

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Практический опыт взаимодействия с ГосСОПКА

Роман Кобцев

Директор по развитию ЗАО «Перспективный мониторинг»

Компоненты работающего решения



- Нормативная база
- Технические аспекты подключения
 - Выполняемые функции
 - Ресурсы
 - Обмен сведениями
- Применение на практике



Центр мониторинга ЗАО «ПМ»

2014
год запуска

23
клиента

28 200
подключенных
узлов

30
операторов,
исследователей,
аналитиков и
инженеров

112 млн.
событий за 6
мес. 2018 г.

434
инцидента ИБ за
6 мес. 2018 г.

<60 мин.
реагирование на
инцидент ИБ

6 600
собственных
сигнатур атак для
IDS

С 2017 года Центр ГосСОПКА класса А



Нормативная база

Что читать



Нормативные правовые акты

- **Основные направления государственной политики** в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803)
- **Концепция** государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12 декабря 2014 г. N К 1274)

Нормативные правовые акты



- **Указ Президента Российской Федерации от 22.12.2017 г. № 620** О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (По сути сменил Указ Президента РФ от 15 января 2013 г. N 31с)
- **Федеральный закон от 26.07.2017 N 187-ФЗ** «О безопасности критической информационной инфраструктуры Российской Федерации»



Приказы ФСБ России

- **Приказ ФСБ России от 24 июля 2018 г. № 366** «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)»
- **Приказ ФСБ России от 24.07.2018 № 367** "Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации«
- **Приказ ФСБ России от 24 июля 2018 г. № 368** «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»



Приказы ФСБ России (Опубликованные проекты)

- **Проект приказа ФСБ России «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»**
- **Проект приказа ФСБ России «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»**
- **Проект приказа ФСБ России «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ»**



Методические документы ФСБ России

- Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные ресурсы Российской Федерации
- Методические рекомендации ФСБ России по установлению причин и ликвидации последствий компьютерных инцидентов связанных с функционированием информационных ресурсов Российской Федерации
- Методические рекомендации НКЦКИ по проведению мероприятий по оценке степени защищенности от компьютерных атак.
- ТРЕБОВАНИЯ к подразделениям и должностным лицам субъектов ГОССОПКА
- РЕГЛАМЕНТ взаимодействия подразделений ФСБ и субъекта ГОССОПКА при осуществлении информационного обмена в области обнаружения предупреждения и ликвидации последствий компьютерных атак



А это обязательно?

187-ФЗ

Статья 9. Права и
обязанности
субъектов КИИ

Субъект критической информационной инфраструктуры обязан незамедлительно информировать о компьютерных инцидентах соответствующие федеральные органы исполнительной власти (НКЦКИ, а также Финцерт ЦБ РФ для финансовых организаций), а также реагировать на компьютерные инциденты в установленном порядке.



Перечень сведений, предоставляемых в ГосСОПКА

Приказ ФСБ России № 367

от 24 июля 2018 г.

«Об утверждении Перечня
информации,

представляемой в ГосСОПКА

и Порядка представления

информации в ГосСОПКА»

- О категорировании объекта
- О нарушении требований по обеспечению безопасности значимых объектов КИИ (по итогам проведения государственного контроля)
- Информация о компьютерных инцидентах, связанных с функционированием объектов КИИ
- Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.



Приказ ФСБ России от 24 июля 2018 г. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»

Два способа предоставления информации в НКЦКИ:

- с использованием технической инфраструктуры НКЦКИ
- посредством электронной, факсимильной, почтовой и телефонной связи.



ГосСОПКА это не только КИИ

ОГВ

Могут быть
подключены к
ГосСОПКА



КИИ

Обязаны быть
подключены к
ГосСОПКА



ГосСОПКА — территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Зона ответственности – совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

Субъекты ГосСОПКА – государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели в силу закона или на основании заключенных с ФСБ России соглашений осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты.

