ИНФОРМАЦИОННАЯ СПРАВКА

от 29 апреля 2022 г.

о результатах мониторинга сведений о критических уязвимостях программного обеспечения государственных информационных систем и объектов критической информационной инфраструктуры, а также связанных с ними компьютерных атаках

УЯЗВИМОСТИ

Опубликована информация об уязвимости операционных систем Windows.

Идентификатор и описание	Возможные меры защиты
BDU:2022-02731 Уязвимость операционных систем Windows связана с ошибками при настройке подписи LDAP в домене. Эксплуатация уязвимости может позволить нарушителю повысить свои привилегии. Для уязвимости существует средство эксплуатации, получившее название «KrbRelayUp»	Компенсирующие меры: - активация настройки объекта групповой политики «Контроллер домена: требования к подписи сервера LDAP»; - установка для атрибута MS-DS-Machine-Account-Quota в AD значения 0 с целью усложнения реализации атаки, лишая любого пользователя возможности добавлять новую учетную запись компьютера в домен; - установка флага «Учетная запись является конфиденциальной и не может быть делегирована» для всех учетных записей администраторов. Источник информации: https://github.com/Dec0ne/KrbRelayUp

Представленная информация об атаках и утечках информации получена по результатам мониторинга открытых источников в сети Интернет и может не соответствовать действительности!

АТАКИ

В Telegram-канале (t.me/itarmyofukraine2022) с начала дня 29 апреля 2022 года координируются DDoS-атаки на Интернет-ресурсы ПАО «Северсталь». Приводятся следующие цели для осуществления атак:

- https://severstal.com/rus;
- https://career.severstal.com;
- 217.175.24.112 (80/tcp, 443/tcp);
- https://news.severstal.com;
- https://distribution.severstal.com;
- 217.175.23.240 (80/tcp, 443/tcp);
- https://market.severstal.com/ru/ru;
- 78.41.110.139 (80/tcp, 443/tcp);
- https://suppliers.severstal.com/en-old/;
- 217.175.24.107 (80/tcp, 443/tcp);
- https://innovations.severstal.com;
- 217.175.24.109 (80/tcp, 443/tcp);
- https://bt.severstal.com;
- 217.175.24.27 (80/tcp, 443/tcp);
- https://staffing.severstal.com/auth;
- 217.175.24.86 (80/tcp, 443/tcp);
- https://lk.mph.severstal.com/login/;

- 178.154.246.131 (22/tcp, 80/tcp, 443/tcp, 9100/tcp);
- https://bstest.severstal.com/login.action;
- 217.175.24.94 (80/tcp, 443/tcp);
- https://chermk.severstal.com;
- 217.175.24.112 (80/tcp, 443/tcp);
- 217.175.24.79 (443/tcp);
- 217.175.23.242 (443/tcp);
- 217.175.23.8 (443/tcp);
- 217.175.24.189 (443/tcp);
- 217.175.24.192 (443/tcp);
- 217.175.24.93 (443/tcp);
- 217.175.24.74 (443/tcp);
- 217.175.24.39 (443/tcp);
- 217.175.24.21 (443/tcp);
- 217.175.24.200 (443/tcp);
- 84.38.185.177 (21/tcp, 22/tcp, 80/tcp, 443/tcp, 5432/tcp, 9100/tcp);
- 217.175.23.3 (53/udp);
- 217.175.23.4 (53/udp);
- 217.175.18.117 (53/udp);
- 13.80.145.65 (53/udp);
- 217.175.25.190 (53/udp).

УТЕЧКИ ДАННЫХ

В Telegram-канале (t.me/cybersecs), курируемом Владиславом Хорохориным, опубликована информация о взломе Казначейства России, Центрального банка Российской Федерации и группы компаний «Организационно-технологические решения», которая якобы разрабатывала программное обеспечение для указанных организаций.

Указывается, что взлом произошел в середине сентября 2021 года, при этом, хакерам удалось получить доступ к контроллерам доменов, репозиториям систем контроля версий, используемому программному обеспечению, а также рабочим документам, отчетностям, перепискам и базам данных Oracle. Однако информация о взломе не разглашалась до начала специальной операции на Украине.

Отмечается, что суммарный объем полученной нарушителями информации составляет более 20 Тб, однако к сообщению прикреплена ссылка на анонимный хостинг для скачивания порядка 3Гб данных, которые, как указано в публикации, содержат доказательства получения несанкционированного доступа: переписку администраторов, рабочие и личные документы разработчиков, рабочие документы о внутренней структуре сети, удостоверяющие сертификаты и другие данные.