国际比特币洗钱 ATM 木马大盗案告破

欧洲刑警组织(Europol)透露，一个国际网络犯罪团伙通过恶意软件控制自动取款机（ATM）按其需要吐钞，从多家银行窃取了 10 多亿美元，并一直利用比特币洗钱。在来自世界各地的调查人员合作下，这位老谋深算的犯罪团伙主谋被

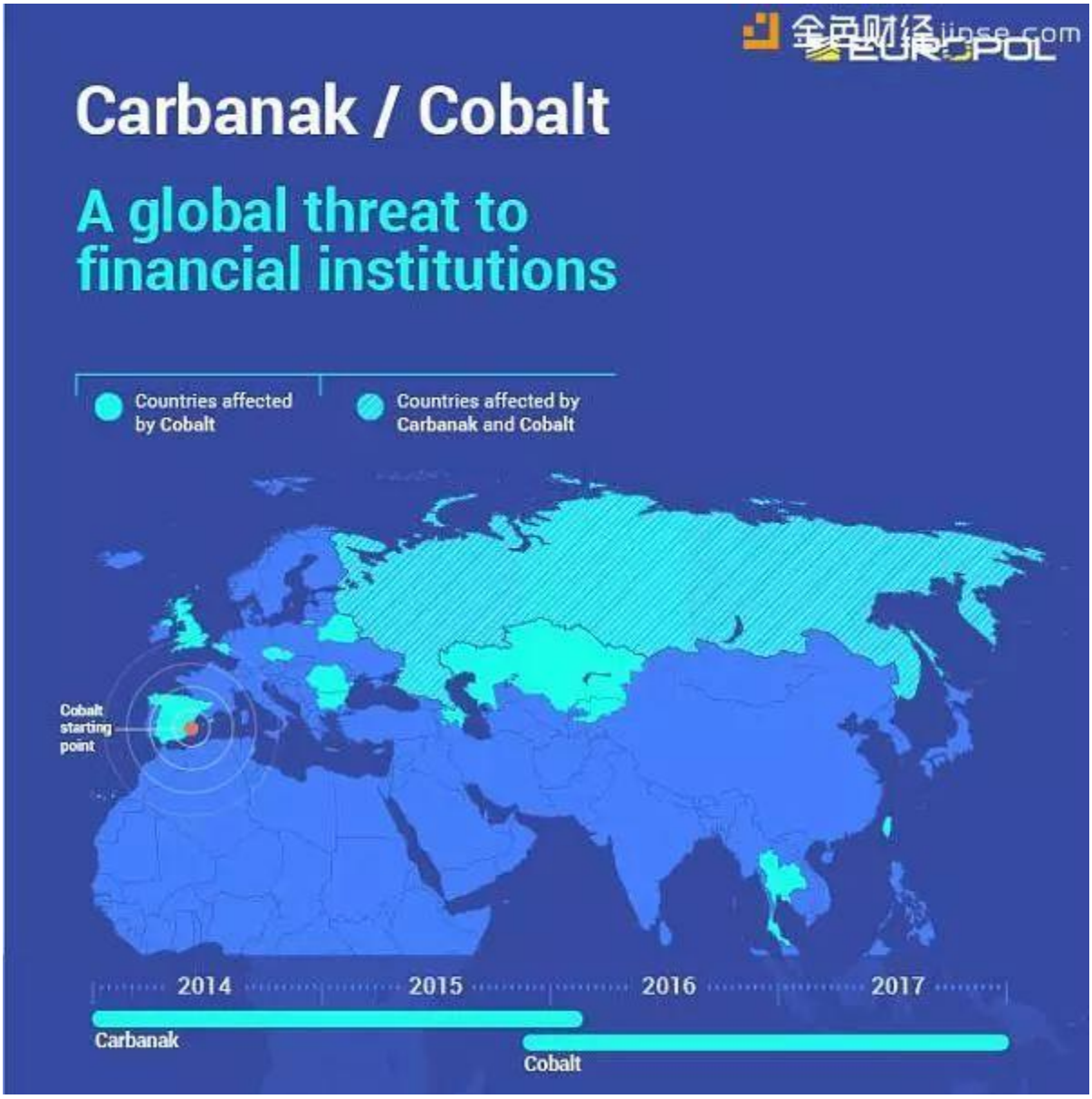
捕。

ATM 木马大盗

欧盟执法合作机构（欧洲刑警组织 Europol）本周一宣布，Carbanak 木马和 Cobalt 木马恶意袭击背后的网络犯罪团伙主谋已在西班牙被捕。这一行动得到美国联邦调查局、罗马尼亚、摩尔多瓦、白俄罗斯、台湾当局以及私营网络安全公司的支持。

在主谋的领导下，受控犯罪分子向银行员工发送带有恶意软件附件的钓鱼邮件。一旦下载，恶意软件允许犯罪分子远程控制受病毒感染的设备，使他们能够访问银行内部网络并控制受感染的自动取款机服务器。他们袭击了 40 多个国家的银行，造成总额超过 10 亿美元的损失。

他们将赃款利用加密货币洗钱，通过与加密货币钱包关联的预付卡购买豪车和豪宅等。欧洲刑警组织下属欧洲网络犯罪中心负责人 Steven Wilson 说道：“逮捕了这个犯罪集团的关键人物之后，其余网络犯罪分子也在劫难逃。”



主谋‘Denis K’

西班牙内政部透露了更多关于此案的细节，称被捕的幕后策划者被称为“Denis K.”，另外还有三名来自俄罗斯和乌克兰的黑帮成员与这名头目一同被捕。警方在一次突击搜查中查获了他们的银行账户、价值 100 万欧元的豪宅、价值 50 万欧元的珠宝以及两辆豪华轿车。

据悉，被盗战利品在俄罗斯和乌克兰的加密货币交易所转换成比特币，然后转移到他们的钱包，他们累积了约 15000 个比特币。Denis K.利用直布罗陀和英国的金融平台将比特币转入预付卡，并在西班牙消费。据称，他还建立了一个“庞大的网络”来进行比特币挖矿，以此作为洗钱手段。

EUROPOL

Carbanak / Cobalt

How it works

1 DEVELOPMENT

The cybercriminal is the brains of the operation and develops the malware

Spear-phishing emails are sent to bank employees to infect their machines

2 INFILTRATION AND INFECTION

The cybercriminal deploys the malware through the bank's internal network, infecting the servers and controlling ATMs

Bank employee

Infected infrastructure

3 HOW THE MONEY IS STOLEN

MONEY TRANSFER

The criminal transfers the money into their account or foreign bank accounts

INFLATING ACCOUNT BALANCES

The criminal raises the balance of bank accounts and money mules withdraw the money at ATMs

CONTROLLING ATMs

The criminal sends a command to specific ATMs to spit out cash and money mules collect the money

4 MONEY LAUNDERING

The stolen money is converted into cryptocurrencies

本文来源： http://www.bitecoin.com/online
