Kaspersky ICS CERT

kaspersky

APT-атаки на промышленные компании в 2020 году

29.03.2021

Version 1.0

С 2018 года Kaspersky ICS CERT ежегодно публикует обзор выявленных в течение года APT-кампаний, направленных на промышленные организации. Обзор основан на результатах исследований «Лаборатории Касперского» и других компаний и дает репрезентативную картину ситуации. В этом обзоре описаны основные события 2020 года, связанные с APT-атаками, и приведены выводы экспертов, которые, на наш взгляд, могут быть полезны как исследователям киберугроз, так и тем, кто решает практические задачи по обеспечению кибербезопасности промышленных предприятий на местах.

APT 33/APT 34

В феврале 2020 года компания ClearSky описала кампанию, имевшую место в последнем квартале 2019 года и нацеленную на компрометацию сетей организаций, работающих в сферах ИТ, телекоммуникаций и безопасности, а также в нефтегазовом, авиационном и государственном секторах по всему миру. Исследователи приписывают эту кампанию иранским злоумышленникам. Кампания Fox Kitten проводилась в целях разведки, но также могла использоваться для распространения вредоносных программ-вайперов, таких как ZeroCleare и Dustman, связанных с группой APT34. Было обнаружено совпадение инфраструктуры Fox Kitten и других группировок, действующих на Ближнем Востоке: APT33 и APT34. Это позволяет предположить, что группировки сотрудничают как в инфраструктуре, так и, возможно, за ее пределами.

Подвергшиеся атаке Fox Kitten страны и отрасли (источник ClearSky)

Первоначальное проникновение в целевые организации осуществлялось с использованием известных уязвимостей в системах с незащищенными службами VPN и RDP. Это позволило атакующим взять под контроль важные корпоративные хранилища информации.

Sofacy

В марте компания TrendMicro описала кампанию APT-группировки Sofacy (также известна как Pawn Storm, Fancy Bear, Sednit, STRONTIUM и APT28), нацеленную на организации в разных частях мира. В течение 2019 и 2020 годов атакующие использовали взломанные адресе электронной почты для рассылки фишинговых писем с целью кражи учетных данных. Большинство скомпрометированных систем принадлежало оборонным компаниям Ближнего Востока. Жертвами этой кампании стали также организации в сфере транспорта, а также в коммунальном и государственном секторах.

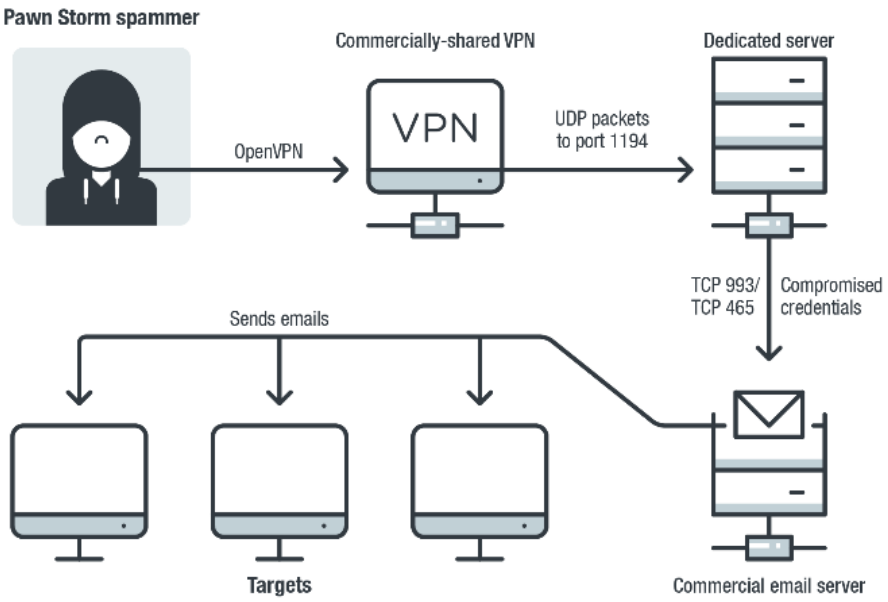


Схема фишинговой атаки Sofacy (Источник: TrendMicro)

Группа также регулярно атаковала многие уязвимые почтовые серверы и службы автообнаружения Microsoft Exchange по всему миру, пытаясь подобрать учетные данные, извлечь данные электронной почты и запустить рассылку фишинговых писем.

