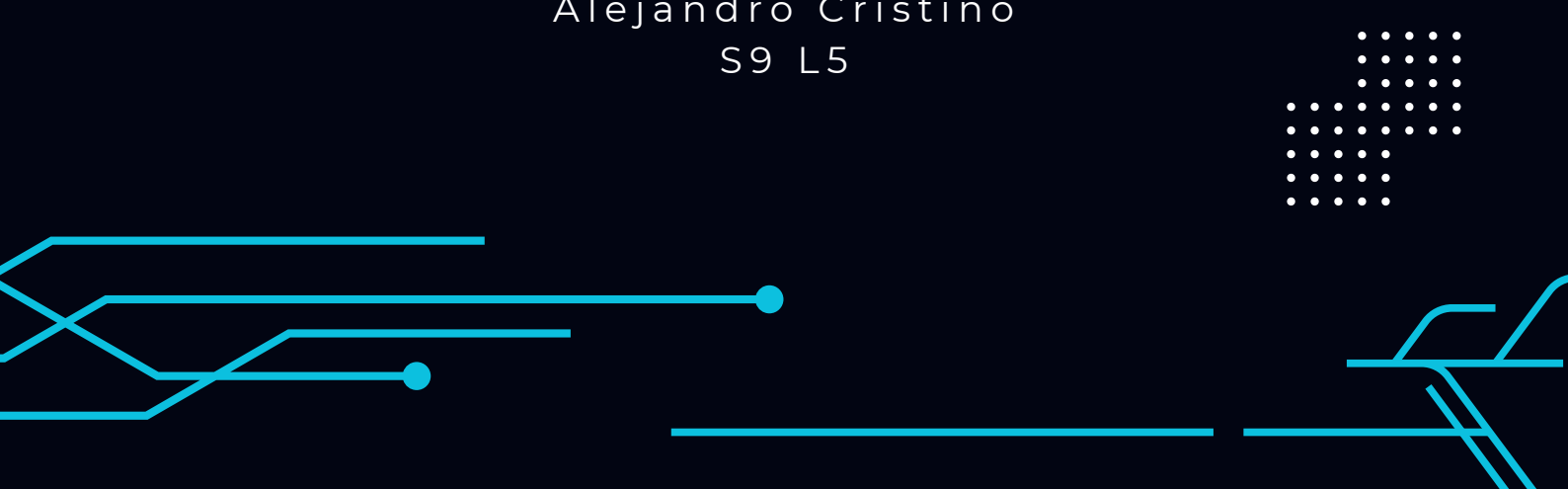




REPORT

BONUS

Alejandro Cristino
S9 L5



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:

1. <https://app.any.run/tasks/d6f73302-d491-4f13-bbfb-caf67648c7d6>
2. <https://app.any.run/tasks/70555e9b-3e91-4126-bb9e-567fcbeb0ac2>

1. Report sull'analisi dell'Attacco di Phishing

Questo report fornisce un'analisi dettagliata di un tentativo di attacco di phishing rilevato tramite un file PDF denominato "data.pdf". Questo report dettaglia il comportamento, i processi coinvolti e le raccomandazioni per prevenire futuri attacchi.

1.1. Descrizione dell'Attacco

- **Tipo di Minaccia:** Phishing
- **Descrizione:** Il file "data.pdf" contiene un documento che simula una comunicazione da parte di DocuSign, un servizio legittimo di firma elettronica. Il documento invita l'utente a cliccare su un link per rivedere e firmare un documento, inducendo un senso di urgenza.

1.2. Attività Malevole Identificate

Processi:

- **All'apertura del file PDF,** vengono eseguiti diversi processi legati a Acrobat.exe. Questo comportamento suggerisce che il file tenta di eseguire azioni non autorizzate, come il download di ulteriori componenti o il collegamento a server remoti.

Connessioni di Rete:

- **Richieste HTTP:** Il file effettua numerose richieste HTTP, alcune delle quali sono dirette a siti legittimi come acroipm2.adobe.com e ocsp.digicert.com, probabilmente per camuffare la sua attività malevola. Tuttavia, le richieste a URL come clickme.ithryv.com e shore-hub.com indicano tentativi di esfiltrazione di dati o ulteriori infezioni del sistema.
- **Risposte 404:** Diversi tentativi di connessione hanno restituito un errore 404 (Not Found), suggerendo che alcune risorse potrebbero non essere più disponibili o che il server di comando e controllo non è raggiungibile.



1.3. Indicatori di Compromissione

MD5 del File: 0D6D5045BC38309ECB90DE1D46EEF01

URL Malevoli:

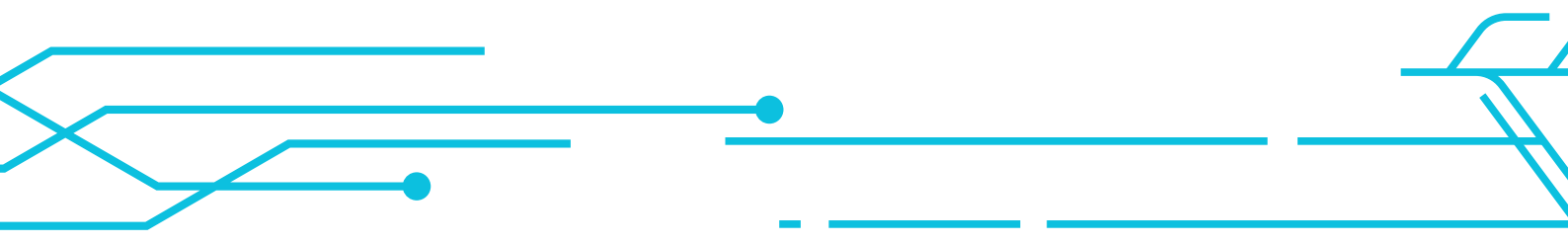
- <https://clickme.ithryv.com>
- <https://shore-hub.com>

1.4. Raccomandazioni per Utenti e Manager

Per gli Utenti:

- **Evitare di cliccare su link sospetti:** Non cliccare su link in email o documenti non richiesti, specialmente se non riconosciuti.
- **Verifica delle Email:** Controllare attentamente il mittente e il contenuto delle email. In caso di dubbio, contattare direttamente l'azienda o il servizio indicato per verificare la legittimità del messaggio.

