2019
第三季電子郵件安全趨勢

ASRC

Spam Mail
Virus Mail
Malicious Mail

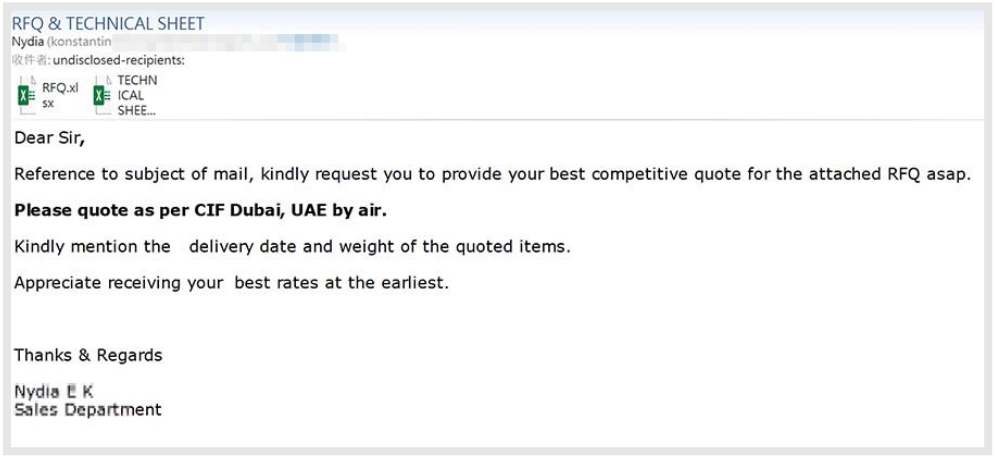
Oct 2019 released.

根據 ASRC 研究中心 (Asia Spam-message Research Center) 的觀察，2019 年第三季不論是垃圾郵件或攻擊郵件，在數量上都有明顯的上升。釣魚郵件以及經過變化後的附件檔釣魚郵件，是所有攻擊郵件中最需要被留意的；其次是漏洞利用的攻擊，今年於電子郵件附檔中最常見的漏洞利用當屬 CVE20144114、CVE20180802 及其後續的衍生變形攻擊。CVE20144114 數量在第三季大增，主要被攻擊的目標有電子、食品及醫療等相關產業；最後則是映像檔病毒以及域名詐騙，這類的威脅雖不直接，但也是資安防禦工事上需要特別留意的。

漏洞利用頻率創高峰，相較今年一月成長超過30倍

CVE20144114 漏洞利用頻率，一季比一季高，9 月份來到了高峰。相較於今年一月份的頻率成長了 30 倍以上，且並非平均分布，而是集中在某些企業單位才出現特大量攻擊，被攻擊目標企業包括電子、食品及醫療等相關產業。其次需要特別留意的是 CVE20180802 漏洞利用，雖然沒有明顯的突發性成長，但是每一個月都有穩定的攻擊數量。

以第三季的樣本來說，最常見的就是夾帶 .xlsx 的附件，少量為 .docx 的附件，附件檔名多半帶有 Swift Copy、Scan、RFQ、Request、Remittance、Quotation、Purchase、Invoice、PO、Payment、Order...等關鍵字。


RFQ & TECHNICAL SHEET
Nydia (konstantin
收件者: undisclosed-recipients:
RFQ.xlsx
TECHNICAL SHEE...
Dear Sir,
Reference to subject of mail, kindly request you to provide your best competitive quote for the attached RFQ asap.
Please quote as per CIF Dubai, UAE by air.
Kindly mention the delivery date and weight of the quoted items.
Appreciate receiving your best rates at the earliest.
Thanks & Regards
Nydia E K
Sales Department

