Кибернетическая война.

Анализ Conficker, Stuxnet, Duqu о пламени, мини-Flame, Гаусса, Махди, чтобы Shamoon

Форум по информационной безопасности

www.gocs.de;-ЕС-инфо-com.de

Сокращенный вариант

Мы первый раз на простой вопрос, потому что на самом деле уже начался?

Этот вопрос можно легко ответить и да, и нет.

Чтобы ответить на этот вопрос, мы даже не потрудились для оценки пресс-релизы по данному вопросу.

Для тех, кто хочет обвинять нас, мы бы использовали "секретную информацию zuhaltende". Давайте еще раз подчеркиваю, мы проанализировали только публично доступные материалы.

За период анализа, мы использовали только в период с "Stuxnet в Shamoon", то есть относительно короткое время.

В то же время ограничения в отношении огромных масс вредоносного было сделано. Потому что это интересно просто типичный "кибернетического стрелы", которые отвечают атрибут "боевых".

Но в то же время типичной структуры, которые характерны для систем вооружения. Но время зависимость отдельных систем вооружения.

Хотя несколько "кибернетического стрелы" были полностью описаны, они позволяют очень интересную информацию. Где можно посмотреть, мы пишем об этом позже, в противном случае они теряют связи. Из-за проведения частей не может построить стратегию защиты или защиты. Это, конечно, только тогда, когда они этого хотят.

Набор в этот период должна кибернетического оружия войны в шпионаже средства для средств поражения, как известно, их, или предполагается, что известно множество.

Мы разделили их на две группы.

Одна группа включает в себя разрушение и саботаж оружия.

Вторая группа включает в себя шпионом систем, подсистем, а некоторые, такие как манипуляции систем.

В рамках этой системы подкатегории манипуляции, методы следует понимать как быть изменена, где информация хранится или удалены. Тем не менее, никаких систем для управления производством.

Первый Группа

Наиболее известными представителями этой группы являются "Stuxnet" и "Shamoon". Их действие заключается в разрушении программных систем управления технологическими процессами. (Stuxnet), а также в уничтожении компьютерной инфраструктуры, таких, как магнитные носители (жесткие диски), и т.д.

Первый известный кибернетический Стрелка характеризуется очень специфическое разрушение модуля. Это происходит только специальных систем управления производством (обогащение урана систем с PLC от Siemens).

При использовании с другими системами управления производством того же производителя, никаких серьезных повреждений не наблюдается.

Первое использование этого кибернетического стрелки характеризуется особенность. Это были первые нападения избирательное применение - то есть - через прямое внедрение в кибернетической системы выполняется (компьютер). По различным данным пресс обе атаки были проведены уполномоченных сотрудников соответствующих центров компьютер.

Это связано с терактами в Иране, а также теракты в Саудовской Аравии, где нефтяная промышленность была поражена.

Степень, в которой внутренние меры безопасности, которые сократили свои потери, не известно.

Может таким образом, любой консервант с системой связи (Интернет или другие каналы связи) не являются эффективными. В таких атак интернет-меры безопасности неэффективны (так называемые кибер-штаб обороны).

Это было верно для использования "Stuxnet" и "Shamoon", так.

Как многие из этих случаев были выполнены уполномоченным сотрудникам неизвестно. Для этого типа атак имеет значение только что состоялось это непосредственно в компьютерной системе.

Этот тип является типом, который требует система защиты непосредственно в компьютерной системе или соответствующие операционные системы и более строгие защитные меры, такие, как внутренняя кодировка или шифрование. Из известных систем защиты друг от друга. Это ничего не значит, эти системы должны быть основаны на ценности информации.

В случае "Stuxnet" произошел после первого использования даже для массового заражения через интернет. Это должно было инфицировано около 60000 единиц. Какой должна быть цель

этого распределения неясно, как "Stuxnet" узкоспециализированные кибернетических стрелка была и остается.

Затем дыр в программном обеспечении системы были использованы лишь после долгого времени, заполненный несколько месяцев.

Была проведена к этому "Flickenschusterei", кибернетическая война (кибервойна) можно было бы успешно выступили на этих отверстий.

Индентора включена очень умная вторжения. Преемник или же продукты платформы используют различные пенетраторов.

Сколько больше дырок, чем там!

Акцент, даже в настоящих результатов, с тем, что только соответствующие вредные модули должны быть заменены другими характеристиками цели.

Такое же поведение также относится к "проникающей" проникнуть в соответствующих кибернетических единиц (компьютерные системы).

Модульность является характерной чертой современных кибернетических стрелки.

Второй Это второй группы является гораздо более обширным. Известные представители Duqu, Пламя, Гаусс, мини-Пламя и Махди.

Эта группа может быть описана как "кибернетическое шпионов". Это кибернетическая шпионы, отмеченные черты классической шпионов.

Это особый и кибернетические интеллекта более подробно.

Группа кибернетических шпионы использовали по-разному. Представители Duqu и Махди был настоящим учреждается только в небольшом количестве. Это означает не что иное, сравнительно немногие из этих кибернетических стрелки были использованы и что может быть, было очень мало обнаружено. Кроме того, на специальных задач это означает, мало известно. Тем не менее, они считают "очень опасным". ВС в частности Также на BSI / Германия. Из других источников, длительное применение не исключено, с новыми модулями шпионаже.

Это можно сравнить с Duqu разведывательных спутников. Он там, но другой не знает!

