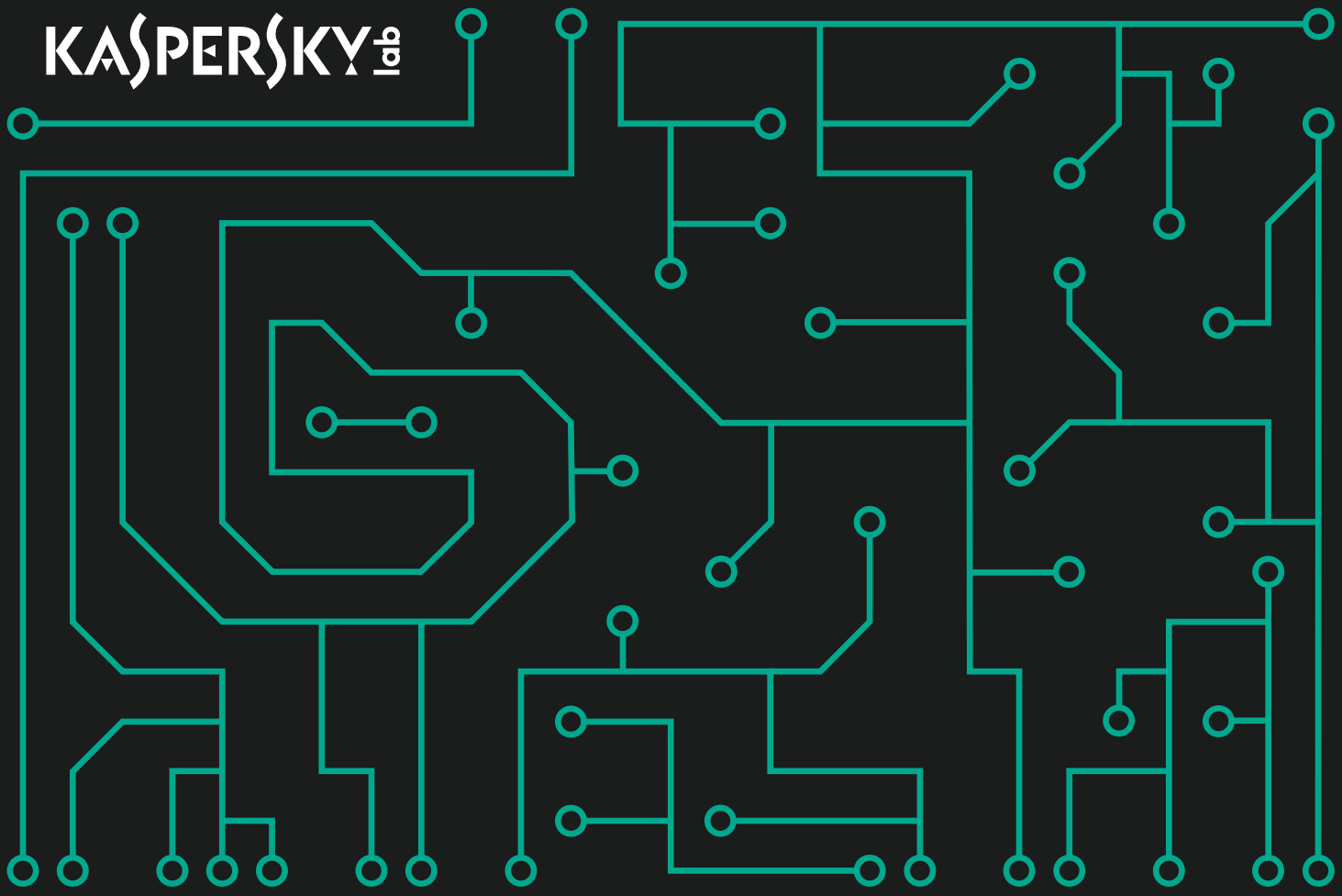