Центр ГосСОПКА – структурная единица ГосСОПКА, представляющая совокупность подразделений и должностных лиц субъекта ГосСОПКА, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и реагирование на компьютерные инциденты в своей зоне ответственности.



Технические аспекты

Что делать

Что делать?



В случае самостоятельного подключения к ГосСОПКА

- ✓ Обеспечить взаимодействие с 8Ц ФСБ России
- ✓ Выполнить организационные и технические требования в соответствии с нормативными правовыми актами и методическими рекомендациями
- ✓ Развернуть специализированные системы взаимодействия с технической инфраструктурой НКЦКИ (для значимых КИИ обязательно, остальным опционально)

В случае подключения через сторонний корпоративный сегмент

- ✓ Заключение соглашения с корпоративным центром
- ✓ Уведомить НКЦКИ о включении своих информационных ресурсов в зону ответственности корпоративного центра.



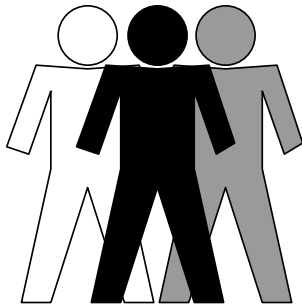
Какие функции выполняют центры ГосСОПКА

| Функции | Центры ГосСОПКа | | |
|--|-----------------|---------|---------|
| | Класс А | Класс Б | Класс В |
| Взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком; | + | + | + |
| Разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов и реагирования на компьютерные инциденты; | + | + | + |
| Эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, выявление ошибок в работе средств и направление производителю средств информации о выявленных ошибках, а также актуализация средств используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств; | + | + | + |
| Прием сообщений об инцидентах от персонала и пользователей информационных ресурсов; | + | + | + |
| Регистрация компьютерных атак и компьютерных инцидентов; | + | + | + |
| Анализ событий информационной безопасности; | + | + | + |
| Инвентаризация информационных ресурсов; | + | + | + |
| Анализ угроз информационной безопасности, прогнозирование их развития и направление в НКЦКИ результатов; | + | + | |
| Составление и актуализация перечня угроз информационной безопасности для информационных ресурсов; | + | + | |
| Выявление уязвимостей информационных ресурсов; | + | + | |
| Формирование предложений по повышению уровня защищенности информационных ресурсов; | + | + | |
| Составление перечня последствий компьютерных инцидентов; | + | + | |
| Ликвидация последствий компьютерных инцидентов; | + | | |
| Анализ результатов ликвидации последствий инцидентов; | + | | |
| Установление причин компьютерных инцидентов. | + | + | |



Необходимые ресурсы

Силы ГосСОПКА



Кадровое обеспечение

Средства ГосСОПКА





Силы ГосСОПКА



| Первая линия | Вторая линия | Третья линия |
|---|--|---|
| Взаимодействие с пользователями | Помощь в расследовании и установлении причин инцидентов | Подготовка и улучшение нормативной базы, описание сценариев выявленных инцидентов |
| Анализ событий и обнаружение компьютерных атак и инцидентов | Координация действий при реагировании на инциденты ИБ | Разработка сигнатурных правил и правил корреляции |
| Регистрация инцидентов ИБ и оповещение заинтересованных лиц | Анализ уязвимостей, анализ защищенности, тестирование на проникновение | Углубленный анализ Инцидентов ИБ, сбор доказательной базы |

Специалисты 1 линии



Специалист по взаимодействию с персоналом и пользователями

- Прием сообщений персонала и пользователей
- Подготовка информации для предоставления в НКЦКИ
- Взаимодействие с НКЦКИ

Специалист по обнаружению компьютерных атак и инцидентов

- Анализ событий информационной безопасности
- Регистрация компьютерных атак и инцидентов

Специалист по обслуживанию средств центра ГосСОПКА

- Обеспечение функционирования средств, размещаемых в центре ГосСОПКА, а также дополнительных средств защиты информационных систем

