Kaspersky ICS CERT

kaspersky

APT и финансовые атаки на промышленные организации во второй половине 2023 года

02.04.2024

Version 1.0

Этот документ содержит обзор сообщений об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта во втором полугодии 2023 года, а также об активности киберпреступных групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. В каждом случае мы постарались кратко изложить основные факты, а также привести полученные исследователями результаты и сделанные выводы, которые, по нашему мнению, могут быть полезны специалистам, занимающимся практическими вопросами кибербезопасности промышленных предприятий.

Среди множества историй выделяются три. В двух из них описываются векторы атак, в результате которых злоумышленники получили доступ к АСУ, и атаки привели к физическому эффекту. Это атака на украинскую энергетическую компанию и атаки на ПЛК Unitronics израильского производства. Третья история — атака на промышленные компании с помощью инструментария MATA — интересна высокой сложностью использованного злоумышленниками инструментария, захватывающим рассказом о продвижении злоумышленников внутри сети скомпрометированной организации и интригой, возникшей при попытке отнесения инструментария к известным APT-группировкам.

Активность корейскоязычных групп

Атаки Lazarus

Атаки на предприятия оборонной промышленности и специалистов по ядерной энергетике

Исследователи «Лаборатории Касперского» обнаружили активную с 2023 года кампанию группы Lazarus, целями которой были предприятия оборонной промышленности и специалисты по ядерной энергетике. Для доступа к корпоративным системам атакующие используют троянизированные приложения, в частности VNC-приложения, содержащие бэкдоры.

В рамках этой кампании злоумышленники из группы Lazarus в социальных сетях убеждают соискателей работы открывать вредоносные приложения якобы для прохождения собеседований. Чтобы избежать обнаружения защитными решениями, использующими поведенческий анализ, приложение-бэкдор работает скрытно, активируясь только когда пользователь выбирает сервер в раскрывающемся меню

троянизированного VNC-клиента. После активации и начального заражения приложение запускает в памяти дополнительную полезную нагрузку и извлекает новый вредоносный код.

Обнаруженный исследователями «Лаборатории Касперского» дополнительный зловред известен как LPEClient и ранее неоднократно применялся группой Lazarus. Он использует продвинутые способы взаимодействия с командным сервером и отключает мониторинг поведения приложений защитными решениями путем удаления хуков для системных вызовов в пользовательском режиме. Было выявлено использование обновленной версии COPPERHEDGE в качестве дополнительного бэкдора, что указывает на наличие комплексной цепочки заражения. Кроме того, исследователи обнаружили вариант этого зловреда, специально предназначенный для передачи нужных файлов с атакуемого компьютера на удаленный сервер. Зловред выполняет эксфильтрацию конкретных файлов, выбранных группой Lazarus, и отправляет их на определенный удаленный сервер.

Данные нашей телеметрии подтвердили многочисленные случаи компрометации различных компаний. В большинстве своем это предприятия, непосредственно связанные с производством оборонной продукции (включая радарные системы, беспилотные летательные аппараты (БПЛА), военные транспортные средства, суда, оружие), а также организации, связанные с морским флотом. Кроме того, в одном из случаев удалось выйти на жертву первоначального заражения. В ходе общения с жертвой исследователи «Лаборатории Касперского» выяснили, что это инженер-ядерщик из Венгрии, который получил вредоносный файл после контакта с подозрительным аккаунтом в Telegram и WhatsApp.

Кампания с использованием бэкдора LightlessCan

Исследователи из компании ESET обнаружили вредоносную кампанию с использованием ранее неизвестного бэкдора LightlessCan. Группе Lazarus удалось скомпрометировать аэрокосмическую компанию в Испании. Начальным вектором атаки была рассылка целевых фишинговых писем; хакеры выдавали себя за рекрутеров из компании Meta и отправляли сообщения разработчикам через систему сообщений LinkedIn.

Бэкдор LightlessCan для Windows умеет имитировать функции многих встроенных команд Windows, таких как ping, ipconfig, systeminfo, sc, net и т.д. В ESET предположили, что при разработке LightlessCan группа Lazarus могла провести реверс-инжиниринг проприетарных системных бинарных файлов, чтобы добавить в RAT-зловред дополнительный функционал. Злоумышленники также настроили LightlessCan таким образом, что

его зашифрованная полезная нагрузка может быть расшифрована только с помощью ключа, который специфичен для скомпрометированного компьютера. Цель состоит в том, чтобы расшифровка полезной нагрузки была возможна в целевой системе и невозможна в какой-либо другой, например в системе, принадлежащей исследователю безопасности.

Operation Blacksmith

Новая кампания группы Lazarus получила у исследователей из Cisco Talos название Operation Blacksmith. В ней еще с марта 2023 года используется как минимум три новых штамма вредоносного ПО на языке DLang для атак по всему миру на организации в сфере производства, сельского хозяйства и физической безопасности. Эта кампания заключается в постоянных оппортунистических атаках на предприятия по всему миру, уязвимая инфраструктура которых размещается в открытом доступе. Эксплуатируются уязвимости n-го дня, такие как CVE-2021-44228 (Log4j).

Два варианта применяемого в атаках вредоносного ПО представляют собой RAT-зловреды. Один из них, NineRAT, использует телеграм-боты и телеграм-каналы для взаимодействия с командным сервером. RAT-зловред, не использующий Telegram, получил у исследователей название DLRAT, а загрузчик, написанный на DLang, фигурирует под названием BottomLoader. Исследователи заметили совпадение между тактиками и методами этой кампании и тактиками и методами, применяемыми группой Onyx Sleet (также известной под названиями PLUTONIUM и Andariel).

Атака на российское ракетостроительное предприятие

Исследователи из SentinelLabs сообщили, что две APT-группы получили постоянный доступ к внутренним системам российского разработчика ракет и спутников. Группа ScarCruft скомпрометировала почтовые системы компании, а группа Lazarus скомпрометировала ее сеть с помощью бэкдора для Windows под названием OpenCarrot. Проанализированный вариант бэкдора OpenCarrot реализует более 25 команд с широким набором функциональных возможностей, характерных для бэкдоров группы Lazarus. Результаты исследования показывают связь между двумя различными группами, связанными с КНДР; допускается возможность совместного использования ими ресурсов, инфраструктуры, имплантов или доступа к сетям жертв.

Атаки Andariel

Исследователи AhnLab Security Emergency Response Center (ASEC) проанализировали недавние атаки группы Andariel на университеты и компании из сферы информационно-коммуникационных технологий, электронного оборудования, судостроения и производства в Южной Корее. Характерной особенностью атак является использование новых вредоносных программ, разработанных на языке Go, включая Goat RAT и DurianBeacon. Последняя также имеет версию, написанную на языке Rust. В одной из атак, обнаруженных ASEC в феврале 2023 года, как утверждается, для распространения бэкдоров, таких как Volgmer и Andardoor, а также reverse shell на языке Golang, известного как 1th Troy, использовались уязвимости в корпоративном решении для передачи файлов под названием Innorix Agent.

Сообщалось о крупной кампании кибершпионажа, в ходе которой APT-группа Andariel взломала целый ряд компаний в Южной Корее и похитила конфиденциальную информацию, связанную с обороной. Расследование ведет полиция Сеула при участии ФБР США. По мнению официальных лиц, хакерам удалось похитить информацию о лазерном оружии, которое используется для обеспечения работы национальной системы ПВО. Органы власти считают, что эти атаки были частью более масштабной киберкампании, в результате которой было украдено более 1,2 ТБ данных, включая корпоративные, государственные и личные данные.

Группе Andariel удалось успешно взломать 14 организаций, также ставших жертвами атак с использованием программ-шифровальщиков. Атаки проводились через слабо контролируемый южнокорейский прокси-сервер, который использовался хакерами 83 раза с декабря 2022 года по март 2023 года из района Рюгён-дон в Пхеньяне. Этот сервер использовался для доступа к веб-сайтам фирм и учреждений, причем группа воспользовалась услугами южнокорейского хостинг-провайдера, который сдает серверы в аренду неидентифицированным клиентам. Среди жертв этих атак — крупные компании в сфере связи, информационной безопасности и информационных технологий, технологические центры, университеты и исследовательские институты, занимающиеся передовыми разработками и технологиями, фармацевтические компании, оборонные предприятия, финансовые организации.

