SANS ISC: InfoSec Handlers Diary Blog - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training InfoSec Handlers Diary Blog

Ransomware news: GlobeImposter gets a facelift, GandCrab is still out there

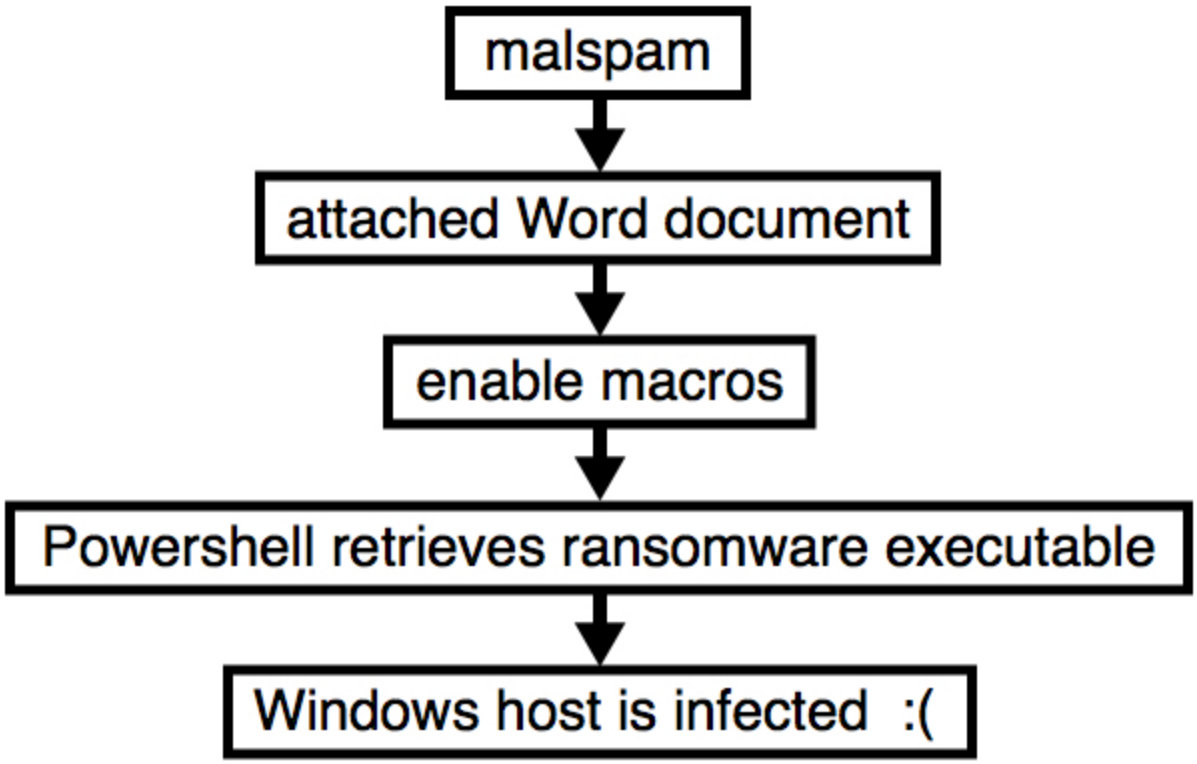
Published: 2018-03-07
Last Updated: 2018-03-07 03:53:31 UTC
by Brad Duncan (Version: 1)

Introduction

I recently found a wave of malicious spam (malspam) that started as early as Monday 2018-03-05 at 18:28 UTC and lasted through at least Tuesday 2018-03-06 at 14:44 UTC. This wave of malspam had Word documents as file attachments, and these Word docs had macros designed to infect Windows hosts with ransomware. When I checked Monday evening, I infected one of my lab hosts with GlobeImposter ransomware. When I checked Tuesday morning, I saw GandCrab ransomware.

This is interesting, because in 2018, I've seen very few examples of mass-distribution malspam pushing ransomware. So far in 2018, such malspam has been pushing mostly information stealers, backdoors, and cryptocurrency miners. So it's always noteworthy when I find something like this.

Today's diary examines this wave of malspam, the infection traffic, and associated indicators.



