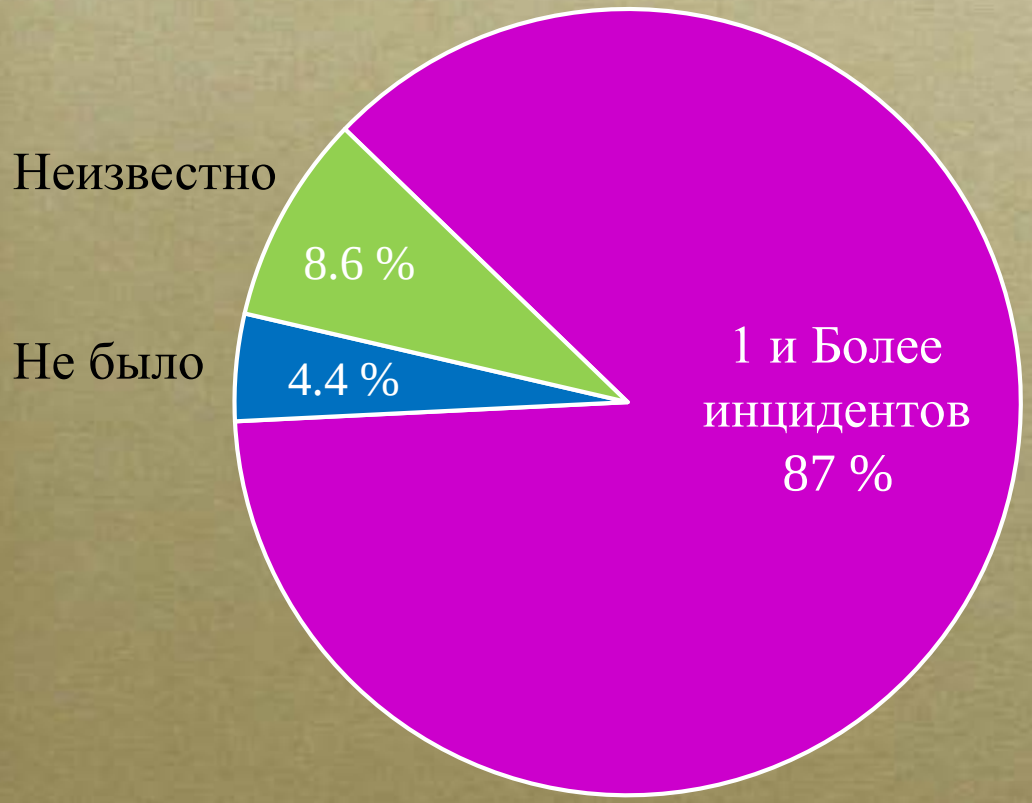
2BSecure Incident Response Team

2Bsecure@matrix

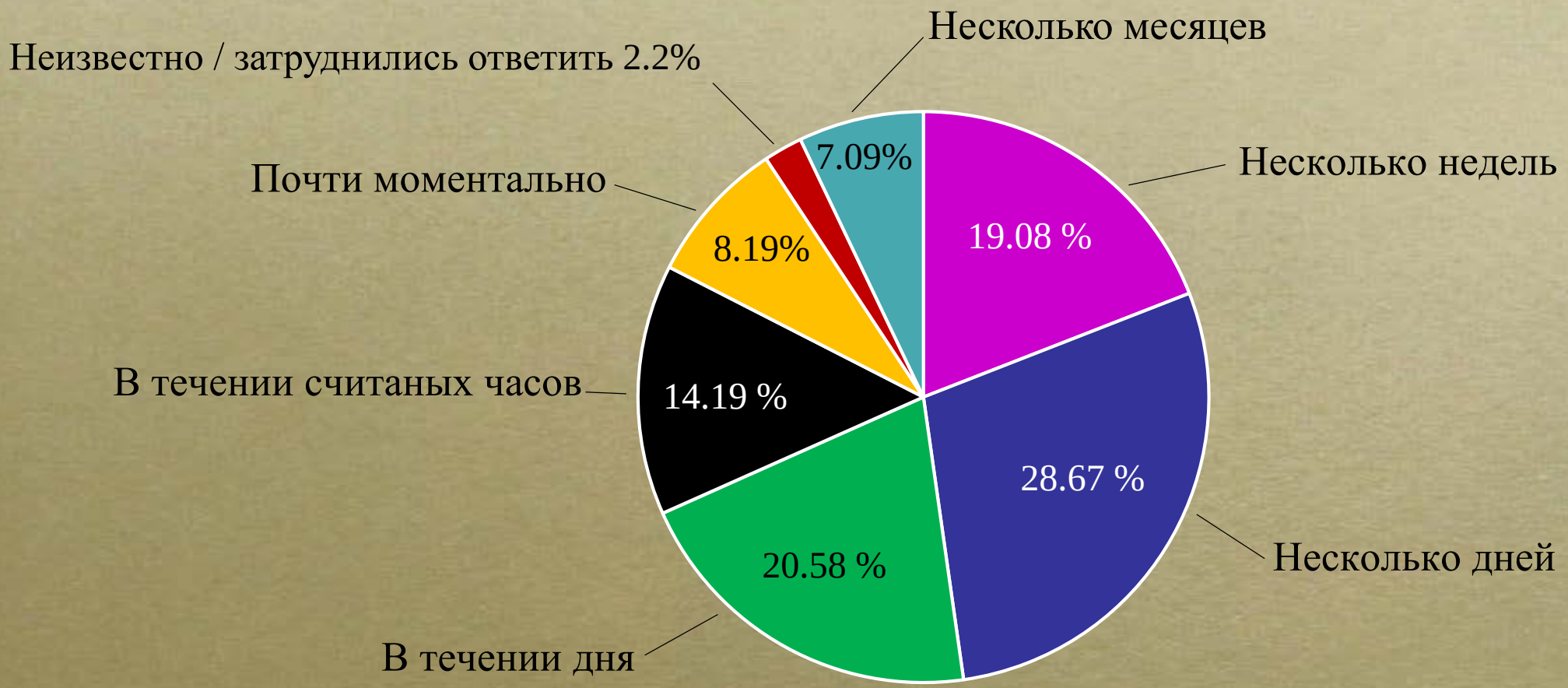
Инциденты за последний год



Тип происшествия	2015	2016	Изменение в %
Вредоносное ПО	62.1%	69.4%	7.3%
Не авторизованный доступ	42.5%	51.2%	8.7%
Утечка данных	38.5%	43.4%	4.9%
ATP или многоступенчатая атака	33.3%	35.7%	2.4%
Утечка через сотрудника	28.2%	25.2%	-3.0%
Атака на отказ в обслуживании	27.6%	21.7%	-5.9%
Несанкционированное повышение привилегий	21.3%	21.7%	0.4%
Атака на отказ в обслуживании для отвлечения внимания	15.5%	11.2%	-4.3%
Атака направленная на нанесение прямого ущерба	14.9%	14.0%	-0.9%
Другие	1.7%	5.4%	3.7%

**The 2016 SANS Incident Response Survey

Время обнаружения



** Kaspersky Security Bulletin 2016

2Bsecure@matrix

Как реагировать на …..?

