Dr.WEB®
dal 1992

Filtraggio della posta tramite gli antivirus Dr.Web

Doctor Web, 2018

La posta è la più grande fonte di diffusione di trojan e spam

Di regola, i trojan arrivano sul computer a seguito di qualche azione dell'utente sui supporti rimovibili o nelle email.

Dalle richieste inviate al supporto tecnico Doctor Web da parte degli utenti che sono rimasti vittime di un trojan cryptolocker della famiglia Encoder, i cui computer erano protetti da un altro antivirus (diverso da Dr.Web):

Ho caricato dalla posta un file — un archivio, poi tutti i file word ed excel e inoltre le immagini sono state criptate. L'estensione era 1TXT.

I file sono criptati in formato 1txt. È stato aperto nella posta un messaggio sospetto ed è iniziata la criptazione.

10/10 circa alle 11 è arrivata un'email nel servizio Yandex, l'ho aperta, ed è avvenuta la criptazione.

Oggi dopo l'apertura di un file dalla posta, tutti i file di formato DOC, XLS si sono trasformati in file di formato VAULT.

Buongiorno! un dipendente ha ricevuto un'email da un'organizzazione con un archivio contrassegnato come urgente, lui l'ha aperto, c'era un file .js, dopodiché ha preso il virus VAULT che ha cifrato tutti i file. Aiutate a disinfettare e decriptare i dati.

È sufficiente proteggere le postazioni per prevenire queste infezioni?

No.

Buongiorno. È arrivato un messaggio via email con un allegato "18.06.18.Gz". L'abbiamo aperto. Si è rivelato essere un virus. Il disco sul computer è suddiviso in due dischi logici. Sul disco "C" molti file e cartelle sono in colore blue. Sul disco "D" no.

Da una richiesta fatta al supporto tecnico Doctor Web

L'analisi del report dell'antivirus (file che è ritrovabile sull'indirizzo %userprofile%\desktop\drweb.log) ha mostrato la seguente situazione:

1. Il cryptolocker era conosciuto dall'antivirus installato sul computer.
2. La cosa più interessante è come è stato lanciato questo trojan:

threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Avvio da parte dell'utente, l'antivirus identifica il trojan e visualizza una notifica.
threat: DPH:Trojan.Encoder.9 ==> send user blocked alert	Un altro avvio!

E queste non sono tutte le ragione perché organizzare il filtraggio della posta sul server.
I flussi di posta che passano attraverso la postazione e il server non coincidono.

- L'utente (o un programma che lui ha accettato di installare senza conoscerne le funzionalità) può inviare e ricevere email:
  - direttamente sui server di posta Internet (tramite il protocollo SMTP), se nella rete è aperta la porta 25;
  - sui servizi di posta, come ad esempio mail.ru/gmail.com tramite i protocolli pop3/imap4.
- L'utente (o un programma che lui ha accettato di installare senza conoscerne le funzionalità) può inviare email attraverso canali privati, e il server non potrà verificarle.
- Il server (o programmi su di esso installati) può creare email inviate su molteplici indirizzi e notificare i destinatari e mittenti su vari eventi.

Tutto ciò che entra all'azienda ed esce dall'azienda via email deve essere controllato PRIMA DELL'ARRIVO sui computer e dispositivi degli utenti.

Nei casi sopra descritti, l'utente semplicemente non doveva ricevere l'email infetta.

Solo l'antivirus per server Dr.Web è in grado di:

- eseguire sul server il filtraggio antivirus e antispam sia della posta esterna (in entrata e in uscita) che di quella interna — sia su un server controllato dall'azienda che su un server affittato;
- filtrare la posta sul gateway, cioè isolando il server stesso da Internet;
- controllare i messaggi di posta archiviati sul server cercando le minacce precedentemente non identificate;
- mettere la posta filtrata in quarantena e/o archivio per eventuali casi di reclamo per filtraggio non corretto;
- proteggere tutte le vie di ricezione e invio della posta tra i mail server di filiali aziendali e la comunicazione con i servizi di posta esterni (Mail.ru, Gmail ecc.);
- recuperare i messaggi inavvertitamente cancellati dai dipendenti dalle caselle di posta e inoltre condurre indagini relative a fughe di informazioni.

L'antivirus per il filtraggio della posta risparmia banda

La presenza di virus e spam nel traffico email porta ai seguenti problemi:

- diminuzione delle prestazioni del server di posta che è occupato dall'elaborazione del traffico parassita;
- aumento del carico sulla rete interna, riduzione delle prestazioni di risorse di rete e della capacità dei canali;
- crash del server in seguito alla ricezione di una "mail bomb";
- fermi macchina.

I virus e i messaggi di spam nel traffico email portano a un aumento dei requisiti per l'hardware dei server di posta e, di conseguenza, alla necessità di potenziare l'hardware o acquistare nuove macchine.

