UNIVERSITÀ DI PISA

Dipartimento di Informatica

Corso di Laurea Triennale in Informatica

Scripting e patching: soluzioni per sicurezza e business continuity con Datto RMM e Autotask PSA

Relatori:

Nikolai Asatiani

Prof. Luca Deri

Presentata da:

Alessandro Cecchi

Sessione invernale

Anno Accademico 2018/2019

Indice

Sommario

I sistemi di monitoraggio e gestione remota e di automazione dei servizi professionali calati nel mondo delle piccole e medie imprese italiane sono in grado di garantire adeguati standard di sicurezza e business continuity. Dopo un breve panoramica sulle principali soluzioni disponibili l'elaborato descrive il lavoro svolto con Datto RMM e Autotask PSA partendo dall'analisi dei problemi da risolvere e giungendo fino alla messa a punto delle soluzioni a questi.

1 Introduzione

In un mondo informatizzato e interconnesso sempre più, anche le piccole e medie imprese del territorio italiano hanno sentito la necessità di dotarsi dei più moderni sitemi di monitoraggio e gestione remota. Il monitoraggio di una grande infrastruttura distribuita non è, tuttavia, un compito poco impegnativo. Le infrastrutture da gestire sono rapidamente cambiate per forma e dimensioni: si è passati dal monitoraggio di una piccola sala computer, con al massimo qualche decina di postazioni, alla necessità di monitorare e gestire sistemi distribuiti di dimensioni tutt'altro che modeste.
Il compito assegnato all'infrastruttura di monitoraggio è cambiato di conseguenza: se in precedenza la complessità del monitoraggio risiedeva sulla rete locale di ciascuna impresa, che era, di fatto, la sola risorsa critica, oggi la complessità del monitoraggio risiede nella rete globale e nella incredibile quantità di risorse ad essa connesse. Dalla crescente diversità delle risorse da monitorare nasce la necessità di svincolare e rendere così indipendente la sonda, che esegue il vero e proprio codice di monitoraggio, dall'applicazione centrale, che ha il ruolo di controllare le sonde tramite un protocollo condiviso.
Il monitoraggio comprende in genere quattro fasi:

- la generazione di eventi, cioè sensori che interrogano entità e codificano le misure secondo un dato schema;
- l'elaborazione degli eventi generati che è specifica dell'applicazione e può avvenire durante qualsiasi fase del processo di monitoraggio, esempi tipici includono il filtraggio secondo alcuni criteri predefiniti, o il riassunto di un gruppo di eventi (ad es, calcolo della media);

- la distribuzione, riferita alla trasmissione degli eventi dalla fonte a tutte le parti interessate;
- infine, la presentazione che comporta in genere un'ulteriore elaborazione, cosicché il grandissimo numero di eventi ricevuti sia fornito tramite una serie di astrazioni che consentano all'utente finale di trarre conclusioni sul funzionamento del sistema monitorato. [22]

Tali carattestiche del mondo in cui i sistemi di monitoraggio sono chiamati a operare richiedono un nuovo approccio progettuale che:

- affronti la scomposizione dell'infrastruttura di monitoraggio in sottosistemi con compiti specifici;
- fornisca i dati del monitoraggio in modo flessibile, evitando la memorizzazione di informazioni da consumare o consegnare all'utente e selezionando la memorizzazione in base all'utilizzo futuro;
- fornisca all'utente un'interfaccia per la configurazione dell'attività di monitoraggio, al posto di un file di configurazione. [5]

Per assicurare una migliore gestione delle risorse e del tempo a disposizione l'infrastruttura di monitoraggio può essere affiancata da un sistema che automatizzi i servizi professionali. Tali sistemi permettono di curare al meglio l'aspetto organizzativo degli interventi critici e non da svolgere sull'infrastruttura gestita e assistono le aziende nella gestione dell'immensa mole di dati associata a una qualsiasi infrastruttura da gestire. [17]
L'impiego di tali strumenti automatici permette di accrescere la qualità del lavoro svolto dal fornitore di servizi gestiti (MSP - Managed Service Provider) e, di fronte alla crescita esponenziale del numero di operazioni e del numero di dispositivi coinvolti garantisce una maggiore resistenza a errori umani. Soprattutto attività molto ripetitive sono fortemente soggette a errori umani, l'adozione di strumenti automatici le rende a prova di errore umano garantendo, in aggiunta, una maggiore ottimizzazione del tempo: piccole e medie imprese non sono, infatti, economicamente in grado di dedicare persone alla gestione manuale di ogni problema informatico, con il risultato che i dispositivi soffrono di una manutenzione ridotta e sono, perciò,

maggiormente esposti a vulnerabilità. Nonostante i singoli programmi software permettano di eseguire aggiornamenti più o meno automatici è necessaria una piattaforma unica che permetta una loro gestione unificata e consenta di reperire e raccogliere tutte le informazioni in un unico punto accessibile e protetto. Un pannello di controllo il più possibile unificato permette di ridurre il tempo necessario all'individuazione, e successivamente alla risoluzione, di uno specifico problema su di un singolo dispositivo. L'industrializzazione dei processi ripetitivi da eseguire sui singoli dispositivi, in modo da evitare per quanto possibile il lavoro manuale, permette alle aziende di risparmiare sulla manutenzione dei propri dispositivi riducendo significativamente il costo a dispositivo senza sacrificarne l'efficienza e la sicurezza. Ogni sistema di monitoraggio porta con sé un costo per l'azienda, ma tale costo è nettamente inferiore ai benefici annessi. Tali strumenti non sono proposti direttamente ad aziende ma a specifiche figure professionali: i fornitori di servizi gestiti. Sempre più fornitori di servizi gestiti propongono alle aziende seguite tipi di assistenza con la formula "tutto incluso" in cui si propone un costo fisso a dispositivo comprendente monitoraggio e assistenza completa e illimitata. Così facendo, a differenza dell'assistenza fornita e fatturata a richiesta, gli obiettivi del fornitore di servizi gestiti e dell'azienda cliente diventano coincidenti: sistemi sempre più stabili e sicuri e mantenuti sempre all'apice delle funzionalità e a prova di fallimenti convengono sia al fornitore di servizi gestiti, che risparmia sugli interventi urgenti e può dedicarsi a un tipo di manutenzione proattiva, sia ovviamente all'azienda cliente.

Lo studio svolto parte da una integrazione tra un'infrastruttura di monitoraggio e un sistema di automazione dei servizi professionali. Una volta realizzata, tale integrazione è stata usata per rispondere alle principali necessità in termini di sicurezza e business continuity delle aziende gestite. Particolare rilevanza è stata assegnata agli attacchi di cryptovirus che, una volta infettata la rete aziendale, criptano i dati presenti sulle macchine e, spesso, ne permettono la decriptazione solo dietro pagamento di un riscatto. Tali minacce informatiche sono ogni anno causa di gravi perdite economiche e di immagine per moltissime imprese italiane sia pubbliche sia private e, secondo sondaggi, sono destinate a diffondersi sempre più nei prossimi anni. [20]

Nei capitoli che seguono sarà esposto lo stato attuale di alcuni strumenti a disposizione dei fornitori di servizi gestiti, lo scenario particolare in cui è stato svolto lo studio, i principali

problemi emersi e le soluzioni proposte. Lo studio si conclude con un'analisi del lavoro svolto e di parte del lavoro ancora da svolgere.

2 Stato dell'arte

Nel capitolo corrente è riportata una breve panoramica sui principali strumenti a disposizione dei fornitori di servizi gestiti per organizzare il monitoraggio e la gestione delle infrastrutture dei clienti e per l'organizzazione interna dal lavoro.

2.1 Sistemi di monitoraggio e gestione remota

Il software di monitoraggio e gestione remota (RMM - Remote Monitoring and Management) è un tipo di applicazione che i fornitori di servizi gestiti utilizzano per gestire e mantenere l'infrastruttura informatica dei loro clienti. Tale software è un'applicazione fondamentale per coloro che forniscono i propri servizi anche a distanza.
I sistemi di monitoraggio e gestione remota possono in generale offrire vari strumenti ma hanno due funzioni principali: fornire dati in tempo reale e non sull'infrastruttura gestita ed eseguire attività di gestione. Il software di monitoraggio e gestione remota consente ai fornitori di servizi di tenere sotto controllo i sistemi informatici dei propri clienti, compresi server, PC, applicazioni e dispositivi mobili, fornendo dati sulle prestazioni e altri rapporti che i tecnici hanno la possibilità di visionare ed esaminare per fornire assistenza. Il software permette inoltre ai fornitori di servizi di eseguire attività di gestione, come patch, aggiornamenti e configurazioni dei servizi stessi agendo sui sistemi informatici dei clienti. Entrambe queste funzioni possono essere eseguite senza alcuna difficoltà in loco, ma il fatto di poterle eseguire in remoto rappresenta un importante vantaggio per le aziende dei fornitori di servizi gestiti.
Per collegare il software di monitoraggio e gestione remota ai sistemi informatici del cliente, un fornitore di servizi gestiti deve installare un software sonda sui server, sui PC e sui dispositivi mobili del cliente. Un aiuto in tale processo di inizializzazione può essere rappresentato

dall'uso di strumenti di creazione e gestione di dominii (ad esempio Active Directory) che, tramite opportuni criteri di gruppo, consentono di eseguire automaticamente compiti prestabiliti su ogni nuovo PC annesso al dominio. Le sonde dei sistemi di monitoraggio, tuttavia, non possono solitamente essere installate su dispositivi privi di sistema operativo - switch e router, per esempio. In tali casi i sistemi di monitoraggio possono offrire funzionalità di gestione della rete che consentono la gestione dei dispositivi tramite Simple Network Managment Protocol (SNMP).
Alcuni prodotti per il monitoraggio e la gestione remota possono anche essere utilizzati per automatizzare processi altrimenti manuali, come l'esecuzione di un controllo de dischi, e fornire la possibilità di creare i propri script personalizzati per soddisfare le necessità del singolo cliente. L'automazione e gli script permettono di affrontare i problemi dell'infrastruttura informatica prima ancora che il cliente ne venga a conoscenza consentendo di fatto un tipo di manutenzione proattiva. [18]

