ЗАВИДОВО, 2 ИЮНЯ 2016

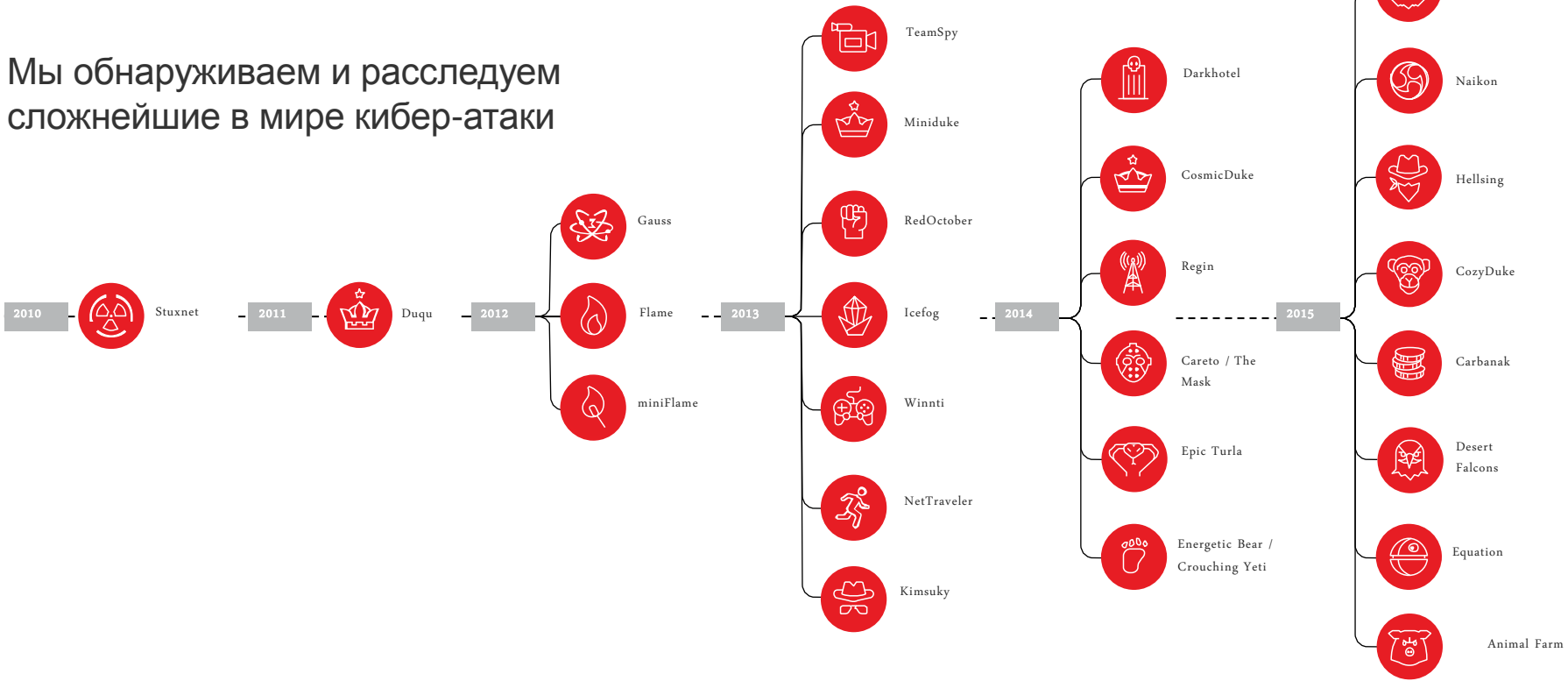
Ландшафт киберугроз в АСУТП

ГЕОРГИЙ ШЕБУЛДАЕВ

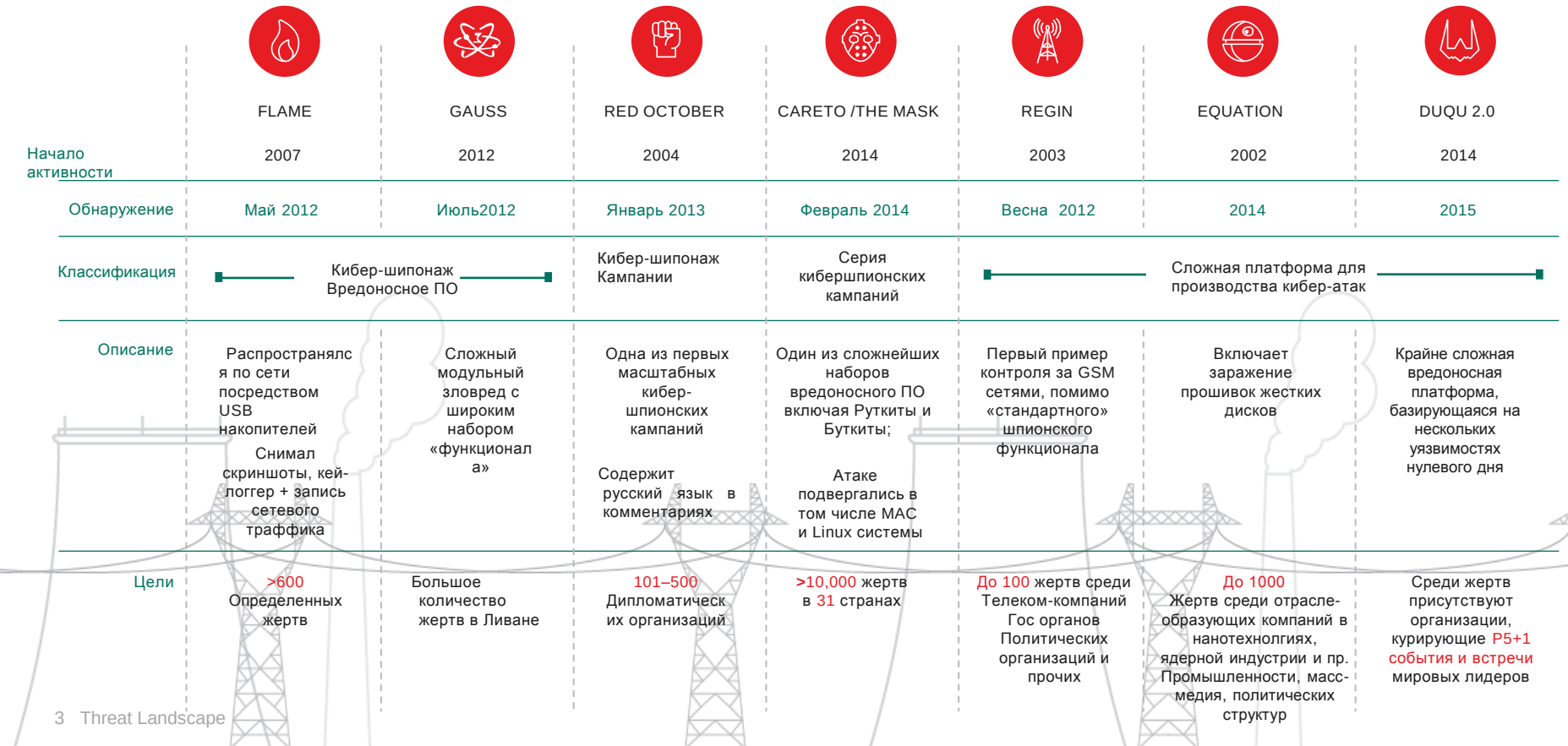
Лаборатория Касперского

ИССЛЕДОВАНИЯ ЛК

Мы обнаруживаем и расследуем сложнейшие в мире кибер-атаки



ЭВОЛЮЦИЯ APT

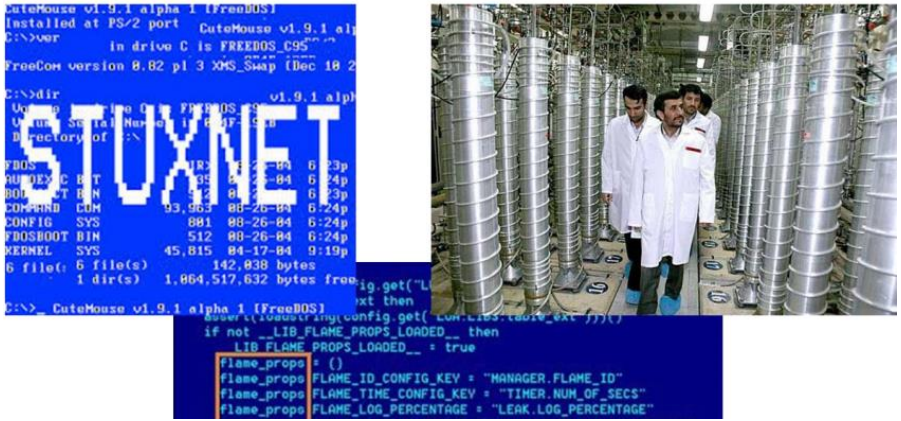


	FLAME	GAUSS	RED OCTOBER	CARETO /THE MASK	REGIN	EQUATION	DUQU 2.0
Начало активности	2007	2012	2004	2014	2003	2002	2014
Обнаружение	Май 2012	Июль2012	Январь 2013	Февраль 2014	Весна 2012	2014	2015
Классификация	Кибер-шпионаж Вредоносное ПО		Кибер-шпионаж Кампании	Серия кибершпионских кампаний	Сложная платформа для производства кибер-атак		
Описание	Распространялся по сети посредством USB накопителей Снимал скриншоты, кей-логгер + запись сетевого траффика	Сложный модульный зловред с широким набором «функционала»	Одна из первых масштабных кибер-шпионских кампаний Содержит русский язык в