L'antivirus per il filtraggio della posta risparmia banda grazie alla possibilità di limitare l'accettazione di diversi allegati e analizzare le email parzialmente accettate.

La posta deve essere filtrata in modo complesso

L'utilizzo di un antivirus senza antispam:

- consente agli hacker di condurre attacchi di spam e phishing ai server di posta aziendali e ai client di posta dei dipendenti; in alcuni casi, il fatto di ricezione di un'email basta per infettare la macchina o per compromettere la sua operatività;
- porta a un aumento del pagamento per il traffico;
- porta a un aumento del carico improduttivo-parassitario sui server di posta;
- riduce la produttività di tutti i dipendenti aziendali che ricevono email e sono costretti a ripulire le caselle di posta dallo spam.

L'antispam Dr.Web funziona sulla base di regole e rimuove efficacemente dai messaggi di posta persino i programmi malevoli non conosciuti dall'antivirus.

Antispam Dr.Web:

- viene fornito come parte di un'unica soluzione (e non come prodotto separato);
- viene installato sullo stesso server insieme al prodotto di filtraggio dei virus

Questo semplifica l'amministrazione e assicura un costo totale più basso rispetto all'acquisto di soluzioni concorrenti.

Vantaggi dell'antispam Dr.Web:

- Non richiede addestramento e inizia a funzionare efficacemente dal momento dell'installazione — a differenza degli antispam dei concorrenti costruiti sull'uso dell'algoritmo bayesiano.
- Il verdetto "è spam" / "non è spam" non dipende dalla lingua del messaggio.
- Permette di impostare diverse azioni per diverse categorie di spam.
- Utilizza le proprie black list e white list grazie a cui non sarà possibile che aziende possano essere compromesse tramite l'inserimento ostile sulle liste di indirizzi indesiderati.
- Ha pochi falsi positivi.
- Richiede l'aggiornamento non più di una volta al giorno, e quindi risparmia banda — le tecnologie uniche di individuazione della posta indesiderata sono basate su diverse migliaia di regole che liberano dalla necessità di scaricare aggiornamenti frequenti e ingombranti.

I prodotti Dr.Web per il filtraggio della posta

Dr.Web Mail Security Suite

Unix: ▪ Sendmail ▪ Postfix ▪ Exim ▪ QMail ▪ Communigate Pro ▪ Courier ▪ ZMailer	MS Exchange	IBM Lotus Domino	Kerio (Windows, Linux, macOS)

Funzionalità di gestione:

- Gestione attraverso un'interfaccia web
- **Gestione attraverso la console di Dr.Web Enterprise Security Suite.** L'integrazione nel sistema di Dr.Web Enterprise Security Suite consente di assicurare la gestione del sistema di protezione antivirus "da un punto" con la massima comodità per l'amministratore di sistema.
- Gestione attraverso una utility della riga di comando.

UNA CHIAVE per qualsiasi prodotto di Dr.Web Mail Security Suite.

Licenze

Per numero di indirizzi	Licenza per server (fino a 3000 indirizzi)	Licenza illimitata per qualsiasi numero di server

Tipi di licenze

- Antivirus
- Antivirus + Antispam
- Antivirus + Antispam + SMTP Proxy
- Antivirus + SMTP Proxy
- Antispam + SMTP Proxy

! La massima qualità del filtraggio viene raggiunta con l'utilizzo del gateway email **Dr.Web SMTP proxy** — un filtro che processa i messaggi prima che arrivino sul server di posta.
Non è necessario ricevere email malevole se il server è collocato su Internet — l'attaccante stesso lo troverà (per esempio tramite il metodo di selezione degli indirizzi).

L'utilizzo di Dr.Web SMTP proxy:

- aumenta significativamente la sicurezza generale della rete;
- migliora considerevolmente la qualità del filtraggio grazie all'assenza di restrizioni imposte dai server di posta;
- riduce il carico sui server di posta interni e sulle postazioni;
- aumenta la stabilità del funzionamento del sistema di verifica email nel suo complesso.

L'utilizzo di una zona demilitarizzata e di strumenti di verifica del traffico email a livello del gateway SMTP aumenta il livello di protezione.

Anche il server di posta deve essere protetto

Un server di posta è semplicemente un servizio collocato su un server di file normale. Pertanto, oltre alla protezione del servizio di posta, è necessario utilizzare anche la protezione del server stesso e dei canali di comunicazione con esso.

