TA402 Uses Complex IronWind Infection Chains to Target Middle East-Based Government Entities

: 11/7/2023

November 14, 2023 Joshua Miller and the Proofpoint Threat Research Team

Key takeaways

- From July through October 2023, Proofpoint researchers observed TA402 engage in phishing campaigns that delivered a new initial access downloader dubbed IronWind. The downloader was followed by additional stages that consisted of downloaded shellcode.
- During the same period, TA402 adjusted its delivery methods, moving from using Dropbox links to using XLL and RAR file attachments, likely to evade detection efforts.
- This threat actor has consistently engaged in extremely targeted activity, pursuing less than five organizations with any single campaign. They have also maintained a strong focus on government entities based in the Middle East and North Africa.
- Proofpoint has tracked TA402 since 2020. Our researchers assess the threat actor is a Middle Eastern advanced persistent threat (APT) group that historically has operated in the interests of the Palestinian Territories and overlaps with public reporting on Molerats, Gaza Cybergang, Frankenstein, and WIRTE.

Overview

In mid-2023, Proofpoint researchers first identified TA402 (Molerats, Gaza Cybergang, Frankenstein, WIRTE) activity using a labyrinthine infection chain to target Middle Eastern governments with a new initial access downloader Proofpoint has dubbed IronWind. From July through October 2023, TA402 utilized three variations of this infection chain—Dropbox links, XLL file attachments, and RAR file attachments—with each variant consistently leading to the download of a DLL containing the multifunctional malware. In these campaigns, TA402 also pivoted away from its use of cloud services like Dropbox API, which Proofpoint researchers observed in activity from 2021 and 2022, to using actor-controlled infrastructure for C2 communication.

As of late October 2023, Proofpoint researchers had not observed any changes in targeting by TA402, an APT group that historically has operated in the interests of the Palestinian Territories, nor identified any indications of an altered mandate despite the current conflict in the region. It remains possible that this threat actor will redirect its resources as events continue to unfold.

Campaign details and IronWind

July 2023 Activity: In July 2023, Proofpoint researchers observed the first of TA402's new, more convoluted infection chain as compared to prior campaign activity from 2021 and 2022 (Figures 1 and 2).

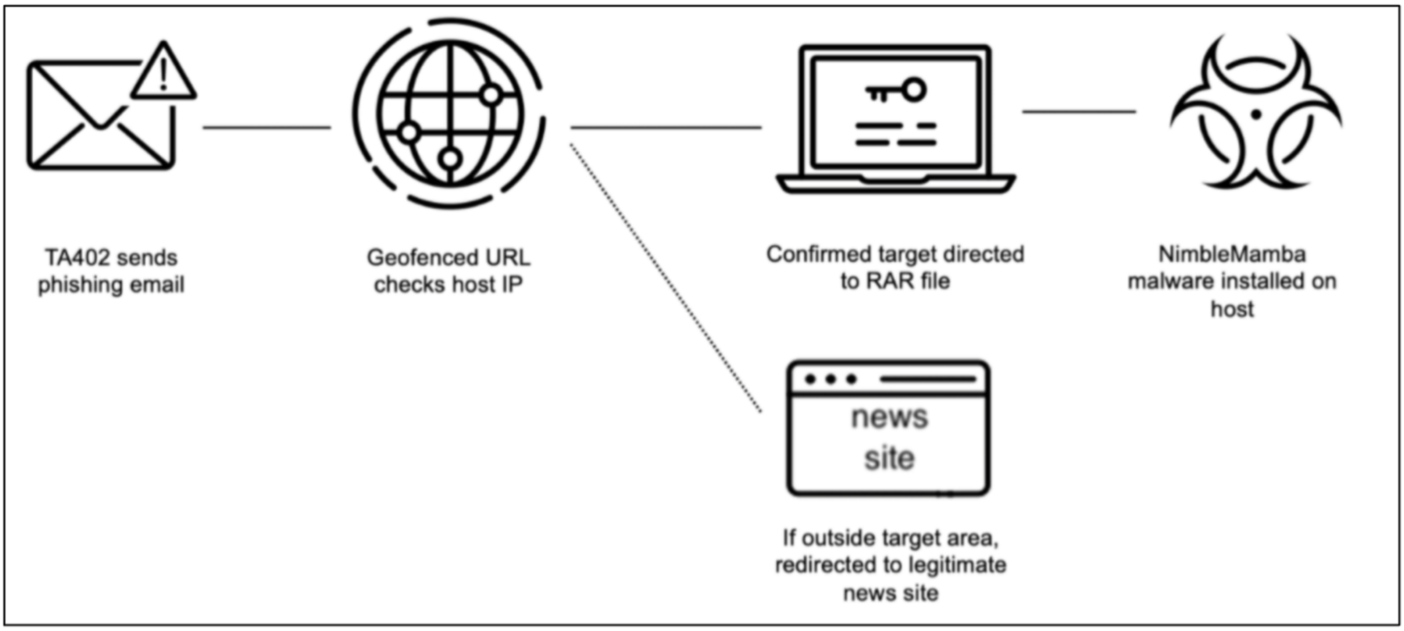
TA402 sends phishing email
Geofenced URL checks host IP
Confirmed target directed to RAR file
NimbleMamba malware installed on host
news site
If outside target area, redirected to legitimate news site

