Threat Group Uses Voice Changing Software in Espionage Attempt

cadosecurity.com/post/threat-group-uses-voice-changing-software-in-espionage-attempt

April 6, 2021

HamasCyberHQ.exe has been removed.

Blog

April 6, 2021

Today we are releasing a report detailing the activities of a Middle Eastern cyber espionage group that performs surveillance on their political opponents.

To execute this operation, the group employs well known social engineering methods. One is to send spear phishing emails with topics of interests to the targets – for example an invitation to a meeting. Another is to set up websites that impersonate news organisations and convince targets to download “articles”.

The third method is to ensnare their victims through conversations. As the conversations continue, the “women” offer up a “video” – laden with malware to infect the target’s system.

In a more modern twist, however, we found evidence of the group using voice changing software to enhance their operation. Below we analayse their toolset, which also includes tools to perform reconnaissance of targets and bulk-deliver malware to them.

The Server

Earlier in 2020 we reviewed a server previously identified as serving malware in targeted attacks. Those behind the attacks had made a misconfiguration on the server which made their attack toolset publicly available.

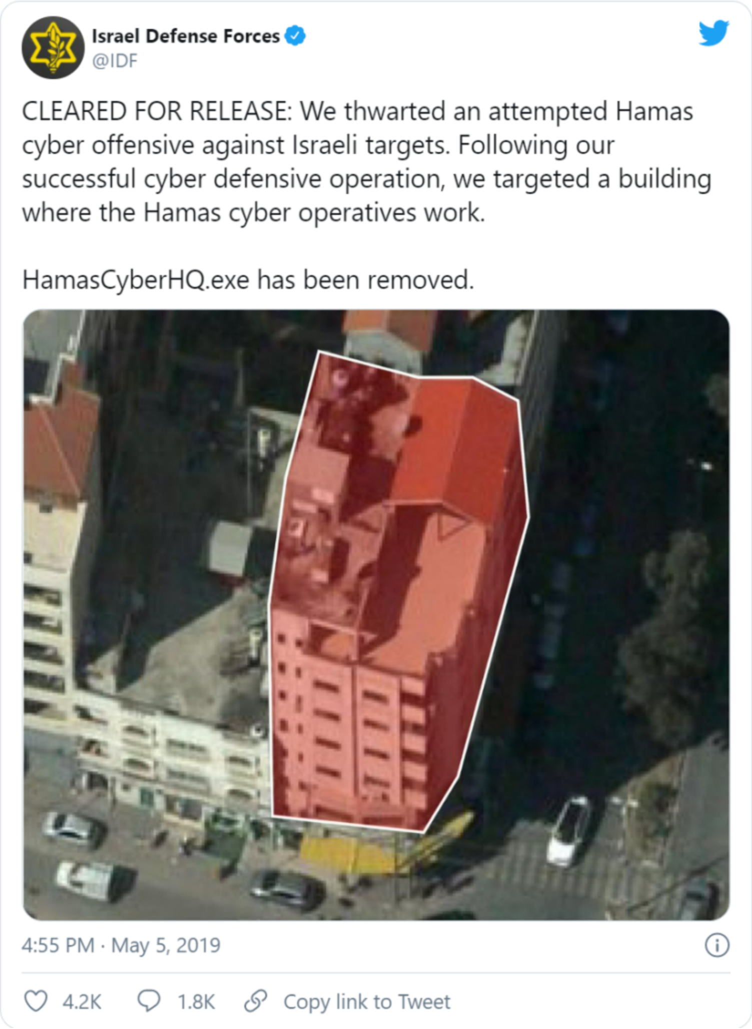
The attack toolset included:

- Malware used for espionage against political opponents
- Tools to identify vulnerable routers;
- A voice changing application;
- Custom tooling to use compromised email accounts to send phishing emails; and
- Phishing code for webmail logins

Background

The wider set of activity involved in the campaign we analyse below was previously described by Chinese Anti-Virus companies 360 Antivirus and Rising. Following on from other recent reporting, we refer to the attackers as APT-C-23.

Whilst there are a number of overlapping groups and members in the region, APT-C-23 are part of a larger group known as "Molerats" and are mostly located in Palestine. They have been reported on by the cyber-security industry as far back as 2012. Generally Molerats target political parties in Palestine and the Israeli government – but they also occasionally target Western Governments. They are perhaps best known for their alleged office being targeted by the IDF in 2019:



