Автор: Нежданов И.Ю.
Статья опубликована - http://analitirus.blogspot.ru/2013/02/blog-post_23.html
23.02.2013

Конкурентная разведка, промышленный шпионаж и защита информации

По своей сути конкурентная разведка и защита информации это два антипода , которые жить друг без друга не могут. По тому отчеты компаний, занимающихся расследованиями инцидентов в области защиты информации, являются весьма ценным материалом с точки зрения выявления новых методов поиска и расшифровки «следов жизнедеятельности» пользователей интернета. А уж такие громкие и разоблачительные тем более…

APT1: разоблачение китайской организации, занимавшейся промышленным кибершпионажем
Компания Mandiant вынесла на суд общественности свой детальный отчет, посвященный расследованию большого количества инцидентов, связанных с несанкционированными проникновениями во внутренние сети различных организаций и их компьютеры по всему миру. Период времени, за который были собраны эти данные, впечатляет — 7 лет. В отчете указывается, что **эти случаи имели целью похищение всевозможной конфиденциальной информации этих скомпрометированных организаций, а также были осуществлены одной и той же группой**. Mandiant пришла к выводу, что за серией этих атак стоит крупная организация китайского происхождения и сами эти операции по вторжению в частные сети организаций велись под прикрытием китайского правительства и спецслужб на протяжении семи лет (!). Более того, эта организация, на самом деле, является крылом или подразделением Народно-освободительной армии Китая. В нашем посте мы приводим выводы, которые были сделаны Mandiant за семилетний период анализа деятельности этой теневой организации. Детальную версию отчета, включая технические подробности вы можете найти здесь.

Введение

Начиная с 2004 года, компания Mandiant занималась расследованием нарушений в сфере компьютерной безопасности в сотнях организаций по всему миру. **Большинство из этих нарушений мы классифицируем как Advanced Persistent Threat, APT**. Мы уже публиковали наш отчет об APT в 2010 г., в котором отмечалась наша позиция по поводу происхождения этих атак, она формулировалась как “Китайское правительство могло санкционировать эту шпионскую деятельность, но не существует способа, который бы позволил выяснить степень его причастности к этому делу”. Теперь, три года спустя, мы обладаемым необходимыми доказательствами для того, чтобы изменить наше оценочное мнение. Мы детально проанализировали сотни случаев нарушений, которые имели место быть в компаниях, и пришли к выводу, что **киберпреступные группы, которые занимаются этой деятельностью располагаются, в первую очередь, в Китае и Китайское правительство знает о них**.

Компания Mandiant продолжает отслеживать десятки групп APT по всему миру, однако этот отчет сосредоточен на наиболее плодовитой из этих групп. Мы назвали эту группу **APT1** и она является, на самом деле, одной из более чем двадцати APT-групп, чьи корни находятся в Китае. **APT1 представляет из себя организацию, которая осуществляла операции кибершпионажа против компаний обширного диапазона деятельности, причем мы зафиксировали, что эти атаки велись, по крайней мере, с 2006 г.** По нашим наблюдениям, эта группа является самой плодовитой в плане количества похищенной ею информации. Масштабы и последствия деятельности группы APT1 впечатляющие.

Активность, которую мы непосредственно наблюдали, возможно, представляет из себя лишь небольшую часть деятельности из той, которую APT1 осуществляли в действительности. Хотя наше исследование не охватывает абсолютно всю деятельность этой организации, мы проанализировали около 150 вторжений в течении 7 лет. Мы также отследили географическое расположение объектов, с которых эти вторжения осуществлялись, их компьютерные системы располагались в Шанхае. Мы раскрыли значительное количество

объектов инфраструктуры APT1, с помощью которых осуществлялась вся деятельность, в том числе управление, команды и методы работы (инструмены, тактика). Были выявлены несколько операторов — лиц, непосредственно управлявших этими операциями.

