КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ | 02 ДЕКАБРЯ 2021

КАК ЭВОЛЮЦИОНИРОВАЛИ ВИРУСЫ-ШИФРОВАЛЬЩИКИ?

ЛУКА САФОНОВ, КИБЕРПОЛИГОН

МОСКВА

Как эволюционировали вирусы-шифровальщики?

Типы ransomware

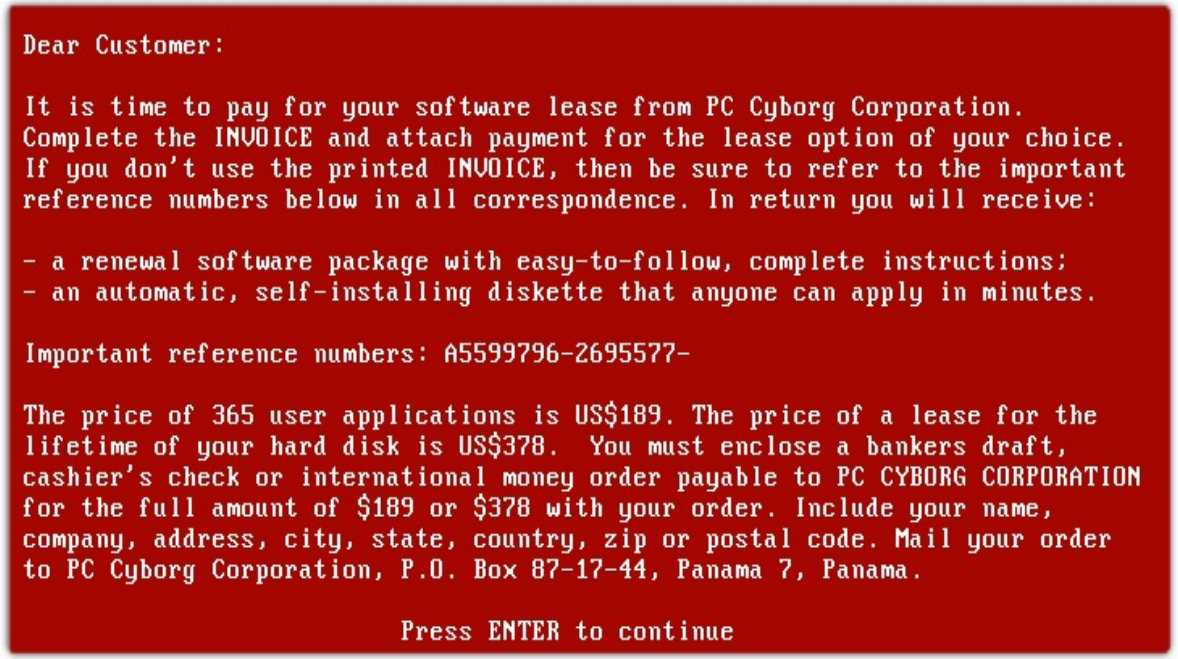
Ransomware, или трояны-вымогатели, — это разновидность зловредных программ, которая за последнее время из просто распространенной стала очень-очень распространенной.

Их можно разделить на два основных типа — шифровальщики (крипторы, локеры, cryptoransomware) и блокировщики (blockers, блокеры).

Шифровальщики, попадая на ваш компьютер, шифруют ценные файлы: документы, фотографии, сохранения к играм, базы данных и так далее — таким образом, что их нельзя открыть.

Троян AIDS

В декабре 1989 года Попп разослал по почте 20 тысяч гибких дисков с подписью «Информация о СПИДе — ознакомительная дискета» сотням медицинских исследовательских институтов в 90 странах. На каждом диске был интерактивный опрос, измерявший риск заражения СПИДом на основании ответов пользователя. Во время прохождения опроса первое ransomware — «AIDS Trojan» шифровало файлы на компьютерах пользователей после перезапуска определённого количества раз.