2.1.1 Datto RMM

Datto RMM opera su una struttura scalabile e ad alta affidabilità ospitata all'interno di Amazon Web Services (AWS) ed è costituito da diverse piattaforme distribuite in varie parti del mondo. Ogni piattaforma è composta da un certo numero di istanze server che gestiscono le differenti aree di prodotto (connettività degli agent, portale web etc.). Ogni utente effettua il login alla piattaforma geograficamente più vicina, sulla base delle informazioni inserite al momento della creazione dell'account. Per garantire piena connettività verso Datto RMM, sul firewall dovrà essere aperta la porta TCP 443 in uscita per specifici indirizzi IP suddivisi per zone geografiche. La connettività tra le sonde e la connessione remota (RDP, VNC, Splashtop etc) dipende da un "Tunnel server" che ha il ruolo di inizializzare la connessione tra le risorse gestite. I Tunnel Server sono ospitati da Datto RMM e vengono usati per creare il tunnel tra dispositivi in modo da rendere poi possibile la connessione remota. Questi server sono dislocati in diverse zone del mondo in modo da massimizzare la copertura e le performance. [1]

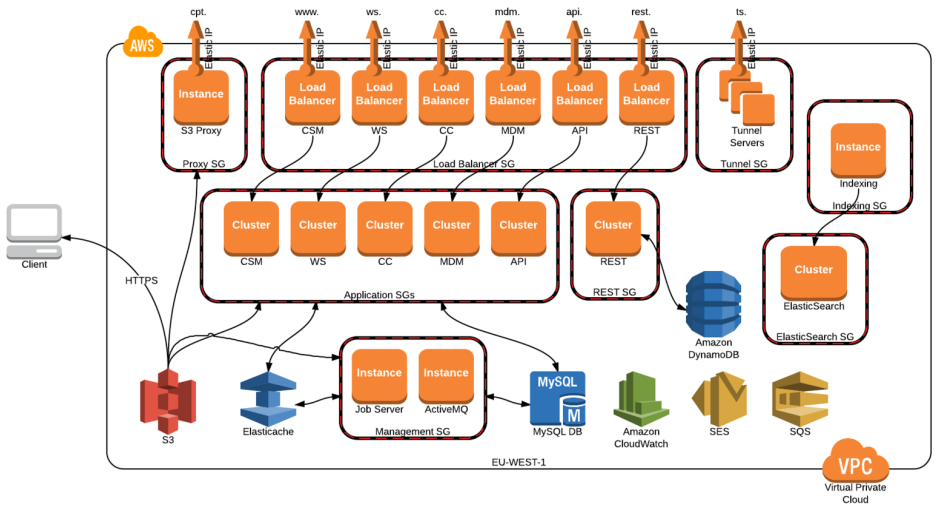

Figura 2.1: Architettura della piattaforma Datto RMM su AWS

Datto RMM permette di organizzare le risorse gestite in siti. I siti permettono di raggruppare assieme i dispositivi di un unico cliente, ma possono essere definiti per raggruppare tutti i dispositivi di una particolare sede o in qualunque altro modo. Oltre ai siti Datto RMM permette di organizzare le risorse gestite in gruppi che, all'interno di un sito, permettono di avere svariati insiemi di risorse raggruppate secondo un criterio stabilito. I gruppi possono essere statici, in cui ogni risorsa è aggiunta manualmente dall'utente, o dinamici in cui le risorse sono aggiunte automaticamente in seguito al soddisfacimento di vincoli prestabiliti.

Datto RMM gestisce le procedura operative standard tramite politiche. Le politiche possono essere definite a livello di account, e quindi essere applicate globalmente a ogni sito, o a livello di sito, per avere effetto solo sulle risorse appartenenti a un determinato sito. Con una politica è possibile definire qualcosa che si desidera fare, come la configurazione di un'impostazione, il controllo di un dato, la ricerca e l'installazione di patch o aggiornamenti. Una politica può essere attivata su tutti i siti dell'accounto su specifici siti o gruppi. È possibile definire un processo automatizzato per l'esecuzione di uno o più componenti tramite i lavori. Un lavoro permette di pianificare l'esecuzione di uno o più componenti su risorse singole o su interi gruppi o siti. L'esecuzione di un lavoro può essere immediata oppure pianificata.

Un componente tipico contiene uno script, scritto in uno dei diversi linguaggi disponibili, ma può anche contenere un programa da installare o un eseguibile da eseguire. I componenti

possono essere creati, modificati e condivisi da ogni utente, questo garantisce che gli amministratori abbiano il completo controllo del codice che ogni componente esegue. I linguaggi di scripting supportati per la creazione di un componente sono: Batch, Bash, VBScript, JavaScript, PowerShell, Python, Ruby, Groovy. In ogni componente è possibile fare riferimento a speciali variabili definite dall'utente. I campi definiti dall'utente sono utilizzati per visualizzare informazioni sul dispositivo che non vengono rilevate durante la normale procedura di verifica del dello stesso. Ogni dispositivo ammette un massimo di 30 campi definiti dall'utente. Le informazioni in tali campi, oltre ad essere accessibili e modificabili all'interno di ogni componente, sono impostabili manualmente dall'utente. Tali informazioni, una volta impostate, possono essere usate per filtrare e raggruppare le risorse gestite. Per impostare le informazioni nei campi definiti dall'utente in un sitema Windows è sufficiente aggiungere un valore in una specifica chiave del registro di sistema, l'agente si occuperà poi di comunicare il valore alla piattaforma. I componenti possono anche essere sfruttati per la creazione di controlli personalizzati da eseguire sulle risorse. Una volta scritto il codice da eseguire è possibile impostare la frequenza del controllo e le eventuali azioni da intraprendere nel caso in cui il controllo evidenziasse un problema. [7]

2.1.2 Kaseya VSA

Come Datto RMM anche Kaseya VSA permette di operare via cloud con modalità molto simili a quanto espresso nel paragrafo precedente. Tuttavia la piattaforma di Kaseya VSA, oltre che su cloud, può essere ospitata su un server locale amministrato dal fornitore di servizi gestiti. Nonostante ciò rappresenti uno svantaggio in termini di scalabilità automatica e aggiornamenti software immediati, permette comunque di avere il pieno controllo della piattaforma anche nel caso di fallimento della rete internet.

Kaseya VSA gestisce le macchine installando anch'esso una sonda su una macchina gestita. La sonda è un servizio di sistema che non richiede che l'utente sia connesso per il proprio funzionamento. La sonda è configurabile e può essere totalmente invisibile all'utente. L'unico scopo della sonda è quello di eseguire i compiti richiesti dalla piattaforma di Kaseya VSA. Ad ogni sonda installata viene assegnato un unico ID macchina. Gli ID macchina possono essere creati automaticamente al momento dell'installazione della sonda o manualmente prima dell'instal-

lazione della stessa. [11] La piattaforma è in grado di trovare e identificare correttamente più macchine con estrema rapidità e semplicità. Con l'implementazione di una singola sonda, una semplice scansione può propagarsi in tutta la rete, eseguire una raccolta di dati che restituisce informazioni critiche sulle macchine che non sono ancora gestite, consentire il controllo delle risorse e rilevare istantaneamente i cambiamenti di rete. [13]
Per raggruppare le macchine gestite Kaseya VSA fa uso degli ID macchina associati a ciascuna di queste. Tutti gli ID macchina sono, infatti, associati a un ID gruppo e, opzionalmente, a un ID sottogruppo. In genere un ID gruppo rappresenta un singolo account cliente. Gli ID sottogruppo rappresentano generalmente una posizione o una rete all'interno di un ID gruppo. Ad esempio, l'identificatore completo per una sonda installata su una macchina gestita può essere definito come jsmith.acme.chicago. In questo caso chicago è un ID sottogruppo definito all'interno dell'ID gruppo chiamato acme. [12]
Altra differenza tra Kaseya VSA e Datto RMM è che le soglie di allarme dei vari controlli possono non essere staticamente determinate. La piattaforma è, infatti, in grado di determinare le giuste soglie servendosi di metodi di apprendimento automatici. In questo modo, le soglie di allarme vengono messe a punto automaticamente in base ai dati sulle prestazioni effettive per macchina. Ogni macchina assegnata raccoglie i dati sulle prestazioni per un periodo di tempo specificato. Durante questo periodo di tempo non vengono attivati allarmi. Al termine della sessione di autoapprendimento, la soglia di allarme per ogni macchina assegnata viene regolata automaticamente in base alle prestazioni effettive della macchina. L'autoapprendimento non può tuttavia essere utilizzato con set di monitor personalizzati. [14]

2.1.3 Nagios

Nagios è un sistema di monitoraggio disponibile solo per l'installazione su server locale amministrato dal fornitore di servizi gestiti. Il design di Nagios è profondamente influenzato dal suo utilizzo originale in infrastrutture che non contemplano il cloud e mostra i suoi limiti quando la complessità del sistema da gestire cresce fino a divenire una federazione di macchine connesse tra loro. [5] Nagios può essere installato su ogni sistema operativo basato su Linux o, in alternativa, su una macchina virtuale Linux in qualsiasi altro ambiente. Nagios permette il monitoraggio di sistemi Linux, Mac OS/X o Windows e integra un avanzato sistema per il

monitoraggio di rete tramite Netflow e SNMP.

