Water Hole Attack 期中報告

Water hole attack, 中譯為水坑攻擊。

什麼是水坑攻擊?

水坑攻擊是一種安全漏洞，攻擊者透過感染該組成員已知訪問的網站來危害特定的最終用戶組。其目標是感染目標用戶的電腦並訪問目標工作場所的網絡。

目標受害者可以是個人、組織或是群體。通常是大型企業、民間組織、宗教團體以及政府機構的員工。雖說水坑攻擊不常見，但它們構成了相當大的威脅，它們很難被檢測到，通常透過安全意識較低的員工、業務合作夥伴或是供應商來針對高度安全的組織。它們可能破壞多層安全性，因此它們具有極大的破壞性。

水坑攻擊如何運作?

此攻擊涉及由攻擊者發起的一系列事件，以獲取對受害者的訪問權。但攻擊者不會直接針對受害者。攻擊者識別目標受害者使用並熟悉的網站或服務，一般而言，目標站點的安全性相對較低，訪問率較高，並且受到受害者的歡迎。攻擊者破壞目標站點並將惡意程式注入站點，通常採用 JS 或是 HTML 的形式。受害者訪問感染站點時，觸發惡

意程式，並開始攻擊感染受害者的電腦。漏洞利用鏈可能已經存在取眾所周知的漏洞利用鏈，也可能是攻擊者自行創建的新漏洞。一旦在受害者的電腦上觸發有效載荷，攻擊者便可以訪問網路上的其他資產並使用該電腦發起樞軸攻擊已達成其他目的。目標是收集受害者的信息抑或是將受害者的電腦作為殭屍網路，嘗試利用或攻擊受害者網路中的其他電腦。

其他類似水坑攻擊的安全漏洞

供應鏈攻擊：在供應鏈攻擊和水坑攻擊中，攻擊者都會破壞第三方服務以感染其他系統，但是在供應鏈攻擊中，受到攻擊的目標通常是目標購買的產品。而不是像水坑攻擊中受攻擊的中立網站。

如何防止水坑攻擊

1. 不允許個人使用公司資源 2.不要向信任第三方站點

3.掃描並監控互聯網流量

水坑攻擊的例子

- 2016 年，總部位於加拿大的民航組織(ICAO)傳播了感染聯合國網路的惡意軟件。
- 2017 年，烏克蘭政府網站遭到入侵以傳播惡意軟件。

期末作業

```
query_str = {"size": 0,"aggregations": {"result": {"terms": {"field":
"winlog.user.name.keyword","order": [{"_count": "desc"}]}}}}
res = es.search(index="winlogbeat", body=query_str)
result = res["aggregations"]["result"]["buckets"]
#print(result)

event_pd = pd.DataFrame(result, columns=["key", "doc_count"])
#print(event_pd)
event_pd.plot(x="key", y="doc_count", kind="bar");
plt.xlabel('name')
plt.ylabel('Log Count')
plt.title('user.name')
```