

Хроники выживания нанооператора: взлом взломанного MikroTika

История

Моя история начинается, как и все подобные. Ночной звонок от коллег, прерванный сон, сообщение: "нас взломали". Это был MikroTik CCR1036, на то время топовая железка, державшая на себе целый район. История была бы не такой интересной, если бы злоумышленники не смогли превратить его в «тыкву». Абсолютно нерабочую железку, кусок металла и текстолита. Нанеся нам колоссальный, по нашим меркам ущерб.



Mikrotik CCR1036

Первые действия

Удивительно, что после взлома все продолжало работать. Паника началась после того, как один из коллег потерял удаленное управление. Оценив ситуацию в том самом телефонном разговоре, я всех успокоил. Ввиду того, что маршрутизатор продолжал выполнять свои задачи, все работы перенесли на завтра. «Спокойно сбросим и зальем новый конфиг», — подумал я.

Попытки сброса

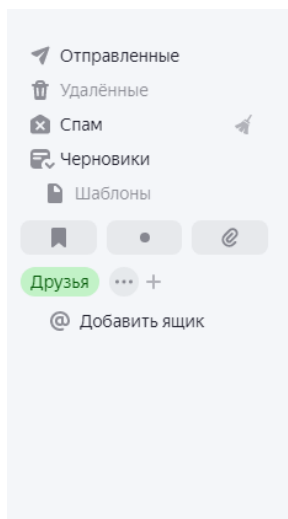
Негодование нашему не было предела. Не в первый день, ни во второй мы не могли сбросить MikroTik. Коллеги из других организаций смеялись над нами, мол, не умеем мы сбрасывать MikroTiki и запускать netinstall. По приезду к нам на помощь, так и уезжали ничего не сделав. Напомню, маршрутизатор так и продолжал обслуживать весь район, что там крутилось внутри - неизвестно, но абоненты не жаловались.

Виной всему, как оказалось, новая защита конфиденциальных данных от производителя. Теперь в любой момент, имея доступ к маршрутизатору, можно было включить режим Protected RouterBOOT. Это режим защиты, в котором блокируется загрузчик, блокируется стандартное поведение кнопки Reset, нельзя сбросить устройство через Netinstall, не работает консоль. Войти в роутер можно только зная логин/пароль админа. Единственный путь для сброса роутера будет переформатирование NAND и RAM, но для этого надо знать, сколько секунд удерживать кнопку Reset. Причем, количество секунд зажатия можно задать любое, например, больше 230, но меньше 231. На практике это приведет к невозможности сброса.

На четвертый день. В пятницу

На четвертый день, в пятницу, микротик перестал работать. Начали звонить абоненты. Коллеги требовали с меня контакты взломщиков: может они хотят выкуп? Доходило до маразма. Никто на меня не выходил, контактов злоумышленников не было.

В конце концов купили новый микротик, а этот отправили представителю производителя. Представитель ответил, что ремонт невозможен. Официальное письмо на английском в Латвию (столица Микротиков) о помощи, также не помогло.



Задача #12345 была обновлена (12.12.2023).

Добрый день.

Проведена диагностика оборудования.

В ходе диагностики обнаружено:

- на RouterOS установлен сторонний пароль;
- отключен LED дисплей;
- отключен режим конфигурации в RouterBOOT;
- отключены стандартные алгоритмы сброса настроек и восстановления ПО с помощью кнопки reset.

Результат:

- для ремонта требуется замена flash с предустановленным ПО; (после такой процедуры требуется восстановление/покупка лицензии)
- в ремонте отказано;
- отсутствуют комплектующие для ремонта.

Для уточнения данных по отправке с Вами свяжется менеджер сервисного центра.

Ответ официального представителя MikroTik в России

Спустя примерно два года

Как-то встретил я своего одноклассника Серегу, друга детства. Не виделись несколько лет. Серега, как оказалось, занимался всем подряд, брался за ремонт любой около компьютерной техники, выезжал на переустановку винды по городу и прочему околокомпьютерному.

Стал я обращаться к Сереге с ремонтом сетевого. И как-то рассказал про печальный опыт с микротиком. Появились мысли у нас обоих, что стоит попробовать отнести пациента к нему, может за что-то и получится зацепиться.

Взламываем

Диагностика Сергея выявила, что на плате маршрутизатора установлены две микросхемы памяти ПЗУ BIOS и NAND. С обоих чипов он сможет считать дампы. Но предупредил, что данные будут сырые и разбираться придется мне.

Закралась у меня надежда, что этот самый тег Protected RouterBOOT и количество секунд хранятся именно в BIOS. Эту версию надо было проверить. Нашел дешевый роутер MikroTik hAP, отдал Сереге, попросил слить дампы до и после установки protected.

