

S9/L5

BONUS

Analisi e report di due file malevoli, data.pdf e un ransomware (phobos) su any.run

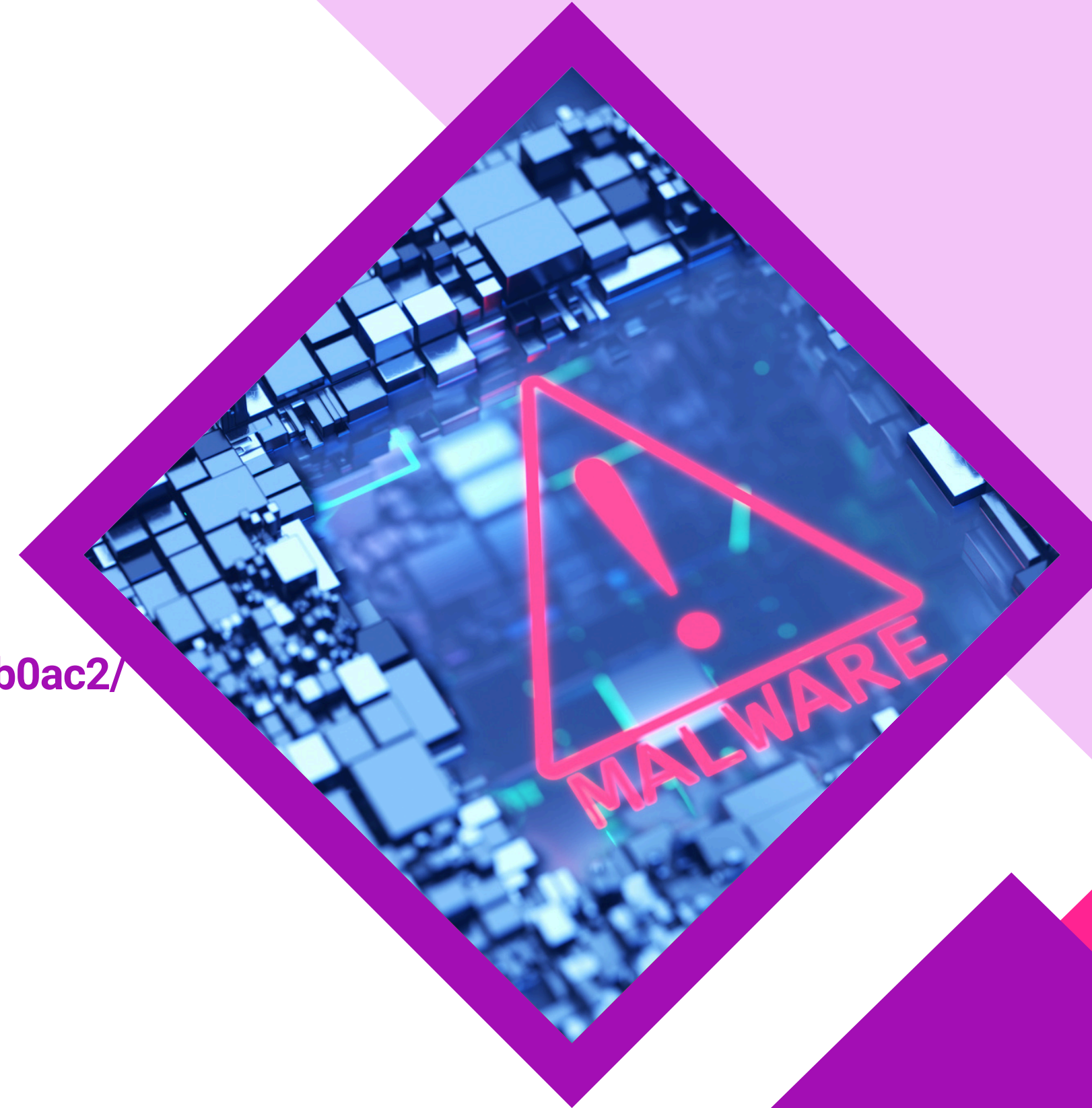


Flavio Scognamiglio

TRACCIA

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/70555e9b-3e91-4126-bb9e-567fcbeb0ac2/>

