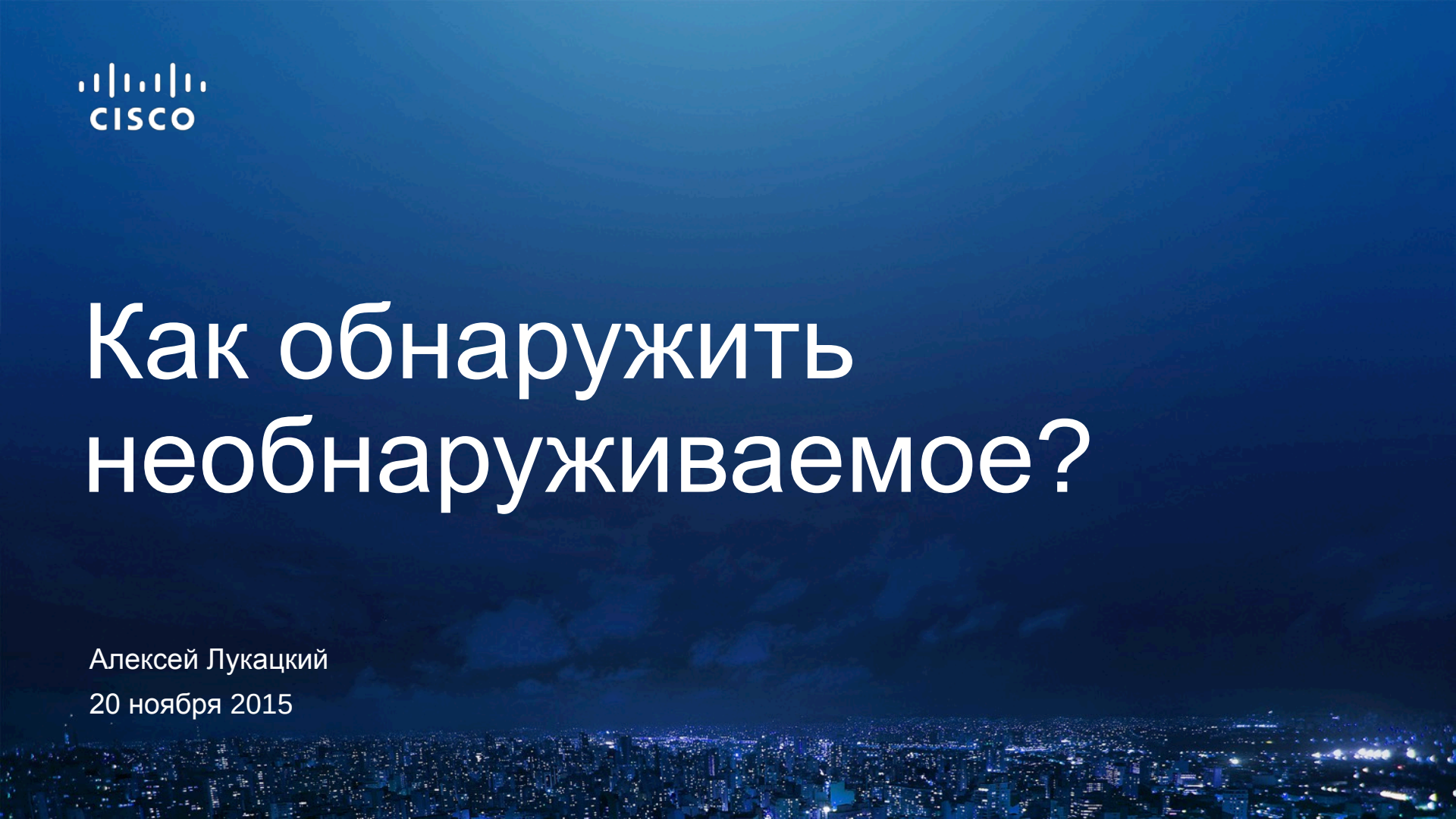


Как обнаружить необнаруживаемое?

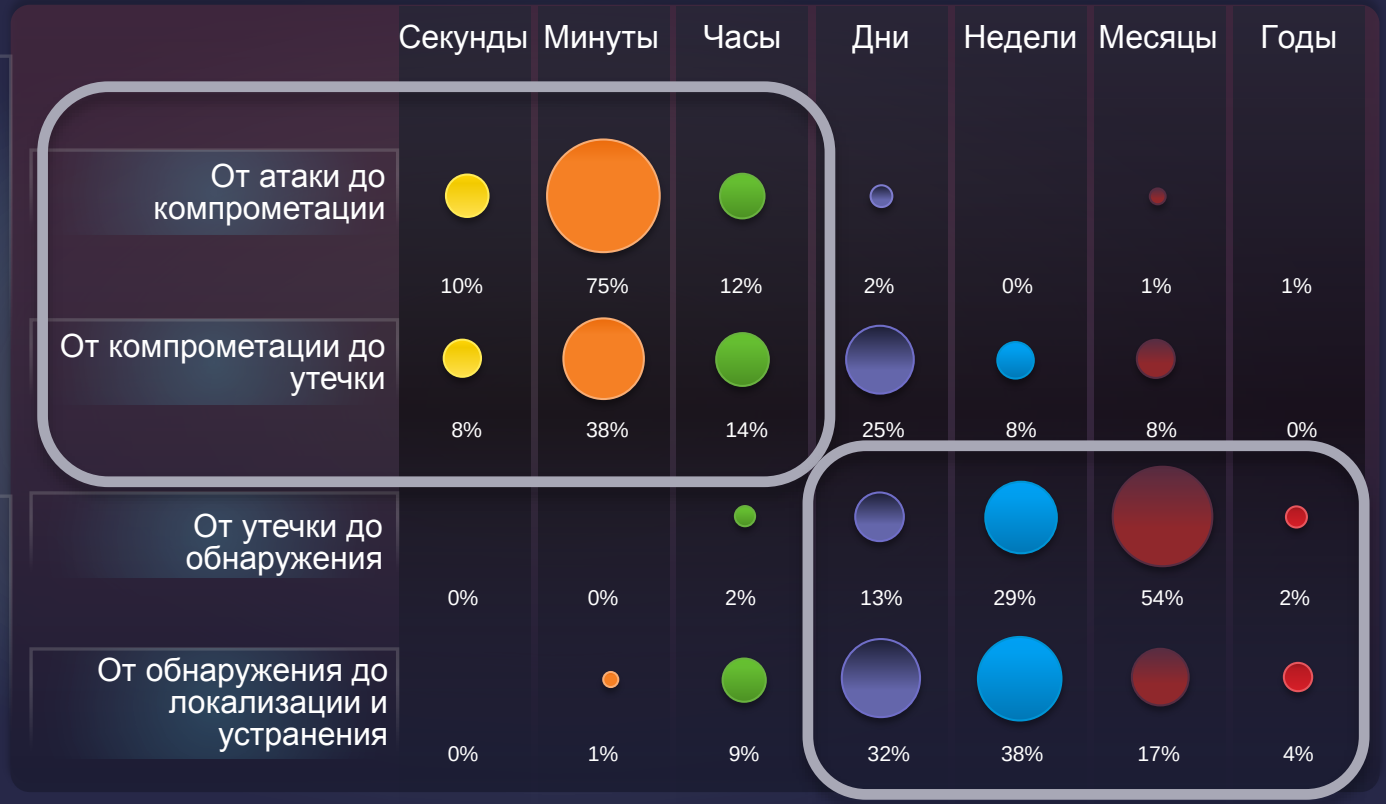
Алексей Лукацкий

20 ноября 2015

Защита периметра – это только начало пути

Взломы осуществляются за минуты

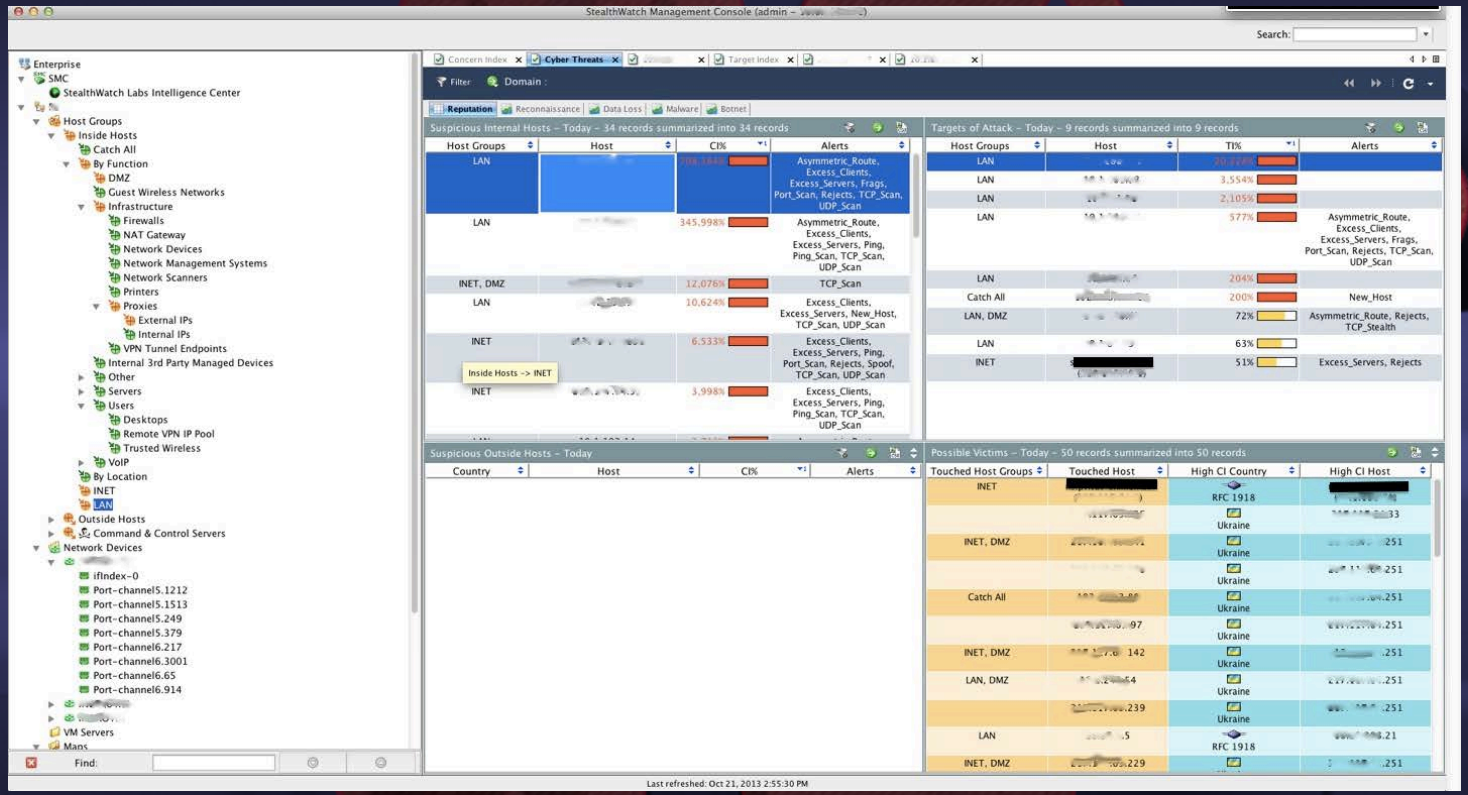
Обнаружение и устранение занимает недели и месяцы