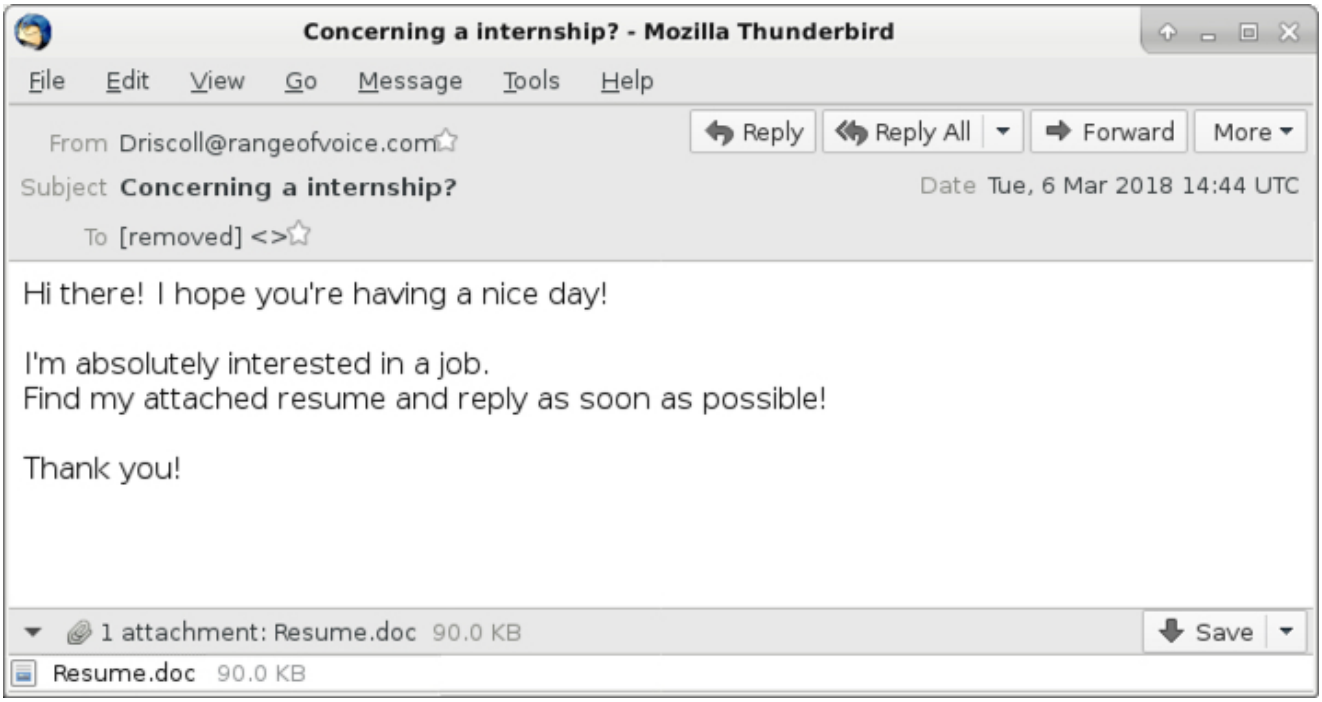
Shown above: Flow chart for an infection from this malspam.

The emails

Patterns for these emails were consistent, but I couldn't match them to a specific campaign. Sending addresses, subject lines, email headers, and message text were all varied. The only consistent part of this malspam was the Word document attachments, which were all named " Resume.doc" with a space before the first letter. And even then, each attachment had a different file hash.

Date/Time	Received: from	Sending address	Subject	Attachment
2018-03-05 18:28 UTC	mta4.latestlog.com ([142.44.146.4])	Shelia@latestlog.com	About a internship.	Resume.doc
2018-03-05 18:56 UTC	mta10.codemefast.com ([66.70.229.10])	Marquetta@codemefast.com	About a job.	Resume.doc
2018-03-05 21:17 UTC	mta10.deliverpatern.com ([142.44.148.10])	Keysha@deliverpatern.com	Concerning a internship?	Resume.doc
2018-03-05 22:48 UTC	mta228.csvforyou.com ([142.44.148.228])	Jon@csvforyou.com	About a position?	Resume.doc
2018-03-05 22:57 UTC	mta10.deliverpatern.com ([142.44.148.10])	Lelah@deliverpatern.com	Regarding a position?	Resume.doc
2018-03-05 23:46 UTC	mta23.codemefast.com ([66.70.229.23])	Gwendoline@codemefast.com	Regarding a job.	Resume.doc
2018-03-05 23:54 UTC	mta82.rangeofvoice.com ([66.70.229.82])	Prissy@rangeofvoice.com	Regarding a job.	Resume.doc
2018-03-05 23:56 UTC	mta96.latestchance.com ([142.44.148.96])	Dina@latestchance.com	Regarding a career.	Resume.doc
2018-03-05 23:57 UTC	mta82.rangeofvoice.com ([66.70.229.82])	Kory@rangeofvoice.com	Concerning a position.	Resume.doc
2018-03-06 00:01 UTC	mta242.captchaworker.com ([142.44.146.242])	Willa@captchaworker.com	About a career?	Resume.doc
2018-03-06 01:11 UTC	mta2.latestlog.com ([142.44.146.2])	Lillian@latestlog.com	Concerning a position?	Resume.doc
2018-03-06 02:50 UTC	mta27.latestlog.com ([142.44.146.27])	July@latestlog.com	Concerning a career!	Resume.doc
2018-03-06 04:11 UTC	mta159.captchaworker.com ([142.44.146.159])	Kina@captchaworker.com	Regarding a position?	Resume.doc
2018-03-06 05:03 UTC	mta217.youthgraphic.com ([66.70.229.217])	Bindy@youthgraphic.com	Regarding a internship.	Resume.doc
2018-03-06 07:35 UTC	mta109.rangeofvoice.com ([66.70.229.109])	Ewart@rangeofvoice.com	Concerning a career?	Resume.doc
2018-03-06 08:51 UTC	mta29.codemefast.com ([66.70.229.29])	tarla@codemefast.com	About a career!	Resume.doc
2018-03-06 09:43 UTC	mta100.latestchance.com ([142.44.148.100])	Gaenor@latestchance.com	Regarding a position?	Resume.doc
2018-03-06 11:32 UTC	mta58.codemefast.com ([66.70.229.58])	Eugenia@codemefast.com	About a internship!	Resume.doc
2018-03-06 12:37 UTC	mta54.latestlog.com ([142.44.146.54])	Oscar@latestlog.com	Concerning a job!	Resume.doc
2018-03-06 13:05 UTC	mta232.csvforyou.com ([142.44.148.232])	Faviola@csvforyou.com	Concerning a job.	Resume.doc
2018-03-06 13:10 UTC	mta178.typesettingsforyou.com ([66.70.229.178])	Maura@typesettingsforyou.com	About a job?	Resume.doc
2018-03-06 13:14 UTC	mta4.latestlog.com ([142.44.146.4])	Amy@latestlog.com	Regarding a job.	Resume.doc
2018-03-06 14:04 UTC	mta1.latestlog.com ([142.44.146.1])	Jason@latestlog.com	Concerning a internship!	Resume.doc
2018-03-06 14:44 UTC	mta88.rangeofvoice.com ([66.70.229.88])	Driscoll@rangeofvoice.com	Concerning a internship?	Resume.doc

