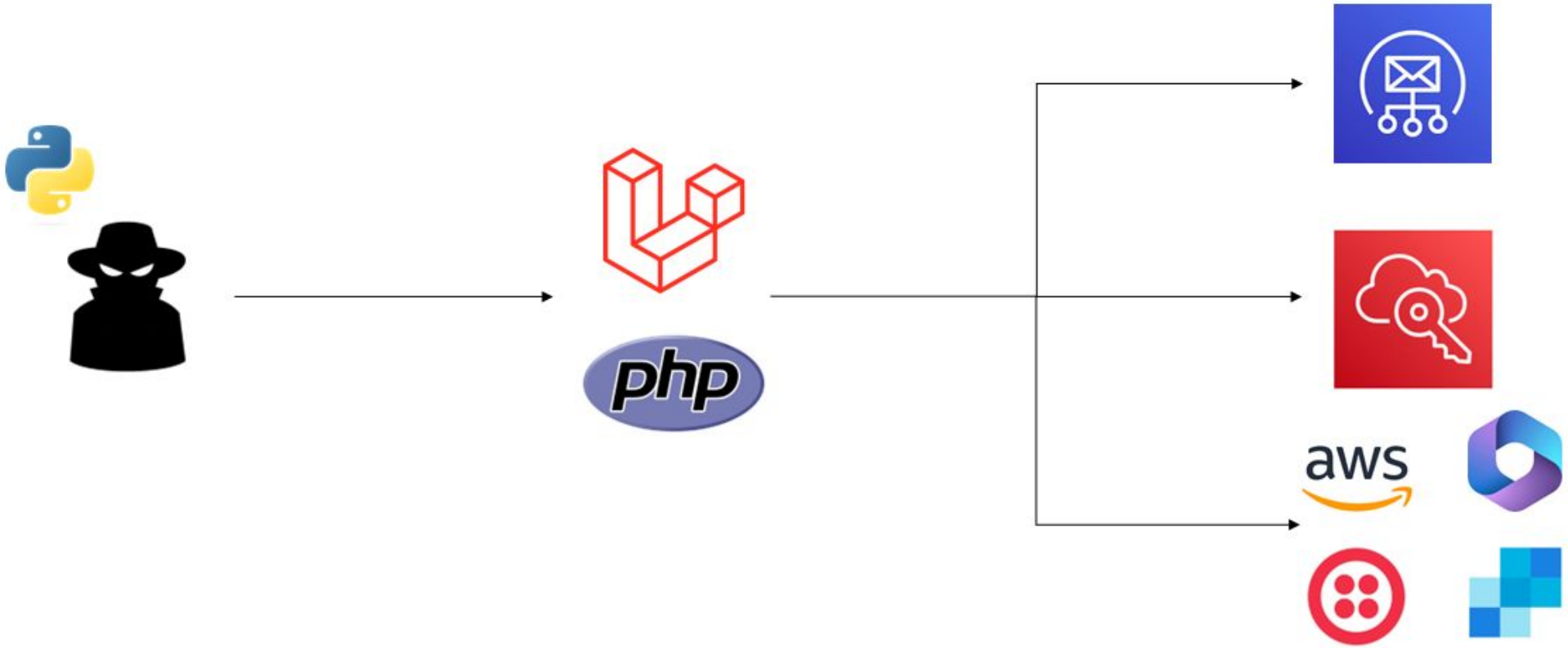
Androxgh0st

Simonazzi Gian Marco – Sicurezza Informatica

Androxgh0st

- Malware in Python
- Target: Web App in Laravel / PHP



Androxgh0st

- Molteplice threat actor
- Decine di versioni personalizzate
- Dicembre 2022: Scoperta
- Gennaio 2024: Allerta CISA-FBI

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

AMERICA'S CYBER DEFENSE AGENCY

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

Known Indicators of Compromise Associated with Androxgh0st Malware

Release Date: January 16, 2024 **Alert Code:** AA24-016A

RELATED TOPICS: CYBER THREATS AND ADVISORIES, MALWARE, PHISHING, AND RANSOMWARE

ACTIONS TO TAKE TODAY TO MITIGATE MALICIOUS CYBER ACTIVITY:

1. Prioritize patching known exploited vulnerabilities in internet-facing systems.
2. Review and ensure only necessary servers and services are exposed to the internet.
3. Review platforms or services that have credentials listed in .env files for unauthorized access or use.

