



# ЗАЩИТА ПРОМЫШЛЕННЫХ СЕТЕЙ



Степан Ульянов  
CCSE CheckPoint MONT

# Факты и реальность



Check Point<sup>®</sup>  
SOFTWARE TECHNOLOGIES LTD.

**Декабрь  
2014**

Металлургический завод в Германии был взломан с помощью фишинговой атаки – Массивные повреждения на заводе

**Декабрь  
2015**

Взлом энергетической компании Украины «Прикарпатьеоблэнерго» благодаря вредоносной атаке BlackEnergy Spear Phishing (19 Января – повтор на подстанции Пивничнах)

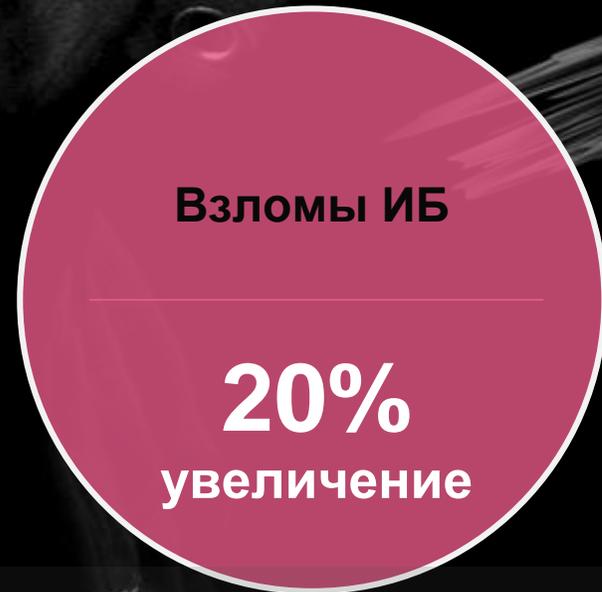
**Март 2016**

Хакеры взломали систему управления очистки водных ресурсов и поменяли уровень химических элементов, которые использовались для обработки водопроводной воды (Kemuri Water Company)

**Май 2017**

Массовое распространение WannaCry пострадало 500 тысяч компьютеров, принадлежащих частным лицам, коммерческим и правительственным организациям, в более чем 200 странах мира

# ICS-CERT Итоги: постоянное увеличение Атак на Критическую Инфраструктуру США



**ICS-CERT: Эти атаки были возможны благодаря архитектурным просчетом построения сетей ICS**

# Почему эти атаки возможны?

Устаревшие и необновленные системы

Ошибки в сегментации, подключение технологических сетей к Интернету

Задержки в обслуживании критических систем препятствуют адекватной защите

# Векторы Атак на корпоративные сети



Внешние накопители



Почтовый Фишинг и Вложения



Удаленная поддержка



Уязвимости в ПО



Гостевые Сети  
Незащищенные Розетки

## CHECK POINT'S

# Решения безопасности для АСУ ТП (Industrial control Systems)

## КИБЕР ЗАЩИТА

Обзор и детальный  
контроль SCADA трафика

Специализированная  
защита от SCADA угроз

Надежные устройства для  
агрессивной среды

SCADA

# Обширная поддержка SCADA/ICS-специализированных протоколов



Свыше **720 АСУ ТП** команд  
в Check Point Application Control

# Детальное протоколирование SCADA трафика

Детальная форензика для расследования инцидентов

## ДЕТАЛЬНО

Time	B...	A...	T...	Origin	Application...	Transa...	Fu...	Function Description	Source	Desti...	...	Matched Ca
Today	10:45:35			gw-71ec22	ModbusAll	33394	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33490	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33490	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33489	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33489	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33488	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33488	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33487	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33487	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33486	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33486	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33485	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:53			gw-71ec22	ModbusAll	33485	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33484	4	Read Input Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33484	4	Read Input Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33483	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33483	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33482	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33482	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33481	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33481	3	Read Holding Registers	HMI-1	PLC-1		SCADA Prot
Today	10:45:51			gw-71ec22	ModbusAll	33480	3	Read Holding Registers - Response	HMI-1	PLC-1		SCADA Prot

**АНАЛИЗ**  
С ПОМОЩЬЮ  
**Check Point**  
**SMARTLOG &**  
**SMARTEVENT**

## ПО ГРУППАМ

Count	Source	Destination	Unit ID	Function Description	Transaction ID	Start Address
500	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Read Holding Registers		
100	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Read Input Registers		10
1	HMI (10.1.1.5)	PLC (20.1.1.5)	1	Write Single Register	19	50

# Полная отчетность по SCADA трафику

Allowed application Modbus\_all

Log Info

## SCADA детально

Modbus	
Unit ID	1
Transaction ID	2667
Function Code	6
Function Description	Write Single Register
Range Start Address	41
Range End Address	41
Quantity	1
Value	0001

Application Properties	
Application Risk	Unknown
Application Name	Modbus_all

Modbus	
Unit ID	1
Transaction ID	2667
Function Code	6
Function Description	Write Single Register
Range Start Address	41
Range End Address	41
Quantity	1
Value	0001

More	
Application ID	20000002
Application Rule ID	{DBD03A47-AA8C-44DB-997}
Application Rule Name	Learning Rule
Application Signature	20000002:1
Primary Category	SCADA Protocols
Proxy Source IP	HMI (10.1.1.5)

