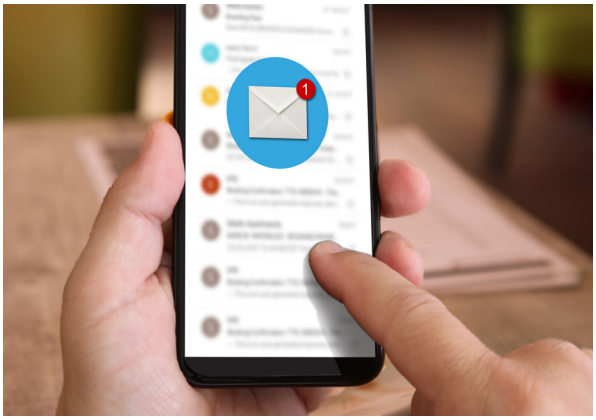
Dridex Malspam Spoofs Messaging from Popular Accounting Software Company

Author: Eric Patterson



Overview

On 5 May, Infoblox observed a malicious spam (malspam) campaign using Microsoft Excel (XLS) documents to deliver the Dridex banking trojan via embedded PowerShell commands.

The malspam distributed in this campaign impersonated messages from Intuit, the software company behind TurboxTax and QuickBooks. Aspects of this campaign differ slightly from those we previously reported on, but the goal of stealing credentials has remained the same.[1,2]

Customer Impact

Dridex was first discovered in 2011 and has consistently been one of the most prolific banking trojans on the market.[3] Threat actors favor this malware for large scale, financially motivated malspam campaigns.

Once the victim is infected, Dridex uses its core functionality of website injections and form grabbing to siphon online banking credentials.

Campaign Analysis

The emails we observed in this campaign all imitated financial invoices with the subject lines “Purchase Order/Invoice <six digits>.” In all instances, the attachment file was named *invoice_<six digits>.xls*. The six digits in the file name did not correspond to those in the subject line. The email sender address is an automated and legitimate email address used by the QuickBooks Online platform for businesses to provide invoicing. The threat actor(s) likely chose it to evade detection and prevent organizations from blocking solely on the Simple Mail Transfer Protocol (SMTP) from address. The message bodies were blank.

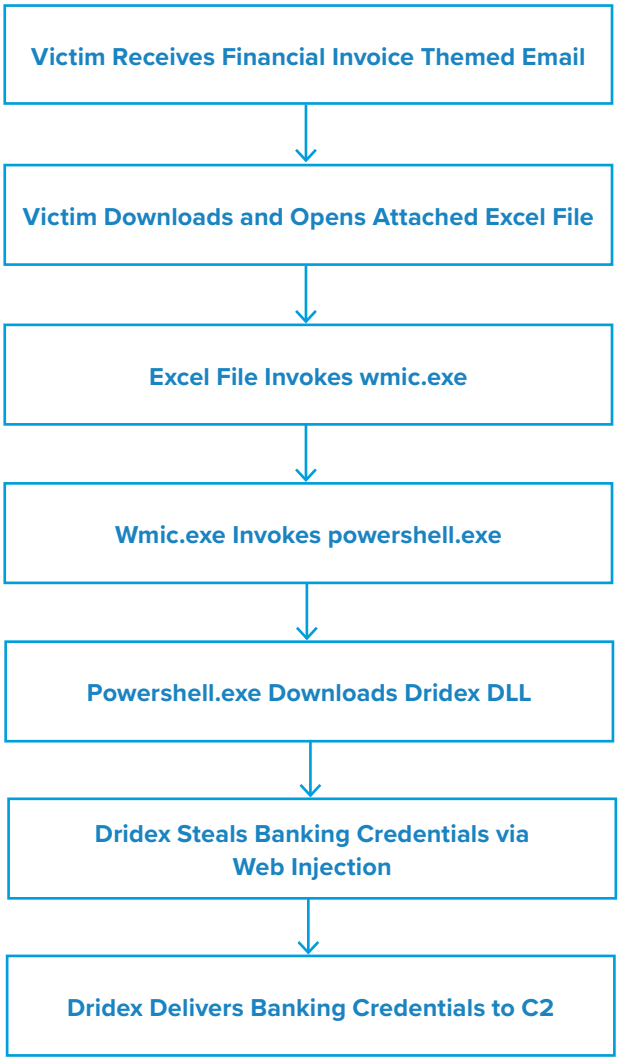
The sending-server IP addresses for this campaign are geographically dispersed with no apparent favoritism to a single country, region, or Internet Service Provider (ISP).

When we analyzed the attachment metadata, we found that this was a more widespread campaign that followed the tactics, techniques, and procedures (TTPs) above, but with slight modifications to the subject lines and attachment names.[4,5,6,7,8,9]

Attack Chain

The attachment we observed is an uncompressed, non-password protected XLS file. Once opened, it immediately appears to error out or quit, but does not provide the user with the customary notification that Windows processes have stopped responding. At this point, the file invokes the Windows Management Interface Command (WMIC) to call *powershell.exe*.

The PowerShell code attempts to download the Dridex } dynamic-link library (DLL); if successful, the malware is installed on the victim host. It then attempts to steal credentials and other data, and transmits that information to its command and control (C2) infrastructure.



Vulnerabilities & Mitigation

Dridex is a prolific banking trojan that is equipped with credential stealing functions. Infoblox recommends the following methods for detecting, preventing, and mitigating Dridex attacks:

- Install and run advanced antivirus software that can detect, quarantine, and remove malware.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Develop traffic rules that can block outbound access to potentially malicious endpoints based on domains or unique URI parameters.
- Implement PowerShell logging to detect any anomalous or malicious use.
- Install strong email security solutions to detect emails with suspicious content.

Endnotes

1. https://docs.google.com/document/d/1hkcJ-uVz9AzVhx0MhYgstTQAAnQ4ZAJefti_OUuoaYY/edit
2. https://docs.google.com/document/d/127k0-EOEAualeh182MbDxXxiRM0dPkgrUAyJpuphwH8/edit
3. https://www.globenewswire.com/news-release/2020/04/09/2014156/0/en/March-2020-s-Most-Wanted-Malware -Dridex-Banking-Trojan-Ranks-On-Top-Malware-List-For-First-Time.html
4. https://twitter.com/reecdeep/status/1257311243796271104
5. https://www.virustotal.com/gui/file/5cf7bc9a59fcd10c02ca84c8dc4993b6f4425c645d863e69ea146668acf244a4 /community
6. https://pastebin.com/KzwFLmrh
7. https://any.run/report/19042ea0e61783a3c281e3f02e0e2e2b07e9421bae0afeeae21febe450510f0c/c1cacdbc-e2d8-46b2-b060-d221c5f3df70
8. https://any.run/report/5cf7bc9a59fcd10c02ca84c8dc4993b6f4425c645d863e69ea146668acf244a4/a0bf5ad3-01f2-4a47-8c46-48a1669c8e22
9. https://bazaar.abuse.ch/sample/5cf7bc9a59fcd10c02ca84c8dc4993b6f4425c645d863e69ea146668acf244a4/

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com