CVE20180802 漏洞利用攻擊樣本

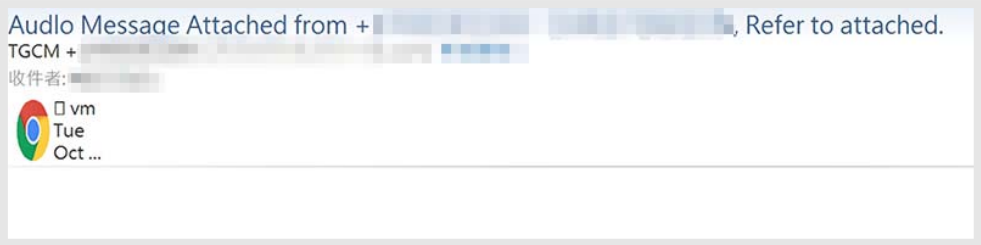
漏洞利用攻擊防禦建議

建議企業單位除了採用合適的郵件過濾軟體之外，也應進行內部軟體資安盤點，將已知的漏洞修補皆予補上，防範後續的N-Day攻擊。

附件檔釣魚郵件利用瀏覽器與收信軟體特性，發展更多更複雜的攻擊組合

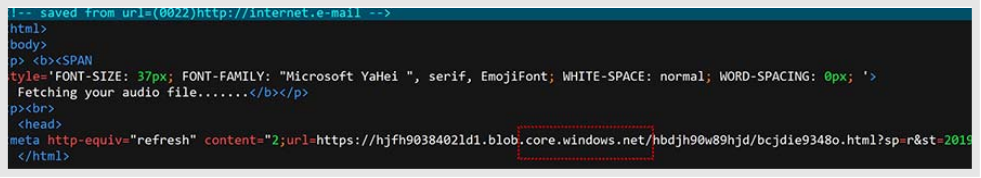
附件檔釣魚郵件近幾年的數量持續佔有一定比例，主要是在一封釣魚郵件中，不直接放入釣魚網站的連結，取而代之的是放入一個帶有釣魚網站連結及其他網頁程式碼的 HTML 附件檔案。與一般釣魚郵件目的相同，是為了騙取收件者的機敏資料，但附件檔釣魚郵件會利用瀏覽器與收信軟體的某些特性，做出更多複雜的攻擊組合。

比方某些收信軟體會將.html 的附件檔內容直接展開在郵件內；.html 由瀏覽器打開後，可以不再受到收信軟體的限制，而能執行 JavaScript、頁面跳轉...等複雜與風險俱高的動作。釣魚的網址，可以躲過郵件掃描；透過合法網站的寄宿，還可繞過瀏覽器釣魚黑名單的封鎖。



附件檔釣魚郵件樣本

附件檔釣魚郵件其中的.html檔展開後，會從本機的HTML頁面，跳轉至真實的釣魚網站



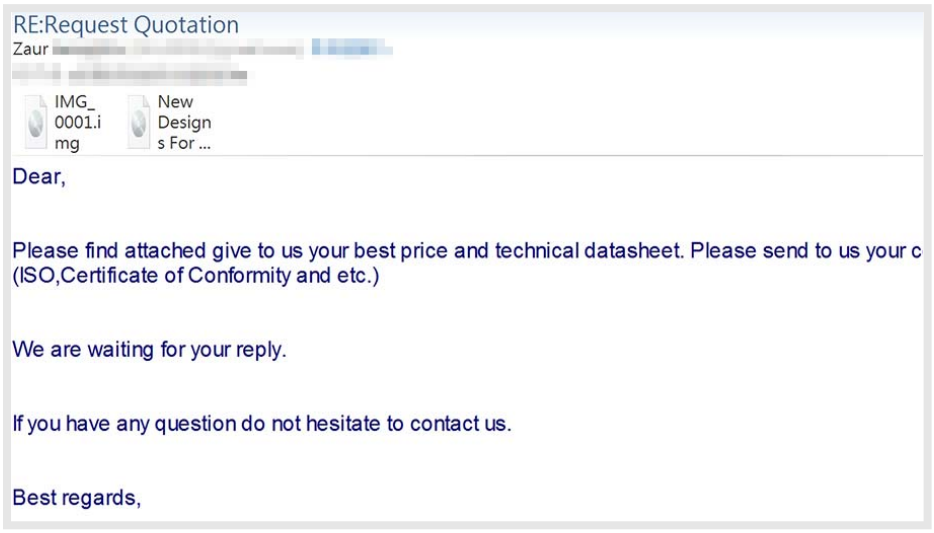
附件檔釣魚郵件其中的.html檔，帶有寄宿於合法網站的釣魚頁面

附件檔釣魚郵件防禦建議

面對釣魚威脅，最好從人員的認知著手！
在任何地方，要求輸入自身的機敏資料時，特別不是由**自身主動為了存取服務進行認證**；當**被動受要求為了做甚麼事，而需要認證**時，一定要與原要求單位以其他管道進行確認。

映像檔有其特定用途，多數防禦機制忽略檢查因而淪為攻擊者工具

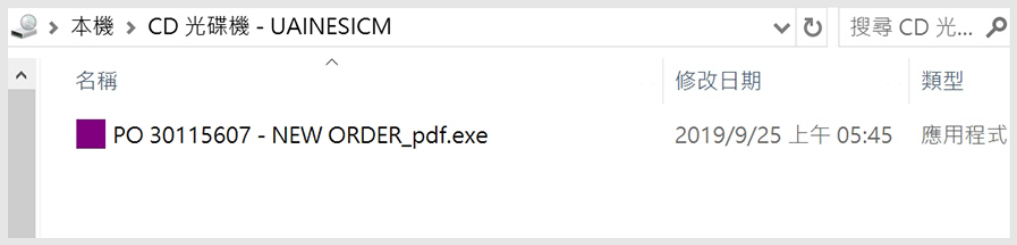
第三季出現了不少夾帶藏有病毒的 UDF 映像檔附件。UDF 映像檔原是用於光碟備份、燒錄前暫存、準備或大量複製光碟之用，其副檔名多為 .iso、.img… 等。由於這類映像檔有其特定用途，部分的防毒牆、防火牆、終端防毒軟體會忽略這類格式檔案的大小限制或其內容的檢查，因此攻擊者就利用此缺口，將病毒嵌在標準合法的 UDF 映像檔格式內，以躲過各種檢查關卡。