Атаки с использованием обновленного фреймворка MATA на промышленные предприятия в Восточной Европе

Эксперты «Лаборатории Касперского» обнаружили новую активную кампанию с использованием фреймворка MATA, в ходе которой были скомпрометированы организации-подрядчики в сфере оборонной промышленности стран Восточной Европы. Кампания длилась более полугода вплоть до мая 2023 года, и в ней было задействовано сразу три новых поколения MATA.

Одна из вредоносных программ является доработанной версией MATA второго поколения. Следующая, которой мы присвоили имя MataDoor, была написана с нуля и может рассматриваться как версия четвертого поколения; версия пятого поколения также была создана с нуля. Во всех этих версиях есть изменения в механизмах шифрования, конфигурации и коммуникационных протоколах.

Злоумышленники продемонстрировали широкие возможности по обходу и использованию в собственных целях защитных решений, установленных в атакованных средах. В ситуациях, когда установить коммуникацию с целевой системой не представлялось возможным, злоумышленники использовали модуль для работы с USB-носителями, позволяющий обмениваться данными с изолированными сетями. Злоумышленники применили множество техник для сокрытия своей активности: использование руткитов и уязвимых драйверов, маскировка файлов под пользовательские приложения, использование портов, открытых для коммуникации легитимных программ, многоуровневое шифрование файлов и сетевой активности вредоносного ПО, установка длительного времени ожидания между подключениями к серверам управления. Это и многое другое показывает насколько сложны могут быть современные таргетированные атаки.

С самых первых версий фреймворка MATA у исследователей имелись некоторые сомнения, как его атрибутировать. С появлением последних поколений MATA это сомнение еще более возросло. С одной стороны, существуют очевидные аргументы, связывающие MATA с APT-группой Lazarus. В то же время, в последних поколениях MATA обнаруживается все больше техник, аналогичных тем, которые используют APT-группы альянса Five Eyes.

Активность, связанная с Ближним Востоком

Атаки Dark Caracal

Отслеживая деятельность группы Dark Caracal, исследователи «Лаборатории Касперского» обнаружили продолжающуюся кампанию, нацеленную на государственные и частные организации в нескольких испаноязычных странах. Dark Caracal известна по кампаниям кибершпионажа как минимум с 2012 года. Атаки направлены против правительственных и военных организаций, коммунальных служб, финансовых учреждений, производственных компаний и военных подрядчиков по всему миру. Известно, что от Dark Caracal страдают тысячи жертв — похищенными оказываются ценные данные, включая интеллектуальную собственность и персональную информацию. Dark Caracal называют «группой кибернаемников» из-за разнообразия целей и очевидной направленности ее кампаний на правительства разных стран. С 2021 года в числе жертв — организации в испаноязычных странах.

Атаки Ballistic Bobcat/Charming Kitten

Исследователи ESET обнаружили продвинутую кампанию кибершпионажа, которую проводила предположительно связанная с Ираном группа Ballistic Bobcat (также известная как APT35, APT42, Charming Kitten, TA453 и PHOSPHORUS). Группа использовала новый бэкдор под названием Sponsor для атак на организации в Бразилии, Израиле и ОАЭ. Среди жертв — предприятия из сферы автомобильной промышленности, производства, машиностроения, финансовых услуг, СМИ, здравоохранения, технологий и телекоммуникаций. Бэкдор Sponsor написан на C++ и предназначен для сбора информации о хосте и обработки команд, получаемых с удаленного сервера; результаты выполнения команд отправляются обратно на сервер.

Согласно отчету, в последней кампании под кодовым названием Sponsoring Access первоначальный доступ осуществляется путем использования известных уязвимостей в серверах Microsoft Exchange. В одном из инцидентов, описанных ESET, в августе 2021 года злоумышленниками была скомпрометирована израильская компания, и в течение нескольких месяцев осуществлялось внедрение инструментов следующих этапов, таких как PowerLess, Plink, а также ряда постэксплуатационных инструментов с открытым исходным кодом, написанных на языке Go.

По мнению экспертов, группа Ballistic Bobcat продолжает работать с помощью нового широкого арсенала инструментов, выискивая возможности использования неисправленных уязвимостей в серверах Microsoft Exchange, доступных из сети.

Атаки Imperial Kitten/Yellow Liderc/Tortoiseshell

По данным исследователей из PwC, APT-группа Liderc (также известная как Imperial Kitten, Tortoiseshell, TA456 и Crimson Sandstorm) проводит атаки типа watering hole для распространения вредоносной программы IMAPLoader, которая использует утилиты Windows для идентификации атакуемых систем и установки дополнительной полезной нагрузки. Целями кампании являются морские, судоходные и логистические организации в Средиземноморье, предприятия атомной, аэрокосмической и оборонной промышленности в США и Европе, а также поставщики управляемых IT-услуг на Ближнем Востоке. В новых атаках используется компрометация легитимных веб-сайтов с помощью вредоносного скрипта на JavaScript, предназначенного для эксфильтрации данных, однако в качестве начального вектора атаки злоумышленники также использовали поддельный документ Microsoft Excel.

После отчета PwC компания CrowdStrike сообщила, что та же самая группа (которую CrowdStrike называет Imperial Kitten) с самого начала конфликта в Палестине проводит атаки на предприятия из транспортной, логистической и технологической сфер на Ближнем Востоке, включая Израиль. Деятельность группы характеризуется использованием социальной инженерии, в частности материалов на тему трудоустройства, для доставки кастомных .NET-имплантов. Злоумышленники используют скомпрометированные веб-сайты для составления профиля посетителей с помощью специального скрипта на JavaScript и проводят эксфильтрацию данных. Помимо атак типа watering hole, злоумышленники также используют эксплойты первого дня, украденные учетные данные, фишинг и атакуют поставщиков IT-услуг для получения первоначального доступа.

Атаки OilRig

Исследователи из ESET проанализировали серию новых загрузчиков группы OilRig (также известной как APT34, Lyceum, Crambus и Siamesekitten), которые эта группа использовала в 2022 году в кампаниях, нацеленных на организации в Израиле, включая медицинскую организацию, производственную компанию и местный орган власти. Все жертвы были ранее затронуты несколькими другими кампаниями OilRig. Новые загрузчики,

получившие названия SampleCheck5000 (SC5k v1-v3), OilCheck, ODAgent и OilBooster, отличаются тем, что для взаимодействия с командным сервером и эксфильтрации данных, а также чтобы скрыть вредоносные коммуникации и замаскировать сетевую инфраструктуру группы, используют легитимные облачные хранилища и облачные почтовые сервисы — Microsoft OneDrive, Exchange Online и Office 365 через Microsoft Graph и Outlook API, а также API Microsoft Office Exchange Web Services (EWS). Эти загрузчики имеют сходство с бэкдорами MrPerfectionManager и PowerExchange — другими недавними новинками в наборе инструментов OilRig, использующими протоколы взаимодействия с командными серверами на базе почтовых коммуникаций.

Атаки Peach Sandstorm/APT33

По данным компании Microsoft, APT-группа Peach Sandstorm (также известная как APT33, Elfin и Refined Kitten) атаковала организации из сферы оборонной промышленности, используя новый бэкдор под названием FalseFont. Это кастомный бэкдор, позволяющий злоумышленникам получать удаленный доступ к зараженным системам, запускать дополнительные файлы и отправлять информацию на командный сервер. Впервые использование этого штамма зловреда было замечено примерно в начале ноября 2023 года. Разработка и использование FalseFont согласуется с активностью Peach Sandstorm, наблюдаемой Microsoft в течение последнего года. Это позволяет предположить, что Peach Sandstorm продолжает совершенствовать свои методы работы.

Активность китайскоязычных групп

Атаки групп TEMP.Hex и UNC4698 с использованием USB

Исследователи из компании Mandiant сообщили о трехкратном увеличении числа атак с использованием USB-накопителей в первой половине этого года. В одной из таких кампаний APT-группа TEMP.Hex (также известная как HoneyMyte) использовала USB-накопители для распространения вредоносной программы Sogu, предназначенной для кражи конфиденциальной информации из систем хостов. Исследователи полагают, что группа TEMP.Hex использует зловред Sogu для сбора информации, представляющей интерес для Китая с точки зрения экономики и национальной безопасности. TEMP.Hex атакует самые разные организации в Европе, Азии и США, включая государственные и медицинские

учреждения, транспортные организации, предприятия из сфер розничной торговли, строительства, разработки и предоставления бизнес-услуг.