APT41 / BARIUM / Winnti

Компания FireEye наблюдала кампанию APT41 (также известную как BARIUM), в которой в период с 20 января 2019 года по 11 марта 2020 года использовались уязвимости в Citrix NetScaler/ADC, маршрутизаторах Cisco

и Zoho ManageEngine Desktop Central. Эта кампания была нацелена на финансовую, строительную, оборонную и промышленную сферу, а также на сферы государственного здравоохранения, высоких технологий, высшего образования и юридический, производственный, вещательный, транспортный, туристический и коммунальный секторы. Жертвы атак были зафиксированы в Австралии, Канаде, Дании, Финляндии, Франции, Индии, Италии, Японии, Малайзии, Мексике, Филиппинах, Польше, Катаре, Саудовской Аравии, Сингапуре, Швеции, Швейцарии, ОАЭ, Великобритании и США. Было отмечено, что на этапе после эксплуатации уязвимости использовалась пробная версия загрузчика Cobalt Strike BEACON, загрузчик VMProtected Meterpreter и шелл-код Cobalt Strike BEACON.

Исследователи из PaltoAlto описали кампанию, в которой группа APT41 использовала уязвимость CVE-2019-19781 для распространения бэкдора Speculoos. Уязвимость затрагивает системы Citrix Application Delivery Controller, Citrix Gateway и Citrix SD-WAN WANOP, что позволяет злоумышленникам удаленно выполнять произвольные команды. Атаки были нацелены на организации в сфере здравоохранения, высшего образования, производства, государственного и технологического секторов во многих регионах, включая Северную и Южную Америку и Европу.

Как мы уже отмечали в предыдущих обзорах APT, некоторые исследователи считают, что APT41 и Winnti — это одна группировка. Использование образцов кода Winnti было замечено в 2020 году при атаках на немецкую химическую компанию и южнокорейскую компанию — разработчик видеоигр. При анализе была обнаружена неизвестная ранее техника для сервера управления (C2), не относившаяся ни к одному из инструментов Winnti Group. Эта техника основана на канале связи туннелирования DNS с использованием кастомизации исходного кода iodine — программного обеспечения с открытым исходным кодом, позволяющего выполнять туннелирование данных IPv4 через DNS-сервер.

Согласно анализу BlackBerry, опубликованному на Black Hat 2020, вредоносное ПО для Linux, применяемое в целях шпионажа против различных компаний полупроводниковой промышленности на Тайване, используется совместно пятью разными китайскими APT-группами, отколовшимися от Winnti. Набор инструментов состоит из шести различных элементов. Первый — это bash-скрипт установщика, сжатый внутри другого шелл-скрипта, задача которого — работать с удаленным сервером сборки. Сервер сборки динамически компилирует пакет вредоносных программ для конкретной цели, затем установщик загружает его в инфраструктуру жертвы. Вредоносная полезная нагрузка включает руткит и бэкдор, а также скрипт установки. Пятый элемент, панель управления атакующих, может

одновременно управлять целями как в Windows, так и в Linux. Наконец, последний элемент — это ботнет Linux XOR DDoS.

PoetRAT

В апреле 2020 исследователи из Cisco сообщили о кампании, нацеленной на энергетические компании и компании государственного сектора в Азербайджане (в том числе на системы SCADA). Атакующие, не принадлежащие ни к одной известной группировке, использовали новое средство удаленного администрирования (RAT) совместно с различными инструментами, нацеленными на кражу учетных данных и сбор ценных данных: запись видео с веб-камер и кражу учетных данных браузера.

В качестве дроппера использовались вредоносные документы Word. RAT, написанный на Python, получила название PoetRAT, поскольку в макросах, встроенных во вредоносные документы Word, есть упоминания различных сонетов Уильяма Шекспира.

В сентябре и октябре 2020 года наблюдались новые целевые фишинговые кампании с использованием обновленных вредоносных программ, в которых скрипты Python были переведены на язык LUA.

