Ландшафт угроз системам промышленной автоматизации

Евгений Гончаров,

Head of Critical Infrastructure Defense,

Kaspersky Lab

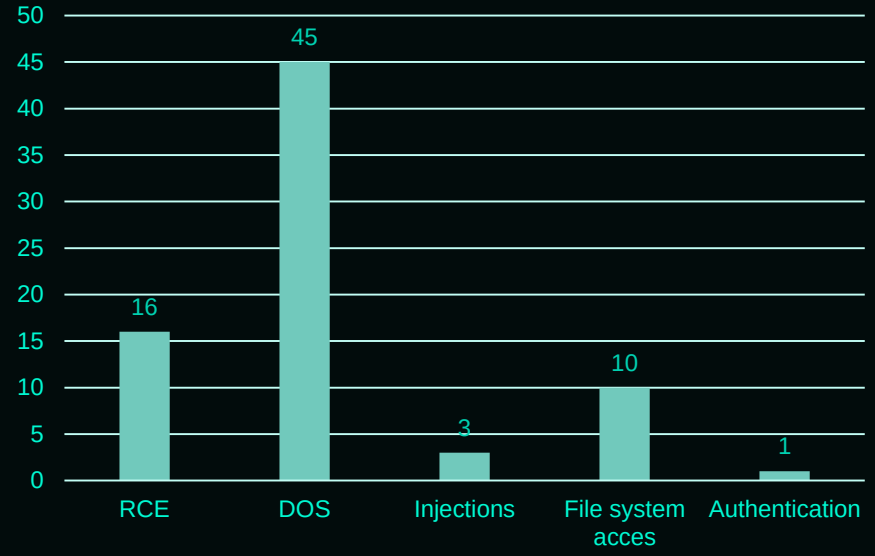
I.

УГРОЗЫ ПРОМЫШЛЕННЫМ ПРЕДПРИЯТИЯМ

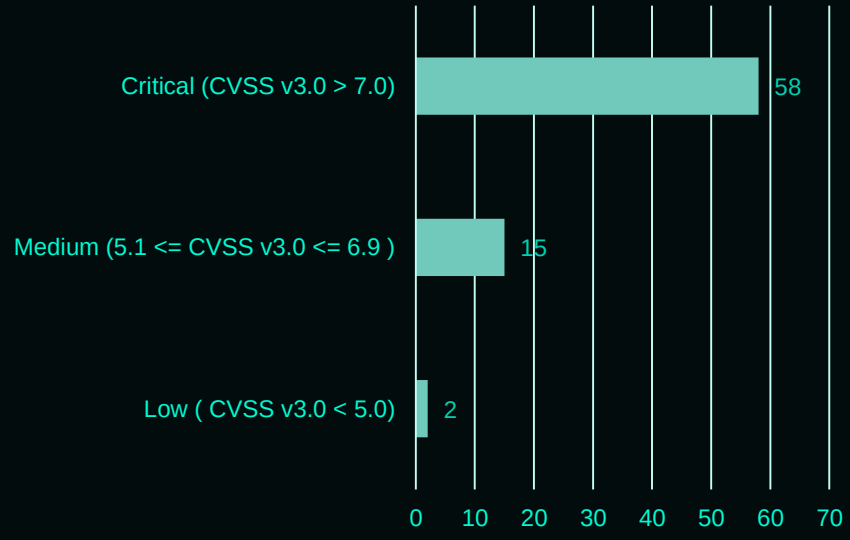
Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

70+ уязвимостей 0го дня в продуктах АСУ ТП

Типы уязвимостей



Уровень критичности (CVSS v. 3.0)



KASPERSKY lab

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

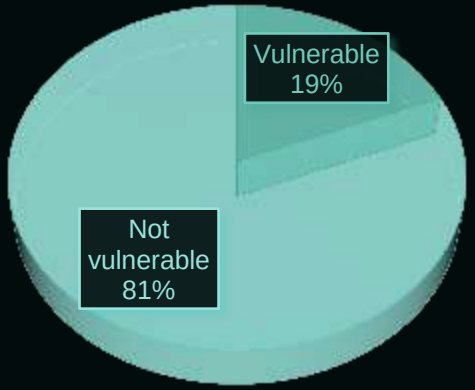
30 уязвимостей исправлено разработчиками (март 2017)

https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-284342.pdf
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-378531.pdf
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-453276.pdf
http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-946325.pdf
….
https://ics-cert.us-cert.gov/advisories/ICSA-16-336-03
…

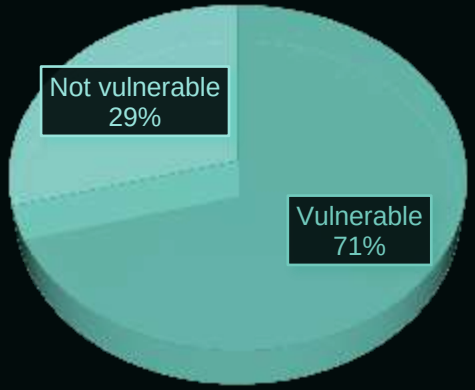
Анализ угроз АСУ

% уязвимого ПО Rockwell Automation по статистике KSN (пример)

CVE-2013-2811



CVE-2014-0750

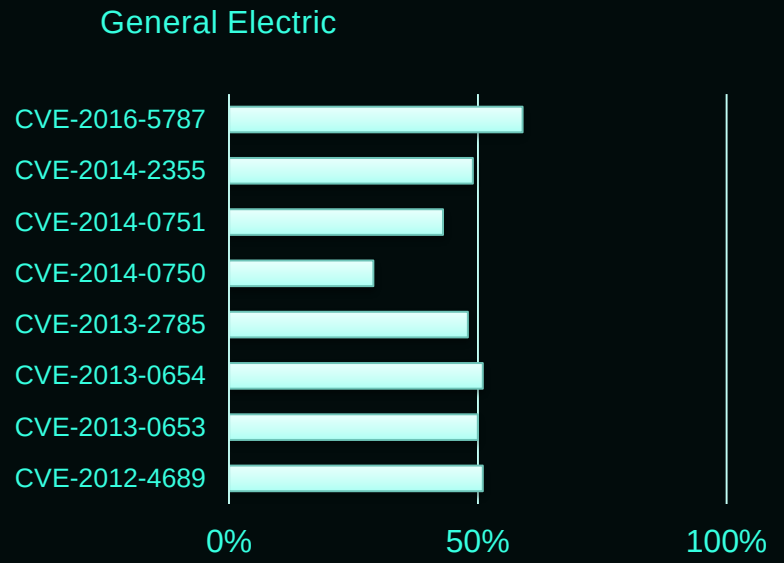


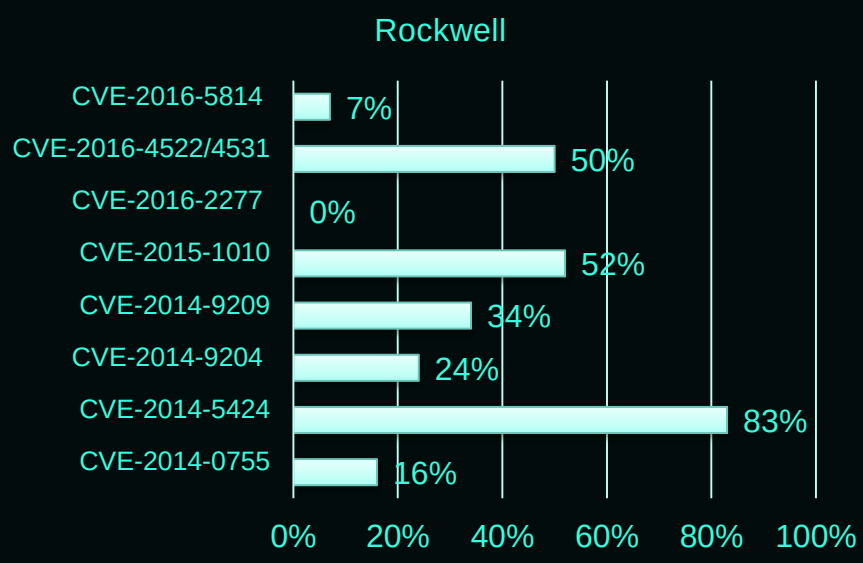
CVE-2016-2277

По данным https://ics-cert.kaspersky.ru

Анализ угроз АСУ

% уязвимого ПО по статистике KSN (пример)

