CYBERSECURITY ADVISORY

# Dridex Malware

**Last Revised:** June 30, 2020 **Alert Code:** AA19-339A



## Summary

This Alert is the result of recent collaboration between the Department of the Treasury Financial Sector Cyber Information Group (CIG) and the Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) to identify and share information with the financial services sector. Treasury and the Cybersecurity and Infrastructure Security Agency (CISA) are providing this report to inform the sector about the Dridex malware and variants. The report provides an overview of the malware, related activity, and a list of previously unreported indicators of compromise derived from information reported to FinCEN by private sector financial institutions. Because actors using Dridex malware and its derivatives continue to target the financial services sector, including financial institutions

and customers, the techniques, tactics, and procedures contained in this report warrant renewed attention. Treasury and CISA encourage network security specialists to incorporate these indicators into existing Dridex-related network defense capabilities and planning. For information regarding the malicious cyber actors responsible for the development and distribution of the Dridex malware, see the Treasury press release, Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware <https://home.treasury.gov/news/press-releases/sm845> and the FBI press release, Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware.

*This Alert does not introduce a new regulatory interpretation, nor impose any new requirements on regulated entities. Except where noted, there is no indication that the actual owner of the email address was involved in the suspicious or malicious activity. If activity related to these indicators of compromise is detected, please notify appropriate law enforcement and the CIG.*

For a downloadable copy of IOCs, see:

- AA19-339A CSV <https://www.cisa.gov/sites/default/files/publications/aa19-339a_white.csv>
- AA19-339A STIX XML <https://www.cisa.gov/sites/default/files/publications/aa19-339a_white_stix.xml>



# Technical Details

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 messages vary widely. 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. Where there is a message body, the body may specifically state that the contents of the e-mail underwent virus scanning or simply directs the victim toward the link or attachment. In other cases, the body 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.



**Example Links and Filenames** (Note: link information is representative. Italicized statements are automatically generated by the cloud storage provider. # represents a random number.):

- Link: HTTPS://WWW.GOOGLE[.]COM/URL?Q=HTTPS://WWW.(*Cloud Services Provider*)[.]COM/S/(*Cloud Account Value*) /RECENT%20WIRE%20PAYMENT %######.SCR?(*Cloud Provided Sequence*)
- Link: HTTPS://WWW.GOOGLE[.]COM/URL?Q=HTTPS://WWW.(*Cloud Services Provider*)[.]COM/S/ *Cloud Account Value*/AUTOMATEDCLEARINGHOUSE%20 PAYMENT####.DOC?(*Cloud Provided Sequence*)

- Link: Malicious File: ID201NLD0012192016.DOC

Attachments or eventual downloads can take a variety of formats. In some instances, 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.

By default, software generally prevents execution of macros without user permission. Attached files, particularly .doc and .xls files, contain instructions on how a user should enable content and specifically macros, effectively using social engineering to facilitate the download. Malicious files sometimes even include screenshots of the necessary actions to enable macros.

## Malware Capabilities



Dridex malware operates from multiple modules that may be downloaded together or following the initial download of a “loader” module. Modules include provisions for capturing screenshots, acting as a virtual machine, or incorporating the victim machine into a botnet. Through its history and development, Dridex has used several exploits and methods for execution, including modification of directory files, using system recovery to escalate privileges, and modification of firewall rules to facilitate peer-to-peer communication for extraction of data. Recent versions of Dridex exploit vulnerability CVE-2017-0199, which allows remote execution of code. This vulnerability is specific to Microsoft Office and WordPad. Microsoft released a patch in 2017.

Once downloaded and active, Dridex has a wide range of capabilities, from downloading additional software to establishing a virtual network to deletion of files. The primary threat to financial activity is the Dridex's 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. Dridex modules package, encrypt, and transmit captured information, screenshots, etc., via peer-to-peer (P2P) networks in the XML format or in binary format, as seen in newer versions. After stealing the login data, the attackers have the potential to facilitate fraudulent automated clearing house (ACH) and wire transfers, open fraudulent accounts, and potentially adapt victim accounts for other scams involving business e-mail compromise or money mule activity.

The Dridex malware has evolved through several versions since its inception, partially to adapt to updated browsers. Although the characteristics described reflect some of the most recent configurations, actors continue to identify and exploit vulnerabilities in widely used software.

## Dridex Malware and Variants

While Dridex is among the most prevalent sources of infection, previous variants and similar malware continue to represent a threat. Dridex is itself an improved variant of the Cridex and Bugat Trojans that preceded it, and it shares some of their codes. Although the previous variants' theft activities operate in mostly the same way, the P2P communication aspects of Dridex improve its concealment and redundancy.



