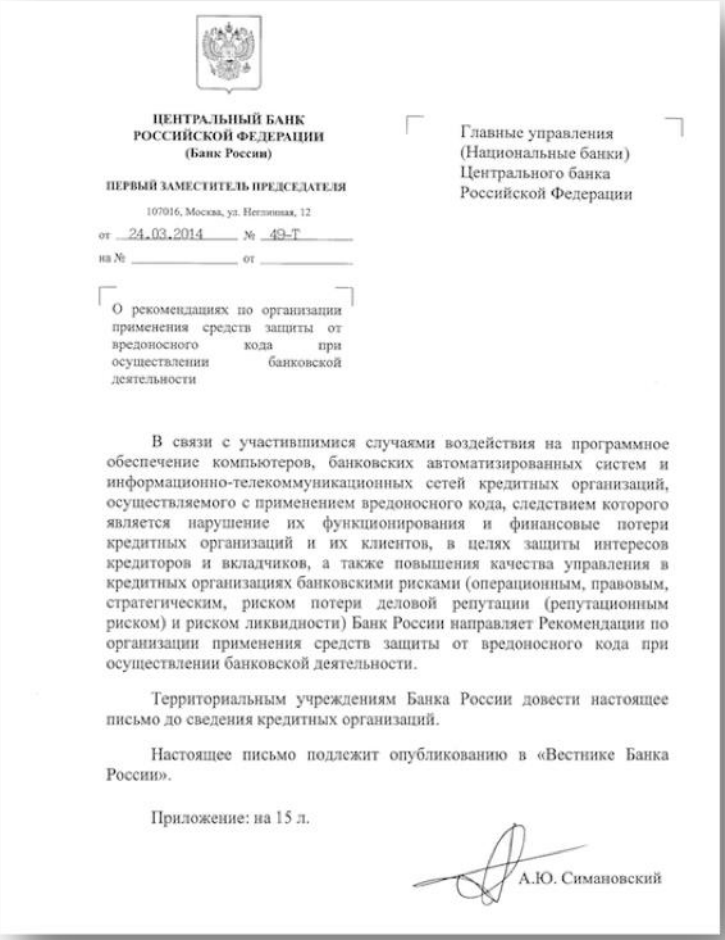
Соответствие решений Cisco требованиям письма Банка России 49-Т

Банк России выпустил письмо 49-Т от 24 марта 2014-го года «О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности». Данное письмо подробно описывает набор организационных и технических мер по защите кредитной организации и ее клиентов от вредоносного кода. По сути данный документ детализирует одноименные высокоуровневые требования, установленные положением Банка России 382-П от 9 июня 2012 года «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» и Комплексом документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».



ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ

107016, Москва, ул. Неглинная, 12

от 24.03.2014 № 49-Т
на № _____ от _____

Главные управления
(Национальные банки)
Центрального банка
Российской Федерации

О рекомендациях по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности

В связи с участившимися случаями воздействия на программное обеспечение компьютеров, банковских автоматизированных систем и информационно-телекоммуникационных сетей кредитных организаций, осуществляемого с применением вредоносного кода, следствием которого является нарушение их функционирования и финансовые потери кредитных организаций и их клиентов, в целях защиты интересов кредиторов и вкладчиков, а также повышения качества управления в кредитных организациях банковскими рисками (операционным, правовым, стратегическим, риском потери деловой репутации (репутационным риском) и риском ликвидности) Банк России направляет Рекомендации по организации применения средств защиты от вредоносного кода при осуществлении банковской деятельности.

Территориальным учреждениям Банка России довести настоящее письмо до сведения кредитных организаций.

Настоящее письмо подлежит опубликованию в «Вестнике Банка России».

Приложение: на 15 л.