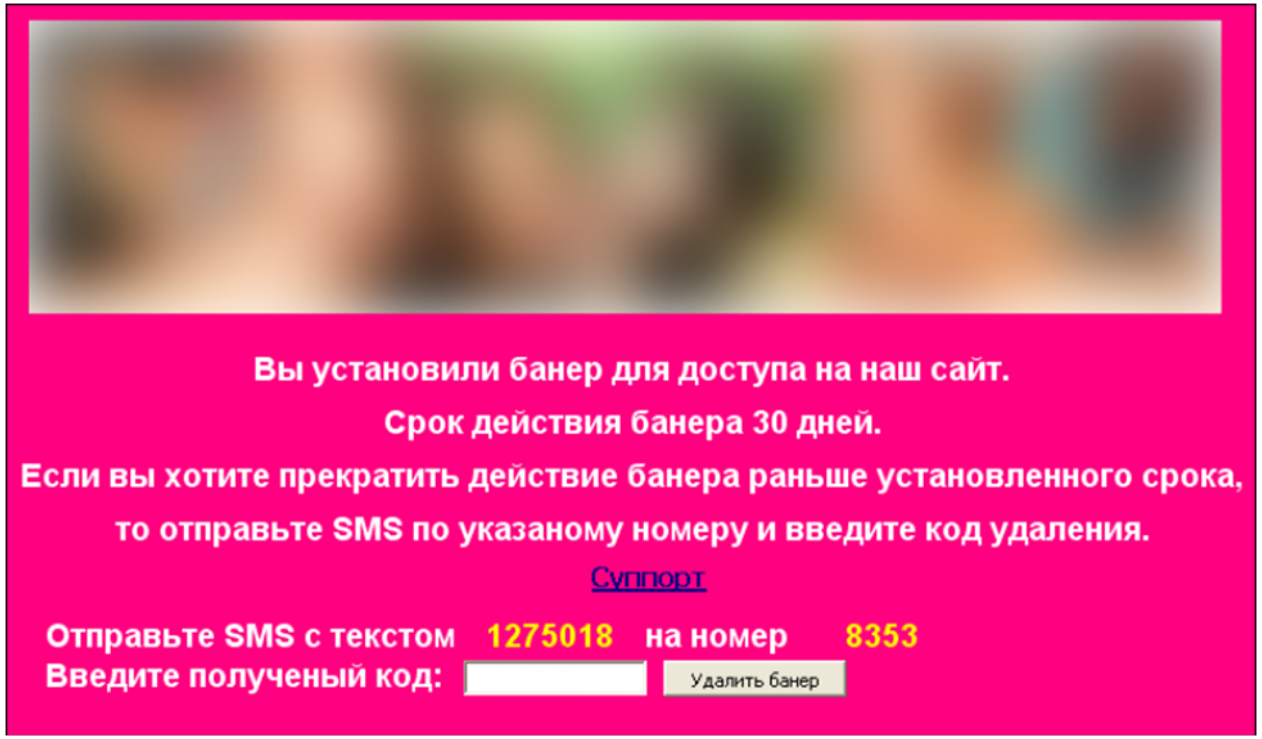
Год 1989

Выкуп $189

Троян PinkBlocker

В июне 2010 года новые блокеры данного семейства выходили буквально раз в час.

Эпидемия прекратилась лишь после того, как правоохранительными органами были задержаны члены данной преступной группировки.



Год 2009

Выкуп 300-15000 рублей

Rise of ransomware

2008-2011 развитие Bitcoin приводит к увеличению количества ransomware-атак: за первые два квартала 2011 года было сообщено о 30 тысячах заражений. К концу третьего квартала это количество удвоилось.

					RANSOMWARE GOES BIG				
	1989 AIDS Trojan	2005 - 2006 GPCode Archiveus	2008 Bitcoin	2012 Reveton	2013-2015 CryptoLocker	2016 Ransom32 Locky	2017 Wanna Cry Petya	2018 New Variants	2019 MegaCortex
Threat	Local Symmetric Encryption	Assymetric Encryption	Invention of Bitcoin	Threats of Criminal Prosecution	Online Assymetric Encryption			Detection avoidance Backups deleted Forensic evidence destroyed	
Delivery	Physically Mailed Floppy Disks	Trojans		Trojans	Online Trojan Email attachments	Online Trojans Email Phishing	Exploit-based propagation	Exploit-based propagation Phishing	Exploit-based propagation
Payment	Payoff to Banks	Website Purchases		Prepaid cash services	Bitcoin	Bitcoin	Bitcoin	Cryptocurrency	Cryptocurrency