Per i Manager:

- **Formazione sulla Sicurezza:** Implementare programmi di formazione continua per educare i dipendenti sui rischi di phishing e su come identificarli.
 - **Soluzioni di Sicurezza Avanzate:** Utilizzare software antivirus e antimalware aggiornati, insieme a firewall e sistemi di prevenzione delle intrusioni (IPS), per monitorare e bloccare attività sospette.
 - **Monitoraggio e Risposta:** Stabilire protocolli chiari per il monitoraggio del traffico di rete e per la risposta agli incidenti, includendo la quarantena di macchine compromesse e la notifica agli utenti di potenziali minacce.
 - **Aggiornamenti Regolari:** Assicurarsi che tutti i sistemi e i software siano aggiornati con le ultime patch di sicurezza per minimizzare le vulnerabilità.
 - **Controllo degli Accessi:** Implementare politiche rigorose di controllo degli accessi per limitare i privilegi degli utenti e prevenire la diffusione delle minacce.
- 

2. Report sull'analisi del Malware

Dall'analisi eseguita tramite la piattaforma Any.Run, è emersa un'infezione da ransomware Phobos. Questo report dettaglia il comportamento del malware, i processi coinvolti e le raccomandazioni per prevenire futuri attacchi.

2.1. Descrizione dell'Attacco

- **Tipo di Minaccia:** Phobos ransomware, stealer
- **Descrizione:** Il ransomware Phobos è progettato per criptare file, rendendo i dati inaccessibili e richiedendo un riscatto per decriptarli. A seguito di questo tipo di attacco, il malintenzionato modifica le impostazioni di sistema per prevenire il ripristino facile, richiedendo pagamenti in criptovaluta in cambio delle chiavi di decrittazione.

2.2. Attività Malevole Identificate

Processi:

- **cmd.exe:** Avviato per eseguire comandi di sistema.
- **conhost.exe:** Utilizzato per gestire i prompt dei comandi.
- **bcdedit.exe:** Utilizzato per modificare le impostazioni di boot, con comandi che disabilitano le politiche di ripristino.
- **wbadmin.exe:** Potrebbe essere utilizzato per manipolare backup.
- **Altri processi:** vsfvc.exe, slui.exe, wbengine.exe, vdsldr.exe, vds.exe, notepad++.exe.

Connessioni di Rete:

- **HTTP Requests:** Connessioni a ocsp.digicert.com per verificare certificati digitali, che potrebbero facilitare comunicazioni sicure del malware.
- **Processi di Comunicazione:** SearchApp.exe e OfficeClickToRun.exe hanno effettuato richieste GET.

2.3. Indicatori di Compromissione

MD5 del file: C5A2EBF80A9A01E79D7CFBDFD3F54877

Modifiche ai File:

- Numerosi file nella directory di Acrobat sono stati rinominati con estensioni **.BACKMYDATA**, indicativo di file criptati dal ransomware.

2.4. Raccomandazioni per Utenti e Manager

Per gli Utenti

- **Identificare e-mail di phishing:** Non aprire allegati o cliccare su link in e-mail sospette. Verificare sempre la legittimità del mittente.
- **Pratiche di Navigazione Sicura:** Evitare di scaricare software o file da fonti non affidabili.
- **Backup Regolari:** Salvare periodicamente i propri dati in una posizione sicura e separata (ad esempio, un hard disk esterno).
- **Aggiornamento dei Software:** Mantenere aggiornati tutti i software, incluso il sistema operativo e le applicazioni utilizzate.
- **Antivirus e Antimalware:** Eseguire scansioni regolari con software antivirus e antimalware.
- **Password Forti:** Utilizzare password complesse e uniche per ogni account.

Per i Manager

- **Implementazione di Backup Centralizzati:** Assicurarsi che esistano backup regolari dei dati aziendali e che questi siano testati periodicamente per verificarne l'integrità.
- **Aggiornamenti e Patch:** Stabilire una politica per aggiornare regolarmente tutti i sistemi e applicazioni.
- **Limitare i Privilegi:** Assegnare ai dipendenti solo i permessi necessari per svolgere il loro lavoro.
- **Autenticazione a Due Fattori (2FA):** Implementare 2FA per tutti gli accessi ai sistemi aziendali.
- **IDS/IPS:** Implementare sistemi di rilevamento e prevenzione delle intrusioni.
- **Monitoraggio del Traffico di Rete:** Utilizzare strumenti per monitorare il traffico di rete e rilevare attività sospette.
- **Procedure di Risposta:** Stabilire e testare regolarmente procedure di risposta agli incidenti per contenere e mitigare rapidamente eventuali infezioni.
- **Formazione Continua:** Organizzare sessioni di formazione continua per il personale sulla sicurezza informatica e le nuove minacce.