АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Спам-кампания “Love you” перенацелена на Японию

5 февраля 2019 года

Изучая свежую волну спама в России, мы обратили внимание на другую атаку. С середины января 2019 года известная кампания “Love you” доработана и перенацелена на Японию, где используется для распространения шифратора GandCrab 5.1.

По данным телеметрии, последняя версия “Love you” запущена 28 января 2019 года, ее активность примерно вдвое превысила первоначальную (см. график ниже). Как и в середине января, с помощью спама распространяется набор вредоносных полезных нагрузок с некоторыми обновлениями. Так, мы видели попытки загрузки криптомайнера, ПО для изменения системных настроек, вредоносного загрузчика, червя Phorpiex, а также шифратора GandCrab версии 5.1.

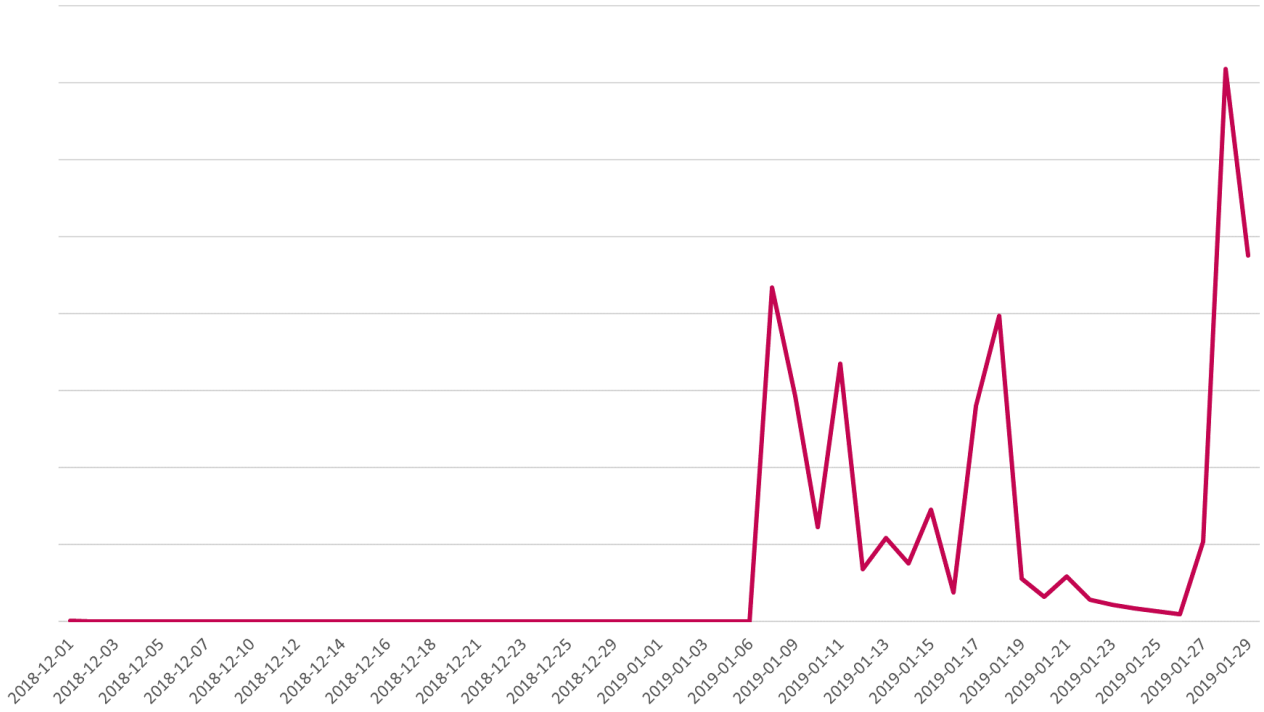

Рисунок 1. Детектирование вредоносных вложений JavaScript, распространяемых в кампании "Love you" и ее последней волне

По состоянию на 29 января 2019 года подавляющее большинство обнаружений приходится на Японию (95%), каждый час детектируются десятки тысяч вредоносных писем. В тот же день JS/Danger.ScriptAttachment (по классификации ESET — вредоносный JavaScript, распространяемый через вложения электронной почты) был четвертой по числу обнаружений угрозой в мире и угрозой №1 в Японии (см. ниже).

