Pro-Russian Group Targeting Ukraine Supporters with DDoS Attacks

decoded.avast.io/martinchlumecky/bobik/

September 6, 2022

by Martin ChlumeckýSeptember 6, 202226 min read

It has now been six months since the war in Ukraine began. Since then, pro-Russian and pro-Ukrainian hacker groups, like KillNet, Anonymous, IT Army of Ukraine, Legion Spetsnaz RF, have carried out cyberattacks. A lesser-known group called *NoName057(16)* is among the pro-Russian groups attacking Ukraine and the countries surrounding it and siding with Ukraine.

NoName057(16) is performing DDoS attacks on websites belonging to governments, news agencies, armies, suppliers, telecommunications companies, transportation authorities, financial institutions, and more in Ukraine and neighboring countries supporting Ukraine, like Ukraine itself, Estonia, Lithuania, Norway, and Poland. A full list of the group's targets can be found at the end of this post.

To carry out DDoS attacks, hacker groups utilize botnets. They control them via C&C servers, sending commands to individual bots, which essentially act as soldiers. Uncovering and tracking botnets is complex and time-consuming.

We got our hands on malware called *Bobik*. *Bobik* is not new, it's been around since 2020, and is known as a Remote Access Trojan. Things have, however, recently changed. Devices infected with *Bobik* are now part of a botnet, and carrying out DDoS attacks for *NoName057(16)*. We can confidently attribute the attacks to the group, as we have analyzed and compared what the C&C server is instructing devices infected with Bobik to do with the attacks the group claims to be responsible for on their Telegram channel.

Toolset

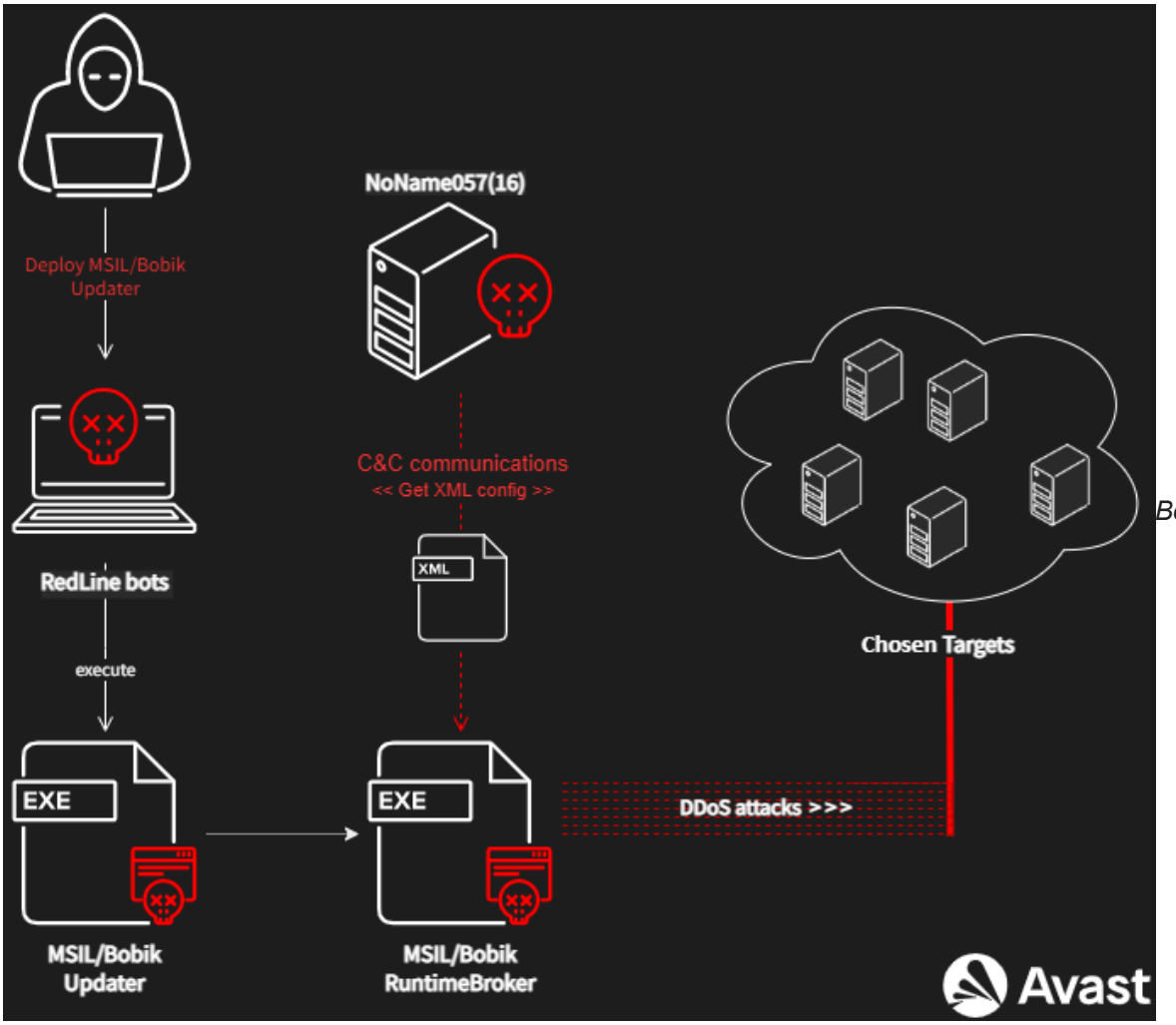
The bots used by the botnet are infected with malware called *Bobik*, which is written in .NET. The malware has not been tied to a certain group in the past, and is actually a Remote Access Trojan. Its spyware functionalities include keylogging, running and terminating processes, collecting system information, downloading/uploading files, and dropping further malware onto infected devices.

Kill Chain

In the wild, one of the most monitored droppers for *Bobik* is *RedLine Stealer*, a botnet-as-a-service cybercriminals can pay for to spread their malware of choice. The usual workflow of *Bobik* is illustrated in the image below.

At first, an unknown group seems to have purchased *RedLine Stealer* to deploy – *Bobik*. The final DDoS module deployment is composed of two basic stages. The first executes *Bobik's Updater* via a *RedLine Stealer* bot. In the second stage, *Bobik's Updater* extracts and drops the final DDoS module (*Bobik's*

