OPTIVERA
информационная безопасность

Трансформация российской ИБ

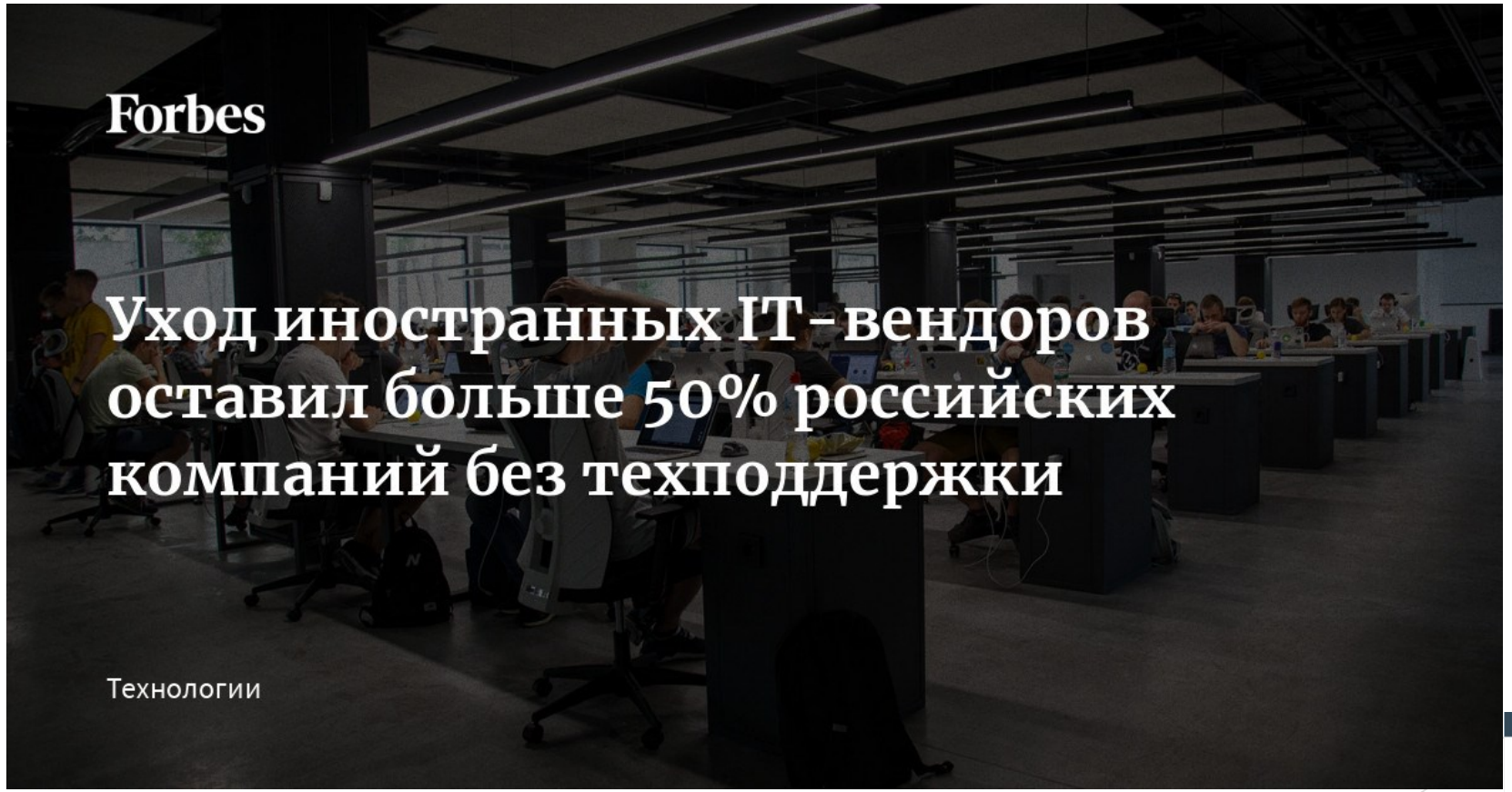
Гарин Григорий

Руководитель департамента
информационной безопасности

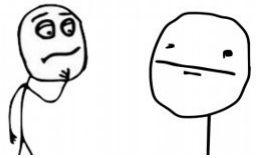
О чем поговорим?

- Как хакеры из фильмов проникли в нашу повседневность и что еще интересного на ИБ-рынке произошло за год

Уход вендоров :(



Задумались о киберустойчивости



- После начала СВО, компании всерьез задумались о своей киберустойчивости.