## Ransomware

Actors distributing Dridex likely employ ransomware with similar configurations. Code for BitPaymer, also known as Friedex, includes numerous similarities to Dridex, despite its function as ransomware rather than data extraction. The two malwares use the same mechanics for several functions, and the authors compiled the codes at nearly the same time. The ransomware distributed through these malwares has targeted U.S. financial institutions and resulted in data and financial loss.

Locky ransomware operates using the same delivery method for the downloader, with similar subject lines and attachments. Attackers also use the same botnets to deliver both Dridex and Locky ransomware, sometimes simultaneously. Variants of Locky include Zepto and Osiris. Locky ransomware and its variants have a wide footprint, with varying impact depending on victim IT policies and practices and network configurations.

### Dridex-related Activity

Although the highest infection rates took place in late 2015 and early 2016, concurrent with Locky ransomware distribution, Dridex continues to impact numerous countries. The Dridex hackers appear to direct the majority of attacks at English-speaking countries. Cybersecurity industry reporting attributes Dridex, BitPaymer, and Locky campaigns, as well as other massive malware spam (malspam) campaigns to actors known alternately as Evil Corp or TA505. (Note: some cybersecurity industry reporting simply refers to the actors as “Dridex” or the “Dridex hackers.”) Actors distribute the malware via massive spam campaigns, sending up to millions of messages per day, although volume of messages varies widely.

## Indicators of Compromise



The following indicators are associated with the activity described in this report:

| Indicator Type | Indicator Value | Associated Activity |
|---|---|---|
| Email address | info[@]antonioscognamiglio[.]it | Dridex |
| Email address | info[@]golfprogroup[.]com | Dridex |
| Email address | cariola72[@]teletu[.]it | Dridex |

| Indicator Type | Indicator Value | Associated Activity |
|---|---|---|
| Email address | faturamento[@]sudestecaminhoes[.]com.br | Dridex |
| Email address | info[@]melvale[.]co.uk | Dridex |
| Email address | fabianurquiza[@]correo.dalvear[.]com.ar | Dridex |
| Email address | web1587p16[@]mail.flw-buero[.]at | Dridex |
| Email address | bounce[@]bestvaluestore[.]org | Dridex |
| Email address | farid[@]abc-telecom[.]az | Dridex |
| Email address | bounce[@]bestvaluestore[.]org | Dridex |
| Email address | admin[@]sevpazarlama[.]com | Dridex |
| Email address | faturamento[@]sudestecaminhoes[.]com.br | Dridex |
| Email address | pranab[@]pdrassocs[.]com | Dridex |
| Email address | tom[@]blackburnpowerltd[.]co.uk | Dridex |

| Indicator Type | Indicator Value | Associated Activity |
|---|---|---|
| Email address | yportocarrero[@]elevenca[.]com | Dridex |
| Email address | s.palani[@]itifsl.co[.]in | Dridex |
| Email address | faber[@]imaba[.]nl | Dridex |
| Email address | admin[@]belpay[.]by | Dridex |
| IP address | 62[.]149[.]158[.]252 | Dridex |
| IP address | 177[.]34[.]32[.]109 | Dridex |
| IP address | 2[.]138[.]111[.]86 | Dridex |
| IP address | 122[.]172[.]96[.]18 | Dridex |
| IP address | 69[.]93[.]243[.]5 | Dridex |
| IP address | 200[.]43[.]183[.]102 | Dridex |
| IP address | 79[.]124[.]76[.]30 | Dridex |
| IP address | 188[.]125[.]166[.]114 | Dridex |
| IP address | 37[.]59[.]52[.]64 | Dridex |
| IP address | 50[.]28[.]35[.]36 | Dridex |
| IP address | 154[.]70[.]39[.]158 | Dridex |

| Indicator Type | Indicator Value | Associated Activity |
|---|---|---|
| IP address | 108[.]29[.]37[.]11 | Dridex |
| IP address | 65[.]112[.]218[.]2 | Dridex |

# Mitigations

Treasury and CISA encourage users and organizations to:

1. Contact law enforcement immediately report regarding any identified activity related to Dridex malware or its derivatives. Please see contact information for FBI and CISA at the end of this report.
2. Incorporate the indicators of compromise identified in this report into intrusion detection systems and security alert systems to enable active blocking or reporting of suspected malicious activity. Note that the above list is not a comprehensive list of all indicators associated with this activity.
3. Report suspicious activity, highlighting the presence of "Cyber Event Indicators." Indicators of Compromise, such as suspicious e-mail addresses, file names, hashes, domains, and IP addresses, can be provided under Item 44 of the Suspicious Activity Report (SAR) form. FinCEN welcomes voluntary SAR filing in circumstances where reporting is not required.



