Trend Micro™

ИНИЦИАТИВА НУЛЕВОГО ДНЯ™

Продвижение скоординированного раскрытия уязвимостей посредством крупнейшей в мире независимой от вендоров программы Bug Bounty

В сфере информационной безопасности по-прежнему существует мнение, что исследователи уязвимостей — это хакеры-злоумышленники. Безусловно, среди таких специалистов есть и те, кто использует свои знания со злым умыслом, однако они составляют очень незначительное меньшинство. В действительности же очень велико количество этичных исследователей, обладающих достаточной квалификацией для обнаружения программных уязвимостей. Они нередко находят новые ошибки в рамках своей повседневной работы по обеспечению безопасности.

Согласно Gartner, *«вендоры систем предотвращения вторжений (IPS) должны обладать исследовательским потенциалом, чтобы анализировать основные и второстепенные угрозы и уязвимости. Это основополагающая возможность, которая позволяет вендорам полностью разобраться в принципах использования уязвимостей и, следовательно, эффективно реагировать на угрозы для вашей организации. Один из критериев оценки вендоров — способность защитить клиентов от уязвимостей раньше, чем они были использованы злоумышленниками. Для этого необходимо инвестировать в исследования».*[1]

Решение Trend Micro™ TippingPoint™ работает на базе собственной исследовательской лаборатории мирового уровня Digital Vaccine® Labs (DVLabs), однако было целесообразно дополнить возможности DVLabs анализом угроз нулевого дня от команды Trend Micro Research, нашей глобальной сети «внешних исследователей». В результате 25 июля 2005 г. была создана программа «Инициатива нулевого дня» (Zero Day Initiative, ZDI).

Основные цели Инициативы нулевого дня:

- расширять возможности внутренних исследовательских команд с помощью методологий, опыта и времени внешних специалистов;
- стимулировать исследователей — через программы финансового поощрения — делиться с пострадавшими вендорами информацией об уязвимостях нулевого дня;
- защищать клиентов Trend Micro/TippingPoint в то время, как пострадавший вендор работает над пакетом исправлений.

Ключевые факты

- Основана в 2005 г.
- Более 10 000 исследователей по всему миру
- Более 6 500 уязвимостей обнаружены и раскрыты для общественности
- Более 25 млн долл. выплачено исследователям
- Мировой лидер в сфере исследования и обнаружения уязвимостей с 2007 г[2]
- Организован новый хакатон Pwn2Own™ Miami с упором на поиск уязвимостей систем ICS/SCADA

Статистика за 2019 г.

- Обнаружено **38 %** всех обнародованных уязвимостей **Microsoft®**
- **#1** внешний поставщик ошибок для Microsoft
- бнаружено **57 %** всех обнародованных **уязвимостей Adobe®**
- **#1** внешний поставщик ошибок для Adobe
- **1 045** уязвимостей опубликовано
- **Более 1,5 млн долл.** присуждено исследователям

РЫНОК УЯЗВИМОСТЕЙ

Рынок уязвимостей информационной безопасности работает как и любой другой мировой рынок: есть покупатели и продавцы, спрос и предложение. Если раньше хакеры обменивали и продавали эксплойты друг другу, чтобы доказать свое превосходство, нарушить традиционные процессы управления ИТ и разработки ПО, а также время от времени обогатиться нечестным путем; то теперь у них и исследователей безопасности есть множество вариантов использования обнаруженных ошибок.

БЕЛЫЙ РЫНОК

Программы Bug Bounty, хакатоны и прямая коммуникация с вендорами создают возможности для ответственного раскрытия уязвимостей.

СЕРЫЙ РЫНОК

Некоторые официально действующие компании работают в серой зоне рынка уязвимостей нулевого дня: продают эксплойты правительствам и правоохранительным органам разных стран мира.

ЧЕРНЫЙ РЫНОК

Уязвимости могут быть проданы покупателю, предложившему наивысшую цену, и использованы против частных или публичных лиц и групп.

