Thamar Reservoir

An Iranian cyber-attack campaign against targets in the Middle East

Clearsky

TLP:WHITE
For public distribution

Contents

Foreword

This report reviews an ongoing cyber-attack campaign dating back to mid-2014. Additional sources indicate this campaign may date as far back as 2011. We call this campaign **Thamar Reservoir,** named after one of the targets, Thamar E. Gindin[1], who exposed new information about the attack and is currently assisting with the investigation.

The campaign includes several different attacks with the aim of taking over the target's computer or gain access to their email account. We estimate that this access is used for espionage or other nation-state interests, and not for monetary gain or hacktivism. In some cases, the victim is not the final target; the attackers use the infected computer, email, or stolen credentials as a platform to further attack their intended target.

The attackers are extremely persistent in their attempts to breach their targets. These attempts include:

- Breaching trusted websites to set up fake pages
- Multi-stage malware
- Multiple spear phishing emails based on reconnaissance and information gathering.
- Phone calls to the target.
- Messages on social networks.

While very successful in their attacks, the attackers are clearly not technically sophisticated. They are not new to hacking, but do make various mistakes, such as grammatical errors, exposure of attack infrastructure, easy to bypass anti analysis techniques, lack of code obfuscation, and more.

These mistakes enabled us to learn about their infrastructure and methods. More importantly, we have learned of 550 targets, most of them in the Middle East, from various fields: research about diplomacy, Middle East and Iran, international relations, and other fields; Defense and security; Journalism and human rights; and more.

Various characteristics of the attacks and their targets bring us to the conclusion that the threat actors are Iranian. In addition, we note that these attacks share characteristics with previously documented activities:

- Attacks conducted using the Gholee malware, which we discovered.
- Attacks reported by Trend Micro in Operation Woolen-Goldfish.
- Attacks conducted by the Ajax Security Team as documented by FireEye.
- Attacks seen during Newscaster as documented by iSight.

For further details and questions, or if you think you are a victim please contact us at:
info [at] clearskysec.com

---

[1] Dr. Gindin is an expert on Iranian linguistics and Pre-Islamic Iran, renowned lecturer and research fellow at the Ezri Center for Iran and Persian Gulf Research in the University of Haifa.
http://www.thmrsite.com/?page_id=198

Modus operandi - investigation of targeted attacks

This chapter contains an in-depth analysis of a series of attacks against one of the Thamar Reservoir targets. The heavy attack began two days after the target, Dr. Thamar E. Gindin, was interviewed on the IDF radio station[2].

Over the course of two weeks, the threat actor used the following attacks against a single target:

1. One spear phishing email containing malware.
2. Three separate email messages with links to a fake log-in page, (including two factor authentication), one of them hosted on a breached website, the other two on dedicated domains.
3. Two phone calls from the attacker, designed to build rapport for one of the phishing emails.
4. Numerous attempts to take over cloud accounts using their Account Recovery mechanism.
5. Numerous messages on Facebook and by e-mail.

While we describe this case mostly from the point of view of a single target, we would like to emphasize that these scenarios repeated themselves for many other targets.

Part 1 -spear phish #1 - with malware

In May 2015 a legitimate email was sent asking several researchers to fill out a form that was sent as a Word document. The attackers obtained this correspondence, presumably by breaching the email account of the sender. They created a new Gmail account with a username similar to that of the original sender. Then, they sent the recipients a follow-up message (including the initial correspondence), asking them to fill up the attached form again. This time, the attachment was a weaponized Microsoft Excel file (The file is analyzed in the "Malware analysis" chapter of this report).

In other cases the attackers used the same methods - sending malware or phishing from a cloud email service (such as Gmail or Hotmail) using a username similar to that used by one of the target's acquaintances.

The malicious email was written in the original language of the correspondence - Hebrew. But it is clear that the attackers do not know Hebrew, as they made grammatical errors in the few words they have added to it (the rest were copied from the original email). Other messages, in English and Farsi, were analyzed by several specialists[3]and were determined to have been written by a native Iranian Persian speaker.