Специалисты 2 линии



Специалист по
оценке
защищенности

- Проведение инвентаризации информационных ресурсов
- Выявление уязвимостей
- Сбор и анализ выявленных уязвимостей и угроз
- Установление соответствия требований по информационной безопасности принимаемым мерам

Специалист по
ликвидации
последствий
компьютерных
инцидентов

- Координация действий при реагировании на компьютерные инциденты и приведение в штатный режим работы
- Взаимодействие с НКЦКИ

Специалист по
установлению
причин
компьютерных
инцидентов

- Установление причин компьютерных инцидентов
- Анализ последствий инцидентов и подготовка перечня компьютерных инцидентов
- Взаимодействие с НКЦКИ

Специалисты 3 линии



Аналитик-методист

- Анализ информации, предоставляемой специалистами 1-й и 2-й линий
- Выявление и анализ угроз информационной безопасности
- Прогнозирование развития угроз
- Разработка рекомендаций по доработке нормативных и методических документов

Технический эксперт

- Экспертная поддержка в соответствии со специализацией (ВПО, настройка средств защиты, применение специализированных технических средств, оценка защищенности и т.п.)
- Формирование предложений по повышению уровня защищенности

Специалист

- Нормативно-правовое и методическое сопровождение деятельности центра ГосСОПКА

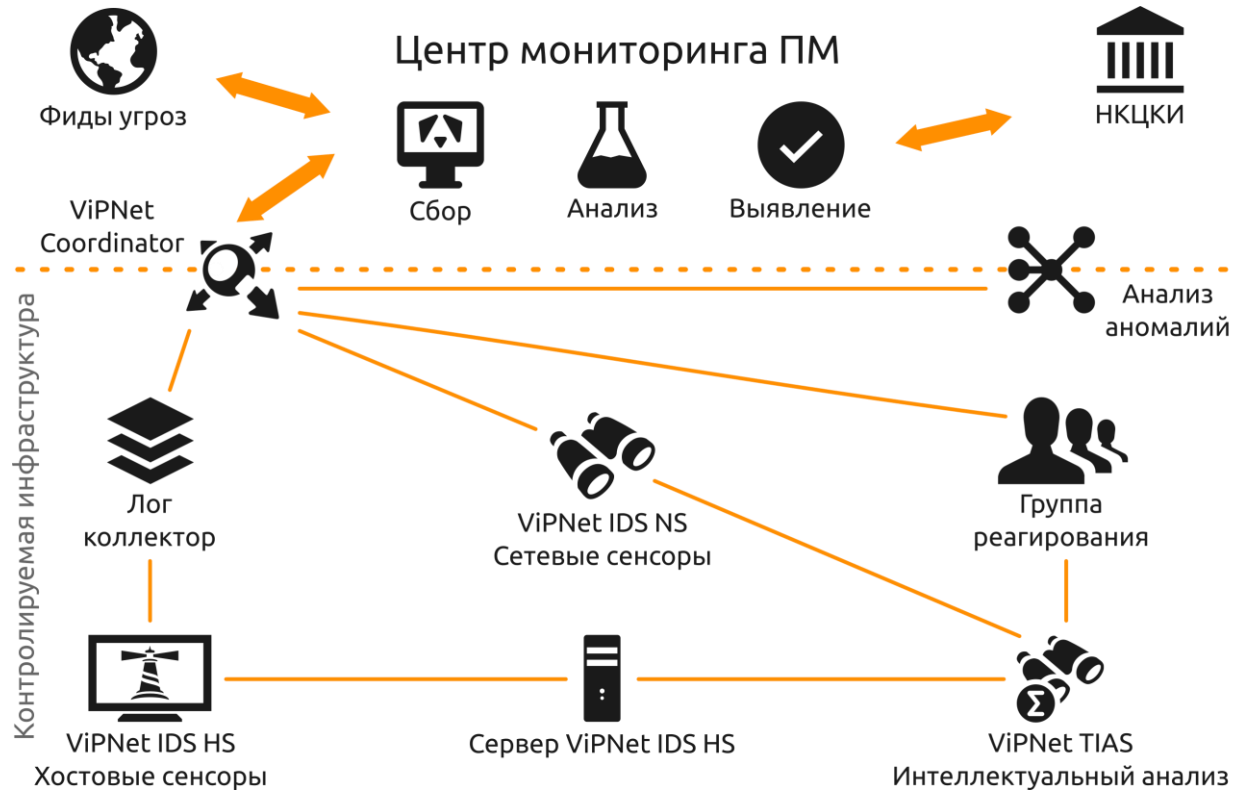
Руководитель

Управление деятельностью центра ГосСОПКА
Взаимодействие с НКЦКИ



Практическое применение

