КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

КАК ЗАЩИТИТЬ КОМПАНИЮ ОТ ПЕРВОЙ ФАЗЫ АТАКИ - КИБЕРРАЗВЕДКИ

Сергей ГОРБАЧЕВ
TECH.INSIDERS

Cyber Kill Chain®

Метод разработан Lockheed Martin для моделирования кибер-атак

КИБЕРРАЗВЕДКА
Атакующий выбирает цель, исследует её уязвимости, оценивает стоимость атаки

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТИ
ПО активируется и эксплуатирует заранее известную уязвимость.

ВООРУЖЕНИЕ
Разработка либо выбор вредоносного ПО для проведения атаки

ВНЕДРЕНИЕ
Инсталляция средств удаленного управления

ДОСТАВКА
Транспортировка вредоносного ПО на территорию жертвы

УПРАВЛЕНИЕ И КОНТРОЛЬ
Взятие под удаленное управление ресурсов жертвы

Целевое действие

Атакующий наносит ущерб: вывод из строя, кража или модицикация информации, атаки на другие цели, и др. …

text 174.84 KB raw download clone embed report print

```
################################################################################################################
================================================================================================================
Hostname    www.bankfab.ae      ISP     First Abu Dhabi Bank P.j.s.c
Continent   Asia        Flag
AE
Country     United Arab Emirates        Country Code    AE
Region  Unknown         Local time  05 Oct 2019 22:14 +04
City    Unknown         Postal Code     Unknown
IP Address  81.16.132.71        Latitude    24
            Longitude   54
================================================================================================================
################################################################################################################
> www.bankfab.ae
Server:     38.132.106.139
Address:    38.132.106.139#53

Non-authoritative answer:
Name:   www.bankfab.ae
Address: 81.16.132.71
>
################################################################################################################
```

FULL RECON

Что обычно сканируют ANONYMOUS

1

HTTP заголовки
На предмет типовых уязвимостей (например XSS, XXE, broken authentication, ..), информация о ПО

2

ОТКРЫТЫЕ ПОРТЫ
Иногда находят порты RDP, SSH доступа, октрытые порты баз данных, сервера разработки

3

НАЛИЧИЕ WAF
Web Application Firewall уделяется особое внимание, потому что серьезно усложняет атаки.

4

SHODAN
Поиск уязвимого оборудования доступного из интернет (принтеры, камеры, роутеры, ...)

5

ИНФРАСТРУКТУРА
Выявляется сетевая инфраструктура цели. Поддомены, связанные домены, IP подсети, другие связанные проекты, закрытая от интернета инфраструктура

6

WHOIS
Обычно статическая информация. Но для целевых атак могут достать и исторические данные.

FULL RECON

Что обычно сканируют ANONYMOUS

7

DNS сервера
Настройки DNS серверов провайдера на предмет уязвимостей (DDoS, захват домена, Men-in-a-middle, ...)

8

Reverse IP lookup
По IP ищутся другие связанные проекты, сайты, более уязвимые.

9

GEO IP
Географические координаты датацентров.

10

ROBOTS.TXT
Иногда в них содержатся deepweb ссылки

11

УТЕЧКИ
Ищутся факты утечек логинов-паролей: censys, webarchive, hackertarget, haveibeenpwned

12

ICMP
Пингуются сервера на возможность ICMP-атак

FULL RECON

Что обычно сканируют ANONYMOUS

13 **DNS записи**
Достаются все возможные записи включая исторические

14 **HTTPS - настройки**
Может использоваться в атаках на уязвимостях HTTPS: TLS 1.0, 1,1,1.2 , deflate compression, downgrade attack, openssl ccs injection, hetrblead ...

15 **INTERESTING FILES**
Открытые файлы PDF, DOC, XLS, конфиг

16 **ПОЛЬЗОВАТЕЛИ**
Выявляются пользователи, их логины, емейлы

17 **ИСПОЛЬЗУЕМОЕ ПО**
Используется для целевых атак, spear-phishing

18 **SEARCH ENGINES**
Информация об утечках и возможных уязвимостях

RECON - НЕВИДИМАЯ УГРОЗА!

Первая часть разведки (RECON, RECONNAISSANCE) проводится без касания периметра жертвы, её технически невозможно детектировать.

А ЧТО ПОТОМ?

После Full Recon по операции #OpSudan в 2019 группа Ghost Squad Hackers вывели из строя всю сеть гос-ресурсов целой страны

#OpSudan

ENISA Threats 2018

Классификация угроз в ЕС
Опубликовано - январь 2019

	THREAT AGENTS						
	Cyber-criminals	Insiders	Nation States	Corporations	Hacktivists	Cyber-terrorists	Script kiddies
Malware	✓	✓	✓	✓	✓	✓	✓
Web-based attacks	✓		✓	✓	✓	✓	✓
Web application attacks	✓		✓	✓	✓	✓	✓
Denial of Service	✓		✓	✓	✓	✓	✓
Botnets	✓		✓	✓	✓	✓	✓
Phishing	✓	✓	✓	✓	✓		✓
Spam	✓	✓	✓	✓			
Ransomware	✓	✓	✓	✓			✓
Insider threat	✓		✓	✓		✓	
Physical manipulation / damage / theft / loss	✓	✓	✓	✓	✓	✓	✓
Exploit kits	✓		✓	✓			
Data breaches	✓	✓	✓	✓	✓	✓	✓
Identity theft	✓	✓	✓	✓	✓	✓	✓
Information leakage	✓	✓	✓	✓	✓	✓	✓
Cyber espionage		✓	✓	✓			