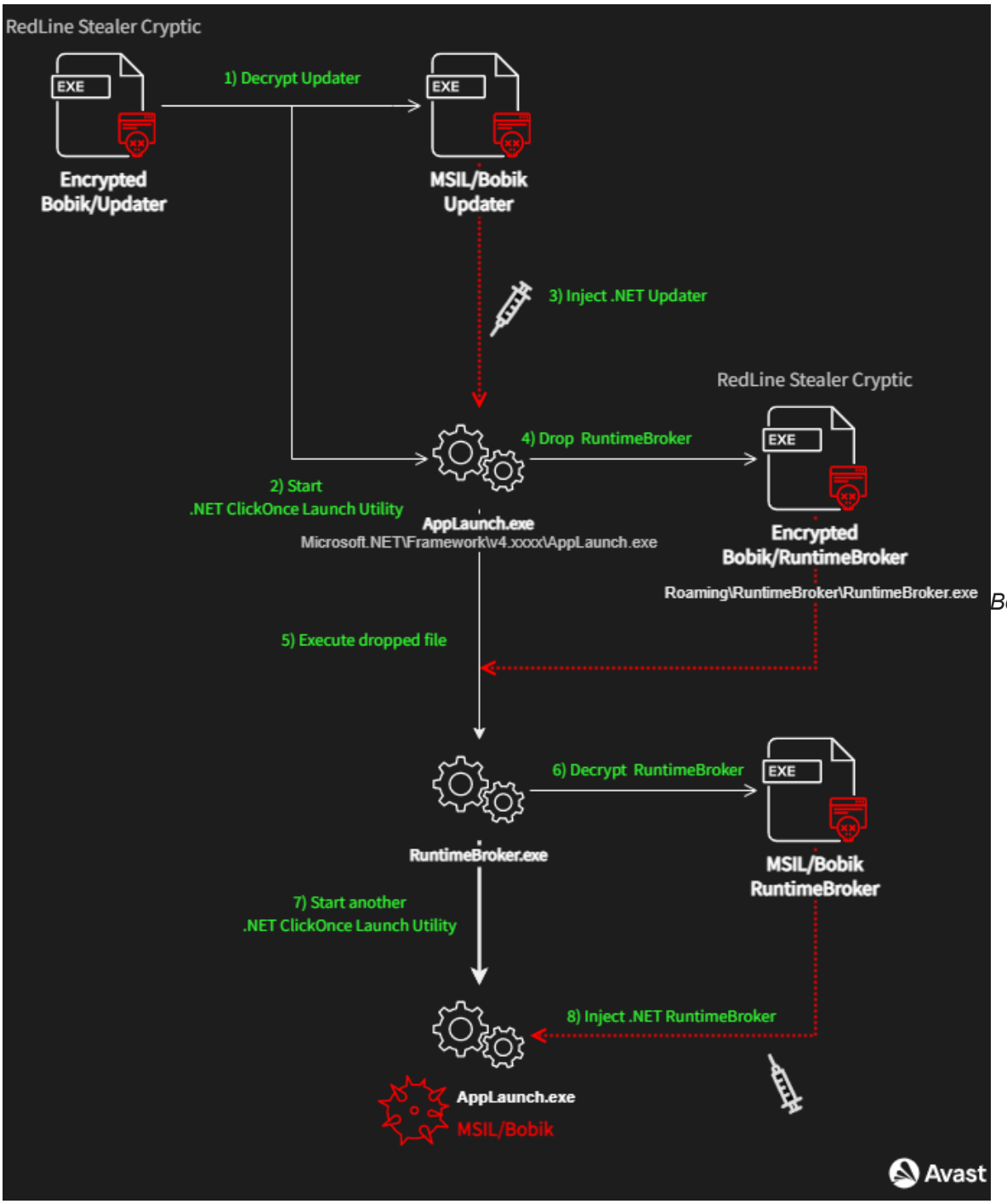
RuntimeBroker) and ensures the module's persistence.



Bobik deployment

When *RuntimeBroker* is run, the module contacts a C&C server and downloads a configuration file defining targets for DDoS attacks. The module then starts the attacks using a defined count of threads, usually five threads.

The detailed workflow of the *Bobik* deployment is shown below. The *RedLine Stealer Cryptic* (installer) deobfuscates the .NET payload of *Bobik's Updater* and injects it into the newly created process of the *.NET ClickOnce Launch Utility* (`AppLaunch.exe`); see steps 1 – 5.



Bobik deployment using RedLine Stealer Cryptic

The same process is used to execute *Bobik's RuntimeBroker* (the DDoS module), because the dropped *RuntimeBroker* is also packaged and obfuscated via *RedLine Stealer Cryptic*. Therefore, the dropped *Bobik's RuntimeBroker* also deobfuscates the .NET payload of *Bobik's RuntimeBroker* and injects it into another `AppLaunch` process; see steps 6 – 8. After all these steps, the Bobik's DDoS module is deployed, persistent, and ready to attack.

C&C Servers and Communication

Since June 1, 2022, we have observed Bobik's network activities. *Bobik bots* communicate with C&C servers located in Russia and Romania. These two servers are already offline. However, another Romanian server is still active and able to send commands to the bots.

C&C Servers

Since tracking the botnet activity, we have captured three production C&C servers controlling *Bobik bots* and one development server. The servers run on OS Ubuntu with Nginx (v 1.18.0). RiskIQ reports all servers as malicious with self-signed certificates and servers with bad reputations that previously hosted many suspicious services.

Server 1

The last active server is `2.57.122.243`, located in Romania, and its first Bobik's activity we saw was on June 13, 2022. We also have two DNS records for this malicious server: `v9agm8uwtjmz.sytes.net` and `q7zemy6zc7ptaeks.servehttp.com`.

Server 2

The second server `2.57.122.82` is also in Romania, but the communication with the *Bobik bots* was deactivated around July 14, 2022. The server is still active. Nevertheless, the server responds with a `502 HTTP` code (Bad Gateway). Based on the findings from **Server 1**, this server used the same `v9agm8uwtjmz.sytes.net` DNS record, which was reconfigured to **Server 1** in the middle of June.

Server 3

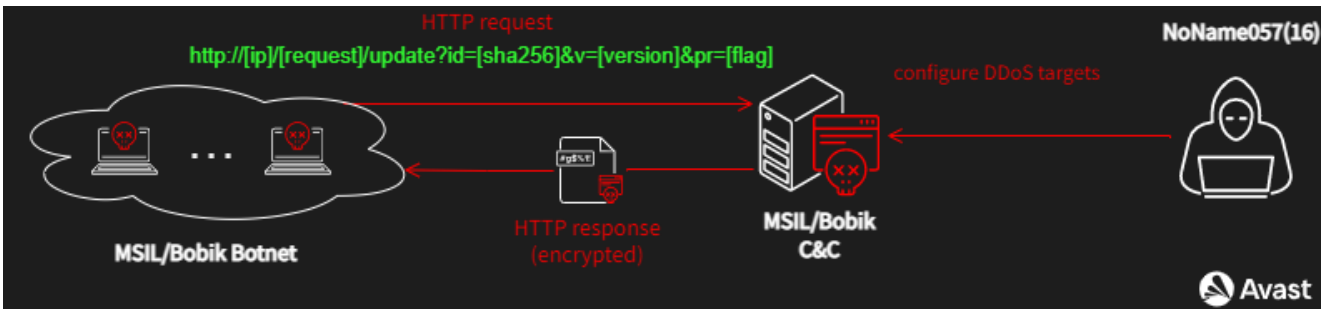
The first Bobik's C&C server we saw was `77.232.41.206` in Russia. The server had opened ports `80` and `443` until June 9, 2022. It is not usable, and therefore *de facto* offline, by *Bobik bots* because there is only one opened port for OpenSSH since *Bobik* requires port `80` for its C&C communication.

Dev Server

One of the C&C servers is a suspected development server at `109.107.181.130`, listening on port `5001`. The server has been active since April and is located in Russia; its reputation is also suspicious. Avast has not detected any hits for this server in the wild. However, one Python sample uses the server as a testing environment.

C&C Communication

The communication between *Bobik bots* and the C&C servers is mediated using a simple unsecured HTTP request and response via the Nginx web server. The bots obtain appropriate commands from the C&Cs utilizing a URL, see the diagram below.



HTTP communication

Request

The request URL uses the following template:
`http://[ip]/[request]/update?id=[sha256]&v=[version]&pr=[flag]`

`ip` : *Bobik bots* hardcode one of the C&C IPs or one of the DNS records, see Section C&C Servers.
`request` : defines the purpose of the communications; we registered three types of requests in the form of a GUID.
– notice: the bots report their states.
– admin: this request can open the admin console of the Nginx web server.

– dropper: is a path to a malicious executable representing *Bobik's RuntimeBroker* followed by an exe file name.
The exact GUIDs are listed in Appendix.
`id` : the hash is computed from Windows Management Instrumentation (WMI) information about a victim's machine like `Win32_DiskDrive`, `Win32_Processor`, `Win32_BaseBoard`, etc. The hash can provide a unique identifier for *Bobik bots*.
`v` : the *Bobik* version; Avast has captured sample versions ranging from 8 to 19.
`pr` : is a flag (0,1) representing whether the communication with C&C has timed out at least once.

A body of the HTTP request contains one simple XML tag with information about the victim; for instance:
`<client a0="1" a1="en-US" a2="en-US" a3="14:03:53" a4="600">; where`

- `a0` : ProductType (1: Workstation, 2: Domain Controller, 3: Server)
- `a1` : CultureInfo.InstalledUICulture
- `a2` : CultureInfo.CurrentUICulture
- `a3` : DateTime.Now
- `a4:` Default timeout for the update of the DDoS target list from the C&C server

See the examples of the notice URLs:

- `http://2.57.122.82/d380f816-7412-400a-9b64-78e35dd51f6e/update?id=AEF97F87751C863548359181B65B60EE86A7D44724040229CDE4622C99AB0B59&v=17&pr=1`
- `http://2.57.122.82/d380f816-7412-400a-9b64-78e35dd51f6e/update?id=67F5318073F09F03E762BF727015384589F00282EA26B1798C10581B8DC27F52&v=16&pr=1`
- `http://v9agm8uwtjmz.sytes.net/d380f816-7412-400a-9b64-78e35dd51f6e/update?id=B5B72AEBEC4E2E9EE0DAC37AC77EBFB679B6EC6D7EE030062ED9064282F404A7&v=18&pr=1`
- `http://q7zemy6zc7ptaeks.servehttp.com/d380f816-7412-400a-9b64-78e35dd51f6e/update?id=BADFD914A37A1FF9D2CBE8C0DBD4C30A9A183E5DF85FCAE4C67851369C2BAF87&v=18&pr=1`

Response

The body of the HTTP response contains an encrypted and gzipped XML file configuring bots to the defined DDoS attacks. See the example below:

```
HTTP/1.1 100 Continue

HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Tue, 07 Jun 2022 17:20:24 GMT
Content-Type: application/octet-stream
Content-Length: 1323
Connection: close

<encrypted-XML>
```

The bot receives the encrypted data that is decrypted using a simple algorithm, as shown below. The full script is located in the IOC repository.

```python
def decrypt(key: bytearray, data: bytes):
    assert len(key) == 256
    array1 = [0] * len(key)
    array2 = [0] * len(key)
    array3 = [0] * len(data)

    for i in range(0, len(key)):
        array1[i] = key[i % len(key)]
        array2[i] = i

    num1 = 0
    for i in range(0, len(key)):
        num1 = (num1 + array2[i] + array1[i]) % 256
        num2 = array2[i]
        array2[i] = array2[num1]
        array2[num1] = num2

    num1 = 0
    num3 = 0
    for i in range(0, len(data)):
        num3+=1
        num3 %= 256
        num1 += array2[num3]
        num1 %= 256
        num2 = array2[num3]
        array2[num3] = array2[num1]
        array2[num1] = num2
        num4 = array2[(array2[num3] + array2[num1]) % 256]
        array3[i] = data[i] ^ num4
    return array3
```

HTTP response decryptor

The encrypted XML file has an elementary structure, as shown below:

```
<config>
   <tasks delay="0" thread_count="-5">
       <task type="http_10" period="0" method="GET" ip="193.59.127.152" port="443" host="www.prezydent.pl"
             path="/kalendarz?query={.,15,20}" response="1" allow_gzip="1" timeout="1000" https="1" id="396782629" />
       <task type="http_10" period="0" method="POST" ip="193.243.159.5" port="443" host="ticket.bus.com.ua"
             path="/user/passwd_recovery" response="1" allow_gzip="1" timeout="1000" https="1"
             body="email={.,5,15}%40gmail.com&amp;ajax=1&amp;fn=passwd_recovery" id="393068713" />
   </tasks>
</config>
```

Decrypted XML config

Most of the XML attributes are intuitive, so we will just explain the compound brackets in the path and body attributes. The configuration often uses dynamically generated pieces (definitions) like this: `{.,15,20}`. The definition dictates what long random text should be generated and in which position.

The definitions are abundantly applied in the path or body of the HTTP requests, where the attackers expect an increased load on the server. The effect is that bots flood servers with meaningless requests. For instance, the first `<task>` in the image directly above (decrypted XML config) uses this definition: `query={.,15,20}` which means that the bots generate random texts of 15 – 20 characters long as requests to, for example, the calendar of Poland's presidential office. Similarly, the second `<task>` flooded the reference system of bus lines in Ukraine with requests for a password reset, as illustrated in this definition `email={.,5,15}%40gmail.com`.

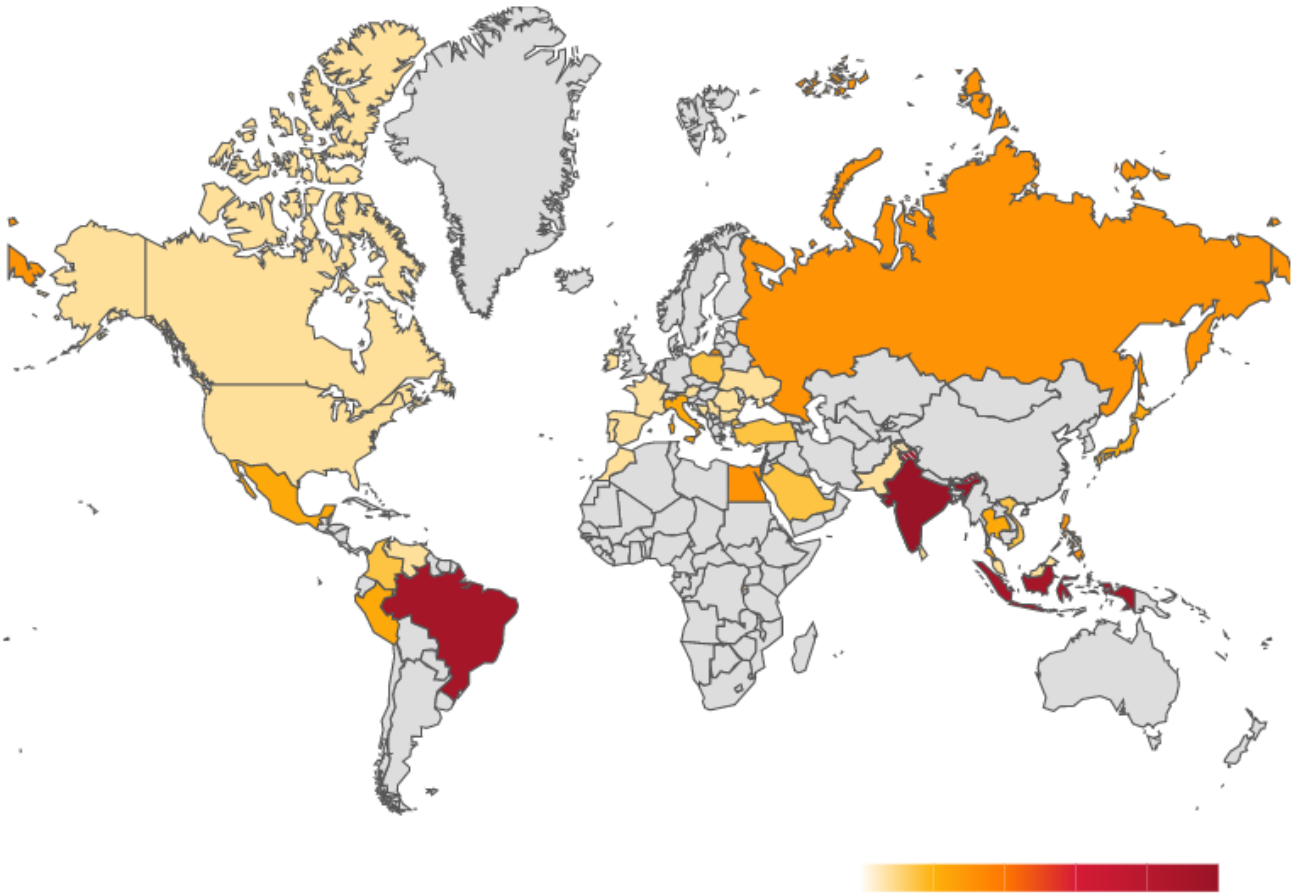
For the most part, we captured definitions sending data to login pages, password recovery sites, and site searches; as can be seen from the XML config snippet below:

