

What is an APT without a sensationalist name?

(Warning: may contain sensationalist names.)

Seth Hardy
The Citizen Lab, Munk School of Global Affairs
University of Toronto

APT APT APT APT APT
APT APT APT APT APT

APT APT APT APT APT APT APT APT APT OMG APT
APT APT APT APT APT LOL APT APT APT APT APT
APT APT APT APT APT APT APT APT APT APT APT

(Introduction)

Background

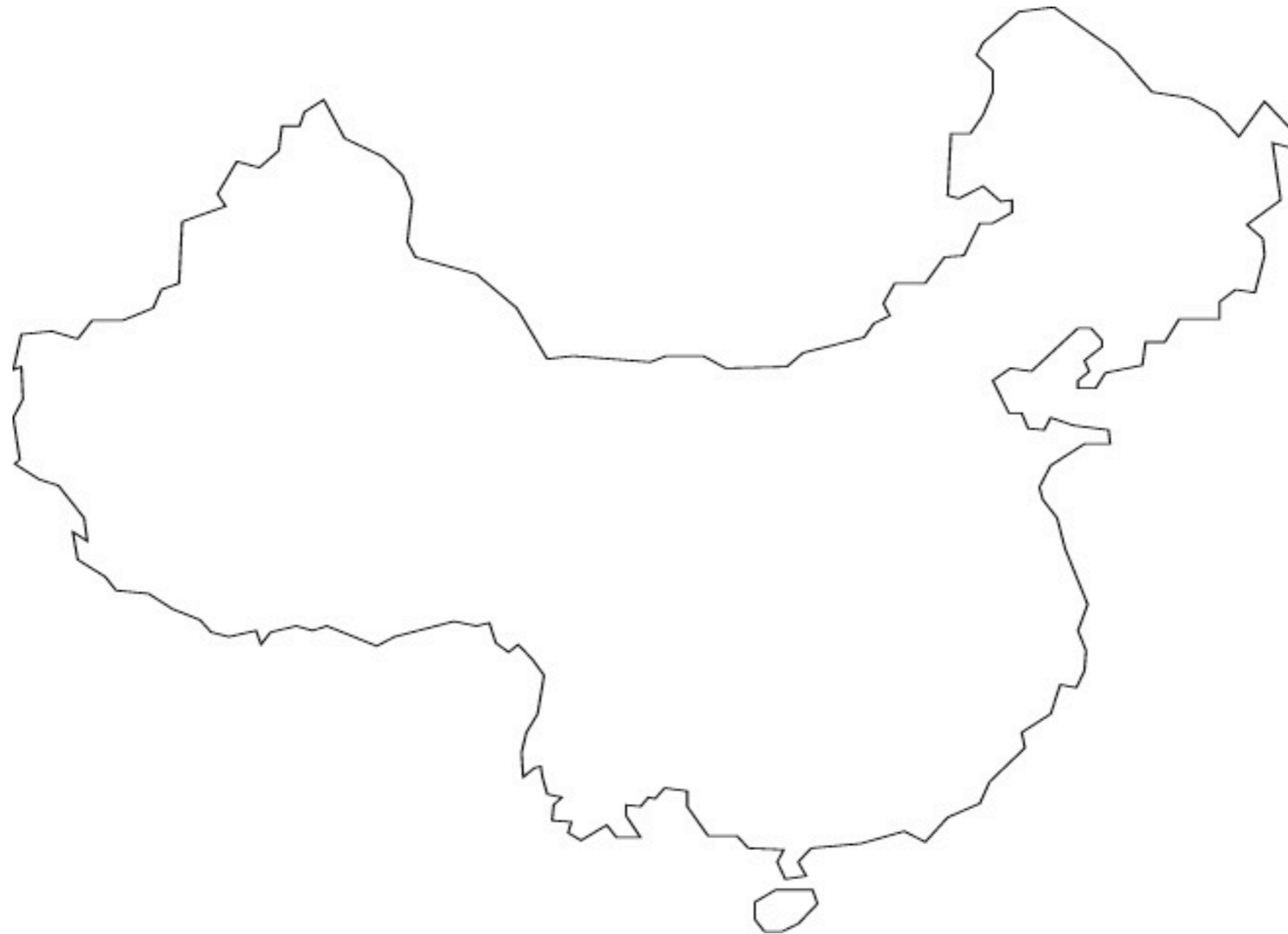
- Human Rights Malware Comparison Project at The Citizen Lab, Munk School of Global Affairs, University of Toronto
- Limited visibility: only participating organizations, only what they send
- Looking primarily at highly targeted attacks and already compromised targets
- Not writing AV detection