Атаки на системы водоснабжения Израиля

В апреле стало известно о кибератаке на критически важную инфраструктуру Израиля, которую приписывают Ирану. Синхронизированная организованная атака была нацелена на систему водоснабжения страны. Инцидент произошел в конце апреля 2020 года. Неясно, удалось ли злоумышленникам получить контроль над какими-либо системами: согласно внутреннему отчету, инцидент был предотвращен киберотделом. Представители Управления водного хозяйства Израиля приказали всем сотрудникам немедленно сменить пароли, «уделяя особое внимание рабочим системам и, в частности, контролю хлора».

В мае, вскоре после новости об атаке на систему водоснабжения Израиля, стало известно, что Израилю приписывается кибератака на иранский порт Шахид Раджаи.

Mikroceen

В мае компания ESET представила технический анализ бэкдора, который использовался в различных целевых атаках на государственные и частные организации с конца 2017 года. Целями атакующих были телекоммуникационные компании, государственные учреждения и компании газовой промышленности в Центральной Азии.

ESET считает, что это вредоносное ПО может быть связано с прошлыми громкими атаками — на российские вооруженные силы (описаны «Лабораторией Касперского»), на правительство Беларуси (описаны Palo Alto) и на государственный сектор Монголии (описаны Check Point).

В арсенал злоумышленников входит средство удаленного администрирования (RAT) Mikroceen (бэкдор на стороне клиента), а также техники бокового перемещения с использованием Mimikatz, WMI и Gh0st RAT. Открытые каталоги на командных серверах, обнаруженные в предыдущем и текущем исследовании, а также утечка инструментов свидетельствуют о слабой операционной безопасности на стороне злоумышленников.

Chafer / APT39 / Remix Kitten

Согласно исследованию компании Bitdefender, APT-группировка Chafer (также известная как APT39 и Remix Kitten) с 2018 года проводила кампании по кибершпионажу, направленные на воздушный транспорт и правительственные организации Кувейта и Саудовской Аравии, вероятно, с целью исследования и кражи данных. В кампаниях использовались инструменты, созданные из подручных средств (“living off the land”), а также инструменты взлома, сканирования и написанные на Python кастомизированные бэкдоры. Активность атакующих приходилась на выходные дни, для компрометации жертв использовалась социальная инженерия.

TA410

В июне исследователи из компании Proofpoint опубликовали результаты анализа нового семейства вредоносного ПО, названного FlowCloud. Это семейство использовалось в кампаниях против коммунальных компаний США между июлем и ноябрем 2019 года.

Это вредоносное ПО обладает функциональностью удаленного администрирования (RAT), обеспечивающей злоумышленникам полный контроль над зараженной системой, включая доступ к установленным приложениям, клавиатуре, мыши, экрану, файлам, службам и процессам, а также возможность отправлять украденную информацию через командный сервер. Вначале вредоносное ПО распространялось во вложениях в виде исполняемых файлов (PE), однако в ноябре злоумышленники перешли на документы Microsoft Office с внедренными макросами. В кампаниях ноября 2019 года фишинговые письма, содержащие вредоносное ПО, отправлялись от имени Американского общества инженеров-строителей (American Society of Civil Engineers,ASCE) с адреса, замаскированного под легитимный домен ASCE.

FlowCloud распространялось одновременно с вредоносным ПО LookBack, которое также применялось в атаках на коммунальные компании США. Исходя из использования общих макросов во вложениях, аналогичных способов установки вредоносного ПО и перекрывающейся инфраструктуры Proofpoint атрибутирует и LookBack, и FlowCloud группировке TA410. Исследователи также обнаружили определенное сходство между группировками TA410 и TA429 (APT10) в плане макросов, используемых этими группировками во вложениях, и инфраструктуры, однако не исключено, что это сходство — результат намеренного запутывания следов злоумышленниками.

Lazarus

«Лаборатория Касперского» тщательно отслеживает продолжающуюся активность группировки Lazarus. В начале 2020 года отмечалось, что Lazarus нацелилась на людей, работающих в сфере науки и в автомобильной промышленности, используя при этом стратегии, похожие на применяемые ранее в атаках на бизнес, связанный с криптовалютами. В этих кампаниях Lazarus использует загрузчик, который отправляет информацию о скомпрометированном устройстве и выборочно извлекает данные, используемые для следующих этапов. В честь загрузчика кампания и получила свое название — DeathNote. В ней применялись документы-приманки, содержащие описания должностей, связанных с аэрокосмической и оборонной отраслями.