- Login data
```
<task
host="identity.tele2.lt"
path="/Account/Login"
body="SkipAutoLogin=False&amp;Username={.,15,20}%40gmail.com&amp;Password=
{.,15,20}&amp"
/>
```
- Search requests
```
<task
host="www.delfi.ee"
path="/otsing?search=
{.,3,12}&amp;domain=kinoveeb.delfi.ee&amp;categoryId&amp;order=PUBLISH_AT&amp;from=2012-
08-22T{d,2,2}%3A{d,2,2}%3A{d,2,2}Z&amp;to=2022-08-22T20%3A59%3A59Z"
/>
```
- Password recovery request
```
<task
host="client.smscredit.lv"
path="/password-recovery"
body="utf8=%E2%9C%93&amp;authenticity_token={.87,87}A%3D%3D&amp;user%5Bemail%5D=
{.,15,20}%40gmail.com&amp;g-recaptcha-response=03ANYolqu{.,539,539}"
/>
```

Consequently, the attackers try to overload a server with these requests, as they are computationally intensive. The requests require many accesses to server databases, e.g., verifying emails for password resetting, trying to login with random data (definitions), etc.

Bobik Botnet

The Avast telemetry data cannot paint a precise picture of the botnet's size, but we can estimate the approximate representation of *Bobik* in the wild, see map below. The map shows where, according to Avast's telemetry, the bots that attempt to carry out DDoS attacks for *NoName057(16)* are located. Avast has protected these devices from *Bobik* or from connecting to the C&C server. Most of the bots are located in Brazil, India, and Southeast Asia.



Distribution of users Avast protected from Bobik

According to our data, the number of *Bobik bots* is a few hundred. However, the total number must be much larger considering the DDoS attacks' acute effectiveness and frequency. We, therefore, estimate there are thousands of *Bobik bots* in the wild.

Selection of DDoS Targets

We estimated a procedure as to how the attackers determine which web servers to DDoS attack because we have configurations of unsuccessful attacks.

The first step is looking for a target that supports Ukraine or a target with anti-Russian views. The attackers analyze the structure of the target's website and identify pages that can cause server overloading, especially requests requiring higher computing time, such as searching, password resetting, login, etc.

The second step is filling in the XML template, encrypting it, and deploying it to the C&C servers. The attackers monitor the condition of the target server and modify the XML configuration based on needs (modification of URL parameters, bodies, etc.) to be more effective. The configuration is changed approximately three times per day.

Suppose the configuration is successful and a targeted server is in trouble. In that case, the configuration is fixed until the web server crashes or a server admins implement anti-DDoS technique or firewall rules based on GeoIP.

If the attack is unsuccessful, a new target is selected, and the whole procedure of selection is repeated.

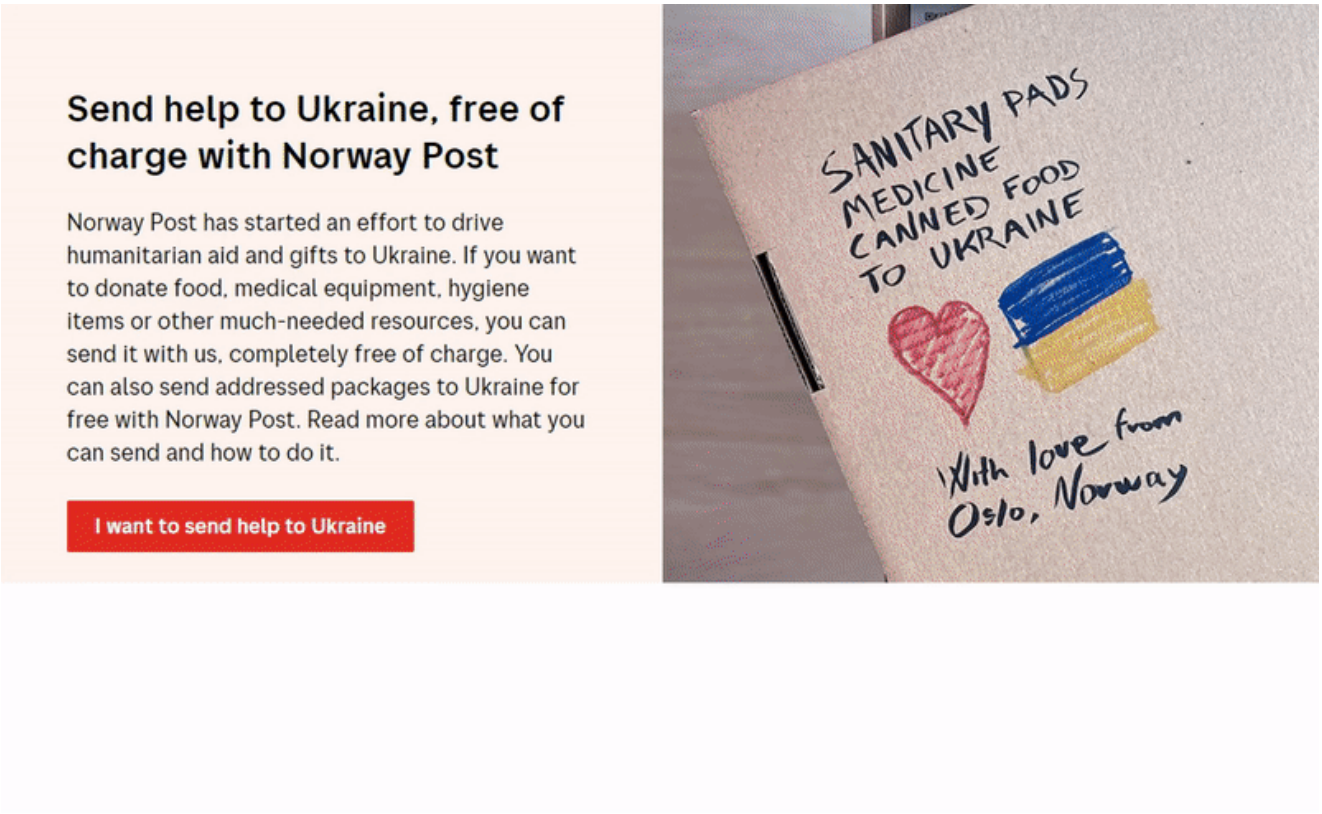
Targets

In the first phase, the attackers targeted Ukrainian news servers they defined as being against the war in Ukraine. Then, the attacks targeted websites belonging to Ukrainian cities, local governments, distribution of electrical power, Ukrainian companies supplying the Ukraine army with weapons, railway, bus, companies, and postal offices.

The second phase targeted organizations publicly supporting Ukraine financially or materially, like Ukraine banks and financial institutions, and operators of local Ukraine gas reservoirs that publicly declared help for the defenders of Ukraine.

As the political situation around the war changed, so did the targets of the DDoS attacks. *Bobik* performed DDoS attacks on GKN Aerospace, which is the supplier of the Northrop Grumman Corporation because the US Defense Department convened a meeting with America's eight prime defense contractors (including Northrop Grumman Corporation) to ensure long-term readiness to meet "Ukraine's weapons needs".

Another global company under attack was Group 4 Securitas (G4S), which published a document assessing and exploring key elements of the conflict in Ukraine. In terms of telecommunications companies, we observed an attack on American telco company Verizon, which declared a waiver of call charges to and from Ukraine. And so, we could continue listing companies that were under *Bobik* attacks due to their support for Ukraine. You can see a few screenshots from affected websites below.



