**Infrastructure Alert Analysis**

*Report*

Analyst: PFC. Powell, Joshua

**Threat:** Dridex P2P Malware

**Alert:** (TA15-286A)

*url:* <https://www.us-cert.gov/ncas/alerts/TA15-286A>

***Date:*** Oct. 13, 2015 *(Last reviewed: Sept. 29, 2016)*

**Description:** This threat affects operating systems (OS). A system infected with Dridex may collect users’ credentials, partake in DDoS attacks, and send spam. Dridex is a multifunctional malware package that leverages obfuscated macros in Microsoft Office and extensible markup language (XML) files to infect systems (us-cert.gov). The goal of Dridex is to infect computers and steal credentials, also obtain money from users’ accounts. Primarily a banking Trojan, Dridex is distributed through emails. The emails appear legitimate and are carefully crafted to entice the victim to click on a hyperlink or to open a malicious attached file (us-cert.gov). Infected computers are capable of stealing credentials through use of keystrokes logging and web injects,

**Vulnerability:** The vulnerability is a 3 out of 5. The threat effectiveness after computer is affected is 4 out of 5 meaning it is a nuisance to deal with and can cost the company millions. Dridex variants are received through emails as spam and immediately affects the system when opened.

**Mitigation**

* Our company must keep our operating systems and application software’s up to date. Install the latest software patches that is available.
* Using legitimate and approved anti-malware tools to identify and remove cyber infections.
* Create a log that cycles out passwords that all users’ use within the company. This does not include personal passwords for other sites, apps, and company user account. These passwords are held by persons’ who are authorized and/or have a certain clearance to access certain company features on the website or access to company areas. The new passwords will be sent out by encrypted txt message. Old programs will be deleted 3 seconds after all text messages have been sent to appropriate users.
* Create a log-list that block and delete emails that are of unknown source, unknown documents and downloads, and from unknown recipients. An employee should always contact and research if a recipient if they believe or unsure if that entity exists.
* Use email blocking software.
* If a computer is affected passwords should be changed immediately and systems need to be transferred to a new system. Users should do the same for all other personal accounts they own if they used it on company computers.