Weekly Feature: Continuous Changes and Experimentation with Dridex Operations

By Visa | Posted At: 03/17/16 12:00 AM EDT

https://apps.fireeye.com/visa-vti/briefings/B-MOZ59EH

Since the beginning of January 2016, both **Visa** and **FireEye** have reported on trends and shifts in the widespread Dridex operation and associated phishing campaigns. Dridex (initially known as Cridex and Feodo), is a credential theft malware family that has been used since at least January 2010. In July 2014, a new version was discovered and the malware was then dubbed "Dridex". Although this new strain was very similar to past versions, it integrated several new functions (such as more robust HTTP injection capabilities) and numerous new commands. Dridex operators also control a set number of botnets, which Visa Threat Intelligence (VTI) actively tracks. Beginning in the second week of February of 2016, PhishMe began to **observe** new, notable techniques being employed by the Dridex operators. The report below details their findings, as well as observations made by VTI from these Dridex campaigns. Based on these findings, VTI assesses that the Dridex operators continue to experiment with new distribution techniques on a regular basis.

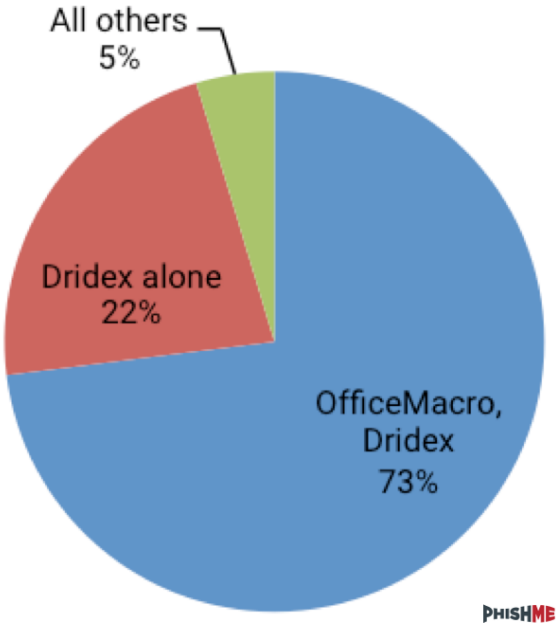
Dridex operators experimenting with distribution methods

On 10 February 2016, PhishMe researchers identified seven new distribution techniques being “tested” by the Dridex operators. These distribution methods include:

- Word documents with Macros (typical Dridex distribution method)

- Neutrino malware
- Pony malware
- Zip with .js deliveries
- Straight .js files attached to the document
- Word exploits (CVE-2012-0158)
- CAB attached files.

Analyzing several campaigns over the course of the month of February, PhishMe was able to graph the distribution trends in multiple campaigns:



Three new techniques analyzed

VTI first began observing the new techniques in phishing campaigns distributing Dridex on 3 February. In a period of one week, VTI observed three separate phishing distribution techniques, demonstrating that the Dridex operators were experimenting and testing these techniques in

order to determine the most effective and successful method. The three specific phishing campaigns are detailed below:

Dridex Word Document Campaign

Beginning on 3 February 2016, VTI **observed** a Dridex botnet 220 campaign utilizing a Weaponized Microsoft Word document as an e-mail attachment. The phishing messages refer to an e-mailed invoice that delivers an .rtf attachment. The Word document is populated with content designed to exploit a Microsoft Office vulnerability, CVE-2012-0158. This facilitates the download and execution of the malware payload stored on a compromised website. This payload is a sample of a Dridex loader binary, which is used to obtain the crucial .dll content at the core of the Dridex Trojan's presence on infected machines. This .dll content is then executed using the Windows explorer.exe process and proceeds to make contact with a set of command and control hosts. From these command and control hosts, this Trojan obtains instructions guiding the collection and exfiltration of sensitive credential data from infected machines.

Dridex .CAB Campaign

Beginning on 4 February 2016, VTI identified a Dridex botnet campaign (number unidentified) utilizing Windows Cabinet archive (.cab) file. These e-mails deliver a .cab archive--a Windows Cabinet archive--containing a single Dridex loader executable. The messages used to deliver this archive inform the recipient that the attached file is an invoice or sales document using a number of different e-mail content sets. The .cab archive, while not common to many end-users, is natively supported and extracted within the Windows ecosystem therefore providing a means of surreptitiously yet effectively delivering this malware. Once extracted from the .cab archive, this Dridex loader binary is then used to obtain the core .dll employed by the Trojan to carry out browser-based credential theft as well as HTTP injection and redirects.

