2015-11-24 - TRAFFIC ANALYSIS EXERCISE - GOOFUS AND GALLANT

ASSOCIATED FILES:

- ZIP file of the PCAP: 2015-11-24-traffic-analysis-exercise.pcap.zip   11.7 MB (11,726,615 bytes)
- TXT file of Snort events: 2015-11-24-traffic-analysis-exercise-snort-events.txt   82.4 kB (82,428 bytes)
- TXT file of Suricata events: 2015-11-24-traffic-analysis-exercise-suricata-events.txt   271.6 kB (271,557 bytes)

ZIP files are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

THE PLAYERS

Tom and Jake are recent hires at your organization's Security Operations Center (SOC). Due to their different personalities, they've earned the nickname "Goofus and Gallant" after a cartoon from the magazine *Highlights for Children*. Tom is Goofus. Jake is Gallant.

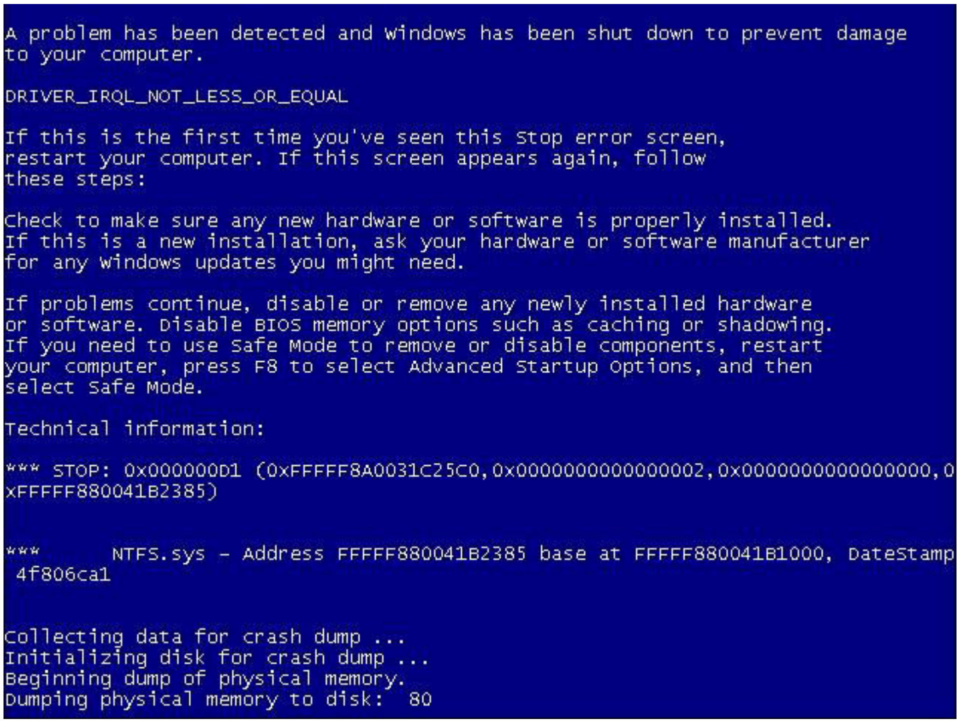
THE STORY

On the Tuesday before Thanksgiving, Tom and Jake are working at the SOC. Tom brought his Windows laptop to the office, and he plans to browse the web. Jake is hard at work reviewing alerts.

Jake's holiday plans are set, and he's happy with the frozen turkey he'd purchased from the supermarket. Tom's more of a "turkey enthusiast." He wants to hunt and kill a turkey for his Thanksgiving meal.

In order to pursue his holiday plans, Tom decides to purchase a shotgun. He fires up his Windows laptop, connects to the SOC's wifi, and starts researching shotguns online.

It's not long before Tom's computer triggers some alerts for suspicious network activity. After those alerts, his laptop crashes!



