«ЭТИКА ПОВЕДЕНИЯ В КИБЕРПРОСТРАНСТВЕ»

Кирюшкина Кира
Руководитель отдела ЗИ ГК ИнфоКуб

Тенденции ИБ 2014-2016 г.

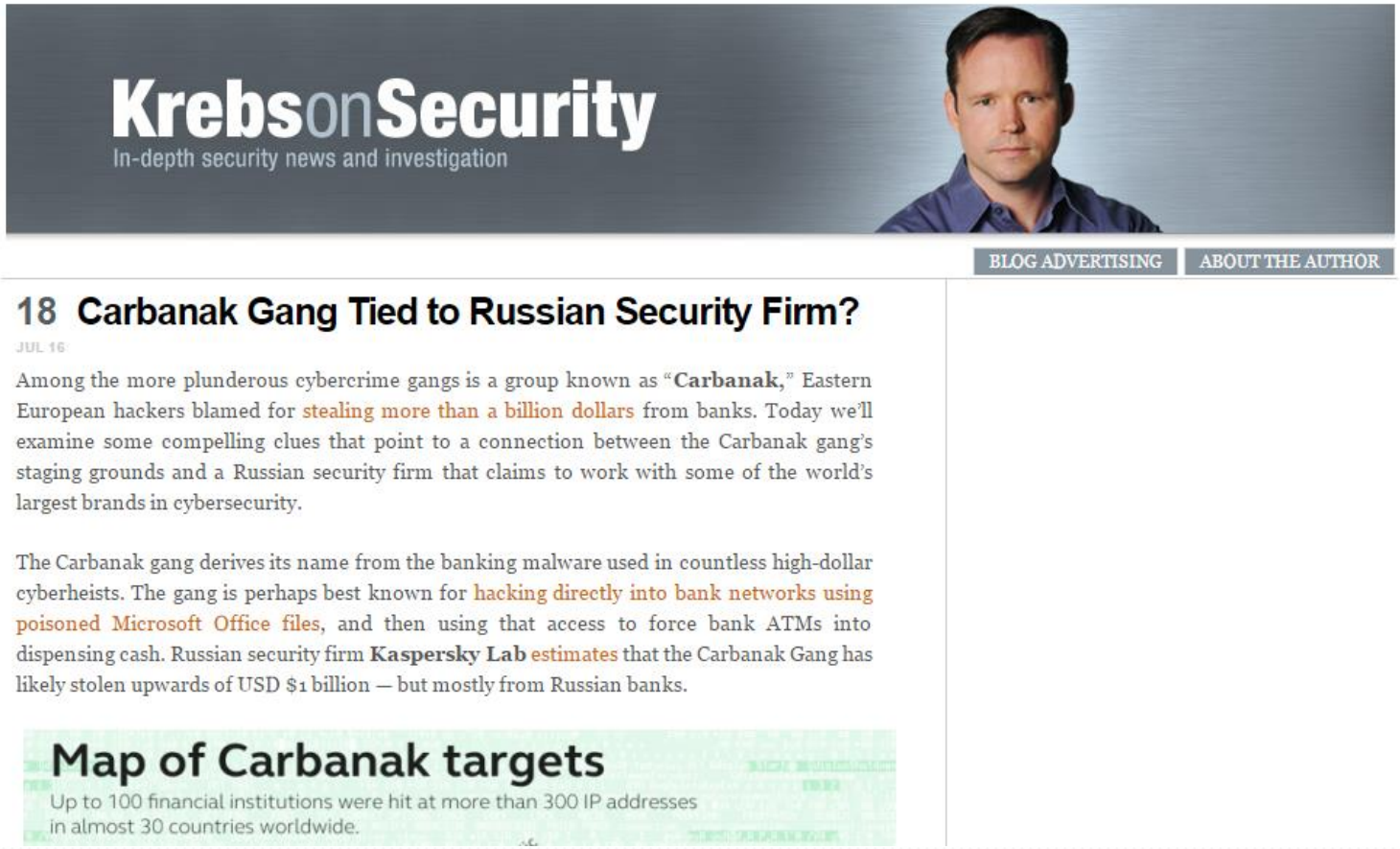
1. Влияние политических событий и международной обстановки
2. Рост конкуренции, стремление к подрыву доверия и репутации брендов
3. Рост числа атак, связанных с IoT
4. Рост роли СМИ и формируемого новостного фона

- спрос на услуги ИБ в регионах
- спрос на продукты ИБ
- спрос на специалистов
- динамичность развития

Акценты ИБ для Заказчиков:

- Этика поведения в сети Интернет, противодействие
- Этика делового общения с представителями СМИ
- Общие принципы поведения в сети Интернет
- Консультации по повышению уровня ИБ грамотности

Инцидент Brain Krebs



KrebsonSecurity
In-depth security news and investigation

BLOG ADVERTISING | ABOUT THE AUTHOR

18 Carbanak Gang Tied to Russian Security Firm?

JUL 16

Among the more plunderous cybercrime gangs is a group known as "**Carbanak**," Eastern European hackers blamed for stealing more than a billion dollars from banks. Today we'll examine some compelling clues that point to a connection between the Carbanak gang's staging grounds and a Russian security firm that claims to work with some of the world's largest brands in cybersecurity.