Figure 1. TA402 infection chain used from November 2021 to January 2022.

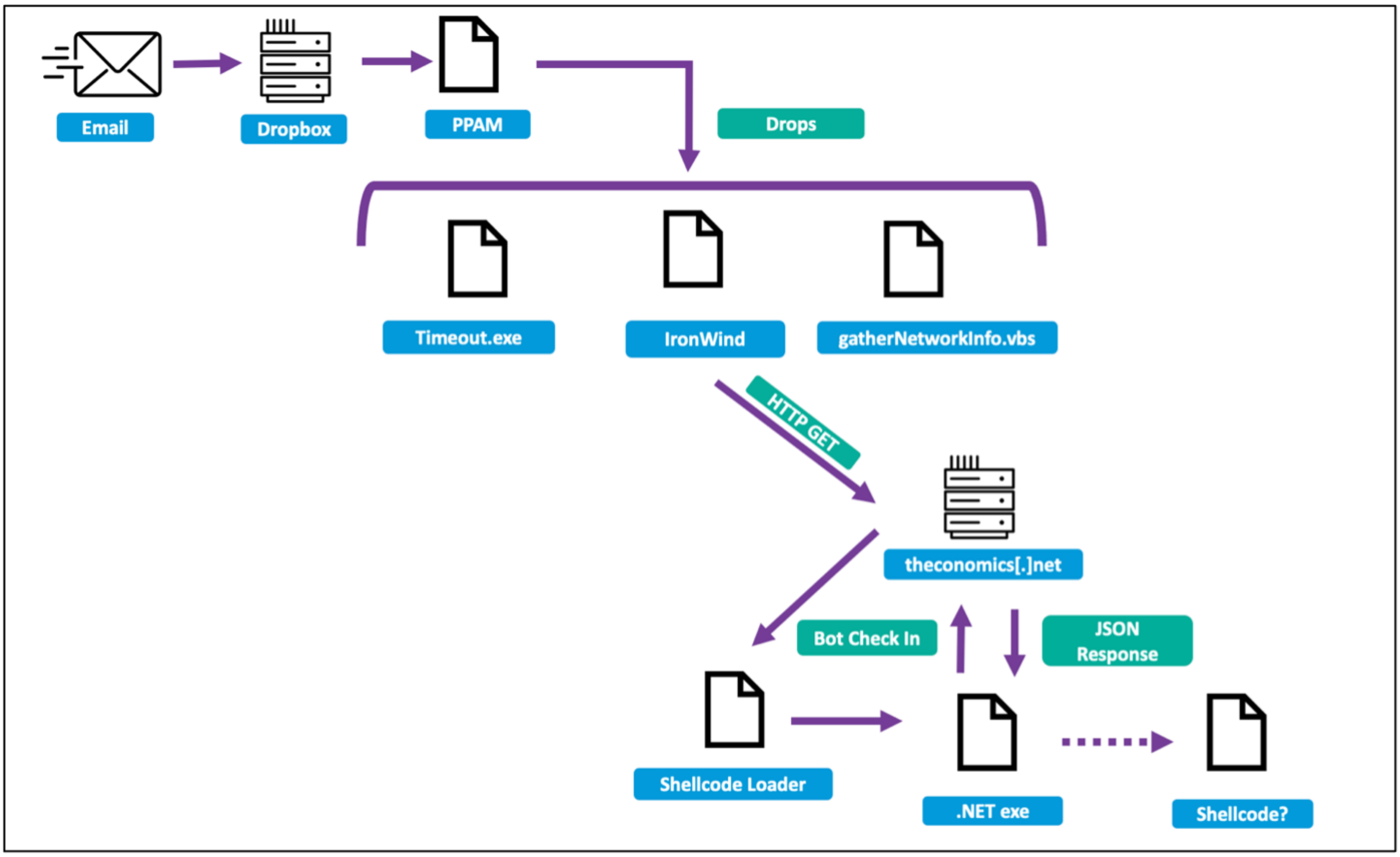

Figure 2. TA402 infection chain used in July 2023 campaign.