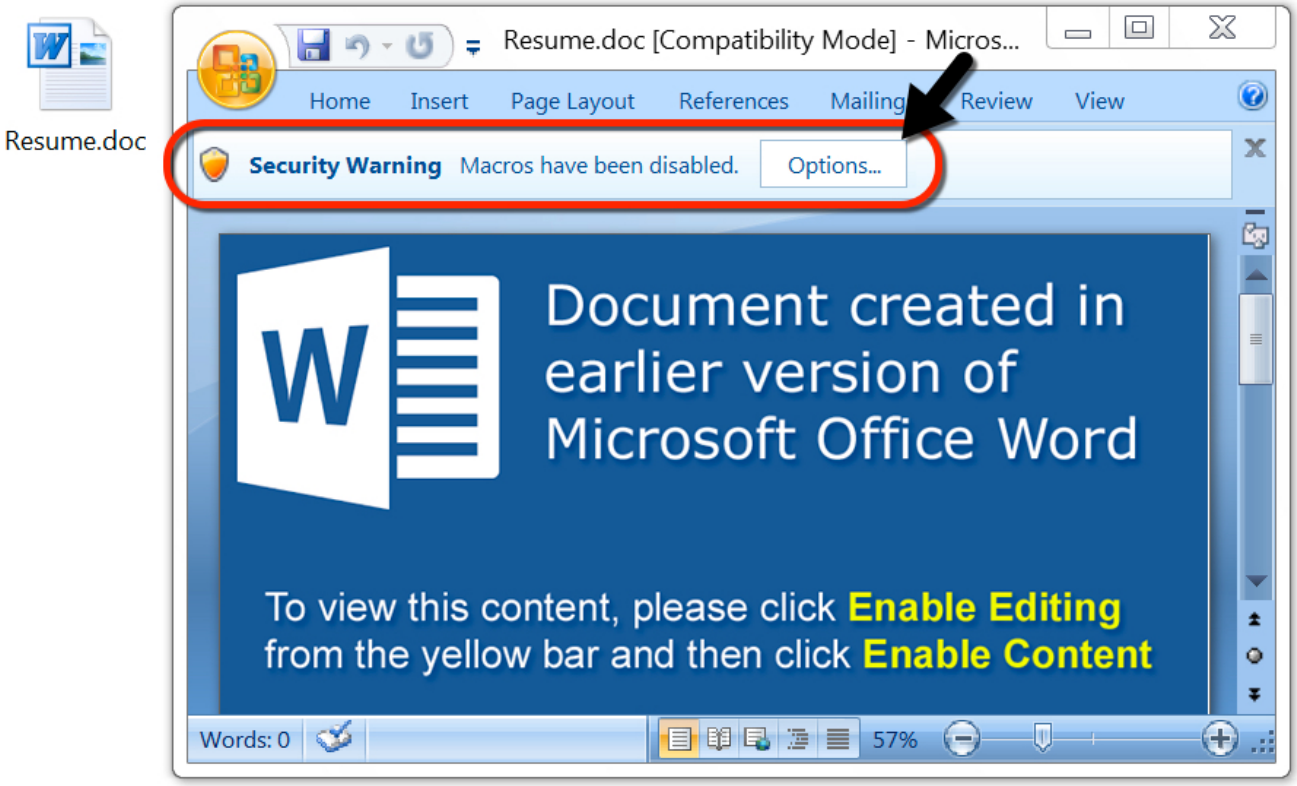
Shown above: Screenshot from the spreadsheet tracker with 24 email samples.



