



АРТ- и финансовые атаки на промышленные организации во втором полугодии 2021 года

Группы злоумышленников, связанные с Китаем.....	3
Атаки группы Lazarus.....	4
Атаки WildPressure.....	5
TortoiseShell.....	5
Шпионская кампания с применением Bandoor RAT в Латинской Америке.....	5
APT31.....	6
Атаки на иранские железные дороги и автозаправки.....	7
Операция Layover — атаки на авиационную отрасль.....	7
Группа FamousSparrow и атаки на инжиниринговые компании.....	8
Использование APT-группами уязвимостей в Zoho ManageEngine.....	10
Атаки APT-C-36.....	11
Атаки DarkOxide на полупроводниковую промышленность.....	11
Атаки ChamelGang.....	12
PseudoManuscript: масштабная серия атак с использованием шпионского ПО.....	12
Operation GhostShell.....	13
Атаки TA2722.....	14
Атаки иранских APT-групп с государственной поддержкой.....	14
Атаки вредоносного ПО Tardigrade на биотехнологические производственные компании ...	15
Атаки Tropic Trooper на транспорт и государственные структуры.....	16
Атаки группы Karakurt.....	17

В отчете описаны APT-атаки на промышленные предприятия, сведения о которых были опубликованы во второй половине 2021 года, а также соответствующей активности групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. Мы старались привести наиболее важные факты, результаты исследований и выводы исследователей, которые, по нашему мнению, могут быть полезны экспертам, которые решают конкретные проблемы, связанные с обеспечением кибербезопасности промышленных предприятий.

Группы злоумышленников, связанные с Китаем

В течение 2020 и 2021 годов «Лаборатория Касперского» [обнаруживала](#) новый модуль загрузчика [ShadowPad](#), получивший название ShadowShredder. Модуль применялся в атаках на объекты критической инфраструктуры в разных странах, в том числе в Индии, Китае, Канаде, Афганистане, Украине и других. В результате дальнейшего исследования были обнаружены и другие импланты, устанавливаемые с помощью ShadowPad и ShadowShredder, такие как бэкдор Quarian, PlugX, Poison Ivy и другие хакерские утилиты. Примечательно, что активность бэкдоров Quarian и Poison Ivy имела общие черты с более ранней активностью [IceFog](#) в атаках на пользователей в Средней Азии. Эта информация была представлена в приватном отчете, в который вошел технический анализ ShadowShredder и атак, в которых вредоносная нагрузка второго этапа связана с ShadowShredder и ShadowPad.

В третьем квартале 2021 года «Лаборатория Касперского» [обнаружила](#) еще один набор тактик, методов и процедур (Tactics, Techniques and Procedures, TTP). Он применялся в атаках на аэрокосмические и оборонные исследовательские организации в Индии между 2019 годом и концом июня 2021 года и включал в себя два ранее неизвестных бэкдора: LGuarian и HTTP_NEWS. Первый из них, по-видимому, является новым вариантом бэкдора Quarian — малоизвестной вредоносной программы, которую китайско-язычные акторы применяют примерно с 2012 года и которую злоумышленники использовали и в данном случае. Подробные сведения о тактике атакующих после эксплуатации уязвимостей и подробные описания применяемого ими на этом этапе инструментария, а также действий, выполняемых на машинах жертв, представлены в приватном отчете.

С помощью технологии «Лаборатории Касперского» для защиты от эксплойтов (Kaspersky Advanced Exploit Prevention) [были обнаружены](#) атаки, в которых применялся эксплойт для уязвимости нулевого дня в нескольких версиях Windows. Сведения о соответствующей уязвимости

были переданы компании Microsoft. Она получила идентификатор CVE-2021-40449 и была закрыта в рамках октябрьского «вторника патчей» 2021 года. Было проанализировано примененное вместе с эксплойтом неизвестное ранее вредоносное ПО, которое получило название «MysterySnail». Были также найдены и изучены другие варианты этого вредоносного ПО, которые применялись в распространенных кампаниях кибершпионажа. Выяснилось, что это вредоносное ПО использовалось в атаках на IT-компании, военных/оборонных подрядчиков и дипломатические учреждения. Благодаря сходству кода и использованию одной и той же инфраструктуры командных серверов эти атаки удалось связать с актором, известным как IronHusky, а также с давней активностью китайско-язычных групп, относящейся к 2012 году.