Повезло! При сравнении дампов, были отличия. Данные писались в BIOS. Серега только и успевал впаивать, выпаивать чип, сливать и заливать данные с моими экспериментами.

Первая неудача

При первом невнимательном изучении я поспешил с выводами и потерял время. Открыв дампы в HEX редакторе, я заметил, что файл содержит в себе загрузчик и две версии BIOS. В загрузчике, который начинается с 0, так и не смог разобраться, какие значения отвечают за выбор BIOS. Первая версия BIOS начинается с адреса 1 000, вторая резервная с 4 000. Недолго думая, я поменял местами между собой BIOS'ы. Довольный своей работой, отправил «золотой» файл Сереге. В ответ звонок, у нас кирпич.

Загрузчик																	Декодированный текст
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	00	00	00	00	00	00	00	00	11	00	00	00	04	00	00	00	
00000010	4F	73	48	01	00	00	01	00	00	01	00	00	00	10	00	00	OsH.....
00000020	02	00	00	00	90	00	00	00	38	02	00	00	B8	1D	76	A1	h...8...ë.vÿ
00000030	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Первый BIOS																	Декодированный текст
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00001000	00	30	48	D1	02	00	00	24	00	FF	00	00	00	00	00	00	.ОНС...\$.я.....
00001010	EF	BE	AD	DE	00	00	03	00	00	10	00	00	00	00	04	00	пс.Ю.....
00001020	00	10	07	00	00	10	00	00	00	30	48	51	21	C4	B4	18	ОНQ!Дг.
00001030	00	30	48	51	41	98	04	30	00	30	48	51	41	08	C0	18	.ОНQA...0.ОНQA.A.
00001040	00	30	48	D1	E1	1F	08	18	C2	20	45	36	00	30	6A	28	.ОНСб...В Е6.0j(
00001050	00	30	48	D1	E2	0F	00	00	00	30	48	D1	A2	20	05	30	.ОНСв...ОНСÿ .0
00001060	00	30	48	51	A0	C0	0A	00	00	30	48	D1	E0	1F	0A	18	.ОНQ A...ОНСа...
00001070	00	30	48	51	04	00	00	20	00	30	48	51	A0	00	0B	00	ОНQ ОНQ
00001080	00	30	48	D1	E0	07	08	18	00	30	48	D1	02	00	00	20	ОНСа ОНС

Второй BIOS																	Декодированный текст
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00040000	00	30	48	D1	02	00	00	24	C0	FF	00	00	00	00	00	00	.ОНС...\$Ая.....
00040010	EF	BE	AD	DE	00	00	03	00	00	10	00	00	00	00	04	00	пс.Ю.....
00040020	00	10	07	00	00	10	00	00	00	30	48	51	21	C4	B4	18	ОНQ!Дг.
00040030	00	30	48	51	41	98	04	30	00	30	48	51	41	08	C0	18	.ОНQA...0.ОНQA.A.
00040040	00	30	48	D1	E1	1F	08	18	C2	20	45	36	00	30	6A	28	.ОНСб...В Е6.0j(
00040050	00	30	48	D1	E2	0F	00	00	00	30	48	D1	A2	20	05	30	.ОНСв...ОНСÿ .0
00040060	00	30	48	51	A0	C0	0A	00	00	30	48	D1	E0	1F	0A	18	.ОНQ A...ОНСа...
00040070	00	30	48	51	04	00	00	20	00	30	48	51	A0	00	0B	00	.ОНQ... .ОНQ ...
00040080	00	30	48	D1	E0	07	08	18	00	30	48	D1	02	00	00	20	ОНСа ОНС