---

[2] The interview revolved around "her own way to being a linguist and an Iranist, and promoting her books "The Good, the Bad and the World - a Journey to Pre-Islamic Iran" and "The Book of Esther, Unmasked" ".

[3]Three of the targets are Iran and the Middle East researchers, and two of them are native Farsi speakers. Going through numerous messages they have received, and in one case a phone call - they have determined that the writer/speaker is native in Iranian Persian.

Below is an example of another case (the email includes the professional signature of the impersonated sender):

> **From:** ██████████ [mailto:████████r@gmail.com]
> **Sent:** 3 February 2015 2:48 PM
> **To:** ████████@████████.ac.iI
> **Subject:** Dear Friends
>
>
> Dear friends,
> Enclosed is some information that I thought might be useful for you.
> As it contains some sensitive info I decided to hide the text.
> You must open the file in a computer or laptop to view it correctly.
> Best,

Part 2 - phone calls to victims

A week later, the attackers called the target's office number. The office manager, who received the call, later said that someone with "bad English" had asked to schedule an interview. The attackers later called the target's personal cell phone, and left a similar message with a callback number in London.

The attackers called the targets in other cases as well. For example, after breaching the password of a victim back in November 2014, the attacker called, pretending to be the assistant of a professor abroad who wished to talk to the victim. After several "unexplained" cut-offs during the call, the attacker said they should switch to Google Hangout, asking for the "conversation code" the victim had just received to his cell phone. The code was actually the second factor authentication for the victim's Gmail account. As soon as he gave it away - the attackers took over his Gmail, Facebook and other accounts.

Part 3 - spear phishing #2

That evening, the target received an email written in Farsi, coming from a spoofed persian@bbc.co.uk email address (the real address of BBC Farsi). The message was a follow up on the call that morning, asking to schedule the interview for the next day:

> **From:** سلام خانم دکتر <persian@bbc.co.uk>
> **Date:** 2015-05-20 22:39 GMT+03:00
> **Subject:** matne mosahebe
> **To:** <redacted>@gmail.com
>
>
> سلام خانم دکتر
> متن مصاحبه بی بی سی فارسی من تماس گرفتم اما متاسفانه نتوانستم با شما صحبت کنیم سوالات روی درایو هست برای برنامه زنده فردا آیا تمایل دا
>
> Document.pdf
>
> Google Drive: You can create, make, share, keep, display all your Data in your account.

The headers of the message indicate that it was spoofed, and was actually sent from a server in Hungary, **mail5.maxer.hu**.

The email contained a linked text, *Document.pdf*, with this URL:

> https://www.google.com/url?q=**http://login-users.com/Drive-Auto/AutoSecond**?Chk=*<redacted>*&sa=D&sntz=1&usg=*<redacted>*

The URL is composed of two parts. The first part is a legitimate Google.com address, with the *q*= parameter. The second part is the value of that parameter - a fake Google Drive log-in page in the attackers controlled domain - *login-users.com*. Upon clicking the link, the target is redirected to the address in the *q*= parameter. This is a trick the attackers use to mislead the target - making her think she is about to visit a legitimate Google website.

