

S9-L5 Extra

Extra Link 1

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

Da questa schermata possiamo prendere coscienza del fatto che il file data.pdf (un file identificato come malevolo) sia stato eseguito su Win 10 Pro. Questo file, avviato, genera automaticamente un doc.

Tra i vari IOC possiamo vedere come questo file determina, una volta lanciato, l'avvio automatico di diversi eseguibili (sotto riportati) e legge anche le chiavi di registro di Microsoft Office:

Application launched itself

- AcroCEF.exe (PID: 5692)
- Acrobat.exe (PID: 6268)
- msedge.exe (PID: 1560)

Reads Microsoft Office registry keys

- Acrobat.exe (PID: 6268)
- msedge.exe (PID: 1560)

Fra le varie azioni che compie ritroviamo quella di modifica del file system; tale file crea, modifica ed elimina file sul sistema, cambiamenti che probabilmente servono ad alimentare i payloads malevoli o per garantirsi un accesso persistente.

Registry activity

☒ Add for printing 

Total events	Read events	Write events	Delete events
30 376	30 206	166	4

Modification events

(PID) Process: (6268) Acrobat.exe	Key: HKEY_CLASSES_ROOT\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppContainer\Mappings\S-1-15-2-2034283098-2252572593-1072577386-2659511007-3245387615-27016815-3920691934
Operation: write	Name: DisplayName
Value: Adobe Acrobat Reader Protected Mode	
(PID) Process: (6136) Acrobat.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\ExitSection
Operation: write	Name: bLastExitNormal
Value: 0	
(PID) Process: (6136) Acrobat.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVEntitlement
Operation: write	Name: bSynchronizeOPL
Value: 0	
(PID) Process: (6136) Acrobat.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation: write	Name: aDefaultRHPViewMode_L
Value: Expanded	
(PID) Process: (6136) Acrobat.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation: write	Name: bExpandRHPInViewer
Value: 1	
(PID) Process: (6136) Acrobat.exe	Key: HKEY_CURRENT_USER\SOFTWARE\Adobe\Adobe Acrobat\DC\AVGeneral
Operation: write	Name: uLastAppLaunchTimeStamp
Value:	



Ecco le network activities:

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
15	71	51	0

HTTP requests

Viene categorizzato come phishing, cliccando su un link nel pdf si arriva ad un sito malevolo.
Questa tipologia di attacco è molto pericolosa che vedere come obiettivi principali la raccolta di:

- **Credenziali di Accesso:** Username e password per account di posta elettronica, banche, social media, e altri servizi online.
- **Informazioni Personali:** Numeri di previdenza sociale, date di nascita, indirizzi, numeri di telefono, ecc.
- **Informazioni Finanziarie:** Numeri di carte di credito, codici di sicurezza, conti bancari, ecc.
- **Dati Aziendali Riservati:** Segreti commerciali, piani strategici, liste clienti, ecc.
- **Dati Sanitari:** Cartelle cliniche e informazioni sanitarie personali.
- Compromissione degli Account.
- Installazione di malware.
- Espansione della botnet.

Per proteggerci da questa tipologia di attacco necessitiamo di:

Consapevolezza e Formazione

- 1. **Educazione Continua:** informarsi e partecipare a programmi di formazione sulla sicurezza informatica.
- 2. **Riconoscere i Segnali di Phishing:** imparare ad identificare le caratteristiche comuni delle email di phishing, come errori grammaticali, URL sospetti, richieste urgenti di informazioni personali.

Pratiche Sicure

- 1. **Non Cliccare su Link Sospetti:** evitare di cliccare su link in email o messaggi sospetti.
- 2. **Non Scaricare Allegati da Fonti Sconosciute:** non aprire allegati in email di mittenti sconosciuti o inaspettati.
- 3. **Verifica dell'Identità del Mittente:** se ricevi una richiesta sospetta da un collega o conoscente, verifica la richiesta con un altro mezzo di comunicazione (es. telefono).