комментариях	Один из сложнейших наборов вредоносного ПО включая Руткиты и Буткиты; Атаке подвергались в том числе MAC и Linux системы	Первый пример контроля за GSM сетями, помимо «стандартного» шпионского функционала	Включает заражение прошивок жестких дисков	Крайне сложная вредоносная платформа, базирующаяся на нескольких уязвимостях нулевого дня
Цели	>600 Определенных жертв	Большое количество жертв в Ливане	101–500 Дипломатических организаций	>10,000 жертв в 31 странах	До 100 жертв среди Телеком-компаний Гос органов Политических организаций и прочих	До 1000 Жертв среди отрасле-образующих компаний в нанотехнолгиях, ядерной индустрии и пр. Промышленности, масс-медия, политических структур	Среди жертв присутствуют организации, курирующие P5+1 события и встречи мировых лидеров

ИСТОРИЯ ИНЦИДЕНТОВ– 2010, НАЧАЛО

КОГДА: 2010

ГДЕ: ИРАН (+15 СТРАН)



КИБЕР-УРОН: зараженные USB– MS OS уязвимости – обнаружение Win CC – конфигурация S7 PLC

ФИЗИЧЕСКИЙ УРОН: (DB890, FC1865,1874) – вредоносные измения в программу ПЛК, сокращен срок службы центрифуг

ФИНАНСОВЫЙ: 20% ЦЕНТРИФУГ ВЫВЕДЕНЫ ИЗ СТРОЯ РАНЕЕ ПОЛОЖЕННОГО СРОКА

ИСТОРИЯ ИНЦИДЕНТОВ– 2008, СПЕКУЛЯЦИИ?

КОГДА: 2008

ГДЕ: ТУРЦИЯ

КИБЕР-УРОН: отключены системы сигнализация отключена, система видео-наблюдения взломаны, 60 часов записей удалены.

ФИЗИЧЕСКИЙ: взрыв, транспортировка нефти остановлена, разлив >30,000 баррелей нефте-продуктов.

Firemen struggle to extinguish the blaze at the Baku-Tbilisi-Ceyhan (BTC) pipeline near the eastern Turkish city of Erzincan on Aug. 7, 2008

ФИНАНСОВЫЙ: $5M/ДЕНЬ ПОТЕРЬ ДЛЯ BP, ~$1B – ПОТЕРИ МЕСТНОЙ ГОСУДАРСТВЕННОЙ КОМПАНИИ ПО ТРАНСПОРТИРОВКЕ

ИСТОРИЯ ИНЦИДЕНТОВ – 2012, SHAMOON, SAUDI ARAMCO

КОГДА: 2008

ГДЕ: САУДОВСКАЯ АРАВИЯ

КИБЕР-УРОН: фишинговый имейл, 35 000 компьютеров выведены из строя (стерта память)