Еще одна группа, фигурирующая у исследователей под именем UNC4698, также использует USB-накопители для распространения вредоносной программы SnowyDrive. SnowyDrive создает бэкдор в зараженных системах, позволяя злоумышленникам удаленно взаимодействовать с устройством. Бэкдор поддерживает множество команд, которые позволяют выполнять файловые операции, осуществлять эксфильтрацию данных, использовать reverse shell, выполнять команды и собирать информацию. Он также распространяется на другие USB-накопители и по сети. Зловред использует DLL Hijacking / Side-loading для загрузки вредоносной DLL-библиотеки посредством легитимных исполняемых файлов, таких как файлы Notepad++, Microsoft Silverlight, VentaFax Software и CAM UnZip Software. Атаки группы UNC4698 нацелены на нефтегазовые организации в Азии.

Атаки Space Pirates

Компания Positive Technologies опубликовала отчет о новых масштабных атаках на Российские и Сербские организации со стороны китайскоязычной группы Space Pirates, деятельность которой исследователи наблюдают с 2022 года. Основная цель группы — шпионаж и кража данных. Группа расширила сферу своих интересов. За последний год ее жертвами стали как минимум 16 организаций в России и одна — в Сербии (одно из министерств). Среди новых жертв можно выделить государственные и образовательные учреждения, предприятия из авиационной, ракетно-космической и сельскохозяйственной отраслей, предприятия военно-промышленного и топливно-энергетического комплекса, а также компании, занимающиеся информационной безопасностью.

На одном из командных серверов был обнаружен сканер уязвимостей Acunetix. Это указывает на вероятный вектор атаки, связанный с эксплуатацией уязвимостей, чего ранее не наблюдалось. Кроме того, целью группы были почтовые архивы PST.

На сервере C2 были обнаружены веб-шелл Godzilla и обфусцированный туннель Neo-reGeorg. Группа также начала использовать вредоносное ПО ShadowPad. Почти при каждом расследовании обнаруживались следы использования зловреда Deed RAT, который все еще находится в процессе разработки. При расследовании инцидента на одном из зараженных устройств была обнаружена 64-разрядная версия этого зловреда, которая практически ничем не отличается от 32-разрядной. На компьютерах, зараженных Deed RAT, были обнаружены два новых плагина.

Первый называется Disk и используется для работы с дисками. Второй плагин называется Portmap и основан на утилите ZXPortMap. Он используется для переадресации портов и поддерживает три сетевые команды.

В ходе одного из расследований был обнаружен ранее неизвестный образец зловреда. Он доставлялся через уже установленный Deed RAT и имел название Voidoor. Жизненный цикл этого зловреда включал взаимодействие через GitHub и форум voidtools. Этот форум, а также анализ репозиториев GitHub вывели исследователей на блог хакера в Китайской сети разработчиков программного обеспечения (CSDN). Исследователи Positive Technologies с определенной долей уверенности предполагают, что найденный автор является одним из разработчиков этого зловреда (если не единственным).

Атаки APT31

Команда Kaspersky ICS CERT выявила более 15 имплантов и их разновидностей, внедренных группой APT31 (также известной как Judgment Panda и Zirconium) в серии атак на промышленные предприятия в Восточной Европе с целью кражи конфиденциальных данных. Это вредоносное ПО обычно устанавливается с использованием подмены DLL (DLL Hijacking) и скрывает следы своей деятельности, с помощью алгоритма RC4 шифруя данные до момента внедрения. Это вредоносное ПО содержит компонент-червь, способный заражать съемные диски и красть конфиденциальные данные из изолированных сегментов сети. Среди других имплантов — разновидности бэкдора FourteenHi, бэкдор MeatBall, имплант, использующий платформу Yandex Cloud в качестве командного сервера, а также импланты, используемые для загрузки файлов в Dropbox.

Атаки UNC4841

В продолжение предыдущего исследования, посвященного эксплуатации группой UNC4841 уязвимости типа «удаленное внедрение команд» (remote command injection), затронувшей Barracuda Email Security Gateway (ESG) (CVE-2023-2868), исследователи из Mandiant предоставили более подробную информацию о методах и тактиках, которые используют эти злоумышленники.

Группа UNC4841 внедрила новое вредоносное ПО, задача которого — обеспечить присутствие злоумышленников на небольшом количестве

высокоприоритетных целей, скомпрометированных либо до выпуска исправления, либо вскоре после этого. При этом используются бэкдоры SKIPJACK и DEPTHCHARGE, а также программа запуска FOXTROT/FOXGLOVE.

Целями злоумышленников были организации из самых разных сфер: в первую очередь правительства государств, хайтек- и IT-компании, местные органы власти, операторы связи, производственные предприятия, колледжи и университеты. Агентство по кибербезопасности и защите инфраструктуры США (CISA) указало дополнительные индикаторы компрометации, связанные с эксплуатацией этой уязвимости.

Атаки Flax Typhoon

Исследователи из Microsoft сообщают, что недавно обнаруженная китайскоязычная APT-группа, получившая название Flax Typhoon, атаковала десятки организаций на Тайване. Flax Typhoon действует с середины 2021 года и атакует правительственные учреждения и учебные заведения, а также особо важные производственные и IT-организации на Тайване. Целью атак является кибершпионаж.

Группа стремится поддерживать доступ к организациям из самых разных отраслей как можно дольше. Flax Typhoon использует минимум вредоносных программ, в основном полагаясь на применение легитимных программ во вредоносных целях. Злоумышленники получали первоначальный доступ путем эксплуатации известных уязвимостей в публично доступных серверах (в VPN-, веб-, Java- и SQL-приложениях) и путем развертывания веб-шеллов, включая China Chopper.

По мнению некоторых исследователей, эта группа действует с середины 2021 года. Однако TeamT5, тайваньская команда по аналитике угроз, оспаривает это предположение, датируя деятельность этой группы, получившей временное кодовое название SLIME13, как минимум 2020 годом.

Атаки Volt Typhoon

Команда Black Lotus Labs из компании Lumen Technologies связала APT-группу Volt Typhoon (также известную как BRONZE SILHOUETTE) с ботнетом под названием KV-botnet, который компрометирует маршрутизаторы, брандмауэры и VPN-устройства для сокрытия вредоносного трафика внутри легитимного. Среди скомпрометированных устройств — брандмауэры Netgear ProSAFE, Cisco RV320, маршрутизаторы DrayTek Vigor и IP-камеры Axis.

KV-botnet использовался в атаках, направленных на телекоммуникационные компании и интернет-провайдеров, территориальное правительство США на острове Гуам, компанию по производству возобновляемых источников энергии в Европе и военные организации США, хотя исследователи классифицируют большинство заражений KV-botnet как оппортунистические.

Начиная с августа 2023 года исследователи наблюдают рост использования новых ботов для KV-botnet. Этот кластер заражал SOHO-устройства, связанные с несколькими крупными сетями. Хотя в исходном бинарном файле не было обнаружено никаких встроенных функций, позволяющих атаковать соседнюю локальную сеть, на SOHO-устройстве можно было создать удаленный терминал (remote shell). Эта возможность могла использоваться как для ручного выполнения команд, так и, возможно, для получения пока не обнаруженного исследователями дополнительного модуля для проведения атак на соседнюю локальную сеть.

Атаки Redfly

Компания Symantec обнаружила новую группу злоумышленников, получившую название Redfly, которая проникла в национальную энергосистему одной из азиатских стран, используя троянец ShadowPad. В отчете говорится, что злоумышленникам удалось украсть учетные данные и скомпрометировать несколько компьютеров в сети организации, и эта атака является последней в серии шпионских вторжений в критическую национальную инфраструктуру страны.

Вариант ShadowPad маскируется под файлы и каталоги VMware на зараженных машинах и закрепляется в системе, регистрируя службу, которая запускается при запуске Windows. Было замечено, что помимо ShadowPad группа Redfly внедряет инструмент PackerLoader для загрузки и выполнения шеллкода, а также кейлоггер, который на разных компьютерах устанавливался под разными именами. Группа действовала довольно методично и последовательно изменяла разрешения для драйвера, который впоследствии использовался для создания дампов файловой системы и получения учетных данных из реестра Windows. Хакеры использовали инструмент для дампа учетных данных из LSASS, а с помощью запланированной задачи осуществлялся запуск Oleview для загрузки файлов с помощью техники side-loading и горизонтального перемещения. Чтобы установить кейлоггер на скомпрометированный компьютер, злоумышленники пытались получить дамп учетных данных с помощью утилиты ProcDump.