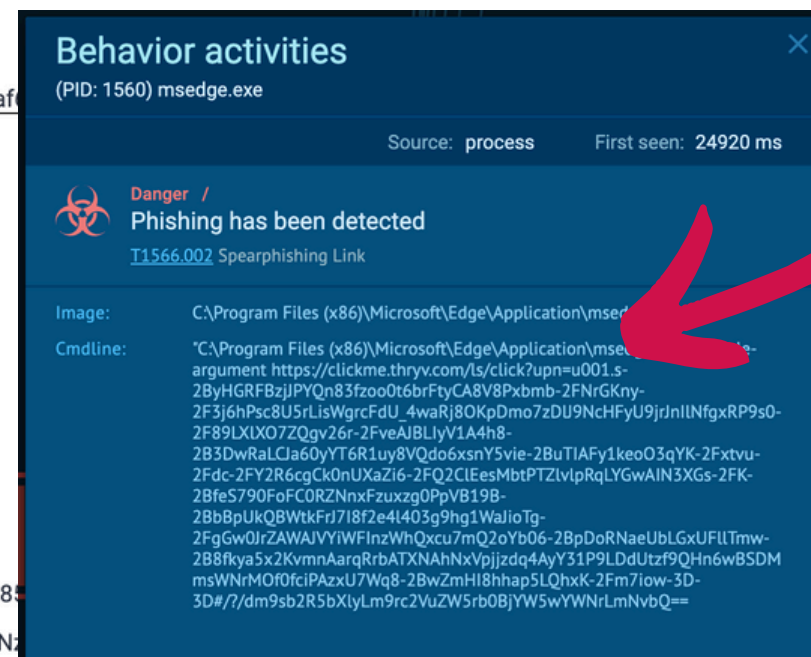


DATA.PDF

Quest'analisi esamina in oggetto un file "data.pdf" contrassegnato come **malevolo**. La data dell'analisi è odierna (26 luglio 2024), e a quanto pare è un malware che si attiva da un pdf inviato alla **vittima**, e una volta aperto, reindirizza ad un sito web di phishing. Si deduce dal report che sia stato testato efficacemente su Windows 10 professional. La build esatta è la **19045**, 64bit).