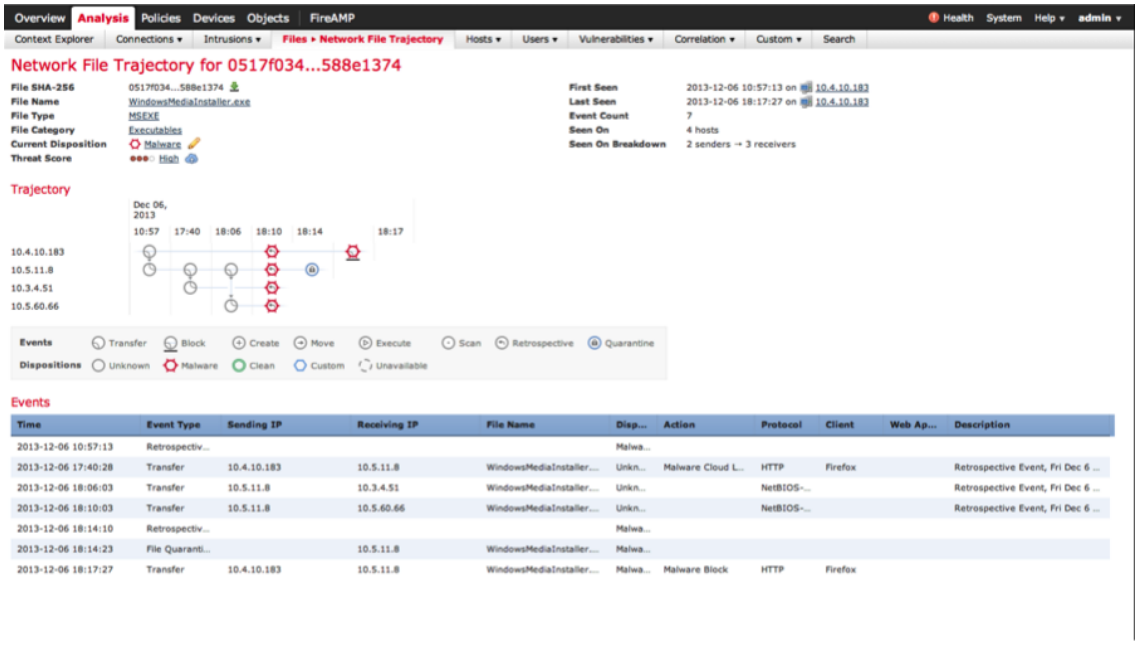
А.Ю. Симановский

Компания Cisco уделяет много внимания теме обеспечения информационной безопасности и, в частности, борьбе с вредоносным кодом, для обнаружения и отражения которого в портфолио Cisco существует немало решений. В первую очередь речь идет о системе Advanced Malware Protection (AMP), которая обеспечивает всестороннюю защиту от известных и неизвестных вредоносных программ. Cisco AMP является платформой, функционирующей на:

- рабочих станциях и серверах под управлением различных операционных систем;

- мобильных компьютерах;
- сетевом шлюзе Cisco AMP Appliance;
- средствах защиты контента E-mail Security Appliance и Web Security Appliance (в виде модуля);
- межсетевом экране следующего поколения Sourcefire NGFW и Cisco ASA (в виде модуля);
- системе предотвращения вторжений Sourcefire NGIPS (в виде модуля).

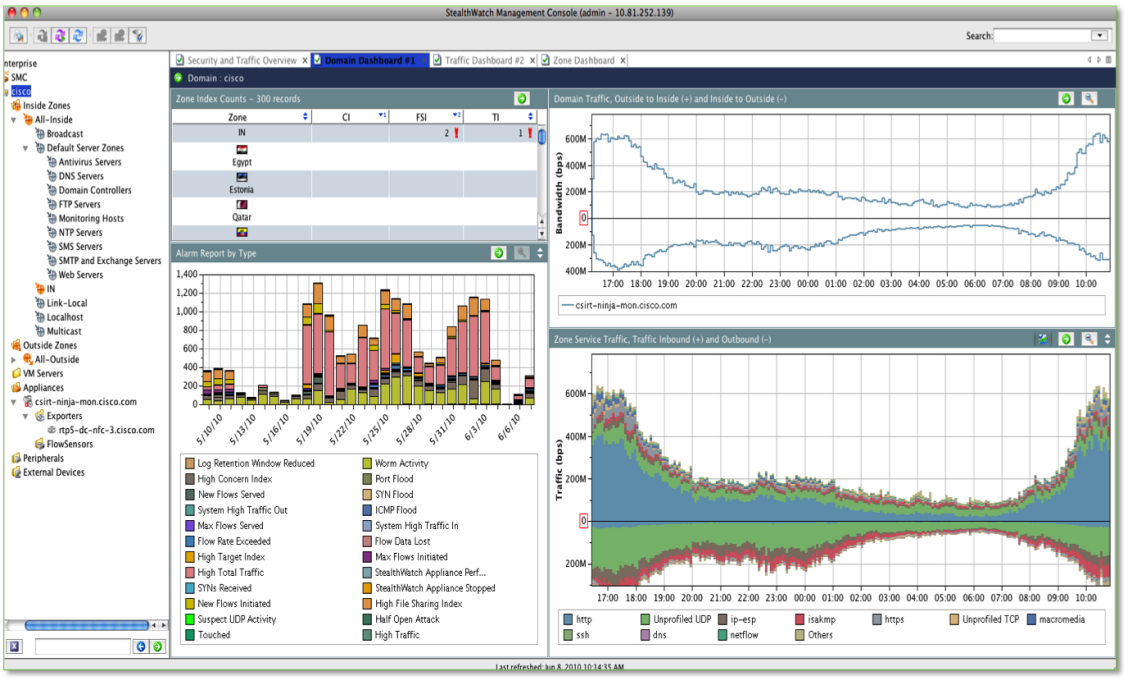
Cisco AMP позволяет выполнить требование 2.1.1 письма 49-Т об установке средств защиты от вредоносного кода на АРМ администраторов, рабочих станциях, файловых серверах, серверах баз данных и приложений, почтовых серверах и Интернет-серверах, межсетевых экранах, а также банкоматах и платежных терминалах.



