臺灣大學計資中心網路組
北區學術資訊安全維運中心

資訊安全分析報告

Mudrop 惡意程式簡介與防制

臺灣大學計資中心網路組
北區學術資訊安全維運中心

摘要

MALWARE-CNC Win.Trojan.Mudrop variant outbound connection 是北區 ASOC 近期偵測到數量最多的惡意連線行為。本文將說明 Mudrop 此惡意程式的背景、行為與危害以及北區 ASOC 是如何進行檢測此惡意程式行為，並說明如何移除此惡意程式的方法。

Mudrop 惡意程式簡介

Mudrop 此惡意程式以 C++開發而成，並發展出數量龐大的變種，Mudrop 惡意程式變種數量估計為百種以上，而每一種變種所造成的危害程度、執行動作、產生檔案與存放路徑皆不同，但主要目的皆為竊取使用者的機敏資料，或取得主機的控制權。

Mudrop 只會對 Windows 作業系統造成影響，而具有高度威脅性的變種皆為利用 Windows 作業系統之重大漏洞進行散播、竊取主機資訊、竄改主機檔案，甚至能夠完全控制主機。

Mudrop 惡意程式主要被附加於網頁、軟體安裝檔或執行檔之中，經由受害者開啟檔案或檔案後感染主機，有些 Mudrop 變種會藉由垃圾信傳播，或感染一部主機後，使該主機經由系統漏洞擴散至鄰近網路的其他主機。

Mudrop 惡意程式的特徵

Mudrop 惡意程式具有以下的特徵

1. 自行連接到特定 IP 位址進行更新或下載更多惡意程式。
2. 依附在正常處理程序(如 explorer 或 svchost 等)中執行，並嘗試取得最高控制權限。
3. 藉由刪除特定 dll 檔案，或強制停止程式運作反制防毒軟體及偵測工具。
4. 修改登錄檔與瀏覽器，不斷嘗試連結外部主機並復原惡意程式。
5. 更改本機上的 hosts 檔案，讓使用者連向惡意網域。

如何防範 Mudrop 惡意程式

Mudrop 惡意程式受害主機皆為下列情況遭受感染

1. 使用來源不明的免費或破解軟體。
2. 未安裝防毒軟體或未察覺防毒軟體已過期。
3. 作業系統未定期更新。
4. 缺乏對郵件社交工程攻擊的認識。

為達成有效防範 Mudrop 惡意程式，應落實以下使用行為

1. 不隨意下載可疑檔案，下載後也應確實執行掃描後再開啟。
2. 確保防毒軟體的可用性，並定期執行系統掃描。
3. 確實開啟作業系統的自動更新。
4. 不隨意開啟不明信件之附件，或從通訊軟體上開啟不明連結。

