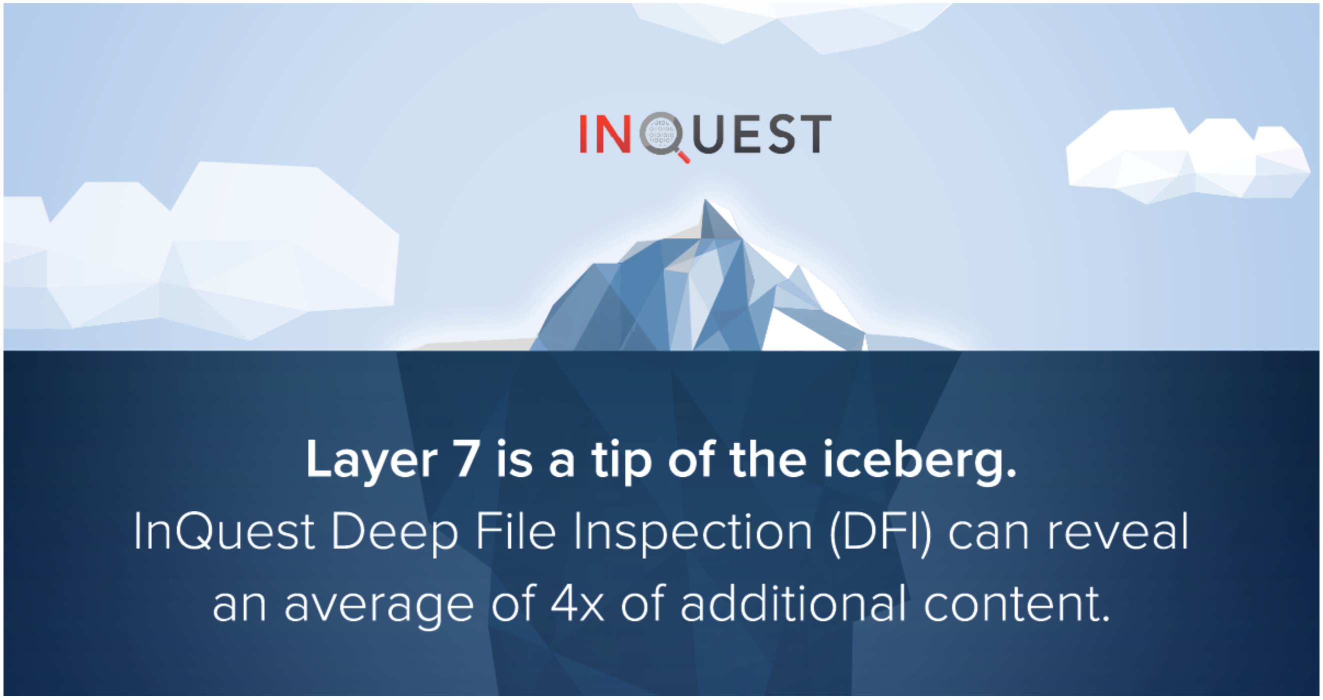
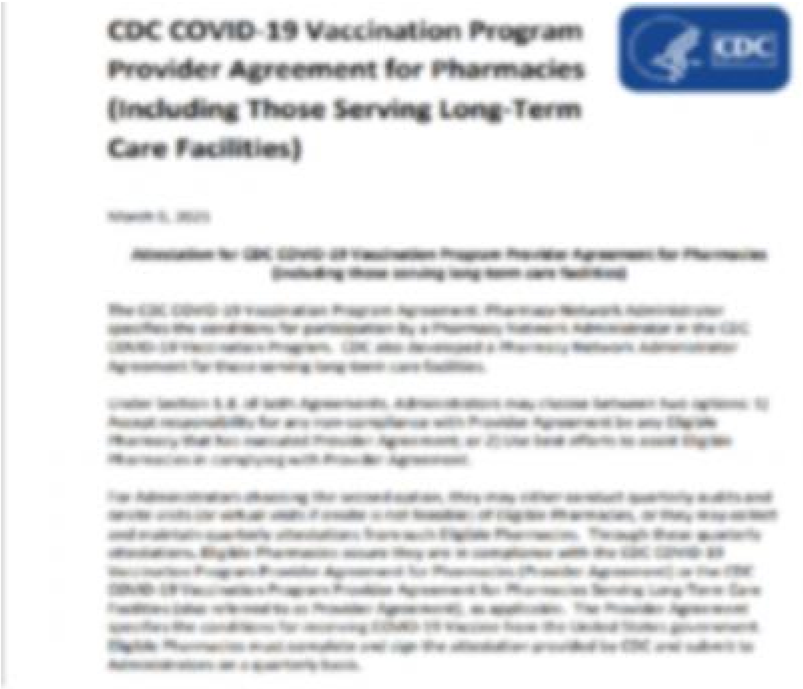
(Don't) Bring Dridex Home for the Holidays

inquest.net/blog/2021/12/20/dont-bring-dridex-home-holidays


INQUEST
Layer 7 is a tip of the iceberg.
InQuest Deep File Inspection (DFI) can reveal
an average of 4x of additional content.

With the holiday season upon us and Log4j-nia still keeping most of us awake at night, we want to revisit an old chum who continues to operate in full swing amidst the chaos. With fresh tactics at their disposal, Dridex continues to target large organizations with somewhat elaborate lures to ensure user interaction and infection. On Monday, December 15th we noticed an uptick in the amount of verified malware hiding behind password-protected Microsoft Excel spreadsheets, specifically ones containing the dated "macrosheet" functionality. One of the ongoing experiments we have running atop of InQuest Labs data is a limited brute force of these suspicious files. We will be exploring additional evasion methods leveraged by the Dridex campaign to deliver the payload.

