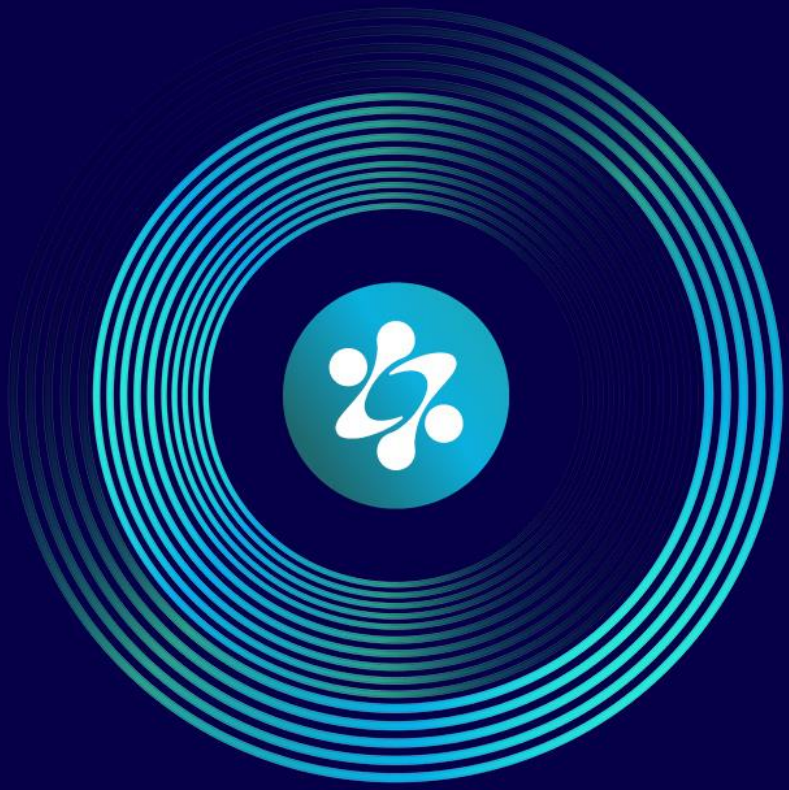

Война «Железных мечей»

В киберизмерении:

Понимание и методы преодоления трудностей

Национальный кибермассив

декабрь 2023 г.

Версия 1.0

מערך הסייבר הלאומי

Оглавление

Управляющее резюме

С начала войны «Железных мечей» Национальный кибермассив выявил активность, которая в некотором смысле активизировалась.

постепенное нападение различных типов на организации в израильском киберпространстве.

Злоумышленники используют широкий спектр методов и приемов, начиная с простых и незамысловатых атак, таких как

Порча веб-сайтов или DoS-атаки, вплоть до целенаправленных атак на организации, образующие цепочку

Поставка многим организациям экономики с целью получения широкого эффекта.

В этом документе Национальный кибермассив рассматривает кибератичность, выявленную на данный момент в киберпространстве.

в Израиле и указывает на ряд выводов, сделанных в первые два месяца боевых действий.

Характер деятельности злоумышленников

1. В годы войны наблюдалось значительное усиление наступательной деятельности. Со временем и постепенно. на сцене Что касается войны, большинство атак направлены на цели повреждения (CNA), в отличие от целей, определенных ранее боевые действия и в их начале больше характеризовались нападениями в целях шпионажа и кражи информации (КНЭ).
2. В течение этого периода мы наблюдали использование техник, тактик и процедур (ТТП), которые часто использовались В других событиях в мире, таких как украинско-российская война. Например, вы можете увидеть сходство между Войны по двум основным вопросам, о которых мы поговорим позже:
    - Использование психологической войны (сознания) как средства отражения кибератак и использование сетей социализация для усиления влияния.
    - Использование неверных и насильников типа.Стеклоочиститель
3. Основные действия злоумышленников в израильском киберпространстве во время войны:
    - Виден четкий контур атаки.**в широкой распылительной деятельности ((Распыление**- В этом плане будет предпринята попытка использовать известные уязвимости и человеческие ошибки в приложении**настройки конфигурации (неправильная конфигурация)**., например, использование слабых паролей и отсутствие мер по блокировке учетной записи. После установки порога неудачных попыток аутентификации.
    - **широкое использование распределенных атак типа «отказ в обслуживании»)(DDoS**- на прикладном уровне (Порча) и на уровне средств массовой информации, а также порча веб-сайтов (Уровень 7)
    - **Множество попыток проникнуть на различные объекты в этом районе.**- Для того, чтобы получить контроль и реализовать утечку информации и/или удаление информации (Wiper).
    - **Действия против системЛинукс**- Добавлена общая активность против установленных систем, Окна Во время войны была обнаружена активность против систем Linux.[1], включая запуск Wiper как часть Атака с целью нанесения ущерба[2][3]. Среди прочего было задокументировано использование различных техник повышения привилегий.

Linux Wiper использует готовые двоичные файлы[1]
https://www.gov.il/he/departments/publications/reports/alert_1668
Linux Wiper использует готовые двоичные файлы[2]
https://www.gov.il/he/departments/publications/reports/alert_1668
Очистка диска[3]

и поддержание контроля с помощью встроенных механизмов планирования операций, таких как запланированные задачи или Cron

рабочие места[4][5].

- **Камеры безопасности и сетевые камеры**(с целью ухудшения возможности использования данного оборудования в целях безопасности – (видеонаблюдение).

на физическом пространстве, а также попытках противника собрать разведданные из районов, наблюдаемых этой техникой.

Атакам также подверглись различные IoT-устройства.

- **влияние на операции**)Со стороны атакующих групп преимущественно в сетях - (Операции влияния

Социальность. Также используются различные каналы и профили, выдающие себя за других, публикующие ложную информацию.

Публикация достоверной информации без контекста (Дезинформация) или дезинформации (Фейковые новости)

соответствующей технологии с целью введения в заблуждение, причинения вреда или попытки манипулировать

Осведомленность об израильской общественности (недостоверная информация)

- **Фишинговые атаки**(С помощью социальной инженерии, как в электронных письмах, так и в сообщениях – Фишинг

, в целях повышения надежности. Иногда даже добавляется элемент отправки личной информации получателя СМС.

чтобы он активировал ссылку или ссылку. Это правда, что это поразительный метод атаки в повседневной жизни, но

В годы войны наблюдался значительный рост такого рода походов.

- **Атака приложениймобильный**(приложения для смартфонов) – или инфраструктуры этих приложений,

Путем публикации приложений, выдающих себя за другое лицо, использования брешей в безопасности в инфраструктуре приложений и многого другого.[6]

- **нападения на организации, входящие вMSP**- которые составляют важную цепочку поставок

для многих организаций экономики. В этой категории вы можете найти веб-хостинг и хостинговые компании, а также компании

Интеграция и предоставление услуг ИКТ.

4. На данный момент в ходе боевых действий были выявлены**о-15 атакующих групп**руководители, действующие в израильском киберпространстве.

Эти группы идентифицированы как связанные с Ираном, Хамасом и Хезболлой.И большинство из них делятся информацией друг с другом

Разведка, методы и инструменты в пользу реализации различных типов атак на объекты в Израиле, против которых они действуют.

https://attack.mitre.org/techniques/T1561/

T1053 — Запланированная задача/задание[4]

https://attack.mitre.org/techniques/T1053/

TA0004 — Повышение привилегий[5]

https://attack.mitre.org/tactics/TA0004/

Мобильные методы[6]

https://attack.mitre.org/techniques/mobile/

5. Предпринимаются попытки привлечь к участию различные целевые аудитории, например, антиизраильских активистов.

в наступательной деятельности против Израиля, делая цели доступными для нападения или простыми инструментами для выполнения

Атаки типа «отказ в обслуживании».

Израильские организации на киберфронте

1. Активность злоумышленников выявлена в отношении организаций, имеющих следующие характеристики:

А. Организации, являющиеся центром деятельности других организаций, как часть цепочки.

Поставки различных организаций в израильской экономике.

Б. Организации в сфере здравоохранения.

третий. Организации водного хозяйства.

д. организации академического сектора.

Бог. Организации в сфере энергетики и топливного снабжения.

и. Организации в транспортной сфере.

Г. Организации, занимающиеся морскими перевозками и таможенным брокерством.

2. Эти организации иногда предоставляют такие услуги, как межотраслевые общие приложения. особенность

Общее, что существует, когда этим организациям причинен вред, — это возможность широкомасштабных последствий для организаций.

больше в секторе или тех, кто пользуется услугами атакуемой организации.

Типы активов, подвергающиеся атаке

1. Активность злоумышленников была обнаружена в отношении большого количества общих активов, используемых в экономике:

А. Системы физической безопасности, обслуживающие различные организации в экономике, например камеры видеонаблюдения.

Б. Открытые интерфейсы управления, такие как интерфейс контроллера с удаленным управлением.

третий. Коммуникационное оборудование, предоставляющее интерфейсы управления для сети Интернет, например Juniper, Cisco.

д. Системы удаленного мониторинга и управления, подключенные непосредственно к Интернету.[7].

Бог. Интерфейсы удаленного доступа, такие как Citrix, Fortinet.

CISA публикует план киберзащиты JCDC по удаленному мониторингу и управлению (RMM)[7]
https://www.cisa.gov/news-events/alerts/2023/08/16/cisa-releases-jcdc-remote-monitoring-and -
план управления-rmm-cyber-defense

И. Серверы веб-почты, такие как интерфейсы Exchange OWA, Roundcube и/или EWS.

Г. Системы управления контентом (CMS), такие как Joomla, Drupal, WordPress.

ЧАСIoT-устройства.

девятый. Интерфейсы API, доступные через Интернет, например интерфейсы REST/SOAP.

Инструменты и методы атаки, используемые злоумышленниками

1. Использование методов атаки на основе инструментов, установленных на объекте атаки в составе операционной системы или

Приложения LOLBAS (двоичные файлы, скрипты и библиотеки Living Off The Land).[8]

2. Предоставление инструментов атаки для использования сторонами без технических знаний. Например, доступ к веб-сайту, который содержит сценарий атаки.

Отказ в обслуживании (DDoS), при котором злоумышленнику достаточно ввести адрес цели атаки.

3. Использование файлообменных сервисов для запуска инструментов атаки или использования законного пользователя для доступа.

первично в сети организации, минуя меры безопасности**и как канал утечки информации.**такие услуги, как

.Microsoft OneDrive, Google Drive, Dropbox, серверы Discord

4. Использование инструментов с открытым исходным кодом, преобразованных злоумышленниками, таких как DCOMpotato.[9],

Когда некоторые из этих инструментов неправильно используют WinAPI.[10]

5. Использование бесплатных и коммерческих прокси-серверов и инфраструктур VPN или, альтернативно, конечных точек, подвергшихся атаке с целью

Используется в качестве назначенного прокси-сервера для обхода ограничений, таких как использование GeoLocation для предотвращения доступа.

танец.

6. Злоупотребление законным функционалом корпоративной электронной почты после захвата почтового ящика.

Почта одного из пользователей организации. Например, установка правил Outlook/OWA/Office365 для отправки

Скопируйте электронное письмо злоумышленнику и удалите отправленное сообщение.

7. Использование Reverse Shell для связи с сервером управления (C&C) и утечки информации.[11]

[8]Примерный список инструментов доступен по адресу: https://lolbas-project.github.io Living Off The Land
Двоичные файлы, сценарии и библиотеки/
[9]Орудия нападения, используемые в Израиле 1671_https://www.gov.il/he/
departments/publications/reports/alert

T1106 — собственный API[10]
https://attack.mitre.org/techniques/T1106/
Обратная оболочка[11]
https://attack.mitre.org/techniques/Тш/1059
T1059 - Интерпретатор команд и сценариев

8. Использование хостинга сайтов и услуг хостинга (Hosting Services\VPS), как инфраструктуры для проведения атак.

9. Список уязвимостей, используемых различными атакующими группами, прилагается в Приложении А.

До сих пор мы сосредоточились на кибератаках, которые были обнаружены в израильском пространстве во время войны.

из причин нанесения ущерба функциональной непрерывности экономики.

В войне есть еще один аспект в контексте нападений, которые приносят экономическую выгоду или имеют форму экономической выгоды;

Киберпреступность

На фоне войны также наблюдалась тенденция роста числа случаев вымогательства в Израиле. Выбор выкупа как наступательного инструмента

Это неудивительно и даже естественно в настоящее время, когда война разума составляет значительную часть кампании. эффект

Сдерживание и хаос, возникающие после атаки с целью выкупа, достигают своих целей. Это простые и удобные в эксплуатации устройства.

Доступны рядовому пользователю и не требуют особых технологических знаний для их реализации. Из анализа содержания отчетов, которые

Полученные Национальной киберсистемой и обработанные нами, появляется ряд идей:

1. **Растущая тенденция в использовании куфиров.Стеклоочиститель**- Нарушители, для которых характерно стирание правила
   Информация в сети. Иногда это действие сопровождается разглашением информации (с целью проведения переговоров о
   информации, унижение жертвы, хвастовство со стороны нападающего) или просто удаление ее с целью нанесения ущерба
   организму и его функциональной непрерывности.
2. **Ущерб типа выкупа, осуществляемый преступными группировками в бизнес-модели- Программы-вымогатели (RaaS
   квалификация)**- Эта модель, предлагающая конфигурацию подписки, позволяет каждому пользователю приобретать продукт по себестоимости.
   ежемесячно и использовать его в своих целях и участвовать в прибыли, полученной от уплаты выкупа
   жертвы. Использование купонов как услуги особенно удобно, поскольку купленный товар поставляется с
   Полная техническая поддержка, не требует высокого уровня технических знаний, наносит ущерб с минимальными усилиями,
   Гарантирует доход и анонимность пользователю. Искупление не является уникальным для каждой жертвы и затрудняет ассоциацию.
   конкретному абоненту в большинстве случаев.
3. **Первоначальное использование наступленияLinux нацелен на серверы на базе Wiper**- Эта тенденция сходится с
   Глобальные отчеты о вымогательстве и преступных группировках одновременно с государственными атакующими группами
   которые концентрируют технологические усилия для разработки вредоносных инструментов против устоявшихся систем.
   на своих оттенках. Экспансия враждебных субъектов в киберпространстве по отношению к системам Unix

Для работы, отличной от Windows, защищающая сторона должна понимать риски и предоставлять ответные меры.

против усиления и действий этих врагов

(12Враг осознает, что человеческий фактор в кибератаке является связующим звеном.) БИБИ, ЛОЛБИН

ослабление. Значительный процент киберинцидентов, обрабатываемых массивом, вызван человеческим фактором.

которые открыли фишинговое электронное письмо, нажали на незнакомую ссылку или загрузили незнакомый файл в свои системы.

Это не уникальная тенденция во время войны, но не исключено, что это предпочтительный вектор.

врагом в это время.

4.**Резкое увеличение использования слабостейкак вектор проникновения для однодневных сетей**- Кажется, что группы

Атака часто следует за публикацией слабых мест и находит «окна» для этих слабых мест.

в очень короткие промежутки времени. Использование этих слабостей не является уникальным для одной группы, и это можно увидеть

Широкое использование этих слабостей государственными атакующими группировками и преступными группировками.

Противодействие террористическим фондам – экономическая кампания

1. На протяжении многих лет Государство Израиль проводит настойчивую экономическую кампанию параллельно с физической и кибервойной.

Против террористических организаций и факторов финансирования этих организаций во всем мире.

2. ХАМАС, как и другие террористические организации в мире, прибегнул к использованию цифровых валют, чтобы затруднить задачу.

за то, что помешал его источникам финансирования, главным образом Ирану. Переход от валюты, не обеспеченной товарами (ФИАТ),

в криптовалюту, помог Хамасу регулярно получать много денег из Ирана в течение двух лет до войны.

«Железные мечи».

3. Во-первых, ХАМАС использовал криптовалюту для получения небольших пожертвований от сторонников со всего мира.

мире, но вскоре перешел к масштабным краудфандинговым кампаниям, в том числе через социальные сети,

Эти доходы достигли в общей сложности миллионов долларов.

4. По данным Национального штаба по борьбе с экономическим терроризмом (MTL), криптовалюта стала неотъемлемой частью деятельности.

Операция Хамас. Перечисленные средства используются, в том числе, на закупку вооружения и финансирование

Другие террористические акты.

Linux Wiper использует готовые двоичные файлы12

https://www.gov.il/he/departments/publications/reports/alert_1668

5. В рамках экономической войны против террористических организаций различные партнеры системы безопасности Израиля определили и конфисковали цифровые кошельки, в которых находились десятки миллионов долларов в самых разных токенах (монетах криптографы), из которых ведущими являются: Bitcoin (BTC), Ethereum (ETH) и Tron (TRX).

6. Национальная киберсистема присоединилась в качестве партнера к экономической кампании с самого начала войны. как часть деятельности Для этого в массиве были разработаны технологические инструменты и методы, которые позволили найти десятки кампаний по финансированию. терроризм,**стоит миллионы долларов**.

7.Разработанные инструменты и методы были созданы для того, чтобы реагировать на вызовы системы безопасности, что отражено к формированию партнерами из сообщества безопасности. В целях оказания помощи в сборе, поиске и обработке информации. Осинт (OSINT) о кампаниях по финансированию терроризма. Технологические инструменты распределены по как можно более широкому кругу Наличие платформ, на которых действуют сборщики средств террористической организации, с упором на платформы. Краудфандинг, социальные сети и многое другое.

идеи

1. После выявления различных моделей атак и тенденций развития в ходе боевых действий можно указать на Некоторые идеи:

А. **По мере затягивания боевых действий смелость и изобретательность нападающих возрастают.**- Это можно увидеть При переходе от атак CNE к атакам CNA, а также «качественным» атакам, таким как атака на больницу.

Б. **Целевые организации, которые обслуживают множество организаций**- Поскольку организация обслуживает больше сторонних организаций Для него, будь то внутри сектора или в качестве поставщика услуг, он становится более привлекательной целью. Для меня потенциальный злоумышленник.

третий. **Множественные атаки помех**- В свете многочисленных атак с целью выкупа или деструктивного стирания (Требуется дворник Подчеркните способность к восстановлению.

Д. **Наличие нескольких резервных копий**- желательно в разных технологиях, из которых хотя бы одна проведена В любое время в автономном режиме имеет решающее значение для восстановления.

Бог. **Воспроизводимость**- Убедитесь, что организация способна успешно восстановить все киберактивы. и информация, начиная с аппаратного уровня и выше в альтернативной среде, на основе нового аппаратного обеспечения и/или Среда общедоступного облака, особенно для случаев, когда злоумышленник нарушит целостность оборудования, Например, нарушение/удаление UEFI/BIOS.

И. **Использование GeoLocation для предотвращения доступа злоумышленников из-за границы**- не считается средством защиты
Герметичность против злоумышленника, имеющего доступ к СМИ целевой страны. Многие злоумышленники обходят
Эти механизмы основаны на использовании бесплатных коммерческих сервисов или атаке на промежуточные серверы.
в стране назначения. Однако рекомендуется реализовать использование данного механизма в сети организации во благо.
Снижение воздействия на сеть и максимальное предотвращение различных типов атак.

Г. **Распределенные атаки типа «отказ в обслуживании»**(Требует предварительной подготовки организации - (DDoS).
Через соглашения с интернет-провайдером и/или специализированной службой фильтрации трафика. Среди прочего,
Реагирование на различные уровни объема и частоты атак с акцентом на уровне
Прикладной и сетевой уровень

ЧАС **Доступ к камерам видеонаблюдения в сети**- Камеры являются важной мерой безопасности на службе организации,
Не подвергайте их прямому доступу в Интернет, установив надежный пароль (и, если возможно,
MFA-аутентификация) и ограничить доступ к ним только соответствующим пользователям. При их установке происходит
Убедитесь, что они не нацелены на чувствительные районы или объекты государственной безопасности.

девятый. **Аварийный персонал**- Заранее подготовиться к отсутствию профессиональных ключевых факторов
В случае чрезвычайной ситуации рекомендуется подготовиться к альтернативным вариантам путем заключения договора на обслуживание/аренды альтернативного ЦС.

Дж. **Повышение бдительности в чрезвычайной ситуации**- Рекомендуется заранее рассмотреть вопрос о повышении бдительности в случае возникновения чрезвычайной ситуации.
Состояние, включая принятие превентивных мер, таких как ускоренное отключение интерфейсов.
из Интернета, предотвращая доступ к второстепенным службам и серверам или ужесточая политики
Серфинг в Интернете.

11 **Объявления для сотрудников**- Рекомендуется повысить осведомленность сотрудников об распространенных моделях атак, в частности
Фишинговые атаки и общепринятые методы борьбы с ними, включая важность сообщения в случае подозрений
за киберинцидент.

12. **Физическая охрана серверных помещений**- Война подняла важность физической безопасности.
и среду серверных и рабочих зон, чтобы сохранить функциональную непрерывность
В случае проникновения на объект или физического повреждения в результате ракетного обстрела.

Методы преодоления и рекомендации

Уменьшение поверхности атаки

1. Рекомендуется принять меры по уменьшению внешней поверхности атаки организации (EASM) посредством непрерывного картирования.

и отслеживание изменений в нем, при этом предпринимая действия по уменьшению поверхности атаки. Например, вы можете отменить

Доступ к чувствительным портам (интерфейсам управления) или к тем, которые не нужны для деловой активности и как можно меньше

Возможное количество и разнообразие корпоративных услуг, доступных из сети Интернет.

Обновления информационной безопасности |

2. Многие производители позволяют подписаться на списки рассылки и получать уведомления об обновлениях информационной безопасности.

непосредственно на электронную почту.Рекомендуется воспользоваться этой возможностью и проверить, как работают производители оборудования.

вашей организацией и постоянно следите за этими публикациями.

3. Рекомендуется проверять установку обновлений, особенно имеющих критическую и высокую классификацию, в течение разумного периода времени до даты.

их публикация. Поскольку злоумышленникам удается эксплуатировать уязвимости уже через несколько часов после их публикации. спать

Очень важно выполнить установку как можно быстрее, поскольку ресурсы напрямую подключены к Интернету.

Доступ к интерфейсам управления из Интернета

4. Рекомендуется избегать использования Интернета для предоставления доступа к интерфейсам управления. может быть использован

В такой службе, как VPN с шифрованием и соответствующей строгой аутентификацией, а также с использованием сотовой инфраструктуры APN или

VPN и оплата для реализации MPLS

5. Настройка каждому пользователю удаленного доступа, в частности с правами администратора, строгой аутентификации (MFA).

6. Реализация механизма Geo-Velocity для обнаружения аномалий в процессе идентификации и управления сессиями.

7. Изучение возможности ограничения удаленного доступа путем применения списка запретов на основе угроз.

: который постоянно обновляется со ссылкой на следующие данные разведки.

1. IP-адреса бесплатных и коммерческих прокси-сервисов, таких как: I2P, Freenet, TOR.

.ZeroNet, KPROXY, CroxyProxy

2. IP-адреса бесплатных и коммерческих VPN-сервисов.

3. IP-адреса, связанные с известными схемами атак.

4. IP-адреса, связанные с враждебными странами.

Усиление защиты конечных точек и серверов

8. Рекомендуется убедиться, что операционные системы и приложения не используются без поддержки производителя (End of Life).

9. Рекомендуется убедиться, что учетные записи пользователей с высокими привилегиями не используются регулярно.

10. Рекомендуется протестировать и активировать следующие механизмы безопасности на конечных точках и серверах:

Безопасная загрузка, защита учетных данных Windows, защита устройства защитника Windows, контролируемый доступ к папкам, песочница Windows, AppLocker, брандмауэр Windows

11. В мультитенантной среде рекомендуется изучить возможность одновременной активации нескольких механизмов.

Чтобы различать различные клиентские среды, в том числе: Экземпляр IAM, выделенный для каждого клиента, шифрование информации каждого

Клиент, использующий выделенный ключ шифрования, с использованием ботов уровня ядра, таких как SELinux и/или

Выделено для всего клиентского трафика VXLAN\Geneve, назначение Chroot

12. Рекомендуется убедиться, что на конечных точках и серверах установлена последняя версия EDR/XDR и поддерживается

и регулярно пополняется. Реализация продуктов этого типа**Доказанная эффективность в предотвращении и сдерживании кибератак.**.

Защита корпоративного сайта

13. Рекомендуется убедиться, что сайт защищен с помощью WAAP.[13], который включает реализацию списка разрешенных на уровне поля.

и ввод, а также его способность определять, исходит ли трафик от человека или от машины, и блокировать последнюю.

14. Рекомендуется убедиться, что веб-сайт разработан и поддерживается в соответствии с принятыми требованиями безопасной разработки,

например OWASP ASVS[14].

Защита корпоративных мобильных приложений |

15. Рекомендуется проверить, что корпоративное мобильное приложение разработано и поддерживается в соответствии с принятыми требованиями.

Для безопасной разработки, например OWASP MASVS.[15].

Защита «бренда».

16. Изучение использования службы защиты бренда для выявления аномалий, таких как создание веб-сайта или

Запуск мобильного приложения Imposter.

17. Проверка выдающего себя мониторинга приложений.

WAAP — защита веб-приложений и API (WAAP)[13]

Стандарт проверки безопасности приложений OWASP[14]
https://owasp.org/www-project-application-security-verification-standard/

Безопасность мобильных приложений OWASP[15]
https://mas.owasp.org/

Защита электронной почты |

18. Рекомендуется периодически проверять параметры конфигурации системы электронной почты на предмет соответствия утвержденным базовым показателям.

Например, правила Outlook, правила транспорта.

19. Блокировка доступа к веб-интерфейсам почты из сети Интернет. Если существует бизнес-требование разрешить это,

Рекомендуется реализовать MFA и защиту с помощью WAF.

20. Убедиться, что система электронной почты позволяет получать электронные письма, рекомендуется только после выполнения следующих тестов:

1. Электронное письмо не является спамом и не отправлено с IP-адреса/домена с низкой репутацией.

2. Письмо не содержит ссылок на IP\Domain IP-адреса с низкой репутацией.

3. Электронное письмо содержит вложение в соответствии с типом, указанным в списке разрешений. Существует идентификатор между расширением файла,

Заголовок, указывающий его тип и полезную нагрузку.

4. Письмо не содержит повреждений – благодаря использованию актуальных подписей и тестированию в песочнице.

для обнаружения подозрительного поведения.

5.Письмо не содержит встроенного кода в текстовом поле.В случае наличия кода данного типа,на массиве

Защитите электронное письмо, чтобы удалить его, или выполните кодирование перед его доставкой пользователю, чтобы это было невозможно.

бежать

6. Система электронной почты четко указывает пользователю, что источник электронной почты находится за пределами организации.

Защита просмотра от организации

21. Блокировка доступа к IP/доменным адресам с низкой репутацией (URL Filtering).

22. Рекомендуется реализовать возможность открытия зашифрованного трафика с целью обнаружения и предотвращения угроз.

23. Отказ пользователю в прямом доступе к Интернету посредством использования буфера, такого как RBI или технологии.

Похожий.

24. Убедиться в возможности скачивания файлов рекомендуется только после прохождения следующих тестов:

1. Файл имеет тип, определенный в списке разрешенных, и между расширением файла и заголовком существует идентичность.

с указанием его типа и полезной нагрузки.

2. Файл не содержит повреждений - за счет использования актуальных сигнатур, а также тестирования в Sandbox.

для обнаружения подозрительного поведения.

Безопасность цепочки поставок

25. Рекомендуется убедиться, что поставщики в цепочке поставок соответствуют требованиям метода цепочки поставок.

Национальный кибермассив.[16]

Физическая охрана |

26. Подготовка к предотвращению возможного физического ущерба объектам и восстановлению после него во взаимодействии с силами безопасности.

физический в организации.

27. Рекомендуется проверить соответствие серверных помещений организации требованиям стандарта 942-TIA или Uptime.

и выше уровня 3, Институт

28. Рекомендуется убедиться, что корпоративная серверная комната и альтернативная площадка (ДР) расположены в разных географических зонах.

и не примыкают друг к другу. В случае отсутствия альтернативного веб-сайта рекомендуется рассмотреть возможность создания веб-сайта этого типа, или

Использование среды публичного облака в качестве замены.

Национальные проекты Национального кибермассива

1.**проектЗЕРКАЛО**-Сообщество: управление восстановлением IR (для) организационной устойчивости

профессионально в целях быстрого и взаимного обмена технической информацией.[17]

2.**планВДП**–Программа раскрытия уязвимостей

Сообщество профессиональных исследователей, которые обеспечивают устойчивость израильской и мировой экономики.

3.**Фишинговые инфраструктуры**- Обнаружение и сообщение об инфраструктурах фишинга и мошенничества в киберпространстве.

4.**Центр отчетности**- В любом случае подозрения на киберинцидент вы можете обратиться в оперативный центр, доступный 24/7 по номеру

119, для сообщения и помощи в случае необходимости.

Отчетность в компьютеризированной форме-

Форма отчета организации

Форма отчета гражданина

Анкета для поставщиков для укрепления цепочки поставок - версия 1.4[16]

https://www.gov.il/he/departments/news/querysupply

[17]проект -Приглашаем к участию в профессиональной группе обмена информацией MIRROR

https://www.gov.il/he/departments/publications/Call_for_bids/mirror_call

Приложение A | Список уязвимостей, часто используемых атакующими группами

Первая часть - слабые места, которые использовали около 15 группировок для атак в Израиле:[18]

Продукт	Продавец	CVSS	CVE
Алер Шлюз си НетС NetScaler АЦП	Цитрикс		CVE-2023-4966 7.5
Системный сервер	системная помощь		CVE-2023-47246 9,8
итнофаз рацион Конфигурация BIG-IP	F5		CVE-2023-46748 8.8
итнофаз рацион Конфигурация BIG-IP	F5		CVE-2023-46747 9,8
bmail e Круглый куб с	Круглый куб		CVE-2023-43770 6.1
WinRAR	РАРЛАБ		CVE-2023-38831 7.8
Юнос ОС	Можжевельник		CVE-2023-36851 5.3
Юнос ОС	Можжевельник		CVE-2023-36847 5.3
Юнос ОС	Можжевельник		CVE-2023-36846 5.3
Юнос ОС	Можжевельник		CVE-2023-36845 9,8
Юнос ОС	Можжевельник		CVE-2023-36844 5.3
ээээ MOVEit Трансф	Прогресс		CVE-2023-34362 9,8
Win32k	Майкрософт		CVE-2023-29336 7.8
ФортиОС	Фортинет		CVE-2023-27997 9,8
и сервер та Центр Слияние Да	Атласиан		CVE-2023-22518 9.8
и сервер та Центр Слияние Да	Атласиан		CVE-2023-22515 9.8
Веб-интерфейс IOS XE	Циско	10,0	CVE-2023-20198
e Управление двигателем	Зохо		CVE-2022-47966 9,8
ээээ бменный сервер	Майкрософт		CVE-2022-41082 8.8
Центр река/данные Слияние Се	Атласиан		CVE-2022-26134 9,8
БИГ-ИП	F5		CVE-2022-1388 9,8
Лог4j2	Апач	9,0	CVE-2021-45046
ер Вордпресс Ко	WordPress		CVE-2021-44223 9,8
ээээ бменный сервер	Майкрософт		CVE-2021-34473 9,8
Лизированный менеджмент a-IQ Центр БИГ-IP и БОЛЬШОЙ	F5		CVE-2021-22986 9,8
Люси Сервер	Люси Сервер		CVE-2021-21307 9,8
БИГ-ИП	F5		CVE-2020-5902 9.8
ээээ Веблогик сер	Оракул		CVE-2020-14882 9.8
SMBv3	Майкрософт	10,0	CVE-2020-0796
троллер (АЦП), ливрея Кон e Приложение Д		9,8	
Устройство АНОП Вт SD-WAN шлюз и	Цитрикс		CVE-2019-19781
d Маршрутизаторы RV325 РВ320 ан с Малый бизнес	Циско		CVE-2019-1653 5.3

[18] Уязвимости, используемые для атак в Израиле 1667_https://www.gov.il/he/departments/publications/reports/alert

Безопасный Импульсное подключение		Иванти	10,0	CVE-2019-11510
ФортиОС		Фортинет		CVE-2018-13379 9.8
рдпад	Офис и By	Майкрософт		CVE-2017-0199 7.8
	Окна	Майкрософт		CVE-2017-0143 8.1

Часть вторая | Слабые стороны использования деятельности киберпреступников в израильском киберпространстве:[19]

CVSS	ВЕС	рВенд	тСПроду
7.2	20273 -CVE-2023	Циско	ИОКС XE
10,0	20198 -CVE-2023		
9.1	20269 -CVE-2023	Циско	АСА, ФТД
7.2	20209 -CVE-2023	Циско	с, СВК Серия скоростных автомагистралей
9,8	20252 -CVE-2023	Циско	Менеджер Катализатор SD-WAN
9,8	3519-CVE-2023	Цитрикс	NetScaler АЦП
7,5	4966-CVE-2023		йаNetScaler шлюз
7,5	4967-CVE-2023		
9,8	29357 -CVE-2023	Майкрософт	SharePoint
5.4	5631-CVE-2023	еКруглый куб	Веб-почта
6.1	35730 -CVE-2020		
9,8	12641 -CVE-2020		
9,8	44026 -CVE-2021		
6.1	41080 -CVE-2023	Апач	Кот
9,8	46604 -CVE-2023	Апач	ActiveMQ
9,8	27997 -CVE-2023	Фортинет	SSL-VPN
9,8	34048 -CVE-2023	VMware	vCenter
8,8	40044 -CVE-2023	Прогресс	WS_FTP
9,6	42657 -CVE-2023		
7,5	3823-CVE-2023	рофренд микрофон	Спектор НГлубокое открытие I
9,8	3824-CVE-2023		Апекс Один
7.2	41179 -CVE-2023		эсс безопасность НБизнес без беспокойства
5.4	29183 -CVE-2023	Фортинет	ФортиПрокси
8,8	34984 -CVE-2023		ФортиОС
			ФортиВеб
9,8	2868-CVE-2023	аБарракуда	ESG
9,8	32560 -CVE-2023	Иванти	ЙЭвеланш, Центр
9,8	38035 -CVE-2023		

источники

https://www.cisa.gov/known-exploited-vulnerabilities-catalog . 1

https://www.gov.il/he/departments/publications/reports/vulncatalog1401 . 2

[19]Активность программ-вымогателей в израильском киберпространстве 1662_https://www.gov.il/he/departments/publications/reports/alert

Обмен информацией с национальным CERT не заменяет обязательства сообщать об этом какому-либо руководящему органу, если такое обязательство применимо к этому органу.

Информация предоставляется «как есть» (как есть), ответственность за ее использование несет пользователь, и для ее реализации рекомендуется привлечь профессионала, имеющего соответствующую подготовку.

16