Arid Viper APT targets Palestine with new wave of politically themed phishing attacks, malware

blog.talosintelligence.com/2022/02/arid-viper-targets-palestine.html

By Asheer Malhotra and Vitor Ventura.

- Cisco Talos has observed a new wave of Delphi malware called Micropsia developed and operated by the Arid Viper APT group since 2017.
- This campaign targets Palestinian entities and activists using politically themed lures.
- The latest iteration of the implant contains multiple RAT and information gathering capabilities.

Executive summary

Cisco Talos has identified a new wave of what is believed to be an ongoing campaign using the Delphi malware since 2017. Talos believes with high confidence that this is the work of the Arid Viper threat actor. This is a group believed to be based out of Gaza that's known to target organizations all over the world. The actor uses the Micropsia implant in the most recent wave that started around October 2021.

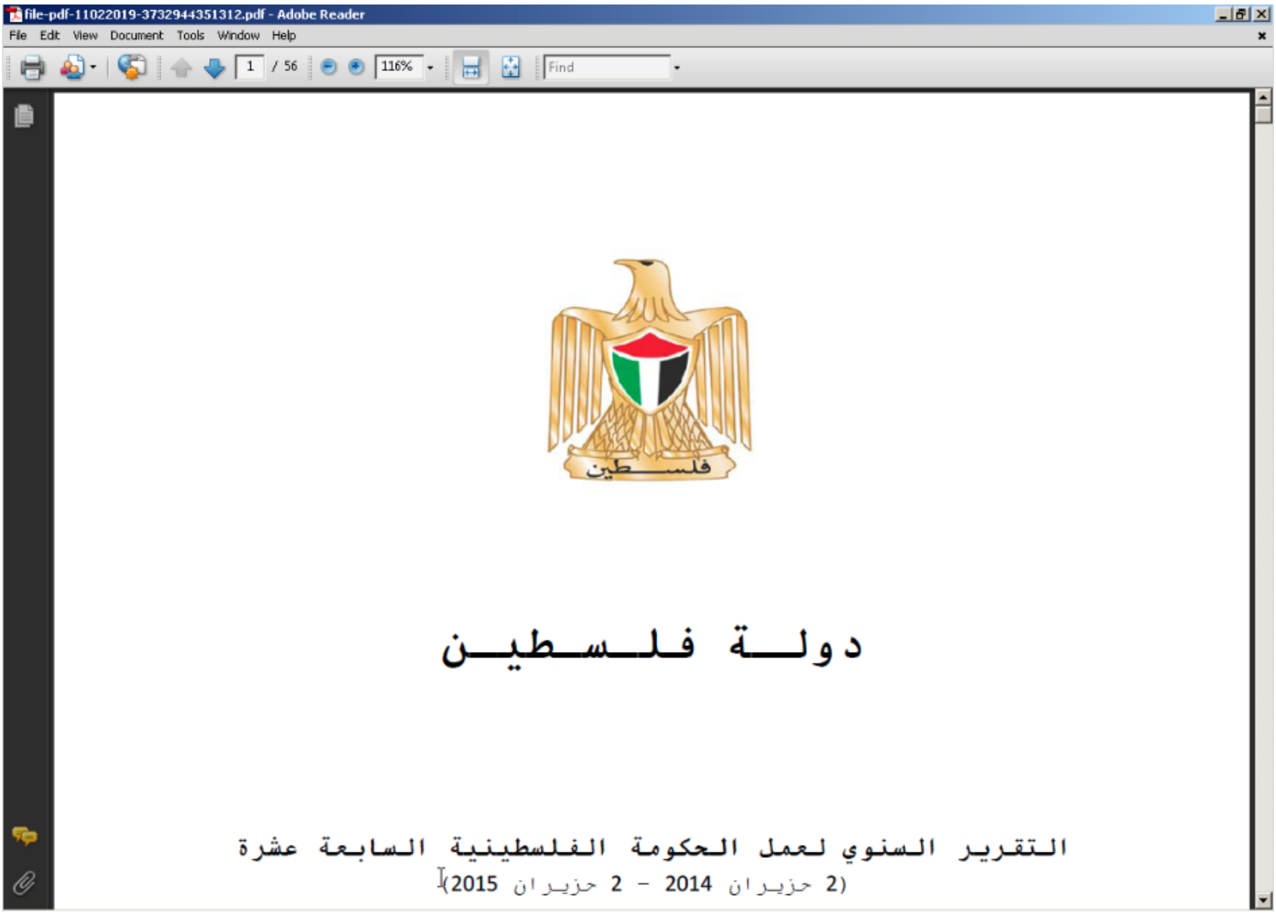
This actor uses their Delphi-based Micropsia implant to target Palestinian individuals and organizations, using politically themed file names and decoy documents. The most recent wave uses content originally published on the Turkish state-run news agency Anadolu and on the Palestinian MA'AN development center to target activists and Palestinian institutions. The tactics, techniques and procedures (TTPs) used in the most recent samples found by Talos lead us to believe this is a campaign linked to the previous campaign we reported on in 2017. Meta exposed this actor in an April 2021 report that focused mainly on mobile targeting operations. However, that did not stop the group, as they've continued to target Windows-based systems. Although this group hasn't technologically evolved, it has the motivation and means to operate longstanding campaigns against the same targets. This level of motivation makes them particularly dangerous to organizations that may come into their crosshairs. An in-depth defense using protections against the several layers of their infection chain is the best strategy to defend against this kind of threat. This should include email security to detect and prevent their most common initial attack vector, along with Cisco Secure Endpoint if the implant is successfully delivered using novel attack vectors. On the network side, Cisco Secure Firewall and Umbrella can be used to detect command and control (C2) communications performed with new versions and variants of their implants.