Israel Defense Forces
@IDF

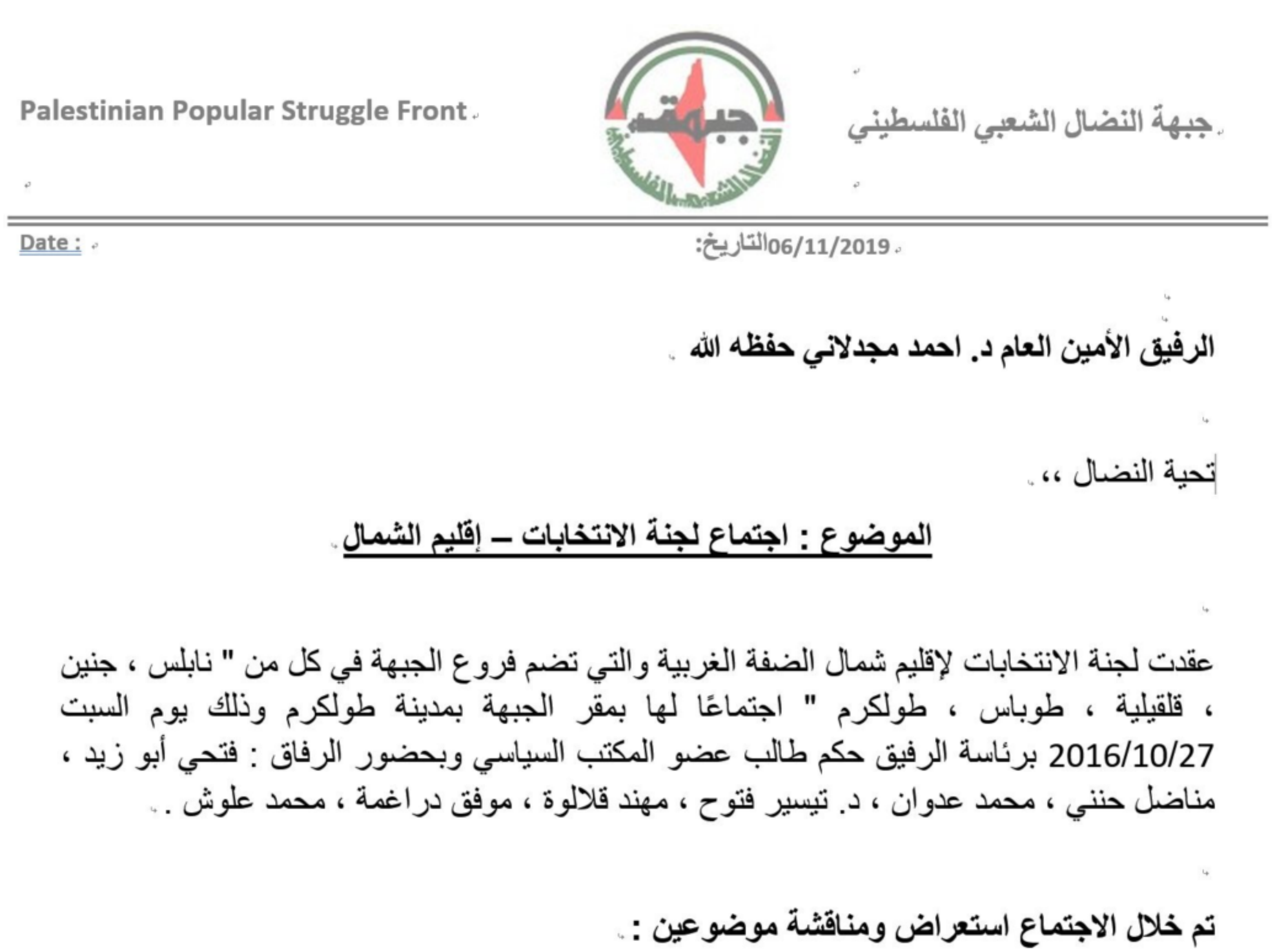
CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

4:55 PM · May 5, 2019

Malware

Others have already reported on the malware that communicates with the server in detail so we will be brief. There are a number of different families of malware but most start with a self extracting rar archive. The archives execute MSHTA/VBScript Downloaders used to install the commodity H-Worm backdoor. The filenames and decoy documents are mostly themed around Palestinian politics. We have included a sample of them in the Appendix.



Palestinian Popular Struggle Front

جبهة النضال الشعبي الفلسطيني

Date :

التاريخ:06/11/2019

الرفيق الأمين العام د. احمد مجدلاني حفظه الله

تحية النضال ،،

الموضوع : اجتماع لجنة الانتخابات – إقليم الشمال

عقدت لجنة الانتخابات لإقليم شمال الضفة الغربية والتي تضم فروع الجبهة في كل من " نابلس ، جنين ، قلقيلية ، طوباس ، طولكرم " اجتماعًا لها بمقر الجبهة بمدينة طولكرم وذلك يوم السبت 2016/10/27 برئاسة الرفيق حكم طالب عضو المكتب السياسي وبحضور الرفاق : فتحي أبو زيد ، مناضل حنني ، محمد عدوان ، د. تيسير فتوح ، مهند قلالوة ، موفق دراغمة ، محمد علوش .

تم خلال الاجتماع استعراض ومناقشة موضوعين :

The file اجتماع لجنة الانتخابات – إقليم الشمال.exe (Election Commission Meeting – Northern Territory .exe) at http://192.119.111[.]4/xx/dv

Phishing Toolset

APT-C-23 are a medium-sophistication group of attackers. They generally rely upon social engineering to convince targets to install their malware.

They have previously been known to impersonate women and target victims on social media to lure them into installing malware.

An article from February 2020 describes how they convinced soldiers in the Israel Defence Forces to install malware. That included using pre-recorded messages in Hebrew saying “Yes” and “No” – presumably as their Hebrew skills were limited.

“Over the last few months militants, who run the Gaza Strip, have attempted to woo soldiers on social media platforms including Telegram, WhatsApp, Facebook and Instagram.