What is an APT?

Advanced persistent threat (APT) usually refers to a group, such as a foreign nation state government, with both the capability and the intent to persistently and effectively target a specific entity. The term is commonly used to refer to cyber threats, in particular that of Internet-enabled espionage, but applies equally to other threats such as that of traditional espionage or attack. Other recognized attack vectors include infected media, supply chain compromise, and social engineering. Individuals, such as an individual hacker, are not usually referred to as an APT as they rarely have the resources to be both advanced and persistent even if they are intent on gaining access to, or attacking, a specific target.

(wikipedia.org)





(Mandiant)

What is an APT?

May 1st, May Day, was dubbed "Blame APT Day" by @Unicorn_Threat on Twitter:

We declare that May 1st (May Day) will be #IBlameAPT day all your screw ups will be given a free pass just blame #APT You're Welcome!.. #UPT

In the wake of high profile hacks at RSA and Department of Energy, our industry and the general public are quickly learning that any compromise can quickly and efficiently be blamed on the dreaded "Advanced Persistent Threat" or APT. Such devious attacks simply cannot be predicted, stopped or blended with orange juice. It doesn't matter if your employees click on PDF attachments and open them with Adobe software, it is clearly the work of an APT!

(attrition.org)

What or Who?

Two camps:

- **What: a type of attack**
“it got past our expensive firewall and IPS and made us look bad, this is clearly an advanced threat”
- **Who: a foreign nation state**
“we can’t name names, but it rhymes with China”

What do we see?

- Social techniques, obvious to really good
 - Events (real and fake)
 - Organizations and people (real and fake)
 - News and current events

What do we see?

- Technical methods, generally obvious
 - Filetype masquerading
 - Unicode RTL override
 - Trojans, trojans in ZIP files, trojans in RAR files, trojans pretending to be video files...
- PDF, DOC, XLS, PPT, JST

How is this different...?

- It isn't

How is this different...?

HOWEVER...

- Human rights organizations and NGOs likely don't have the things large corporations do:
 - Information security budgets
 - IT employees
 - Security appliances that cost tens or hundreds of thousands of dollars
 - Dedicated work computers
 - Security resources to educate employees on how to deal with threats, or even that the threats exist

But companies keep saying...

- Google: “highly sophisticated and targeted attack”
- RSA: “extremely sophisticated cyber attack” and “[o]ur investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat”
- Harvard: “sophisticated individual or group” (Wasn’t this a website defacement? Does that even count?)

What is an APT?

- Advanced:
CVEs that are years old
“Run this executable, it’s relevant, seriously”
“It has an Excel icon and claims to be salary figures”
- Persistent:
They are persistent: it’s easier to attack than defend
- Threat:
Well, they keep working...

Haven't we heard this before?

- “*Targeted trojan*”
- “*Spear phishing*”
- “*Cyber warfare*”
- Do we really need more names?

This is the new normal.

- APTs are “different” because they are not smash and grab
- Note the quotes - that means sarcasm
- What are the actual figures on smash and grab attacks?
 - Not everyone is cool enough to get hacked by LulzSec
- The plural of anecdote is not data - I (unfortunately) worked for a major AV company for a few years.
- Financial malware, botnets do the same thing...

Real World Example

(without the shady FUD and AV pitch)

One family, multiple targets

- Five samples sent to four organizations
 - From our visibility, this is big (but not surprising)
- Distinctive characteristics with no public reports
- Three human rights organizations plus one unknown
- Most with a different C2 server; one duplicate
- Different vectors: executables, XLS
 - Dalai Lama video
 - Article about residential high-rise fire

Targeted attack: News Site

- Six pictures of a high-rise fire
- Two are actually “screensavers” (.scr) with RTL override filenames
- Executables move and delete self, drop and open image



Let's call it: Sharky RAT

It seemed like a good
name at the time...
(thanks, McAfee)



Remote Administration Tool

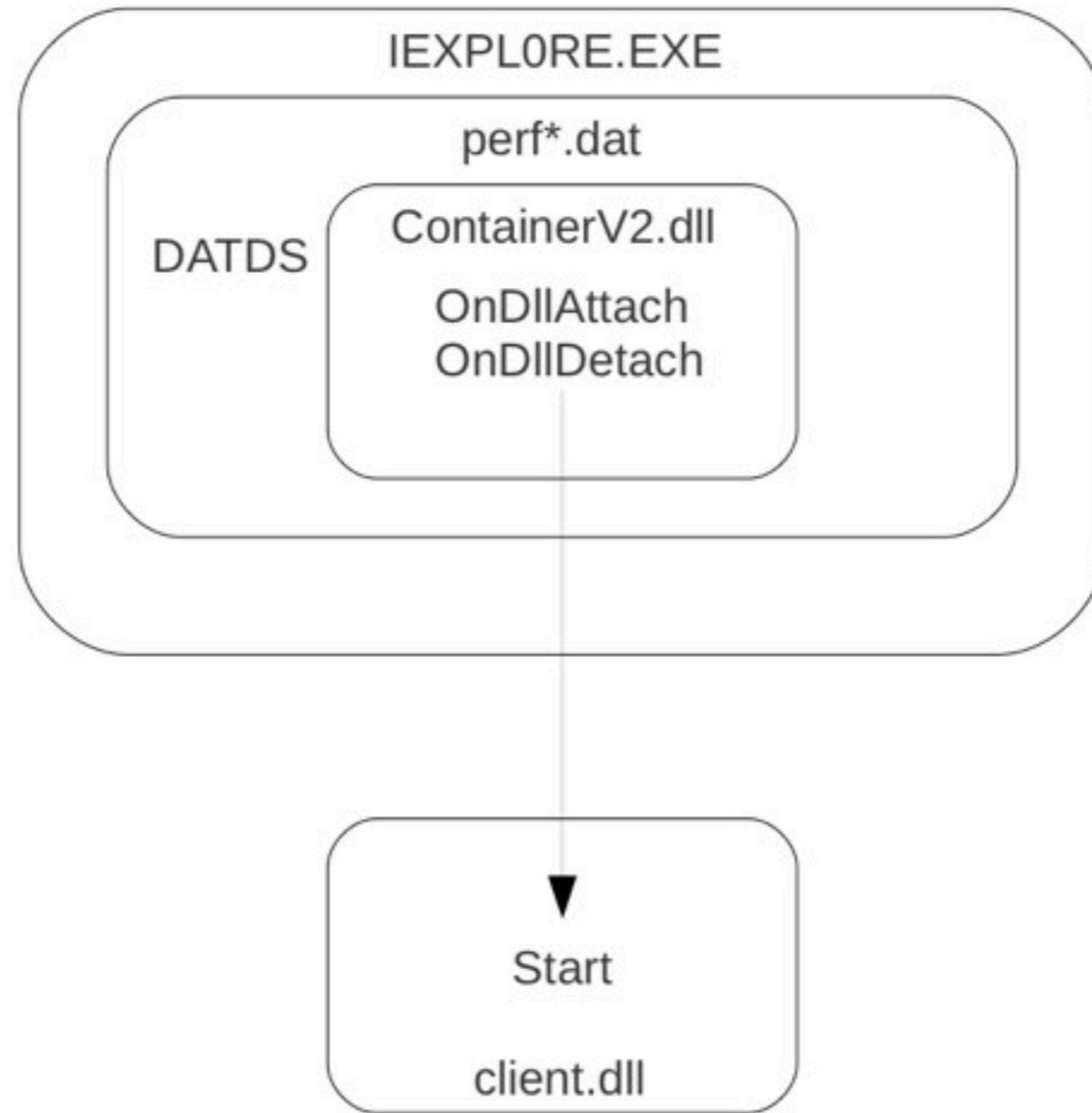
From Wikipedia:

