RANSOMWARE: ANALISI TECNICA E CONSIDERAZIONI GIURIDICHE ALLA LUCE DEL CASO CONTI

Candidato: Morandini Giulio, giulio.morandini1@edu.unifi.it

Relatore: Pietropaoli Stefano, stefano.pietropaoli@unifi.it

Correlatore: Pugliese Rosario, rosario.pugliese@unifi.it

Riassunto:

L'obiettivo principale della tesi è quello di analizzare il problema del ransomware, approfondendolo con uno studio del caso del gruppo Conti.

In una prima fase analizzerò il problema ransomware in sè, studiandone le tipologie e come funziona un attacco di questo tipo. Per fare ciò utilizzerò un piccolo ransomware molto semplice che ho scritto personalmente.

Focalizzeremo l'attenzione soprattutto sulle conseguenze che un attacco di questo genere può avere in una rete aziendale, analizzandone anche possibili tecniche di prevenzione e un efficace ripristino dei dati.

Queste tecniche dovranno essere seguite e aggiornate costantemente, mantenendole al passo coi tempi per poter ottenere risultati soddisfacenti.

Questo perchè i ransomware sono in continua evoluzione, e la seconda parte dell'elaborato ha l'obiettivo di analizzare questo fatto, con una particolare focus sul caso Conti. Verrà approfondita la composizione del gruppo e il modus operandi, analizzando l'attacco alle strutture IT della Costa Rica del 2022. Successivamente verranno descritti i nuovi gruppi cybercriminali, come scrivono i loro malware e le correlazioni che possono avere col gruppo Conti, prendendo come esempio il gruppo 3AM e come esso abbia sviluppato le tecniche di profilazione ed estorsione dei dati, utilizzando anche i social network. Proprio parlando di Conti, l'ultimo capitolo dell'elaborato analizzerà nel dettaglio il codice del malware utilizzato dal gruppo criminale.

Verranno studiati gli argomenti dell'eseguibile, l'offuscamento degli API e delle stringhe, le note per il riscatto e il portale web, la rimozione delle copie shadow, la strategia multi-thread, come il software applica la crittografia, la blocklist e la gestione dei file occupati, i file in whitelist e infine la scansione e la cifratura della rete.