Shown above: Screenshot from one of the emails.

The attachments

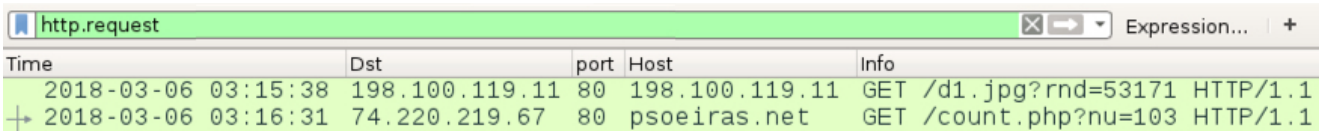
The attachments were typical Word documents with malicious macros. They work similar to malicious macros seen in other malspam campaigns, using Powershell to retrieve a malware binary to infect a vulnerable Windows host.



Shown above: One of the attached Word documents.

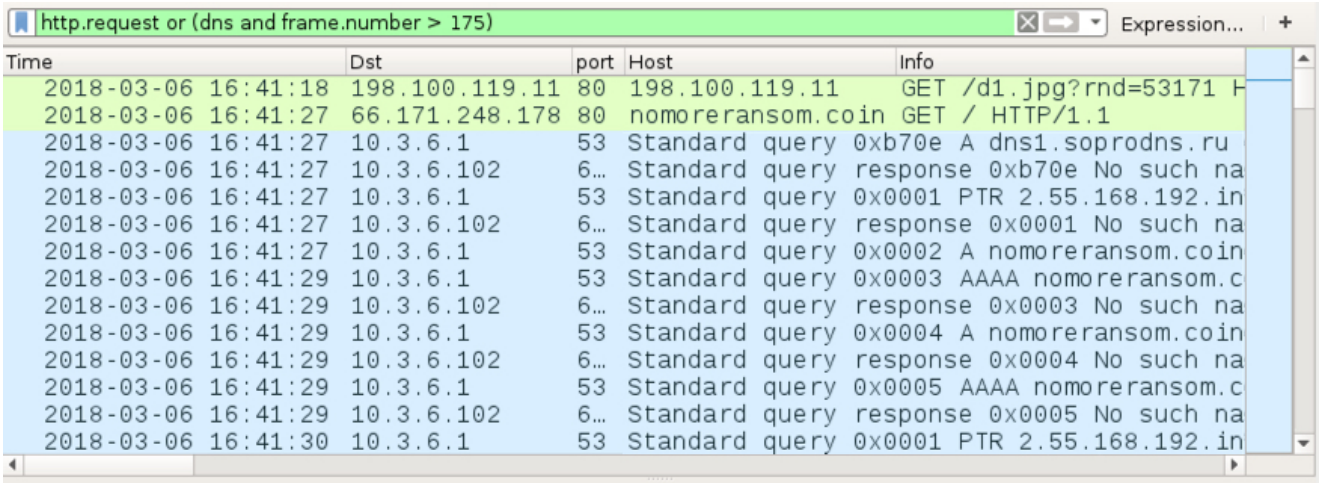
The traffic

Infection traffic from Monday evening showed indicators of GlobeImposter ransomware. After the macro used Powershell to retrieve the ransomware binary from a server at 198.100.119.11, I saw an HTTP request to ***psoeiras.net*** for an IP address check. The URL to ***psoeiras.net*** was similar to what I've documented before with GlobeImposter ransomware infections.



Shown above: Traffic from an infection filtered in Wireshark on Monday evening (US time).