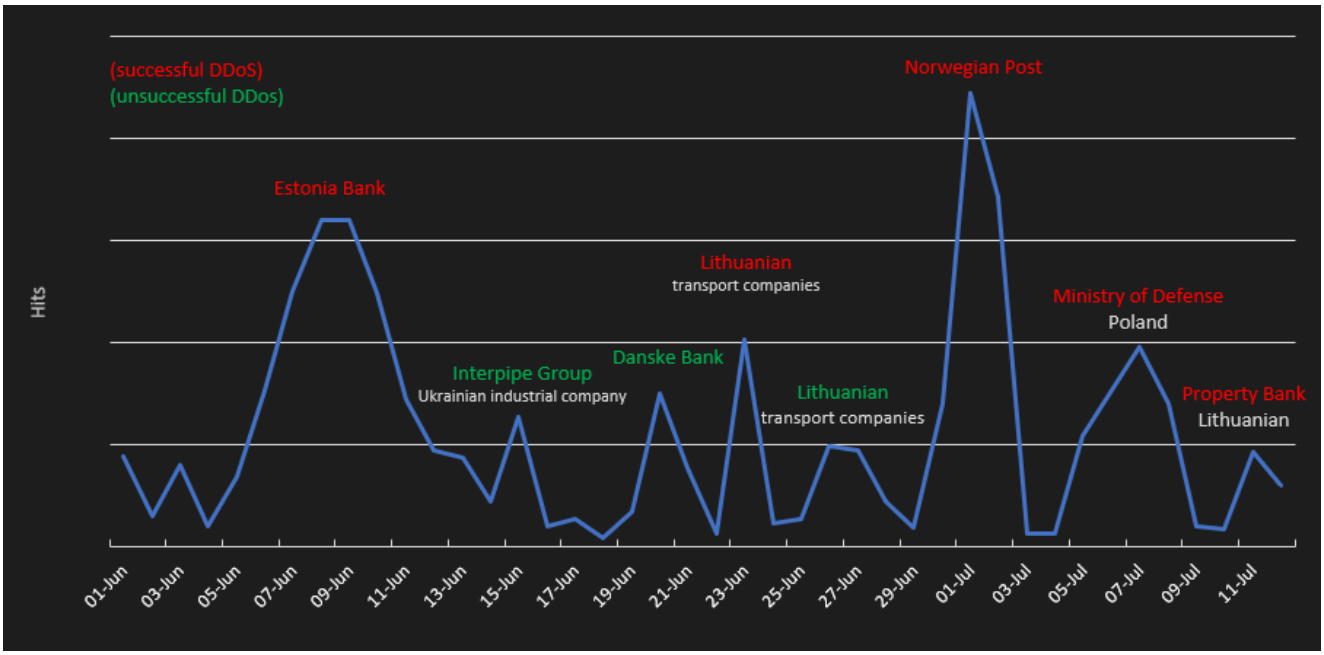
Screenshots of websites supporting Ukraine

Other attacks were more politically motivated based on government declarations of a given country. Baltic states (Lithuania, Latvia, and Estonia) were the significant targets, outside Ukraine, of DDoS attacks carried out by the group. Let's summarize targets outside of Ukraine, chronologically, since we started monitoring *Bobik*.

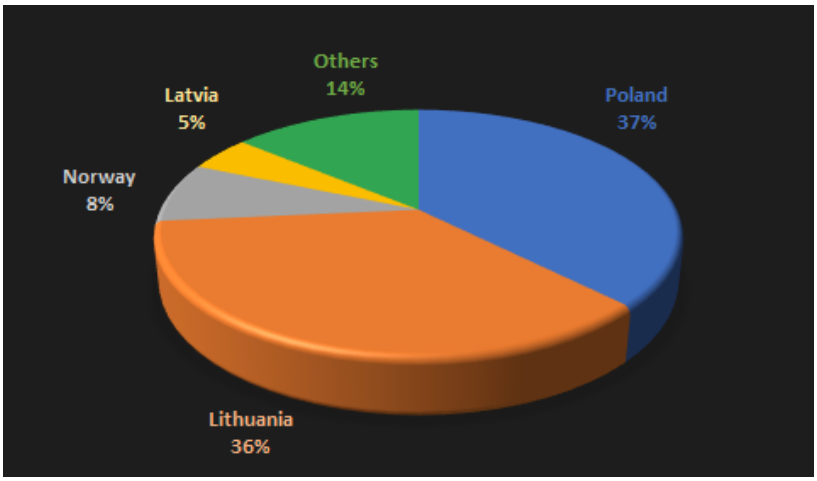
- **June 7, 2022:** Significant DDoS attack on Estonia central bank; see Twitter.

- **June 18, 2022:** *Bobik* configuration changed to target Lithuanian transportation companies, local railway, and bus transportation companies after Lithuanian authorities announced a ban on transit through their territory to the Russian exclave of Kaliningrad of goods that are subject to EU sanctions. The attackers also targeted financial sectors in Lithuania, like UAB General Financing, Unija Litas, and more.
- **July 1, 2022**: Goods were stopped by Norwegian authorities destined for the roughly 400 miners in the town of Barentsburg employed by the Russian state coal mining company Arktikugol. *NoName057(16)'s* DDoS attacks focused on Norwegian websites as retaliation for the blockade. The main targets were transportation companies (Kystverket, Helitrans, Boreal), the Norwegian postal service (Posten), and financial institutions (Sbanken, Gjensidige).
- **July 7, 2022**: There were not any specific acts by Poland that caused the group to specifically target Polish sites. However, Poland has supported Ukraine from the beginning of the Ukraine conflict, and therefore sites in the country became targets. The first wave of DDoS attacks on Polish sites was aimed at government websites like the Polish Cyberspace Resource Center, Polish 56th Air Base, Military Recruitment Center in Chorzów, and more.
- **July 9, 2022**: *Bobik* was reconfigured back to target Lithuanian websites, focusing on energy companies (Ignitis Group, KN), transportation companies (Ingstad & Co, Asstra-Vilnius), and banks (Turto Bankas, Šiaulių Bankas, Swedbank, SEB, Kredito unija Litas).
- **July 25, 2022**: Polish sites were targeted again, this time the Polish government and airports were attacked. We observed a DDoS configuration including the Polish Sejm, Presidential Office, Ministry of National Defense, Poznań Airport, Szczecin Goleniów Airport, Gdansk Airport, Kraków Airport, and more.
- **August 5, 2022**: Polish regional and district courts were targeted.
- **August 9, 2022**: When Finland announced their intention to join NATO, the *Bobik* configuration was reconfigured to target Finnish government institutions, like the Parliament of Finland (Eduskunta), State Council, Finnish police, and more.
- **August 14, 2022:** Latvian financial sector (Latvian Payment Services and Electronic Money, Luminor Interneto bankas) was attacked.
- **August 16, 2022**: The second wave of attacks on the Polish justice system began. We monitored a configuration with specific district courts in Krakow, Olsztyn, Warszawa, Poznan.
- **August 23, 2022**: Estonia's largest news portal, Delfi, was under DDoS attack because it published Russophobic content.
- **August 26, 2022**: The group targeted another Estonian company, Tallink Grupp, a company providing transport services in the northern Baltic Sea region, including air transport. Tallink's airports, such as Kärdla, Tartu, and Pärnu were targeted.
- **August 27, 2022**: Lithuania's ministries of National Defense, Culture, Education, Science and Sports, and Public Procurement Offices were targeted, along with the airports and transport companies.
- **August 29, 2022**: Ukrainian banks were under DDoSed by the group after a long break. We observed Acordbank, Trust capital, JSC Poltava-Bank, and Pravex Bank under attack.
- **September 1 and 2, 2022**: Ukrainian schools were under attack at the beginning of the new school year. Fortunately, none of the group's 14 targets were taken down.
- **September 3, 2022**: Polish armaments plants (Dezamet, Zakłady Mechaniczne Tarnów) and Lithuanian investment companies (Unija Litas, General Financing Bankas) were the group's first victims after their unsuccessful attack attempts on Ukrainian school institutions.
- **September 6, 2022**: The second attempt to attack Ukrainian school institutions (Athens School in Kyiv, Cherkasy National University, First Cambridge Education Center, and more).