The fake Google Drive log-in page was customized to the target; her real username was already filled in:
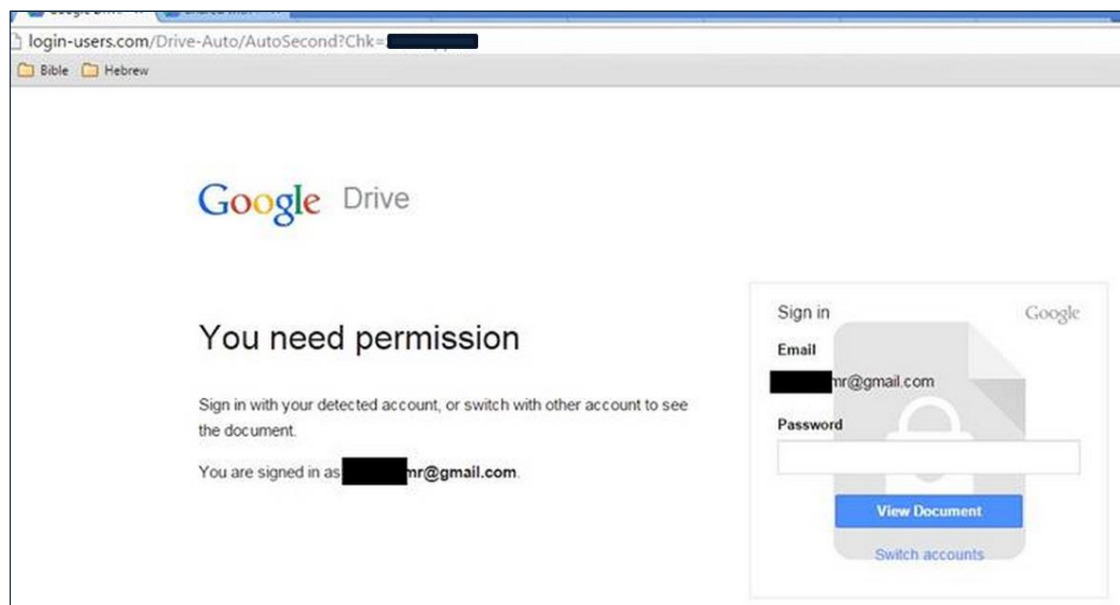
The Whois information for the domain is similar to those used in legitimate Google owned domain, except for the 'd' instead of 'b' in the "registrant-email" value: gmail-a**d**use@google.com:

```
Registry Registrant ID:
Registrant Name: MarkMonitor, Inc.
Registrant Organization: Google Inc.
Registrant Street: 1600 Amphitheatre Parkway
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6506188571
Registrant Fax Ext:
Registrant Email: gmail-aduse@google.com
Registry Admin ID:
```

The attacker sent three follow-up emails to make sure the target had received the first one, from the same server in Hungary and with the Reply-To address **saeed.kn2003@gmail.com**.

```
From: =?utf-8?B?2LPZhNin2YUg2K7Yp9mG2YUg2K/aqdiq2LE=?= <persian@bbc.co.uk>
Reply-To: saeed.kn2003@gmail.com
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: 8bit
Message-Id: <E1YvACk-0001sA-7F@mail5.maxer.hu>
Date: Wed, 20 May 2015 22:03:02 +0200
```

Part 4 - breaking into an Israeli research institute to set up phising page #3

The next morning, several targets received an email inviting them to participate in an "Iran Israel Forum" of an Israeli research institute. The email can be seen below (sensitive information has been redacted):

```
From: <redacted> <noreply@<redacted>.ac.il>
Date: Thu, May 21, 2015 at 9:32 AM
Subject: You Are Invited To <redacted> Iran Israel Forum
To: <redacted>@gmail.com

Dear Dr. Gindin
You are invited to Iran Israel Forum of <redacted>
Default language of forums is English because of different members from different countries.
Members of forum include Israel and United State statesmen and Iranian fans of Israel.
Your invitation code: #86216574
We are glad to meet you in our forum.
Access To Forum

Sincerely yours
<redacted> communication manager.
```

The headers of the email indicate that they the email was not spoofed, and had been sent from the research institute. As can be seen, the email contained various grammatical mistakes. Moreover, anyone who knows

the institute would notice that parts of the message are inaccurate (this will not be elaborated here in order not to expose the institute's identity).

The words "Access To Forum" linked to a page within the real, compromised, website of the institute. The page contained more information about the "forum", and offered four "sign in" options, as can be seen in the screenshot below:

Clicking one of the sign-in options led to a custom made log-in page, again, with the target's username, email, and picture already present:
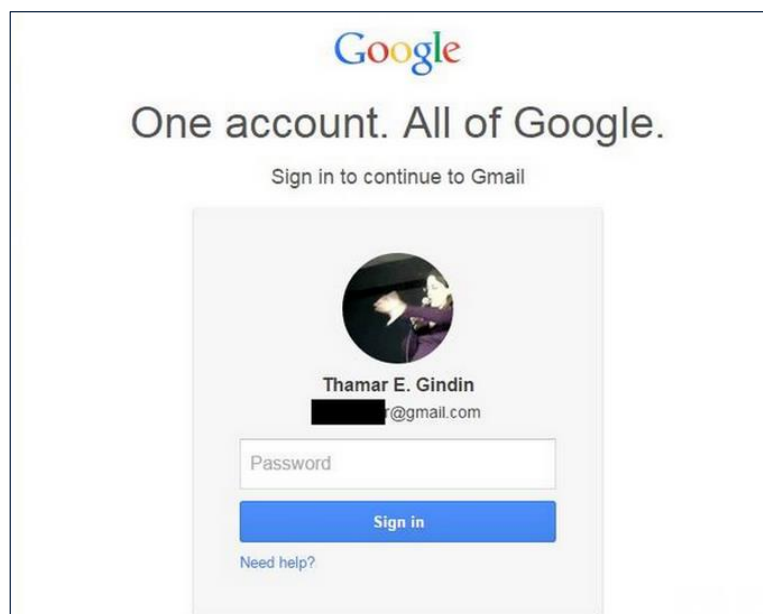
After submitting a password, the victim is taken to the next fake page in which she is asked to submit the two factor authentication code she has just received to her phone:

Upon submission, the victim is redirected to a static "registration confirmed" page.

Interestingly, the log file for the previous pages was hosted publicly on the same virtual folder. The log contained the false credentials the target submitted (as she recognized this was a fake)[4]:
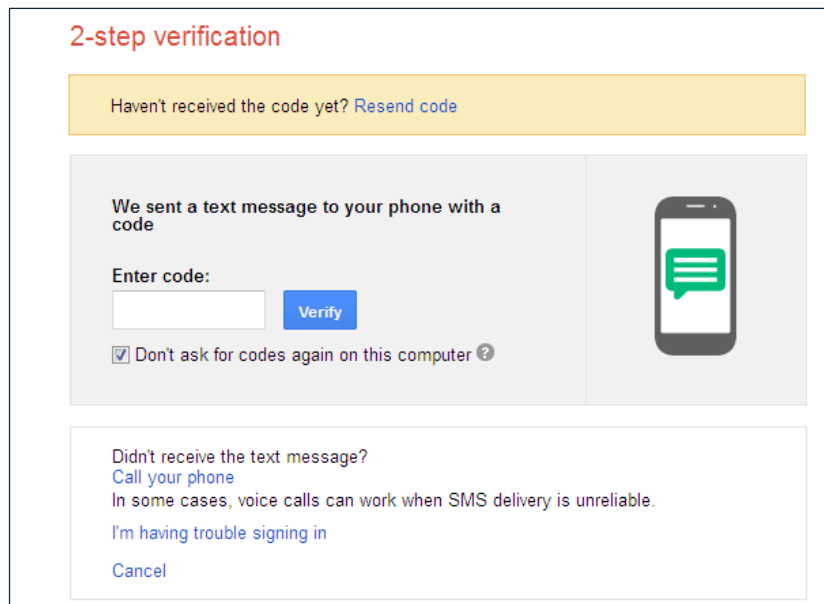

We reported the breach to the institue, and they investigated and cleaned it off. They informed us that their own servers were never breached. Rather, a server run by a researcher who was givenn a "virtual folder" within their domain was. This, of course, did not change the end result - the attackers managed to implant a fake page within the Instititue domain, and were able to send an email using the same domain. This pattern is recurring: The attackrs go after "low hanging fruits" in order to reach their goal rather than using advnaced techincal means.

Part 5 - spear phishing #4

Four days later, the target received the following email from the same fake address as in part 1:

---

[4] The "pass" filed intermingled with the IP filed in the original log, file due to bidirectionality issues.

The email contained the real textual signature of the sender, and the word Toda (Thank you, in Hebrew), as the sender usually writes.

The hyperlink text in the message appeared to be leading to youtube.com, but in fact linked to a fake address that only looked like a YouTube domain.