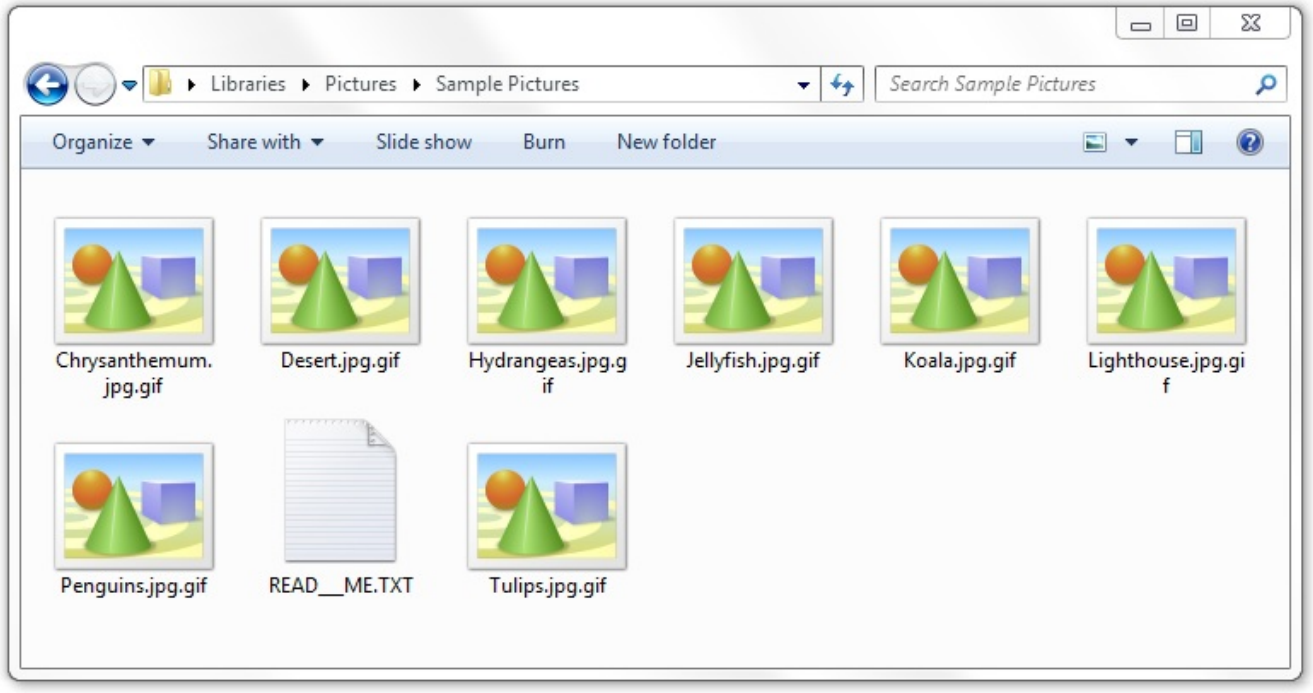
When I checked again Tuesday morning, I saw the same URL to 198.100.119.11 for a ransomware binary However, this time, the follow-up HTTP request for the IP address check went to ***nomoreransom.coin***, with follow-up DNS queries for ***nomoreransom.bit*** and ***gandcrab.bit***. These domains are typical for what I've previously documented with GandCrab ransomware.



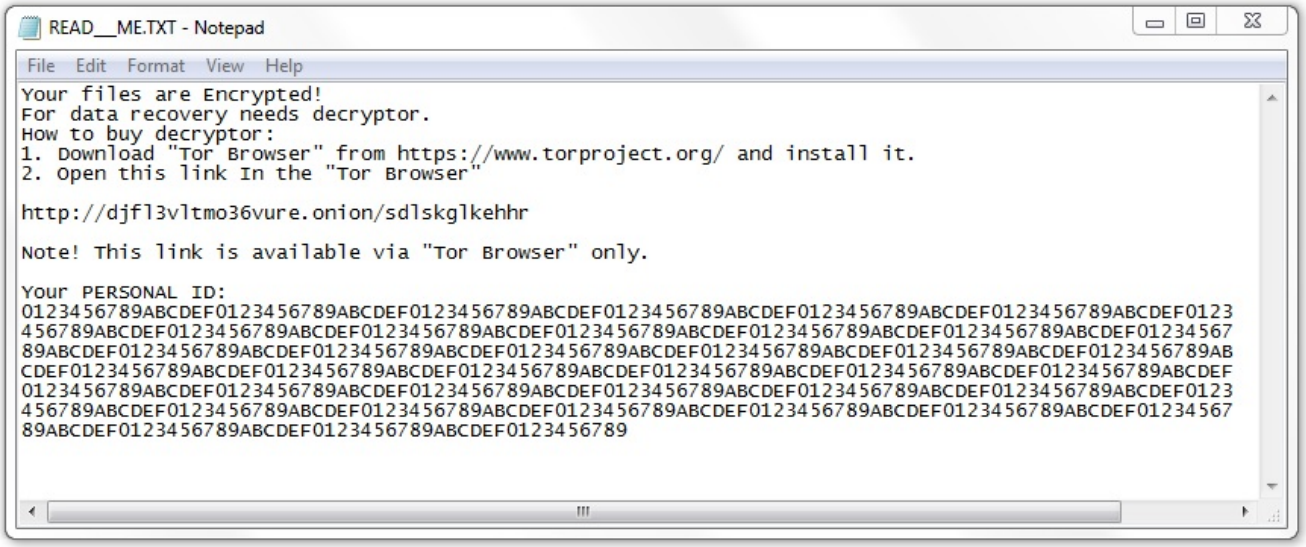
Shown above: Traffic from an infection filtered in Wireshark on Tuesday morning (US time).

