LATERAL NEWS — LATERALCODE

LE UNICHE SPIEGAZIONI POSSIBILI SONO CHE NON RIUSCIATE A CAPIRE, CHE FACCIATE FINTA oppure che…

21 giugno 2024

Avviso: articolo NON politically correct.

Consiglio non richiesto: leggete fino in fondo oppure non iniziate affatto, le mezze misure vanno bene solo in trattoria.

■ Incentivo: per chi arriva in fondo, una sorpresa che rende TUTTO più facile (*)

La scorsa settimana il *National Cyber Security Centre* olandese ha pubblicato una notizia. Per i più volenterosi questo è il link: https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices . Basterà chiedere a Google di tradurre e leggerselo.

Per i più pigri invece ecco 6 estratti:

1. “[…] il **MIVD** ha condotto ulteriori ricerche ed è diventato evidente che la campagna di spionaggio informatico cinese sembra essere **molto più grande di quanto precedentemente noto**.”

2. “[…] ha dimostrato che l’attore statale ha ottenuto l’accesso ad almeno **20.000 sistemi FortiGate** in tutto il mondo sia nel 2022 che nel 2023 entro pochi mesi attraverso la vulnerabilità con le caratteristiche CVE-2022-42475.”

3. “[…] la ricerca mostra che l’attore statale dietro questa campagna era a conoscenza di questa vulnerabilità nei sistemi FortiGate almeno **due mesi prima che Fortinet annunciasse la vulnerabilità**. Durante questo cosiddetto periodo ‘zero-day’, l’attore ha infettato **14.000 dispositivi**. Gli obiettivi includono dozzine di governi (occidentali), organizzazioni internazionali e un gran numero di aziende nel settore della difesa”

4. “Anche se una vittima installa aggiornamenti di sicurezza da FortiGate, l’attore statale continua a mantenere questo accesso”

5. “(I) dispositivi edge (quali firewall, server VPN, router, server di posta elettronica ecc. n.d.r.) […] sono l’obiettivo preferito per i malintenzionati. I dispositivi edge si trovano ai bordi della rete IT e dispongono regolarmente di una connessione diretta a Internet.”

6. “La compromissione iniziale di una rete IT è difficile da prevenire se l’attaccante utilizza uno zero-day”

Che abbiate letto l’articolo oppure gli estratti dovrebbero comunque esservi sufficienti le **diciassette parole** del punto 4:

“Anche se una vittima installa aggiornamenti di sicurezza da FortiGate, l’attore statale continua a mantenere questo accesso”

Cosa volete di più? Ok, se siete ingordi, troverete sollazzo con quanto aggiunge *Red Hot Cyber* nel suo articolo a commento (link all’articolo: https://www.redhotcyber.com/post/cyber-spionaggio-cinese-20-000-sistemi-fortigate-compromessi-lo-rivelano-i-servizi-di-intelligence-olandesi/) :

“Gli esperti avvertono che Coathanger è in grado di ‘sopravvivere’ ai riavvii del sistema e agli aggiornamenti del firmware”

[OT: dite la verità, avete contato le parole poco fa?]

LA PORZIONE DA TRATTORIA (tradotto: dovete reggere la botta)

Insomma, visto che sovente si parla di virus (benché, altrettanto spesso, in maniera impropria) siamo giunti, *obtorto collo*, a parlare di **minacce residenti**, proprio come l’herpes labialis che preso una volta te lo tieni per tutta la vita.

I vostri sistemi hanno l'herpes…

- Questo **cambierà il vostro modo di pensare alla sicurezza**? O continuerete ancora a parlare **compulsivamente** di "*difesa proattiva*" (faccio persino fatica a scriverlo!), *Zero Trust*, intercettazione e analisi (evito più che posso la solita sequela di termini inglesi perché fa troppo fico e qui siamo in trattoria)?

- Vi abbandonerete ancora, lascivi, tra le braccia sensuali dell'intelligenza artificiale? Esiste **un livello di delega che vi fa paura** oppure vi sta davvero tutto bene così, comodamente eterocontrollato?

- Continuerete ancora a scommettere alla cieca sulle mirabolanti capacità dei *big player* (ops, scappato l'inglesismo) che sponsorizzano così tanti convegni e simposi "all'avanguardia", dove chi parla sono sempre i soliti noti, con un sacco di fuffa e di sovrastrutture tecniche, **lessicali** e **markettare** (però le parole della frase di prima le avete contate, non si sa mai vi stessi fregando)?

- Continuerete ancora a preferire l'**integrità della vostra carriera** di consulenti, CISO, IT manager ecc. all'**integrità dei dati e delle reti** che, in teoria, sareste chiamati a proteggere con la vostra preparazione, dedizione e ricerca? Ma lo capisco sapete, in fondo se vi rasano i dati dopo che avete scelto la GRANDE MARCA, il GRANDE PARTNER (spesso pure straniero: geniale!) chi potrà mai rimproverarvi, quale CdA potrebbe mai incolparvi… (*)

SÌ, MA ADESSO?