The graph below shows a timeline of *Bobik* DDoS attacks, including successful and unsuccessful attacks from the beginning of June to mid-July 2022, captured by Avast telemetry.



Finally, we inspected all hosts from the XML configuration files within our three-month observation period. The pie chart below illustrates that sites from Lithuania and Poland are the main targets of the *NoName057(16)* group.



Looking at the distribution of attacked institutions, courts come in first, and second is logistic companies, followed by banks. The remaining targets are airports, transportation, and logistic companies, governments, and telecommunications companies. A full list of the targets can be found at Appendix.

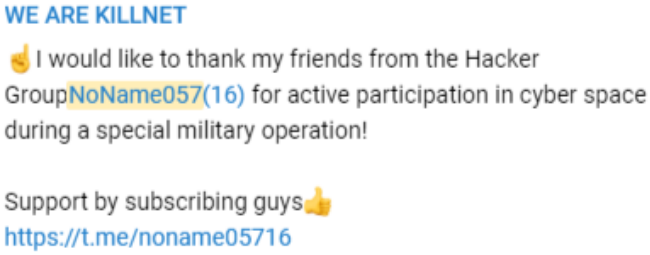
Identifying NoName057(16)

We have tried identifying the hacker group controlling *Bobik bots* and C&C servers. It was evident that the group must be pro-Russia, so we looked for the most famous DDoS attacks.

Shortly after the war in Ukraine began, a pro-Russia hacking group called Killnet appeared and began carrying out DDoS attacks against companies and governments supporting Ukraine, and even targeted the 2022 Eurovision Song Contest.

Bobik initially attacked websites Killnet has marked as “undesirable”. Killnet reports their DDoS attacks on their Telegram account. At first, it looked like the attacks carried out by *Bobik* distantly resembled Killnet’s activity, because the timeline of attacked countries was similar to the XML configurations. However, many successful DDoS attacks by *Bobik* were not posted by Killnet.

On June 21, 2022, the Killnet group publicly thanked a group called *NoName057(16)* for their support during a "special military operation":



When we finished analyzing *NoName057(16)'s* Telegram channel, we confirmed that *NoName057(16)* is responsible for the DDoS attacks performed by the *Bobik bots*. All the XML configurations we captured from the *NoName057(16)* C&C servers exactly match the posts on the Telegram channel.

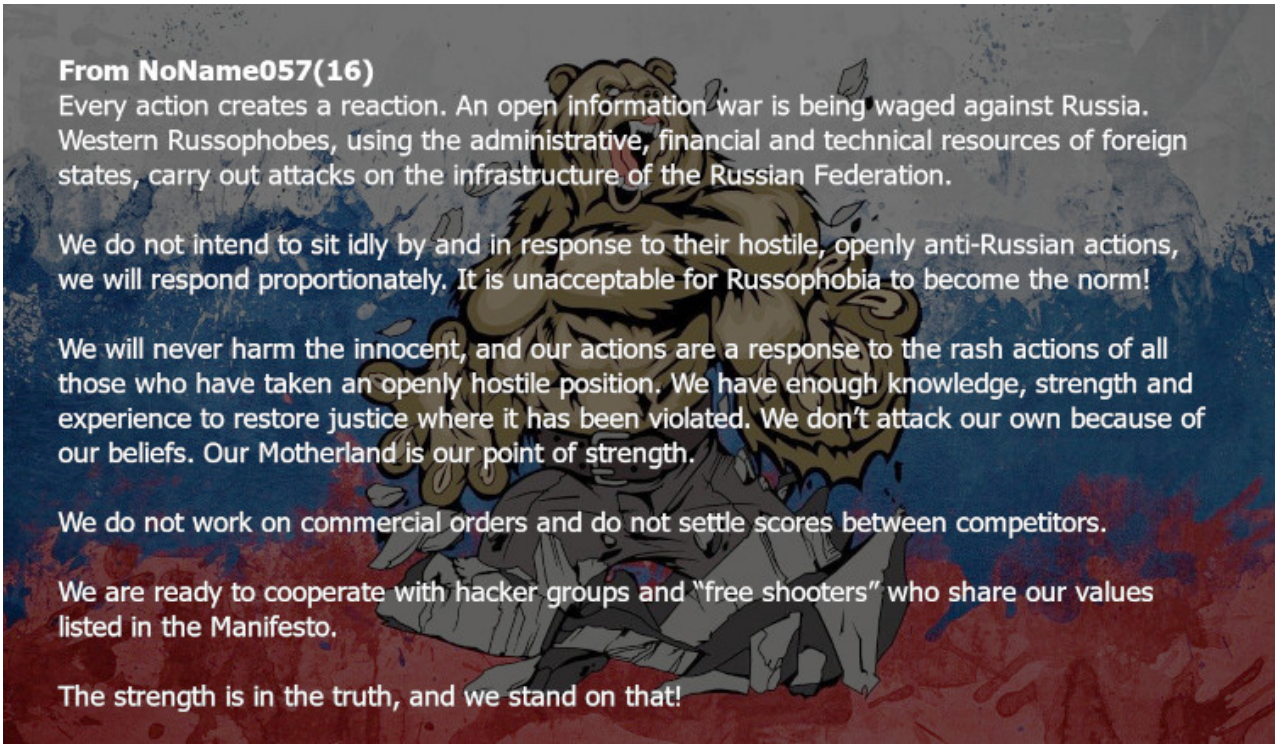
NoName057(16)

NoName057(16) is a little-known pro-Russian hacker group. They boast about their successful attack attempts on their Telegram channel, which has more than 14K subscribers. The group was active before we began tracking them on June 1, 2022. Their Telegram channel was created on March 11, 2022. We suspect they were either using a different set of botnets before June 1, 2022, or updating the malware used to control the bots in June.

NoName057(16) has been threatening to punish "propaganda" sources that "lie" about the Russian "special operation" in Ukraine, as well as governments from neighboring countries supporting them in their fight against Russia. The group became visible in the media at the beginning of August after carrying out successful attacks on Finnish and Polish parliaments.

A Wikipedia page about *NoName057(16)* was created on August 17, 2022. The page summarizes the group's main activity. It classifies the group as a pro-Russia hacker group that claimed responsibility for cyberattacks on Ukrainian, US, and European websites belonging to government agencies, media, and private companies.

NoName057(16) released a manifesto declaring cyberwar as an act of revenge for open information war against Russia:



As the group increased its activities and media profile, it became easier to determine they were behind the attacks. Therefore, we can clearly state that *Bobik* is controlled by the pro-Russian hacker group called *NoName057(16)*.

Success Rate

The group only reports successful DDoS attacks on their Telegram channel. Although the reported number of successful attacks seems large, statistical information indicates the contrary.

The group exclusively concentrates on DDoS attacks. They do not try to steal data or gain access to systems like other dangerous groups. The question is if they have the necessary knowledge, strength, and infrastructure to do more. Carrying out DDoS attacks is straightforward and does not require deep technical knowledge. Furthermore, the *Bobik* implementation only sends a simple HTTP request.

Our three-month observation shows that the group's attack success is **around 40%**. We compared XML configurations captured by Avast to the achievements the group posts on their Telegram channel. Moreover, there is a particular set of targets, making up **~20%** of their posts on Telegram, *NoName057(16)* claimed they successfully attacked, but we did not match them to the targets listed in their configuration files. For example, *NoName057(16)* claims to be responsible for attacking websites belonging to Lithuanian airports on June 25, 2022:

NoName057(16)

Lithuanian airport websites, together with the Internet resource of their directorate, continue to be in "isolation"!

Thanks to our attacks, they are still available only from Lithuanian IP addresses, and their speed, to put it mildly, leaves much to be desired.

