FireEye

Click It Up: Targeting Local Government Payment Portals

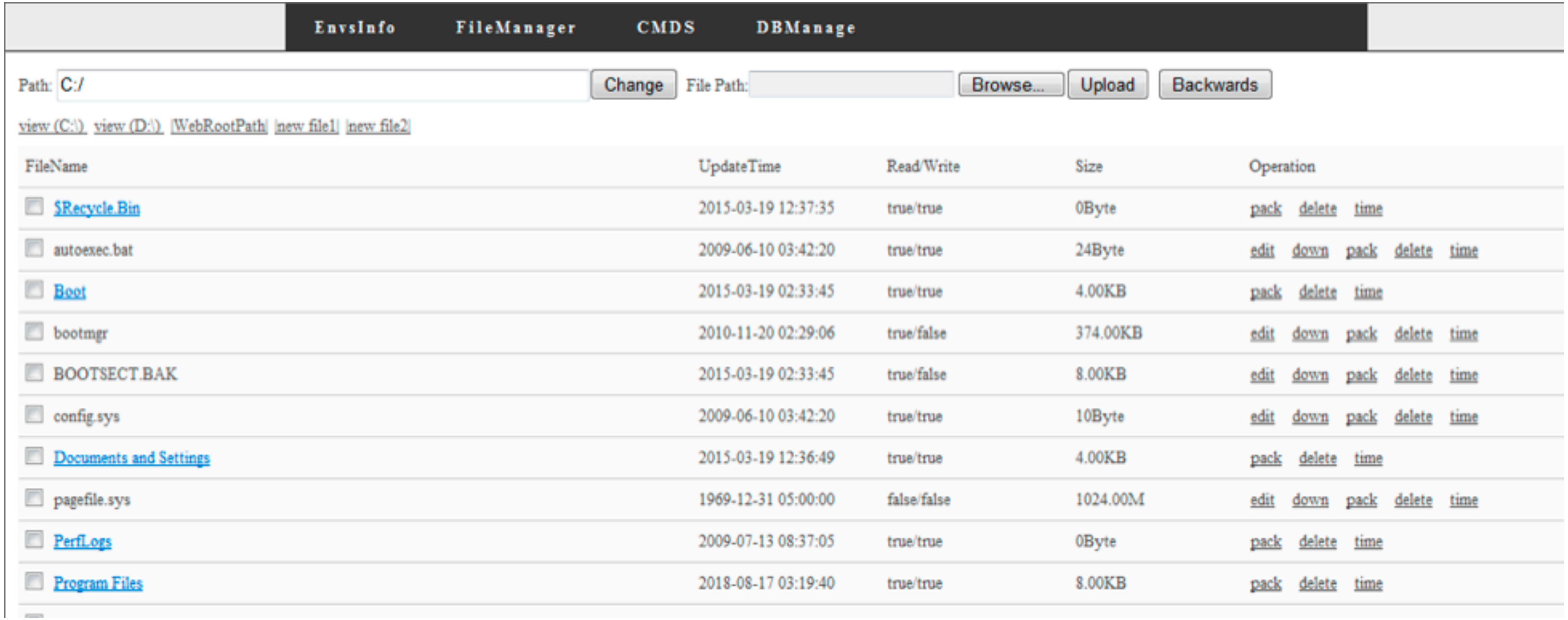
Nick Richard, Principal Threat Intelligence Analyst

CASE STUDY OVERVIEW

- Targeting on-premise Click2Gov instantiations since October 2017
- Exploit WebLogic vulnerability
- Upload SJavaWebManage webshell
- Install FIREALARM and harvest payment card data via console
- Upgrade to SPOTLIGHT, sniffed HTTP traffic for payment card data
- Get paid

https://www.fireeye.com/blog/threat-research/2018/09/click-it-up-targeting-local-government-payment-portals.html