Временная шкала событий в % от общего числа взломов

Источник: 2012 Verizon Data Breach Investigations Report

Пример из жизни: в банке сидел троян Zeus



Современный вредоносный код многогранен

Постоянные обновления увеличили уровень проникновения Angler до 40%

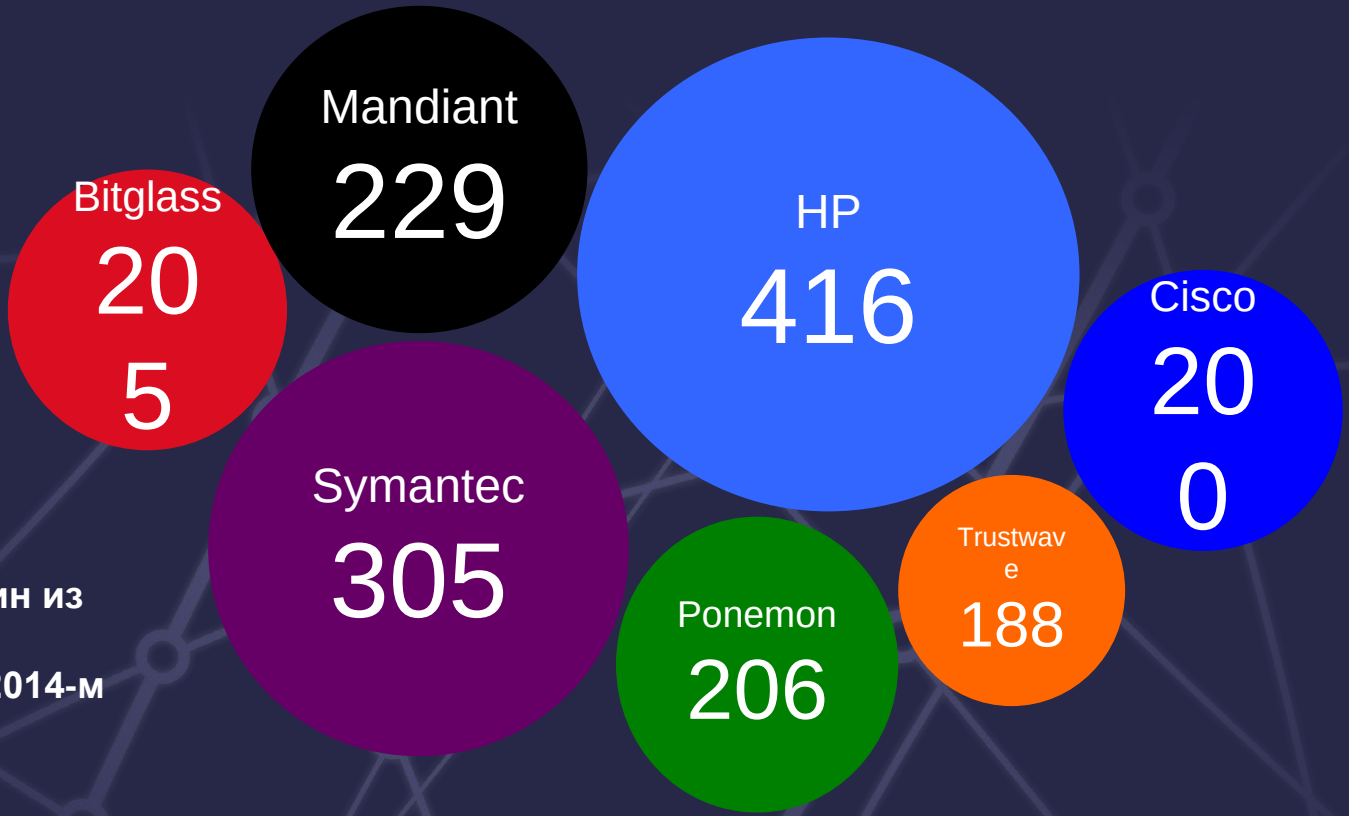
В два раза эффективнее, чем другие exploit kits в 2014

Dridex: краткосрочность и постоянная мутация

Использование «старых» методов, краткосрочность и постоянная мутация приводят к сложностям в блокировании

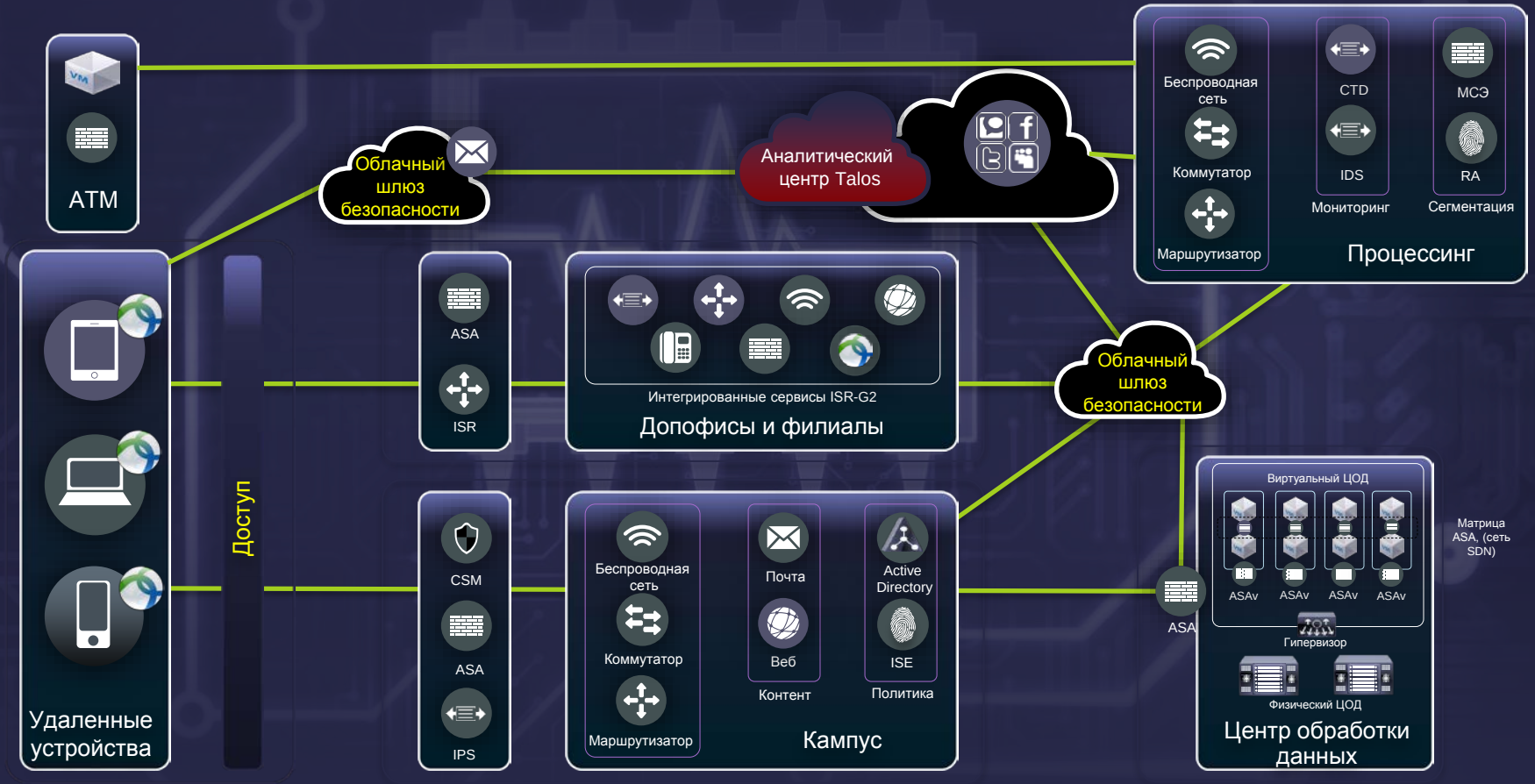
Мы обнаружили с начала года 850 уникальных образцов рассылок Dridex, действующих не более нескольких часов

Время обнаружения вторжений слишком велико



2287 дней – один из самых долгих инцидентов в 2014-м году

Делаете ли вы что-то не только на периметре?



Что мешает увидеть все на периметре?

Наличие Wi-Fi

Сложно контролировать собственных пользоватеоей

Отсутствие мониторинга

Фокусировка на контроле периметра и полное отсутствие мониторинга внутренней сети

Левые точки доступа и 3G

Неразрешенные точки доступа и 3G-модемы

Бреши в настройках МСЭ

Некорректно настроенные МСЭ или забытые правила

Флешки и CD

Попадание вредоносного кода, минуя защитный периметр

Отсутствие визуализации

Отсутствие видимости распространения подозрительных файлов и вредоносного кода

Отсутствие анализа ВПО

Сложность анализа подозрительных файлов

Вы не можете защитить то, чего не видите

На периметре вы видите только верхушку айсберга

Что сеть может сделать для вас?

Сеть как сенсор

Обнаружить аномальный трафик и вредоносы

Например, коммуникации с вредоносными сайтами или эпидемию ВПО внутри сети

Обнаружить использование приложений и нарушение пользователями политик

Например, доступ к финансовому серверу, работу по Skype или утечки данных

Обнаружить посторонние устройства в сети

Например, работу несанкционированных 3G/4G-модема или точки доступа

С помощью чего сеть это может делать?

Сеть как сенсор

Видимость сети, контроль, контекст и аналитика

ACI Vision: Policy Based, Automated Security at Scale

Устройство

Трафик

Приложения

Пользователи

Вредоносы

Обнаружение [illegible] (NetFlow, TrustSec)

Обнаружение [illegible] ПО (IPS Module, Wireless IPS (wIPS), Sourcefire NGIPS)

Обнаружение изменения конфигурации в рамках внутренних устройств (NetFlow, Lancope)

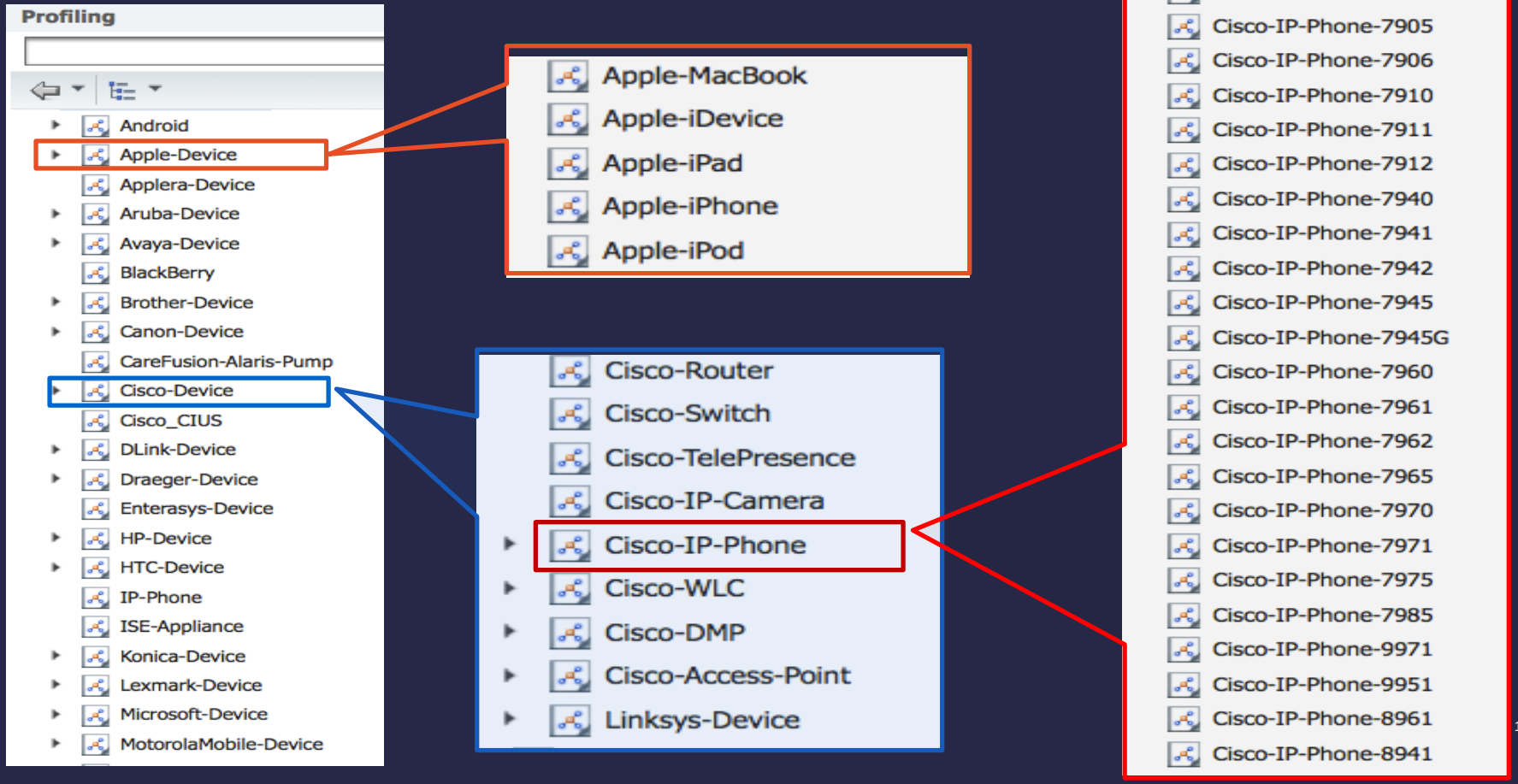
Обнаружение распространения вредоносного ПО внутри (NetFlow, Lancope)

Обнаружение управления и работы вредоносного ПО (NetFlow, Lancope)

Обнаружение утечек данных (NetFlow, Lancope)