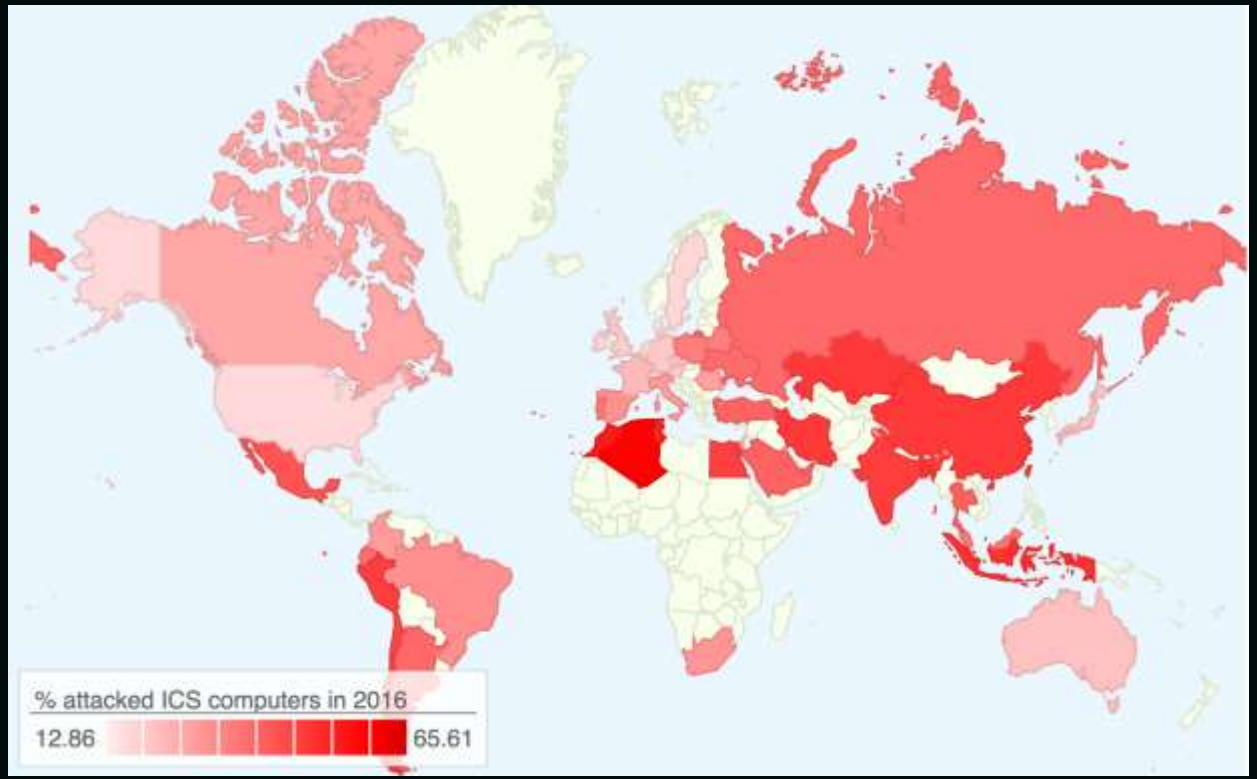




По данным https://ics-cert.kaspersky.ru

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

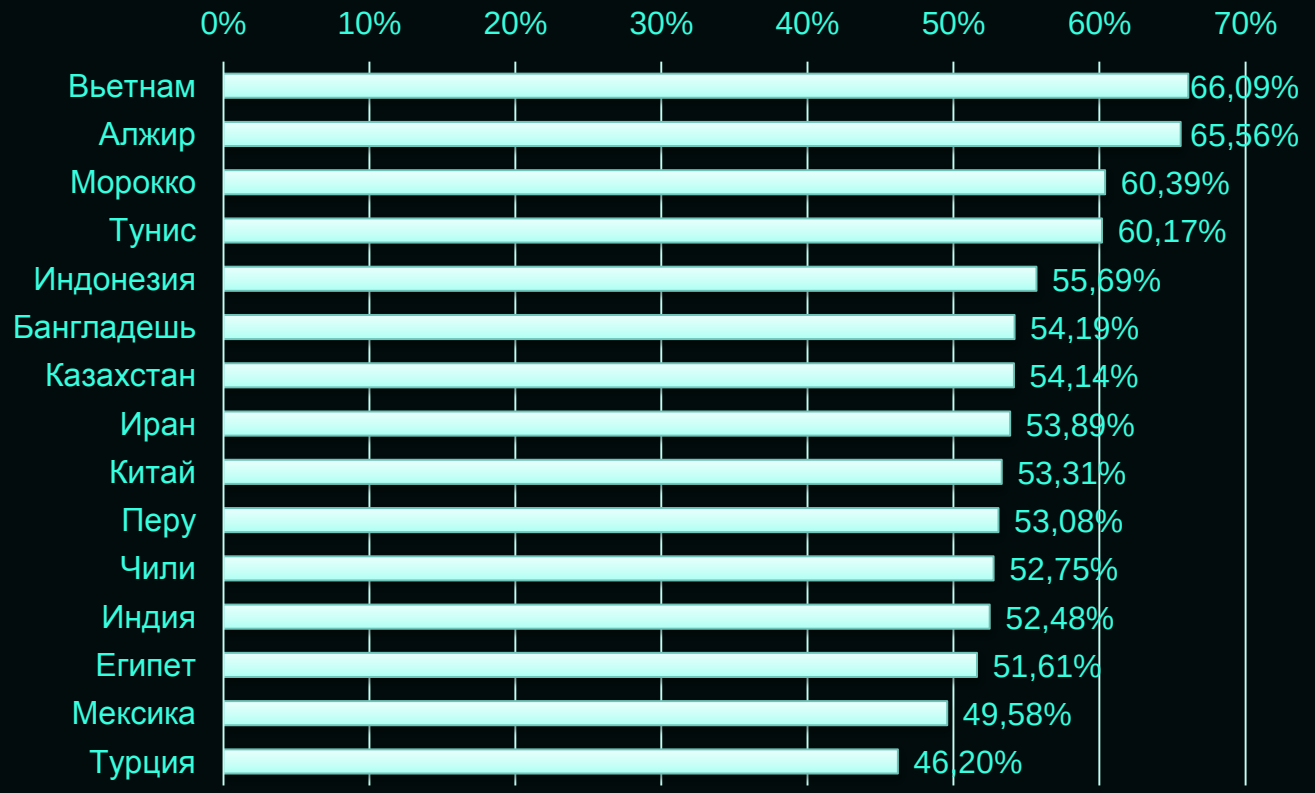
% атакованных промышленных компьютеров в 2016 году