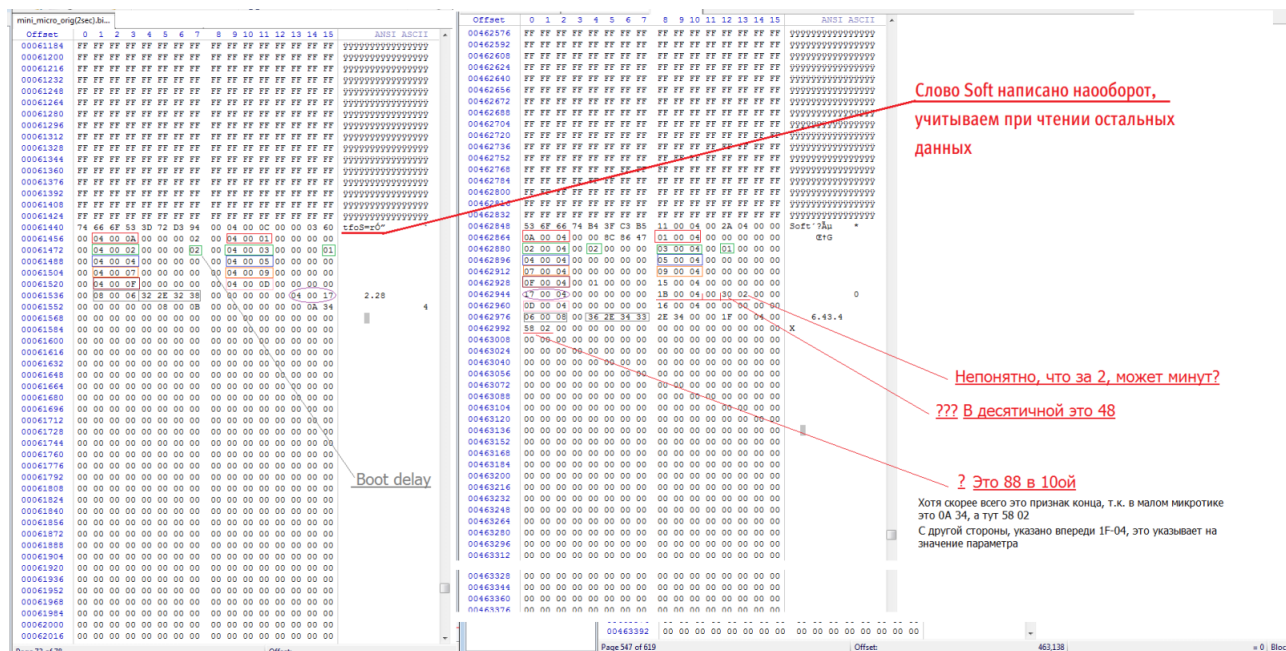
Адресация и разделение памяти

Истина где-то рядом

Пока мы занимались изучением «низкоуровневого взлома», параллельно отправил наработки на завод Микротик в Латвию. Как и обещали, ответ пришел в течении семи «бизнес-дней»: ничем помочь не можем.

Энтузиазм не утихал, у нас еще были козыри в рукаве в виде разных дампов с домашнего роутера MikroTik hAP, которые были почему-то отвергнуты сразу. На первый взгляд, BIOS'ы этих двух роутеров не имеют ничего общего. Хотя, если приглядеться, они как два брата, вот только в hAP в отличии от CCR, данные пишутся задом наперед.

В этот раз я был более внимательным. Не торопясь, я сравнивал BIOSCCR и зеркальный hAP. Пытался понять набор байт, накопить какую-то информацию для построения картины. И вот заметил очевидное: помимо загрузчика и двух вариантов BIOS, есть еще область под названием «Soft», начинающаяся с адреса 71 000, хранящая в себе значения ключей Routerboard, заданных в интерфейсе.



Старая памятка тех лет в оригинальном виде, которой мы обменивались

Визуально я смог примерно увидеть эти байты, отвечающие за количество секунд для сброса маршрутизатора. Но никак не смог перевести их в человеческую систему счисления. Поэтому самым «умным» решением на тот момент было обнулить все байты. Справедливости ради, хочу отметить, что возможно это просто какой-то другой флаг, отвечающий за protected boot. В конце области Soft увидел нечто похожее на hash-сумму, немного огорчился, но трогать ее не стал.

Простой рецепт

Звонит Серега и говорит: «Залил твоего Франкенштейна, маршрутизатор начал вести себя очень странно, выдал ошибку прошивки и запустил netinstall. Прошил его новой прошивкой, теперь он как новый!»

Мы уже догадались оба, что достаточно было нарушить целостность области Soft (не сходится hash) в BIOS, и MikroTik даст возможность восстановить себя. В железной части я не участвовал, но сделать все это можно простым программатором CH341A с прищепкой.

Размышления

Следов злоумышленников я не смог найти, в процессе восстановления все данные были утеряны. Прошивка была свежая для того года. Предположительно, взлом был произведен через web-интерфейс MikroTik под названием webfig. Возможно, с внутренней сети. Возможно - конкурентами. Рассказать к сожалению нечего.

Несмотря на то, что в коллективе это была моя зона ответственности, меня никто даже косвенно не винил. Убытки были огромные. Но, спустя, казалось бы, столько времени, я смог свести их к 0. Сегодня этот MikroTik работает и обслуживает уже другой район.

Вроде как оказалось все просто и очевидно, лекарство от проблемы банальное, но в интернете информации нет. Поэтому хочу поделиться с вами этим полезным материалом - как можно восстановить такую «тыкву».

Какие выводы сделал я?

Нужно всегда обновляться и следить за безопасностью =).

Но если ты нанооператор, с временем и деньгами бывают проблемы, возможно, стоит в будущем присмотреться к другим вендорам. Держать у себя на запас резервное оборудование.

Предыдущая история из жизни нанооператора - [здесь](#).