Arid Viper threat actor

Arid Viper, also known as Desert Falcon or APT C-23, was first exposed in 2015. This threat actor's main motivation is espionage and information theft, and has been attributed to malicious operators politically motivated towards the liberation of Palestine. Its victimology is dispersed all over the world, including Palestinian organizations and individuals. Arid Viper is not a technically evolved actor, however, it is known to target mobile and desktop platforms, including Apple iOS. Their toolkit consists of Delphi packers and compilers around their staple malware, Micropsia. This implant has also been ported to other platforms with versions based on Python and an Android version.

Campaign

Talos has identified new waves of this campaign against Palestinian individuals and organizations. It uses the same TTPs that we published in our first report on this actor back in 2017. The image below shows an example of a lure used in 2019 — while the file name refers to an annual report from 2018, the contents actually mention 2014 and 2015.


file-pdf-11022019-3732944351312.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 56
116%
Find
فلسطين

دولة فلسطين

التقرير السنوي لعمل الحكومة الفلسطينية السابعة عشرة
(2 حزيران 2014 - 2 حزيران 2015)

Example of the decoy document from 2019.

The table below shows a small chronology of malicious implants masquerading as documents of interest being created with the same themes, which we associate with high confidence to the same ongoing campaign.

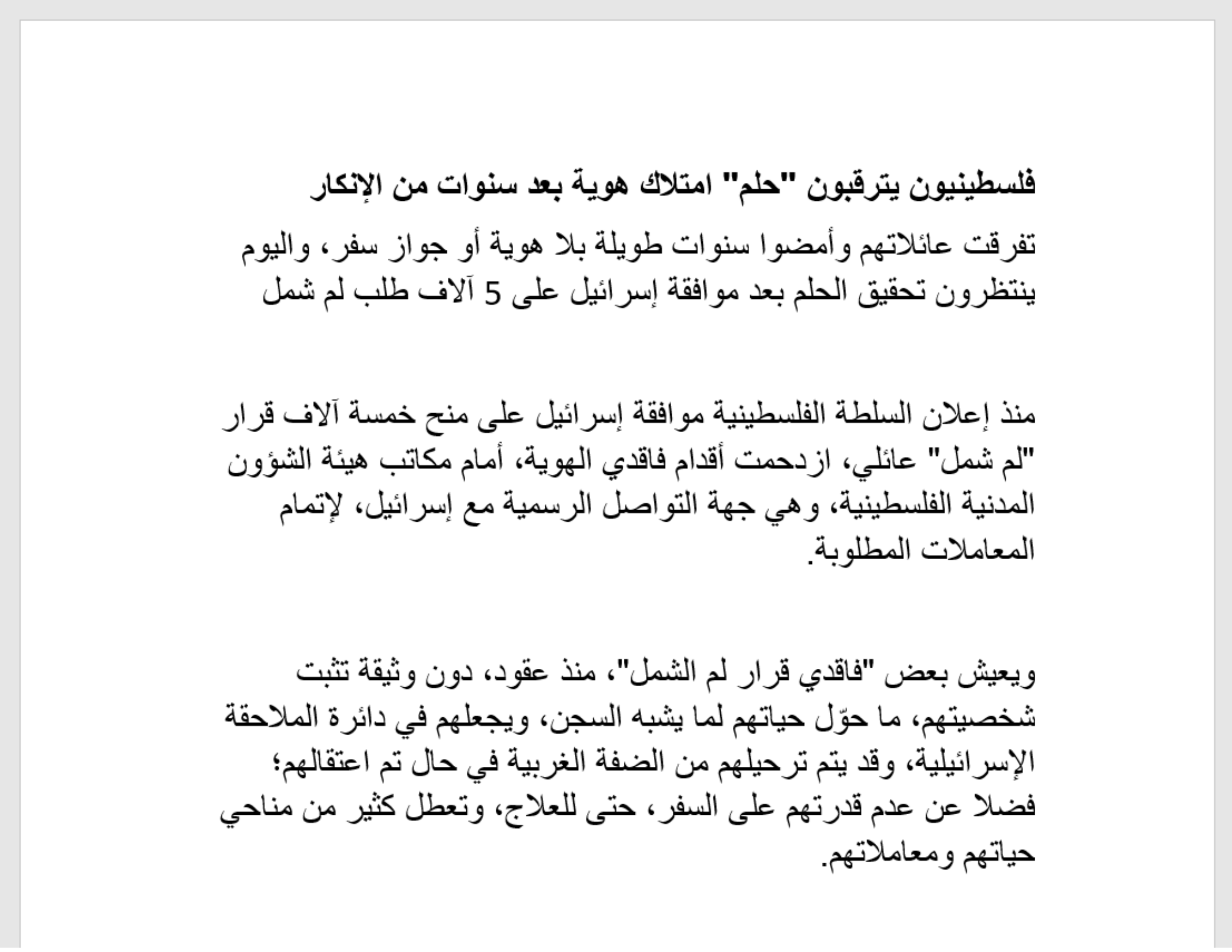
File name	Date
Altarnatives_Palestine_898409234986798852_98794832784327324889_pdf.exe	Mar. 30, 2017
Plan_Palestine_8984092665951234986798852_98794832784327324889_pdf.exe	April 17, 2017
صحيفة _ اتفاق على ممر مائي بين غزة وقبرص.com (An agreement on a waterway between Gaza and Cyprus.com)	Nov. 11, 2018
Annual-Report-2018-11022019-12654684513-73579536-pdf.exe	Feb. 11, 2019
General Secretariat for the Council of Ministers General Budget Law year 1839-2021 (9).xz	Oct. 07, 2020
general secretariat for the council of ministers 1839-2021.exe	Oct. 08, 2020
General Secretariat for the Council of Ministers 1839-2021.zip	Nov. 24, 2020
Questions about the study of freedoms 78639846 docx.exe	Feb. 25, 2021
The opening and maturity of the elections _ 7895349857823525_pdf.xz	Mar. 16, 2021
Introduction to sustainable development 47823579856 275672566 pdf exe	Sept. 10, 2021
Reunification investigation - civil affairs 4937837635 423789926 docx.exe	Sept. 23, 2021

The use of politically themed lures reduced during 2018 and 2019, but we observed a definite increase in their usage in 2020 and 2021. Talos also observed other themes being used by this group (to deliver Micropsia) during 2018 and 2019 and into 2020/21, but they were not considered as part of this campaign in analysis and are beyond the scope of this research.