General Info

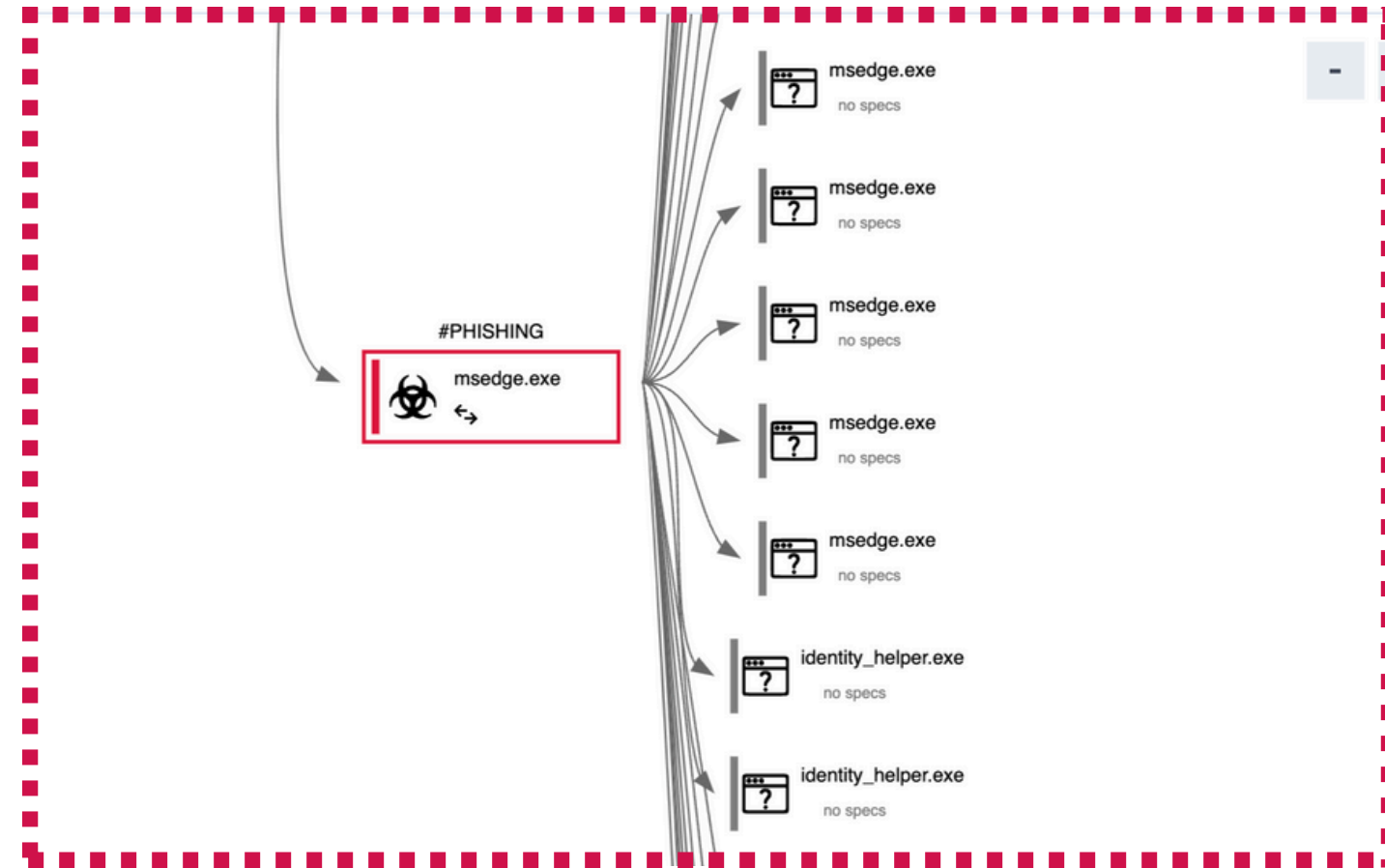
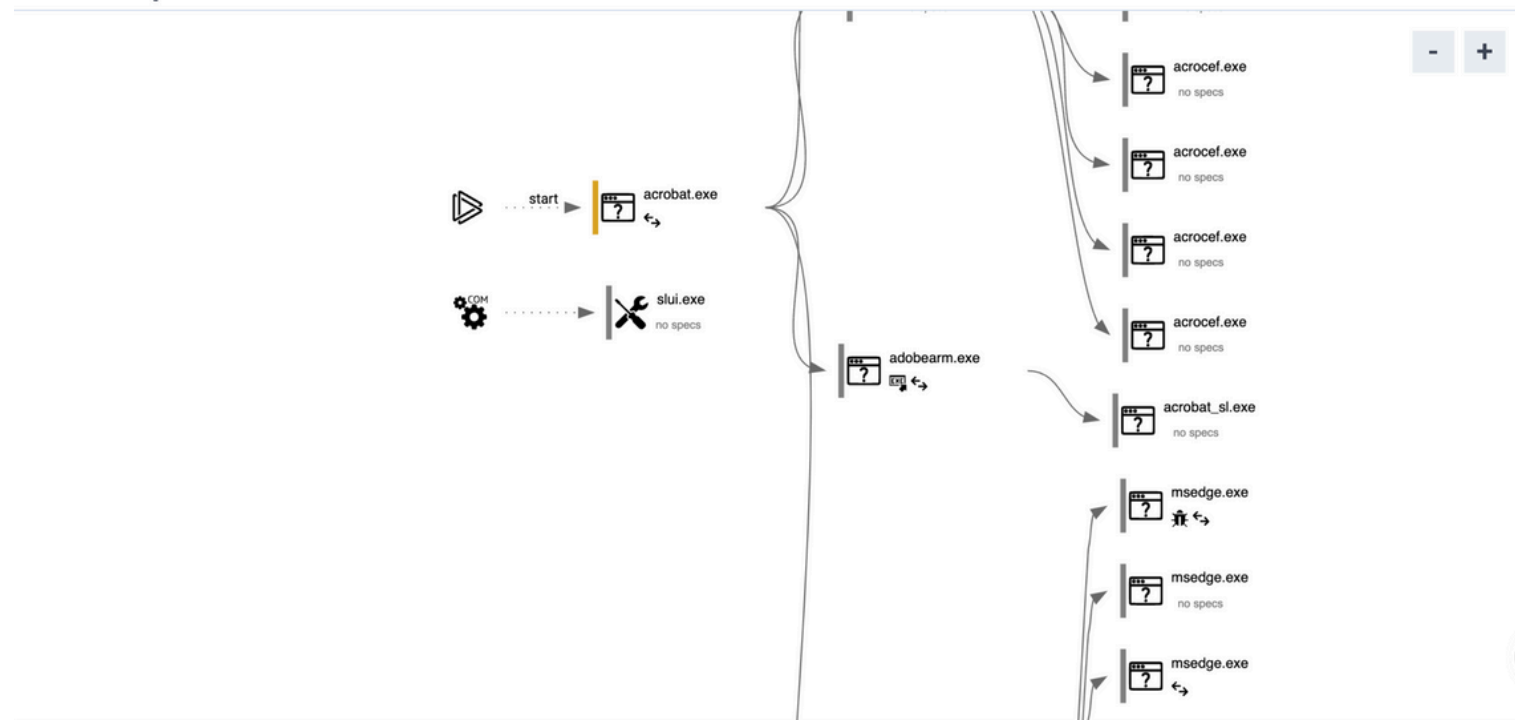
File name: data.pdf
Full analysis: <https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf>
Verdict: **Malicious activity**
Analysis date: July 26, 2024 at 08:20:40
OS: Windows 10 Professional (build: 19045, 64 bit)
Tags: **generated-doc** **phishing**
Indicators: 
MIME: application/pdf
File info: PDF document, version 1.7, 1 pages
MD5: 0D06D5045BC3830E9CB90DE1D46EEF01
SHA1: C50A73C13C29A392BA00DC8E9DF7B44815E4EEAD
SHA256: AE5C5FC7DFED3A2A19405B35FBAE8F3D82D285FC85
SSDEEP: 3072:TMJMarkKziW9WSgoMqi/Hq+CGQUf0wyah:IKGN



Il processo **msedge.exe** (che sarebbe il browser di default su windows 10), viene sfruttato per aprire un **url contenente svariati parametri**. Sembra un url costruito per nascondere l'effettivo sito web di destinazione (anche se tanto nascosto alla fine non è).

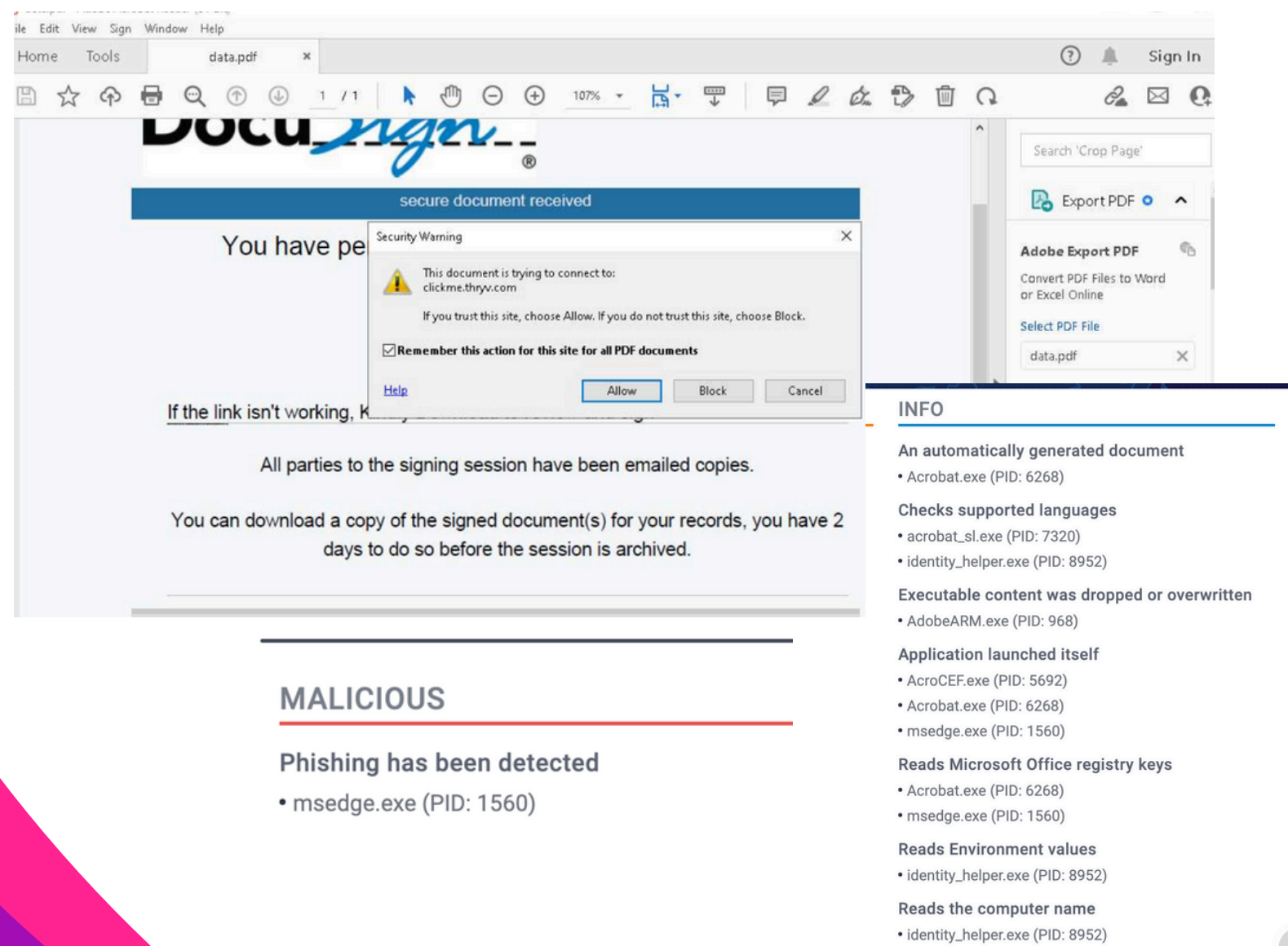
DATA.PDF

Dal grafo dell'analista e dal report, a parte i primi due processi di cui uno riguarda la licenza di windows, sembrerebbe si tratti di un documento generato automaticamente. Una sorta di spearphishing mirato. Adobe reader, lettore pdf, apre il file. Tra i vari processi che lancia c'è quello postato nella slide precedente, che contiene il link di phishing:



DATA.PDF

Analizzando il comportamento del malware dagli screenshot forniti dall'analista, noto che il documento richiama l'attenzione dell'utente incitandolo a firmare. Improvvisamente appare l'alert che avverte del redirect al sito di phishing:



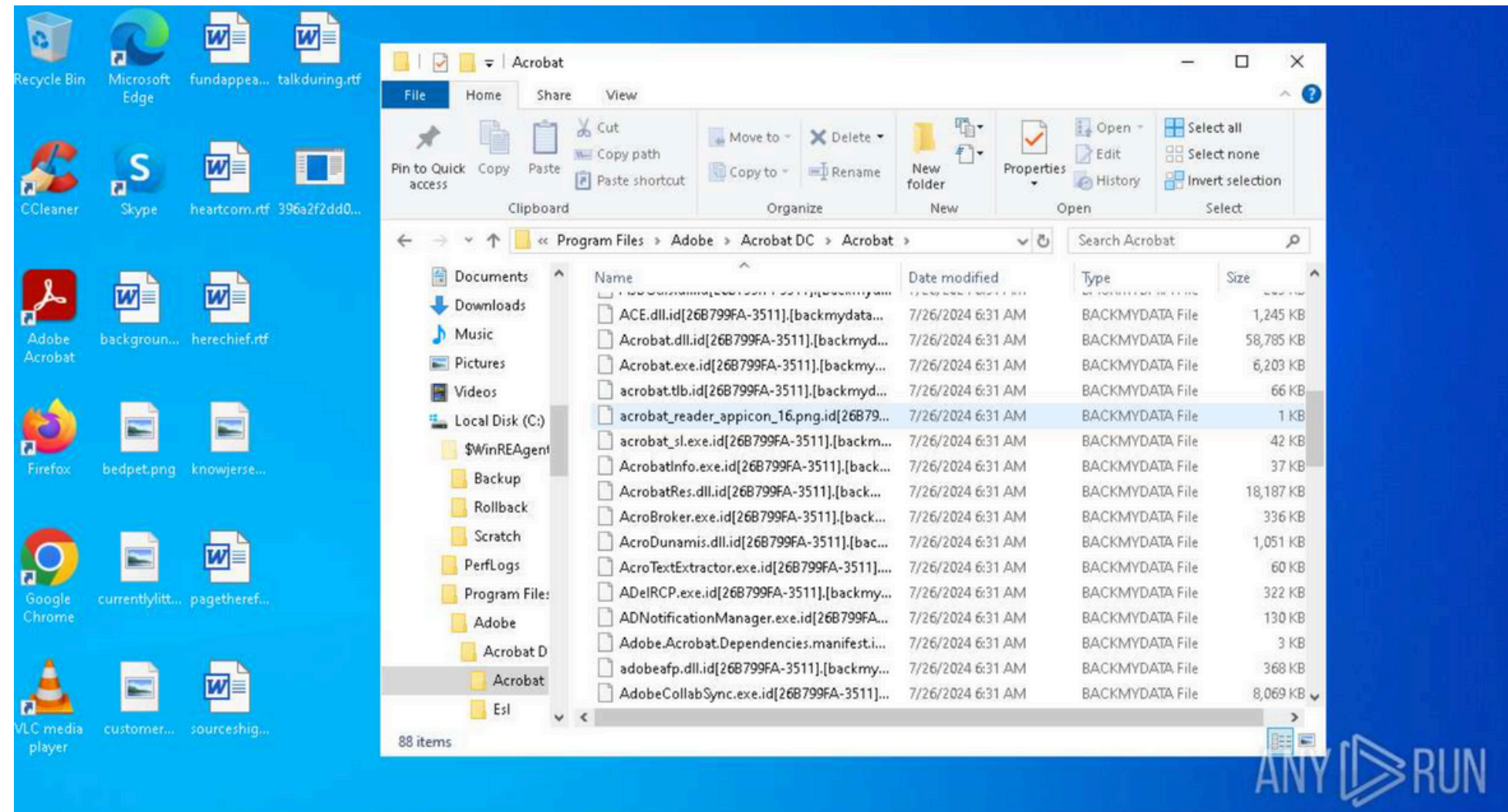
Il PDF è stato generato automaticamente da un'applicazione o script, come indicato dai processi coinvolti. I file acrobat.exe e AcroCEF.exe sono associati alla gestione e visualizzazione di PDF, mentre identity_helper.exe gestisce identificatori utente e AdobeARM.exe è legato agli aggiornamenti di Adobe Reader. Il documento evidenzia anche attività come la lettura di chiavi di registro e valori ambientali, indicando un'integrazione tra applicazioni e un avvio automatico di Acrobat senza intervento diretto dell'utente.