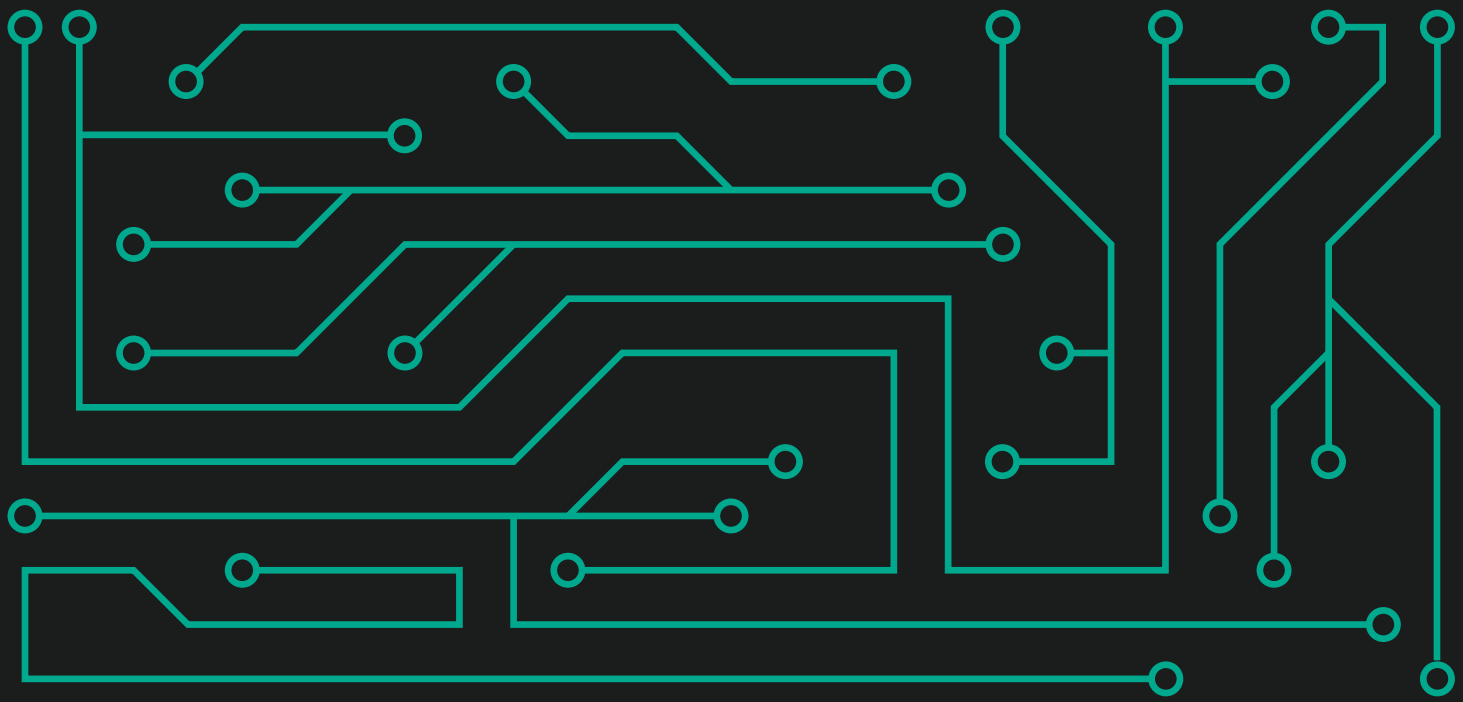
KASPERSKY lab



