360° Ampire

КОНФЕРЕНЦИЯ КИБЕРПОЛИГОНОВ

Вместе против цифровой уязвимости

28 МАРТА 2024

Москва, Конгресс-центр МТУСИ

Миллионеры из трущоб

360° Ampire

Галкин Николай

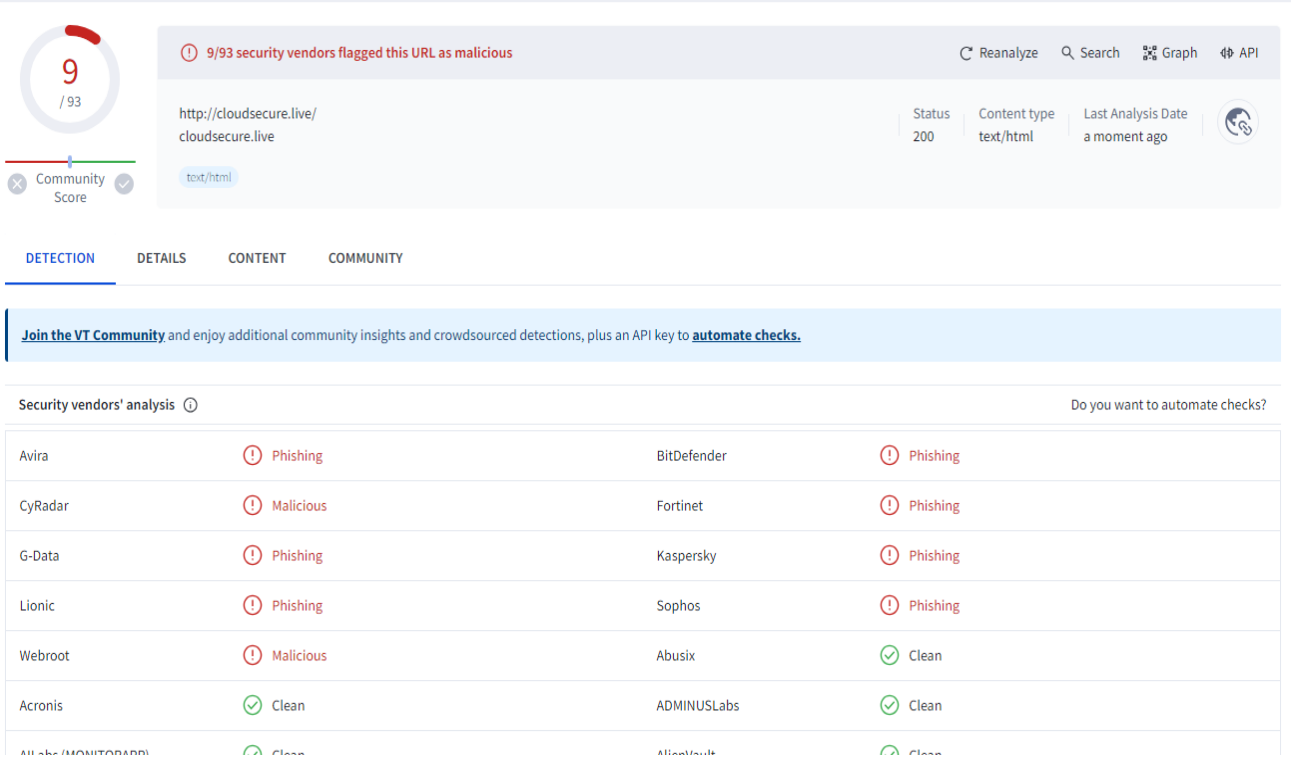
Руководитель направления **исследования киберугроз**

Хромова Анна

Руководитель направления **исследования информационного пространства**

Один домен - пять APT...