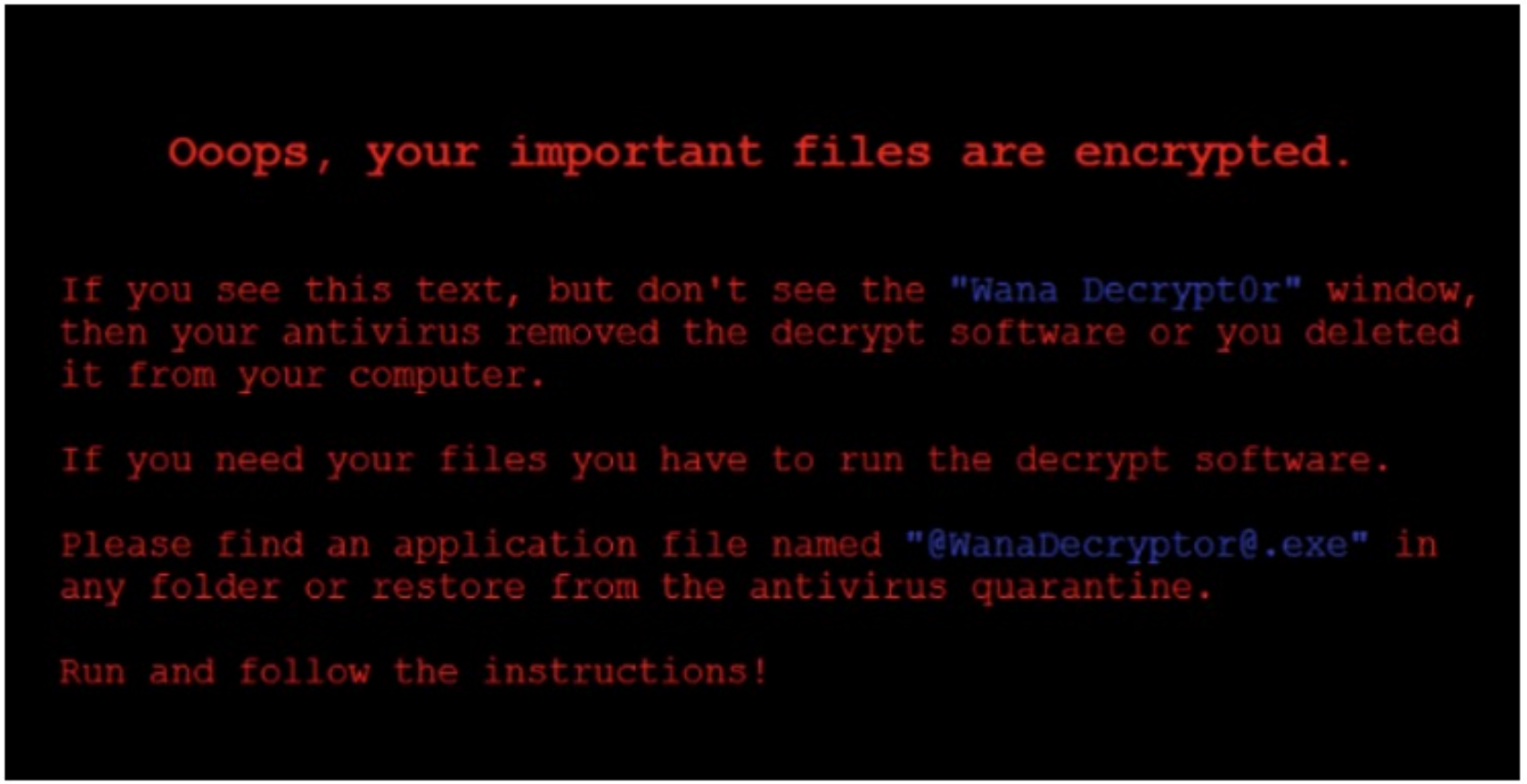
WannaCry

https://habr.com/ru/post/328606/

LukaSafonov 14 мая 2017 в 20:50

Анализ шифровальщика Wana Decrypt0r 2.0

Информационная безопасность *



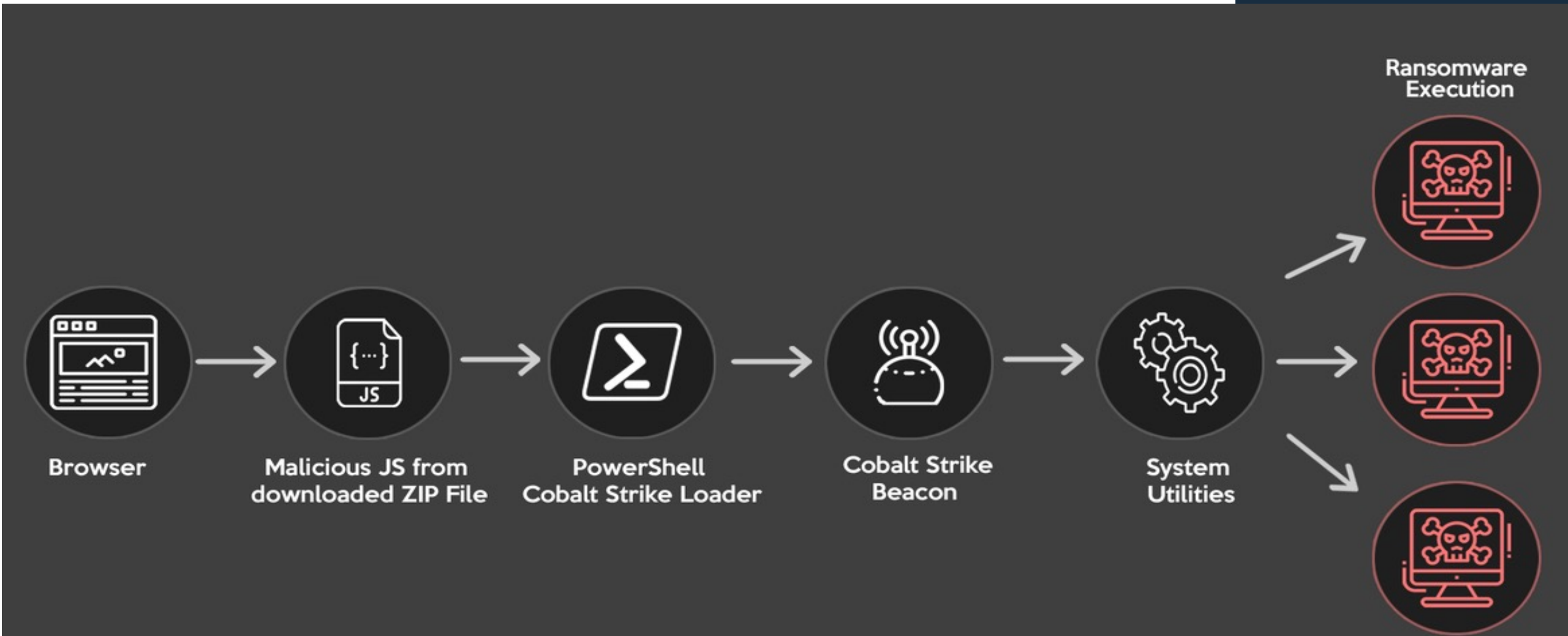
WannaCry

На поведенческом уровне оба объекта схожи и шифруют файлы пользователя. Первый объект имеет функции сетевого червя и пытается распространяться в сети через уязвимость в SMBv1, для чего он перебирает множество IP-адресов случайным образом и пытается соединиться на порт 445 (SMB).

Таким образом, вирус обладает способностью к самораспространению не только по локальной сети, но и возможность атаковать другие компьютеры в мировом масштабе.

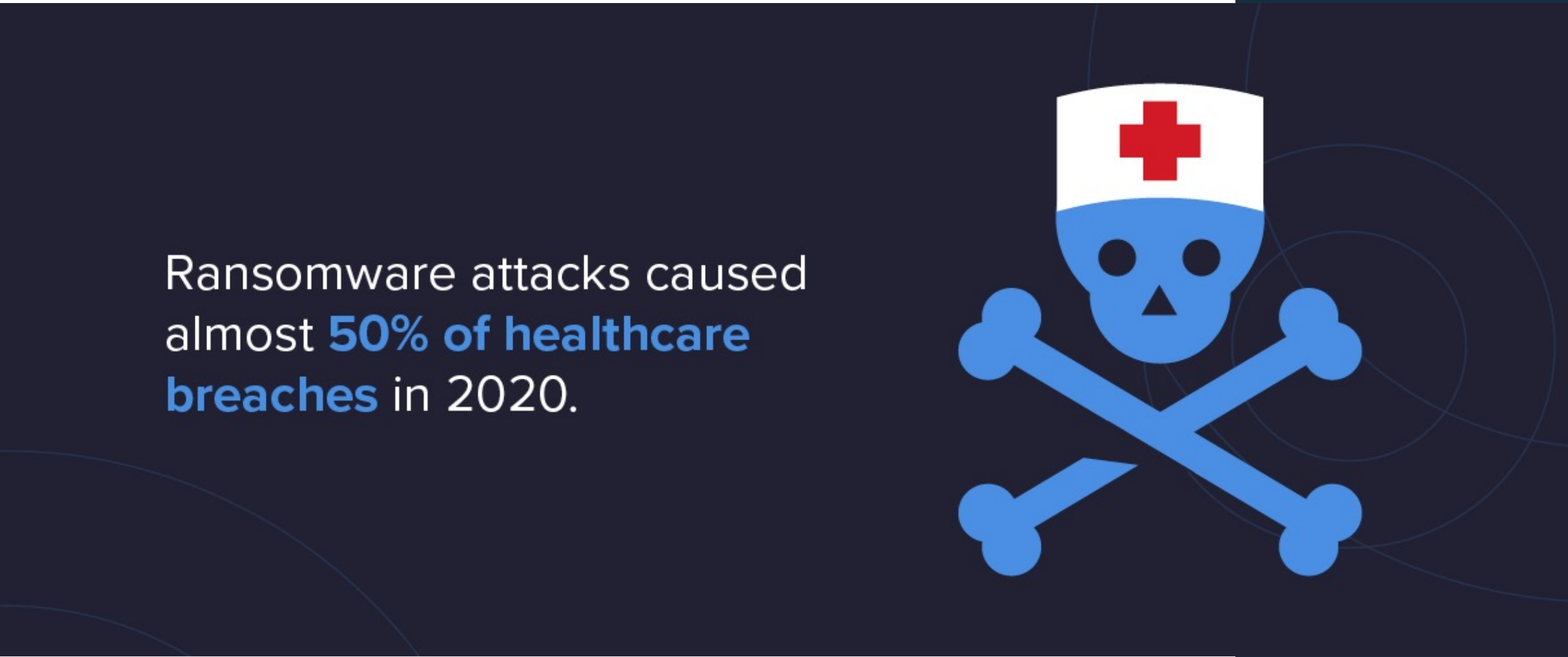
2019 смена тактики

Кибер-преступники начали делать основной упор на критически важную инфраструктуру и крупные организации.



2020 https://www.hhs.gov/sites/default/files/2021-hph-cybersecurity-forecast.pdf

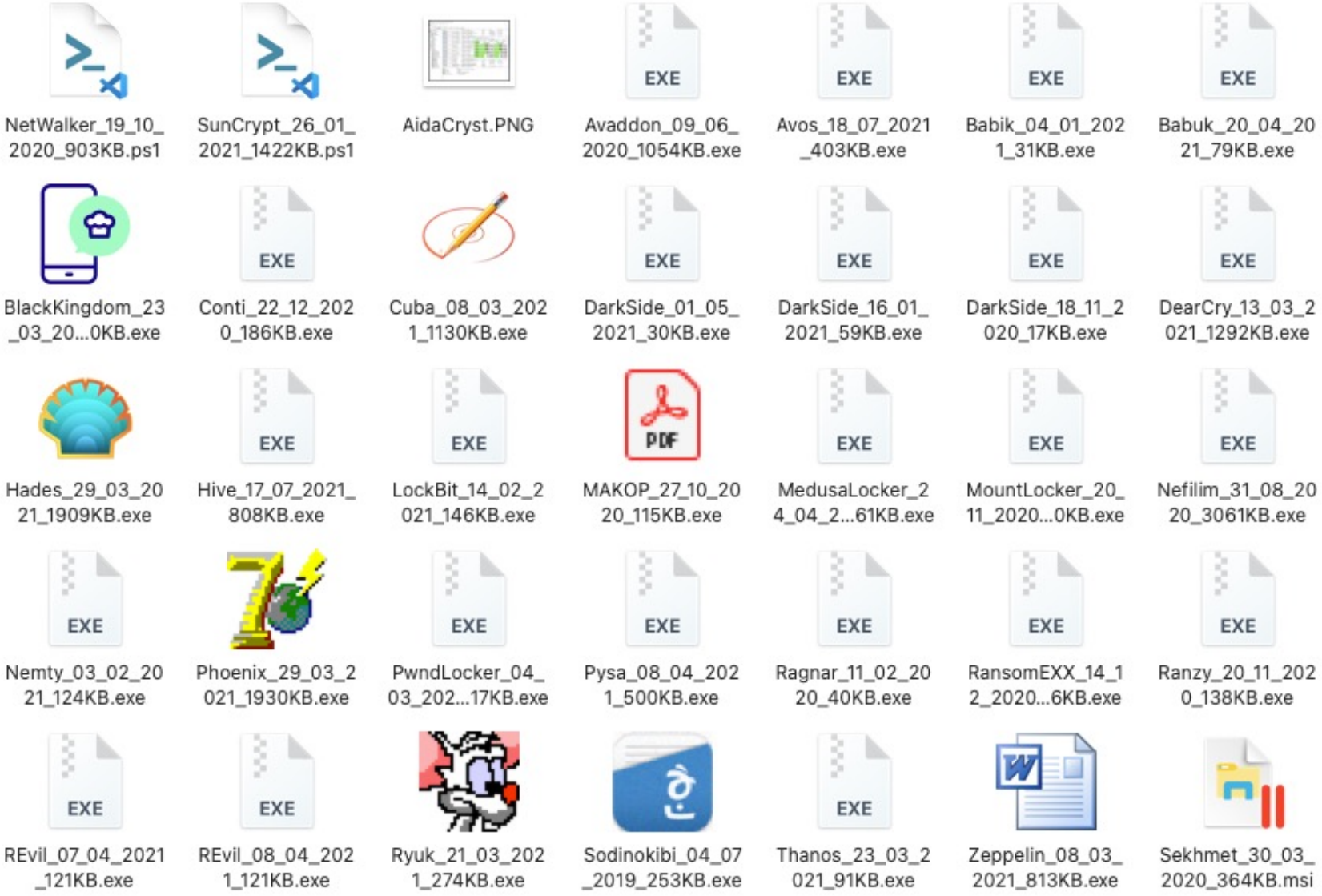
Атаки программ-вымогателей стали причиной почти 50% всех утечек данных в сфере здравоохранения в 2020 г.



2021 диверсификация бизнеса

Еще один способ монетизации — продажа данных. Например, Sodinokibi недавно объявили о проведении открытых аукционов, на которых данные достаются участнику, сделавшему самую высокую ставку. Стартовая цена таких торгов составляет $50-100K в зависимости от качества и содержания данных.

Кто стоит за вымогателями?



Модель RaaS

REvil affiliate program
Unknown · 06/05/2020 2

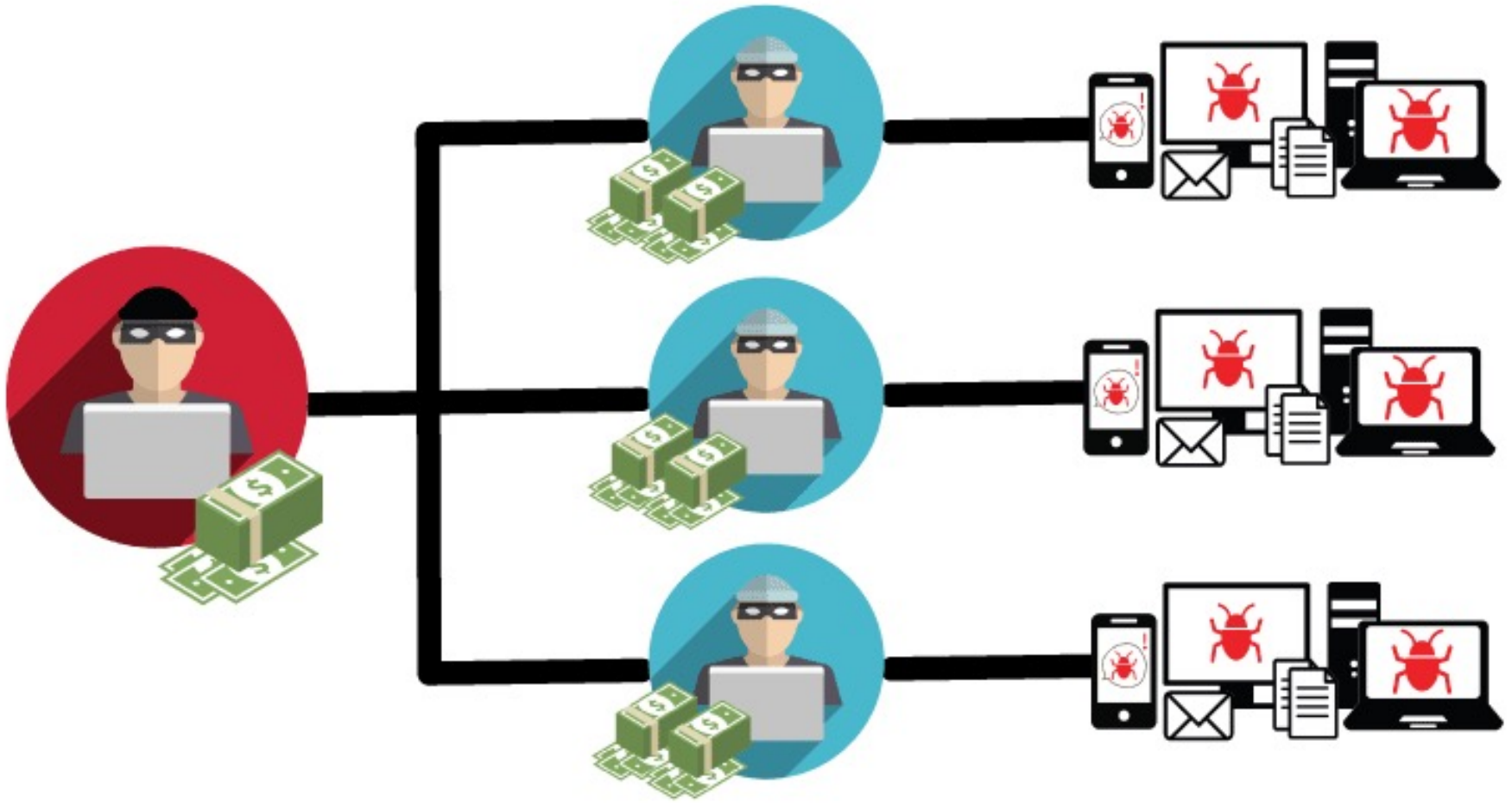
[Affiliate Program] Darkside Ransomware
darksupp · Tuesday at 20:27

[PARTNER] NetWalker Ransomware
Bugatti · 03/20/2020

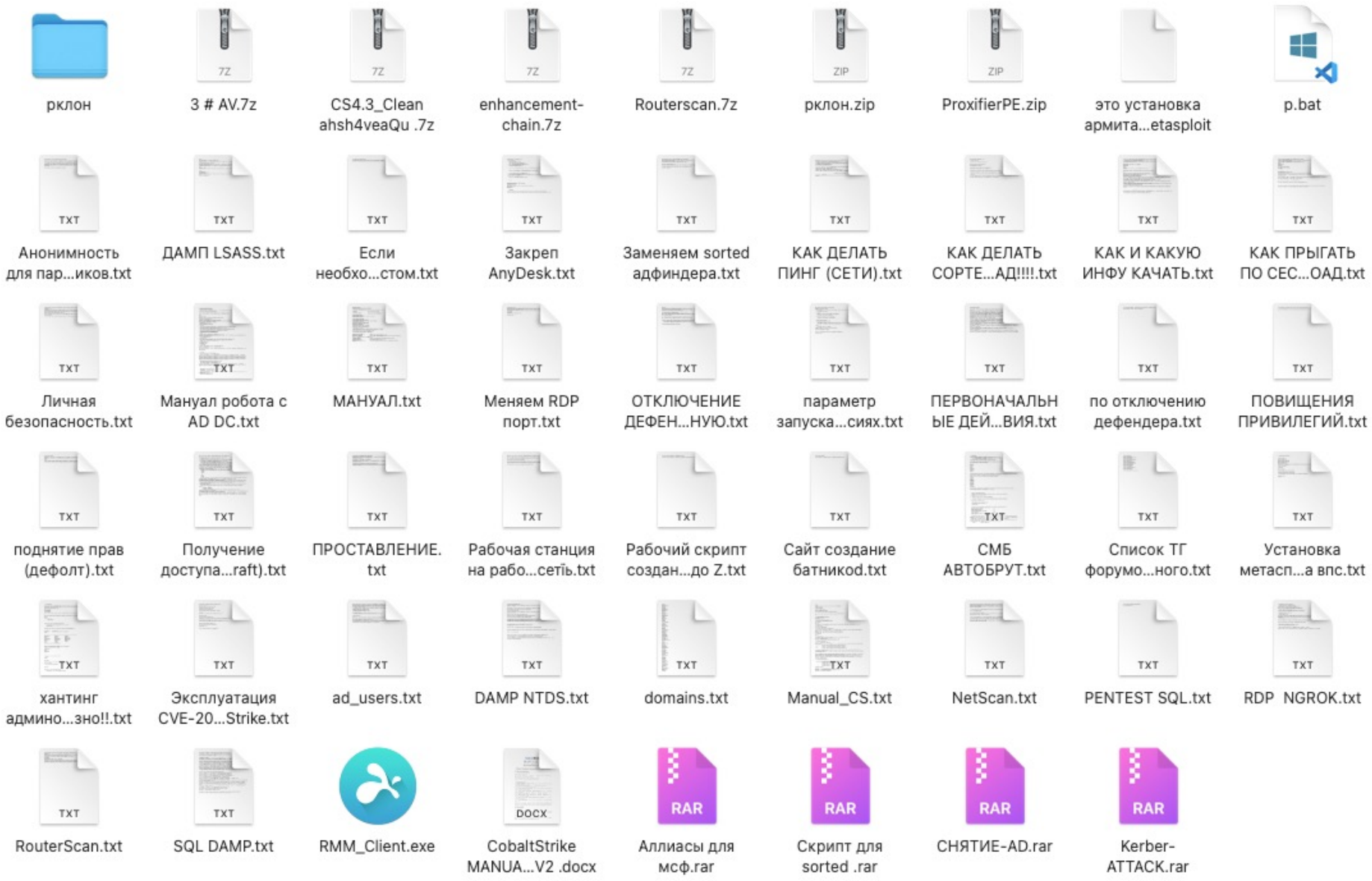
[PARTNERSHIP PROGRAM] Avaddon Ransomware
Avaddon · 06/02/2020 2

Cryptolocker LockBit affiliate program
LockBIt · 01/17/2020 2

Cryptoloker affiliate program
ranzycorp · 13.10.2020



Низкий порог входа в Ransom



Выводы: число атак ransomware увеличится

Проанализировав активность блокчейн-адресов, которые засветились во время ransomware-атак, специалисты подсчитали, что общая сумма выплат кибервымогателям в 2020 году выросла на 311% и достигла 350 миллионов долларов.

luka@cyberpoly.ru

info@antilocker.ru