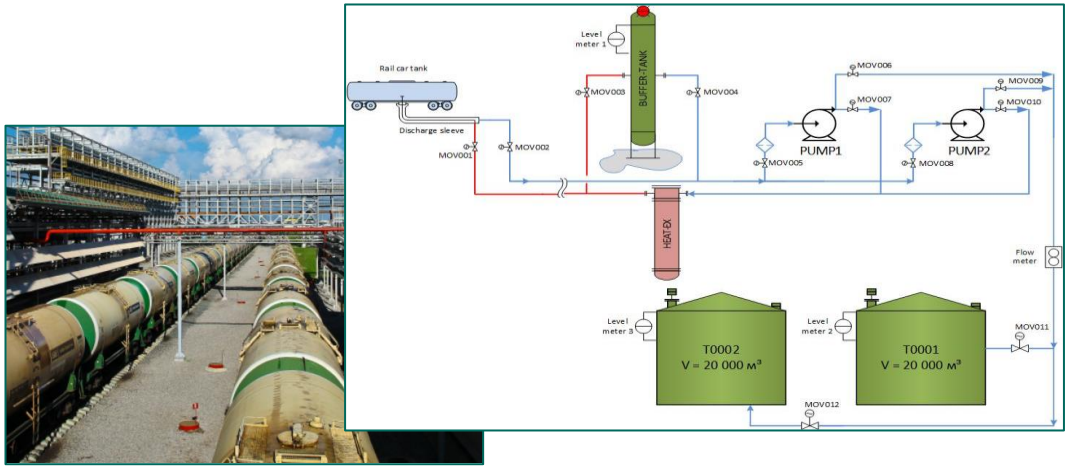
ФИЗИЧЕСКИЙ: остановлена местная отгрузка нефти

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

ФИНАНСОВЫЙ: ПРОСТОЙ – 17 ДНЕЙ, НА 18ЫЙ КОМПАНИЯ НАЧАЛА ОТГРУЗКИ БЕСПЛАТНО

РЕАЛЬНЫ ЛИ РИСКИ? (ИССЛЕДОВАНИЕ ЛК)

- Терминал с нефтяными цистернами, как правило, существует на каждом нефтеперерабатывающем предприятии
- Цель злоумышленника: вызвать аварию на производстве



Последовательность вредоносных действий остается незамеченной, и в результате злоумышленник внедряется в пункт разгрузки

	2-4 часов	2-6 часов	8-24 часов	0.5-2 часов	Авария
Получение доступа к технологической сети	Обнаружение ПЛК	Взлом пароля от ПЛК	Получение и анализ конфигурации ПЛК	Вредоносное изменение логики управления	Уход из системы

РЕАЛЬНЫ ЛИ РИСКИ? (ИССЛЕДОВАНИЕ ЛК)

КОГДА : ОКТЯБРЬ 2015

ГДЕ: МОСКВА

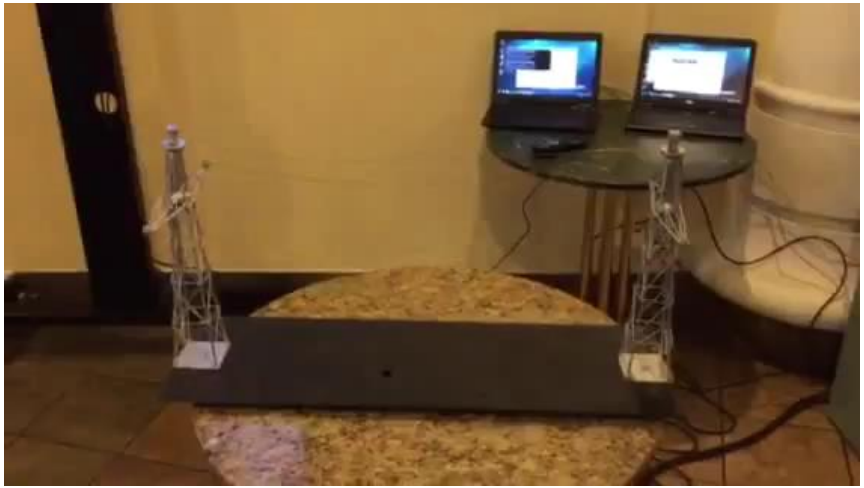
ЦЕЛЬ: Тест на проникновение модели подстанции 500kV

- Реальное оборудование и конфигурация
- Улучшенные настройки безопасности
- 4 команды специалистов ИБ
- Цель – продемонстрировать физический урон.