Выполненный анализ привел нас к выводу о том, что APT1, скорее всего, спонсируется правительством Китая и, к тому же, является одной из наиболее продвинутых таких компаний. Мы считаем, что APT1 в состоянии вести длительные по времени и обширные по диапазону действий операции по кибершпионажу, в значительной степени потому, что получает прямую поддержку правительства. Мы попытались идентифицировать эту организацию, и пришли к выводу, что подразделение 61398 Народно-освободительной армии Китая (People's Liberation Army (PLA's) Unit 61398) похожа на группировку APT1 по своей миссии, возможностям и ресурсам. PLA Unit 61398 также располагается, приблизительно, в той же местности, откуда мы зафиксировали активность APT1.

Ключевые находки

Находка #1

APT1 представляет из себя одно из подразделений Народно-освободительной армии Китая (НОАК) (2nd Bureau of the People's Liberation army (PLa) General staff Department's (GsD) 3rd Department (总参三部二局)), которое наиболее широко известно своим военным ведомством Military unit Cover Designator (MuCD) as unit 61398 (61398部队).

- Природа деятельности этого подразделения 61398 засекречена и является государственной тайной; однако мы полагаем, что эта группа вовлечена в незаконные операции, связанные с проникновением в другие сети или системы.
- Центральное здание 61398 представляет из себя 12-этажное строение, которое было построено в начале 2007 г.
- Мы считаем, что в блоке 61398 работают сотни, а, возможно, и тысячи людей.
- Китайский провайдер China Telecom организовал специальные скоростные коммуникационные линии на основе опто-волоконной инфраструктуры для этого блока, это было сделано во имя национальной безопасности.
- Mandiant отследил активность APT1 в четырех крупных компьютерных сетях в Шанхае и установил, что две из них обслуживают район базирования подразделения 61398.

Находка #2

Группа APT1 систематически осуществляла кражу сотен терабайт данных у, по крайней мере, 141-й организации, а также продемонстрировала возможности по хищению этих данных из десятков организаций одновременно.

- **Начиная с 2006 г., Mandiant обнаружила, что APT1 скомпрометировала 141 организацию, которые охватывают 20 основных отраслей промышленности.**
- APT1 имеет четко определенную методологию атаки, которая была отточена годами и предназначалась для похищения больших объемов ценной интеллектуальной собственности.
- Как только группа APT1 получала доступ в сеть жертвы, они время от времени возвращались в эту скомпрометированную сеть, в течении нескольких месяцев или лет

и похищала широкий спектр информации интеллектуальной собственности, включая технологические проекты, данные закрытых процессов производства, результаты испытаний, бизнес-планы, электронные письма и т. д.

- APT1 использует некоторые инструменты и техники, которые мы прежде не наблюдали в арсенале других групп, включая два инструмента, которые предназначены для кражи электронной почты — GETMAIL и MAPIGET.
- APT1 поддерживают установленный ранее доступ к компьютерным сетям жертв в среднем 356 дней. Самый длинный период времени, на который APT1 смогли получить доступ к скомпрометированной сети был 1764 дня или 4 года и 10 месяцев.
- Среди других масштабных краж, которые были предприняты APT1, мы наблюдали один случай, при котором было похищено 6,5 терабайт данных у одной организации, в течении 10 месяцев атаки.
- В первом месяце 2011 г., APT1 успешно скомпрометировали, по крайней мере, 17 новых жертв, которые работали в 10 различных отраслях промышленности.

Находка #3

Целями APT1 были организации из широкого диапазона отраслей промышленности, причем это были страны, в которых основным языком является английский (англо-говорящие).

- Из 141 одной компании-жертвы APT1, в 87% случаев штаб-квартиры этих компаний находились в англо-говорящих странах.
- Отрасли промышленности, которые были атакованы через APT1 соответствуют тем отраслям, которые Китай выделил как стратегические для развития, в том числе, четыре из семи стратегически важных отраслей промышленности были выделены Китаем в своем пятилетнем плане.

Находка #4

У APT1 есть обширная инфраструктура, в которую входят компьютерные системы по всему миру.

- APT1 контролирует тысячи систем, с помощью которых осуществляет несанкционированные вторжения.
- В последние два года мы наблюдали, что APT1 использует в своей деятельности 937 командных C&C сервера, с которыми связаны 849 различных IP-адресов в 13 странах мира. Большинство из этих 849 адресов были зарегистрированы в Китае (709) и США (109).
- В течении последних трех лет мы наблюдали, что APT1 использовали доменные имена, которые транслировались в 988 уникальных IP-адресов.
- За два года (период с Января 2011 до Января 2013) мы подтвердили, что группа APT1 произвела 1905 попыток операций входа (login) на свои серверы, с которых осуществлялись атаки на компании, при этом использовались 832 различных IP-адреса с использованием инструмента Remote Desktop.
- В последние несколько лет мы зафиксировали 2551 доменное имя, принадлежащее серверам APT1.

Находка #5

Размер инфраструктуры APT1 подразумевает, что она представляет из себя большую организацию с десятками, а может быть и сотнями человеческих операторов.

- Существующая инфраструктура APT1, по нашим оценкам, включает в себя более 1000 серверов.
- Учитывая объем, продолжительность и тип атаки, операторы APT1 должны были быть напрямую поддержаны лингвистами, исследователями open source продуктов, авторами вредоносного ПО, экспертами по различным отраслям; эти люди должны были помочь с переводом поручений от запрашивающей стороны к самим операторам, а также осуществлять помощь при передаче похищенной информации от оператора, обратно, к запрашивающей стороне.
- APT1 также было бы необходимо значительное количество IT-сотрудников, отвечающих за поддержку рабочих компьютеров, бухгалтерия, специалисты по управлению инфраструктурой и логистикой.

Находка #6
В стремлении подчеркнуть, что существуют физические лица, которые непосредственно управляют компьютерами, Mandiant выявляет три персоны, которые связаны с деятельностью APT1.

- Первый человек, “UglyGorilla”, приниал активное участие в операциях APT1, начиная с 2004 г. Его деятельность включала в себя регистрацию доменов для APT1, а также он является автором вредоносного ПО, которое используется APT1 при выпонении атак. «UglyGorilla» публично выразил свою заинтересованность в участии в “кибер-войсках” Китая в Январе 2004 г.
- Второй персонаж, которого мы называем “DOTA”, зарегистрировал десятки учетных записей электронной почты, которые использовались для проведения атак с использованием фишинга и методов социальной инженерии. “DOTA” использовал несколько телефонных номеров Шанхая, в процессе регистрации этих аккаунтов.
- Мы обнаружили, что оба и “UglyGorilla” и “DOTA” использовали те же доменные имена и IP-адреса, которые используются APT1.
- Третий человек, под ником “SuperHard” является создателем семейств таких вредоносных программ как AURIGA и BANGAT, которые мы наблюдали в схемах APT1 и других групп APT. Мы отмечаем, что “SuperHard” проживал в Шанхае.

Находка #7
Mandiant опубликовала более 3 тыс. показателей компрометации, которые должны помочь в защите от операций, проводимых APT1. В частности, эта информация включает:

- Около 3 тыс. APT1 индикаторов, включая имена доменов, IP-адреса и хэши MD5 вредоносного ПО.
- Примеры индикаторов компрометации (Indicators of Compromise) и подробные описания более сорока семейств вредоносного ПО.
- Тринадцать сертификатов шифрования X.509, которые использовались APT1.

У нас осталось мало сомнений относительно того, кто стоит за такими масштабными и беспрерывными атаками, которые осуществлялись на всевозможные отрасли

промышленности. Мы считаем, что совокупности доказательств, приведенных в этом документе достаточно, чтобы утверждать что APT1 является подразделением 61398. Тем не менее, мы признаем, что есть и другая, маловероятная версия. Например, в Шанхае существует и другая, секретная, похожая на подразделение 61398 группировка, которая имеет доступ к Шанхайской телекоммуникационной инфраструктуре. Эта группа также выполняет длительные по времени операции кибершпионажа.

Размер и месторасположение блока 61398

Мы считаем, что размер строений и офисных помещений для группы 61398 включает в себя площадь в 130,663 квадратных фута пространства и рассчитано на 2 тыс. человек.

Рис. Район будущего базированя блока (2006 г., до строительства).