Хакотичность

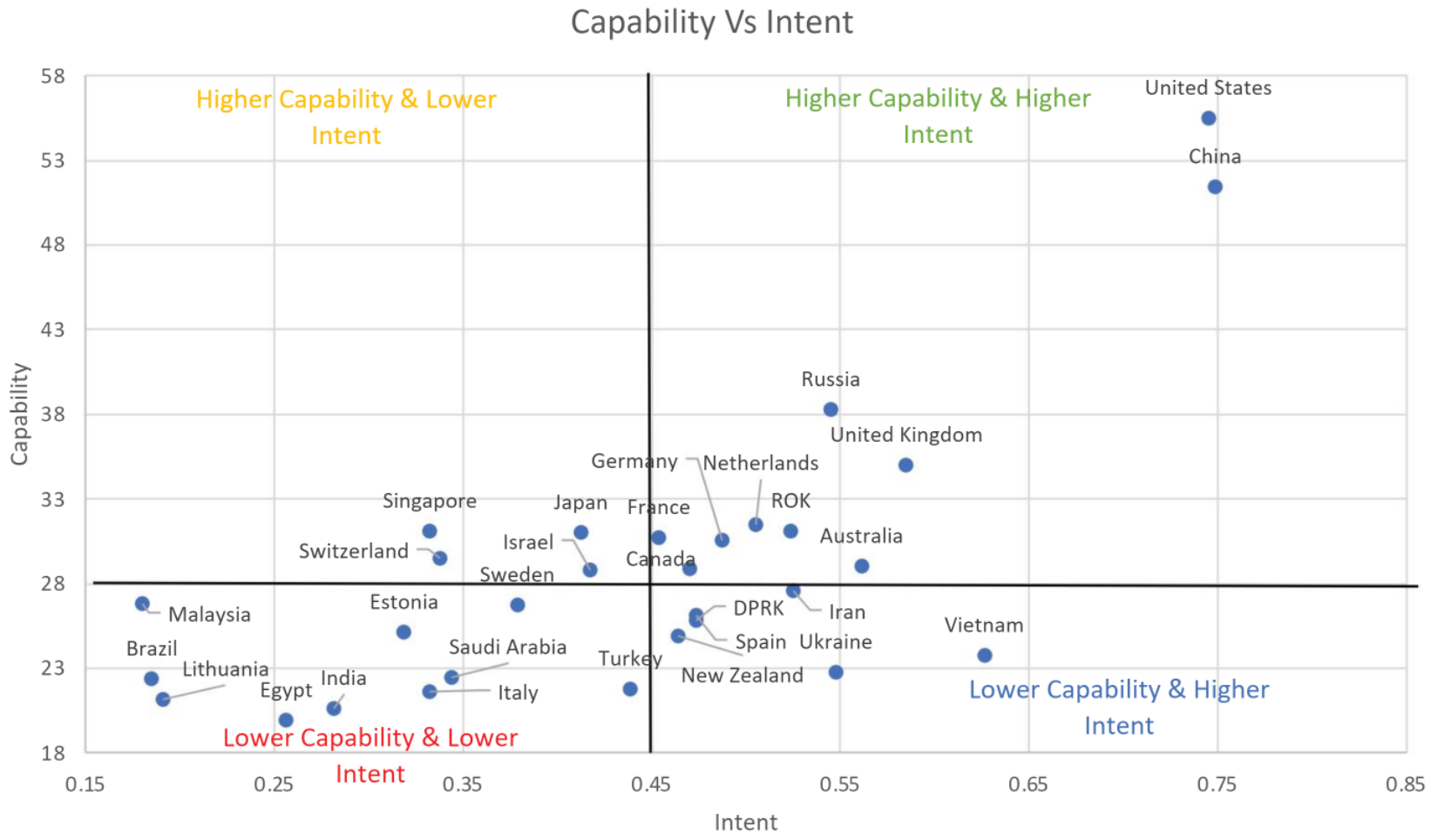
- В самом начале хакеры атаковали зарубежные компании, которые не уходили из России
- Затем «русские хакеры» стали атаковать всех «недружественных», а
- украинские хакеры нападали на РФ бизнес, имеющих хоть какое-то отношение к специальной военной операции.

Такая неразборчивость в мишенях лишний раз показала, что думать о своей киберустойчивости стало насущной необходимостью

Ведущие «хакерские страны» начали легитимизировать группировки

- Журналисту из Голландии удалось пообщаться с одним из нерядовых участников ИТ-армии , который признает не только сотрудничество со спецслужбами, но и прямое управление с их стороны.
- Швейцария проанализировала ИТ-армию, ее структуру, задачи, экосистему и т.п. Также делается предположение, что ИТ-армия действует не по своей инициативе, а следует полученным от спецслужб указаниям
- Власти РФ также намекали на возможность участия компетентных специалистов в кибервойсках (но пока без конкретики)

Рейтинг национального индекса киберсилы



Проблематика?