Как это работает



Инвентаризация



Система инвентаризации



Inventory System Search REPORTS JSON 🔍 📄 ⚙️

Advanced Monitoring resources list **MSK-W0038 Software List**

| Host Name | Timestamp | os_version | arch | Application Name | Version | CVE count | Approve |
|-----------|------------|-------------------------------------|--------------|------------------------------------|------------|-----------|---------|
| MSK-W0038 | 1515745587 | Майкрософт Windows 10 Корпоративная | 64-разрядная | | | 0 | ✗ |
| MSK-W0057 | 1517401048 | Майкрософт Windows 10 Корпоративная | 64-разрядная | 64 Bit HP ClO Components Installer | 13.2.1 | 0 | ✓ |
| MSK-W0326 | 1515745985 | Майкрософт Windows 10 Корпоративная | 64-разрядная | 7-Zip 17.01 beta (x64) | 17.01 beta | 0 | ✓ |
| MSK-W0603 | 1515745813 | Майкрософт Windows 10 Корпоративная | 64-разрядная | 7-Zip 9.20 (x64 edition) | 9.20.00.0 | 2 | ✓ |
| MSK-W1595 | 1515745810 | Майкрософт Windows 10 Корпоративная | 64-разрядная | Adobe Reader XI (11.0.23) MUI | 11.0.23 | 26 | ✓ |

Rows per page: 5 1-5 of 5 < >

Rows per page: 5 1-5 of 111 < >

<> Selected: Adobe Reader XI (11.0.23) MUI ⚠️ cpe:"cpe:/a:adobe:acrobat_reader" 🔔 cve:26

- 🚫 CVE-2013-3346 (cvss:10) ▾
- 🚫 CVE-2013-3342 (cvss:10) ▾
- 🚫 CVE-2013-3341 (cvss:10) ▾
- 🚫 CVE-2013-3340 (cvss:10) ▾
- 🚫 CVE-2013-3339 (cvss:10) ▾
- 🚫 CVE-2013-3338 (cvss:10) ▾
- 🚫 CVE-2013-3337 (cvss:10) ▾
- 🚫 CVE-2013-2736 (cvss:10) ▾