По данным https://ics-cert.kaspersky.ru

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

ТОП 15 стран по % атакованных промышленных компьютеров в 2016 году

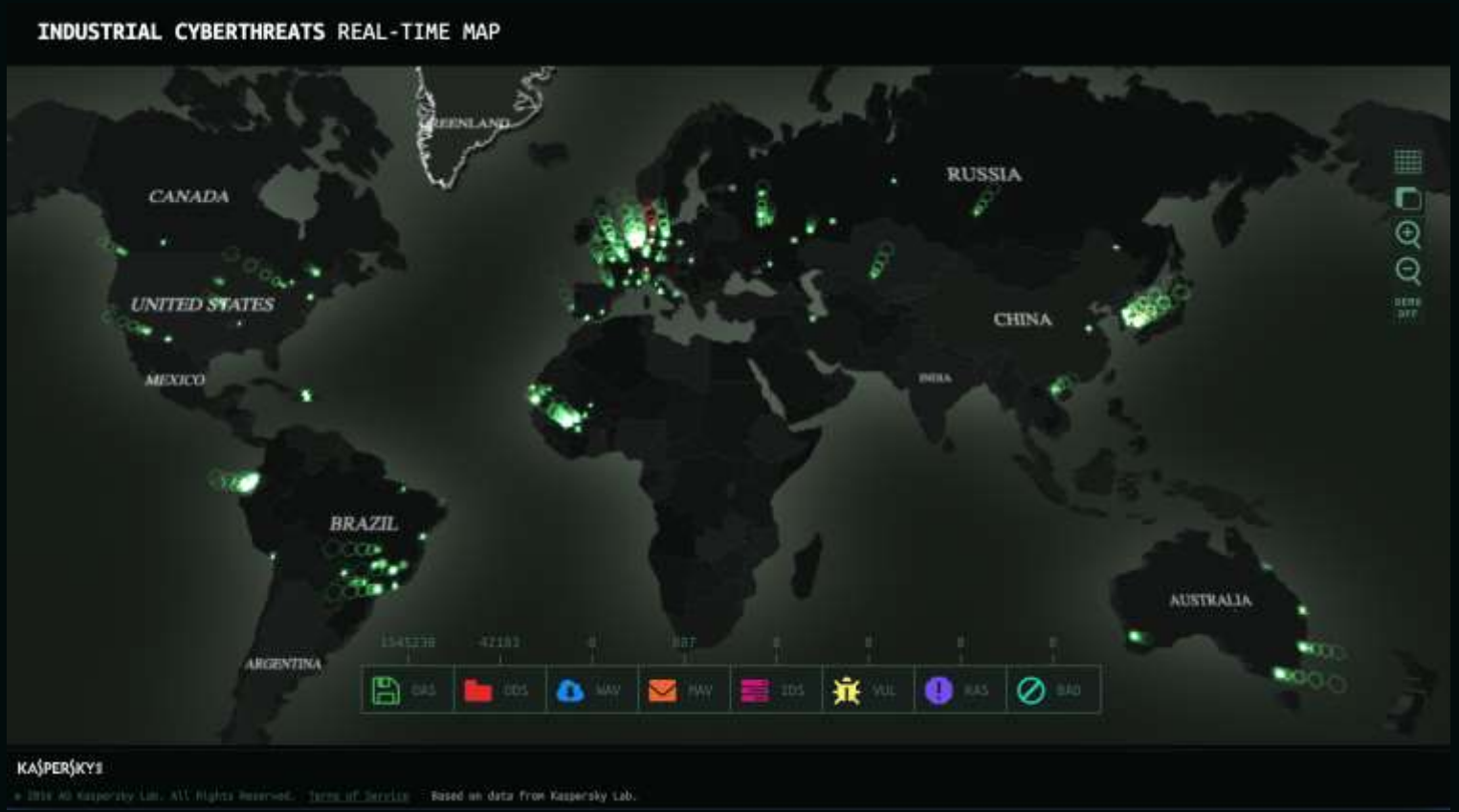


По данным https://ics-cert.kaspersky.ru

KASPERSKY lab

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

Карта атак промышленных систем в «реальном времени»

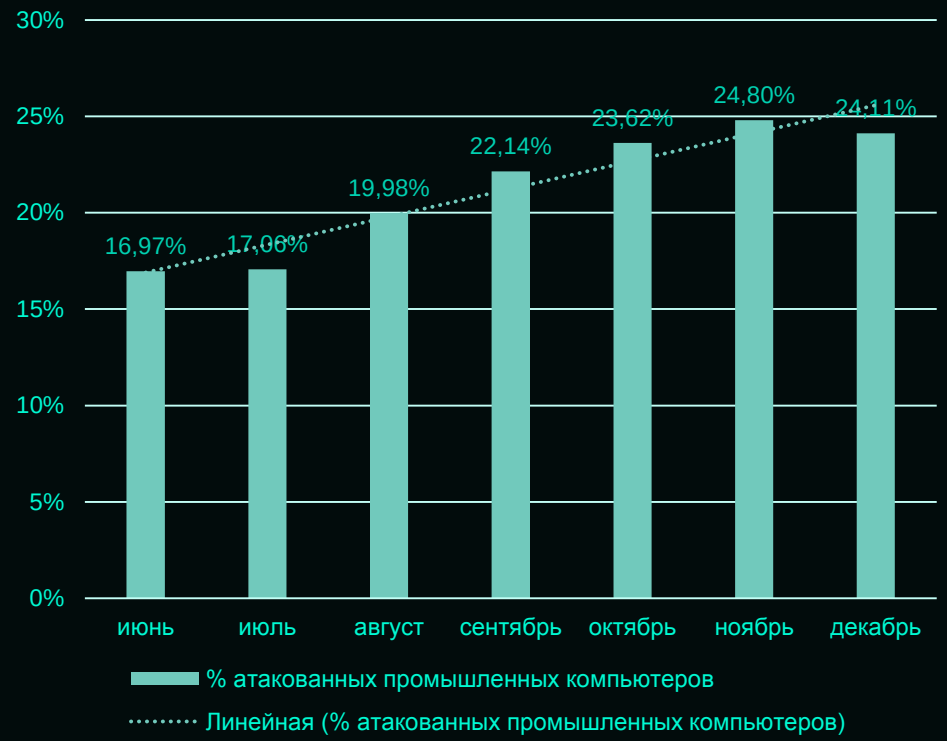


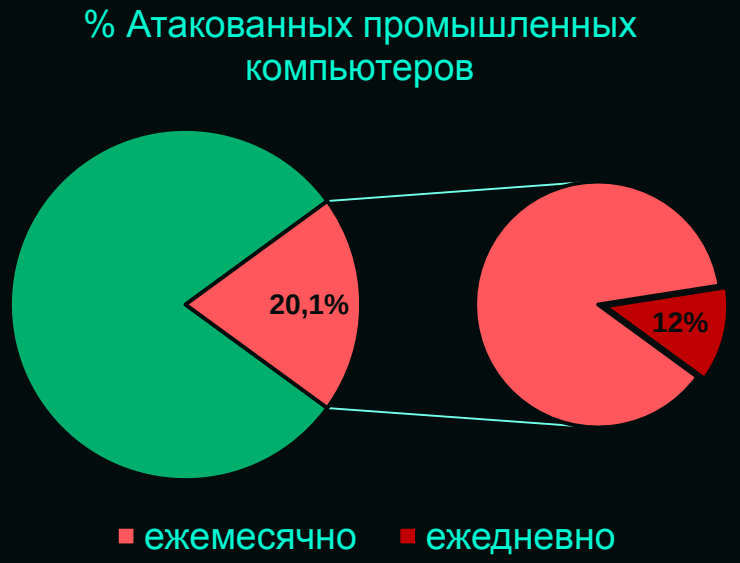
https://ics-cybermap.kaspersky.com

KASPERSKY lab

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

промышленных систем в «реальном времени»



