KASIM 2021
plus

Redington

Veritas ile Veri Yönetimi ve Güvenliği

Redington Türkiye, distribütörlüğünü üstlendiği Santa Clara, ABD merkezli teknoloji şirketi Veritas için YouTube kanalında ve farklı dijital platformlarda yayımladığı Türkçe içerikli kısa videolarla, şirketin veri güvenliği alanındaki liderliğine vurgu yapıyor. Veritas, 2021 yılında da Gartner Magic Quadrant'ta yer alarak liderliğini 16'ncı kez tescillemiş bulunuyor.

VİDEOLARA ULAŞMAK İÇİN İLGİLİ KAREKODU OKUTUNUZ.

“Gelin, bilişim ekosisteminin birleştirici gücü Redington Türkiye aracılığıyla Veritas Ransomware Protection ile tanışın, fidye yazılımlara karşı güvende olun.”

Siber Saldırılara Karşı Önleminizi Alın

- ✔ NetBackup sunucusu ve/veya yedekleme cihazına fiziksel erişimi kısıtlayın.
- ✔ NetBackup sunucularını bilinen güvenlik kurallarına göre sıkılaştırın.
- ✔ Sadece gerekli olan iletişim protokollerini kullanın.
- ✔ İstemcilerin güvenliğini sağlayın.
- ✔ Güvenlik yamalarını ve uyarılarını dikkate alın.
- ✔ Felaket kurtarma planınızı test edin.
- ✔ Veri kaybına karşı geri dönüş süreçlerini oluşturun.
- ✔ Güvenlik denetimleri, incelemeleri ve eğitimlerini sık sık gerçekleştirin.
- ✔ Yedekleme sunucusu için kritik sistem koruması sağlayın.

Enterprise Vault Suite Nedir ve Ne Yapar?

- ✔ Enterprise Vault, portföyünün tamamını tek bir lisansta birleştiren, dijital uyumluluk için geniş ve kapsamlı bir çözüm sunan eşsiz bir sistem.
- ✔ Arşivlenen içeriği esnek şekilde saklar.
- ✔ Sıkıştırma ve tek kopya saklama ile depolama maliyetini azaltır.
- ✔ Hızlı geri dönüş için içeriği dizinler.
- ✔ Politika tanımlamak ve uygulamak kolaydır.
- ✔ Kimlik doğrulama güvenlik kontrolleri kullanır.
- ✔ Arşivlenen içeriğin HTML kopyasını oluşturarak gelecekteki erişilebilirliğini güvence altına alır.

“Gelin, Redington aracılığıyla Veritas Enterprise Vault Suite ile tanışın, şirketinizin veri yönetimi ve arşivleme çözümlerinde fark yaratın.”

Fidye Yazılımlara Karşı Korunuyor musunuz?

BÜYÜYEN TEHDİT

Fidye yazılımlar hızla hem kurumların hem son kullanıcıların karşılaştığı en tehlikeli siber tehditlerden biri haline geldi ve tüm dünyada her yıl neredeyse milyar dolarlara ulaşan kayıplara yol açıyor. Yedekleme konusunda bütünleşik bir yaklaşımın benimsenmesi verilerinizi her nerede olursa olsun korumanıza olanak sağlıyor.

91%

Fidye yazılım saldırılarında yaygın olarak kullanılan oltalama e-postalarıyla başlayan siber atakların oranı.[1]

71%

Fidye yazılım saldırısına uğrayan kurumların altyapılarına bulaşma oranı .[2]

$10k

Fidyeler, izlenemeyen bitcoin ile ödenen, kullanıcı başına 10.000$'a kadar çıkan tutarlarda olabiliyor.[3]

GLOBAL FİDYE YAZILIM ZARARLARI

Global fidye yazılımı ticari zararlarının

2021'e kadar yıllık 20 milyar dolar'ı bulması

bekleniyor.

Fidye yazılım saldırıları tüm işletim sistemleri için bir tehdittir:

iOS
Apple iOs™

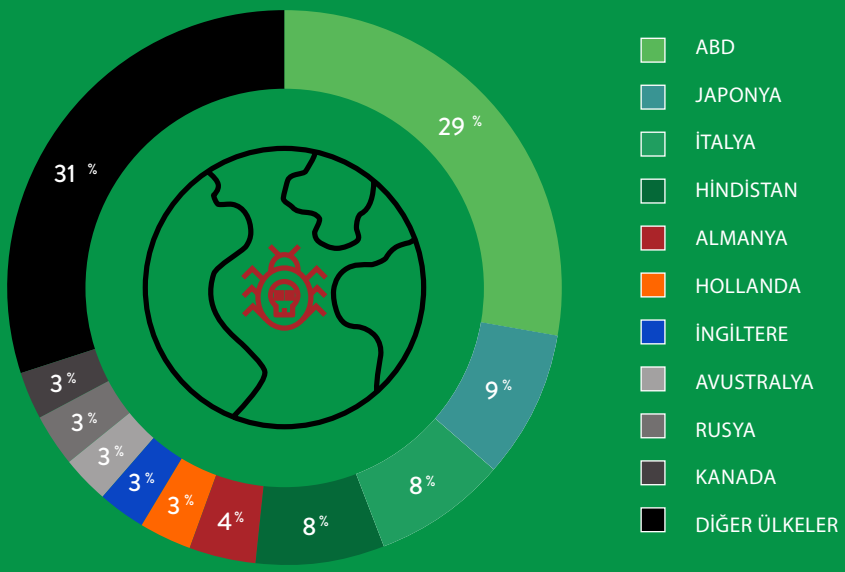
Windows
Microsoft Windows™

Android™

Linux™

Ülkelere göre fidye yazılım etkisi.

ABD, diğer ülkelerin hepsinden daha çok fidye yazılım saldırılarından etkileniyor. ABD'nin daha çok hedeflenmesinin nedeni, saldırıya maruz kalanların %64'ünün fidyeyi ödediğinin raporlanması olabilir.



FİDYE YAZILIM SALDIRILARI HER ZAMANKİNDEN DAHA SIK GERÇEKLEŞİYOR.

2 dakikada bir

2016 başı

40 saniyede bir

2016 sonu

14 saniyede bir

2019 sonu

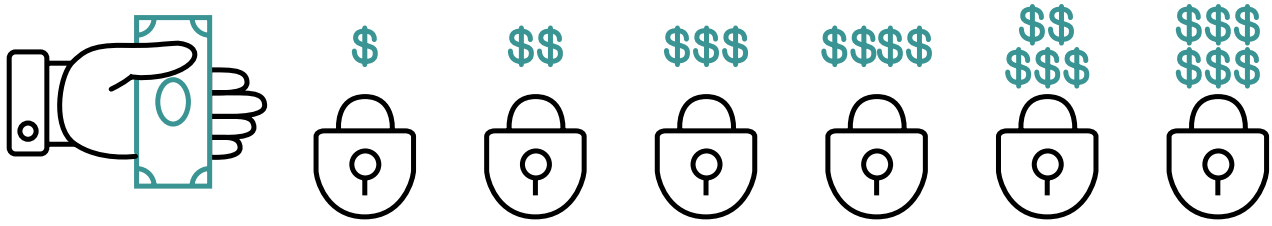
11 saniyede bir

2021

ASIL SORU: FİDYE ÖDEMELİ MİSİNİZ?

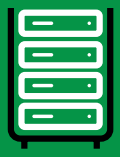
Fidye yazılım saldırısına uğrayanların fidye ödemenin her zaman işe YARAMADIĞINI bilmesi gerekiyor. Bazı saldırganlar ilk ödemeyi aldıktan sonra fidye talep etmeye devam edecektir. Şifre çözme süreci, iyi uygulanmazsa dosyalara zarar verebilir. Ve, daha da kötüsü:

Fidye ödeyenlerin %20'si şifre çözme anahtarı alamıyor.



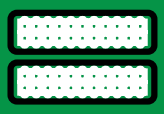
FİDYE YAZILIM SALDIRILARINA KARŞI HAZIRLIKLI OLUN

NetBackup sunucusu ve/veya yedekleme cihazına fiziksel erişimi kısıtlayın.



NetBackup sunucularını bilinen güvenlik kurallarına göre sıkılaştırın.

Sadece gerekli olan iletişim protokollerini kullanın.



İstemcileri güvenliğini sağlayın.

Güvenlik yamalarını ve uyarılarını dikkate alın.

Felaket kurtarma planınızı test edin.

Veri kaybına karşı geri dönüş süreçlerini oluşturun.

Güvenlik denetimleri, incelemeleri ve eğitimleri sık sık gerçekleştirin.

Yedekleme sunucusu için kritik sistem koruması sağlayın.

KILAVUZU EDİNİN

Fidye yazılım raporumuzu okuyun ve bu tehditlere karşı kurumunuzu nasıl koruyabileceğinizi öğrenin.

1. Siber saldırıların %91'i oltalama e-postaları ile başlar.
2. Bilinmesi Gereken Fidye Yazılım İstatistikleri 2018
3. Intermedia Ransomware 101: İşletmenizin fidye yazılım saldırıları hakkında bilmesi gerekenler.
4. Global fidye yazılım maliyetinin 2021'e kadar 20 milyar dolara ulaşması öngörülüyor.
5. ABD fidye yazılımından en çok etkilenen ülke olmayı sürdürüyor.
6. Kötü niyetli yazılım için neden fidye ödememelisiniz ?

VERITAS™