

# S9\_L5

## Unit 3 - CS0424

MATTEO BELTRAMI MARZOLINI  
CYBEREAGLES

---

Giorno 5 - BONUS

### TRACCIA

#### BONUS:

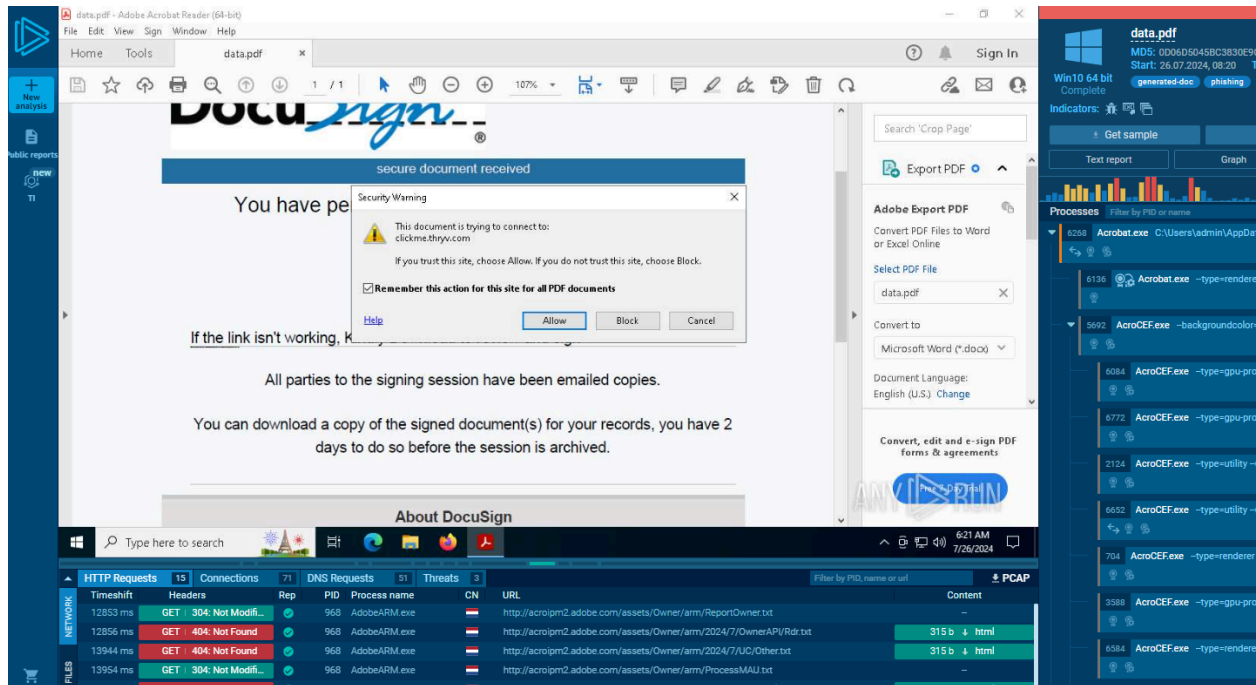
Analizzare le seguenti segnalazioni caricate su anyrun e fare un piccolo report di ciò che si scopre relativo all'eventuale attacco spiegando ad utenti e manager la tipologia di attacco e come evitare questi attacchi in futuro:

*[https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6 /](https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6/)*

*[https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2 /](https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2/)*

# SVOLGIMENTO

<https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6/>



Controllando la segnalazione possiamo notare che la tipologia del file è un PDF e che contiene script o collegamenti a siti malevoli. Spesso usato in attacchi di phishing per ingannare gli utenti a cliccare su link dannosi o scaricare malware.

Le possibili prevenzioni per evitare possibili attacchi simili in futuro, possono consistere in:

## Formare il Personale:

- Riconoscere le E-mail di Phishing, fare attenzione a email con errori, richieste urgenti o mittenti sconosciuti.
- Passare il mouse sui link per controllare l'URL prima di cliccare.

---

## Filtri per le E-mail:



- Usare filtri che blocchino email sospette.
- Implementare tecniche come SPF, DKIM e DMARC per verificare l'autenticità delle email.


## Verifica dei Link nei PDF:

- Utilizzare strumenti che controllano i PDF per link o contenuti malevoli.
- Richiedere la verifica dei link nei documenti prima di aprirli.

### General Info

---

File name: data.pdf  
Full analysis: <https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6>  
Verdict: **Malicious activity**  
Analysis date: July 26, 2024 at 08:20:40  
OS: Windows 10 Professional (build: 19045, 64 bit)  
Tags: **generated-doc** **phishing**  
Indicators:    
MIME: application/pdf  
File info: PDF document, version 1.7, 1 pages  
MD5: 0D06D5045BC3830E9CB90DE1D46EEF01  
SHA1: C50A73C13C29A392BA00DC8E9DF7B44815E4EEAD  
SHA256: AE5C5FC7FDFED3A2A19405B35FBAE8F3D82D285FC8516963E713171257F2906B  
SSDEEP: 3072:TMJMarKKzIW9WSgoMqi/Hq+CGQUf0wyah:IKGNzT9sxcCGP0gh

 [ANY.RUN](#) is an interactive service which provides full access to the guest system. Information in this report could be distorted by u:  
[ANY.RUN](#) does not guarantee maliciousness or safety of the content.