Kaspersky Security Bulletin 2018

СЮЖЕТ ГОДА: МАЙНЕРЫ



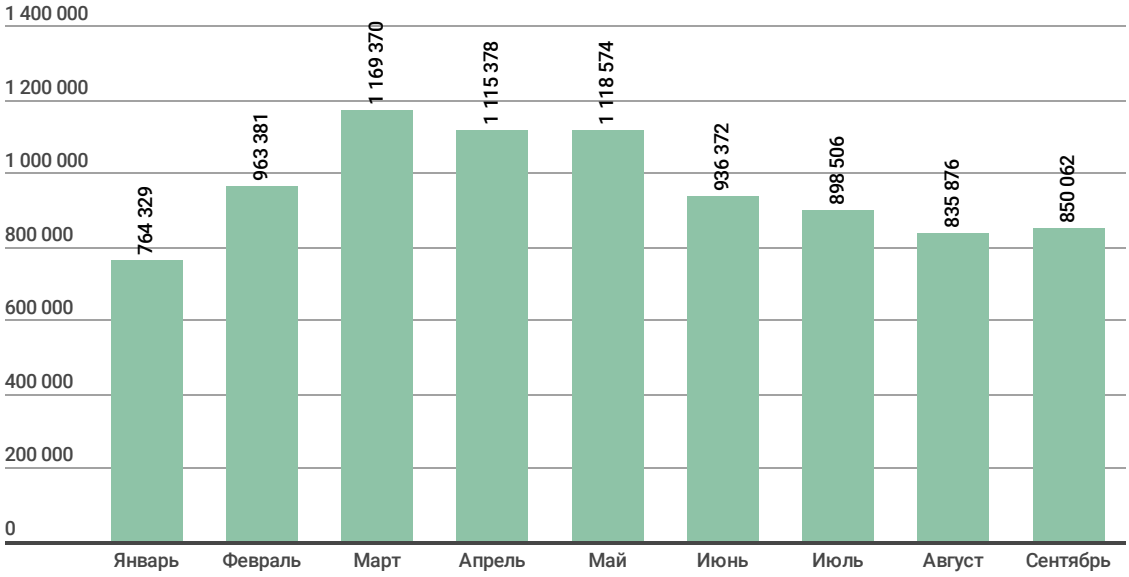
СОДЕРЖАНИЕ

Криптовалютные майнеры, заражающие компьютеры ничего не подозревающих пользователей, действуют, по сути, по той же бизнес-модели, что и программы-вымогатели: вычислительные мощности жертвы используются для обогащения злоумышленников. Только в случае с майнерами пользователь может долгое время не замечать, что свободные 70-80% мощности центрального или графического процессора его ПК используются для генерации виртуальных монет. Зашифрованные документы и сообщение от вымогателей не заметить гораздо сложнее.

На компьютеры пользователей и корпоративные машины криптомайнеры попадают обычно вместе с рекламным ПО, взломанными играми и прочим пиратским контентом. При этом «порог входа», а именно — сам процесс создания майнера, сейчас довольно низок: злоумышленникам в этом помогают готовые к использованию партнерские программы, открытые майнинг-пулы и билдеры майнеров. Кроме этого, существует еще один метод кражи вычислительных ресурсов — встраивание в веб-страницы скрипта для майнинга, который запускается в тот момент, когда пользователь открывает сайт в браузере. Особняком стоят злоумышленники, чья цель не частные компьютеры, а серверы крупных компаний, чье заражение — более трудоемкий процесс.

ТЕНДЕНЦИИ

2018 год начался с роста количества атак, связанных с майнерами. Однако после падения курса основных криптовалют, длившегося с января по февраль, можно было заметить тенденцию на снижение активности заражений — так же как и падение общего интереса к криптовалютам. Из графика видно, что если количество атак криптомайнеров и сократилось, то угроза все еще остается актуальной. На сколько снизится количество заражений после ноябрьского обвала курса биткойна, покажет время.



Количество уникальных пользователей, атакованных майнерами, Q1–Q3 2018

ПО для скрытого майнинга пользовалось большой популярностью у владельцев ботнетов, что подтверждает собранная нами статистика по файлам, загружаемым зомби-сетями: бум криптомайнеров пришелся на первый квартал 2018 года, а доля этого вредоносного ПО в первой половине года составила 4,6% от общего количества всех скачанных ботнетами файлов. Для сравнения: во второй половине 2017 года этот показатель составлял менее трех процентов (2,9%). Из этого следует, что злоумышленники стали чаще рассматривать ботнеты как средство распространения ПО для майнинга криптовалют.