РЕАЛЬНЫ ЛИ РИСКИ? (ИССЛЕДОВАНИЕ ЛК)

КИБЕР-УРОН: RTU и терминалы защиты атакованы после проникновения в технологический сегмент

- Эксплуатированы множество уязвимостей в протоколе IEC 61850 (MMS/GOOSE) и архитектуре SIEMENS DIGSI.
- РЗА отключено, прошивка терминала изменена, найдены 3 уязвимости 0-дня
- 2 из 8 терминалов выведены из строя (Закирпичены)
- Множественные манипуляции с силовыми ячейками



ФИЗИЧЕСКИЙ УРОН: ПЕРВОЕ КЗ ЧЕРЕЗ 3 ЧАСА, 2 ТЕРМИНАЛА ВЫВЕДЕНЫ ИЗ СТРОЯ

УГРОЗЫ СЕГОДЯ. ДЕКАБРЬ 2015

Как исследования коррелируют с реальной жизнью

КОГДА: ДЕКАБРЬ 2015

ГДЕ: УКРАИНА

КИБЕР-УРОН: Заражение BlackEnergy2 посредством фишингового имейла, Прошивки RTU изменены, диспетчерские ПК атакованы и «затерты», DDoS атака на колл-центры.


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 УРОН:, удаленное уравление операторами выведено из строя, отключение напряжения на7 110kV и 23 35 kV подстанциях

ФИНАНСОВЫЙ: ОТКЛЮЧЕНИЕ ЭКЛЕКТРОЭНЕРГИИ В 5 РЕГИОНАХ НА 6 HOURS

ТЕКУЩАЯ СИТУАЦИЯ В БЕЗОПАСНОСТИ АСУТП

Растущий тренд — количество инцидентов растет (ICS-CERT)

FY 2014

245

Инцидентов

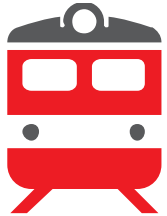
FY 2015

295

Инцидентов

59%

Нефтегаз, Генерация (Hydro, Nuclear), КВО



25%

Транспорт и коммуникации

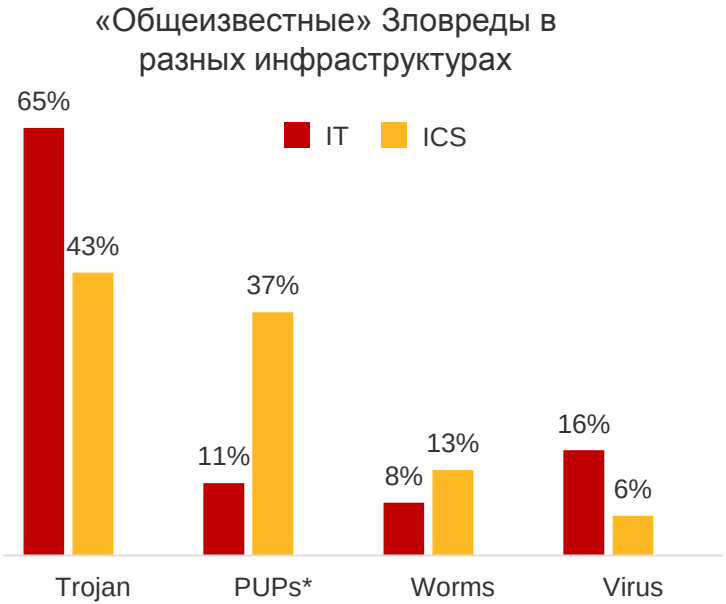
ЦЕЛЬ — ПОЛУЧИТЬ ДОСТУП К SCADA СИСТЕМАМ, ПЛК И НАНЕСТИ ВРЕД ТЕХ ПРОЦЕССУ

KASPERSKY lab

ВРЕМЯ ПРОСТОЯ

Source: RISI Annual Summary 2013

ЧТОБЫ СТАТЬ ЖЕРТВОЙ – НЕ НУЖНО БЫТЬ ЦЕЛЬЮ



Стандартное вредоносное ПО

- Citadel, Kido, Shamoon, итд.

Таргетированные Атаки (APTs)

- Duqu, Flame, Gauss, Crouching Yeti (Energetic Bear), Epic Turla, Equation

Кибероружие

- Stuxnet

** **PUPs** — Potentially unwanted programs*
*** Source: Kaspersky Security Network*

KASPERSKY lab

ЧТОБЫ СТАТЬ ЖЕРТВОЙ – НЕ НУЖНО БЫТЬ ЦЕЛЬЮ

Цепочка доставки: Crouching Yeti / Energetic Bear

Запущена in 2010. Более 2800 жертв по миру

Watering hole: скомпрометированы отраслевые ресурсы:
gse.com.ge, gamyba.le.lt, chariotoilandgas.com, longreachoilandgas.com, vitogaz.com…

