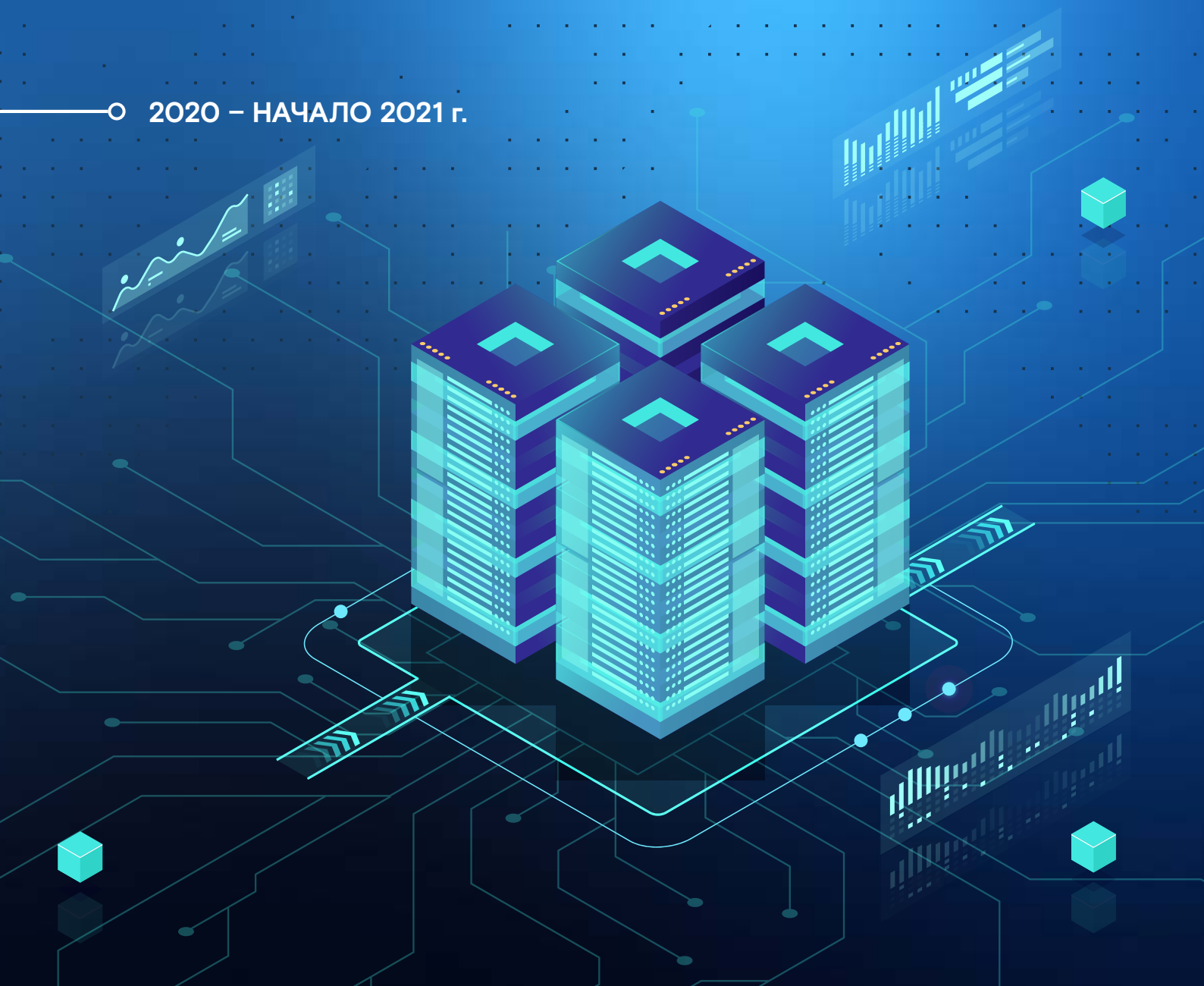
Ростелеком
Солар

Отчет Solar JSOC об актуальных уязвимостях в инфраструктурах российских организаций – субъектов КИИ

2020 – НАЧАЛО 2021 г.



ОГЛАВЛЕНИЕ

1 ИНФОРМАЦИЯ О КОМПАНИИ

«Ростелеком-Солар», компания группы ПАО «Ростелеком», – национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью. В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар». Solar JSOC – крупнейший в России коммерческий центр противодействия кибератакам, лидер российского рынка Security Operations Center (SOC).

СПИСОК СЕРВИСОВ SOLAR JSOC:

- Мониторинг и анализ инцидентов
- Комплексный контроль защищенности
- Расследование и реагирование на инциденты
- Анализ угроз и внешней обстановки
- Построение SOC и его частных процессов*
- Консалтинг

*В том числе центров ГосСОПКА

2 УРОВНИ НАРУШИТЕЛЕЙ

В основе нашего исследования лежит модель уровней нарушителей, которая учитывает значительное расслоение подходов злоумышленников к атакам на инфраструктуру. Согласно данной модели, выделяются пять основных категорий нарушителей:

КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ	Взлом устройств и инфраструктур с низким уровнем защиты для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
КИБЕРХУЛИГАН/ ЭНТУЗИАСТ-ОДИНОЧКА	Хулиганство, нарушение целостности инфраструктуры	Официальные и open-source-инструменты для анализа защищенности
КИБЕРКРИМИНАЛ/ ОРГАНИЗОВАННЫЕ ГРУППИРОВКИ	Приоритетная монетизация атаки: шифрование, майнинг, вывод денежных средств	Кастомизированные инструменты, доступное ВПО, доступные уязвимости, социальный инжиниринг
КИБЕРНАЕМНИКИ/ ПРОДВИНУТЫЕ ГРУППИРОВКИ	Нацеленность на заказные работы, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	Самостоятельно разработанные инструменты, приобретенные 0-day-уязвимости
КИБЕРВОЙСКА/ ПРОГОСУДАРСТВЕННЫЕ ГРУППИРОВКИ	Кибершпионаж, полный захват инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	Самостоятельно найденные 0-day-уязвимости, разработанные и внедренные «закладки»

3 ВВЕДЕНИЕ

За последний год уровень киберактивности злоумышленников ожидаемо вырос. Прямое влияние на увеличение числа компьютерных атак на организации оказал массовый переход компаний на удаленный режим работы и перевод большинства активностей в онлайн-формат.

В рамках данного отчета мы разбираем два ключевых аспекта защищенности организаций, которые относятся к критической информационной инфраструктуре: защищенность периметра и возможные последствия при ее низком уровне, а также фактические компрометации инфраструктур различным вредоносным ПО и их возможные последствия.

ОТЧЕТ СОСТАВЛЕН НА ОСНОВАНИИ:

- данных центра противодействия кибератакам Solar JSOC;
- результатов технических расследований Solar JSOC CERT;
- результатов проектов по анализу защищенности;
- данных с киберсистем «Ростелеком-Солар» для наблюдения за действиями атакующих (ханипотов, сенсоров и др.);
- данных с систем противодействия DDoS-атакам «Ростелекома».

КЛЮЧЕВЫЕ ВЫВОДЫ

- Большинство российских организаций уязвимы перед злоумышленниками с низкой квалификацией. Низкий уровень киберзащиты также позволяет профессиональным группировкам использовать простые хакерские инструменты, чтобы быстрее проникнуть во внутреннюю сеть жертвы и дальше развить более сложную таргетированную атаку, которая может привести к фатальным последствиям.

- В среднем по стране более 9,8% российских организаций заражены различным ВПО.

- На внешних периметрах компаний встречаются старые, но функциональные уязвимости (BlueKeep, EternalBlue, Heartbleed), а уровень своевременной установки патчей от новых уязвимостей крайне низкий. А самыми уязвимыми элементами внешнего периметра на данный момент являются веб-приложения и системы удаленного доступа (VPN).
- Также за последний год более чем на 60% выросло число автоматизированных систем управления технологическими процессами (АСУ ТП), доступных из интернета, и почти в 2 раза увеличилось количество хостов с уязвимым протоколом SMB.
- Основной проблемой во внутренних сетях является некорректное управление паролями (слабые и словарные пароли применяются повсеместно).
- Большая часть выявленных экспертами «Ростелеком-Солар» уязвимостей имеют высокую степень критичности, то есть их эксплуатация напрямую влияет на бизнес-процессы организации, может привести к хищению конфиденциальной корпоративной информации, денежных средств и потере контроля над инфраструктурой.

4 ВНЕШНИЙ ПЕРИМЕТР

В данном разделе рассмотрены уязвимости внешнего периметра, найденные в результате исследования открытых источников, а также в ходе пилотных проектов, технических расследований и работ по тестированию на проникновение.

ЭКСПЕРТЫ «РОСТЕЛЕКОМ-СОЛАР» ВЫЯСНИЛИ, ЧТО:

• ручной или полуручной процесс обновления ПО отсутствует в более чем 90% организаций;

• среднее время установки обновлений составляет более 42 дней.

При этом часть уязвимостей, которые встречаются в инфраструктуре, были обнаружены достаточно давно, но все равно остаются незакрытыми. Ниже приведены наиболее значимые уязвимости, обнаруженные до 2020 года, которые мы до сих пор встречаем у некоторых заказчиков:

3998
хостов подвержено уязвимости **Heartbleed**

1754
хоста подвержено уязвимости **EternalBlue**

11 497
хостов подвержено уязвимости **BlueKeep**

1. 1 апреля 2014 года команда безопасности Google опубликовала данные уязвимости CVE-2014-0160, впоследствии получившей название Heartbleed. При этом стоит заметить, что уязвимость существовала с 2011 года и на момент публикации уже более 15% веб-сайтов были подвержены ей.

2. 14 марта 2017 года хакерская группировка The Shadow Brokers опубликовала сведения об уязвимости CVE-2017-0144 и исполняемый код эксплойта, известного как EternalBlue. Спустя два месяца появился шифровальщик WannaCry, поразивший десятки тысяч компьютеров и ставший головной болью нескольких тысяч организаций по всему миру. Ущерб от атаки был настолько огромным, что Microsoft впоследствии выпустила обновления даже для уже неподдерживаемых операционных систем.

3. В сентябре 2019 года в составе фреймворка Metasploit появился эксплойт уязвимости CVE-2019-0708 в протоколе RDP (протокол удаленного рабочего стола), получившей название BlueKeep. По оценкам экспертов, количество устройств, подверженных этой уязвимости, соизмеримо с жертвами EternalBlue.

Эксплуатация вышеперечисленных уязвимостей в свое время вызвала широкий резонанс в обществе, а вендоры оперативно выпустили обновления. Тем не менее мы видим, что эти ошибки до сих пор активно используются хакерами для преодоления внешнего периметра и проникновения во внутреннюю сеть.

Реализация описанных уязвимостей не требует от злоумышленников высокой квалификации: эксплойты для этих уязвимостей входят в популярные фреймворки, и эксплуатировать их могут даже автоматизированные средства (например, ботнеты).

От большинства угроз на внешнем периметре можно защититься своевременной установкой обновлений. Однако многие компании до сих пор игнорируют даже самые простые превентивные меры ИБ-защиты.

5 САМЫЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ

Среди самых часто встречающихся уязвимостей на внешних хостах мы отметили:

CVE-2015-0204

Уязвимость в OpenSSL (более известная как FREAK) позволяет скомпрометировать защищенное подключение HTTPS. Ее успешная эксплуатация дает возможность провести атаку типа Man-in-the-Middle, когда злоумышленник может перехватить и расшифровать передаваемые между корреспондентами сообщения. В этом случае соединение по HTTPS переключается на менее защищенную версию протокола, при этом пользователю оно по-прежнему видится доверенным, а системы безопасности не генерируют никаких предупреждений.

CVE-2015-4000

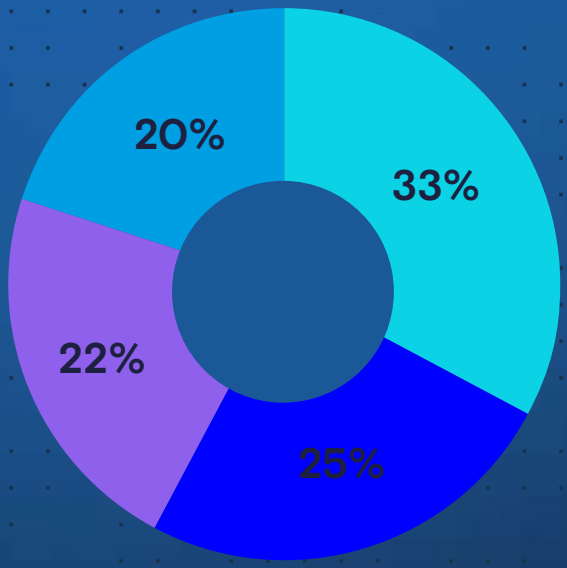
Уязвимость в криптографическом протоколе TLS версий 1.2 и ниже, которая позволяет снизить стойкость алгоритма шифрования путем подмены запросов ClientHello и ServerHello. Успешная эксплуатация также дает возможность провести атаку типа Man-in-the-Middle и расшифровать трафик.

CVE-2020-0796

Уязвимость в протоколах SMBv3, которая позволяет запустить произвольный код на стороне SMB-сервера или SMB-клиента в случае подключения к скомпрометированному SMB-серверу. В случае подобной атаки злоумышленник может воспроизвести сценарии, аналогичные распространению вирусов-шифровальщиков WannaCry и Petya. Компания Microsoft присвоила этой уязвимости критический уровень угрозы.

CVE-2019-0708

Также известна как BlueKeep. Это критическая уязвимость в службе удаленных рабочих столов (Remote Desktop Services, RDP), позволяющая атакующему без аутентификации произвести на машине жертвы удаленный запуск произвольного кода с правами SYSTEM. Наиболее известные сценарии ее успешной эксплуатации – это распространение шифровальщиков WannaCry и Petya.



САМЫЕ РАСПРОСТРАНЕННЫЕ УЯЗВИМОСТИ ВНЕШНЕГО ПЕРИМЕТРА

- CVE-2015-0204
- CVE-2015-4000
- CVE-2020-0796
- CVE-2019-0708

ПО РЕЗУЛЬТАТАМ АНАЛИЗА СОБРАННЫХ ДАННЫХ ЭКСПЕРТЫ SOLAR JSOC ОТМЕЧАЮТ, ЧТО:

1. За последний год более чем на **60%** выросло число автоматизированных систем управления технологическими процессами (АСУ ТП), доступных из интернета, что ведет к значительному росту рисков нарушения устойчивого функционирования промышленных объектов, большая часть которых относится к КИИ. Как правило, атаки на стратегически важные промышленные объекты реализуют злоумышленники с высокой квалификацией – кибернаемники и проправительственные группировки. При этом чаще всего их конечной целью является не прямая монетизация атаки (например, через вирусы-шифровальщики), а промышленный шпионаж и кибертерроризм. Поэтому промышленным предприятиям необходимо особенно ответственно подходить к мониторингу доступных из сети интернета АСУ ТП, ведь даже наличие СЗИ не защищает от ошибок (0-day-уязвимостей), допущенных при разработке ПО для промышленного сектора.

2. Слабые и словарные пароли до сих пор являются ключом от внутренней сети компаний. Компрометация учетной записи путем подбора паролей – все еще один из самых популярных способов проникновения в периметр организации. Реализовать подобную атаку могут даже автоматизированные системы и киберхулиганы. Профессиональные хакеры ищут слабые пароли, ведь скомпрометированная учетная запись избавляет их от необходимости преодолевать внешние СЗИ организации.

3. Во время пандемии почти **в 2 раза** выросло число хостов с уязвимым SMB (сетевой протокол для удаленного доступа к файлам и принтерам). Такие уязвимости особенно опасны, так как позволяют удаленно запускать произвольный код без прохождения аутентификации.
При этом эксплуатировать их могут даже низкоквалифицированные злоумышленники.

2880
АСУ ТП доступны из внешней сети

705
баз данных имеют слабые пароли

14 491
хост имеет уязвимый протокол SMB

6 РЕЗУЛЬТАТЫ ВНЕШНИХ ПЕНТЕСТОВ

Уязвимость большинства организаций перед киберпреступниками также показали работы по тестированию на проникновение внешнего периметра, проведенные командой Solar JSOC в 2020 году (для отчета собраны данные по 43 проектам).

В ходе проведения работ команде отдела анализа защищенности Solar JSOC удалось преодолеть внешний периметр и попасть во внутреннюю сеть в большей части проектов:

РЕЗУЛЬТАТЫ ПРОЕКТОВ ПО ВНЕШНЕМУ ПЕНТЕСТУ

В связи с тем, что организациям в период пандемии пришлось оперативно (и не всегда корректно) выстраивать процессы удаленной работы сотрудников, наиболее уязвимыми системами на внешнем периметре оказались веб-приложения (например, корпоративные порталы, почтовые приложения) и сервисы удаленного доступа (VPN). Именно их хакеры чаще всего использовали для проникновения во внутреннюю сеть организации, что в допандемийный период встречалось гораздо реже.

Критические уязвимости, обнаруженные в результате внешних тестирований на проникновение, и процент проектов, в которых они встречались:

44%
Некорректная настройка прав доступа

29%
Возможность внедрения SQL-кода

21%
Отсутствие защиты от brute force

21%
Небезопасная десериализация объекта

14%
Отсутствие дополнительного фактора при аутентификации в критических сервисах

14%
Открытое перенаправление

Наиболее распространенной уязвимостью оказалась некорректная настройка прав доступа. Это связано со сложной логикой современных веб-приложений, которые включают в себя различную функциональность для большого количества пользовательских ролей. Эксплуатация данной уязвимости может привести к таким последствиям, как получение доступа к персональным данным и к привилегированной функциональности приложения.

Также высокой степенью критичности обладают уязвимости, которые дают возможность проводить SQL-инъекции. В случае успеха подобной атаки хакер получает доступ к информации из базы данных веб-приложения и даже может выполнять произвольные команды на атакуемом сервере. В части реализованных экспертами «Ростелеком-Солар» проектов внедрения SQL-кода было достаточно, чтобы проникнуть в периметр организации, причем уязвимая функциональность была доступна любому неавторизованному пользователю. В некоторых инфраструктурах внедрение SQL-кода привело к компрометации сервера приложения.

Слабая парольная политика – еще один часто встречающийся недостаток безопасности инфраструктуры, характерный даже для организаций со «зрелой» командой ИБ. Почти в четверти проверенных инфраструктур отсутствует защита от brute force, то есть атак методом подбора паролей. А так как многие пользователи используют слабые словарные пароли, компрометация их учетных записей становится совсем простой задачей даже для злоумышленников с низкой квалификацией.

В случае с VPN распространенной ошибкой оказалось отсутствие дополнительного фактора аутентификации при подключении к сервису. Таким образом, если злоумышленник получит учетные данные пользователя (из открытых источников, путем подбора пароля или через уязвимости веб-приложений), то сможет легко проникнуть во внутреннюю сеть через VPN-подключение. Для ИБ-подразделения организации подключение атакующих через VPN с использованием скомпрометированной учетной записи сотрудника является трудно детектируемым инцидентом, так как такие действия соответствуют легитимной активности пользователя.

7 ДАННЫЕ С СЕНСОРОВ И ЛОВУШЕК

В этом разделе мы описываем наиболее популярное ВПО, которое используют злоумышленники. По данным «Ростелеком-Солар», **более 9,8% российских организаций уже скомпрометированы** различными семействами ВПО. В ходе анализа данных с сенсоров команда Solar JSOC CERT отметила наибольшую активность следующего ВПО:

3,4%
организаций заражены Glupteba

2,3%
организаций заражены PonyStealer

1,5%
организаций заражены Trojan-Spy.Win32.Windigo

0,8%
организаций заражены NjRAT

GLUPTEBA

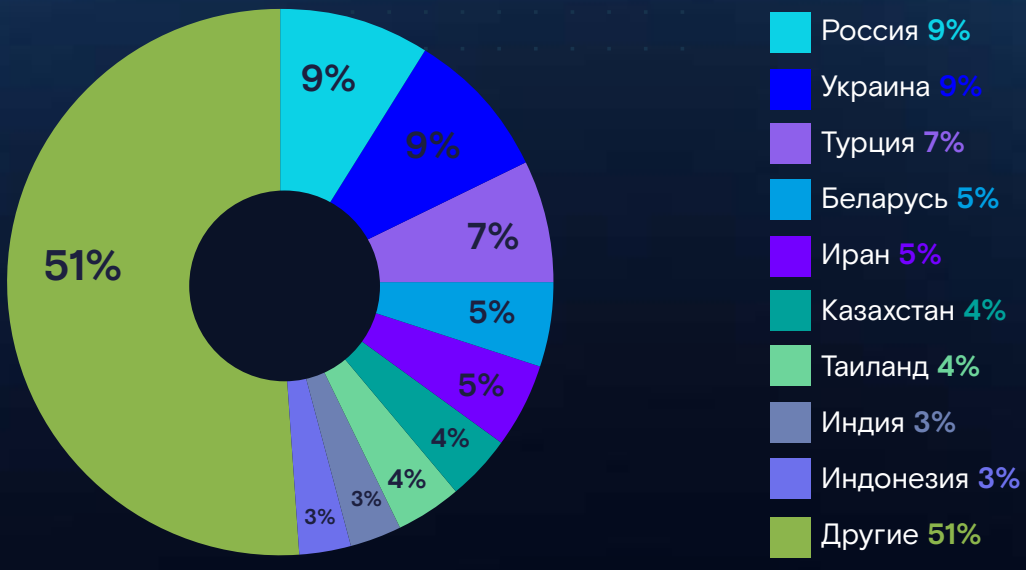
GLUPTEBA – это модульное ВПО, написанное на языке Go. Вредонос постоянно обновляется и дорабатывается авторами, а использование множества техник для защиты своих файлов от обнаружения позволяет ему долго оставаться незамеченным.

Основной модуль ВПО – csrss.exe, который чаще всего располагается в директориях C:\Windows\RSS\ и %TEMP%\csrss.

Само ВПО представляет собой модульную структуру, но привести исчерпывающий состав модулей затруднительно в связи с регулярными обновлениями. Специалистами были обнаружены следующие модули:

- Proxy;
- Browser credential stealer;
- Port-scanner;
- Miner (XMRig);
- модули для сбора различной информации о системе;
- модуль для поиска и эксплуатации уязвимостей сетевого оборудования Mikrotik (в том числе для брутфорса паролей учетной записи администратора), а также других производителей: D-Link, Ubiquiti, Zyxel, Hikvision (IP Camera).

ДОЛЯ ОБНАРУЖЕНИЙ ПО СТРАНАМ



Данные ESET

ОСНОВНЫЕ ОСОБЕННОСТИ GLUPTEBA:

- Повышение привилегий вплоть до SYSTEM (UAC-bypass → SYSTEM через токен TrustedInstaller).
- Проверка окружения на признаки виртуализации (VirtualBox, VMWare, Parallels) и песочницы (Any.Run).
- Использование руткитов для сокрытия запущенного процесса и директории, в которой располагаются файлы ВПО, а также завершения указанных процессов (службы WinmonFS, WinmonProcessMonitor, Winmon).
- Использование автозапуска (со случайными именами ключей, сгенерированных по алгоритму https://github.com/yelinaung/go-haikunator/blob/master/haikunator.go) и задач (on-logon) для закрепления в системе. Стоит отметить, что с помощью одной из задач производится повторная загрузка ВПО через certutil.exe.
- Обход встроенного брандмауэра Windows путем добавления своих файлов в исключения (netsh advfirewall firewall add rule name=»csrss» dir=in action=allow program=»C:\WINDOWS\rss\csrss.exe» enable=yes).
- Обход Windows Defender путем добавления себя в исключения (HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Paths\ (C:\Windows), HKLM\SOFTWARE\Microsoft\Windows Defender\Exclusions\Processes\ (csrss.exe)).
- Загрузка и запуск дополнительных модулей.

- Обновление своего исполняемого файла, обновление конфигурации (в более старых версиях располагалась в ветке реестра HKCU\Software\Microsoft\TestApp, теперь – в HKCU\Software\Microsoft\%4 bytes from SID digest%). Конфигурация пишется в реестр открытым текстом, шифрование не используется.

- Распространение при помощи уязвимости EternalBlue (используется архив с библиотеками ShadowBrokers).

PONYSTEALER

PONYSTEALER – один из наиболее распространенных стилеров среди киберпреступников. ВПО предназначено для похищения паролей учетных записей и другой чувствительной информации, работает с большим количеством разнообразных приложений.

TROJAN-SPY.WIN32.WINDIGO

В 2011 году компания ESET при содействии ряда экспертных групп обнаружила масштабную сеть скомпрометированных серверов, преимущественно работающих на ОС Linux и UNIX. На тот момент, по оценкам экспертов, поражены были порядка 25 000 серверов по всему миру. В списке жертв оказались cPanel.net и Kernel.org. Операцию масштабного заражения ESET назвали Windigo, позднее это имя закрепилось за ботнетом.

Несмотря на то, что ботнет известен с 2011 года, проверка индикаторов компрометации подтверждает высокую активность его распространения.

ЦЕЛИ РАСПРОСТРАНЕНИЯ ВПО:

- рассылка спама;
- кража конфиденциальных данных;
- кликфрод.

NJRAT (BLADABINDI)

NJRAT (также известный как Bladabindi) – это троян, используемый злоумышленниками для удаленного администрирования. Впервые он был обнаружен в 2012 году, а многие эксперты приписывают его создание хакерской группировке **Sparclyheason.**

ЦЕЛИ РАСПРОСТРАНЕНИЯ ТРОЯНА:

- загрузка ВПО;
- создание/изменение файлов;
- кража конфиденциальных данных;
- установка/запуск приложений.

ДАННЫЕ С ЛОВУШЕК (HONEYPOT)

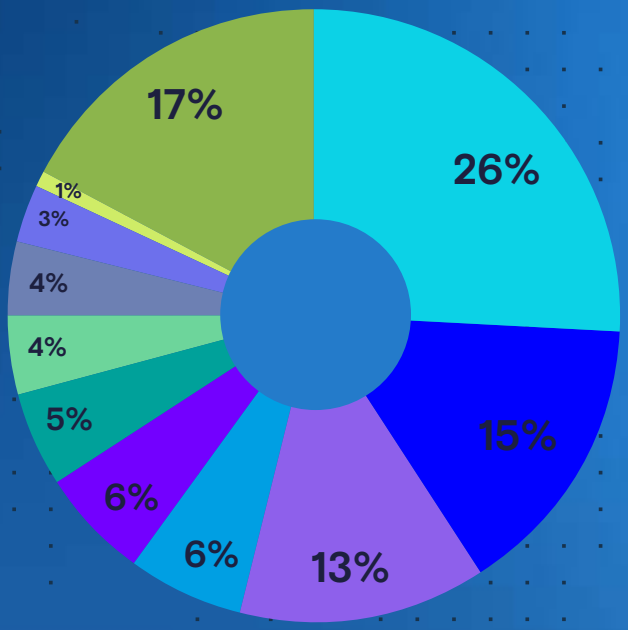
HONEYPOT – это ловушка, имитирующая уязвимый ресурс. Если злоумышленники его атакуют, то ИБ-специалисты смогут подробно изучить векторы, техники и инструменты, используемые хакерами. В данном разделе приведена статистика и описание наиболее актуальных уязвимостей, которые злоумышленники активно эксплуатировали с начала 2021 года.

CVE-2021-21972

В начале марта 2021 года появились первые публичные эксплойты ранее обнаруженной уязвимости **CVE-2021-21972** в **VMware vCenter Server**. Данная уязвимость позволяет при наличии доступа к веб-интерфейсу выполнить без аутентификации произвольный код на сервере. Эксперты Solar JSOC CERT, в свою очередь, отмечают, что с конца февраля ежедневно предпринимаются попытки сканирования и эксплуатации данной уязвимости.

ПРИНАДЛЕЖНОСТЬ К СТРАНАМ УНИКАЛЬНЫХ IP, С КОТОРЫХ АТАКУЮТ VMWARE VSPHERE:

- Китай 26%
- Германия 15%
- США 13%
- Франция 6%
- Нидерланды 6%
- Гонконг 5%
- Россия 4%
- Турция 4%
- Сингапур 3%
- Иран 1%
- другие 17%

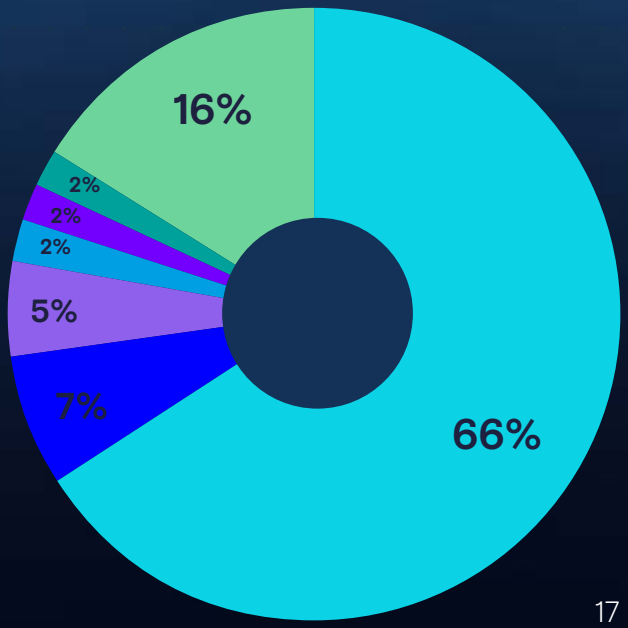


УЯЗВИМОСТИ В MICROSOFT EXCHANGE

Также команда Solar JSOC CERT отмечает, что с момента выхода внепланового обновления критических уязвимостей в Microsoft Exchange происходит активное сканирование серверов на наличие web-shell, которые применялись группировкой Hafnium. В среднем с момента публикации сервиса до первых попыток сканирования проходит менее 4 часов.

ПРИНАДЛЕЖНОСТЬ К СТРАНАМ УНИКАЛЬНЫХ IP, С КОТОРЫХ АТАКУЮТ EXCHANGE

- США 66%
- Германия 7%
- Нидерланды 5%
- Китай 2%
- Литва 2%
- Монголия 2%
- Другие 16%



8 ПРОЧИЕ УЯЗВИМОСТИ

С начала 2021 года зафиксирован всплеск эксплуатации уязвимости удаленного исполнения кода в Oracle Weblogic **CVE-2020-14882**. Чаще всего она используется для распространения ботнетов, устанавливающих майнеры криптовалют.

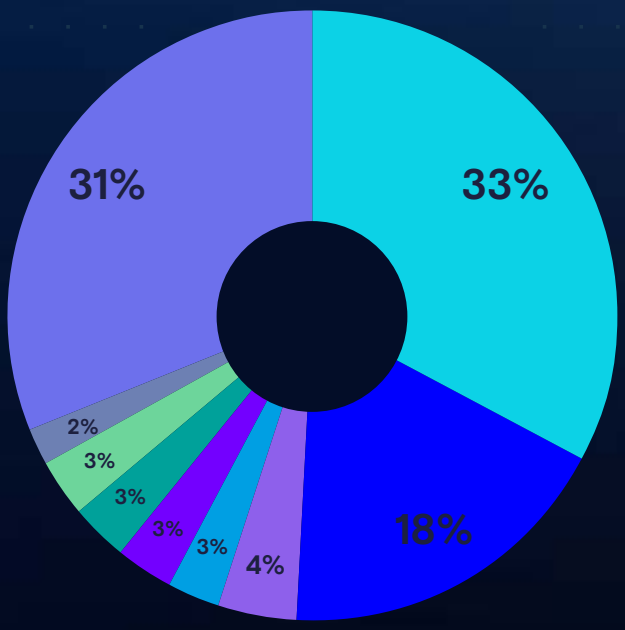
По-прежнему в огромном количестве отмечаются попытки эксплуатации уязвимости в протоколе SMB **EternalBlue CVE-2017-0144**.

В российском сегменте отмечаем распространение бот-сети семейства Dota, которая чаще всего при заражении устанавливает ПО для майнинга криптовалюты **Monero**.

Brute force слабых и словарных паролей по протоколу SSH по-прежнему занимает лидирующие позиции среди активностей злоумышленников. Наибольшее число brute-force-атак осуществляется с IP-адресов Китая.

ПРИНАДЛЕЖНОСТЬ К СТРАНАМ УНИКАЛЬНЫХ IP, С КОТОРЫХ АТАКУЮТ ПО ПРОТОКОЛУ SSH:

- Китай 33%
- США 18%
- Франция 4%
- Германия 3%
- Гонконг 3%
- Республика Корея 3%
- Бразилия 3%
- Нидерланды 2%
- Другие 31%



9 РЕЗУЛЬТАТЫ ВНУТРЕННИХ ПЕНТЕСТОВ

Незащищенность организаций перед злоумышленниками, успешно проникшими во внутреннюю сеть, подтверждают результаты работ по тестированию на проникновение внутреннего периметра, проводимых командой отдела анализа защищенности Solar JSOC. Эксперты компании смогли получить полный контроль над доменом во всех проектах.

Большую часть векторов атак, в результате которых атакующим удалось закрепиться и повысить привилегии, смог бы реализовать низкоквалифицированный злоумышленник, обладающий минимальными правами в домене.

В части проектов для получения максимальных привилегий экспертам Solar JSOC потребовалась всего одна атака.

Основной проблемой во внутренних сетях является некорректное управление паролями. Так, самыми распространенными уязвимостями оказались: хранение учетных данных на общих файловых ресурсах и в групповых политиках, а также использование слабых паролей. Общие файловые ресурсы и групповые политики являются небезопасным местом для хранения учетных данных, так как любой авторизованный в домене пользователь может получить к ним доступ. В ряде организаций в общедоступных файлах хранились учетные данные локальных администраторов и администраторов баз данных и доменов. А простые пароли были установлены не только у рядовых пользователей, но даже у некоторых администраторов доменов, что сразу приводило к получению контроля над всей инфраструктурой.

100%
Хранение учетных данных на файловых ресурсах

75%
Использование словарных паролей

75%
Запуск сервиса от имени привилегированной учетной записи

50%
Чтение памяти процесса isass.exe

50%
Хранение паролей в поле «комментарий» в свойствах учетных записей

50%
Некорректно сконфигурированные средства антивирусной защиты

50%
Наличие учетных данных в групповых политиках

50%
Использование учетных данных по умолчанию

Ростелеком
Солар

Задать вопрос или
попробовать сервис

solar@rt-solar.ru
+7 (499) 755-07-70
rt.ru
rt-solar.ru