Атаки группы Lazarus

Эксперты «Лаборатории Касперского» [отметили](#), что группа Lazarus применяет в атаках на оборонную промышленность фреймворк вредоносного ПО [MATA](#). Ранее Lazarus использовала MATA для атак на различные отрасли с киберпреступными целями, в том числе для кражи клиентских баз и распространения программ-вымогателей. Однако в данном случае MATA применялась для кибершпионажа. Группа применяла приложение, которым заведомо пользовалась выбранная жертва, дополненное троянским функционалом — это известная особенность группы Lazarus. Запуск приложения приводит к многоступенчатому процессу заражения, который начинается с загрузчика. Далее загрузчик скачивает дополнительное вредоносное ПО со взломанных серверов, используемых в качестве командных. «Лабораторией Касперского» были получены несколько компонентов MATA, включая плагины. Вредоносное ПО MATA, которое применялось в рамках данной кампании, усовершенствовано по сравнению с более ранними версиями, и некоторые его компоненты подписаны легитимным краденным сертификатом. Это исследование позволило обнаружить более тесную связь между фреймворком MATA и группой Lazarus, включая факт наличия связи между вредоносным загрузчиком, скачивающим вредоносное ПО MATA, и операцией TangoDaiwo, которая ранее была атрибутирована группе Lazarus.

Атаки WildPressure

После проведенного ранее [исследования](#) кампании WildPressure, в ходе которой были атакованы промышленные организации на Ближнем Востоке, были [обнаружены новые образцы](#) вредоносного ПО WildPressure. Среди найденных в этот раз образцов — написанная на Python многоплатформенная троянская программа, предназначенная для операционных систем Windows и macOS, скрипт на VBScript с функцией саморасшифровки, троянец Milum, написанный на C++, оркестратор и несколько плагинов. Предполагаемые мишени атак в том же регионе Ближнего Востока связаны с нефтегазовой промышленностью.

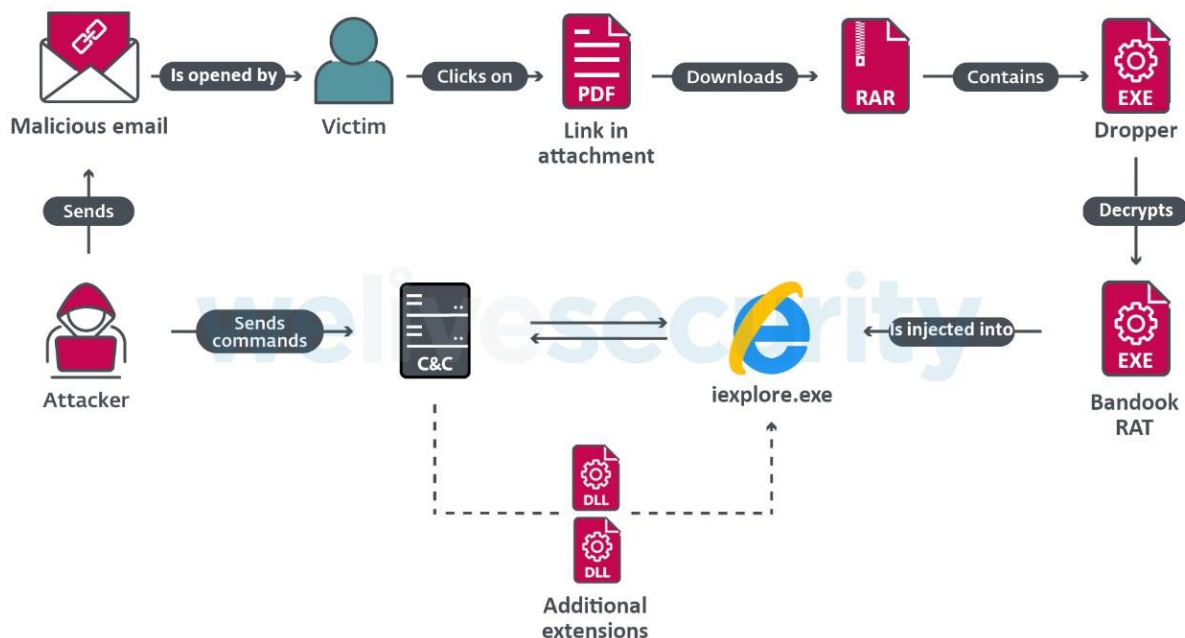
TortoiseShell

15 июля 2021 года Facebook [отключил](#) около 200 учетных записей, которые, по его словам, использовались иранской хакерской группой «TortoiseShell» в рамках кампании кибершпионажа, направленной в первую очередь на военных и сотрудников оборонных и аэрокосмических компаний США. ТТР группы включают использование социальной инженерии, фишинга и кражи учетных данных, троянцев удалённого доступа (Remote Access Trojans, RAT), инструментов для сбора информации об устройствах и сети, кейлоггеров, вредоносного ПО Syskit.