Зловреды инжектированы в пакеты обновлений SCADA ПО:
eWon, MB Connect Lone GmbH, MESA Imaging…

250 скачиваний зараженных пакетов **от производителя SCADA**

Критическая инфраструктура была использована для проникновения в корпоративную

АДАПТАЦИЯ «ФИНАНСОВОГО» БОТНЕТА

Citadel: зловред для банков нацелен на индустриальные системы

КОГДА: **2014**
ГДЕ: Ближний Восток
Кибер-урон:
Citadel модифицирован
Для атаки нефте-химического производства

The New York Times

Bits

SUBSCRIBE | LOG IN

Middle Eastern Petrochemical Plants Are Targets of Hackers

By NICOLE PERLROTH
SEPTEMBER 15, 2014

SAN FRANCISCO — Security researchers at IBM said they had uncovered a series of hacking attacks aimed at Middle Eastern petrochemical companies.

The researchers, at IBM's Trusteer division, said the hackers were using a variant of financial malware known as Citadel, which was first discovered in 2012.

Citadel was originally engineered to steal victims' banking credentials by capturing their keystrokes and taking computer screenshots. But the researchers said that hackers targeting petrochemical companies have altered Citadel to add more functions: to take complete control over a victim's PC and allow hackers to gain access to a victim's corporate network. They have also made modifications in the malware to evade antivirus products and traditional security controls.

КИБЕРШПИОНАЖ: EQUATION

APT нацеленная на множество индустриальных компаний

КОГДА: **2001 – 2015**

Масштаб: всемирный

national nuclear center
railways / metro development company
aerospace / automotive supplier
national airports
plasma research organization
national oil company
national engineering / scientific commission
national space agencies
power generation / distribution

KASPERSKY

УЯЗВИМОСТИ: ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Что такое Watering hole

Эксплуатация ЧЕЛОВЕЧЕСКОГО ФАКТОРА

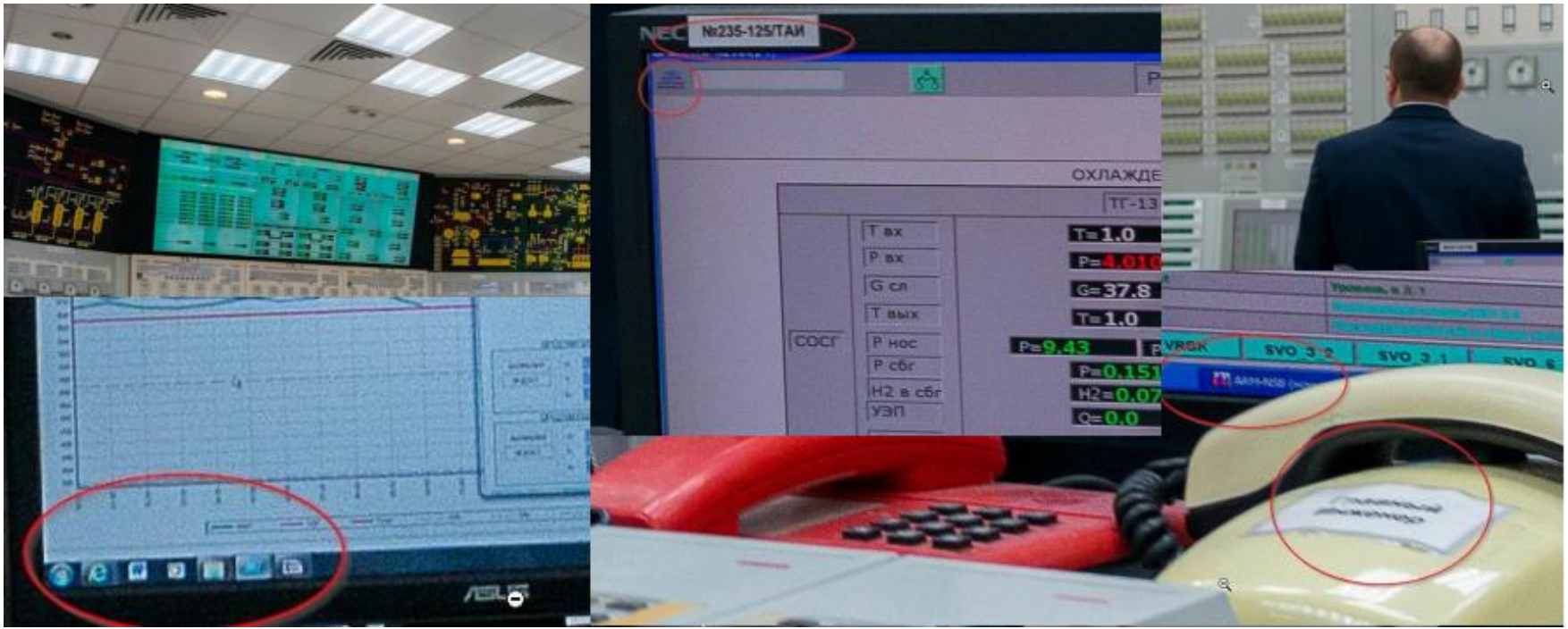
Множество жертв одновременно включая тех, кого не было в «целевом списке»

