G-Bundle Finance

Высокотехнологичная защита финансовых организаций от современных киберугроз

Гогуа Шалва

Директор по работе с партнерами в РФ и СНГ

GROUP-IB СЕЙЧАС

НАША КОМПАНИЯ В ЦИФРАХ:

1,300+
высокотехнологичных расследований по всему миру

600+
специалистов и разработчиков

450+
защищенных клиентов по всему миру

60
стран присутствия

11
ключевых сервисов

6
продуктов

120+
патентов

4
региона с исследовательскими центрами

Singapour, UAE, Russia, Netherlands

ГЛОБАЛЬНОЕ ПАРТНЕРСТВО:

INTERPOL

EUROPOL

ПРИЗНАНИЕ ВЕДУЩИМИ МИРОВЫМИ ЭКСПЕРТАМИ:

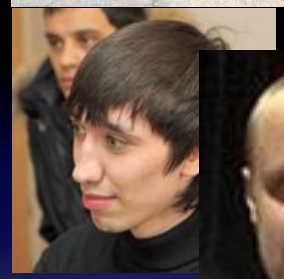
FORRESTER® IDC Gartner

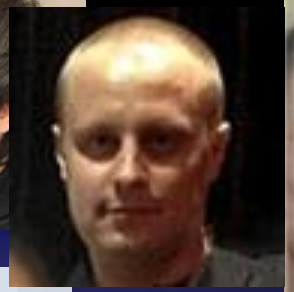