По мнению Symantec, наиболее очевидным мотивом группы является шпионаж. Идентифицированные инструменты и инфраструктура, использованные в недавней кампании против энергосистемы одной из стран, имеют пересечения с ранее зарегистрированными атаками, которые приписывались группе APT41 (известной также как Brass Typhoon, Wicked Panda, Winnti и Red Echo).

Атаки на компании по производству полупроводников в Восточной Азии

Компании по производству полупроводников в Восточной Азии (Тайвань, Гонконг, Сингапур) подверглись атаке с использованием сообщений, якобы исходящих от Taiwan Semiconductor Manufacturing Company (TSMC).

В атаках применялся бэкдор HyperBro, который использовал электронно подписанный бинарный файл CyberArk (fv_host.exe, переименованный злоумышленниками в vfhost.exe) для динамической загрузки сторонних DLL, в результате чего в памяти выполнялся имплант Cobalt Strike Beacon. Адрес командного сервера, заданный в коде импланта Cobalt Strike, был замаскирован под легитимный адрес jQuery CDN, что позволило обойти защиту брандмауэра.

Во втором варианте атаки хакеры использовали взломанный веб-сервер Cobra DocGuard для загрузки дополнительного бинарного файла McAfee (mcods.exe) и вредоносного файла (который потом загружается в mcods.exe с использованием техники DLL side-loading и зашифрованный шеллкод Cobalt Strike. В данном случае хакеры использовали ранее недокументированный бэкдор на языке Go под названием ChargeWeapon, предназначенный для сбора и передачи данных жертвы, закодированных по алгоритму Base64, на командный сервер.

Исследователи из EclecticIQ приписали эту кампанию связанной с Китаем APT-группе из-за использования ею зловреда HyperBro, который почти всегда применялся группой Lucky Mouse (также известной как APT27, Budworm и Emissary Panda). Они также обнаружили тактические сходства с RedHotel и Earth Lusca.

Активность русскоязычных групп

Атаки с использованием DroxiDat/SystemBC

Неизвестные злоумышленники атаковали электроэнергетическую компанию в Африке, используя Cobalt Strike Beacon и DroxiDat, новый вариант полезной нагрузки SystemBC. Эта атака произошла на третьей и четвертой неделях марта 2023 года в ходе небольшой волны атак по всему миру. В одном из нескольких связанных между собой инцидентов был обнаружен шифровальщик Nokoyawa, который связан с эксплуатацией уязвимости нулевого дня и, возможно, связан с группой, распространявшей шифровальщик Hive. На сегодняшний день группа, стоящая за использованием шифровальщика Nokoyawa, не имеет точной политической атрибуции. Однако, судя по всему, программа используется одной из старых русскоязычных киберпреступных групп или одним из партнеров разработчиков шифровальщика (возможно, Pistachio Tempest или FIN12).

Атаки APT29/Midnight Blizzard/Nobelium

Исследователи из Microsoft сообщают, что группа Midnight Blizzard (также известная как Nobelium) использует чаты Microsoft Teams для атак на сотрудников правительств, неправительственных организаций, IT-служб, технологических компаний, предприятий дискретного производства и СМИ. В целом, по данным текущего расследования, эта кампания затронула до 40 отдельных организаций по всему миру.

Злоумышленники использовали скомпрометированные учетные записи Microsoft 365 для создания доменов, маскирующихся под организации, предоставляющие техническую поддержку. Затем они используют эти домены для отправки в чате сообщений со ссылками на фишинговые веб-страницы. С их помощью злоумышленники пытаются получить учетные данные получателя сообщения, в частности код многофакторной аутентификации.

Команда реагирования на инциденты FortiGuard сообщила, что в октябре 2023 года американская организация по производству биомедицинских препаратов была скомпрометирована из-за критической уязвимости в TeamCity (CVE-2023-42793), эксплойт для которой был опубликован 27 сентября 2023 года. TeamCity — это продукт компании JetBrains, используемый для контроля и автоматизации процессов компиляции, сборки, тестирования и выпуска программного обеспечения.

Изначально атака осуществлялась с использованием кастомного скрипта-эксплойта, написанного на Python. Злоумышленники использовали эксплойт для TeamCity, чтобы установить сертификат SSH, который использовался для обеспечения доступа к рабочей среде другой жертвы. После выполнения команд обнаружения злоумышленники загружали DLL-файл AclNumsInvertHost.dll на хост TeamCity и снова использовали RCE-уязвимость в TeamCity для создания в Windows запланированной задачи, в которой использовалась ссылка на этот DLL-файл в целях закрепления в системе.

Библиотека AclNumsInvertHost.dll и несколько других DLL-файлов, полученные с веб-сервера злоумышленников, соответствуют правилу Yara для известного семейства вредоносных программ под названием GraphicalProton, которое исторически было связано с группой APT29 (также известной как Dukes, CozyBear и NOBELIUM/Midnight Blizzard/BlueBravo). Учитывая сходство применяемых методов с ранее зафиксированной деятельностью и результаты идентификации полезной нагрузки GraphicalProton, специалисты FortiGuard со средней степенью уверенности предполагают, что эта атака была частью новой кампании группы BlueBravo/APT29.

В совместном сообщении, опубликованном 13 декабря, ФБР, Агентство по кибербезопасности и защите инфраструктуры (CISA), АНБ США, Служба военной контрразведки Польши (SKW), CERT Polska (CERT.PL) и Национальный центр кибербезопасности Великобритании (NCSC) предупредили, что группа APT29 активно эксплуатирует уязвимость, связанную с обходом аутентификации (CVE-2023-42793) в TeamCity. Обнаружив сотни скомпрометированных устройств, эти ведомства предупредили десятки компаний в США, Европе, Азии и Австралии.

Атаки с использованием уязвимости WinRAR

Уязвимость CVE-2023-38831 в архиваторе WinRAR для Windows — это баг высокой степени критичности, который эксплуатируется с начала 2023 года. В августе компания RARLabs выпустила версию WinRAR 6.23, в которой эта уязвимость была исправлена.

Атаки Sandworm

Threat Analysis Group (TAG) компании Google обнаружила несколько хакерских групп с государственной поддержкой, эксплуатирующих уязвимость CVE-2023-38831 в архиваторе WinRAR для Windows.

В апреле 2023 года команда TAG в своем блоге сообщила о группе FROZENBARENTS (также известной как SANDWORM), которая проводит

атаки на предприятия энергетического сектора и продолжает операции по взлому и краже информации. В начале сентября хакеры из Sandworm внедряли инфостилер Rhadamanthys в ходе фишинговых атак с использованием поддельных приглашений поступить в украинскую школу управления дронами. Rhadamanthys — это коммерческая программа для кражи информации, способная, помимо прочего, собирать и передавать учетные данные браузера и информацию о сеансах работы. Она работает по подписке и может быть арендована на 30 дней всего за 250 долларов.

Атаки APT28

Группа APT28 (также известная как Frozenlake, Fancy Bear, Strontium и Sednit) также использовала эту ошибку для доставки вредоносного ПО в ходе атак на энергетическую инфраструктуру Украины с использованием фишинговой кампании. В этой кампании использовался документ-приманка с приглашением на мероприятие, проводимое Центром Разумкова — украинским центром экономических и политических исследований.

Компания Proofpoint также сообщила об использовании этой группировкой уязвимости CVE-2023-38831. По данным исследователей Proofpoint, группа TA422 использовала эти уязвимости для начального доступа к правительственным, аэрокосмическим, образовательным, финансовым, производственным и технологическим объектам, вероятно, чтобы получить доступ к учетным данным пользователей или инициировать дальнейшую вредоносную активность.

В сентябре 2023 года злоумышленники рассылали вредоносные письма от имени геополитических организаций, используя саммит БРИКС и заседание Европейского парламента в качестве тем-приманок, чтобы побудить адресатов открыть письма. Исследователи также заметили, что в период с сентября 2023 года по ноябрь 2023 года злоумышленники рассылали целям документы-приманки, содержащие ссылку, переход по которой запускал цепочку вредоносных действий со стороны сервиса Mockbin.

В ноябре 2023 года группа TA422 отказалась от использования Mockbin для первоначальной фильтрации и перенаправления и стала применять прямую отправку URL-адресов на базе InfinityFree.

Mysterious Werewolf

Исследователи из Cyble Research and Intelligence Labs (CRIL) обнаружили целевую фишинговую атаку на одного из российских поставщиков полупроводниковых изделий. Фишинговое письмо было замаскировано

под официальное сообщение от Министерства промышленности и торговли России и содержало архив-обманку с именем resultati_sovehchaniya_11_09_2023.rar.

