Red Hot Cyber

https://www.redhotcyber.com/post/e-stata-lockbit-a-colpire-la-westpole-cosa-hanno-sottratto-oltre-a-bloccare-le-infrastrutture/

E’ stata LockBit a colpire la WestPole. Cosa Hanno Sottratto oltre a Bloccare le Infrastrutture?

Chiara Nardini : 18 Dicembre 2023 18:28

La misteriosa entità responsabile dell’attacco ransomware che ha colpito WestPole (https://www.redhotcyber.com/post/il-service-provider-italiano-westpole-e-rimasto-vittima-di-un-attacco-informatico-il-sito-web-risulta-offline/),

causando problemi estesi a PA Digitale (https://www.redhotcyber.com /post/attacco-a-westpole-pa-digitale-invia-a-rhc-un-comunicato-stampa-servizi-riattivati-gradualmente-e-nessuna-esfiltrazione-di-dati/) e numerose altre entità della Pubblica Amministrazione (https://www.redhotcyber.com/post/se-il-cloud-va-giu-va-giu-tutto-attacco-a-westpole-scopriamo-le-amministrazioni-colpite/), è finalmente stata identificata.

Da fonti vicino alla questione, ad attaccare WestPole è stata la Cyber gang LockBit, gang che i nostri lettori conoscono bene e che abbiamo intervistato circa un anno fa (https://www.redhotcyber.com/post/red-hot-cyber-intervista-lockbit-3-0/). Ricordiamo che LockBit ha messo a segno in Italia moltissimi attacchi informatici. Tra i più noti il colossale attacco all'ospedale ULSS6 di Padova (https://www.redhotcyber.com/post/i-dati-della-ulss6-euganea-di-padova-sono-online-pubblicati-da-lockbit/), ma anche la ASP Messina (https://www.redhotcyber.com/post/i-dati-della-asp-messina-sono-online-pubblicati-da-lockbit-scopriamo-cosa-contengono/), e i comuni di Villafranca (https://www.redhotcyber.com/post/il-comune-di-villafranca-colpito-da-lockbit-2-0/), Gonzaga (https://www.redhotcyber.com/post/il-comune-di-gonzaga-colpito-dal-ransomware-lockbit-2-0/) e Gorizia (https://www.redhotcyber.com/post/e-stato-lockbit-3-0-a-colpire-il-comune-di-gorizia-9gg-alla-pubblicazione-dei-dati/).

LockBit è a tutti gli effetti una azienda criminale, composta da centinaia di persone con compiti differenti. Da chi sviluppa il malware a chi ha la gestione delle infrastrutture e chi in effetti effettua il lavoro sporco. Si chiamano "affiliati"; ovvero dei criminali specializzati che utilizzano la tecnologia malware creata dalla gang e la lanciano verso le infrastrutture violate.

In sintesi si tratta di una “piramide” a tutti gli effetti di criminali informatici che collaborano assieme con skill differenti per arrivare ad un unico scopo: estorcere quanto più denaro possibile.

Quindi oltre al danno subito per il blocco dei servizi di WestPole, ora rimane da chiarire e e quali dati siano riusciti ad esfiltrare da Westpole e del danno derivante dalla pubblicazione e lo sfruttamento di tale dati nel darkweb.

Aggiornamento delle 21:15: Poco fa è arrivata una nota in redazione dell’Agenzia di Cybersicurezza Nazionale (ACN) che riporta ufficialmente che ha colpire la WestPole è stata la cybergang filorussa LockBit 3.0. L’Agenzia scrive quanto segue:

Roma, 18 Dicembre - L’Agenzia per la Cybersicurezza Nazionale da diversi giorni è in contatto con la Westpole S.p.A. e con PA Digitale S.p.A. per dare loro il massimo supporto al contenimento dei disservizi dovuti all’attacco informatico di tipo ransomware portato a segno dal gruppo di hacker russofono Lockbit 3.0.

L’attività svolta ha consentito il ripristino di tutti i servizi impattati, nonché il recupero dei dati oggetto dell’attacco per più di 700 dei soggetti pubblici nazionali e locali, legati alla catena di approvvigionamento di PA Digitale S.p.A.
Per le restanti Amministrazioni – sono circa 1.000 i soggetti pubblici legati contrattualmente a PA Digitale S.p.A. per l’erogazione di servizi gestionali di varia natura – resta l’esigenza di recuperare i dati risalenti ai 3 giorni precedenti l’attacco, avvenuto l’8 dicembre.

È inoltre da precisare, come confermato dalla stessa società PA Digitale, che l’attività svolta consente di scongiurare la paventata, mancata erogazione degli stipendi di dicembre e delle tredicesime a favore dei dipendenti di alcune Amministrazioni locali indirettamente impattate.

