## باج‌افزار

مجرمان سایبری در حملات ویرانگر باج‌افزاری از تکنیک‌های مختلف جهت تشویق کاربران به دانلود و اجرای پیوست‌های مخرب استفاده می‌کنند.

## فیشینگ

بیش از نیمی از ایمیل‌های ارسالی، مربوط به حملات فیشینگ هستند. در این حملات هویت افراد و برندهای بنام مورد اعتماد قربانی، جعل می‌شود. سپس از کاربر درخواست می‌شود که بر روی یک لینک کلیک کرده و وارد یک سرویس تحت وب شود.

## فیشینگ هدفمند

مهاجم در فیشینگ هدفمند که یک نوع فیشینگ اختصاصی است، هویت یک شرکت یا فرد خاص را جعل می‌کند. پیام‌های فیشینگ معمولی برای هزاران کاربر ارسال می‌شوند اما فیشینگ هدفمند به صورت اختصاصی و با تمرکز بر روی یک شرکت یا شخص خاص طراحی می‌شود.

## نفوذهای اطلاعاتی

ایمیل یکی از روش‌های پر طرفدار مهاجمان برای نفوذ به سیستم‌های هدف است. ممکن است اطلاعات حساس به صورت تصادفی و ناخواسته یا عمداً توسط کارمندان افشا شوند. اگرچه منشأ بسیاری از رخنه‌های اطلاعاتی، پایگاه‌های داده هستند ولی امکان استفاده از ایمیل برای سرقت اسرار سازمان‌ها و سایر اطلاعات حساس وجود دارد.

## اسپم

ممکن است حتی پیام‌های اسپم ظاهراً بی‌خطر هم حاوی تهدیدات ایمیلی بسیار جدی باشند. حجم بالای پیام‌های اسپم نیز بر روی بهره‌وری تأثیر دارد و وقت کارمندان را هم می‌گیرد.

## کی‌لاگر

کی‌لاگرها اطلاعات تایپ شده توسط کاربر را سرقت و برای مهاجمان ارسال می‌کنند. به این ترتیب مهاجم به اعتبارنامه‌های کاربری و همچنین اطلاعات زمینه‌ای قابل استفاده در فیشینگ هدفمند دسترسی پیدا می‌کند. ممکن است کی‌لاگرها در فایل‌های ظاهراً سالم مخفی شوند و در هنگام باز شدن فایل توسط کاربر به صورت مخفیانه نصب شوند.

## جعل هویت دامنه

مهاجمان معمولاً در حملات فیشینگ هدفمند از جعل دامنه استفاده می‌کنند تا قربانی را متقاعد کنند که پیام ارسالی توسط یک شرکت خاص فرستاده شده است.