Сетевые угрозы

В текущем году исполнилось 45 лет с момента зарождения Интернета, который способствовал ускорению развития практически всех технологий.

Число объектов, подключенных к Сети, достигло 4 млрд. Только число web-сайтов составило 625 329 303 (*рис. 1*).

В 2012 г. доходы киберпреступников превысили доходы от наркотрафика. Формируются кибермии, разрабатывается кибероружие (APT). Для создания государственных botnet часто сознательно заражаются сайты государственных учреждений.

Компания *Symantec* ежедневно детектирует около 73 тыс. файлов, содержащих вредоносные коды. Точное число атак разных видов неизвестно, но оно исчисляется десятками миллионов.

Далее приводится список наиболее опасных видов (этот перечень постоянно изменяется и пополняется):

- APT (advanced persistant threat) — один из основных видов кибероружия;
- Phishing (кибермошенничество);
- Троянский конь — кража конфиденциальных данных;
- SQL-injection — вторжение на сайты, использующие реляционные базы данных;
- Drive-by-download — взлом машины при посещении вредоносного сайта;
- DDoS — блокировка доступа к сайтам;
- CSS/CSRF (Cross-Site Request Forgeries);
- атаки нулевого дня — неизвестные пока атаки и по этой причине крайне опасные;
- подмена субдомена DNS, автоматическая переадресация на вредоносный сайт;
- вирус/червь;
- Google injection — использование для атаки результатов поиска.

Для создания вредоносных программ привлекаются высокооплачиваемые специалисты. Среди актуальных направлений — банковские атаки (интернет-банкинг), управление большими бот-сетями и разработка новых атак нулевого дня.

Выявление факта атаки достаточно непростая работа. Разные виды атак требуют разных усилий (*рис. 2*).

Среднее время жизни атаки нулевого дня составляет около 300 дней. Процветающим криминальным бизнесом в России являются заказные DDoS-атаки интернет-магазинов (доход одного из школьников, который занялся этой деятельностью, составил около 1 млн долл. в год).

Семенов Юрий Алексеевич — начальник Лаборатории инфокоммуникационных технологий Института теоретической и экспериментальной физики МФТИ, кандидат физико-математических наук, доцент.

Доклад был сделан 30 ноября 2012 г. на конференции, посвященной памяти Сергея Петровича Капицы, которая состоялась в Российском новом университете.

В последние десять лет многообразие вредоносных кодов увеличивалось на 50% ежегодно.

В 2012 г. 53% компаний считали, что надежность и безопасность сети важнее, чем производительность или адаптивность.

В докладе 2012 WEB Security Report (Blue Coat) сообщается об увеличении числа вредоносных сайтов на 240%, в среднем любая организация сталкивается с 5000 новыми угрозами каждый месяц.

Благодаря полиморфности детектируется только 24% всех вредоносных кодов, что облегчает APT-атаки.

В день появляется 50 000 новых сигнатур в дополнение к 6–20 млн уже известных. Более тысячи различных типов атак угрожает смартфону или планшету. Новой атаки можно ожидать каждый день.

Средняя стоимость киберпреступления в 2012 г. выросла на 40% по сравнению с 2011 г. Число успешных атак достигло 102 в неделю (против 72 в 2011 г. и 50 — в 2010 г.).

Гари Дэвис (Gary Davis) из фирмы McAfee привел пример, когда система водоснабжения Южной Калифорнии наняла хакера проверить надежность ее сети управления. Хакер за час добился доступа и полного контроля над системой и осуществил добавление оговоренных химических веществ в воду. Это показывает, насколько уязвимы современные системы управления.

На *рис. 3* представлено типичное географическое распределение хакеров.

Поток атак сети Межведомственного суперкомпьютерного центра РАН в пике достигает 65 тыс. в час. Ниже показан пример распределения источников атак МСЦ РАН (*рис. 4*). ЭС

ПЭС 13029/12.02.2013

Рисунок 1

Рост числа узлов в 1994–2012 гг.

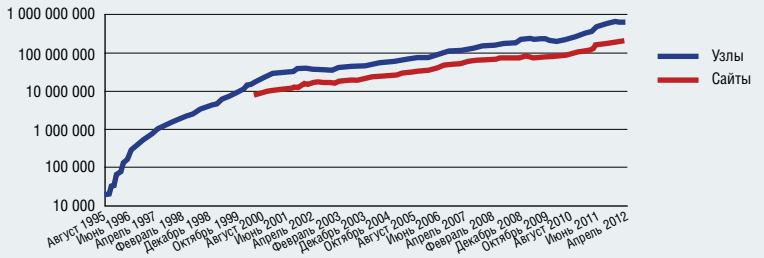

Рисунок 2

Число дней для выявления атаки

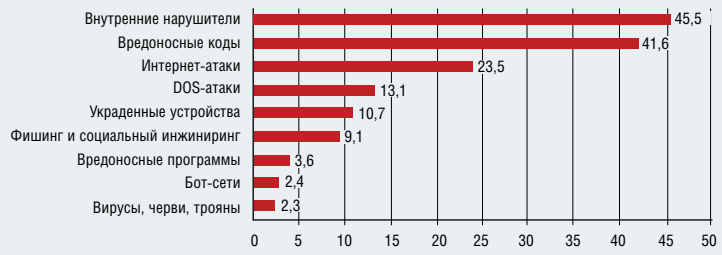

Рисунок 3

Географическое распределение IP-адресов атакеров

Рисунок 4

Географическое распределение атак сети МСЦ РАН