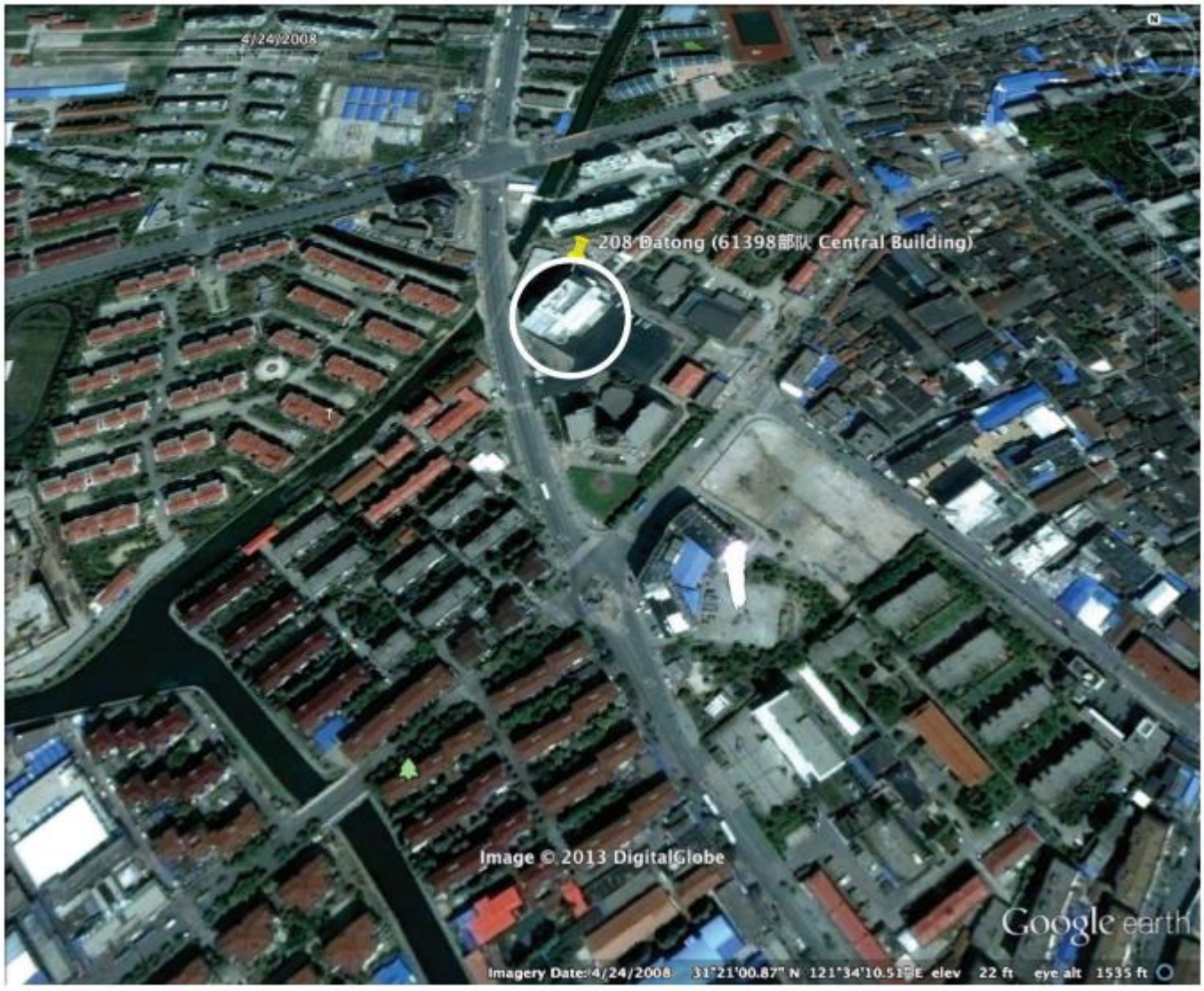

Рис. Построенное главное здание блока (2008 г.)