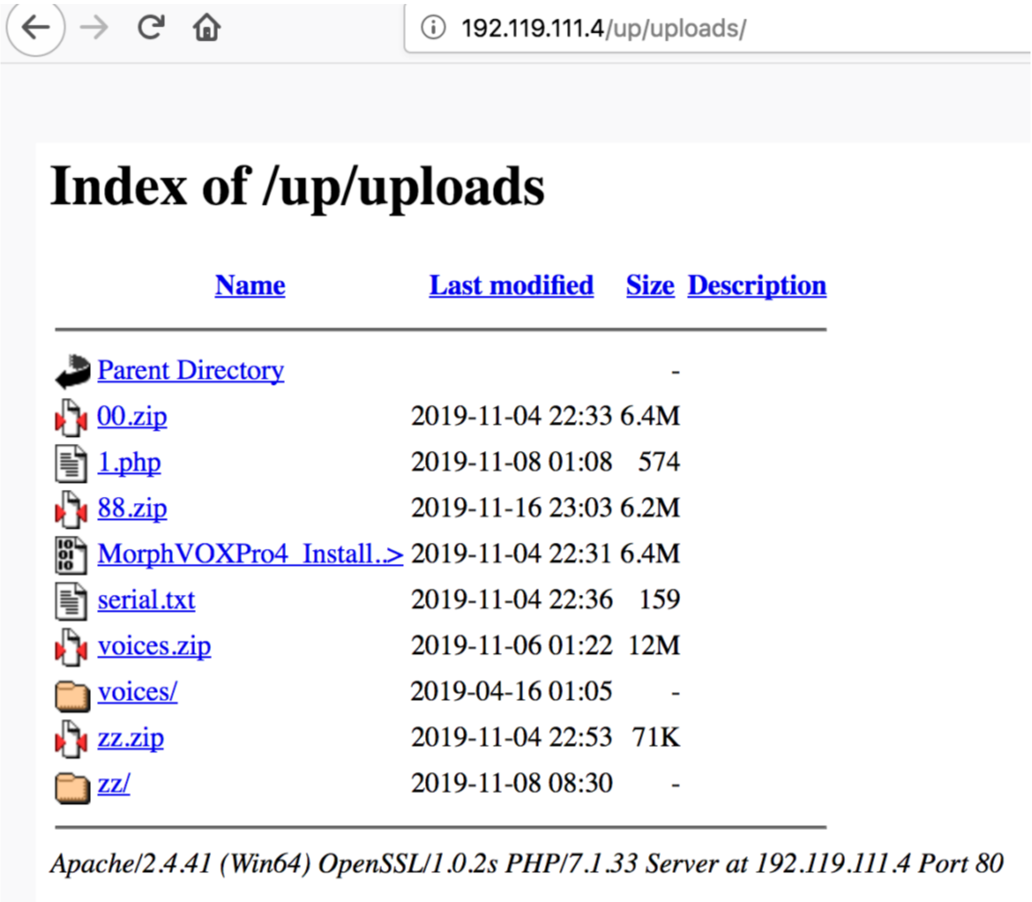
Using fake personas of attractive Israeli women, the militants behind the profiles claimed they were immigrants with hearing difficulties to explain why they could not speak on the phone, and why they were not fluent in Hebrew.

They also used Israeli slang in their communiques, doctored photos to prevent a reverse image search online and sent generic voice messages of women's voices saying "yes" and "no" to further bolster credibility.

As soon as the apps were downloaded it gave Hamas complete control over the phone: including transferring files to the Hamas server, allowing access to the phone's data, SMS messages, contacts, microphone and camera to remotely take pictures, Lt Col Conricus said."

As well as not speaking Hebrew, it's likely the attackers faced another problem impersonating women. A number of the people thought to be behind these attacks have previously been identified. All are men.

That may help to explain what we found in the folder "/up/uploads" on the public server:



192.119.111.4/up/uploads/

Index of /up/uploads

Name	Last modified	Size	Description
Parent Directory		-	
00.zip	2019-11-04 22:33	6.4M	
1.php	2019-11-08 01:08	574	
88.zip	2019-11-16 23:03	6.2M	
MorphVOXPro4_Install..>	2019-11-04 22:31	6.4M	
serial.txt	2019-11-04 22:36	159	
voices.zip	2019-11-06 01:22	12M	
voices/	2019-04-16 01:05	-	
zz.zip	2019-11-04 22:53	71K	
zz/	2019-11-08 08:30	-	

Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 Server at 192.119.111.4 Port 80

Figure 3: The public directory on the server 192.119.111[.]4

The file "88.zip" contains photos from the instagram account of a female model (we have blurred the photos):

The file “00.zip” contains the installation for Morph Vox Pro, a voice changing application, including a serial key and voices pack:

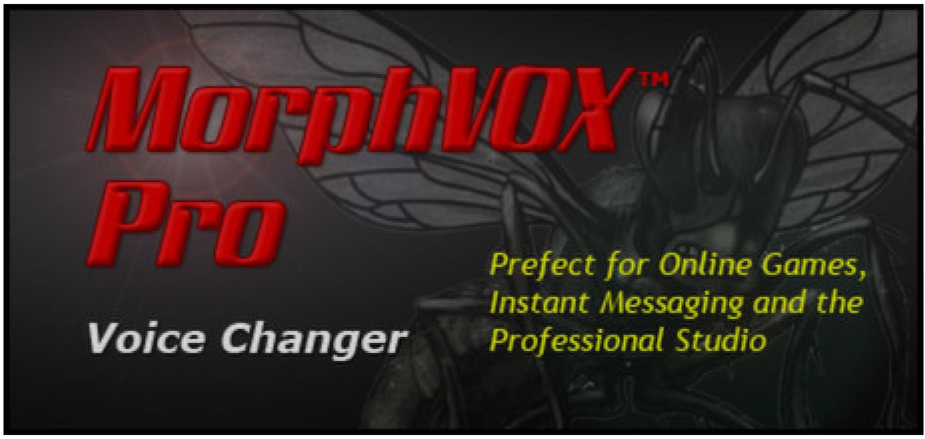
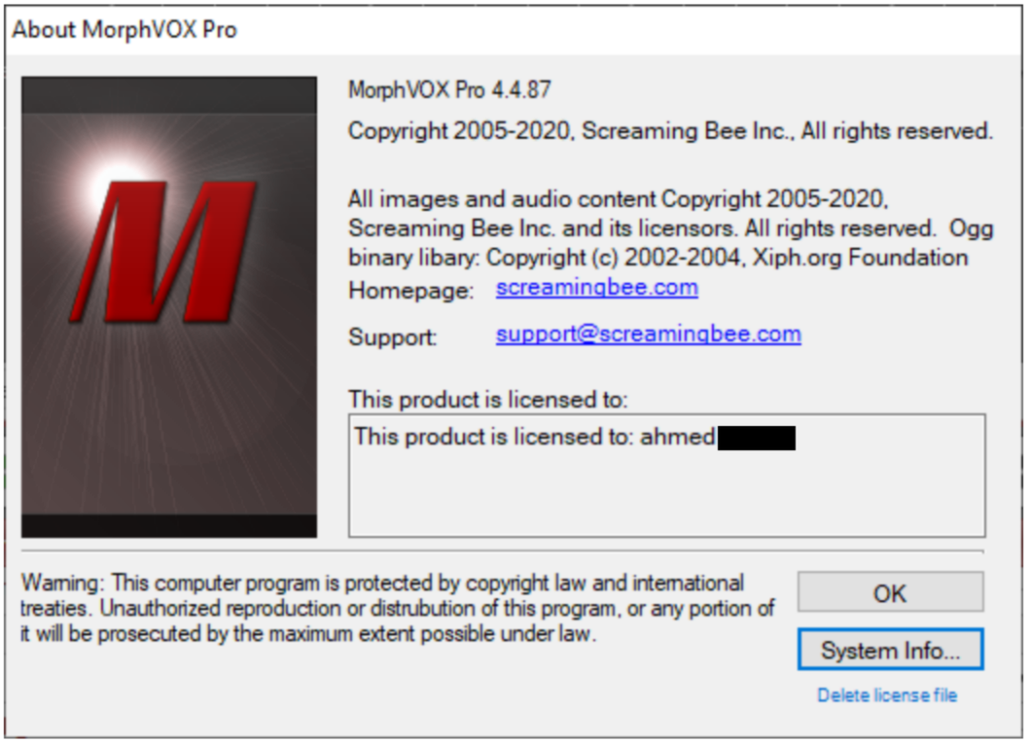

MorphVOX™
Pro
Voice Changer
Prefect for Online Games, Instant Messaging and the Professional Studio

Figure 4: Voice Changing application MorphVox Pro

The Serial Key is assigned to an “Ahmed [redacted]”:



About MorphVOX Pro

MorphVOX Pro 4.4.87

Copyright 2005-2020, Screaming Bee Inc., All rights reserved.

All images and audio content Copyright 2005-2020, Screaming Bee Inc. and its licensors. All rights reserved. Ogg binary libary: Copyright (c) 2002-2004, Xiph.org Foundation

Homepage: screamingbee.com

Support: support@screamingbee.com

This product is licensed to:

This product is licensed to: ahmed [redacted]

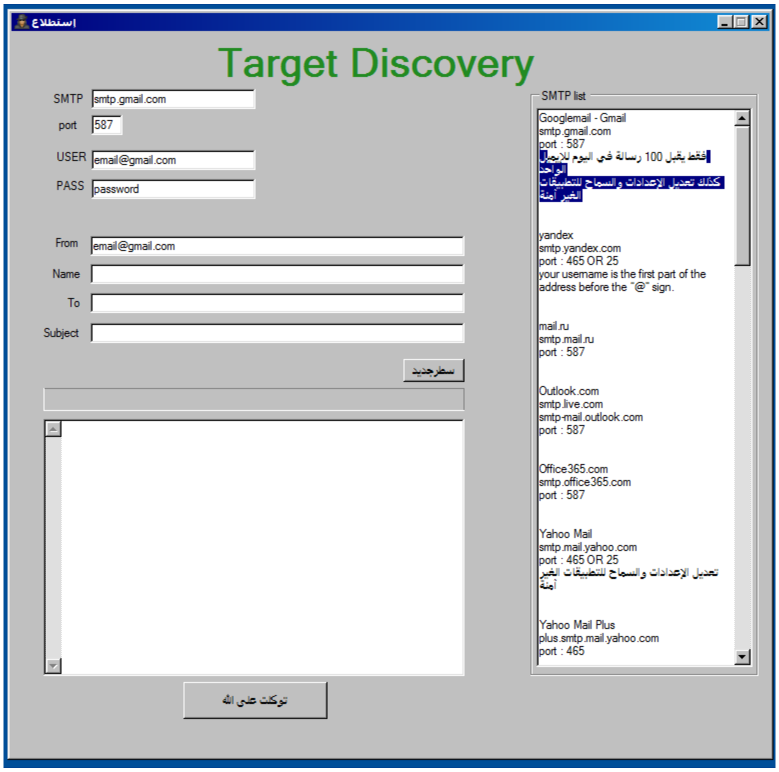
Warning: This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distrubution of this program, or any portion of it will be prosecuted by the maximum extent possible under law.

Given the context of both previous APT-C-23 attacks and the other contents of the folder, we think the most likely explanation for MorphVox being part of their toolset is that it was used to produce audio messages in a female voice to encourage targets to install their malware.

Other analysts have reported on manipulated images being used to enable misinformation in the wider Israeli-Palestinian Conflict. And there have been previous reports of fraudsters using DeepFake audio impersonations. But this is the first time we're aware of evidence, albeit indirect, of attackers using voice changing software to enable espionage.

