

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

ИТОГИ

КОД ИБ ИТОГИ

02 ДЕКАБРЯ 2021

КАК ЭВОЛЮЦИОНИРОВАЛИ ВИРУСЫ- ШИФРОВАЛЬЩИКИ?

ЛУКА САФОНОВ, КИБЕРПОЛИГОН



МОСКВА



Как эволюционировали
вирусы-шифровальщики?



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.

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

Год
Выкуп

1989
\$189

Троян PinkBlocker

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

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



Вы установили банер для доступа на наш сайт.
Срок действия банера 30 дней.
Если вы хотите прекратить действие банера раньше установленного срока,
то отправьте SMS по указанному номеру и введите код удаления.

[Суппорт](#)

Отправьте SMS с текстом **1275018** на номер **8353**
Введите полученный код:

Год
Выкуп

2009

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 *

Oops, your important files are encrypted.

If you see this text, but don't see the "Wana Decrypt0r" window, then your antivirus removed the decrypt software or you deleted it from your computer.

If you need your files you have to run the decrypt software.

Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.

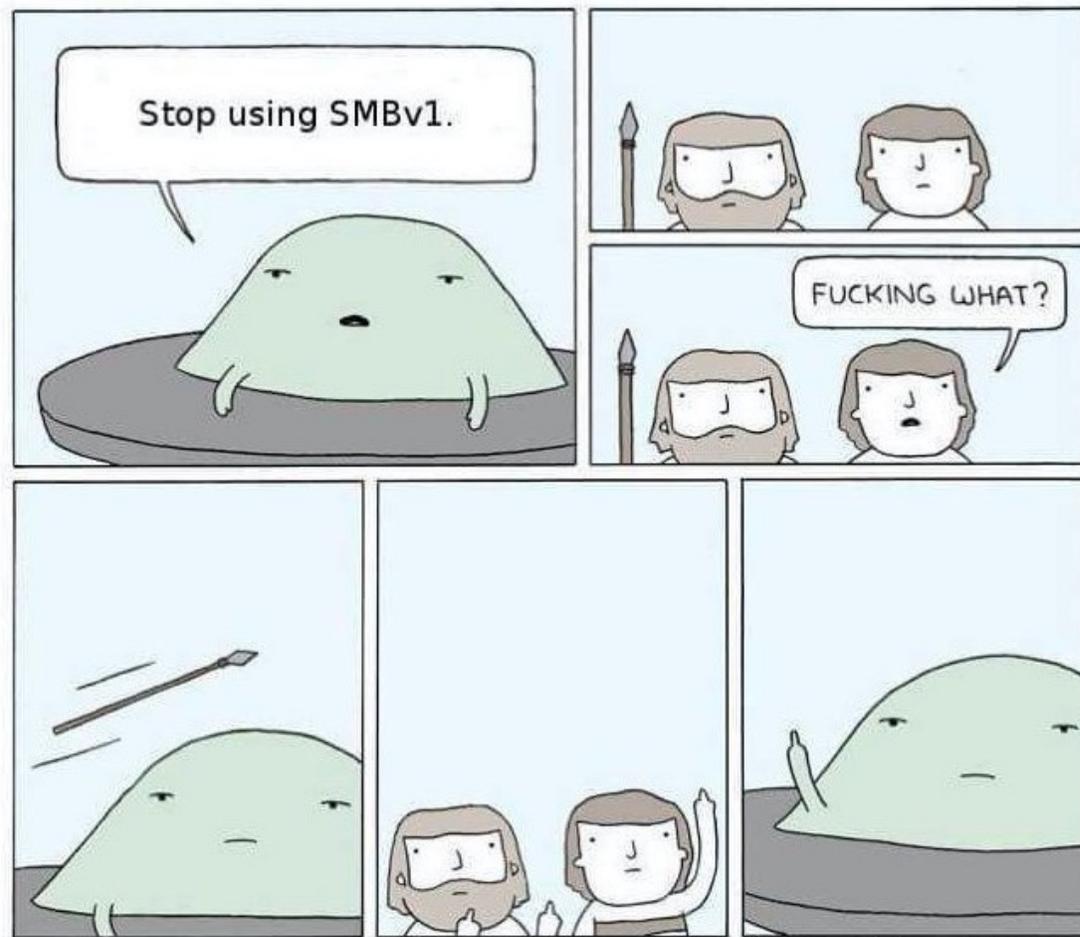
Run and follow the instructions!