TA402 engaged in a phishing campaign using a compromised Ministry of Foreign Affairs email account to target Middle Eastern government entities. The emails used an economic-themed social engineering lure ("برنامج التعاون الإقتصادي مع دول مجلس التعاون الخليجي 2023-2024" [Machine Translation: Economic cooperation program with the countries of the Gulf Cooperation Council 2023-2024"]) to deliver a Drobox link that downloaded a malicious Microsoft PowerPoint Add-in (PPAM) file. The PPAM file contained a macro that dropped three files: version.dll (IronWind), timeout.exe, and gatherNetworkInfo.vbs. Timeout.exe was used to sideload IronWind. Once sideloaded, IronWind sent an HTTP GET request to a known TA402 C2 domain, theconomics[.]net, which was hosted on 191.101.78[.]189 at the time of analysis in August 2023. Proofpoint researchers have observed TA402 leveraging Dropbox for malware delivery since at least December 2021.

After receiving the HTTP GET request, the C2 responded with shellcode that represented the third stage of the infection chain. During Proofpoint's analysis, the shellcode used reflective .NET loaders to conduct WMI queries. The shellcode also served as a multipurpose loader, downloading the fourth stage—a .NET executable that used SharpSploit, a .NET post-exploitation library written in C#.

The .NET executable continued to use HTTPS POSTs and GETs to theconomics[.]net for C2 and received JSON responses. It passed authentication via a custom UserAgent string, "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:<tag>) Gecko/<auth> Firefox/3.15" and almost certainly would have downloaded additional shellcode payloads. Based on Proofpoint analysis, this UserAgent is unique enough to be used for detection purposes. Proofpoint researchers did not observe the fifth stage at the time of analysis but took note that the last stage payload contained unused code, suggesting TA402 may be making further updates and adjustments to the malware.

August 2023 activity: In August 2023, TA402 shifted to sending an attached XLL file to load IronWind using “قائمة الأشخاص والكيانات (المصنفة إرهابية) من قبل هيئة مكافحة غسيل الأموال وتمويل الإرهاب” as a lure instead of using a malicious PPAM file delivered via Drobox. The machine translation of the lure is as follows: “List of persons and entities (designated as terrorists) by the Anti-Money Laundering and Terrorist Financing Authority.” TA402 used the same compromised Ministry of Foreign Affairs email account observed in the July activity. As part of the initial infection process, TA402 sent a base64 encoded check in to Request Inspector—a third-party service for creating endpoints for HTTP requests—to exfiltrate some system information.

October 2023 activity: In October 2023, TA402 shifted a portion of its infection chain yet again. This time the threat actor sent a RAR file attachment that contained a renamed version of tabcal.exe for sideloading IronWind and propsys.dll (IronWind) instead of using a malicious PPAM file delivered via Dropbox or an attached XLL file to load the malware. The delivered malware again used Request Inspector for initial check in and a new TA402 C2 domain, inclusive-economy[.]com.

TA402 also continued to leverage a compromised Ministry of Foreign Affairs email account to send phishing emails with the lure "تقريــر وتوصيــات الـدورة (110) بخصوص الحرب على غزة,” which translates to “Report and Recommendations of the 110th Session on the War on Gaza.” Currently, TA402 only appears to be using the conflict for lure purposes. Additionally, TA402 continues to phish, indicating the conflict has not significantly disrupted the group’s operations.

IronWind: PDB analysis

During malware analysis, Proofpoint researchers identified TA402 had failed to sanitize the group’s PDB paths during malware development for multiple stages. A YARA rule for hunting purposes is attached at the end of this blog.

Based on the following PDB paths, Proofpoint researchers assess with moderate confidence that the IronWind malware project name is \tornado\ and malware development is broken out by function, including IA (the IronWind dropper), stager (the stager DLL), and payloads.

- VT Stage 1: C:\Users\Win\Desktop\Reno\NewTor\27-07-2023\tornado\tornado\Payloads\BAR_33\I.A\out\IA.pdb
- July 2023 Stage 2: C:\Users\User\Desktop\tornado\Payloads\WKS_10\I.A\out\stagerx64.pdb
- August 2023 Stage 1: C:\Users\Win\Desktop\Reno\NewTor\27-07-2023\tornado\tornado\Payloads\BAR_38\I.A\out\IA.pdb
- August 2023 Stage 2: C:\Users\Win\Desktop\Reno\NewTor\NewIA-Tornado-WithStealer\Payloads\KIL_03\I.A\out\stagerx64.pdb
- Stage 4: K:\prj\WIP\C# - Payload\Client-Side\https\client-Divided\KALV\obj\Release\KALV.pdb

Geofencing

TA402 regularly employs geofencing techniques to make detection of its malicious activity more difficult. This aspect of the threat actor’s tactics, techniques, and procedures has remained consistent since at least 2020. Even with the more elaborate infection chains observed in 2023, TA402 continues to include URLs that will at times redirect to decoy documents hosted on legitimate document hosting platforms if the geofencing is not bypassed.

