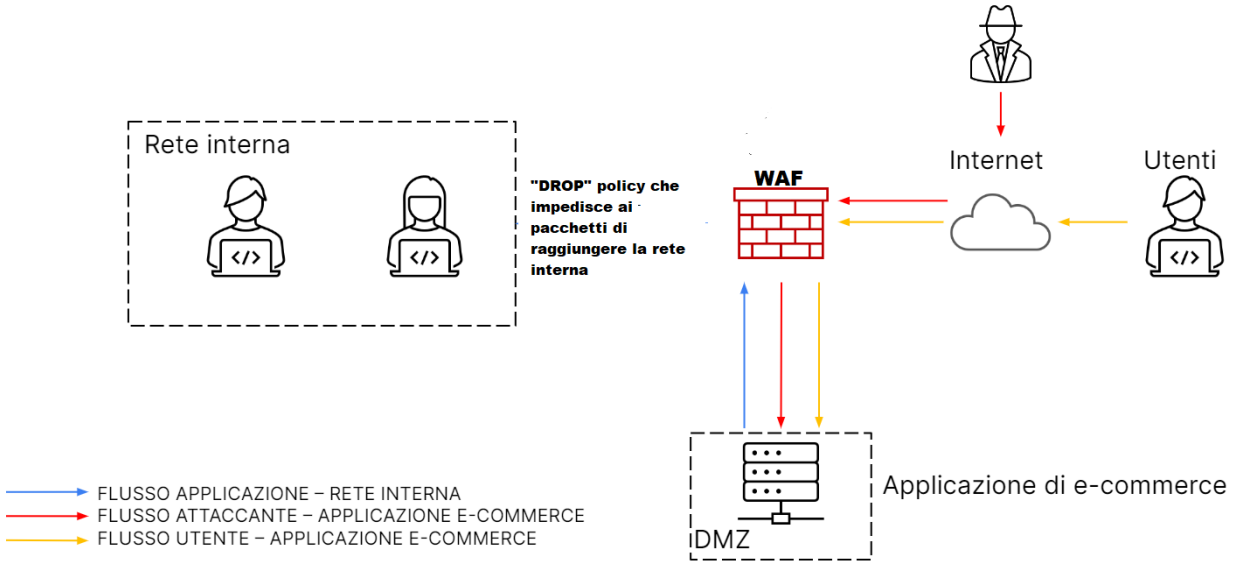
Di Edoardo Castelli

EPICODE Unit 3 Project 1

Il progetto settimanale di questa Unit prevede la messa in sicurezza di un server Web sul quale gira un servizio di e-commerce, attraverso il quale l'attaccante potrebbe avere accesso alla rete interna della compagnia che eroga il servizio.

1) Configurazione Infrastrutturale:

Nel primo punto della traccia in questione, è richiesto di implementare delle misure preventive con un budget minimo, motivo per cui, andando a rispettare quanto richiesto dal potenziale cliente e senza andare a stravolgere l'infrastruttura, si può implementare un firewall che possa agire anche come WAF (Web Application Firewall) e utilizzare come ulteriore linea di difesa una policy "Drop" che impedisca al flusso di traffico di raggiungere l'intranet dal Server, secondo lo schema presentato di seguito.



2) Analisi link malevoli:

In questo secondo punto è richiesto di analizzare il comportamento di probabili link malevoli utilizzati come vettori di attacco, con conseguente Report.

- **Report "Linklosco1":**

Una volta esaminato il link con tool quali Anyrun e Virustotal, sarà possibile concludere che tale risorsa nasconda in verità codice malevolo che permette ad un utente remoto di aprire una shell sulla macchina infetta.

General Info

Add for printing

URL:	https://gist.github.com/chinmay-sh/037cd30cf125202a8b85fffcc0c2cf42/raw/7154ffd746be8626495a6ae7073889972c458ddf/DNS_Changer.ps1
Full analysis:	https://app.any.run/tasks/8a2c185d-5a11-4aac-9286-43c641e1991a
Verdict:	Suspicious activity
Analysis date:	June 29, 2023 at 10:50:12
OS:	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Indicators:	
MD5:	7CD193E2B99F15030CA538B924B4498C
SHA1:	07A04D3C4279FFFE62968A4F76133B1AC71B490F
SHA256:	3B9E727C56BFA9A16E5311F8D17472B9DCBE2F1E149FA2924EDA013611076D39
SSDEEP:	3:N8tMCMEd2NMOYVVqJS3ERXM7JUqET+hdSadtSXG2dzKhYMN:21MEgNMOYVlUOadyfjSNWYMN

