Dridex Banking Trojan Hides in Fake Payroll Notifications

Author: Christopher Kim

Overview

During the week of 2 December, we observed a malicious email campaign distributing Dridex banking trojan. Similar to our first Dridex report[1] in June, the emails had password-protected Microsoft Office document attachments that used macros with hardcoded URLs to download and execute Dridex payloads.

On 5 December, the Department of Treasury Financial Sector Cyber Information Group and the Department of the Treasury's Financial Crimes Enforcement Network published a joint awareness alert regarding Dridex.[2] On the same day, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and the Department of Justice indicted two Russian nationals for developing and distributing Dridex.[3]

Customer Impact

Dridex is a banking trojan that was first discovered in 2011[4] and became one of the most distributed of its kind by 2015.[5] Dridex operators have historically targeted the financial services sector, including both financial institutions and their customers.

Actors typically distribute Dridex via email spam campaigns. The actors use social engineering methods to persuade victims to open malicious email attachments by using keywords and themes that are commonly associated with important business documents. Keywords used by Dridex campaigns include "invoice", "eFax", "payroll", "receipt", "order", "scan", "debit note", "itinerary", and others.

Campaign Analysis

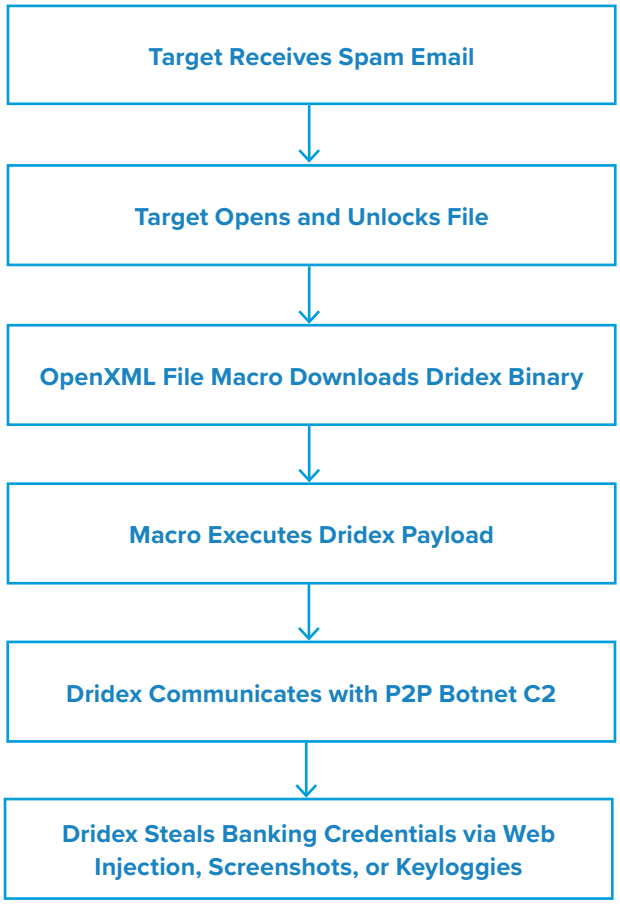
In the campaign we observed, the malicious emails mimicked an automated payroll notification from Automatic Data Processing, Inc. (ADP), an American provider of human resource management software. Each of these emails included an attached OpenXML file whose name began with "payroll_" and ended with 6 random digits and a ".doc" file extension.

The OpenXML files in this campaign each contained a macro with an embedded Dridex payload URL. Some of these Dridex payload URLs were hosted by compromised websites running a vulnerable version of WordPress, while others were hosted by domains that were registered with Openprovider on 3 December. We suspect these domains were registered by the threat actor due to their unusual domain names and the fact that they were used for this campaign less than a week after they were registered.

Attack Chain

Victims who opened the attached OpenXML files in this campaign were prompted to enter a 3 to 4 digit password found in the body of the email. When victims entered the password and enabled document macros, the file executed a PowerShell command to download the Dridex payload from an external website. The command used a VBScript named visitcard.vbs to write the Dridex payload to c:\Colorfonts32\secpi15.exe.

After the OpenXML loader executed the Dridex binary, the malware attempted to make a TCP connection over port 443 to a peer-to-peer (P2P) botnet command and control (C2). The P2P botnet C2 is responsible for providing the infected machine with a bot module and list of peers to communicate with. The bot module contains all of the core functionality that Dridex uses to steal user credentials. This includes the ability to take screenshots of the victim's system, log the victim's keypresses, and perform web injection attacks against specific website targets (e.g. banking websites).[6]



Vulnerabilities & Mitigation

Dridex is a dangerous malware that is equipped with credential stealing functions. Infoblox recommends the following methods for 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.
- Implement web proxies and create traffic rules that can block outbound access to potentially malicious endpoints based on unique URI parameters.
- Dridex uses PowerShell to download its binary. Organizations should implement logging for PowerShell to identify malicious use.
- Install strong email security solutions to detect emails with suspicious content.

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--19
2. https://www.us-cert.gov/ncas/alerts/aa19-339a
3. https://home.treasury.gov/news/press-releases/sm845
4. https://www.kaspersky.com/about/press-releases/2017_the-dridex-banking-trojan-an-ever-evolving-threat
5. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/dridex-financial-trojan.pdf
6. https://www.forcepoint.com/blog/x-labs/dridex-shadows-blacklisting-stealth-and-crypto-currency

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