The Carbanak gang derives its name from the banking malware used in countless high-dollar cyberheists. The gang is perhaps best known for hacking directly into bank networks using poisoned Microsoft Office files, and then using that access to force bank ATMs into dispensing cash. Russian security firm **Kaspersky Lab** estimates that the Carbanak Gang has likely stolen upwards of USD $1 billion — but mostly from Russian banks.

Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.

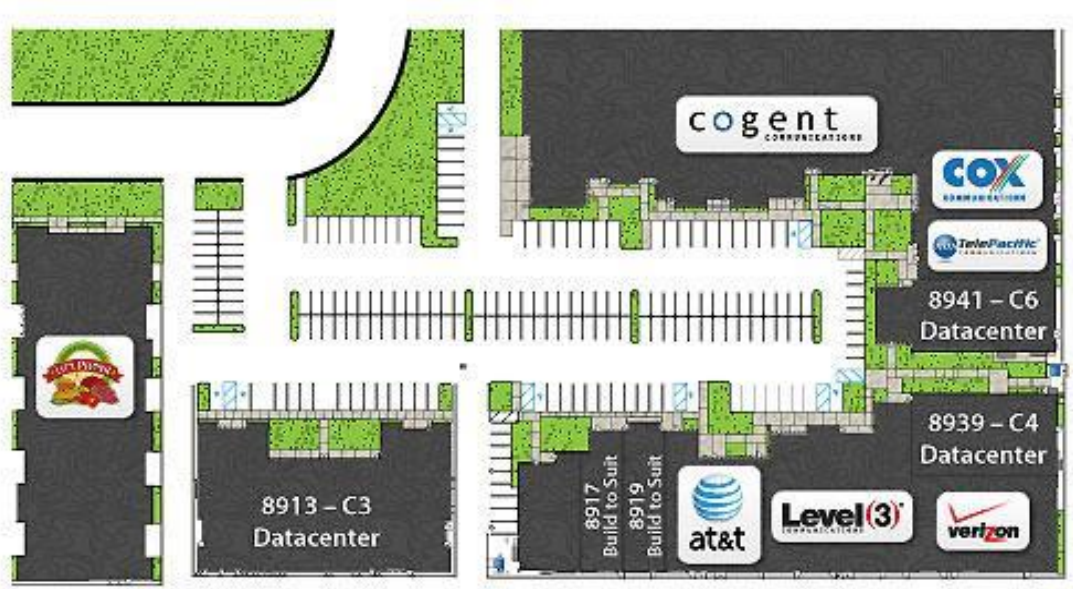
https://krebsonsecurity.com/2016/07/carbanak-gang-tied-to-russian-security-firm/

Последствия

1) атаки на почтовые и VPN-сервера, регулярное сканирование , повышенный интерес к ресурсам, вирусная активность (попытки НСД, брутфорс, DDOS-атаки);
2) репутационные риски и подрыв доверия;
3) временные и финансовые затраты компании;
4) повышение затрат на собственную безопасность;
5) применение нестандартных решений для повышения уровня безопасности сети;

Последствия

66.240.236.119 подсеть Carinet (California Regional Intranet), San Diego, CA, 92123, US



https://www.google.ru/maps/place/CARI.net/@32.8302321,-117.134722,3a,75y,148.34h,83.56t/data=!3m7!1e1!3m5!1sShcnDQbIPmSv2uy-OfTn2Q!2e0!6s%2F%2Fge00.ggpht.com%2Fcbk%3Fpanoid%3DShcnDQbIPmSv2uy-OfTn2Q%26output%3Dthumbnail%26cb_client%3Dmaps_sv.tactile.gps%26thumb%3D2%26w%3D203%26h%3D100%26yaw%3D128.85612%26pitch%3D0%26thumbfov%3D100!7i13312!8i6656!4m5!3m4!1s0x80dbffb6c6999825:0xa586f746ec0f63d7!8m2!3d32.8294871!4d-117.1336958!6m1!1e1

Пример ЦОДа Сан Диего

А что, если не противодействовать?!

Любая неосторожность при размещении информации может повлечь за собой тяжелые репутационные и финансовые последствия.

Помимо внедрения современных средств защиты информации в компаниях, нужно уделять внимание обучению собственного персонала основам поведения в сети Интернет.

Благодарим за внимание

Thank you for your time!

По вопросам и предложениям:
Кира Кирюшкина
E-mail: info@infokube.ru
Моб.: +79058615101