The page contained a "private Youtube video", asking the viewer to sign in in order to watch it:
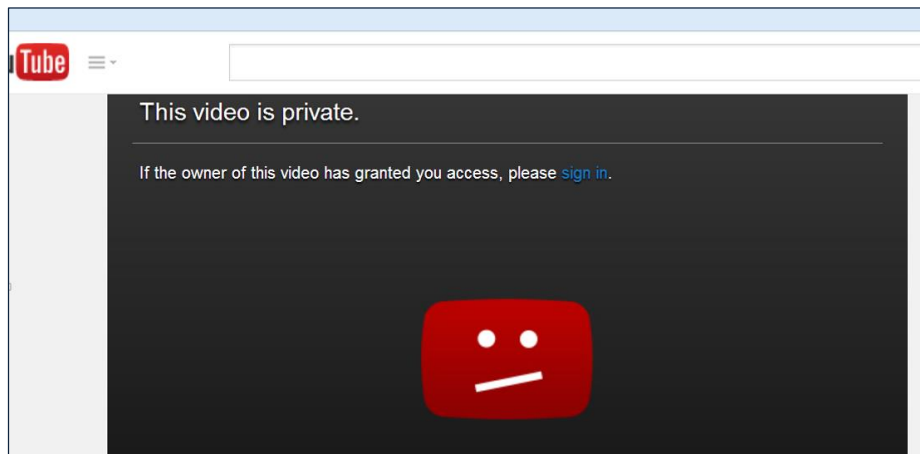
After signing in, the page redirected to a specific interview in target's real YouTube channel - proving once again that the attacks are targeted and based on reconnaissance.

Part 6 - Abusing account recovery mechanisms

During the writing of this article, the attackers continued to attempt to take over various accounts of the target. For example, they tried to fool Google into giving them access to the target's Gmail accounts using the Google Account Recovery process[5] (a process which in certain cases enables one to regain access to an account even if the password and other means of authentication are unavailable).

The attackers tried similar methods against the target's account on Facebook and Yahoo, and had also set up a fake Hotmail account, which was used as the secondary email to which the recovered password should be sent.

Part 7 - Private messages

The target has been contacted by various "weird" characters on Facebook and by e-mail. They have been asking her various questions that have nothing to do with her professional expertise and tried to contact her in various ways. The conversation are conducted in Persian.

We cannot find a direct connection between these Facebook characters and the above mentioned attacks. However, in addition to them happening close to the attacks, we do know that at least one of the accounts is fake.

---

[5] https://www.google.com/accounts/recovery/

One of the fake characters who has engaged in conversation, is using throughout her profile pictures of a Russian model, and has presented herself as with different, contradicting, background stories in conversations with different targets.

Targets and further incidents

Targets

So far we have exposed a list of more than 500 targets by name and email.

The targets come, mostly, from the following fields:

- Both Academic researchers and practitioners in the fields of counter-terror, diplomacy, international relations, Iran and Middle East, and other fields, such as Physics.
- Security and defence.
- Journalists and Human rights activists.
- Other similar fields.

In some cases the attackers tried to breach the account of a relative or colleague of the real target.