## Recommendations for All Organizations

The following mitigation recommendations respond directly to Dridex TTPs:

- 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.
- Treasury and CISA 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.

The National Institute of Standards and Technology (NIST) has published additional information on malware incident prevention and handling in their Special Publication 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops <https://www.nist.gov/publications/guide-malware-incident-prevention-and-handling-desktops-and-laptops>.

## Why Best Practices Matter

The National Security Agency (NSA) recently published its *Top Ten Cybersecurity Mitigation Strategies* (this is the current website for Top 10 mitigation strategies). Aligned with the NIST Cybersecurity Framework, the Strategies offer a risk-based approach to mitigating exploitation techniques used by Advance Persistent Threat (APT) actors.

The *Strategies* counter a broad range of exploitation techniques used by malicious cyber actors. NSA's mitigations set priorities for enterprise organizations to minimize mission impact. The mitigations also build upon the NIST Cybersecurity Framework functions to manage cybersecurity risk and promote a defense-in-depth security posture. The mitigation strategies are ranked by effectiveness against known APT tactics. Additional strategies and best practices will be required to mitigate the occurrence of new tactics.

1. **Update and Upgrade Software Immediately.** Apply all available software updates, automate the process to the extent possible, and use an update service provided directly from the vendor. Automation is necessary because threat actors study patches and create exploits, often soon after a patch is released. These "N-day" exploits can be as damaging as a zero-day. Vendor updates must also be authentic; updates are typically signed and delivered over protected links to assure the integrity of the content. Without rapid and thorough patch application, threat actors can operate inside a defender's patch cycle.

2. **Defend Privileges and Accounts.** Assign privileges based on risk exposure and as required to maintain operations. Use a Privileged Access Management (PAM) solution to automate credential management and fine-grained access control. Another way to manage privilege is through tiered administrative access in which each higher tier provides additional access, but is limited to fewer personnel. Create procedures to securely reset credentials (e.g., passwords, tokens, tickets). Privileged accounts and services must be controlled because threat actors continue to target administrator credentials to access high-value assets, and to move laterally through the network.
3. **Enforce Signed Software Execution Policies.** Use a modern operating system that enforces signed software execution policies for scripts, executables, device drivers, and system firmware. Maintain a list of trusted certificates to prevent and detect the use and injection of illegitimate executables. Execution policies, when used in conjunction with a secure boot capability, can assure system integrity. Application Allow listing should be used with signed software execution policies to provide greater control. Allowing unsigned software enables threat actors to gain a foothold and establish persistence through embedded malicious code.
4. **Exercise a System Recovery Plan.** Create, review, and exercise a system recovery plan to ensure the restoration of data as part of a comprehensive disaster recovery strategy. The plan must protect critical data, configurations, and logs to ensure continuity of operations due to unexpected events. For additional protection, backups should be encrypted, stored offsite, offline when possible, and support complete recovery and reconstitution of systems and devices. Perform periodic testing and evaluate the back plan. Update the plan as necessary to accommodate the ever-changing network environment. A recovery plan is a necessary mitigation for natural disasters as well as malicious threats including ransomware.
5. **Actively Manage Systems and Configurations.** Take inventory of network devices and software. Remove unwanted, unneeded, or unexpected hardware and software from the network. Starting from a known baseline reduces the attack surface and establishes control of the operational environment. Thereafter, actively manage devices, applications, operating systems, and security configurations. Active enterprise management ensures that systems can adapt to dynamic threat environments while scaling and streamlining administrative operations.