Most recent decoys

The politically motivated content in the decoy documents, along with the use of the Arabic language, point to the victims being Palestinian individuals and organizations.

The most recent decoy document from September 2021 contains an article about the reunification of Palestinian families, originally published by the Anadolu Agency on Sept. 3, 2021.



فلسطينيون يترقبون "حلم" امتلاك هوية بعد سنوات من الإنكار

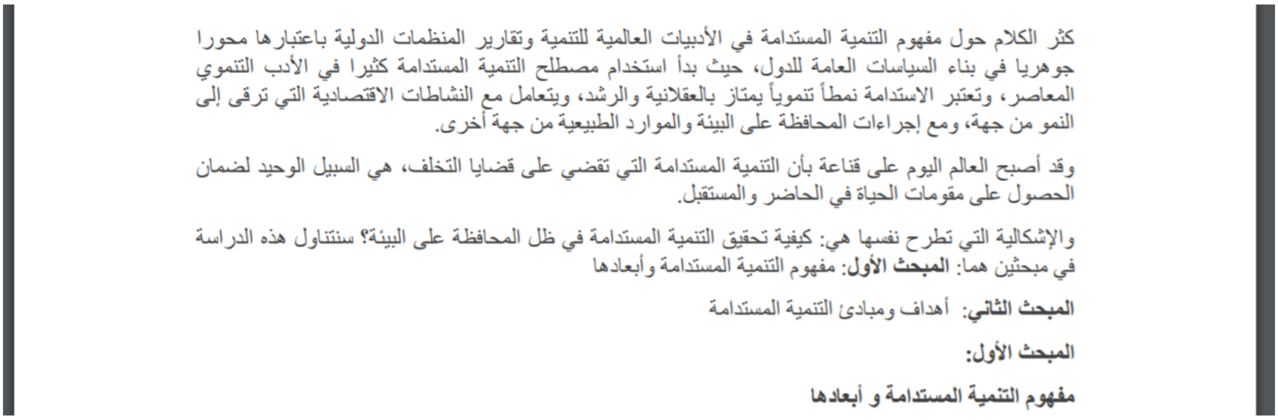
تفرقت عائلاتهم وأمضوا سنوات طويلة بلا هوية أو جواز سفر، واليوم
ينتظرون تحقيق الحلم بعد موافقة إسرائيل على 5 آلاف طلب لم شمل

منذ إعلان السلطة الفلسطينية موافقة إسرائيل على منح خمسة آلاف قرار
"لم شمل" عائلي، ازدحمت أقدام فاقدي الهوية، أمام مكاتب هيئة الشؤون
المدنية الفلسطينية، وهي جهة التواصل الرسمية مع إسرائيل، لإتمام
المعاملات المطلوبة.

ويعيش بعض "فاقدي قرار لم الشمل"، منذ عقود، دون وثيقة تثبت
شخصيتهم، ما حوّل حياتهم لما يشبه السجن، ويجعلهم في دائرة الملاحقة
الإسرائيلية، وقد يتم ترحيلهم من الضفة الغربية في حال تم اعتقالهم؛
فضلا عن عدم قدرتهم على السفر، حتى للعلاج، وتعطل كثير من مناحي
حياتهم ومعاملاتهم.

Decoy document containing text on Palestinian reunification.

Another decoy, also from September 2021, consists of an article on social and economically sustainable development in Palestine by the MA'AN development center — a Palestinian development and training institution aimed at community development.



كثر الكلام حول مفهوم التنمية المستدامة في الأدبيات العالمية للتنمية وتقارير المنظمات الدولية باعتبارها محورا جوهريا في بناء السياسات العامة للدول، حيث بدأ استخدام مصطلح التنمية المستدامة كثيرا في الأدب التنموي المعاصر، وتعتبر الاستدامة نمطاً تنموياً يمتاز بالعقلانية والرشد، ويتعامل مع النشاطات الاقتصادية التي ترقى إلى النمو من جهة، ومع إجراءات المحافظة على البيئة والموارد الطبيعية من جهة أخرى.

وقد أصبح العالم اليوم على قناعة بأن التنمية المستدامة التي تقضي على قضايا التخلف، هي السبيل الوحيد لضمان الحصول على مقومات الحياة في الحاضر والمستقبل.