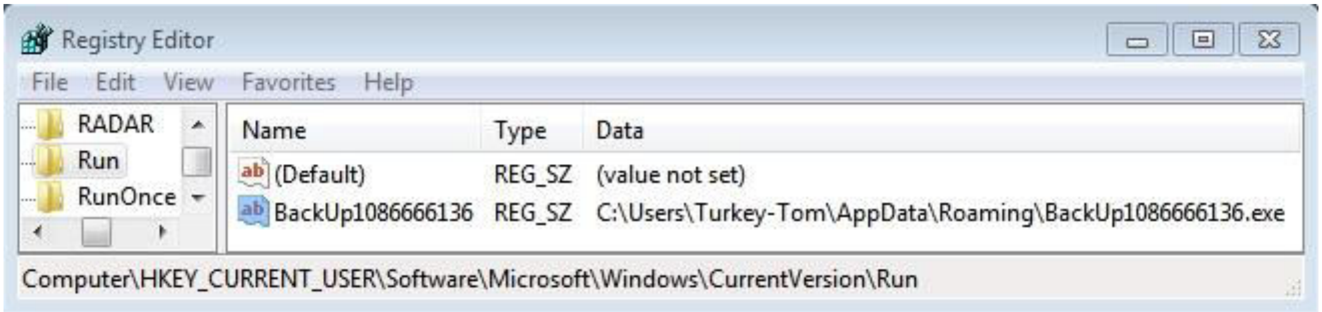
```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0xFFFFF8A0031C25C0,0x0000000000000002,0x0000000000000000,0
xFFFFF880041B2385)


***      NTFS.sys - Address FFFFF880041B2385 base at FFFFF880041B1000, DateStamp
 4f806ca1


Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  80
```

Shown above: Screenshot of Tom's computer crashing.

THE AFTERMATH

You're the supervisor for both Goofus and Gallant. The goofus Tom will likely be fired at some point due to his poor work ethic. Jake is certainly gallant, but he's still a relatively inexperienced analyst. You'll have to figure out what happened to Tom's laptop.

You check Tom's machine and quickly find a suspicious registry entry. It looks like Goofus infected his laptop. The SHA256 hash for the file referenced in the registry is: ***d16ad130daed5d4f3a7368ce73b87a8f84404873cbfc90cc77e967a83c947cd2***