Для внедрения полезной нагрузки злоумышленники также использовали уязвимость WinRAR CVE-2023-38831.

Вредоносная полезная нагрузка .NET, агент Athena фреймворка командных серверов Mythic, имеет обширный набор встроенных команд, предназначенных для выполнения различных действий на атакуемых системах. Агент Athena характеризуется такими возможностями, как кросс-платформенность (работа в Windows, Linux и OSX), поддержка SOCKS5, обратная переадресация портов, рефлексивная загрузка сборок, модульная загрузка команд и многими другими. В данном случае агент настроен на использование Discord в качестве канала связи с командным сервером.

Команда BI.ZONE Cyber Threat Intelligence также отслеживала этот кластер активности, получивший название Mysterious Werewolf, и обнаружила еще одну атаку в рамках этой кампании, на этот раз направленную на российские промышленные предприятия. Злоумышленники выдавали себя за Министерство промышленности и торговли РФ и использовали фишинговые письма, содержащие архив с именем Pismo_izveshcanie_2023_10_16.rar. Архив содержал вредоносные CMD-файлы, которые использовали уязвимость CVE-2023-38831 для запуска PowerShell-скрипта и последующей загрузки агента Athena. Злоумышленники использовали динамический DNS-сервис и фреймворки постэксплуатации, а также запланированную задачу запускать агент каждые 10 минут.

Прочие атаки APT28/Fancy Bear

Подразделение CERT-UA сообщило о целенаправленной кибератаке на критически важный объект энергетической инфраструктуры в Украине. Злоумышленники рассылали электронные письма, в которых побуждали пользователей скачать легитимный на первый взгляд архивный файл. Этот архив содержал вредоносные скрипты, которые компрометировали компьютер и выполняли эксфильтрацию конфиденциальных данных, используя такие сервисы, как mockbin.org и mocky.io.

Исследователи из Zscaler проанализировали основные компоненты этой атаки и еще одной кампании, получившей название Steallt и имеющей похожие методы и тактики, которые соответствуют «почерку» группы APT28 (Fancy Bear). По словам исследователей, злоумышленники похищали и эксфильтровывали хеши NTLMv2 с помощью кастомных версий PowerShell-скрипта Nishang's Start-CaptureServer, а также выполняли

различные системные команды. В ходе этой кампании злоумышленники атаковали цели в Австралии, Польше и Бельгии.

С марта исследователи из Microsoft наблюдали фишинговые атаки группы TA422 (также известной как APT28, Forest Blizzard, Strontium, Fancy Bear и Fighting Ursa), направленные на правительственные, энергетические, транспортные и неправительственные организации в США, Европе и на Ближнем Востоке.

Злоумышленники используют две уязвимости. Первая (CVE-2023-23397) — это уязвимость, с повышения привилегий в Microsoft Outlook. Эта уязвимость не требует никаких действий пользователя. Исследователи из Palo Alto обнаружили, что за последние 20 месяцев группа использовала эту уязвимость для атак как минимум на 30 организаций в 14 странах, включая организации из сферы энергетики, транспорта, телекоммуникаций и ВПК. Во всех кампаниях для сбора сообщений NTLM-аутентификации из сетей жертв использовались сетевые устройства Ubiquiti. Первоначально Microsoft исправила уязвимость в Outlook в марте, предупредив, что она активно эксплуатируется. Позже компания обновила свои рекомендации для клиентов.

Компания Proofpoint сообщила об использовании второй уязвимости (CVE-2023-38831, см. выше).

Прочие атаки Sandworm/Hades

По данным исследователей из Mandiant, группа Sandworm (также известная как Hades) осуществила кибератаку на украинскую электрокомпанию. Атака началась в июне 2022 года и завершилась в октябре 2022 года, вызвав отключение электроэнергии. Вектор первоначального доступа в IT-среду определен не был.

Сначала злоумышленники внедрили веб-шелл Neo-REGEORG на сервер, публично доступный в интернете. Через месяц хакеры запустили инструмент туннелирования GOGETTER, написанный на языке Golang, чтобы проксировать обмен зашифрованными данными с командным сервером, используя библиотеку Yamux с открытым исходным кодом.

Группа Sandworm получила доступ к OT-среде компании через гипервизор, на котором располагался управляющий экземпляр системы SCADA для подстанции жертвы, и поддерживала этот доступ в период до 3 месяцев.

Кульминацией атаки стали действия, имевшие физический эффект.

Сначала группа Sandworm с помощью ISO-файла образа CD-ROM запустила штатную утилиту scilc.exe компании ABB, вероятно, для выполнения вредоносных команд, написанных на языке SCIL (Supervisory Control Implementation Language) от ABB. Результатом этого стало отключение подстанций 10 октября 2022 года.

Основываясь на анализе временных меток файлов, специалисты Mandiant полагают, что злоумышленникам потребовалось 2 месяца на разработку возможностей проникновения в OT-среду. Загрузка ISO-образа стала возможной благодаря тому, что на виртуальной машине, на которой работала MicroSCADA, была включена функция автозапуска, позволяющая автоматически запускать CD-ROM — физический или виртуальный (например, ISO-файл). Утилита scilc.exe входит в состав программного комплекса MicroSCADA, и группа Sandworm использовала ее для выполнения команд SCIL, которые сервер преобразовывал в команды IEC 101/104 и передавал на удаленные терминальные устройства подстанции.

Согласно выводам исследователей, на скомпрометированном сервере MicroSCADA была установлена устаревшая версия программного обеспечения, которая предоставляла доступ по умолчанию к SCIL-API. Использование в атаке легитимного бинарного файла свидетельствует о переходе хакеров к техникам living-off-the-land (LoL/LOTL) — в этом случае злоумышленники используют более компактные и универсальные инструменты, что затрудняет обнаружение угроз.

Далее, 12 октября 2022 года, Sandworm внедрила новую версию вредоносной программы CADDYWIPER, уничтожающую данные, — возможно, в попытке затруднить анализ вторжения. Компания Mandiant не указала местоположение атакованного энергетического объекта, продолжительность и масштаб отключения электричества.

Другое

Атаки RedEnergy

Исследователи из Zscaler ThreatLabz обнаружили вредоносную .NET-программу RedEnergy, которая используется в атаках на предприятия энергетической, нефтегазовой, телекоммуникационной и машиностроительной отраслей. Зловред позволяет злоумышленникам похищать информацию из различных браузеров, а также обладает функцией шифровальщика (Stealer-as-a-Ransomware).

Злоумышленники используют тактику FAKEUPDATES, чтобы обманом побудить жертв загрузить вредоносную программу RedEnergy, замаскированную под обновления браузера. Злоумышленники использовали страницы LinkedIn для атаки на жертв и перенаправляли их на мошеннический URL-адрес, а также использовали достаточно авторитетные профили, включая Филиппинскую компанию по производству промышленного оборудования и несколько организаций в Бразилии.

Зловред действует в несколько этапов, начиная с запуска замаскированных вредоносных исполняемых файлов. Он закрепляется в системе, взаимодействует с DNS-серверами и загружает дополнительную полезную нагрузку с удаленных адресов. RedStealer взаимодействует с серверами по протоколу HTTPS, сохраняет себя в каталоге автозапуска Windows и создает пункт в меню «Пуск». Исследователи также обнаружили подозрительную активность по протоколу FTP — это позволяет предположить, что он используется злоумышленниками для передачи украденных данных. После успешного проведения атаки используется модуль шифрования данных. К зашифрованным файлам добавляется расширение .FACKOFF!, и одновременно удаляются резервные копии.

Фишинговая кампания с использованием QR-кодов

Исследователи из Cofense обнаружили фишинговую кампанию, использующую вредоносные QR-коды для кражи учетных данных аккаунтов Microsoft. Кампания продолжается как минимум с мая 2023 года. Одна из целей — неназванная американская энергетическая компания, которая получила около 29% из более чем 1000 писем.

Большинство фишинговых писем — подделка под уведомления о безопасности от Microsoft. Больше всего писем получили организации из сфер производства, страхования, высоких технологий и финансовых услуг — 15%, 9%, 7% и 6% писем соответственно.

Большинство обнаруженных фишинговых ссылок — URL-адреса перенаправления Bing (26%), а также два домена, связанных с приложением Salesforce (15%) и сервисами Web3 компании Cloudflare. Использование перенаправляющих URL-адресов Bing, а также сокрытие фишинговых ссылок в QR-кодах, встроенных в изображения или документы, и другие приемы обфускации помогли вредоносным сообщениям обойти контроль безопасности и попасть в почтовые ящики получателей.