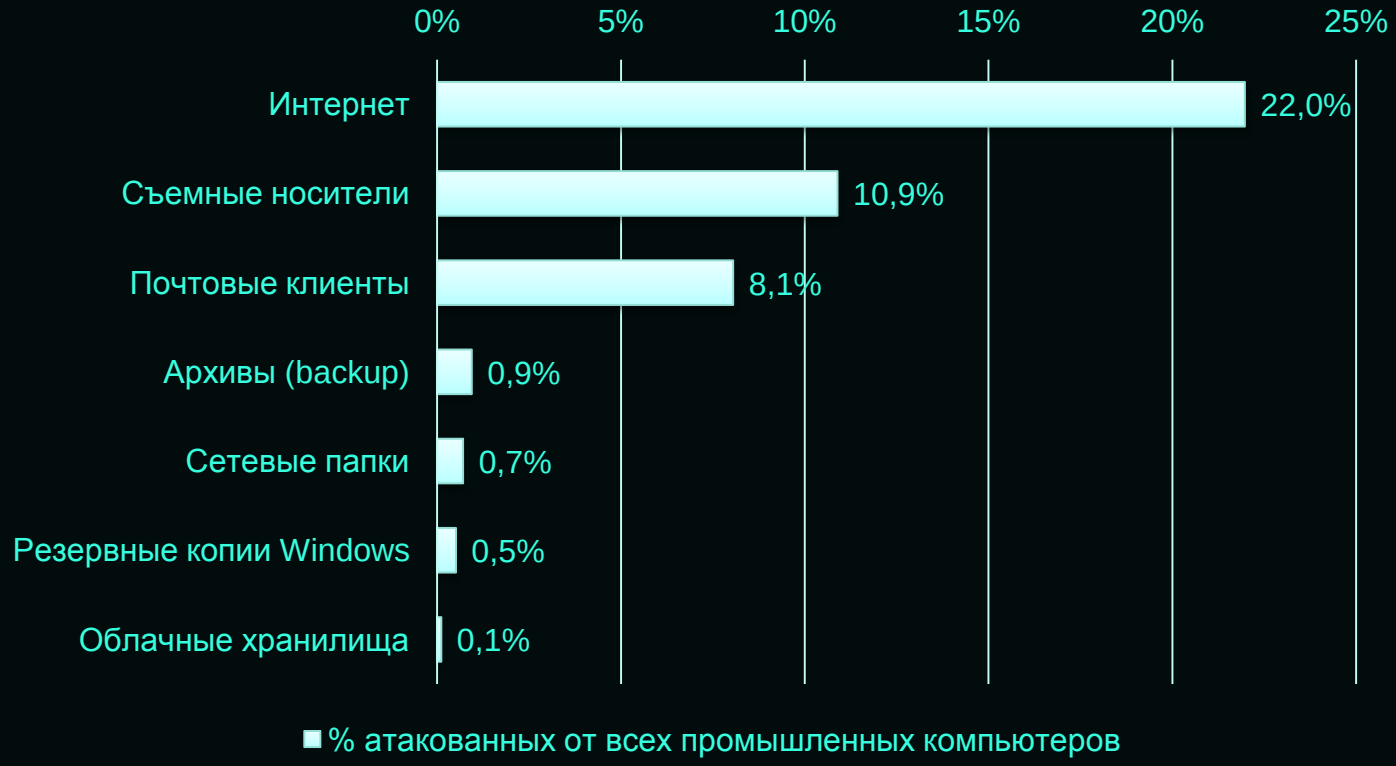


По данным https://ics-cert.kaspersky.ru

KASPERSKY lab

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

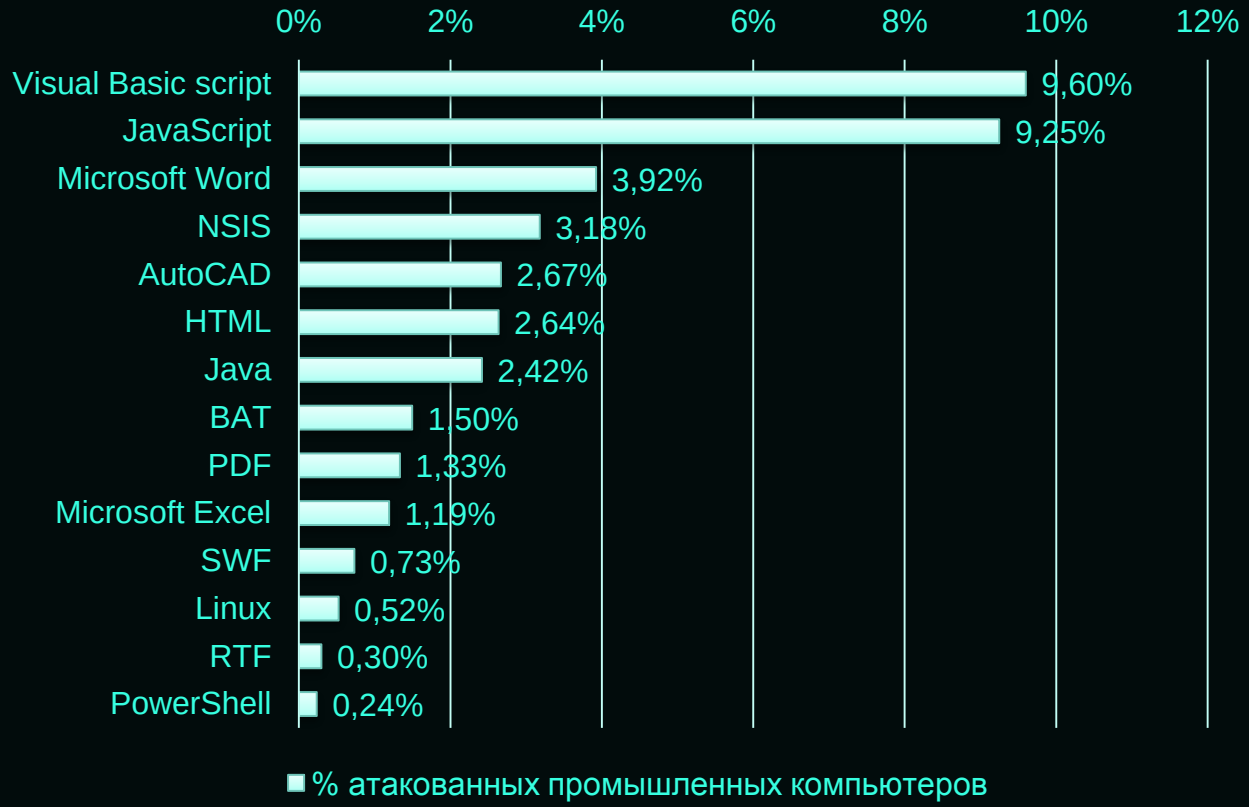
Основные источники угроз АСУТП



По данным https://ics-cert.kaspersky.ru

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

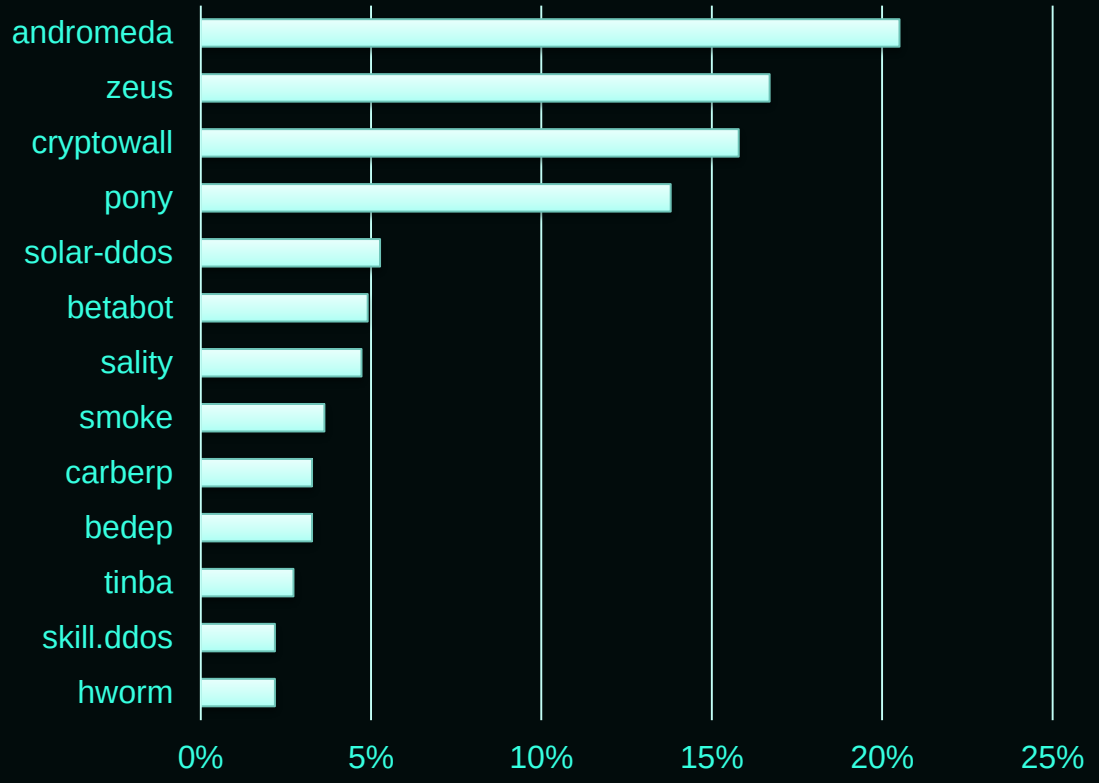
Основные источники угроз АСУТП - 3е-стороннее ПО



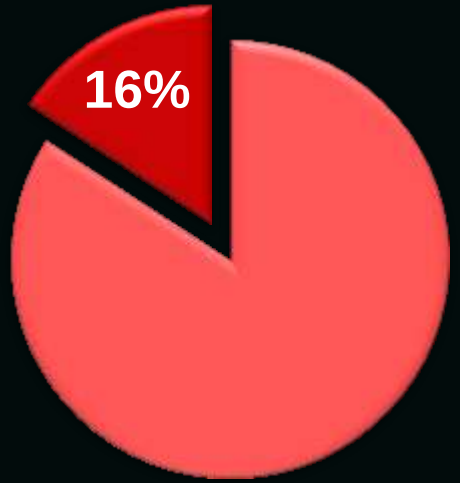
По данным https://ics-cert.kaspersky.ru

Анализ угроз АСУ Q3-Q4 2016 (по данным KL ICS CERT)

Заражения АСУТП - бот-нет-агентами



% бот-сетей среди всех угроз АСУ



По данным https://ics-cert.kaspersky.ru

KASPERSKY lab

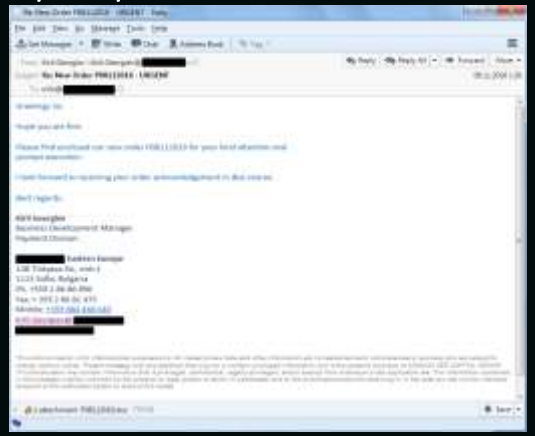
II.