Legend:
Primary group for threat: ✓
Secondary group for threat: ✓

Кто представляет угрозу

	РИСК		
	Количество	Вероятность	Примеры
APT Группы	300	Высокая в некоторых отраслях	MageCart APT35 Cobalt ...
Хактивисты	25	Низкая	ANONYMOUS MILW0RM LULZSEC ....
Defacers	5000+	Высокая	B4CKD00R CR45H Trenggalek Cyber Army TurkishSpyHacker BLACK PHANTOM CYBER ...
Конкуренты		Высокая	

ЧТО ДЕЛАТЬ?

— дешевле предупредить атаку, чем устранять ее последствия.

#CODEIB

АНТИ-RECON

Заградительные меры против Recon

1

Google, Yandex, DuckDuckGo
Внимательно изучите информацию о вашей компании в поисковых системах
site:ваш домен

2

Recon-NG
Утилита позволяет увидеть 80% скрытой информации о вашей компании.

3

Shodan
Проверьте, что эта система уже узнала о вас.

4

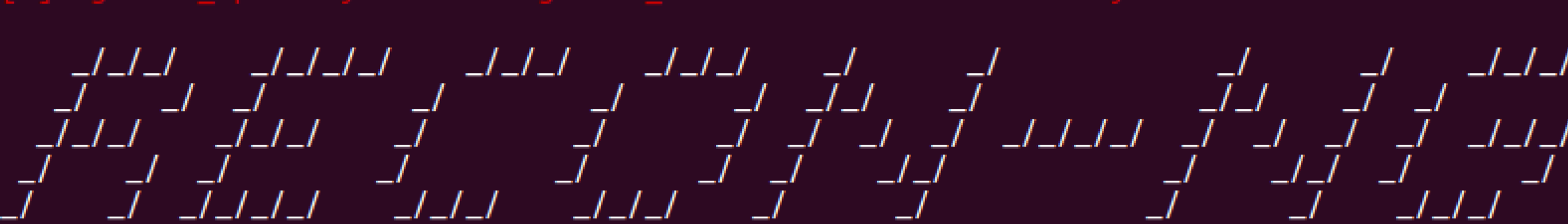
УТЕЧКИ О СОТРУДНИКАХ
Найдите утечки данных сотрудников и минимизируйте возможность их эксплуатации: Haveibeenpwned, pastebin, censys, ...

5

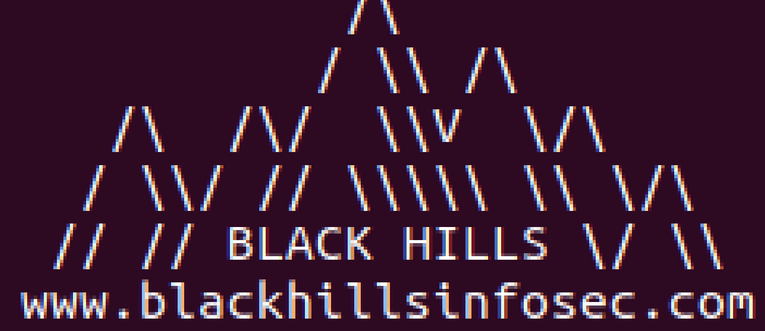
SSL-Transparency
Не регистрируйте прозрачные SSL для внутренних серверов — это делает их видимыми публично.
.

6

ДЕЗИНФОРМАЦИЯ
Если информацию сложно удалить — сделайте её неактуальной, либо заместите на дезинформацию.



Sponsored by...



[recon-ng v4.9.2, Tim Tomes (@LaNMaSteR53)]

[77] Recon modules
[8] Reporting modules
[2] Import modules
[2] Exploitation modules
[2] Discovery modules

[recon-ng][default] >

RECON-NG DEMO

#CODEIB

ОБОРОНА

Что важно после RECON.

1

OWASP TOP 10
Веб-приложения обязательно должны проверяться на OWASP top 10 уязвимости.

2

Web Application Firewall
Он прикроет некоторые элементы инфраструктуры, и сделает невозможным эксплуатацию многих угроз.

3

МЕЖСЕТЕВОЙ ЭКРАН
Настройте его правильно, обеспечьте возможность мониторинга даже в условиях DDoS атаки.

4

Intrusion Detection System
Используйте хотя бы бесплатные версии IDS (Snort, Suricata), позволят вам выловить невидимые ранее угрозы.

5

ПЕРСОНАЛ
Обучение безопасности: сильные пароли, контроль от утечек, не использовать рабочие пароли в других системах, фишинговые киберученья.

6

РЕЗЕРВНОЕ КОПИРОВАНИЕ
Обеспечить резервное копирование и процесс восстановления максимально быстро. Защищать резервные данные.

7. ФЕЙКОВАЯ ИНФРАСТРУКТУРА

Поверните Recon в свою пользу.
Это ваш единственный способ что-то сказать атакующему.

Направьте его на HoneyPot или фейковую инфраструктуру.

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ

s@insiders.tech

https://insiders.tech

КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