APT- и финансовые атаки на промышленные организации в третьем квартале 2024 года

26.12.2024 Version 1.0

Этот документ содержит обзор сообщений об APT- и финансовых атаках на промышленные предприятия, информация о которых была раскрыта в третьем квартале 2024 года, а также о связанной с этим активности групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. В каждом случае мы кратко изложили основные факты, а также привели полученные исследователями результаты и выводы, которые могут быть полезны специалистам, занимающимся практическими вопросами кибербезопасности промышленных предприятий.

Основные события квартала

В течение квартала было опубликовано множество исследовательских работ и технических бюллетеней, подробно описывающих атаки, мишенями или жертвами которых стали организации промышленного сектора. С нашей точки зрения, наиболее интересными для исследователей и полезными для специалистов по кибербезопасности являются следующие:

FrostyGoop: редкий случай обнаружения и раскрытия сведений об инструментарии, специально предназначенном для технологических систем. Предположительно, этот инструмент, поддерживающий взаимодействие по протоколу Modbus, был применен в атаке на коммунальную компанию в Западной Украине, в результате которой 600 многоквартирных домов на два дня остались без отопления в холодный зимний период в конце 2023 года.

Librarian Ghouls — еще одна кампания, мишенями которой стали промышленные предприятия. Хотя в этой шпионской кампании злоумышленники не нацеливались непосредственно на технологические системы, они пытались получить данные 3D- и 2D-графики и моделирования, а также конструкторские и проектные файлы различных CAD-систем, что говорит об их интересе к проектированию и разработке новых промышленных продуктов и технологий.

Червь CMoon, который распространялся через взломанный сайт российской энергетической компании, и атаки **TIDRONE/Operation WordDrone**, представлявшие собой, по-видимому, либо атаки на цепочку поставок, либо эксплуатацию уязвимости в продукте ERP для получения первоначального доступа к системам жертвы, вновь подтверждают тезис, что эти широко обсуждаемые векторы атаки, когда сторонний сервис подвергается взлому с целью заражения других систем, ни в коем случае не следует исключать из моделей угроз современных промышленных предприятий.

Атаки на транспорт и логистику в Северной Америке: в ходе кампаний использовались диалоговые окна с упоминаниями Samsara, AMB Logistic и Astra TMS — программных продуктов для управления работой транспорта и автопарков. Злоумышленники применили схему социальной инженерии под названием ClickFix, жертву которой обманным путем побуждают скопировать и запустить вредоносный PowerShell-скрипт для «исправления технической проблемы». Интересно, что исследователи выявили как минимум 15 скомпрометированных учетных записей электронной почты, использованных в кампании. Злонамеренное использование легитимных корпоративных аккаунтов делает атаку гораздо более эффективной по сравнению с обычными случаями, когда вредоносная инфраструктура применяется для отправки фишинговых писем с поддельными заголовками.

Атаки PhantomCore/Head Mare — еще один случай, когда злоумышленники отправляли вредоносные письма со взломанных аккаунтов электронной почты. Кроме того, они размещали вредоносное ПО в инфраструктуре подвергшихся хакерской атаке организаций.

В отчетах было описано несколько современных техник, применяемых на начальной стадии атаки:

- **Атаки с использованием MSC-файлов/AppDomainManager Injection**. Среди описанных техник атаки, заслуживающих внимания, есть новая техника под названием GrimResource, использующая уязвимость Windows XSS, информация о которой была передана Microsoft почти шесть лет назад и которая до сих пор не устранена. Любопытно, что в той же кампании используется другая уязвимость Microsoft, о которой исследователи сообщили несколько лет назад и которая с тех пор в основном применялась специалистами Red Team, но редко встречалась в дикой среде — AppDomainManager Injection.
- **Атаки с использованием Microsoft Sway**. Бесплатный доступ к публичным облачным сервисам использовался для первоначальной компрометации систем нетривиальным способом. Злоумышленники разместили в Microsoft Sway фишинговые страницы для кампании по краже учетных данных Microsoft 365. Страницы содержали только QR-коды, побуждая жертв открывать вредоносные страницы входа в аккаунт на мобильных устройствах. Злоумышленники использовали Cloudflare Turnstile, чтобы заставить жертву пройти капчу, что позволяло им скрыть вредоносную страницу от автоматических инструментов статического анализа, обеспечивая таким образом хорошую репутацию домена, на котором эта страница была размещена. Наконец, они использовали бесплатный тарифный план сервиса Cloudflare Workers в качестве вредоносного обратного

прокси для оригинальных (легитимных) страниц входа Microsoft, что позволило им реализовать атаку attacker-in-the-middle, которая авторизует пользователя на легитимной странице, одновременно собирая учетные данные, одноразовые токены входа и файлы куки для последующего использования.

- **TA415/APT41.** Фишинговая кампания, основанная на злонамеренном использовании формата файла .search-ms.

Отдельного внимания заслуживают атаки **Flax Typhoon/Raptor Train** — сложного трехуровневого ботнета, состоящего из 200 000 маршрутизаторов малых и домашних офисов (SOHO), который не использовался для DDoS-атак, но сетевая активность которого, как оказалось, была задействована в атаках на критически важные секторы в США и на Тайване.

Юго-Восточная Азия и Корея

Атаки Andariel

Агентство по кибербезопасности и безопасности инфраструктуры США (CISA), Агентство национальной безопасности (NSA), Федеральное бюро расследований (FBI) в сотрудничестве с другими авторами 25 июля опубликовали бюллетень кибербезопасности о поддерживаемой на государственном уровне кибергруппе, известной под именами Andariel, Onyx Sleet (ранее PLUTONIUM), DarkSeoul, Silent Chollima и Stonefly/Clasiopa. По сведениям авторов бюллетеня, эта группа ориентирована преимущественно на атаки на оборонные, аэрокосмические, ядерные и инжиниринговые организации в США, Японии, Южной Корее и Индии. Группа прошла путь от деструктивных атак на организации в США и Южной Корее до специализированных атак, связанных с кибершпионажем и вымогательством. В бюллетене описываются используемые группой инструменты, тактики и техники, а также индикаторы компрометации.

Исследователи из Microsoft и Mandiant тоже опубликовали отчеты об активности Andariel/APT45/Onyx Sleet, предоставив информацию об используемых инструментах, TTP (тактики, техники и процедуры), IoC и затронутых атаками отраслях. В отчетах также содержится информация об атаках, о которых «Лаборатория Касперского» писала в 2021 и 2022 годах.