Рис. Главное здание блока (центральный вход).
Доказательства, которые мы собрали о блоке, его целях и инфраструктуре показывают, что:

- В блоке работают сотни, возможно, тысячи сотрудников.
- На работу в блок требуются люди, прошедшие подготовку в сфере IT-безопасности, эксплуатации компьютерных сетей и хорошим знанием английского языка.
- Блок обладает масштабной, развитой инфраструктурой сооружений в районе “Pudong New Area” в Шанхае.
- Блок был бенефициаром специальной опто-волоконной инфраструктуры коммуникаций, которая была предоставлена государственным предприятием China Telecom под эгидой национальной безопасности.

APT1: годы шпионажа

Наши исследования показали, что за время своей деятельности, с 2006 г., APT1 выкрали десятки терабайт данных из, по крайней мере, 141-й организации, работающих в различных отраслях промышленности. Примечательно, что мы наблюдали одновременные атаки на эти организации со стороны APT1. После того как группа устанавливала контроль над внутренней сетью жертвы, она осуществляла кражу данных, причем, в течении нескольких месяцев или лет. Похищенная информация, как правило, включала в себя интеллектуальную собственность, например, чертежи, схемы закрытых производственных процессов, бизнес-

планы, почту и многое другое. Мы считаем, что деятельность APT1 по кибершпионажу, которую мы отслеживали, представляет из себя лишь небольшую часть деятельности этой группы.

Начиная с 2006 года мы видели, что APT1 постоянно расширяла доступ, компрометируя все новые и новые жертвы. На рисунке показана временная шкала из 141-го случая компрометирования различных компаний. Каждый пункт на этой шкале представляет отдельную жертву и фиксирует дату первоначальной активности APT1 в компьютерной сети организации. Мы оценили, что, в среднем, APT1 получала доступ к сети жертвы на 356 дней. Наибольший период времени, на котороый APT1 получала доступ к компьютерной сети жертвы длился, по крайней мере, 1,764 дня или четыре года и десять месяцев.

Рис. Концентрация атак APT1 по годам.

География APT1 и нацеленность на промышленность

Организации, на которые в первую очередь, была нацелена APT1, в основном, располагались в англоговорящих странах. Тем не менее, мы также видели небольшое количество целей, располагавшихся в других странах, отличных от англоговорящих. Мы зафиксировали, что 87% проникновений было осуществлено в компании, штаб-квартиры которых располагались в англоговорящих странах. Согласно нашей статистике, 115 жертв были расположены в США и 7 в Канаде и Англии. В случае остальных 19 жертв, 17 из них принадлежали группе стран, для которых английский является основным языком. К этим учреждениям относятся международные компании, а также иностранные правительства, в которых английский язык является основным.

Рис. География компаний, атакованных APT1.

APT1 продемонстрировали возможности по краже данных из десятков организаций, которые работают в широком диапазоне отраслей промышленности, причем кражи из различных

организаций происходили в один и тот же период времени. Рисунок ниже дает обзор самых ранних известных дат активности APT1 против 141-й жертвы, которые представляют 20 основных отраслей промышленности. В первом месяце 2011 года мы видим, что APT1 успешно скомпрометировали 17 новых жертв, работавших в 10 различных отраслях промышленности. Так как мы уже наблюдали, что группа остается активной в скомпрометированной сети каждой жертвы, в среднем на год, после даты первоначальной компрометации, мы заключаем, что APT1 совершил эти 17 новых вторжений при одновременном сохранении доступа к сетям своих предыдущих жертв.