В начале 2024 года нашим клиентам начали приходить письма, содержащие фишинговую рассылку с вредоносным вложением. В каждом из данных писем фигурировал домен cloudsecure[.]live

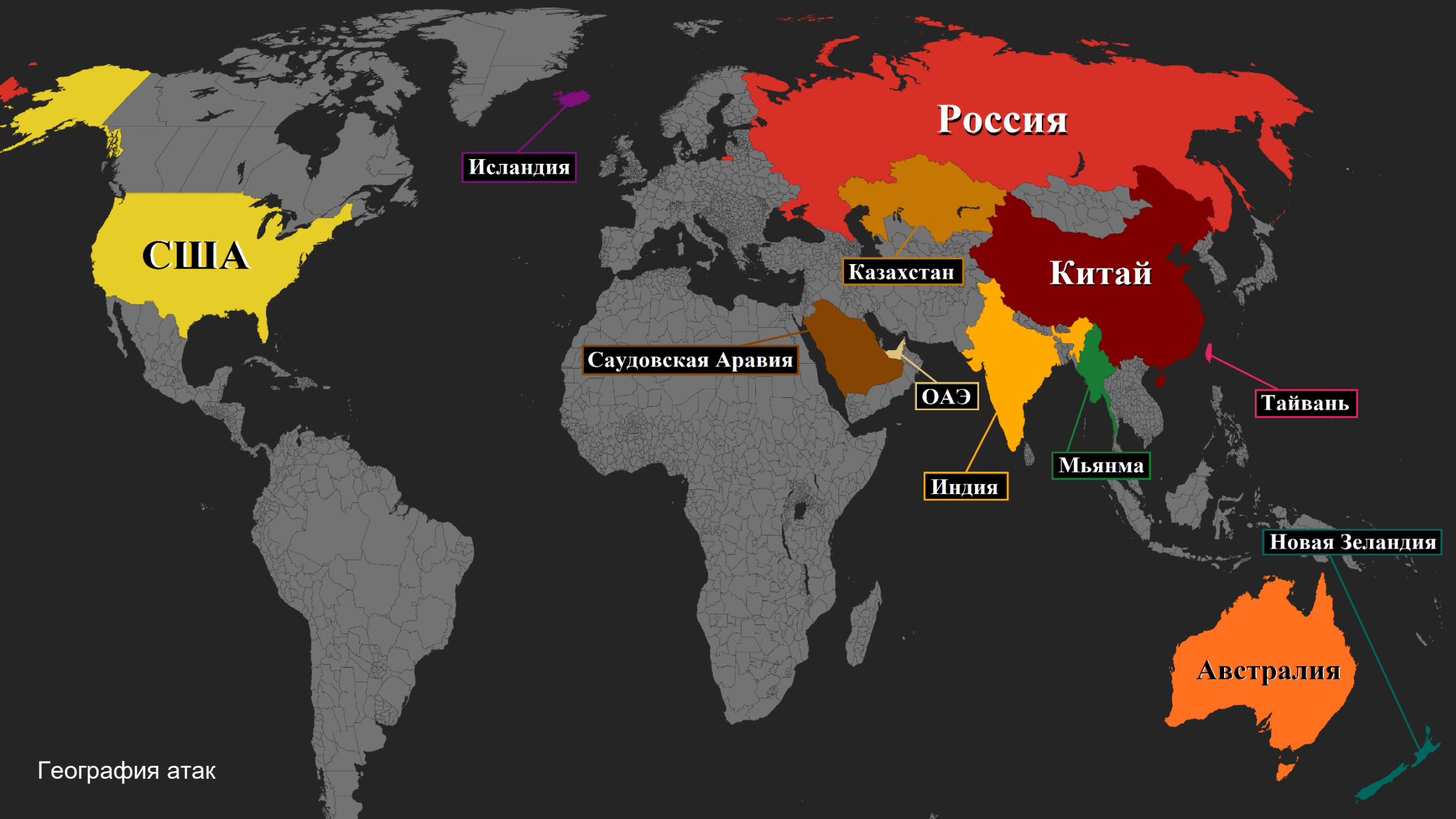


Ampire 360°

CyberRoot управляет рисками других

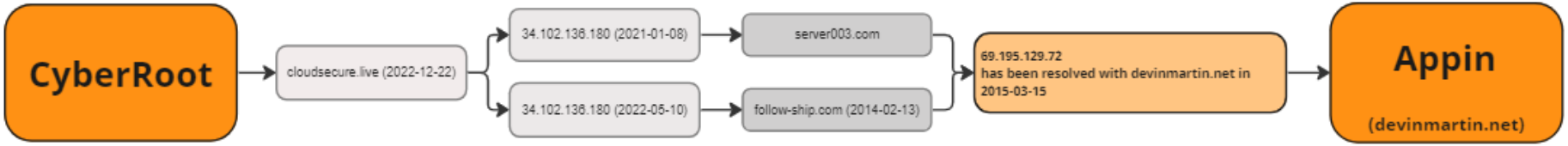
2013 г.