Spearphish Delivery Tool

The server also provides information on how the attackers deliver their malware. The file recon.exe is used to bulk-send malicious phishing emails to targets:



SMTP smtp.gmail.com
port 587
USER email@gmail.com
PASS password
From email@gmail.com
Name
To
Subject

SMTP list

Googlemail - Gmail
smtp.gmail.com
port : 587
فقط يقبل 100 رسالة في اليوم للإيميل الواحد
كذلك تعديل الإعدادات والسماح للتطبيقات الغير آمنة

yandex
smtp.yandex.com
port : 465 OR 25
your username is the first part of the address before the "@" sign.

mail.ru
smtp.mail.ru
port : 587

Outlook.com
smtp.live.com
smtp-mail.outlook.com
port : 587

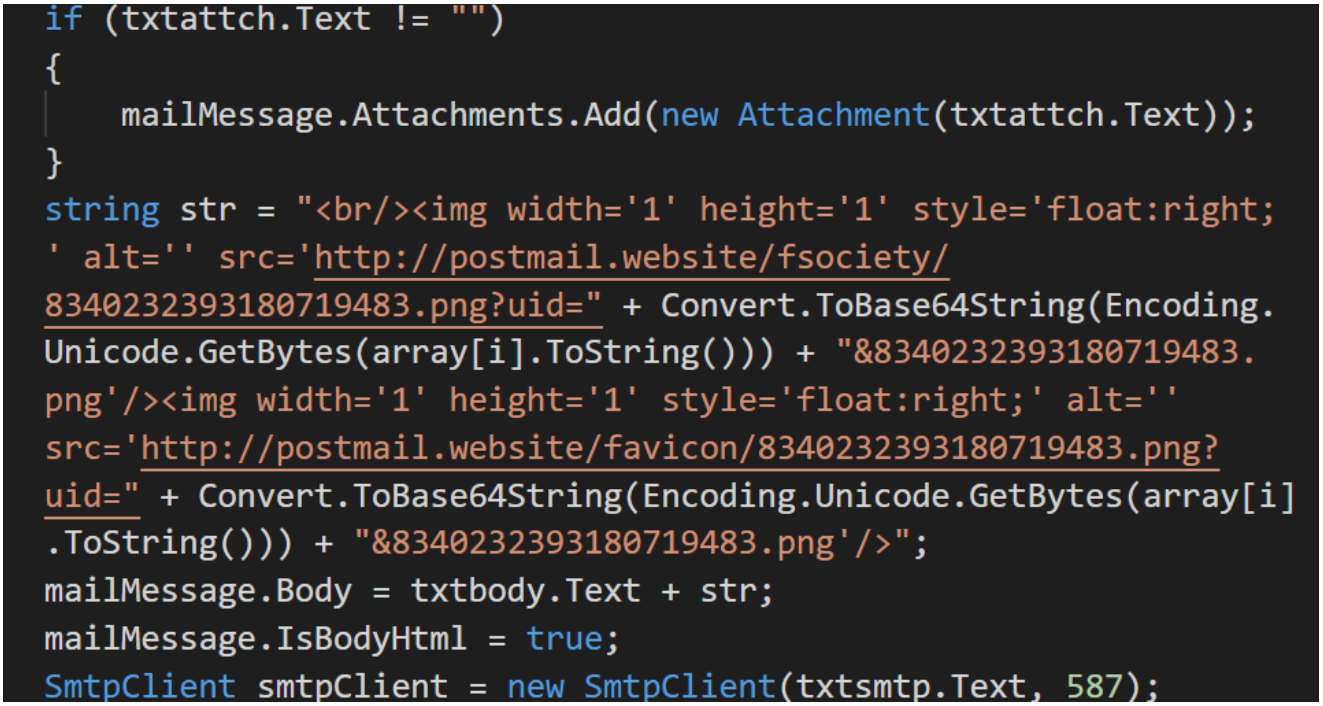
Office365.com
smtp.office365.com
port : 587

Yahoo Mail
smtp.mail.yahoo.com
port : 465 OR 25
تعديل الإعدادات والسماح للتطبيقات الغير آمنة

Yahoo Mail Plus
plus.smtp.mail.yahoo.com
port : 465

The application provides advice on how to send the emails, such as the maximum number of messages that can be sent from each mail provider.