A differenza di altri sistemi di monitoraggio, Nagios non include al suo interno meccanismi preconfezionati per controllare lo stato dei dispositivi o della rete. Si basa totalmente su programmi esterni, chiamati plugin, che contengono il vero e proprio codice di monitoraggio. I plugin sono eseguibili o script (Perl, Shell, Python, Ruby, etc.) che possono essere eseguiti da una riga di comando per controllare lo stato di un dispositivo o di servizi di rete. Nagios usa i risultati dei plugin per determinare lo stato corrente dei dispositivi monitorati e dei servizi di rete. Nagios si occupa dell'esecuzione di un plugin ogni volta che c'è la necessità di ottenere un dato aggiornato sullo stato di un dispositivo o di un servizio di rete. Il plugin al suo interno può eseguire qualsiasi comando per effettuare il controllo e poi, semplicemente, restituisce l'esito a Nagios. Nagios si occupa, a questo punto, di elaborare i dati ricevuti e intraprendere le azioni necessarie (allarmi, notifiche, esecuzione di contromisure, etc.).

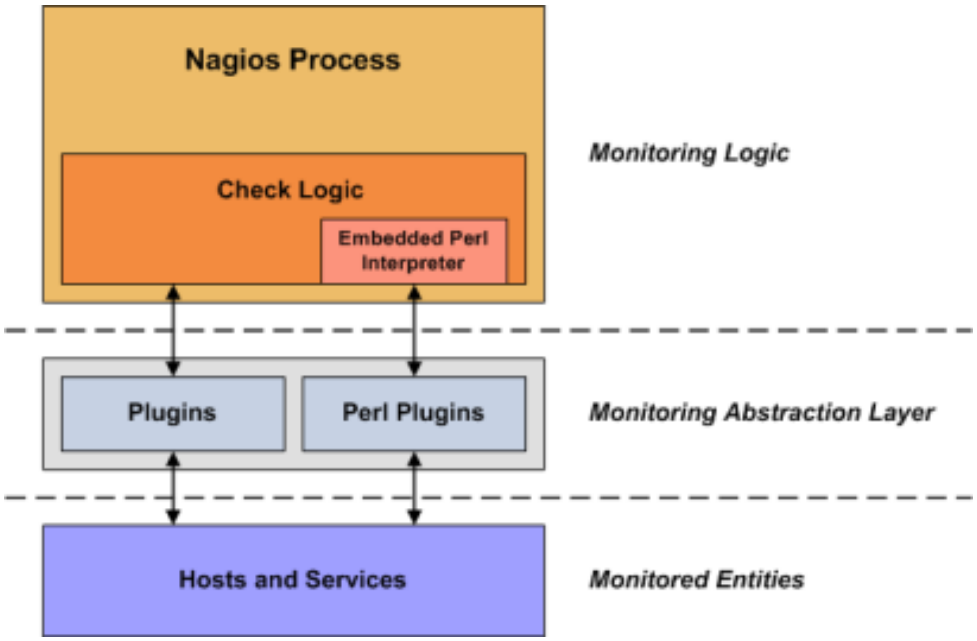

Figura 2.2: Meccanismo di monitoraggio di Nagios Core

I plugin agiscono, dunque, come un vero e proprio strato di astrazione tra la logica di monitoraggio interna di Nagios e i servizi e dispositivi che vengono monitorati. Un aspetto positivo di un'architettura così composta è che permette il monitoraggio di praticamente qualsiasi dispositivo che possa essere monitorabile. Se da un lato ciò permette di monitorare tutto il

monitorabile, dall'altro preclude a Nagios la possibilità di conoscere che cosa sta effettivamente monitorando: Nagios non è in grado di comprendere le specifiche di ciò che controlla ma si limita a tenere traccia dei cambiamenti di stato delle risorse. Solamente i plugin conoscono le specifiche della risorsa che stanno monitorando.
Nagios è in grado di monitorare dispositivi e servizi in due modi: attivamente e passivamente. I controlli attivi sono avviati dalla logica di controllo di Nagios. Nel momento in cui Nagios ha bisogno di ricevere dati aggiornati sullo stato di un dispositivo o servizio esegue uno o più plugin per ottenere i risultati del controllo. I controlli attivi possono essere eseguiti sia a intervalli regolari, sia su richiesta. I controlli passivi sono, invece, avviati ed eseguiti da applicazioni esterne e i risultati sono poi sottoposti a Nagios per la loro elaborazione.
La differenza principale tra controlli attivi e passivi è che i controlli attivi sono avviati ed eseguiti da Nagios, mentre i controlli passivi sono eseguiti da applicazioni esterne. Un esempio di eventi asincroni che si prestano a essere monitorati passivamente sono le trap SNMP, dal momento che non è possibile sapere a priori quante posssano essere generate in un intervallo di tempo e dunque non è possibile monitorare il loro stato ogni pochi minuti. I controlli passivi si servono di un file di comando esterno che memorizza i risultati di tutti i controlli passivi che periodicamente è letto ed elaborato da Nagios. L'elaborazione dei risultati dei controlli attivi e passivi è sostanzialmente identica e permette una perfetta integrazione delle informazioni provenienti da applicazioni esterne in Nagios. [16]
L'architettura di Nagios soffre, tuttavia, per la presenza di un agente di monitoraggio centralizzato, che è esposto a diventare il vero collo di bottiglia nelle grandi installazioni. [5]

2.2 Sistemi di automazione dei servizi professionali

Un sistema di automazione dei servizi professionali (PSA - Professional Services Automation) è un tipo di suite di applicazioni che fornisce a un'azienda le funzionalità necessarie per gestire i principali processi aziendali. Nel settore informatico i fornitori di servizi gestiti possono utilizzare un tale sistema per la gestione delle loro operazioni quotidiane. Un sistema di automazione dei servizi professionali può comprendere una serie di funzionalità, ma i componenti chiave includono la gestione di progetti aziendali, la gestione delle risorse e la gestione del

tempo e delle spese. Tutto ciò ha lo scopo di aiutare le aziende a rispettare le tappe e le tempistiche dei progetti, assegnare risorse ai progetti per ottimizzare l'utilizzo del personale e tenere traccia del tempo impiegato e delle spese sostenute ai fini della fatturazione.
La maggior parte dei sistemi di automazione dei servizi professionali sono basati sul cloud e il SaaS è un tipico modello di distribuzione. L'approccio cloud semplifica l'onere di acquisto di risorse e di gestione di una soluzione locale: il che rappresenta un vantaggio per le aziende di servizi professionali che cercano di evitare i costi della tecnologia onsite, concentrandosi al contempo sui loro compiti principali. Gli strumenti basati su cloud possono anche rendere più semplice per le aziende la gestione di una forza lavoro sempre più distribuita e mobile.
I sistemi di automazione dei servizi professionali tendono a differenziarsi per il livello di integrazione che offrono rispetto ad altri software e strumenti di automazione. Alcuni fornitori offrono soluzioni integrate che comprendono anche sistemi di monitoraggio e gestione remota e sistemi di business continuity. [17]
Un sistema di automazione dei servizi professionali di qualsiasi fornitore di servizi gestiti deve integrarsi con tutte le applicazioni critiche di cui il fornitore ha bisogno per gestire il proprio lavoro, fornendo piena visibilità sui clienti, sulle operazioni interne e sulla redditività. La soluzione deve essere, dunque, costruita appositamente per i fornitori di servizi gestiti e avere un'esperienza utente ottimale per flussi di lavoro e processi aziendali. Una tale piattaforma automatizzata di gestione aziendale permette di perdere ridondanza e inefficienza e di ottenere un quadro completo con piena visibilità delle metriche più importanti per le operazioni di servizio.
La regolazione dei flussi di lavoro e le notifiche aiutano a guidare l'automazione in tutta la piattaforma. Al verificarsi di un evento è possibile aggiornare automaticamente un'entità, intervenire e notificare alle persone ciò che è stato fatto. Apposite funzioni consentono di stabilire a priori le fasi di intervento, standardizzare i processi e tenere traccia delle varie responsabilità. Un sistema di controllo e gestione remota e un sistema di automazione dei servizi professionali unificati consentono di riunire tutti i dati, i dispositivi, gli utenti e le operazioni effettuate in un unico luogo. Una piattaforma unificata permette di accelerare l'erogazione dei servizi informatici, migliorare l'efficienza operativa, e offrire ai clienti una migliore esperienza e una maggiore consapevolezza del lavoro svolto dal fornitore di servizi gestiti. [15]

2.2.1 Autotask PSA

Autotask PSA è un sistema di automazione dei servizi professionali specifico per fornitori di servizi gestiti basato su cloud. Aiuta ad automatizzare e ottimizzare i processi aziendali critici e i flussi di lavoro per la fornitura di servizi in base. Tramite l'integrazione con un sistema di monitoraggio e gestione remota permette di convertire tutti o alcuni avvisi generati dal sistema di monitoraggio in tickets.

