Stuxnet: как, зачем и почему?

Александр Матросов

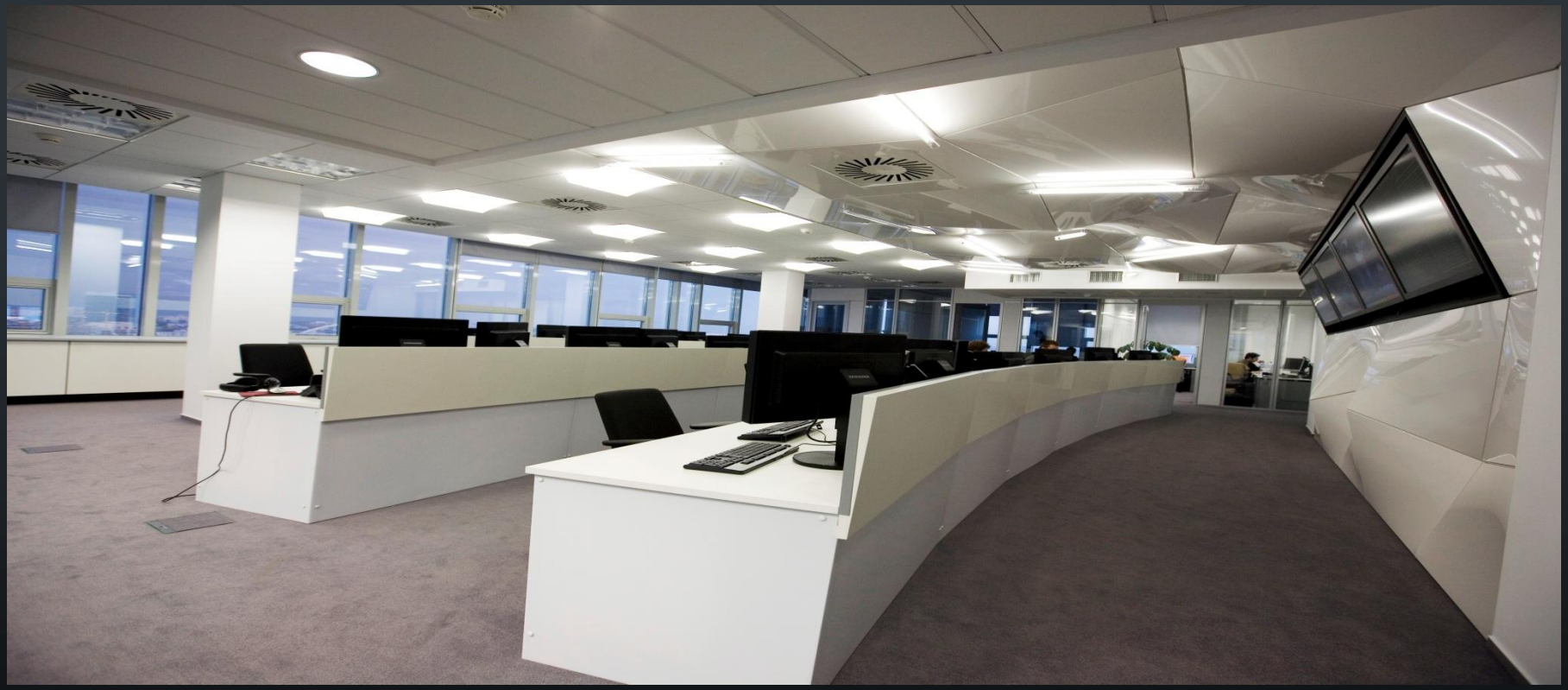
руководитель центра вирусных исследований и аналитики

Пара слов о вирусной лаборатории

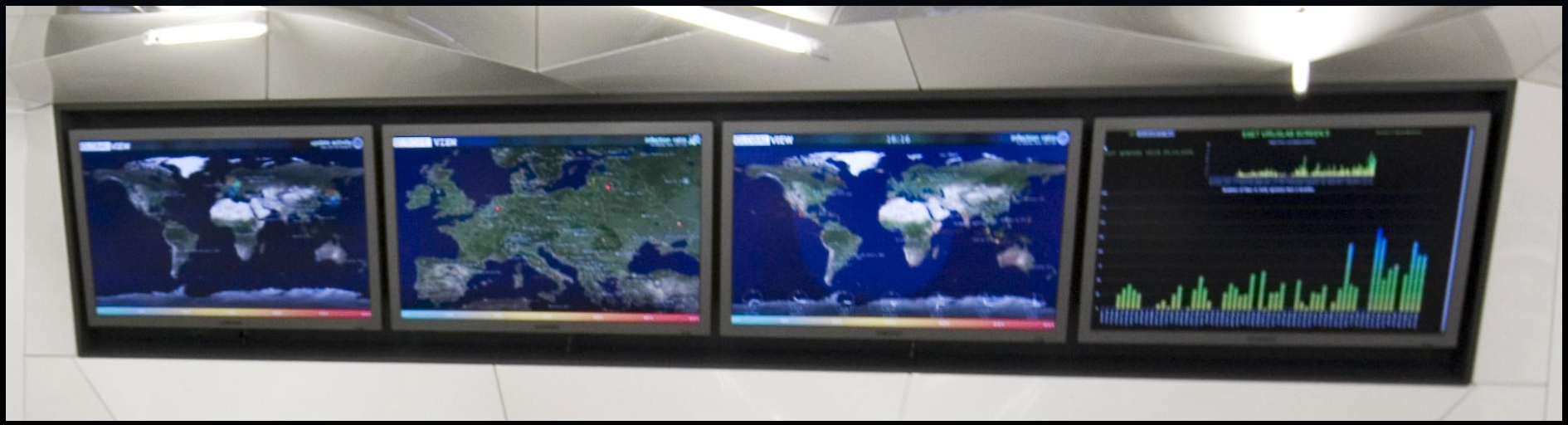
более **300,000** уникальных сэмплов ежедневно