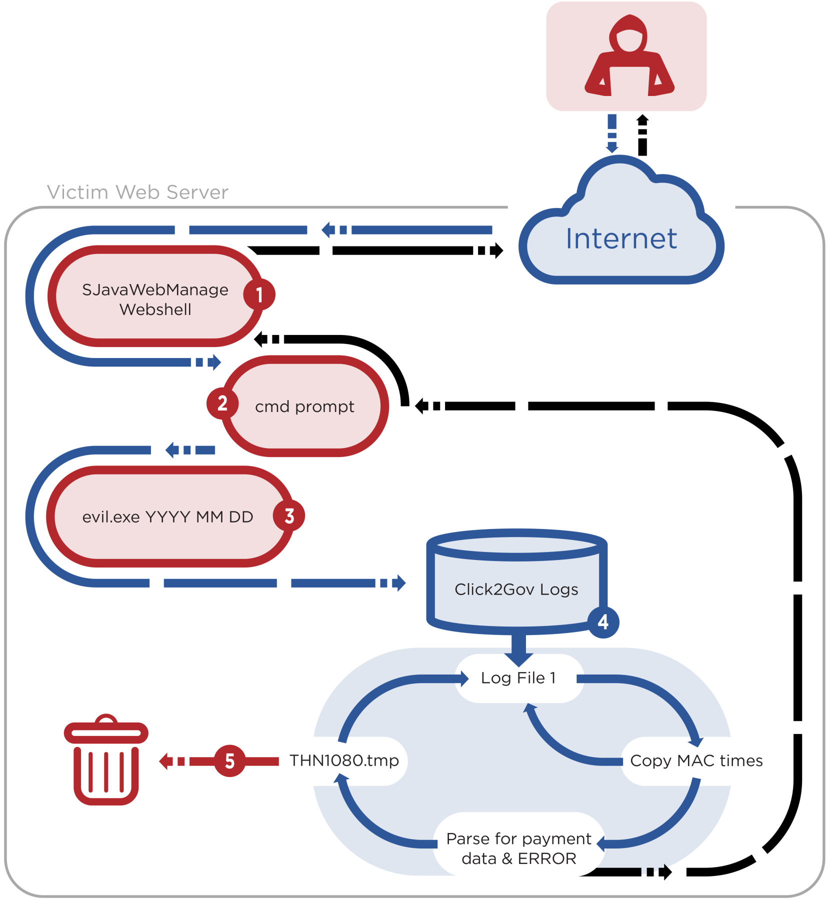
SJavaWebManage



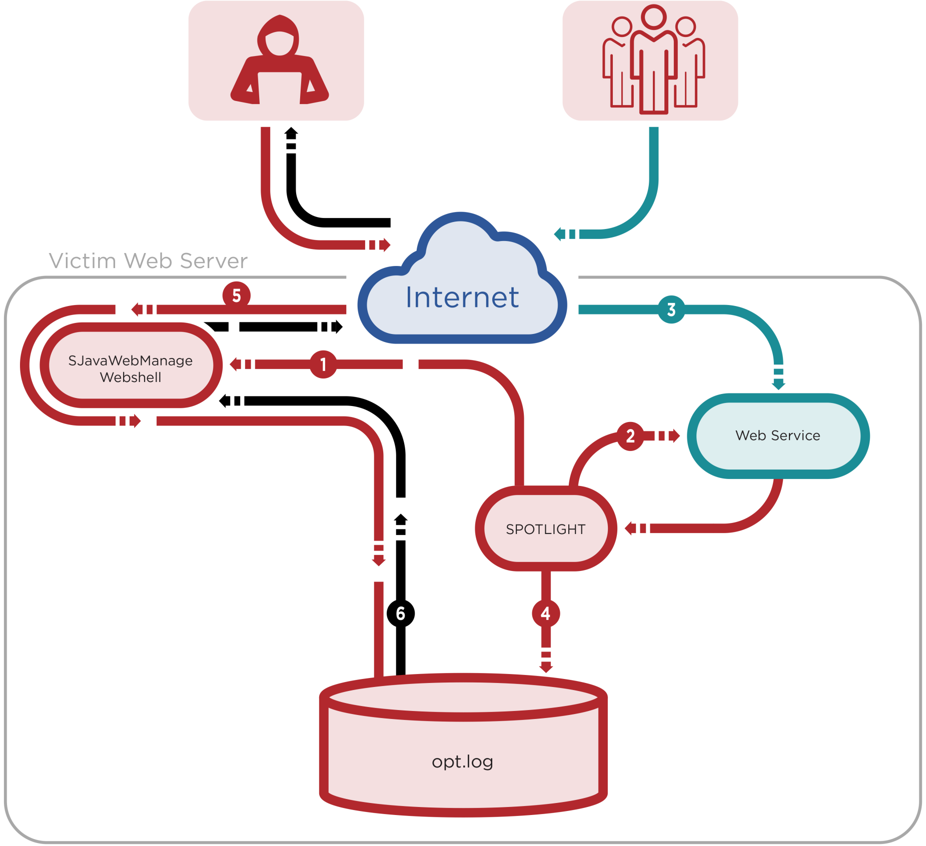
Path: C:/

FileName	UpdateTime	Read/Write	Size	Operation
□ $Recycle.Bin	2015-03-19 12:37:35	true/true	0Byte	pack delete time
□ autoexec.bat	2009-06-10 03:42:20	true/true	24Byte	edit down pack delete time
□ Boot	2015-03-19 02:33:45	true/true	4.00KB	pack delete time
□ bootmgr	2010-11-20 02:29:06	true/false	374.00KB	edit down pack delete time
□ BOOTSECT.BAK	2015-03-19 02:33:45	true/false	8.00KB	edit down pack delete time
□ config.sys	2009-06-10 03:42:20	true/true	10Byte	edit down pack delete time
□ Documents and Settings	2015-03-19 12:36:49	true/true	4.00KB	pack delete time
□ pagefile.sys	1969-12-31 05:00:00	false/false	1024.00M	edit down pack delete time
□ PerfLogs	2009-07-13 08:37:05	true/true	0Byte	pack delete time
□ Program Files	2018-08-17 03:19:40	true/true	8.00KB	pack delete time