Шпионская кампания с применением Bandoor RAT в Латинской Америке

Обновленные версии троянца удаленного доступа Bandoor [применяются](#) в кампании против корпоративных сетей в испаноговорящих странах, прежде всего Венесуэле. Основные мишени в кампании, получившей название «Bandidos», — это корпоративные сети в Венесуэле. Некоторые из атакованных организаций работают в производственной сфере, остальные в строительстве, здравоохранении, сервисах, связанных с программным обеспечением, и в розничной торговле. В цепочке заражения используются сообщения целенаправленного фишинга с вложенным PDF-файлом, содержащим URL-ссылку, ведущую к зашифрованному RAR-архиву, который, в свою очередь, устанавливает вредоносное ПО Bandoor. Bandoor — это старый троянец удаленного доступа. Существуют упоминания его доступности в интернете, относящиеся еще к 2005 году,

хотя о его применении организованными группами впервые стало известно только в 2016 году.



Процесс заражения Bandoor RAT (Источник: ESET)

Еще один [отчет](#) об этой активности опубликован компанией ProofPoint, отслеживающей этого актора под именем TA2721 (а также «Caliente Bandits»).

APT31

По данным исследования [Positive Technologies Expert Security Center \(PT ESC\)](#), в апреле 2021 года получателям в Монголии были отправлены электронные письма с ранее неизвестной вредоносной утилитой удаленного доступа во вложении. Впоследствии аналогичные атаки были выявлены в России, Республике Беларусь, Канаде и США. В общей сложности с января по июль 2021 года было проведено около десятка атак, где использовались найденные образцы вредоносного ПО. Среди целей злоумышленников — правительственный сектор, аэрокосмические и оборонные предприятия, а также международные финансовые компании и сектор высоких технологий. Анализ образцов вредоносного ПО, данные об именах рабочих директорий и ключей реестра, техники и механизмы, применяемые злоумышленниками, позволили соотнести этот зловред с активностью группы APT31 (известной также под именами Judgment Panda и Zirconium), которая предположительно имеет китайское происхождение. Обнаруженные в июле [атаки на французские компании](#), связанные со

взломом домашних и офисных маршрутизаторов, также связывают с активностью этой группы. Последние данные об этой группе говорят о расширении географии ее интересов за счет стран, где обнаружена ее растущая активность, — в частности, России.

Атаки на иранские железные дороги и автозаправки

Ранее неизвестный вайпер, получивший название «Meteor», [был применен](#) в атаке на систему железных дорог Ирана, [осуществленной](#) 9 июля 2021 года. В результате атаки было прервано железнодорожное сообщение, а пассажирам через табло и доски объявлений было предложено обращаться за дополнительной информацией по телефону 64411 — это номер канцелярии Верховного лидера Али Хаменеи. На момент публикации информации о вайпере Meteor отсутствовали сведения о его связи с какой-либо из известных групп злоумышленников и с какими-либо другими атаками. При этом известные артефакты указывают на то, что программа создана в последние три года и предназначена для неоднократного применения. Злоумышленники, которых эксперты SentinelLabs считают новой группой, также вывели из строя сайт и компьютерные системы Министерства дорог и городского развития Ирана.

В октябре 2021 года [кибератака](#) на систему продажи субсидированного топлива по выпускаемым государством смарт-картам привела к длинным очередям на иранских автозаправках. Ответственность за атаку взяла на себя группа, называющая себя «Predatory Sparrow» (хищный воробей). Злоумышленники также взломали цифровые рекламные щиты в Тегеране и других частях страны и вывели на них сообщение «Хаменеи, где наше топливо?». По заявлению властей Ирана, за атакой стоит неназванное иностранное государство.