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.

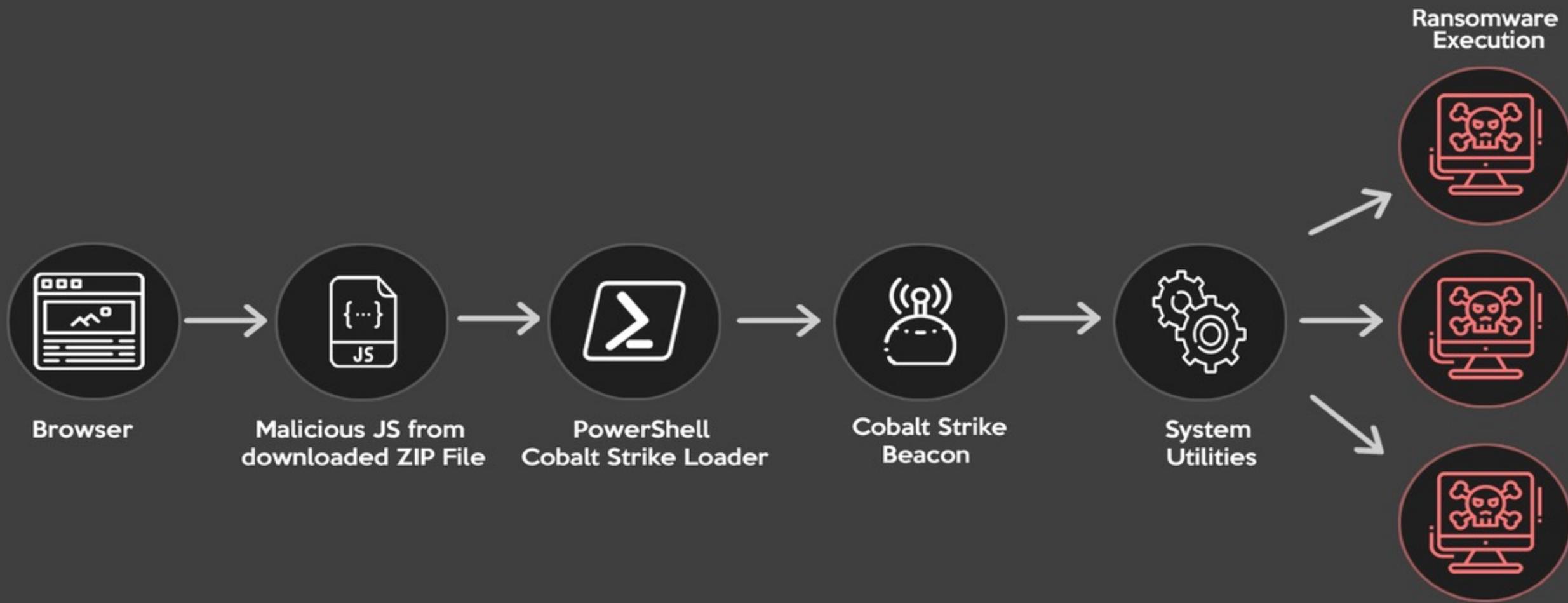
BUT THEY COULD NOT UNDERSTAND ITS ALIEN LANGUAGE



poorlydrawnlines.com

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.

Ransomware attacks caused almost **50% of healthcare breaches** in 2020.



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.

DATA BREACH

Кто стоит за вымогателями?

 NetWalker_19_10_2020_903KB.ps1	 SunCrypt_26_01_2021_1422KB.ps1	 AidaCryst.PNG	 Avaddon_09_06_2020_1054KB.exe	 Avos_18_07_2021_403KB.exe	 Babik_04_01_2021_31KB.exe	 Babuk_20_04_2021_79KB.exe
 BlackKingdom_23_03_20...0KB.exe	 Conti_22_12_2020_186KB.exe	 Cuba_08_03_2021_1130KB.exe	 DarkSide_01_05_2021_30KB.exe	 DarkSide_16_01_2021_59KB.exe	 DarkSide_18_11_2020_17KB.exe	 DearCry_13_03_2021_1292KB.exe
 Hades_29_03_2021_1909KB.exe	 Hive_17_07_2021_808KB.exe	 LockBit_14_02_2021_146KB.exe	 MAKOP_27_10_2020_115KB.exe	 MedusaLocker_24_04_2...61KB.exe	 MountLocker_20_11_2020...0KB.exe	 Nefilim_31_08_2020_3061KB.exe
 Nemty_03_02_2021_124KB.exe	 Phoenix_29_03_2021_1930KB.exe	 PwndLocker_04_03_202...17KB.exe	 Pysa_08_04_2021_500KB.exe	 Ragnar_11_02_2020_40KB.exe	 RansomEXX_14_12_2020...6KB.exe	 Ranzy_20_11_2020_138KB.exe
 REvil_07_04_2021_121KB.exe	 REvil_08_04_2021_121KB.exe	 Ryuk_21_03_2021_274KB.exe	 Sodinokibi_04_07_2019_253KB.exe	 Thanos_23_03_2021_91KB.exe	 Zeppelin_08_03_2021_813KB.exe	 Sekhmet_30_03_2020_364KB.msi

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

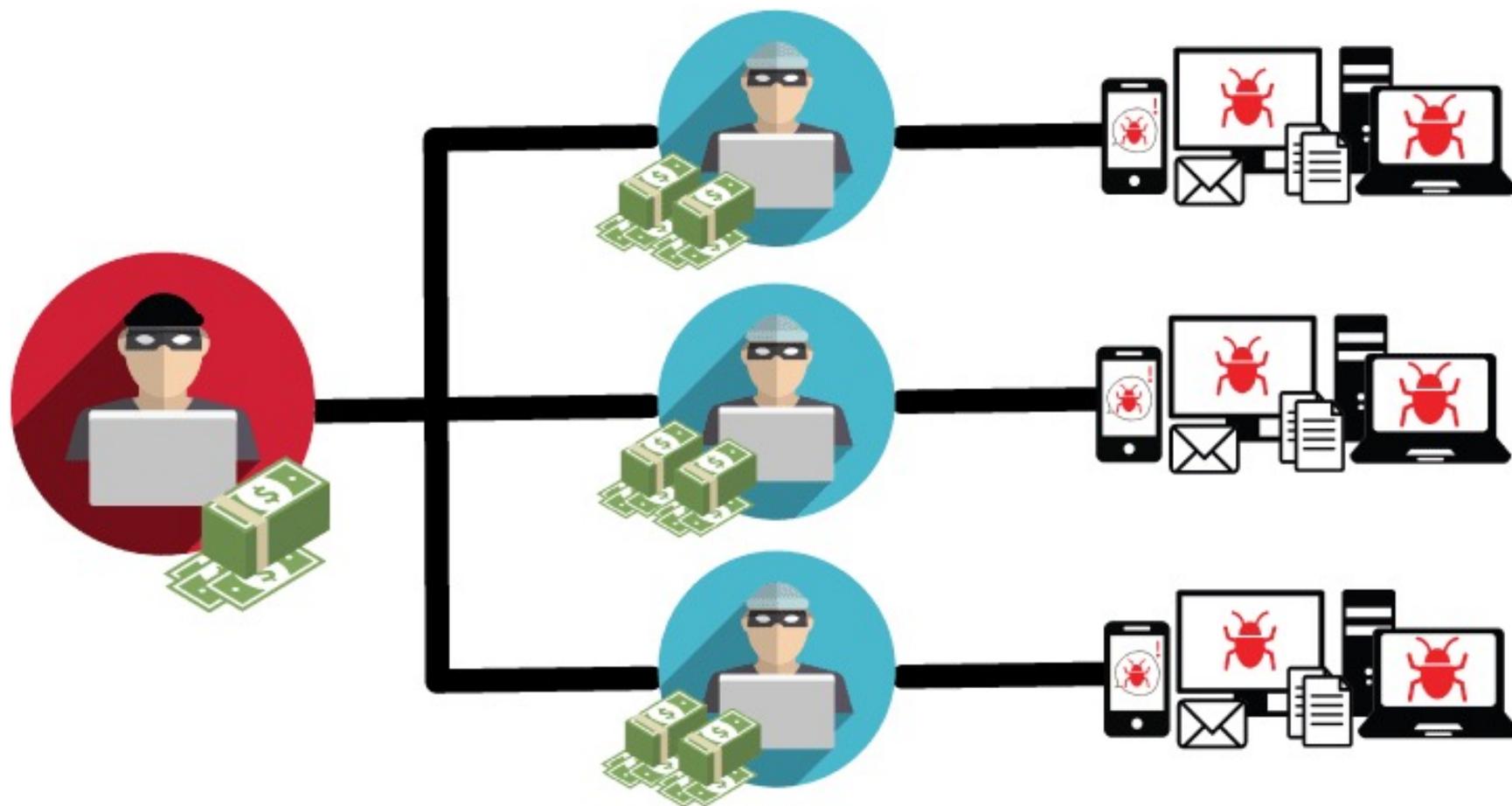
Avaddon · 06/02/2020 2

Cryptolocker LockBit affiliate program

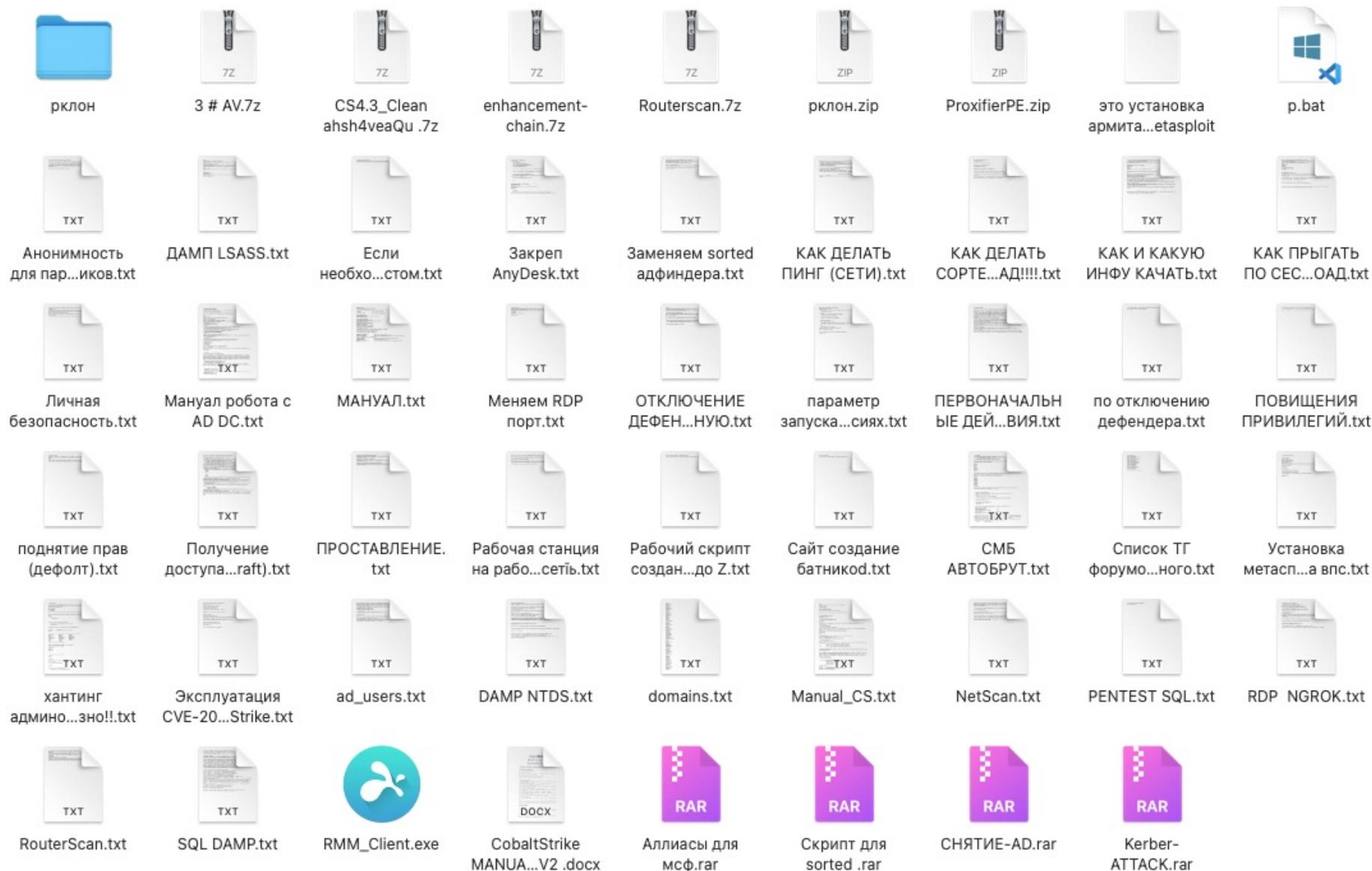
LockBit · 01/17/2020 2

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