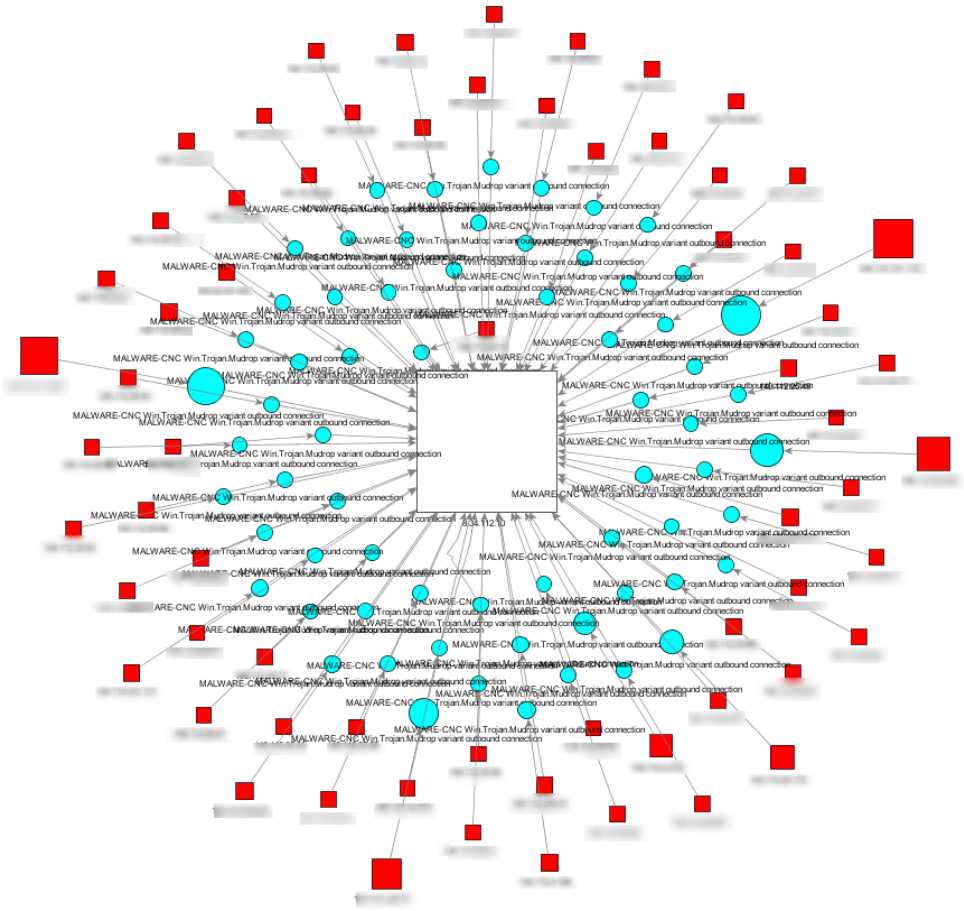
如何檢測及移除 Mudrop 惡意程式

一旦主機遭 Mudrop 惡意程式感染後，Mudrop 惡意程式會開始嘗試進行更新、資料回傳、下載更多惡意程式等等行為，此時便會對外部主機產生特定通訊行為，圖一與圖二為北區 ASOC 實際偵測到受感染主機對外通訊而觸發的事件資訊。

可以發現 Mudrop 惡意程式所進行資料傳輸的目標皆為特定的 C&C server(圖中為 8.34.112.10)，此資訊能夠加入到惡意網域名單中並加以封鎖，使 Mudrop 惡意程式無法回傳資訊或進行更新，藉此降低 Mudrop 惡意程式可能造成的危害。

結束時間	名稱	攻擊者位址	目標位址
8 八月 2014 22:59:39 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:59:38 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:58:05 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:58:02 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:56:50 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:56:47 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:56:39 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:56:09 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:30:37 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:29:35 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:29:31 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:17:45 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:17:28 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 22:17:25 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:59:38 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:59:37 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:30:36 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:29:35 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:29:31 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:25:37 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:25:27 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10
8 八月 2014 21:17:43 CST	MALWARE-CNC Win.Trojan.Mudrop varia...		8.34.112.10

圖一　Mudrop 惡意程式觸發之事件列表

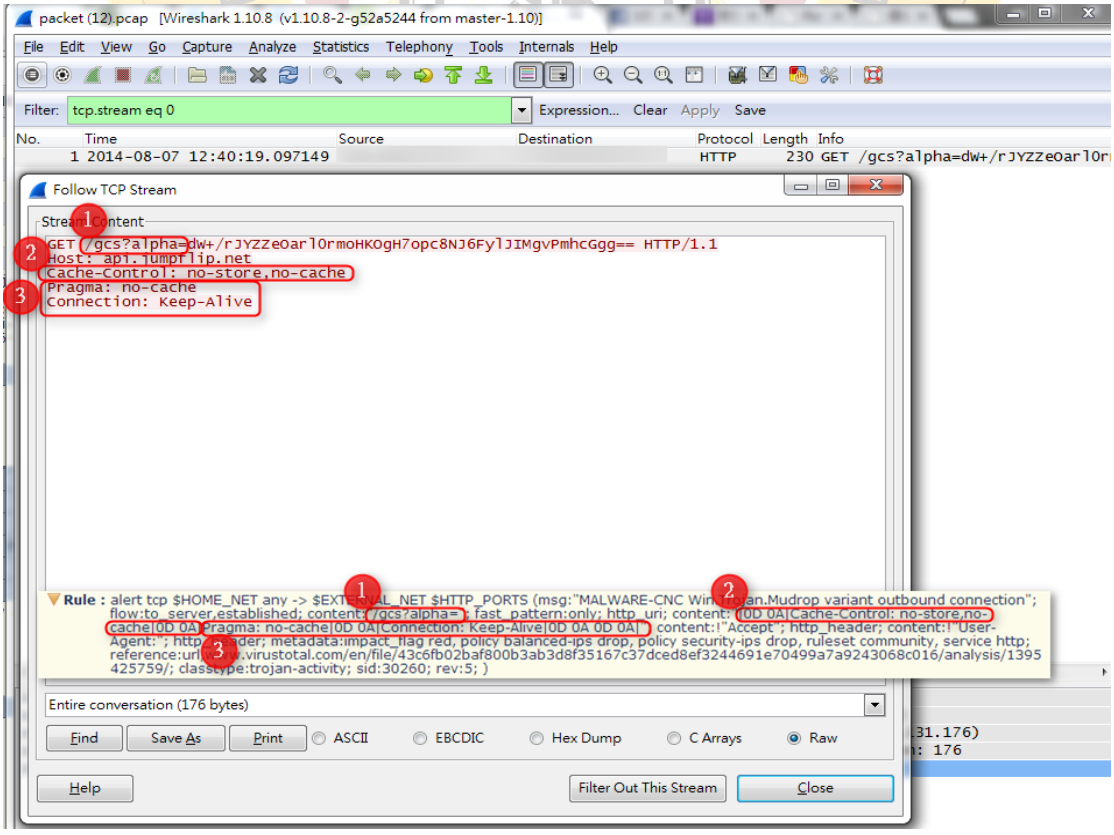


圖二　Mudrop 事件圖，受感染主機(紅色方點)與 8.34.112.10(白色方點)通訊

北區 ASOC 針對 Mudrop 惡意程式，已於 IPS 中佈署偵測規則，下列文字敘述為佈署於 IPS 中的規則之一。

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS
(msg:"MALWARE-CNC Win.Trojan.Mudrop variant outbound connection";
flow:to_server,established;
content:"/gcs?alpha="; fast_pattern:only; http_uri;
content:"|0D 0A|Cache-Control: no-store,no-cache|0D 0A|Pragma: no-cache|0D 0A|Connection: Keep-Alive|0D 0A 0D 0A|";
content:!"Accept"; http_header;
content:!"User-Agent:"; http_header;
metadata:impact_flag red, policy balanced-ips drop, policy security-ips drop, ruleset community, service http;
reference:url,www.virustotal.com/en/file/43c6fb02baf800b3ab3d8f35167c37dced8ef3244691e70499a7a9243068c016/analysis/1395425759/;
classtype:trojan-activity;
sid:30260;
rev:5;)

由下圖的封包內容可確認，受感染主機透過 http 協定格式嘗試與外部主機通訊，並因封包特徵符合 IPS 偵測規則而產生事件告警資訊。



但在受感染的主機上來看，除了 Mudrop 惡意程式會主動對外進行資料的傳輸以外，由於變種數量非常龐大，且因為每個變種在主機上所產生的行為與檔案皆不相同，不易使用共同的判斷方法來對主機進行檢測。

檢測 Mudrop 惡意程式建議的方式為使用防毒軟體來進行全系統掃描來進行檢測，並利用防毒軟體本身的刪除功能進行惡意的移除。需要注意的是，Mudrop 惡意程式與大部分難纏的惡意軟體一樣，附加在檔案中時非常容易刪除，一旦經啟動後就無法輕易的利用防毒程式進行完整刪除，甚至經防毒軟體刪除後仍不斷重複被偵測到，此時則需要搜尋並使用其他對應的工具軟體刪除。

Mudrop 惡意程式具有更新的特性，只要新的偵測工具一出現，Mudrop 惡意程式透過更新的反制工具，使偵測工具無法執行。具高威脅性的 Mudrop 惡意程式變種的特徵之一，利用阻擋特定程序名稱、特定程式碼、以及刪除特定 dll 檔案的方式來反制防毒軟體或偵測工具。

Mudrop 惡意程式並不會主動感染系統映像檔或還原檔，若無法有效的刪除 Mudrop 惡意程式，受感染的主機可以利用系統還原的方式將設備回復到原先的正常狀態，並在還原之後再利用防毒軟體進行全系統掃描，以防止具有 Mudrop 的惡意檔案再次被開啟，造成重複感染。

參考資料

http://www.securitystronghold.com/gates/trojan-dropper.win32.mudrop.html