At first glance, the samples containing image lures appear to be using blurred documents to entice users to enable macros. We have observed a variety of different subject lures during this campaign including a CDC COVID-19 form along with a fake resume, a personnel form and fake spreadsheets. As seen in the last two lure images, attackers seem to also be masquerading as the NPD group and their DecisionKey reporting software.

- 

  CDC COVID-19 Vaccination Program Provider Agreement for Pharmacies (Including Those Serving Long-Term Care Facilities)

  March 5, 2021

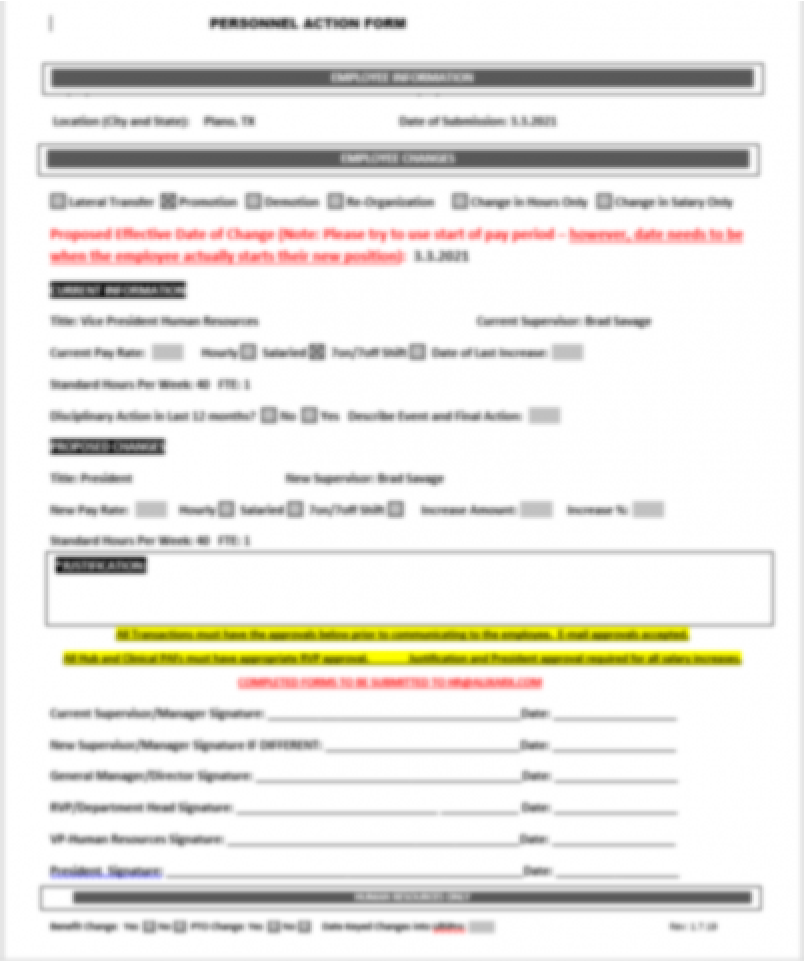
  Attestation for CDC COVID-19 Vaccination Program Provider Agreement for Pharmacies (including those serving long-term care facilities)

  The CDC COVID-19 Vaccination Program Agreement, Pharmacy Network Administrator specifies the conditions for participation by a Pharmacy Network Administrator in the CDC COVID-19 Vaccination Program. CDC also developed a Pharmacy Network Administrator Agreement for those serving long-term care facilities.

  Under Section 3.8. of both Agreements, Administrators may choose between two options: 1) Accept responsibility for any non-compliance with Provider Agreement by any Eligible Pharmacy that has executed Provider Agreement; or 2) Use best efforts to assist Eligible Pharmacies in complying with Provider Agreement.

  For Administrators choosing the second option, they may either conduct quarterly audits and onsite visits (or virtual visits if onsite is not feasible) of Eligible Pharmacies, or they may collect and maintain quarterly attestations from each Eligible Pharmacies. Through these quarterly attestations, Eligible Pharmacies assure they are in compliance with the CDC COVID-19 Vaccination Program Provider Agreement for Pharmacies (Provider Agreement) or the CDC COVID-19 Vaccination Program Provider Agreement for Pharmacies Serving Long-Term Care Facilities (also referred to as Provider Agreement), as applicable. The Provider Agreement specifies the conditions for receiving COVID-19 Vaccine from the United States government. Eligible Pharmacies must complete and sign the attestation provided by CDC and submit to Administrators on a quarterly basis.

  CDC COVID-19 Lure

- 

  PERSONNEL ACTION FORM

  EMPLOYEE INFORMATION

  Location (City and State): Plano, TX Date of Submission: 3.3.2021

  EMPLOYEE CHANGES

  ☐ Lateral Transfer ☒ Promotion ☐ Demotion ☐ Re-Organization ☐ Change in Hours Only ☐ Change in Salary Only

  Proposed Effective Date of Change (Note: Please try to use start of pay period – however, date needs to be when the employee actually starts their new position): 3.3.2021

  CURRENT INFORMATION

  Title: Vice President Human Resources Current Supervisor: Brad Savage

  Current Pay Rate: Hourly ☐ Salaried ☒ 7on/7off Shift ☐ Date of Last Increase:

  Standard Hours Per Week: 40 FTE: 1

  Disciplinary Action in Last 12 months? ☐ No ☐ Yes Describe Event and Final Action:

  PROPOSED CHANGES

  Title: President New Supervisor: Brad Savage

  New Pay Rate: Hourly ☐ Salaried ☐ 7on/7off Shift ☐ Increase Amount: Increase %:

  Standard Hours Per Week: 40 FTE: 1

  *JUSTIFICATION:

  All Transactions must have the approvals below prior to communicating to the employee. E-mail approvals accepted.

  All Hub and Clinical PAFs must have appropriate RVP approval. Justification and President approval required for all salary increases.

