Dridex

Dridex is a banking trojan commonly distributed through emails containing malicious Excel documents. Researchers have tied Dridex operations to other malware toolkits such as Ursnif, Emotet, TrickBot, and DoppelPaymer ransomware.

PAIRS WITH THIS SONG

ANALYSIS

Editor's note: *While the detection opportunities and analysis on this page are still relevant, it has not been updated since 2021.*

Analysis

Dridex is a well known banking trojan that shares both code similarities and overlapping infrastructure with Gameover Zeus. The operators of Dridex are referred to by various names, including **TA505** and **INDRIK SPIDER**. When it first showed up on the scene **in 2014**, it delivered malicious Word documents containing VBA macros. Over the years it has used other formats such as malicious JavaScript and Excel documents. Even though the initial payload delivery format has changed, Dridex has consistently focused on getting into user mailboxes and ushering users into unwittingly executing malicious code on their endpoints. Malicious emails containing Dridex attachments encourage clicking by giving the attached Excel documents enticing names like "Invoice," "Inv," "Outstanding," "Payment," or "Statement."

XLM macros

These macros utilize the Binary Interchange File Format (**BIFF**), an early cousin of the better-known **Visual Basic for Applications** (VBA) macros. Excel 4.0 macros offer similar functionality as VBA macros but give adversaries the distinct advantage of being able to hide in plain sight; macro code can be spread throughout a spreadsheet over disparate cells, rendering analysis difficult and making it not immediately obvious that executable code is even present.

Previously, XLM also allowed code execution without being subjected to the scrutiny of the **Microsoft Antimalware Scan Interface** (AMSI), which made it easier for Dridex and other malware to use XLM to evade defenses. As of March 2021, **Microsoft has added AMSI coverage for Excel 4.0 macros**, enabling vendors to acquire insight into runtime execution. Ultimately, if your organization doesn't have a business use for executing macros in your environment, it's better to **disable them altogether**.

Later stages

Beyond the initial delivery, one of the most common techniques we observed Dridex using throughout the year was **DLL search order hijacking** of various legitimate Windows executables. The Dridex operators don't stick to a single Windows executable when doing search order hijacking, necessitating multiple detection analytics to catch this behavior. We also observed Dridex persisting as a **scheduled task**. In fact, Dridex's place in our top 10 threats is due in no small part to scheduled tasks left over from incomplete remediation efforts. This pattern emphasizes the importance of cleaning up persistence when responding to threats.

While Dridex is a threat in and of itself, in 2020 we also observed multiple environments where Dridex led to the ransomware family DoppelPaymer—and we've observed the same pattern in early 2021. Similar to other "ransomware precursor" families in our top 10 such as **TrickBot**, **Emotet**, and **Qbot**, the threat of follow-on ransomware emphasizes the need for quick identification and remediation of Dridex in any environment. Given the long history of Dridex consistently evolving to combat modern-day security controls while maintaining the same means of payload delivery, the best way to protect your organization from Dridex is filtering emails at your mail gateways to prevent its delivery.

Detection opportunities

Detection opportunity 1

Scheduled task creation containing system directory
ATT&CK technique(s): T1053.005 Scheduled Task/Job: Scheduled Task
ATT&CK tactic(s): Persistence

Details: Dridex maintains persistence via the creation of scheduled tasks (`schtasks.exe`) within system directories such as `windows\system32\`, `windows\syswow64`, `winnt\system32` and `winnt\syswow64`. Identifying the instances of `schtasks.exe` where the command line contains both the flag `/create` and a system path often helps us identify existing or residual instances of Dridex on an endpoint.

Detection opportunity 2

Excel spawning `regsvr32.exe`
ATT&CK technique(s): T1218.010 Signed Binary Proxy Execution: Regsvr32
ATT&CK tactic(s): Defense Evasion

Details: Dridex uses Excel macros as a springboard to initiate additional malicious code via Register Server (`regsvr32.exe`). While files called by `regsvr32` traditionally end in `.dll` (as in the first example below), we often observe this threat and others using different file extensions to avoid recognition as a DLL (as in the second example below). Detecting this type of activity can be as easy as identifying any instances where `excel.exe` is spawning `regsvr32.exe` as a child process, as this activity is uncommon in most environments.

Detection opportunity 3

DLL search order hijacking
ATT&CK technique(s): T1574.001 **Hijack Execution Flow: DLL Search Order Hijacking**
ATT&CK tactic(s): Persistence, Privilege Escalation, Defense Evasion

Details: Another opportunity for detection is based around **search order hijacking**. This type of attack is successful when a Windows native binary executes from within a directory that contains one or more malicious DLL binaries. These unassuming DLLs opportunity requires some work: start by cataloging all native Windows binaries, and then write detection analytics for any instances where these binaries are executed from anywhere other than their standard locations. Admittedly, this leads to a lot of detection analytics due to the volume of native Windows binaries, but we’ve found that creating these analytics is worth the effort to catch Dridex as well as other threats that use DLL search order hijacking.

demo
now

Search

- Managed Detection and Response (MDR)
- Readiness Exercises
- Linux EDR
- Atomic Red Team™
- Mac Monitor
- What’s New?
- Plans

- Deliver Enterprise Security Across Your IT Environment
- Get a 24×7 SOC Instantly
- Protect Your Corporate Endpoints and Network
- Protect Your Users’ Email, Identities, and SaaS Apps
- Protect Your Cloud
- Protect Critical Production Linux and Kubernetes
- Stop Business Email Compromise
- Replace Your MSSP or MDR
- Run More Effective Tabletops
- Train Continuously for Real-World Scenarios
- Operationalize Your Microsoft Security Stack
- Minimize Downtime with After-Hours Support

RESOURCES

- View all Resources
- Blog
- Integrations
- Guides & Overviews
- Cybersecurity 101
- Case Studies
- Videos
- Webinars
- Events
- Customer Help Center
- Newsletter

PARTNERS

- Overview
- Incident Response
- Insurance & Risk
- Managed Service Providers
- Solution Providers
- Technology Partners
- Apply to Become a Partner

COMPANY

- About Us
- The Red Canary Difference
- News & Press
- Careers – We’re Hiring!

info@redcanary.com

+1 855-977-0686 Privacy Policy Trust Center and Security Cookie Settings