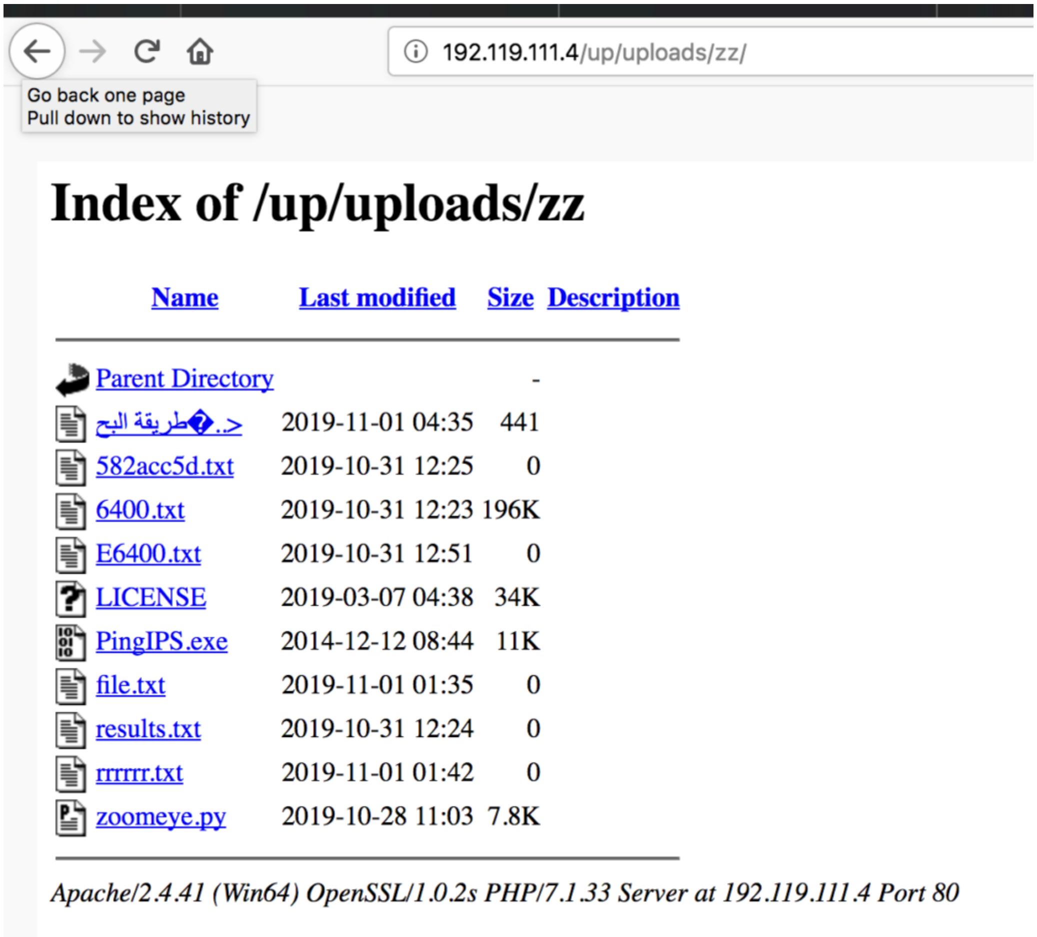
The source code for recon.exe shows that tracking images are also included in sent emails:



```
if (txtattch.Text != "")
{
    mailMessage.Attachments.Add(new Attachment(txtattch.Text));
}
string str = "<br/><img width='1' height='1' style='float:right;
' alt='' src='http://postmail.website/fsociety/
8340232393180719483.png?uid=" + Convert.ToBase64String(Encoding.
Unicode.GetBytes(array[i].ToString())) + "&8340232393180719483.
png'/><img width='1' height='1' style='float:right;' alt=''
src='http://postmail.website/favicon/8340232393180719483.png?
uid=" + Convert.ToBase64String(Encoding.Unicode.GetBytes(array[i]
.ToString())) + "&8340232393180719483.png'/>";
mailMessage.Body = txtbody.Text + str;
mailMessage.IsBodyHtml = true;
SmtpClient smtpClient = new SmtpClient(txtsmtp.Text, 587);
```

Router Exploitation

Another folder, called “zz”, included another interesting mix of tools:

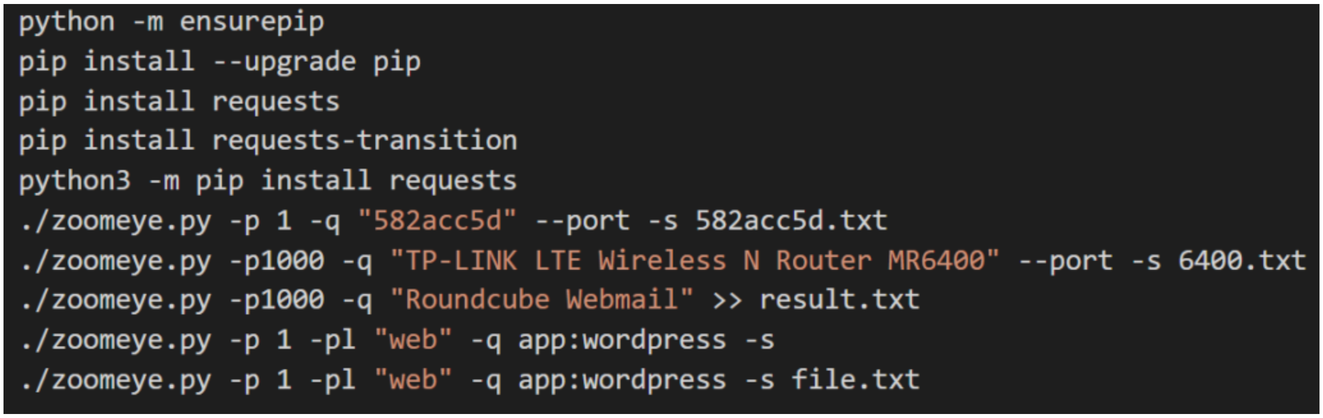


Index of /up/uploads/zz

Name	Last modified	Size	Description
Parent Directory		-	
طريقة البح�..>	2019-11-01 04:35	441	
582acc5d.txt	2019-10-31 12:25	0	
6400.txt	2019-10-31 12:23	196K	
E6400.txt	2019-10-31 12:51	0	
LICENSE	2019-03-07 04:38	34K	
PingIPS.exe	2014-12-12 08:44	11K	
file.txt	2019-11-01 01:35	0	
results.txt	2019-10-31 12:24	0	
rrrrrr.txt	2019-11-01 01:42	0	
zoomeye.py	2019-10-28 11:03	7.8K	