6. **Continuously Hunt for Network Intrusions.** Take proactive steps to detect, contain, and remove any malicious presence within the network. Enterprise organizations should assume that a compromise has taken place and use dedicated teams to continuously seek out, contain, and remove threat actors within the network. Passive detection mechanisms, such as logs, Security Information and Event Management (SIEM) products, Endpoint Detection and Response (EDR) solutions, and other data analytic capabilities are invaluable tools to find malicious or anomalous behaviors. Active pursuits should also include hunt operations and penetration testing using well documented incident response procedures to address any discovered breaches in security. Establishing proactive steps will transition the organization beyond basic detection methods, enabling real-time threat detection and remediation using a continuous monitoring and mitigation strategy.
7. **Leverage Modern Hardware Security Features.** Use hardware security features like Unified Extensible Firmware Interface (UEFI) Secure Boot, Trusted Platform Module (TPM), and hardware virtualization. Schedule older devices for a hardware refresh. Modern hardware features increase the integrity of the boot process, provide system attestation, and support features for high-risk application containment. Using a modern operating system on outdated hardware results in a reduced ability to protect the system, critical data, and user credentials from threat actors.
8. Segregate Networks Using Application-Aware Defenses. Segregate critical networks and services. Deploy application-aware network defenses to block improperly formed traf and restrict content, according to policy and legal authorizations. Traditional intrusion detection based on known-bad signatures is quickly decreasing in effectiveness due to encryption and obfuscation techniques. Threat actors hide malicious actions and remove data over common protocols, making the need for sophisticated, application-aware defensive mechanisms critical for modern network defenses.

9. **Integrate Threat Reputation Services.** Leverage multi-sourced threat reputation services for files, DNS, URLs, IPs, and email addresses. Reputation services assist in the detection and prevention of malicious events and allow for rapid global responses to threats, a reduction of exposure from known threats, and provide access to a much larger threat analysis and tipping capability than an organization can provide on its own. Emerging threats, whether targeted or global campaigns, occur faster than most organizations can handle, resulting in poor coverage of new threats. Multi-source reputation and information sharing services can provide a more timely and effective security posture against dynamic threat actors.
10. **Transition to Multi-Factor Authentication.** Prioritize protection for accounts with elevated privileges, remote access, and/or used on high value assets. Physical token-based authentication systems should be used to supplement knowledge-based factors such as passwords and PINs. Organizations should migrate away from single factor authentication, such as password-based systems, which are subject to poor user choices and susceptible to credential theft, forgery, and reuse across multiple systems.

# Contact Information

## Reporting Suspected Malicious Activity

To report an intrusion and request resources for incident response or technical assistance, contact CISA (central@mail.cisa.dhs.gov or 1-844-Say-CISA), FBI through a local field offic <https://www.fbi.gov/contact-us/field-offices>, or FBI's Cyber Division (CyWatch@fbi.gov or 855-292-3937).

Institutions should determine whether filing of a Suspicious Activity Report ("SAR") is required under Bank Secrecy Act regulations. In instances where filing is not required, institutions may file a SAR voluntarily to aid FinCEN and law enforcement efforts in protecting the financial sector. Financial institutions are encouraged to provide relevant cyber-related information and indicators in their SAR reporting. For questions regarding cyber SAR filing, please contact the FinCEN Resource Center (FRC@fincen.gov or 1-800-767-2825).

# Open-Source Reporting on Dridex

The following represents an alphabetized selection of open-source reporting by U.S. government and industry sources on Dridex malware and its derivatives:


- "Dridex P2P Malware," US-CERT Alert (TA15-286A), https://www.cisa.gov/news-events/alerts/2015/10/13/dridex-p2p-malware <https://www.cisa.gov/news-events/alerts/2015/10/13/dridex-p2p-malware>, 13 October 2015.
- "Dridex Threat Profile," New Jersey Cybersecurity & Communications Integration Cell, https://www.cyber.nj.gov/threat-landscape/malware/trojans/dridex <https://www.cyber.nj.gov/threat-landscape/malware/trojans/dridex>, accessed 15 April 2019.
- Alert Logic, "Dridex malware has evolved to Locky Ransomware," No date, https://www.alertlogic.com/resources/industry-reports/ransomware-in-focus/ <https://www.alertlogic.com/resources/industry-reports/ransomware-in-focus/>, accessed 11 March 2019.
- Avast Blog, "A closer look at the Locky ransomware," 10 March 2016, https://blog.avast.com/a-closer-look-at-the-locky-ransomware <https://blog.avast.com/a-closer-look-at-the-locky-ransomware>, accessed 6 February 2019.
- Brett Stone-Gross, Ph.D., "Dridex (Bugat v5) Botnet Takeover Operation," Secureworks, 13 October 2015, https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation <https://www.secureworks.com/research/dridex-bugat-v5-botnet-takeover-operation>, accessed 6 February 2019.
- Brewster, Thomas, "Cops Knock Down Dridex Malware that Earned 'Evil Corp' Cybercriminals At Least $50 Million," Forbes, 13 October 2015, https://www.forbes.com/sites/thomasbrewster/2015/10/13/dridex-botnet-takedown/#2b883f00415b <https://www.forbes.com/sites/thomasbrewster/2015/10/13/dridex-botnet-takedown/#2b883f00415b>.
- Chandler, Andy, "FBI announces Dridex gang indictment and praises Fox-IT," Fox-IT, 13 October 2015, https://www.fox-it.com/en/about-fox-it/corporate/news/fbi-announces-dridex-gang-indictments-praises-fox/, accessed 7 February 2019.