A **Remote Administration Tool** (a **RAT**) is a piece of software that allows an operator to control a system as if he has physical access to that system. The operator controls the RAT through a network connection. Such tools provide an operator the following capabilities:

- Screen/camera capture or image control
- File management (download/upload/execute/etc.)
- Shell control (from command prompt)
- Computer control (power off/on/log off if remote feature is supported)
- Registry management (query/add/delete/modify)
- Other software product-specific functions

Also known as a Remote Access Trojan.

How Sharky Works



How Sharky Talks

- ContainerV2 sets up two connections
 - POST, GET, HTTP CONNECT proxy
- Very distinctive handshake
- “Encrypted” with a one byte XOR key
- Downloads and executes client
- Sends configuration file with system info

How Sharky Talks

```
POST /indexNNNNNNNNNN.asp HTTP/1.1
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1;)
Host: update.microsoft.com
Connection: Keep-Alive
Content-Type: text/html
Content-Length: %.6d
```

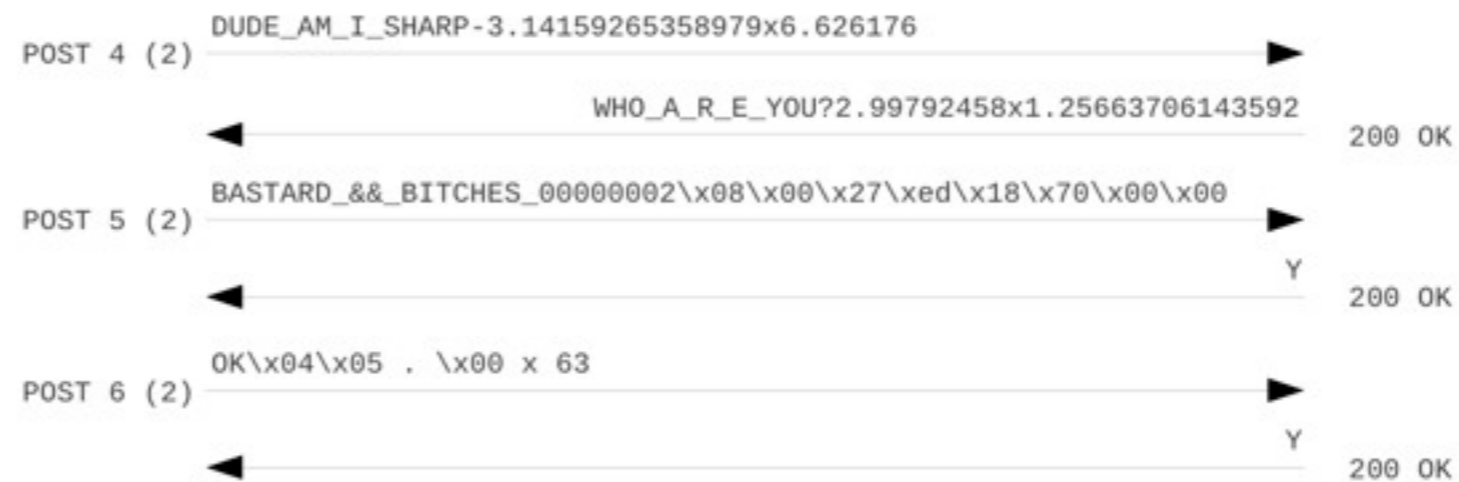
```
[payload]
```

How Sharky Talks

Connection 1:



