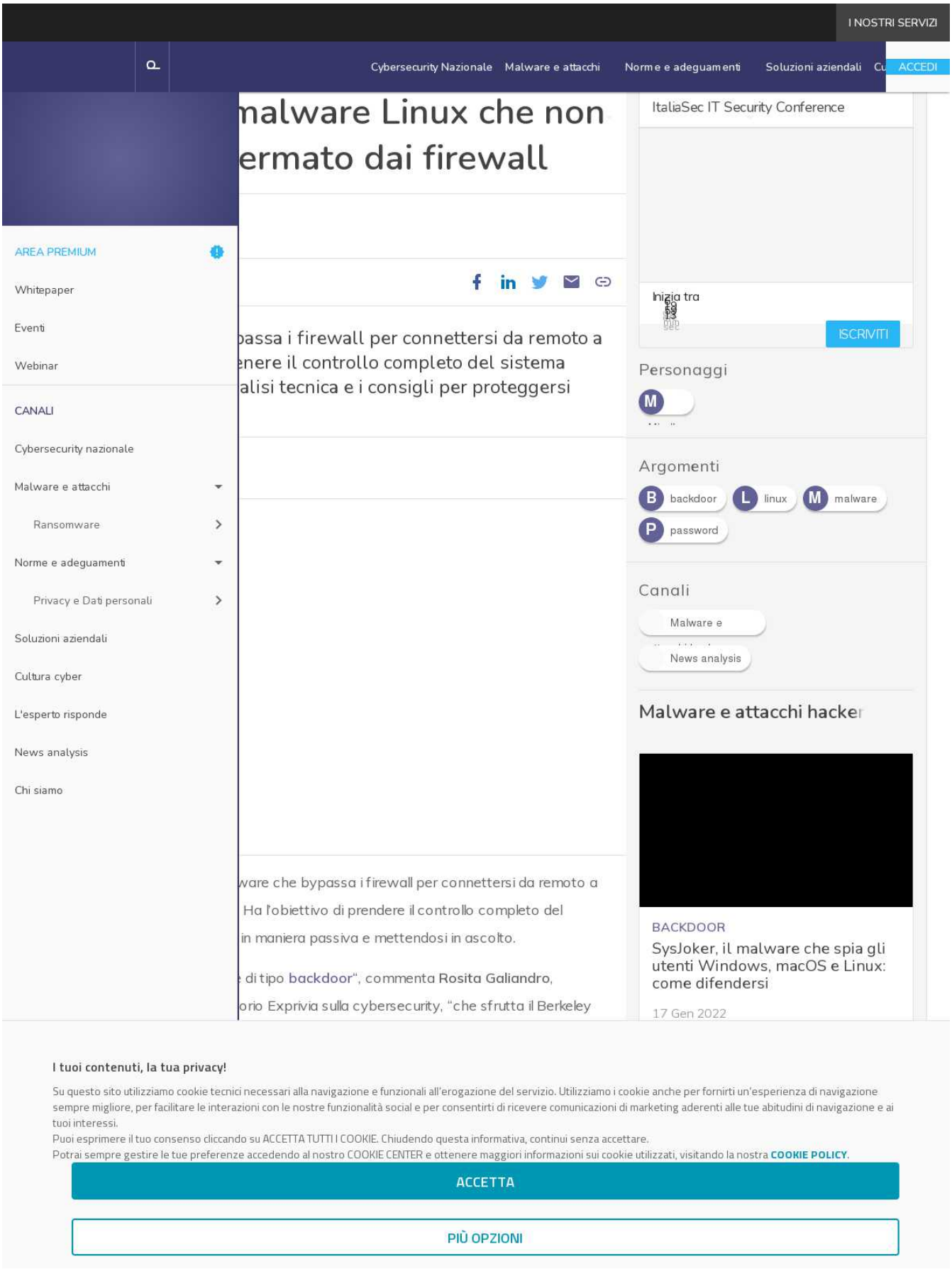

BPFdoor, il malware Linux che non può essere fermato dai firewall

La backdoor passiva bypassa i firewall per connettersi da remoto a una shell di Linux e ottenere il controllo completo del sistema target. Ecco la nostra analisi tecnica e i consigli per proteggersi BPFdoor è un malware che bypassa i firewall per connettersi da remoto a una shell di Linux. Ha l'obiettivo di prendere il controllo completo del sistema sotto attacco, in maniera passiva e mettendosi in ascolto."BPFdoor è un malware di tipo backdoor", commenta Rosita Galiandro, Responsabile Osservatorio Exprivia sulla cybersecurity, "che sfrutta il Berkeley Packet Filter (BPF) per funzionare da backdoor e procedere con la ricognizione. In particolare, BPF è utilizzato per le trasmissioni di pacchetti di dati e la regolamentazione dell'accesso, nonché per l'analisi del traffico di rete".Indice degli argomenti Linux nel mirino di BPFdoorCome agisce il malwareL'analisi tecnica dell'attività che svolge la backdoor Linux nel mirino di BPFdoor A scoprire BPFdoor sono stati i ricercatori di sicurezza di Sandfly Security, secondo cui il nuovo malware grazie alle sue carattersitiche backdoor è riuscito ad agire di nascosto contro i sistemi Linux e Solaris senza essere notata per oltre cinque anni. WEBINAR 25 Maggio 2022 - 14:30Cybersecurity 360Summit: nuove strategie, nuove minacce e nuove difese! Sicurezza Sicurezza dei dati Inizia tra: 814326 Iscriviti al WebinarLeggi l'informativa sulla privacy Email * Consente l'invio di comunicazioni promozionali inerenti i prodotti e servizi di soggetti terzi rispetto alle Contitolari che appartengono al ramo manifatturiero, di servizi (in particolare ICT) e di commercio, con modalità di contatto automatizzate e tradizionali da parte dei terzi medesimi, a cui vengono comunicati i dati. "BPFdoor è un malware ideale per sferrare attacchi continuativi e per lo spionaggio industriale", continua Rosita Galiandro, "dato che non richiede l'apertura di porte o regole del firewall: infatti, ne è immune ed è in grado di rispondere ai comandi provenienti da qualsiasi indirizzo IP". Come agisce il malware "Sfruttando una funzione di sniffing", sottolinea Rosita Galiandro, "che opera nell'interfaccia al livello di rete, BPFdoor non è soggetto alle regole del firewall e resta in "ascolto" di pacchetti dalle porte ICMP, UDP e TCP. Tramite il rilevamento di specifici pacchetti, dotati di valori ben precisi e, nel caso di UDP/TDP, di una password, la backdoor si attiva eseguendo uno dei comandi supportati, ad esempio attivando una Reverse Shell"."Questo metodo di filtraggio dei pacchetti si presta bene a operazioni furtive non solo per la mancanza di apertura della porta, ma anche per il basso sovraccarico della CPU richiesto per eseguire il filtraggio".Infatti, "gli attaccanti sfruttano vari router compromessi come tunnel VPN per eseguire BPFDoor tramite Virtual Private Servers (VPS). Gli utenti interessati rimangono all'oscuro dell'attacco e della sua persistenza nel sistema", mette in guardia la nostra esperta di cyber security.BPFdoor ha versioni per Linux e sistemi Solaris SPARC Systems, ma potrebbe mettere nel mirino BSD tramite