ThreatSense.Net technology

ESET




Threat
Lab

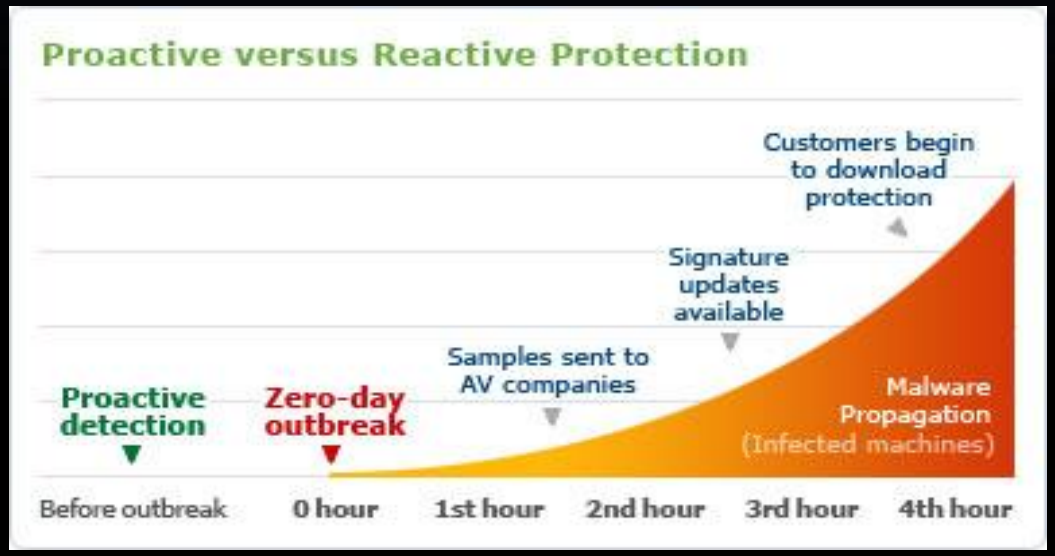


ThreatSense.Net technology

eset

ThreatSense.Net technology

ThreatSense technology



eset

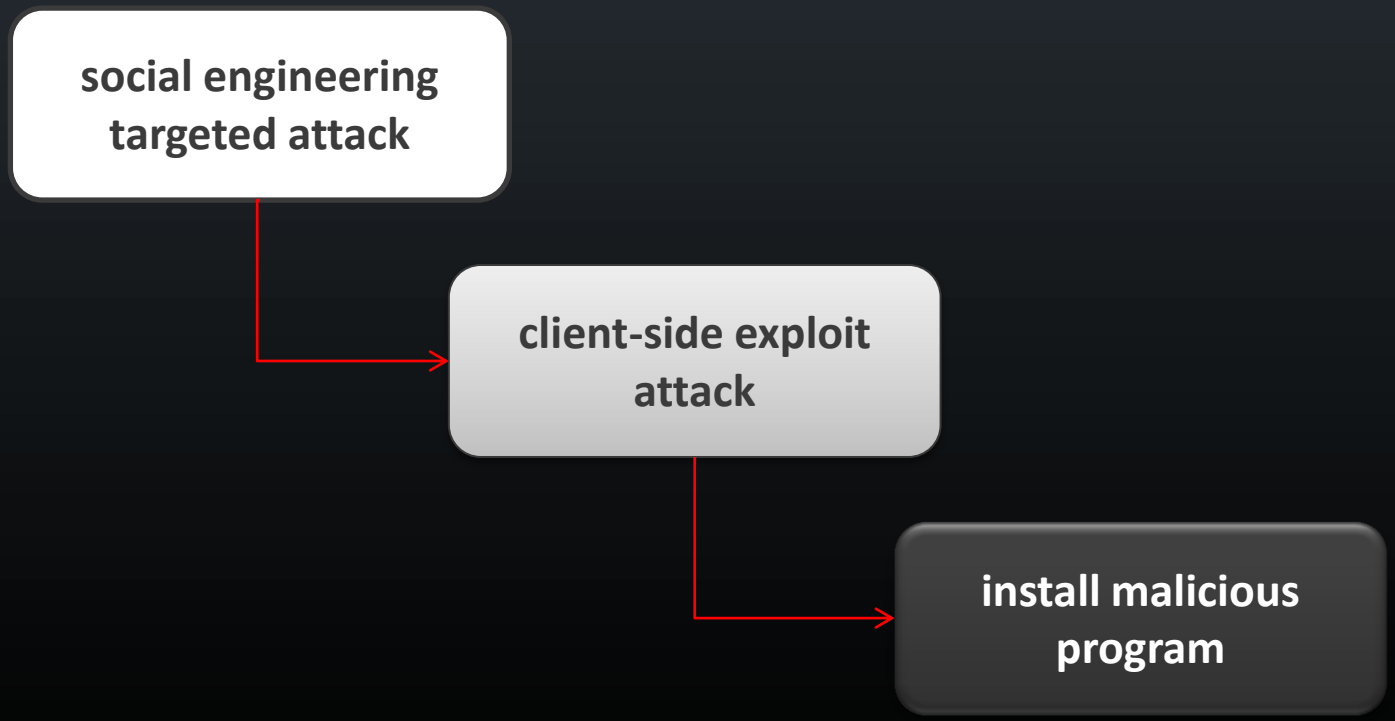
План доклада

- Целевые атаки
- Червь Stuxnet – развитие атаки
- Проблемы обратного анализа больших программ
- Готова ли Россия к кибервойне?
- Что будет дальше?