Connection 2:

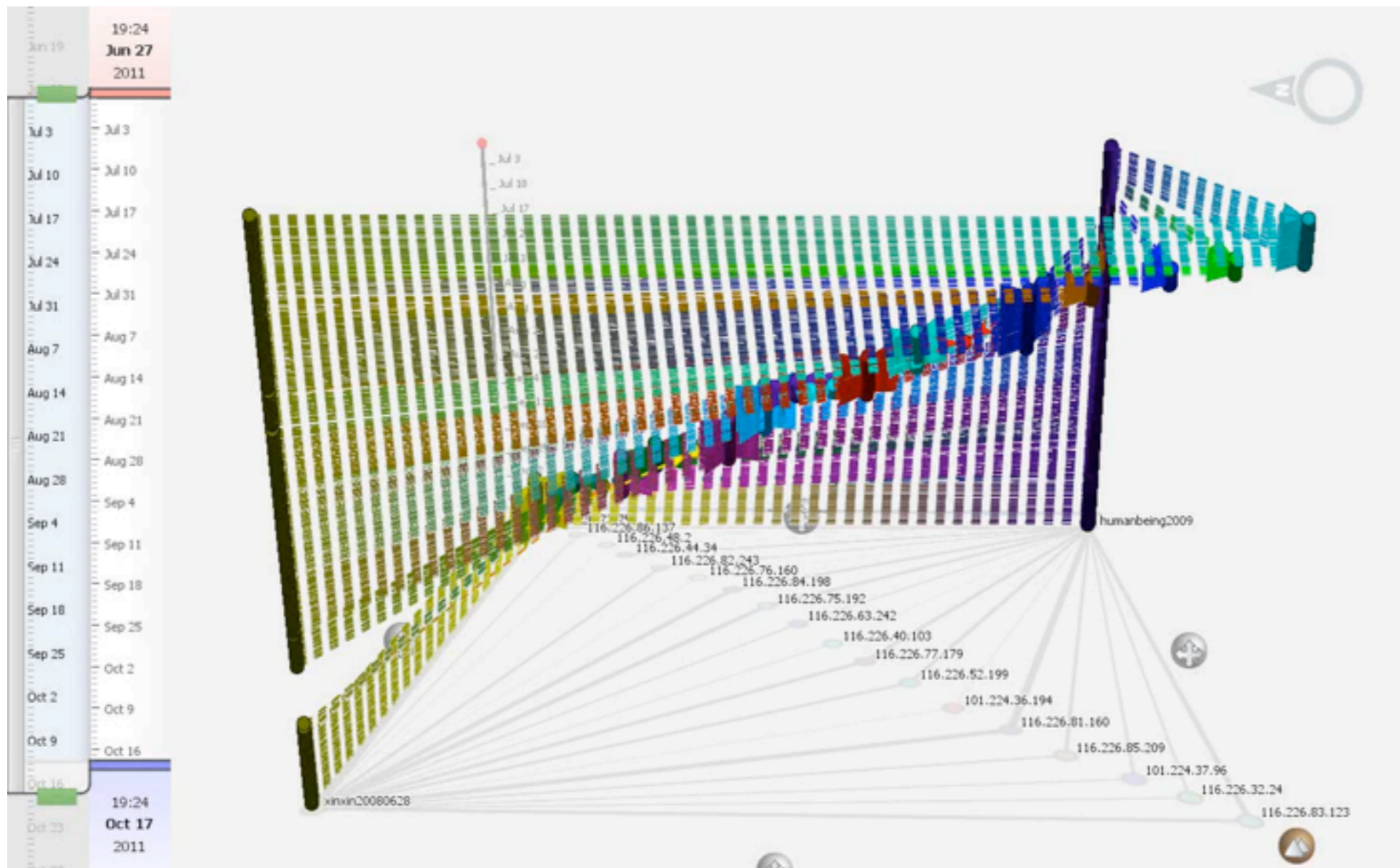


How Sharky Talks



Once the ContainerV2 DLL downloads the client DLL, it hands off control (specifically: two open sockets and the config file) via the client DLL start() function.