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Behavior activities

Add for printing

MALICIOUS

Bypass execution policy to execute commands
- powershell.exe (PID: 3300)

SUSPICIOUS

The process executes Powershell scripts
- powershell.exe (PID: 2272)

The process bypasses the loading of PowerShell profile settings
- powershell.exe (PID: 2272)

Reads the Internet Settings
- powershell.exe (PID: 2272)
- powershell.exe (PID: 3300)

Application launched itself
- powershell.exe (PID: 2272)

Using PowerShell to operate with local accounts
- powershell.exe (PID: 3300)

Starts POWERSHELL.EXE for commands execution
- powershell.exe (PID: 2272)

INFO

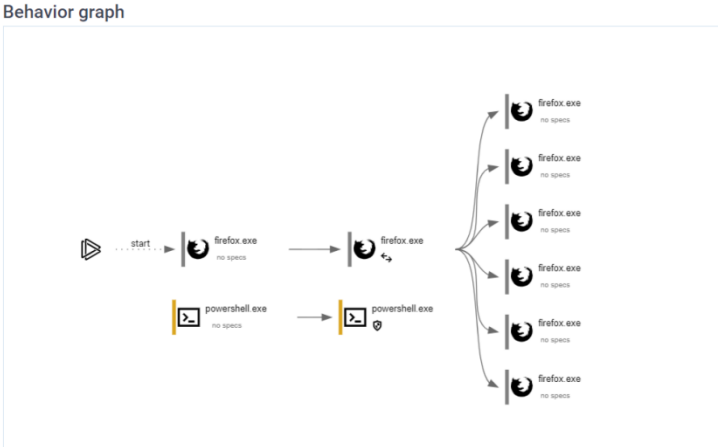
Application launched itself
- firefox.exe (PID: 2976)
- firefox.exe (PID: 3384)

The process uses the downloaded file
- powershell.exe (PID: 2272)
- firefox.exe (PID: 3384)

Manual execution by a user
- powershell.exe (PID: 2272)

Come si può notare dal feedback del tool, il link sopracitato non sembra riportare malware di sorta nel vero senso del termine, ma il codice iniettato sulla macchina va comunque a bypassare le policy di esecuzione della Powershell di Windows, andando ad operare sul funzionamento dei server DNS, concedendo di fatto all'attaccante l'esecuzione del prompt da remoto. Di seguito il comportamento del programma riportato dal tool Anyrun.