Контроль вредосноного кода на уровне маршрутизаторов может быть осуществлен тремя путями:

- путем перенаправления проверяемого трафика на соответствующий защитный шлюз с помощью протокола ICAP/WCCP,
- с помощью технологии Application Visibility & Control (NBAR2), встроенной в операционную систему Cisco IOS и позволяющей
  создавать различные сигнатуры для контролируемого трафика,
- с помощью системы анализа аномальной и подозрительной активности Cisco Cyber Threat Defense

(CTD), которая получает с сетевого оборудования анализируемый трафик с помощью протокола Netflow.



Выделенное отдельно требование по обязательной защите электронной почты от вредоносного кода (п.2.1.14) реализуется с помощью решения Cisco E-mail Security Appliance, доступного в виде аппаратного или виртуального устройства, и оснащенного сразу несколькими механизмами обнаружения вредоносных программ во входящих и исходящих почтовых сообщениях:

- Параллельно работающие антивирусные механизмы, использующие сигнатурный принцип работы.
- Механизм Outbreak Filter, позволяющий обнаруживать эпидемии вредоносных программ по мета-данным (дата отправки сообщения, размер и тип вложения, отправитель и т.п.)
- Модуль обнаружения и отражения неизвестного вредоносного кода Advanced Malware Protection.

Все упомянутые решения не только работают в автоматическом режиме (п.2.1.7) и в автоматическом режиме обновляются (п.2.1.13), но и управляются централизованно с помощью систем управления FireSIGHT, Cisco Prime и Cyber Threat Defense соответственно. Частота обновления составляет 3-5 минут.

Упомянутое в п.2.1.23 разделение сети кредитной организации на подсети (сегментация) может быть реализована с помощью большого количества решений Cisco - коммутаторов локальных сетей Cisco Catalyst, сред виртуализации Cisco Nexus и сетей хранения данных Cisco MDS, маршрутизаторов Cisco ISR и ASR, межсетевых экранов Cisco ASA и IOS Firewall, точек и контроллеров беспроводного доступа и других решений.

В п.2.1.26 письма 49-Т говорится о локализации средств и вычислительной техники и объектов инфраструктуры, подвергшихся воздействию вредоносного кода. Эта непростая задача может быть также реализована в автоматическом режиме с помощью следующих решений Cisco:

- Решение Cisco Identity Service Engine (ISE), позволяющее обнаруживать и локализовывать узлы, нарушающие установленные политики безопасности. За счет интеграции Cisco ISE с различными решениями управления событиями безопасности (SIEM) возможно автоматическое блокирование зараженных узлов или пользователей, угрожающих кредитной организации.
- Решение Cisco AMP, обладающее функцией File Trajectory, позволяющей отображать путь распространения вредоносного кода по сети кредитной организации и предпринимать своевременные действия по локализации и недопущению распространения вредоносных программ.
- Решение Cisco Cyber Threat Defense, не только обнаруживающее аномальную и подозрительную активность, являющуюся следствием попадания в сеть вредоносного кода, но и блокирующее ее путем управления настройками сетевого оборудования.

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:badPwdCour 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

Требование об информировании клиентов об угрозах воздействия вредоносного кода и способах борьбы с ним (п.4.2.7) может быть реализован с помощью централизованных информационных сервисов Cisco - Cisco Security Intelligence Operations (SIO), Cisco SenderBase, Cisco IntelliShield, которые позволяют оперативно получать уведомления не только о новых угрозах и уязвимостях в различном программном и программно- аппаратном обеспечении, но и об источниках угрозах.

Дополнительная информация

Для получения дополнительной информации, в том числе и на русском языке, обо всех упомянутых решениях напишите на электронную почту security-request@cisco.com или посетите сайт www.cisco.ru - http://www.cisco.com/web/RU/about/brochures/index.html

Для получения доступа к бесплатным уведомлениям о современных угрозах посетите сайт www.cisco.com - http://www.cisco.com/security.

Для проверки источника угроз или подозрительного сайта, распространяющего вредоносный код, посетите сайт www.senderbase.org - http://www.senderbase.org/

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

Казахстан, 050059, Алматы,
бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, Лэндмарк здание III, 3-й этаж
Телефон: +994-12-437-48-20, факс: +994-12-437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998-71-140-4460, факс: +998-71-140 4465

Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками корпорации Cisco и/или ее дочерних компаний в США и других странах. Чтобы просмотреть список товарных знаков Cisco, перейдите по ссылке: www.cisco.com/go/trademarks. Товарные знаки сторонних организаций, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает наличия партнерских взаимоотношений между Cisco и любой другой компанией. (1110R)