Attribution

Proofpoint researchers attributed the campaigns to TA402 based on tactics, techniques, and victimology. The 2023 campaigns share similarly themed lures as historical TA402 activity and retain a focus on Arabic-speaking targets located in the Middle East. Over the years, TA402 has consistently targeted government entities based in the Middle East and North Africa, at times going after the same targets repeatedly. TA402's use of compromised Ministry of Foreign Affairs email accounts, geofencing, and decoy documents additionally contributed to the attribution.

Proofpoint researchers also assess TA402 operates in support of Palestinian espionage objectives with a focus on intelligence collection. This is consistent with prior Proofpoint published reports on this threat actor. While Proofpoint recognizes that TA402 overlaps with a number of publicly reported threat actors, including Molerats, WIRTE, and Frankenstein, Proofpoint researchers cluster independently based on internal malware analysis and investigations.

Conclusion

Based on Proofpoint's tracking of this threat actor since 2020, TA402 remains a persistent and innovative threat actor that routinely retools its attack methods and malware in support of its cyber espionage mandate. Its ongoing use of geofencing and decoy documents continues to serve its detection evasion efforts. While TA402 is an intelligence collection focused threat actor with a specific interest in Middle Eastern and North African government entities, the group could find itself under direction to adjust its targeting or social engineering lures in reaction to the ongoing Israel-Hamas conflict.

Indicators of Compromise (IOCs)

INDICATOR	TYPE
9b2a16cbe5af12b486d31b68ef397d6bc48b2736e6b388ad8895b588f1831f47 5d773e734290b93649a41ccda63772560b4fa25ba715b17df7b9f18883679160 19f452239dadcd7544f055d26199cb482c1f6ae5486309bde1526174e926146a A4bf96aee6284effb4c4fe0ccfee7b32d497e45408e253fb8e1199454e5c65a3 26cb6055be1ee503f87d040c84c0a7cacb245b4182445e3eee47ed6e073eca47 cbb89aac5a2c93a02305846f9353b013e6703813d4b6baff8eb89ee938647af3 c98dc0b930ea67992921d9f0848713deaa5bba8b4ba21effd0b00595dd9ed28c ac227dd5c97a36f54e4fa02df4e4c0339b513e4f8049616e2a815a108e34552f 6ab5a0b7080e783bba9b3ec53889e82ca4f2d304e67bd139aa267c22c281a368 e2ba2d3d2c1f0b5143d1cd291f6a09abe1c53e570800d8ae43622426c1c4343c d8cde28cf2a5884daddf6e3bc26c80f66bc3737e426b4ba747d49d154999fbc1 81fc4a5b1d22efba961baa695aa53201397505e2a6024743ed58da7bf0b4a97f 3b2a6c7a39f49e790286185f2d078e17844df1349b713f278ecef1defb4d6b04	SHA256

7bddde9708118f709b063da526640a4132718d3d638505aafce5a20d404b2761 883e035f893483b9921d054b3fa014cef90d90b10dcba7d342def8be2e98ce3c 4b0a48d698240504c4ff6275dc735c8162e57f92224fb1d2d6393890b82a4206 4018b462f2fcf1b0452ecd88ab64ddc5647d1857481f50fa915070f5f1858115 3d80ea70b0c00d12f2ba2c7b1541f7d0f80005a38a173e6962b24f01d4a2a1de	
theconomics[.]net |191.101.78[.]189	Domain | IP (C2)
inclusive-economy[.]com healthcaption[.]com	Domains

ET Signatures

YARA Rule

```
rule TA402_PDB

{ meta:

    author = "Proofpoint inc."

    description = "Finds TA402 related PDB paths"

    date = “2023-09-27”

  strings:

$pdb1 = "C:\\Users\\Win\\Desktop\\Reno\\NewTor" ascii wide

$pdb2 = "C:\\Users\\User\\Desktop\\tornado\\" ascii wide

$pdb3 = "K:\\prj\\WIP\\C# - Payload\\Client-Side\\https\\client-Divided\\KALV\\obj\\Release\\KALV.pdb" ascii wide

$pdb4 = "K:\\prj\\WIP\\C# - Payload\\Client-Side" ascii wide

  condition:

any of them

}
```