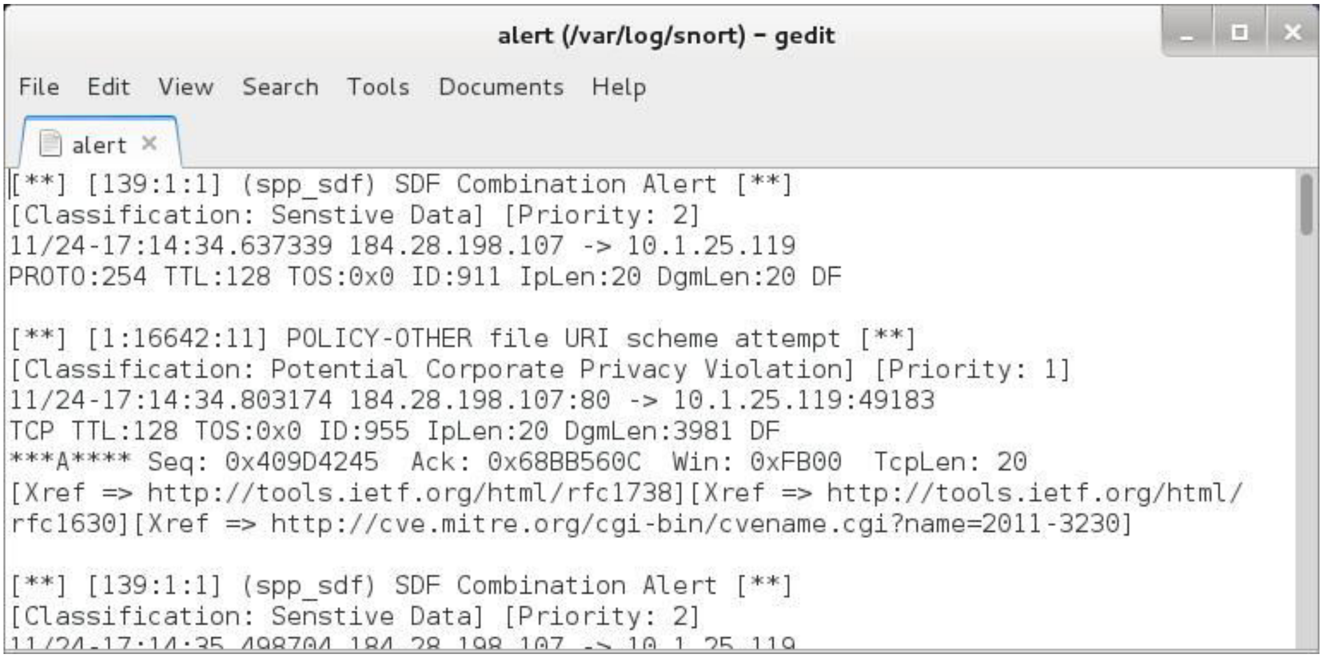


Name	Type	Data
(Default)	REG_SZ	(value not set)
BackUp1086666136	REG_SZ	C:\Users\Turkey-Tom\AppData\Roaming\BackUp1086666136.exe

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

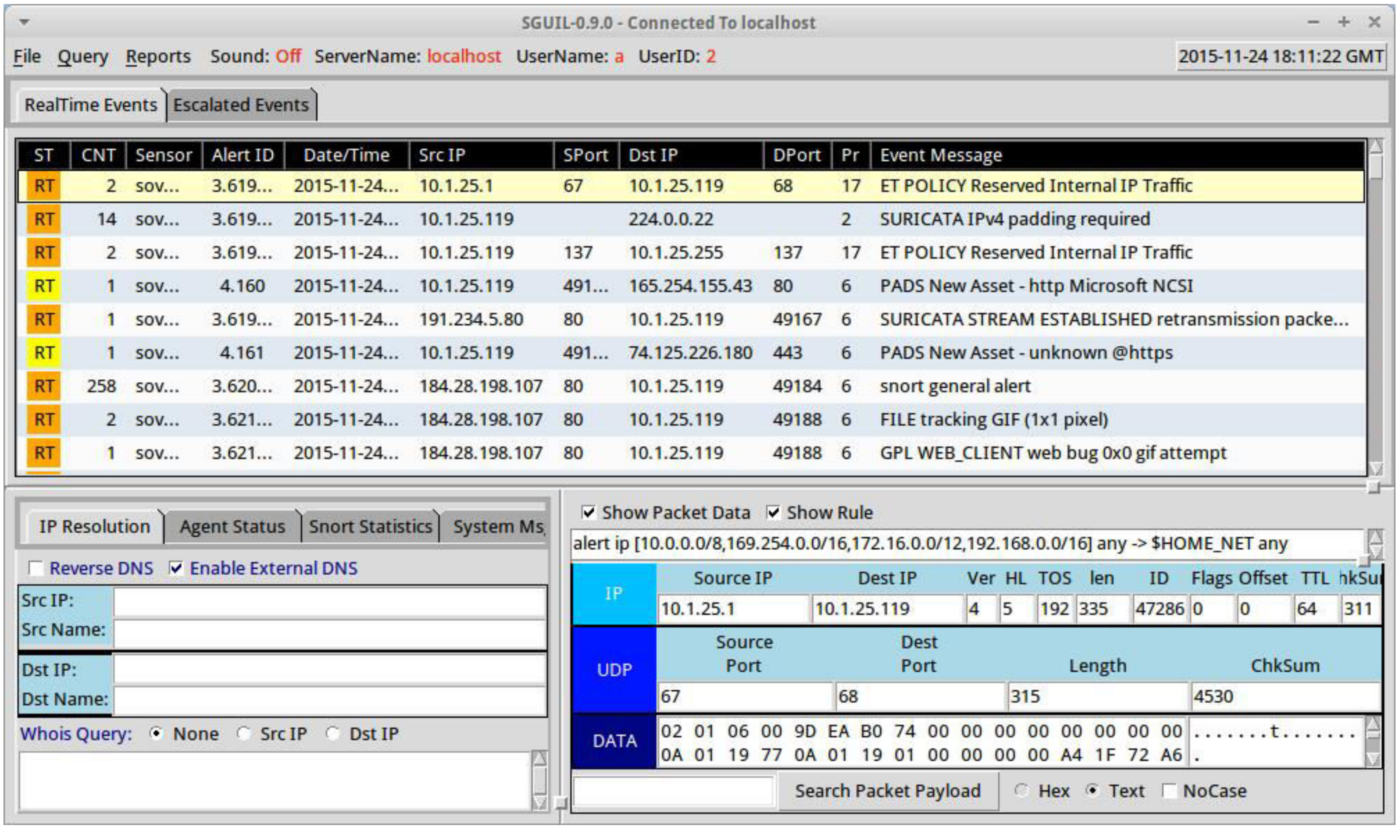
Shown above: Registry entry from the infected Windows laptop.