АТАКИ НА ПРОМЫШЛЕННЫЕ ПРЕДПРИЯТИЯ

Масштабная атака на промышленные компании

500+ промышленных организаций и их поставщиков («Нигерийский» сервис)

Примеры писем:



Заражённые домены:

alreyadbplastics.com	Nigeria
xpweb.win	Ghana
heinevy.com	Nigeria
overseas-operation.com	Nigeria
metaksen.com	Taiwan
charlogistics.com	USA
btinterment.com	Nigeria
kinqnuts-raaphorst.com	Nigeria
watersysterns.com	Nigeria
hidroquil-ar.com	Nigeria
thai-nidhi.com	Nigeria
ms45-hinet.net	Nigeria
fullone2u.com	USA

Md5:

0431fb071b43075967d95dca4e4b74a4
060aba7b0dfe98f344a08525794f3a39
0b7f872d098ef8f1dd0e52f6d5c5a92e
0eb12f0c3aa4ec1db178fbbe69a329cf
10bd1bcf24e12761df2ac8574cd5421e
11b949dafc35aaab4595ed5d5119731f
139ac7a3ea98a743ab53e5dc9a143d14
1c000371cda75156c5af004ca4b08e08
27ede7277a5c482d156bf8cad3d67ecf
36db408c729e4eec4b67593dbe6e21cb
4231e1ddf6cd6edc269b65221e983a2a
51966a70638915dbd7be9f15592cb453
51a5f21d781c8ab2b081ca3d044bb548
57beddcde4930bff12554c70ac0d486e
57da8a2813c9b1cb6598609e10faf1b4
652e2222f3523296020ae0adaa392036
6dd0b2770a7d7bcdecc5f6eebbde4d7c
7e5c5279a6b25fc25e822277a0e67893
94083460473c6ccf96060c3f35bda8f0
a598c6964f7f9aef6e6ad21c630e744a
abaaba5109c19f658f9eaf56551c0996
b0a68240b82a8d4ff46a9bb4833c243a
ba4dcb0af37929c7f85d0830e4fb7682
bcd6efb7ba13404999640cbf4a8300ef
c31f027c91a17e696d3badb647b4776e
c5674b866e3362bc09dfab0385b44bec
df1ff7cc193e6daabdb54e44d7d376c1
ead4bbedddba4cd1d0b31a82987ffce4
f1e7507e85804477b46041c4f79a6318

Snort -правила

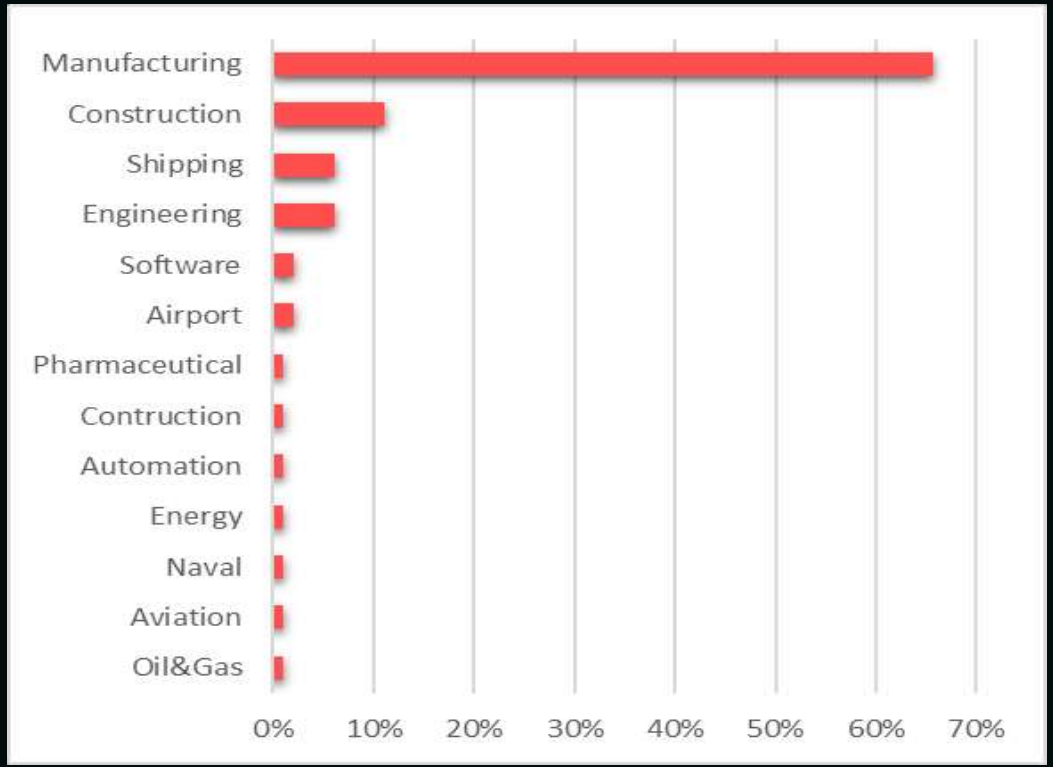
alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"Zeus C&C call"; flow:established,to_server; content:"POST "; depth:5; nocase; content:!"/ HTTP"; content:" HTTP/1."; content:"|0D 0A|Accept|3a| */*|0D 0A|User-Agent|3a| Mozilla"; distance:1; within:34; content:"|0D 0A|"; distance:0; content:"Content-Length|3a| "; distance:0; content:!"0"; within:1; content:"Connection|3a| Keep-Alive|0D 0A|"; distance:0; content:"|3a| no-cache"; distance:0; content:"|0D 0A 0D 0A|"; distance:0; content:!"Content-Type|3a| "; content:!"NetflixId="; content:!".baidu."; sid: #{RecordId};)

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:" Zeus C&C call"; flow:established,to_server; content:"POST"; http_method; content:".php"; http_uri; content:"HTTP/1."; content:"|0D 0A|Accept|3a| */*|0D 0A|User-Agent|3a| Mozilla"; distance:1; within:34; fast_pattern; content:!"Accept-"; http_header; content:!"Content-Type|3a|"; http_header; content:!"Referer|3a|"; http_header; pcre:"/^Accept\x3a *\/*\r\nUser-Agent\x3a[^\r\n]+?\r\nHost\x3a[^\r\n]+?\r\nContent-Length\x3a[^\r\n]+?\r\nConnection\x3a[^\r\n]+?\r\n(?:Pragma|Cache-Control)\x3a[^\r\n]+?\r\n(?:\r\n)?$/H";; sid: #{RecordId};)

По данным https://ics-cert.kaspersky.ru

Цели атаки на промышленные компании (индустрии)

500+ промышленных организаций и их поставщиков («Нигерийский» сервис)



По данным https://ics-cert.kaspersky.ru

III.