Forensics on an infected Windows host

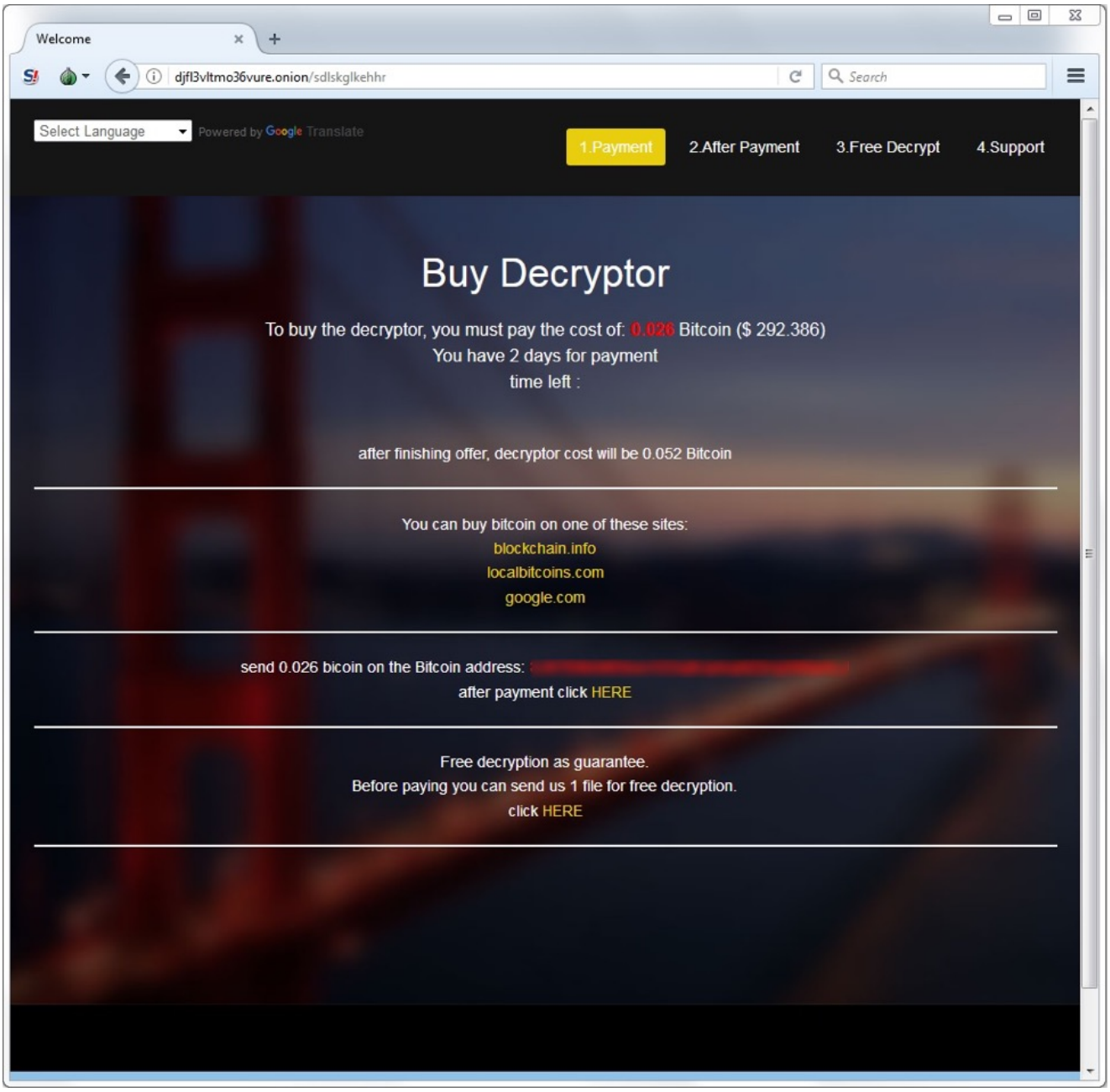
The GandCrab ransomware sample didn't encrypt any files on my lab host, but the GlobeImposter binary did. All files encrypted by the GlobeImposter sample used a ***.gif*** file extension. Previous samples of GlobeImposter I'd tested in December 2017 used ***Read__ME.html*** for the decryption instructions, but this 2018 sample used ***Read__ME.txt***. The GlobeImposter decryptor seen through my Tor browser had a visual upgrade with a nice background image, but it still had the same basic setup as before.