  COMPLETED FORMS TO BE SUBMITTED TO HR@[illegible].COM

  Current Supervisor/Manager Signature: ____________________ Date: __________

  New Supervisor/Manager Signature if DIFFERENT: ____________________ Date: __________

  General Manager/Director Signature: ____________________ Date: __________

  RVP/Department Head Signature: ____________________ Date: __________

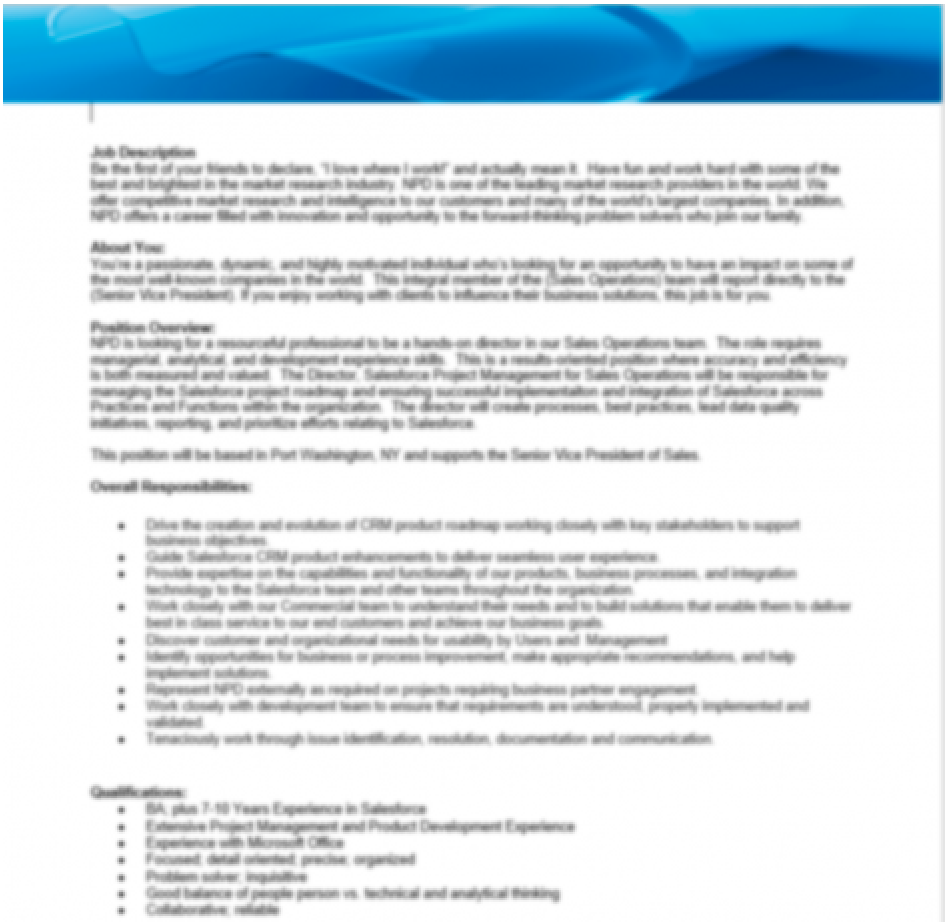
  VP-Human Resources Signature: ____________________ Date: __________

  President Signature: ____________________ Date: __________

  HUMAN RESOURCES ONLY

  Benefit Change: Yes ☐ No ☐ PTO Change: Yes ☐ No ☐ Date Keyed Changes into [illegible] Rev: 1.7.19

  Personnel Form Lure

- 

Job Description
Be the first of your friends to declare, "I love where I work!" and actually mean it. Have fun and work hard with some of the best and brightest in the market research industry. NPD is one of the leading market research providers in the world. We offer competitive market research and intelligence to our customers and many of the world's largest companies. In addition, NPD offers a career filled with innovation and opportunity to the forward-thinking problem solvers who join our family.

About You:
You're a passionate, dynamic, and highly motivated individual who's looking for an opportunity to have an impact on some of the most well-known companies in the world. This integral member of the (Sales Operations) team will report directly to the (Senior Vice President). If you enjoy working with clients to influence their business solutions, this job is for you.

Position Overview:
NPD is looking for a resourceful professional to be a hands-on director in our Sales Operations team. The role requires managerial, analytical, and development experience skills. This is a results-oriented position where accuracy and efficiency is both measured and valued. The Director, Salesforce Project Management for Sales Operations will be responsible for managing the Salesforce project roadmap and ensuring successful implementation and integration of Salesforce across Practices and Functions within the organization. The director will create processes, best practices, lead data quality initiatives, reporting, and prioritize efforts relating to Salesforce.

This position will be based in Port Washington, NY and supports the Senior Vice President of Sales.

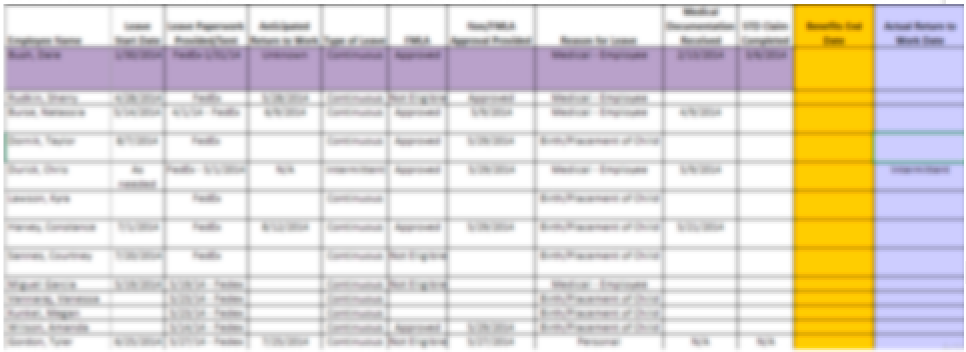
Overall Responsibilities:

- Drive the creation and evolution of CRM product roadmap working closely with key stakeholders to support business objectives.
- Guide Salesforce CRM product enhancements to deliver seamless user experience.
- Provide expertise on the capabilities and functionality of our products, business processes, and integration technology to the Salesforce team and other teams throughout the organization.
- Work closely with our Commercial team to understand their needs and to build solutions that enable them to deliver best in class service to our end customers and achieve our business goals.
- Discover customer and organizational needs for usability by Users and Management
- Identify opportunities for business or process improvement, make appropriate recommendations, and help implement solutions.
- Represent NPD externally as required on projects requiring business partner engagement.
- Work closely with development team to ensure that requirements are understood, properly implemented and validated.
- Tenaciously work through issue identification, resolution, documentation and communication.