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

Vulnerabilità (Laravel)

- File .env (con credenziali) esposto
  - HTTP GET
  - HTTP POST (se Laravel in Debug)
- CVE-2018-15133
  - RCE tramite deserializzazione token XSRF

```
else:
    get_source = requests.post(url, data={"0x[]":"androxgh0st"}, headers=headers, tir
    if "<td>APP_KEY</td>" in get_source:
        resp = get_source
if resp:
```

Sample Androxgh0st su Github

- `/.env.dist`
- `/.env.save`
- `/environments/.env.production`
- `/.env.production.local`
- `/.env.project`
- `/.env.development`
- `/.env.production`
- `/.env.prod`
- `/.env.development.local`
- `/.env.old`
- `/<insert-directory>/.env`
- `/.aws/credentials`
- `/aws/credentials`
- `/.aws/config`
- `/.git`

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

Altre vulnerabilità

- CVE-2017-9841
  - PHPUnit
  - RCE
- CVE-2021-41773
  - Apache web server
  - RCE / Path traversal
- CVE-2019-6340
  - Drupal
  - RCE
- CVE-2022-29464
  - WSO2
  - RCE

- `/.env/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//admin/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//api/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//backup/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//blog/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//cms/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//demo/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//dev/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`
- `//laravel/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php`

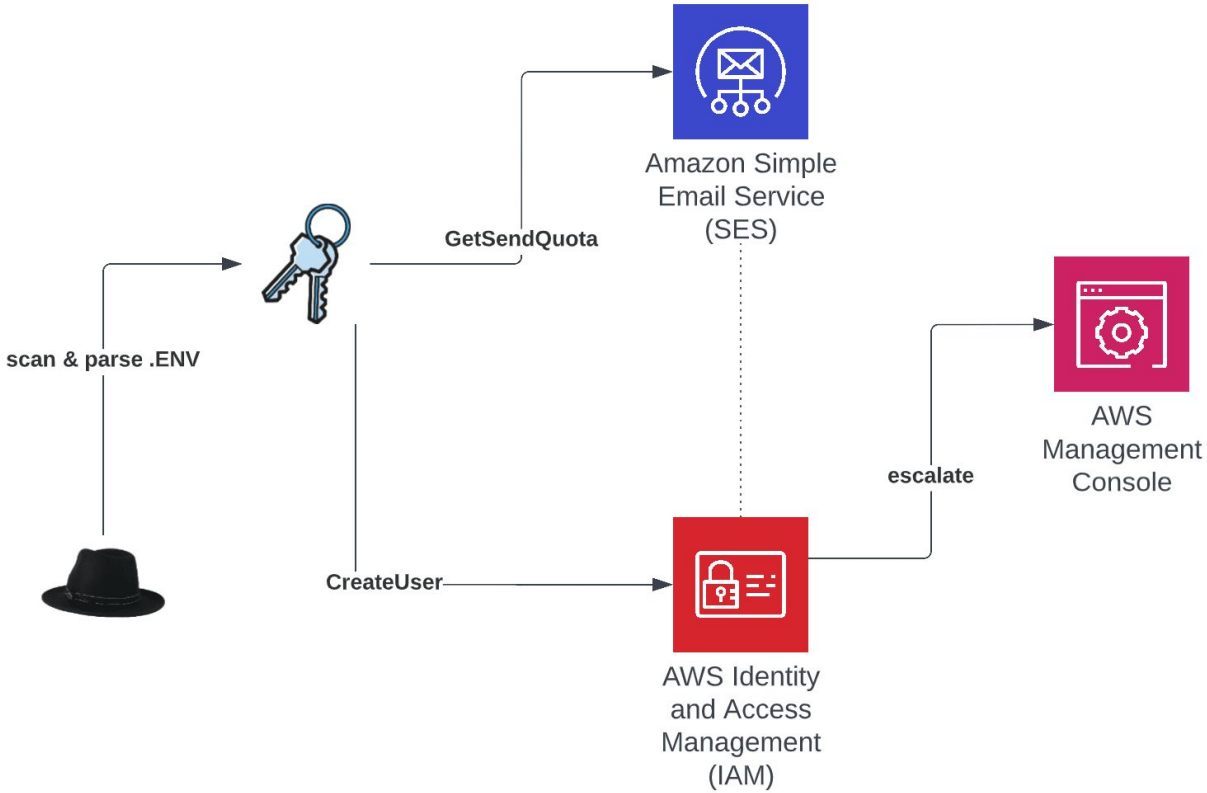
https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

Vulnerabilità: MITRE

Tactic	Name	ID
Reconnaissance	Active Scanning	T1595
Initial Access	Exploit Public-Facing Application	T1190
Command and Control	Ingress Tool Transfer	T1105
Discovery	File and Directory Discovery	T1083

Comportamento

- Installazione webshell su host
- Esfiltrazione credenziali
- Accesso AWS
  - Controllo AWS Simple Email Service
  - Escalation verso AWS Management
- Cryptomining
- Botnet
  - Scanning
  - DDOS?

