УДК 004.49

ИЗУЧЕНИЕ КОМПЬЮТЕРНОГО ВИРУСА ILOMO / CLAMPI / LIGATS

М. Гончаров, Д. Санчо, Р. Макардл

Тренд Микро

Поступила в редакцию 09.11.2010 г.

Аннотация. Иломо как троян присутствует на просторах сети Интернет с конца 2005 года, являясь долгожителем современной эры вредоносного программного обеспечения. За это время он претерпел заметные изменения, которые позволяют ему оставаться трудно детектируемым для разнообразных антивирусных продуктов. Назначение вируса очень простое – кража конфиденциальной информации (доступ к почте, информация о кредитных картах и доступ к банковским счетам) с компьютеров жертв. Изучение Иломо – это наглядный пример того, каким образом возможно искать пути в борьбе с «умными» вирусами.

Ключевые слова: Иломо, Лигатс, Клампи, Бот Сеть, Ботнет, центр управления сетью; исследования бот сети.

Abstract. Ilomo as a trojan has been present in the malware landscape since the end of 2005, making it a veteran of the modern malware era. During that time it has changed its code constantly with an emphasis being placed on making the malware very difficult to reverse engineer, and also with the goal of staying under the radar. The purpose behind Ilomo is very simple – information theft. Ilomo steals all password details from the infected machine (e.g. those held in protected storage) and also monitors all web traffic from the machine, with the goal of stealing login credentials for online banking, online email accounts and other sensitive information. Research of Ilomo is the good example of how its possible to fight and looking for solutions against permanently changing malware in the wild.

Keywords: Ilomo, Ligats, Clampi; Botnet, Command and Control Server, Botnet research.

ВВЕДЕНИЕ

Иломо присутствует на просторах Интернета с 2005 года и уже является одним из ветеранов новой эры вредоносного программного обеспечения. Цель Иломо проста – хищение персональной информации с компьютера жертвы. Точнее – кража всех возможных учетных записей, хранящихся на зараженном компьютере, а также, что более опасно, прослушивание сетевого трафика и кража учетных записей, паролей к ним и контрольных кодов, используемых для онлайн-банковских операций.

Со дня своего появления код Иломо постоянно претерпевал изменения для усложнения расшифровки и обнаружения антивирусным программным обеспечением. Код программы прошел заметные эволюционные изменения. В настоящее время данный вирус исчисляется, предположительно, сотнями вариантов и известен под именами Ilomo, Clampi и Ligats.

Изучение вариантов Иломо в данной работе было проведено при использовании ограниченного количества вариантов и является попыткой авторов найти особенности данного вируса при работе на лабораторной машине, максимально приближенной к оборудованию обычного пользователя. Основной задачей исследования было получение максимально подробной информации о поведении вируса для последующего использования при подготовке антивирусного программного обеспечения.

1. РАСПОЗНАВАНИЕ ПРИНАДЛЕЖНОСТИ БИНАРНЫХ ФАЙЛОВ К ИЛОМО

Известно, что Иломо относится к вирусным программам типа «Троянский Конь» [1] и распространяется, как и многие другие трояны, путем эксплуатации уязвимости веб-браузеров.

Иломо передается через спам и инфицированные интернет-страницы в виде бинарного файла. Бинарные файлы Иломо, как у некоторых других вирусов, функционально разделяются на 2 типа: дроппер и основной исполняемый файл. Дроппер (от англ. drop – бросать, сбрасывать) производит скачивание основного исполняемого кода файла на машину жертвы для последующего заражения системы. Под заражением системы нужно понимать не только прямое исполнение основного бинарного файла, но и подготовку системы путем изменения реестра, переименования файлов, изменения прав и так далее. Обычно эти два файла (дроппер и основной исполняемый) знакомы антивирусным компаниям и детектируются под различными именами путем сравнивания сигнатур, эвристическим или поведенческим определением.

Некоторые варианты вируса Иломо были исследованы Джо Стюартом, который на конференции Black Hat USA 2009 [2] представил структуру Ilomo как набор модулей жестко привязанных друг к другу. По его мнению, на сегодня существует семь модулей. Значения ключей модулей от «M00» до «M06» обозначают принадлежность бинарного модуля к различным функциональным подсистемам:

– M00 (Codename «SOCKS»): позволяет проводить сетевой трафик третьих лиц через зараженную машину. Данный метод часто используется для оплаты услуг через Интернет краденными кредитными картами для сокрытия местонахождения плательщика. Цель – вызвать подозрение, что именно владелец зараженной операционной системы использует краденые кредитные карты, поскольку именно его сетевые данные (IP Address) сохраняются на стороне серверов, осуществляющих прием к оплате кредитными картами.

– M01 (Codename «PROT»): крадет данные из Windows protected storage (например, пароли к веб-сервисам: email, forums...).

– M02 (Codename «LOGGER»): производит запись всего HTTP POST/GET трафика запросов, идущего к определенному списку веб-адресов.

– M03 (Codename «SPREAD»): скачивает системное приложение PSExec, которое позволяет распространяться между машинами внутри офисной/домашней сети.

– M04 (Codename «LOGGEREXT»): вставляет код в страницы банковских онлайн-операций для получения дополнительной информации о пользователе (логин, пароль, номер транзакции, номер секретного кода для осуществления транзакции, номера кредитовых и дебетовых карт и пин-коды к ним и так далее).

– M05 (Codename «INFO»): получает общую информацию о зараженной машине (сетевые данные, установленное программное обеспечение, конфигурация, антивирусное программное обеспечение) и отправляет на сервера управления для последующей обработки и использования.

– M06 (Codename «ACCOUNTS»): дополнительный дроппер для загрузки на машину различного вредоносного коммерческого программного обеспечения.

В нашем случае при тестировании в лабораторных условиях ряда собранных файлов (семплов) были замечены сходства с ранее известными вариантами Иломо. Лабораторный анализатор, использующий сканирующие модули ведущих антивирусных производителей (Symantec, McAfee, Trend Micro, F-Secure, DrWeb, Microsoft, Kaspersky), определяет эти файлы под именами: TROJ_ILOMO, Win32/Ilomo.BA, Trojan.Win32.Agent2.ekk, Trojan.Clampi. Варианты файлов, определяемых как семейство Иломо, приведены в таблице 1.

2. ОРГАНИЗАЦИЯ ЛАБОРАТОРНОГО ИЗУЧЕНИЯ ИЛОМО

Для анализа выборки файлов Иломо был получен исходный код бинарного файла путем использования технологии реверс-инжиниринга [3] с помощью OllyDbg [4]. Также с целью получения полной картины были использованы лабораторные ресурсы для запуска вирусных файлов на различных версиях платформы Microsoft Windows (как физически, так и виртуально) при определении поведения заражения. Для мониторинга использовались как общедоступные инструменты, так и специализированное программное обеспечение.

Мониторинг проводился как на клиентской (заражаемой), так и на шлюзовой частях. На клиентской части машины предварительно устанавливается операционная система Linux RescueCD [5]. Далее на заранее подготовленное место диска выкладываются снимки операционной системы Windows XP и различных сервисных пакетов для последующего автоматического развертывания (также на заранее

Таблица 1

Варианты файлов (MD5, SHA1) – список файлов, которые использовались для инфицирования лабораторного оборудования

Имя файла	MD5	SHA1	Размер байт	Дата обнаружения
nCdecontainer.exe	d42e6b073d3fcf7c-89ba049a0e6375e6	cbb5279380325d0ffface-fd5b9fac72c3302dcc2d	125952	2009.11.30
uninstall.exe	4b8b532f5b3ab47c-29fdf33917ab11e0	932931746bb2b1c54a38-475c144d87b9a8d40c8a	417792	2009.09.21
sound.exe	61316320065e85ff-4a6a594d7fedf141	197863d7985fc1450406-2fa65a2e2d1db1fbf96c	513024	2009.08.03
virus_made_safe	dff0121c90aada6a-2ae3ef0838913170	de78e3ce0d2eba22436b-12eab30890d20915e4e8	481792	2009.06.01
c.exe	9771ea9dec9b5f9e-071ed9ef7514448f	d26c5393045ac200e420-aaee7ea33bc90e38cb2f	628224	2009.07.26

подготовленную область дискового пространства). Подготовка снимков системы для полной совместимости производится на схожем оборудовании, оптимально – на той же машине. Снимок системы и последующее развертывание производится при помощи программы partimage [6]. После развертывания следуют автоматический перезапуск системы и запуск специального программного обеспечения InstallRight [7]. Затем происходит получение файлов для тестирования (заражения) с внешнего носителя, в нашем случае – с сетевого диска по протоколу smb/samba. Инфицирование тестовой системы, снятие результатов анализа и перезапуск в позицию развертывания производится в циклическом режиме. Автоматизация развертывания системы, получения тестируемых файлов, их инициализация или запуск и перезагрузка системы осуществляется посредством написания скриптов autorun в Linux RescueCD и скриптов управления Microsoft Windows.

На шлюзе устанавливается операционная система SmoothWall [8], которая обладает удобным интерфейсом для контроля сетевой активности. При каждом заражении на шлюзе производится журналирование сетевой активности в реальном времени при помощи ntop. Файл журнала записывается на внешний носитель, в нашем случае – NFS-сервер, для последующего анализа в ручном режиме при помощи программы Wireshark [9].

Приведем основные результаты исследования Иломо.

3. ДРОППЕР (ИЛОМО ИНСТАЛЯТОР)

Как уже было сказано, дроппер выполняет роль инсталятора с функциями доставки файлов на компьютер жертвы, установки их и необходимых для этого изменений реестра.

Первоначально дроппер создает в реестре заражаемой операционной системы (в нашем случае – Microsoft Windows XP SP2 ENG VMWare Guest) запись следующего содержания:

HKCU\Software\Microsoft\Internet Explorer\Settings\GID = “0x00000210”.

Этот ключ в реестре является знаком, что машина заражена вариантом вируса Иломо. По мнению авторов, данная запись указывает версию вредоносного программного обеспечения. Во время тестовых заражений оборудования авторы получили следующие значения: “0x00000210”, “0x0000020D”, “0x0000020C” и “0x0000020B”, которые могут быть истолкованы как версии 2.0.16, 2.0.13, 2.0.12 и 2.0.11, соответственно.

Следующий шаг – добавление в реестр ключа, соответствующего переменной окружения Microsoft Windows XP %APPDATA% для обозначения места расположения основного бинарного файла:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Appdata = “%USERPROFILE\Application Data”.

Как только два приведенных выше условия выполнены, следующий шаг для дроппера Иломо – инсталяция на заражаемую машину основного бинарного файла и создание начальной

точки загрузки файла в систему. Для этого в реестре операционной системы добавляется список файлов и путей к ним:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Run.

Затем из дроппера извлекается бинарный файл и помещается в файловую систему, исходя из значения переменной окружения %APPDATA% и ключа реестра **Run**. Значение, путь и имя файла, скорее всего, случайным образом генерируется дроппером с использованием значения **Run**. На рис.1 приведены данные, полученные при исследовании.

Registry Value	File Name
TaskMon	%APPDATA%\taskmon.exe
System	%APPDATA%\service.exe
EventLog	%APPDATA%\event.exe
Setup	%APPDATA%\msiexeca.exe
Windows	%APPDATA%\helper.exe
Init	%APPDATA%\logon.exe
Svchosts	%APPDATA%\svchosts.exe
Lsass	%APPDATA%\lsas.exe
CrashDump	%APPDATA%\dumpreport.exe
UPNP	%APPDATA%\upnpsvc.exe
Sound	%APPDATA%\sound.exe
RunDll	%APPDATA%\rundll.exe

Рис. 1. Ключи реестра хранения данных вредоносной программы.

Следующим шагом деятельности вредоносного кода является создание в реестре записи, которая хранит важные данные для коммуникации зараженной машины с удаленными сервисами для получения управляющих команд и передачи персональных данных с зараженной машины,

HKCU\Software\Microsoft\Internet Explorer\Settings\Gateslist.

Данные о списке хранятся как значение ключа в шестнадцатеричном формате. При конвертации получается список из примерно 80 адресов, по которым может осуществляться коммуникация. Часть списка приведена на рис. 2.