Надо полагать, те источники с обновленным использования. В соответствии с известным опытом развития различных платформах, "Duqu и Stuxnet" более продвинутых системах используется.

Даже эта линия развития проявляется в известных системах шпионаже.

Также считает, что платформа - принцип применения. Это ничего не значит, а испытаны и проверены системы разработаны с помощью новых модулей для типа задачи. В то же время, опыт может быть изменен со взрослыми решения и оптимизированные для удовлетворения

растущих требований. Анализ касается модулей, а также коммуникационных модулей. Последнее имеет особое значение, так как они выиграли должны передавать информацию в скрытом серверов. Это относится к количеству информации, а также за секретность. По этой причине, «восстановленная информация" передается в зашифрованном или зашифрованном виде. Тот же принцип был использован во второй мировой войне. Таким образом, информация, полученная от "Enigma", закодированные для дальнейшей передачи. Какая процедура используется на британской стороны пришли кажется еще быть тайной. Весь этот процесс получил название "Ultra".

Это помешало, что немецкая сторона получает знания "коллапс" в системе шифрования Enigma в то время как расшифрованный информация защищена. Он также дал аналогию в восьмидесятых годах в контексте информации расшифрованы ex.DDR ZCO.

Это старый метод можно обнаружить даже в кибернетическом шпионов. Опять же, информация защищена, таким образом, нет никакого видения шпионаже информацию. Кроме того, в связи с этим информацию, которая передается от коробки передач к серверам, а не руководство к "интересной информацией".

Кибернетический объект, который был выяснен этого кибернетического стрелки должны получить никаких существенных доказательств того, что информацию для выяснения значения.

Опять же, есть очень интересный подход:

(1)

Некоторые покупатели покупают "магнитный носитель" с интересной и ценной информации для них (например, данные налоги для немецких неплательщиков налогов) и платить миллионы €. Значение этой информации несколько.

На рынке информации, как правило, известно, что европейские финансовые власти искать "информацию о деньгах умножения».

Так как эта информация не будет продана на рынке, они будут доступны только для "незаконно". Эти действия осуществляются "уполномоченного лица".

(2)

Другая форма сбора информации, которая требует использования кибернетических агентов предпочтительнее других.

В этом случае взять на себя функцию стрелки кибернетических коллектор информации в странных кибернетических систем. Информация, собранная здесь, будут переданы через коммуникационный сервер. В некоторых случаях, данные должны быть направлены массовые размером 5 гигабайт. Тем не менее, они могут быть больше или меньше.

Сбор данных с помощью "кибернетического стрелка" является более гибким по сравнению с человеческой источник. Использование этих стрелок позволяет дать ответ клиенту соответствующую идеально подходит.

Отсюда следует, конечно, преимущество, что вы можете сделать быстрые изменения, потому что основной, открыл другую неизвестных источников.

Среди характеристик кибернетического интеллекта, несомненно, слышал быстрой изменчивости в цель.

Различные подходы зависят от соответствующих форм правления.

Эти небольшие Spionagehelferlein есть, как и любая другая программа или кибернетические размер стрелки. Некоторые из этих стройных, в то время как другие большие лодки. Они исходят из одной и той же платформе.

Наиболее известны «большая лодка" является "Пламя".

Применение кибернетических шпионы очень разные.

Так как некоторые Duqu или мини-Flame быть использованы только в небольших количествах. Ожидается, для каждой системы до 60 инфекций.

Общее количество этих специальных кибернетических шпионов, таким образом, около 120 инфекциям.

Кажется, здесь будет весьма специфичным и чувствительным кибернетических шпиона.

Информация доступна для анализа не могут быть оценены.

Другие, однако, использоваться в меру. В то время как инфекции были обнаружены в 10.000 или больше.

Пламя инфекции примерно от 5000 до 6000

Гаусс около 2500 инфекциями

Махди более 700 инфекций

Conficker около 60.000 или, возможно, даже больше.

Нормы эти кибернетические шпионы были до 10-кратного до 100-кратного по специальным системам. В некоторых случаях это значение может быть превышено значительно (Conficker).

Территория заражения колеблется от менее 68 200 и не более до 100.000 или более инфекций.

Реальная цифра гораздо выше. Из анализа других вредных систем можно считать факторами, от 3 ... 8.

Причины большого числа неизвестных известны случаи, и не будет обсуждаться.

По географическому распределению "вредоносных программ найден", которые будут рассматриваться здесь намеренно не указано. Так как количество приложений кибернетических стрелки поставляет другим, разные результаты. В то же время, использование некоторых кибернетических стрелки в геополитическом нелогично.

Очень интересным моментом является анализ Fragegestellung, в каких областях, политике, экономике, военных, научных исследований и разработок, инфраструктуры и так посвященном

Их результаты очень интересны.

Эти результаты не публикуются, как «неправильное толкование» между опошлять и паникерства кибернетической войны может привести к сценариям конца света.

Перед анализом 10.12.2012

Примечания:

Этот материал является частью "Форум по информационной безопасности".

Там публикуются и обновляются непрерывно.

Этот материал основан только на общедоступных публикаций.

Опубликованные в Интернете по следующим адресам:

www.gocs, де или -www.gocs.eu или www.gocs.info или www.gocs.com.de

23.12.2012 Берлин,

Автор Старая GOCS

Используется с разрешения автора. Этот анализ будет постоянно обновляться. Ошибки исключены.