Strumenti di Sicurezza

- 1. **Utilizzare Software Anti-Phishing:** installare ed aggiornare regolarmente software anti-phishing e antivirus.
- 2. **Configurare i Filtri Email:** utilizzare filtri email per ridurre il numero di email di phishing che raggiungono la tua casella di posta.

Monitoraggio e Risposta

- 1. **Monitoraggio degli Account:** controllare regolarmente gli account per attività sospette.
- 2. **Segnalazione di Phishing:** segnalare tentativi di phishing al proprio provider di email.

Procedure Aziendali

- 1. **Politiche di Sicurezza:** implementare politiche di sicurezza aziendali rigorose che includano protocolli specifici per prevenire, riconoscere e rispondere agli attacchi di phishing.
- 2. **Simulazioni di Phishing:** eseguire test di phishing interni per valutare la consapevolezza dei dipendenti e migliorare la formazione.

Extra Link 2

Il secondo link, invece tratta di un report eseguito su un ramsonware, ecco le generalità:

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 extensions, which leaves no chance to recover the infected files.

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

Malware Trends Tracker >>>

S9-L5 Extra

3

Ecco, invece, la lista di attività malevole che tale ramsonware attua:

MALICIOUS

- Drops the executable file immediately after the start
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
 - 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)
- Changes the autorun value in the registry
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4432)
- PHOBOS has been detected
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)
- Using BCDEDIT.EXE to modify recovery options
- cmd.exe (PID: 1256)
- Deletes shadow copies
- cmd.exe (PID: 1256)
- Renames files like ransomware
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)
- Actions looks like stealing of personal data
- 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe (PID: 4180)

Anche questo malware va a modificare vari file, ecco i numeri precisi:

Registry activity

Total events	Read events	Write events	Delete events
2 301	2 231	50	20

Modification events

(PID) Process:	(2348) 396a2f2dd09c936e93d250e8467ac7a9c0a923ea7f9a395e63c375b877a399a6.exe	Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet S
Operation:	write	Name:	ProxyBypass
Value:	1		

Questo è il numero di richieste di network:

Network activity

HTTP(S) requests

2

TCP/UDP connections

18

DNS requests

9

Threats

0

Analizziamo qualche misura di protezione nei confronti di un attacco ransomware (principalmente si gioca d'anticipo cercando di limitare quanto più possibile i danni):

1. **Backup regolari:** effettuare backup periodici dei dati importanti su supporti esterni o nel cloud. Assicurarsi che i backup non siano collegati al sistema principale per evitare che vengano infettati.
2. **Software di sicurezza:** utilizzare antivirus e antimalware aggiornati.
Questi strumenti possono rilevare e bloccare molte minacce prima che causino danni.
3. **Aggiornamenti del sistema:** mantenere il sistema operativo, il software e le applicazioni aggiornati per sfruttare le patch volte a mitigare le vulnerabilità potenzialmente exploitabili dai ransomware.
4. **Limitare i privilegi:** utilizzare account utente con privilegi limitati (privilegio minimo) per ridurre l'impatto dell'eventuale attacco (se e quando accadrà).
Solo gli amministratori dovrebbero avere diritti di amministratore.
5. **Firewall e filtri di rete:** implementare firewall e filtri di rete per bloccare il traffico sospetto e impedire che i ransomware comunichino con i server di comando e controllo.

Buone pratiche restano:

- Formare adeguatamente il personale (questo punto è collegato al phishing dato che i ransomware, spesso, diffondono tramite email di phishing);
- Controllare gli accessi ed implementare politiche di controllo degli stessi;
- Segmentazioni della rete per limitare la diffusione del ramsonware
- Monitoraggio continuo della rete.

I ramsonware causano molti danni, tra i principali:

- Perdita di dati, questi vengono crittografati e resi inaccessibili;
- Interruzioni delle attività, tale attacco può paralizzare molti servizi;
- Costi di riscatto e costi di recupero;
- Danno reputazionale;
- Furto di dati ed informazioni.