Целевые атаки

Классификация целевых атак

Типичный сценарий целенаправленной атаки



Целевой обход защитных средств

Червь Stuxnet – развитие атаки

Чем же так интересен Stuxnet?

Внедрение кода в SCADA системы

- Возможность влиять на промышленные процессы
- Нельзя не учесть возможность изменения целей

До сих пор неясны цели и мотив атаки

- Версий много, но единого мнения нет
- Все имеющиеся улики только косвенные

Легальная цифровая подпись

- Realtek Semiconductor Corps
- JMicron Technology Corp

Огромное кол-во векторов атаки

- 5 уязвимостей нулевого дня!
- Дополнительные пути распространения

Код самого червя

- Используется продуманная ООП архитектура
- Код реализован на очень высоком уровне

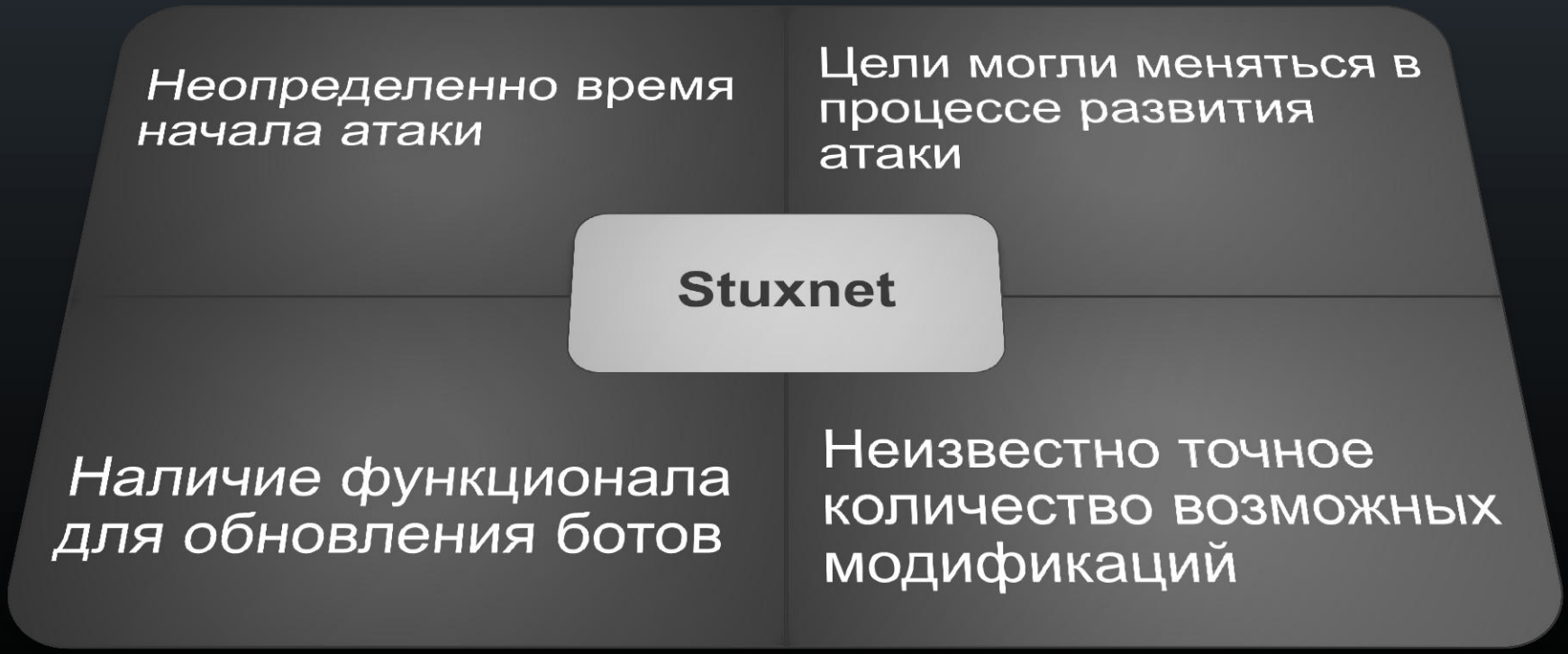
eset

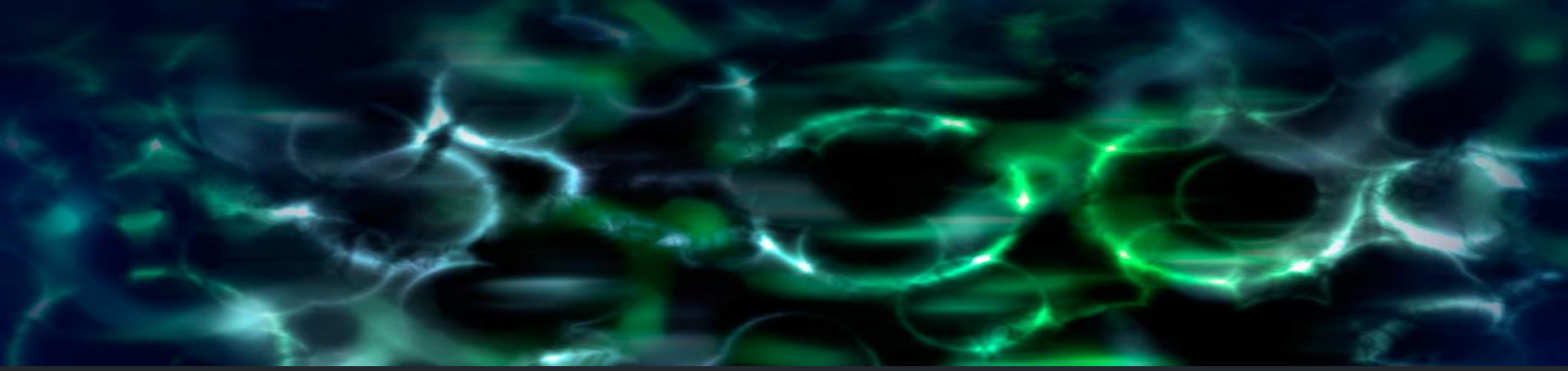
Развитие атаки Stuxnet во времени

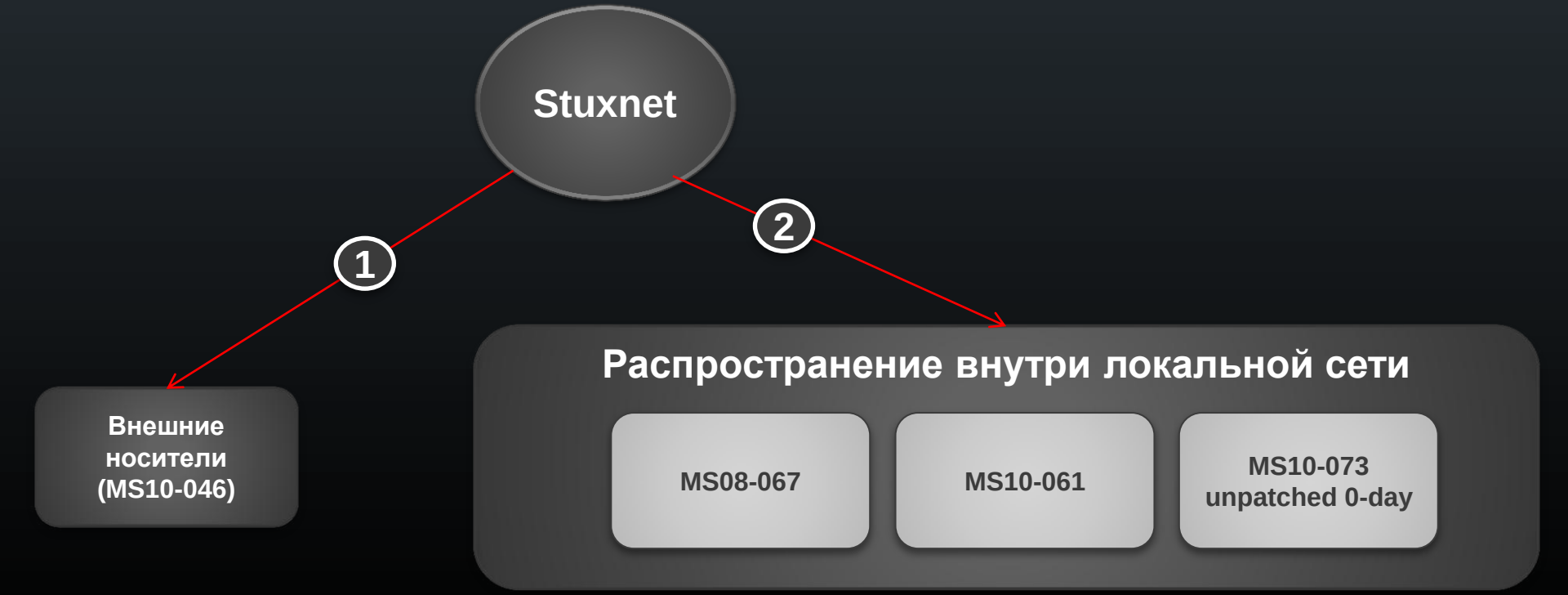
Январь 2010	Июнь 2010	Июль 2010	Июль 2010	Август 2010	-> 2010
Stuxnet driver signed with a valid Realtek certificate		MS Security Advisory for LNK/PIF vulnerability	Stuxnet driver signed with a valid JMicron certificate	MS10-046	MS10-061 MS10-073

Iran	Indonesia	India	Pakistan	Uzbekistan	Russia	Kazakhstan	Belarus
52,2%	17,4%	11,3%	3,6%	2,6%	2,1%	1,3%	1,1%
Kyrgyzstan	**Azerbaijan**	**United States**	**Cuba**	**Tajikistan**	**Afghanistan**	**Rest of the world**	
1,0%	0,7%	0,6%	0,6%	0,5%	0,3%	4,6%	

Почему нельзя делать однозначных выводов?