Who Sharky Talks To



Talking to Sharky

```
handshaking and establishing sockets:
0001 <4919> -> DUDE_AM_I_SHARP-3.14159265358979x6.626176
      OK <4919> <- WHO_A_R_E_YOU?2.99792458x1.25663706143592
0002 <4919> -> BASTARD_&&_BITCHES_00000000 's!p
      OK <4919> <- Y
0003 <4919> -> X
      OK <4919> <- OK
0004 <4920> -> DUDE_AM_I_SHARP-3.14159265358979x6.626176
      OK <4920> <- WHO_A_R_E_YOU?2.99792458x1.25663706143592
0005 <4920> -> BASTARD_&&_BITCHES_00000000 's!p
      OK <4920> <- Y
0006 <4919> -> [payload length 67]
      OK <4919> <- Y
0007 <4920> -> X
      OK <4920> <- ≡
handshake successful
downloading client.dll binary:
0008 <4920> -> X
      OK <4920> <- [payload length 61440]
binary downloaded: [eb51b384fcbbe468a6877f569021c5d1]
sending config file:
1001 <4920> -> [payload length 4758]
      OK <4920> <- Y
config file accepted
1002 <4919> -> [empty keylog packet]
      OK <4919> <- Y
1003 <4920> -> X
      OK <4920> <- 0a 00 00 00 07 00 07 00 b8 00
1004 <4919> -> [empty keylog packet]
      OK <4919> <- Y
1005 <4920> -> X
      OK <4920> <- 0a 00 00 00 0a 00 0a 00 b8 00
```

Sharky Config

```
POST /index000001001.asp
00000000 10 00 01 01 04 [REDACTED] |.....[REDACTED]| ← first C2 server
00000010 [REDACTED] 00 00 00 00 |.....|
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000100 00 00 00 00 00 00 90 1f e7 03 01 00 01 00 00 00 |.....|
00000110 78 00 00 31 32 37 2e 30 2e 30 2e 31 00 00 00 00 |x..127.0.0.1....|
00000120 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000210 00 00 00 00 90 1f 01 78 00 00 00 00 00 00 00 00 |.....X.....|
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000250 00 00 00 00 00 00 00 78 00 00 00 00 00 00 00 00 |.....X.....|
00000260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000290 00 00 00 00 00 00 00 00 00 00 00 00 31 31 31 35 |.....1115| ← campaign name
000002a0 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |f.....|
000002b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000390 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff |.....|
000003a0 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff |.....|
*
00000450 [REDACTED] |.....[REDACTED]| ← first C2 server
00000460 [REDACTED] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000470 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
00000650 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
00000660 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
*
```