Top Threats

Japan | Day | More | JSON / XML / DOC

	Threat Name	Change	Prevalence Level	
1	JS/Danger.ScriptAttachment	▲	39.2 %	Map-Timeline
2	HTML/ScrInject	▼	10.02 %	Map-Timeline
3	JS/Adware.Agent.AA	▼	7.23 %	Map-Timeline
4	SMB/Exploit.DoublePulsar	▼	5.58 %	Map-Timeline
5	JS/Redirector	▼	2.41 %	Map-Timeline
6	HTML/Refresh	▼	1.94 %	Map-Timeline
7	JS/CoinMiner	▼	1.94 %	Map-Timeline
8	VBA/TrojanDownloader.Agent.MHD	▼	1.73 %	Map-Timeline
9	HTML/FakeAlert	▼	1.61 %	Map-Timeline
10	VBS/TrojanDownloader.Agent.PWC	▼	1.26 %	Map-Timeline

Japan | Day | More | JSON / XML / DOC

Рисунок 2. JS/Danger.ScriptAttachment был угрозой №1 в Японии по состоянию на 29 января

Сценарий атаки

В последней кампании атакующие изменили тексты рассылок, перейдя от «Love You» в теме письма к заголовкам, связанным с Японией. Прежним осталось множество смайлов в теме и теле письма.

Темы писем, которые мы видели в ходе анализа:

— Yui Aragaki ;)
— Kyary Pamyu Pamyu ;)
— Kyoko Fukada ;)
— Yuriko Yoshitaka ;)
— Sheena Ringo ;)
— Misia ;)
(японские звезды шоу-бизнеса)

Изученные вредоносные вложения представляют собой ZIP-архивы, замаскированные под изображения с именами формата PIC0-[9-digit-number]2019-jpg.zip. На рисунке ниже представлены примеры таких писем.