Преодолевает сегментацию

Применимо в АСУТП

УЯЗВИМОСТИ: ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Социальная инженерия



KASPERSKY lab

УЯЗВИМОСТИ: ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Социальная инженерия

STUXNET:

Информация об схеме каскада центрифуг могла быть получена с официального сайта компании

IR-1 cascade model

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

УЯЗВИМОСТИ: ПО И ПТК АСУТП

Уязвимости ПТК

Alert (ICS-ALERT-15-225-02A)

Rockwell Automation 1766-L32 Series Vulnerability (Update A)

Original release date: August 13, 2015 | Last revised: August 20, 2015

Alert (ICS-ALERT-15-225-01A) More Alerts

Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A)

Original release date: August 13, 2015 | Last revised: August 20, 2015

Alert (ICS-ALERT-15-225-01A) More Alerts

Rockwell Automation 1769-L18ER and A LOGIX5318ER Vulnerability (Update A)

Original release date: August 13, 2015 | Last revised: August 20, 2015

Source: US ICS-CERT

Удаленный злоумышленник может получить доступ к ПЛК

УЯЗВИМОСТИ: УДАЛЕННЫЙ ДОСТУП

Коммунальная компания скомпрометирована – Слабый пароль

В 2014, неназванная публичная производственная компания подверглась удаленной кибератаке в результате которой был получен доступ к технологической инфраструктуре

ПО, используемое организацией для организации удаленного обслуживания было доступно через интернет.

Эти системы включали remote access ПО со слабыми паролями.

Системы были подтвержены множественным векторам атак. Предыдущие вторжения также были обнаружены.

Производители АСУ настаивают на настройке уданенного доступа/управления к их оборудованию

УЯЗВИМОСТИ: АРЕНДОВАННЫЕ КАНАЛЫ

Региональная электросетевая компания

Многие критические объекты – распределенные инфраструктуры / (Иногда принадлежат разным компаниям)

ПРОБЛЕМА: не возможно или экономически нецелесообразно строить собственные каналы связи

РЕШЕНИЕ: Используются каналы от провайдеров

ИНЦИДЕНТ:

- Потеряна связь между двумя подстанциями
- Расследование показало, что один из маршрутизаторов был размещен в жилом здании
- **Роутер был использован обычными жильцами, в том числе и нелигитимно**

УЯЗВИМОСТИ: СЛАБЫЕ РЕГЛАМЕНТЫ

Расширенная поверхность атаки

СЦЕНАРИЙ 1: ПО «серой зоны»

- Оператор SCADA системы должен переавторизовываться 20 раз в сутки.
- Персонал устанавливает Websurf, чтобы «заглушить» функцию блокировки ПК

ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ:

- Свободный доступ для кого угодно

СЦЕНАРИЙ 2: Файло-обменники

- Использование внутренних и внешних файловых шар для организации информационного обмена с корпоративной сетью (в т ч Dropbox)

ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ:

- Открытие легкого вектора проникновения в технологическую сеть

KASPERSKY lab

ЧТО ЗАТРУДНЯЕТ ОБЕСПЕЧЕНИЕ ИБ СЕГОДНЯ?

- **Недостаточная осведомленность, смесь слухов и реальности, недостаток данных**

- **Информационные системы в промышленности:**
  - Старые
  - Незащищенные
  - С трудом поддаются обновлению

- **Типовые «офисные» средства ИБ не подходят**

- **Недостаток навыков ИБ, и обще-принятой практики ИБ АСУ ТП**
- **Отчуствие четко определенных ответственных за процесс обеспечения ИБ АСУТП**

ARE WE READY TO DEFEND?

KASPERSKY lab