Группа Lazarus стала использовать новые методы доставки своих инструментов. Прежде всего, они разработали собственный документ-приманку, применив методы удаленного внедрения шаблонов. Ранее они доставляли жертвам документы со встроенными макросами, но затем стали

применять еще один этап, чтобы помешать обнаружению. Для создания троянских приложений они использовали Sumatra PDF — программу для чтения PDF-файлов с открытым исходным кодом. Атакующие создали троянскую программу для чтения PDF-файлов, которую отправляют жертвам вместе с созданным ими PDF-файлом. Если жертва открывает этот файл, троянская программа просмотра PDF-файлов внедряет вредоносные файлы и показывает ложные документы, чтобы обмануть жертву. Злоумышленники очень осторожно доставляют финальную часть вредоносной нагрузки и выполняют ее в памяти. К счастью, финальная часть вредоносного ПО была обнаружена. Это оказался вариант Manuscrypt, одного из активно используемых инструментов Lazarus. Это тот же вариант вредоносного ПО, данные о котором опубликовало агентство Cybersecurity and Infrastructure Security Agency (CISA), — COPPERHEDGE.

22 июля «Лаборатория Касперского» обнаружила подозрительный файл архива, загруженный на VirusTotal из итальянского источника. Файл представлял собой список вредоносных скриптов, журналов доступа, файлов вредоносных документов и нескольких снимков экрана, связанных с обнаружением подозрительных файлов с помощью решений безопасности. Исследователи «Лаборатории Касперского» определили, что эти вредоносные файлы связаны с кампанией DeathNote группы Lazarus, и уверены, что они имеют отношение к атаке на израильскую оборонную компанию. Были обнаружены скрипты веб-шелл, скрипты для командного сервера и вредоносные документы, идентифицированы несколько пользователей, подключившихся к взломанному командному серверу, а также метод, используемый для доступа к командному серверу.

Летом 2020 года «Лаборатория Касперского» выяснила, что группа Lazarus начала атаки на оборонную промышленность в глобальном масштабе с помощью кластера ThreatNeedle. Группа использовала тему COVID-19 в адресных фишинговых письмах, содержащих личную информацию получателей, собранную из общедоступных источников. Закрепившись в системе, злоумышленники собирали учетные данные жертв и продвились дальше, ища ключевые ресурсы в среде жертвы. Они преодолели сегментацию сети, получив доступ к компьютеру с внутренним маршрутизатором и настроив его как прокси-сервер. Это позволило им пересылать украденные данные из внутренней сети на свой удаленный сервер. Группа настроила командные серверы для разных этапов атаки, повторно используя отдельные скрипты, которые уже использовались в предыдущих атаках Lazarus.

Еще одну кампанию, возможно, имеющую связь с группой Lazarus, проанализировали исследователи ESET. Целевые атаки на аэрокосмические

и военные компании в Европе и на Ближнем Востоке имели место с сентября по декабрь 2019 г. Атаки, получившие название Operation In(ter)ception, основывались на социальной инженерии с использованием LinkedIn, а также многоэтапном применении кастомизированного вредоносного ПО. Чтобы действовать незаметно, злоумышленники часто перекомпилировали вредоносное ПО, использовали собственные утилиты Windows и имитировали работу легального программного обеспечения и компаний. Хотя убедительных доказательств связи этих атак с известными злоумышленниками не обнаружилось, исследователи нашли несколько свидетельств, указывающих на возможную связь с группой Lazarus, включая сходство целей, среды разработки и используемых методов сокрытия от анализа.

Gorgon APT

В августе компания Seqrite описала волну атак на микробизнес, малые и средние предприятия в Индии, приписываемую группе Gorgon (также известна как Subaat) — группе злоумышленников, которая считается связанной с интересами Пакистана. Отметим, что малые и средние предприятия, на которых занято около 40% рабочей силы страны, считаются основой индийской экономики. На них приходится почти 45% обрабатывающей промышленности Индии.

В описанных атаках темы, связанные с COVID, использовались для того, чтобы заставить жертв открыть вредоносные документы. Один из примеров — прикрепленный файл с именем "face mask order.zip" (заказ медицинских масок), который эксплуатировал уязвимость CVE-2017-11882 для выполнения произвольного кода на компьютере. Финальная часть вредоносного ПО — это клавиатурный шпион Agent Tesla.