帶有 .img 附件的映象檔病毒郵件

帶有 .iso 附件的中文內容映象檔病毒郵件

病毒被嵌在標準的 UDF 映像檔格式內，這個映像檔其實可以被掛載於虛擬光碟機；也能夠被一般的解壓縮軟體打開而執行內容，且 Microsoft Windows 預設以檔案總管作為此類映像檔的開啟關聯程式，收件者十分容易因為誤執行而中毒。



標準的 UDF 映像檔可以被掛載於虛擬光碟機，掛載後，裡面的可執行檔就是病毒的本體

映像檔病毒防禦建議

設定顯示被隱藏的副檔名；而管理者也要意識到映像檔也可以被運用於攻擊，並作為資安策略的考量。

域名詐騙再進化，提供線上購買續費，竊取機敏資訊運用於後續攻擊

域名詐騙郵件由來已久，過去常見的域名詐騙，多半單純利用純社交工程的手段，以域名已過期、將遭佔用，誘騙收件者回覆後，進一步進行互動與詐騙。這類詐騙郵件提及的域名，有時是受害單位沒註冊過但非常相似的域名，因此若受害者思慮不周，直接查詢郵件中提及的域名，可能信以為真落入攻擊者的圈套。


BRAND & DOMAIN NAME REGISTRATION

Tim [redacted] 2018/7/23 下午 06

(Please forward this letter to your President or CEO. Thank you)

Dear Sir or Madam,

We are the Department of Asian Domain & Brand Registration Service in China. We have a formal affair to confirm with you. Our Registration Department received an application from PRCV GROUP who applies to register [redacted] as their Brand Name and some top-level domain names through our organization. We found the main body of domain names they apply to register is same as your company. We inform you of this matter because it involves your intellectual property.

Now we are handling this registration. Please let me know whether or not you authorized them to register these names. If you authorize them, I will formally pass through their registration; if not, please let us know as soon as possible in order to handle this issue better. Looking forward to your reply. Have a nice day!

Best Regards

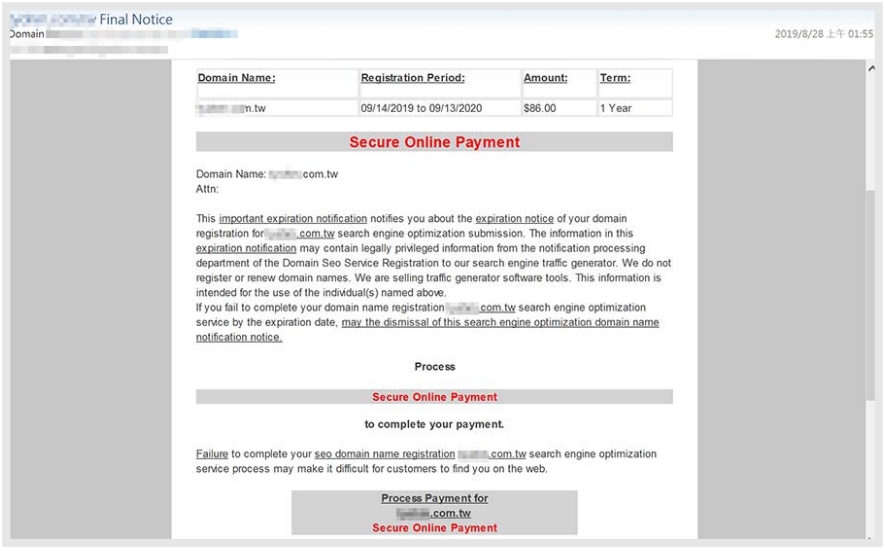
Tim Huang
Head [redacted]
Tel: [redacted] 6512-0084
No. [redacted], Hefei , China

過去常見的域名詐騙樣本

在第三季出現不少進化版的域名詐騙。大致與過去的域名詐騙內容差不多，但是多了可以線上購買或續用域名的連結，可供受害人點擊。當受害人信以為真並點擊後，則會連到釣魚網站，並要受害人填妥詳細的機敏資料，攻擊者得手後便可做後續的身分冒用或入侵受害者所用的各種網路服務。