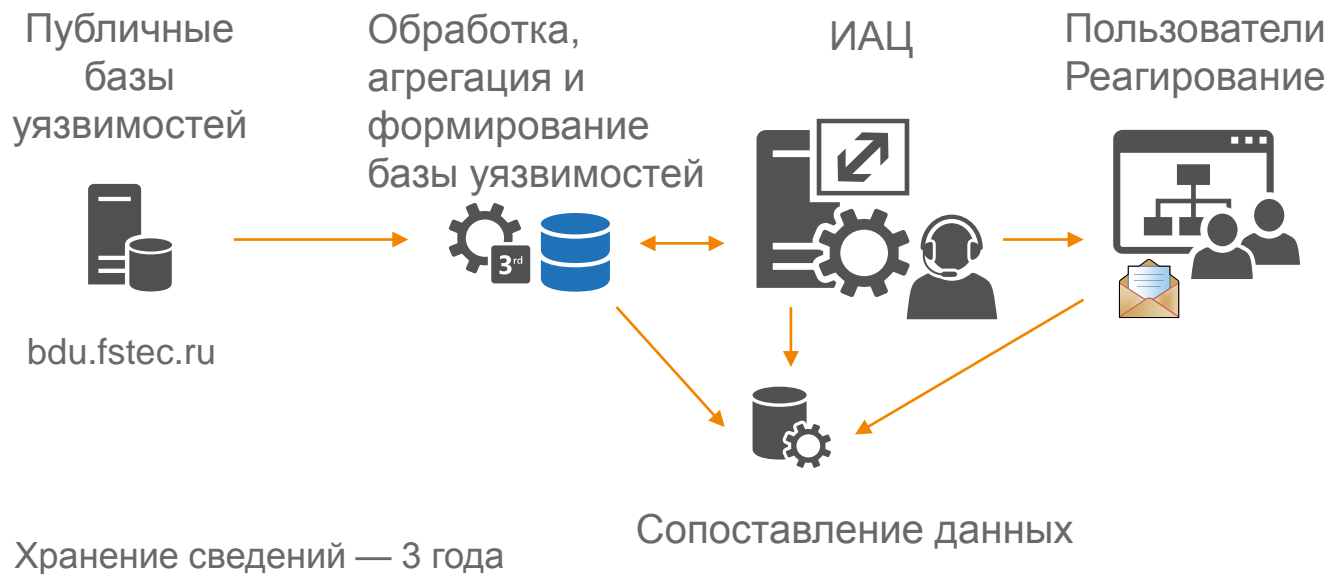
| Ввод в эксплуатацию | Ежемесячно | Ежеквартально | Ежегодно |
|----------------------------|---|--|--------------------------------|
| анализ документации | сетевое и системное сканирование | контроль устранения ранее выявленных уязвимостей | тестирование на проникновение |
| анализ исходного кода | контроль выполнения требований безопасности | | оценка соответствия мер защиты |



- Анализ в реальном времени
- Экспертная поддержка
- Интерфейс взаимодействия для обработки уязвимостей и принятия решений



Обработка уязвимостей





Vulnerability Prevention

Уязвимости | Продукты | Компоненты | Отчеты | Мой профиль | Выход (Demo)

Вы не получаете уведомления о новых или незакрытых уязвимостях по почте.
Вы можете настроить рассылку и список уязвимостей на главной странице.
Вы можете экспортировать уязвимости из списка ниже.

Список уязвимостей с CVSS выше или равным 0.5 (6)

Отобразить назначенные мне (4)

Поиск

Поиск по полям: #, CVE, Комментарий, Описание

| # | V2: AV | V2: Score | V3: AV | V3: Score | CVE | Статус | Продукт | Компоненты | Ответственный | Создана | Обновлена | Client Status Changed At |
|------|---------|-----------|---------|-----------|---------------|----------|-----------------------|----------------------------|---------------|------------------|------------------|--------------------------|
| 7512 | NETWORK | 10.0 | NETWORK | 9.8 | CVE-2015-8812 | новая | Linux Server 1 | linux_kernel - 3.10.1 | developer | 09/06/2017 14:39 | 07/08/2017 14:31 | 27/06/2017 12:54 |
| 7117 | LOCAL | 7.2 | LOCAL | 7.8 | CVE-2017-2636 | новая | Linux Server 1 | linux_kernel - 3.10.1 | | 09/06/2017 14:39 | 07/08/2017 13:45 | 28/06/2017 06:11 |
| 7063 | NETWORK | 9.3 | NETWORK | 8.1 | CVE-2017-0143 | новая | APM Windows msk-w0423 | windows_10 - 1511 | | 02/06/2017 17:37 | 07/08/2017 12:32 | 27/06/2017 12:55 |
| 6997 | NETWORK | 9.3 | NETWORK | 8.8 | CVE-2016-0184 | новая | APM Windows msk-w0423 | windows_10 - 1511 | | 02/06/2017 17:34 | 07/08/2017 15:18 | 27/06/2017 12:56 |
| 5544 | NETWORK | 10.0 | NETWORK | 9.8 | CVE-2016-0705 | в работе | Linux Server 1 | openssl - 1.0.1e-2+deb7u13 | | 29/02/2016 16:07 | 07/08/2017 12:45 | 27/06/2017 12:55 |
| 5535 | NETWORK | 10.0 | NETWORK | 9.8 | CVE-2016-4275 | новая | APM Windows msk-w0423 | flash_player - 10.0.0.584 | | 11/10/2016 14:53 | 07/08/2017 12:49 | 17/10/2016 15:32 |



