|  |  |
| --- | --- |
| Рег.номер уведомления | Предоставляет НКЦКИ |
| Дата и время регистрации уведомления | Предоставляет НКЦКИ |
| **Общие сведения** | |
| Категория | Уведомление о компьютерном инциденте |
| Тип события ИБ | Заражение ВПО |
| Статус реагирования | Меры приняты, инцидент исчерпан |
| Проводятся мероприятия по реагированию на инцидент |
| Возобновлены мероприятия по реагированию на инцидент |
| Необходимость привлечения сил ГосСОПКА | Да |
| Нет |
| Краткое описание события ИБ |  |
| Сведения о средстве или способе выявления |  |
| Дата и время выявления |  |
| Дата и время завершения |  |
| Ограничительный маркер TLP | TLP:WHITE |
| TLP:GREEN |
| TLP:AMBER |
| TLP:RED |
| Владелец информационного ресурса |  |
| Заявитель |  |
| Оценка последствий КИ | Влияние на конфиденциальность: Высокое |
| Влияние на конфиденциальность: Низкое |
| Влияние на конфиденциальность: Отсутствует |
| Влияние на целостность: Высокое |
| Влияние на целостность: Низкое |
| Влияние на целостность: Отсутствует |
| Влияние на доступность: Высокое |
| Влияние на доступность: Низкое |
| Влияние на доступность: Отсутствует |
| Краткое описание иной формы последствий компьютерного инцидента |  |
| **Информация о контролируемом ресурсе, на котором выявлен КИ** | |
| Наименование |  |
| Информация о категорировании ОКИИ | Информационный ресурс не является объектом КИИ |
| Объект КИИ без категории значимости |
| Объект КИИ третьей категории значимости |
| Объект КИИ второй категории значимости |
| Объект КИИ первой категории значимости |
| Сфера функционирования | Здравоохранение |
| Наука |
| Транспорт |
| Связь |
| Банковская сфера и иные сферы финансового рынка |
| Энергетика и Топливно-энергетический комплекс |
| Атомная энергия |
| Оборонная промышленность |
| Ракетно-космическая промышленность |
| Горнодобывающая промышленность |
| Металлургическая промышленность |
| Химическая промышленность |
| СМИ |
| Государственная/муниципальная власть |
| Образование |
| Наличие подключения к сети Интернет | Да |
| Нет |
| **Местоположение контролируемого ресурса** | |
| Страна/Регион |  |
| Населенный пункт или геокоординаты |  |
| **Технические сведения о контролируемом ресурсе** | |
| IPv4-адрес (маршрутизируемый) атакованного ресурса |  |
| IPv6-адрес (маршрутизируемый) атакованного ресурса |  |
| Доменное имя атакованного ресурса |  |
| URI-адрес атакованного ресурса |  |
| Email-адрес атакованного ресурса |  |
| Атакованная сетевая служба и порт/протокол |  |
| **Технические сведения о вредоносной системе** | |
| IPv4-адрес вредоносной системы [Центр управления ВПО] |  |
| IPv4-адрес вредоносной системы [Элемент инфраструктуры ВПО] |  |
| IPv4-адрес вредоносной системы [Источник распространения ВПО] |  |
| IPv4-адрес вредоносной системы [Тип неопределен] |  |
| IPv6-адрес вредоносной системы [Центр управления ВПО] |  |
| IPv6-адрес вредоносной системы [Элемент инфраструктуры ВПО] |  |
| IPv6-адрес вредоносной системы [Источник распространения ВПО] |  |
| IPv6-адрес вредоносной системы [Тип неопределен] |  |
| Доменное имя вредоносной системы [Центр управления ВПО] |  |
| Доменное имя вредоносной системы [Элемент инфраструктуры ВПО] |  |
| Доменное имя вредоносной системы [Источник распространения ВПО] |  |
| Доменное имя вредоносной системы [Тип неопределен] |  |
| URI-адрес вредоносной системы [Центр управления ВПО] |  |
| URI-адрес вредоносной системы [Элемент инфраструктуры ВПО] |  |
| URI-адрес вредоносной системы [Источник распространения ВПО] |  |
| URI-адрес вредоносной системы [Тип неопределен] |  |
| Email-адрес вредоносного объекта |  |
| Хеш-сумма вредоносного модуля (1) |  |
| Вердикт антивирусного средства (в случае сработки) (1) |  |
| Хеш-сумма вредоносного модуля (2) |  |
| Вердикт антивирусного средства (в случае сработки) (2) |  |
| Хеш-сумма вредоносного модуля (3) |  |
| Вердикт антивирусного средства (в случае сработки) (3) |  |
| Описание используемых уязвимостей |  |