Исследователи из Cofense не приписали новую кампанию каким-либо конкретным злоумышленникам.

Атаки Mysterious Team Bangladesh

Исследователи из Group-IB Threat Intelligence проанализировали деятельность хактивистской группы Mysterious Team Bangladesh. Эта группа, которая обычно атакует организации из логистического, правительственного и финансового секторов в Индии и Израиле (и в меньшей степени в Австралии, Сенегале, Нидерландах, Швеции и Эфиопии), была связана с более чем 750 DDoS-атаками и 78 взломами веб-сайтов с июня 2022 года. Эта группа, предположительно из Бангладеш, также получала доступ к веб-серверам и административным панелям, вероятно, используя известные уязвимости в безопасности (например, уязвимые версии PHPMyAdmin и WordPress) или слабые пароли.

Атаки с использованием программы-шифровальщика Cuba

Исследователи из «Лаборатории Касперского» представили анализ программы-шифровальщика Cuba, где рассмотрели историю создавшей ее группы и присущие ей методы и тактики.

Группа привлекла к себе внимание в 2020 году, тогда же она получила название Tropical Scorpius. Авторы Cuba атаковали организации в США, Канаде, Австралии и Европе, совершив серию крупных атак на нефтяные компании, производственные предприятия, финансовые службы, правительственные, медицинские и другие учреждения.

Группа использует классическую модель двойного вымогательства: похищает, а затем шифрует данные с помощью симметричного алгоритма Xsalsa20, а для ключа шифрования применяет асимметричный алгоритм RSA-2048. Программа-шифровальщик шифрует документы, изображения и архивы. Также она останавливает все SQL-службы, чтобы зашифровать все доступные базы данных. Она ищет данные как на локальных, так и на сетевых ресурсах.

Помимо шифрования, группа похищает конфиденциальные данные, которые ей удается найти в атакованной организации. Тип данных, которые ищут хакеры, зависит от отрасли, к которой относится компания-жертва. Группа использует как известные «классические» средства доступа к учетным данным, так и кастомные приложения: Bughatch, Burntcigar, Cobeacon, Hancitor (Chanitor), Termite, SystemBC, Veeamp, Wedgecut, RomCOM RAT, Mimikatz, PowerShell, PsExec, Remote Desktop Protocol. В основном используются уже известные программные уязвимости,

например комбинация ProxyShell и ProxyLogon, для атаки на серверы Exchange, а также дыры в безопасности сервиса резервного копирования и восстановления данных Veeam.

В своем отчете исследователи из «Лаборатории Касперского» представляют результаты расследования одного из инцидентов, уделяя особое внимание анализу ранее недокументированного ПО, методам и тактикам группы. Также публикуются индикаторы компрометации и правила Sigma и YARA.

Атаки Core Werewolf

Исследователи из BI.ZONE Threat Intelligence сообщили в своем телеграм-канале о новых атаках группы Core Werewolf, направленных на предприятия оборонной и энергетической промышленности России, а также другие объекты критической инфраструктуры, с целью шпионажа.

Злоумышленники рассылали письма с вложенным архивом UKAZ.PDF.ZIP, который содержал исполняемый вредоносный файл с именем «О предоставлении информации по согласованию и наградам.exe». Исполняемый файл представляет собой самораспаковывающийся архив, который при запуске выводит на экран жертвы ожидаемый документ в формате PDF или Microsoft Word. В последней обнаруженной кампании это был документ с текстом приказа заместителя генерального директора известной промышленной компании. В это же самое время в фоновом режиме устанавливался легитимный инструмент UltraVNC, который позволял злоумышленникам получить полный контроль над скомпрометированным устройством.

По данным BI.ZONE, группа Core Werewolf действует как минимум с декабря 2021 года, а информация о ее методах и тактиках уже публиковалась ранее.

Атаки на российские промышленные предприятия

Исследователи «Лаборатории Касперского» сообщили о кампании шпионажа, направленной на ряд российских государственных и промышленных организаций, с использованием кастомного бэкдора, написанного на языке Go.

Начальный вектор атаки — письмо с вредоносным архивом под названием finansovyy_kontrol_2023_180529.rar. Архив содержал документ-приманку в формате PDF, используемый для отвлечения жертвы, а также скрипт NSIS, который получает бэкдор с внешнего URL-адреса и запускает его.

Функционал бэкдора ограничен шпионскими действиями и в основном ориентирован на поиск файлов с определенными расширениями и чтение содержимого буфера обмена. Все данные, отправляемые на командный сервер, шифруются по алгоритму AES, а чтобы избежать анализа, зловред проверяет среду, в которой находится. Результаты этих проверок отправляются на командный сервер на начальной стадии заражения и используются для профилирования жертвы.

Вредоносная активность была обнаружена в июне 2023 года, а в середине августа исследователи обнаружили новую версию зловреда. Она стала лучше обходить защитные меры, что свидетельствует о постоянной планомерной работе злоумышленников по оптимизации атак.

Атаки XDSpy

Исследователи из F.A.C.C.T. сообщают, что APT-группа XDSpy атакует российские металлургические предприятия и предприятия военно-промышленного комплекса. Новые вредоносные рассылки обнаружены 21-22 ноября и были направлены на адреса одного из российских металлургических предприятий, а также научно-исследовательского института, специализирующегося на разработке военных ракет. В обоих случаях в подписи к письмам был расположен логотип научно-исследовательского института ядерных исследований, а в качестве адреса отправителя был указан адрес электронной почты логистической компании из Калининграда. Кроме того, было обнаружено еще одно письмо, отправлявшееся российским металлургическим предприятиям, но с белорусского адреса.

Цепочка атак APT-группы в новой ноябрьской кампании соответствует описанным ранее атакам группы XDSpy. Письма содержат ссылку на PDF-файл, который, в свою очередь, ведет к загрузке вредоносного ZIP-архива. Архив содержит LNK-файл и файл скрипта для командной строки. В ходе атаки C#-код компилируется во вредоносную полезную нагрузку .NET и происходит ее запуск. Выбор жертв группы XDSpy коррелирует с ее предыдущими целями из числа военных и финансовых организаций, а также энергетических, исследовательских и горнодобывающих компаний в Российской Федерации.

Несмотря на то что APT-группа действует с 2011 года, международные исследователи до сих пор не знают, в интересах какой страны она работает.

Атаки с использованием DarkWatchman RAT

Исследователи из F.A.C.C.T. обнаружили новую кампанию с использованием бесфайлового JavaScript-зловреда DarkWatchman. Она связана с атаками на российские компании и маскируется под рассылки курьерской службы доставки Pony Express. В список рассылки входят 30 получателей из различных банковских учреждений, торговых точек, операторов связи, сельскохозяйственных и топливно-энергетических компаний, логистических и IT-компаний.

В сообщениях указывалось, что срок бесплатного хранения товара истек, а в приложенном к письму архиве находился счет, содержавший RAT-зловред DarkWatchman. Письма отправлялись с домена ponyexpress[.]site, который ранее уже использовался для фишинга. Более того, многоканальный телефонный номер, указанный в письме, на самом деле принадлежит курьерской службе Pony Express.

RAT-зловред DarkWatchman давно используется против российских организаций. Ранее операторы RAT DarkWatchman распространяли вредоносное ПО под видом архива с результатами фальшивого тендера Министерства обороны РФ и поддельных повесток из военкомата, а также через поддельный сайт российского разработчика в области криптографии.

Атаки Hellhounds

Исследователи из Positive Technologies раскрыли деятельность новой группы Hellhounds, которая нацелена на российские коммерческие и государственные организации. Кампания получила название Operation Lahat, поскольку данные телеметрии с зараженных хостов отправлялись на аккаунт с именем пользователя lahat.

Расследование началось в октябре 2023 года, когда специалисты PT CSIRT обнаружили факт компрометации одной из энергетических компаний с помощью троянца Decoy Dog. Decoy Dog активно используется в атаках на российские организации как минимум с сентября 2022 года. Однако образец, обнаруженный на хосте жертвы, представлял собой новую усовершенствованную модификацию троянца.