- Специалисты CyberRoot отслеживали в социальных сетях пользователей, представляющих для них интерес.
- Они анализировали ключевые характеристики аккаунтов подписчиков и родственников этих пользователей, а затем создавали собственные учетные записи, максимально похожие на них.


Исландия
США
Россия
Казахстан
Китай
Саудовская Аравия
ОАЭ
Индия
Мьянма
Тайвань
Новая Зеландия
Австралия
География атак

Ampire 360°

CyberRoot управляет рисками других




```
rule UPX_Packer
{
    meta:
        sid = "901871"
        description = "Обнаружены следы упаковщика UPX"
        reference = "cujo.com/blog/upx-anti-unpacking-techniques-in-iot-malware/"
        techniques = "T1027.002"
    strings:
        $s1 = { 31 2E 32 3? 00 55 50 58 }
        $s2 = { 32 2E 30 30 00 55 50 58 }
        $s3 = { 60 BE ?? ?? ?? ?? 8D BE ?? ?? ?? ?? 57 89 E5 8D 9C }
        $s4 = { 90 61 BE ?? ?? ?? ?? 8D BE ?? ?? ?? ?? 57 83 CD FF }
        ...
        $45 = { 60 E8 ?? ?? ?? ?? 58 83 E8 3D 50 8D B8 FF 57 8D B0 }
        $46 = { 66 C7 05 ?? ?? ?? 00 75 07 E9 ?? FE FF FF }
    condition:
        uint16(0) == 0x5A4D and for any of ($*) : ( $ at pe.entry_point )
}
```

BellTroX и DarkBasin – вор вору двоюродный брат

2013 г.

Руководитель: Сумит Гупта

Information Security Consultant
BellTroX D|G|TAL Security (P) Ltd
янв. 2012 г. – настоящее время · 12 лет 3 мес.
New Delhi Area, India

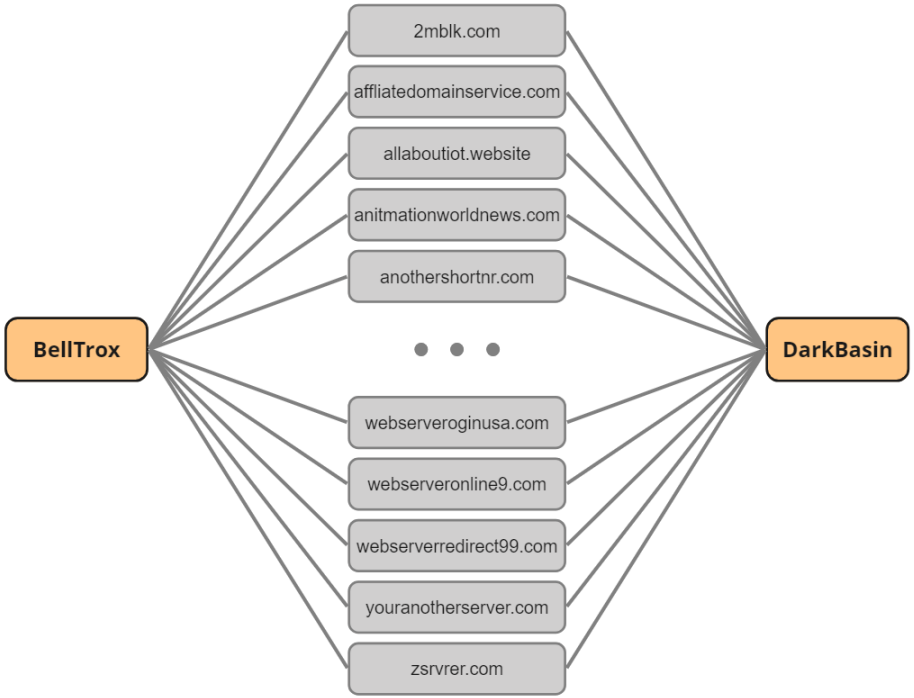
We are engaged in providing Cyber Intelligence Service.
At Cyber Intelligence Division of BellTroX D|G|TAL Security (P) Ltd. we understand the needs of companies and how internal and external issues can dramatically impact the bottom line and risks to your company...