Кража коммерческой информации

Вирус

Вторжение хакеров

Социальная инженерия

Кража ноутбука

Системный сбой

Пожар

Атака на отказ в обслуживании

Инцидент 1

Ransom in Big Scale

И
Ransom in Big Scale

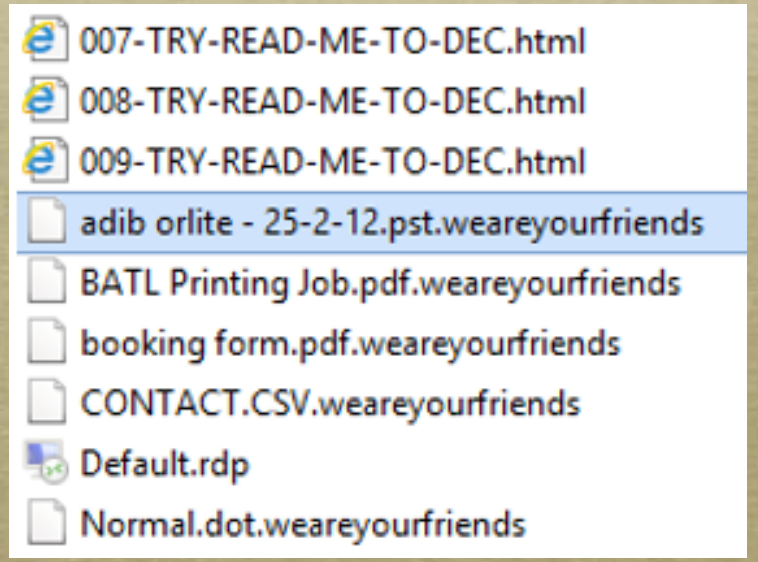
Порядка 600 станций и серверов пострадало в местном филиале

Около 8000 по всему миру

Парализована работа компании

Ransom in Big Scale

- *Зашифрованы документы, базы данных, резервные копии*
- *Расширения файлов изменено на* ***.wearyourfriends***
- *Пострадали все включенные ночью серверы и рабочие станции*



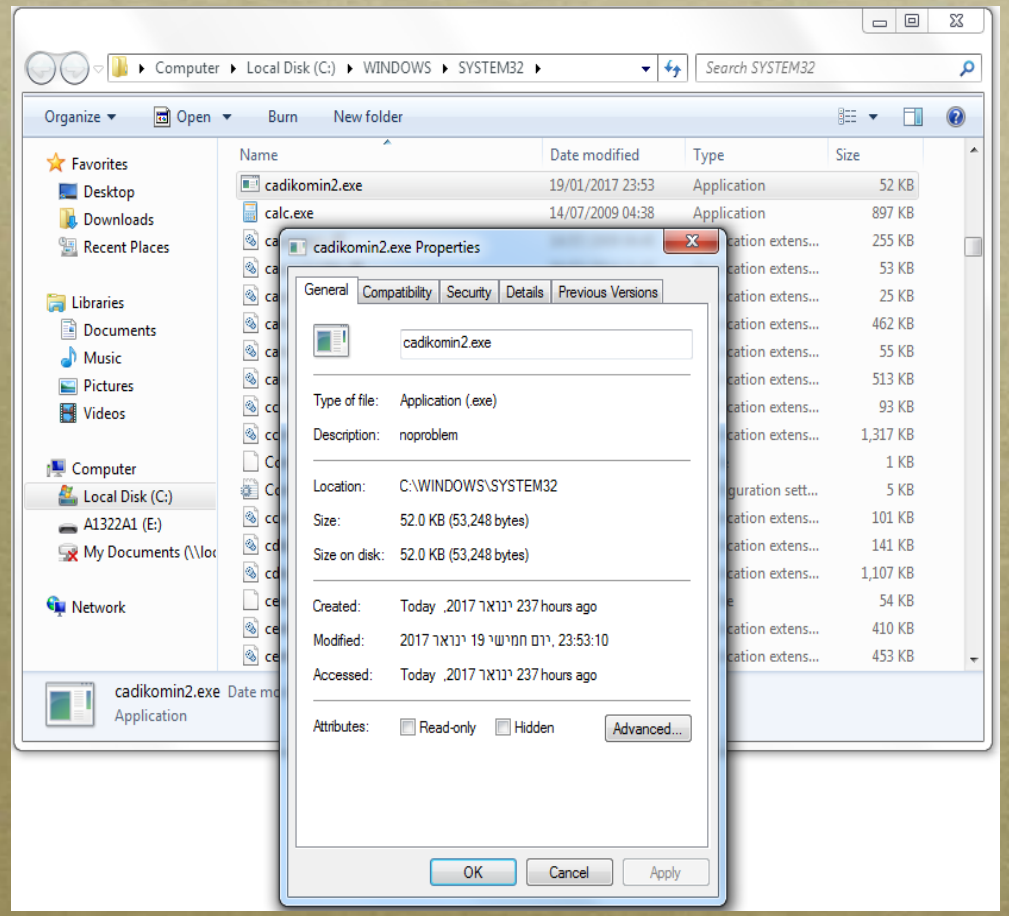
Ransom in Big Scale

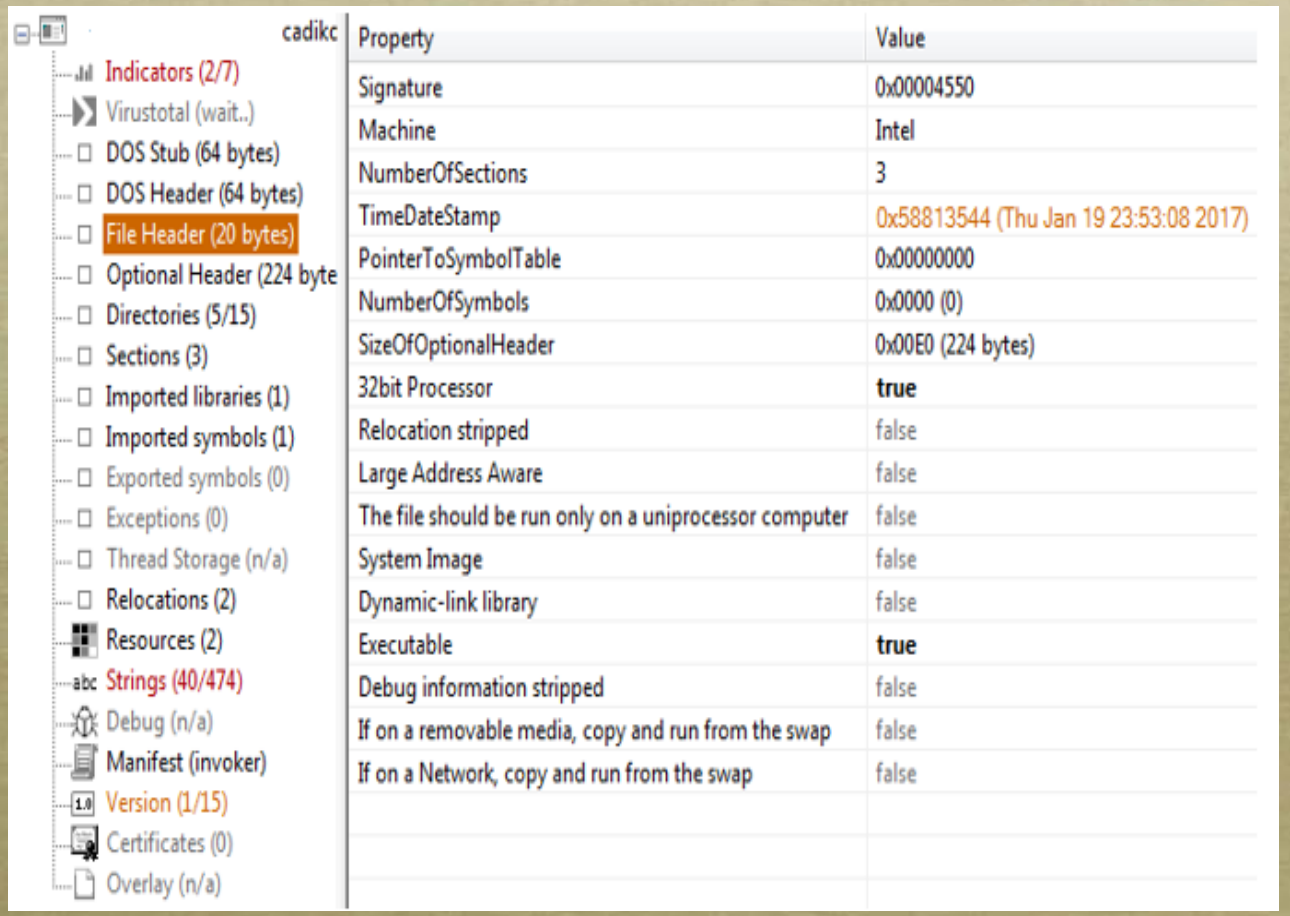
- *23/01/2017 06:15:44 Blocked by Access Protection rule NT AUTHORITY\SYSTEM* ***C:\WINDOWS\SYSTEM32\CADIKOMIN2.EXE*** *C:\Program Files (x86)\Common Files\McAfee\Engine\signlic.txt.weareyourfriends Common Standard Protection:Prevent modification of McAfee Scan Engine files and settings Action blocked : Create*

- *23/01/2017 06:15:44 Blocked by Access Protection rule NT AUTHORITY\SYSTEM* ***C:\WINDOWS\SYSTEM32\CADIKOMIN2.EXE*** *C:\Program Files (x86)\COMMON FILES\McAfee\Engine\x64\signlic.txt Common Standard Protection:Prevent modification of McAfee Scan Engine files and settings Action blocked : Write*

2Bsecure@matrix

Ransom in Big Scale



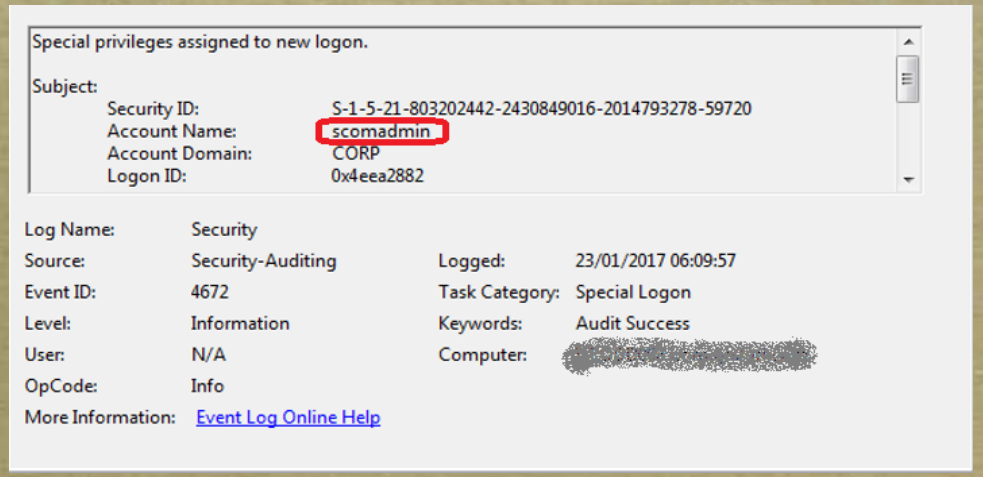


СлучаRansom in Big Scale

- *Файл запущен с удаленной машины с помощью PSEXEC*

CVTRES.EXE	Prefetch	23/01/2017, 01:00
W32TM.EXE	Prefetch	23/01/2017, 01:00
COMPATTELRUNNER.EXE	Prefetch	23/01/2017, 03:57
DELFILE2.EXE	Prefetch	23/01/2017, 04:31
PSEXESVC.EXE	Prefetch	23/01/2017, 06:09
CADIKOMIN2.EXE	Prefetch	23/01/2017, 06:09
CHROME.EXE	Prefetch	23/01/2017, 06:51
NTOSBOOT	Prefetch	23/01/2017, 08:21

- *Для распространения использованы права привилегированного пользователя*



Special privileges assigned to new logon.

Subject:
Security ID: S-1-5-21-803202442-2430849016-2014793278-59720
Account Name: scomadmin
Account Domain: CORP
Logon ID: 0x4eea2882

Log Name: Security
Source: Security-Auditing
Logged: 23/01/2017 06:09:57
Event ID: 4672
Task Category: Special Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: [redacted]
OpCode: Info
More Information: Event Log Online Help

СлучаRansom in Big Scale

Инцидент 2

Первичные симптомы

Бесконтрольная перезагрузка серверов

Часть серверов не поднимаются

Некоторое ПО перестало функционировать

Предшествующий инцидент

Сервер Exchange пострадал от вымогателя

1. Работа почтового сервера восстановлена

2. Ущерб минимизирован

3. Причина инцидента не установлена

Паника !!!!!!

1. *Дата Центр отключен*
2. *Вся организация не функционирует*
3. *Ущерб увеличен многократно*

Выводы

1. Планирование инцидентов и применение планов

2. Сбор и анализ логов

3. Проведение полного расследование