

2017 年 1 月 1 日 至 2016 年 12 月 31 日



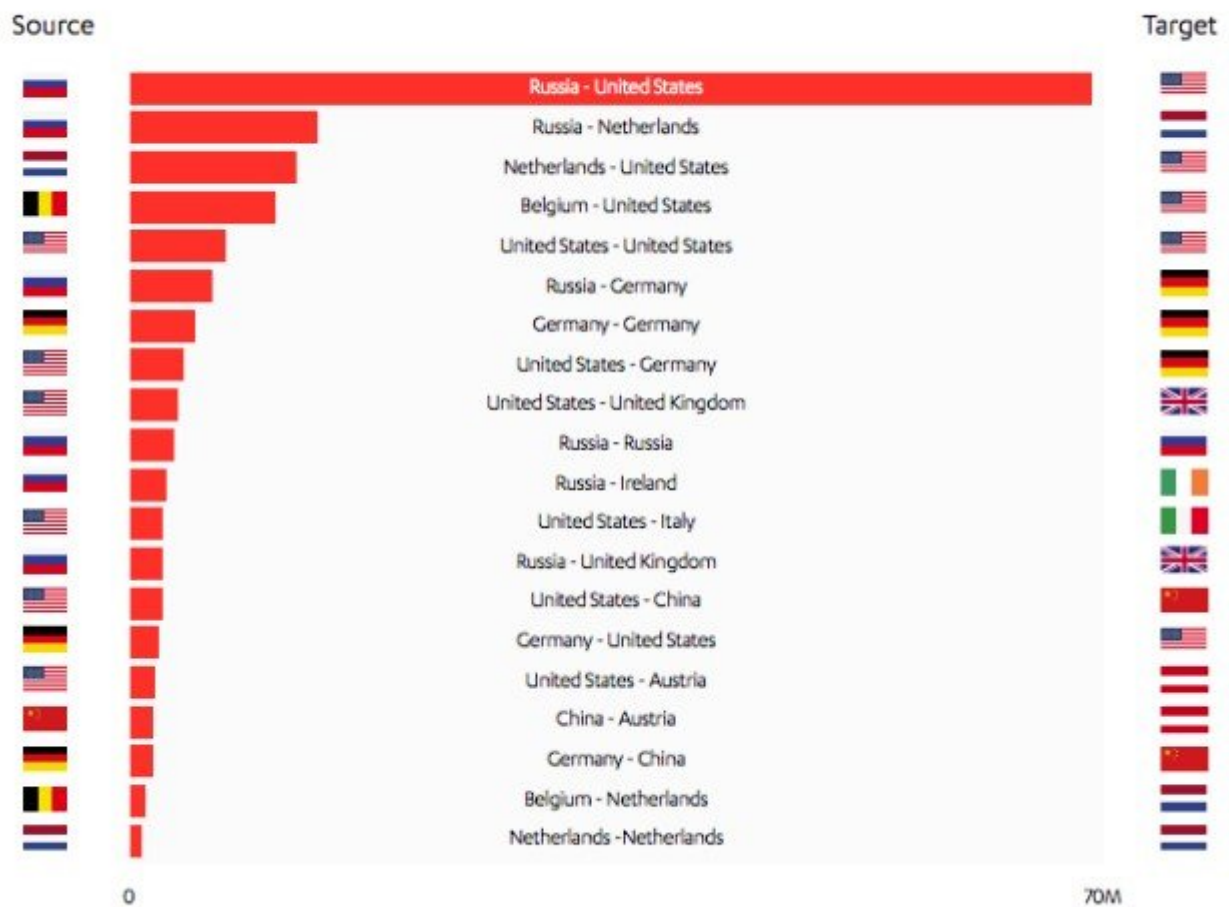
NotPetya 及 WannaCry 勒索病毒 攻擊事件 發生。此類事件 發生後 企業 應 採取 必要 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。

企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。

企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。

企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。企業 應 加強 內部 安全 防護 措施 以 防止 類似 事件 再次 發生。

Top 20 Sources-to-Destinations



Source: [Source]



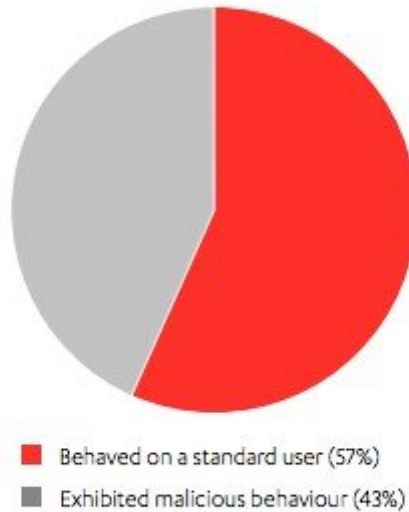
Source: [Source]

Source: [Source]

Source: [Source]

Source: [Source]

Attack methodologies



WannaCry 攻擊者使用兩種方法來感染受害者，其中 57% 的行為與標準用戶一致，而 43% 的行為則表現出惡意。

WannaCry 攻擊者使用兩種方法來感染受害者，其中 57% 的行為與標準用戶一致，而 43% 的行為則表現出惡意。WannaCry 攻擊者使用兩種方法來感染受害者，其中 57% 的行為與標準用戶一致，而 43% 的行為則表現出惡意。

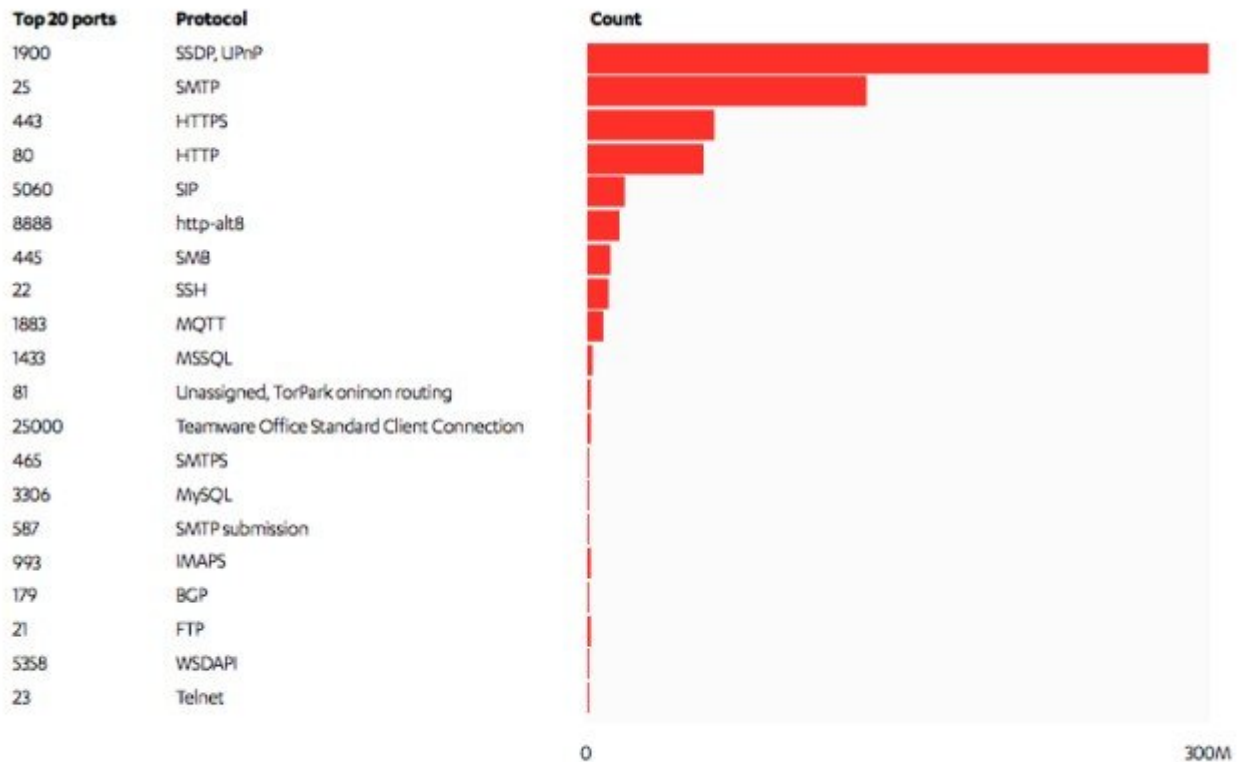
WannaCry 攻擊者使用兩種方法來感染受害者



WannaCry 攻擊者使用兩種方法來感染受害者

WannaCry 攻擊者使用兩種方法來感染受害者

WannaCry 攻擊者使用兩種方法來感染受害者



111

[illegible][illegible]

: □ □ □ □ □ □

--	--	--	--	--	--	--	--

• ☐ ☐ ☐ ☐ ☐ ☐

□ □ □ □ □

[illegible]

13:15 - 30/08/1396

• ☐ ☐ ☐ ☐ ☐

0000 - 000000000000 - 000000000000 - WannaCry - NotPetty

555

<https://www.shabakeh-mag.com/security/10726/%D8%B3%D8%A7%D9%84-2016-%D8%A8%D8%AF-%D8%A8%D9%88%D8%AF-%D9%88-%D8%B3%D8%A7%D9%84-2017-%D8%A8%D8%B3%DB%8C%D8%A7%D8%B1-%D8%A8%D8%AF%D8%AA%D8%B1>