Qualifications:

- BA, plus 7-10 Years Experience in Salesforce
- Extensive Project Management and Product Development Experience
- Experience with Microsoft Office
- Focused; detail oriented; precise; organized
- Problem solver; inquisitive
- Good balance of people person vs. technical and analytical thinking
- Collaborative; reliable

Fake Resume Lure

- 

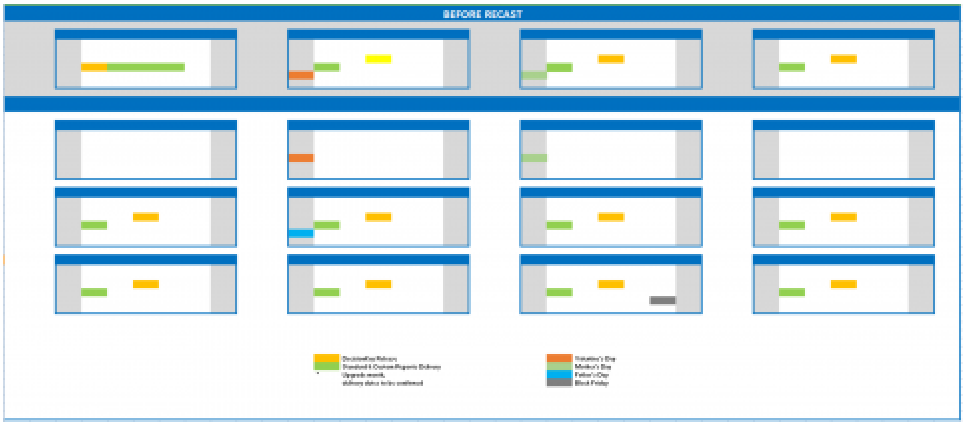
Employee Name	Leave Start Date	Leave Paperwork Provided/Sent	Anticipated Return to Work	Type of Leave	FMLA	Non/FMLA Approval Provided	Reason for Leave	Medical Documentation Received	STD Claim Completed	Benefits End Date	Actual Return to Work Date
[illegible]	[illegible]	FedEx [illegible]	Unknown	Continuous	Approved		Medical - Employee	[illegible]	[illegible]		
[illegible]	[illegible]	FedEx	[illegible]	Continuous	Not Eligible	Approved	Medical - Employee				
[illegible]	[illegible]	[illegible] - FedEx	[illegible]	Continuous	Approved	[illegible]	Medical - Employee	[illegible]			
[illegible]	[illegible]	FedEx		Continuous	Approved	[illegible]	Birth/Placement of Child				
[illegible]	As needed	FedEx - [illegible]	N/A	Intermittent	Approved	[illegible]	Medical - Employee	[illegible]			Intermittent
[illegible]		FedEx		Continuous			Birth/Placement of Child				
[illegible]	[illegible]	FedEx	[illegible]	Continuous	Approved	[illegible]	Birth/Placement of Child	[illegible]			
[illegible]	[illegible]	FedEx		Continuous	Not Eligible		Birth/Placement of Child				
[illegible]	[illegible]	[illegible] - FedEx		Continuous	Not Eligible		Medical - Employee				
[illegible]		[illegible] - FedEx		Continuous			Birth/Placement of Child				
[illegible]		[illegible] - FedEx		Continuous			Birth/Placement of Child				
[illegible]		[illegible] - FedEx		Continuous	Approved	[illegible]	Birth/Placement of Child				
[illegible]	[illegible]	[illegible] - FedEx	[illegible]	Continuous	Not Eligible	[illegible]	Personal	N/A	N/A		

Fake Spreadsheet

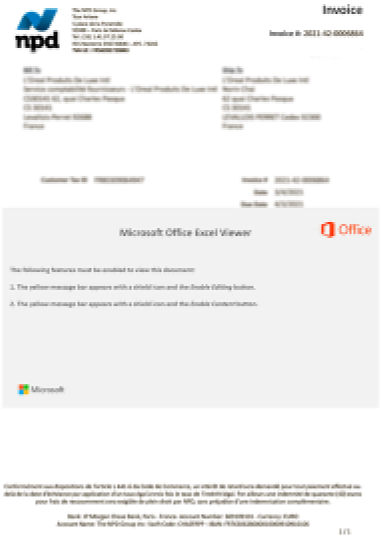
1

-
  Fake Spreadsheet

2

- 

  DecisionKey Lure

- 

  NPD Group Lure

Lure Gallery

Continuing the trend of delivering initial stage content via maldocs, Dridex has shifted to generating random numerical passwords to protect attached Microsoft Office docs. Dridex operators have gone as far as crafting emails that appear to be legitimate team/department memos and instructions. What follows are examples of these emails sent containing passwords to decrypt the attached documents.