والإشكالية التي تطرح نفسها هي: كيفية تحقيق التنمية المستدامة في ظل المحافظة على البيئة؟ سنتناول هذه الدراسة في مبحثين هما: **المبحث الأول**: مفهوم التنمية المستدامة وأبعادها

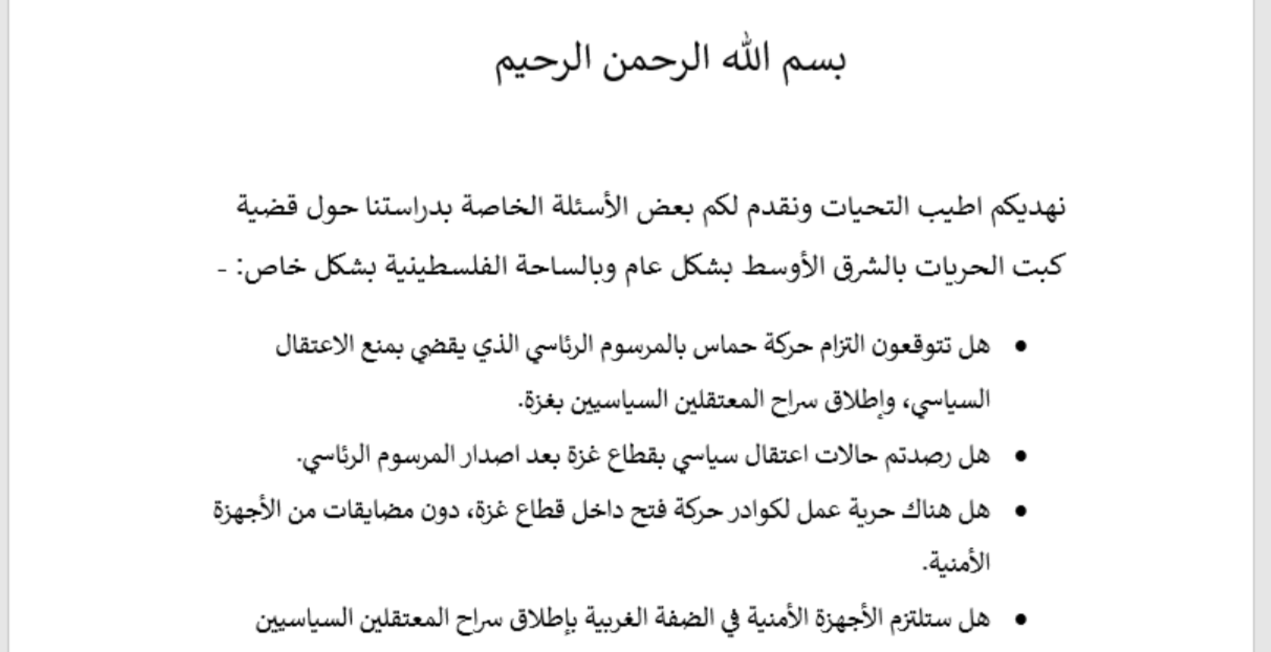
المبحث الثاني: أهداف ومبادئ التنمية المستدامة

المبحث الأول:

مفهوم التنمية المستدامة و أبعادها

Decoy document containing an article on Palestinian sustainable development.

Another decoy from July 2021 consisted of a patient's report containing affidavits from the State of Palestine's Ministry of Health. During March and February 2021, we observed the use of politically themed decoys. One of these decoys consisted of a list of questions from a Palestinian activist on the Presidential decree issued on Feb. 20, 2021, ordering the respect of freedom of expression ahead of legislative elections in May.



بسم الله الرحمن الرحيم

نهديكم اطيب التحيات ونقدم لكم بعض الأسئلة الخاصة بدراستنا حول قضية كبت الحريات بالشرق الأوسط بشكل عام وبالساحة الفلسطينية بشكل خاص: -

- هل تتوقعون التزام حركة حماس بالمرسوم الرئاسي الذي يقضي بمنع الاعتقال السياسي، وإطلاق سراح المعتقلين السياسيين بغزة.
- هل رصدتم حالات اعتقال سياسي بقطاع غزة بعد اصدار المرسوم الرئاسي.
- هل هناك حرية عمل لكوادر حركة فتح داخل قطاع غزة، دون مضايقات من الأجهزة الأمنية.
- هل ستلتزم الأجهزة الأمنية في الضفة الغربية بإطلاق سراح المعتقلين السياسيين

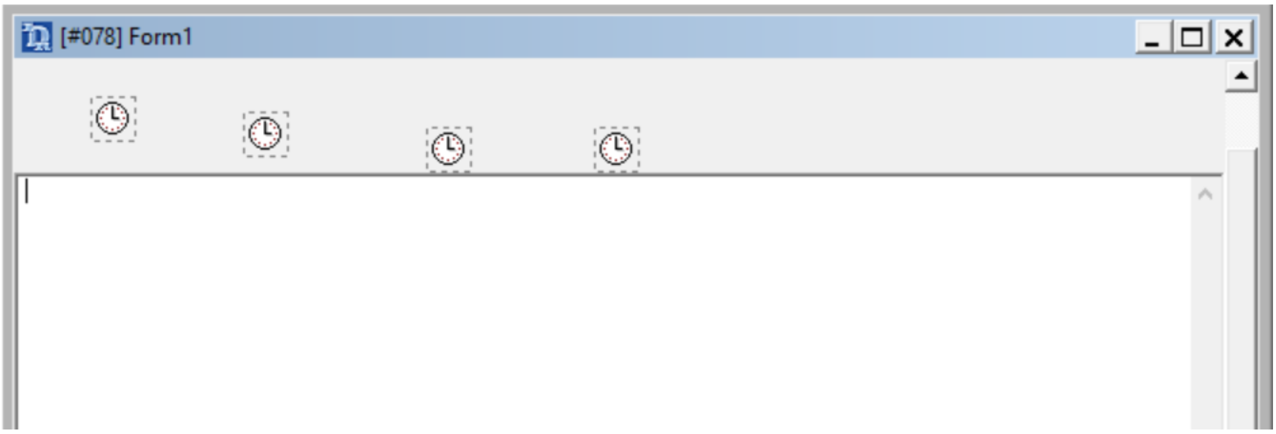
Decoy containing a list of questions from a Palestinian activist.