kuppingercole ANALYSTS

FROST & SULLIVAN

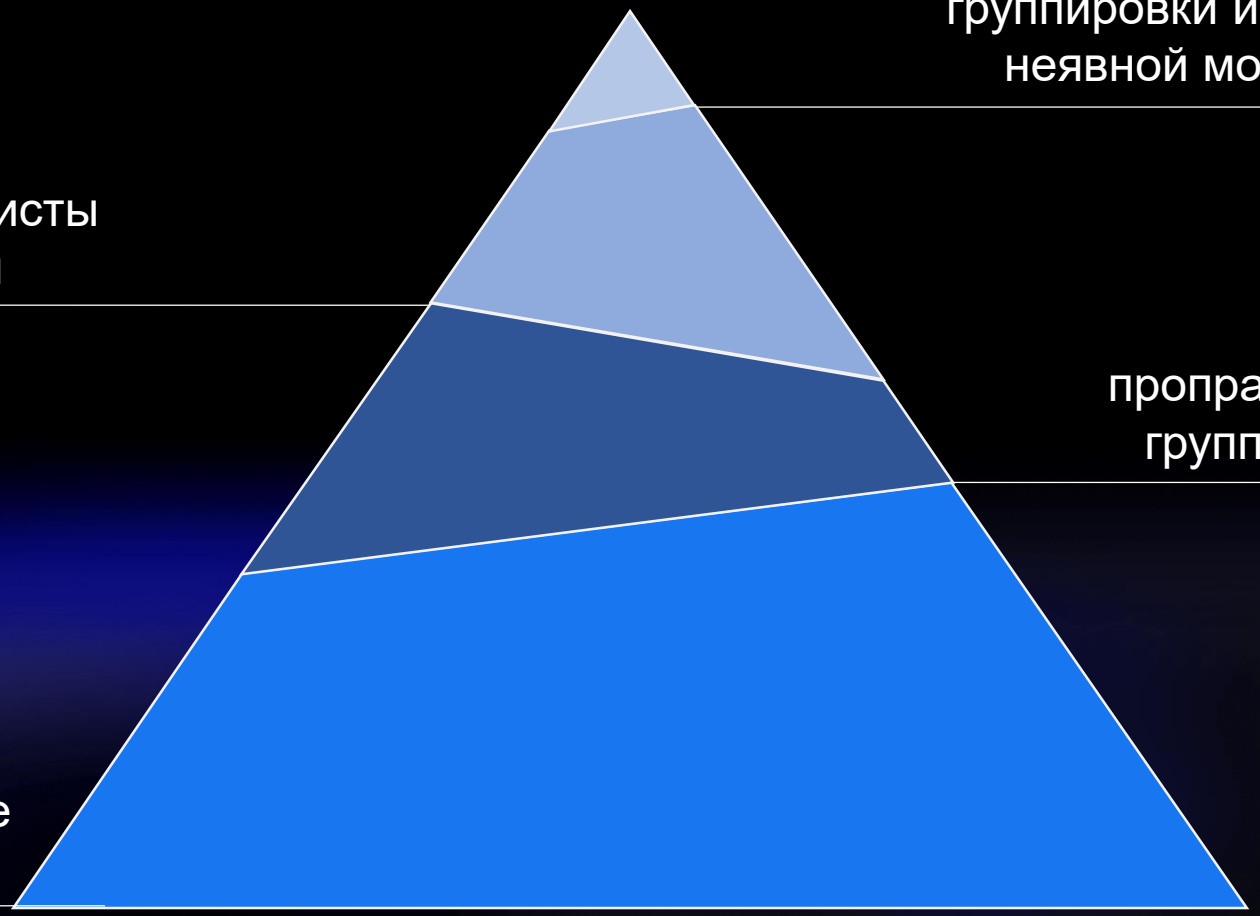
Киберпреступность сегодня

ЛИЦО КИБЕРПРЕСТУПНОСТИ



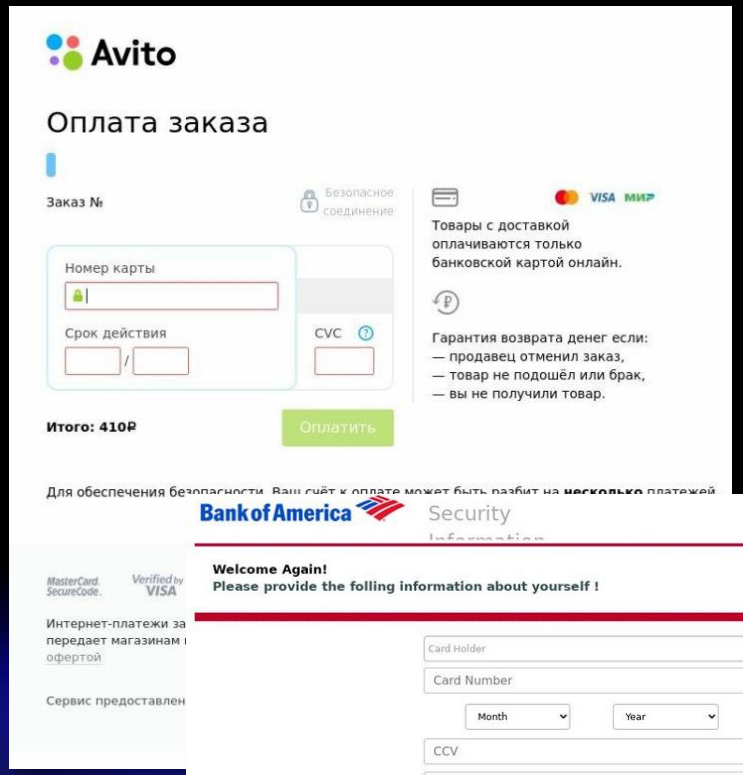


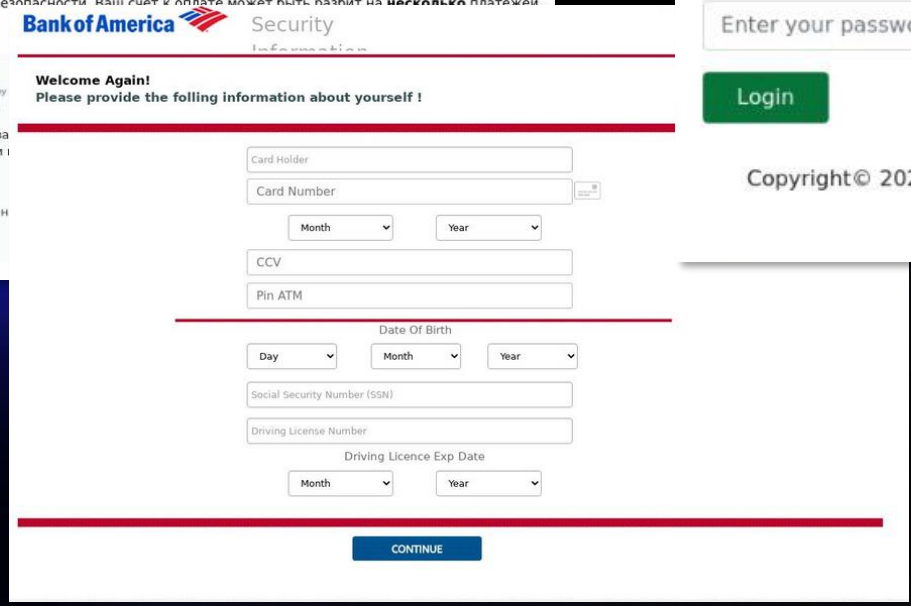
МОТИВАЦИЯ

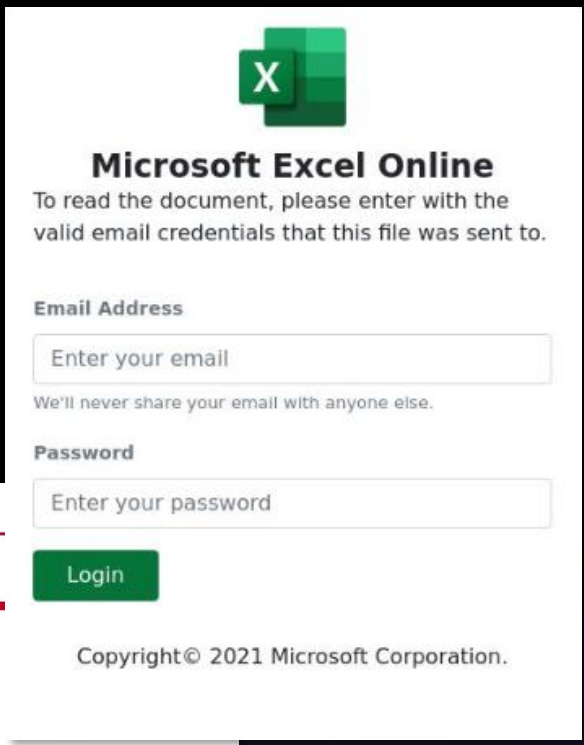

группировки и хакеры с неявной мотивацией
кибертеррористы и хактивисты
проправительственные группировки и хакеры
финансово мотивированные киберпреступники

ВЕБ-ФИШИНГ И СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

- Одноразовые ссылки
- Блокировка по User-agent
- Блокировка по регионам
- Блокировка по подсетям
- Редиректы на официальные сайты







ПЕРСОНАЛЬНАЯ МОШЕННИЧЕСКАЯ ССЫЛКА

https://yeahphones.site/**s10xs/dns/?osv=**Windows**%**2010.0**&isp=**GARS**%**20Telecom**&ip=**111.107.142.11 **&key=ey**
J0aW1lc3RhbXAiOiIxNTU0Mzg4MjYzIiwiaGFzaCI6IjIwZGQwM2I2Y2UxMDI1NzJhZWY1NDM0MTZhNzZjODY2ZjIy
YzZmZDgifQ%3D%3D&td=7ktpj.bemobtrk.com&bemobdata=c%3D227bad15-b386-42e0-911b-
674575ed6cd8..a%3D0..b%3D0..e%3D1554388262666418..c1%3D9627..c2%3D9254..c3%3D1554388262666418..r
%3D**https**%253A%252F%252Futarget.ru%252F**goto**%252F9254%252F44db6ebf9c%252F#

key={"timestamp":"1554388263",
"hash":"20dd03b6ce102572aef543416a76c866f22c6fd8"}
- в кодировке **base64**

Снижается вероятность обнаружения

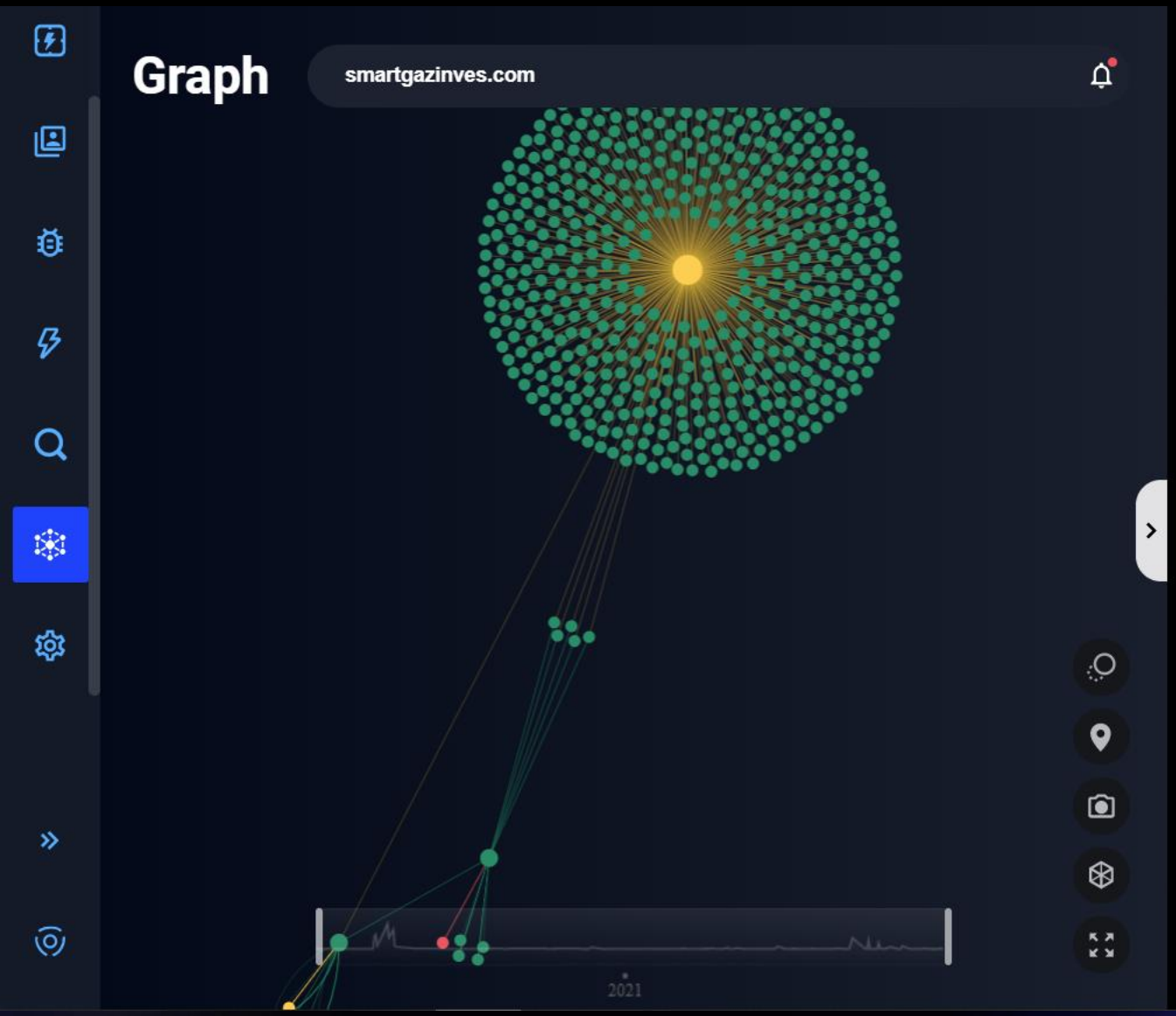
Затрудняется процесс реагирования

Большее время работы ресурса

Большее количество жертв

Ссылка работает только один раз и только у одного конкретного пользователя

КАК ЭТО ВИДИТ GROUP-IB



Nodes details

Domains 535 | IP 3 | SSL 5 | SSH 1 | Contacts 2 | Attribution 1

Sort by: Domain | Registrar | Reg date | Exp date | E-mail | IP

Registrar date 2021.06.27 — Exp date 2022.06.27

Domain name	Registrar
hotprices.in.ua	uadrs

IP-address	E-mail	Owner
185.179.189.164	svetl01211@gmail.com	service online llc

Registrar date 2021.05.21 — Exp date 2022.05.21

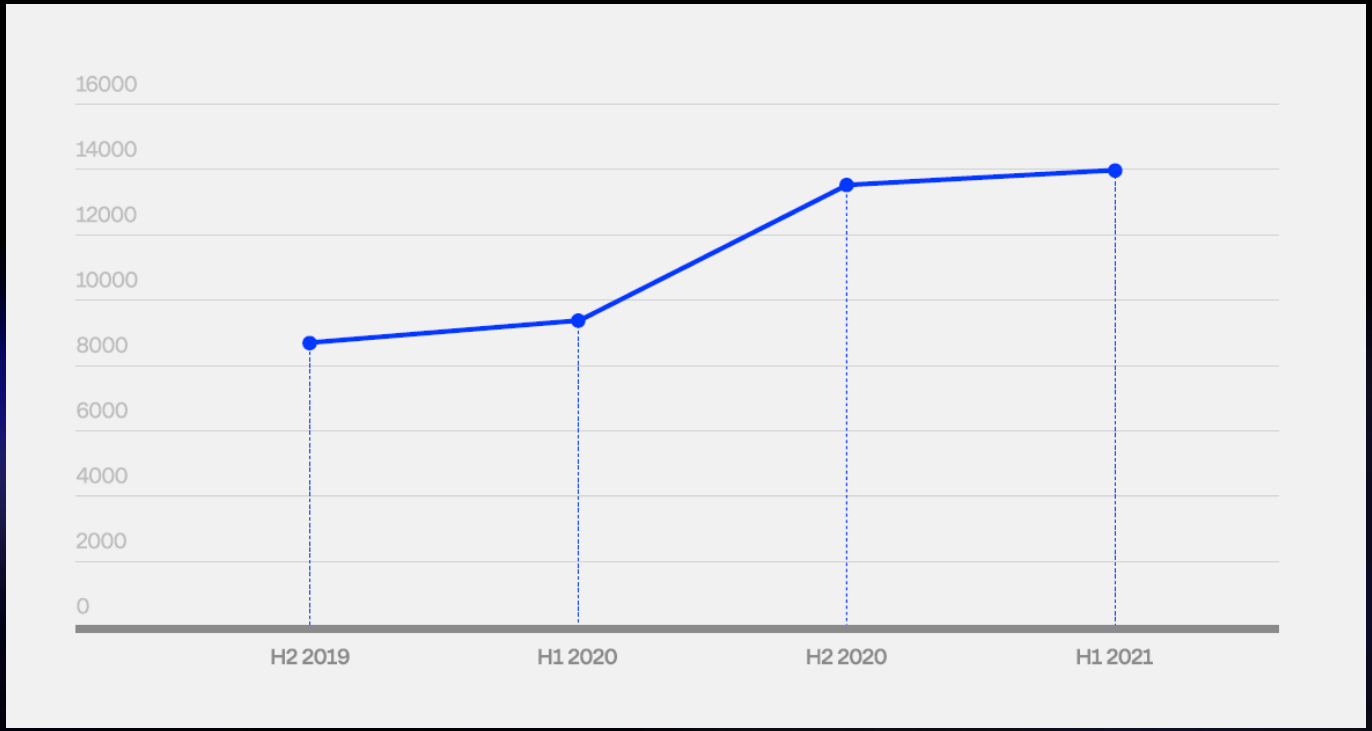
Domain name	Registrar
oshamiv.in.ua	uadrs

IP-address	E-mail	Owner
185.68.16.232	svetl01211@gmail.com	service online llc

МАСШТАБ

27 000

Уникальных фишинговых доменов
было заблокировано CERT-GIB в 2021