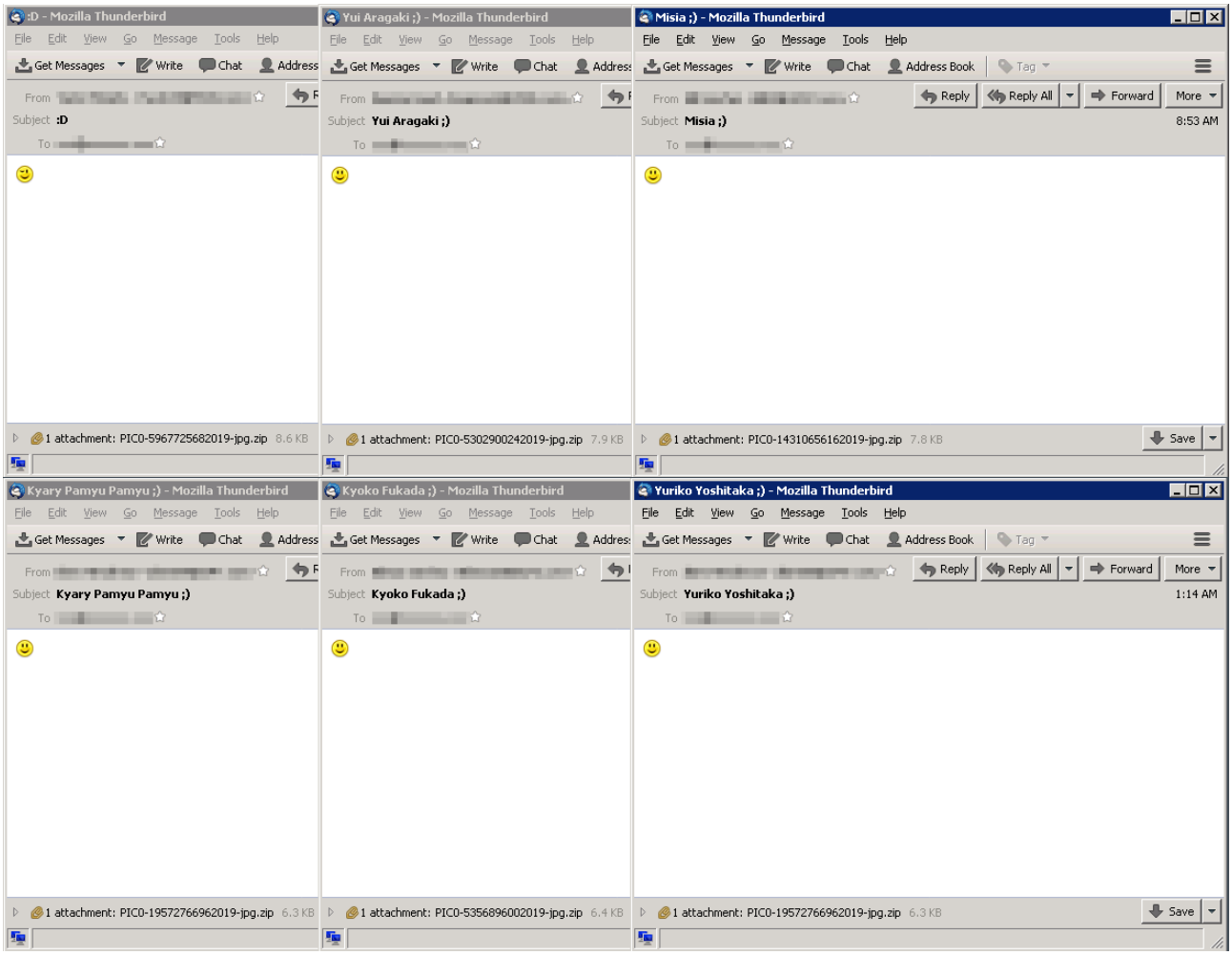

Рисунок 3. Примеры спам-писем из «японской» кампании

ZIP-архив содержит JavaScript-файл с именем в том же формате, но заканчивающимся только на .js. После извлечения и запуска JavaScript загружает полезную нагрузку первого этапа с C&C-сервера атакующих – EXE-файл, детектируемый продуктами ESET как Win32/TrojanDownloader.Agent.EJN. URL-адреса, на которых размещена эта полезная нагрузка, имеют путь, заканчивающийся на bl*wj*b.exe (имя файла изменено) и krabler.exe; эта полезная нагрузка загружается в C:\Users\[username]\AppData\Local\Temp[random].exe.

Полезная нагрузка первого этапа скачивает одну из следующих финальных полезных нагрузок с того же C&C-сервера:

— шифратор GandCrab версии 5.1
— криптомайнер
— червь Phorpiex
— загрузчик, работающий в соответствии с языковыми настройками (скачивает полезную нагрузку только в том случае, если языковые настройки зараженного компьютера соответствуют Китаю, Вьетнаму, Южной Корее, Японии, Турции, Германии, Австралии или Великобритании)
— ПО для изменения системных настроек