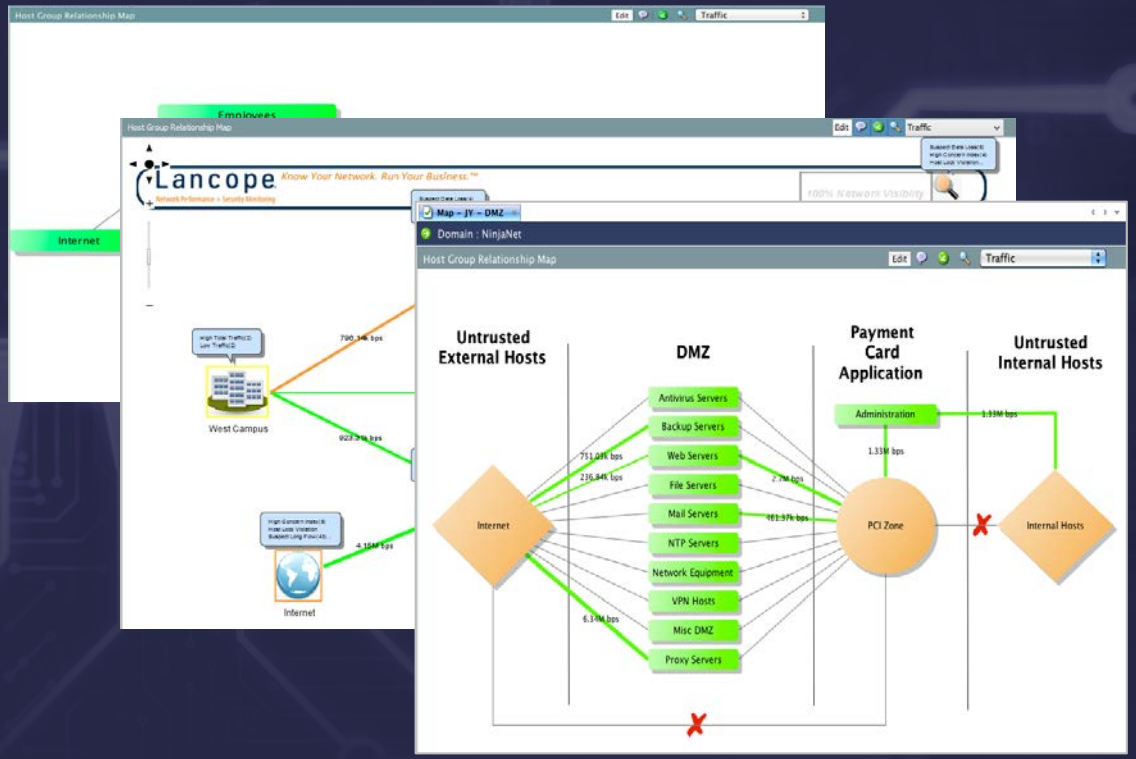
Система раннего предупреждения (Cisco Security Intelligence Operations)

Обнаружение посторонних устройств



Визуализация информационных потоков

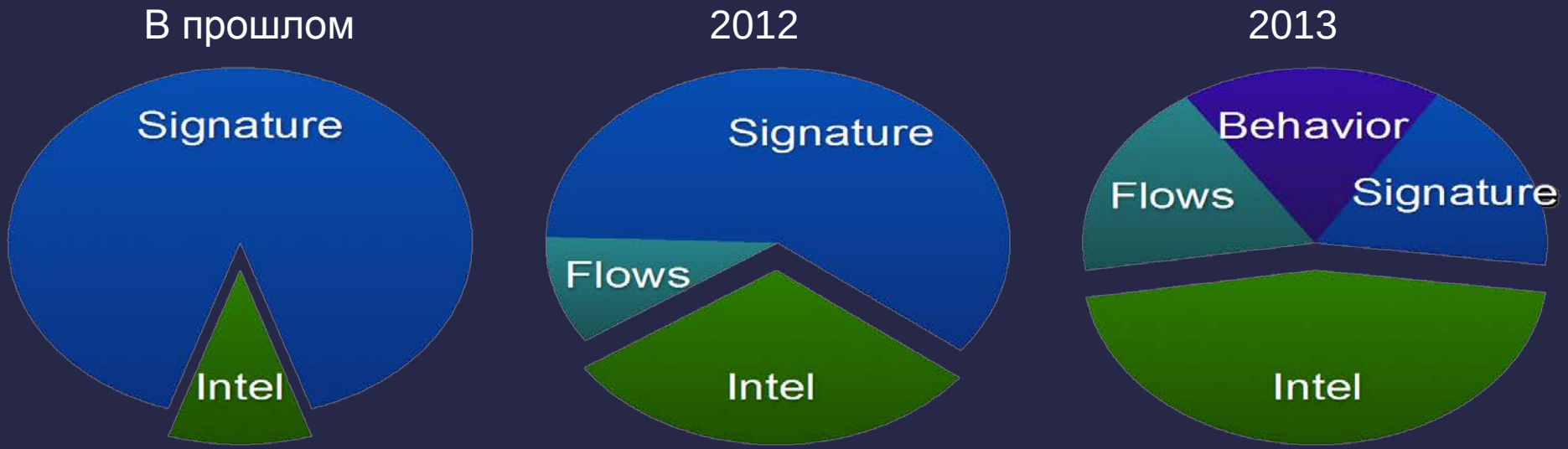
- Моделирование сетевых потоков «как правильно»
- Показ реальных информационных потоков между узлами и группами узлов с нужным уровнем детализации карты сети
- Отслеживание ошибок в настройках межсетевых экранов и обнаружение «левых» подключений



Опыт Cisco: идентификация и блокирование посторонних беспроводных устройств

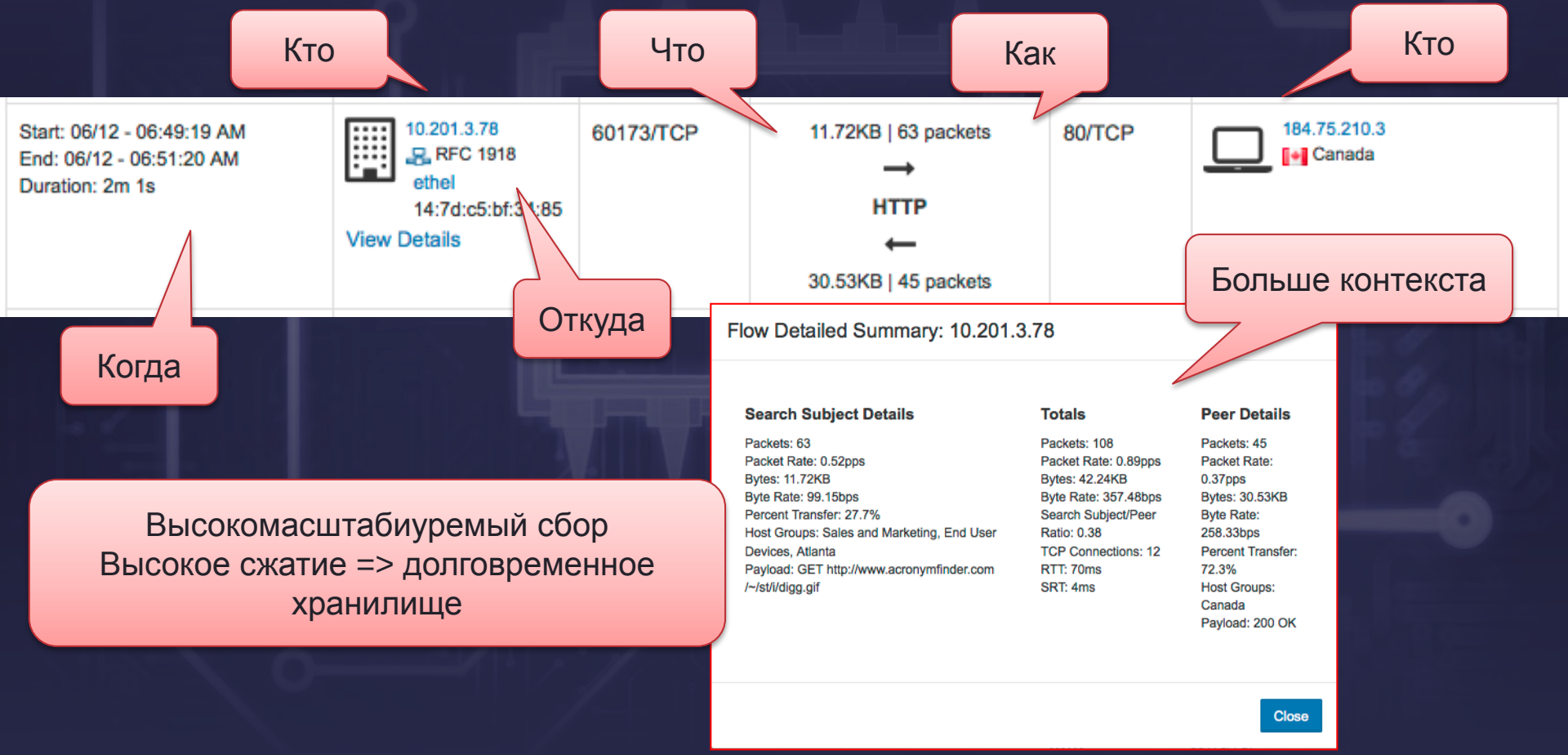
- Само мобильное устройство не может сказать, что оно «чужое»
  - Нужен внешний независимый контроль с помощью систем контроля доступа, в т.ч. и беспроводного
- Cisco Wireless Controller / Cisco Wireless Adaptive IPS / Cisco Wireless Location Services помогают контролировать беспроводной эфир
  - Все это часть функционала платформы Cisco Mobility Services Engine

Опыт Cisco: комбинируйте методы обнаружения



Необходимо использовать различные способы изучения угроз
Сетевые потоки | Поведение | Сигнатуры | Исследования

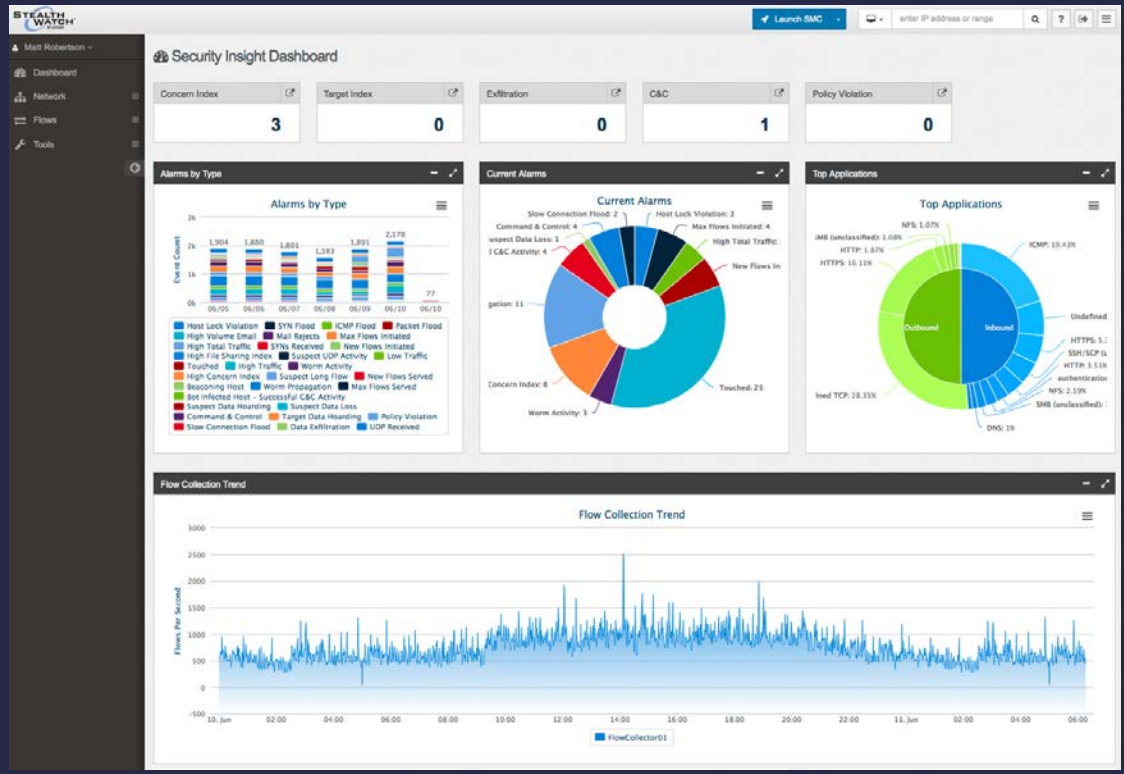
Что такое NetFlow?



Высокомасштабируемый сбор
Высокое сжатие => долговременное хранилище

Обнаружение вредоносного кода на базе NetFlow

- Что делать, когда вы не можете поставить сенсор IPS на каждый сегмент сети?
- У вас же есть NetFlow на каждом коммутаторе и маршрутизаторе
- Отдайте его для обнаружения аномальной активности
  - Сканирование
  - Целенаправленные угрозы
  - Эпидемии вредоносного ПО
  - DDoS
  - Утечки данных
  - Ботнеты

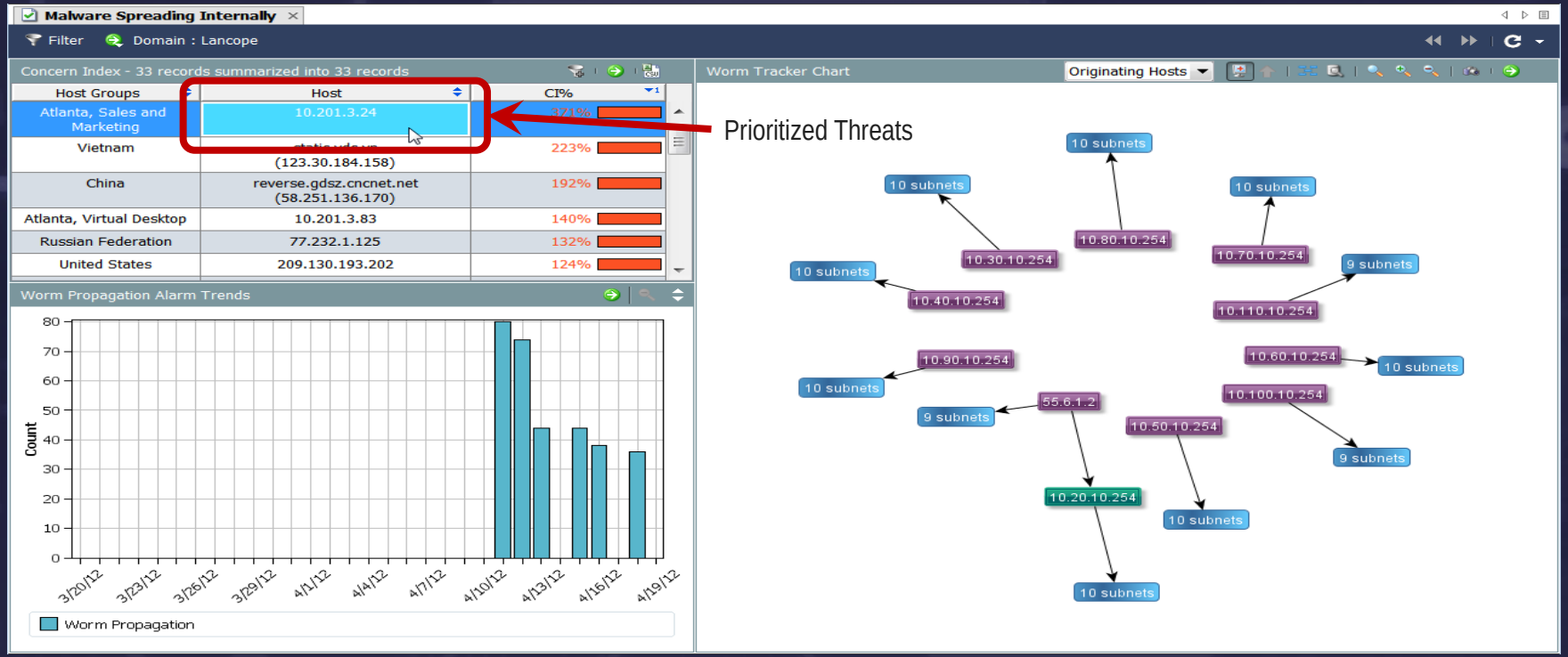


NetFlow – сердце подхода «Сеть как сенсор»

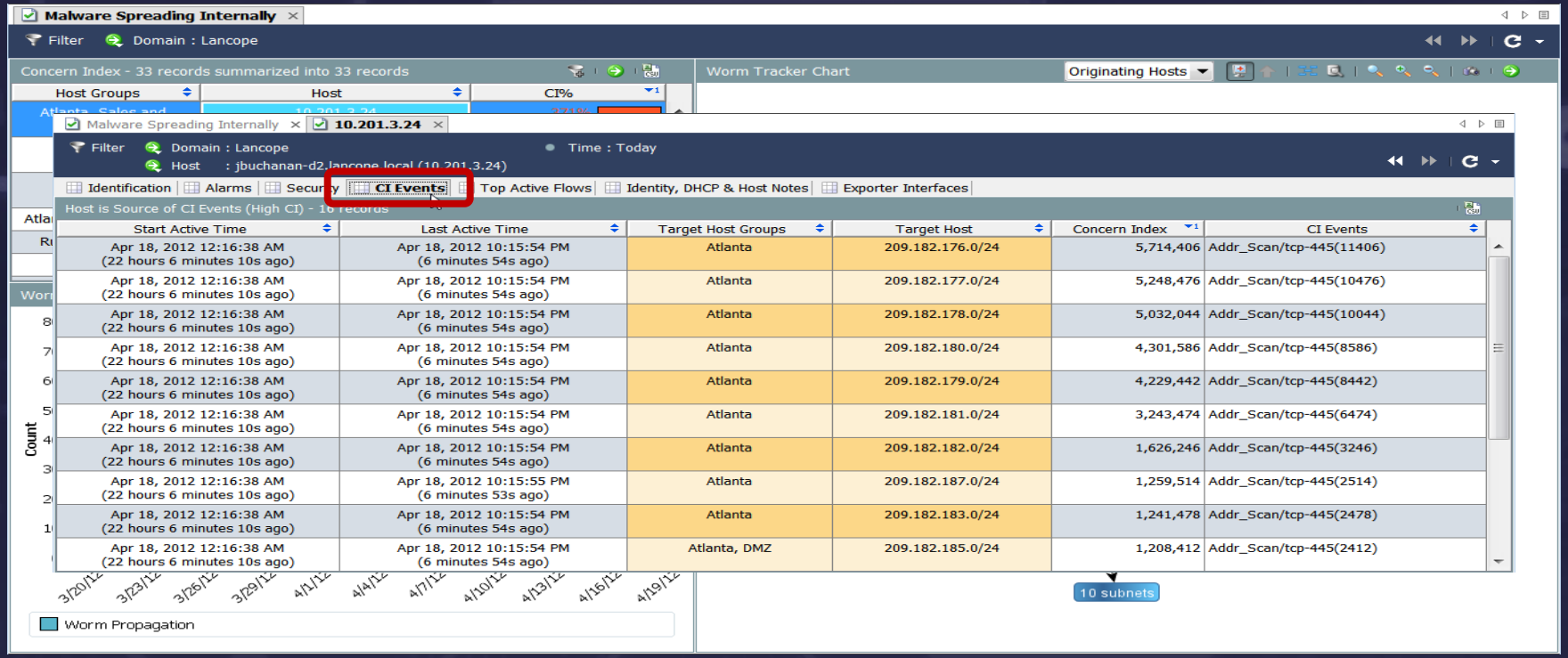
NetFlow в действии: атака в процессе реализации

	Стадия атаки	Обнаружение
1	**Использование уязвимостей** **Злоумышленник сканирует IP-адреса и порты для поиска уязвимостей (ОС, пользователи, приложения)**	▪ NetFlow может обнаружить сканирование диапазонов IP ▪ NetFlow может обнаружить сканирование портов на каждом IP-адресе
2	**Установка вредоносного ПО на первый узел** **Хакер устанавливает ПО для получения доступа**	▪ NetFlow может обнаружить входящий управляющий трафик с неожиданного месторасположения
3	**Соединение с “Command and Control”** **Вредоносное ПО создает соединение с C&C серверами для получения инструкций**	▪ NetFlow может обнаружить исходящий трафик к известным адресам серверов C&C
4	**Распространение вредоносного ПО на другие узлы** **Атака других систем в сети через использование уязвимостей**	▪ NetFlow может обнаружить сканирование диапазонов IP ▪ NetFlow может обнаружить сканирование портов на каждом IP-адресе внутреннего узла
5	**Утечка данных** **Отправка данных на внешние сервера**	▪ NetFlow может обнаружить расширенные потоки (HTTP, FTP, GETMAIL, MAPIGET и другие) и передачу данных на внешние узлы

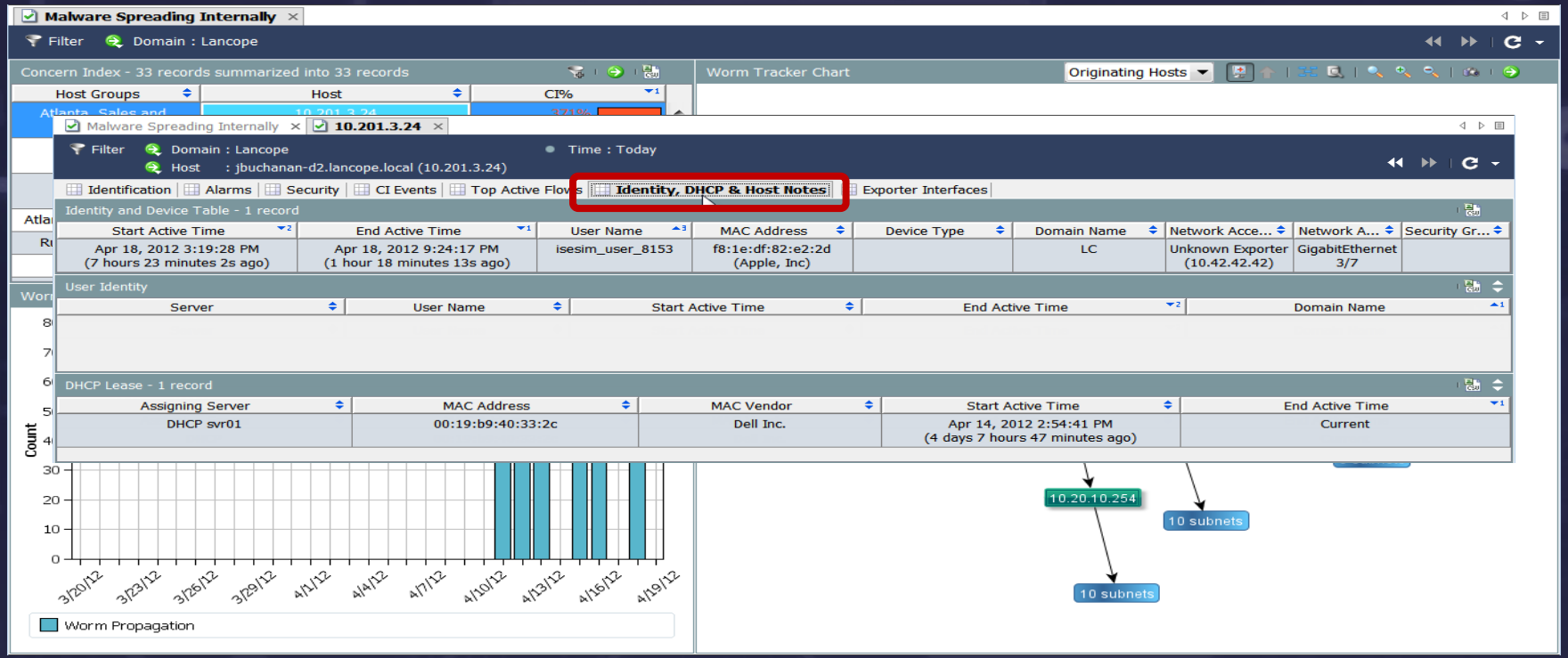
Обнаружение вредоносного кода с помощью NetFlow



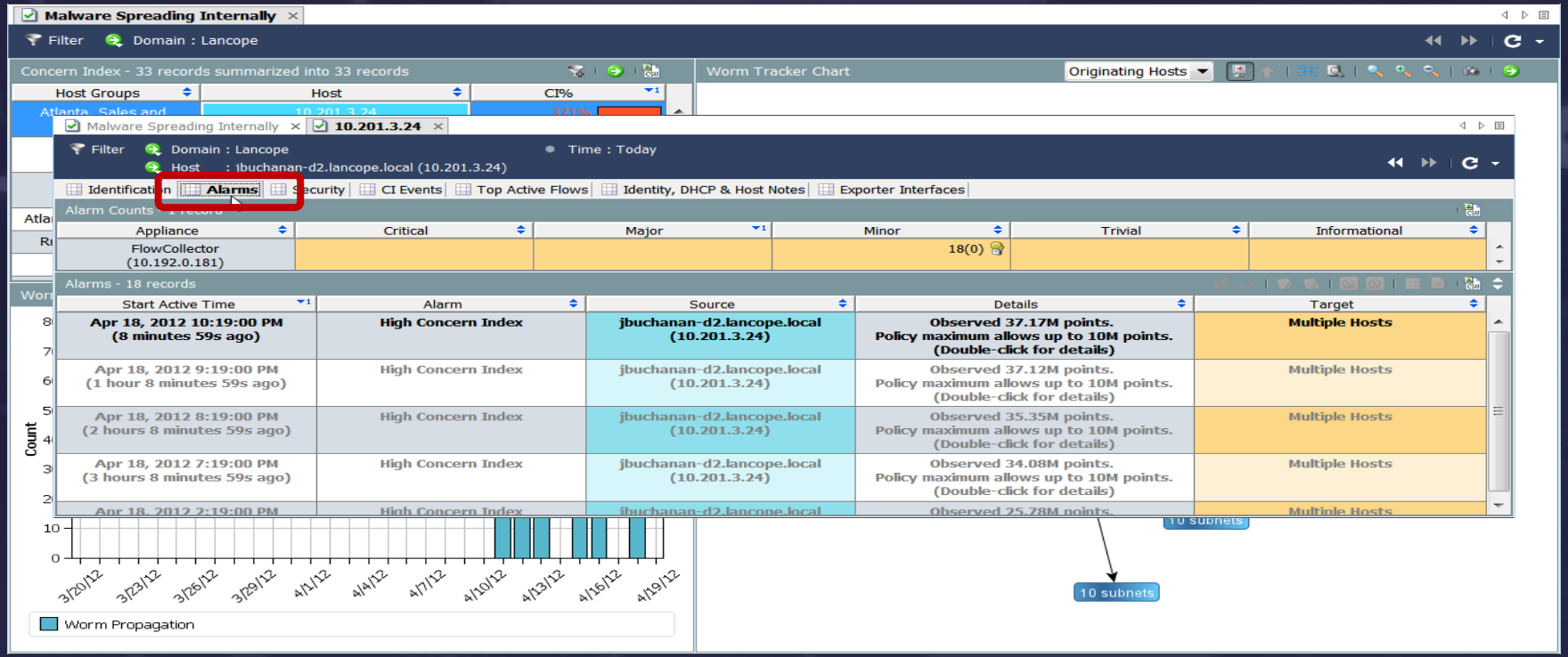
Обнаружение вредоносного кода с помощью NetFlow



Обнаружение вредоносного кода с помощью NetFlow



Обнаружение вредоносного кода с помощью NetFlow



Обнаружение вредоносного кода с помощью NetFlow

Более 100 алгоритмов обнаружения

Concern Index

Domain : NinjaNet Time : Today

Host Group : Outside Hosts

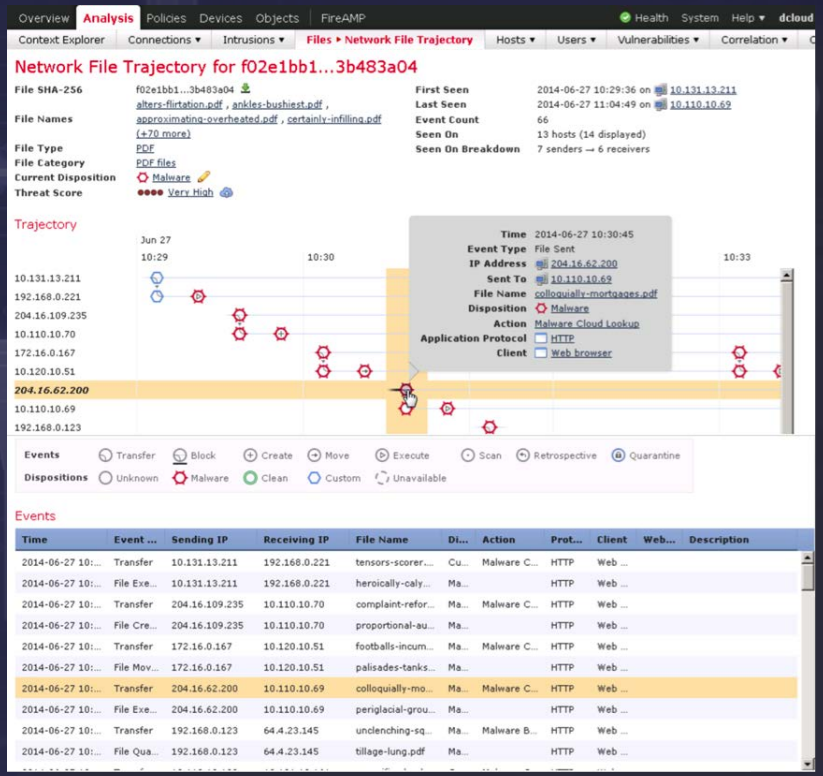
Summary – 13 records summarized into 13 records

Country	Host	CI		Alerts	Client Services
United States	70.46.194.122.nw.nuvox.net	28,545,681		Excess_Clients, Long_Ping, New_Host, Ping, Ping_Scan, Rejects, TCP_Scan	VMware-client, auth, bgp, dnstcp, finger, ftp, h323, http, http-alt, https, imap4, ipp, isakmp, kerberos, ms-rpc, ncp, netbios-ss, nntp, pop, pop3s, rtsp, samba-web, slp, smb, smtp, ssh, tacacs, telnet, time, unix-rpc, whois, wins, 17/tcp, 30/tcp, 199/tcp, 256/tcp
United States	10-234-115-208.reverse.lstn.net	7,226,510		Excess_Clients, TCP_Scan	icq, kazaa, mc-client, ms-rpc, rat, socks, 1032/tcp, 1034/tcp, 1036/tcp, 1042/tcp
Germany	a81-14-226-150.net-htp.de	2,362,728		TCP_Scan	smb
Korea, Republic Of	183.110.241.106	2,131,262		Excess_Clients, TCP_Scan	UPnP, bittorrent, dc++, finger, h323, http, ipp, irc, macromedia, ms-olap, ms-sms, msn-im, mysql, netmeeting, postgressql, remote-desktop, rsync, smtp, vnc, wbem, xwindows, 655/tcp, 730/tcp, 1044/tcp, 3339/tcp
China	86.12.142.61.broad.dg.gd.dynamic.163data.com.cn	1,919,609		UDP_Scan	sql-server
China	211.143.23.132	1,908,593		UDP_Scan	sql-server
China	211.141.79.26	31,052		UDP_Scan	sql-server
China	61.160.107.254	12,035		Ping_Scan	
China	58.221.28.142	9,018		New_Host, TCP_Scan	6239/tcp, 14433/tcp, 18530/tcp, 22627/tcp

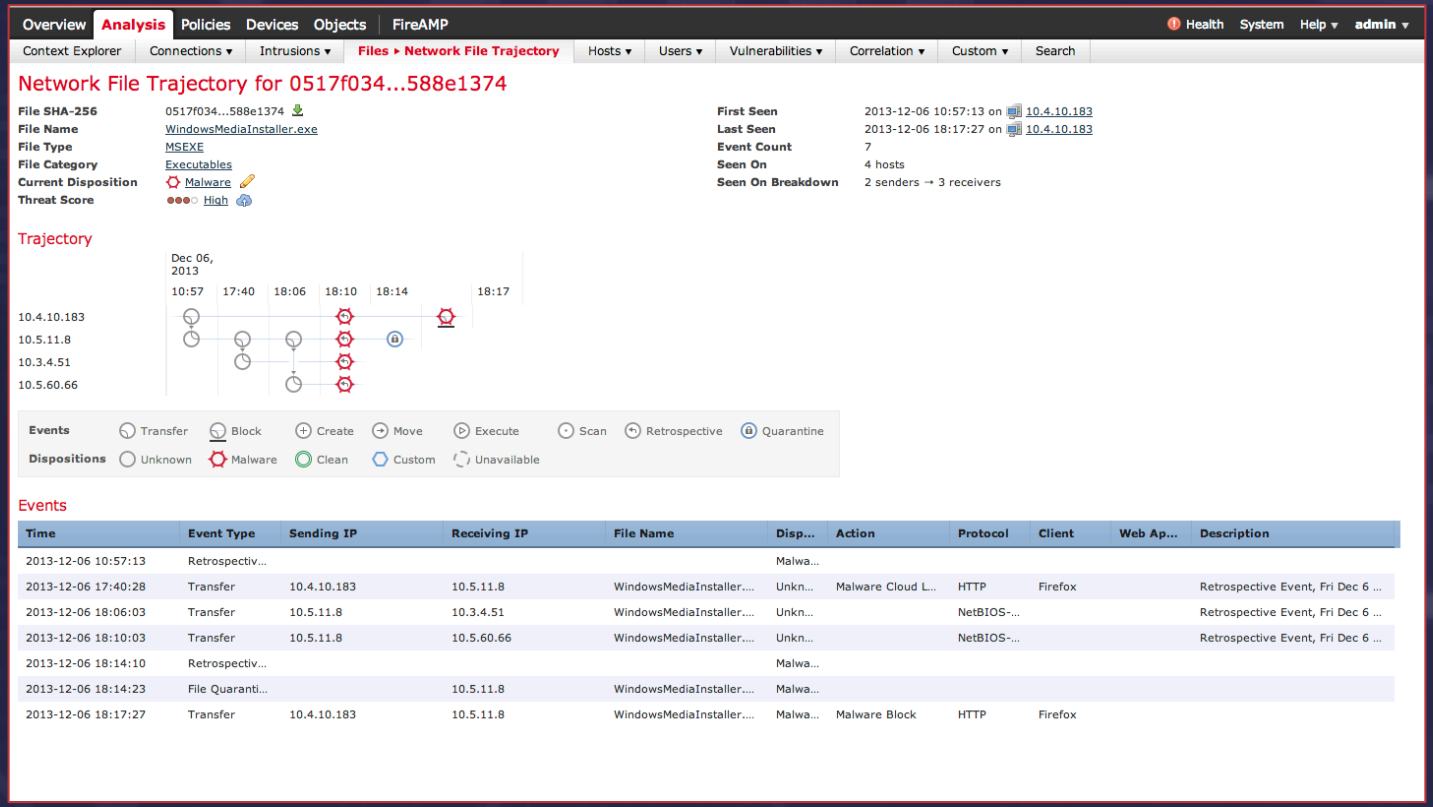
- Addr_Scan/tcp
- Addr_Scan/udp
- App_Fake/tcp
- App_Fake/udp
- Bad_Flag_ACK
- Bad_Flag_All
- Bad_Flag_NoFlg
- Bad_Flag_Rsrvd
- Bad_Flag_RST
- Bad_Flag_SYN_FIN
- Bad_Flag_URG
- Bad_Flags
- Frag:First_Too_Short
- Frag:Packet_Too_Long
- Frag:Sizes_Differ
- Half_Open_Attack
- ICMP_Comm_Admin
- ICMP_Dest_Host_Admin
- ICMP_Dest_Host_Unk
- ICMP_Dest_Net_Admin
- ICMP_Dest_Net_Unk
- ICMP_Flood
- ICMP_Frag_Needed
- ICMP_Host_Precedence
- ICMP_Host_Unreach
- ICMP_Host_Unreach_TOS
- ICMP_Net_Unreach
- ICMP_Net_Unreach_TOS
- ICMP_Port_Unreach
- ICMP_Precedence_Cutoff
- ICMP_Proto_Unreach
- ICMP_Src_Host_Isolated

Визуализация движения вредоносных файлов в сети

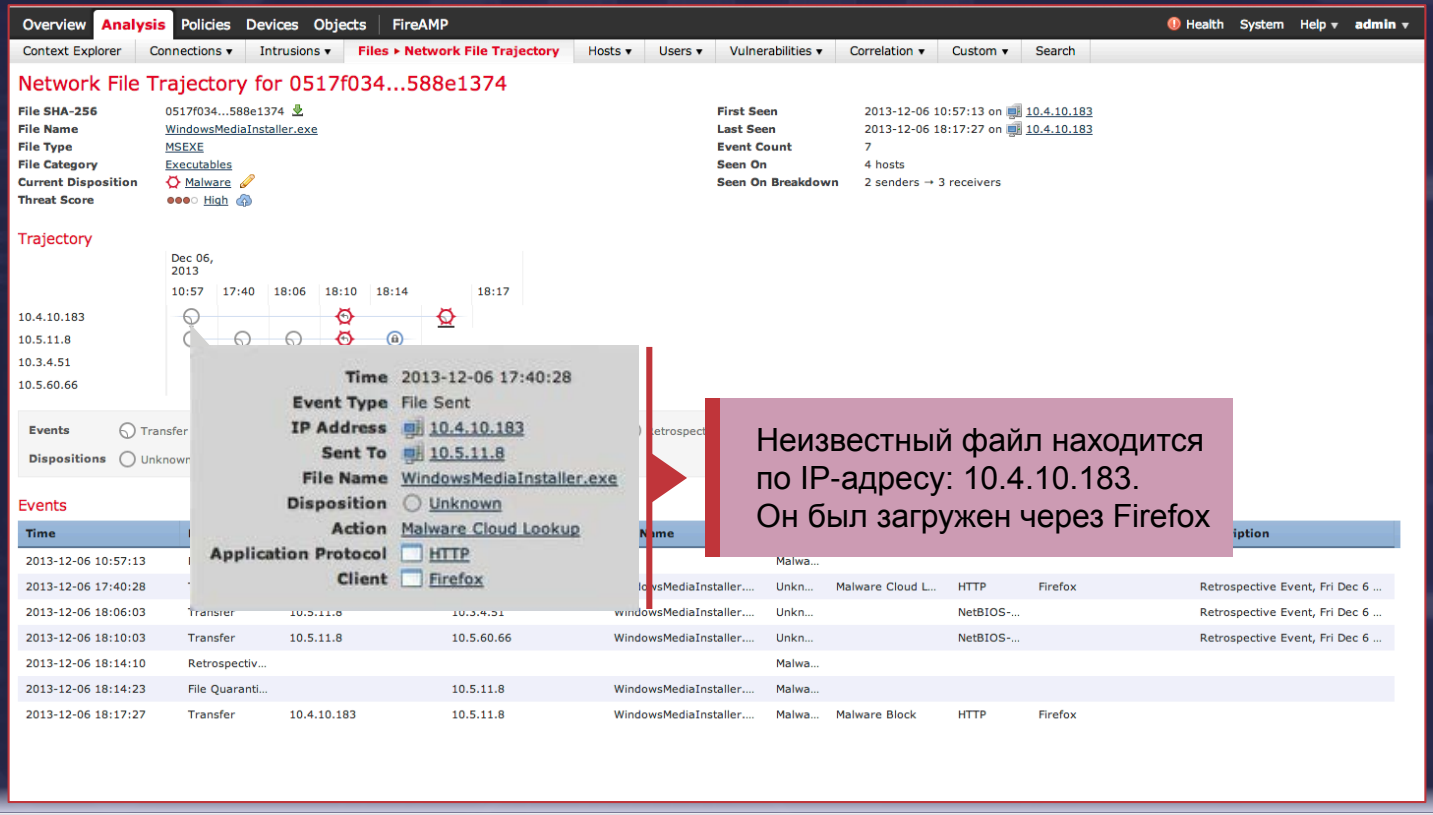
- Какие системы были инфицированы?
- Кто был инфицирован?
- Когда это произошло?
- Какой процесс, узел или пользователь был отправной точкой?
- Почему это произошло?
- Что еще произошло?
- С кем контактировал зараженный узел?



Что такое «сетевая траектория»?

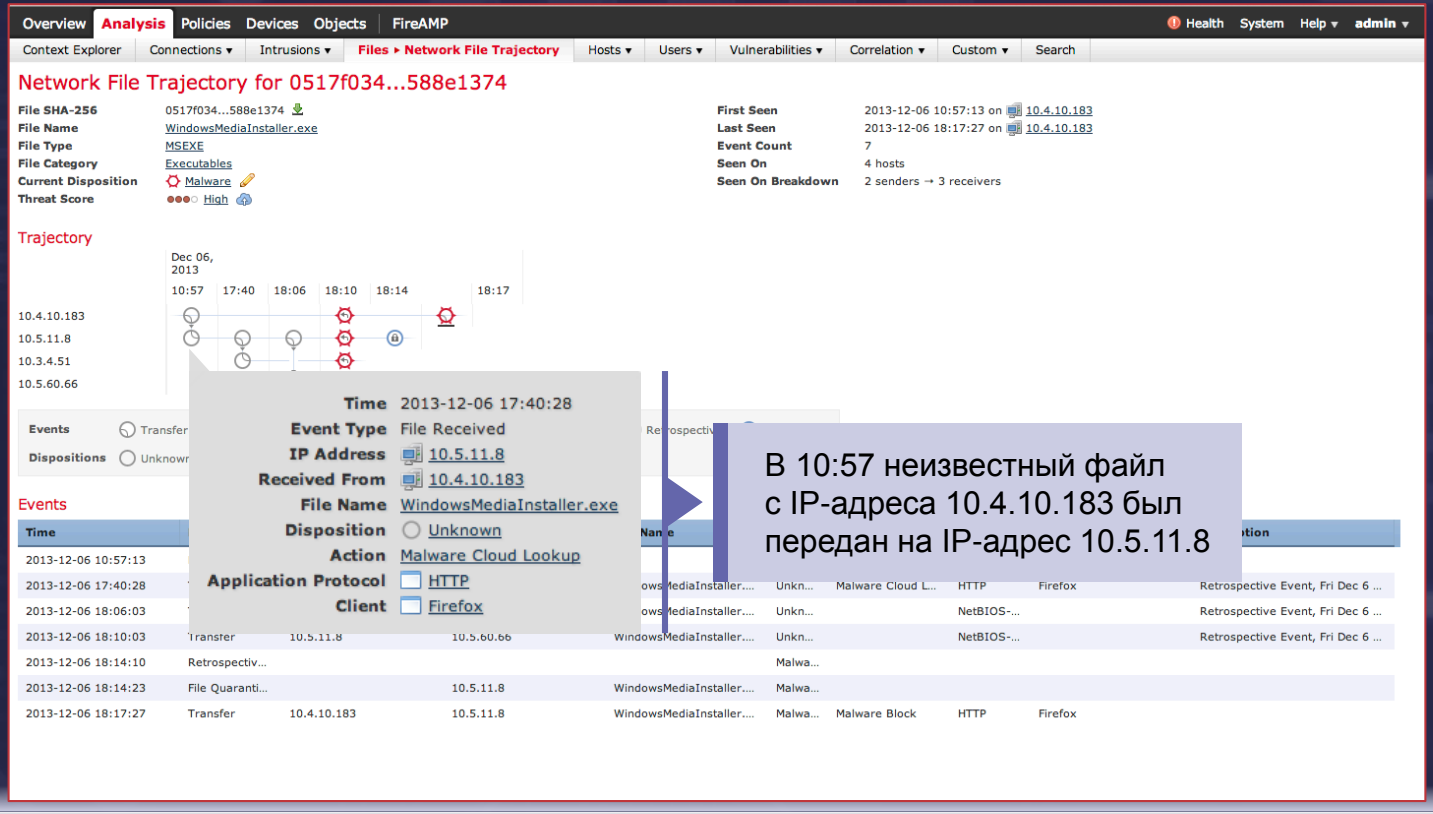


Что такое «сетевая траектория»?

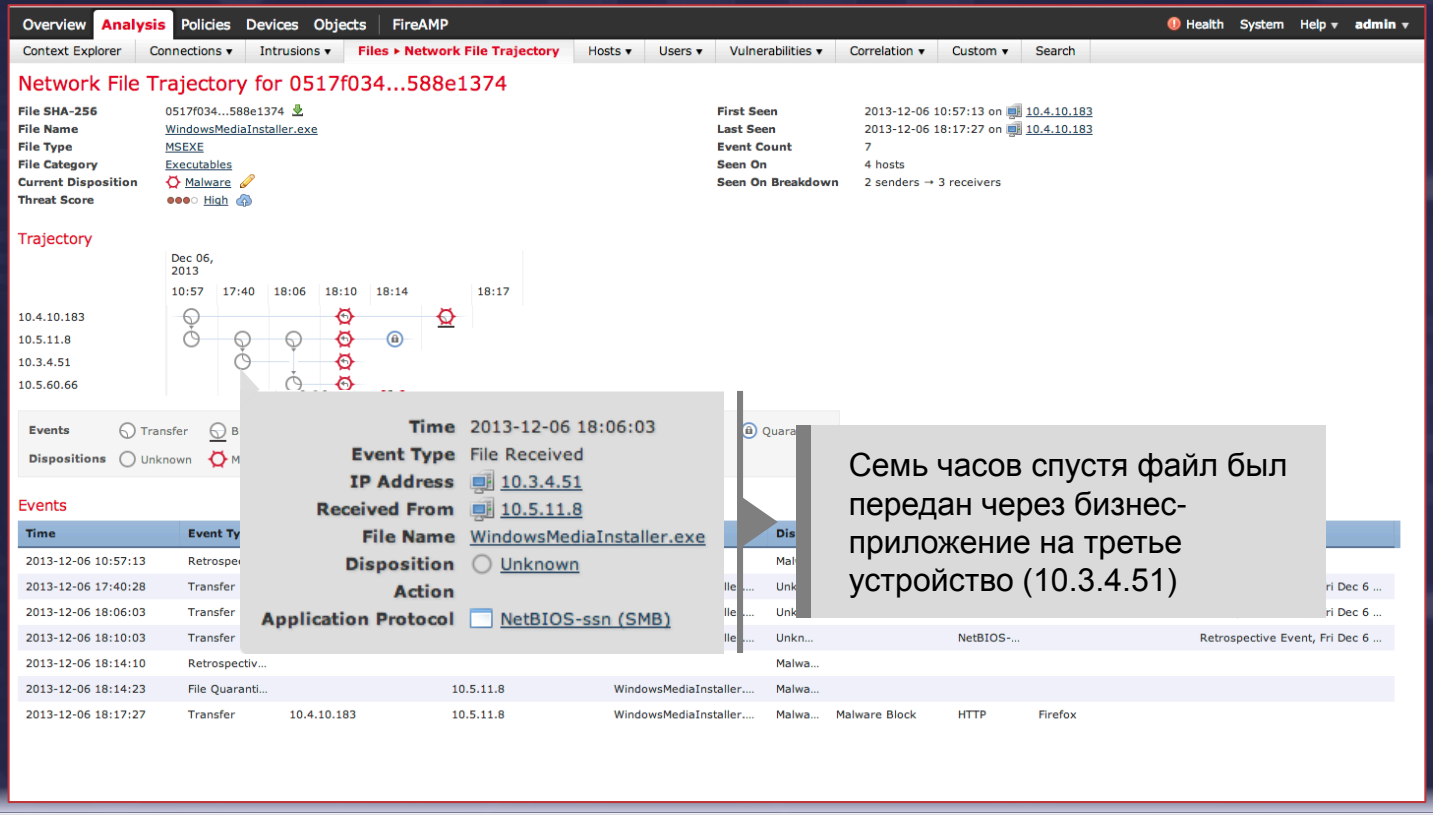


Неизвестный файл находится по IP-адресу: 10.4.10.183.
Он был загружен через Firefox

Что такое «сетевая траектория»?

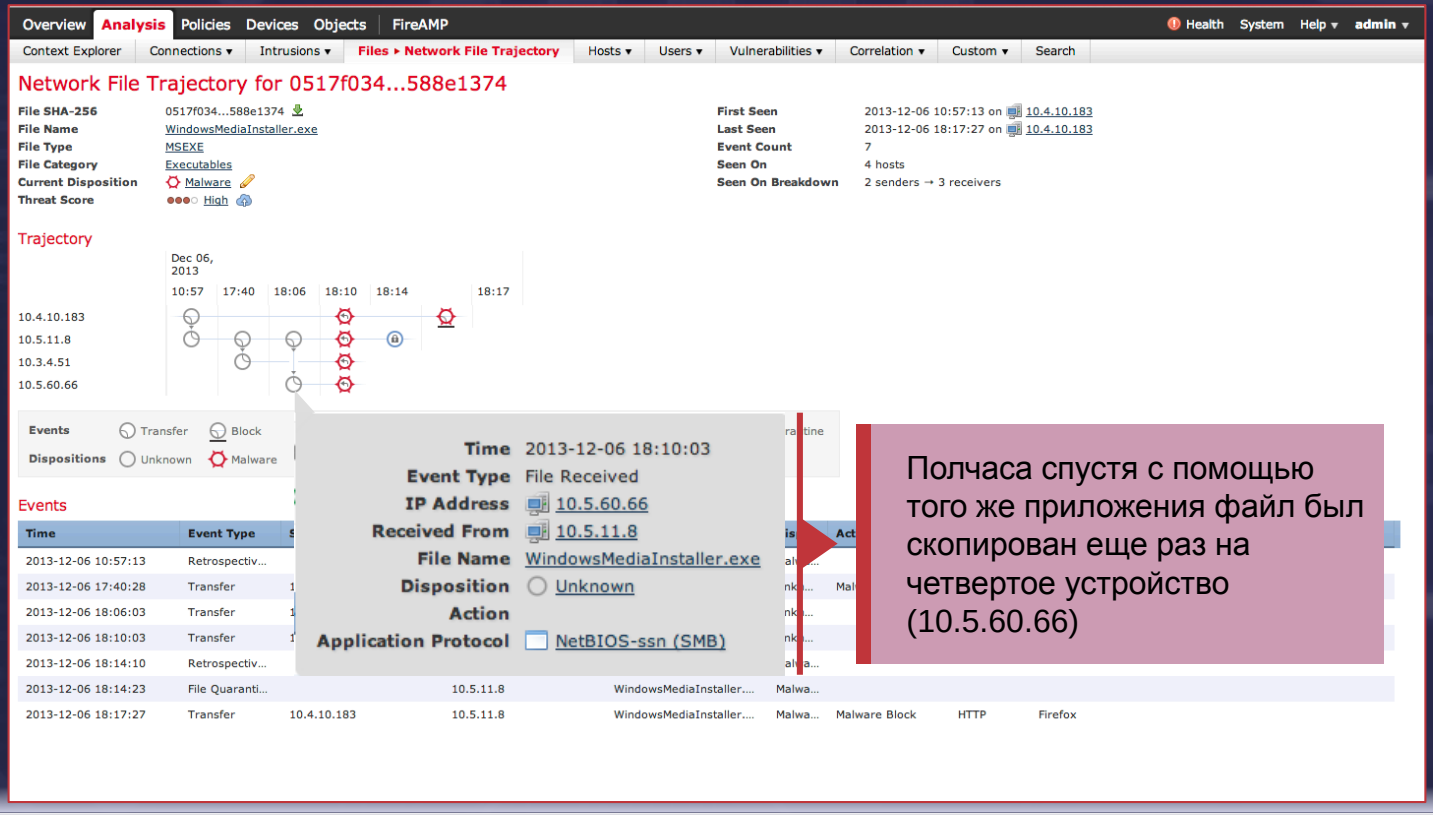


Что такое «сетевая траектория»?

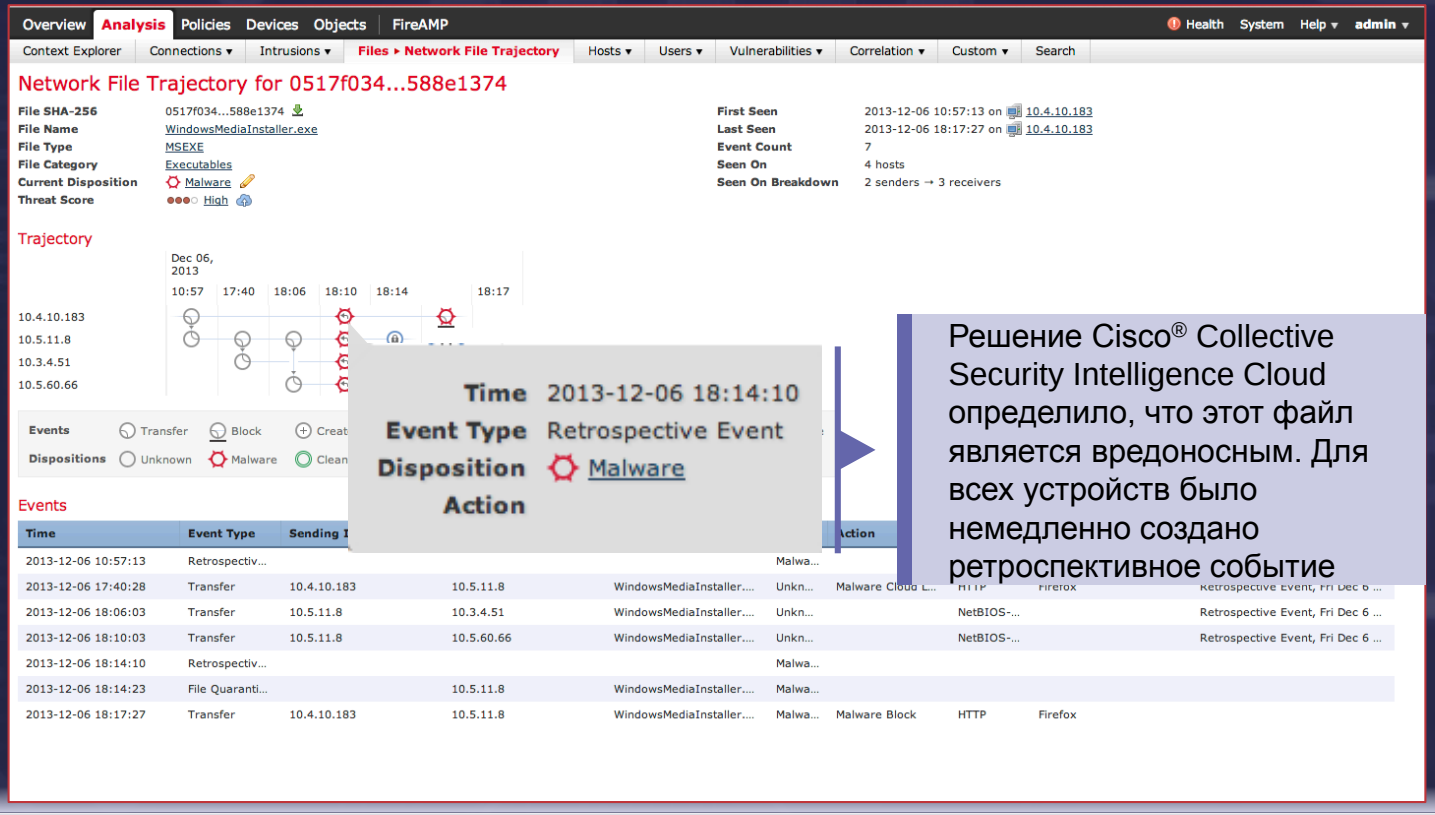


Семь часов спустя файл был передан через бизнес-приложение на третье устройство (10.3.4.51)

Что такое «сетевая траектория»?

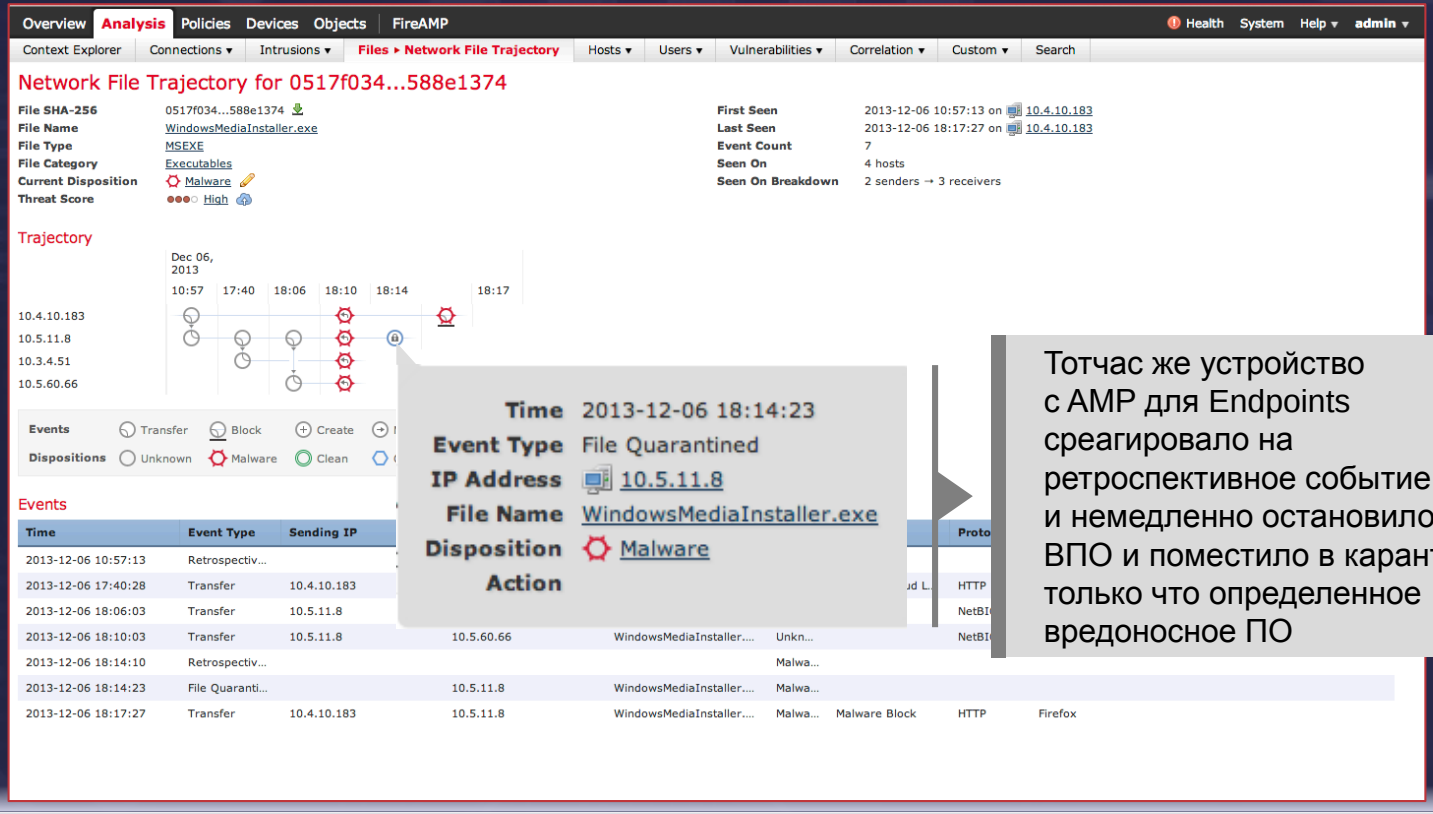


Что такое «сетевая траектория»?



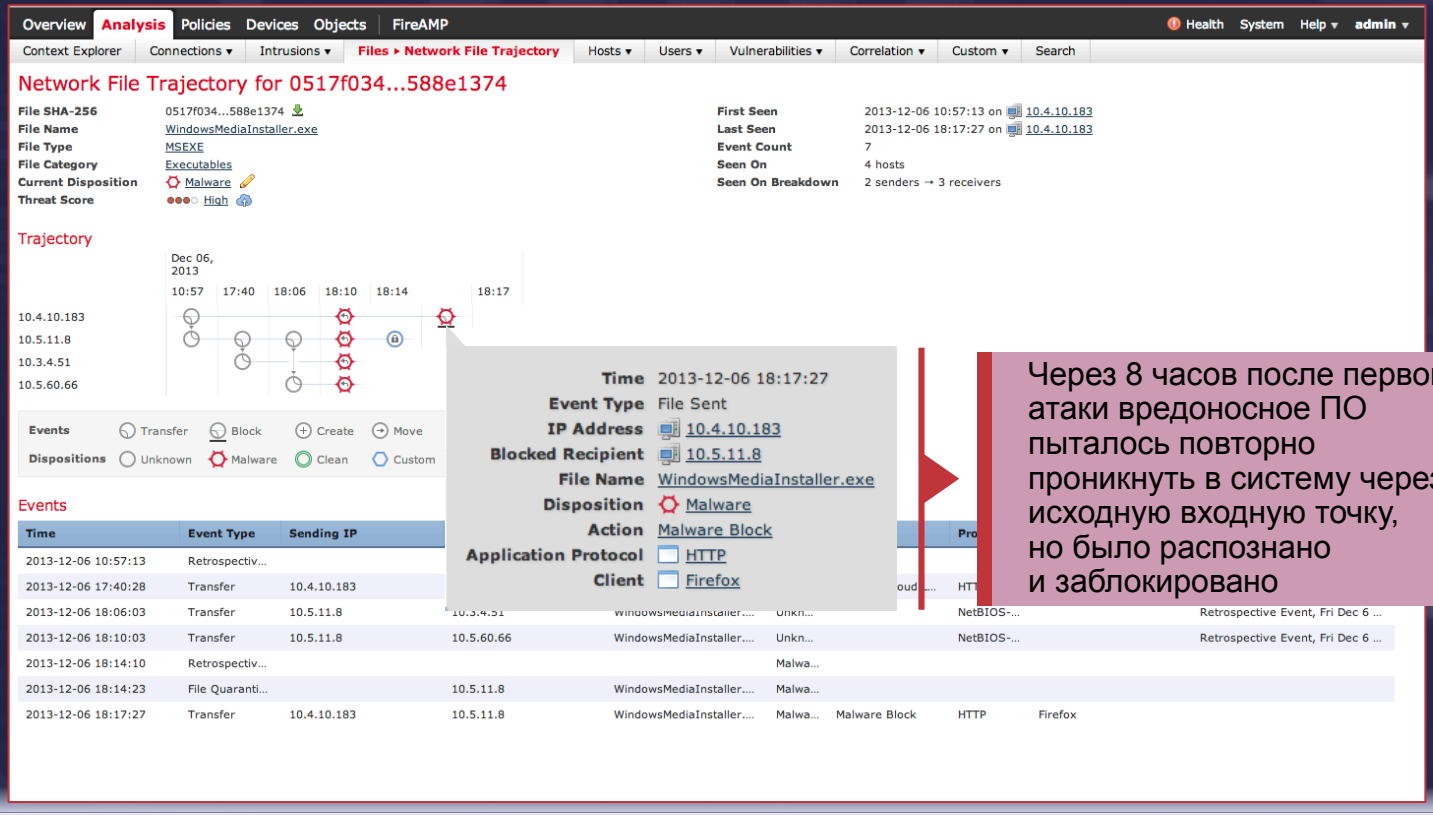
Решение Cisco® Collective Security Intelligence Cloud определило, что этот файл является вредоносным. Для всех устройств было немедленно создано ретроспективное событие

Что такое «сетевая траектория»?



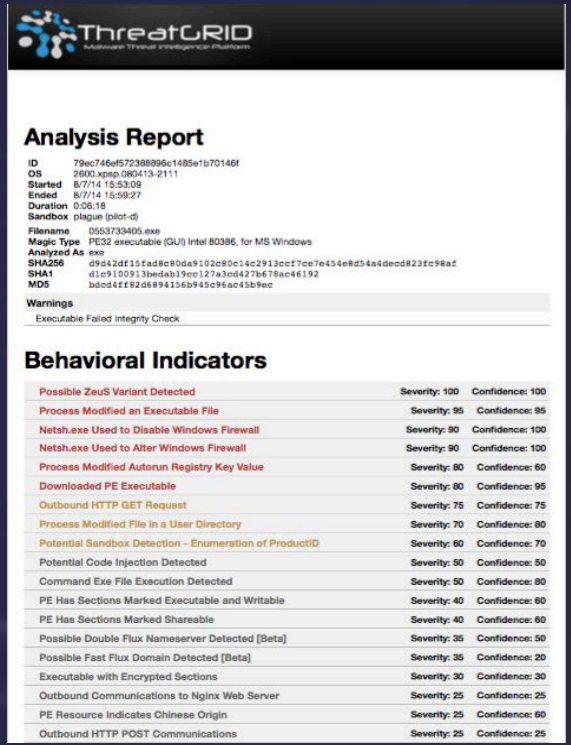
Тотчас же устройство с AMP для Endpoints среагировало на ретроспективное событие и немедленно остановило ВПО и поместило в карантин только что определенное вредоносное ПО

Что такое «сетевая траектория»?



Глубокий анализ подозрительных файлов

- Нередко бывает необходимость анализировать файлы, попавшие в службу безопасности на флешках или иных носителях, а также проводить более глубокий анализ обнаруженных с помощью Cisco AMP вредоносных программ
- Организация может захотеть создать собственную службу Threat Intelligence или Security Operations Center



ThreatGRID
Malware Threat Intelligence Platform

Analysis Report

ID	79ec746ef572388896c1485e1b70146f
OS	2600.xpsp.080413-2111
Started	8/7/14 15:53:09
Ended	8/7/14 15:59:27
Duration	0:06:18
Sandbox	plague (pilot-d)
Filename	0553733405.exe
Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
Analyzed As	exe
SHA256	d9d42df15fad8c80da9102c80c14c2913ccf7ee7e454e8d54a4decd823fc98af
SHA1	d1e9100913bedab19ec127a3cd427b678ac46192
MD5	bdcd4ff82d6894156b945c96ac45b9ec

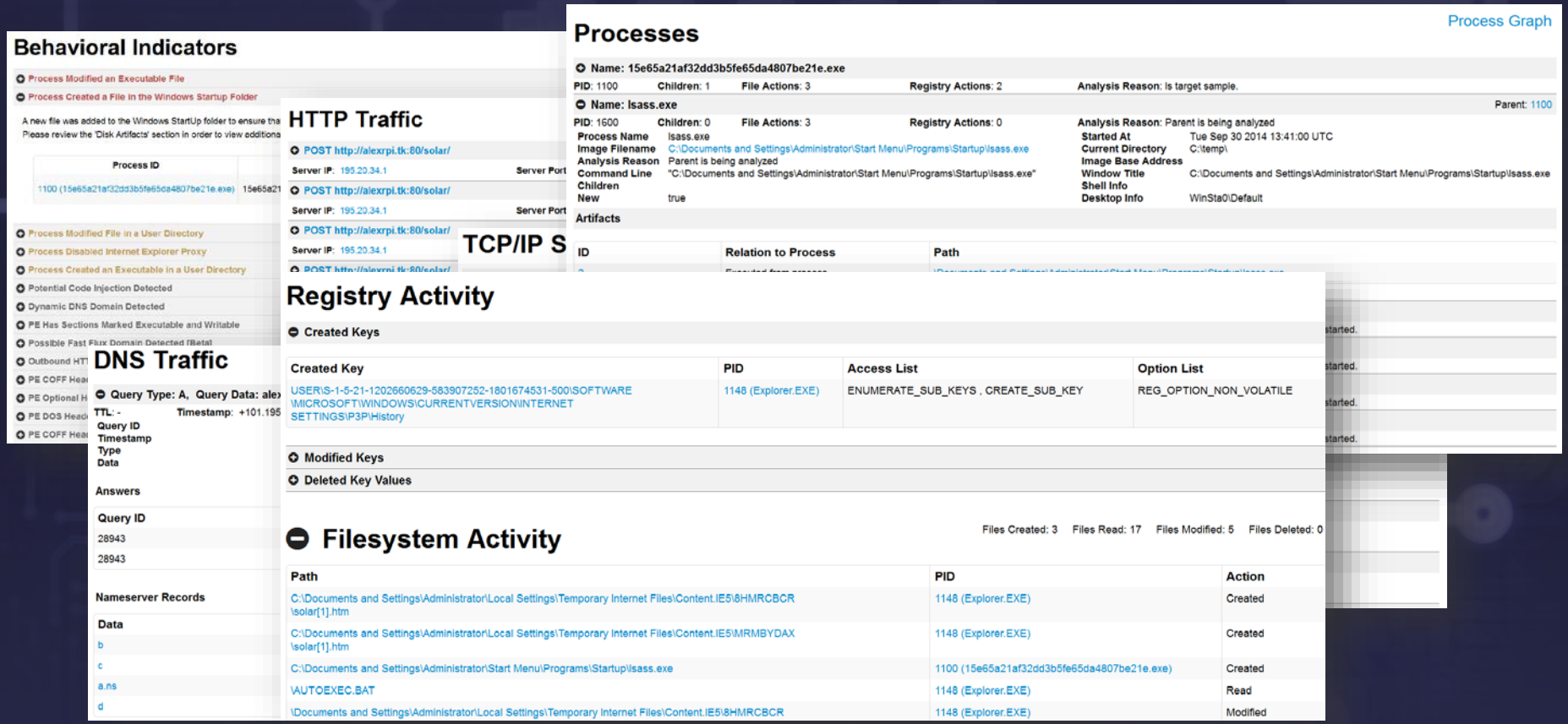
Warnings

Executable Failed Integrity Check

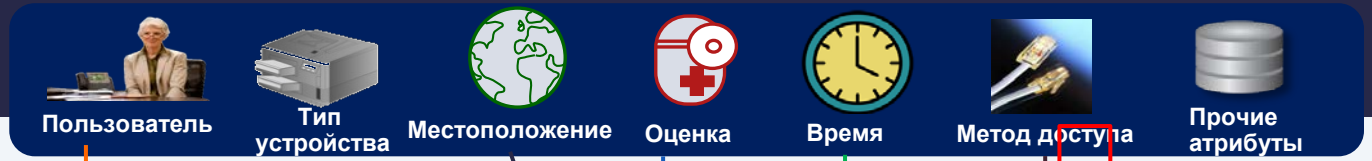
Behavioral Indicators

Possible ZeuS Variant Detected	Severity: 100	Confidence: 100
Process Modified an Executable File	Severity: 95	Confidence: 95
Netsh.exe Used to Disable Windows Firewall	Severity: 90	Confidence: 100
Netsh.exe Used to Alter Windows Firewall	Severity: 90	Confidence: 100
Process Modified Autorun Registry Key Value	Severity: 80	Confidence: 60
Downloaded PE Executable	Severity: 80	Confidence: 95
Outbound HTTP GET Request	Severity: 75	Confidence: 75
Process Modified File in a User Directory	Severity: 70	Confidence: 80
Potential Sandbox Detection - Enumeration of ProductID	Severity: 60	Confidence: 70
Potential Code Injection Detected	Severity: 50	Confidence: 50
Command Exe File Execution Detected	Severity: 50	Confidence: 80
PE Has Sections Marked Executable and Writable	Severity: 40	Confidence: 60
PE Has Sections Marked Shareable	Severity: 40	Confidence: 60
Possible Double Flux Nameserver Detected [Beta]	Severity: 35	Confidence: 50
Possible Fast Flux Domain Detected [Beta]	Severity: 35	Confidence: 20
Executable with Encrypted Sections	Severity: 30	Confidence: 30
Outbound Communications to Nginx Web Server	Severity: 25	Confidence: 25
PE Resource Indicates Chinese Origin	Severity: 25	Confidence: 60
Outbound HTTP POST Communications	Severity: 25	Confidence: 25

Детальный анализ подозрительных файлов



Не забывайте про разграничение доступа на уровне сети



Authorization Policy At A Glance

First Matched Rule Applies

Standard

Status	Rule Name	Identity Groups	Other Conditions	Permissions
Enabled	Profiled Cisco IP Phones	Cisco-IP-Phone		Cisco_IP_Phones
Enabled	Game_Console	Game_Console-Registered		Game_Console
Enabled	Domain_Computer	Any	demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers AND San_Jose AND CERTIFICATE:Subject Alternative Nam MATCHES .*(demo.local)$ AND Radius:User-Name MATCHES ^(host)	AD_Login
Enabled	Employee-Wired	Any	Employee_Wired AND Posture_Compliant	Employee
Enabled	Employee-Wireless	Workstation	Employee_Wireless AND Posture_Compliant AND LDAP1:badPwdCou MATCHES [0-5]	Employee_Wireless
Enabled	Employee-iPAD	Apple-iPad	Employee_Wireless AND Posture_Compliant AND North_America	Employee_iPAD
Enabled	Contractor-iPAD	Android OR Apple-iPad OR Apple-iPhone OR Apple-iPod OR BlackBerry	Contrator_Wireless AND Posture_Compliant AND North_America	Contractor_iPAD
Enabled	Guest-Wired	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wired AND Posture_Compliant	Guest
Enabled	Guest-Wireless	Guest	Business_Hours AND DEVICE:Device Type EQUALS All Device Types#Wireless AND Posture_Compliant	Guest_Wireless
Disabled	Default-Posture	Any		CWA_Posture_Remediation
Enabled	Default	Any		Central_Web_Auth

5 принципов обнаружения необнаруживаемого

Защита периметра и рабочих станций – это важно!

Это необходимо, но уже недостаточно

Включите и анализируйте NetFlow

Поймите, что у вас значит нормально

Обнаруживайте необнаруживаемое… Заранее

Контролируйте радиоэфир

Мониторьте Wi-Fi, 3G/4G

Идентифицируйте и профилируйте устройства в сети

Вы должны знать, что у вас в сети может быть, а чего нет

Используйте платформы Threat Intelligence

Анализируйте то, что пропускается всеми средствами защиты

Видимость | **Фокус на угрозы** | **Платформы**

Где вы можете узнать больше?

Пишите на security-request@cisco.com

Быть в курсе всех последних новостей вам помогут:

- http://www.facebook.com/CiscoRu
- http://twitter.com/CiscoRussia
- http://www.youtube.com/CiscoRussiaMedia
- http://www.flickr.com/photos/CiscoRussia
- http://vkontakte.ru/Cisco
- http://blogs.cisco.ru/
- http://habrahabr.ru/company/cisco
- http://linkedin.com/groups/Cisco-Russia-3798428
- http://slideshare.net/CiscoRu
- https://plus.google.com/106603907471961036146/posts
- http://www.cisco.ru/

Спасибо