Attachment:	Schedule.xls
Subject:	calendar 2022

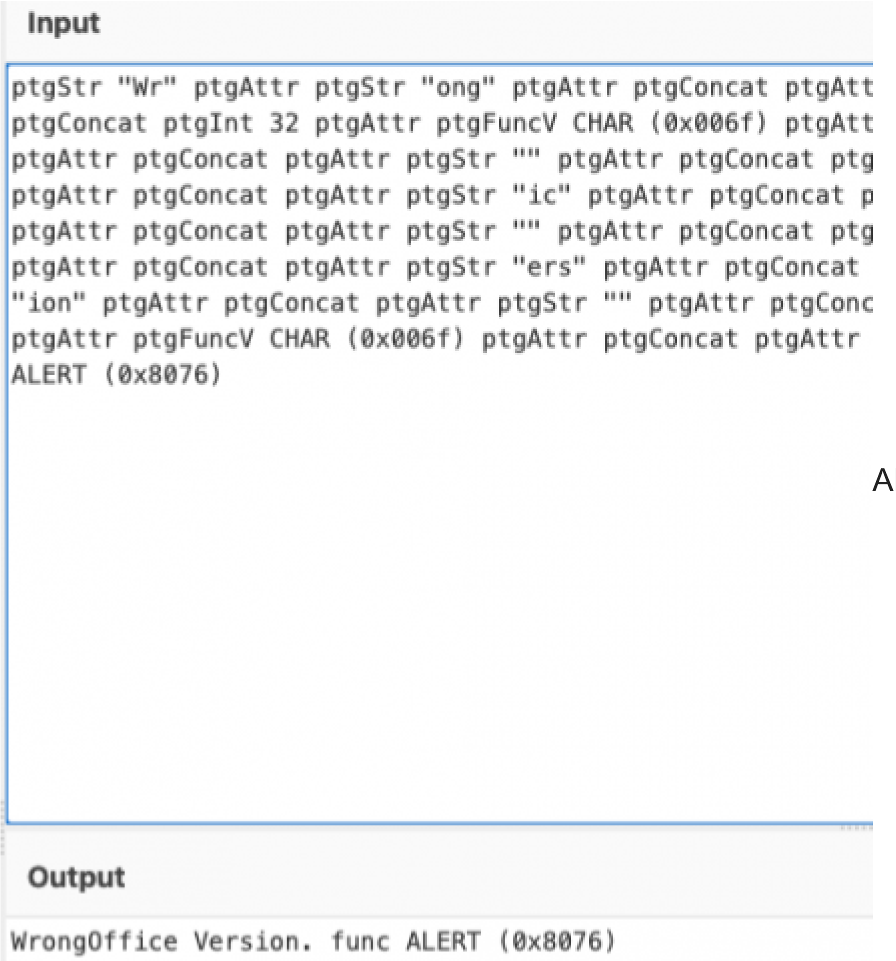
Body:	All the group leaders, staff, and concerned membersThis is being informed to you that from 22th December the office will work according to the new working time that has been agreed by all the board of directors in the annual general meeting held today. Following are the details of the new timings.All the staff members and personnel are requested to make note of the timing and come to office as per the new time from the mentioned date.Please e-sign the attached document till the end of the day.excel is secure encrypted PW 61164All the group leaders, staff, and concerned membersThis is being informed to you that from 22th December the office will work according to the new working time that has been agreed by all the board of directors in the annual general meeting held today. Following are the details of the new timings.All the staff members and personnel are requested to make note of the timing and come to office as per the new time from the mentioned date.Please e-sign the attached document till the end of the day.excel is secure encrypted PW 86819

Email Example 1

Attachment:	NewRegulations.xls
Subject:	new regulations
Body:	Due to new federal law from December, 16th (more information is in the attached document):- All unvaccinated employees (with no exceptions) have to make their shot until December, 17th. Those who will not do it in time will be dismissed without warning. Please, find more information in the attached document.- All vaccinated employees from COVID-19 must immediately view attached document for instructions. It informs you on the consequences of lying about vaccination.Please fill out the form in the attached document excel is secure encrypted PW 74826 Due to new federal law from December, 16th (more information is in the attached document):- All unvaccinated employees (with no exceptions) have to make their shot until December, 17th. Those who will not do it in time will be dismissed without warning. Please, find more information in the attached document.- All vaccinated employees from COVID-19 must immediately view attached document for instructions. It informs you on the consequences of lying about vaccination.Please fill out the form in the attached document excel is secure encrypted PW 37129

Email Example 2

An effective evasion method to slow analysis efforts, especially if one is not actively cracking documents or zip archives as password protected content continues to become more mainstay amongst malware families. Once cracked, we notice a macrosheet containing suspicious content; and with a little deobfuscation, we have our first clues.