porting. L’analisi tecnica dell’attività che svolge la backdoor BPFDoor effettua una serie di operazioni appena è in esecuzione per garantirsi persistenza e passare indisturbato ai sistemi di controllo. Rosita Galiandro ci spiega quali: diventa memory resident e utilizza l’Anti-Forensic e l’evasione per nascondersi; carica uno sniffer Berkeley Packet Filter (BPF) che gli consente di controllare in modo efficiente il traffico e di lavorare con qualsiasi firewall in esecuzione localmente per vedere i pacchetti; alla ricezione di un pacchetto speciale, modifica il firewall locale per consentire all’indirizzo IP dell’attaccante di accedere a risorse come una spawned shell o di riconnettersi a una bind shell; le operazioni sono nascoste con il mascheramento dei processi per evitare il rilevamento.Inoltre, continua l’analista, “un metodo di detection riguarda il controllo di file insoliti presenti nella directory /dev/shm, come ad esempio /dev/shm/kdmtmpflush: Source: /bin/dash (PID: 20771) Chmod directory: /bin/chmod -> /bin/chmod 755 /dev/shm/kdmtmpflush”.Altra tecnica che si sta dimostrando efficace è quella di “eseguire dei controlli basati su delle robuste regole YARA che permettono di rilevare pattern di attacco già riscontrati in installazioni accertate di BPFDoor”.Infine, conclude Galiandro, ecco “una raccolta di hash e Indicatori di Compromissione (IOC): MD5: 4574b9a820d22c411d53aa2f1b56b045 SHA-1: e6fc57807585331b85cc957cb5c4767b9f5faf5b SHA-256: 07ecb1f2d9ffbd20a46cd36cd06b022db3cc8e45b1ecab62cd11f9ca7a26ab6d 144526d30ae747982079d5d340d1ff116a7963aba2e3ed589e7ebc297ba0c1b3 1925e3cd8a1b0bba0d297830636cdb9ebf002698c8fa71e0063581204f4e8345 4c5cf8f977fc7c368a8e095700a44be36c8332462c0b1e41bff03238b2bf2a2d c80bd1c4a796b4d3944a097e96f384c85687daeedcdcf05cc885c8c9b279b09c dc8346bf443b7b453f062740d8ae8d8d7ce879672810f4296158f90359dcae3a 591198c234416c6ccbcea6967963ca2ca0f17050be7eed1602198308d9127c78 599ae527f10ddb4625687748b7d3734ee51673b664f2e5d0346e64f85e185683 5b2a079690efb5f4e0944353dd883303ffd6bab4aad1f0c88b49a76ddcb28ee9 fd1b20ee5bd429046d3c04e9c675c41e9095bea70e0329bd32d7edd17ebaf68a f47de978da1dbfc5e0f195745e3368d3ceef034e964817c66ba01396a1953d72 5faab159397964e630c4156f8852bcc6ee46df1cdd8be2a8d3f3d8e5980f3bb3 76bf736b25d5c9aaf6a84edd4e615796fffc338a893b49c120c0b4941ce37925 93f4262fce8c6b4f8e239c35a0679fbbbb722141b95a5f2af53a2bcafe4edd1c 96e906128095dead57fdc9ce8688bb889166b67c9a1b8fdb93d7cff7f3836bb9 97a546c7d08ad34dfab74c9c8a96986c54768c592a8dae521ddcf612a84fb8cc c796fc66b655f6107eacbe78a37f0e8a2926f01fecebd9e68a66f0e261f91276 f8a5e735d6e79eb587954a371515a82a15883cf2eda9d7ddb8938b86e714ea27 fa0defdabd9fd43fe2ef1ec33574ea1af1290bd3d763fdb2bed443f2bd996d73″.@RIPRODUZIONE RISERVATA