	H2 2017		H1 2017	
1	Lethic	17.0%	njRAT	5.2%
2	Neutrino.POS	4.6%	Lethic	5.0%
3	njRAT	3.7%	Khalesi	4.9%
4	Emotet	3.5%	Miners	4.6%
5	Miners	2.9%	Neutrino.POS	2.2%
6	Smoke	1.8%	Edur	1.3%
7	Cutwail	0.7%	PassView	1.3%
8	Ransomware	0.7%	Jimmy	1.1%
9	SpyEye	0.5%	Gandcrab	1.1%
10	Snojan	0.3%	Cutwail	1.1%

Самые загружаемые угрозы, H2 2017 — H1 2018

Продолжая тему ботнетов, нельзя не упомянуть, что в третьем квартале 2018 года мы зафиксировали спад количества DDoS-атак, и, по мнению наших экспертов, наиболее вероятная причина этому — «перепрофилирование» мощностей ботсетей с DDoS-атак на майнинг криптовалюты. Повлияла на это не только высокая популярности «крипты», но и высокая конкуренция на «DDoS-рынке». Она привела к удешевлению атак для клиентов, но не для самих ботоводов, на плечах которых по-прежнему лежит немало не очень законных «организационных моментов».

Майнинг же выгодно отличается тем, что при определенных подходах к его организации он может быть незаметен для владельца зараженной машины, и, таким образом, шансов столкнуться с киберполицией у злоумышленника гораздо меньше. А перепрофилирование имеющихся серверных мощностей и вовсе выводит их владельца из поля зрения правоохранительных органов. Есть косвенные доказательства того, что владельцы многих известных ботнетов сменили вектор деятельности, переключившись на майнинг. Так, например, сильно упала DDoS-активность ботнета Yoyo, хотя данных о его расформировании не поступало.

Кроме этого, майнингу стали уделять столько же (или больше) внимания, как шифровальщикам: в этом году мы встретили несколько примеров перепрофилированного вредоносного ПО, получившего дополнительные функции, связанные с добычей криптовалюты. А технические приемы, используемые авторами майнеров, становились все изощреннее.

Так, в июле этого года в поле нашего зрения попала интересная реализация майнера, которую мы назвали PowerGhost. Зловред умеет незаметно закрепляться в системе и распространяется внутри крупных корпоративных сетей, заражая как рабочие станции, так и серверы. Чтобы майнер как можно дольше оставался незамеченным пользователем и защитными решениями, установленными на компьютеры, используется множество бесфайловых техник. Заражение происходит удаленно с использованием эксплойтов или инструментов удаленного администрирования (Windows Management Instrumentation). При заражении запускается однострочный powershell-скрипт, который скачивает основное тело зловреда и сразу запускает его, не записывая на жесткий диск.

Еще один пример перепрофилирования — троянец-вымогатель Trojan-Ransom.Win32.Rakhni, первые образцы которого были обнаружены «Лабораторией Касперского» еще в 2013 году. Майнинговые же функции — новинка 2018 года. При этом решение об их задействовании зависит от наличия на зараженной машине папки %AppData%\Bitcoin. Если она существует, загрузчик скачает шифровальщик. Если папки нет и при этом у компьютера более двух логических процессоров, будет скачан майнер. Чтобы зловред остался в системе незамеченным, разработчики сделали его похожим на продукты Adobe. Это отражается в иконке и названии исполняемого файла, а также в поддельной цифровой подписи, где используется название компании Adobe Systems Incorporated.

Научилось подсаживать на компьютеры утилиты для майнинга и некогда исключительно рекламное ПО — PBot. Зловред распространяется через сайты-партнеры, которые внедряют в свои страницы скрипты, перенаправляющие пользователя на рекламные ссылки. Типичная схема распространения выглядит следующим образом:

1. Пользователь заходит на один из сайтов партнерской сети.
2. Нажатие любой точки на странице приводит к появлению нового окна браузера, в котором открывается промежуточная ссылка.
3. Ссылка отправляет пользователя на страницу загрузки PBot, задача которой — обманным путем добиться скачивания и запуска зловреда.

Среди всех незаконно добываемых криптовалют наиболее популярной является monero (xmr). Это обусловлено анонимностью ее алгоритма, относительно высокой стоимостью на рынке и легкостью продажи, так как ее принимает большинство крупных криптовалютных бирж. Для ботсети, добывающей эту монету незаконно, важно, что ее можно майнить, используя CPU. По некоторым данным, незаконно было добыто порядка 5% от всего оборота криптовалюты на сумму в $175 млн.

