PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
INFORMATION SYSTEMS SECURITY DIVISION

DRIDEX MALWARE
(CSB19-06)

SUMMARY

The Dridex malware, and its various iterations, has the capability to impact confidentiality of customer data and availability of data and systems for business processes. According to industry reporting, the original version of Dridex first appeared in 2012, and by 2015 had become one of the most prevalent financial Trojans. We expect actors using Dridex malware and its derivatives to continue targeting the financial services sector, including both financial institutions and customers.

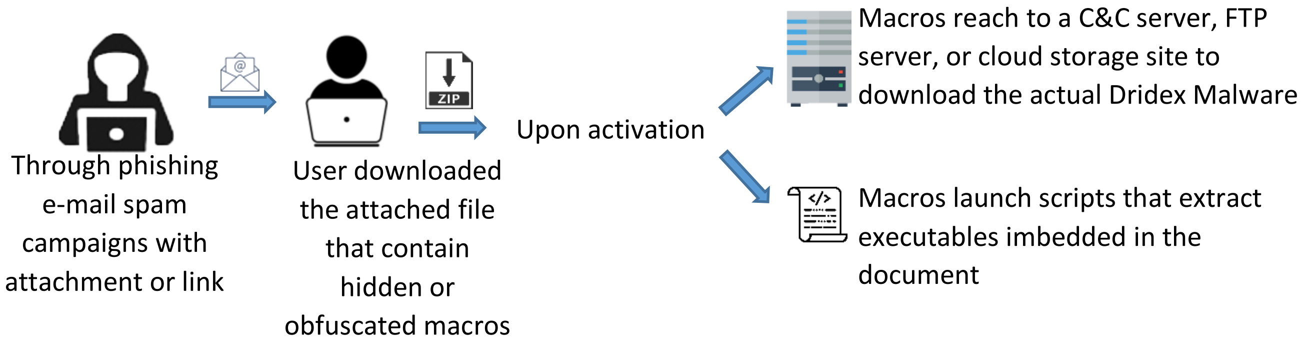
DRIDEX-RELATED PHISHING ATTRIBUTES

Actors typically distribute Dridex malware through phishing e-mail spam campaigns.

- **Phishing messages** employ a combination of legitimate business names and domains, professional terminology, and language implying urgency to persuade victims to activate open attachments.
- **Sender** e-mail addresses can simulate individuals (name@domain.com), administrative (admin@domain.com, support@domain.com), or common “do not reply” local parts (noreply@domain.com).
- **Subject and attachment** titles can include typical terms such as “invoice”, “order”, “scan”, “receipt”, “debit note”, “itinerary”, and others.
- The **e-mail body** may contain no text at all, except to include attachments with names that are strings of numbers, apparently relying on the subject line and victim curiosity to coerce the opening of the malicious file. It may specifically state that the contents of the e-mail underwent virus scanning or simply directs the victim toward the link or attachment. Or it may include a long, substantive message, providing multiple points of contact and context for the malicious attachment.
- **Attachment and hyperlink** names vary from random sets of numbers or imitation automatic filenames from scanners to filenames purporting to reference financial records. Attachments may or may not have direct references using the same file name or strings of numbers in the bodies of the e-mails.

Malware downloaders are concealed in compressed files using the ZIP or RAR file formats. Occasionally compressed files within compressed files (double zipped) are used. The compressed files can include extensible markup language (.xml), Microsoft Office (.doc, .xls), Visual Basic (.vbs), JavaScript (.jar), or portable document format (.pdf) files. Many of the files, rather than containing the actual malware, contain hidden or obfuscated macros. Upon activation, the macros reach to a command and control server, FTP server, or cloud storage site to download the actual Dridex malware. In other cases, macros launch scripts that extract executables imbedded in the document as opposed to downloading the payload. This can be done through social engineering.

HOW IT WORKS



Through phishing e-mail spam campaigns with attachment or link

User downloaded the attached file that contain hidden or obfuscated macros

Upon activation

Macros reach to a C&C server, FTP server, or cloud storage site to download the actual Dridex Malware

Macros launch scripts that extract executables imbedded in the document

SECURITY RISKS

- Modification of directory files;
- Modification of firewall rules to facilitate peer-to-peer communication for extraction of code;
- Remote execution of data (Microsoft Office and WordPad);
- Infiltrate browsers;
- Once downloaded and active – downloading software to establishing a virtual network to deletion of files;
- Ability to infiltrate browsers, detect access to online banking applications and websites, and inject malware or keylogging software, via API hooking, to steal customer login information. After stealing the login data, they have the potential to facilitate fraudulent automated clearing house and wire transfers, open fraudulent accounts, and potentially adapt victim accounts for other scams involving business e-mail compromise or money mule activity.

MITIGATIONS

- Ensuring systems are set by default to prevent execution of macros.
- Inform and educate employees on the appearance of phishing messages, especially those used by the hackers for distribution of malware in the past.
- Update intrusion detection and prevention systems frequently to ensure the latest variants of malware and downloaders are included.
- Conduct regular backup of data, ensuring backups are protected from potential ransomware attack.
- Exercise employees' response to phishing messages and unauthorized intrusion.
- If there is any doubt about message validity, call and confirm the message with the sender using a number or e-mail address already on file.
- Remind users and administrators to use the following best practices to strengthen the security posture of their organization's systems:
- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable file and printer sharing services. If these services are required, use strong passwords or Active Directory authentication.

- Restrict users’ ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and require regular password changes.
- Exercise caution when opening email attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on workstations, and configure it to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious email attachments; ensure the scanned attachment is its “true file type” (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs).
- Scan all software downloaded from the Internet before executing.
- Maintain situational awareness of the latest threats.
- Implement appropriate access control lists.
- Exercise cybersecurity procedures and continuity of operations plans to enhance and maintain ability to respond during and following a cyber incident.

REFERENCE

- https://www.us-cert.gov/ncas/alerts/aa19-339a;