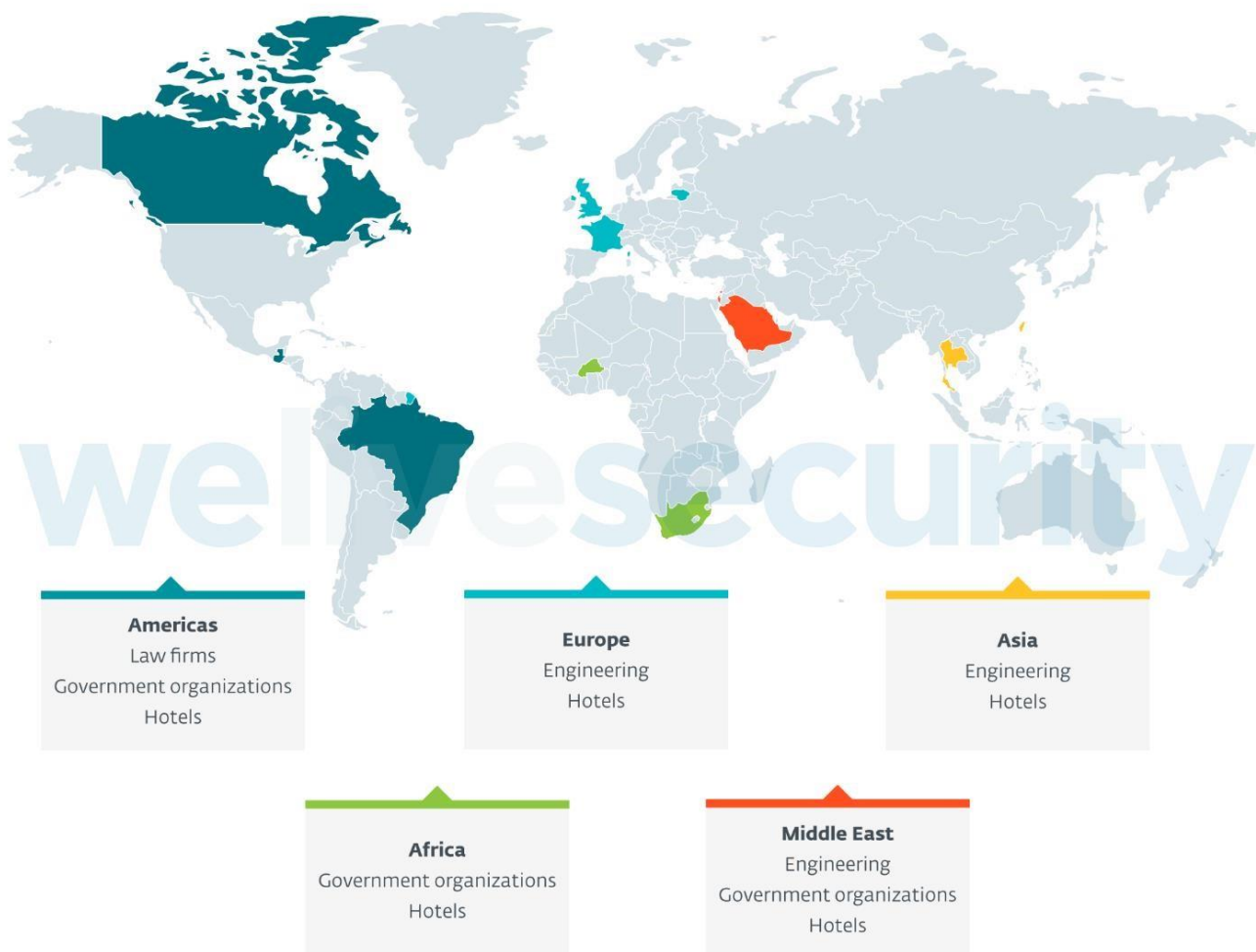
Операция Layover — атаки на авиационную отрасль

Исследователи Cisco Talos [считают](#), что группа злоумышленников из Нигерии ведет атаки на авиационную отрасль уже по крайней мере два года. Во всех своих атаках группа применяла стандартное вредоносное ПО, а также использовала приобретенные через онлайн-форумы криптографические ключи, чтобы скрыть свою активность. Злоумышленники распространяли троянцы

удаленного доступа AsyncRAT и njRAT с помощью документов-приманок, рассчитанных на специалистов авиационной промышленности. Жертвы атак могли столкнуться с кражей данных, финансовым мошенничеством, а также с последующими кибератаками, имеющими значительно более серьезные последствия.

Группа FamousSparrow и атаки на инженеринговые компании

По данным исследований ESET, [новый бэкдор](#), получивший название «SparrowDoor», применяется при проведении атак на государственные организации, инженеринговые компании, адвокатские конторы и гостиницы в Европе, на Ближнем Востоке, в Северной и Южной Америке (но не в США), Азии и Африке. Эксперты связывают бэкдор с новой APT-группой под названием «FamousSparrow». История группы прослеживается с 2019 года, однако в текущих атаках используется обнаруженная в марте 2021 года уязвимость ProxyLogon. Эксперты «Лаборатории Касперского» также расследовали эти атаки и считают со средней или высокой степенью уверенности, что данное специалистами ESET описание группы «FamousSparrow» в реальности соответствует нескольким наборам вредоносной активности от разных операторов.



Географическое распределение мишеней FamousSparrow (Источник: [ESET](#))

Эксперты «Лаборатории Касперского» [обнаружили](#), что один и тот же сервер упоминался как используемый группой FamousSparrow для доставки бэкдора SparrowDoor и как сервер китайско-язычного актора GhostEmperor, причем, возможно, обе группы использовали его примерно в одно и то же время в июле 2020 года. По данным телеметрии «Лаборатории Касперского», в число объектов атак GhostEmperor входили государственные структуры и телекоммуникационные компании в Юго-Восточной Азии, в том числе несколько известных организаций в Малайзии, Таиланде, Вьетнаме и Индонезии, а также несколько аналогичных жертв в таких странах как Египет, Эфиопия и Афганистан.