Инициатива нулевого дня стала первым шагом к созданию «белого рынка» уязвимостей, который призван подорвать функционирование черного рынка путем законной покупки исследований ошибок, которые затем могут быть раскрыты пострадавшим вендорам. В результате уязвимости покидают рынок, не попадают в руки потенциальных злоумышленников, а вендоры получают возможность устранить ошибку до того, как информация о ней будет обнародована. Инициатива нулевого дня предлагает пострадавшим вендорам скоординированное раскрытие уязвимостей (на основе программы вознаграждения исследователей) для предотвращения неожиданных атак на корпоративные среды.

КАК ЭТО РАБОТАЕТ?

В то время как команда ZDI проводит собственные внутренние исследования, сообщество внешних «охотников за ошибками» по-прежнему остается ценным активом программы. Сумма, предлагаемая исследователю за обнаружение конкретной уязвимости, зависит от следующих критериев:

- Широко ли распространен уязвимый продукт?
- Может ли использование ошибки привести к компрометации сервера или клиента? На каком уровне привилегий?
- Была ли уязвимость выявлена в конфигурациях/установках по умолчанию?
- Критичны ли уязвимые продукты *(например, базы данных, серверы онлайн-магазинов, DNS-серверы, маршрутизаторы, межсетевые экраны, системы ICS/SCADA и т. д.)?*
- Нужно ли злоумышленнику прибегать к социальной инженерии *(например, вынуждать пользователя перейти по ссылке, зайти на сайт, подключиться к серверу и т. д.)?*

- **Информация об уязвимости передана:** исследователь передает информацию о незакрытой уязвимости команде ZDI, которая проверяет уязвимость, определяет ее значимость и предлагает исследователю соответствующее вознаграждение.
- **Вендор уведомлен:** команда ZDI ответственно и оперативно информирует соответствующих вендоров о проблемах безопасности, обнаруженных в их продуктах или услугах.
- **Фильтр Digital Vaccine® создан:** одновременно с информированием вендора команда Trend Micro TippingPoint разрабатывает фильтр Digital Vaccine для защиты клиентов от незакрытой уязвимости.
- **Ответ вендора:** в рамках Инициативы нулевого дня у вендора есть четыре месяца, чтобы принять меры в отношении уязвимости.
- **Уязвимость закрыта или по-прежнему не исправлена:** вендор должен выпустить пакет исправлений или сообщить команде ZDI о невозможности или отсутствии намерений закрыть уязвимость.
- **Публичное раскрытие информации:** команда ZDI осуществляет ответственное раскрытие информации об уязвимости на сайте программы в соответствии с политикой раскрытия уязвимостей.

В 2019 году благодаря эксклюзивному доступу к информации об уязвимостях, обнаруженных Инициативой нулевого дня, клиенты Trend Micro TippingPoint получали защиту в среднем на 81 день раньше выпуска исправлений вендором *(если вендор вообще выпускал исправления)*. Клиенты защищены во время любой потенциальной массовой атаки, что особенно критично на начальном этапе, когда эксплуатация уязвимости с большой вероятностью затронет пользователей. Кроме того, клиенты могут контролировать процесс установки пакетов исправлений, получая упреждающую защиту в период между обнаружением уязвимости и доступностью исправления.

> *“Pwn2Own — действительно ценная инициатива. Эти соревнования показывают, как разные исследователи пытаются обойти существующие меры снижения рисков, чтобы создать по-настоящему боевой эксплойт. Понимание различных подходов к атакам вдохновляет нас как вендоров на создание инструментов защиты нового поколения.”*[3]

Пелеус Ули (Peleus Uhley),
старший научный сотрудник безопасности, Adobe Systems

МИРОВОЙ ЛИДЕР В СФЕРЕ ИССЛЕДОВАНИЯ И ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ

С 2007 года Инициатива нулевого дня от Trend Micro является ведущей в мире программой исследования уязвимостей по версии компании Frost & Sullivan[4]. На протяжении 12 лет эксперты Frost & Sullivan собирали данные о раскрытых уязвимостях, чтобы определить наиболее надежных поставщиков ошибок. С 2019 года этим исследованием занимается компания IHS Markit (теперь — OMDIA). Ее специалисты отслеживают как сами программные уязвимости, так и организации, которые их раскрывают.