Vulnerability Prevention

Уязвимости | Продукты | Компоненты | Отчеты | Мой профиль | Выход (Demo)

Уязвимость #7117

Комментарии (2)

| | | | |
|------------------|-----------------------|-----------|------------------|
| Статус | новая | создана | 09/06/2017 14:39 |
| Статус Аналитика | подтверждена | обновлена | 07/08/2017 13:45 |
| CVE | CVE-2017-2636 | | |
| Продукт | Linux Server 1 | | |
| Уязвимое ПО | linux_kernel - 3.10.1 | | |
| CPEs | 21 | | |
| Ответственный | нет (назначить) | | |

CVE-2017-2636

Комментарий

Состояние гонки существует в drivers/tty/n_hdlc.c ядра Linux при обращении к списку n_hdlc.tbuf. Данная уязвимость позволяет локальным, непривилегированным пользователям повысить уровень своих привилегий или вызвать отказ в обслуживании (двойное освобождение), используя настройку дисциплины линии HDLC.

Уровень опасности: Высокий
Воздействие: Повышение привилегий
Вектор атаки: Локальный

Описание

Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.

Ссылки

| | | |
|--------------|---|------------|
| MLIST | http://www.openwall.com/lists/oss-security/2017/03/07/6 | 03/07/2017 |
| VID | http://www.securityfocus.com/bid/96732 | 03/13/2017 |

Cvss v3

| | |
|---------------------------------------|-----------|
| SCORE | 7.8 |
| SCORE | UNCHANGED |
| Вектор доступа (AV) | LOCAL |
| Сложность доступа (AC) | LOW |
| Privileges Required (PR) | LOW |
| User Interaction (UI) | NONE |
| Воздействие на конфиденциальность (C) | HIGH |
| Воздействие на целостность (I) | HIGH |
| Воздействие на доступность (A) | HIGH |

Cvss v2

| | |
|------------------------|-------|
| SCORE | 7.2 |
| Вектор доступа (AV) | LOCAL |
| Сложность доступа (AC) | LOW |