I ticket rappresentano in AutotaskPSA l'unita di lavoro di base. Ciascun ticket può essere generato automaticamente (ad esempio da un sistema di controllo e gestione remote integrato), manualmente da un cliente oppure da un operatore. I tickets sono organizzati in code: un ticket può essere aggiunto automaticamente a una coda mediante specifici filtri. Ad esempio è possibile deviare tutti i ticket generati automaticamente in seguito ad avvisi in una coda o in un altra a seconda della tipologia (errore software o hardware). Ciascun ticket ha un proprio stato che permette di verificare a colpo d'occhio se un incarico è già stato preso in carico da un operatore, è già parzialmente risolto o è definitivamente chiuso. Autotask PSA permette di gestire molteplici operatori anche con ruoli e livelli di sicurezza distinti: ogni operatore (identificato come "risorsa" da Autotask PSA) può avere accesso all'intero sistema o solo a specifici settori e può prendere in carico tickets da una o più code.

Autotask PSA permette inoltre di associare a ogni cliente un contratto che, oltre a stabilire i termini economici del servizio offerto, tiene traccia del livello di servizio pattuito con il cliente: in base al livello di servizio stabilito dal contratto tutti i tickets creati per un cliente incorporano al loro interno una tabella di marcia che stabilisce il tempo massimo che può intercorrere tra la creazione dello stesso e la sua presa in carico da parte di un operatore, il tempo massimo che può intercorrere tra la presa in carico e lo studio di una soluzione, tra lo studio e la messa a punto della soluzione e, infine, la chiusura del ticket. Dato che i livelli di servizio possono essere molto variegati in caso di aziende con molti clienti, ciascun ticket, le cui tempistiche non sono state rispettate, genera avvisi per l'operatore che lo ha preso in carico ed è messo in risalto sulla pagina principale della piattaforma per tutti gli operatori che, in accordo al loro livello di sicurezza, hanno la possibilità di intervenire attivamente alla risoluzione del ticket. Tutto ciò assicura una gestione migliore del lavoro da svolgere e rende molto remote le possi-

bilità che uno o più avvisi, anche critici, generati da un sistema di controllo e gestione remota integrato, rimangano insoluti per un lungo intervallo di tempo causando potenziali perdite di immagine al fornitore di servizi gestiti e ricadute economiche al cliente.
Autotask PSA riunisce tutte le informazioni dei clienti in una interfaccia unica, compresi contratti, dispositivi e dati, in modo da poter fornire un servizio superiore e più reattivo; permette, inoltre, di tracciare ogni cosa in modo che nulla riesca a sfuggire e fornire visibilità ai clienti di tutti o parte dei dati e di tutti o parte dei dettagli sui ticket generati e sulla loro risoluzione. [3]
Inoltre, Autotask PSA è distribuito su data center georidondanti in modo da garantire un alto livello di recupero da disastri anche naturali, incorpora moderni algoritmi di crittografia per assicurare la non compromissione dei dati dei clienti e fornisce un'applicazione mobile per rendere possibile una gestione e presa in carico di nuovi tickets molto più veloce e immediata. [15]

2.3 Active Directory

Nei sistemi operativi Windows Server, Active Directory permette di creare e gestire un controllore di dominio. Un controllore di dominio è un server che risponde alle richieste di autenticazione di sicurezza (login, verifica delle autorizzazioni, ecc.) all'interno di un dominio Windows Server. Una politica di gruppo è un insieme di impostazioni che definiscono l'aspetto di un sistema e come si comporterà per un insieme definito di utenti delle risorse connesse al dominio. [21]

3 Scenario operativo

Il lavoro è stato svolto in uno scenario operativo in cui la piattaforma Datto RMM preesistente non era ancora integrata alla piattaforma Autotask PSA. La prima fase del lavoro svolto ha riguardato prorio tale integrazione. Grazie a strumenti automatici e tecniche predefinite ben documentate l'integrazione è stata effettuata in tempi molto rapidi. Una volta realizzata l'integrazione tra Datto RMM e Autotask PSA l'attenzione è stata rivolta a problemi di sicurezza e business continuity che quotidianamente causano non pochi grattacapi ai gruppi di sicurezza informatica di tutto il mondo. Nel capitolo seguente saranno descritti nel dettaglio i principali problemi affrontati, mentre nel seguito del capitolo corrente sarà preso in esame l'ambiente in cui il lavoro è stato svolto.
Per permettere lo sviluppo e la prova di ogni script creato si è resa necessaria la creazione di un piccolo ambiente di prova che simulasse in piccolo gli aspetti principali che caratterizzano l'ambiente reale in cui gli script sarebbero stati chiamati a operare. La creazione di un ambiente di prova completamente autonomo dall'ambiente reale ha permesso di non interrompere il corretto funzionamento dei PC aziendali durante la messa a punto degli script ma, al contempo, ha anche permesso di adattare gli script alle necessità proprie del reale ambiente aziendale.

3.1 Ambiente reale

L'ambiente in cui gli script creati sono stati chiamati a operare è un ambiente aziendale composto da circa 125 macchine, con macchine che da una settimana all'altra possono essere sostituite, aggiunte o rimosse. Di queste macchine 12 sono veri e propri server ciascuno con specifici compiti amministrativi all'interno dell'ambiente. Delle restanti macchine al principio

del periodo preso in esame (della durata di poco meno di due mesi) solamente 12 eseguivano l'ultima versione del sistema operativo di casa Microsoft (Microsoft Windows 10), 1 eseguiva Microsoft Windows 8.1, mentre le restanti macchine si dividevano tra Microsoft Windows 7 e il ben più obsoleto Microsoft Windows XP. Al termine del periodo di lavoro, grazie alla sostituzione delle macchine più datate e all'applicazione dell'aggiornamento a Microsoft Windows 10 in alcune macchine con Microsoft Windows 7 tramite un apposito componente eseguibile direttamente dalla piattaforma Datto RMM, la situazione vede la maggioranza delle macchine che esegue l'ultima versione del sistema oparativo di casa Microsoft contro circa 40 macchine che ancora eseguono Microsoft Windows 7 o Microsoft Windows XP. Dato che il supporto per Microsoft Windows 7 terminerà il 14 Gennaio 2020, continuerà il processo di aggiornamento o sostituzione delle macchine che ancora eseguono tale sistema operativo o versioni precedenti.

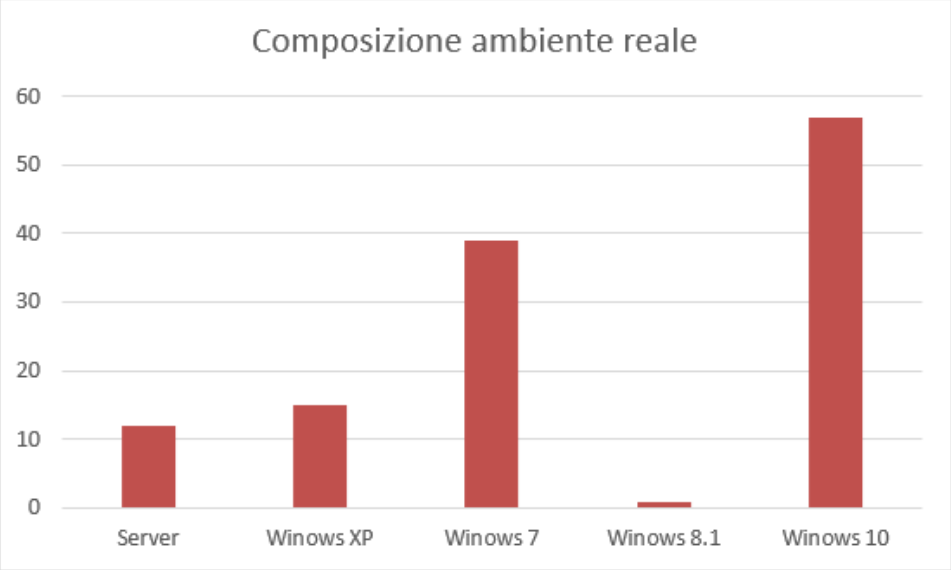

Figura 3.1: Macchine dell'ambiente reale

L'intero ambiente aziendale è gestito come dominio Active Directory con più server che ricoprono il ruolo di controllori di dominio: questo permette di garantire l'accesso con privilegi standard a tutti i dipendenti e accessi privilegiati a determinate categorie di impiegati. Nonostante il dominio sia sempre operativo e funzionante un'analisi più approfondita ha rilevato che su alcuni PC erano ancora presenti e utilizzati utenti locali esterni al dominio cpn privi-

legi amministrativi sulla macchina. Poiché tale difetto rischiava di annichilire gli standard di sicurezza e controllo garantiti dal dominio Active Directory è stato creato un apposito script per revocare i privilegi amministrativi a tali utenti esternio al dominio.