JS-СНИФФЕРЫ

96 СЕМЕЙСТВ JS-СНИФФЕРОВ ОБНАРУЖЕНО

1 ГОС ГРУППА ИСПОЛЬЗУЕТ JS-СНИФФЕРЫ

19 РЕТЕЙЛ КОМПАНИЙ СКОМПРОМЕТИРОВАННО

Получение доступа к сайту → Получение сниффера → Установка сниффера → Монетизация

КАРДИНГ

	Text data	Dumps
Total number	28 296 585 ↑	63 788 590 ↑
Market volume	$361 684 617 ↑	$1 540 043 892 ↑
Lowest price	$0.1 ↓	$0.25 ↓
Highest price	$150	$500
Average price	$12.78 ↓	$21.88 ↓

На $1,02 млрд
вырос общий рынок кардинга

На 22,7 млн
выросло количество продаваемых дампов

На 15,8 млн
выросло количество продаваемых текстовых данных

ШИФРОВАЛЬЩИКИ – УГРОЗА №1

Тренды

- Партнерские программы
- Первичное проникновение – фишинг, RDP, уязвимости в публичных приложениях
- Использование разнообразных троянов для удаленного доступа
- Хищение важных данных, угрожая их публикацией

КАРТА СОЮЗОВ

кооперация операторов шифровальщиков
и распространителей вредоносных программ

TRICKBOT	QAKBOT	DRIDEX	SDBBOT
Ryuk Conti REvil RansomExx	ProLock Egregor DoppelPaymer	DoppelPaymer	ClOp

ZLOADER	ICEDID	BUER	BAZAR
Ryuk Egregor	RansomExx Maze Egregor	Maze Ryuk	Ryuk

1

Refresh

INFO

Company: 1

Description: 1

FILES

Linux

Windows

Show builds

PAYMENT INFO

$ [redacted]

Paid: $ 0

Pending: $ 0

Remaining to pay

[redacted] BTC (+20%) Rate: $ [redacted]

[redacted] XMR Rate: $ [redacted]

Fixed rate:

Enable BTC:

Enable XMR:

Not paid

Transactions [0]

BOTS STATISTIC

0	0 (0%)	0	0 GB	0	0
Bots	With reports	Summary files	Summary size	Windows	Linux

Search...