#### Software environment set and analysis options

### Behavior activities

---

#### MALICIOUS

---

Phishing has been detected  
• msedge.exe (PID: 1560)

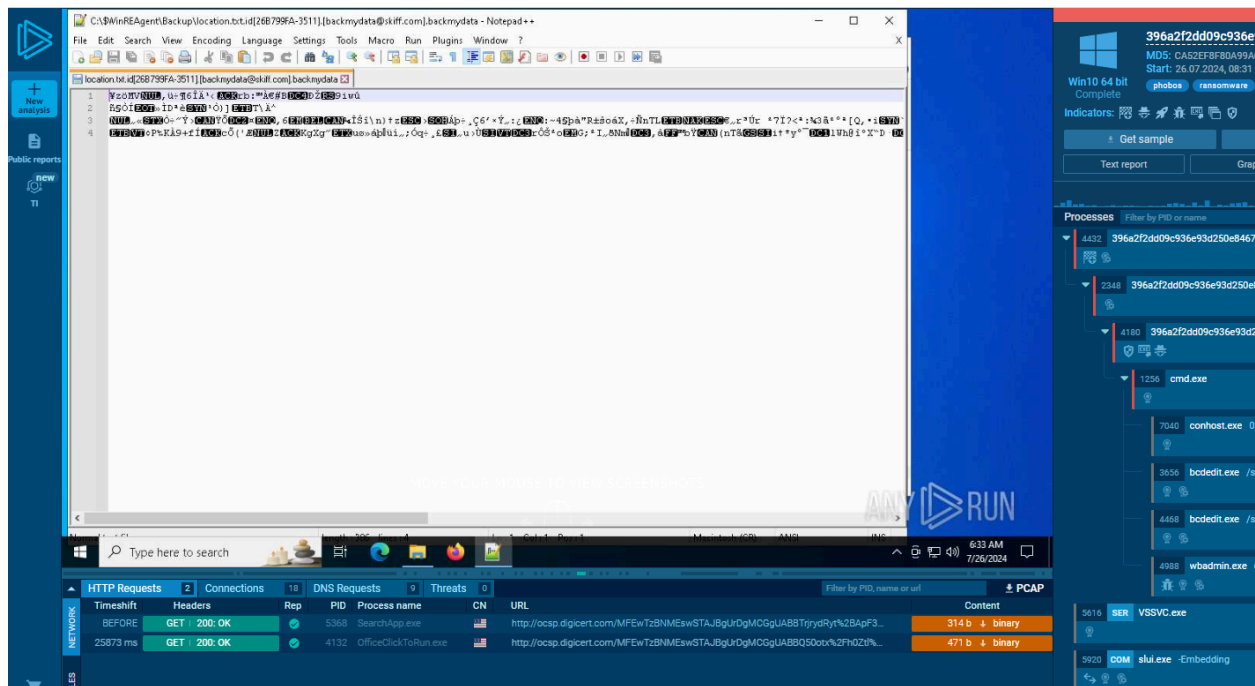
#### SUSPICIOUS

---

No suspicious indicators.

**<https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcb0ac2/>**

In questo caso si può notare, invece, la presenza di un eseguibile dannoso, identificato come un malware. Esegue codice malevolo per rubare dati, permette accesso remoto o danneggia i file.



Le possibili prevenzioni per evitare possibili attacchi simili in futuro, possono consistere in:

### **Antivirus e antimalware:**

- Usare antivirus aggiornati per rilevare e bloccare file malevoli.
- Effettuare scansioni frequenti per individuare minacce.

### **Aggiornamenti software:**

- Mantenere i sistemi e i software aggiornati per chiudere le vulnerabilità.
- Abilitare aggiornamenti automatici per applicare le ultime patch.

Politiche di sicurezza:

- Limitare i permessi degli utenti per ridurre l'impatto di infezioni.
- Impostare politiche per limitare l'esecuzione di file sconosciuti.

Backup regolari:

- Effettuare backup regolari e sicuri per poter ripristinare i dati in caso di attacco.
- Verificare periodicamente che i backup funzionino correttamente.

General Info

File name:

396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6

Full analysis:

<https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2>

Verdict:

Malicious activity

Threats:

Phobos Ransomware Stealer

Phobos is a ransomware that locks or encrypts files to demand a ransom. It uses AES encryption with different e

Analysis date:

July 26, 2024 at 08:31:20

OS:

Windows 10 Professional (build: 19045, 64 bit)

Tags:

phobos ransomware stealer

Indicators:

MIME:

application/x-dosexec

File info:

PE32 executable (GUI) Intel 80386, for MS Windows

MD5:

CA52EF8F80A99A01E97DC8CF7D3F5487

SHA1:

D4BF7B56D1F022E14A870D724E8DA274288BC5DB

SHA256:

396A2F2DD09C936E93D250E8467AC7A9C0A923EA7F9A395E63C375B877A399A6

SSDEEP:

768:UyVHL0Nw1ALXbLwHi/WEhFOYQJ7zs7ERdxmEeQ/9BLQ6XGHFG9IaLNTrMh5Xgh6D:UymNrLwC/WPYQ3CU

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by u

[ANY.RUN](#) does not guarantee maliciousness or safety of the content.

Software environment set and analysis options

Behavior activities

MALICIOUS	SUSPICIOUS
<div>Drops the executable file immediately after the start</div> <ul style="list-style-type: none"><li>• 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)</li><li>• 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)</li></ul>	<div>Application launched itself</div> <ul style="list-style-type: none"><li>• 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)</li><li>• 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 2348)</li></ul>