Deployment

During this investigation, Talos could not find any email or social media posts that were somehow linked to the Micropsia implants. However, we found the implants and compressed files containing the implants. This follows the same pattern that we described in our 2017 post about this actor. It is highly likely that the threat actor has continued to use the email vector to deliver their lures and implants.

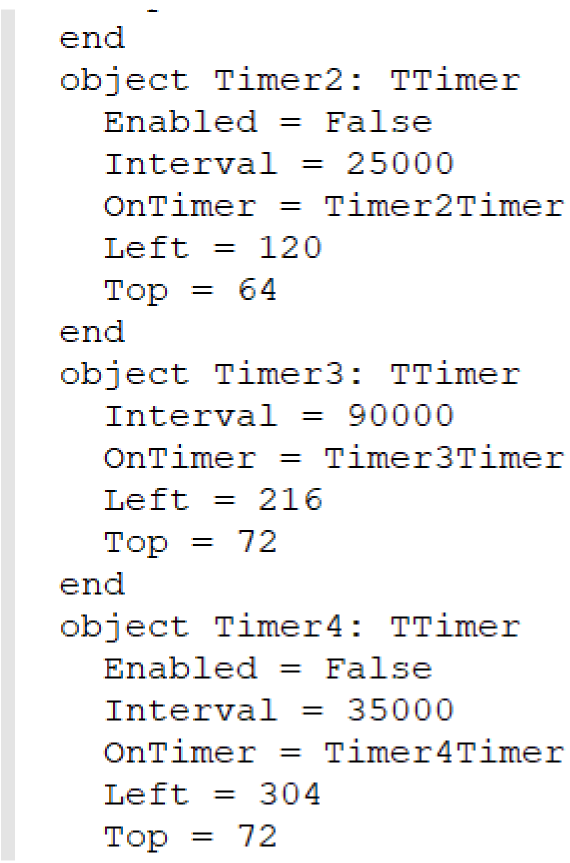
Implant analysis

The implant used to target Palestinian entities consists of Delphi-based versions of Micropsia. This implant consists of a Delphi form with four buttons and four timers implemented to carry out different malicious activities described below.



Form1 containing the four timers.

```
object Button1: TButton
  Left = 24
  Top = 9
  Width = 75
  Height = 25
  Caption = 'Button1'
  TabOrder = 1
  OnClick = Button1Click
end
object Button2: TButton
  Left = 120
  Top = 8
  Width = 75
  Height = 25
  Caption = 'Button2'
  TabOrder = 2
  OnClick = Button2Click
end
object Button3: TButton
  Left = 216
  Top = 8
  Width = 75
  Height = 25
  Caption = 'Button3'
  TabOrder = 3
  OnClick = Button3Click
end
object Button4: TButton
  Left = 312
  Top = 9
  Width = 75
  Height = 25
  Caption = 'Button4'
  TabOrder = 4
  OnClick = Button4Click
end
object IdMemo: TMemo
  Left = 476
  Top = 8
  Width = 151
  Height = 26
  TabOrder = 5
end
object Timer1: TTimer
  Interval = 2000
  OnTimer = Timer1Timer
  Left = 40
  Top = 56
```



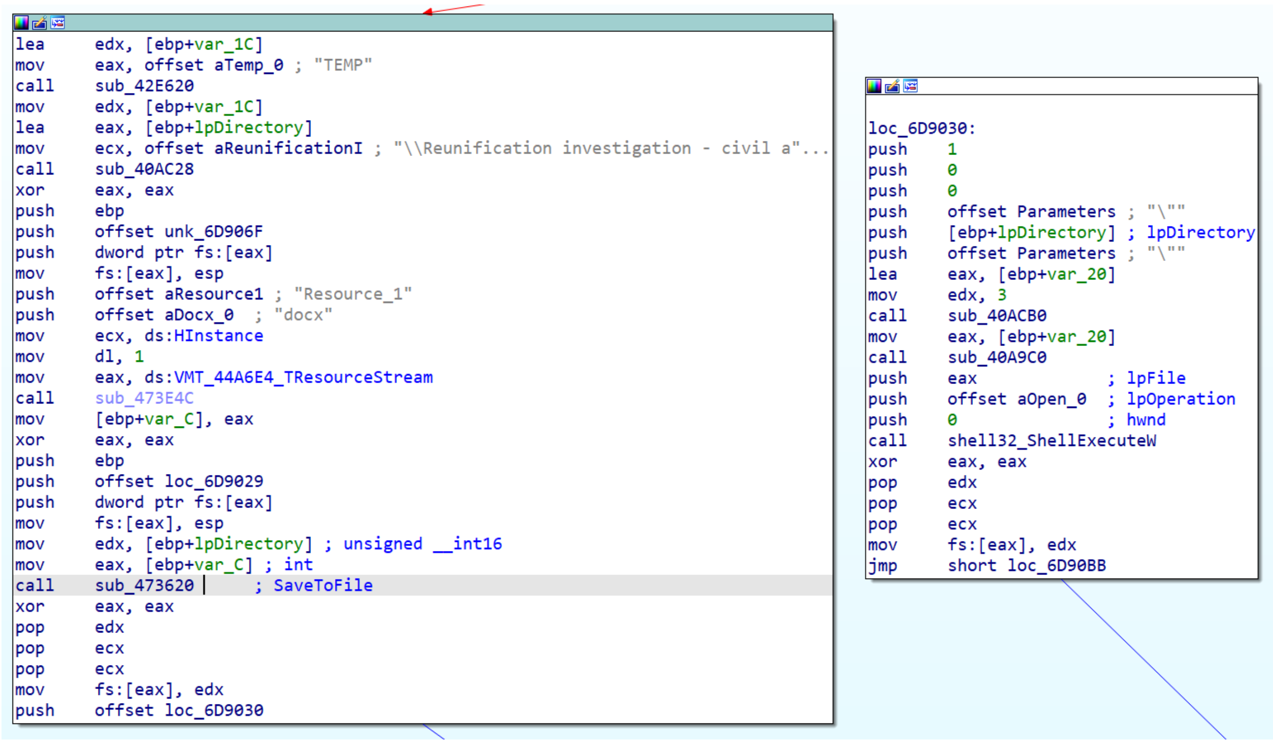
```
end
object Timer2: TTimer
  Enabled = False
  Interval = 25000
  OnTimer = Timer2Timer
  Left = 120
  Top = 64
end
object Timer3: TTimer
  Interval = 90000
  OnTimer = Timer3Timer
  Left = 216
  Top = 72
end
object Timer4: TTimer
  Enabled = False
  Interval = 35000
  OnTimer = Timer4Timer
  Left = 304
  Top = 72
```

Form1 contents

All the malicious functionalities are implemented through the timers configured in the implant.

Deploying the decoy document

One of these timers is responsible for extracting the decoy document and saving it to the %TEMP% folder and then displaying it via ShellExecute:



```
lea     edx, [ebp+var_1C]
mov     eax, offset aTemp_0 ; "TEMP"
call    sub_42E620
mov     edx, [ebp+var_1C]
lea     eax, [ebp+lpDirectory]
mov     ecx, offset aReunificationI ; "\\Reunification investigation - civil a"...
call    sub_40AC28
xor     eax, eax
push    ebp
push    offset unk_6D906F
push    dword ptr fs:[eax]
mov     fs:[eax], esp
push    offset aResource1 ; "Resource_1"
push    offset aDocx_0  ; "docx"
mov     ecx, ds:HInstance
mov     dl, 1
mov     eax, ds:VMT_44A6E4_TResourceStream
call    sub_473E4C
mov     [ebp+var_C], eax
xor     eax, eax
push    ebp
push    offset loc_6D9029
push    dword ptr fs:[eax]
mov     fs:[eax], esp
mov     edx, [ebp+lpDirectory] ; unsigned __int16
mov     eax, [ebp+var_C] ; int
call    sub_473620      ; SaveToFile
xor     eax, eax
pop     edx
pop     ecx
pop     ecx
mov     fs:[eax], edx
push    offset loc_6D9030
```

```
loc_6D9030:
push    1
push    0
push    0
push    offset Parameters ; "\""
push    [ebp+lpDirectory] ; lpDirectory
push    offset Parameters ; "\""
lea     eax, [ebp+var_20]
mov     edx, 3
call    sub_40ACB0
mov     eax, [ebp+var_20]
call    sub_40A9C0
push    eax             ; lpFile
push    offset aOpen_0  ; lpOperation
push    0               ; hwnd
call    shell32_ShellExecuteW
xor     eax, eax
pop     edx
pop     ecx
pop     ecx
mov     fs:[eax], edx
jmp     short loc_6D90BB
```

Decoy document extracted and displayed to the target.

Now, if the implant is started with the "-start" command-line switch, it will skip the process for dropping and displaying the decoy document and jump straight to its RAT functionalities.

Establishing persistence

Another timer is used to establish persistence for the implant on the endpoint.

Here, the implant will establish persistence by obtaining its current command line, which is then used to create a shortcut for itself in the %TEMP% directory. The shortcut to run the implant contains the "-start" switch (used to skip the displaying of the decoy document). This shortcut is then moved over to the currently logged-in user's Startup folder to complete persistence across reboots and re-logins.

Information Gathering

The remaining two timers will gather preliminary system information and activate the RAT capabilities of the implant.

The sequence of actions followed for gathering system information from the endpoint are as follows:

1. Generate a pc ID for the infected endpoint. Save this value into a data file, such as: "%APPDATA%\dsfjj45k.tmp"

2. Gather the Computername and username from ENV. Concatenate the computername, username and pcid into format: <COMPNAME>_<username>_<pcid>

3. Gather installed AV information from the endpoint via "winmgmts:\\localhost\root\SecurityCenter2" using query "SELECT * FROM AntiVirusProduct". From the AV information obtained, record the DisplayName.

4. Get OS information specifically the installed product name.

5. Get the current implant's command line and record it.

All this data gathered from the system is individually base64-encoded and assigned to HTTP form query variables with the following name-value pairs:

vcqmxylcv= base64 encoded <COMPNAME>_<username>_<pcid>
vcnwaapcv= base64 encoded AV Name list.
vcllgracv= base64 encoded OS version string.
vcwjlxycv= base64 encoded implant command line.
vccodwfcv= base64 encoded hardcoded flag.

The data is then sent to the implant's C2 server via an HTTP POST request, which is fairly standard in Micropsia implants.

RAT capabilities

Once the preliminary information has been sent, the implant now begins its remote access trojan (RAT) activity and waits for command codes from the C2 server.

The implant now uses two additional HTTP form variables to transmit the output of the commands executed on the endpoint:

vcgqjdlrcv = hardcoded value 0.
mugnaq = base64 encoded screenshot or command output.

The C2 issues distinct command codes to the implant to carry out various actions on the infected endpoint.

The commands follow the format: ;<cmd_code>;<base64_encoded_supporting_data>;

Field name	cmd_code	supporting_data
Example	cmd	aXBjb25maWc

The above example would run the ipconfig command on the endpoint.

The command codes accepted by the implant are listed here:

Command code	Description
"1" or "2" or "sh"	Capture screenshots to the %TEMP% directory and exfiltrate.
"log"	Send the current activity log (recorded in an internal Memo) to the C2.
"cmd"	Execute the command specified and send output to C2.
"df"	Download file from a specified remote location into a local path specified by the C2.
"zero"	Exit execution.
"lehar"	Ask for the next command from the C2.

We have observed implants using two distinct URLs to instrument communications with the C2, one for exfiltration of screenshots and the other for all the other RAT commands.

For example one of the implants used a distinct URL for screenshots:

hxxp[s]://deangelomcnay[.]news/qWIlIdKf2buIH0k/GbrHoIfRqtE69hH/ZCgbo9EVhYMA8PX

While another URL was used for all other commands:

hxxp[s]://deangelomcnay[.]news/qWIlIdKf2buIH0k/GbrHoIfRqtE69hH/bu5EmpJE7DUfzZD

Conclusion

Since its initial disclosure by Talos in 2017, this campaign from Arid Viper has become a long-standing offensive cyber attack spanning well into 2021.

State-sponsored actors and privateer groups rely heavily on stealth in their operations. The public disclosures of campaigns and targeted attacks are usually followed by the actors taking down their infrastructure and revamping their implants to avoid discovery of their malicious assets.

However, in the case of Arid Viper, the continued use of the same TTPs over the past four years indicates that the group doesn't feel affected by the public exposure of its campaigns and implants, and continues to operate business as usual. This complete lack of deterrence makes them a dangerous group once they decide to target an organization or individual.

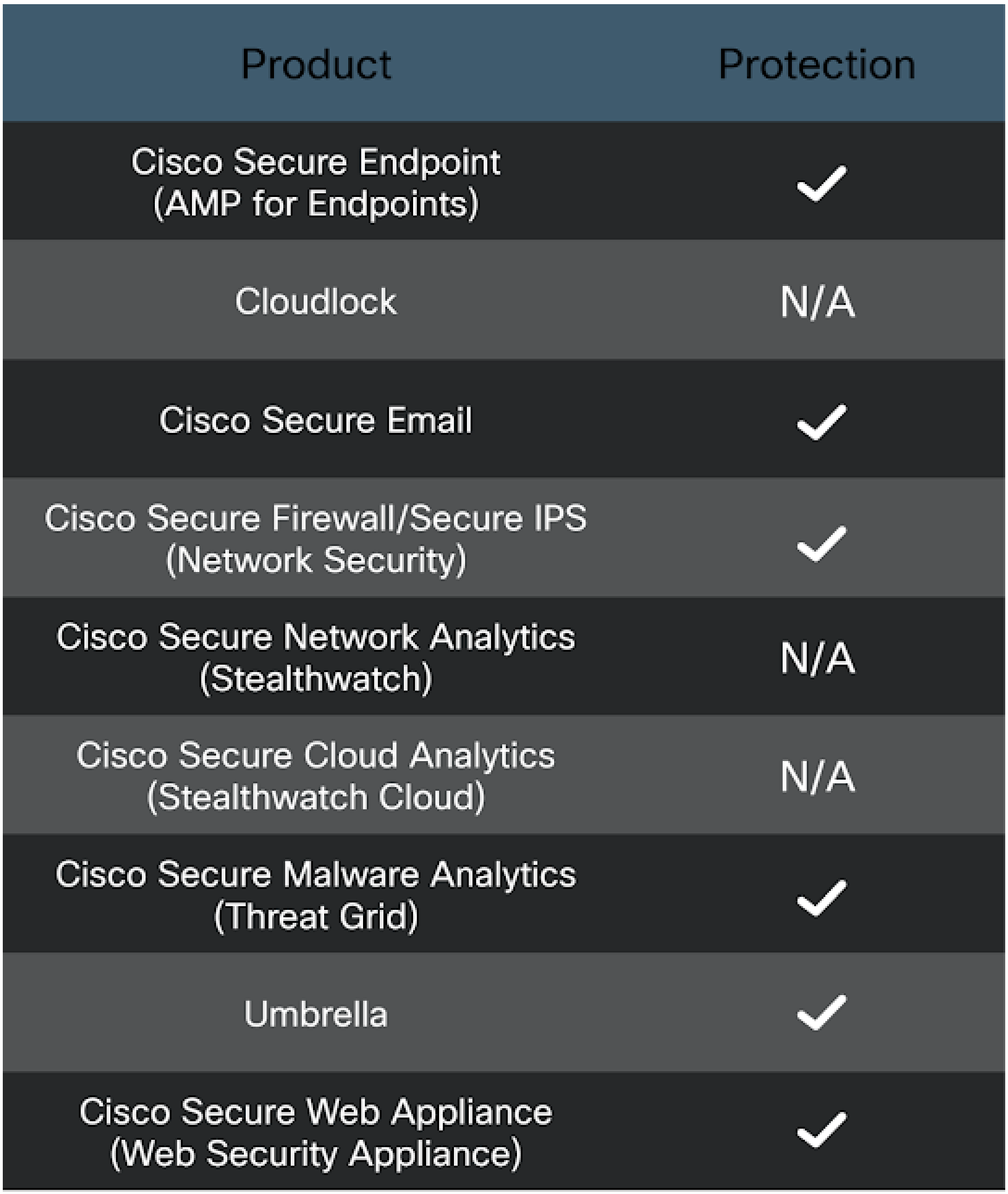
The lack of change also points to a certain level of success with their current TTPs. The new campaign and accompanying versions of Arid Viper's Micropsia implant disclosed in this research by Talos brings the spotlight back to their politically themed campaign to remind potential victims that the group is still very active.

Arid Viper is a prime example of groups that aren't very advanced technologically, however, with specific motivations, are becoming more dangerous as they evolve over time and test their tools and procedures on their targets. Implants such as Micropsia come in various forms such as Delphi, Python and Android. Such RATs proliferated and operated by a highly motivated threat actor who refuses to back down, consist of a variety of functionalities and are constantly evolving. These RATs can be used to establish long-term access into victim environments and additionally deploy more malware purposed for espionage and stealing information and credentials.