GandCrab 5.1 шифрует файлы, добавляя случайное расширение из пяти символов к их именам. Требования выкупа, содержащие это расширение в именах файлов и их содержимом, создаются в каждой папке, затронутой шифратором.

```
---=    GANDCRAB V5.1    =---

**********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED**********************

        *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****

Attention!

All your files, documents, photos, databases and other important files are encrypted and have the extension: .XSXEWH

The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.


The server with your key is in a closed network TOR. You can get there by the following ways:

-------------------------------------------------------------------------------------

| 0. Download Tor browser - https://www.torproject.org/

| 1. Install Tor browser
| 2. Open Tor Browser
| 3. Open link in TOR browser:   http://gandcrabmfe6mnef.onion/34571e618494ffbb
| 4. Follow the instructions on this page

-------------------------------------------------------------------------------------


On our page you will see instructions on payment and get the opportunity to decrypt 1 file for free.


ATTENTION!

IN ORDER TO PREVENT DATA DAMAGE:

* DO NOT MODIFY ENCRYPTED FILES
* DO NOT CHANGE DATA BELOW

---BEGIN GANDCRAB KEY---
lAQAABonidc2J8EaQjmatZ+R8rFechyrh5A0xwIS6bP01UVIw4RbhB7/Vw6/XSoAUHWa+5scfVrIXVa5BwxIKBt861dzaUPLMyt56Mt8uvNbTIfFASFkqdZaHYHJuN45b6XJAOgJzudgMZ6/25Bpi1xBiF5zFvk55f2Vl
HXR8q2OXRs7zDOzoUnkMr9mnVLLCuofmoof/4m8ramT8e8YVzR8VO+C8KYT1SEp/5yk557w147f66Mvc/78NiaiMTiIhYeF4qqIMRx6H1uqKzZlfYIvv2UoSrV4Sj24Wyu/3yDQQpEMCPSJPpYsX/NaMwVW1I3JPlu2fa
QuW4lcp1GWS37HHYDKsAYnq9wxzVwxXABT4oMW1mposDCMUP7/fwcbbj00vQW29sd65pp3jZdlYQKKHG7U5UO7rGldfQ76ZwXu85FqgGyd7rUhhLUeqwtyzRP7d3J1XTJ4duT8xy/aEGntsQ+kNR1igD3LBZ9ZKXE8NZt
---END GANDCRAB KEY---
```

Рисунок 4. Требование выкупа GandCrab v5.1

Полезная нагрузка данной кампании скачивается с IP-адреса 92.63.197[.]153, геолокация которого соответствует Украине. Адрес использовался в кампании “Love you” с середины января.

АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

Индикаторы компрометации

Примеры хешей вредоносных вложений ZIP

```
8551C5F6BCA1B34D8BE6F1D392A41E91EEA9158B
BAAA91F700587BEA6FC469FD68BD8DE08A65D5C7
9CE6131C0313F6DD7E3A56D30C74D9E8E426D831
83A0D471C6425DE421145424E60F9B90B201A3DF
57F94E450E2A504837F70D7B6E8E58CDDFA2B026
```

Детектирование ESET: JS/Danger.ScriptAttachment

Примеры хешей загрузчиков JavaScript

```
cfe6331bdbd150a8cf9808f0b10e0fad4de5cda2
c50f080689d9fb2ff6e731f72e18b8fe605f35e8
750474ff726bdbd34ffc223f430b021e6a356dd7
1445ea29bd624527517bfd34a7b7c0f1cf1787f6
791a9770daaf8454782d01a9308f0709576f75f9
```

Детектирование ESET: JS/TrojanDownloader.Agent.SYW или JS/TrojanDownloader.Nemucod.EDK

Примеры хешей полезной нагрузки первого этапа

```
47C1F1B9DC715D6054772B028AD5C8DF00A73FFC
```

Детектирование ESET: Win32/TrojanDownloader.Agent.EJN

Примеры хешей финальной полезной нагрузки

Шифратор GandCrab `885159F6F04133157871E1D9AA7D764BFF0F04A3` Win32/Filecoder.GandCrab.E
Криптомайнер `14E8A0B57410B31A8A4195D34BED49829EBD47E9` Win32/CoinMiner.BEX
Червь Phorpiex `D6DC8ED8B551C040869CD830B237320FD2E3434A` Win32/Phorpiex.J
Загрузчик `AEC1D93E25B077896FF4A3001E7B3DA61DA21D7D` Win32/TrojanDownloader.Agent.EEQ
ПО для изменения системных настроек `979CCEC1DF757DCF30576E56287FCAD606C7FD2C` Win32/Agent.VQU

C&C-сервер, используемый в кампании

```
92.63.197[.]153
```