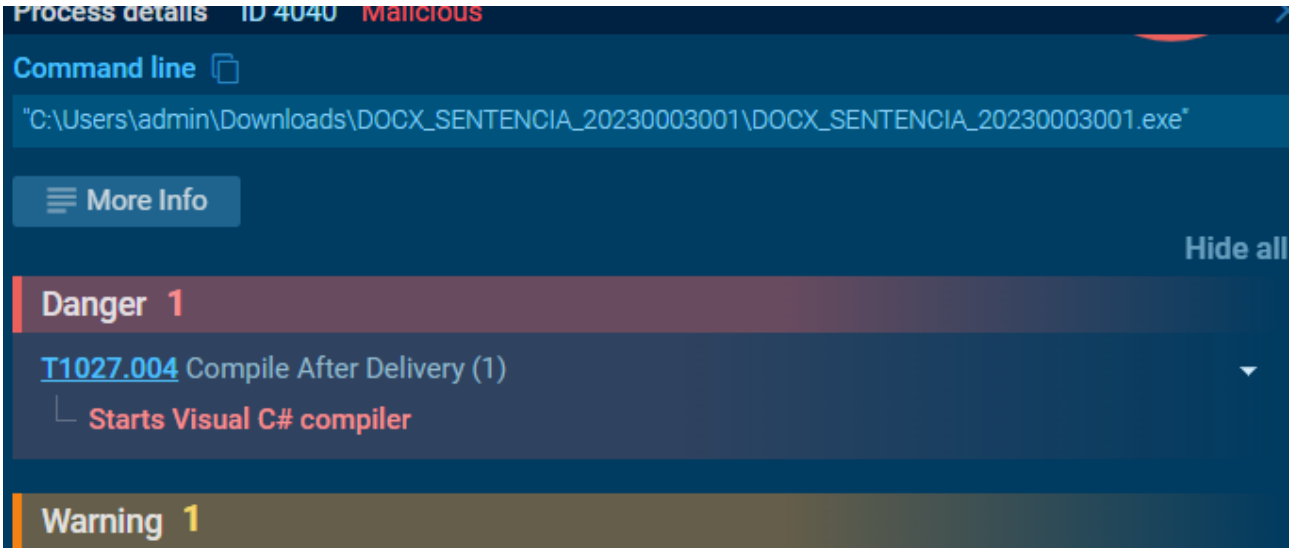
Behavior graph



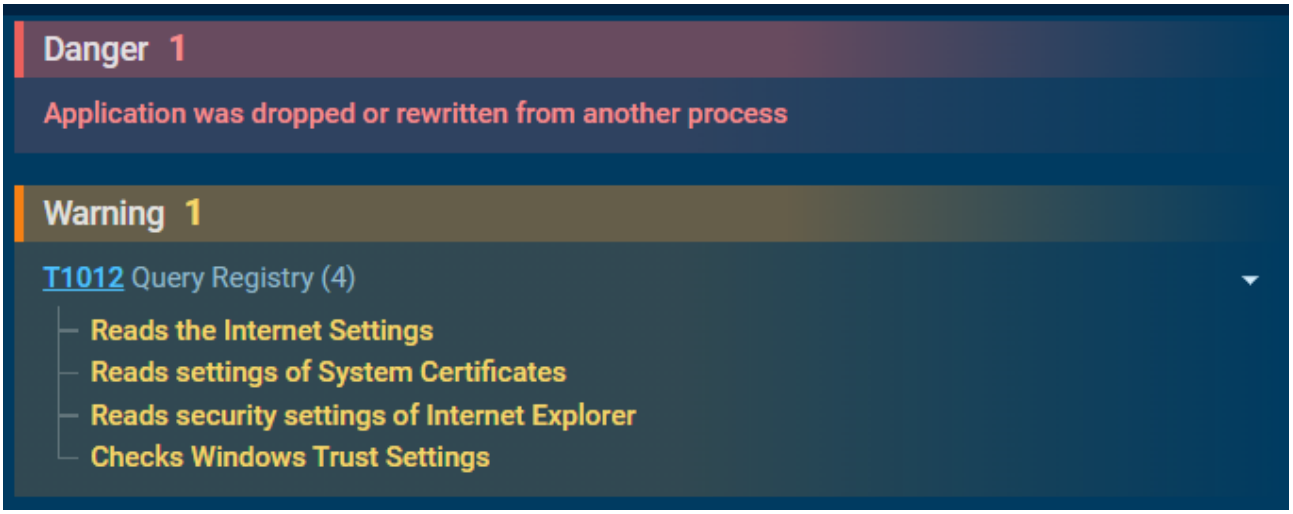
Si noti in particolare come l'attacco ha avuto successo tramite il download del link da Browser e come tramite lo stesso browser l'attaccante abbia accesso a Powershell.

- Report "Linklosco2":

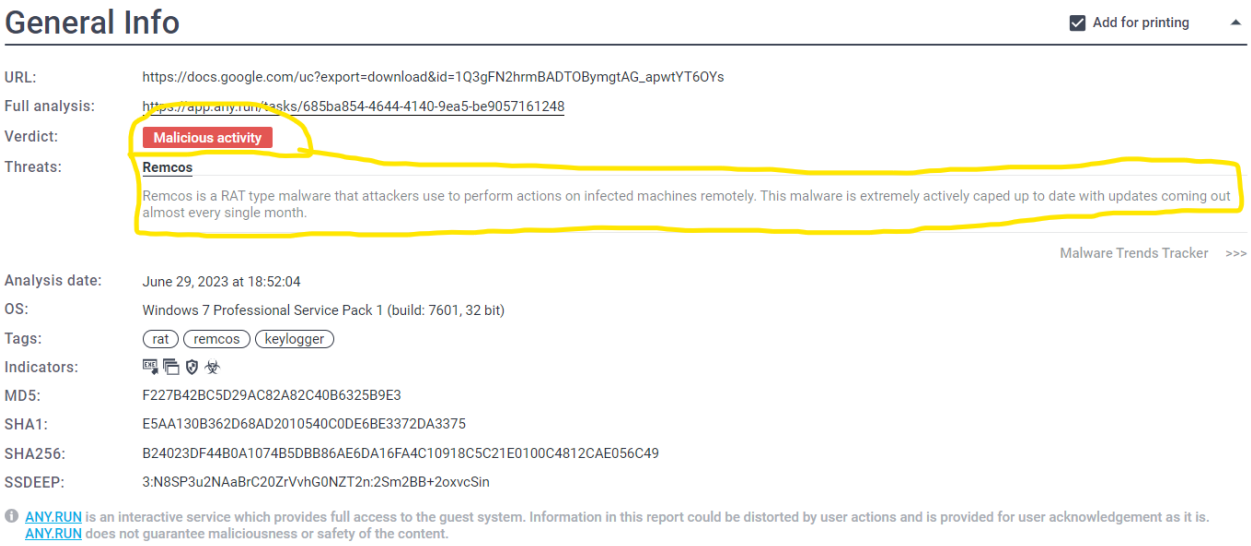
Anche con questo secondo link si procede mediante l'analisi di tool automatizzati, nello specifico i medesimi utilizzati per il primo. In questo caso, Anyrun presenta fin da subito la potenzialità che si tratti di un Malware, come si può notare dal compilatore che viene lanciato.



