Realistic Delivery Notices Drop Dridex Banking Trojan

Author: Eric Patterson

Overview

On 24 September, Infoblox observed a malicious spam (malspam) email campaign distributing the Dridex banking trojan via emails spoofing FedEx package delivery notifications.[1]

In previously reported Dridex campaigns, the emails masqueraded as notifications from other legitimate companies such as Automatic Data Processing, Inc. (ADP), eFax, and Intuit.[2,3,4]

Customer Impact

Dridex was first discovered in 2011 and has consistently been one of the most prolific banking trojans on the market.[5] Threat actors typically favor this malware for large scale, financially-motivated malspam campaigns.

Once a victim is infected, Dridex uses its core functionalities of website injections and form grabbing to siphon online banking credentials and pilfer funds from the victims.

Campaign Analysis

Emails in this campaign imitate FedEx Shipment delivery notifications with subject lines containing *FedEx Shipment <fake 12-digit tracking number>: Delivered.* The message body itself uses HTML formatting to mimic the layout, format, and style of a standard FedEx delivery email. By all measurable standards, the malicious message body appears identical to legitimate emails sent by FedEx.

The email senders are slight variations of FedEx's legitimate email accounts.

The email infrastructure for delivering the Dridex malware includes fraudulent sites with a wide range of top-level domains (TLDs). The registration information for the associated domains also makes use of various registrars and nameservers with no discernable pattern or preference.

Attack Chain

Within the body of the message is a fake 12-digit tracking number that when clicked, automatically downloads a ZIP file to the victim's machine from one of many malicious hosting domains. Extracting the ZIP archive yields a screensaver file (SCR) with the same name as an Adobe PDF icon. This method of using SCR files with PDF icons is a well-known technique of Dridex and the banking malware community as a whole.

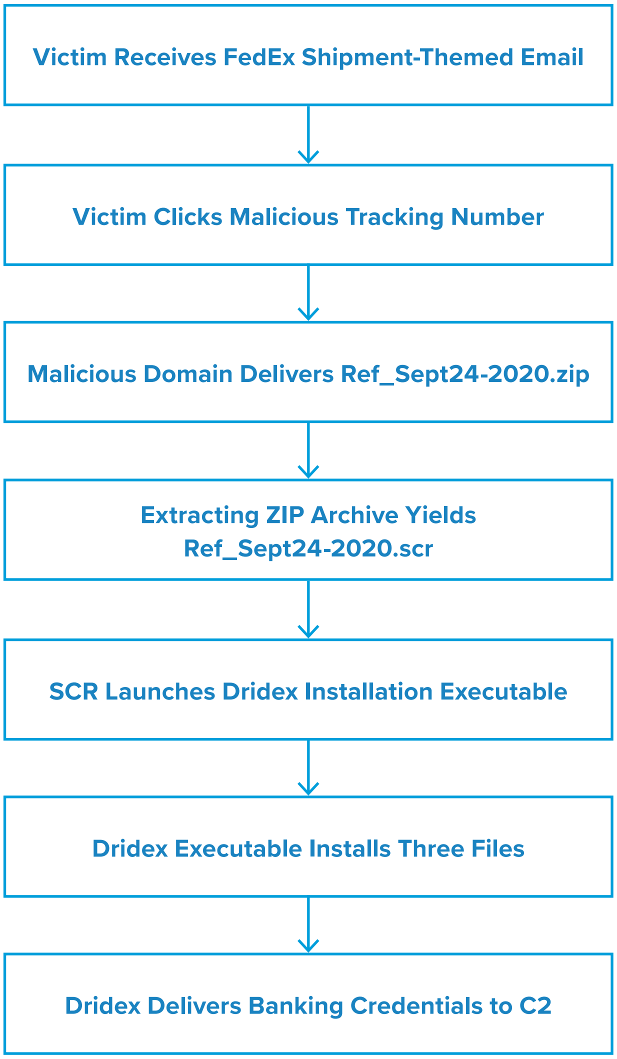
Clicking on the SCR file will launch the Dridex installation executable (EXE) of the same name, which then installs three dynamic-link library (DLL) files onto the victim's machine: *ACTIVEDS.dll*, *VERSION.dll*, and *DUI70.dll*. Each of these files is installed by a legitimate Windows process: *ApplySettingsTemplateCatalog.exe, ie4uinit.exe,* and *DmNotificationBroker.exe,* respectively.

Once installed, Dridex will attempt to uncover and steal sensitive banking information belonging to the victim and transmit that to one of its active command and control (C2) channels via SSL.[6]

Vulnerabilities & Mitigation

Dridex is a 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.


Victim Receives FedEx Shipment-Themed Email
Victim Clicks Malicious Tracking Number
Malicious Domain Delivers Ref_Sept24-2020.zip
Extracting ZIP Archive Yields Ref_Sept24-2020.scr
SCR Launches Dridex Installation Executable
Dridex Executable Installs Three Files
Dridex Delivers Banking Credentials to C2

Endnotes

1. https://www.malware-traffic-analysis.net/2020/09/24/index.html
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--51
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--19
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--72
5. 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
6. https://www.joesandbox.com/search?q=fad001d463e892e7844040cabdcfa8f8431c07e7ef1ffd76ffbd190f49d7693d

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