می‌خواهی بدانی **مهاجمان چطور از ابزارها و سایت‌هایی که لینک اجرایی/شارکد یا Shortcut/EXE می‌سازند سوءاستفاده می‌کنند** تا به قربانیان آسیب بزنند. این سؤال کاملاً امنیتی و آموزشی است.  
در ادامه، مراحل و شیوه‌ سوءاستفاده مهاجمین را شماره‌وار همراه توضیح مختصر آورده‌ام.

**مراحل سوءاستفاده مهاجمان از ابزارهای آنلاین برای ساخت شارکد/Shortcut/EXE**

1. **مبهم‌سازی (Obfuscation) یا رمزگذاری بدافزار**
   * مهاجم ابتدا کد مخرب (مثلاً بک‌دور، کی‌لاگر، استخراج رمزعبور و ...) را با ابزارهای Obfuscate یا Cryptor مبهم می‌کند تا آنتی‌ویروس‌ها سخت‌تر شناسایی کنند.
2. **تبدیل به فایل اجرایی با ابزار سازنده EXE یا Binder**
   * کد مخرب را توسط PyInstaller یا ابزار مخصوص دیگر به فایل اجرایی (exe) یا اسکریپت با فرمت دیگر مثل scr, com, bat تبدیل می‌کند.
   * گاهی با File Binder چند فایل اجرایی/عکس/صوت/... را یکی می‌کند تا فایل نهایی ظاهر سالمی داشته باشد.
3. **ساخت Shortcut (شورتکات) یا فایل اتوران با آیکون فریبنده**
   * برای جلب نظر کاربران، ابزار آنلاین یا آفلاین انتخاب می‌شود که به فایل اجرایی/Shortcut یک آیکون جذاب می‌دهد، مثلاً عکس شبکه اجتماعی، اپلیکیشن محبوب یا عکس شخصی.
   * نام فایل نیز شبیه فایل‌های رایج انتخاب می‌شود (مثلاً Instagram Manager.exe یا بازی جدید.exe)
4. **استفاده از ابزارهای Steganography برای پنهان‌سازی فایل**
   * ممکن است فایل اجرایی را داخل یک عکس (JPG, PNG)، آهنگ (MP3)، PDF و ... جاسازی کنند تا فریب‌دهنده‌تر باشد.
   * ابزارهایی مانند OpenStego، Steghide و ... برای این مرحله استفاده می‌شوند.
5. **آپلود فایل آلوده روی سایت‌های اشتراک‌گذاری و تولید لینک مستقیم قابل دسترس**
   * فایل (EXE یا Shortcut) را روی سرورهای ابری (Google Drive، Dropbox، Mediafire، Mega…) آپلود می‌کنند تا یک لینک کوتاه و کم‌ریسک بسازند.
6. **ساخت یا کوتاه‌کردن لینک مخرب (URL Shortener)**
   * از سرویس‌های کوتاه‌کننده مانند bit.ly یا cutt.ly یا tinyurl برای مخفی‌کردن URL اصلی و گمراه‌کردن کاربر بهره می‌برند.
7. **انتشار لینک از طریق مهندسی اجتماعی**
   * مهاجم لینک را برای قربانیان از راه‌های مختلف می‌فرستد:
     + ایمیل فیشینگ (Phishing Email)
     + پیامک، واتساپ، تلگرام، اینستاگرام و سایر شبکه‌های اجتماعی
     + کامنت‌گذاری در سایت‌ها و گروه‌های گفت‌وگو
   * پیام همراه لینک معمولاً ترغیب‌کننده یا هیجان‌برانگیز (جایزه، ادعای نیاز به کمک فوری، فایل جذاب، عکس لو رفته و ...) است.
8. **کلیک، دانلود و اجرای فایل توسط قربانی**
   * با کلیک روی فایل، قربانی فایل مخرب را اجرا می‌کند و دستورات یا بدافزار بدون اطلاع اجرا می‌شود.
   * بدافزار ممکن است اطلاعات را بدزدد، به ایمیل/سرور مهاجم بفرستد، یوزرنیم و پسورد را ذخیره کند یا حتی دسترسی کامل به کامپیوتر بگیرد.
9. **حذف خودکار یا مخفی‌سازی بدافزار**
   * بعضی بدافزارها بعد از اجرا، خود را حذف یا مخفی می‌کنند تا ردیابی نشوند.
10. **مانیتورینگ و کنترل از راه دور (در صورت کارکرد Backdoor)**
    * در بعضی حملات، ارتباط با سرور فرمان (C&C) برقرار می‌شود تا کنترل بیشتر داشته باشند.

**نکات و توصیه امنیتی:**

* هرگز روی فایل اجرایی و مخصوصاً فایل با فرمت نامعمول که از منبع نامطمئن دانلود کردی کلیک نکن.
* فایل‌هایی که پسوند دوبل دارند (مثلاً .jpg.exe یا .pdf.exe) یا آیکون گول‌زننده دارند، غالباً مخرب‌اند.
* اگر پیامی غیرعادی با لینک کوتاه شدیدی ترغیب به دانلود کرد، به آن مشکوک باش.
* آنتی‌ویروس را به‌روزرسانی و شناسایی بلادرنگ فعال نگه دار.
* استفاده‌ی نادرست از این دانش غیرقانونی است—تنها برای افزایش امنیت شخصی و آموزشی از آن استفاده کن.