Infine, i rallentamenti dei servizi digitali che si sono registrati nella mattinata odierna sono dovuti alla congestione degli accessi simultanei e non rappresentano una conseguenza diretta dell’attacco informatico.

Agenzia per la cybersicurezza nazionale

L'ACN CONTINUA L'AZIONE DI SUPPORTO AI SOGGETTI IMPATTATI DAL RANSOMWARE LOCKBIT 3.0

L'agenzia per la cybersicurezza nazionale precisa che la maggior parte dei servizi erogati attraverso dalle realtà colpite è in via di riprino

nota per la stampa

Roma, 18 Dicembre - L'Agenzia per la Cybersicurezza Nazionale da diversi giorni è in contatto con la Westpole S.p.A. e con PA Digitale S.p.A. per dare loro il massimo supporto al contenimento dei disservizi dovuti all'attacco informatico di tipo ransomware portato a segno dal gruppo di hacker russofono Lockbit 3.0.

L'attività svolta ha consentito il ripristino di tutti i servizi impattati, nonché il recupero dei dati oggetto dell'attacco per più di 700 dei soggetti pubblici nazionali e locali, legati alla catena di approvvigionamento di PA Digitale S.p.A.

Per le restanti Amministrazioni – sono circa 1.000 i soggetti pubblici legati contrattualmente a PA Digitale S.p.A. per l'erogazione di servizi gestionali di varia natura – resta l'esigenza di recuperare i dati risalenti ai 3 giorni precedenti l'attacco, avvenuto l'8 dicembre.

È inoltre da precisare, come confermato dalla stessa società PA Digitale, che l'attività svolta consente di scongiurare la paventata, mancata erogazione degli stipendi di dicembre e delle tredicesime a favore dei dipendenti di alcune Amministrazioni locali indirettamente impattate.

Infine, i rallentamenti dei servizi digitali che si sono registrati nella mattinata odierna sono dovuti alla congestione degli accessi simultanei e non rappresentano una conseguenza diretta dell'attacco informatico.

Come nostra consuetudine, lasciamo sempre spazio ad una dichiarazione dell'azienda qualora voglia darci degli aggiornamenti su questa vicenda che saremo lieti di pubblicarla con uno specifico articolo dando risalto alla questione.

RHC monitorerà l'evoluzione della vicenda in modo da pubblicare ulteriori news sul blog, qualora ci fossero novità sostanziali. *Qualora ci siano persone informate sui fatti che volessero fornire informazioni in modo anonimo possono utilizzare la mail crittografata del whistleblower. (https://www.redhotcyber.com/whistleblower)*

Il ransomware LockBit

Il ransomware, è una tipologia di malware che viene inoculato all'interno di una organizzazione, per poter cifrare i dati e rendere indisponibili i sistemi. Una volta cifrati i dati, i criminali chiedono alla vittima il pagamento di un riscatto, da pagare in criptovalute, per poterli decifrare.

Qualora la vittima non voglia pagare il riscatto, i criminali procederanno con la doppia estorsione, ovvero la minaccia della pubblicazione di dati sensibili precedentemente esfiltrati dalle infrastrutture IT della vittima.

Per comprendere meglio il funzionamento delle organizzazioni criminali all'interno del business del ransomware as a service (RaaS), vi rimandiamo a questi articoli:

LockBit è una cyber gang criminale che adotta il modello **ransomware-as-a-service (RaaS),** anche se la sua struttura presenta variazioni che la differenziano da un tipico modello di affiliazione.

LockBit ransomware è un malware progettato per bloccare l'accesso degli utenti ai sistemi informatici in cambio di un pagamento di riscatto. Questo ransomware viene utilizzato per attacchi altamente mirati contro aziende e altre organizzazioni e gli "affiliati" di LockBit, hanno lasciato il segno minacciando le organizzazioni di tutto il mondo di ogni ordine e grado.

Si tratta del modello **ransomware-as-a-service (RaaS)** dove gli affiliati depositano del denaro per l'uso di attacchi personalizzati su commissione e traggono profitto da un quadro di affiliazione. I pagamenti del riscatto sono divisi tra il team di sviluppatori LockBit e gli affiliati attaccanti, che ricevono fino a ¾ dei fondi del riscatto.

E' considerato da molte autorità parte della famiglia di malware "LockerGoga & MegaCortex". Ciò significa semplicemente che condivide i comportamenti con queste forme consolidate di ransomware mirato ed ha il potere di auto-propagarsi una volta eseguito all'interno di una rete informatica.

LockBit è una cyber gang che restite da molto tempo nel mercato delle affiliazioni RaaS rinnovandosi costantemente. Ha iniziato le sue operazioni a settembre 2019 chiamandosi ABCD per poi cambiare il suo nome in Lockbit. Successivamente il marchio è stato rinominato in LockBit 2.0 apportando diverse novità e a giugno 2021, sono stati apportati dei cambiamenti introducendo la piattaforma Lockbit 3.0.