Apache/2.4.41 (Win64) OpenSSL/1.0.2s PHP/7.1.33 Server at 192.119.111.4 Port 80

The file طريقة البحث.txt or “Research Method.txt” contains example commands to find vulnerable routers using the ZoomEye internet scanning service:



```
python -m ensurepip
pip install --upgrade pip
pip install requests
pip install requests-transition
python3 -m pip install requests
./zoomeye.py -p 1 -q "582acc5d" --port -s 582acc5d.txt
./zoomeye.py -p1000 -q "TP-LINK LTE Wireless N Router MR6400" --port -s 6400.txt
./zoomeye.py -p1000 -q "Roundcube Webmail" >> result.txt
./zoomeye.py -p 1 -pl "web" -q app:wordpress -s
./zoomeye.py -p 1 -pl "web" -q app:wordpress -s file.txt
```

The file PingIPs.exe is part of an attack toolset that we’ve seen previously. It was uploaded to VirusTotal from a IP address in Palestine. It includes a custom GUI and password list for SipVicious – a tool to hack Voice over IP systems.

Other Tools

The folder “support” contained a credential phishing page for Microsoft accounts. It sends stolen credentials to https://www.hotmiali[.]com/master/login/login

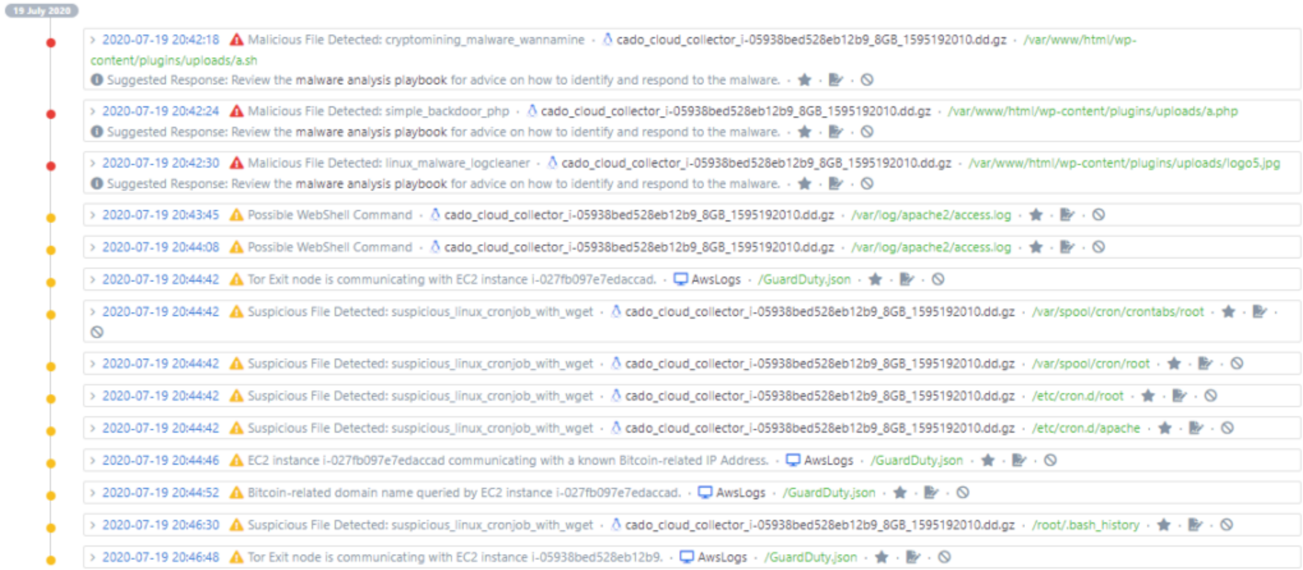
Detection and Response

The malware described in this report is generally well detected by anti-virus, and we have provided indicators of compromise in the Appendix.

US-CERT provides advice on how to avoid falling victim to social engineering attacks. You should always be particularly suspicious of anyone you haven't met asking you to download files, and avoid installing Mobile applications that are not from the official Google or Apple stores.

About Cado Security

Cado Security specialises in providing tooling and techniques that allow organisations to threat hunt and investigate cloud and container systems.



```
19 July 2020
2020-07-19 20:42:18 Malicious File Detected: cryptomining_malware_wannamine · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/www/html/wp-content/plugins/uploads/a.sh
Suggested Response: Review the malware analysis playbook for advice on how to identify and respond to the malware.
2020-07-19 20:42:24 Malicious File Detected: simple_backdoor_php · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/www/html/wp-content/plugins/uploads/a.php
Suggested Response: Review the malware analysis playbook for advice on how to identify and respond to the malware.
2020-07-19 20:42:30 Malicious File Detected: linux_malware_logcleaner · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/www/html/wp-content/plugins/uploads/logo5.jpg
Suggested Response: Review the malware analysis playbook for advice on how to identify and respond to the malware.
2020-07-19 20:43:45 Possible WebShell Command · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/log/apache2/access.log
2020-07-19 20:44:08 Possible WebShell Command · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/log/apache2/access.log
2020-07-19 20:44:42 Tor Exit node is communicating with EC2 instance i-027fb097e7edaccad. · AwsLogs · /GuardDuty.json
2020-07-19 20:44:42 Suspicious File Detected: suspicious_linux_cronjob_with_wget · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/spool/cron/crontabs/root
2020-07-19 20:44:42 Suspicious File Detected: suspicious_linux_cronjob_with_wget · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /var/spool/cron/root
2020-07-19 20:44:42 Suspicious File Detected: suspicious_linux_cronjob_with_wget · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /etc/cron.d/root
2020-07-19 20:44:42 Suspicious File Detected: suspicious_linux_cronjob_with_wget · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /etc/cron.d/apache
2020-07-19 20:44:46 EC2 instance i-027fb097e7edaccad communicating with a known Bitcoin-related IP Address. · AwsLogs · /GuardDuty.json
2020-07-19 20:44:52 Bitcoin-related domain name queried by EC2 instance i-027fb097e7edaccad. · AwsLogs · /GuardDuty.json
2020-07-19 20:46:30 Suspicious File Detected: suspicious_linux_cronjob_with_wget · cado_cloud_collector_i-05938bed528eb12b9_8GB_1595192010.dd.gz · /root/.bash_history
2020-07-19 20:46:48 Tor Exit node is communicating with EC2 instance i-05938bed528eb12b9. · AwsLogs · /GuardDuty.json
```

If you are interested in knowing more, please don't hesitate to reach out, our pilot program is now open.

References

https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-operation-arid-viper.pdf

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2015/09/20081818/Cyberattack_against_Israeli_and_Palestinian_targets.pdf

https://www.clearskysec.com/wp-content/uploads/2016/01/Operation%20DustySky_TLP_WHITE.pdf

https://unit42.paloaltonetworks.com/unit42-targeted-attacks-middle-east-using-kasperagent-micropsia/

https://blog.lookout.com/frozencell-mobile-threat https://www.virusbulletin.com/uploads/pdf/conference_slides/2018/FinkelsteinKayal-VB2018-APTC23.pdf

https://ddanchev.blogspot.com/2019/05/exposing-yet-another-currently-active.html

https://www.jpost.com/israel-news/idf-foils-hamas-operation-targeting-soldiers-operation-rebound-617744

https://cybersecurity.att.com/blogs/labs-research/alien-labs-2019-analysis-of-threat-groups-molerats-and-apt-c-37

https://www.clearskysec.com/glancelove/

https://web.archive.org/web/20170311074704/https://www.idfblog.com/2017/01/11/hamas-fake-facebook-profiles-target-israeli-soldiers/

https://www.timesofisrael.com/idf-warns-soldiers-hamas-trying-to-spy-on-them-with-fake-dating-world-cup-apps/

https://www.timesofisrael.com/idf-hamas-hacked-soldiers-phones-by-posing-as-pretty-girls/

https://www.timesofisrael.com/idf-hamas-again-tries-to-catfish-soldiers-with-fake-women-on-social-media/

https://www.cybereason.com/hubfs/dam/collateral/reports/Molerats-in-the-Cloud-New-Malware-Arsenal-Abuses-Cloud-Platforms-in-Middle-East-Espionage-Campaign.pdf

Indicators of Compromise
mslove.mypressonline[.]com
postmail[.]website
israanews.zz.com[.]ve
adamnews.for[.]ug
martnews.aba[.]ae
fateh.aba[.]ae
mmksba100.linkpc[.]net
new2019.mine[.]nu
webhoptest.webhop[.]info
mmksba.simple-url[.]com
mmksba.dyndns[.]org
formore.for-more[.]biz

Palestinian Status Assessment 2019.exe
B6a31f6c12c2a51b507be44ce14b39728e38a63392b0f327dbbc4b71785d6148
Circulating.exe

7d3386e0659e1a7be0588b2401c9f8b54831be4d131b9ee89d43b98361331364
safaratt.exe
3c9f7f5ca27cb2c376a70d0aa2bd19b2008702e7c03c0802d8b9140fa712390e

(Served from https://drive.google[.]com/uc?export=download&id=1cZc93fSqdHXvUPJnSVfEsHiIE6gSoZx7)

03d82852bbb28d1740e50206e7726c006b9b984a8309e2f203e65a67d7d3bcad
ed7e46b0cf27b8f728cdd71a7c4ae98afde8d2e63f0817eb322c8e77bdd767c5
e15a9edb83570ecf5a77db28ee365a9498f522eab3c89d6dce4b9644571e9344
e04869dc0ad21a83279655bff6ac4d78262269c94766198e7e947beb99c13025
cab92dd0d3fea724edd141f5cc5ebc5758a10acead18c238a0b8cb747a991f8c
94b95524fe91cba52371bd41a81be4643458fe4402401ab10699005254de1c5d
367853e84f366ca08a437e10fda28dae42f3863af359736c46f018dac0c529be
01b9d12713708ea911df3798eed67a5ae682b474c7390a0f7053791c479c8ed1
3853e0bf00d6dbfc574bc0564f0c90b93a66d644dd4dc8b8c00564f0b6edf581
B767d0e9892cf7b554e74bc7d0d26d64a3262959763ddc0efd525abc2addc375

About The Author

Chris Doman

Chris is well known for building the popular threat intelligence portal ThreatCrowd, which subsequently merged into the AlienVault Open Threat Exchange, later acquired by AT&T. Chris is an industry leading threat researcher and has published a number of widely read articles and papers on targeted cyber attacks. His research on topics such as the North Korean government's crypto-currency theft schemes, and China's attacks against dissident websites, have been widely discussed in the media. He has also given interviews to print, radio and TV such as CNN and BBC News.

About Cado Security

Cado Security provides *the* cloud investigation platform that empowers security teams to respond to threats at cloud speed. By automating data capture and processing across cloud and container environments, Cado Response effortlessly delivers forensic-level detail and unprecedented context to simplify cloud investigation and response. Backed by Blossom Capital and Ten Eleven Ventures, Cado Security has offices in the United States and United Kingdom. For more information, please visit https://www.cadosecurity.com/ or follow us on Twitter @cadosecurity.

Prev Post Next Post