Stuxnet
1
2
Внешние носители (MS10-046)
Распространение внутри локальной сети
MS08-067
MS10-061
MS10-073 unpatched 0-day

Stuxnet Under the Microscope

Более детальный анализ в нашем аналитическом отчете:

«**Stuxnet Under the Microscope**»

Aleksandr Matrosov, Senior Virus Researcher

Eugene Rodionov, Rootkit Analyst

David Harley, Senior Research Fellow

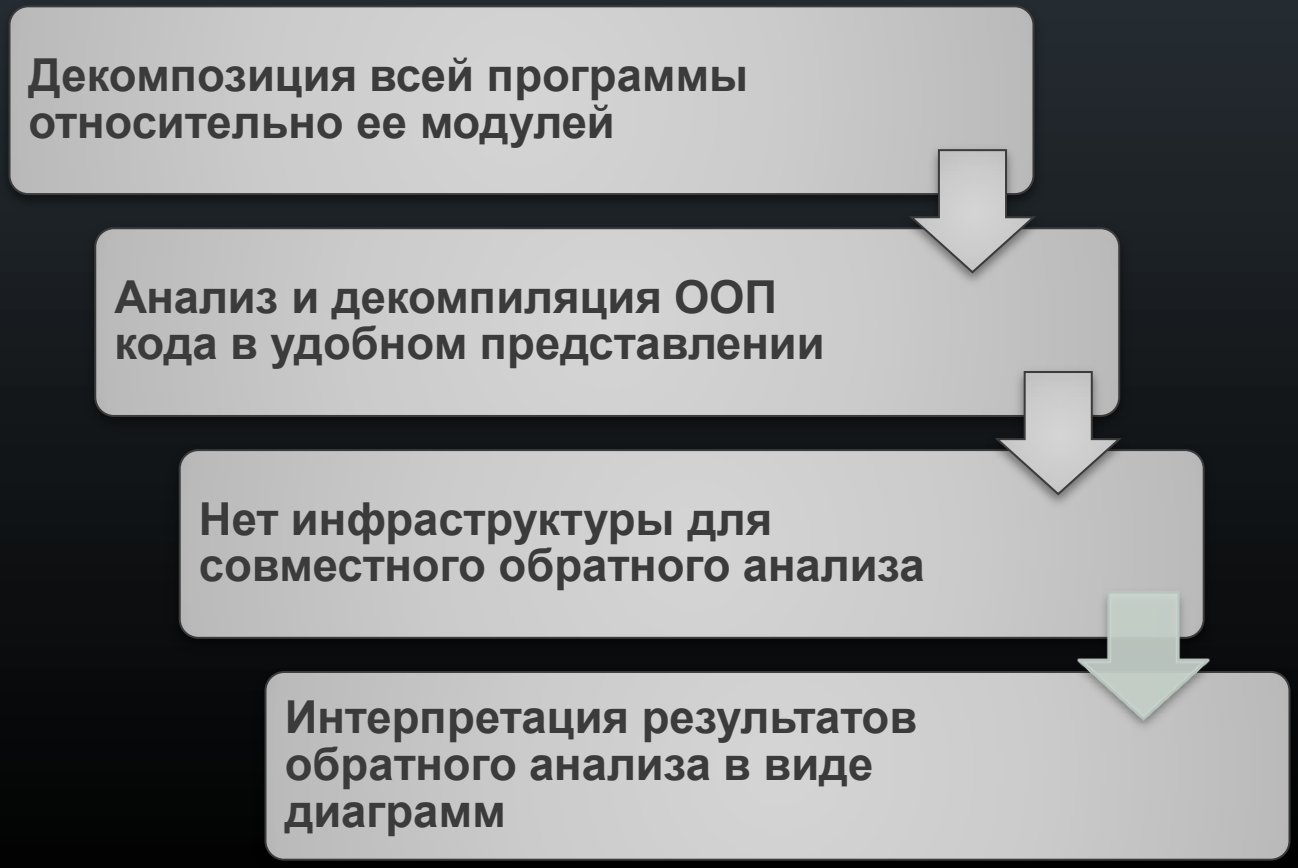
Juraj Malcho, Head of Virus Laboratory

Revision 1.1

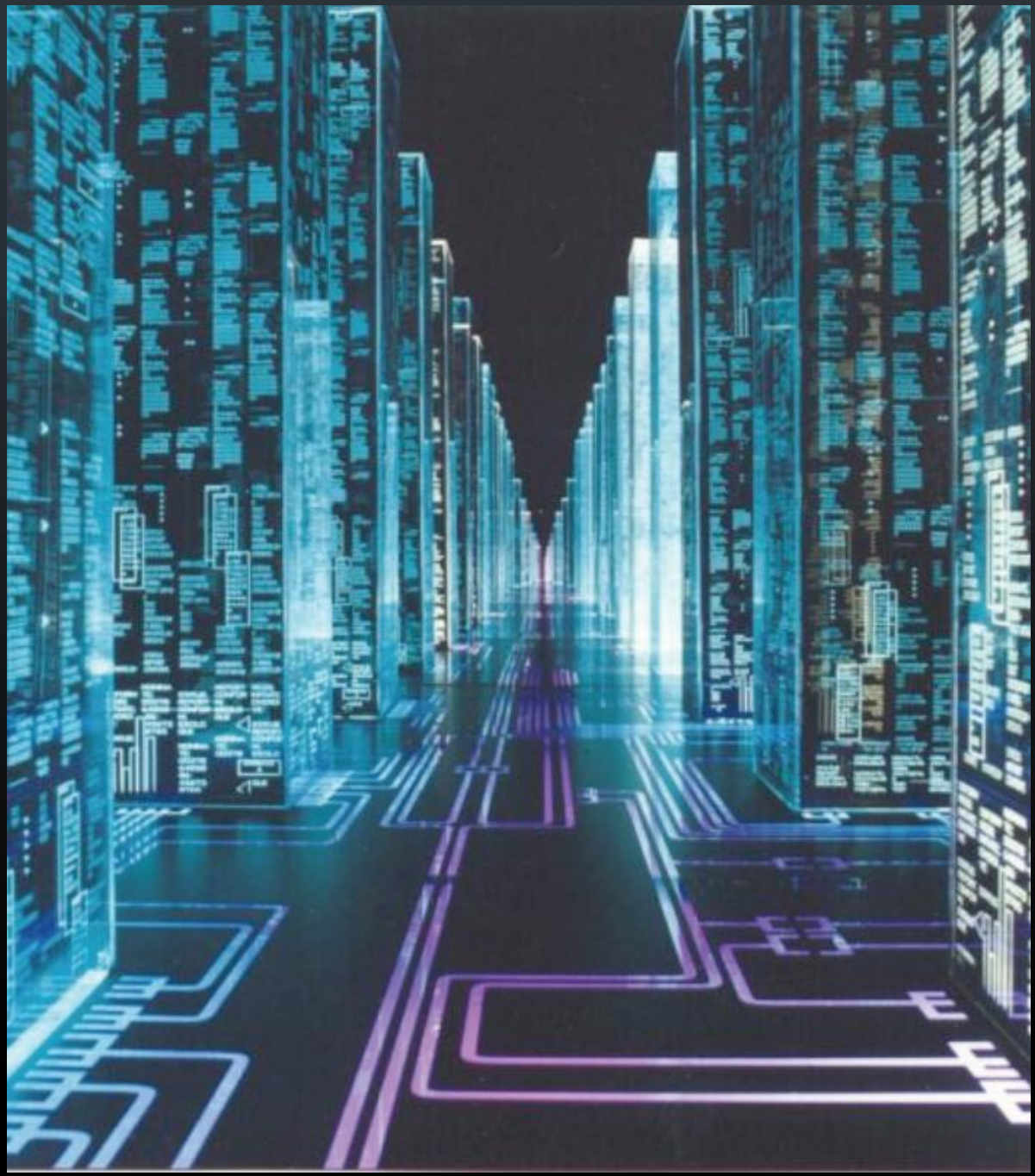
http://www.eset.ru/.company/.viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf

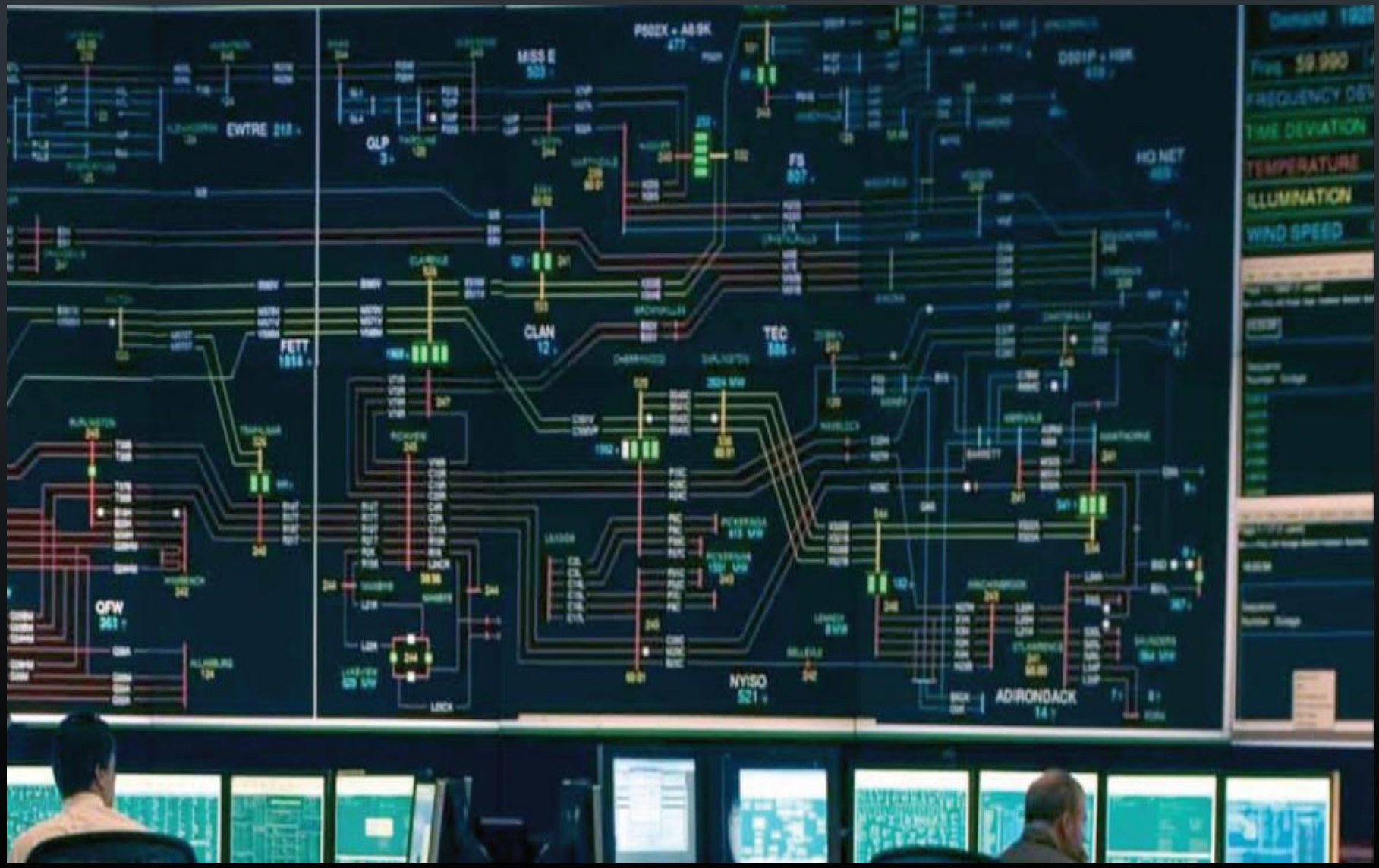
Проблемы обратного анализа больших программ