LockBit 3.0 introduce diverse novità (https://www.redhotcyber.com/post/lockbit-si-evolve-in-lockbit-3-0-aggiunto-un-bug-bounty-program/), come una piattaforma di bug-hunting relativa alle infrastrutture utilizzate dalla gang, l'acquisto di criptovaluta, una nuova sezione per gli affiliati e ulteriori modi per monetizzare che possono essere sintetizzate in:

- **Estensione del "countdown":** la vittima può pagare dei soldi per estendere il countdown per la pubblicazione dei dati;
- **Distruzione di tutte le informazioni:** la vittima può pagare per distruggere tutte le informazioni esfiltrate dalla sua organizzazione;
- **Download dei dati in qualsiasi momento:** la vittima può pagare per ottenere l'accesso al download esclusivo di tutti i dati esfiltrati dell'azienda.

Ovviamente il costo per ogni tipologia di "servizio" è differente e si può pagare in Bitcoin o in Monero.

Le vittime di LockBit in Italia

Lockbit, ha già colpito numerose organizzazioni sia pubbliche che private in Italia, in tutte e tre le varianti ransomware rilevate.

Facendo riferimento alle organizzazioni private delle quali abbiamo parlato su Red Hot Cyber troviamo:

- La clinica fisioterapica italiana Don Serafino (https://www.redhotcyber.com/post/la-clinica-fisioterapica-italiana-don-serafino-ronchi-colpita-da-lockbit-3-0/)
- Studio Barba (https://www.redhotcyber.com/post/litaliana-studio-barba-e-stata-colpita-dal-ransomware-lockbit-3-0/)
- MWD Digital (https://www.redhotcyber.com/post/litaliana-mwd-digital-colpita-dal-ransomware-lockbit-3-0/)
- Alpa (https://www.redhotcyber.com/post/litaliana-alpa-colpita-dal-ransomware-lockbit-3-0/)
- Multinazionale FAAC (https://www.redhotcyber.com/post/la-multinazionale-italiana-faac-e-la-prima-vittima-di-lockbit-3-0/)
- Datalit (https://www.redhotcyber.com/post/litaliana-datalit-e-rimasta-vittima-del-ransomware-lockbit-2-0/)
- Vainieri (https://www.redhotcyber.com/post/litaliana-vainieri-trasporti-e-stata-attaccata-da-lockbit/)
- Firbarcaiolo (https://www.redhotcyber.com/post/lazienda-italiana-firbarcarolo-colpita-da-lockbit-2-0/)
- Venegoni (https://www.redhotcyber.com/post/lockbit-attacca-i-salumi-italiani-il-salumificio-venegoni-colpito-dal-ransomware/)
- SG Service Sud (https://www.redhotcyber.com/post/lazienda-italiana-sg-

service-sud-colpita-da-lockbit-2-0/)
- Eredi Riva (https://www.redhotcyber.com/post/lazienda-italiana-erediriva-vittima-del-ransomware-lockbit-2-0/)
- Multimmobiliare Ticino (https://www.redhotcyber.com/post/lazienda-multimmobiliare-del-ticino-vittima-della-gang-lockbit-2-0/)
- Ingesw (https://www.redhotcyber.com/post/litaliana-ingesw-colpita-dal-ransomware-lockbit-2-0/)
- Jannone (https://www.redhotcyber.com/post/litaliana-jannone-colpita-dal-ransomware-lockbit-2-0/)
- Il giallo della Farmacia statuto (https://www.redhotcyber.com/post/lockbit-sbaglia-vittima/) (Errore di target)
- Rosa Group (https://www.redhotcyber.com/post/cyber-attacco-allitaliana-rosa-group-vittima-di-lockbit-2-0/)
- Progetto Edile (https://www.redhotcyber.com/post/litaliana-progetto-edile-e-stata-violata-da-lockbit-2-0/)
- Guzzanti (https://www.redhotcyber.com/post/litaliana-guazzini-vittima-di-lockbit-ransomware/)
- Crich (https://www.redhotcyber.com/post/litaliana-crich-vittima-del-ransomware-lockbit-2-0/)
- Confindustria Caserta (https://www.redhotcyber.com/post/confindustria-caserta-colpita-da-lockbit-2-0/)
- ISMEA (https://www.redhotcyber.com/post/litaliana-ismea-colpita-da-lockbit-2-0/)
- Montanari (https://www.redhotcyber.com/post/litaliana-montanari-colpita-dal-ransomware-lockbit-2-0/)
- Matteoli (https://www.redhotcyber.com/post/litaliana-matteoli-colpita-dal-ransomware-lockbit-2-0/)
- IDM (https://www.redhotcyber.com/post/attacco-informatico-all-italiana-idm-di-treviso-da-parte-di-lockbit-2-0/)
- Torello (https://www.redhotcyber.com/post/l-italiana-torello-e-tata-colpita-dal-ransomware-lockbit-2-0-d89/)
- Isnardi (https://www.redhotcyber.com/post/l-azienda-italiana-isnardi-colpita-da-lockbit-2-0-countdown-a-8-giorni/)
- La Ponte Marmi (https://www.redhotcyber.com/post/l-italiana-la-ponte-marmi-e-rimasta-vittima-del-ransomware-lockbit-2-0/)