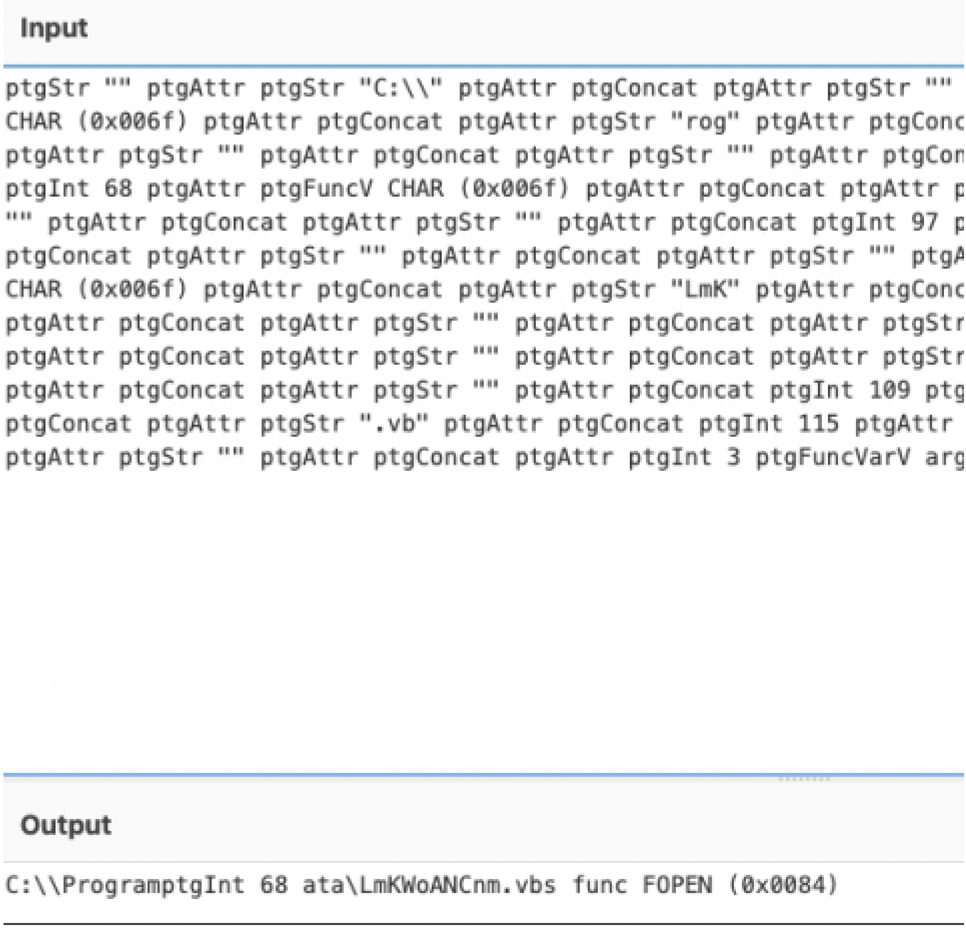
Input

```
ptgStr "Wr" ptgAttr ptgStr "ong" ptgAttr ptgConcat ptgAtt
ptgConcat ptgInt 32 ptgAttr ptgFuncV CHAR (0x006f) ptgAtt
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptg
ptgAttr ptgConcat ptgAttr ptgStr "ic" ptgAttr ptgConcat p
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptg
ptgAttr ptgConcat ptgAttr ptgStr "ers" ptgAttr ptgConcat
"ion" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConc
ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat ptgAttr
ALERT (0x8076)
```

Output

```
WrongOffice Version. func ALERT (0x8076)
```

ALERT (lure)



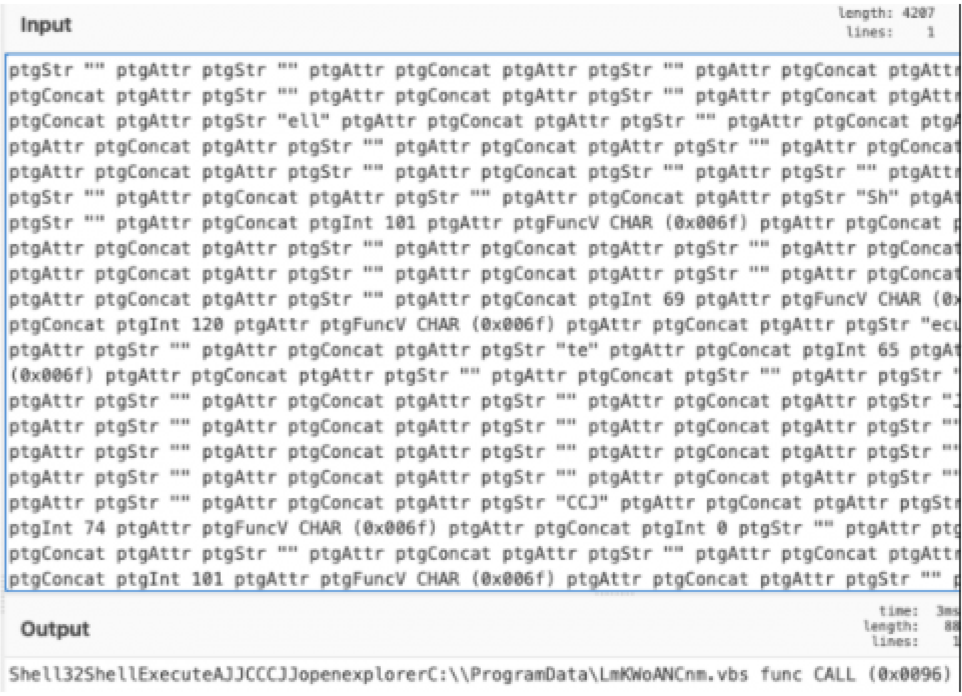
Input

```
ptgStr "" ptgAttr ptgStr "C:\\" ptgAttr ptgConcat ptgAttr ptgStr ""
CHAR (0x006f) ptgAttr ptgConcat ptgAttr ptgStr "rog" ptgAttr ptgConc
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgCon
ptgInt 68 ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat ptgAttr p
"" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgInt 97 p
ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgA
CHAR (0x006f) ptgAttr ptgConcat ptgAttr ptgStr "LmK" ptgAttr ptgConc
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgInt 109 ptg
ptgConcat ptgAttr ptgStr ".vb" ptgAttr ptgConcat ptgInt 115 ptgAttr
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgInt 3 ptgFuncVarV arg
```