Next you review the network alerts. Unfortunately, your organization is too cheap for any commercial intrusion detection system (IDS). Fortunately, lower-cost solutions have been implemented. You have access to Snort alerts using the Snort registered ruleset. You also have access to Suricata alerts using the EmergingThreats free ruleset.


alert (/var/log/snort) - gedit
File Edit View Search Tools Documents Help
alert

```
[**] [139:1:1] (spp_sdf) SDF Combination Alert [**]
[Classification: Senstive Data] [Priority: 2]
11/24-17:14:34.637339 184.28.198.107 -> 10.1.25.119
PROTO:254 TTL:128 TOS:0x0 ID:911 IpLen:20 DgmLen:20 DF

[**] [1:16642:11] POLICY-OTHER file URI scheme attempt [**]
[Classification: Potential Corporate Privacy Violation] [Priority: 1]
11/24-17:14:34.803174 184.28.198.107:80 -> 10.1.25.119:49183
TCP TTL:128 TOS:0x0 ID:955 IpLen:20 DgmLen:3981 DF
***A**** Seq: 0x409D4245  Ack: 0x68BB560C  Win: 0xFB00  TcpLen: 20
[Xref => http://tools.ietf.org/html/rfc1738][Xref => http://tools.ietf.org/html/
rfc1630][Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=2011-3230]

[**] [139:1:1] (spp_sdf) SDF Combination Alert [**]
[Classification: Senstive Data] [Priority: 2]
11/24-17:14:35.498704 184.28.198.107 -> 10.1.25.119
```

Shown above: Snort events on the traffic using Snort 2.9.7.6 and the Snort Registered ruleset.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	2	sov...	3.619...	2015-11-24...	10.1.25.1	67	10.1.25.119	68	17	ET POLICY Reserved Internal IP Traffic
RT	14	sov...	3.619...	2015-11-24...	10.1.25.119		224.0.0.22		2	SURICATA IPv4 padding required
RT	2	sov...	3.619...	2015-11-24...	10.1.25.119	137	10.1.25.255	137	17	ET POLICY Reserved Internal IP Traffic
RT	1	sov...	4.160	2015-11-24...	10.1.25.119	491...	165.254.155.43	80	6	PADS New Asset - http Microsoft NCSI
RT	1	sov...	3.619...	2015-11-24...	191.234.5.80	80	10.1.25.119	49167	6	SURICATA STREAM ESTABLISHED retransmission packe...
RT	1	sov...	4.161	2015-11-24...	10.1.25.119	491...	74.125.226.180	443	6	PADS New Asset - unknown @https
RT	258	sov...	3.620...	2015-11-24...	184.28.198.107	80	10.1.25.119	49184	6	snort general alert
RT	2	sov...	3.621...	2015-11-24...	184.28.198.107	80	10.1.25.119	49188	6	FILE tracking GIF (1x1 pixel)
RT	1	sov...	3.621...	2015-11-24...	184.28.198.107	80	10.1.25.119	49188	6	GPL WEB_CLIENT web bug 0x0 gif attempt

```
alert ip [10.0.0.0/8,169.254.0.0/16,172.16.0.0/12,192.168.0.0/16] any -> $HOME_NET any
```

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	hkSu
	10.1.25.1	10.1.25.119	4	5	192	335	47286	0	0	64	311

UDP	Source Port	Dest Port	Length	ChkSum
	67	68	315	4530

```
DATA  02 01 06 00 9D EA B0 74 00 00 00 00 00 00 00 00  ........t.......
      0A 01 19 77 0A 01 19 01 00 00 00 00 A4 1F 72 A6  .
```

Shown above: Suricata events on the traffic using Sguil on Security Onion with the EmergingThreats ruleset.

REPORTING

You were able to retrieve a pcap of network traffic to Tom's laptop. You'll need to do a report. At a minimum, your report should include:

- Date and approximate time of the infection.
- The infected computer's IP address.
- The infected computer's MAC address.
- The infected computer's host name.
- What caused the infection