Атаки Kimsuky

Согласно изданию Der Spiegel, хакерская группа, связанная с властями Северной Кореи, атаковала немецкого производителя оружия Diehl Defence, запустив фишинговую кампанию, основанную на поддельных предложениях о работе и продвинутых методах социальной инженерии. Атака, за которой стоит APT-группа Kimsuky (также известная как APT43), использовала PDF-файлы со специально созданными целевыми фишинговыми приманками, содержащими якобы предложения для сотрудников Diehl Defence о работе в американских оборонных компаниях. По данным издания, исследователи из Mandiant обнаружили, что перед проведением фишинговых атак злоумышленники провели тщательную разведку в отношении Diehl Defence. Der Spiegel сообщает, что адрес сервера, который хакеры Kimsuky использовали в ходе атаки, содержал слово «Uberlingen» как указание на местоположение компании Diehl Defence в Юберлингене на юге Германии. На сервере злоумышленников также были размещены вызывающие доверие страницы входа на немецком языке, похожие на страницы сайтов провайдера телекоммуникационных сервисов Telekom и почтового сервиса GMX, что указывает на массовую кражу учетных данных немецких пользователей. Насколько успешной была атака и сколько информации удалось получить хакерам, не уточняется.

Национальный центр кибербезопасности Южной Кореи (NCSC) предупредил, что группы Kimsuky и Andariel атаковали организации в стране. NCSC считает, что целью злоумышленников была кража сведений, составляющих коммерческую тайну. В январе 2024 года были атакованы строительные компании, государственные учреждения и местные органы власти; в ходе этих атак использовались программы установки с троянским функционалом, подписанные цифровой подписью. В апреле группа Andariel использовала уязвимость в южнокорейской VPN для распространения поддельных обновлений программного обеспечения, которые устанавливали DoraRAT на компьютеры строительных и машиностроительных компаний. DoraRAT — это компактная троянская программа удаленного доступа (RAT) с минимальным функционалом, что позволяет ей действовать более скрытно. Вариант, использованный в этой атаке, был сконфигурирован для кражи больших файлов и отправки их на командный сервер злоумышленников.

Атаки UNC2970

Исследователи из компании Mandiant обнаружили атаки группы, отслеживаемой как UNC2970, на менеджеров высшего звена в компаниях

энергетического и аэрокосмического секторов. В ходе этих атак использовались фишинговые сообщения на тему вакансий с целью получения конфиденциальных данных. Подвергшиеся атаке организации находятся в США, Великобритании, Нидерландах, на Кипре, в Швеции, Германии, Сингапуре, Гонконге и Австралии. Злоумышленники взаимодействуют с целями через электронную почту и WhatsApp, устанавливая доверительные отношения, а затем отправляют вредоносный ZIP-файл под видом описания вакансии. ZIP-архив содержит зашифрованный PDF-файл и троянизированную версию программы с открытым исходным кодом SumatraPDF, предназначенной для просмотра PDF-документов. Таким образом злоумышленники запускают многоэтапную атаку, которая в конечном итоге устанавливает ранее не описанный бэкдор, получивший название MISTPEN. Деятельность этой группы пересекается с активностью TEMP.Hermit.

Атаки SideWinder

Исследователи из BlackBerry обнаружили новую кампанию кибершпионажа, нацеленную на порты и морские объекты в Индийском океане и Средиземном море, проводимую группой SideWinder (также известной как Razor Tiger, Rattlesnake и T-APT-04). Объекты атак находятся в Пакистане, Египте, Шри-Ланке, Бангладеш, Мьянме, Непале и на Мальдивах. Атака начиналась с фишинговых писем, содержащих вредоносный документ с тщательно подобранными логотипами и темами, знакомыми объектам атаки, часто связанными с конкретной портовой инфраструктурой. Злоумышленники использовали специально подготовленные вредоносные документы, реализующие технику удаленного внедрения шаблона (remote template injection, CVE-2017-0199). Вредоносная нагрузка последнего этапа, доставляемая документами, — это вредоносный код на JavaScript. Эта кампания пересекается с активностью, описанной в отчете «Лаборатории Касперского» о SideWinder.

Атаки SloppyLemming

По сообщению компании Cloudflare, группа SloppyLemming (также известная как Outrider Tiger) атакует правоохранительные органы, организации в государственных структурах, энергетической, образовательной, телекоммуникационной и технологической отраслях в Пакистане, Бангладеш, Шри-Ланке, Непале и Китае. Злоумышленники с помощью фишинговых электронных писем обманным путем заставляют жертв пройти по вредоносной ссылке, ведущей на страницу, используемую для кражи

учетных данных. Они также применяют собственный инструмент под названием CloudPhish для создания вредоносного Cloudflare Worker, реализующего журналирование учетных данных и их отправку на командный сервер.

В некоторых атаках группа SloppyLemming использовала схожие методы для захвата токенов Google OAuth, а также применяла зараженные RAR-архивы для эксплуатации уязвимости удаленного выполнения кода (CVE-2023-38831) в WinRAR. В таких RAR-архивах содержится PDF-файл и исполняемый файл, который, помимо отображения документа-приманки, скрытно загружает DLL-библиотеку, служащую загрузчиком троянца удаленного доступа (RAT), размещенного на сервисе Dropbox. Еще в одной цепочке заражения, используемой SloppyLemming, задействованы фишинговые приманки, привлекающие жертв на поддельный сайт, якобы принадлежащий пакистанскому Совету по информационным технологиям Пенджаба, после чего те перенаправляются на другой URL-адрес, по которому размещен файл. Загруженный файл является легитимным исполняемым файлом, используемым для сайдлоадинга DLL-библиотеки, взаимодействующей с Cloudflare Worker.

Активность китайскоязычных групп

Атаки APT41

По данным исследователей из компании Mandiant, группа APT41 (также известная как Barium, Wicked Panda, Wicked Spider, Earth Baku, Axiom, Blackfly, Brass Typhoon, Bronze Atlas, HOODOO, Red Kelpie, TA415 и Winnti) осуществляла атаки, связанные с кражей данных у компаний транспортно-логистического, медийного, технологического и автомобильного секторов по всему миру, преимущественно в Италии, Испании, на Тайване, в Таиланде, Турции и Великобритании. Злоумышленники с 2023 года использовали известные вредоносные программы и общедоступные инструменты для проникновения в системы целевых организаций и закрепления в них. APT41 применяла веб-шеллы ANTSWORD и BLUEBEAM для выполнения вредоносного ПО DUSTPAN, которое, в свою очередь, запускало бэкдор BEACON для связи с командным сервером. Затем группа использовала вредоносное ПО DUSTTRAP для активности с непосредственным участием операторов, SQLULDR2 для копирования данных из баз данных и PINEGROVE для отправки украденных данных на Microsoft OneDrive. Интересно, что вредоносное ПО DUSTTRAP и его компоненты — как те, что использовались в этой кампании, так и найденные на VirusTotal — были

подписаны легитимными сертификатами, предположительно украденными у южнокорейских игровых компаний. Ранее специалисты Mandiant наблюдали использование одного из этих сертификатов другой китайскоязычной группировкой — UNC3914.

Исследователи из Proofpoint обнаружили кампанию кибершпионажа с использованием вредоносного ПО, получившего название Voldemort. Злоумышленники атаковали более 70 организаций, рассылая письма от имени налоговых органов из различных стран Европы, Азии и США. Атакованные организации представляют 18 разных секторов, но почти четверть из них — страховые компании. Половину объектов атаки составили аэрокосмические и транспортные компании и организации из сферы высшего образования, среди жертв атаки также были компании из автомобильного, энергетического и производственного секторов. Электронные письма содержали ссылку, ведущую на посадочную страницу, предлагающую просмотреть документ. Если строка User Agent содержит слово windows, происходит перенаправление браузера на URI, туннелированный через TryCloudflare и оканчивающийся на .search-ms, на котором жертве предлагается открыть проводник Windows. При согласии выполняется скрытый запрос Windows Search с параметрами поиска, указанными в .search-ms файле. В этом файле используется особенность формата, которая приводит к отображению в проводнике Windows LNK или ZIP-файла-приманки с внешнего ресурса, как если бы этот файл находился непосредственно в папке «Загрузки» на компьютере жертвы. LNK/ZIP-файл использует иконку PDF, маскируясь под соответствующий тип файла, и сочетание этих двух приемов может убедить получателя в том, что он имеет дело с PDF-файлом на локальном диске, и повысить вероятность запуска вредоносного файла пользователем.

При выполнении LNK-файла запускается PowerShell для выполнения скрипта Python. Скрипт собирает информацию о компьютере, загружает документ-приманку PDF и открывает его. Затем он загружает защищенный паролем ZIP-файл и извлекает содержимое: легитимный исполняемый файл, связанный с WebEx, и DLL Voldemort для сайдлоадинга. Voldemort — это бэкдор с возможностями сбора информации и загрузки дополнительной вредоносной нагрузки. Он использует для связи с командным сервером Google Sheets. Эксперты Proofpoint обнаружили фреймворк Cobalt Strike, размещенный на инфраструктуре злоумышленников, и, вероятно, это одна из полезных нагрузок вредоносного ПО, доставленного на системы жертв.

Аналитики Proofpoint считают, что к этой кампании имеет отношение связанная с Китаем группа TA415 (также известная как APT41 и Brass Typhoon). Эта уверенность основана на множестве недавно обнаруженных

и подтвержденных с высокой степенью достоверности связей между инфраструктурой, используемой в кампании, в рамках которой распространяется Voldemort, и известной инфраструктурой, атрибутируемой TA415, включая совпадения с активностью, сведения о которой были ранее опубликованы компанией Mandiant. Более того, в конце августа 2024 года Proofpoint выявила целенаправленную кампанию с почти идентичной цепочкой атаки для доставки бэкдора Voldemort. В этих атаках злоумышленники выдавали себя за тайваньскую ассоциацию аэрокосмической промышленности и неоднократно атаковали около пяти аэрокосмических компаний в США и на Тайване, что соответствует типичному профилю целей TA415 и других групп, связанных с Китаем. В этой кампании TA415/APT41 использовала фишинговые письма с URL-адресами Google AMP Cache, которые перенаправляли жертв на защищенные паролем 7-Zip-файлы, размещенные на OpenDrive. Эти архивы содержали вредоносные файлы ярлыков Microsoft (LNK), которые пытались загрузить скрипт Python, размещенный на paste[.]ee. Эта активность продолжалась до конца сентября 2024 года и также была нацелена на небольшое количество химических, страховых и производственных компаний.

Атаки MirrorFace

Эксперты JPCERT/CC зафиксировали атаки на японские организации со стороны группы MirrorFace с использованием вредоносного ПО LODEINFO и NOOPDOOR. Если ранее объектами атак MirrorFace были СМИ, политические организации, аналитические центры и университеты, то с 2023 года их мишенями стали производственные компании и исследовательские институты. TTP группы также изменились: ранее она использовала фишинговые письма, а теперь эксплуатирует уязвимости в продуктах Array AG и FortiGate. Группа также использует шелл-код NOOPDOOR, который внедряется в легитимные приложения с помощью XML- или DLL-файлов, устанавливает связь с командным сервером через порт 443 и выполняет действия по разведке, развитию атаки и отправке украденных данных. NOOPDOOR также применяет различные методы обхода защиты, включая, в частности, манипуляцию временными метками, удаление журналов событий Windows и файлов. В некоторых случаях злоумышленники используют инструмент GO Simple Tunnel (GOST), являющийся HTTP/SOCKS5 прокси.

Атаки TIDRONE/Operation WordDrone

По информации, опубликованной исследователями компании Trend Micro, ранее неизвестная кибершпионская группа, получившая название TIDRONE и, вероятно, связанная с китайскоязычными группами, атаковала производителей дронов на Тайване. Общей чертой жертв этих атак является использование одного и того же программного обеспечения для планирования ресурсов предприятия (ERP), что указывает на возможную атаку через цепочку поставок. Конкретный вектор первоначального доступа, примененный для компрометации систем жертв, остается неизвестным, но Trend Micro выявила внедрение специально созданных вредоносных программ, таких как CXCLNT и CLNTEND, использующих инструменты для удаленного доступа к компьютеру вроде UltraVNC. Оба инструмента запускаются путем подмены DLL через приложение Microsoft Word. CXCLNT обладает базовыми возможностями загрузки и выгрузки файлов, а также функциями устранения следов, сбора информации о жертвах, включая списки файлов и имена компьютеров, и загрузки вредоносного ПО (EXE и DLL) следующих этапов. Инструмент CLNTEND, который впервые был обнаружен в апреле 2024 года, является средством удаленного доступа (RAT), поддерживающим широкий набор протоколов для сетевого взаимодействия, включая TCP, HTTP, HTTPS, TLS и SMB (порт 445).

Компания Acronis опубликовала результаты собственного анализа этой кампании, которой она присвоила имя Operation WordDrone, сообщив, что ее эксперты наблюдали атаки с апреля по июль 2024 года. Эти атаки отличает использование техники под названием Blindside, чтобы избежать обнаружения средствами защиты конечных точек (EDR), перед развертыванием инструмента CLNTEND (также известного как ClientEndPoint). Acronis также сообщила, что вредоносные артефакты были обнаружены в папке тайваньского программного обеспечения ERP под названием Digiwin, а это указывает на возможность либо атаки через цепочку поставок, либо эксплуатации уязвимости в продукте для получения первоначального доступа. Кроме того, была обнаружена DLL-библиотека с неясным функционалом, но исследователи предполагают, что она используется для проксирования выполнения команд бэкдора ClientEndPoint/CLNTEND таким образом, чтобы они выполнялись в контексте пользователя с dllhost в качестве родительского процесса, а не в контексте SYSTEM с родительским процессом winword.exe, что могло бы вызвать подозрения.

Атаки Flax Typhoon/Raptor Train

Исследователи Black Lotus Labs сообщили подробности о ботнете под названием Raptor Train, предположительно связанном с китайской кибершпионской группой Flax Typhoon. Этот ботнет состоит из более чем 200 000 устройств, включая маршрутизаторы малых и домашних офисов (SOHO), устройства NVR/DVR, NAS и IP-камеры. На данный момент не зафиксировано использование ботнета Raptor Train для проведения DDoS-атак, и исследователи подозревают, что эта возможность сохраняется на будущее. Тем не менее, в последние четыре года регистрировалась определенная сетевая активность ботнета, направленная на критически важные секторы США и Тайваня, включая военные и государственные организации, высшие учебные заведения, телекоммуникационные компании, оборонные предприятия и IT-сектор. Управление инфраструктурой ботнета осуществляется через несколько распределенных серверов вредоносной нагрузки и командных серверов (C2), централизованный бэкенд на Node.js и фронтенд Sparrow на основе кроссплатформенного приложения Electron. Это обеспечивает широкий спектр возможностей, включая масштабируемую эксплуатацию ботов, управление уязвимостями и эксплойтами, удаленное управление инфраструктурой командных серверов, загрузку и выгрузку файлов, удаленное выполнение команд и возможность проведения широкомасштабных DDoS-атак с использованием устройства интернета вещей. В большинстве случаев операторы ботнета не внедряли механизмы закрепления в системе, выдерживающие перезагрузку. Основной имплант, используемый на большинстве узлов первого уровня, называется Nosedive и представляет собой кастомизированную версию импланта Mirai. С узлами данного ботнета связываются возможные попытки эксплуатации серверов Atlassian Confluence и программно-аппаратных комплексов Ivanti Connect Secure.

В день публикации отчета Black Lotus Labs агентства из стран «Пяти глаз» выпустили бюллетень, посвященный ботнету, с рекомендациями по минимизации связанной с ним угрозы. Также Министерство юстиции США объявило о проведении санкционированной судом операции по нарушению работы ботнета, включающей взятие под контроль его инфраструктуры и отправку команд для отключения вредоносного ПО на скомпрометированных устройствах.

Атаки с использованием MSC-файлов/AppDomainManager Injection

Исследователи из NTT выявили волну атак, начавшихся в июле 2024 года, нацеленных на государственные учреждения Тайваня, военные структуры Филиппин и энергетические организации Вьетнама. Наблюдались два сценария атак: загрузка ZIP-файла с подготовленного злоумышленниками сайта и получение ZIP-файла в письме в ходе целенаправленной фишинговой атаки. В обоих случаях ZIP-файл содержал вредоносный MSC-файл, открытие которого пользователем запускало атаку. Вредоносный MSC-файл эксплуатировал неисправленную установкой патча Windows XSS-уязвимость в apds.dll с использованием техники GrimResource для выполнения встроенного JavaScript-кода. В конечном итоге выполнялся код VBScript, который загружал и сохранял четыре файла и запускал oncesvc.exe — легитимный dfsvc.exe от Microsoft. Загруженный файл конфигурации oncesvc.exe.config содержал информацию для загрузки версии сборки, отличной от предопределенной в приложении. Злоумышленники использовали это, чтобы заставить легитимный EXE-файл загрузить внешнюю DLL-библиотеку. Такое вредоносное поведение называется AppDomainManager Injection. Этот метод используется специалистами Red Team, но редко наблюдается в дикой среде. В этой кампании в конечном итоге использовались маяки CobaltStrike для компрометации среды атакуемой системы. После изучения характеристик загрузчика и инфраструктуры злоумышленников, использованных в этой атаке, исследователи пришли к выводу, что этот подход схож с методами группы APT41. Отчет AhnLab описывает аналогичный случай атаки. Сообщается, что в атаке использовались документы-приманки PDF о японской оборонной промышленности на корейском языке и файл readme.docx.

Активность, связанная с Ближним Востоком

Атаки Peach Sandstorm

С апреля по июль исследователи Microsoft наблюдали, как группа Peach Sandstorm (также известная как APT33, Elfin и Refined Kitten) использовала новый нестандартный многоступенчатый бэкдор под названием Tickler в атаках на спутниковые, коммуникационные и нефтегазовые секторы, а также на федеральные и государственные органы в США и ОАЭ. Группа также продолжала атаки с распылением паролей на организации

образовательного сектора для получения доступа к инфраструктуре, а также на организации спутниковой индустрии, государственные учреждения и предприятия оборонного сектора в качестве основных целей для сбора разведывательной информации. Кроме того, исследователи наблюдали использование LinkedIn для сбора разведывательной информации и, возможно, атак с использованием социальной инженерии на организации в секторах высшего образования, спутниковой связи и обороны. Известно, что после получения доступа к системам организации Peach Sandstorm продвигается по ее сети и осуществляет действия, направленные на достижение целей, с использованием протокола SMB. В более ранней атаке на международную фармацевтическую компанию группа также загрузила и установила AnyDesk — коммерческий инструмент удаленного мониторинга и управления (RMM). По крайней мере, в одной атаке на ближневосточного оператора спутниковой связи злоумышленники Peach Sandstorm скомпрометировали систему пользователя, отправив вредоносный ZIP-файл через сообщение в Microsoft Teams, после чего установили на систему AD Explorer и сделали снимок Active Directory.

Активность испаноязычных групп

Атаки BlindEagle

Исследователи «Лаборатории Касперского» опубликовали отчет об APT-группе под названием Blind Eagle (APT-C-36). Группа действует как минимум с 2018 года и атакует организации и отдельных людей в Колумбии, Эквадоре, Чили, Панаме и других странах Латинской Америки, ориентируясь на разные сектора, включая государственные учреждения, финансовые организации, энергетические и нефтегазовые компании. Blind Eagle демонстрирует адаптивность и гибкость в выборе целей своих атак, переключаясь между чисто финансовыми кампаниями и кибершпионажем. APT-группа известна атаками с использованием целенаправленного фишинга, в которых она, выдавая себя за государственные органы или банковские учреждения, распространяет различные общедоступные троянские программы, такие как AsyncRAT, BitRAT, Lime RAT, NjRAT, Quasar RAT и Remcos RAT. Рассылаемые группой фишинговые письма содержат ссылку, якобы ведущую на официальный сайт организации. Письма также включают в себя файл PDF или Microsoft Word, содержащий тот же URL-адрес, а в некоторых случаях дополнительные детали, призванные придать сообщению оттенки срочности и легитимности. Первый набор URL перенаправляет пользователей на контролируемые

субъектом сайты, на которых размещен загрузчик первого этапа, но только после того, как жертва была идентифицирована как принадлежащая к целевой стране; в противном случае пользователь перенаправляется на легитимный сайт. Загрузчик первого этапа доставляется в виде сжатого ZIP-архива, который, в свою очередь, содержит сценарий Visual Basic, отвечающий за извлечение вредоносной нагрузки следующего этапа с жестко закодированного удаленного сервера, в качестве которого может использоваться, например, хостинг изображений, сервер Pastebin, Discord или GitHub. Вредоносное ПО второго этапа, зачастую замаскированное с помощью стеганографических техник, представляет собой DLL или .NET-инжектор, который затем связывается с еще одним сервером для получения троянской программы последнего этапа. Группа часто использует техники внедрения в процессы для выполнения средства удаленного доступа (RAT) в памяти легитимного процесса. BlindEagle использует RAT с открытым исходным кодом в качестве последнего звена в своей цепочке атаки, модифицируя их для достижения целей кампании. Хотя TTP группы кажутся простыми, их эффективность позволяет BlindEagle поддерживать высокий уровень активности.

Активность и цели русскоязычных групп в России

Атаки BlackJack

Группа BlackJack атакует государственные учреждения, телекоммуникационные и промышленные компании в России, используя инструменты с открытым исходным кодом и вредоносное ПО. Исследования «Лаборатории Касперского» показали, что группа применяет программу-вымогатель LockBit и вайпер Shamoon, написанный на Go, для нанесения серьезного ущерба своим жертвам. Для поддержания постоянного доступа к скомпрометированным ресурсам жертв злоумышленники используют туннелирование с помощью утилиты ngrok. BlackJack устанавливает различные средства удаленного доступа (RAT), такие как Radmin, AnyDesk и SSH-клиент PuTTY. Телеметрия «Лаборатории Касперского» и технологии обнаружения сходства выявили пересечения с другими группами хактивистов, такими как Twelve и пока не атрибутированный кластер активности, с общими вредоносными инструментами и специфическими TTP.

Атаки ReaverBits

Исследователи F.A.C.C.T. сообщили о новой группе ReaverBits, атакующей российские компании вредоносными рассылками от имени различных компаний и министерств. Группа осуществляла атаки на федеральный фонд, а также на российские компании из сфер розничной торговли, телекоммуникаций, процессинговую компанию и агропромышленное объединение. Было зафиксировано около пяти рассылок группы: две в декабре 2023 года, две в январе 2024 года и последняя в мае. Группа активно применяет спуфинг, используя MetaStealer в качестве вредоносной нагрузки. В одной из атак группа использовала загрузчик LuckyDownloader, предположительно воспользовавшись услугой стороннего актора, отслеживаемого по имени LuckyBogdan.

Атаки с использованием скриптов Unicorn

В начале сентября исследователи «Лаборатории Касперского» зафиксировали вредоносную рассылку, направленную на кражу конфиденциальных данных. Атаке подверглись российские энергетические компании, заводы, а также поставщики и разработчики электронных компонентов. Вредоносное ПО распространяется в виде почтовых вложений или файлов на «Яндекс Диске», на которые ведет ссылка из письма. Рассылаемый таким образом файл представляет собой RAR-архив, внутри которого содержится файл с двойным расширением PDF + LNK. Вредоносный ярлык запускает приложение mshta, которое скачивает и выполняет файл HTML Application (HTA). При запуске HTA выполняется вредоносный VBS-скрипт, который создает на диске два скрипта. Они автоматически запускаются через две задачи, созданные в планировщике, и определенные ключи реестра. Первый скрипт ищет документы, архивы и изображения размером менее 50 МБ, а также копирует содержимое папки Telegram Desktop. Второй скрипт отправляет собранные файлы на сервер злоумышленников, используя расшифрованный код из реестра. Решения «Лаборатории Касперского» детектируют эти скрипты с вердиктом Trojan-Spy.VBS.Unicorn. Связи с известными группами не установлены.

Атаки PhantomCore/Head Mare

Исследователи F.A.C.C.T. отслеживают новую активность и кибератаки группы PhantomCore, которая атакует российские организации с начала 2024 года. В марте F.A.C.C.T. впервые сообщила о деятельности этой группы

кибершпионов, названной по их уникальному троянцу удаленного доступа PhantomRAT. Злоумышленники переписали PhantomRAT с C# на Go, добавив новые команды. Кроме того, они разработали загрузчик PhantomDL версии 3 (v.3), а затем выпустили еще одну версию (v.4), частично дополнив ее возможностями PhantomRAT. Используя эти инструменты, группа провела новые атаки на различные российские предприятия: приборостроительный завод, завод полимерных материалов, механический завод, технопарк, лизинговую, нефтегазовую и ИТ-компании. Анализируя эти атаки, исследователи отметили, что злоумышленники сначала внедряются в сторонние организации и затем используют их для атак на основные цели, отправляя вредоносные письма со скомпрометированных адресов и размещая вредоносное ПО в инфраструктуре взломанных компаний. В частности, им удалось скомпрометировать для последующих атак производителя бытовой и промышленной химии, разработчика программного обеспечения, интегратора медицинских технологий, дистрибьютора металлургической продукции и строительную компанию.

Исследователи F.A.C.C.T. зафиксировали 5 сентября новые атаки группы PhantomCore на ИТ-компанию, конструкторское бюро и производителя высокотехнологичного оборудования беспроводной связи в России. Весной и летом PhantomCore атаковала российские организации в различных секторах, преимущественно в промышленности. Отличительной чертой деятельности злоумышленников является первоначальная компрометация сторонних организаций для проведения фишинговых атак.

Исследователи отметили несколько рассылок с вероятно скомпрометированного адреса компании, специализирующейся на строительстве и автоматизации объектов электроэнергетики и транспорта. Атакующие отправляли фишинговые письма с вложенным архивом, защищенным паролем, содержащим легитимный документ PDF, выполняющий роль приманки, и вредоносный исполняемый файл. При открытии архива использовалась уязвимость CVE-2023-38831 для автоматического запуска программы. В качестве основного инструмента применялось вредоносное ПО PhantomCore.KscDL_trim — урезанная версия загрузчика PhantomCore.KscDL, написанная на C++ и упакованная инструментом UPX. Загрузчик обладает следующими возможностями: загрузка и запуск файлов с C2-адреса, выполнение произвольных команд в командной строке Windows. В ходе анализа исследователи получили несколько команд с сервера управления и установили, что злоумышленники предварительно профилируют жертву, решая, интересна ли она для дальнейшего развития атаки.

Исследователи «Лаборатории Касперского» считают, что за атаками с использованием PhantomDL и PhantomRAT стоит группа хактивистов Head Mare, появившаяся в 2023 году. В ходе расследования атак на организации в России исследователи определили методы и инструменты, используемые Head Mare, и установили связь с вредоносной активностью, изученной экспертами F.A.C.C.T. Для получения первоначального доступа группа проводит различные фишинговые кампании, распространяя RAR-архивы, эксплуатирующие уязвимость CVE-2023-38831 в WinRAR, которая позволяет выполнять в системе произвольный код. Группа использует собственные вредоносные программы PhantomDL и PhantomCore для первоначального доступа и эксплуатации. Для других задач Head Mare преимущественно применяет общедоступное программное обеспечение, такое как Sliver (основной C2-фреймворк), ngrok, rsockstun (оба используются для пивотинга), XenAllPasswordPro и Mimikatz. Кроме того, Head Mare применяет программы-вымогатели LockBit и Babuk (сгенерированные с помощью общедоступного билдера). Злоумышленники создают задачи планировщика и значения реестра с именами MicrosoftUpdateCore и MicrosoftUpdateCoree, маскируя свою деятельность под задачи, связанные с программным обеспечением Microsoft. Многие инструменты, используемые Head Mare, имеют названия, типичные для легитимных программ, и расположены по стандартным или похожим на стандартные путям. Анализируемые образцы вредоносного ПО преимущественно обнаруживались в организациях, находящихся в России, но в Беларуси тоже было зафиксировано несколько образцов. Компании, являющиеся мишенями атак этой группы, в основном работают в секторах, связанных с государственным управлением, производством, технологиями, энергетикой, транспортом и сферой развлечений.

Атаки подразделения 29155

Агентство США по кибербезопасности и инфраструктурной безопасности (CISA), Федеральное бюро расследований (FBI), Агентство национальной безопасности (АНБ) и службы безопасности девяти других стран 5 сентября опубликовали совместный бюллетень по кибербезопасности (CSA), посвященный активности подразделения 29155, предположительно связанного с Главным управлением Генерального штаба Вооруженных сил Российской Федерации (ранее известным как ГРУ). Считается, что подразделение 29155 несет ответственность за атаки на украинские власти и критически важную инфраструктуру, а также на ключевые секторы, включая правительственные структуры, финансовые сервисы, транспортные системы, энергетику и здравоохранение стран-членов НАТО, ЕС, Центральной Америки и Азии. С деятельностью подразделения 29155

связывают атаки с применением вайпера WhisperGate. В документе приведены технические подробности, включая уязвимости, которые злоумышленники использовали для первоначального доступа, индикаторы компрометации, а также тактики, техники и процедуры. Злоумышленники из подразделения 29155 применяют характерные для Red Team методы и общедоступные инструменты для проведения кибероперациий. Известно, что они используют VPN для анонимизации своей деятельности и пытаются эксплуатировать слабые места в системах, доступных из интернета. Пятерым офицерам подразделения 29155 и одному гражданскому лицу в США были предъявлены обвинения в предполагаемых атаках на Украину и 26 стран НАТО.

Атаки Librarian Ghouls

В начале июля исследователи из «Лаборатории Касперского» сообщили о новой волне целевых атак, в ходе которых злоумышленники рассылали вредоносные файлы, замаскированные под документы, для сбора конфиденциальной информации с компьютеров различных компаний. С тех пор «Лаборатория Касперского» продолжила отслеживать активность группы, получившей название Librarian Ghouls, и выявила изменения в их тактике. Новыми мишенями атак стали компании, занимающиеся проектированием и разработкой в различных отраслях, научно-исследовательские институты, предприятия ракетно-космической и авиационной промышленности, а также организации, работающие в областях газопереработки, нефтехимии и обороны. Кроме того, под прицелом оказались производители водолазного оборудования, систем связи и радиолокации, автомобильных компонентов, автоматизированных систем управления технологическими процессами и полупроводниковых устройств.

Метод проведения атак остался прежним: вредоносные файлы распространяются в виде RAR-архивов с поддельными документами в формате .SCR. После запуска такой файл загружает на компьютер дополнительные вредоносные компоненты, собирает интересующие злоумышленников данные и отправляет на их сервер. Однако цели группы и формат собираемых данных изменились: помимо офисных документов и данных из мессенджера Telegram, злоумышленников теперь интересуют файлы, связанные с программным обеспечением для моделирования и разработки промышленных систем. В список файлов, собираемых вредоносным ПО для отправки, было добавлено несколько расширений, характерных для узкоспециализированного ПО, такие как файлы для автоматизированной системы проектирования SolidWorks, российской

САПР KOMPAS-3D, файлы .m3d, используемые различными программами для создания трехмерных моделей объектов, и файлы .dwg, применяемые в таких САПР, как AutoCAD, CorelCAD и другие. Кроме того, вредоносное ПО начало похищать документы в формате *.pdf.

Атаки с применением агента Loki

Исследователи из «Лаборатории Касперского» обнаружили ранее неизвестный бэкдор Loki, который использовался в серии целевых атак в июле. Более десятка российских компаний из различных отраслей, включая машиностроение и здравоохранение, уже столкнулись с этой угрозой, однако число потенциальных жертв может быть выше. Анализируя вредоносный файл и открытые источники, исследователи установили, что Loki является приватной версией агента для фреймворка с открытым исходным кодом Mythic. Обнаруженный агент Loki совместим с Mythic и представляет собой версию агента для другого фреймворка — Havoc. Однако, в отличие от агента для Havoc, Loki был разделен на загрузчик и DLL-библиотеку, реализующую основную функциональность вредоносного ПО. Обе версии агента используют алгоритм хеширования djb2 для скрытия функций и API-команд с незначительными отличиями. После запуска на выполнение загрузчик Loki генерирует пакет с информацией о зараженной системе и отправляет его в зашифрованном виде на командный сервер (C2). В ответ сервер отправляет DLL, которая выполняется в памяти. В ходе детального анализа исследователи обнаружили около 15 версий загрузчика и два активных C2, а также получили образец основного DLL-модуля версии, датируемой маем. Основной модуль, как и загрузчик, основан на версии агента для Havoc, однако список поддерживаемых команд частично позаимствован из других агентов Mythic. Он не хранится в виде обычного текста в DLL; вместо этого в коде библиотеки указаны несколько хешей. При получении команды от сервера ее имя хешируется и сравнивается с хешем, хранящимся в DLL. Сам агент не поддерживает туннелирование трафика, поэтому злоумышленники используют общедоступные сторонние утилиты — ngrok и gTunnel — для доступа к частным сегментам сети. Из-за недостаточности данных не удалось отнести Loki к какой-либо известной группе вредоносных программ.

Атаки Stone Wolf

Исследователи BI.ZONE обнаружили новую хакерскую группу, получившую имя Stone Wolf, которая использует коммерческий инфостилер Meduza

для атак на российские организации. Злоумышленники рассылают фишинговые письма от имени легитимной организации, занимающейся промышленной автоматизацией, для доставки стилера Meduza. В рамках выявленной кампании Stone Wolf распространяла архив под названием Dostavka_Promautomatic.zip, содержащий три файла: цифровую подпись (файл .p7s), легитимный документ-приманку (.docx) и вредоносную ссылку, замаскированную под PDF-документ (Scan_127-05_24_dostavka_13.05.2024.pdf.url). После перехода по вредоносной ссылке с удаленного SMB-сервера загружался файл, который затем выполнялся, что в конечном итоге приводило к установке стилера Meduza. По данным разработчиков Meduza, исполняемый файл содержит модуль, ограничивающий возможность проведения атак в странах СНГ, однако в исследованном образце такая проверка отсутствовала. Стилер собирает информацию о системе, включая версию ОС, имя устройства, время, данные о процессоре, оперативной памяти и графическом адаптере, разрешение экрана и внешний IP-адрес устройства. Кроме того, он способен похищать учетные данные из Outlook, браузеров, криптокошельков, сессий Telegram и Steam, токены Discord, данные из менеджеров паролей, Windows Credential Manager и Windows Vault, а также считывать список активных процессов и установленных приложений. Собранные данные отправляются на командный сервер по протоколу TCP.

Атаки червя CMoon

В конце июля исследователи «Лаборатории Касперского» обнаружили ранее неизвестное вредоносное ПО, распространяемое через сайт одной из российских энергетических компаний. Злоумышленники заменили ссылки на загрузку нормативных документов в нескольких разделах ресурса на другие, ведущие к вредоносным исполняемым файлам. Всего на сайте энергетической компании было заменено около двух десятков ссылок, каждая из которых загружала самораспаковывающийся архив. Все архивы содержали соответствующие документы и один и тот же исполняемый файл — новое вредоносное ПО, которое эксперты «Лаборатории Касперского» назвали CMoon по соответствующим строкам в коде файла. Уровень сложности атаки указывает на то, что она была рассчитана на посетителей конкретного сайта и тщательно подготовлена.

CMoon способен загружать конфиденциальные и платежные данные с зараженного устройства, запускать DDoS-атаки, а также распространяться на другие устройства. Червь может искать и отправлять на сервер злоумышленников файлы из пользовательских папок «Рабочий стол», «Документы», «Фото», «Загрузки» и с внешних носителей,

содержащие подстроки secret, service, password и другие ключевые слова в тексте, что свидетельствует о целенаправленном характере атаки. Также зловред может загружать файлы с информацией о защите системы, действиях пользователя и его учетных данных. Кроме того, вредоносное ПО способно делать снимки экрана. Файлы, содержащие сохраненные пароли, cookies, закладки, историю браузера, а также информацию для автозаполнения форм, включая данные кредитных карт, собирались из веб-браузеров. Червь также отслеживает подключенные USB-накопители. После уведомления компании о компрометации, вредоносные файлы и ссылки были удалены с сайта 25 июля.

Атаки OldGremlin

Исследователи F.A.C.C.T. сообщили о возвращении группы-вымогателей OldGremlin, которая атаковала российские компании в 2020–2022 годах. Группа была неактивна с сентября 2022 года, но почти два года спустя злоумышленники возобновили деятельность, сделав новую рассылку, в которой использовали новый инструмент — OldGremlin.JsDownloader. Эксперты F.A.C.C.T. обнаружили электронное письмо, загруженное на AnyRun от имени сотрудника «Диадок» с адреса makarova@diadok[.]net, получателем которого был сотрудник крупной российской нефтехимической компании. Письмо было отправлено 12 августа, а домен diadok[.]net, с которого было отправлено вредоносное письмо, имитирует оригинальный домен компании «Контур.Диадок» — diadoc[.]ru. В письме содержалась ссылка на загрузку invoice.xlsx. При нажатии на ссылку загружался архив с LNK-файлом, который подключался к серверу WebDav, выполняя команду для загрузки JavaScript-файла для следующего этапа атаки и легитимного интерпретатора Node.js, который использовался для запуска этого JavaScript-файла. Запуск этого скрипта открывает файл-приманку XLS, доступный по WebDav-пути, а также декодирует и запускает вредоносный загрузчик (OldGremlin.JsDownloader) в формате Base64. Этот загрузчик OldGremlin.JsDownloader получает с командного сервера, расшифровывает и выполняет следующий JavaScript-код.

Другое

Атаки UAC-0180

CERT-UA опубликовал предупреждение о вредоносной активности группы UAC-0180, направленной против украинских оборонных предприятий.

Злоумышленники распространяют поддельные электронные письма с темами, связанными с закупками, пытаясь обманом заставить получателей открыть вложенный ZIP-файл, содержащий PDF-документ. При нажатии на вложение запускается вредоносное ПО GLUEEGG, которое расшифровывает и выполняет загрузчик DROPCLUE. Это запускает цепочку заражения, приводящую к установке легитимного программного обеспечения для удаленного управления ATERA.

Атаки FrostyGoop

Ранее неизвестное вредоносное ПО, получившее название FrostyGoop, предположительно было использовано в целевой атаке на муниципальную районную энергетическую компанию в Украине, которая обеспечивала центральное отопление более чем 600 многоквартирных домов во Львове. Атака осуществлялась на контроллеры температуры ENCO поставщика энергии: сначала устанавливалась версия прошивки, не отправляющая телеметрию, а затем на контроллеры отправлялись команды, заставляющие их сообщать неверные данные измерений. По данным компании Dragos, это «привело к нарушению подачи электроэнергии к отопительным службам».

FrostyGoop — это специально предназначенный для АСУ ТП инструмент, написанный на языке Golang, впервые использующий протокол Modbus для прямого воздействия на системы. Он может читать и записывать в регистры устройств АСУ ТП, содержащие входные данные, выходные данные и данные конфигурации. Вредоносное ПО принимает необязательные аргументы командной строки, использует отдельные конфигурационные файлы для определения целевых IP-адресов и команд Modbus, а также записывает вывод в консоль и/или JSON-файл. Расследование атаки в Украине показало, что злоумышленники, возможно, получили доступ к сети жертвы через неопределенную уязвимость во внешнем маршрутизаторе Mikrotik. Сетевые активы, включая роутер Mikrotik, четыре сервера управления и контроллеры системы центрального отопления, не были адекватно сегментированы, что способствовало успеху атаки.

Атака на транспортно-логистический сектор в Северной Америке

Компания Proofpoint обнаружила кампанию, нацеленную на транспортно-логистический сектор в Северной Америке. Proofpoint отслеживает эту активность с конца мая и считает, что группа, вероятно, имеет финансовую

мотивацию, хотя не смогла приписать ее конкретному злоумышленнику. Хакеры используют скомпрометированные легитимные учетные записи электронной почты, принадлежащие транспортным и судоходным компаниям, и затем внедряют URL-адреса Google Drive, ведущие к внутреннему URL-файлу, или прикрепляют URL-файл в существующую переписку. При нажатии устанавливается вредоносное ПО, такое как Lumma, StealC, NetSupport, DanaBot, Arechclient2, предназначенное для кражи информации с устройств жертв. Proofpoint выявил по крайней мере 15 скомпрометированных учетных записей электронной почты, использованных в кампании, но остается неясным, как хакеры получили доступ к этим учетным записям. В этих кампаниях также использовались диалоговые окна с упоминаниями Samsara, AMB Logistic и Astra TMS — программного обеспечения, применяемого в управлении транспортом и автопарком, — которые использовались для реализации техники под названием ClickFix. Диалоговые окна побуждали пользователей копировать, вставлять и запускать закодированный в Base64 скрипт PowerShell, содержащийся в HTML. Скрипты PowerShell вели к MSI-файлу, который использовался для загрузки DanaBot.

Атаки RansomHub

Агентство по кибербезопасности и инфраструктурной безопасности США (CISA), Федеральное бюро расследований (FBI), Центр обмена информацией между штатами и ее анализа (MS-ISAC) и Министерство здравоохранения и социальных служб (HHS) 29 августа опубликовали совместный бюллетень кибербезопасности (CSA), содержащий информацию о группе RansomHub, предоставляющей услуги «программа-вымогатель как сервис» (RaaS), ранее известной как Cyclops and Knight. С момента своего появления в феврале 2024 года RansomHub зашифровала и отправила злоумышленникам данные как минимум 210 жертв, представляющих такие критически важные секторы инфраструктуры, как водоснабжение и водоотведение, информационные технологии, государственные услуги и объекты, здравоохранение и общественное здоровье, экстренные службы, продовольствие и сельское хозяйство, финансовые услуги, коммерческие объекты, критически важное производство, транспорт и связь. Документ содержит технические детали, включая уязвимости, которые эксплуатируют злоумышленники RansomHub для первоначального доступа, а также индикаторы компрометации и тактики, методы и процедуры. После получения первоначального доступа лица, связанные с RansomHub, создавали учетные записи пользователей для закрепления в системе, повторно активировали отключенные учетные

записи и использовали Mimikatz. Затем они перемещались по сети с помощью таких методов, как RDP, PsExec, AnyDesk, Connectwise, N-Able, Cobalt Strike, Metasploit и других. Была зафиксирована отправка данных злоумышленникам с использованием таких инструментов, как PuTTY, Amazon AWS S3 buckets/tools, HTTP POST-запросы, WinSCP, Rclone, Cobalt Strike, Metasploit и других методов. Кроме того, агентства упомянули среди используемых инструментов BITSAdmin, Sliver, SMBExec, CrackMapExec, Kerberoast и AngrylPScanner.

Атаки, использующие Microsoft Sway

Согласно данным Netskope Threat Labs, масштабная фишинговая кампания с использованием QR-кодов злонамеренно использовала Microsoft Sway — облачный инструмент для создания онлайн-презентаций — для размещения посадочных страниц с целью обмана пользователей Microsoft 365 и получения их учетных данных. Исследователи обнаружили эти атаки в июле 2024 года после фиксации 2000-кратного увеличения трафика на фишинговые страницы, доставляемые через Microsoft Sway. Этот всплеск резко контрастирует с минимальной активностью, зафиксированной в первой половине года, что свидетельствует о масштабах этой кампании. Основными мишенями были пользователи в Азии и Северной Америке, особенно в секторах технологий, производства и финансов. Электронные письма направляли потенциальных жертв на фишинговые посадочные страницы, где им предлагалось сканировать QR-коды, которые перенаправляли их на другие вредоносные веб-сайты. Злоумышленники использовали технику transparent phishing, злоупотребляя бесплатным сервисом Cloudflare Workers, который использовался в качестве вредоносных обратных прокси-серверов для легитимных страниц входа. Таким образом, они похищали у жертв учетные данные и коды многофакторной аутентификации учетных записей Microsoft, показывая им при этом легитимную страницу входа. Злоумышленники также использовали Cloudflare Turnstile — инструмент, предназначенный для защиты веб-сайтов от ботов, чтобы скрыть фишинговый контент своих целевых страниц от статических сканеров, что помогало поддерживать хорошую репутацию фишингового домена и избегать блокировки веб-фильтрами.

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