Автор: Алина Саратова НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2466 19.07.2017, 13:58
9

Wired: ваш гид в инфраструктуру русских команд хакеров

«Русские хакеры» – это словосочетание приводит в трепет всех: от Европы до Америки. Несмотря на нашу техническую государственную отсталость, русские хакеры страшнее всех на свете. В глазах американского обывателя нет страшнее хакеров из России. Масла в огонь подлила газета: Wired, напечатав статью «YOUR GUIDE TO RUSSIA'S INFRASTRUCTURE HACKING TEAMS» о российских хакерских группировках. Сегодня мы предлагаем вам ознакомиться с классификатором русских хакеров по версии Wired.

Поскольку известно, что киберпреступники нацелились на более десяти американских энергетических компаний, в том числе и на АЭС, расположенную в Канзасе, то эксперты по кибербезопасности ищут доказательства, которые помогут установить виновников. Если не знать, кто виноват, то компания не сможет быстро найти причину нападения на ее IT-структуру: или это погоня за наживой, или шпионаж, или проба хакерского «пера» - как это было с уже дважды столкнувшейся с такими атаками Украиной.

Американские чиновники нашли разгадку части тайны киберпреступлений, щедро делясь своими откровениями с Washington Post: хакеры, стоящие за коммунальными атаками на США, работают на российское правительство. Только возникает вопрос: какие именно хакеры из групп Кремля попытались воздействовать на систему электроснабжения США?

Ведь Россия – это единственная страна, в которой работает несколько хакерских группировок, которые много лет нападают на энергопредприятия. У каждой из этих групп – свои методы, своя направленность и мотивация, и расшифровка «почерка» киберпреступников, поможет определить нужное противодействие.

И вот что мы знаем о группах, которые могут это сделать.

Energetic Bear

Первым кандидатом среди российских хакерских групп можно назвать группу кибершпионов, определенных как Energetic Bear. Она еще известна под именами DragonFly, Koala и Iron Liberty. Впервые группа попала в поле зрения охранной фирмы Crowdstrike в 2014 году, когда начала выводить из строя сотни объектов в десятках стран. А в 2010 году эта же группировка, используя так называемый «водопой» атак, заразила множество машин трояном Havex. Вроде бы бесцельное нападение, как оказалось, имело-таки цель: киберпреступники использовали фишинговые сообщения для поставщиков программного обеспечения АСУТП, внедряя Havex. Таким образом, группа разрушила цепи производственного контроля, потенциально давая хакерам доступ к сетке системы питания на производственных предприятиях.

- Эта хакерская группа также настроена на нефтяную и газовую промышленность, - уверяет Адам Майерс, вице-президент компании Crowdstrike. – В цели Energetic Bear входит все: от добытчиков газа до компаний, которые перевозят сжиженный газ и нефть для снабжения предприятий энергетики.

Для доказательства принадлежности группы к русским хакерам, эксперты Crowdstrike также нашли код группы

и артефакты на русском языке, а также то, что часы ее работы совпадают с рабочим временем в Москве. Мейерс утверждает, что эти данные говорят о том, что российское правительство может использовать эту группировку для защиты собственной нефтехимической промышленности, так что для Европы и Америки лучше использовать несколько каналов поставки топлива. «Если вам угрожают отключить газ, который подается в страну, вы будете хотеть знать, насколько серьезна эта угроза и как правильно себя обезопасит», - говорит Мейерс.

Другие эксперты по кибербезопасности уверяют, что вредоносные программы, которые внедряет Energetic Bear, имеют возможность сканирования инфраструктуры и оборудования промышленных сетей. Группа собирает данные для будущих разрушительных атак.

После того, как фирмы, специализирующиеся на кибербезопасности, выпустили серию анализов хакерской группы Energetic Bear летом 2014 года, группа внезапно исчезла.

Sandworm

Аналитики по кибербезопасности полагают, что только одна хакерская структура в действительности смогла отключить сотни тысяч людей от электроснабжения. Это сделала команда под названием Sandworm, также известный как Voodoo Bear и Telebots, напавшая на украинские электросети в 2015 и 2016 годах.

Группировка Sandworm не специализируется на атаках на электроэнергетику или энергетический сектор. Она в последние три года терроризирует Украину, с которой Россия находится в состоянии войны после вторжения в Крым в 2014 году. Группировка с 2015 года бесчинствует практически во всех слоях украинского общества, уничтожив сотни компьютеров в медиакомпаниях, удаляя или навсегда шифруя терабайты данных в госучреждениях и парализуя инфраструктуру, в том числе и по продажам железнодорожных билетов. Расшифровать файлы, зашифрованные группировкой Sandworm, невозможно.

Ряд компаний связывает данную группировку с атаками на американские энергетические компании в 2014 году, когда они были заражены одним и тем же вирусом, который в дальнейшем хакеры использовали в своих атаках на Украину.

С Россией группировку связали на основе русскоязычных документов, найденных на одной из групп командно-управляющих серверов, а также по уязвимости нулевого дня, которую представили на Российской конференции хакеров, и явный фокус внимания группы на Украину.

Palmetto Fusion

Хакеры, которые стоят за свежими попытками вторжений в структуру энергетики и ЖКХ, остаются гораздо более таинственными, чем Energetic Bear или Sandworm. Эта группировка занимается фишинговыми атаками с 2015 года, избрав своей целью такие страны, как Ирландия и Турция. При этом аналитики кибербезопасности еще не нашли доказательств, которые указывали бы на принадлежность этой хакерской группировки к русским командам.

В течение нескольких лет эксперты по кибербезопасности отслеживали работу новой группировки и группы Sandworm, но не нашли общих методов и общей инфраструктуры деятельности. Но, несмотря на это, по словам американских чинов, которые приводит Washington Post, группа Palmetto Fusion используется для оказания секретных услуг русской ФСБ.

Некоторые исследователи считают, что группировка Sandworm работает под эгидой российской военной разведки, известной как ГРУ. Как доказательство своих рассуждений, они приводят ориентированность группы на Украину и ее ранние нападения на НАТО и другие военные организации Европы и США.

Palmetto Fusion, несмотря на заверения некоторых специалистов по кибербезопасности, не является преемницей Energetic Bear. Они не используют те же фактические инструменты и методы, хотя их атаки и очень похожи между собой. Так, новая команда при одной из атак использовала сочетание фишинга и трюка с использованием протоколов Microsoft «server message block» для получения учетных данных от пострадавших,но техника такой атаки была отлична от той, которую использовала группа Energetic Bear.

Energetic Bear исчезла в конце 2014 года, а Palmetto Fusion начала свои атаки в 2015 году, и поэтому она по-прежнему частично считается принадлежащей к российским хакерским группам. Сроки указывают на то, что Медведь перестроился, набрал новые инструменты и методы, чтобы скрыть эту связь.

Частично отслеживая деятельность Palmetto Fusion, эксперты все же ждут возвращения Energetic Bear. Они уверены, что русские спецслужбы не сдадутся из-за небольшой неудачи, и поэтому Медведь восстанет из спячки в любой момент.

Автор: Алина Саратова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 2466 19.07.2017, 13:58
9
URL: https://babr24.com/?IDE=272455 Bytes: 7372 / 7215 Версия для печати

Автор текста: **Алина Саратова**.

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