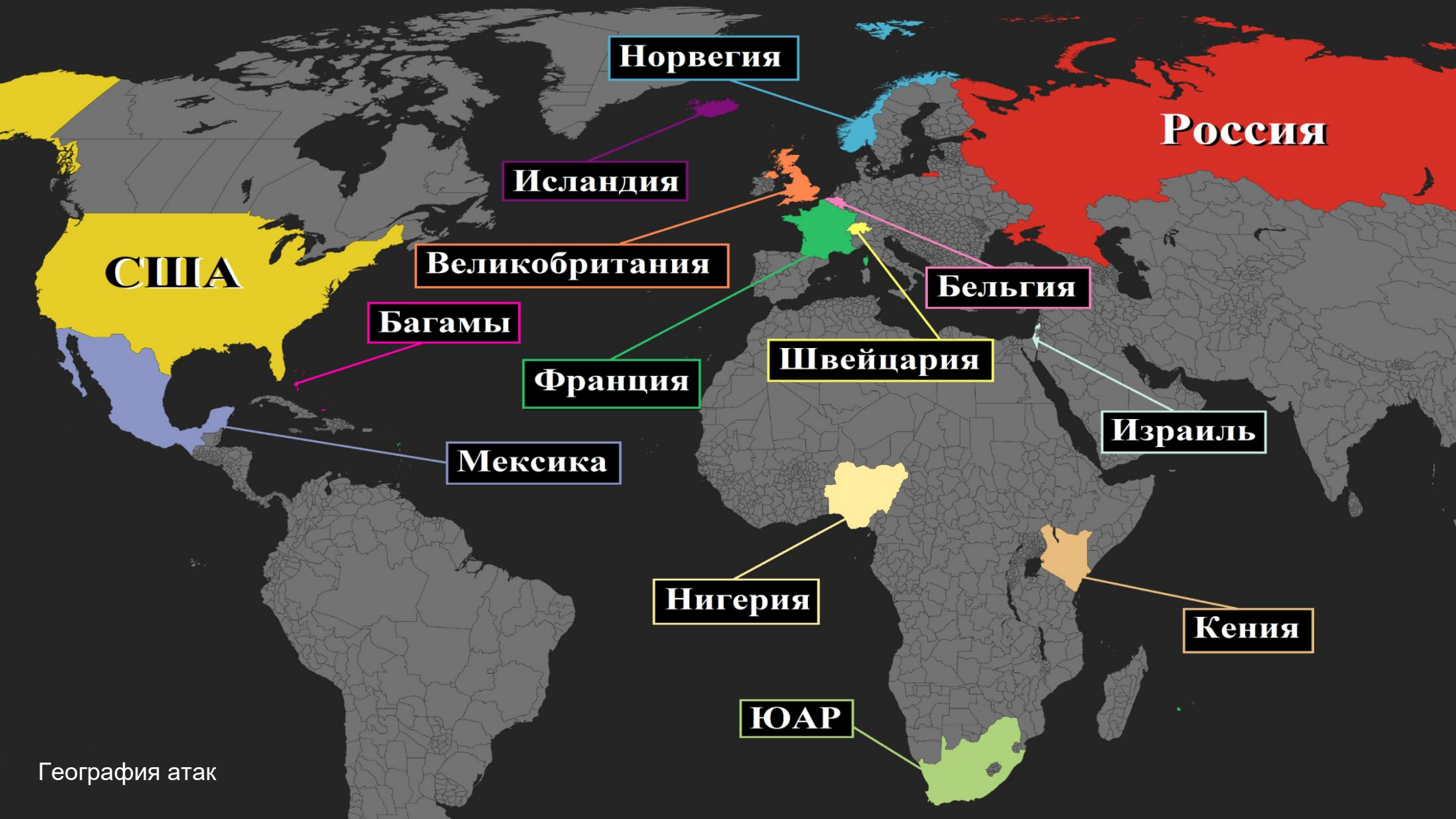
Some of the services we offer are:

