Scoperto un APT mai rilevato in precedenza a livello globale **Leggi...**

Home Page » News

Security News

Mercoledì 11 Gennaio 2017

Eye Pyramid, che cos'è e come scoprire se si è stati infettati

Una complessa attività di indagine denominata ***Eye Pyramid***, condotta dal *Cnaipic, Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche* del servizio Polizia Postale e delle Comunicazioni e coordinata dalla Procura della Repubblica di Roma, ha fatto luce su un **esteso sistema di cyberspionaggio** messo in piedi con attacchi informatici di tipo ***APT* (*Advanced Persistent Threat*).**

L'invio di un messaggio di posta elettronica contenente un **allegato malevolo** è alla base della creazione di una **vera e propria centrale di sorveglianza** ai danni di **numerose autorità politiche e militari** di strategica importanza e di **sistemi informatici utilizzati da Stato e altri enti pubblici** come *istruzione.it, gdf.it, bancaditalia.it, camera.it, senato.it, esteri.it, tesoro.it, finanze.it, interno.it.*

A svelare l'esistenza del malware è stata proprio un'email indirizzata ad un amministratore di sistema di un'importante infrastruttura nazionale, al quale non è passata inosservata. L'email, dopo essere stata oggetto di analisi tecnica, è stata segnalata al *Cnaipic, Centro nazionale anticrimine informatico della Polizia Postale.*
Il messaggio di posta elettronica conteneva dunque un tipo di **malware** utilizzato generalmente per le campagne di ***spear phishing***, ovvero phishing focalizzato su uno specifico obiettivo.

I protagonisti del cyberspionaggio si sono avvalsi dunque di una *botnet*, una vasta rete di computer creata infettando i dispositivi con un malware di tipo ***Rat* (Remote access tool)**, che consente, una volta installato, il **pieno controllo da remoto del dispositivo infetto** e che avrebbe permesso dunque agli hacker per lungo tempo di acquisire in maniera silenziosa informazioni riservate per poi riversarle all'interno di server localizzati negli Stati Uniti.

A seguito di queste vicende di cyberspionaggio al centro della cronaca, la cui reale portata è tutt'altro che chiarita, **il nostro team Cert sta operando le necessarie verifiche per**

CONTATTACI

Vedi anche:

- Yarix rilascia il secondo YSOC Security Report
- Sicurezza Convergente 4 Club TI
- Scoperto un APT mai rilevato in precedenza a livello globale
- Offerte di lavoro | Cybersecurity
- Var Group attraverso Yarix acquisisce il 10% di Athesys
- Var Group, Yarix e Darktrace insieme a Cybertech Europe 2019
- WunderVAR | Play your future with Var Group
- Offerta di lavoro | Security Sales Specialist
- Sharing Experiences in Compliance | Bologna 2 ottobre
- Offerta di lavoro | Cybersecurity Manager
- Offerta di lavoro | Junior Security Engineer
- Attacco hacker a Bonfiglioli neutralizzato anche grazie all'intervento di Yarix
- Yarix presenta il primo YSOC Security Report
- Richmond Cyber Resilience Forum, Gubbio 19-21 giugno
- Start Your Industry 4.0
- Vulnerabilità critica in Remote Desktop: Microsoft rilascia le patch anche per Windows XP e Windows Server 2003 (CVE-2019-0708)
- L'exploit ThrAngryCat potrebbe colpire milioni di dispositivi Cisco (CVE-2019-1649 CVE-2019-1862)
- Var Group acquisisce il 60% di Gencom
- YCERT: Analisi di Gootkit, malware all'attacco di PA e aziende

escludere che le reti dei clienti siano state oggetto di violazione mediante utilizzo dello stesso malware.

Per quanti desiderino eseguire dei controlli sui propri PC Windows, mettiamo a disposizione uno script in VBS, di cui si può fare il **download**.

Dalla lettura dell'ordinanza di custodia cautelare predisposta dal GIP si possono infatti estrarre degli elementi utili ad eseguire dei controlli sui sistemi Windows. Il malware utilizzato si appoggia ad un componente commerciale di terze parti (MailBee.NET.dll prodotto dalla Afterlogic co.) per la comunicazione attraverso email.
Questo prodotto è licenziato e la stessa licenza che identifica univocamente il licenziatario è stata utilizzata a partire dalle prime infezioni del malware nel 2010, fino a dicembre 2015.

La chiave di licenza, nelle macchine infette, è registrata in una apposita sezione del registro di sistema. Essendo la chiave parzialmente nota attraverso la lettura dell'ordinanza del GIP (alcune parti non sono correttamente identificabili, a causa della bassa qualità della scansione), è facile verificarne la presenza nel registro. Da analisi già effettuate da altri malware analyst sono emerse altre chiavi di licenze potenzialmente coinvolte.
Per semplificare l'individuazione della chiave di licenza nel proprio PC, abbiamo dunque preparato un semplice **script in VBS**, **che verifica l'eventuale presenza di una delle sottostringhe della chiave di licenza** che, se rinvenute, costituiscono un forte indicatore dell'avvenuta infezione.

Dopo aver aperto il file .zip, al cui interno è presente un file con estensione .vbs, è sufficiente fare un doppio clic sopra.

Gli hash MD5 del file compresso e dello script all'interno sono i seguenti:

053fffd972019704756ee95d9f1e7287 *eyepyramid-check.zip
7c5a986075ade28aaba18d335dd34ef8 *eyepyramid-check.vbs

Reti resilienti a prova di cyber attack... anche in ambienti OT

Var Group ti aspetta al Security Summit Milano

Var Group e Yarix di nuovo in campo con CyberChallenge.IT

Live Webinar Digital Security con Var Group e Microsoft

Offerta di lavoro | Cyber Security Specialist

Var Evolution, l'innovazione vissuta

Blockchain per l'innovazione, Yarix e Var Group investono nella startup Commerc.io.

Sextortion, ricatto in bitcoin con minaccia di divulgazione

Var Group, Yarix e Darktrace insieme a Cybertech Europe 2018

AI e Machine Learning: Kleis entra nella Digital Security Division di Var Group

Offerta di lavoro | Tecnico sistemista

Var Group annuncia la quarta partnership nel segno della sicurezza

La nuova normativa PSD2 tra opportunità e sfide, Milano 28 giugno

Offerte di lavoro | Cyber Security

Richmond Cyber Resilience Forum, Gubbio 21-22 giugno

Security Summit Roma, Seminario Bitdefender - Yarix

Var Group e Yarix Partner di ABI Banche e Sicurezza 2018

BLOCKCHAIN E IMPRESA - 28/03 Camera di Commercio di Firenze

NUOVA PRIVACY - 28/03 Confcommercio di Treviso

Sicurezza Convergente, un approccio olistico

Var Group e la sua Cyber Division Yarix annunciano l'acquisizione del 19% di Blockit

Security Summit Milano, Seminario Bitdefender - Yarix

Offerta di lavoro | IT Security Specialist

Var Group e Yarix Gold Sponsor di ITASEC18

Var Group e Yarix in campo con CyberChallenge.IT

Campagna di malspam minaccia le aziende italiane

Industrial CyberSecurity: Var Group e Yarix a ICS Forum

Breach Compilation: un'imponente risorsa facilita l'accesso a 1,4 miliardi di credenziali

Rischio Cyber e normativa europea GDPR: Milano, 4 dicembre

Grave vulnerabilità in Microsoft Office sfruttata dal gruppo Cobalt

GDPR e Cyber Security nella sanità: Firenze, 30 novembre

GDPR: Var Group e la sua Cyber Division Yarix acquisiscono il 20% di Privatamente