In-depth defense strategies based on a risk analysis approach can deliver the best results in the prevention. However, this should always be complemented by a good incident response plan which has been not only tested with tabletop exercises, but also reviewed and improved every time it is put to the test on real-world engagements.

Coverage

Ways our customers can detect and block this threat are listed below.



Product	Protection
Cisco Secure Endpoint (AMP for Endpoints)	✓
Cloudlock	N/A
Cisco Secure Email	✓
Cisco Secure Firewall/Secure IPS (Network Security)	✓
Cisco Secure Network Analytics (Stealthwatch)	N/A
Cisco Secure Cloud Analytics (Stealthwatch Cloud)	N/A
Cisco Secure Malware Analytics (Threat Grid)	✓
Umbrella	✓
Cisco Secure Web Appliance (Web Security Appliance)	✓

Cisco Secure Endpoint (formerly AMP for Endpoints) is ideally suited to prevent the execution of the malware detailed in this post. Try Secure Endpoint for free here.

Cisco Secure Web Appliance web scanning prevents access to malicious websites and detects malware used in these attacks.

Cisco Secure Email (formerly Cisco Email Security) can block malicious emails sent by threat actors as part of their campaign. You can try Secure Email for free here.

Cisco Secure Firewall (formerly Next-Generation Firewall and Firepower NGFW) appliances such as Threat Defense Virtual, Adaptive Security Appliance and Meraki MX can detect malicious activity associated with this threat.

Cisco Secure Network/Cloud Analytics (Stealthwatch/Stealthwatch Cloud) analyzes network traffic automatically and alerts users of potentially unwanted activity on every connected device.

Cisco Secure Malware Analytics (Threat Grid) identifies malicious binaries and builds protection into all Cisco Secure products.

Umbrella, Cisco's secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs and URLs, whether users are on or off the corporate network. Sign up for a free trial of Umbrella here.

Cisco Secure Web Appliance (formerly Web Security Appliance) automatically blocks potentially dangerous sites and tests suspicious sites before users access them.

Additional protections with context to your specific environment and threat data are available from the Firewall Management Center.

Cisco Duo provides multi-factor authentication for users to ensure only those authorized are accessing your network.

Open-source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCS

Hashes

d4e56e3a9dec89cc32df78aa4ba8b079aa5e697ed99a1e21e9bd31e85d5d1370
1d4e54529feef53850f97f39029a906d53f3d4b2aea8373e27c413324a55681c
bc03948ce4d88f32017d4a1725a05341d3ff72a616645d9893b8f5d11068217f
8a730266c62fa79435497b1d7db38011e63b6c53b48593d65c24c36044d92dba
f2f36a72cfb25cef74ff0ea8e3ad1c49c6dc3e128fd60a2717f4c5a225e20df2
895adb54a13d9ebf3f7215f1bad77c0c548e7dd4c58c3a338d440520efcb8fc9
27eaeb7f0195230e22d5beacc05b7d944aaec4894fbc02824f59b172e360713f
7b9087d91a31d03dd2c235d8debf8ed10f4b82c430a236d159e06e7fb47464a9
aa507bbe5d2a32f6e1e3f311c1baf93fd4707def8596083f26683e85972f5ac0
c9d7b5d06cd8ab1a01bf0c5bf41ef2a388e41b4c66b1728494f86ed255a95d48
0a55551ade55705d4be6e946ab58a26d7cf8087558894af8799931b09d38f3bc
c7e74330440fcf8f6b112f5493769de6cdbdea5944ab78697ab115c927cbd0a1
2d03ff4e5d4d72afffd9bde9225fe03d6dc941982d6f3a0bbd14076a6c890247
e288d7e42c8cdbf0156f008ff7d663f8c8e68faa2e902d51f3287f1bceae79b2
5463b3573451d23f09cb3f6f3c210de182ed0dd8a89459381a7f69aa7f8ac9b4

Hostnames

deangelomcnay[.]news
julianSturgill[.]info
earlahenry[.]com
nicholasuhl[.]website
cooperron[.]me

dorothymambrose[.]live
ruthgreenrtg[.]live

URLs

hxxp://deangelomcnay[.]news/qWIIIdKf2buIH0k/GbrHoIfRqtE69hH/ZCgbo9EVhYMA8PX
hxxp://deangelomcnay[.]news/qWIIIdKf2buIH0k/GbrHoIfRqtE69hH/bu5EmpJE7DUfzZD
hxxps://cooperron[.]me/qWIIIdKf2buIH0k/GbrHoIfRqtE69hH/
hxxps://cooperron[.]me/qWIIIdKf2buIH0k/GbrHoIfRqtE69hH/
hxxps://dorothymambrose[.]live/hx3FByTR5o3zNZYD/sYkaiHz0Mse13C79dy1I/
hxxp://dorothymambrose[.]live/hx3FByTR5o3zNZYD/sYkaiHz0Mse13C79dy1I/
hxxps://nicholasuhl[.]website/X2EYSWlzSZgSUME210Zv/YPPV6kFl2PwwF0TEVHMy/
hxxp://nicholasuhl[.]website/X2EYSWlzSZgSUME210Zv/YPPV6kFl2PwwF0TEVHMy/
hxxps://earlahenry[.]com/Ct2azbEP57LtWgmK/lWaPwemAJ3LPFmDH/
hxxp://earlahenry[.]com/Ct2azbEP57LtWgmK/lWaPwemAJ3LPFmDH/
hxxp://juliansturgill[.]info/um2NxySaF4L5mSYE/KY1hNeVvrE1XCrKP/