Обнаружение КА и инцидентов



Собираем всё

Детектируем,
что знаем

Анализируем
новое

Много шума

Быстрое и точное
реагирование

Постоянное обновление
базы знаний

Управление и обработка инцидентов



Портал Информация Расследование

Инциденты Добавить

| ID | Название | Критичность | Система | Пораженные активы | Тип | Статус | Состояние | Время фикса |
|--------------------------|--|-------------|---------------------------------|-------------------|------------------|--------|----------------|------------------|
| 5b9275bc232fba000ec1085c | Множественные попытки доступа по RDP к узлу контр... | high | 971fe2b4-3fb6-4f9b-af82-d558... | | brute_forces | новый | предполагаемый | 07.09.2018 15:57 |
| 5b7d9010232fba000c20855e | sdfsdf | high | 971fe2b4-3fb6-4f9b-af82-d558... | | traffic_hijac... | новый | предполагаемый | 22.08.2018 19:32 |
| 5b7d8fc7232fba000c20855c | fdfdgdfg | | 971fe2b4-3fb6-4f9b-af82-d558... | | | новый | предполагаемый | 22.08.2018 19:31 |
| 5b7d8d8f232fba0017971b6f | ssdfsdf | high | 971fe2b4-3fb6-4f9b-af82-d558... | | traffic_hijac... | новый | предполагаемый | 22.08.2018 19:21 |
| 5b7ae68e232fba000eb009e8 | вапвап | high | 971fe2b4-3fb6-4f9b-af82-d558... | | traffic_hijac... | новый | предполагаемый | 20.08.2018 19:04 |
| 5b6c3c58232fba000c208551 | | | 971fe2b4-3fb6-4f9b-af82-d558... | | | новый | предполагаемый | 09.08.2018 16:06 |
| 5b6adb9232fba000b94edb9 | bbb | | 971fe2b4-3fb6-4f9b-af82-d558... | | | новый | предполагаемый | 08.08.2018 15:02 |
| 5b6ad9f1232fba000b94edb7 | sdfsdf | | 971fe2b4-3fb6-4f9b-af82-d558... | | | новый | предполагаемый | 08.08.2018 14:54 |
| 5b6ad8ac232fba000eb009e5 | aaa | | 971fe2b4-3fb6-4f9b-af82-d558... | | | новый | предполагаемый | 08.08.2018 14:49 |
| 5b6ad4ad232fba000b94edae | | | 971fe2b4-3fb6-4f9b-af82-d558... | 10.91.142.28 | | новый | предполагаемый | 08.08.2018 14:31 |

Выводить по 20 < < 1/1 > > Всего: 10

Карточка инцидента



Портал Информация Расследование

Инциденты / 5b9275bc232fba00ec1085c Синхронизировать с НКЦКИ Редактировать

⚠ Множественные попытки доступа по RDP к узлу контролируемой сети

| | | | | |
|----------------------------------|--|--|--|---|
| Критичность: high | Система: 971fe2b4-3fb6-4f9b-af82-d55837207f84 | Дата фиксации: 07.09.2018 15:57 | Дата создания: 07.09.2018 15:57 | Дата изменения: 07.09.2018 16:05 |
| Состояние: предполагаемый | Статус: новый | Пользователь: | Метаправила: | <input checked="" type="checkbox"/> Необходимо содействие НКЦКИ |
| Тип: brute_forces | Ограничительный маркер: | Количество событий: | | |

Описание инцидента:
Выявлены многочисленные попытки подбора пароля для доступа по RDP к узлу контролируемой сети

Рекомендации
2018-09-07T12:05:45.129000Z
1. Отключить пораженный актив от вычислительной сети
2. Провести интервьюирование владельца
3. Заблокировать на межсетевом экране IP-адрес атакующего
4. Провести аудит открытых портов и запущенных служб и закрыть неиспользуемые
5. Настроить ограничение количества неуспешных попыток доступа в систему
6. Ограничить доступ списком доверенных IP-адресов
Установить пароли надлежащей сложности для доступа к узлу

Действия
2018-09-07T12:07:37.214000Z
Сформирован белый список доступа
2018-09-07T12:08:08.421000Z
Заблокирован IP адрес атакующего на МСЭ

События История Комментарии Пораженные активы **Влияние** Файлы Контакты

brute_forces 1
brute_force-0

id: 122334

| | | | |
|-------------------|-------------|----------------------------------|----------------------------------|
| Цель | URL: | Тип сетевого сервиса: RDP | Источники |
| IP: 125.54.12.354 | | | ip 15.55.21.14 15.25.55.14 |





Спасибо за
внимание!

И подключайтесь к
ГосСОПКА

Роман Кобцев

Директор по развитию бизнеса
компании «Перспективный мониторинг»
Roman.Kobtsev@amonitoring.ru