3.2 Ambiente di prova

Creato con l'obiettivo di astrarre le varie sfaccettature dell'ambiente reale, l'ambiente di prova è composto di quattro macchine virtuali in esecuzione contemporanea su una singola macchina fisica. Nello specifico una di esse ricopre il ruolo di server (con sistema operativo Microsoft Windows Server 2016) mentre le altre eseguono tre diverse versioni del sistema operativo Windows (10, 7, XP). Con tale diffenziazione di ruoli e sistemi operativi è stato possibile emulare la diversità di macchine e sistemi operativi utilizzati nell'ambiente reale.

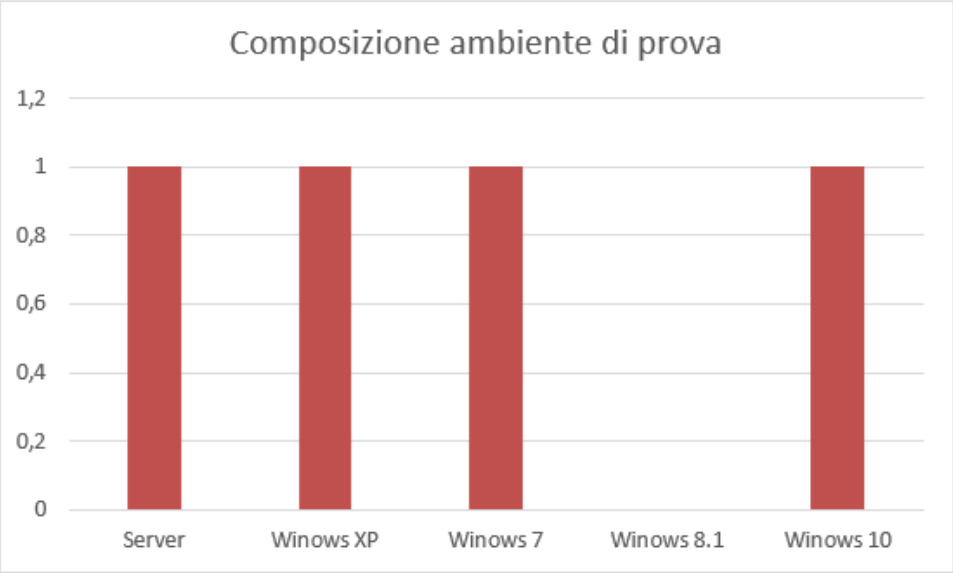

Figura 3.2: Macchine dell'ambiente di prova

Oltre a ciò è stato creato un dominio Active Directory che fosse il più possibile simile a quello reale: il server ha giocato il ruolo di controllore di tale dominio, mentre l'accesso alle macchine era permesso a due utenti generici e a un utemte con diritti amministrativi. Per ricreare appieno la situazione dell'ambiente reale sono stati, inoltre, creati utenti locali con

diritti amministrativi in ogni macchina. La presenza di un tale ambiente si è rivelata di vitale importanza per lo sviluppo e la messa a punto di tutti gli script, in modo particolare di quelli che, se non opportunamente configurati, rischiano di far perdere agli utenti il controllo del proprio PC.

4 Descrizione del problema

Un problema comune a molte infrastrutture gestite e che negli utlimi periodi non accenna a risolversi definitivamente o a calare di intensità, ma che, anzi, la maggioranza di fornitori di servizi gestiti teme che andrà solo aumentando almeno nel futuro più prossimo è rappresentato da particolari malware che criptano i dati presenti in una macchina: i criptovirus.
Nel seguito di questo capitolo saranno analizzate le principali caratteristiche che accomunano i criptovirus e i meccanismi principali tramite cui riescono a infettare anche un'infrastruttura ben gestita e costantemente monitorata.

4.1 Cryptovirus

Il download di file sospetti o sconosciuti dal web può rivelarsi dannoso per l'utente e può risultare in una compromissione del proprio PC e i dati in esso contenuti. Un particolare tipo di malware sono i cryptovirus. Tale tipo di malware prende di mira i file dell'utente, li cripta utilizzando metodi di crittografia anche all'avanguardia, e chiede che venga pagato un riscatto (di solito in bitcoin e all'interno di un periodo di tempo limitato) in modo che la chiave segreta venga rilasciata all'utente. Solo guardando il caso di WannaCry, è evidente che i cryptovirus costituiscono un'industria multimilionaria guidata dai criminali informatici. [2]
Molte violazioni hanno successo a causa di attacchi di phishing, siti Web dannosi, annunci web e attacchi diretti alle piccole imprese scarsamente difese. La formazione continua dei dipendenti per aiutarli a rimanere vigili è indubbiamente una buona pratica per le piccole e medie imprese, ma spesso non è sufficiente. [9] Molti attacchi sfruttano le vulnerabilità di base del sistema operativo. Nella maggior parte dei casi, la patch per questa vulnerabilità è già stata rilasciata dal fornitore, ma non è stata applicata alla macchina. L'adozione di una soluzione per

il controllo e la gestione remota permette di ridurre il rischio che tali vulnerabilità rimangano presenti tramite l'utilizzo di politiche di aggiornamento automatico del software. [20]
Anche la presenza di un programma antivirus aggiornato e funzionante sembra non essere sufficiente a prevenire attacchi da cryptovirus: l'85% dei fornitori di servizi gestiti raggiunti da uno studio [9] ha riferito che le vittime avevano soluzioni antivirus installate e funzionanti. I cryptovirus cercano di passare inosservati ai controlli di sicurezza abusando di processi affidabili e legittimi, per poi sfruttare i sistemi interni per crittografare il numero massimo di file e disabilitare i processi di backup e recupero prima che un team di sicurezza se ne accorga. [10]
I moderni cryptovirus si basano sull'offuscamento per il loro successo. Alcuni cryptovirus sfruttano la PowerShell di Windows per eseguire uno script PowerShell da Internet, impostato per avviare automaticamente l'attacco dopo diversi giorni. Questo fa apparire l'attacco dal nulla. In questo scenario, il vero e proprio attacco di crittografia dei file viene eseguito dal fidato processo della Powershell di Windows, facendo credere al sistema di protezione che sia un'applicazione affidabile a modificare i documenti. Il codice può essere, inoltre, compilato per una singola vittima, protetto da una password unica o eseguito solo in un determinato lasso di tempo. Questo ostacola ulteriormente sia l'analisi automatica all'interno di sandbox che il reverse engineering manuale da parte di ricercatori per determinare lo scopo del campione. Nel momento in cui la vittima si rende conto di ciò che sta succedendo, è troppo tardi, poiché questi attacchi avvengono tipicamente nel bel mezzo della notte quando il personale IT riposa. In genere la minaccia viene eseguita su uno o più PC compromessi, abusando di un account utente privilegiato per attaccare anche documenti in remoto ospitati, ad esempio, su server non direttamente infettati. [19]
I tipi di attacco possono variare dalla crittografia solo di tipi specifici di file, come in BitCrypt, fino a crittografare l'intero disco rigido, come nel caso di Petya. Dopo che i file sono criptati, viene spesso visualizzata una finestra di messaggio che di solito dichiara lo schema di cifratura utilizzato (ad es. RSA-2048) e indica l'importo del riscatto chiesto per decriptare i file. Il comportamento dei cryptovirus può variare in base alla famiglia a cui appertengono: possono aprire i files da criptare in sola lettura e crearne una copia criptata eliminando l'originale (è il caso di alcune versioni di WannaCry), oppure sovrascrivere in loco i files con una loro versione

criptata (è il caso di GrandCrab). Nel caso di WannaCry ci sono, inoltre, sette località che non sono criptate; questo accade in modo che il virus non rischi accidentalmente di crittografare un file che è fondamentale per l'esecuzione dello stesso (nello specifico: /Local Settings/Temp, /Program Files (x86), /WINDOWS, /AppData/Local/Temp, /Program Files, /ProgramData). [2] Per garantire che le vittime paghino i soldi del riscatto, i cryptovirus cercano di criptare il maggior numero possibile di documenti, rischiando a volte anche di mettere a repentaglio, o volutamente paralizzando, il PC. I documenti da criptare possono essere memorizzati su unità locali fisse e rimovibili, così come su unità remote condivise. Il cryptovirus potrebbe persino dare priorità a determinate unità o dimensioni dei documenti per assicurarsi il successo prima di essere rilevato dal sistema di protezione o notato dalle vittime. La rapidità di rilevamento e la tempestività di intervento giocano dunque un ruolo fondamentale nella lotta ai cryptovirus. [19]

4.2 Programmi predefiniti

Alcune estensioni di file rappresentano un pericolo se eseguite con un doppio click, dal momento che eseguono comandi non tracciabili e perciò potemzialmente pericolosi. Tali estensioni di norma non sono utili per l'utilizzo giornaliero dei PC. Spesso al principio di un attacco c'è prorio un file con estensione pericolosa (.bat, .ps1, etc.) che, tramite meccanismi di ingegneria sociale, si presenta come un documento legittimo e induce l'utente ad aprirlo con un doppio click scatenando l'infezione. [4]

4.3 Attività pianificate

Nuove tipologie di attacco oggi sempre più sfruttate utilizzano approcci privi di file che non coinvolgono l'installazione di alcun file sul disco rigido. Tutto ciò rende tale tipo di minacce difficili da rilevare da un programma antivirus. Un'attività pianificata può essere creata per eseguire script powershell o effettuare un innalzamento dei privilegi. Le attività pianificate vengono eseguite in modo che l'attaccante possa mantenere la persistenza anche in caso di riavvio delle macchine. [6] Tali attacchi sono difficili da individuare anche per il fatto che

coinvolgono programmi legittimi che solitamente non sono controllati da programmi antivirus.