Чего не хватает прямо сейчас?



Готова ли Россия к кибервойне?




EWTRE
GLP
MSS E
FETT
CLAN
FS
TEC
HQ NET
NYISO
ADIRONDACK
OFW
TIME DEVIATION
TEMPERATURE
ILLUMINATION
WIND SPEED

Как создать киберармию и атаковать Россию

Чарльз Миллер — один из самых знаменитых американских экспертов по кибербезопасности. До недавнего времени он пять лет работал в наиболее секретной спецслужбе США — Агентстве национальной безопасности. Сотрудники этого ведомства стали прообразом «Людей в черном», а его аббревиатура NSA в шутку расшифровывается как No Such Agency — «нет такого агентства». Миллер также является одним из лучших американских хакеров. Ему удалось первым обнаружить уязвимость в MacBook Air и за две минуты написать для нее вредоносный код. Чтобы взломать браузер Safari, Миллеру потребовалось десять секунд, столько же ушло на выявление дефекта в системе SMS-сообщений с iPhone. Месяц назад он представил в Центре кибербезопасности НАТО доклад «Как создать киберармию и атаковать США». Специально для «Русского Newsweek» он подготовил отчет и по России.

Российский сценарий

Численность киберармии: 517 человек
Стоимость: $86 млн
Сроки подготовки: 2 года

КИБЕРВОИНЫ:

Коллекторы ботов

Обязанности: заражение чужого компьютера эксплойтами (например, с помощью спама, рекламных баннеров или вредоносных программ) для превращения его в бот. Используют как уже известные эксплойты, так и zero day эксплойты.

40 дипломированных специалистов — зарплата – $75 000 в год
10 студентов факультетов информатики — зарплата – $40 000 в год

Агентура

Обязанности: поступление на работу в ключевые гражданские и военные учреждения и коммерческие организации, подготовка условий для атаки изнутри посредством получения доступа к закрытым системам и подключения их к интернету с помощью беспроводного оборудования.

10 опытных завербованных агентов — зарплата по договоренности
10 студентов факультетов информатики — зарплата – $40 000 в год

Разработчики

Обязанности: создание средств дистанционного контроля зараженных компьютеров, подготовка DDoS-атак.

20 дипломированных специалистов — зарплата – $60 000 в год
10 опытных специалистов — зарплата – $125 000 в год
10 студентов факультетов информатики — зарплата – $40 000 в год

Специалисты по уязвимостям

Обязанности: поиск известных дефектов безопасности и ранее неизвестных уязвимых мест в операционных системах, программах, браузерах, серверах, сетях, смартфонах.

10 экспертов мирового класса — зарплата – $250 000 в год
10 студентов факультетов информатики — зарплата – $40 000 в год

Разработчики эксплойтов

Обязанности: создание зловредных программ или кодов, которые эксплуатируют уязвимости для заражения компьютера.

10 экспертов мирового класса — зарплата – $250 000 в год
40 разработчиков с опытом использования Metasploit — зарплата – $100 000 в год
20 студентов факультетов информатики — зарплата – $45 000 в год

Специалисты по поддержке ботнетов

Обязанности: поддержка и управление сети зараженных компьютеров-зомби как внутри, так и вне атакуемой страны, мониторинг рынка антивирусных программ.

150 дипломированных специалистов — зарплата – $60 000 в год
20 студентов факультетов информатики — зарплата – $45 000 в год

Операторы

Обязанности: проникновение через установленное внедренными агентами оборудование в закрытые системы, изучение и взлом закрытых систем, проникновение в сложные цели.

40 специалистов по взлому систем — зарплата – $100 000 в год
10 студентов факультетов информатики — зарплата – $40 000 в год

Тестеры

Обязанности: проверка надежности и эффективности всех разработанных программ, ботнетов и средств дистанционного контроля.

