified IP address

Sends packets with ASDU addresses from the configuration

Tko prijeti?

houseatreides94

arrakis02

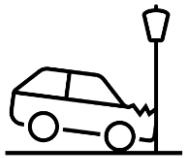
BasharoftheSardaukars

SalusaSecundus2

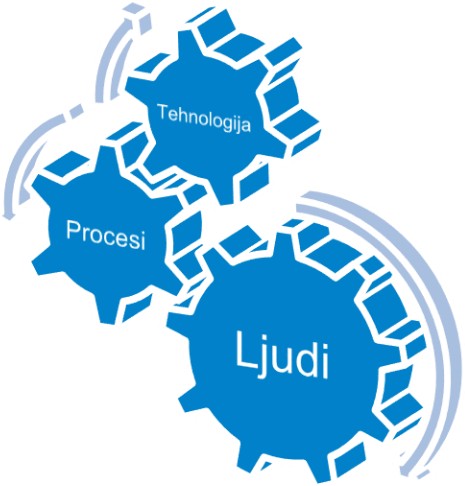
epsiloneridani0

Kako postati otporan?

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset management	Identity management	Anomalies and events	Response planning	Recovery planning
Governance	**Access control**	Continuous monitoring	Response communications	Recovery improvements
Risk assessment	**Awareness training**	**Detection process**	Response analysis	Recovery communications
Risk management	**Data security**		Response mitigation	**Backup**
Supply chain risk management	**Information protection**		Response improvements	**Redundancy**
	Maintenance			
	Protective technology			
	Personnel security			



Zaključak



info.digital@koncar.hr