Un malware che sfrutta un'attività pianificata spesso crea determinati requisiti per il lancio che gli permettono di rimanere silente nel PC della vittima per periodi di tempo anche lunghi in attesa del momento prestabilito per entrare in azione. Una volta che si presenta l'opportunità il malware può entrare in azione e scaricare altro codice dannoso o programmare una nuova attività pianificata per rimanere sempre in memoria. [8]

5 Contromisure adottate

Dopo un'attenta analisi dei problemi più comuni presenti nelle infrastrutture da monitorare, il lavoro si è concentrato nel trovare delle contromisure adatte per sopperire alle mancanze di comuni software antivirus sfruttando le potenzialità offerte da Datto RMM.
Nel seguito sono dunque descritti in dettaglio i vari script powershell messsi a punto per raggiungere tale scopo. Ogni script è stato inizialmente scritto e testato nell'ambiente di prova per poi essere successivamente immesso nell'ambiente reale. A causa della presenza di versioni datata del sistema operativo Microsoft Windows si è reso necessario lo sviluppo di più versioni dello stesso script per garantire la sua compatibilità a partire dalla versione 2.0 di powershell.

5.1 Programmi predefiniti

Lo script è un metodo semplice e automatizzato per cambiare l'associazione tra estensione di files e programma predefinito per la loro apertura. Inizialmente pensato per l'associazione di estensioni potenzialmente pericolose (.vbs, .bat, etc.) a programmi che ne annullano il potenziale melevolo, come banali editor di testo. Per eseguire lo script è sufficiente specificare l'estensione da associare e il percorso dell'eseguibile a cui associarla. Lo script si serve di funzionalità integrate nei sistemi operativi Microsoft Windows per creare una associazione tra estensione e tipo di file (nel caso non ve ne sia già presente una) e impostare il programma scelto come programma predefinito per l'apertura di tali tipi di file. Nella sua estrema semplicità la procedura, effettuata per opportune estensioni, permette di impedire il lancio involontario da parte dell'utente di codice malevolo ricevuto da una fonte male intenzionata (ad esempio un indirizzo di posta elettronica compromesso) mascherato da file innoquo con una semplice doppia estensione nascosta (e.g.: .pdf.bat) per ingannare un utente non scrupolosamante at-

tento.
Lo script può, tuttavia, essere utilizzato anche per gestire l'apertura di qualsiasi tipo di file preferendo un programma piuttosto che un altro. Questo si rivela molto utile nel caso di politiche aziendali circa programmi particolari che i dipendenti devono usare per determinati tipi di file o altro.

5.2 Amministratori locali

Per impedire che l'utente che normalmente utilizza il PC possegga privilegi amministrativi e sia in grado, seppur involontariamente, di compromettere la macchine, è utile la creazione di un nuovo profilo utente che rivesta il ruolo di amministratore locale della macchina.
Lo script per la creazione di amministratori locali permette di creare un nuovo amministratore locale sui PC in cui è eseguito. È possibile specificare nome utente,lunghezza della password da generare e il campo definito dall'utente in cui salvare la password generata assieme al nome utente. Tramite opportuni parametri il nuovo amministratore può diventare l'unico amministratore del PC rimuovendo ogni altro amministratore presente oppure decidendo di preservarne alcuni specificandone i nomi utente. Opportuni parametri permettono di specificare il nome utente da associare al nuovo account amministratore, la lunghezza in caratteri della password da generare casualmente che sarà poi assegnata al nuovo account amministratore e una breve descrizione dell'account.
Per autorizzare la rimozione dei privilegi amministrativi di eventuali altri amministratori rilevati nel PC è sufficiente attivare l'opzione dedicata. Lo script permette inoltre di inserire una lista di nomi utente che, se presenti tra gli amministratori del PC, devono mantenere i loro privilegi amministrativi.
Una volta lanciata l'esecuzione dello script, come prima operazione lo script crea due liste di utenti: la prima contenente tutti gli account utente rinvenuti sul PC, la seconda contenente tutti gli account utente rinvenuti che hanno privilegi amministrativi. Lo script legge il contenuto del campo definito dall'utente specificato per verificare l'eventale presenza di un altro account amministratore creato tramite script. Lo scopo di tale controllo è non avere macchine in cui ci sia più di un account amministratore creato traminte questo metodo: se ciò accades-

se, infatti, le informazioni del secondo account creato andrebbero a sovrascrivere quelle del primo dal momento che condividono il medesimo campo definito dall'utente. Se nel campo sono rinvenute informazioni riguardanti un vecchio account amministrativo non oiù presente nel sistema, lo script procede alla creazione di un nuovo account se e solo se l'apposito parametro per la creazione forzata è impostato. Una volta passati tutti i controlli lo script genera una password casuale della lunghezza scelta, la salva nel custom field impostato e procede alla creazione del nuovo account amministratore. Se si richiede la rimozione di ogni altro profilo con privilegi amministrativi lo script scorre la lista di amministratori creata al primo passo e rimuove i privilegi amministrativi a ogni account utente presente in tale lista, eccetto per i profili utente da mantenere.
Nel caso in cui il PC su cui lo script è lanciato faccia parte di un dominio Active Directory potrebbe essere opportuno inserire il gruppo "Domain Admins" tra gli utenti a cui non togliere i privilegi amministrativi per evitare che gli amministratori di dominio perdano diritti ammnistrativi sul PC in questione.

5.3 Attività pianificate

Lo script dedicato alle attività pianificate permette di eseguire un controllo costante delle attività pianificate create in un PC. Lo script opera appoggiandosi a un file che mantiene costantemente aggiornato. Il file contiene un elenco delle attività pianificate all'interno del PC con dettagli sull'eseguibile da lanciare e i parametri da utilizzare per il lancio.
Come parametri in ingresso lo script accetta il perscorso e il nome del file di appoggio e una lista di attività considerate sicure che, anche rinvenute tra le pianificate, non saranno evidenziate come sospette dallo script. Dare la possibilità di specificare una lista di operazioni "affidate" si è reso necessario in seguito ad alcuni test in ambiente di prova: il rumore generato, infatti, dalle attività quotidianamente pianificate dal sistema operativo per il suo corretto funzionamento non avrebbe altrimenti permesso di rilevare e richiamare l'attenzione su attività veramente sospette.
Lo script, eseguito a intervalli di tempo regolari, richiede al sistema una lista completa delle attività pianificate presenti nel sistema e la confronta con le attività contenute nel file di

appoggio (corrispondenti alle attività pianificate presenti nel sistema alla precendente esecuzione dello script). Nel momento in cui una o più attività rinvenute non sono però presenti all'interno del file di appoggio, se non sono elencate tra le attività considerate "affidabili" scatta l'allarme: lo script fallisce con l'errore "New scheduled task found" e riporta tra le informazioni i dettagli sulle attività pianificate rilevate, il percorso dell'eseguibile e gli argomenti ad esse associati.

5.4 Files civetta

Per contrastare e rilevare il prima possibile la presenza di un criptovirus all'interno di un macchina è stato progettato un meccanismi di controllo di specifici files definiti nel seguito files civette. Tali files vengono in un primo momento immessi in una macchine in percorsi specifici, tipicamente presi di mira dal malware, o in un percorso crato ad ho sul disco principale. Lo scopo di questa duplice politice di dispiegamento è cercare di rilevare più famiglie di criptovirus possibili. Dato che l'utente potrebbe volontariamente o involontariamente manipolare o eliminare alcuni files civetta presenti in percorsi che quotidianamente utilizza e controlla, i files civetta immessi in tali percorsi vengonon tutti marcati come nascosti all'utente. Tuttavia, un tale approccio rischia di non essere efficace nella rilevazione di un criptovirus configurato per saltare files marcati come nascosti considerandoli al pari dei files di sistema. Per ovviare a tale eventualità è stato ideato il secondo meccanismo di dispiegamento che utilizza una cartella creata ad hoc con un nome facilmente comprensibile all'utente della macchina, ma non altrettanto facilmente escludibile da un criptovirus, contenente un file civetta, questa volta non nascosto.
Il file civetta creato e immesso nelle macchine non è altro che un semplice file di testo contenente un passo del celebre Lorem ipsum e, con una grandezza di 3.439 byte si assicura di essere scelto tra i primi files da criptare da parte di eventuali criptovirus.