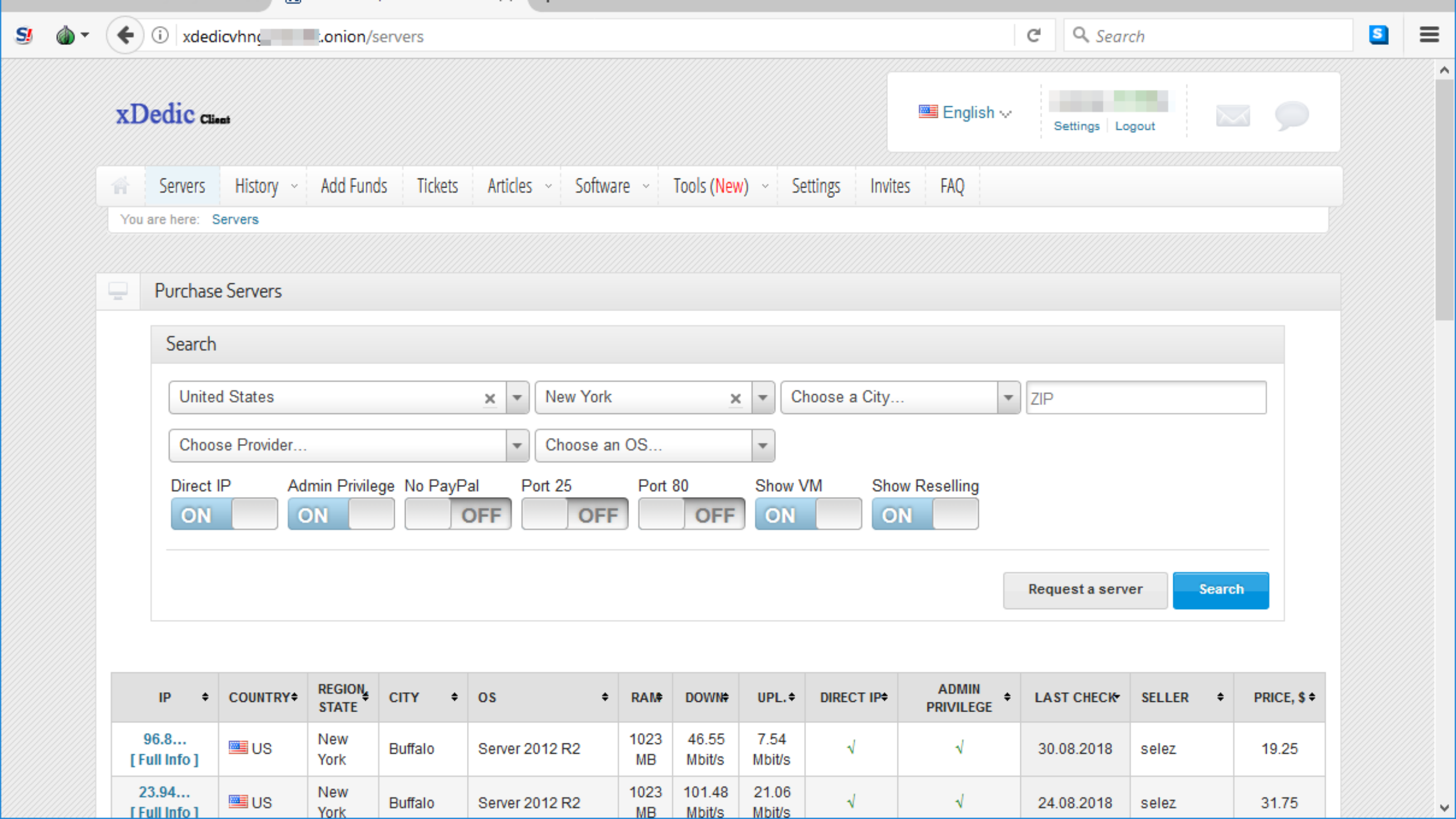
All

Bots not found

LANDING INFO

Discount price: 10 days , 00:00:00 (not launched)

User status: Offline


xdedicvhn[redacted].onion/servers
Search
xDedic Client
English
Settings
Logout
Servers
History
Add Funds
Tickets
Articles
Software
Tools (New)
Settings
Invites
FAQ
You are here: Servers
Purchase Servers
Search
United States
New York
Choose a City...
ZIP
Choose Provider...
Choose an OS...
Direct IP
ON
Admin Privilege
ON
No PayPal
OFF
Port 25
OFF
Port 80
OFF
Show VM
ON
Show Reselling
ON
Request a server
Search
IP
COUNTRY
REGION, STATE
CITY
OS
RAM
DOWN
UPL.
DIRECT IP
ADMIN PRIVILEGE
LAST CHECK
SELLER
PRICE, $
96.8... [Full Info]
US
New York
Buffalo
Server 2012 R2
1023 MB
46.55 Mbit/s
7.54 Mbit/s
√
√
30.08.2018
selez
19.25
23.94... [Full Info]
US
New York
Buffalo
Server 2012 R2
1023 MB
101.48 Mbit/s
21.06 Mbit/s
√
√
24.08.2018
selez
31.75

ТЕХНОЛОГИИ GROUP-IB

Задачи G-Bundle Finance:

Обнаружить и остановить сложную целевую атаку

Оценить защищенность и усилить команду

Обнаружить утечку данных или угрозы в Darkweb

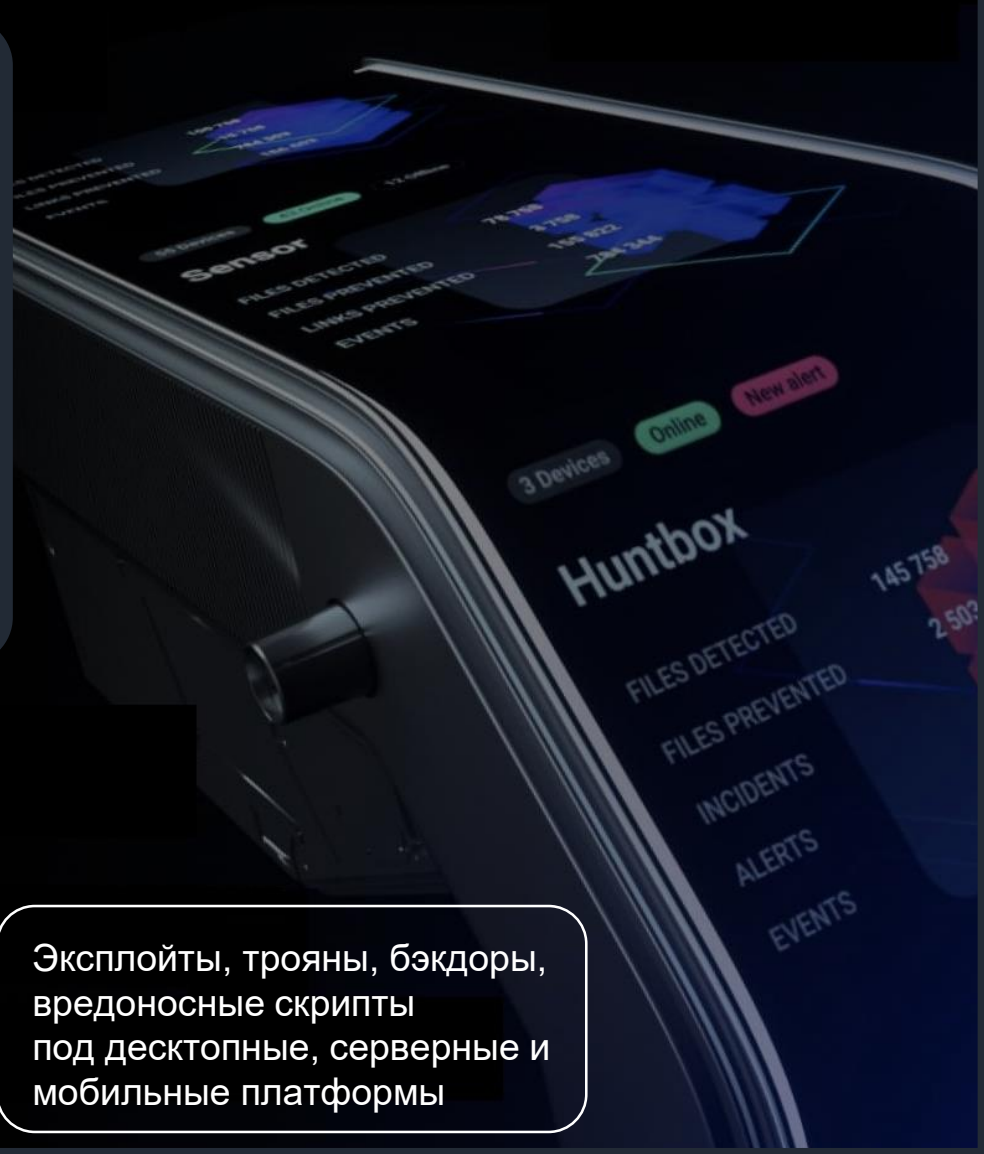
Защитить клиентов и корпоративные порталы

Group-IB Threat Hunting Framework

Система для обнаружения и остановки целевых атак, которые могут привести к утечке данных.

В бандл вошли следующие разделы Group-IB THF:

- **Sensor –** сетевой анализ трафика с возможностью автоматической блокировки вредоносного ПО (до 250 Мбит/с);
- **Polygon Cloud –** детонация вредоносного ПО в изолированной среде (до 4000 файлов);
- **CERT-GIB Monitoring –** мониторинг средствами Group-IB.



Group-IB THF предотвращает:

- Угрозы нулевого дня
- Шифровальщики
- Бестелесные угрозы
- Скрытые каналы передачи данных
- Эксплойты, трояны, бэкдоры, вредоносные скрипты под десктопные, серверные и мобильные платформы

CERT-GIB

CERT-GIB (Computer Emergency Response Team) — центр круглосуточного реагирования на инциденты информационной безопасности

- Мониторим появление фишинговых ресурсов и распространение вредоносного ПО
- Оперативно блокируем опасные сайты в доменах .RU, .РФ, и еще более чем 2500 доменных зон
- Оказываем профессиональную поддержку от специалистов Group-IB с многолетним опытом реагирования на киберинциденты
- Работаем по всему миру через сеть партнеров, контакты с хостинг-провайдерами и регистраторами доменных имен

Компетентная организация Координационного центра национального домена сети Интернет и Фонда развития интернета

Аккредитованный член международных сообществ FIRST и Trusted Introducer

Член организации OIC-CERT (Organisation of The Islamic Cooperation — Computer Emergency Response Teams)

Партнер IMPACT – международного партнерства по противодействию киберугрозам

Авторизован Университетом Карнеги-Меллон, официально использует торговую марку CERT

Group-IB Threat Intelligence & Attribution

Система для исследования и атрибуции кибератак и обнаружения признаков утечки данных в уникальных закрытых источниках.

В бандл вошли следующие разделы Group-IB TI&A:

- **Dark web** – раздел, содержащий сведения о готовящейся атаке, предложения услуг инсайдеров, обсуждения релевантных вредоносов, уязвимостей и т.п. на андеграундных площадках;
- **Скомпрометированные аккаунты** – раздел с информацией об утекших в результате работы вредоносного ПО или фишинговых страниц логинов и паролей, которые могут использоваться для доступа к сервисам организации и реализации атак;
- **Скомпрометированные банковские карты** – текстовые данные или “дампы” магнитных полос карточек, в том числе сотрудников и клиентов компании. А также данные о том, как произошла утечка: через зараженный POS-терминал, атакованный онлайн-магазин или фишинговую страницу.

Group-IB Fraud Hunting Platform

Система для борьбы с мошенничеством и утечками данных с онлайн-порталов компании и из мобильных приложений.

В бандл вошли следующие разделы Group-IB FHP:

- **Web Snippet*** – клиентский модуль, встраиваемый в веб-приложение для сбора параметров устройства, индикаторов компрометации и поведения пользователя;
- **Mobile SDK*** – клиентский модуль, встраиваемый в мобильное приложение для сбора параметров устройства, индикаторов компрометации и поведения пользователя;
- **Processing Hub** – модуль для анализа и корреляции данных из клиентского модуля, а также выявление мошенничества;
- **Выделенный антифрод-аналитик.**

*Ограничение до 1000 пользователей для юридических лиц и до 5000 пользователей для физических лиц.

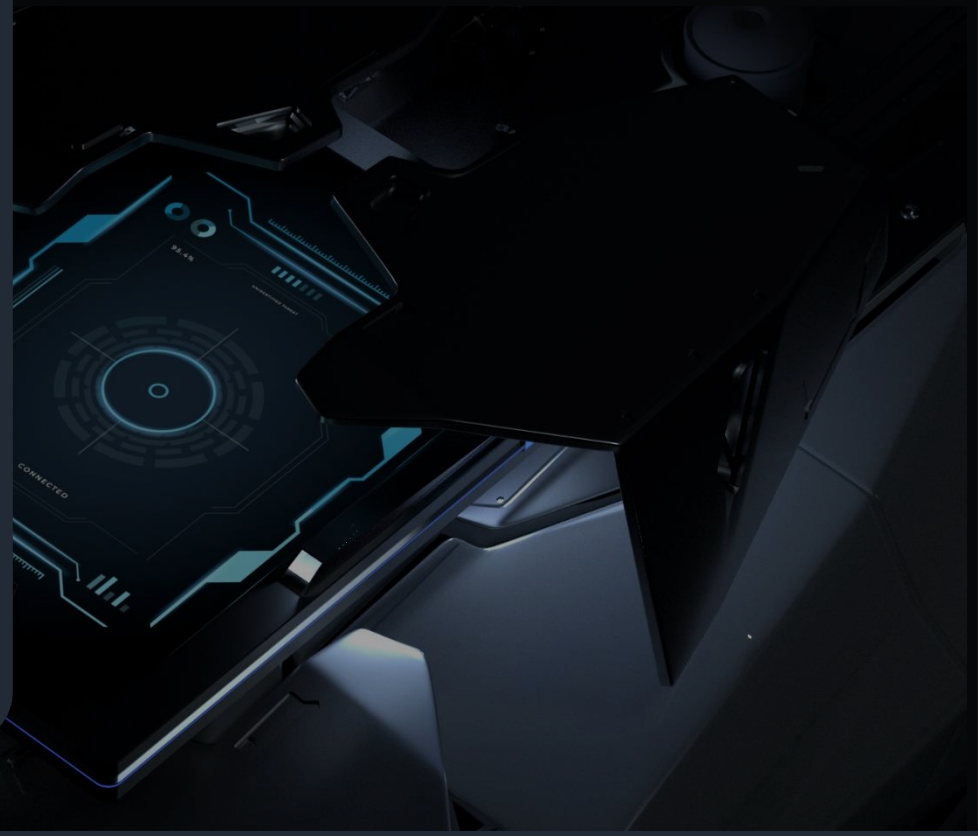
Экспресс-анализ защищенности внешнего периметра

Для предотвращения эксплуатации уязвимостей внешнего периметра и финансовых потерь важно быть в курсе слабых мест безопасности ваших сервисов. Специалисты Group-IB проведут качественный экспресс-анализ защищенности внешнего периметра