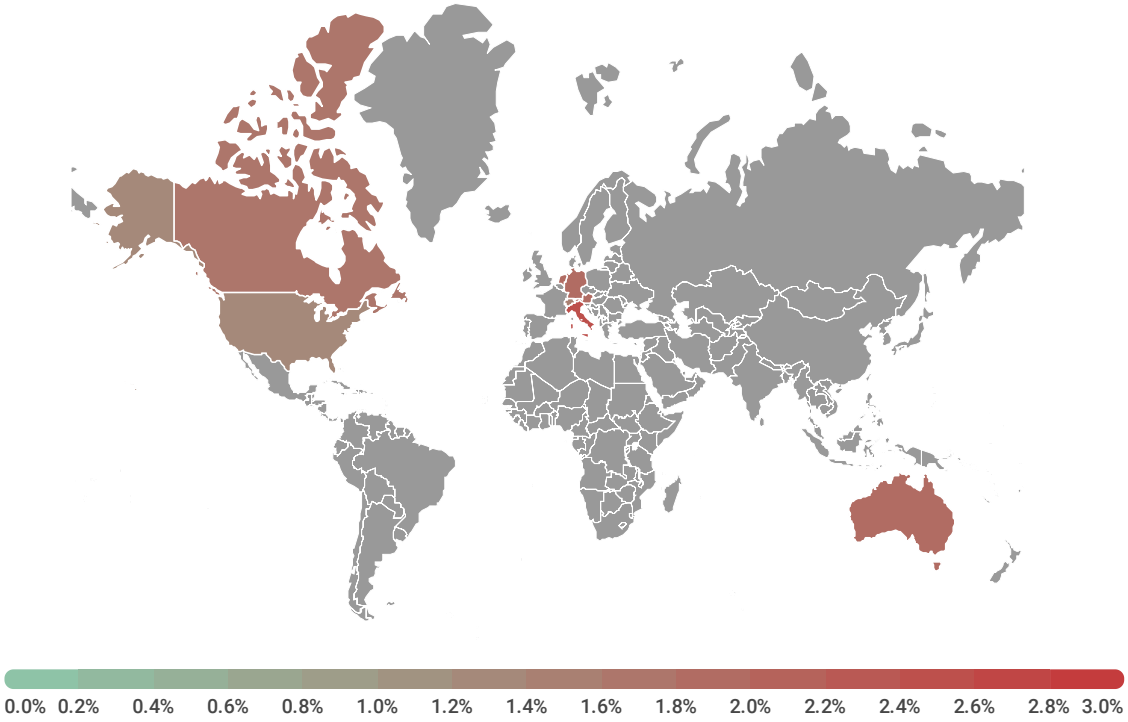
ФАКТОРЫ, ВЛИЯЮЩИЕ НА РАСПРОСТРАНЕНИЕ МАЙНЕРОВ

По данным, которые мы получили из различных источников, можно сделать вывод, что законодательное регулирование криптовалют не сильно влияет на распространение скрытого майнинга. Так, например, в Алжире и Вьетнаме криптовалюты либо запрещены, либо их использование сильно ограничено местным законодательством. Но при этом Вьетнам находится на третьей строке в рейтинге стран — лидеров по количеству атак майнеров, а Алжир на шестой. В то же время Иран, где идет подготовка законодательных актов, регулирующих криптовалюту, и планируется разработка и эмиссия собственных «монет», — на седьмой.

Страна	Статус криптовалют	% атак
Казахстан	Не запрещена, не легализована	16,75%
Вьетнам	Запрещена эмиссия (майнинг)	13,00%
Индонезия	Признана биржевым товаром	12,87%
Украина	Обращение регулируется законодательством	11,19%
Россия	Рассматривается законодательное регулирование	10,71%
Алжир	Запрещена	9,03%
Иран	Готовит законодательное регулирование, планируется создание собственной криптовалюты	7,21%
Индия	Думают запретить, идут слушания	7,20%
Таиланд	Обращение регулируется законодательством	6,76%
Тайвань	Не запрещена	5,81%

TOP-10 стран по доле атак майнеров с января по октябрь 2018 года (включены только страны с более чем 500 000 клиентов «Лаборатории Касперского»)

Для сравнения: реже всего жертвами криптомайнеров становились пользователи США — 1,33% от общего количества атак; в Швейцарии с этим видом вредоносного ПО столкнулось всего 1,56% пользователей, а замыкает тройку Англия, где атаки пришлись на долю 1,66%.