5.4.1 Dispiegamento

Lo script per il dispiegamento dei files civetta si occupa di copiare nel file system del PC su cui viene lanciato il file allegato ("civetta") con l'estensione specificata in speciali percorsi pre-

impostati di tutti gli utenti. Lo script,inoltre, registra i percorsi di ogni file “civetta” creato all’interno di uno speciale file di controllo. Al termine scorre rapidamente il file di controllo alla ricerca di eventuali riferimenti pendenti.

Tramite opportuni parametri lo script permette la scelta del percorso speciale in cui copiare il file “civetta”, a scelta tra “Documents”, “Desktop”, “Pictures” e una cartella creata ad hoc sul disco principale denominata “___aaa_non_cancellare”; di specificare l’estensione da assegnare al file “civetta”; di modificare il percorso del file di controllo. Inoltre, con un parametro dedicato, consente all’utente di bonificare il file di controllo eliminando ogni riferimento pendente a files “civetta” non più presenti nel file system. Per eseguire il dispiegamento vero e prorpio lo script genera, innanzitutto, una lista di percorsi in cui andare a copiare il file “civetta”: nel caso in cui il percorso speciale scelto sia la cartella “___aaa_non_cancellare” la procedura è immediata; in caso contrario lo script esplora l’intero file system alla ricerca dei percorsi speciali scelti. Nel condurre l’esplorazione, partendo dalpercorso “C:\Users\”, lo script esamina ogni sotto-percorso alla ricerca di un percorso speciale scelto: così facendo lo script è in grado di scovare, ad esempio, il Desktop di ogni utente, anche nel caso in cui questo sia localizzato in un percorso diverso dal percorso standar. Una volta generata la lista dei percorsi da utilizzare, lo script controlla per ognuno di questi l’eventuale presenza di un file“civetta” con la medesima estensione dispiegato in precedenza: se tale file “civetta” è rilevato lo script controlla che il percorso corrispondente al file sia presente all’intero del file di controllo e, in caso contrario, lo aggiunge. Se il file “civetta” con l’estensione specificata non è presente nel percorso preso in esame, lo script ne genera uno copiandovi il file “civetta” allegato e assegnando a quest’ultimo l’estensione specificata. Lo script procede con un controllo sull’effettiva presenza nel file system del file “civetta” appena creato e, in caso contrario, registra e segnala l’avvenuto errore. Se non riscontra errori nella creazione del file “civetta”, lo script procede etichettando come “Hidden” il file a meno che non sia all’interno della cartella “___aaa_non_cancellare”.

Una volta terminata la distribuzione dei files “civetta” lo script effettua una rapida verifica della consistenza del file dicontrollo: per ogni percorso contenuto nel file di controllo lo script verifica che il corrispondente file “civetta” sia effettivamente presente e, in caso contrario registra e segnala l’errore. Se il parametro apposito è impostato lo script segnala l’errore come “warning” ed elimina il riferimento pendente dal file di controllo senza registrare l’errore.

Prima di terminare lo script controlla la presenza di eventuali errori registrati e l'effettiva presenza di almeno un file "civetta" all'interno del file system. Se non vi sono errori registrati ed è presente almeno un file "civetta" nel file system lo script termina con un stato di successo, in ogni altro caso lo script termina con insuccesso. L'esplorazione dell'intero file system è chiaramente un'oparazione onerosa in termini di cicli macchina; si è tuttavia resa necessaria per garantire l'efficaia dello script anche qualora percorsi speciali quali il Desktop di uno o più utenti non si trovino nel percorso standard (ad esempio usando OneDrive è possibile che il Desktop di uno o più utenti siano all'interno di una sottocartella di OneDrive). Inoltre, un'esplorazione completa del file system permette di scovare tutti e soli gli utenti effettivamente presenti sul PC. Considerato che lo script per il dispiegamento dei files civetta è destinato all'utilizzo una tantum, l'onerosità dell'esplorazione è considerabile accettabile.
La creazione e la consistenza del file di controllo sono di fondamentale importanza per il corretto funzionamento del successivo script di controllo dei file "civetta" sparsi nel file system.

5.4.2 Controllo

Lo script per il controllo dei files civetta verifica in ogni percorso presente all'interno del file di controllo specificato l'esistenza e la consistenza del file "civetta" precedentemente creato dallo script per il dispiegamento dei files civetta. Se uno dei files in questione dovesse sparire dal file system o dovesse venire alterato nei contenuti lo script segnala immediatamente lo stato di errore riportando i dettagli in diagnostica.
Tra i parametri in ingresso lo script richiede il valore hash corretto di ogni file "civetta" (calcolato utilizzando SHA512) e il percorso del file di controllo da usare. La prima operazione eseguita dallo script è la verifica dell'esistenza del file di controllo inserito. Se tale file non è presente nel file system al percorso indicato lo script termina con stato "Control file not found", inserendo tra le informazioni di diagnostica il percorso del file di controllo non trovato. Lo script prosegue estraendo i percorsi dei files "civetta" da monitorare presenti nel file system. Per ogni percorso lo script controlla, innanzitutto, l'esistenza del file "civetta". In seguito lo script calcola il valore hash di quest'ultimo servendosi dell'algoritmo SHA512. Il valore hash calcolato è dunque confrontato con quello passato in ingresso. Nel caso in cui lo script abbia riscontrato almeno un file "civetta" non più presente sul file system o con un valo-

re hash differente dall'originale, esso terminerà con stato "Error" inserendo tra le informazioni di diagnostica i dettagli di ogni errore rilevato.
Nel caso in cui non sia stato possibile controllare alcun file "civetta" (e.g.: il file di controllo è vuoto) lo stato è modificato in "No file to check". Se non sono stati riscontrati errori lo script termina con successo con stato "All Checked", in ogni altro caso lo script termina con insuccesso. Nel caso in cui vari files "civetta" risultino non più presenti sul file system può essere utile, dopo essersi assicurati che non siano stati manipolati da malware che modificano alche il nome dei files, eseguire nuovamente lo script di "Civetta files Deploy" attivando l'opzione di bonifica del file di controllo per rimuovere eventuali falsi positivi dovuti a files non trovati.

5.5 Schede di rete

Pensato per isolare completamente un PC infetto, lo script si occupa di disabilitare ogni scheda di rete connessa allo stesso. Per farlo ottiene innanzitutto la lista di ogni interfaccia di rete connessa al PC, nel farlo include molte più interfacce delle schede di rete fisicamente connesse al PC ma, essendo una procedura di emergenza ed essendo che nel più ci sta il meno, il fatto non è considerato un difetto. Ottenuta la lista delle interfacce di rete lo script prosegue disabilitandole una ad una.
Si noti che , così facendo la sonda non sarà più in grado di comunicare con la piattaforma di controllo remoto né di ricevere da essa istruzioni: il PC risulterà offline è si renderà necessario un intervento in loco da parte di un tecnico.

6 Conclusioni

Sicurezza e business continuity sono temi molto caldi nell'attuale panorama aziendale italiano. Soluzione di recente impiego, come Datto RMM e Autotask PSA permettono di facilitare il compito dei fornitori di servizi gestiti e di soddisfare i crescenti bisogni delle imprese in termini di sicurezza e business continuity. Soluzioni come quelle proposte in questo studio consentono di innalzare ancor di più l'asticella della sicurezza intformatica all'interno di un'azienda. Tali soluzioni sono, infatti, in grado di prevenire errori e disattenzioni molto frequenti degli utenti aziendali di PC, che incolontariamente rischiano di mettere seriamente a repentaglio gli affari della loro azienda. Inoltre, grazie a un monitoraggio costante, permettono di rilevare più rapidamente un'infezione da criptovirus e, una volta rilevata, permettono inoltre di isolarla e segnalarla prontamente al gruppo di tecnici preposti almantenimento dell'infrastruttura informatica aziendale.
Sebbene durante il periodo preso in esame in questo studio non siano emerse criticità tali da verificare il corretto funzionamento delle soluzioni qui proposte, le stesse, messe alla prova in un ambiente fittizio, si sono mostrate estrememente efficenti nel rispondere agli attacchi, garantendo così gli obiettivi di sicurezza e business continuity che hanno mosso l'intero attività.

6.1 Lavori futuri

Parlando di sicurezza in ambito informatico è chiaro che non è possibile parlare di una cosa statica. Dato che gli attaccanti sono continuamente alla ricerca di nuove vie per infettare le macchine, lo sviluppo di nuovi script e l'aggiornamento di quelli frutto del lavoro svolto nel corso di questo studio deve necessariamente continuare.