■ Bene, ma cosa fareste adesso se foste fra coloro che gestiscono quelle reti e quei dispositivi con l'herpes labialis? Prendereste qualche aciclovir digitale? Cambiereste apparati? Fornitore?

■ O mestiere?

■ E se invece foste fra coloro che (ancora) non ne sono colpiti? Vi affidereste a qualche iperbolica soluzione di IA, magari in difesa proattiva (lo avete capito, sì, che è una baggianata)?

Dai, facciamo i seri.

■ Esiste una tecnologia creata da **mente umana** (!), realizzata sulla base di criteri progettuali di **pensiero sistemico e laterale** (che l'IA se li scorda), la quale problemi come quello riportato nell'articolo non li considera neanche perché… non sono un problema!

■ Esiste una tecnologia creata da mente umana che risolve in un colpo solo le minacce relative a:

intrusioni

esfiltrazioni

backdoor (anche già residenti)

zero-day

DDoS

attacchi supply chain

phishing

(Sì, ma voi proseguite pure sulla solita strada, eh?!)

■ Esiste una tecnologia creata da **mente umana italiana**, unica al mondo e brevettata (tradotto: o compri tricolore o nisba… il che non è poco!)

■ Esiste una tecnologia creata da mente umana **provata e collaudata con successo** negli ambienti più disparati, ostili e sensibili.

■ Esiste una tecnologia creata da mente umana che potete **mettere alla prova quando e come volete** (basta chiedere) per vedere se mantiene ciò che promette; certo, occorre un po' di voglia di cambiare davvero e di fare meglio, altrimenti è difficile che al mattino vi alziate e ve la troviate installata in casa.

■ Esiste una tecnologia, che si chiama **ZeroSurface®**, creata da mente umana ma…

…ma sì, dai, voi **continuate a fidarvi e a farvi servire dai "big"**, specie se **stranieri** e a mezza porzione, condita però da un po' di paroloni in salsa barbecue e sana IA, che in fin dei conti **non si nega a nessuno**.

(*) FONDAMENTALE NOTA DI CHIARIMENTO (se siete arrivati sin qua vi siete meritati il bonus promesso!)

…ma se avete saltato tutto per arrivarci subito, sappiate che non ve lo godete appieno. Fate voi.

Per coloro che finora hanno messo su un piatto della bilancia l'integrità della propria carriera e sull'altro il merito di evolvere (seriamente) i loro sistemi proteggendoli come mai prima di oggi **ma con una tecnologia nuova**, ecco il *grammo di antimateria* che **disintegra i vostri alibi**.

Lo ZeroSurface® rende "semplicemente" **irraggiungibili** -> quindi **indisponibili** -> quindi **"invisibili"** gli oggetti che protegge pur continuando a garantirne la fruibilità. Come ciò avvenga (brevemente: con autorizzazioni asimmetriche e distribuite) non è argomento di questo articolo (ne trovate tanti in giro). Vi basti qui sapere che è quanto di più simile a un cavo di rete sconnesso o a una rete air gap che però "continua a comunicare" come volete voi.

Ciò detto, perché i vostri alibi non tengono?

1. ■ PERCHÉ INSTALLARE UNA PROTEZIONE ZEROSURFACE® **NON RICHIEDE NESSUNA MODIFICA ALLO STATU QUO DEI VOSTRI SISTEMI**

2. ■ PERCHÉ **L'INSTALLAZIONE PREVEDE TEMPI BREVISSIMI** (nei casi standard da poche ore a due settimane)

3. ■ PERCHÉ POTETE **TESTARLA SENZA MODIFICARE LA UX** DELLA VOSTRA STRUTTURA FRUENDO DI UNA **PROVA IN PARALLELO** (da una parte coloro che continueranno a usare applicazioni e servizi come d'abitudine, dall'altra un numero a piacere di persone da voi scelte che testeranno la modalità ZS®). Anche qui, basta chiedere.

4. ■ PERCHÉ QUALUNQUE, SOTTOLINEIAMO "QUALUNQUE", SISTEMA DI "SICUREZZA" VOI ABBIATE GIÀ, **LO ZS® PROTEGGE E RENDE IRRAGGIUNGIBILE (QUINDI INATTACCABILE) PURE LUI** (crepi l'avarizia)

5. ■ E INFINE PERCHÉ SEMMAI VOLESTE TIRARVI INDIETRO (VAI A SAPERE PERCHÉ) **BASTERÀ QUALCHE MINUTO (un quarto d’ora al massimo) PER TORNARE ISTANTANEAMENTE ALLA CONDIZIONE INIZIALE** E A QUEL PUNTO… in bocca al lupo

Avete sentito questo schianto? Erano i vostri alibi.

Gianluigi Merlino

Lateral News — Articoli, idee e riflessioni sullo sviluppo tecnologico e sulla sicurezza informatica non “mainstream”

lateralcode.it