Below is the target distribution by country:
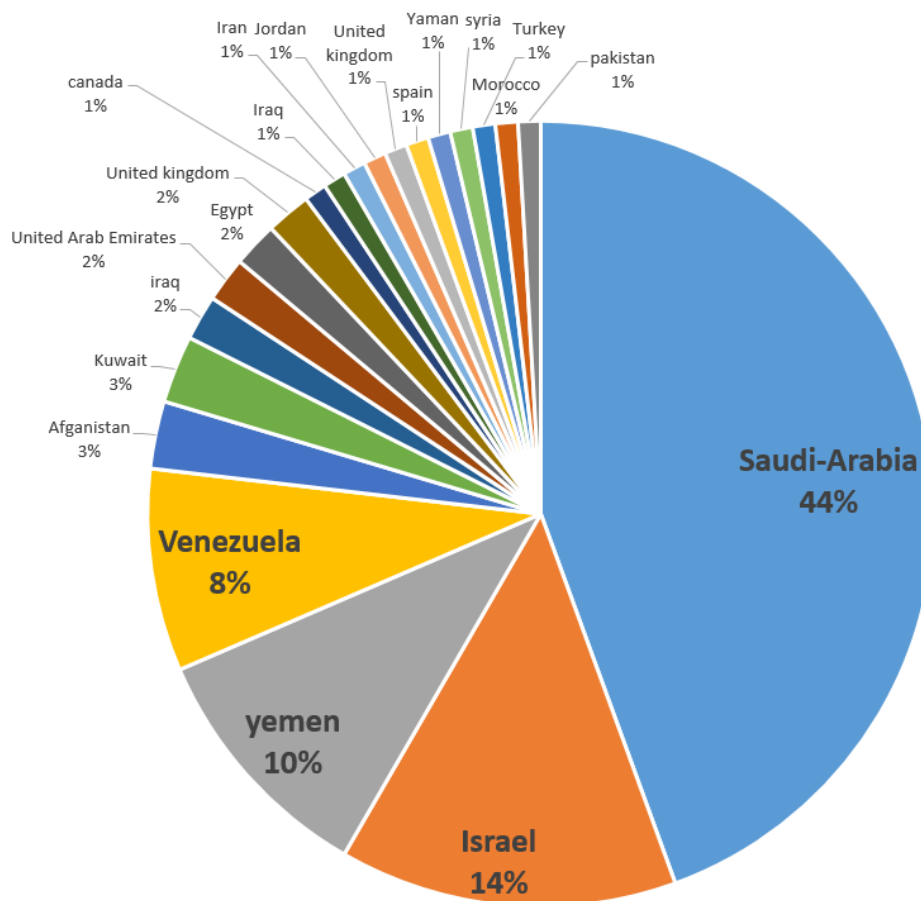
Further incidents

We have investigated and can publicly mention the following incident by the same threat actor:

- A security company had numerous employees targeted with customized phishing pages. The attackers managed to infect computers within the company and steal information. In several other cases numerous employees from the same organization were targeted.
- A fake Gmail account was set up using the name of the head of a research center. Following, several of his contacts received targeted phishing email from the fake account.
- A fake domain has been set up, imitating that of the "Interdisciplinary Center Herzliya", an Israeli college (unrelated to the research institute described above), and has been used in attacks.

The table below correlates between the threat actor behind the Thamar Reservoir campaign and the name of threat actor or campaign, as given in other reports:

Threat actor / campaign	Correlations	Certainty
Gholee[6] by Clearsky	Overlapping infrastructure and malware.	High
Rocket Kitten[7], Operation WOOLEN-GOLDFISH by Trendmicro	Overlapping infrastructure and malware.	High
Ajax Security Team, Operation Saffron Rose[8] by FireEye	Similar TTPs and interests - Attacks against universities and researchers; Use of fake conference pages; Use of a domain that spoofs the name of the targeted organization.	Medium
Newscaster[9] by iSight	Similar TTPs - pretending to be a reporter in order to get close to approach the victim.	Medium

---

[6] http://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign
[7] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-woolen-goldfish.pdf
[8] https://www.fireeye.com/resources/pdfs/fireeye-operation-saffron-rose.pdf
[9] http://www.isightpartners.com/2014/06/uncovering-newscaster-experts-cyber-threat-intelligence/

The Iranian connection

Several characteristics of the attacks have led us to the conclusion that an Iranian threat actor is the likely culprit. We assume, though do not have direct evidence, that it is being supported by the Iranian regime, or performed by the Regime itself:

- The context of the attacks and cover stories all revolve around Iran. Importantly, as determined by several professionals - the attackers speak and write in native Iranian Persian and make mistakes characteristic of Persian speakers. In one of the hacked accounts, when retrieved, the interface language had been changed to Persian.

- The targets and victims match the interests of Iran. Moreover, rather than stealing money or performing high key "cyber terror" attacks (such as information leaks or deferments), the attackers only steal information and use the access to computers for further attacks - indicating espionage, IP theft , etc.

- The TTPs match those of attackers and attacks that were attributed to Iran by other security companies, as mentioned in the previous chapter.

- Some of the domains and IPs used by the attackers in the cases we investigated were mentioned and attributed to an "Iranian threat group" in an advisory by the Financial Sector Cyber Intelligence Group, and the Department of the Treasury, CIG Circular 35[10]

---

[10]http://webcache.googleusercontent.com/search?q=cache:dzV7dGdsTU8J:theatre.fsu.edu/index.php/content/download/208893/1786893/file/20150311_WASP.pdf

Malware analysis

The malicious Excel file (mentioned in 'Part 1 - speared email message containing malware') serve as a Dropper - it creates two files and runs them. When opening the excel file (.xlsb), the user sees a blank sheet and the standard "Macros have been disabled" message. If enabled by the user, the macro drops **NTUSER.dat{GUID}.exe** and **tmp.bat**. The content of the excel sheet is then presented. It is case specific and customized to the victim.

Different malware can be downloaded to the infected computer. On an infected computer we have analyzed, we found CWoolger Keylogger.

The macro, two files, and CWoolger are analyzed below.

Macro

The VBA macro is similar to that used to drop Gholee, as we reported about 8 month ago[11]. However, in current case, a simple downloader was used instead of Gholee.

The VBA contains a series of functions built of VBA Character Codes:

```
Function A0()
c = ""
c = c + Chr(77) + Chr(90) + Chr(119) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Ch
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(42) + Chr(0) + Chr(0) + Chr(0) + Chr(32) + Chr(0) + Chr(0) + Chr(
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(120) + Chr(0) + Chr(0) + Chr(0) + Chr(84) + Chr(104) + Chr(105) +
c = c + Chr(114) + Chr(111) + Chr(103) + Chr(114) + Chr(97) + Chr(109) + Chr(
c = c + Chr(110) + Chr(111) + Chr(116) + Chr(32) + Chr(98) + Chr(101) + Chr(3
c = c + Chr(32) + Chr(105) + Chr(110) + Chr(32) + Chr(68) + Chr(79) + Chr(83)
c = c + Chr(100) + Chr(101) + Chr(46) + Chr(13) + Chr(10) + Chr(36) + Chr(14)
```

```
Function A2()
c = ""
c = c + Chr(12) + Chr(135) + Chr(202) + Chr(211) + Chr(250) +
c = c + Chr(137) + Chr(69) + Chr(12) + Chr(15) + Chr(191) + Ch
c = c + Chr(211) + Chr(224) + Chr(139) + Chr(77) + Chr(8) + Ch
c = c + Chr(139) + Chr(69) + Chr(248) + Chr(137) + Chr(69) + C
c = c + Chr(149) + Chr(255) + Chr(255) + Chr(255) + Chr(199) +
c = c + Chr(0) + Chr(129) + Chr(125) + Chr(248) + Chr(173) + C
c = c + Chr(39) + Chr(0) + Chr(0) + Chr(0) + Chr(15) + Chr(191
c = c + Chr(69) + Chr(8) + Chr(102) + Chr(137) + Chr(69) + Chr
```

These are constructed into a single variable and then written as a file to disc, creating and running NTUSER.dat{GUID}.exe

```
file_text = file_text + A0() + A1() + A2() + A3() + A4() + A5() + A6() + A7() + A8()
```

Next, tmp.bat is written and executed.

---

[11]http://www.clearskysec.com/gholee-a-protective-edge-themed-spear-phishing-campaign

tmp.bat

Tmp.Bat contains two lines. The first create a registry key without prompting the user for permission, telling the computer to run NTUSER.dat{GUID}.exefrom %USERPROFILE% every time the computer starts, naming it "My App". For example:

REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "My App" /t REG_SZ /F /D "C:\Users\Nisa\NTUSER.dat{813E7E06-2AC5-4F3D-94DA-CF6E298F7B18}.exe"
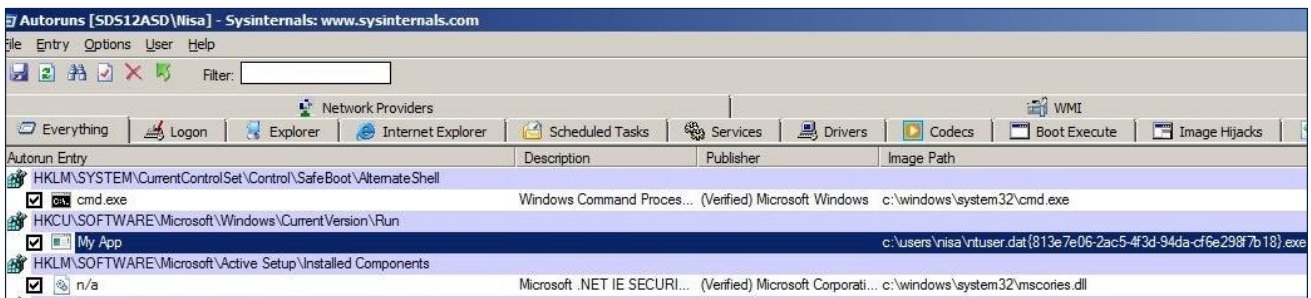
The second line deletes tmp.bat.

NTUSER.dat{GUID}.exe

The dropped exe file (55ff220e38556ff902528ac984fc72dc) is a Downloader. It is created in %UserProfile%, sized 8.5KB, and is recognized by 19 out of 57 antiviruses on Virus Total[12] (the sample was not submitted by us).

It contains simple mechanisms to detect and prevent analysis, such as IsDebuggerPresent:

The malware tries to download files form a remote address, apparently "stage two", the actual malware.

CWoolger Keylogger

We have not been able to get the final malware when running the malicious excel file and dropper in the lab, as the server was not responding. However, we have performed forensic analysis of the computer used by a target who opened the malicious Excel file.

That computer was infected with CWoolger keylogger. An analysis of this tool can be read in Trendmicro's paper "Operation WOOLEN-GOLDFISH"[13] in chapter "Wool3n.H4t's Recent Activities: CWoolger Keylogger".

Below are additional notes about the infection we found:

---

[12]virustotal.com/en/file/072a43123e755ad1bdd159488a85a353227ec51f273c4f79c26ff7e4656c0ef4/analysis/
[13] http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-woolen-goldfish.pdf

- The CWoolger exe file was located in *%appdata%\microsoft\windows\templates***wlg.exe**
- To gain persistency, a link to the exe file was placed in in the Startup folder, with the name "WinDefender" and the notepad icon.
- A file containing the collected keystrokes is saved in *%temp%* in a file called **wlg.dat.** it is sent to an attacker controlled server every 15 minutes.

These findings are similar to those found by Trendmicro – indicating that the attackers have been using the same tool for months.

We would like to thank Omri moyal, VP Research at Minerva Labs for assisting the analysis.

Technical indicators and IoC

Domains

Domains hosting phishing pages:

login-users[.]com
drives-google[.]co
qooqle[.]co
video[.]qooqle[.]co
drive-google[.]co
gfimail[.]us
Google-Setting[.]com
Google-Verify[.]com
Mail-Verify[.]com

IPs

IPs of phishing pages:

107.6.172.51
5.39.223.227
31.192.105.10

Malware

Downloader:

MD5	55ff220e38556ff902528ac984fc72dc
SHA-1	b67572a18282e79974dc61fffb8ca3d0f4fca1b0
SHA-256	072a43123e755ad1bdd159488a85a353227ec51f273c4f79c26ff7e4656c0ef4

MD5	b4790618672197cab31681994bbc10a4
SHA1	d5b2b30fe2d4759c199e3659d561a50f88a7fb2e
SHA-256	1c9e519dca0468a87322bebe2a06741136de7969a4eb3efda0ab8db83f0807b4

MD5	60f5bc820cf38e78b51e1e20fed290b5
SHA1	476489f75fed479f19bac02c79ce1befc62a6633
SHA256	69e48eb82ce7387d65cc1a82c5a6a170dc6121d479736b1dd33358d09c483617

Malicious Email accounts

Fake or breached email accounts, from which malicious messages were sent:

saeed.kn2003@gmail.com