Vilnius airport
Kaunas Airport
Airport Palangi
Lietuvos oro uostai ("Lithuanian airports")

We continue to explicitly hint to the Lithuanian authorities that they should immediately withdraw their decision to ban the transit of Russian cargo from the Kaliningrad region to Russia

NoName057(16) claiming to be responsible for a DDoS attack on Lithuanian airports, posted on NoName057(16)'s Telegram channel

However, we did not find any records of the attack in the configuration files. The likelihood of them not using all of their bots in attacks is slim. In addition to this outage, *NoName057(16)* declared the sites were under a continuous fourteen-day attack. This would require an extensive bot network, especially considering the group performed other attacks during the same time frame, and the websites were still offline. From what we have seen, it is unlikely that *NoName057(16)* has an extensive bot network. Moreover, most of their DDoS attacks last a few hours, maximally a few days.

Impact and Protection

The power of the DDoS attacks performed by *NoName057(16)* is debatable, to say the least. At one time, they can effectively strike about thirteen URL addresses at once, judging by configuration history, including subdomains. Furthermore, one XML configuration often includes a defined domain/target as a set of subdomains, so *Bobik* effectively attacks five different domains within one configuration. Consequently, they cannot focus on more domains for capacity and efficiency reasons.

Most of the successful attacks result in servers being down for several hours or a few days. To handle the attacks, site operators often resort to blocking queries coming from outside of their country. It is a typical and suitable solution for local servers/domains such as local ticket portals of local bus/train companies, local institutions/companies, etc. Therefore, the DDoS impact on these domains has a minimal effect on the servers of local and smaller companies. Some operators or owners of affected servers have unregistered their domains, but these are extreme cases.

The DDoS attacks carried out were more difficult to handle for some site operators of prominent and significant domains, such as banks, governments, and international companies. After a successful attack, we noticed larger companies implementing enterprise solutions, like Cloudflare or BitNinja, which can filter incoming traffic and detect DDoS attacks in most cases. On the other hand, most large, international companies expect heavier traffic and run their web servers in the Cloud with anti-DDoS solutions, making

them more resilient to attacks. For example, the group was unsuccessful in taking down sites belonging to Danish bank, Danske Bank (attacked June 19 – 21, 2022), and Lithuanian bank, SEB (attacked July 12 – 13, 2022 and July 20 – 21, 2022).

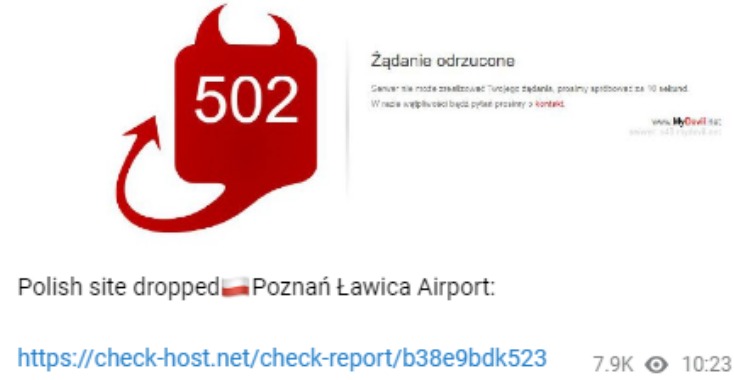
The success of DDoS attacks depends on victim selection. The more "successful" attacks affected companies with simple sites, including about us, our mission, and a contact page, for example. These types of companies do not use their web pages as the main part of their business. These servers are therefore not typically designed to be heavily loaded and do not implement anti-DDoS techniques, making them a very easy target.

The group's DDoS attack on Poznań-Ławica Airport in Poland took the site offline for 16 minutes. *NoName057(16)* configured *Bobik bots* based on the `<tasks>` shown in the screenshot below:

```
<task method="GET"  ip="31.186.81.254" port="443" host="poznanairport.pl" path="/?s={.,15,20}"/>
<task method="POST" ip="31.186.81.254" port="443" host="poznanairport.pl" path="/wp-json/wpf/v1/forms/2828/"
      body="------WebKitFormBoundaryr5DPm0TCB7IDuEV2 Content-Disposition: form-data; name=&quot;email&quot;
            {.,15,20}@gmail.com"/>
<task method="GET"  ip="31.186.81.254" port="443" host="poznanairport.pl" path="/wp-json/api/v1/blog/?page={.,1,2}"/>
```

XML configuration for Poznań-Ławica Airport

They tried to overload the server with requests for searching, form submitting, and getting data via WordPress API. When the server started to return `502 errors`, *NoName057(16)* did not forget to brag on their Telegram channel. They also included a link to check-host.net to prove their "revenge".



NoName057(16)'s Telegram post related to their DDoS attack on Poznań-Ławica Airport

However, affected servers very often run back online within several minutes if they implement some anti-DDoS techniques because the algorithms learn to recognize the given type of attacks. The check-host.net report below demonstrates that the DDoS attack on Poznań-Ławica Airport had a minimal impact since the website was offline for 16 minutes.

Check website https://poznanairport.pl/

Checked on Tue Jul 26 08:18:40 UTC 2022 | Check again

Location	Result	Time	Code	IP address
Czechia, C.Budejovice	Server error	0.116 s	502 (Bad Gateway)	31.186.81.254
Finland, Helsinki	Server error	0.164 s	502 (Bad Gateway)	31.186.81.254
Germany, Frankfurt	Server error	0.089 s	502 (Bad Gateway)	31.186.81.254
Hong Kong, Hong Kong	Server error	4.333 s	502 (Bad Gateway)	31.186.81.254
Iran, Tehran	Server error	1.216 s	502 (Bad Gateway)	31.186.81.254
Italy, Milan	Server error	0.226 s	502 (Bad Gateway)	31.186.81.254
Kazakhstan, Karaganda	Server error	0.483 s	502 (Bad Gateway)	31.186.81.254
Lithuania, Vilnius	Server error	0.229 s	502 (Bad Gateway)	31.186.81.254
Moldova, Chisinau	Server error	0.234 s	502 (Bad Gateway)	31.186.81.254
Netherlands, Amsterdam	Connection timed out			31.186.81.254
Poland, Olsztyn	Server error	0.064 s	502 (Bad Gateway)	31.186.81.254
Portugal, Viana	Server error	0.265 s	502 (Bad Gateway)	31.186.81.254
Russia, Moscow	Server error	0.261 s	502 (Bad Gateway)	31.186.81.254
Russia, Moscow	Server error	0.261 s	502 (Bad Gateway)	31.186.81.254
Serbia, Belgrade	Server error	0.207 s	502 (Bad Gateway)	31.186.81.254
Switzerland, Zurich	Server error	0.288 s	502 (Bad Gateway)	31.186.81.254
Turkey, Istanbul	Server error	0.309 s	502 (Bad Gateway)	31.186.81.254
UK, Kettering	Server error	0.178 s	502 (Bad Gateway)	31.186.81.254
Ukraine, Khmelnytskyi	Server error	0.185 s	502 (Bad Gateway)	31.186.81.254
Ukraine, Kyiv	Server error	0.161 s	502 (Bad Gateway)	31.186.81.254
USA, Atlanta	Server error	1.286 s	502 (Bad Gateway)	31.186.81.254
USA, Los Angeles	Server error	0.822 s	502 (Bad Gateway)	31.186.81.254