域名詐騙防禦建議

域名的註冊、管理，應有固定的管理人員與監控流程；若真的需要購買、續用域名，應主動尋訪合適的合作廠商協助，而非照著可疑郵件的指示進行。


Final Notice

2019/8/28 上午 01:55

Domain Name:	Registration Period:	Amount:	Term:
[redacted]n.tw	09/14/2019 to 09/13/2020	$86.00	1 Year

Secure Online Payment

Domain Name: [redacted].com.tw
Attn:

This important expiration notification notifies you about the expiration notice of your domain registration for [redacted].com.tw search engine optimization submission. The information in this expiration notification may contain legally privileged information from the notification processing department of the Domain Seo Service Registration to our search engine traffic generator. We do not register or renew domain names. We are selling traffic generator software tools. This information is intended for the use of the individual(s) named above.
If you fail to complete your domain name registration [redacted].com.tw search engine optimization service by the expiration date, may the dismissal of this search engine optimization domain name notification notice.

Process

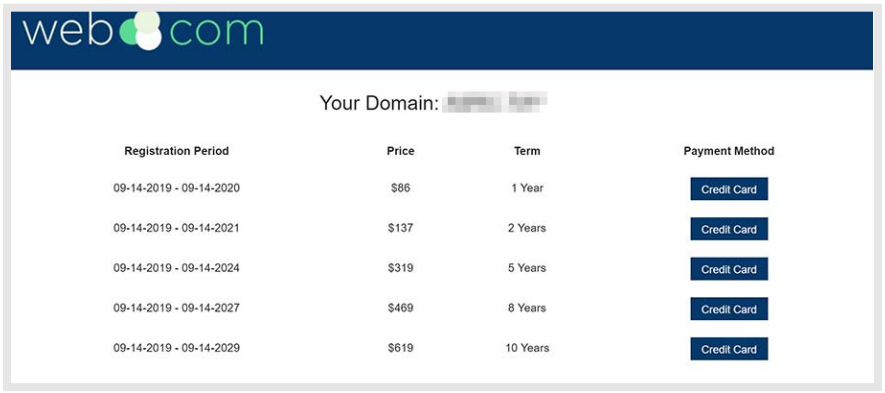
Secure Online Payment

to complete your payment.

Failure to complete your seo domain name registration [redacted].com.tw search engine optimization service process may make it difficult for customers to find you on the web.

Process Payment for [redacted].com.tw
Secure Online Payment

◀ 域名詐騙郵件多了可以線上購買或續用域名的連結


webcom

Your Domain: [redacted]

Registration Period	Price	Term	Payment Method
09-14-2019 - 09-14-2020	$86	1 Year	Credit Card
09-14-2019 - 09-14-2021	$137	2 Years	Credit Card
09-14-2019 - 09-14-2024	$319	5 Years	Credit Card
09-14-2019 - 09-14-2027	$469	8 Years	Credit Card
09-14-2019 - 09-14-2029	$619	10 Years	Credit Card

◀ 看似真正的域名購買釣魚網站


Secure Transaction

Billing Information	
First Name:	
Last Name:	
Company Name:	
Country:	United States
Address:	
City:	
State/Province:	- Select State -
Zip/Postal Code:	
Phone Number:	
Fax Number:	
Email Address:	
Website Address:	

Continue

◀ 主要用以騙取受害者機敏資料，以進行後續身分冒用等攻擊

結語

曾經暴露在外的電子郵件信箱，經網路爬蟲收錄之後，天天都被迫收到許多廣告與攻擊郵件，幾乎難以有洗白的一天，這種情況持續了多年，雖然大家對於郵件位址不隨意暴露在公開的網頁開始有了安全意識，但暴露在外的文件內帶有電子郵件信箱的情況仍然不少，這其實是值得留意的問題。

此外，各種資安事件之間，慢慢的都不是獨立存在了，只要曾經發生過入侵，或是個人、企業單位的資料曾經遭到外洩，接踵而來的就是一次一次 BEC 攻擊，或是收不完的網路釣魚郵件。電子郵件的攻擊手段不斷地推陳出新，雖然少有橫空出世般新穎攻擊手法出現，但透過「利用」、「連接」、「交錯」將舊有攻擊手段緩慢持續的演進，卻是從未停止過的！

關於ASRC 垃圾訊息研究中心

ASRC 垃圾訊息研究中心 (Asia Spam-message Research Center)，長期與中華數位科技合作，致力於全球垃圾郵件、惡意郵件、網路攻擊事件等相關研究事宜，並運用相關數據統計、調查、趨勢分析、學術研究、跨業交流、研討活動..等方式，促成產官學界共同致力於淨化網際網路之電子郵件使用環境。

更多資訊請參考 www.asrc-global.com

ASRC垃圾訊息研究中心