Sharky Config

00000690	[REDACTED]	[REDACTED]	active C2 server
000006a0	[REDACTED]	[REDACTED]	
000006b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[REDACTED]	
*			
00000790	c0 a8 cc 32 80 05 00 00 9c 00 00 00 05 00 00 00	[...2.....]	IP, process ID, version
000007a0	01 00 00 00 28 0a 00 00 02 00 00 00 53 65 72 76	[...(.Service	Windows version
000007b0	69 63 65 20 50 61 63 6b 20 33 00 00 00 00 00 00	ice Pack 3.....]	
000007c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000820	00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00	[.....]	memory, disk, locale
00000830	00 01 01 00 f0 fd 1f 00 8c 5e 19 00 b5 01 00 00	[.....^.....]	
00000840	f1 4f 00 00 91 34 00 00 50 41 4c 32 00 00 00 00	[.0...4..PAL2...]	computer name
00000850	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000940	00 00 00 00 00 00 00 00 75 73 65 72 00 00 00 00	[.....user....]	account name
00000950	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000a40	00 00 00 00 00 00 00 00 53 6f 6d 65 6f 6e 65 00	[.....Someone.]	user name
00000a50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000b40	00 00 00 00 00 00 00 00 53 6f 6d 65 77 68 65 72	[.....Somewher]	user organization
00000b50	65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[e.....]	
00000b60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000c40	00 00 00 00 00 00 00 00 [REDACTED]	[.....[REDACTED]]	serial number
00000c50	[REDACTED] 00 [REDACTED]	[.....]	
00000c60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000d40	00 00 00 00 00 00 00 00 49 6e 74 65 6c 28 52 29	[.....Intel(R)]	computer info
00000d50	20 43 6f 72 65 28 54 4d 29 32 20 51 75 61 64 20	Core(TM)2 Quad	
00000d60	43 50 55 20 20 20 20 51 39 36 35 30 20 20 40 20	CPU Q9650 @	
00000d70	33 2e 30 30 47 48 7a 00 00 00 00 00 00 00 00 00	3.00GHz.....]	
00000d80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00000f40	00 00 00 00 00 00 00 00 f7 b6 00 00 00 00 00 00	[.....]	Windows path
00000f50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
00000f60	00 00 00 00 00 00 00 00 43 3a 5c 57 49 4e 44 4f	[.....C:\WINDO	
00000f70	57 53 00 00 00 00 00 00 00 00 00 00 00 00 00 00	WS.....]	
00000f80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00001060	00 00 00 00 00 00 00 00 00 00 00 00 43 3a 5c 44	[.....C:\D]	temp path
00001070	4f 43 55 4d 45 7e 31 5c 75 73 65 72 5c 4c 4f 43	OCUME-1\user\LOC	
00001080	41 4c 53 7e 31 5c 54 65 6d 70 00 00 00 00 00 00	ALS-1\Temp.....]	
00001090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	
*			
00001170	43 3a 5c 44 4f 43 55 4d 45 7e 31 5c 75 73 65 72	[C:\DOCUME-1\user]	executable name
00001180	5c 4c 4f 43 41 4c 53 7e 31 5c 54 65 6d 70 5c 70	\LOCALS-1\Temp\p	
00001190	65 72 66 38 35 30 61 30 39 2e 64 61 74 00 00 00	erf850a09.dat...	
000011a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	[.....]	video capture info
*			
00001290	00 00 00 00 4f 4b	[....OK]	

What Sharky Does

- By default, two connections:
 - Command request (X)
 - Data channel
- At the start, command 0xB8 (keylogger)
- Others include: shutdown, restart, registry manipulation, file manipulation, process manipulation, command execution, service manipulation, audio/video capture, keyboard and mouse use, ...

Where is it from?

- C2 servers: almost all in one /16
- One AS - Shanghai
- Dynamic DNS hosting - Chinese
- Chinese name for one C2 domain
- Targets Chinese AV software

Where is it from?

- C2 servers: almost all in one /16
- One AS - Shanghai
- Dynamic DNS hosting - Chinese
- Chinese name for one C2 domain
- Targets Chinese AV software

“we don't know”

Observations

Again: This is the new normal.

- APTs exist. They are not going away.
- Don't buy the hype.
 - Alternately: Participate in Blame APT Day (May 1st).
- Organizations such as NGOs are particularly vulnerable due to the state of the AV industry.
- We need to raise the low bar (almost free), not the high bar (appliances ain't cheap).

APTs vs. Other (Long-Term) Malware

- APTs have low protection
 - Frequently no or unsophisticated packing
 - Few if any anti-debugging tricks
- Financially-motivated malware is usually the opposite
 - Need to protect against competitors as well as AV companies

NGO/Nonprofit Defense

- AV software - keep up to date
- Firewall software - watch outbound traffic
- Education, education, education
 - Specifically: what bad email looks like
- (none of these should surprise you)

What else can be done?

(without a dedicated IT person)

- Hosted email, documents
- Use a Mac (or maybe Ubuntu, maybe)
- Education: a little really does go a long way
 - Stop opening attachments
 - Stop opening attachments
 - Stop opening attachments

Questions?

