Оригинальная статья

УДК 338.97:622.33 © О.А. Степанов, Р.О. Степанов, 2021

О возрастании угрозы хакерских атак на индустриальные объекты

DOI: http://dx.doi.org/10.18796/0041-5790-2021-11-25-26

Рассматривается проблема возрастающей угрозы хакеров, связанная с крупнейшей «утечкой» уникальных паролей в Интернет.

***Ключевые слова**: индустриальные объекты, хакеры, утечка паролей, защита.*

Для цитирования: Степанов О.А., Степанов Р.О. О возрастании угрозы хакерских атак на индустриальные объекты // Уголь. 2021. № 11. С. 25-26. DOI: 10.18796/0041-5790-2021-11-25-26.

СТЕПАНОВ О.А.
Доктор юрид. наук, профессор,
главный научный сотрудник Центра уголовного,
уголовно-процессуального законодательства
и судебной практики Института законодательства
и сравнительного правоведения
при Правительстве Российской Федерации,
117218, г. Москва, Россия,
e-mail: o_stepanov28@mail.ru

СТЕПАНОВ Р.О.
Канд. техн. наук,
директор Дирекции по Арктическим программам,
заместитель директора
НИИ «Радиоэлектроники и лазерной техники»
МГТУ им. Н.Э. Баумана,
105005, г. Москва, Россия,
e-mail: stepanovr@bmstu.ru

ВВЕДЕНИЕ

Генеральный директор «Лаборатории Касперского» Е. Касперский прогнозирует, что число кибератак на индустриальные объекты будет возрастать из-за того, что профессиональные хакерские группировки стоят на грани того, чтобы перейти в индустриальную киберпреступность. Поскольку количество хакеров и уровень сложности их атак возрастают, то «как только предприятие попадает в Интернет, его сразу необходимо защищать» [1].

ГЛАВНОЙ УГРОЗОЙ ДЛЯ ИНДУСТРИАЛЬНЫХ ОБЪЕКТОВ ЯВЛЯЕТСЯ ВИРУС-ВЫМОГАТЕЛЬ

Согласно исследованию «Лаборатории Касперского», хакерские группировки при применении вирусов-шифровальщиков получают до 40% выкупа [1].

По оценкам Сбербанка, потери российской экономики от действий киберпреступников в 2020 г. могли составлять порядка 3,5 трлн руб. Только объем рынка продаж с краденых банковских карт приблизился к 145 млрд руб. При этом большая часть кибератак исходила с территории России [2].

Так, в октябре 2020 г. неизвестные хакеры атаковали компании, занимающиеся разработкой вакцины от коронавируса в Японии. Преступники пытались украсть конфиденциальную информацию о разработках лекарства с апреля 2020 г. [3].

5 мая 2021 г. хакерской атаке подвергся крупнейший на Восточном побережье США газопровод Colonial Pipeline. Ежедневно по трубопроводу транспортируется около 45% топлива, потребляемого на Восточном побережье. Оператор был вынужден заплатить хакерам выкуп в размере 4,4 млн дол. США [4].

1 июня 2021 г. стало известно, что крупнейший в мире производитель мяса, бразильская компания JBS SA, пострадала от хакерских атак на свои филиалы в Австралии и странах Северной Америки. Эта кибератака привела к приостановке работы пяти крупных мясоперерабатывающих заводов компании в США, которые не безосновательно заподозрили в кибератаке на JBS «российских хакеров» [5].

Поскольку такими «атаками занимаются криминальные группировки», то Россия, как и любая страна, обязана сделать все необходимое, чтобы остановить и привлечь к ответственности преступную организацию, которая предпринимает с ее территории действия не только «в отношении кого-либо еще» — считает госсекретарь США Э. Блинкен [6].

При этом важно обратить внимание на то, что в последних двух случаях со стороны хакеров не было попыток украсть чужие технологии либо оказать влияние на общественное мнение – с помощью вирусов-вымогателей ими решались чисто экономические задачи.

Угрозы подобного рода следует принимать во внимание при проработке вопросов информационной защиты объектов угольной промышленности на территории России, и особенно в арктической зоне, где условия работы наиболее сложные.

ЗАКЛЮЧЕНИЕ

Ранее автором уже обращалось внимание на актуальность такой проработки [7, 8, 9]. Однако в настоящее время важно учитывать то обстоятельство, что хакеры способны активизировать атаки на индустриальные объекты из-за получения в свое распоряжение необходимых паролей к информационным системам.

Так, 10 июня 2021 г. в сети была обнародована крупнейшая в истории подборка паролей, которые ранее «утекали» в Интернет после взломов данных (в текстовом файле, опубликованном на одном из хакерских форумов, содержалось около 8,4 млрд уникальных паролей, имеющих длину от шести до 20 символов).

В связи с этим при организации соответствующих защитных мероприятий на объектах угольной промышленности важно учитывать то, что хакеры могут использовать данную утечку для создания словаря паролей в целях осуществления атак методом их распыления на огромное количество онлайн-аккаунтов [10].

Список литературы

1. «Лаборатория Касперского» ожидает роста активности атак хакеров на индустриальные объекты // Финансовая газета. 01 июня 2021. [Электронный ресурс]. URL: https://news.rambler.ru/internet/46537009/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (дата обращения: 15.10.2021).

2. Темная сторона даркнета // Коммерсантъ. 19.03.2021. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/4732215 (дата обращения: 15.10.2021).

3. Японии предрекли судьбу Украины из-за России // LENTA.RU. 10 июня 2021. [Электронный ресурс]. URL: https://lenta.ru/news/2021/06/10/sudba/ (дата обращения: 15.10.2021).

4. Демидов А. Глава Colonial Pipeline рассказал, сколько компания заплатила хакерам // Газета.ru. 19 мая 2021. [Электронный ресурс]. URL: https://www.gazeta.ru/tech/news/2021/05/19/n_15997772.shtml (дата обращения: 15.10.2021).

5. Титаренко Д. Крупнейший в мире производитель мяса подвергся хакерской атаке // Газета.ru. 01 июня 2021. [Электронный ресурс]. URL: https://www.gazeta.ru/business/news/2021/06/01/n_16046480.shtml (дата обращения: 15.10.2021).

6. Лежапекова А. Блинкен призвал Россию прекратить кибератаки // Газета.ru. 04 июня 2021. [Электронный ресурс]. URL: https://www.gazeta.ru/politics/news/2021/06/04/n_16059098.shtml (дата обращения: 15.10.2021).

7. Степанов О.А. О правовом регулировании отношений в сфере безопасного функционирования и развития систем искусственного интеллекта // Уголь. 2020. № 6. С. 21-22. DOI: 10.18796/0041-5790-2020-6-21-22.

8. Степанов О.А., Печегин Д.А. Право как средство обеспечения безопасности объектов угольной промышленности в условиях цифровизации // Уголь. 2019. № 9. С. 54-55. DOI: 10.18796/0041-5790-2019-9-54-55.

9. Степанов О.А., Степанов А.О. О противодействии киберпреступной деятельности // Уголь. 2021. № 3. С. 14-15. DOI: 10.18796/0041-5790-2021-3-14-15.

10. Крупнейшая в истории подборка паролей утекла в сеть // LENTA.RU. 10 июня 2021. [Электронный ресурс]. URL: https://lenta.ru/news/2021/06/10/paroli/ (дата обращения: 15.10.2021).

Original Paper

UDC 338.97:622.33 © O.A. Stepanov, R.O. Stepanov, 2021
ISSN 0041-5790 (Print) • ISSN 2412-8333 (Online) • Ugol' – Russian Coal Journal, 2021, № 11, pp. 25-26
DOI: http://dx.doi.org/10.18796/0041-5790-2021-11-25-26

Title
ON INCREASING THREAT OF HACKER ATTACKS ON INDUSTRIAL FACILITIES

Author
Stepanov O.A.[1], Stepanov R.O.[2]

[1] Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, 117218, Russian Federation
[2] Research Institute of Radioelectronics and Laser Technology of Bauman University, Moscow, 105005, Russian Federation

Authors Information
Stepanov O.A., Doctor of Law Sciences, Professor, Chief Researcher of the Center for Criminal Law, Criminal Procedure Legislation, Judicial Practice, e-mail: o_stepanov28@mail.ru
Stepanov R.O., PhD (Engineering), Director of the Directorate for Arctic Programs, Deputy Director, e-mail: stepanovr@bmstu.ru

Abstract
The paper addresses the growing threat of hacker attacks related to the largest leakage of unique passwords in the Internet.

Keywords
Industrial facilities, Hackers, Password leakage, Protection.

References
1. Kaspersky Lab expects an rise in hacking activity at industrial facilities. *Fingazeta.ru,* June 1, 2021. [Electronic resource]. Available at: https://news.rambler.ru/internet/46537009/?utm_content=news_media&utm_medium=read_more&utm_source=copylink (accessed 15.10.2021). (In Russ.2. The dark side of the DarkNet. *Kommersant.ru,* March 19, 2021. [Electronic resource]. Available at: https://www.kommersant.ru/doc/4732215 (accessed 15.10.2021). (In Russ.).
3. Japan was foretold the fate of Ukraine because of Russia. *LENTA.RU*, June 10, 2021. [Electronic resource]. Available at: https://lenta.ru/news/2021/06/10/sudba/ (accessed 15.10.2021). (In Russ.).
4. Demidov A. CEO of Colonial Pipeline revealed how much the company paid to hackers. *Gazeta.ru*, May 19, 2021. [Electronic resource]. Available at: https://www.gazeta.ru/tech/news/2021/05/19/n_15997772.shtml (accessed 15.10.2021). (In Russ.).
5. Titarenko D. The world's largest meat producer suffered a hacker attack. *Gazeta.ru*, June 1, 2021. [Electronic resource]. Available at: https://www.gazeta.ru/business/news/2021/06/01/n_16046480.shtml (accessed 15.10.2021). (In Russ.).
6. Lezhapekova A. Blinken urges Russia to stop cyber attacks. *Gazeta.ru*, June 4, 2021. [Electronic resource]. Available at: https://www.gazeta.ru/politics/news/2021/06/04/n_16059098.shtml (accessed 15.10.2021). (In Russ.).
7. Stepanov O.A. On the legal regulation of relations in the field of safe functioning and development of artificial intelligence systems. *Ugol',* 2020, (6), pp. 21-22. (In Russ.). DOI: 10.18796/0041-5790-2020-6-21-22.
8. Stepanov O.A. & Pechegin D.A. Law as a means of ensuring the safety of coal industry facilities in the context of digitalization. *Ugol',* 2019, (9), pp. 54-55. (In Russ.). DOI: 10.18796/0041-5790-2019-9-54-55.
9. Stepanov O.A. & Stepanov A.O. On counteracting cybercrimes. *Ugol',* 2021, (3), pp. 14-15. (In Russ.). DOI: 10.18796/0041-5790-2021-3-14-15
10. The largest collection of passwords ever leaked to the Internet. *LENTA.RU*, June 10, 2021. [Electronic resource]. Available at: https://lenta.ru/news/2021/06/10/paroli/ (accessed 15.10.2021). (In Russ.).

For citation
Stepanov O.A. & Stepanov R.O. On increasing threat of hacker attacks on industrial facilities. *Ugol',* 2021, (11), pp. 25-26. (In Russ.). DOI: 10.18796/0041-5790-2021-11-25-26.

Paper info
Received June 15, 2021
Reviewed September 18, 2021
Accepted October 15, 2021