

BEEP!

Rootloft-office cyber-ops console

UNAUTHORIZED EXTENSION DETECTED

Thousands installs on the company network

شنو هاد الهجوم؟! هاد

99% ديال المستخدمين مركبين ؟extensions

SWOOSH!

CRACK!

permission creep

SaaS

```

permissions
{
  "permissions": [
    "scripting",
    "scripting", "cookies"
  ]
}

```

SWOOSH!



البيانات
كتتسرب!

و sessions
cookies
ضايعين!

SHADOW AI
EXTENSIONS

BOOM!

CRACK!

ZZZT!

PERMISSION
GRANTED

PERMISSION
GRANTED

- CVE ALERTS
- CVE ALERTS
- CVE ALERTS

PERMISSION
GRANTED

PERMISSION
VAULT

PERMISSION
VAULT

SESSION
MANG



فين ال-CVE؟

كنقلبو فال-logs و MongoDB

TICK!
CLACK!

TICK!
CLACK!
DING!

ガ
レ
ツ

ズ
ツ
ツ
ド
ド
ド
ッ!

API CALLS



API Sstaskks

	TIMESTAMP	
09:58:01 recent browser extension		6176
38:98:993 apt eabotnlge	2022:02:00:23	
38:00:400 apt respilers		
38:50:400 recent browser extension updates	2022:02:09:20	

VULNERABILITIES



COMPROMISED ACCOUNTS

Recent browser extension updates

- API calls (for browser extension updates)
- API calls (no browser extension updates)
- CVE matrix (CVE matrix)



EXTENSION



EXTENSION



EXTENSION



MONGODB COMPROMISED ACCOUNTS

- permissions
- cookies
- scripting
- tabs

TICK!
CLACK!
DING!



SUSPICIOUS COMMIT

```
100  2022-02-09 10:00:00  100  2022-02-09 10:00:00  100  2022-02-09 10:00:00
101  2022-02-09 10:00:01  101  2022-02-09 10:00:01  101  2022-02-09 10:00:01
102  2022-02-09 10:00:02  102  2022-02-09 10:00:02  102  2022-02-09 10:00:02
103  2022-02-09 10:00:03  103  2022-02-09 10:00:03  103  2022-02-09 10:00:03
104  2022-02-09 10:00:04  104  2022-02-09 10:00:04  104  2022-02-09 10:00:04
105  2022-02-09 10:00:05  105  2022-02-09 10:00:05  105  2022-02-09 10:00:05
106  2022-02-09 10:00:06  106  2022-02-09 10:00:06  106  2022-02-09 10:00:06
107  2022-02-09 10:00:07  107  2022-02-09 10:00:07  107  2022-02-09 10:00:07
108  2022-02-09 10:00:08  108  2022-02-09 10:00:08  108  2022-02-09 10:00:08
109  2022-02-09 10:00:09  109  2022-02-09 10:00:09  109  2022-02-09 10:00:09
110  2022-02-09 10:00:10  110  2022-02-09 10:00:10  110  2022-02-09 10:00:10
```




CLANG!

DLP + Permission Audit

BOOM!

PATCH SUCCESS

API GATEWAYS

الثغرات!
سدينا

Permissions
API محمي!

BOOM!

Permission-clinge

Permission-change
confirmation changs..

BOOM!

CLANG!

WHOOSH!