For Private Investigators:-
Email Interception Services
Computer Interception Services
Phone Interception Services
Computer Forensics
Mobile Forensics
Email Forensics
Data Leakage Investigation

Other Professional Services are :-
Corporate Espionage Investigation
Competitive Intelligence
Due Diligence
Executive Vetting
Mergers & Acquisitions Intelligence
Money laundering Investigation
Business Partner Vetting
Customer-Supplier Vetting
Data Theft Investigation
Civil Investigation
Criminal Investigation
Social Engineering Awareness Assessment

BellTroX и DarkBasin – вор вору двоюродный брат





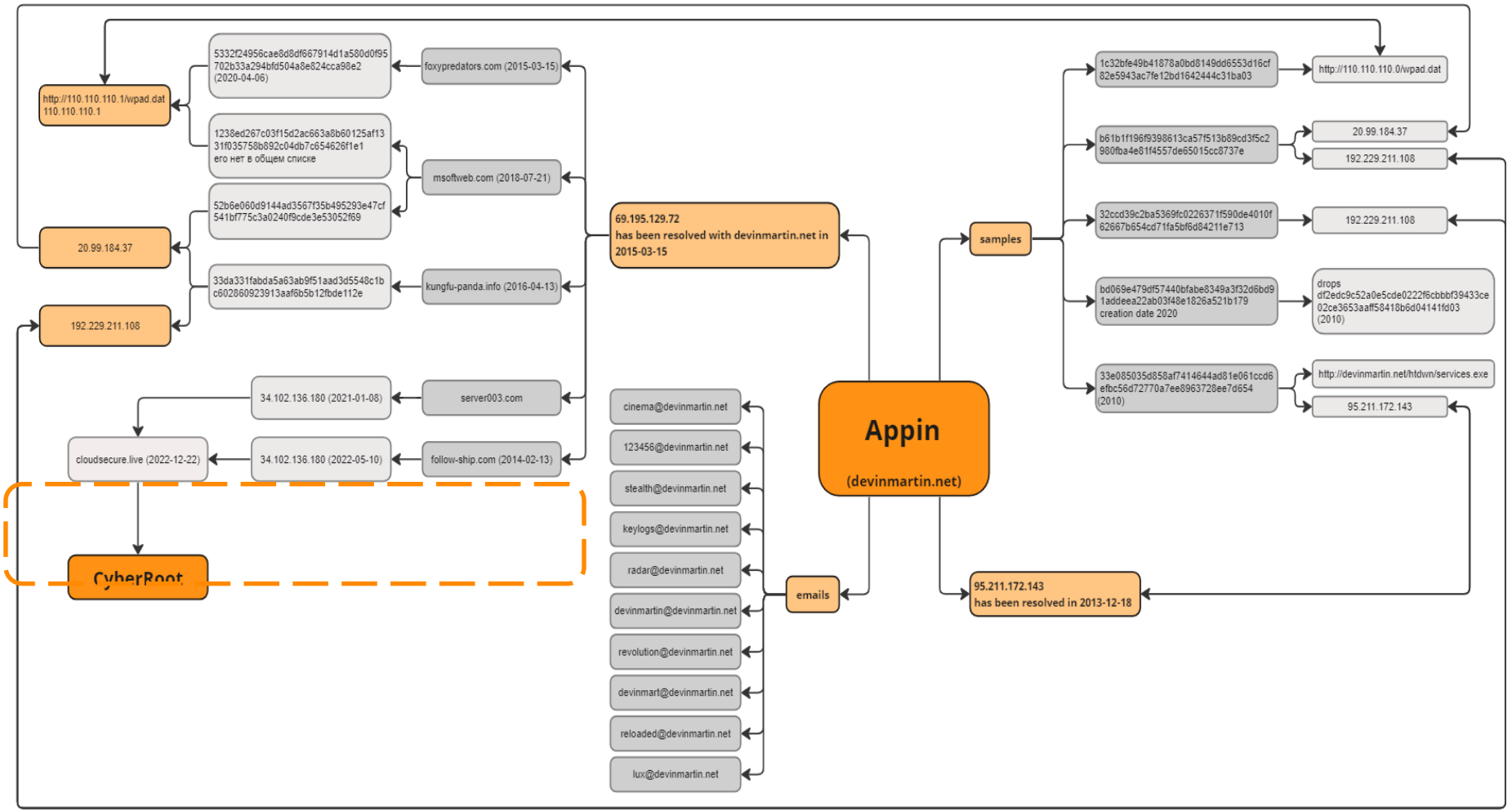
География атак

Троянский слон

Ampire 360°

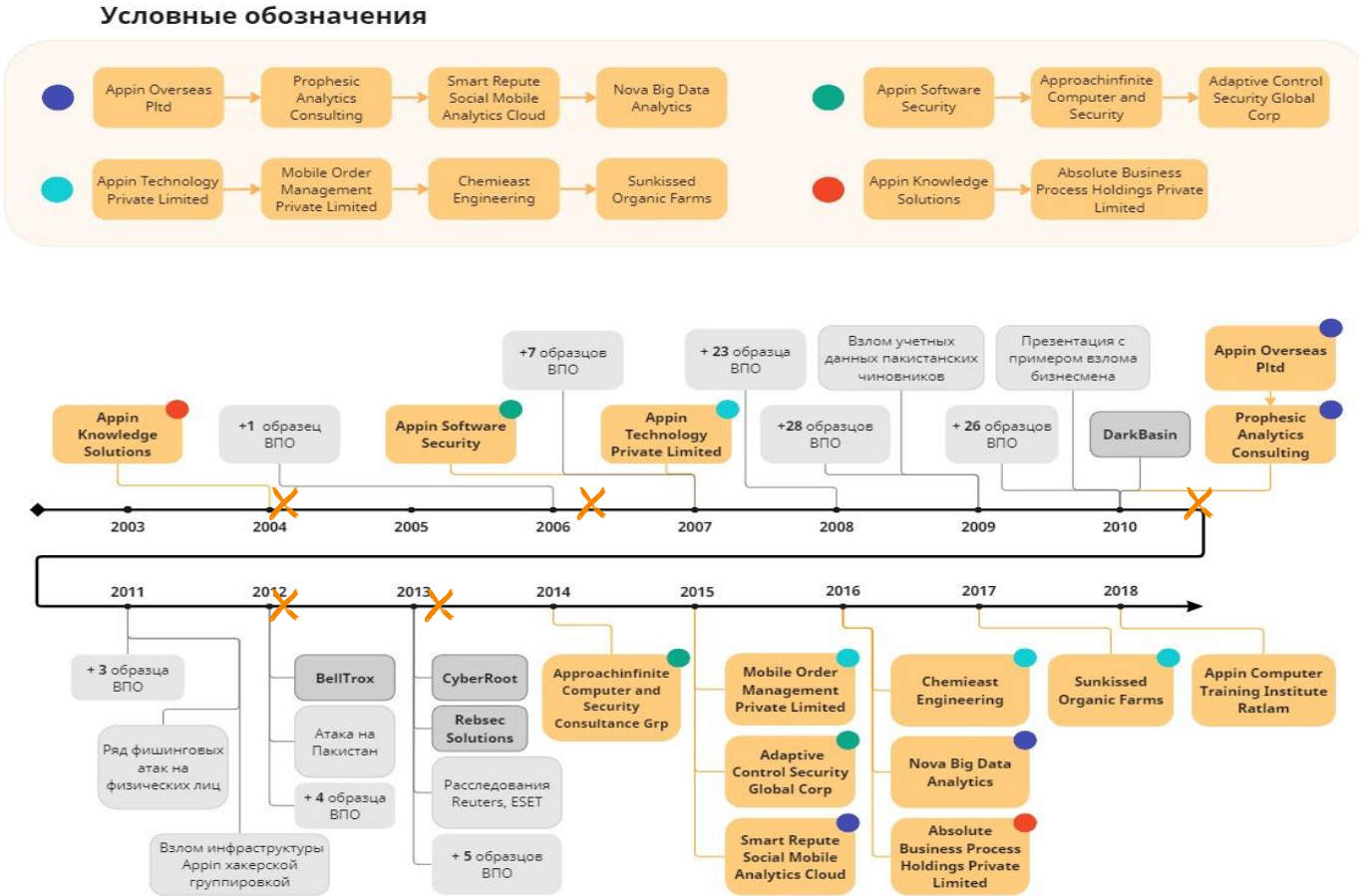
Организация Appin задумывалась как образовательный стартап, который вскоре стал международной франшизой.