CactusPete

В августе «Лаборатория Касперского» опубликовала отчет о деятельности в течение нескольких лет CactusPete — специализирующейся на кибершпионаже китайскоговорящей APT-группировки (также известна как LoneRanger, Karma Panda и Tonto Team),.

Сообщается, что группировка осуществляла целевые атаки на организации из Южной Кореи, Японии, США и Тайваня, по крайней мере, в период 2012 — 2014 годов. В 2018 году деятельность CactusPete существенно расширилась. В 2019 году группировка сосредоточилась на военных, дипломатических,

оборонных, производственных и правительственных целях в Азии и Восточной Европе. Также с 2018 года целями атак CactusPete становились предприятия в добывающей, энергетической, финансовой и телекоммуникационной сфере.

Весьма вероятно, что в течение последних шести лет CactusPete полагалась на одну кодовую базу и варианты вредоносных имплантов. Группировка занимается целевым фишингом, развертывает эксплойты Word и Equation Editor, применяет переупакованные уязвимости нулевого дня в VBScript, использованные ранее группой DarkHotel, поставляет модифицированные и скомпилированные уникальные варианты Mimikatz — средства кражи учетных данных, кейлоггеры, различные эксплойты повышения привилегий, старые утилиты, обновленный набор бэкдоров и модулей бэкдоров. «Фирменный» бэкдор группы CactusPete был назван Bisonal или Korlia (варианты Dustbiscuit). Он обновлялся и использовался в атаках, начиная с 2019 года. Также в кампании 2019 года APT-группировка CactusPete использовала новый метод установки на компьютеры обновленной версии бэкдора DoubleT. Злоумышленники внедрили новый модуль-установщик в папку автозагрузки Microsoft Word, скорее всего, используя вредоносный документ. Этот вредоносный установщик отвечает за установку и запуск новой версии бэкдора DoubleT, использующего новый метод шифрования адреса командного сервера.

«Лаборатория Касперского» обнаружила связь между вредоносной программой ShadowPad и группой CactusPete. В начале 2019 года группа CactusPete использовала бэкдор HighProof и начала развертывание вредоносной программы ShadowPad против нескольких жертв. В конце 2019 года вредоносная программа ShadowPad уже широко использовалась в атаках CactusPete.

Вредоносное ПО ShadowPad было впервые обнаружено «Лабораторией Касперского» в 2017 году. После тщательного расследования был найден легальный программный модуль, который был взломан и использован в сложной атаке на цепочку поставок. С тех пор вредоносная программа ShadowPad использовалась в ряде крупных кибератак, при этом для разных атак использовались разные наборы плагинов. Основными примерами таких атак являются инцидент CCleaner в 2017 году и атаки ShadowHammer в 2018 году.

Palmerworm / BlackTech

В сентябре компания Symantec рассказала, как группа Palmerworm (также известная как BlackTech) использовала ранее неизвестное вредоносное ПО

в шпионских атаках на организации в Японии, США, Китае и на Тайване. Атаки, начавшиеся в 2019 году и продолжившиеся в 2020 году, нацелены на организации в сфере СМИ, строительства, машиностроения, электроники и финансов. В этой кампании злоумышленники использовали собственное вредоносное ПО, инструменты двойного назначения и подручные средства («living-off-the-land»). Palmerworm также применяла украденные сертификаты для подписи своего вредоносного ПО. Symantec не выяснила, какой вектор заражения группа Palmerworm использовала для получения первоначального доступа к сетям жертв в рамках этой кампании, однако ранее было зафиксировано, что для получения доступа к сетям атакуемых компаний использовалась адресная рассылка фишинговых электронных писем.

IAmTheKing

1 октября 2020 года агентство DHS CISA опубликовало информацию о семействе вредоносных программ SlothfulMedia, приписываемых продвинутым злоумышленникам. «Лаборатория Касперского» с 2018 года отслеживала активность этой группы в своих приватных отчетах и поделилась некоторой информацией.