Карта стран с наименьшей долей атак майнеров, январь — октябрь 2018 года (включены только страны с более чем 500 000 клиентов «Лаборатории Касперского»)

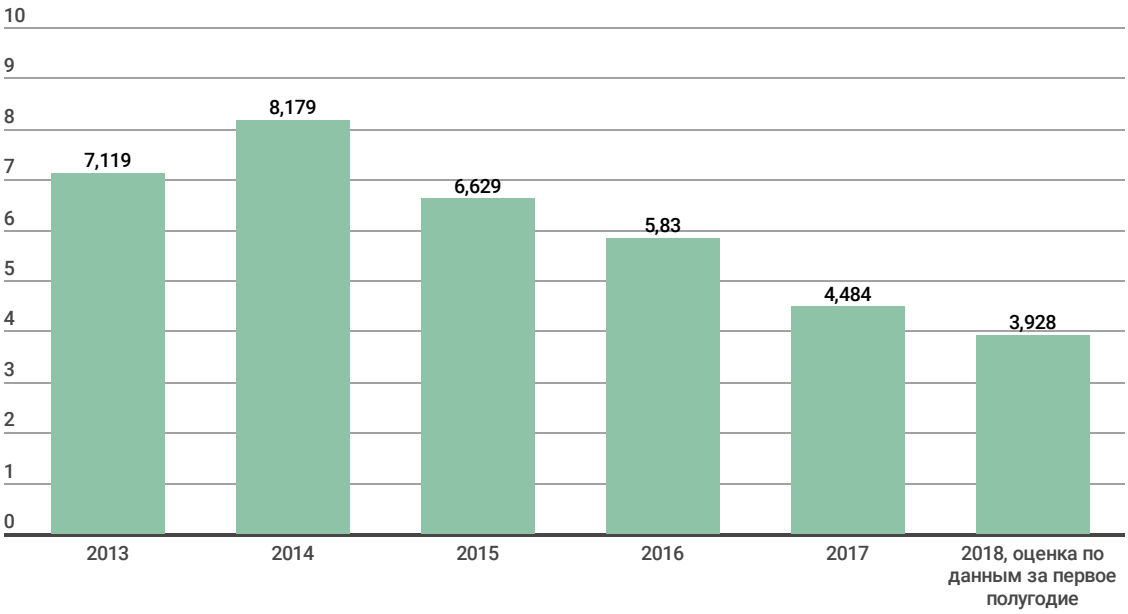
Не влияет на распространенность майнеров и стоимость электроэнергии: она сильно разнится от страны к стране. К тому же этот фактор не важен для злоумышленника, эксплуатирующего чужие ресурсы.

СПОСОБЫ РАСПРОСТРАНЕНИЯ

Если посмотреть на распространение пиратского ПО в странах с наибольшим количеством атак майнеров, можно увидеть четкую корреляцию: чем свободней распространяется нелицензионное ПО, тем больше майнеров. Это подтверждает и наша статистика, говорящая, что чаще всего майнеры попадают на машины жертв вместе с пиратским ПО.