В 2011 году после взлома их инфраструктуры хакерской группировкой Tigers of Indian Cyber была опубликована информация о вредоносной деятельности компании.


Appin
(devinmartin.net)
69.195.129.72
has been resolved with devinmartin.net in 2015-03-15
95.211.172.143
has been resolved in 2013-12-18
samples
emails
http://110.110.110.1/wpad.dat
110.110.110.1
20.99.184.37
192.229.211.108
cloudsecure.live (2022-12-22)
CyberRoot
5332f24956cae8d8df667914d1a580d0f95702b33a294bfd504a8e824cca98e2
(2020-04-06)
foxypredators.com (2015-03-15)
1238ed267c03f15d2ac663a8b60125af1331f035758b892c04db7c654626f1e1
его нет в общем списке
msoftweb.com (2018-07-21)
52b6e060d9144ad3567f35b495293e47cf541bf775c3a0240f9cde3e53052f69
33da331fabda5a63ab9f51aad3d5548c1bc602860923913aaf6b5b12fbde112e
kungfu-panda.info (2016-04-13)
34.102.136.180 (2021-01-08)
server003.com
34.102.136.180 (2022-05-10)
follow-ship.com (2014-02-13)
cinema@devinmartin.net
123456@devinmartin.net
stealth@devinmartin.net
keylogs@devinmartin.net
radar@devinmartin.net
devinmartin@devinmartin.net
revolution@devinmartin.net
devinmart@devinmartin.net
reloaded@devinmartin.net
lux@devinmartin.net
1c32bfe49b41878a0bd8149dd6553d16cf82e5943ac7fe12bd1642444c31ba03
http://110.110.110.0/wpad.dat
b61b1f196f9398613ca57f513b89cd3f5c2980fba4e81f4557de65015cc8737e
20.99.184.37
192.229.211.108
32ccd39c2ba5369fc0226371f590de4010f62667b654cd71fa5bf6d84211e713
192.229.211.108
bd069e479df57440bfabe8349a3f32d6bd91addeea22ab03f48e1826a521b179
creation date 2020
drops
df2edc9c52a0e5cde0222f6cbbbf39433ce02ce3653aaff58418b6d04141fd03
(2010)
33e085035d858af7414644ad81e061ccd6efbc56d72770a7ee8963728ee7d654
(2010)
http://devinmartin.net/htdwn/services.exe
95.211.172.143

Таймлайн развития Appin

Ampire 360°



Ampire 360°

Продолжение следует... Rebsec?

