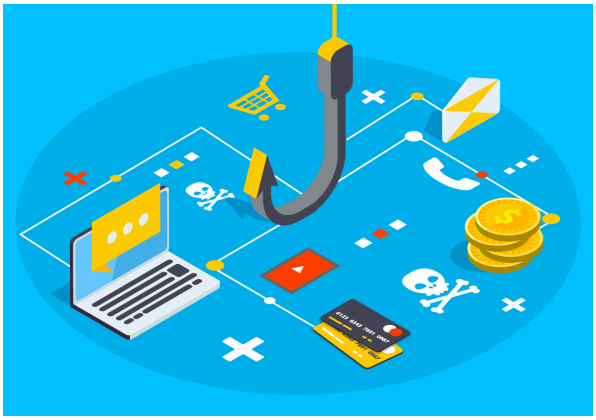
Dridex Banking Trojan

Author: Chris Kim



Overview

On 13 June, we discovered emails distributing a banking trojan named Dridex. In keeping with previous Dridex campaigns, the emails masqueraded as messages from eFax - a global leader in online fax services.

The email infrastructure for delivering the Dridex downloader included fraudulent sites with a select set of top level domains (TLDs). All of the domains were registered through Namecheap, a registrar that had recently started a sale for domains that match those we observed as part of the campaign.[1]

Customer Impact

Dridex is a banking trojan that was first discovered in 2011.[2] Threat actors use spam emails to deliver fake Microsoft documents embedded with malicious macros. Many of these emails are delivered by the Necurs botnet.

Since 2012, Necurs has forced millions of infected clients to deliver some of the most popular banking trojans.[3] Once a client has been infected, Dridex operators use web injection methods to steal the user's online banking credentials and funds from the victim's bank accounts.

Campaign Analysis

The emails we detected on 13 June showed subject lines that imitated messages from eFax. Threat actor(s) have used this particular spoof to distribute Dridex as well as other malware such as Hancitor, Pony Loader, Zeus Panda, etc.[4]

All the emails we observed were delivered by SMTP mail servers geolocated in Russia and configured to IP addresses in several classless inter-domain routing (CIDR) blocks.

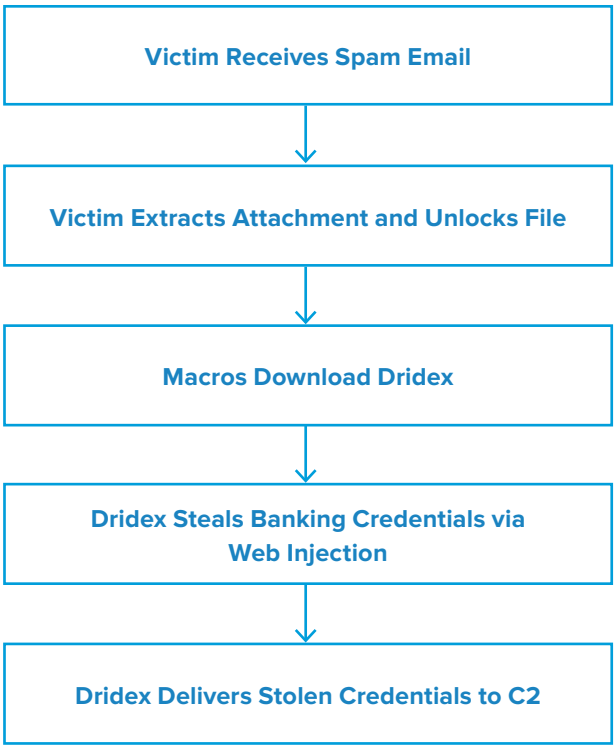
The email senders were tied to accounts that used fraud domains with .club, .host, .site, and .xyz TLDs. The threat actor(s) selected several domain names and registered each one to all 4 TLDs. For example: domain[.]club, domain[.]host, domain[.]site, and domain[.]xyz.

All of the sender account domains were registered with Namecheap on 13 June. It is possible the threat actor(s) took advantage of Namecheap's recent domain registration sale to bulk configure the email bots.

Attack Chain

The attachment for each email was a compressed file that used the extension .zip or .rar. Within each file, we found a password-protected Microsoft document. It was embedded with malicious macros that attempted to download the trojan payload from an external URL.

When we began our analysis on the Microsoft documents, the domain from the URL was already suspended. According to the cyber security community, the URL dropped a Dridex binary and then connected to its command and control (C2) server.[5]



Vulnerabilities & Mitigation

We recommend the following methods to prevent and mitigate infections from banking trojans like Dridex:

- Delete suspicious looking emails, especially if they come with links or attachments.
- Install reputable email security solutions that can detect malicious attachments.
- Use caution when conducting online banking sessions and beware of unusual website appearances that may indicate a web injection.
- Be wary of documents that require the user to enable macros to view content.
- Frequently monitor banking account activity for anomalous behavior and indicators of compromise.

Endnotes

1. https://www.namecheap.com/promos/amazing88s/
2. https://www.kaspersky.com/about/press-releases/2017_the-dridex-banking-trojan-an-ever-evolving-threat
3. https://www.cyber.nj.gov/threat-profiles/botnet-variants/necurs
4. https://isc.sans.edu/forums/diary/Malicious+spam+with+Word+document/20225/
5. https://twitter.com/James_inthe_box/status/1139210749484531713