Shown above: Encrypted files on a Windows host infected with GlobeImposter.

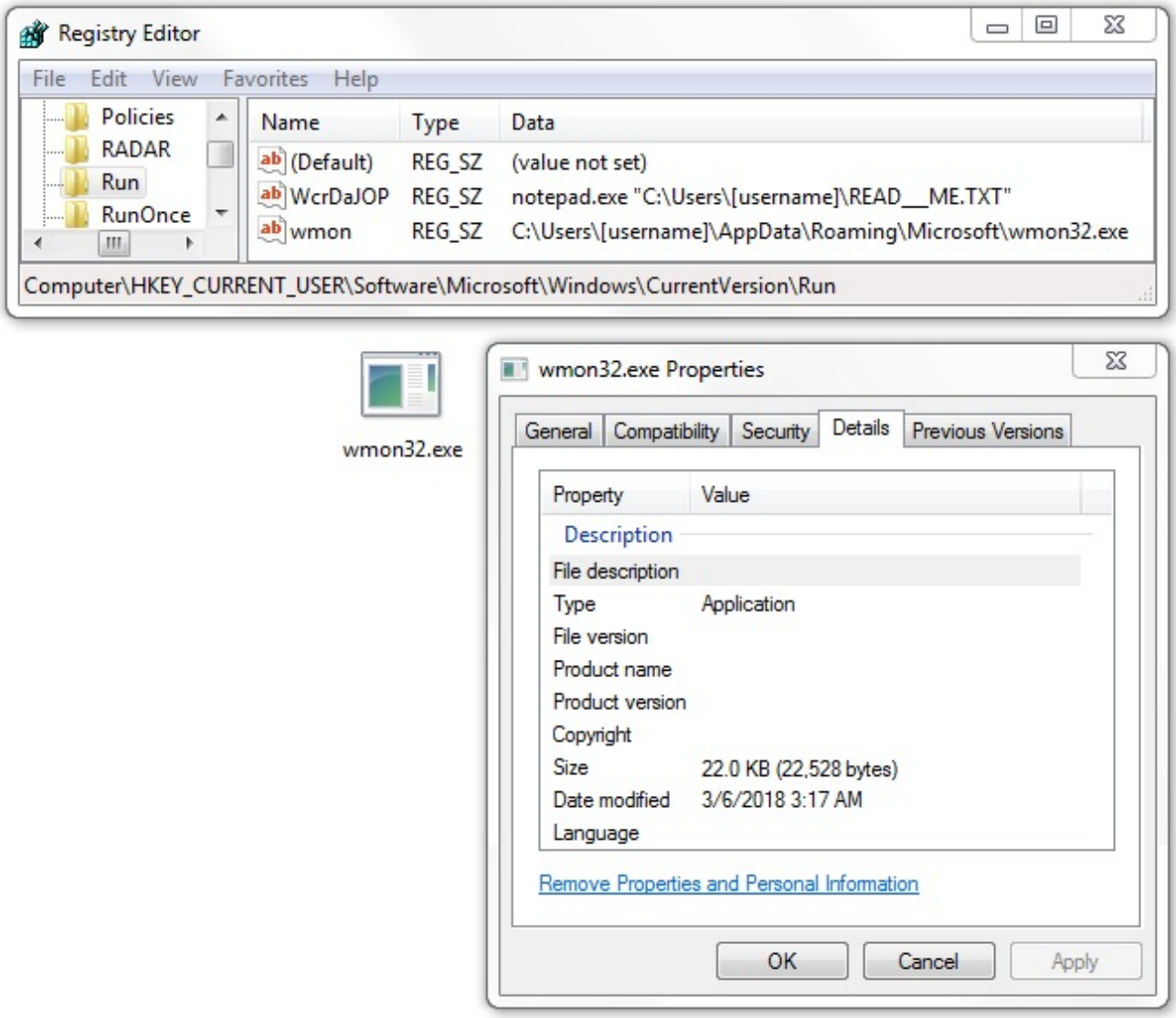


Shown above: GlobeImposter decryption instructions.



Shown above: GlobeImposter decryptor viewed on a Tor browser.

The GlobeImposter infection stayed persistent on my infected lab host through the Windows registry. Like many malware samples I've seen, this one used the ***HKCU\Software\Microsoft\Windows\CurrentVersion\Run*** registry key. However, the binary used for persistence was not the same binary used during the initial infection. The persistent binary for this GlobeImposter infection was only 22,528 bytes.



Shown above: Malware made persistent on my host infected with GlobeImposter.

Indicators

See below for a list of URLs, domains, and file hashes associated with this malspam.

