Автор: Артур Скальский  РАССЛЕДОВАНИЯ, МИР 

# Хакеры переходят от криминала к терроризму

Компьютерная преступность переходит от киберкриминального этапа к кибершпионскому и кибертеррористическому. На смену идее массового заражения приходит концепция точечного удара.

Однако это не означает, что персональные компьютеры перестали интересовать сетевых мошенников. К таким выводам пришли аналитики «Лаборатории Касперского» в отчете по информационным угрозам за третий квартал текущего года.

По мнению специалистов антивирусной лаборатории, одним из самых важных и интересных событий третьего квартала 2010 года в мире IT-безопасности стали атаки червя Stuxnet. Напомним, вредоносная программа Win32/Stuxnet, предназначенная для атак на программное обеспечение класса SCADA производства компании Siemens AG — систем управления и контроля, используемых в промышленности, была обнаружена в июле текущего года. Первый случай проникновения Stuxnet на компьютеры с приложениями SCADA, которые обычно не соединены с Интернетом, был выявлен 14 июля в Германии.

Тревога, вызванная появлением червя Stuxnet, была столь сильной, что Департамент национальной безопасности США создал 4 экспертных группы для оценки слабых мест в промышленных системах управления. Бюджет, выделенный на работу экспертов, составил 10 миллионов долларов, а в следующем году его планировали увеличить до 15 миллионов.

Червь Stuxnet до сих пор приковывает внимание экспертов по безопасности из разных стран, и на это есть причины. Одна из них — компоненты червя имели действующие цифровые сертификаты, то есть, вирусописателям удалось где-то «позаимствовать» закрытые ключи электронных цифровых подписей (ЭЦП) известных компаний.

После анализа действий червя эксперты пришли к выводу, что Stuxnet создан специально для промышленного шпионажа и, теоретически, может использоваться для осуществления диверсий. Основная его задача, по данным «Лаборатории Касперского», изменить логику работы контроллеров (Simatic PLC) в частотных преобразователях, которые используются для контроля скорости вращения двигателей. Причем эти контроллеры работают с очень высокоскоростными двигателями, для которых существует небольшое количество применений — например, в центрифугах.

Несмотря на то, что эксперты не сомневаются в целенаправленности создателей Stuxnet, цель атаки до сих пор точно не установлена. Аналитики «Лаборатории Касперского» объясняют этот факт тем, что организации, против которых направлены такие атаки, крайне редко публикуют информацию о нападении, так как это может негативно сказаться на их репутации. А это, в свою очередь, мешает антивирусным компаниям проанализировать поведение вредоносной программы в зараженной системе.

По официальной статистке Siemens, на начало сентября было известно о заражении 15 промышленных систем SCADA по всему миру.

## Пользователям ПК не стоит расслабляться

Повышенное внимание к вредоносным программам, направленным на промышленные предприятия, вовсе не означает, что пользователям домашних компьютеров можно забыть об угрозах.

В течение третьего квартала в Kaspersky Security Network (KSN) было зафиксировано более 600 миллионов попыток заражения компьютеров пользователей вредоносными и потенциально нежелательными программами, что на 10% больше, чем в предыдущем квартале. На вредоносные программы пришлось около 535 млн всех обнаруженных объектов.

По данным «Лаборатории Касперского», 83% площадок, используемых для распространения вредоносных

программ, находится в 10 странах мира. США, Китай и Россия по-прежнему в тройке «лидеров».

С интернет-ресурсов, расположенных в разных странах, в третьем квартале было совершено более 156 млн атак. Заражение может произойти как по вине самого пользователя, если он кликнет по непроверенной ссылке, так и незаметно для него — с помощью техники drive-by загрузки, основанной на использовании эксплойтов. Причем больше всего попыток заражения компьютеров пользователей вредоносными программами из Интернета было выявлено в России — атакам подверглись 52,8% компьютеров.

Самыми «активными» вредителями по-прежнему остаются всевозможные «троянцы». Второе место занимают черви, среди которых особо «шустрыми» стали Worm.Win32.FlyStudio.cu, Worm.Win32.Mabezat.b, Worm.Win32.VBNA.b и Worm.Win32.Autoit.xl. На третьем месте семейство Trojan-Downloader.

Самым значимым изменением в списке платформ, на которых выполняются обнаруженные в Интернете вредоносные программы, стало появление в нем мобильной ОС Android. Первая в мире вредоносная программа класса Trojan-SMS под названием FakePlayer для смартфонов на базе Android была обнаружена в августе текущего года.

По мнению специалистов «Лаборатории Касперского», в настоящее время мир переживает новый виток развития вирусописательства. На смену идее массового заражения, как это было с червями Klez, Medoom, Sasser, Kido и т.п., приходит концепция точечного удара. При этом значительно повысился уровень вредоносных технологий.

В перспективе на ближайшее время аналитики прогнозируют увеличение количества вирусных инцидентов, связанных с подписанными вредоносными файлами — с украденными цифровыми подписями.

Автор: Артур Скальский © BFM.RU РАССЛЕДОВАНИЯ, МИР 3473 07.12.2010, 11:21 450
URL: https://babr24.com/?ADE=90179 Bytes: 5071 / 5062 Версия для печати

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

**ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:**

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

**СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:**

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта