

УДК 004.89
ББК 32.973.4:16.8
С46

Переводчик Анна Власюк
Научный редактор Александр Алексеев
Редактор Камилл Ахметов

Скулкин О.

С46 Шифровальщики : Как реагировать на атаки с использованием программ-вымогателей / Олег Скулкин. — М. : Альпина ПРО, 2023. — 205 с.

ISBN 978-5-206-00080-1

Шифровальщики — это программы, которые находят уязвимости в сетях предприятия, чтобы потом с помощью этих уязвимостей внедриться в сети, завладеть ценной для предприятия информацией и далее вымогать деньги из руководства компании. Разумеется, программы эти создаются людьми, которые могут как объединяться в преступные группы, так и действовать поодиночке.

В последние годы растет число кибератак именно с помощью программ-шифровальщиков. К сожалению, этот тренд не обошел и Россию: количество таких атак только за 2021 г. выросло более чем в три раза.

Именно поэтому так кстати в русском переводе выходит книга Олега Скулкина, выдающегося эксперта не только в российской, но и в международной цифровой криминалистике. Автор рассказывает обо всем, что касается шифровальщиков, — от истории атак до цифровых улики. Внутри его повествования вполне естественно выглядят фрагменты программного кода, а кое-где — цветные скриншоты.

По мнению автора (а оно основано на более чем десятилетнем опыте работы в сфере информационной безопасности), сети и деньги предприятия можно уберечь, если понимать жизненный цикл атак программ-вымогателей. Об этом цикле подробно рассказывается во второй главе книги, а также в последней главе, где автор помогает читателям научиться реконструировать универсальный жизненный цикл атаки, которому подчиняются все шифровальщики, какими бы индивидуальными особенностями они ни обладали.

УДК 004.89
ББК 32.973.4:16.8

Все права защищены. Никакая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами, включая размещение в сети Интернет и в корпоративных сетях, а также запись в память ЭВМ для частного или публичного использования, без письменного разрешения владельца авторских прав. По вопросу организации доступа к электронной библиотеке издательства обращайтесь по адресу: mylib@alpina.ru

ISBN 978-5-206-00080-1 (рус.)
ISBN 978-1-80324-044-2 (англ.)

Copyright © 2022 Packt Publishing
© Перевод, оформление. ООО «Альпина ПРО», 2022

СОДЕРЖАНИЕ

Предисловие	9
Введение	11

01

Знакомство с современными атаками с использованием программ-вымогателей	16
--	-----------

Глава 1. История современных атак с использованием программ-вымогателей _____	18
Глава 2. Жизненный цикл современной атаки с использованием программы-вымогателя _____	28
Глава 3. Процесс реагирования на инциденты _____	42

02

Врага нужно знать в лицо: как действуют банды операторов программ-вымогателей	54
--	-----------

Глава 4. Киберразведка и программы-вымогатели _____	56
Глава 5. Тактики, техники и процедуры групп, занимающихся распространением программ-вымогателей _____	66
Глава 6. Сбор данных о киберугрозах, связанных с программами-вымогателями _____	92

03

Практика реагирования на инциденты	106
---	------------

Глава 7. Цифровые криминалистические артефакты и их основные источники _____	108
Глава 8. Методы первоначального доступа _____	128
Глава 9. Методы постэксплуатации _____	144
Глава 10. Методы кражи данных _____	162
Глава 11. Методы развертывания программ-вымогателей _____	176
Глава 12. Унифицированный жизненный цикл атак с использованием программ-вымогателей _____	192