Исследователи сообщили, что группа Hellhounds прилагает значительные усилия, чтобы скрыть свои действия на хостах и в сети. На первом этапе злоумышленники используют загрузчик Decoy Dog, который защищен модифицированной версией упаковщика UPX. В отличие от обычного UPX, эта модификация распаковывает не исполняемый файл, а шеллкод,

написанный полностью на языке ассемблера и использующий только системные вызовы Linux. Сам загрузчик запускается в системе и маскируется под легитимную службу cron. На втором этапе уже используется основная полезная нагрузка, которая представляет собой модифицированную версию кросс-платформенного многофункционального бэкдора Pupy RAT и которую исследователи называют Decoy Dog.

Жертвами атак стали не менее 20 российских организаций, большинство из которых относятся к государственному сектору, сферам информационных технологий, космической промышленности, энергетики, а также строительства, транспорта и логистики.

Анализ методов и тактик злоумышленников не позволил исследователям связать их ни с одной из ранее известных APT-групп.

По данным PT, группа Hellhounds причастна ко взлому российского оператора связи, в результате которого удалось вывести из строя некоторые службы этого оператора. Об этом сообщили исследователи из Solar 4RAYS в своей презентации «Thanos' blip for the telecom operator» («Скачок Таноса для оператора связи») на SOC-Forum 2023.

Атаки Cloud Atlas

Исследователи из F.A.C.C.T. обнаружили новую кампанию кибершпионажа, проводившуюся APT-группой Cloud Atlas (также известной как Clean Ursa, Inception, Oxygen) и направленную на российское агропромышленное предприятие и государственную исследовательскую компанию. Эта группа известна тем, что регулярно проводит кампании, нацеленные на Россию, Беларусь, Азербайджан, Турцию и Словению.

Начальной точкой новой кампании стала рассылка фишинговых сообщений под видом поддержки участников специальной военной операции и постановки на воинский учет. Используется документ-приманка, который эксплуатирует уязвимость CVE-2017-11882 шестилетней давности, связанную с повреждением содержимого памяти в редакторе формул Microsoft Office. Эту уязвимость группа Cloud Atlas использовала еще в октябре 2018 года. Письма поступают с популярных российских почтовых сервисов "Яндекс Почта" и Mail.ru компании VK. Успешная эксплуатация уязвимости приводит к выполнению шеллкода, который отвечает за загрузку и запуск обфусцированного HTA-файла. Загруженное вредоносное HTML-приложение впоследствии запускает VBS-файлы, которые отвечают за получение неизвестного VBS-кода с удаленного сервера и запуск этого кода. На момент проведения исследования VBS-код следующего этапа был недоступен.

Атаки Grayling

Исследователи из Symantec предоставили информацию о новой APT-группе, получившей название Grayling, которая в рамках кампании кибершпионажа, длившейся не менее четырех месяцев, проводила атаки преимущественно на тайваньские организации. Деятельность группы началась в феврале 2023 года и продолжалась как минимум до мая 2023 года. Атаки были нацелены на похищение конфиденциальной информации у производственных, IT- и биомедицинских компаний Тайваня, а также у жертв в США, Вьетнаме и странах Океании.

Группа использовала технику DLL side-loading с помощью экспортируемого API-вызова SbieDll_Hook для загрузки таких инструментов, как загрузчик Cobalt Strike. Затем группа использовала популярный инструмент постэксплуатации Cobalt Strike Beacon. Злоумышленники также устанавливали Havoc — фреймворк командного сервера с открытым исходным кодом, используемый на этапе постэксплуатации подобно Cobalt Strike. Согласно отчету, группа Grayling использовала общедоступный шпионский инструмент NetSpy, эксплуатировала старую уязвимость Windows, связанную с повышением привилегий (CVE-2019-0803), загружала и запускала шеллкод. На этапе постэксплуатации злоумышленники также с помощью команды kill завершали все процессы, перечисленные в файле processlist.txt, и делали дамп учетных данных с помощью Mimikatz.

Атака на критическую инфраструктуру Дании

Датская команда SektorCERT сообщила об одновременной кибератаке на 22 компании, связанные с энергетическим сектором страны, 11 мая 2023 года. В частности, одна из организаций потеряла связь с тремя своими удаленными объектами — работники организации вынуждены были выезжать на объекты, связь с которыми прервалась.

Злоумышленники использовали критическую уязвимость, связанную с инъекцией команд (CVE-2023-28771) и затрагивающую брандмауэры Zyxel. Были успешно скомпрометированы 11 компаний: злоумышленники выполняли вредоносный код, чтобы узнать конфигурацию брандмауэра и определить свои дальнейшие действия. Некоторые из внедренных полезных нагрузок связаны с вариантом Mirai Moobot.

Ведомство приписало эти атаки или, по крайней мере, часть из них, группе Sandworm (также известной как Hades), но без "уверенности". Трафик одной из пострадавших организаций был связан с IP-адресом, который ранее

использовался Sandworm. Однако SektorCERT настаивает на том, что атрибутирование нельзя провести с уверенностью из-за общего недостатка доказательств.

Атаки AeroBlade

Исследователи из BlackBerry обнаружили ранее неизвестную хакерскую кибершпионскую группу, получившую название AeroBlade и нацеленную на организации аэрокосмического сектора США. Кампания проводилась в два этапа: тестовая волна в сентябре 2022 года и более продвинутая атака в июле 2023 года.

В атаках использовался целевой фишинг с вредоносными документами, внедрявшими полезную нагрузку в виде reverse shell. В обеих атаках с помощью reverse shell выполнялись подключения к одному и тому же IP-адресу командного сервера, а на этапе фишинга злоумышленники использовали одни и те же документы-приманки. Финальный вариант reverse shell в атаке 2023 года был более скрытным, в нем использовалось больше методов обфускации и противодействия анализу, а также имелась возможность снятия списка каталогов на зараженных компьютерах.

BlackBerry со степенью уверенности выше средней считает, что целью атак был коммерческий кибершпионаж, направленный на сбор ценной информации.

Атаки через USB с использованием Vetta Loader

В ходе расследования, проведенного командой ZLab компании Yoroi, была обнаружена APT-атака, направленная на ряд итальянских компаний, в основном из сфер промышленности, производства и цифровой печати. Метод проведения этой атаки заключается в использовании зараженных USB-накопителей. Это объясняется тем, что в этих сферах для обмена данными очень часто используют USB-накопители.

Исследователи обнаружили как минимум четыре различных варианта одного и того же вредоносного загрузчика под названием Vetta Loader, который запускается в рамках цепочки заражения с использованием USB-накопителей, причем все эти варианты написаны на разных языках программирования — NodeJS, Golang, Python, .NET. Все они работают по одной и той же схеме, связываясь с командным сервером, а затем загружая другую полезную нагрузку. Последние версии загружаемой полезной нагрузки на момент анализа были уже недоступны. Были обнаружены первоначальный инструмент, предназначенный

для заражения USB-устройств, а также другие модули, способные собирать системную информацию, и вредоносная программа — клиппер для Bitcoin.

Исследователи из Yoroi со степенью уверенности выше средней полагают, что атаки проводились италоязычными злоумышленниками.

Предупреждения CISA

Бюллетень CISA по уязвимостям CVE-2022-47966 и CVE-2022-42475

В бюллетене, подготовленном Агентством по кибербезопасности и защите инфраструктуры США (CISA), ФБР и Национальной кибернетической группой (CNMF), были подробно описаны атаки на американскую авиационную организацию. Предполагается, что атаки начались в январе.

В бюллетене говорится, что прогосударственные- APT-группы, использовав критическую уязвимость удаленного выполнения кода (CVE-2022-47966), получили несанкционированный доступ к экземпляру системы Zoho ManageEngine ServiceDesk Plus, используемой организацией, а затем начали перемещаться по сети этой организации. Другие APT-группы использовали уязвимость переполнения буфера в куче (CVE-2022-42475) в FortiOS SSL-VPN, чтобы внедриться на аппаратный брандмауэр Fortinet, используемый организацией.

С помощью эксплойта для Zoho злоумышленникам удалось получить доступ к веб-серверу на корневом уровне и создать локальную учетную запись пользователя с административными привилегиями. После этого злоумышленники смогли загрузить вредоносное ПО, составить список ресурсов сети, получить учетные данные администратора и далее горизонтально перемещаться по сети организации.

Было неясно, каков был результат этих атак: просто доступ к данным, их изменение или же утечка, поскольку организация не определила четко, где централизованно хранятся ее данные, а агентство CISA имело ограниченный доступ к сети.