Использование APT-группами уязвимостей в Zoho ManageEngine

16 сентября 2021 года ФБР, Агентство по кибербезопасности и защите инфраструктуры (CISA) и Киберкомандование Береговой охраны США заявили в [совместном бюллетене безопасности](#), что, по их мнению, группы злоумышленников с государственной поддержкой активно используют в атаках вновь обнаруженную уязвимость (CVE-2021-40539) в решении для управления паролями и единой регистрации Zoho ManageEngine ADSelfService Plus. Это может привести к удаленному выполнению кода (RCE) и обеспечить злоумышленникам более широкий доступ к корпоративной сети. Данная уязвимость использовалась в атаках на учебные и научные учреждения, военных подрядчиков и объекты критической инфраструктуры в разных отраслях, включая транспорт, информационные технологии, производственный сектор, телекоммуникации, логистику и финансы.

В рамках этой кампании злоумышленники предприняли попытку взлома компьютерной сети Порта Хьюстона — одной из крупнейших портовых администраций США. Представители порта [заявили](#) об успешном отражении атаки и о том, что «никакие операционные данные и системы не пострадали в результате» попытки вторжения.

В декабре CISA и ФБР опубликовали новый [совместный бюллетень безопасности](#), согласно которому злоумышленники активно используют еще одну новую уязвимость в Zoho ManageEngine ServiceDesk Plus (CVE2021-44077). По оценке ФБР и CISA, APT-акторы используют эту уязвимость в атаках на объекты критической инфраструктуры в таких отраслях как здравоохранение, финансовые сервисы, электроника и консалтинг в области информационных технологий.

Согласно [отчету](#) компании Palo Alto, на момент выхода бюллетеня безопасности не было общедоступных концептуальных эксплойтов (proof-of-concept exploits) для уязвимости CVE-2021-44077 ([теперь это уже не так](#)). Это говорит о том, что APT-группа, возможно, создала [код эксплойта](#) самостоятельно. За три осенних месяца 2021 года были успешно атакованы по крайней мере 13 организаций в технологической отрасли, энергетике, здравоохранении, образовании, финансовой отрасли и оборонной промышленности. Кроме того, отмечалось, что после эксплуатации уязвимости злоумышленники загружали на системы жертв новый дроппер. Аналогично более ранней тактике, применявшейся для атак на ПО ADSelfService, этот дроппер устанавливает веб-шелл Godzilla,

дающий злоумышленникам более широкий доступ к зараженным системам и возможность закрепиться на них. Компания Palo Alto Networks дала этому комплексу активности название «Tilted Temple» и обнаружила свидетельства возможной связи между этими атаками и активностью группы APT27 (Emissary Panda), которая ранее использовала Godzilla в атаках на значимые объекты. Тем не менее, найденных доказательств недостаточно для уверенной атрибуции.

Атаки APT-C-36

Компания Trend Micro опубликовала [отчет](#) о новой кампании, использующей целенаправленные фишинговые рассылки писем, содержащих в качестве вредоносной нагрузки троянец удаленного доступа BitRAT. По результатам атрибуции считается, что это кампания группы, известной как APT-C-36 (а также как Blind Eagle), которая переработала свои методы, взяв на вооружение множество стандартных троянцев удаленного доступа (RAT) и фильтрацию по геолокации с целью избежать обнаружения. Атакам предположительно подверглись организации в различных секторах, включая государственные органы, финансы, здравоохранение, телекоммуникации, энергетику и нефтегазовую отрасль. При этом большинство объектов атак последней по времени кампании находится в Колумбии, а меньшая часть — в Эквадоре, Испании и Панаме.

Атаки DarkOxide на полупроводниковую промышленность

С сентября 2019 года компания CrowdStrike [отслеживает активность](#) пока еще не названного актора, проводящего целенаправленные атаки на организации полупроводниковой отрасли в Азиатско-Тихоокеанском регионе. Подразделение CrowdStrike Intelligence отслеживает этот кластер активности под именем DarkOxide. Чем мотивирована отслеживаемая активность, пока определить не удалось, однако применяемые тактика, методы и процедуры, а также выбор объектов атаки говорят о том, что группа нацелена скорее на кражу конфиденциальной информации, чем на прямое получение финансовой выгоды. Атака на потенциальную жертву начинается с привлечения ее внимания на деловой платформе социальных медиа под видом кампании по набору персонала. Затем потенциальной жертве предлагается скачать документ-приманку, якобы относящийся к

вакансии, который на самом деле представляет собой исполняемый файл с двойным расширением. Файлы-приманки в этих атаках имеют нетипичные для исполняемых файлов расширения, такие как .PIF (program information file — файл сведений о программе) и .SCR (скринсейвер). При выполнении вредоносной нагрузки для скачивания еще одного вредоносного исполняемого бинарного файла используется несколько скриптовых интерфейсов, включая PowerShell и Visual Basic Script. Этот второй исполняемый файл, также имеющий расширение .PIF или .SCR, в свою очередь устанавливает экземпляр легитимного средства удаленного доступа Remote Utilities с заданным адресом командного сервера. В некоторых, достаточно редких, случаях кроме Remote Utilities устанавливался также файловый менеджер Total Manager Pro.

Вероятно, это делалось для поиска определенных файлов в файловой системе или для упаковки файлов с целью отправки их злоумышленникам.

Атаки ChamelGang

Во втором квартале 2021 года команда Positive Technologies Expert Security Center (PT ESC) [провела расследование](#) в компании топливно-энергетического комплекса. В ходе расследования выяснилось, что сеть компании была скомпрометирована неизвестной группой с целью хищения данных. Эксперты дали новой группе название ChamelGang. Уже после расследования этого инцидента, 16 августа 2021 года, специалисты PT ESC обнаружили еще одну атаку — были скомпрометированы серверы российской компании из авиационно-промышленного сектора, а для проникновения была использована цепочка уязвимостей ProxyShell. В ходе дальнейшего мониторинга угроз информационной безопасности (threat intelligence), связанных с активностью группы, исследователи нашли ещё 13 взломанных организаций в десяти странах мира. Злоумышленники использовали такие известные вредоносные программы, как FRP, Cobalt Strike Beacon, и Tiny SHell. Кроме того, они применяли новые, ранее неизвестные вредоносные программы — ProxyT, BeaconLoader и бэкдор DoorMe.

PseudoManuscrypt: масштабная серия атак с использованием шпионского ПО

В июне 2021 года эксперты Kaspersky ICS CERT [обнаружили вредоносную программу](#), загрузчик которой был схож с загрузчиком вредоносной

программы Manuscript, входящей в арсенал APT группы Lazarus. В период с 20 января по 10 ноября 2021 года обнаруженный загрузчик был использован в атаках более чем на 35 000 компьютеров в 195 странах мира. Не менее 7,2% всех компьютеров, атакованных вредоносным ПО PseudoManuscript, являются частью систем промышленной автоматизации (АСУ ТП). Среди жертв атак PseudoManuscript — значительное число промышленных и государственных организаций, в том числе предприятия военно-промышленного комплекса и исследовательские лаборатории. Основной модуль PseudoManuscript обладает обширными и разнообразными шпионскими функциями, среди которых кража данных VPN-соединений, регистрация нажатий клавиш, создание снимков и запись видео с экрана, запись звука с микрофона, кража данных из буфера обмена и данных журнала событий операционной системы (что также делает возможным кражу данных о RDP подключениях) и многое другое. Многие косвенные улики указывают на то, что стоящая за атакой группа, вероятно, связана с Китаем. В частности, в некоторых образцах вредоносного ПО присутствуют комментарии на китайском языке. Данные отправляются на сервер злоумышленников по протоколу KCP, реализованному с помощью библиотеки, которая ранее была замечена только во вредоносном ПО китайской группы APT41.

Operation GhostShell

Экспертная группа Cybereason Nocturnus [опубликовала отчет](#) об Operation GhostShell — кампании целенаправленного кибершпионажа против аэрокосмической и телекоммуникационной отраслей преимущественно на Ближнем Востоке, часть жертв которой находится также в США, России и Европе. В рамках Operation GhostShell злоумышленники охотятся на конфиденциальную информацию о критически важных активах, инфраструктуре и технологиях. Неизвестный ранее действующий скрытно троянец удаленного доступа, получивший название «ShellClient», выполняет роль основного средства шпионажа. Его развитие продолжается как минимум с 2018 года. По мнению исследователей, за атакой стоит новая иранская группа злоумышленников, получившая имя «MalKamak». Данные расследования указывают на возможные связи с APT-группой Chafer (APT39) и APT-группой Agrius (которую эксперты «Лаборатории Касперского» отслеживают под именем «BlackShadow»).

Атаки TA2722

Компания Proofpoint [обнаружила](#) новую, высокоактивную киберкриминальную группу, которой было дано название TA2722 / Balikbayan Foxes. На протяжении 2021 года группа провела ряд кампаний, в рамках которых рассылала фишинговые сообщения от имени филиппинских государственных организаций, включая Департамент здравоохранения, Филиппинскую администрацию по трудоустройству за рубежом (Philippine Overseas Employment Administration, POEA) и Таможенное бюро (Bureau of Customs). Среди основных целей TA2722 — организации в таких отраслях как грузоперевозки/логистика, производство, деловые услуги, фармацевтика и энергетика. В число интересующих группу географических регионов входят Северная Америка, Европа и Юго-Восточная Азия. В фишинговых рассылках используются URL-ссылки на OneDrive, ведущие на RAR-архивы с внедренными в них UUE-файлами, вложение в формате PDF с внедренной в него ссылкой на OneDrive или другой вредоносной URL-ссылкой, ведущей на сжатые исполняемые файлы (файлы .iso), загружающие и выполняющие вредоносное ПО, или на сжатые документы MS Excel, содержащие макрокоманды, которые, если разрешить их выполнение, загружают вредоносное ПО. Цель кампании — распространение троянцев удаленного доступа Remcos и Nanoscore для получения доступа к компьютеру жертвы и последующей кражи данных с него.

Атаки иранских APT-групп с государственной поддержкой

В совместном [бюллетене безопасности](#), выпущенном CISA, ФБР, Австралийским центром кибербезопасности (Australian Cyber Security Centre, ACSC) и Национальным центром кибербезопасности Соединенного Королевства (UK National Cyber Security Centre, NCSC), сообщается об идущей в настоящее время вредоносной кампании, которую авторы бюллетеня связывают с поддерживаемой на государственном уровне иранской APT-группой, проводящей атаки на организации в секторах здравоохранения и транспорта. Эта группа по крайней мере с марта 2021 года использует в своих атаках уязвимости в продуктах Fortinet и по крайней мере с октября 2021 года — уязвимость ProxyShell в Microsoft Exchange. После получения первоначального доступа злоумышленники применяют программы-вымогатели, крадут данные с зараженных систем и вымогают деньги у жертв атак.

Согласно [отчету](#), опубликованному Symantec, специалисты компании обнаружили серию атак, проведенных во второй половине 2021 года и нацеленных на телекоммуникационные компании, ряд организаций, предоставляющих IT-сервисы, и одну коммунальную компанию. Атаки, объектами которых стали организации в Израиле, Иордании, Кувейте, Саудовской Аравии, Объединенных Арабских Эмиратах, Пакистане, Таиланде и Лаосе, вероятнее всего, связаны с иранскими хакерами, поддерживаемыми на государственном уровне. На данный момент достоверно установить, кто стоит за этими атаками, не удалось, однако некоторые улики указывают на связь с иранской группой Seedworm (она же MuddyWater). Хотя первоначальный вектор большинства атак пока не установлен, имеются улики, указывающие на то, что по крайней мере в одном случае, возможно, использовалась целенаправленная фишинговая рассылка. В одной атаке на коммунальную компанию в Лаосе, которую исследователи назвали нехарактерной для этой кампании, злоумышленники, по-видимому, использовали для первоначального проникновения в сеть компании уязвимость в публичном сервисе — на это указывает то, что первой была заражена машина, работавшая, как указано в отчете, в качестве веб-сервера IIS. Затем атакующие использовали PowerShell для доставки вредоносных утилит и скриптов в сеть компании и, в конечном итоге, для подключения к серверу веб-почты организации в Таиланде, а также к серверам, связанным с IT-сервисами другой тайской компании.

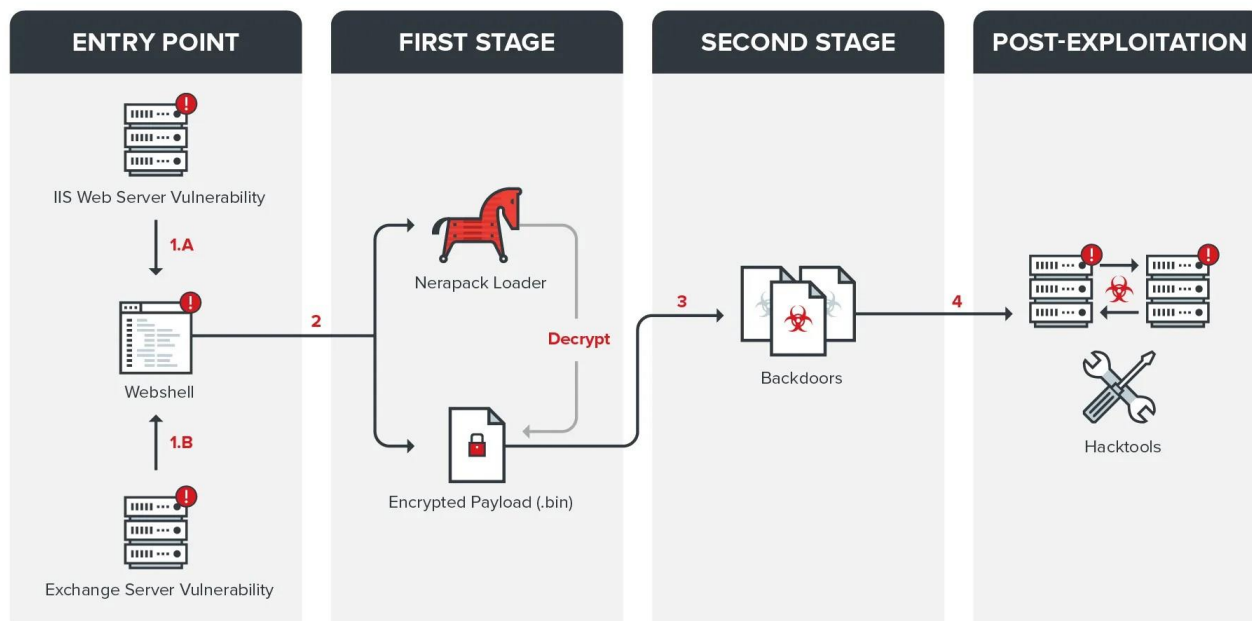
Атаки вредоносного ПО Tardigrade на биотехнологические производственные компании

Центр Bioeconomy Information Sharing and Analysis Center (BIO-ISAC) опубликовал [бюллетень безопасности](#) с описанием вредоносного ПО, примененного в атаках на производственные компании в сфере биотехнологий. Вредоносная программа, получившая название Tardigrade (тихоходка), была впервые обнаружена при расследовании атаки программы-вымогателя, цели которой, возможно, включали шпионаж. Программа Tardigrade имеет троянскую функциональность и использует сложные методы ухода от обнаружения. Исследователи обнаружили, что Tardigrade имеет сходство с популярным вредоносным загрузчиком SmokeLoader/Dofoil, но имеет более сложную функциональность и предлагает злоумышленникам расширенный набор возможностей

настройки. В частности, она может принимать решения о заражении других машин в сети, исходя из собственной внутренней логики.

Атаки Tropic Trooper на транспорт и государственные структуры

Компания Trend Micro [обнаружила](#), что в июле 2020 года АРТ-группа TropicTrooper/Earth Centaur атаковала организации в транспортной отрасли, а также государственные органы, связанные с транспортом. Было отмечено, что группа пыталась получить доступ к некоторым внутренним документам (такими как расписания полетов и документы финансового планирования), а также персональным данным на зараженных машинах (таким как история поисковых запросов). Группа злоумышленников использовала уязвимости в сервере Internet Information Services (IIS) и сервере Microsoft Exchange для проникновения в систему с последующей установкой веб-шеллов, загрузчика .NET и бэкдоров первого этапа. В зависимости от зараженной системы группа применяет бэкдоры, использующие различные протоколы. Кроме того, может использоваться обратный прокси-сервер, чтобы обойти мониторинг со стороны систем защиты сети. Группа также использует фреймворки с открытым исходным кодом для создания нестандартных бэкдоров, что позволяет ей более эффективно создавать новые варианты бэкдоров. После успешной эксплуатации уязвимостей на атакуемой системе злоумышленники применяют различные хакерские инструменты для обнаружения и компрометации машин, подключенных к интранету организации-жертвы, а также средства вывода украденной информации. Группа использует уязвимости для взлома сайтов, которые затем задействует в качестве командных серверов.



©2021 TREND MICRO

Этапы внедрения Earth Centaur в системы атакуемых организаций
(Источник: [Trend Micro](#))

Атаки группы Karakurt

Компания Accenture Security [обнаружила](#) новую группу злоумышленников, называющую себя Karakurt Hacking Team. Группа является финансово мотивированной и приспособленческой по природе. Она специализируется исключительно на краже данных с последующим вымоганием денежных средств. В настоящее время исследователям Accenture Security известно более чем о 40 организациях-жертвах, имеющих разный размер и принадлежащих разным отраслям, включая энергетику и промышленное производство. 95% известных жертв находятся в Северной Америке, остальные 5% — в Европе. Злоумышленники, как правило, используют учетные данные в качестве вектора первоначального проникновения в сети атакуемых организаций, а затем задействуют уже установленные приложения для заражения новых машин в сети и вывода украденных данных при их наличии. Кроме того, злоумышленники, как правило, несколько раз связываются с каждой жертвой по разным каналам связи, чтобы усилить давление на жертв при попытках вымогательства.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», направленный на координацию усилий производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей ИТ-безопасности для защиты промышленных предприятий от кибератак. Kaspersky ICS CERT направляет свои усилия в первую очередь на выявление потенциальных и существующих угроз, нацеленных на системы промышленной автоматизации и промышленный интернет вещей.

[Kaspersky ICS CERT](#)

ics-cert@kaspersky.com