10 дипломированных специалистов — зарплата – $60 000 в год
5 студентов факультетов информатики — зарплата – $40 000 в год

Техобеспечение

Оборудование

– в среднем два компьютера на человека
– отдельная тестовая лаборатория с 50 компьютерами
– смартфоны, роутеры и прочее сетевое оборудование

Программное обеспечение

– подписка на MSDN (библиотека официальной документации Microsoft для разработчиков), IDA Pro (программа, анализирующая вирусы и защитные системы), Hex Rays (используется для анализа программного кода), Core Impact (тестирует эксплойты) и др.

Удаленные серверы

«Можно просто использовать чужие», – Миллер

Административно-технический персонал

20 технических консультантов ($100 000 в год) – эксперты по специализированному оборудованию и программному обеспечению, например, медицинскому, авиационному и др.

10 системных администраторов ($50 000 в год) поддерживают работоспособность систем, устанавливают программное обеспечение, в том числе клиентское.

5 старших менеджеров ($200 000 в год) из расчета один старший менеджер на 10 менеджеров.

47 менеджеров ($100 000 в год) из расчета 1 менеджер на 10 киберсолдат. Поддерживают коммуникации между подразделениями, занимаются логистикой.

СТАДИИ ПОДГОТОВКИ:

Первые три месяца

– Специалисты по уязвимостям начинают поиск известных брешей в безопасности
– Разработчики эксплойтов пишут и отлаживают вредоносные программы
– Разработчики пишут программы удаленного контроля
– Поиск и идентификация сложных целей
– Агенты устраиваются на работу в учреждения с закрытыми системами: например, в администрацию президента или аппарат правительства, ключевые министерства, крупнейшие банки, нефтегазовые корпорации, объекты инфраструктуры

3-6 месяцев

– Специалисты по уязвимостям начинают поиск ранее неизвестных уязвимостей
– Разработка zero day эксплойтов
– Начинается заражение компьютеров для создания ботнетов
– Продолжается разработка сложных целей и закрытых систем

6-9 месяцев

– Начинается вторжение в сложные цели и закрытые системы
– Продолжается заражение компьютеров (на этом этапе в сети должно быть не менее 500 000 компьютеров-зомби)

После 1 года

– Продолжается вторжение в сложные цели и закрытые системы, поддержка доступа к уже взломанным сложным целям и закрытым системам
– Продолжается заражение компьютеров (в сети не менее 5 млн компьютеров-зомби)
– Zero day эксплойты разработаны для многих браузеров и операционных систем

1,5 года

– Большинство сложных целей и часть закрытых систем взломаны и заражены
– Продолжается заражение компьютеров (в сети не менее 100 млн компьютеров-зомби в атакуемой стране и за ее пределами)
– Zero day эксплойты доступны для всех браузеров, операционных систем

2 года

– Большинство сложных целей и часть закрытых систем доступны для дистанционного контроля
– В сети до 100–500 млн ботов (в том числе и 20% персональных компьютеров в атакуемой стране), много зараженных смартфонов

АТАКА

Нарушена работа систем управления гражданских и военных служб

Полное отключение электричества или перебои в электроснабжении

Хаос в системах контроля над воздушным и железнодорожным транспортом

Сотовая связь отключена или работает со значительными перебоями

Интернет не работает

Нарушена передача финансовых данных (банковских переводов, электронных платежей и т. д.), работа биржи и банков

Страна парализована

СЛОВАРЬ

Уязвимость – ошибка или дефект безопасности в программе, веб-приложении или операционной системе

Эксплойт – программа или фрагмент вредоносного программного кода, использующая уязвимость в программном обеспечении для проникновения в систему в обход антивирусного обеспечения

Metasploit – программный пакет для проведения тестов эксплойтов, используемый как специалистами по безопасности, так и хакерами

Бот или зомби-компьютер – машина в сети, зараженная бот-программой и используемая без ведома владельца

Zero day эксплойты – эксплойты, использующие недавно появившиеся уязвимости в операционных системах или программах, еще неизвестные их разработчикам

Ботнет – компьютерная сеть ботов. Используется, например, для проведения DDoS-атаки или распространения спама

DDoS-атака – организация большого количества ложных запросов от ботов на серверы или сайты с целью вывода их из строя

Закрытая система – внутренняя локальная сеть организации, содержащая важные или секретные документы, или сеть служебных компьютеров, управляющих техническими системами, которые не имеют выхода в интернет

Сложные цели (hard targets) – хорошо защищенные важнейшие цели хакерской атаки. Например, телекоммуникационные корпорации, банковские и финансовые службы, системы управления воздушным движением

Комментарии российских экспертов к сценарию Чарльза Миллера читайте на сайте runewsweek.ru

Европейский сценарий:

Численность киберармии: 750 человек
Стоимость: $ 112 млн.
Сроки подготовки: 2 года

Американский сценарий:

Численность киберармии: 592 человека
Стоимость: $ 98 млн.
Сроки подготовки: 2 года

http://www.runewsweek.ru/article/v-mire/24631-kak-sozdat-kiberarmiyu-i-atakovat-rossiyu

Что будет дальше?

100% Virus Free Podcast

Еженедельный подкаст о компьютерной безопасности и не только

http://www.eset.ru/.company/podcast/

http://twitter.com/virlab

eset

Спасибо за внимание ;)

Александр Матросов

http://twitter.com/matrosov

http://amatrosov.blogspot.com/