Protocol	TCP (6)
Destination Port	502
Source Port	49159
Service Name	Modbus

# Полный контроль и видимость SCADA трафика

## ПРОТОКОЛЫ и КОМАНДЫ

Source	Destination	Applications/Sites	Action
 Any	 Any	 High Risk	 Block  Blocked
 Control_servers	 PLCs	 Modbus Protocol-write single register  Modbus Protocol-write multiple coils  Modbus Protocol-write file record  Modbus Protocol-write single coil	 Allow
 Monitor_servers	 PLCs	 Modbus Protocol-read input register  Modbus Protocol-read coils  Modbus Protocol-read file record	 Allow

## ПАРАМЕТРЫ КОМАНД

Standard Function    15: Write Multiple Coils

Any Address

Address Range    100 - 200

Custom Function

Function Range    1 - 1

# Настройка Политик и Правил устанавливая Функции и Значения (Functions and Values)

SCADA Application - Modbus

General Properties

Name: **Modbus** [Black]

Comment:

Primary Category: SCADA Protocols

Protocol: Modbus

Unit

Any Unit

Specified Unit ID 0 - 0

Function

Any Function

Standard Function **06: Write Single Register**

Any Address

Address Range 0 - 0

Custom Function

Function Range 1 - 1

Value

Any Value

Specified Value **0 - 1500**

Allow out of range values

OK Cancel

Protocol

Command  
(Function)

Allowed  
values and  
ranges

Active or  
Passive  
Policy

Name	Source	Destination	Applications/Sites	Action
Block High Risk apps	Any	Any	High Risk	Block Blocked
Control servers	Control_servers	PLCs	Modbus Protocol-write single register Modbus Protocol-write multiple coils Modbus Protocol-write file record Modbus Protocol-write single coil	Allow
Monitor servers	Monitor_servers	PLCs	Modbus Protocol-read input register Modbus Protocol-read coils Modbus Protocol-read file record	Allow
Block SCADA traffic	Any	Internal PLCs	SCADA Protocols	Block

# Виртуальный пачтинг с помощью свыше 200 специализированных IDS/IPS сигнатур

**ЗАЩИТА**  
с помощью  
**Check Point**  
**IPS**

Protection	Severity
Shield Citect SCADA ODBC Overflow Attempt	Medium
Shield Rockwell RSLogix Denial of Service Vulnerability	Critical
Shield SCADA Engine OPC Client Buffer Overflow Vulnerability	High
Shield Schneider Electric UnitelWay Windows Device Driver Buffer Overflow	Critical
<b>Shield Siemens Tecnomatix FactoryLink Stack Overflow Vulnerability</b>	<b>Critical</b>
Shield Siemens Automation License Manager Multiple Vulnerabilities	Critical
Shield ScadaTEC SCADAPhone and ModbusTagServer Buffer Overflow	High
Shield RealWin HMI Service Buffer Overflow 2	High
Shield Automated Solutions Modbus/TCP Master OPC server Modbus TCP Header	High
Shield RealWin INFOTAG/SET_CONTROL Packet Processing Buffer Overflow	High
Shield Unauthorized Miscellaneous Request to a PLC	Critical
Shield Broadcast Request from an Authorized Client	Critical
Shield IGSS SCADARMS Report Template WriteFile Command Buffer Overflow	Critical
Shield IGSS SCADA STDREP Request Buffer Overflow	High
Shield Iconics Genesis SCADA Freeing of Uninitialized Memory Trigger	High
<b>Shield Rockwell RNA Message Negative Header Length</b>	<b>Critical</b>
Shield Intellicom NetBiter Config HICP Hostname Buffer Overflow	Medium
Shield WonderWare SuiteLink DOS Attempt	High

# Быстрый анализ подозрительного трафика между контроллерами

**АНАЛИЗ**  
с помощью  
**Check Point**  
**SMARTEVENT**

Edit Event Definition

Name Filter Count logs Event Format GUI representation

The new event is triggered by:

a single log.

multiple logs over a period of time.

Detect the event when at least  logs occurred over a period of  seconds.

Each event definition may have multiple Event Candidates existing simultaneously. Log records are passed to Event Candidates based on the value of selected log fields. For example, if "Service" is selected, each log with a different service will create a new Event Candidate, while logs with the same service will be directed to the same Event Candidate.

Анализ риска с помощью специализированных отчетов угроз

Просмотр попыток отправить избыточные команды

Просмотр попыток сетевой разведки

# Check Point 1200R

Специально разработанный защищенный шлюз безопасности

- **Полнофункциональный** шлюз безопасности Check Point
- **6x1GbE портов** и firewall throughput до 2Gbps
- **Соответствует** самым жестким регуляторным требованиям: IEC 61850-3 и IEEE 1613
- **Компактный безвентиляторный** дизайн; температурный диапазон от -40°C до 75°C



# OT Security Blueprint

## Management Facility

Main Control Center



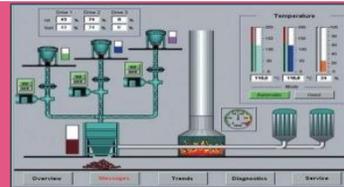
SCADA Historian

SmartEvent



SCADA VPN

Control & monitor



Control  
Monitor



PLC1

PLC2

PLC3



PLC4

Shop Floor

Shop Floor