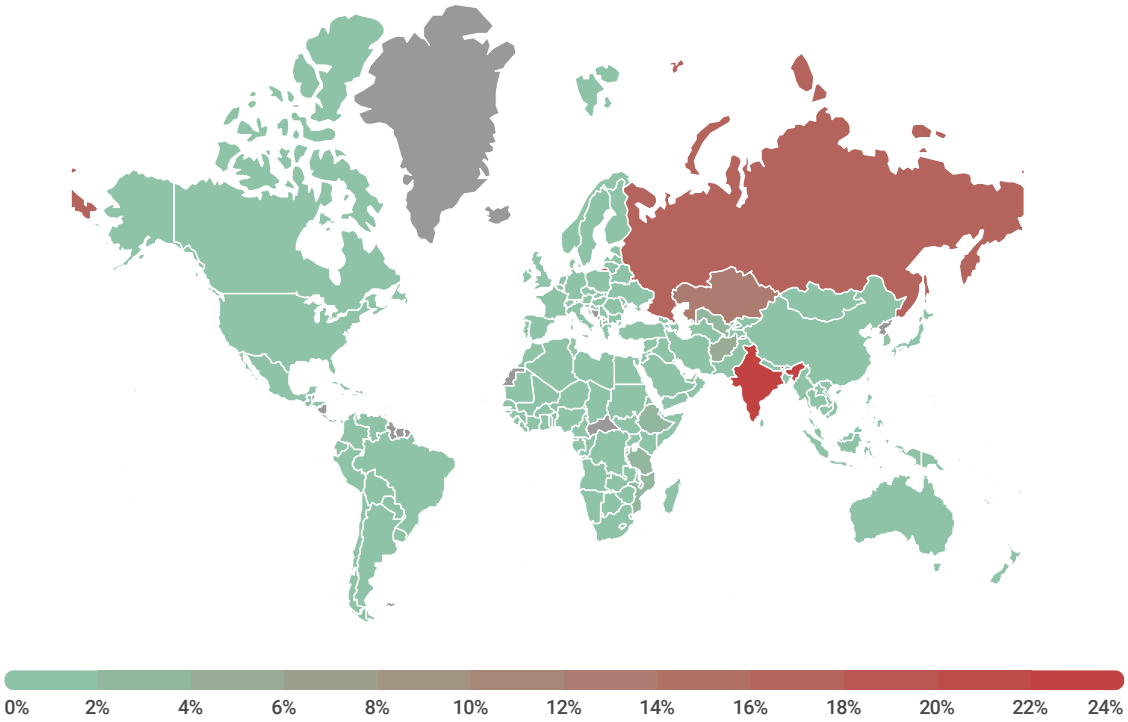
Еще один вектор проникновения майнеров на компьютеры — инсталляторы рекламного ПО, распространяемые с помощью социальной инженерии. Более изощренные варианты, например распространение посредством уязвимостей, таких как EternalBlue, нацелены на серверные мощности и встречаются реже.

Кроме этого не стоит забывать о USB-накопителях, используемых с целью распространения ПО для майнинга криптовалют как минимум с 2015 года. Процент обнаружений популярного биткойн-майнера Trojan.Win64.Miner.all на съемных устройствах ежегодно растет примерно на 1/6. В 2018-м каждый десятый пользователь, пострадавший от зловредов, передаваемых через «флешки», был жертвой именно этого майнера (приблизительно 9,22%; для сравнения, в 2017 году этот показатель составил 6,7%, а в 2016-м — 4,2%).



Количество уникальных пользователей (в миллионах), на компьютерах которых было обнаружено вредоносное ПО в корневых каталогах, что является основным признаком заражения через съемные носители, 2013–2018 гг. Источник — KSN.

Trojan.Win32.Miner.ays/Trojan.Win.64.Miner.all был обнаружен в Индии (23,7%), России (18,45%) и Казахстане (14,38%), но отдельные случаи зафиксированы также в странах Азии и Африки, в Европе (в Великобритании, Германии, Нидерландах, Швейцарии, Испании, Бельгии, Австрии, Италии, Дании и Швеции), США, Канаде и Японии.



Доля пользователей, пострадавших от биткойн-майнеров на съемных носителях, 2018. Источник: KSN (включены только страны с более чем 10 000 клиентов «Лаборатории Касперского»)

ВЫВОД

Если подводить итоги прошедшего года, можно выделить следующие тезисы:

1. Рост популярности и стоимости криптовалют убедил киберпреступников в необходимости вкладывать ресурсы в разработку новых техник для майнеров, которые, по нашим данным, постепенно приходят на смену троянцам-вымогателям.
2. Активность скрытого майнинга снижается в моменты падения цен на криптовалюты.
3. На распространение скрытого майнининга не влияют такие факторы, как законодательное регулирование криптовалют или стоимость электроэнергии в регионе.
4. Часто майнеры попадают на компьютеры жертв при скачивании нелицензионного контента или установке пиратского ПО. Соответственно, наибольшее распространение данный вид угроз получил в странах с низким уровнем регулирования рынка нелицензионного ПО, а также общей цифровой грамотности пользователей.