FOPEN

Output

```
C:\\ProgramptgInt 68 ata\LmKWoANCnm.vbs func FOPEN (0x0084)
```



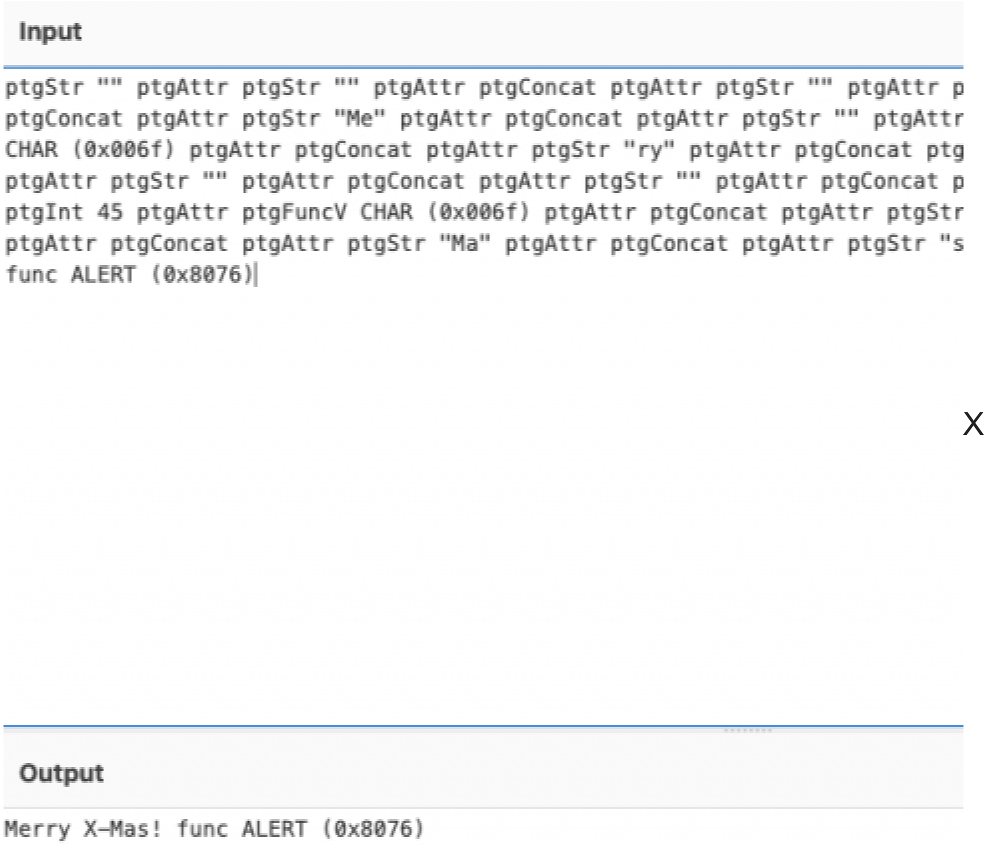
```
ptgStr "" ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr
ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr
ptgConcat ptgAttr ptgStr "ell" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgA
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgStr "" ptgAttr ptgStr "" ptgAttr
ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "Sh" ptgAt
ptgStr "" ptgAttr ptgConcat ptgInt 101 ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat p
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat
ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgInt 69 ptgAttr ptgFuncV CHAR (0x
ptgConcat ptgInt 120 ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat ptgAttr ptgStr "ecu
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "te" ptgAttr ptgConcat ptgInt 65 ptgAt
(0x006f) ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgStr "" ptgAttr ptgStr "
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "J
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr ""
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr ""
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr ""
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "CCJ" ptgAttr ptgConcat ptgAttr ptgStr
ptgInt 74 ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat ptgInt 0 ptgStr "" ptgAttr ptg
ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr
ptgConcat ptgInt 101 ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat ptgAttr ptgStr "" p
```

```
Shell32ShellExecuteAJJCCCJJopenexplorerC:\\ProgramData\LmKWoANCnm.vbs func CALL (0x0096)
```

CALL

As we can see, the macro calls an embedded .vbs file that fetches the next step of the attack chain. Using Discord’s CDN servers for distribution as threat actors have been leveraging heavily in recent campaigns, Dridex fetches a .bin that fetches additional payloads upon execution. The payloads specific to Dridex are easily identifiable by URI pattern/file name, which will not be published due to the racially insensitive nature of their naming convention.

Like any campaign, we can expect that future iterations of Dridex will change tactics and become more elusive. Changes observed between now and the numbered password uptick see slight changes in URI patterns and lure messages. We will continue monitoring these changes as the Dridex campaign continues on.



```
ptgStr "" ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr p
ptgConcat ptgAttr ptgStr "Me" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr
CHAR (0x006f) ptgAttr ptgConcat ptgAttr ptgStr "ry" ptgAttr ptgConcat ptg
ptgAttr ptgStr "" ptgAttr ptgConcat ptgAttr ptgStr "" ptgAttr ptgConcat p
ptgInt 45 ptgAttr ptgFuncV CHAR (0x006f) ptgAttr ptgConcat ptgAttr ptgStr
ptgAttr ptgConcat ptgAttr ptgStr "Ma" ptgAttr ptgConcat ptgAttr ptgStr "s
func ALERT (0x8076)
```

```
Merry X-Mas! func ALERT (0x8076)
```

X-mas Lure

As we get together with loved ones this season, we must remain vigilant of those seeking to rain on our revelry as we move into the new year. From all of us at InQuest: stay safe, happy holidays and happy new year.

InQuest customers are protected against this and other forms of password-protected evasion tactics through a unique email content sourced password cracking algorithm. If you're curious to read more, schedule a brief or request a free email security assessment.

IOCs

Subjects
calendar 2022 new regulations

File Names

ListPromotion.xls
NewRegulations-open.xls
NewRegulations.xls
Schedule.xls
Termination letter changes.xls
Termination+letter+final.xls
Termination list.xls
TerminationList.xls
Termination of 12-2021.xls