- DHS CISA, “Alert (TA15-286A), Dridex P2P Malware,” https://www.cisa.gov/news-events/alerts/2015/10/13/dridex-p2p-malware <https://www.cisa.gov/news-events/alerts/2015/10/13/dridex-p2p-malware>, accessed 4 June 2019.
- Eduard Kovacs, “Dridex still active after takedown attempt,” Security Week, 19 October 2015, https://www.securityweek.com/dridex-still-active-after-takedown-attempt <https://www.securityweek.com/dridex-still-active-after-takedown-attempt>, accessed 11 March 2019.
- Geoff White, “How the Dridex Gang makes millions from bespoke ransomware,” Forbes, 26 September 2018, https://www.forbes.com/sites/geoffwhite/2018/09/26/how-the-dridex-gang-makes-millions-from-bespoke-ransomware/ <https://www.forbes.com/sites/geoffwhite/2018/09/26/how-the-dridex-gang-makes-millions-from-bespoke-ransomware/>, accessed 11 March 2019.
- MS-ISAC, “Cybercrime Technical Desk Reference,” 31 August 2018, https://www.cisecurity.org/wp-content/uploads/2018/09/MS-ISAC-Cyber-Crime-Technical-Desk-Reference.pdf <https://www.cisecurity.org/wp-content/uploads/2018/09/ms-isac-cyber-crime-technical-desk-reference.pdf>, accessed 6 February 2019.
- O’Brien, Dick. “Dridex: Tidal waves of spam pushing dangerous financial Trojan,” Symantec, February 2016, https://docs.broadcom.com/doc/dridex-financial-trojan <https://docs.broadcom.com/doc/dridex-financial-trojan>, accessed 4 February 2019.
- Poslušný, Michal, “FriedEx: BitPaymer ransomware the work of Dridex authors,” welivesecurity by ESET, 26 January 2018, https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/ <https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/>, accessed 6 February 2019.
- Proofpoint, “Dridex Campaigns Hitting Millions of Recipients Using Unpatched Microsoft Zero-Day,” https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day <https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day>, accessed 5 February 2019.

- Proofpoint, “High-Volume Dridex Banking Trojan Campaigns Return.” https://www.proofpoint.com/us/threat-insight/post/high-volume-dridex-campaigns-return <https://www.proofpoint.com/us/threat-insight/post/high-volume-dridex-campaigns-return>, accessed 1 February 2019.
- Proofpoint, “Threat Actor Profile: TA505, From Dridex to GlobeImposter,” <//www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter>https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter <https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter>, accessed 6 February 2019.
- Roland Dela Paz and Ran Mosessco. “New year, new look – Dridex via compromised FTP,” ForcePoint, 18 January 2018, https://blogs.forcepoint.com/blog/security-labs/new-year-new-look-dridex-compromised-ftp, accessed 4 February 2019.
- Sanghavi, Mithun. “DRIDEX and how to overcome it.” Symantec Official Blog, 30 March 2015, https://community.broadcom.com/symantecenterprise/viewdocument/dridex-and-how-to-overcome-it?CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments, accessed 4 February 2019.
- Security Intelligence Blog, “URSNIF, EMOTET, DRIDEX and BitPaymer Gangs Linked by a Similar Loader,” Trend Micro, 18 December 2018, https://www.trendmicro.com/en_us/research/18/l/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader.html <https://www.trendmicro.com/en_us/research/18/l/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader.html>, accessed 6 February 2019.
- Talos Group, “Threat Spotlight: Spam Served With a Side of Dridex,” Cisco Blogs, 6 April 2015, https://blogs.cisco.com/security/talos/spam-dridex <https://blogs.cisco.com/security/talos/spam-dridex>, accessed 4 February 2019.


# Revisions

**December 5, 2019:** Initial version

**December 5, 2019:** Added links to Treasury and FBI press releases

**January 2, 2020:** Updated CISA contact information

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

## Tags

**Nation-State Actor**: Russia

## Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top