В бюллетене не говорится о причастности к атаке каких-либо конкретных APT-групп, но отмечается, что расследование CISA выявило ранее встречавшиеся тактики, методы и процедуры, которые могут быть атрибутированы нескольким APT-группам.

Бюллетень CISA по программе-шифровальщику Snatch

ФБР и Агентство по кибербезопасности и защите инфраструктуры (CISA) выпустили совместный бюллетень по кибербезопасности (Cybersecurity Advisory, CSA) с информацией об известных индикаторах компрометации, методах и тактиках злоумышленников, связанных с вариантом шифровальщика Snatch, обнаруженным в ходе расследования ФБР 1 июня 2023 года.

В предупреждении говорится о том, что злоумышленники атакуют критическую инфраструктуру организаций из различных сфер — информационных технологий, военной промышленности США, а также пищевой и сельскохозяйственной отраслей.

С середины 2021 года операторы программы Snatch постоянно совершенствуют свою тактику, следуя текущим тенденциям в киберпреступном мире. Они были замечены в покупке украденных данных у других использующих шифровальщики групп с целью дополнительного шантажа жертв, чтобы те заплатили выкуп во избежание публикации своих данных в блоге Snatch.

Во многих атаках операторы Snatch использовали слабые места в протоколе RDP, чтобы получить доступ уровня администратора к атакуемой сети. В других случаях они использовали украденные или купленные учетные данные для начального закрепления в системе. Проникнув в сеть, злоумышленники могут провести до трех месяцев, исследуя сеть в поисках нужных файлов и папок.

В бюллетене ФБР и CISA говорится, что операторы Snatch используют в скомпрометированных сетях как легитимные, так и вредоносные инструменты. Среди них инструменты, используемые после компрометации, такие как Metasploit — инструмент тестирования на проникновение с открытым исходным кодом, или инструмент Cobalt Strike для горизонтального перемещения по сети, а также различные утилиты, например sc.exe, для создания, опроса, добавления и удаления служб и выполнения других задач.

Предупреждение CISA об атаках BlackTech

В совместном бюллетене АНБ, ФБР, агентства CISA, Национального полицейского агентства Японии и Японского национального центра готовности к инцидентам и стратегии кибербезопасности (NISC) сообщается, что APT-группа под названием BlackTech (также известная как Palmerworm, Temp.Overboard, Circuit Panda и Radio Panda) незаметно модифицирует прошивку маршрутизаторов Cisco IOS и использует

доверительные доменные отношения маршрутизаторов для перемещения из дочерних организаций в основные целевые организации в США и Японии. Взломам подверглись правительственные организации, промышленные предприятия, СМИ, компании из сферы технологий, электроники и телекоммуникаций.

Кастомная прошивка содержала бэкдор. Функции бэкдора активируются и деактивируются с помощью сформированных специальным образом TCP- или UDP-пакетов. Ведомства призвали транснациональные организации сделать ревизию всех сетевых коммуникаций со своими дочерними офисами и указали ряд мер безопасности, которые необходимо принять, чтобы снизить потенциальный риск стать жертвой этой APT-группы.

Компания Cisco выпустила бюллетень, в котором отмечается, что наиболее распространенным вектором первоначального доступа в этих атаках являются украденные или слабозащищенные учетные данные администратора. Признаков того, что злоумышленники эксплуатировали какие-либо уязвимости Cisco, обнаружено не было.

Предупреждения CISA о программе-шифровальщике Rhysida

Агентство CISA, ФБР и Межгосударственный центр обмена информацией и анализа (MS-ISAC) выпустили совместное предупреждение, в котором предоставили специалистам по киберзащите индикаторы компрометации для шифровальщика Rhysida, информацию о его обнаружении и о тактиках и методах злоумышленников. Эти данные были получены в сентябре 2023 года в ходе расследований.

Злоумышленники, стоящие за шифровальщиком Rhysida, совершают оппортунистические атаки на организации из различных сфер. Они используют модель Ransomware-as-a-Service (RaaS, «шифровальщик как услуга»). С мая 2023 года операторы Rhysida компрометировали организации в сфере образования, производства, информационных технологий и государственного управления, а любой выплаченный выкуп делился между группой и ее партнерами.

Операторы Rhysida используют внешние удаленные сервисы, такие как VPN, а также уязвимость Zerologon (CVE-2020-1472) и фишинговые кампании, чтобы получить первоначальный доступ и закрепиться в сети. Также утверждается, что эта группа имеет сходства с другой использующей шифровальщики группой, известной как Vice Society (другие названия — Storm-0832 и Vanilla Tempest).

Предупреждения CISA о программе-шифровальщике LockBit 3.0

21 ноября 2023 года Агентство CISA, ФБР, Межгосударственный центр обмена информацией и анализа (MS-ISAC) и Центр кибербезопасности Австралийского управления радиотехнической обороны (ASD's ACSC) выпустили совместное предупреждение, в котором приводятся индикаторы компрометации, методы и тактики злоумышленников, а также методы обнаружения шифровальщика LockBit 3.0, эксплуатирующего уязвимость CVE-2023-4966 с кодовым названием Citrix Bleed и поражающего устройства управления доставкой веб-приложений (ADC) Citrix NetScaler и аппаратные шлюзы NetScaler Gateway. Уязвимость позволяет злоумышленникам обойти требования к паролю и многофакторной аутентификации, в результате чего они могут получить контроль над пользовательскими сессиями на устройствах Citrix NetScaler ADC и Gateway.

LockBit — это семейство программ-шифровальщиков, используемое с сентября 2019 года по модели Ransomware-as-a-Service (RaaS, «шифровальщик как услуга»). Партнеры LockBit 3.0 совершали атаки на организации различного масштаба, в том числе критической инфраструктуры, в различных сферах– образования, энергетики, финансовых услуг, пищевой промышленности, сельского хозяйства, государственных и аварийных служб, здравоохранения, производства и транспорта.

Предупреждение CISA об атаках CyberAv3ngers

Агентство CISA, ФБР, АНБ, Агентство по охране окружающей среды и Национальное управление кибербезопасности Израиля 14 декабря опубликовали совместный бюллетень по кибербезопасности, посвященный группе, называющей себя CyberAv3ngers и ответственной за атаку на муниципальное управление водоснабжения города Аликиппа, штат Пенсильвания. В этом совместном бюллетене, выпущенном в дополнение к ноябрьскому предупреждению CISA, ведомства привели индикаторы компрометации, а также тактики и методы злоумышленников.

Группа активно проводит атаки на программируемые логические контроллеры (ПЛК) Unitronics серии Vision производства Израиля. Эти ПЛК часто используются в системах водоснабжения и водоотведения, а также в других отраслях, среди прочего в энергетике, пищевой промышленности и здравоохранении. После компрометации ПЛК хакеры

повреждают их пользовательский интерфейс, что может сделать устройства неработоспособными.

По информации ведомств, связанные с КСИР злоумышленники с 22 ноября атаковали несколько объектов водоснабжения в США, использующих ПЛК Unitronics Vision. Жертвы находились в различных штатах.

Предупреждение CISA о Star Blizzard

В совместном информационном бюллетене, опубликованном 7 декабря, участники альянса «Пять глаз» (Агентство CISA в координации с Национальным центром кибербезопасности Великобритании, Центр кибербезопасности Австралийского управления радиотехнической обороны, Канадский центр кибербезопасности (CCCS), Новозеландский национальный центр кибербезопасности (NCSC-NZ), а также АНБ, ФБР и Национальная кибернетическая группа США) предупредили о совершенствовании методов фишинга, используемых группой Star Blizzard, и ее атаках на частных лиц и организации, включая правительство США и предприятия ВПК.

В предупреждении рассказывается о тактиках и методах этой группы, задокументированных на основе реальных наблюдений. Злоумышленники используют типичные фишинговые приемы и размещают в электронном письме или в документе ссылку, по всей видимости, на нужный документ или сайт. В результате жертва попадает на контролируемый злоумышленниками сервер, где ей предлагается ввести свои учетные данные.

Star Blizzard использует в своих фишинговых кампаниях фреймворк EvilGinx с открытым исходным кодом, позволяющий собирать учетные данные и cookie-файлы сессий для успешного обхода двухфакторной аутентификации. Затем злоумышленники используют украденные учетные данные для входа в почтовый ящик жертвы и похищают письма и вложения. Они также устанавливают правила переадресации почты, обеспечивая таким образом постоянный доступ к переписке жертв, и при этом используют скомпрометированные учетные записи электронной почты для дальнейшей фишинговой активности.

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