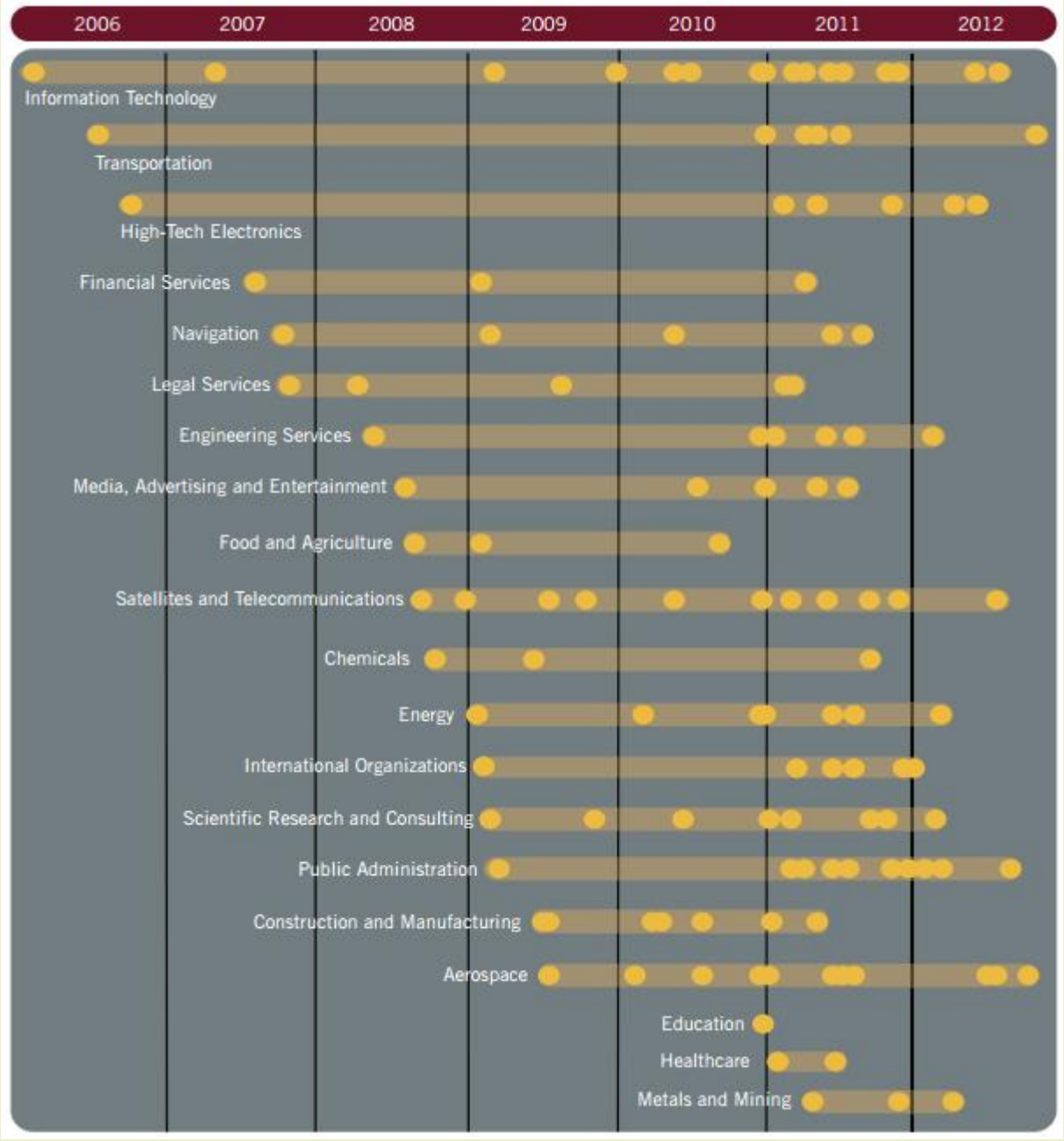

Рис. Временная шкала, представляющая отметки времени начала компрометации APT1 сетей различных организаций в отраслях индустрии. Отметки на шкале показывают первоначальную дату компрометации.

Мы считаем, что выбранные для атаки отрасли промышленности со стороны APT1 были сделаны не случайно и соответствуют стратегическим приоритетам Китая. Наши наблюдения подтверждают, что деятельность APT1 направлена на, по крайней мере, четыре из семи стратегически важных отраслей промышленности, которые Китай выделил в своем 12-м пятилетнем плане.