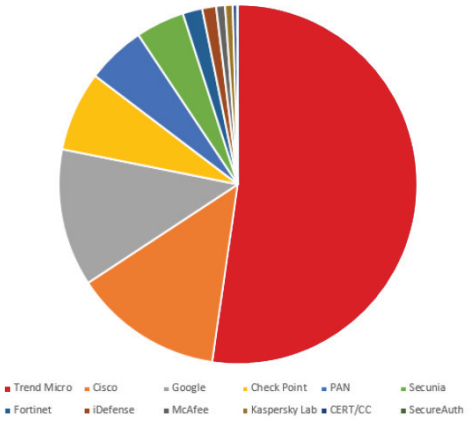
Pwn2Own™

ZDI является спонсором хакатона Pwn2Own с 2007 года. Участники взламывают широко используемые системы и ПО с помощью ранее неизвестных уязвимостей. Цель Pwn2Own — продемонстрировать уязвимости широко используемых устройств и программ, а также оценить прогресс, достигнутый в сфере безопасности за прошедший год. В 2020 году соревнования Pwn2Own прошли в 13 й раз, но впервые в виртуальном формате из-за пандемии COVID-19. Суммарный размер выплат составил 250 тыс. долл.

Pwn2Own™ Tokyo

Хакатон Pwn2Own Tokyo был организован в ответ на расширение поверхности атак на мобильные устройства, умные колонки, телевизоры и NAS-серверы. Ценные данные, хранящиеся на мобильном устройстве, как и любые другие данные, могут быть скомпрометированы непосредственно злоумышленниками или вредоносным ПО. Цель Pwn2Own Tokyo — показать, что уязвимости существуют и могут быть использованы точно так же, как и на более традиционных платформах: компрометация данных через вредоносные загрузки. Главное отличие в том, что пользователи не ожидают таких атак на мобильные платформы или устройства, а следовательно, не меняют свое поведение.

IHS Markit: рынок раскрытия уязвимостей, 2019 г.



КАКОВЫ ПРЕИМУЩЕСТВА ИНИЦИАТИВЫ НУЛЕВОГО ДНЯ ДЛЯ КЛИЕНТОВ TREND MICRO?

Результат исследования уязвимостей и программы Bug Bounty в рамках Инициативы нулевого дня — более безопасные продукты и более защищенные клиенты. Без Инициативы нулевого дня многие уязвимости так и остались бы за закрытыми дверями или были бы проданы на черном рынке и использованы в противозаконных целях.

- Благодаря эксклюзивному доступу к информации об уязвимостях, обнаруженных Инициативой нулевого дня, клиенты получают упреждающую защиту до выпуска исправления вендором, а также дополнительную защиту устаревшего программного обеспечения с истекшим сроком поддержки.
- Наше длительное сотрудничество с ведущими вендорами ПО и исследовательским сообществом продолжает повышать значимость безопасности в жизненном цикле разработки продуктов.

Подробную информацию об Инициативе нулевого дня см. на сайте **www.zerodayinitiative.com**

TREND MICRO™

Securing Your Connected World

Подробную информацию о том, какие персональные данные мы собираем и зачем, вы найдете в Уведомлении о конфиденциальности на нашем веб-сайте:

https://www.trendmicro.com/privacy

1 Gartner, Inc. "Defining Intrusion Detection and Prevention Systems" («Определение систем обнаружения и предотвращения вторжений»). 20 сентября 2016 г.

2 Отчет IHS Markit "Public Cybersecurity Vulnerability Market, 2018" («Открытый рынок уязвимостей кибербезопасности, 2018 г.»)

3 Пелеус Ули (Peleus Uhley). "Reflections on Pwn2Own" («Размышления о Pwn2Own»). Security @ Adobe (блог), 16 апреля 2016 г.

4 Отчет Frost & Sullivan: Analysis of the Global Public Vulnerability Research Market (Анализ глобального рынка исследования уязвимостей)