Dridex JavaScript Campaign

Beginning on 11 February, VTI **observed** a Dridex botnet 220 campaign utilizing a malicious JavaScript file (Nemuncod Downloader) as an e-mail attachment. This distribution method shifted away from the traditional technique of delivering the Dridex Trojan using Microsoft Office documents (as described above). This set of messages delivers JavaScript applications designed to download a malware executable to deliver the Dridex malware. The simplistic emails employed simple phishing lures including, "more scans" and “unpaid invoice”, and “your services may be suspended”, in the subject line. Some campaigns were observed being distributed with empty e-mail bodies. Once executed, each of the JavaScript applications attached to these messages has the capability of downloading and executing a Dridex loader executable from payload locations. This Dridex loader binary is then used to obtain the core .dll employed by the Trojan to carry out browser-based credential theft as well as HTTP injection and redirects

VTI notes that these three distribution methods should not be considered as an all-inclusive list. The examples above specifically detail three recent techniques. As the PhishMe research indicates in Section 1, the Dridex operators have tested at least seven techniques recently.

VTI expects experimentation to continue

As FireEye notes in its report on 4 February 2016, Dridex phishing/spam represents the highest volume of all malicious e-mail observed worldwide. In 2015 specifically, Dridex was identified as one of the top 5 most prolific malware campaigns to be delivered via spam/phishing. In October 2015, as previously **reported** by VTI, the U.S. Department of Justice, the U.K.’s National Crime Agency, Europol and international information security firms joined together in an effort to “take-down” the malware. Despite the law enforcement arrest of one of the figures believed to be instrumental in the malware development and distribution, Dridex continues to evolve and expand its influence.

In addition to the changes detailed in this report, VTI has also identified other shifts regarding distribution methods related to the Dridex operation. On 29 January 2016, security researchers at Zscaler, an information security company, **reported** that two malware families (Dridex and Kasidet) were being deployed simultaneously against victim systems. Using previously established,

standard Dridex phishing e-mails, actors delivered the Dridex malware, as well as the Kasidet malware packages. While these two malware samples were previously observed in infections independently, the simultaneous deployment demonstrated that the cyber criminal underground continues to modify its toolsets and criminal tactics. VTI detailed this campaign in a previous daily **report** on 22 February.

In addition, as reported on 16 February, VTI identified two primary distribution patterns of the **Locky ransomware**, which demonstrated technical similarities and infrastructure overlap with the Dridex banking Trojan operation. VTI assessed that this overlap with the prolific Dridex operation allowed the Locky ransomware to almost immediately impact multiple industries worldwide. Within its first week, based on VTI research, Locky ransomware surpassed any other normally observed malicious e-mail campaigns, including Dridex, Zeus, and Cryptowall, and reportedly targeted multiple industry verticals, including healthcare and financial institutions.

VTI analysis of the Locky campaigns suggests that there are at least two affiliate Dridex campaigns (two customers of the Locky service). The two affiliate campaigns closely resemble two known Dridex campaigns:

(Affiliate ID = 1; Dridex 12X-like distribution) campaigns

(Affiliate ID = 3; Dridex 22X-like distribution) campaigns

One of the most important characteristics of Locky ransomware was its apparent appropriation of the mechanisms used to deliver the Dridex banking Trojan, leading to speculation that this ransomware tool represents yet another diversification in the criminal operation that has historically used the Dridex Trojan. Based on the numerous alterations in the distribution methods of the Dridex operations and links with other malware families, VTI assesses that the operators behind Dridex continue to experiment with their cyber crime campaign and seek to identify the most financially successful method for compromising end user and enterprise networks.

In general, enterprise users must be aware of threats from malicious applications, messages and e-mail attachments that could launch malware on their personal and corporate devices. Users accessing enterprise networks should not open attachments or follow prompts that disable security features on their mobile devices and personal computers. Organizations should employ strong defensive toolsets in order to mitigate threats, such as Dridex, and other prevalent malware and ransomware. E-mail gateway and exchange appliances can detect and drop most phishing attempts from known campaigns, including Dridex. In addition, up to date antivirus enterprise solutions on end user workstations can also provide another layer of security in order to stop threats, including Dridex, from successfully infecting an organization's workstation.

VTI is providing identified indicators of compromise associated with the most recent reporting along with this weekly report. A list of IP addresses associated with the malware, sources by **PhishMe**, is provided.

Indicators (26)

IPs (26)

185.24.92.236

91.239.232.145

144.76.73.3

103.245.153.70

193.17.184.250

41.86.46.245

41.38.18.230

62.109.133.248

217.35.78.204

148.202.223.222

181.177.231.245

141.89.179.45

188.126.116.26

5.9.37.137

141.16.91.132

46.183.66.210

178.118.31.240

103.23.154.184

174.70.100.90

200.69.183.183

185.47.108.92

200.57.183.176

194.126.100.220

194.95.134.106

176.53.0.103

181.53.255.145