Advanced Persistent (и не только)Threats

Наша повседневная работа

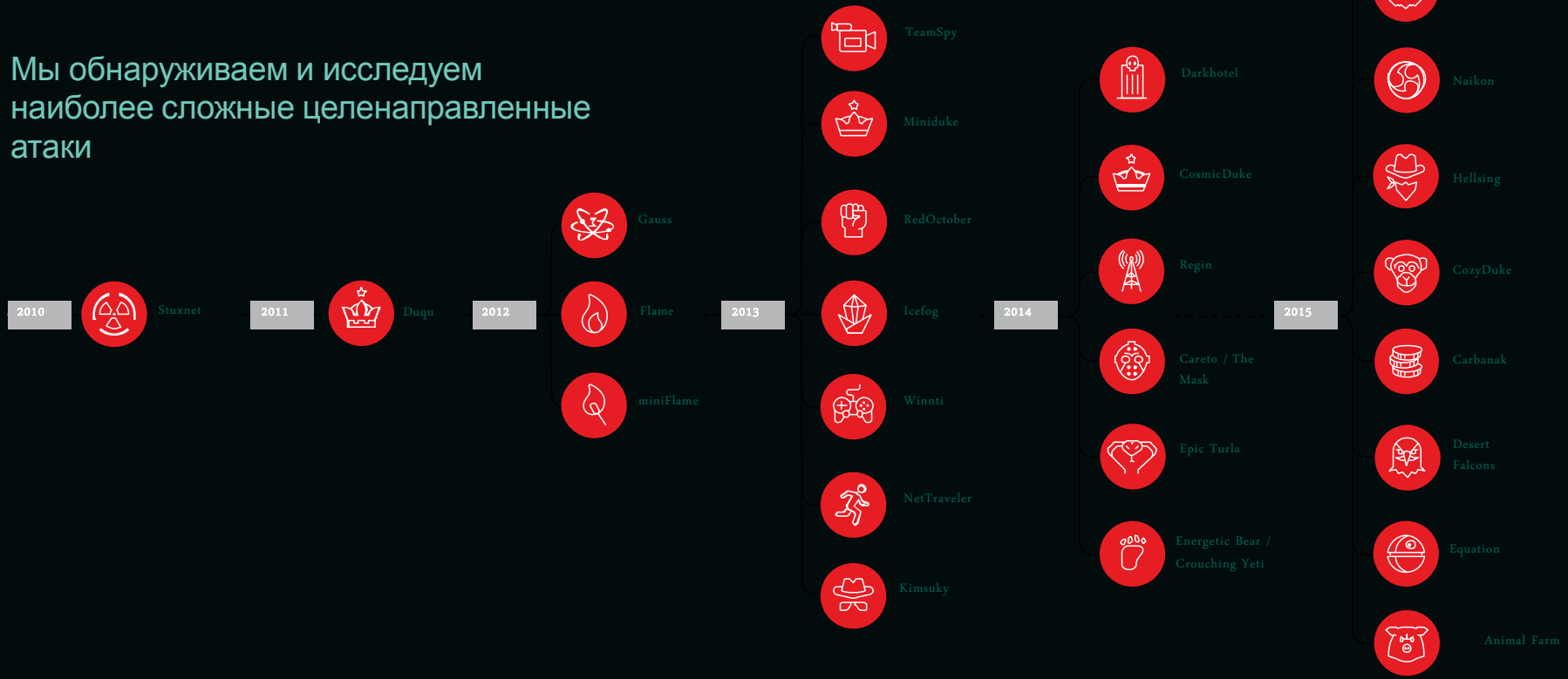
Типы обнаруживаемых и исследуемых «Лабораторией Касперского» угроз

KASPERSKY

Наша повседневная работа

Наиболее громкие атаки, обнаруженные и расследованные нами

Мы обнаруживаем и исследуем наиболее сложные целенаправленные атаки



KASPERSKY lab

Наша повседневная работа

% целевых атак, направленных на промышленные предприятия

25% всех целевых атак, обнаруженных и расследованных ЛК в 2016г направлены, в том числе, на промышленные предприятия!

IV

ПРАКТИЧЕСКИЕ УЧЕНИЯ

ICS Threat Vector Modelling – Energy

Industrial CTFs organized in 2015-2016

KASPERSKY lab

V

КИБЕРИНЦИДЕНТЫ

КИБЕРИНЦИДЕНТЫ: ЭНЕРГЕТИКА

УКРАИНА, ДЕКАБРЬ 2015

КИБЕР-АТАКА:

- один из управляющих компьютеров заражен BalckEnergy2 посредством фишинговой email-атаки
- резервные источники питания (UPS) атакованы
- RTU микропрограмма изменена
- средства удаленного управления уничтожены
- DDoS-атака на центры телефонной поддержки

12/24/2015

Dear customers!

Dec. 23, 2015, from 15:35 - 16:30, third parties were made illegal entry into information-technological system of remote access to equipment telecontrol substations of 35-110 kV JSC "Kyivoblenergo."

As a result, it was disconnected 7 (seven) 110 kV substations and 23 (twenty three) substation 35 kV. This led to the repayment of about 80,000 different categories of customers on the reliability of electricity supply.

Electricity was restored to all consumers employees of the Company at **18:56** the same day.

We apologize for the situation and thank you for your understanding.

PJSC "Kyivoblenergo"

ФИЗИЧЕСКИЙ УЩЕРБ:

- секционные выключатели удаленно управлялись злоумышленниками
- удаленное управление было заблокировано для легитимных операторов
- отключение электричества на 7-и 110 кВ и 23-х 35 кВ подстанциях
- 3 области, более 225 000 потребителей осталось без электричества более чем на 6 часов.

БОЛЕЕ 225 000 ПОТРЕБИТЕЛЕЙ ОБЕСТОЧЕНО НА 6 ЧАСОВ В 5ТИ ОБЛАСТЯХ

КИБЕРИНЦИДЕНТЫ: ЭНЕРГЕТИКА

УКРАИНА, ДЕКАБРЬ 2016

КИБЕР-АТАКА:
НА ПОДСТАНЦИЮ «СЕВЕРНАЯ» 330КВ

ФИЗИЧЕСКИЙ УЩЕРБ:

- Отключение потребителей на 1ч 15 мин

ОТКЛЮЧЕНИЕ РАЙОНОВ КИЕВА

КИБЕРИНЦИДЕНТЫ: НЕФТЬ И ГАЗ

САУДОВСКАЯ АРАВИЯ, 2012

КИБЕР-АТАКА:

- Червь Shamoon повредил около 35 000 компьютеров (удалил данные и исполняемые файлы)
- Пострадали системы документооборота
- Потребовалась срочная замена 50 000 жёстких дисков (что отразилось на цене дисков на глобальном рынке)

Saudi Aramco suffered the worst hack in world history in 2012.

ФИЗИЧЕСКИЙ УЩЕРБ: ОСТАНОВЛЕНА ОТГРУЗКА НЕФТЕПРОДУКТОВ НА ТЕРРИТОРИИ СТРАНЫ

- НА 18ЫЙ ДЕНЬ ПРОДУКТ НАЧАЛИ ОТГРУЖАТЬ БЕЗ ПОДТВЕРЖДЕНИЯ ОПЛАТЫ

КИБЕРИНЦИДЕНТЫ: НЕФТЬ И ГАЗ

САУДОВСКАЯ АРАВИЯ, НОЯБРЬ 2016 – ЯНВАРЬ 2017

КИБЕР-АТАКА SHAMOON 2.0 STONEDRILL

Saudi Aramco suffered the worst hack in world history in 2012.

ПОДРОБНОСТИ НА SAS 2017 (2-5 АПРЕЛЯ 2017)

КИБЕРАТАКА: ВОДА и ЭЛЕКТРОЭНЕРГЕТИКА

BWL, МИЧИГАН, США 2016

КИБЕР-АТАКА:

- Фишинговая атака – доставка ransomware
- Заблокирована бухгалтерская система и почта
- Отключены телефонные линии, включая службу поддержки клиентов
- Клиентам не выставлялись счета на оплату

ЭКОНОМИЧЕСКИЙ УЩЕРБ:

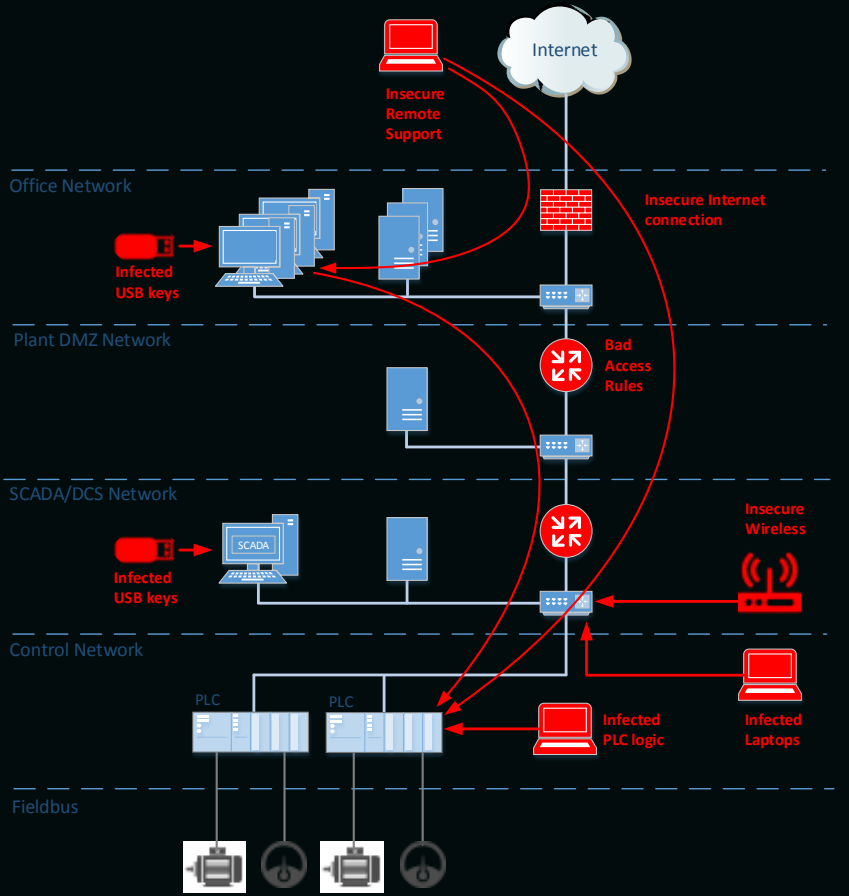
ВЫПЛАТА ВЫКУПА В $25К.
ПЕРВЫЙ ЗАДОКУМЕНТИРОВАННЫЙ СЛУЧАЙ RANSOMWARE ДЛЯ

ЗАТРАТЫ НА УЛУЧШЕНИЕ КИБЕРЗАЩИТЫ СОСТАВИЛИ $2.4M

VI

МОДЕЛИРОВАНИЕ УГРОЗ

ВЕКТОРЫ КТИБЕР-АТАК

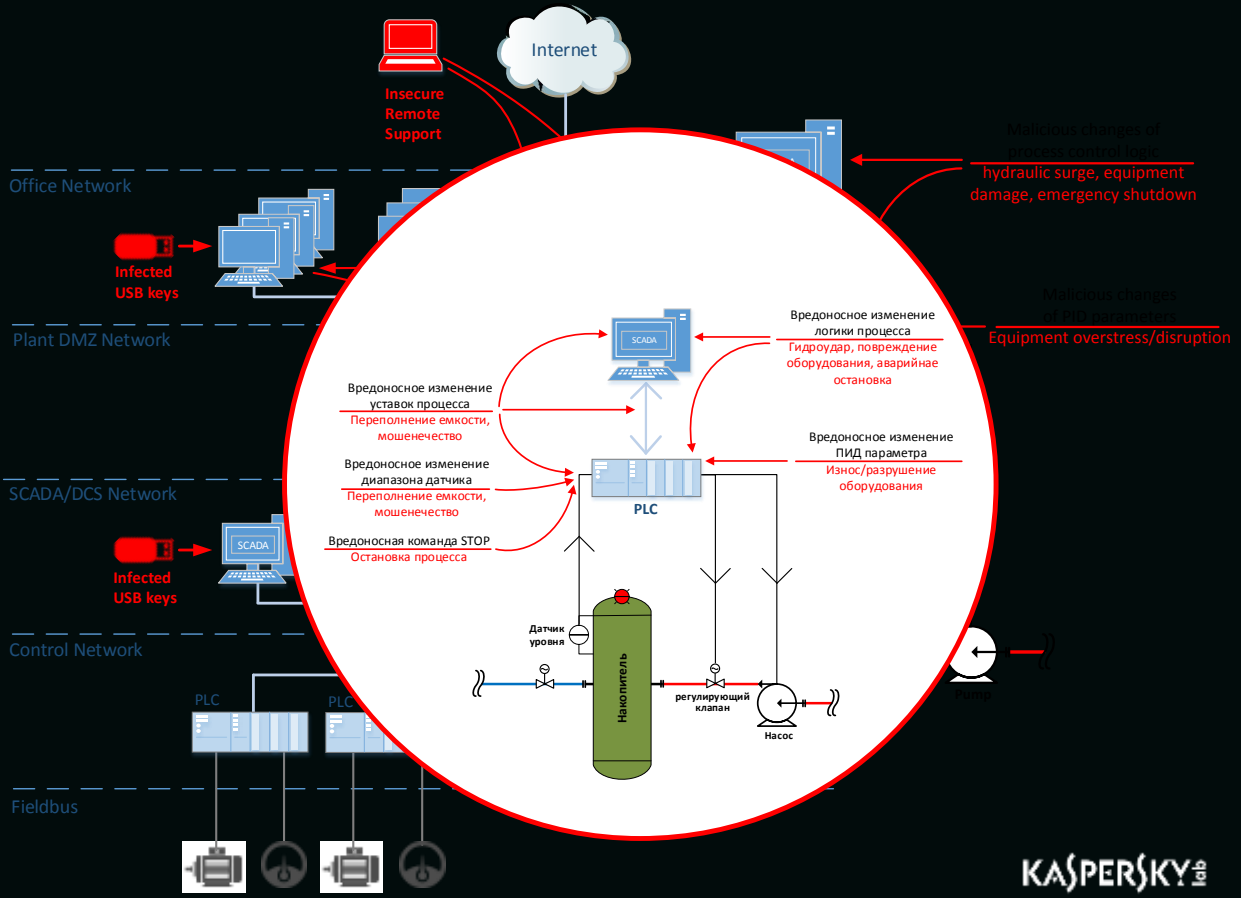


KASPERSKY lab

КИБЕР-ФИЗИСЕСКАЯ СОСТАВЛЯЮЩАЯ

Главные факторы риска:

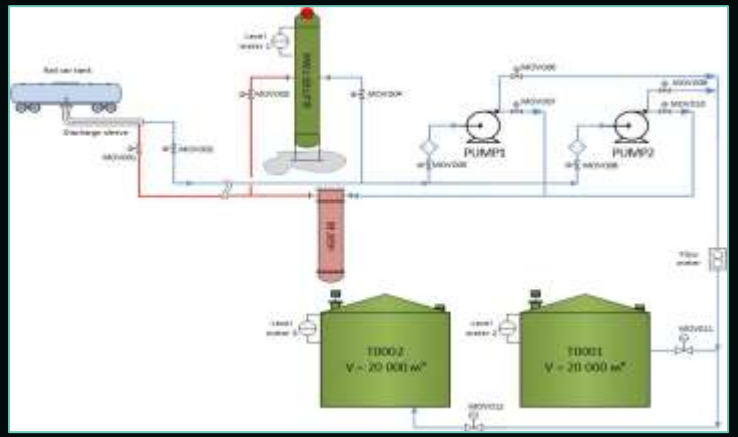
- Сотрудники
- Подрядчики
- Поставщики



KASPERSKY lab

МОДЕЛИРОВАНИЕ АТАКИ

- ЖД терминал разгрузки нефтепродуктов
- Цель кибер-преступника – инициировать промышленную аварию.



Нарушитель предпринимает последовательность действий в попытке завладеть управлением элементами АСУ ТП и нанести физический урон вредоносных команд.