- «Военные» хакеры работают по «приказу» - с ними проще;
- Хакеры-патриоты = проблема (тк привыкли к безнаказанности, имеют высокую экспертизу, огромный инструментарий);

> И что будет потом с этими обученными хакерами и имеющимся инструментарием? Против кого он будет направлен? За чьими данными будут охотиться те, кто сейчас является киберпатриотом?

- Чем > атак, тем лучше наша «практическая» безопасность.
- Осталось дело за регуляторами

Скидки и акции у злоумышленников

- Не только хакеров стало больше, сколько автоматизация их деятельности вышла на новый уровень, позволяющий им скинуть цены на свои услуги.

(Crime-as-a-Service, Ransomware-as-a-Service, DDoS-as-a-Service, C2-as-a-Service и т.п.)

Стоимость ПДн упала чуть ли не вдвое из-за массы утечек в рынке

Увеличение трат на оценку защищенности

- Компании начинают уделять больше времени предотвращению атак, а именно оценке защищенности своих внутренних систем/приложений/сервисов, используя для этих целей различные инструменты от сканеров уязвимостей и покупки BAS-решений до регулярного пентеста и формирования площадок Bug Bounty

CNews

Российским хакерам предложили проверить «Госуслуги» на прочность. За это хорошо заплатят

2 дня назад

интерфакс

Минцифры заплатит до 1 млн рублей за обнаружение уязвимостей на "Госуслугах" и в ЕСИА

2 дня назад

SecurityLab

Минцифры проверит защищенность Госуслуг на платформе Standoff 365 Bug Bounty

2 дня назад

Яндекс начинает выплачивать **в 2 раза больше** за найденные уязвимости в сервисах и инфраструктуре компании. В 2023 году за обнаруженную ошибку можно будет получить до 1,5 млн рублей.

«Тинькофф» запустил на платформе BI.ZONE программу ...

«Тинькофф» запустил публичную программу по поиску ошибок и уязвимостей в своих сервисах за вознаграждение на платформе BI.ZONE Bug Bounty.

Страхование киберрисков где-то рядом

- Количество атак и рост законодательных инициатив стало серьезным драйвером для улучшения своей ИБ или идеальным моментом для страхования своих рисков. Многие иностранные компании уже используют данную практику. Наши «коллеги по цеху» уже активно смотрят в эту сторону.

Только помните, что некоторые страховые атаки хакеров все чаще рассматривают как проявления кибервойны, а это форс-мажор и отказ от страховых выплат.

Консолидация рынка

- Росатом купил «Код Безопасности», «Эльбрус»
- Ростелеком купил «Новые Технологии Безопасности», собирается купить «Мегафон» и что-то еще

Наши реалии изменились, мы пока не можем в условиях мобилизационной экономики жить как прежде.

ИБ компании не могут развиваться в прежнем ритме:

- им перестают давать кредиты
- у них перестают покупать решения
- они теряют разработчиков (кто уезжает за деньгами, кто от мобилизации).

В результате нас ждет серьезная консолидация рынка, на котором выживут крупные независимые ИБ-игроки и «дочки» крупных холдингов и госкорпораций.

Необходимо умерить аппетиты

- Мы очень привыкли к Cisco, Palo Alto, Fortinet, IBM, Microsoft и хотим альтернативу в виде такого же качества и функционала, но уже от российских коллег.
- Чуда в одночасье не произойдет – нельзя в моменте сделать отечественные продукты лучше, быстрее, функциональнее.

Поэтому сейчас мы должны немного умерить свои аппетиты и в течении n-го времени покупать обещания по типу:

«Мамой клянусь скоро все будет!!!»

Еще минутку…

- Необученный персонал в 2023 году будет обходится очень дорого, в виду увеличения числа атак
- Государство усиливает внимание за ИБ (250-й Указ, 266-ФЗ, дополнения в существующие ФЗ и тд)
- Open Sourse или возвращение «блудного сына»
- Атаки на поставщиков услуг или на разработчиков ПО становятся массовее
- Кибербез становится непрерывным (на SOC смотрят уже не как на напиток)
- Нехватка кадров ощущается все острее

А что у соседей

- Есть потребность
- Есть $$
- Есть желание развиваться
- Есть присутствие ведущих вендоров

- Нет экспертизы
- Нет понимания точки старта
- Нет сервиса уровня РФ (не в обиду коллегам)

С П А С И Б О!