- MCS (https://www.redhotcyber.com/post/l-italiana-mcs-morandi-violata-dal-ransomware-lockbit-2-0/)
- Delta Leading Broker (https://www.redhotcyber.com/post/delta-leading-broker-s-r-l-di-roma-violata-da-lockbit-2-0/)
- Mecfond (https://www.redhotcyber.com/post/l-italiana-mecfond-colpita-da-lockbit-2-0/)
- Cilento Spa (https://www.redhotcyber.com/post/l-italiana-cilento-spa-colpita-dal-ransowmare-lockbit/)
- Selini Group (https://www.redhotcyber.com/post/selini-group-colpita-dal-ransomware-lockbit/)
- Blowtherm (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-blowtherm-rivendicato-da-lockbit-tra-13gg-la-pubblicazione-dei-dati/)
- STIM (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-stim-group-14-gb-di-dati-nelle-mani-di-lockbit/)
- Gruppo Multimedica (https://www.redhotcyber.com/post/lockbit-colpisce-litaliana-multimedica-tra-3gg-la-pubblicazione-dei-dati/)
- Comacchio (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-comacchio-da-parte-di-lockbit-i-samples-sono-online/)
- OMS (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-oms-components-da-parte-di-lockbit/)
- Errebielle (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-errebielle-da-parte-di-lockbit-34gb-di-dati-online/)
- Tenosys (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-tecnosysitalia-da-parte-di-lockbit-tra-9gg-i-dati-online/)
- Lubrimetal (https://www.redhotcyber.com/post/attacco-informatico-allitaliana-lubrimetal-da-parte-di-lockbit-tra-14gg-i-dati-online/)
- Cassa Ragionieri (https://www.redhotcyber.com/post/il-mistero-dei-dati-dellitaliana-cassa-ragionieri/)
- Trudi (https://www.redhotcyber.com/post/attacco-informatico-allazienda-italiana-dei-peluche-trudi-rivendicato-dalla-cybergang-lockbit/)
- Gruppo Beltrame (https://www.redhotcyber.com/post/lazienda-siderurgica-italiana-gruppo-beltrame-e-stata-vittima-di-un-attacco-informatico/)
- Cantina Tollo (https://www.redhotcyber.com/post/attacco-informatico-a-cantina-tollo-da-parte-di-lockbit-un-encomio-per-la-comunicazione/)

- Belletti (https://www.redhotcyber.com/post/litaliana-belletti-ascensori-vittima-del-ransomware-lockbit-3-0/)
- Your Private Italy (https://www.redhotcyber.com/post/i-viaggi-di-lusso-in-italia-sono-stati-colpiti-dal-ransomware-lockbit/)

Invece per quanto concerne le azienda pubbliche abbiamo:

- ASP Messina (https://www.redhotcyber.com/post/i-dati-della-asp-messina-sono-online-pubblicati-da-lockbit-scopriamo-cosa-contengono/)
- Comune di Villafranca (https://www.redhotcyber.com/post/il-comune-di-villafranca-colpito-da-lockbit-2-0/)
- Agenzia Nazionale Turismo (https://www.redhotcyber.com/post/lagenzia-italiana-del-turismo-colpita-dal-ransomware-lockbit-2-0/)
- ULSS6 di Padova (https://www.redhotcyber.com/post/i-dati-della-ulss6-euganea-di-padova-sono-online-pubblicati-da-lockbit/)
- Comune di Gonzaga (https://www.redhotcyber.com/post/il-comune-di-gonzaga-colpito-dal-ransomware-lockbit-2-0/)
- Comune di Gorizia (https://www.redhotcyber.com/post/e-stato-lockbit-3-0-a-colpire-il-comune-di-gorizia-9gg-alla-pubblicazione-dei-dati/)

Chiara Nardini

Esperta di Cyber Threat intelligence e di cybersecurity awareness, blogger per passione e ricercatrice di sicurezza informatica. Crede che si possa combattere il cybercrime solo conoscendo le minacce informatiche attraverso una costante attività di "lesson learned" e di divulgazione. Analista di punta per quello che concerne gli incidenti di sicurezza informatica del comparto Italia.