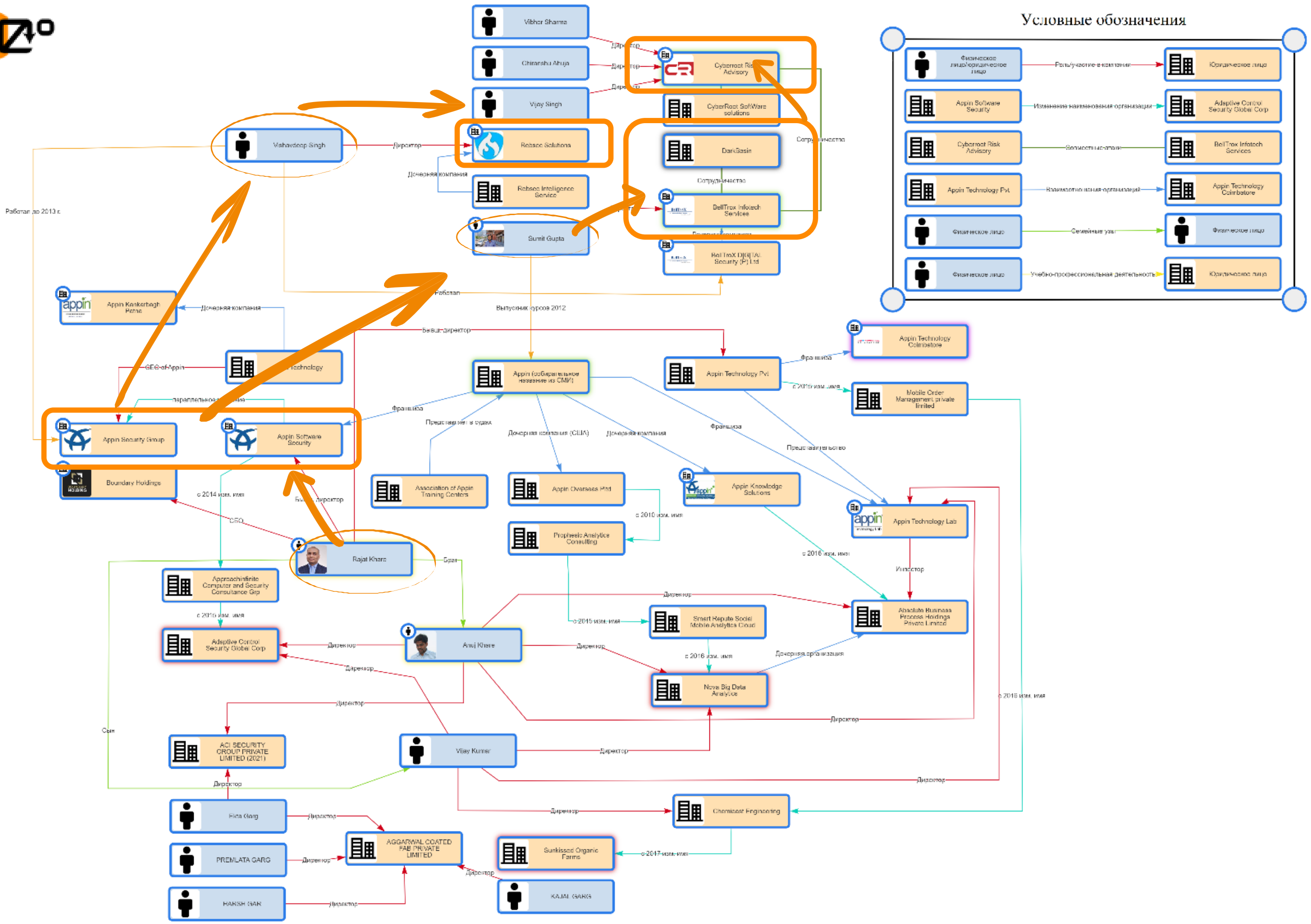
LinkedIn India
https://in.linkedin.com › vish... · Перевести эту страницу

Vishavdeep Singh - Amritsar, Punjab, India

Vishavdeep Singh. Entrepreneur. Amritsar, Punjab, India. 218 followers 222 ... **Rebsec** Services. CEO at **Rebsec**. Amritsar · Connect · Rahul kumar. Deputy Manager in ...

Генеральный директор: Вишавдип Сингх, ранее работал в BellTroX и Appin

Ampire 360°



Условные обозначения
Vibhor Sharma
Chiranshu Ahuja
Vijay Singh
Vishavdeep Singh
Robsec Solutions
Robsec Intelligence Service
Sumit Gupta
Cyberroot Risk Advisory
CyberRoot SoftWare solutions
DarkBasin
BellTrox Infotech Services
Appin Technology Pvt
Appin Technology Coimbatore
Mobile Order Management private limited
Appin Security Group
Appin Software Security
Boundary Holdings
Rajat Khare
Association of Appin Training Centers
Appin Overseas Pvt
Appin Knowledge Solutions
Appin Technology Lab
Prophecis Analytics Consulting
Adaptive Control Security Global Corp
Anuj Khare
Smart Repute Social Mobile Analytics Cloud
Nova Big Data Analytics
Absolute Business Process Holdings Private Limited
ACI SECURITY GROUP PRIVATE LIMITED (2021)
Vijay Kumar
Ritu Garg
PREMLATA GARG
HARSH GARG
AGGARWAL COATED FAB PRIVATE LIMITED
Sunkissed Organic Farms
KAJAL GARG
Chemicast Engineering
Физическое лицо
Юридическое лицо
Работал до 2013 г.
Выпускник курсов 2012
Франшиза
Директор
Брат
Сын

360° Ampire

Благодарим за внимание!