Группировка получила название IAmTheKing — соответствующие строки были обнаружены в образце используемой атакующими вредоносной программы. С 2018 года в арсенале IAmTheKing были выявлены различные семейства вредоносных программ — KingOfHearts, QueenOfHearts и QueenOfClubs, последнее из которых агентство DHS CISA назвало SlothfulMedia. Помимо вредоносных программ этих семейств группа использовала бэкдор PowerShell, утилиту для снимков экрана, утилиты Windows ProcDump и PsExec, а также общедоступные техники бокового перемещения с помощью LaZagne и Mimikatz.

До 2020 года группа IAmTheKing занималась исключительно сбором секретных данных крупных российских организаций. Среди пострадавших — государственные органы, подрядчики военных заказов, государственные строительные агентства, университеты и компании энергетического сектора. В 2020 году были также обнаружены отдельные инциденты с участием IAmTheKing в странах Центральной Азии и Восточной Европы. DHS CISA также сообщает о деятельности группировки на Украине и в Малайзии.

MontysThree

В октябре 2020 года «Лаборатория Касперского» опубликовала отчет о новой вредоносной активности. Летом 2020 года «Лаборатория Касперского» обнаружила ранее неизвестный многомодульный набор инструментов C++, используемый в целевых атаках промышленного шпионажа с 2018 года. Никакого сходства с уже известной вредоносной активностью в отношении кода, инфраструктуры, тактики, методов и процедур (TTP) не наблюдалось, поэтому набор инструментов и атакующая группировка были признаны новыми. Авторы вредоносной программы назвали набор инструментов MT3. Согласно этой аббревиатуре набор инструментов получил название MontysThree.

MontysThree настроен для поиска определенных типов документов, включая хранящиеся на съемных носителях. Он содержит языковые артефакты правильного русского языка и конфигурации для поиска папок, существующих только в кириллических версиях Windows. Вредоносная программа использует основные легальные облачные сервисы, такие как Google, Microsoft и Dropbox, для связи с командным сервером. Она также использует кастомизированную стеганографию и несколько схем шифрования: помимо настраиваемого XOR-шифрования, модули используют алгоритмы 3DES и RSA для расшифровки конфигурации и обмена данными. Модуль начальной загрузки распространяется внутри самораспаковывающихся архивов RAR с именами, связанными со списком номеров телефонов сотрудников, технической документацией и результатами медицинских тестов, и маскируется под файлы pdf или doc.