Check website https://poznanairport.pl

Checked on Tue Jul 26 08:34:46 UTC 2022 | Check again

Location	Result	Time	Code	IP address
Czechia, C.Budejovice	OK	0.701 s	200 (OK)	31.186.81.254
Finland, Helsinki	OK	0.898 s	200 (OK)	31.186.81.254
Germany, Frankfurt	OK	0.430 s	200 (OK)	31.186.81.254
Hong Kong, Hong Kong	OK	6.752 s	200 (OK)	31.186.81.254
Iran, Tehran	OK	2.044 s	200 (OK)	31.186.81.254
Italy, Milan	OK	0.659 s	200 (OK)	31.186.81.254
Kazakhstan, Karaganda	OK	1.997 s	200 (OK)	31.186.81.254
Lithuania, Vilnius	OK	1.081 s	200 (OK)	31.186.81.254
Moldova, Chisinau	OK	1.128 s	200 (OK)	31.186.81.254
Netherlands, Amsterdam	OK	0.414 s	200 (OK)	31.186.81.254
Poland, Olsztyn	OK	0.492 s	200 (OK)	31.186.81.254
Portugal, Viana	OK	1.334 s	200 (OK)	31.186.81.254
Russia, Moscow	OK	1.423 s	200 (OK)	31.186.81.254
Russia, Moscow	OK	1.306 s	200 (OK)	31.186.81.254
Serbia, Belgrade	OK	1.027 s	200 (OK)	31.186.81.254
Switzerland, Zurich	OK	0.680 s	200 (OK)	31.186.81.254
Turkey, Istanbul	OK	2.027 s	200 (OK)	31.186.81.254
UK, Kettering	OK	0.466 s	200 (OK)	31.186.81.254
Ukraine, Khmelnytskyi	OK	1.094 s	200 (OK)	31.186.81.254
Ukraine, Kyiv	OK	0.800 s	200 (OK)	31.186.81.254
USA, Atlanta	OK	2.049 s	200 (OK)	31.186.81.254
USA, Los Angeles	OK	2.178 s	200 (OK)	31.186.81.254

Check-host.net report for the DDoS attack on Poznań-Ławica Airport, which took the site offline for 16 minutes

On June 23, 2022, *NoName057(16)* reported on Telegram that Lithuanian authorities lifted a ban on the transit of Russian cargo to Kaliningrad. The group attributes the lifting of the ban, amongst other things, to the efforts of their cyber attacks on Lithuania's infrastructure, which is debatable at best. However, the attacks on Lithuanian servers have continued.

Performance

The botnet went into an idle state on September 1, 2022, at 6 PM UTC, and remained idle persisted for 12 hours. The botnet was reactivated on September 2, 2022, at 4 AM UTC. The XML file sent to the bots contained empty `<tasks>`, like in this example: `<config><tasks delay="0" thread_count="-6"/></config>`

A decline in the botnet's performance may be a possible explanation for this. The group only posted two general posts to their Telegram channel on September 1 and 2, 2022, instead of boasting about successful attacks, our first indication the botnet might not be performing well.

The first post was about the beginning of the new school year and day of knowledge. The group also mentioned being on the defense of the cyber front for their country and the for the safety of the younger generation. The second post was about "information guns and DDoS tanks" that worked quietly on very difficult and important work.

In fact, *NoName057(16)* changed targets ten times each day in the XML configurations, which is abnormal. We monitored the targets for these days, and none of the attacks were successful. Therefore, it is evident that the botnet had some trouble.

Most of the sites attacked by the group have implemented anti-DDoS protections. This slowdown implies that the botnet is relatively static without many changes, such as recruiting new bots or dynamically changing bots' IPs. A static botnet is an advantage for anti-DDoS protections, because malicious traffic can be easily identified.

NoName057(16) has continued to attack other easier targets since September. Only the future will reveal the Bobik botnet's successes and failures. However, the attack's success rate has been only around 25% since the beginning of September.

Conclusion

We investigated and analyzed malware used to carry out DDoS attacks on sites in and around Ukraine, starting in June, 2022. We identified the malware as a .NET variant of a RAT called *Bobik*, including a DDoS module, and spreading via a bot-net-as-a-service, *RedLine Stealer*.

The first technical part of this investigation uncovered C&C servers and the HTTP communication protocol used by the *Bobik bots*. We also successfully decrypted the HTTP protocol, including its parameters. This allowed us to monitor the C&C servers and collect information about the botnet architecture and XML configurations defining the DDoS targets.

The second aim was to determine the bad actors behind the attacks. We identified a pro-Russian hacker group called *NoName057(16)*, as the users or possibly even the authors of *Bobik*, based on the XML configurations and what the group posts to their Telegram channel.

NoName057(16) focuses exclusively on DDoS attacks and looks for companies and organizations that support Ukraine or are “anti-Russian”. They do not try to steal data or gain access to the system like other dangerous groups. Therefore, we can declare that their activities are only harmful in the sense that they can lose companies’ business while their sites are offline, but attacked sites that have gone offline have luckily recovered quickly. Their activities are more annoying than dangerous.

We found that the successful attacks defined by *NoName057(16)* make up just ~ 40% of all of their attack attempts. The success of their attacks depends on the quality of the targeted infrastructure. The evidence suggests that well-secured and designed servers can withstand the group’s DDoS attacks.

The group focuses on servers/domains as retaliation for cyber-attacks and sanctions on Russia. All successful attacks, and even successful attacks the group is not responsible for (but claims to be), are posted to their Telegram channel.

If you are concerned your device might be infected with *Bobik* and supporting NoName057(16)’s efforts, we highly recommend you install security software, like Avast Antivirus, which detects, blocks and can remove *Bobik*.

IOCs

The full list of IoCs is available in the IOC repository

Appendix

GUIDS

```
http://[ip]/[request]/update?id=[sha256]&v=[version]&pr=[flag]
```

[request]	value
notice	bcaa8752-51ff-4e35-8ef9-4aefbf42b482 d380f816-7412-400a-9b64-78e35dd51f6e
admin	27bff71b-42c0-4a47-ba39-04c83f2f40bb

dropper
fb82275d-6255-4463-8261-ef65d439b83b/<file_name>

<**file_name**>
Q7yheyG7.exe
afVAcUJTvDvM.exe
XuS1qxZa.exe
AdminService.exe
Q7yheyG7.exe
xLZ6auza.exe
BAebY2lBT7ee.exe

Bobiks' Targets

Website-URL	Company Name	Company Type	Country
22-09-06			
auth.cdu.edu.ua	Cherkasy National University	Education	Ukraine
back.libera.school	Online school Libera School	Education	Ukraine
cdo.org.ua	Distance Education Center	Education	Ukraine
chat.cdo.org.ua	Distance Education Center	Education	Ukraine
check.cambridge.ua	First Cambridge Education Centre	Education	Ukraine
company.shodennik.ua	Schodennyk	Education	Ukraine
courses.prometheus.org.ua	Prometheus	Education	Ukraine
do.mlt.gov.ua	Education Online	Education	Ukraine
education.umj.com.ua	Ukraininan Medical Journal	Healthcare	Ukraine
learn.lifeschool.org.ua	Kids Life School	Education	Ukraine
libera.school	Libera School	Education	Ukraine
osvita.diia.gov.ua	Diia. Digital Education	Education	Ukraine
school.angstremua.com	Lyceum Angstrom	Education	Ukraine
school.meridian.com.ua	Meridian School	Education	Ukraine
ukr.voshozdenieschool.com.ua	Private general education distance school	Education	Ukraine
vumonline.ua	VUM Online	Education	Ukraine
www.athens.kiev.ua	School of Athens	Education	Ukraine
www.mathema.me	Matema	Education	Ukraine

Full list of the targets can be found in the IOC repository

References

[1] Threat Encyclopedia
[2] US Defense Department convened a meeting with America's eight prime defense contractors
[3] Ukraine Conflict Overview And Impact To Security In The UK
[4] Verizon Waives Calling Charges to and From Ukraine
[5] Kaliningrad sanctions to take effect, Lithuania says
[6] Norway Greenlights Blocked Goods for Russian Arctic Miners
[7] Hacker wars heat up as the pro-Russian Killnet attacks Italy
[8] What is known about the Russian hacker group NoName057(16), which hacked the website of the Finnish Parliament?
[9] Russian hacker group NoName057 (16) attacks Poland and Finland
[10] Wikipedia – NoName057(16)

Tagged asddos, malware