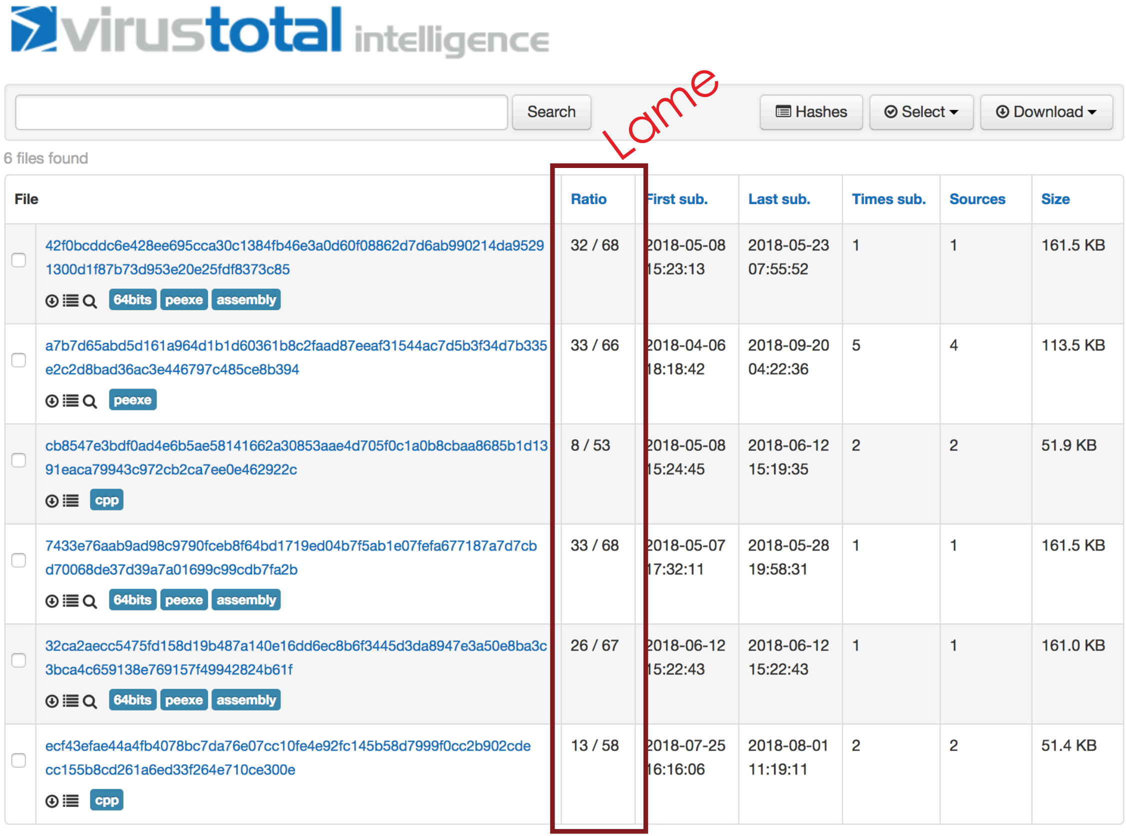
FIREALARM


Internet
Victim Web Server
SJavaWebManage Webshell
1
2
cmd prompt
evil.exe YYYY MM DD
3
Click2Gov Logs
4
Log File 1
Copy MAC times
Parse for payment data & ERROR
THN1080.tmp
5

SPOTLIGHT


Victim Web Server
Internet
5
3
1
SJavaWebManage Webshell
2
Web Service
SPOTLIGHT
6
4
opt.log

#Fail



virustotal intelligence

Lame

6 files found

□	File	Ratio	First sub.	Last sub.	Times sub.	Sources	Size
□	42f0bcddc6e428ee695cca30c1384fb46e3a0d60f08862d7d6ab990214da9529 1300d1f87b73d953e20e25fdf8373c85 64bits peexe assembly	32 / 68	2018-05-08 15:23:13	2018-05-23 07:55:52	1	1	161.5 KB
□	a7b7d65abd5d161a964d1b1d60361b8c2faad87eeaf31544ac7d5b3f34d7b335 e2c2d8bad36ac3e446797c485ce8b394 peexe	33 / 66	2018-04-06 18:18:42	2018-09-20 04:22:36	5	4	113.5 KB
□	cb8547e3bdf0ad4e6b5ae58141662a30853aae4d705f0c1a0b8cbaa8685b1d13 91eaca79943c972cb2ca7ee0e462922c cpp	8 / 53	2018-05-08 15:24:45	2018-06-12 15:19:35	2	2	51.9 KB
□	7433e76aab9ad98c9790fceb8f64bd1719ed04b7f5ab1e07fefa677187a7d7cb d70068de37d39a7a01699c99cdb7fa2b 64bits peexe assembly	33 / 68	2018-05-07 17:32:11	2018-05-28 19:58:31	1	1	161.5 KB
□	32ca2aecc5475fd158d19b487a140e16dd6ec8b6f3445d3da8947e3a50e8ba3c 3bca4c659138e769157f49942824b61f 64bits peexe assembly	26 / 67	2018-06-12 15:22:43	2018-06-12 15:22:43	1	1	161.0 KB
□	ecf43efae44a4fb4078bc7da76e07cc10fe4e92fc145b58d7999f0cc2b902cde cc155b8cd261a6ed33f264e710ce300e cpp	13 / 58	2018-07-25 16:16:06	2018-08-01 11:19:11	2	2	51.4 KB