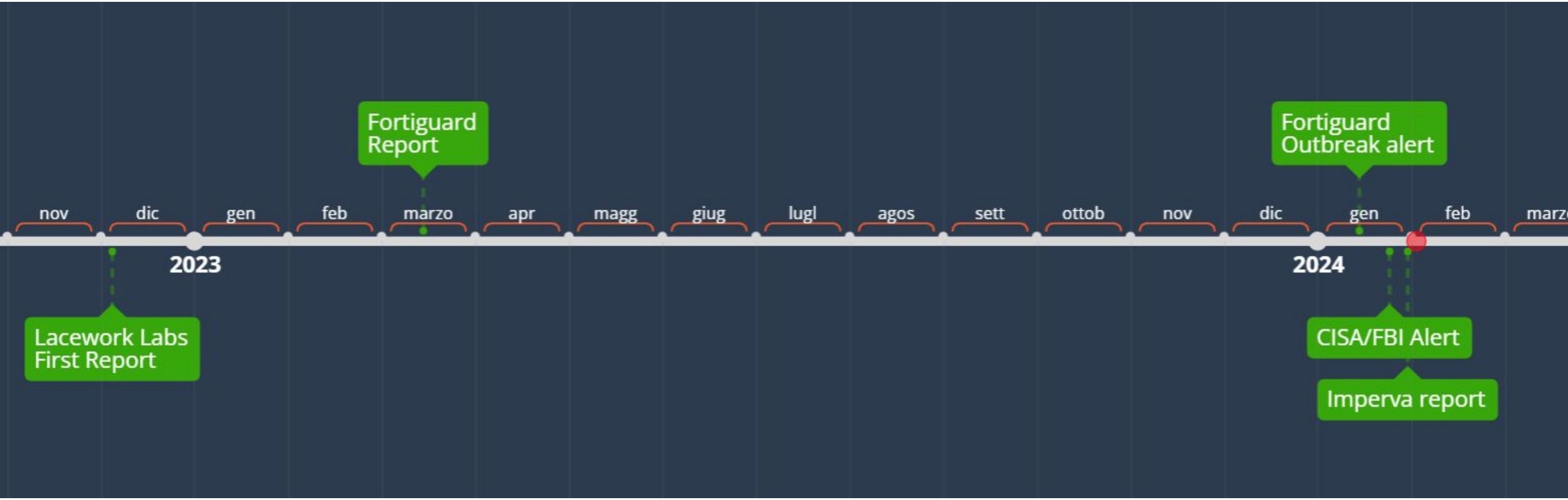


https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys/

Comportamento: MITRE

Tactic	Name	ID
Persistence	Server Software Component: Web Shell	T1505.003
Credential Access	Unsecured Credentials: Credentials In Files	T1552.001
Defense Evasion	Valid Accounts	T1078
Collection	Email Collection	T1114
Persistence	Create Account	T1136
Resource Development	Acquire Infrastructure: Botnet & Web Services	T1583.005 / T1583.006

Timeline


Fortiguard Report
Fortiguard Outbreak alert
nov
dic
gen
feb
marzo
apr
magg
giug
lugl
agos
sett
ottob
nov
dic
gen
feb
marz
2023
2024
Lacework Labs First Report
CISA/FBI Alert
Imperva report

Mitigazioni

- Controllare URL esposti
- Laravel: CVE-2018-15133 e modalità Debug
- Deployment senza .env in host
- PHP sospetti (RCE e webshell)
- Monitorare API call AWS
  - *GetSendQuota*
  - *CreateUser*
  - *DeleteAccessKey*

Riferimenti

https://www.lacework.com/blog/androxghost-the-python-malware-exploiting-your-aws-keys/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-016a

https://fortiguard.fortinet.com/threat-signal-report/5066/androxgh0st-malware-actively-used-in-the-wild

https://attack.mitre.org/matrices/enterprise/

https://www.imperva.com/blog/imperva-uncovers-new-indicators-of-compromise-for-androxgh0st-botnet/