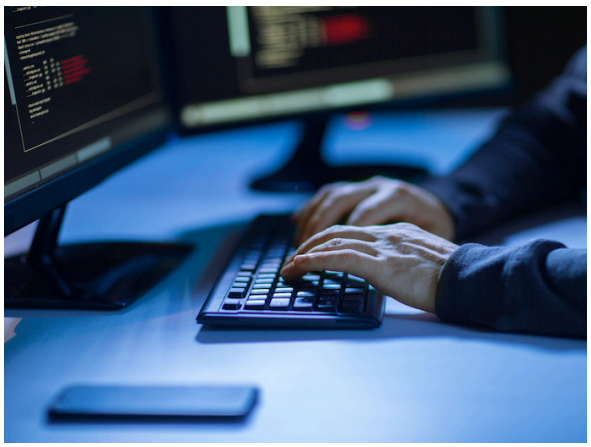
PHILOS: Real-time Detection and Automated Mitigation of BGP Prefix Hijacking Attacks

Risultati in breve

Un software difende le reti da interruzioni e attacchi informatici

È stato sviluppato un nuovo software per individuare e mitigare in pochi secondi le interruzioni di rete e gli attacchi informatici. Questa tecnologia potrebbe far risparmiare ogni anno milioni di euro in riparazioni e perdite commerciali, e offrire un servizio più affidabile agli utenti Internet.

SICUREZZA



© Syda Productions, Shutterstock

Internet, la rete delle reti con un successo senza precedenti e una portata a livello mondiale, dipende fortemente da alcune tecnologie essenziali. Una di queste tecnologie è il Border Gateway Protocol (BGP).

«Il BGP è il collante che tiene assieme Internet», spiega Xenofontas Dimitropoulos, coordinatore del progetto PHILOS e ricercatore presso la Fondazione per la ricerca e la tecnologia Hellas in Grecia. «Si tratta di un protocollo di rete di fondamentale importanza, utilizzato dai fornitori di servizi Internet (ISP) per scambiarsi informazioni sui percorsi che verranno utilizzati per inviare traffico a diverse destinazioni».

Sebbene questo protocollo sia stato progettato all'incirca tre decenni fa, esso non autorizza e convalida di default le informazioni scambiate tra ISP per stabilire

percorsi end-to-end. In pratica ciò significa che un ISP può intenzionalmente, o come capita più spesso, accidentalmente, inviare percorsi erronei ad un vicino, inducendolo erroneamente a selezionare un router sbagliato per inviare traffico.

«Ciò può provocare interruzioni del servizio Internet», afferma Dimitropoulos. «E può persino aprire la strada a sofisticati attacchi informatici, con tanto di intercettazioni o manipolazioni del traffico Internet».

Gli attacchi informatici possono essere devastanti. I criminali possono impersonare le reti delle vittime, rubare informazioni sensibili o intercettare e manipolare furtivamente il traffico diretto a destinazioni legittime. Incidenti simili fanno spesso notizia in quanto causano grande scompiglio.

Reti di protezione

Una delle ragioni per cui è così difficile porre rimedio a questa debolezza è il fatto che esistono letteralmente decine di migliaia di ISP sparsi nel mondo. Nuovi componenti aggiuntivi di sicurezza BGP dovrebbero essere adottati dalla maggioranza degli ISP perché possano essere efficaci.

«Ma il BGP resta comunque vulnerabile a numerosi attacchi, di conseguenza gli ISP sono poco motivati ad implementare componenti aggiuntivi di sicurezza BGP», aggiunge Dimitropoulos. «E così l'utilizzo a livello globale procede molto lentamente».

Il progetto PHILOS, con il sostegno del Consiglio europeo della ricerca, ha cercato di risolvere il problema della debolezza relativa ai protocolli BGP adottando una strategia differente. Il team si è prefissato di sviluppare e testare un nuovo software di prova di concetto in grado di rilevare e mitigare in pochi secondi incidenti come le grandi interruzioni di servizi.

«Abbiamo sviluppato un software chiamato ARTEMIS, e lo abbiamo testato con alcuni ISP reali in Grecia e negli Stati Uniti», osserva Dimitropoulos. «Per fare ciò abbiamo lavorato a stretto contatto con gli operatori di rete ISP. È stato fondamentale che abbiano accettato di testare questo approccio all'avanguardia per proteggere la loro rete».

Ciò che distingue l'approccio di PHILOS, sottolinea Dimitropoulos, è il fatto che il software fornisce il rilevamento e la mitigazione automatica in tempo reale utilizzando algoritmi e tecnologie innovativi, riducendo così i tempi di rilevamento e mitigazione da ore e giorni a pochi secondi.

Una brillante idea commerciale

I potenziali benefici per gli IPS sono evidenti. Le interruzioni di rete costano milioni di euro, disturbano le attività delle aziende e lasciano i consumatori estremamente insoddisfatti del servizio. Ciò si ricollega al secondo obiettivo chiave del progetto PHILOS, ovvero, esaminare il potenziale di commercializzazione del software tramite una futura start-up.

Dimitropoulos e il suo team hanno presentato ARTEMIS a varie conferenze degli operatori di rete, allo scopo di far conoscere il proprio approccio innovativo alla sicurezza della rete. È stato utile il fatto che molti dei principali fornitori di servizi Internet di telecomunicazione abbiano utilizzato ARTEMIS attraverso il progetto PHILOS per proteggere la loro rete.

«Stiamo vagliando attivamente le opportunità di commercializzazione di questa tecnologia», afferma Dimitropoulos. «Il nostro obiettivo è creare un'azienda spin-off nel 2021, e attualmente abbiamo in corso delle trattative con potenziali clienti e investitori. Portare questa innovazione sul mercato e dar vita ad attività sostenibili nel lungo periodo sarebbe indubbiamente un grande risultato».

Parole chiave

PHILOS, Internet, attacchi informatici, BGP, rete, ISP, software, algoritmi

Scopri altri articoli nello stesso settore di applicazione

Chiave di certificazione su più livelli per le infrastrutture critiche

Occhi e orecchie ovunque per proteggere i porti europei

Rafforzare la resilienza degli ospedali alle minacce

Un quadro per la sicurezza informatica 4.0 a tutela degli interessi dell'Industria 4.0

Informazioni relative al progetto

PHILOS

ID dell'accordo di sovvenzione: 790575

DOI
10.3030/790575

Progetto chiuso

Data della firma CE
9 Aprile 2018

Finanziato da
EXCELLENT SCIENCE - European Research Council (ERC)

Costo totale
€ 150 000,00

Contributo UE
€ 150 000,00

Coordinato da

Data di avvio
1 Gennaio 2019

Data di completamento
30 Giugno 2020

IDRYMA TECHNOLOGIAS KAI EREVNAS
Greece

Ultimo aggiornamento: 11 Dicembre 2020

Permalink: https://cordis.europa.eu/article/id/428568-software-defends-networks-against-outages-and-cyberattacks/it