SHA256 hashes for all attachments named " Resume.doc":

- 02d9a2643082ee6751472cfbe4760a3d9afb00a263c698eca3b748d012fcb66a
- 05ec663bd1c8521f48affc6dfebf0a6fe410711b70096b5c4be2bac37c7f262b
- 4027d8bad7ae8b5f2a88f414417ced73a50ee5fa0d60bf4d5395dc8953037b3c
- 43d2c9efb6cc5907f7c04c719e83c3404b629bbf849c83fb053b6f23ddf84d81
- 4b4ade15d6ed8eba53d1064170dee191e07da1baafeeecc3b8fdb4803a44a628
- 50994124ce7d6ebc5b59b29e4278eb78997726d8e6cb902a8ccc437e4fda1a6d
- 5490b18af502fa3a576ff5612eefff34dd75edd7bd567519f2b25da1d885de60
- 56e6c1521070d58e525bad12d222c04952676c4b0d77136c9720a3263f9c557f
- 6242c95fed475bc708c49b2bb7ad292f43d42fbcbd0b68502db01ea4a44ae656
- 63f070add2cd6b6a6c212c82f1003b35fd45c4ae8787a2da2ec9e16c5e16c0e5

- 69e706c4ddcd8ea4e9f0745e5bdcef760b0e553549bf26526ef51746244f292c
- 6a193b0362506748a165b320f72bcd2d149760d66f287bc2271f30328a11181e
- 72d18a2df77c75fc3949f34c37e0339039a211e2086fab5c92d2b41064fb5030
- 75e92c7e36ff1cac3cff5b11426916d64b7956022cb668f4f675f3f2fc0e7fe7
- 767b6094e57e940540192fceb1fe31c8311588d998d6f71a4099623fec0d5488
- 92e56ae3f7f014ae8f348e0dc6c2a68936dc878d56e4c9b777202a9000fd6899
- 9d41bb0167c7a19d69be0eb29920054e9b8cfa132a89129b31ecaa3338887e1d
- a77afbcc935a6c0290e0a290f10913f343be31d955ce7f2f2446e605a0d89165
- a84730972266ee371c8a5b9906102842f9834b6bd36413f8e15808aa79d1c136
- a96c1911b31beaa2d6fedc654fb568e0ee82160d439e4ac38d53c24a441b0436
- b8ccfed35c590ab7bb1fd619eb085905515fde9c6dff7f592b391a516f8cc52a
- cb32fc84a036ab47b60569b3fdc718de9858555b349c90e188a8b7cd4602a264
- ee6b7d944abaec4cb3bc2780489f81d337724164d76c2056d37cc225ea57a6d5

The following are malware samples retrieved from my infected lab hosts:

SHA256 hash:
61bed70b1568fce8dc67c91bab1884027631bdf2c8b8ba63d54ce32d7e429a76
- File size: 223,744 bytes
- File location: C:\Users*[username]*\AppData\Local\Temp\41097.exe
- File description: GandCrab ransomware

SHA256 hash:
d6535b7caf79cc9b624e5f8878aa1d8717bdd84778fde47caad4ed75e322ef97
- File size: 867,840 bytes
- File location: C:\Users*[username]*\AppData\Local\Temp\41097.exe
- File description: GlobeImposter ransomware

SHA256 hash:
41056643ee135ac0fce3237d69b32370102887b22c0250e2e0b515b25f525183
- File size: 22,528 bytes
- File location: C:\Users*[username]*\AppData\Roaming\Microsoft\wmon32.exe
- File description: Executable persistent for the GlobeImposter ransomware infection

The following are URLs and domains associated with these infections:

- 198.100.119.11 port 80 - ***198.100.119.11*** - GET /d1.jpg?rnd=53171 (returned ransomware binaries)
- 74.220.219.67 port 80 - ***psoeiras.net*** - GET /count.php?nu=103 (IP address check from GlobeImposter)
- 66.171.248.178 port 80 - ***nomoreransom.coin*** - GET / (IP address check from GandCrab)
- ***nomoreransom.bit*** (domain associated with GandCrab)

- ***gandcrab.bit*** (domain associated with GandCrab)
- ***hxxp://djfl3vltmo36vure.onion/sdlskglkehhr*** (GlobeImposter decryptor)

Final words

Although ransomware is down compared to last year, every once in a while we still see a wave of malspam like this, pushing recent ransomware families seen in prior mass-distribution campaigns. So far in 2018, GlobeImposter and GandCrab are the only ones I've seen in mass-distribution malspam. However, these recent samples don't seem to be any more dangerous now than they were before.

As always, properly-administered Windows hosts are unlikely to get infected. To infect their computers, users would have to ignore multiple warnings to retrieve and activate the malicious Word document, which includes bypassing Protected View. System administrators and the technically inclined can also implement best practices like Software Restriction Policies (SRP) or AppLocker to prevent these types of infections.

Pcap and malware samples for today's diary can be found here.

Brad Duncan
brad [at] malware-traffic-analysis.net

Keywords: