

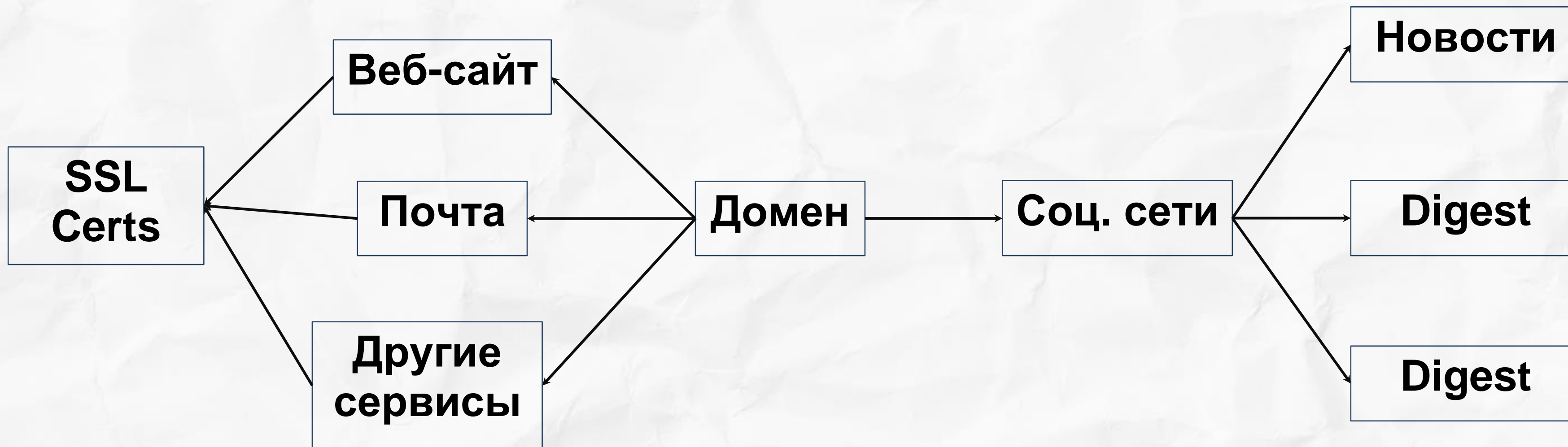
Конкурентная разведка: ОПЫТ ИСПОЛЬЗОВАНИЯ В ПЕНТЕСТЕ

ОБО МНЕ

- Работаю в LMSecurity
- Программирую на Python
- Изучаю OSINT 1 год



Типичная схема роста бизнеса в глобальной сети



Домены, субдомены, IP адреса и SSL сертификаты



WHOIS Search, Domain Name, Website, and IP Tools

- Информация о регистрации домена
- Связь домена и IP адреса
- Просмотр DNS записей
- Использование поисковых систем
- Агрегаторы информации о SSL сертификатах

Criteria Type: Identity Match: ILIKE Search: 'sberbank.ru'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities
	6424235307	2022-03-27	2022-02-18	2023-03-21	securepayments.sberbank.ru	securepayments.sberbank.ru www.securepayments.sberbank.ru
	6410878785	2022-03-25	2022-03-11	2023-03-11	web-si20-uat.mobile-sbe-dev.sbrf.ru	kskarpenko@sberbank.ru
	6410878786	2022-03-25	2022-03-11	2023-03-11	sberbank-ru.os-psi.sberbank.ru	adm.sberbank-ru.os-psi.sberbank.ru sberbank1-ru.os-psi.sberbank.ru sberbank-com.os-psi.sberbank.ru sberbank-ru.os-psi.sberbank.ru www.sberbank1-ru.os-psi.sberbank.ru www.sberbank-com.os-psi.sberbank.ru www.sberbank-ru.os-psi.sberbank.ru
	6410878787	2022-03-25	2022-03-23	2023-03-23	*.webquik-test.sberbank.ru	*.webquik-test.sberbank.ru webquik-test.sberbank.ru
	6404755970	2022-03-24	2022-03-24	2023-04-25	stat.esr.sberbank.ru	stat.esr.sberbank.ru
	6404218161	2022-03-24	2022-03-24	2023-04-23	*.meetup.sberbank.ru	*.meetup.sberbank.ru meetup.sberbank.ru
	6396710097	2022-03-23	2022-03-23	2023-03-14	rms.sberbank.ru	rms.sberbank.ru rms.sberbank.ru