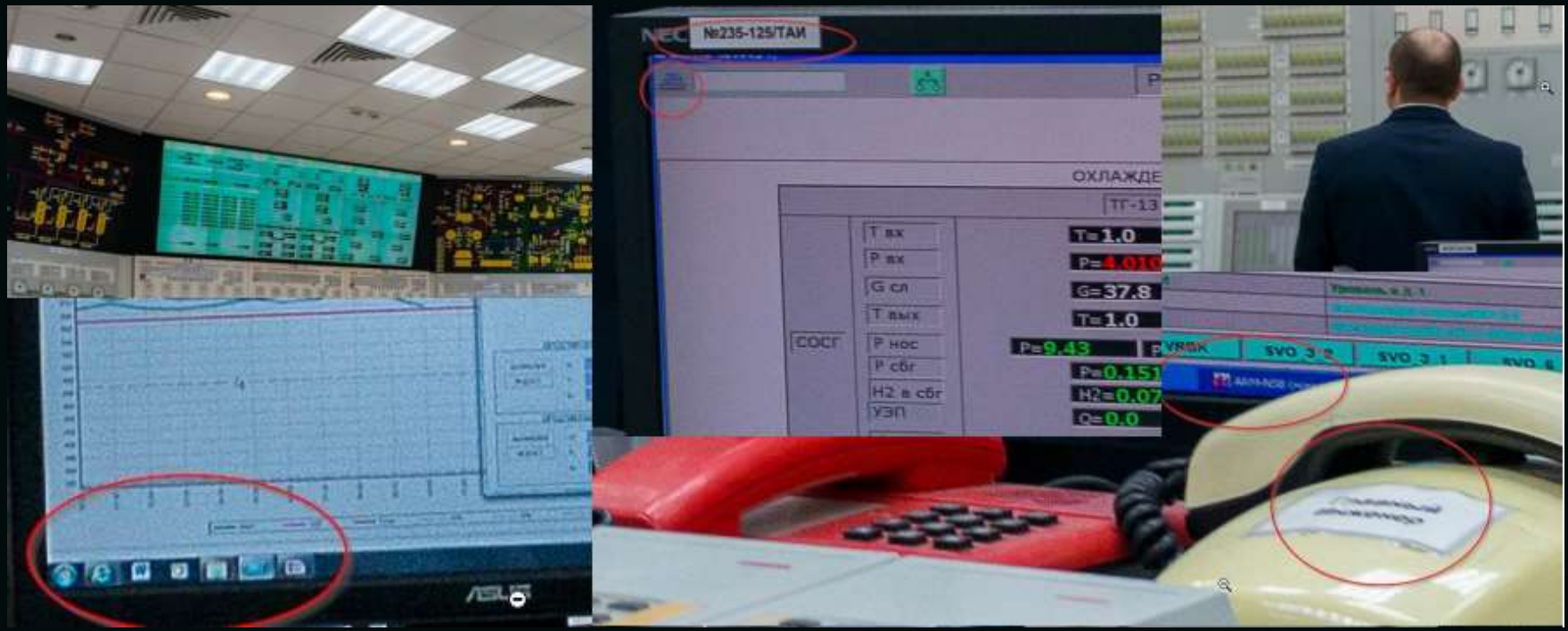
0,5-48 часов	1-4 часа	0,5-6 часов	1-24 часа	0.5-2 часа	ИНЦИДЕНТ
Получение доступа к сети	Сбор информации об АСУ ТП	Подбор пароля ПЛК	Выгрузка и анализ деталей проекта из ПЛК	модификация логики управления	Физический ущерб

VII

ФАКТОРЫ РИСКА

ФАКТОРЫ РИСКА : ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Применение методов социальной инженерии



KASPERSKY lab

ФАКТОРЫ РИСКА : ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Применение методов социальной инженерии

STUXNET:

Информация об элементах критической инфраструктуры была доступна на офиц. сайтах

IR-1 cascade model

RCG	1							2							3							4							5							6						
Line 1			⊕		⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Line 2	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Line 3	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
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

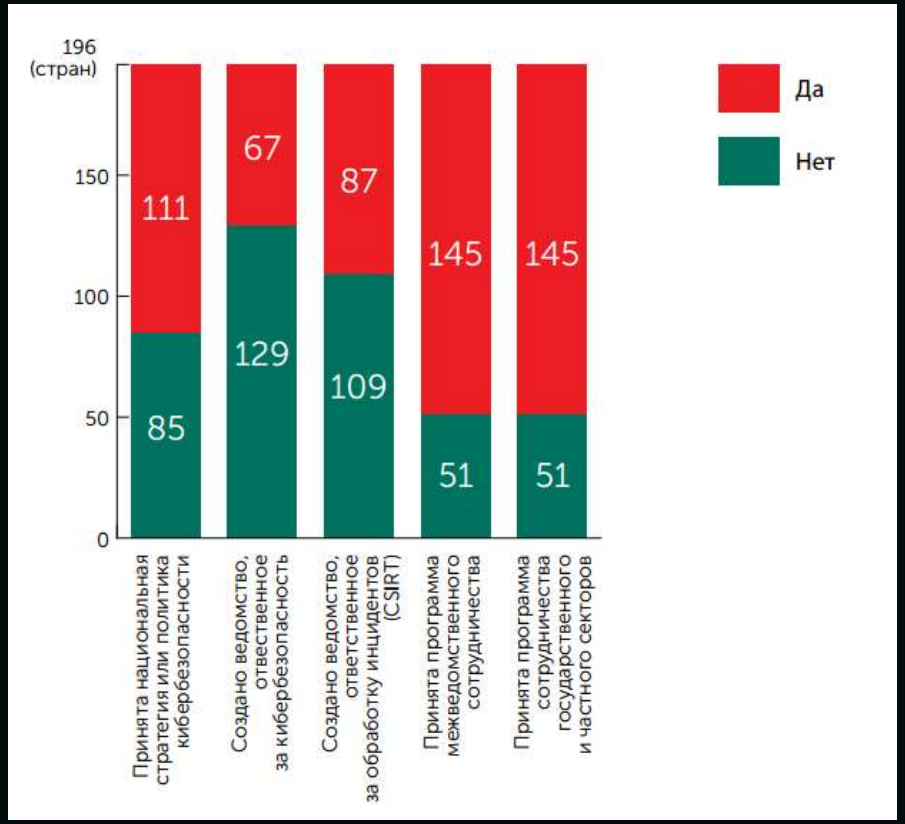
Row: Row number of a centrifuge quadruple, corresponding to the floor markings

VIII

АНАЛИЗ ДЕЯТЕЛЬНОСТИ РЕГУЛЯТОРОВ

Анализ деятельности регуляторов

Индикатор зрелости управления безопасностью КИ на гос. уровне

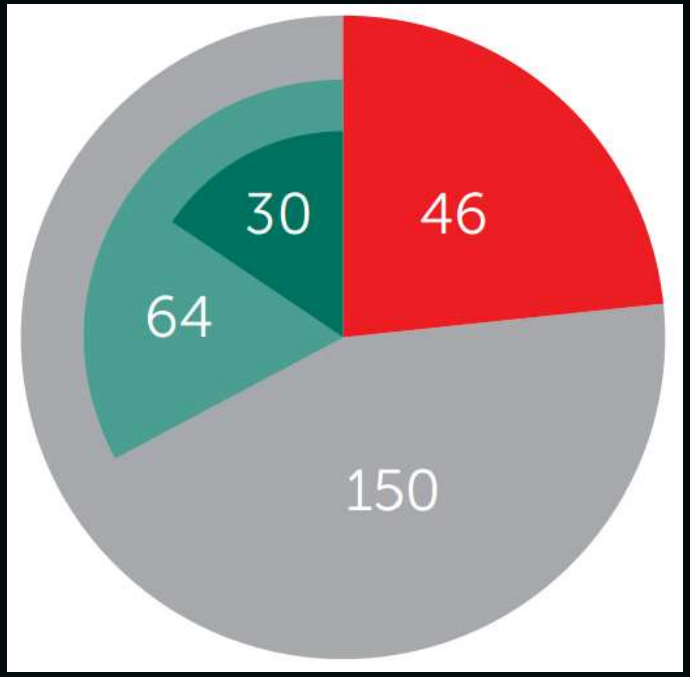


1) Стратегия или политика кибербезопасности
2) Официальное ответственное за кибербезопасность ведомство
3) Официальное ответственное за обработку инцидентов ведомство (CSIRT)
4) Программа межведомственного сотрудничества в области кибербезопасности
5) Программа сотрудничества государственного и частного секторов в области кибербезопасности

По данным https://ics-cert.kaspersky.ru

Анализ деятельности регуляторов

Индикатор зрелости управления безопасностью КИ на гос. уровне



- Страны, в которых отсутствует управление кибербезопасностью на государственном уровне
- Страны, в которых начата деятельность по управлению кибербезопасностью на государственном уровне
- Страны, имеющие ответственное ведомство, csirt и официально принятую стратегию или политику кибербезопасности
- Страны, имеющие ответственное ведомство, csirt и официально принятую стратегию или политику кибербезопасности, а также программы сотрудничества государственных и частных субъектов в сфере кибербезопасности

По данным https://ics-cert.kaspersky.ru

СПАСИБО

evgeny.goncharov@kaspersky.com
Ics-cert@kaspersky.com