COME DIFENDERSI

Per difendersi, mantieni aggiornati il software e i sistemi di sicurezza per rilevare attività sospette e potenziali minacce. Inoltre, verifica attentamente l'origine e la legittimità dei documenti e dei processi automatizzati, evitando di aprire file o link non verificati.

RANSOMWARE/STEALER PHOBOS

Phobos è un **ransomware** che blocca o crittografa i file per richiedere un riscatto. Utilizza la crittografia AES con diverse estensioni, il che non lascia alcuna possibilità di recuperare i file infetti. Inoltre, ottiene accesso non autorizzato alle informazioni degli utenti e le trasferisce agli attaccanti.



RANSOMWARE PHOBOS

E' un'analisi molto lunga, ma in linea di massima Il ransomware in questione si attiva immediatamente all'avvio, rilasciando un file eseguibile con il nome **396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe**, che si manifesta in più processi con diversi **PID**. Questo file modifica il registro per eseguire **se stesso automaticamente**, rinomina i file compromessi e utilizza comandi per eliminare le copie **shadow** e modificare le opzioni di ripristino con **BCDEDIT.EXE**. Per nascondere le sue tracce, il ransomware elimina file di sistema legittimi, crea file con nomi simili a quelli di sistema e manipola il file desktop.ini per mascherare le cartelle. Inoltre, legge informazioni di sicurezza e di sistema, come le impostazioni di Internet Explorer e la data di installazione di Windows. Il ransomware avvia anche cmd.exe per eseguire comandi e VSSVC.exe, vds.exe, e wbengine.exe per attività di servizio. Infine, gestisce e controlla le impostazioni della posizione del computer e le informazioni del server proxy.

COPIE SHADOW?

Eh già. Il ransomware a quanto pare prevede tutto. Le copie shadow, gestite dal Volume Shadow Copy Service (VSS) di Windows, permettono di creare backup di file e cartelle anche mentre sono in uso, conservando versioni precedenti per il recupero. Questi backup periodici facilitano il ripristino dei dati in caso di perdita o corruzione. Tuttavia, come in questo caso, i ransomware mirano a eliminare queste copie **per impedire il recupero dei dati compromessi**.



IL BACKUP E' QUELLA COSA CHE ANDAVA FATTA PRIMA

Per difendersi da un **ransomware**, è cruciale adottare una strategia proattiva. Inizia con **backup regolari** dei tuoi dati su supporti **esterni** o nel **cloud**, mantenendo queste copie isolate dalla rete principale. Assicurati che il sistema operativo e le applicazioni siano **sempre aggiornati con le ultime patch di sicurezza**. Utilizza un software antivirus e anti-malware aggiornato per rilevare e bloccare minacce. Evita di aprire allegati o cliccare su link sospetti nelle email. **Limita i privilegi di accesso per ridurre la diffusione delle infezioni e fornisci formazione continua agli utenti sui segnali di attacchi ransomware.**

GRAZIE



Flavio Scognamiglio