HE HURRICANE ELECTRIC INTERNET SERVICES

5.255.192.0/18

Quick Links: [BGP Toolkit Home](#), [BGP Prefix Report](#), [BGP Peer Report](#), [Exchange Report](#), [Bogon Routes](#), [World Report](#), [Multi Origin Routes](#), [DNS Report](#), [Top Host Report](#), [Internet Statistics](#), [Looking Glass](#), [Network Tools App](#), [Free IPv6 Tunnel](#)

Network Info Whois DNS IRR

Results truncated to 1,000 entries.

IP	PTR	A
5.255.192.5	cstatic-rostov02.regions.yandex.net	
5.255.192.6	proxy-rostov01.cdn.yandex.net	
5.255.192.7	proxy-rostov02.cdn.yandex.net	
5.255.192.8	proxy-rostov03.cdn.yandex.net	
5.255.192.9	cache-rostov01.cdn.yandex.net	
5.255.192.10	cache-rostov02.cdn.yandex.net	



- Сканирование IP адресов
- Определение ПО и его версий
- Сканирование Веб-приложений
- Определение ПО, его версии и используемых плагинов
- Поиск открытых директорий



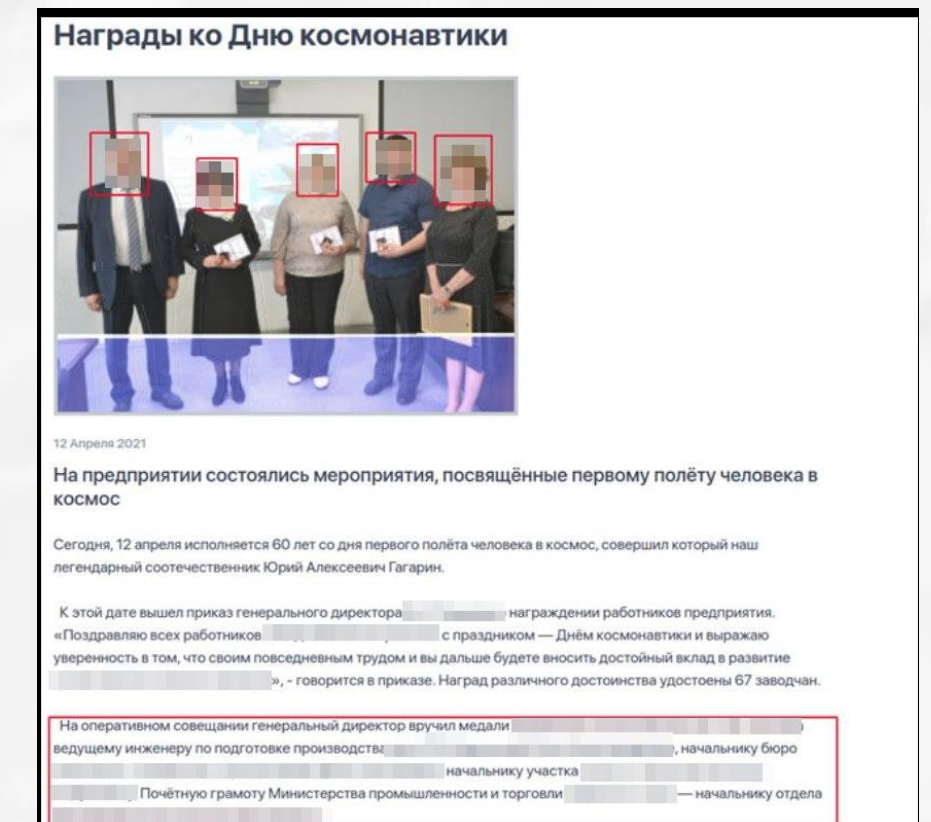
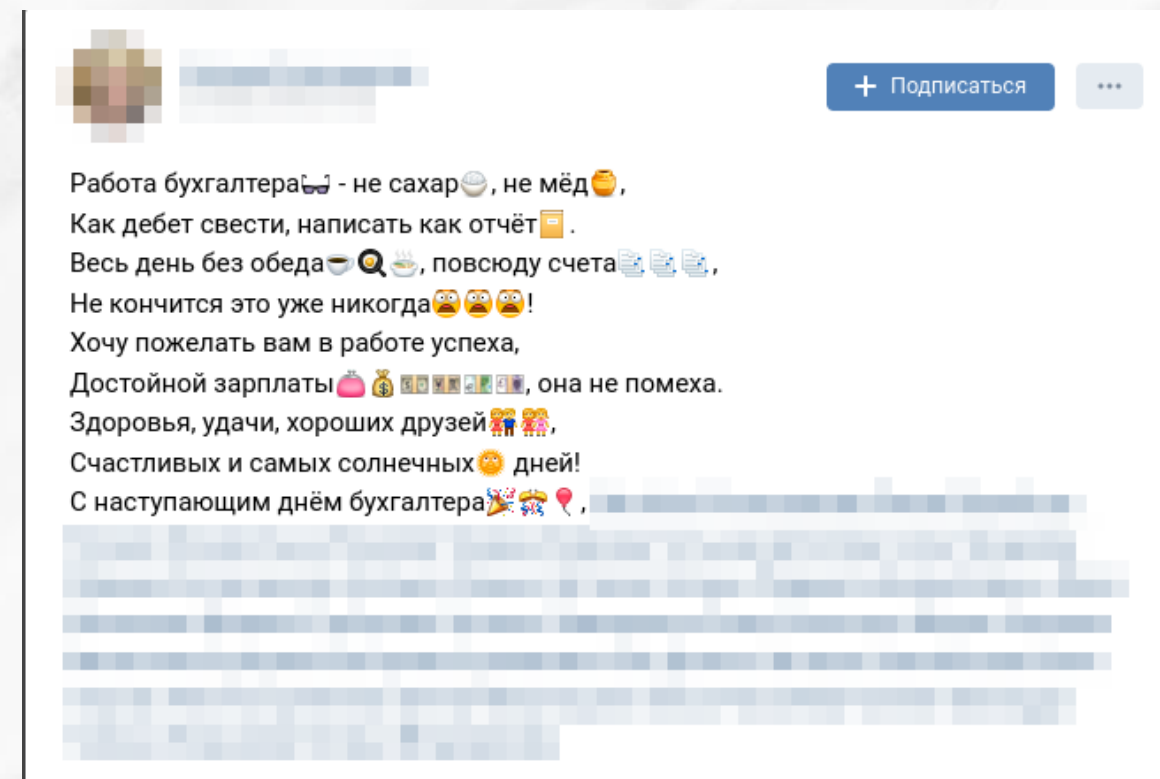
Социальные сети

Профиль компании

- Фото / Видео
- Участники
- Посты
- Новости
- Газета
- Digest

Личные профили сотрудников

- Посты
- Фото (с рабочего места)



Публикуемые документы

Инструменты:

- Foca
- Metagoofill

Информация:

- Имена пользователей
- Даты создания и изменения
- Используемое ПО



Метод грубой силы

Дано:

- куча личной информации о сотрудниках

Нужно:

- составить список паролей для брута

Источники:

- Сервисы утечек
- Словари паролей (ТОП-10-е6)
- Генераторы паролей на основе личной информации



Выводы:

- Проведите организационные мероприятия по ИБ
- СисАдмин \neq сотрудник ИБ
- Планово проводите пентесты и аудиты ИБ
- Регулярно производите резервное копирование данных
- Не позволяйте сотрудникам смешивать работу и личную жизнь

**ГОТОВ ОТВЕТИТЬ
на ваши
вопросы!**

TG: t.me/eolgert

