Актуальные угрозы безопасности информации в современных условиях

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

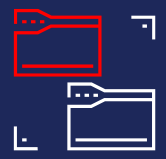
Атаки и угрозы в 2022 году

1. Массированные DDOS атаки, в т.ч. на инфраструктурные элементы рунета
2. Отключения провайдеров от крупных магистральных каналов
3. Атаки на СМИ для создания инфоповодов
4. Массовые отзывы сертификатов
5. Прекращение функционирования СЗИ зарубежных производителей
6. Появление вредоносного кода в обновлениях ПО

Основные изменения в 2023

1. Более высокий уровень координации атакующих
2. Смена направленности с создания инфоповодов на нанесение реального урона
3. Большее количество утечек, меньшее количество фейков
4. DDOS-атаки как маскировка выгрузки данных
5. Многочисленные атаки через цепочку поставщиков
6. Увеличение времени присутствия в атакованной инфраструктуре

Информационные атаки 2023



Утечки, собранные
из старых данных

Утечки с завышенной
ценностью (почти публичная
информация)

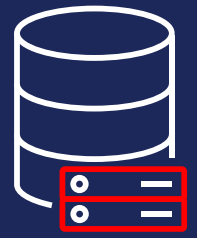
Утечки из других компаний,
выдаваемые за КИИ
или системообразующие
предприятия

Данные, собранные
из открытых источников

Наибольшая зона риска

Промышленность

Органы государственной власти и муниципального управления



ИТ-компании и разработчики ПО как цепочка поставки

ТОП-4 векторов проникновения

1. Подрядчики и системы, имеющие сопряжение с целевой инфраструктурой
2. Эксплуатация уязвимостей на периметре
3. Фишинг
4. «Обычное» ВПО, как точка входа для профессиональных кибергруппировок

Атаки через подрядчиков. Что нужно предпринять

1. Минимизировать каналы удаленного управления и вообще доступ сторонних специалистов из внешних систем
2. Контролировать действия внешних пользователей, особенно администраторов
3. Отслеживать информацию об инцидентах, например, утечках в подрядных организациях
4. Иметь план действий на случай появления признаков компрометации инфраструктуры подрядчика.
5. Выдвигать требования по обеспечению безопасности инфраструктур подрядчиков

Атаки на web – дефейсы, но не только

Хакеры взломали сайты российских правительственных учреждений

8 марта 2022, 21:25
1627

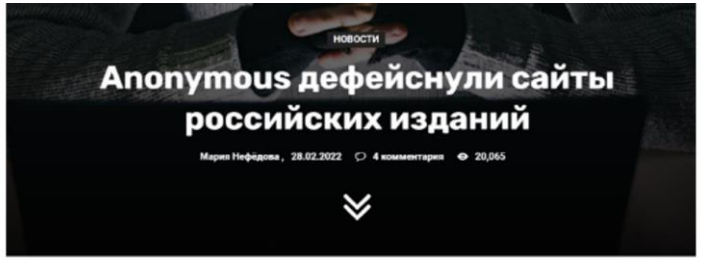
КИБЕРАТАКИ КИБЕРБЕЗОПАСНОСТЬ ХАКЕРЫ ФСИН МИНКУЛЬТУРЫ

Фото: ИЗВЕСТИЯ/Александр Казаков

Взломанная линия: власти усилили контроль за работой Рунета

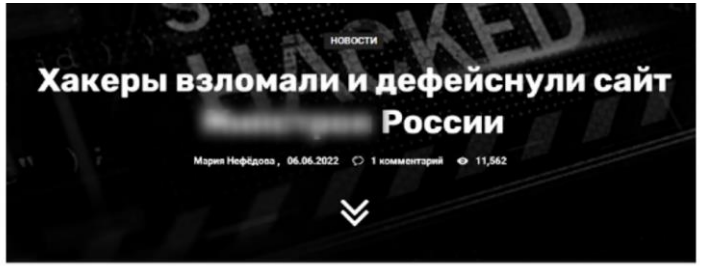
При открытии веб-страниц появляется коллаж изображений на тему спецоперации РФ по защите Донбасса.

Инцидент прокомментировали в Министерстве культуры. В ведомстве указали, что сайт подвергся DDoS-атакам, которые замедлили работу сервера. Начаты технические работы по восстановлению штатного функционирования ресурса.

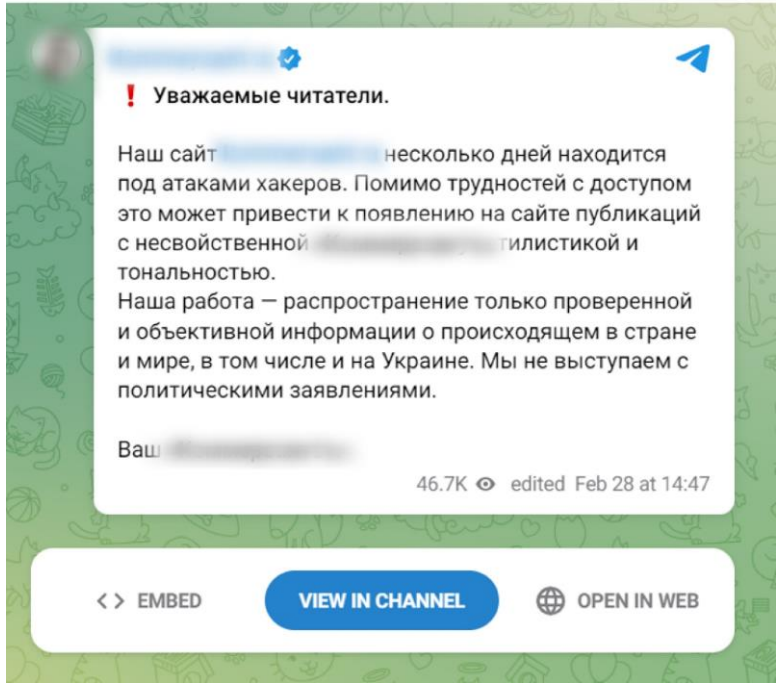


Хактивисты Anonymous продолжают войну, недавно объявленную против российских властей.

Отметим, что это неполный список. В частности, уже сообщалось, что сообщение хакеров



Хакеры дефейснули ресурс, поменяли заголовок сайта на лозунг с украинским приветствием и оставили послание на главной странице, заявив, что сайт взломан группой DumpForums[.]com. В записке злоумышленники потребовали заплатить выкуп в размере 0,5 биткоина до 7 июня 2022 года, в противном случае угрожая опубликовать данные сотрудников министерства в открытом доступе.



Спасибо за внимание!

incident@cert.gov.ru

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