Si noti inoltre che il processo del probabile Malware viene inserito nel sistema attraverso un processo che verrà riscritto:



Alla luce di quanto fin'ora esaminato si continua con l'analisi dei processi e la lettura del report fornito dal tool, che andrà a confermare quanto già sospettato in base ai molteplici avvisi critici forniti dalla precedente analisi.



Il report testuale conferma definitivamente quanto già sospettato: un Malware è stato iniettato nella macchina bersaglio.

Nello specifico si tratta di Remcos, (acronimo di Remote Control & Surveillance Software), uno strumento commerciale di accesso remoto per controllare i computer bersaglio, appartenente alla categoria dei RAT (Remote Access Trojan).

Da documentazione ufficiale, Remcos è "pubblicizzato" come software legittimo che può essere utilizzato per scopi di sorveglianza e Pentest, ma è stato utilizzato in numerose campagne di hacking.

Compiuta l'installazione, il malware apre una backdoor sul computer, garantendo ad un utente remoto la totale libertà di azione sulla macchina infetta.
Quasi ironica è la provenienza di questo programma, in quanto è stato sviluppato dalla società di sicurezza informatica BreakingSecurity.
Si può inoltre notare dallo screen che segue, quanto avanzato sia il malware esaminato in base al numero di processi autonomi che riesce ad eseguire una volta compilato e lanciato.

Behavior activities

Add for printing

MALICIOUS

Application was dropped or rewritten from another process
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Starts Visual C# compiler
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Uses Task Scheduler to run other applications
- cmd.exe (PID: 3604)
- cmd.exe (PID: 3200)
- cmd.exe (PID: 2628)
- cmd.exe (PID: 2960)

Remcos is detected
- csc.exe (PID: 3824)

REMCOS detected by memory dumps
- csc.exe (PID: 3824)

SUSPICIOUS

The process creates files with name similar to system file names
- WinRAR.exe (PID: 1944)

Drops a system driver (possible attempt to evade defenses)
- WinRAR.exe (PID: 1944)
- procexp.exe (PID: 3476)

Reads settings of System Certificates
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads security settings of Internet Explorer
- Autoruns.exe (PID: 4056)
- procexp.exe (PID: 3476)

Reads the Internet Settings
- Autoruns.exe (PID: 4056)
- csc.exe (PID: 3824)

Connects to unusual port
- csc.exe (PID: 3824)

Starts CMD.EXE for commands execution
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)

INFO

The process uses the downloaded file
- chrome.exe (PID: 2064)
- chrome.exe (PID: 2356)
- chrome.exe (PID: 1140)
- WinRAR.exe (PID: 1944)
- chrome.exe (PID: 3868)
- WinRAR.exe (PID: 3092)
- chrome.exe (PID: 2880)

Application launched itself
- chrome.exe (PID: 3140)

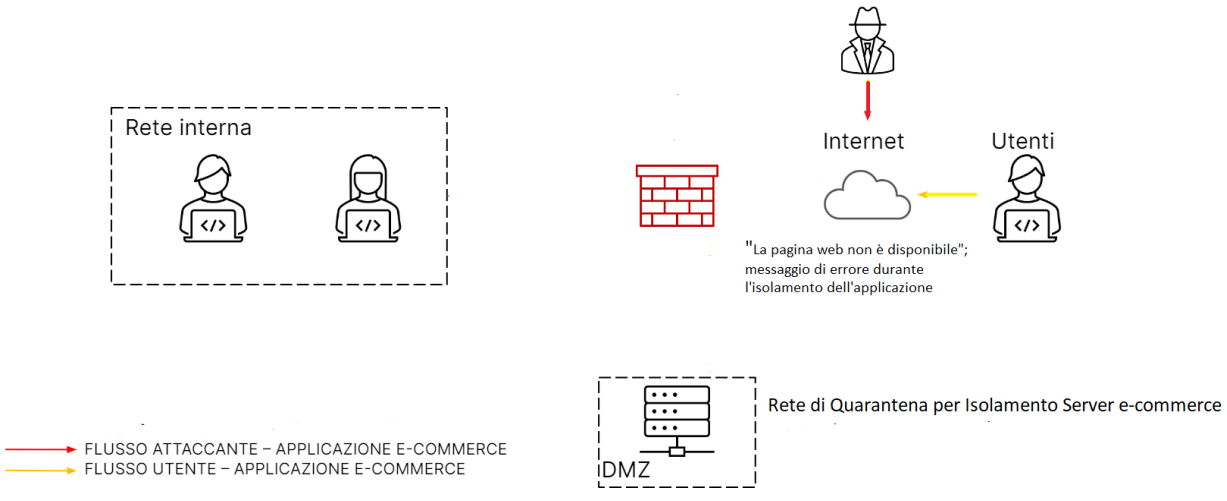
Manual execution by a user
- WinRAR.exe (PID: 1944)
- Autoruns.exe (PID: 4056)
- WinRAR.exe (PID: 3092)
- DOCX_SENTENCIA_20230003001.exe (PID: 4040)
- wmpnscfg.exe (PID: 1156)
- DOCX_SENTENCIA_20230003001.exe (PID: 3912)
- DOCX_SENTENCIA_20230003001.exe (PID: 2432)
- DOCX_SENTENCIA_20230003001.exe (PID: 312)

Executable content was dropped or overwritten
- WinRAR.exe (PID: 1944)

Per una visualizzazione più chiara della struttura, si raccomanda la consultazione del "Behavior Graph" proposto da Anyrun.

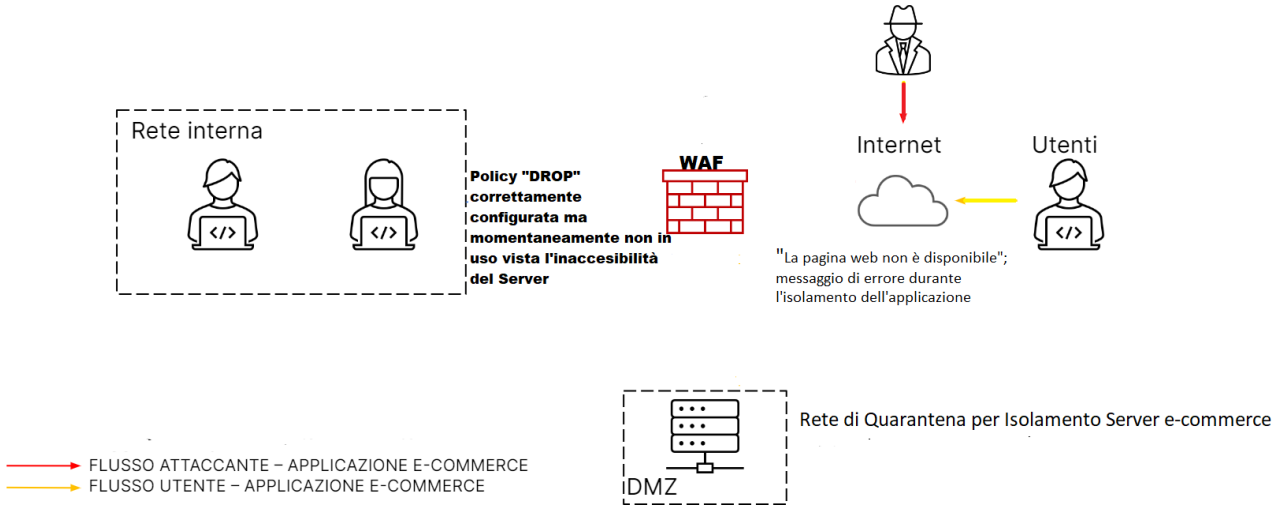
3)Incident Response all'iniezione di un Malware:

Nel terzo punto della traccia è richiesto di intervenire sullo stesso server di e-commerce già visto precedentemente, una volta però che lo stesso risulti essere infetto da un Malware. In accordo con le richieste, si procede quindi con l'Isolamento del server per evitare la divulgazione di dati sensibili sul web e il potenziale rischio di infezione di altre macchine connesse al medesimo, tra cui quelle dell'Intranet, creando una rete di Quarantena in accordo con la figura che segue.



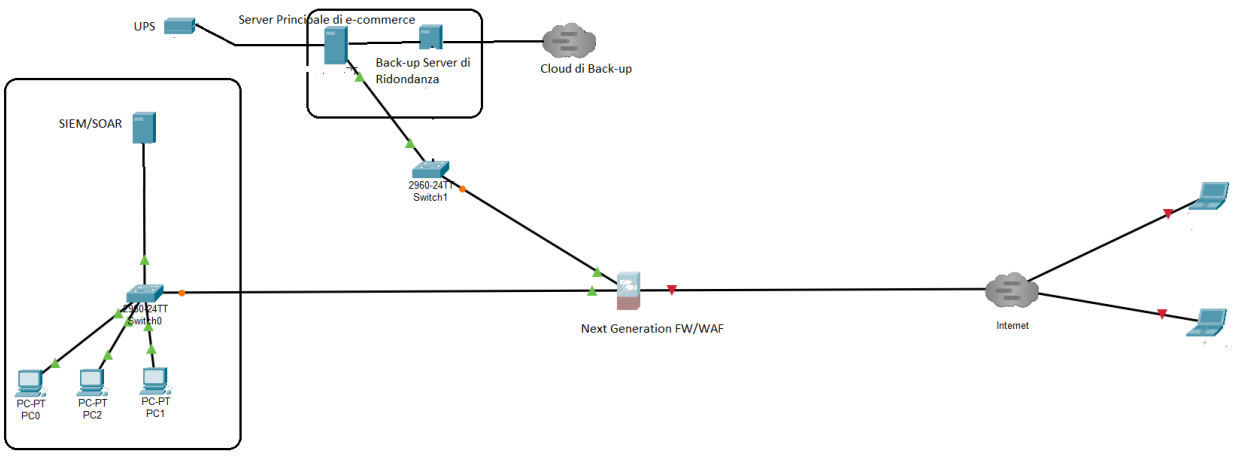
4) Unione dei punti 1 e 3 della traccia:

Nel penultimo punto del lavoro odierno, si richiede di mostrare dunque la dinamica dell'Incident Response sulla rete correttamente configurata in accordo al punto 1. Di seguito la rappresentazione grafica.



5) Miglioramento dell'Infrastruttura con maggior budget:

In conclusione viene richiesta una possibile configurazione di rete più sicura ed articolata, partendo dal presupposto di avere un cospicuo budget a disposizione rispetto a quanto ipotizzato al punto 1. Con il budget a nostra disposizione (una cifra di "media entità"), sarà possibile aumentare notevolmente le difese dell'infrastruttura, pur non arrivando, chiaramente, agli standard di grandi aziende multinazionali.



In accordo con l'immagine di cui sopra e con il budget sopracitato (inferiore a 50/60.000 euro), si decide di proporre al cliente un'implementazione senz'altro notevole ai fini dell'aumento della sicurezza che comprende:

- **Un Firewall di nuova generazione anche configurabile come WAF (circa 10/12.000 euro)**
- **Un UPS ad alto Wattaggio che garantisca circa venti minuti di autonomia in caso di assenza di corrente (8.000 euro)**
- **Un SIEM che centralizzi i controlli dei log ed un SOAR per la gestione delle minacce (2.000 euro cad.)**
- **Un secondo Server di Back-Up che garantisca il principio della ridondanza (5.000 euro)**
- **Un Cloud su cui eseguire back-up dei server come ulteriore garanzia (2.000 euro /anno ca.)**
- **Qualora si volesse aggiungere ulteriore protezione ai Server e si fosse disposti a spendere ulteriormente, sarebbe possibile aggiungere Condizionatori per il raffreddamento dei Server e misure di sicurezza per la sala quali controlli delle impronte digitali e guardie armate (10.000).**