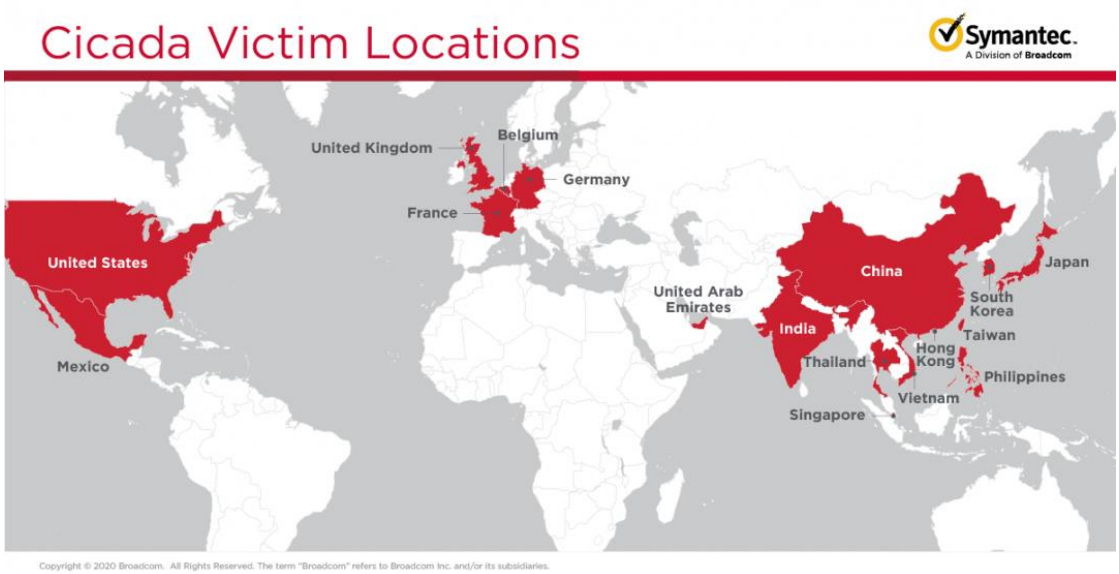
MuddyWater

Согласно отчету компании Telsy, опубликованному в октябре, APT группировка MuddyWater в мае 2020 года использовала социальную инженерию, нацеленную на сотрудников аэрокосмической отрасли и авионики в Италии. Все жертвы подверглись атаке через LinkedIn; злоумышленники маскировались под рекрутеров компании, занимающейся созданием спутниковых снимков. Сотрудникам атакуемых компаний было предложено скачать вложение, содержащее информацию о фальшивом отпуске на работе. Загруженные вложения представляли собой архив, содержащий файл vCard (VCF), использующий уязвимость 2019 года (ZDI-19-013, ZDI-CAN-6920), которая позволяет запускать локальный файл, когда пользователь переходит по ссылке на веб-сайте.

Атакующие использовали сложную, многоэтапную цепочку заражений, основанную на скриптах PowerShell и исполняемых файлах, результат работы которой — внедрение мощного ранее неизвестного средства удаленного администрирования (RAT). В компании Telsy утверждают, что атакующие были заинтересованы в получении информации именно о космических и аэрокосмических исследованиях.

Cicada / APT10

В ноябре компания Symantec сообщила о кампании продолжительностью один год, нацеленной на японские компании, включая дочерние компании в 17 странах по всему миру, которая приписывается группировке Cicada (также известной как APT10, Stone Panda и Cloud Hopper). Цели этой кампании относятся к разным отраслям, включая автомобильную, фармацевтическую, машиностроительную, а также работу поставщиков управляемых услуг (MSP).



Страны, в которых находились компании, атакованные Cicada (Источник: Symantec)

В этих атаках злоумышленники использовали широкий спектр подручных инструментов, техник двойного назначения и общедоступных средств. Они использовали собственное вредоносное ПО Backdoor.Hartip, динамическую загрузку библиотеки DLL и уязвимость ZeroLogon.

SolarWinds

13 декабря 2020 года компании FireEye, Microsoft и SolarWinds объявили об обнаружении крупной сложной атаки на цепочку поставок с эксплуатацией уязвимостей Orion IT — платформы мониторинга и управления инфраструктурой компании SolarWinds. Атака на цепочку поставок SolarWinds была разработана очень профессионально, с четким акцентом на то, чтобы вредоносный код оставался незамеченным как можно дольше. Вредоносное ПО Sunburst, используемое в атаке, включает сложную схему отчетности, проверки и обновления атакуемой системы, и напоминает другие атаки на цепочки поставок, такие как Shadowhammer и Shadowpad. Официально подтверждено, что около 18 000 пользователей могли установить версию SolarWinds с бэкдором, хотя информация о количестве организаций, в которых атака получила развитие и были развернуты инструменты второго этапа, ограничена.

В рамках проекта Kaspersky ICS CERT были проанализированы общедоступные данные о DNS-именах и телеметрии, что позволило определить, сколько промышленных организаций использовали версию SolarWinds с бэкдором. Однако не удалось получить никаких доказательств того, что какая-либо из промышленных организаций, отправлявших телеметрию, подверглась атакам со стороны злоумышленников. Есть предположения о нескольких промышленных организациях, представляющих интерес для злоумышленников, список которых был получен на основе анализа истории DNS-ответов от сервера управления. Некоторые организации из этого списка возможных жертв второй стадии атаки уже подтвердили, что их системы были скомпрометированы.

Заключение

Основные тенденции, наблюдаемые в отчетах об APT-угрозах в 2020 году:

1. Атакующие расширяют набор своих целей, включая в него промышленные организации; расширяется также география атак.
2. Злоумышленники используют пандемию COVID-19 для привлечения потенциальных жертв.
3. Геополитика остается важным мотивом для некоторых APT-группировок, о чем свидетельствует деятельность группы MuddyWater (компрометация системы водоснабжения Израиля), активность группы PoetRAT и другие атаки.
4. В 2020 году была обнаружена весьма изощренная атака на цепочку поставок, скомпрометировавшая программное обеспечение SolarWinds, отличающаяся от других атак своим масштабом и сложностью.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com