58.185.113.146/w0tc8xvhSVcan9N8
61.153.3.48/Oc0LWlskOXxqvMHA
64.18.143.52/MldLsmdK1Lsdn5Ka
66.7.197.104/IFQG1NO7bKZj842i
66.96.234.5/Nkl9Sj2NajNgE9Na
66.98.144.21/OjlxuZZWR0rdqg21
66.98.153.17/iZkzNqoPiHeOQaUl
66.98.176.64/FZbD2PHaCNBhbo6Y
66.128.55.82/3kbLJ2Aghp5Tw4Vk
66.199.237.3/9skLsoPfJls4Kks1
66.225.237.140/0AlndjA0dj1lllqq
66.226.76.83/FjFcB74BmllgzEhr
66.240.226.206/5fEBBpqPFNGYGbuH

Рис. 2. Некоторые адреса, по которым осуществляется коммуникация Иломо.

Также дроппер вносит в реестр еще два дополнительных значения в ключе «Internet Explorer\Settings»:

HKCU\Software\Microsoft\Internet Explorer\Settings

“KeyM” = <BLOB OF BINARY DATA>

“KeyE” = “0x00010001”,

для хранения расширений основного файла.

После всего проделанного дроппер Иломо скачивает в зависимости от операционной системы и ее языка дополнительные модули, которые расширяют функциональные возможности основного исполняемого файла. Скачанные файлы помещаются в реестр управления браузером, отвечающий за хранение конфигурационных данных, и сохраняются там в бинарном виде, зашифрованном при помощи симметричного алгоритма шифрования Blowfish [10].

И, наконец, дроппер запускает основной исполняемый файл при помощи API WinExec и завершает свою работу.

4. ОСНОВНОЙ ИСПОЛНЯЕМЫЙ ФАЙЛ (ИЛОМО ТРОЯН)

Основной исполняемый файл является ядром вредоносной программы. Первое, что делает основной исполняемый файл Иломо, создает mutex-запись. Это процедура, гарантирует, что на операционной системе будет работать только одна копия программы. Для Иломо значение mutex всегда выглядит так:

Global\\QYWBUUMFRMUZSPV.

Основной целью Иломо, как уже было заявлено, является кража персональной информации с машины жертвы. Очевидно, что все вышеупомянутые модули Иломо в большей или меньшей степени предназначены для достижения этой цели. Однако в ходе описываемого исследования подгружался лишь модуль, имеющий активность, схожую с модулем M04. Обнаружить и исследовать другие дополнительные модули не представилось возможным.

Подгружаемый в данном случае модуль осуществляет вставку в скрытое окно браузера. Перед данной операцией запущенный бинарный файл производит проверку системы на совместимость. Доказательством тому служит проверка вирусом Иломо системы на присутствие в ней браузера Internet Explorer посредством запроса CLSID:

0002DF01-0000-0000-C000-00000000-0046.

После проверки совместимости с системой Иломо приступает к основным действиям. Сначала вставляется (инжектируется) код в скрытый процесс Internet Explorer. Процесс находится в состоянии спящего ожидания (Suspended Mode) с невидимым окошком. Необычным является способ, при помощи которого осуществляется запуск данного процесса через командную строку (Рис.3).

Рис. 3. Командная строка инжектирования Иломо в процесс Internet Explorer.

На первый взгляд данный набор символов выглядит как случайно сгенерированное значение, направляемое в iexplore.exe (кстати, из данного примера видно, откуда такое странное имя у данной вредоносной программы). Эксплуатируемая здесь техника частично объясняет причины использования командной строки и аргументов для запуска копии программы из командной строки. API **CreateRemoteThread** создает выделенный поток в ячейке памяти **0x7C812F1D**, которая относится к уже запущенному спящему процессу, о котором мы упомянули ранее. Детальное изучение данного адреса памяти показывает, что это функция **GetCommandLineA**, относящаяся к функциям ядра системы и портированная в нашем случае в память Internet Explorer. **GetCommandLineA** возвращает указатель на переменную, которая используется как параметр для текущего процесса. В нашем случае это приведенный выше набор символов. При более тщательном изучении можно увидеть, что это shell-код. Иломо использует необычный способ для инжектирования его в область памяти, используемую Internet Explorer. Можно представить процесс пошагово:

1. Основной исполняемый файл вызывает функцию CreateRemoteThread по адрресу 0x004A23DC, передавая некоторое значение (в нашем случае 0x0D, 0x31, и так далее).

2. Созданный поток вызывает функцию CreateFileMapping, которая создает – маппирует файл со случайным именем.

3. Поток вызывает функцию MapViewOfFile, которая возвращает адрес по маске 0x00CX0000 (где X значения 2,3,4 или 5).

4. Основной исполняемый файл вызывает функцию ReadProcessMemory с параметром (например, 0x00C20000) и возвращает 21 байт данных, из которых первые 8 байт – случайное имя обьекта FileMapping (шаг 2), затем 1 байт со значением 0x00, 4 байта с адресом 0000C200, еще 1 байт со случайным значением и, наконец, 7 байт со значением 00 00 00 5D 24 4A 00.

После процесса инжектирования необходимо произвести манипуляции для успешного запуска инжектированного кода. Для этого основной исполняемый файл использует адрес памяти, возвращаемый при использовании упомянутой ранее функции GetCommandLine. Далее он производит дополнительный запуск потока для исполнения ранее инжектированного shell-кода.

5. КОММУНИКАЦИЯ ИЛОМО С УПРАВЛЯЮЩИМ СЕРВЕРОМ

Коммуникация Иломо с сетью происходит посредством HTTP-протокола (порт 80) и зашифрованного потока данных. Для начала производится определение IP-адресов доменов

admin.viennaweb.at
drugs4sale.loderunner.in
webmail.re-factoring.cn

путем обращения к DNS-серверу, используемому операционной системой по умолчанию. После этого вредоносная программа пытается отправить HTTP-запрос на авторизацию серверу управления. Если обратить внимание на код, который посылается серверу для авторизации, то можно увидеть, что закодированный запрос состоит из изменяемых от запроса к запросу и статичных частей (рис. 4). Разберем запрос на составные части.

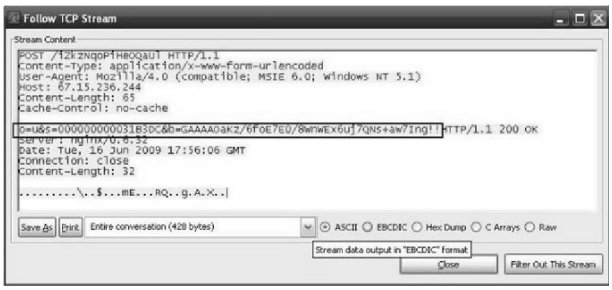

Рис.4 Пример обмена данными между зараженным клиентом и сервером управления.

Набор символов (в нашем случае / **iZkzNqoPiHeOQaul)**, следующий за командой

POST, является уникальным кодом сервера, куда обращается клиент вредоносной программы. Данный набор символов статичен до того момента, пока не будет изменен сервер запросов. Список серверов, обслуживающих бот-сеть Иломо, можно найти в таблица 2.

В рамке обозначен набор команд, посылаемых серверу:

1) значение параметра «o» обозначает, какую операцию клиент запрашивает у сервера:

– «u» используется для запроса на обновление данных,

– «c» используется для отправки инструкции keep-alive;

2) значение параметра «s» – уникальный идентификатор зараженной машины;

3) значение параметра «b» – данные коммуникации.

Путем визуального анализа, реверс-инжиниринга и выборочной обработки HTTP запросов удалось обнаружить, что для шифрования коммуникации используется алгоритм Blowfish с 448-битным ключом сессии. Эти ключи заранее согласованы как на клиентской, так и на серверной стороне при использовании 2048 RSA-шифрования для обмена ключами [11]. Первым этапом обмена информацией является запрос клиента на обновление списка серверов, которые отвечают за коммуникацию клиент-сервер. Как уже отмечалось ранее, список GatesList хранится в реестре операционной системы.

Иломо производит мониторинг веб-адресов, посещаемых клиентской машиной. Для этого на клиентской стороне производится подсчет CRC32 хостов и портов обращений, и чексуммы отправляются для проверки на сервер управления. Если чексумма присутствует в списке на сервере, он сообщает клиенту о необходимости записи всех действий (попытки входа, введенные логины и пароли, секретные коды транзакций) клиентской машины и передачи данных на сервер, в противном случае журналирование не производится. Авторам удалось получить список из 4600 веб-адресов, которые были «интересны» данной вредоносной программе. Некоторые веб-адреса из этого списка можно найти в табица 3.

Таблица 2

Список серверов по стране нахождения и имени провайдера, с которыми осуществлялась коммуникация зараженного лабораторного оборудования (зараженных клиентов)

IP	CIDR провайдера	Имя провайдера	Страна
202.181.96.87	202.181.96.0/21	SAKURA-NET	JP
	202.181.104.0/22		
207.218.248.49	207.218.192.0/18	NETBLK-THEPLANET-BLK-EV1-1	US
207.44.162.2	207.44.128.0/17	NETBLK-THEPLANET-BLK-EV1-9	US
207.44.240.22			
208.100.14.127	208.100.0.0/18	STEADFAST-2	US
208.116.50.186	208.116.0.0/18	FORTRESSITX	US
208.66.43.161	208.66.40.0/21	SPIDER-1	US
209.62.7.178			
209.85.100.7	209.85.0.0/17	NETBLK-THEPLANET-BLK-EV1-15	US
209.85.112.10			
209.85.120.100			
209.85.66.220			
216.55.142.115	216.55.128.0/18	ABAC1999A	US
216.55.190.49			
216.86.152.211	216.86.144.0/20	STEADFAST-1	US
217.172.172.98			
58.185.113.146	58.185.113.144/28	KARCHER-SG	SG
61.153.3.48	61.153.3.0/24	HANGZHOU-IDC-CENTER	CN
64.18.143.52	64.18.128.0/19	RVB-NTBLK-1	US
66.128.55.82	66.128.48.0/20	GIP-NET-1	US
66.199.237.3	66.199.224.0/19	NETBLK-EZZI	US

Окончание таблицы 2

IP	CIDR провайдера	Имя провайдера	Страна
66.225.237.140	66.225.237.0/24	HOSTFORWEB-3	US
	66.225.238.0/24		
66.226.76.83	66.226.64.0/19	ABAC2002A	US
66.240.226.206	66.240.192.0/18	CARI-2	US
66.7.197.104	66.7.192.0/19	DIMECNET	US
66.96.234.5	66.96.192.0/18	NOC	US
66.98.144.21	66.98.128.0/17	NETBLK-THEPLANET-BLK-EV1-11	US
66.98.153.17			
66.98.176.64			
67.15.136.169	67.15.136.128/26	EVRY-81	ES
67.15.150.130			
67.15.161.131	67.15.161.128/28	EVRY-133	JO
67.15.236.244	67.15.236.240/28	EVRY-262	US
69.30.254.66	69.30.254.64/29	WII-1378-01	IN
69.57.140.18	69.57.128.0/19	NETBLK-THEPLANET-BLK-EV1-12	US
69.94.138.140	69.94.128.0/19	DATANOC	US
70.84.236.194	70.84.0.0/14	NETBLK-THEPLANET-BLK-13	US
72.233.28.167	72.232.0.0/16	LAYERED-TECH-	US
	72.233.0.0/17		
72.29.66.235	72.29.64.0/19	HOSTDIME-PI-1	US
72.29.87.61			
78.108.183.225	78.109.29.128/29	VDSWIN20	UA
78.109.29.129			
78.109.31.54			
78.47.61.232	78.47.61.224/27	ALEXANDER-RUZHENTSEV	DE
82.150.65.102	82.150.64.0/19	DK-POWERLINE-20030818	DK
83.175.218.163	83.175.218.160/29	PSOE-VALENCIA	ES
83.223.180.71	83.223.176.0/20	CABOTVM	PT
84.16.229.188	84.16.228.0/23	NETDIRECT-NET	DE
87.118.101.27	87.118.96.0/19	DE-KEYWEB-III	DE
91.121.100.128	91.121.64.0/18	OVH	FR
92.48.96.229	92.48.96.224/29	Poundhost-3679	GB
94.75.221.70	94.75.221.0/24	LEASEWEB	NL

Таблица 3

Список веб-адресов (например, начинающихся на букву «b»), при запросе к которым осуществлялась кража персональных данных

bancorio.com.ar	bankofscotlandhalifaxonline.co.uk
bancosantander.com.co	bankpass.it
banesco.com	bankphb.com
banesconline.com	bankpuliabas.it
banesto.es	bankrcb.com
bangkokbank.com	banksa.com.au
banguat.gob.gt	bankserv.com
banka-celje.si	banksinopac.com.tw
banka-koper.si	banksnb.com
bankalbilad.com.sa	banksterling.com
bankalfalah.com	bankwest.com.au

