ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4796 di Venerdì 16 ottobre 2020

Allarme rosso per gli attacchi agli ATM

Le principali agenzie della sicurezza informatica degli Stati Uniti hanno lanciato un allarme rosso per i ripetuti attacchi, portati dalla Corea del Nord, al sistema mondiale di gestione degli ATM

Sono ben quattro le agenzie della sicurezza informatica degli Stati Uniti che hanno lanciato un allarme rosso per i ripetuti attacchi portati ai sistemi ATM mondiale, da parte della Corea del Nord. Le agenzie coinvolte sono la Cybersecurity and Infrastructure Security Agency (CISA), il Department of the Treasury (Treasury), lo Federal Bureau of Investigation (FBI) e U.S. Cyber Command (USCYBERCOM). Il documento, che ha portato all'attenzione di tutte le banche mondiali questa tipologia di attacco, si chiama "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks.".

Già in passato la Corea del Nord aveva attaccato con tecniche informatiche i sistemi finanziari mondiali, ma da febbraio 2020 l'attività si è intensificata, concentrandosi su trasferimenti fraudolenti di denaro e erogazione di contante dalle macchine automatiche.

Il documento allegato offre una panoramica di questo schema di attacco informatico, con un profilo del gruppo di Hackers responsabili per questa attività e con l'indicazione di possibili misure di mitigazione dell'attacco. I sistemi di intelligence della Corea del Nord finanziano una squadra di Hackers, chiamata BeagleBoyz, che svolge attività informatiche fraudolente indirizzate a numerosi paesi del mondo.

Ad esempio, nel 2018 questa banda di Hackers riuscì a compromettere il sistema SWIFT, che rappresenta il sistema mondiale di interscambio di informazioni finanziarie fra banche ed altre istituzioni.

Questo comportamento illecito è stato sanzionato anche da una risoluzione del consiglio di sicurezza delle Nazioni Unite, perché ha portato a significativi spostamenti di fondi in favore della Corea del Nord. Inoltre questo tipo di attacchi ha diminuito la credibilità dei sistemi finanziari internazionali, creando a catena numerosi problemi operativi.

Questi attaccanti hanno più volte reso inutilizzabili i sistemi informativi bancari e non è improbabile che anche i recentissimi attacchi, che hanno colpito le banche italiane, possano essere riconducibili a questi criminali informatici. Ad esempio, nel 2018 una banca africana non ha potuto rendere servizi ATM ai propri clienti per quasi due mesi, a seguito di un attacco informatico di alto livello. In Cile, migliaia di computer bancari sono stati messi fuori servizio da un attacco similare.

Gli attacchi in genere sono diretti a macchine che utilizzano sistemi Windows e dal 2015 al 2020 queste sono state le nazioni del mondo colpite da questi attacchi: Argentina, Brazil, Bangladesh, Bosnia and Herzegovina, Bulgaria, Chile, Costa Rica, Ecuador, Ghana, India, Indonesia, Japan, Jordan, Kenya, Kuwait, Malaysia, Malta, Mexico, Mozambique, Nepal, Nicaragua, Nigeria, Pakistan, Panama, Peru, Philippines, Singapore, South Africa, South Korea, Spain, Taiwan, Tanzania, Togo, Turkey, Uganda, Uruguay, Vietnam, Zambia.

Il documento allegato, in lingua inglese, offre in ampio dettaglio con illustrazione delle varie tecniche di attacco. In particolare, queste tecniche di attacco sono stato in grado di compromettere lo schema normativo ISO 8583, utilizzato nei sistemi Windows. Gli specialisti raccomandano di effettuare immediatamente aggiornamenti di tutti i sistemi operativi coinvolti, per rendere più difficile l'intrusione da parte di estranei.

È importante segnalare che, oltre alle "consuete" tecniche di attacco, negli ultimi tempi questa squadra di hacker ha aggredito anche lo scambio di cripto valute, sottraendo addirittura milioni di dollari per ogni attacco. Il grande vantaggio dell'attacco alle cripto valute è che l'attaccante ha a disposizione uno strumento irreversibile per convertire cripto valuta in valute tradizionali. Lo strumento informatico che è stato violato, per portare a termine i furti di cripto valuta, viene chiamato COPPERHEDGE. Anche in questo caso, le quattro agenzie americane della sicurezza hanno messo a disposizione strumenti di contrasto di questa tipologia di attacco.

Joint Cybersecurity Advisory (pdf)

Adalberto Biasiotti