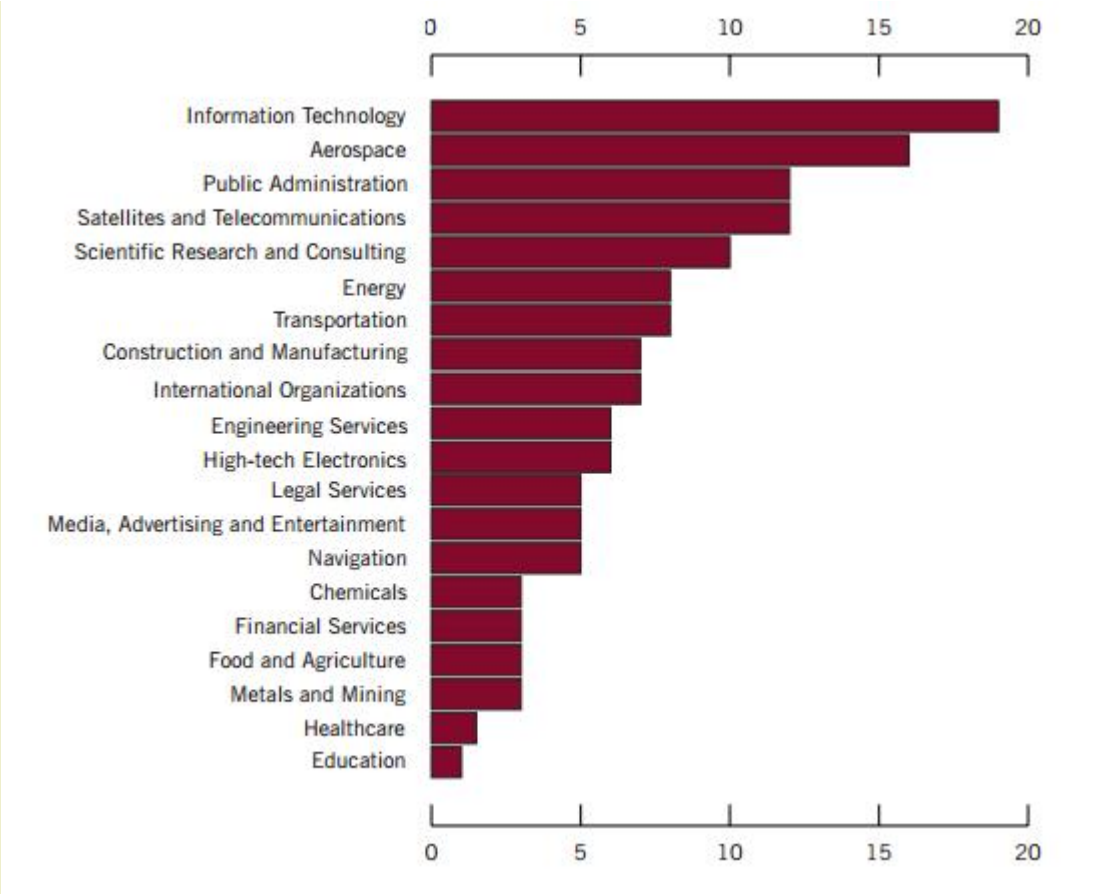

Рис. Жертвы APT1, классифицированные по отраслям промышленности.

Заключение

Можно без преувеличения сказать, что компания Mandiant вывела на новый уровень расследования подобного рода. Здесь действует правило: если вам нужно **публично** обвинить страну, в данном случае Китай, в кибершпионаже государственного уровня, вы должны собрать доказательства для этого. Видимо Mandiant это удалось. Отчет Mandiant действительно произвел эффект разорвавшейся бомбы, по крайней мере, общественности показали доказательства, а не слухи. Реакция со стороны security-сообщества была неоднородной. Например, можно недоумевать по поводу того, зачем компания сделала всю эту информацию публичной или почему AV-компании, в таком случае, оказались, отчасти, бессильны перед такого уровня угрозой, по части обнаружения вредоносных тел. Компания Symantec через неделю после публикации отчета Mandiant заявила, что также отслеживала деятельность группы APT1 и опубликовала свои индикаторы APT1. Мы все же полагаем, что **в данном случае имеет место сбор доказательств и улик причастности китайской организации государственного уровня к делу промышленного кибершпионажа с целью последующего их обнародования для широкой аудитории**. Слово публичный здесь является ключевым, так как можно поставить под сомнение (а может быть и нет), что упоминаемые в отчете Mandiant атаки представляли из себя реальную угрозу интересов национальной безопасности США (по крайней мере, вовлеченные в эту операцию лица пришли к выводу, что публикация этого отчета именно сейчас пойдет им на руку).