Oltre a ciò un obiettivo a breve termine è quello di integrare ancor di più il monitoraggio dell'infrastruttura di rete in Datto RMM. Questo è reso possibile rinnovando le strumentazioni fisiche che permettono la connettività con infrasrutture di nuova generazione che consentono un controllo e un livello di configurabilità impensabili con le infrastrutture attuali.
Integrate le infrastrutture di rete sarebbe certamente interessante lavorare a una migliore e più profonda integrazione tra sistemi antivirus e Datto RMM. L'integrazione consentirebbe di monitorare a fondo l'attività del software antivirus installato sulle macchine e inserire ogni allarme proveniente da tale software nello stesso canale degli allarmi generati all'interno di Datto RMM.
Questo aprirebbe la strada a un obiettivo ancora più ambizioso: sfruttare le otenzialità di Autotask PSA per mostrare al cliente le informazioni principali sulla sua azienda presenti all'interno della piattaforma e consentire al team informatico interno all'azienda la visione delle informazioni tecniche utili per rispondere prontamente a un attacco dall'esterno o a un'infezione interna.

A Esempio di codice

Di seguito è riportato il codice dello script per la creazione di amministratori locali. Il codice dello script è scritto per Powershell versione 2.0+

```
$list_admin_2_save=$env:admin_2_save.Split(",")

Write-Host "Create New Administrator [WIN 7+]"
Write-Host "-------------------------------------"
Write-Host "  Username:             $env:user_name"
Write-Host "  Password length:      $env:user_password_length"
Write-Host "  Remove other admins:  $env:remove_other_admin"
Write-Host "  Custom field to use:  $env:CustomField"
Write-Host "  Force creation:       $env:force_creation"
Write-Host "  Admins to save:"
foreach($listed_admin in $list_admin_2_save) {Write-Host "    - $listed_admin"}
Write-Host "-------------------------------------"
Write-Host ""
function Get-RandomCharacters($length, $characters) {
    $random = 1..$length | ForEach-Object { Get-Random -Maximum $characters.length }
    $restore_ofs=$private:ofs
    $private:ofs=""
    $return_string=[String]$characters[$random]
    $private:ofs=$restore_ofs
    return $return_string
}

$NetUser = (wmic useraccount get name)
$LineCount = ($NetUser | Measure).Count
$Count = $LineCount-1
$UserList=@()
do {
    $temUser=$NetUser[$Count].TrimEnd(" ")
    if($temUser){$UserList += $temUser}
    $Count -= 1
}
while ($Count -gt 1)
$lista1=$UserList

Write-Host "Users found in system:"
$lista1 | ForEach-Object { Write-Host "  - $_" }

$lista2=net localgroup Administrators
$NetUser = (net localgroup Administrators)
$LineCount = ($NetUser | Measure).Count
$Count = $LineCount-3
```

```
$UserList=@()
do {
    $UserList += $NetUser[$Count]
    $Count -= 1
}
while ($Count -gt 5)
$lista2=$UserList

Write-Host "Administrators found in system:"
$lista2 | ForEach-Object { Write-Host " - $_" }

$user_2_create=$true

$UDF=(get-item "env:UDF_$env:CustomField").Value
if ($UDF) {
    $found_admin=$UDF.Split(" ")[0]

    Write-Host ""
    #Check if admin username found is equal to admin username specified
    if($found_admin -eq $env:user_name){
        #Check if admin is already present in the system
        if($lista1 -contains $env:user_name){
            Write-Host "WARNING: $env:user_name special admin already found in system!"
            Write-Host "Making $env:user_name Administrator..."
            net localgroup "Administrators" $env:user_name /add
            $user_2_create=$false
        }
        else {
            Write-Host "WARNING: $env:user_name admin info found in system reg but $env:user_name admin not found in system!"
            if ($env:force_creation -eq $true) {
                Write-Host "WARNING: $env:user_name admin info in system reg will be overwritten!"
            }else {
                Write-Host "ERROR: Enable force creation to overwrite $env:user_name admin info in system reg!"
                exit 1
            }
        }
    } else {
        #Check if admin username found is present in the system
        if($lista1 -contains $found_admin){
            Write-Host "ERROR: $found_admin special admin already found in system!"
            Write-Host "Making $found_admin Administrator..."
            net localgroup "Administrators" $found_admin /add
            exit 1
        }else {
            #Other admin info found in system reg but admin username found is not present in the system: check if info can
             be overwritten
            Write-Host "WARNING: $found_admin admin info found in system reg but $found_admin admin not found in system!"
            if ($env:force_creation -eq $true) {
                Write-Host "WARNING: $found_admin admin info in system reg will be overwritten!"
            }else {
                Write-Host "ERROR: Enable force creation to overwrite $found_admin admin info in system reg!"
                exit 1
            }
        }
    }
}

if ($user_2_create -and $lista1 -contains $env:user_name) {
    Write-Host ""
    Write-Host "ERROR: $env:user_name found in users list but $env:user_name is not a special admin!"
    exit 1
```

```
}

#Create new user?
if($user_2_create){
    #Create randomic password
    Write-Host "Generating random user password..."
    $user_password = Get-RandomCharacters -length $env:user_password_length
      -characters 'qwertyuioplkjhgfdsazxcvbnmMNBVCXZASDFGHJKLPOIUYTREWQ1234567890\?=)(/&%$!,.;:-_@#[]*'
    Write-Host "  Generated: $user_password"
    Write-Host "Done"
    Write-Host ""

    Write-Host "Writing password in custom field..."
    REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\CentraStage /v "Custom$env:CustomField" /t REG_SZ /d "$env:user_name : '$user_password'" /f
    Write-Host "Done"
    Write-Host ""

    #Create new user account
    Write-Host "Creating new user account..."
    Write-Host "     Name: '$env:user_name'"
    Write-Host "     Password: '$user_password'"
    net user $env:user_name $user_password /add /Y
    Write-Host "Done"
    Write-Host ""

    #Make new user account administrator
    Write-Host "Making new user administrator..."
    net localgroup "Administrators" $env:user_name /add
    Write-Host "Done"
}

#Remove other admin?
if ($env:remove_other_admin -eq $true) {
    Write-Host ""
    Write-Host "Revoke all other Administrators..."
    $lista2 | ForEach-Object {
        $username=[String]$_
        $pos = $username.IndexOf("\")
        $username = $username.Substring($pos+1)
        if ($list_admin_2_save -contains $username) {
            Write-Host "  $username ($_) found in admins to save"
        } else {
            if ($username -ne $env:user_name) {
                Write-Host "  revoking $username ($_) ..."
                net localgroup "Users" $_ /add
                net localgroup "Administrators" $_ /delete
            }
        }
    }
    Write-Host "Done"
    Write-Host ""
}

exit 0
```

Bibliografia

[1] Achab. *Requisiti di Rete per Datto RMM.* Achab.it, 2019.

[2] Abdurrahman Akkas, Christos Nestoras Chachamis, and Livio Fetahu. *Malware Analysis of WanaCry Ransomware.* Massachusetts Institute of Technology, 2017.

[3] Autotask. *10 ways unifying IT service delivery maximizes profits and productivity.* Autotask, 2018.

[4] Furio Borsi. *L'automazione per bloccare nuovi virus e attacchi.* Achab.it, 2019.

[5] Augusto Ciuffoletti. *Beyond Nagios - Design of a Cloud Monitoring System.* Università di Pisa - Dept. of Computer Science, Pisa, ITALY, 2016.

[6] Matteo Cuscusa. *Malware fileless: cosa sono e come difendersi dai virus "invisibili".* Cybersecurity360.it, 2018.

[7] Datto. *Datto RMM Web Portal Version 7.7.0.* Datto, 2019.

[8] Roger A. Grimes. *Malware loves Windows Task Scheduler.* CSO, 2011.

[9] Helpnetsecurity. *Ransomware is the leading cyber threat experienced by SMBs.* helpnetsecurity.com, 2018.

[10] Helpnetsecurity. *Attack tools and techniques used by major ransomware families.* helpnetsecurity.com, 2019.

[11] Kaseya. *Agent User Guide Version R95.* Kaseya, 2019.

[12] Kaseya. *Kaseya® Virtual System Administrator™ Online User Assistance*. help.kaseya.com, 2019.

[13] Kaseya. *Manage and Automate All of IT with VSA*. Kaseya, 2019.

[14] Kaseya. *Monitor User Guide Version R95*. Kaseya, 2019.

[15] Katie Martel. *The Ultimate IT PSA Buyer's Guide*. Datto, 2018.

[16] Nagios. *Nagios Support Knowledgebase*. support.nagios.com, 2018.

[17] Margaret Rouse and John Moore. *Professional services automation (PSA)*. SearchITChannel.com, 2017.

[18] Margaret Rouse, John Moore, and Spencer Smith. *RMM software (remote monitoring and management software)*. SearchITChannel.com, 2018.

[19] Sophoslabs. *Sophos 2020 Threat Report*. sophos.com, 2019.

[20] Ian van Reenen. *Ransomware is a big problem, but it's also a big opportunity for MSPs to educate clients*. helpnetsecurity.com, 2018.

[21] Wikipedia.org. *Active Directory*. https://it.wikipedia.org/wiki/Active_Directory, 2019.

[22] Serafeim Zanikolas and Rizos Sakellariou. *A taxonomy of grid monitoring systems*. School of Computer Science, The University of Manchester, Manchester, UK, 2004.