- Un server di posta può essere infettato sia dall'interno che dall'esterno.
- Solo la protezione del server stesso e dei canali di comunicazione con esso (sia di quelli interni che di quelli esterni) può prevenire che esso diventi una fonte di infezione nel caso in cui nella rete si infiltrerà un virus sconosciuto.
- Qualsiasi server ha bisogno di protezione — sia un server che si trova all'interno dei locali aziendali che uno esterno affittato

Conseguenze tecniche dell'infezione di un server	Conseguenze commerciali dell'infezione di un server
▪ Diminuzione delle prestazioni del server o la sua totale inoperatività (fermi macchina). ▪ Aumento del carico sulla rete interna, riduzione delle prestazioni di risorse di rete e della capacità dei canali. ▪ Rifiuto del servizio — l'azienda sarà disconnessa da Internet o inserita su una black list per l'invio di spam se è diventata parte di una botnet. ▪ Aumento dei costi dell'infrastruttura informatica (pagamento del traffico parassita / aumento del numero di server / costi di archiviazione della posta, incluso lo spam).	▪ Interruzione della continuità dei: – ritardi nello svolgimento dei doveri d'ufficio da parte dei dipendenti; – ritardi nell'adempimento degli obblighi dell'azienda nei confronti dei clienti; – blocco della ricezione della posta da parte dei partner a causa di inserimento dell'azienda sulle black list; ▪ deterioramento della reputazione agli occhi dei consumatori e dei partner; ▪ un'opinione che l'azienda sia tecnologicamente arretrata; ▪ i clienti vanno via — rifiuto dell'utilizzo dei servizi aziendali.

L'antivirus per la protezione del server risparmia banda

- La posta verrà filtrata una volta sul server e non diverse volte su ciascuna postazione — questo migliorerà le loro prestazioni, e i dipendenti si lamenteranno meno frequentemente di rallentamenti dei PC dell'ufficio.
- Grazie all'utilizzo dell'antispam in Dr.Web Mail Security Suite, diminuisce il carico improduttivo-parassitario sul server di posta (la quantità di spam in un traffico email arriva fino al 98%, e il filtraggio avrà un effetto favorevole sul funzionamento del server di posta). Ritardi nella consegna della posta e messaggi persi saranno un fenomeno raro!

La soluzione giusta: Dr.Web Server Security Suite + Dr.Web Mail Security Suite

- Le tecnologie di protezione preventiva incluse in Dr.Web Server Security Suite per Windows proteggeranno persino dalle minacce e dagli exploit non ancora conosciuti, dai tentativi di comunicazione di oggetti malevoli gestiti in remoto con un server dei malintenzionati (gestione di botnet e spionaggio). Senza dipendere dai database dei virus e dalla frequenza di aggiornamento.
- Il modulo di auto-protezione Dr.Web SelfPROtect, che non ha pari nel mercato, non consentirà di disattivare l'antivirus Dr.Web e di ottenere il controllo del server — il filtraggio della posta non verrà fermato, e la copia di backup del server sarà protetta da tentativi di criptazione o distruzione.
- **Avvio prima ancora che sia finito il caricamento del sistema operativo!** Il funzionamento al livello più basso possibile del sistema operativo!

L'azienda Doctor Web

Doctor Web — fornitore russo di software antivirus di protezione delle informazioni sotto il marchio Dr.Web. I prodotti Dr.Web vengono sviluppati fin dal 1992. L'azienda è un attore chiave nel mercato russo dei software studiati per soddisfare un'esigenza essenziale delle aziende — quella di sicurezza delle informazioni.

Doctor Web è stata la prima azienda ad offrire sul mercato russo il modello innovativo di utilizzo dell'antivirus come servizio e fino ad oggi rimane leader indiscusso del mercato russo dei servizi internet di sicurezza per i fornitori di servizi informatici.

Si fidano di Dr.Web

Grazie alla presenza nell'organico Doctor Web di esperti di varie problematiche di sicurezza delle informazioni, l'azienda può tenere conto, al livello massimo, delle particolarità di lavoro di aziende di varie dimensioni e con diversi profili di attività e offrire ai clienti la migliore scelta di prodotti di qualità con un costo totale minimo.

Tra i consumatori dei prodotti Dr.Web ci sono utenti privati da tutte le regioni del mondo e grandi imprese russe, piccole organizzazioni e aziende della spina dorsale. La geografia degli utenti di Dr.Web testimonia l'alta fiducia nel prodotto creato da programmatori russi di talento.

Ecco solo alcuni clienti di Dr.Web: https://customers.drweb.com.

Perché Dr.Web?

Tutti i diritti sulle tecnologie Dr.Web appartengono all'azienda Doctor Web. L'azienda è uno dei pochi fornitori di antivirus al mondo che possiedono le proprie tecnologie uniche di rilevamento e neutralizzazione di programmi malevoli; ha il proprio laboratorio antivirus, un servizio di monitoraggio dei virus globale e un servizio di supporto tecnico.

2-12A, 3rd street Yamskogo polya,
Moscow, Russia, 125040
Tel.: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97

www.drweb.com