Окончание таблицы 3

bankboubyan.com	banquebcp.fr
bankbps.pl	banque-casino.fr
bankcardservices.co.uk	banque-chaix.fr
bankdirect.com	banque-france.fr
bankfirst.com	banquelaurentienne.ca
bankhapoalim.com	banquemisr.com.eg
bankhost.com	banquemondiale.org
bankinter.com	banquepopulaire.fr
bankmandiri.co.id	banrep.gov.co
bankmuscat.com	banreservas.com.do
bankmuscatonline.com	bapro.com.ar
bankmw.com	barclays.com
bankniaga.com	barclays.co.uk
bankofamerica.com	barclays.es
bankofbaroda.com	barclays.fr
bankofbermuda.com	barclays.pt
bankofcyprus.com	batelco.jo
bankofcyprus.co.uk	bayfed.com
bankofgreece.gr	bbandt.com
bankofny.com	bbkonline.com
bankofscotland.co.uk	bbvabancocontinental.com

Ручная проверка заражения Иломо

При обнаружении следующих изменений/следов на клиентской машине можно с большой достоверностью утверждать, что клиент заражен одной из разновидностей Иломо:

Ключи реестра:

· HKCU\Software\Microsoft\Internet Explorer\Settings\GID

· HKCU\Software\Microsoft\Internet Explorer\Settings\Gateslist

· HKCU\Software\Microsoft\Internet Explorer\Settings\

Переменные окружения:

· ILOMOIAJAAAAAAJAJAJAJAJAJAJAJAJAF (нарпавляемые к IEXPLORER)

· C:\Windows\System32\cmd.exe /c dir /s c:\Windows>nul && del [место инсталятора]

Сетевое поведение:

Отправляется зашифрованный HTTP трафик на адрес (в нашем случае 216.55.137.46/M1JJ9znqqoFqAKpy) и используется POST метод отправки параметров “o”, “s” и “b”

В процессе изучения Иломо не было замечено сетевой активности типа «червь», при которой вредоносное программное обеспечение может распространяться по сетевым ресурсам окружения.

СПИСОК ЛИТЕРАТУРЫ

1. Carnegie Mellon University (1999): “CERT Advisory CA-1999-02 Trojan Horses”.

2. *Joe Stewart* Black Hat USA 2009 – Clampi Trojan stealing online bank information.

3. *Warden R.* (1992). Software Reuse and Reverse Engineering in Practice. London, England: Chapman & Hall.

4. Eilam, Eldad (2005). Reversing: Secrets of Reverse Engineering OllyDBG. Wiley Publishing. p. 595.

5. RescueCD http://www.sysresccd.org.

6. Partimage http://www.partimage.org/.

7. InstallRight http://www.epsilonsquared.com/.

8. SmoothWall Gateway http://www.smoothwall.org/.

9. Orebaugh, Angela; Ramirez, Gilbert; Beale, Jay (February 14, 2007), Wireshark & Ethereal Network Protocol Analyser Tool-kit, Syngress, pp. 448, ISBN 1597490733.

10. Алгоритм Blowfish. Максим Парыгин http://www.javable.com/columns/crypto/algorythms/01/index.pdf

11. RSA http://www.rsa.com.

Максим Гончаров – старший вирус-аналитик, фирма Тренд Микро, Мюнхен Германия. E-mail: max_goncharov@trendmicro.de

Дэвид Санчо – старший вирус-аналитик фирма Тренд Микро. Корк Ирландия. E-mail: david_sancho@trendmicro.ie

Роберт Макардл – старший вирус-аналитик фирма Тренд Микро. Корк Ирландия. E-mail: robert_mcardle@trendmicro.ie

Maxim Goncharov – Senior Threat Researcher. Trend Micro GmbH. Munich, Germany. E-mail: max_goncharov@trendmicro.de

David Sancho – Senior Threat Researcher. Trend Micro Inc. Cork, Irland. E-mail: david_sancho@trendmicro.ie

Robert McArdle – Senior Threat Researcher. Trend Micro Inc. Cork, Irland. E-mail: robert_mcardle@trendmicro.ie