File Hashes

InQuest Labs Original Corpus

InQuest Labs Cracked Corpus

Hashes
0686491aa486f3b480ff5d08e2a78073ad8ad63cbc4942ebd784bf2b90d1afc9
0921806294ab9eb15ef8c033053a73b32e1fb637c382aeadf341e49156448079
0a4088122055f8828b2d6b954d76643b7e5d7f76b4b99900daebd04334ec17c3
1028198982d01df42681e6349f4e6489b050c6514362a677cd6d7162537ee736
104abbd10d5587eaa07b33d239369b214e513ea54da9bfddbedf6e44a1fb3494
10cfe05b10e4b247ac3e918393ce2dad51b2aa13c7ced6bbfa2752002229ce6a
15c437e91417d855b91f41c86d0df02851a2ae5fe16a305f3a343c1aafcbc55a
178c2f792e2b76b3b80e7e79f8c1628f9e54c14becd51cfde7eda9e29a37674b
179d4c96f9d5de2519e804fa009691bfc04d24c717c9dcafa68b813d1ef64757
1934699d56433ac8d58bbfb0a0b3cb979706eac4efbf81e1b4cf1c4795beeae5
1990a83fd7142096670c16e45d205568fe6a98b020b4a78fa655af5e2afc36f4
1b2c57b7f3341c8fcb5c3e1cf12d9dfef0bdf5c9e9f8c6dbc3a161966b377c17
1d82f0434f050ec3103410284ccc427d340b3677333ed67b7e54f9386c2b4daf
1fc6b5f37524fe0259a8174722bb77e5fa9c6b29493ec88984b3a1edd68d358f
2540b66d3575c77d6cf56b7a25c84ee8b3afb890830bc18434eb0eb9a4a025f3
2ab4e259e13de4b04f17b1e851203864869d0dad03e300cb78acf07a75989ab2
2f83a466b51feeeb909c925b011c2a29b5336866a6dfda7ecdf386a207a1ab22
39ae495bd79387da5aab647902175063942257 1a8a5ed3cce568993b7f27a1e5
415f0a18582c924995d56dde9bc0cca4550d8c79cda4c1187e01ca3e1adbd33d
4a9be1cf5c7999fd13ad44209f5c2f81d1c7bbab6945fd7a1386d40cd1528d42
55fd2be2dd8141e8a6b07b369f6960ae9535d4dac6e6c09066af09e9f2e3bfd0
6311ce8ae1ed5cd931ba9b996c3a9a30b013042124fa1907b8b1eed9c0a11afc
6b93b95aeba2a91c36927c24a78d31e4e3268c4933e9a8a59c97bbc132ba4aa3
6e36d6f550af23338dbb92581d196a05416e219d35870200637610fe61f90ac8
7027e4f966d496fe1723f3034307262fcf31b87913879b2e022de8bd7a0009bb
729ae5efdc4bc5e64c94a4ff74d8c2fda2343944871cb9634ff57a5660672669
7ac987ae495672f54536de3561ed2edd83bc7ab3c4e2aa7555236d6a5a15e965
7c17f15c6ab4e803c583c81045732c9093a7e3fc85d83fdda7b6e923cc00f98d
7dccaa7dabc4d729cb8492f7b58b960d684777e2ffeeae19b8d44b6191252060
81d3d6adc2ab7d0dfa7748eb3b47e0f948dcf08c748ebd88fc92c5f4003fe02f
85907df576440c2edb02b61c481a57729e237658b34c10a907df4c9e5436fe73
8a7c11ff964ef6e0ab96b0d4899094ea4449f9de7b021dfda4ef365bbf7226eb

```
928c58601658b9bd9c6b2021f718d1cc84aa38887fb1578c30b39f821b729e38
95c207832e20186155d7eb796c88dfc386b45bab717613b1951052ae8444adf5
9fe48a35ff5d31f60e0291341bcd6a4ebdb7d4bcbcb2f58037cc9ba528ff91d2
a7298803d33dfcbbdc6cd04231f73109c19a939924900a8124632c2c6531339d
a8374e62bc825095adad9a4e568731b9f1ed36558ba281b4a59ac07f5d321a36
afeb058e768bba01a899ec138adde91977149de666b112bad5cc77f8c3e4ee18
b0f2e254c80df8d67a1021b741a93645df10a8038924fa1f20ef70794595eb0e
b7c939d47e33a90b86b969255462c16aee9d8a3d95dd2728bdc11bf55f9095a4
b9064644e469f03905832e6a48e39cec42cc98d25279deaea01bd33a9355ae7a
bdb84f388788f2889497af7e7c1c5ea09ebcf505c8b0e50372492d39a853b8b3
c5995cf378c326aaa5464f4125c5ce772c452ebab0d1f65000cf47868ab46aa2
cacedbdb1abeff00898b498627812045ece2437d0539598b9dee4f15692f6487
ce36e90bae23604deb114b2fffbc2ab6939c2b4b1797c8cd154a7bcd66bfa33d
cee04b4f340a4a6cfc3c2b7bc84a0b486bc25824ac31595e47f806075df2e29d
d42a9b79de88fecde78c64786683b9e02decd120ce17e63516cd858fc5146c37
d68846240eec544727b5a115ea79a03421431553287eb6415c46781106aa717a
da9280ec7b4cadcd65ac497033d0f14accc7f7ebfd9139748df51bc727ac727f
df807b304a0c28d61eec8ca1edd0dd7c8291eb1303fab1201fb328202e48539e
e143c6a2e50f0829f45b2e9ce83130ed859dd49952eb58a7526bebefeef1ebf8
e729271973068c6d8737fb84e480f39b006e19a2aa05b8b29dd7336098c2682b
e759f093144212c013449ad30d20118bfc0b690d9e6696a1a2e354017ee3095b
ef77b0d67b2f4195cb3398d9f6a65c2d46640101f86cd310895e074efdc351e7
f418f6181041880893ccb1838048266dd9702e1b5007907dc272fe9aeaa25e17
f74097096a707d3a5d6c08527566d9f1b60ab0d24aaca12d3631e0f8c81fd74e
f9e83c29d54c4e506a95d71890a8ea26337bedb99f31f90183a67099182de965
faf66c114394d16e2616a622016432ef72b460fa5f96443d7569dedff63bff34
fe949281566ffdd1f539cd26b28df307ca14a058aa02f0d5ed05506d51e73773
```

Raw hash list

Tags

threat-intel dridex threat-hunting