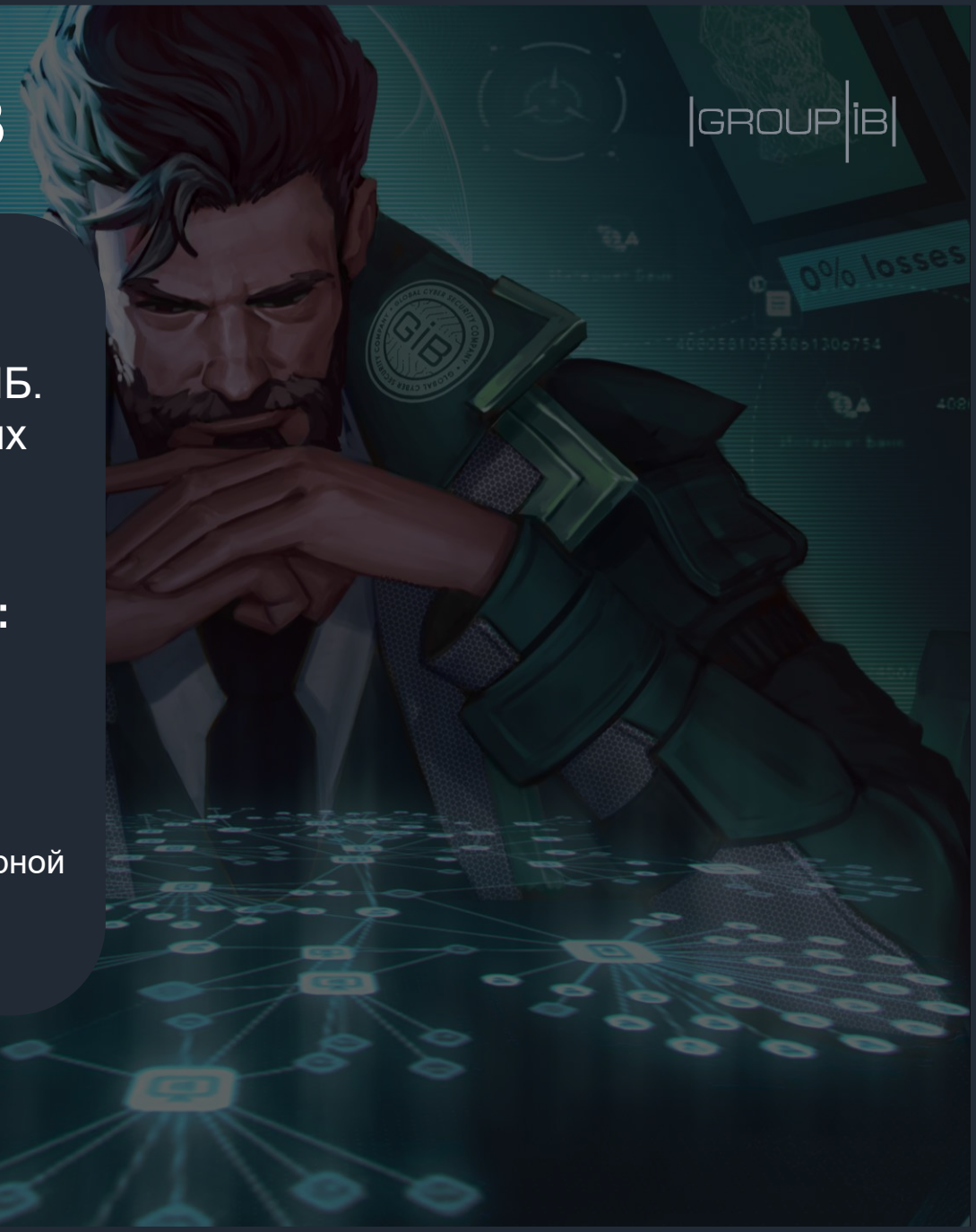
Длительность – 10 дней

Результат:

- детальный технический отчет,
- краткое резюме для руководителей,
- возможность онлайн-встречи с экспертами Group-IB для совместного обсуждения результатов анализа.



Киберобразование от Group-IB



Чтобы обезопасить вашу компанию и предотвратить возможные кибератаки, необходимо обеспечить высокий уровень подготовки ваших специалистов по ИБ. Мы предлагаем авторские обучающие курсы для ваших технических специалистов.

В бандл вошли следующие курсы (один на выбор):

- **Incident Responder –** обучающий курс по эффективному реагированию на выявленный инцидент и ликвидации его последствий

  Длительность: 2 дня

- **Digital Forensics Analyst: Basic –** обучающий курс по компьютерной криминалистике в рамках расследования инцидентов ИБ.

  Длительность: 3 дня

Преимущества G-Bundle Finance

Команда профессионалов

Обучение проводят сертифицированные специалисты Group-IB, которые принимали участие в реагировании и расследовании громких киберпреступлений в России и в мире

Уникальные данные об угрозах

Благодаря собственной системе мониторинга и анализа угроз Group-IB TI&A и доступу к закрытым источникам мы получаем актуальную и значимую информацию

Устранение сетевых уязвимостей

Экспресс-аудит поможет обнаружить уязвимые места периметра компании, а высокопроизводительный классификатор на основе ИИ продукта Group-IB THF поможет обезопасить инфраструктуру

Запатентованная технология детонации ВПО

Платформа детонации вредоносного ПО с тонкими настройками реалистичных рабочих станций, понятной и подробной отчетностью и методами анализа, которых нет ни в одной "песочнице"

Легковесность клиентской части

Анализ приложений и поведения клиента производится не на стороне клиента, а на серверной инфраструктуре Group-IB FHP, что позволяет не нагружать устройство клиента

Синергетический подход к проектам

Благодаря синергии экспертов Лаборатории компьютерной криминалистики, CERT-GIB и TI&A мы непрерывно обогащаем свои решения и знания специалистов актуальными сведениями о тактиках и техниках злоумышленников

GROUP-IB

PREVENTING AND INVESTIGATING CYBECRIME SINCE 2003

info@group-ib.com
+65 3159-3798

linkedin.com/organization/1382013
instagram.com/group_ib

www.group-ib.com
group-ib.com/blog

twitter.com/GroupIB_GIB
facebook.com/groupibHQ