Temporal aspects of cyber operations… time favours the defence, but achieving mission success can be near instant

Vietnam. A sniper would fire from the hill every night.

So they prepared a response

Nothing was held back, they unleashed it all

It was not even a firefight, which would require someone on the other side returning fire.

The next morning a search of the hill found only a short blood trail. They don’t know if it was a success. This is a bit like cyber. The defence can make a big show of everything they’ve done, but they have no feedback loop, no way to tell that they succeeded. All they know is when they fail, and that isn’t even consistent. Cyber is very asymmetric in information, not just in capabilities. Offence has empirical proof of success, defence has occasional empirical proof of failure. That is a hard environment to build a successful strategy or develop good tactics.

Information asymmetries hinder cyber defence. But, time is on their side. . . except when it isn't

Recorded Future

RFUN 2017

Defence: time is against, then for you

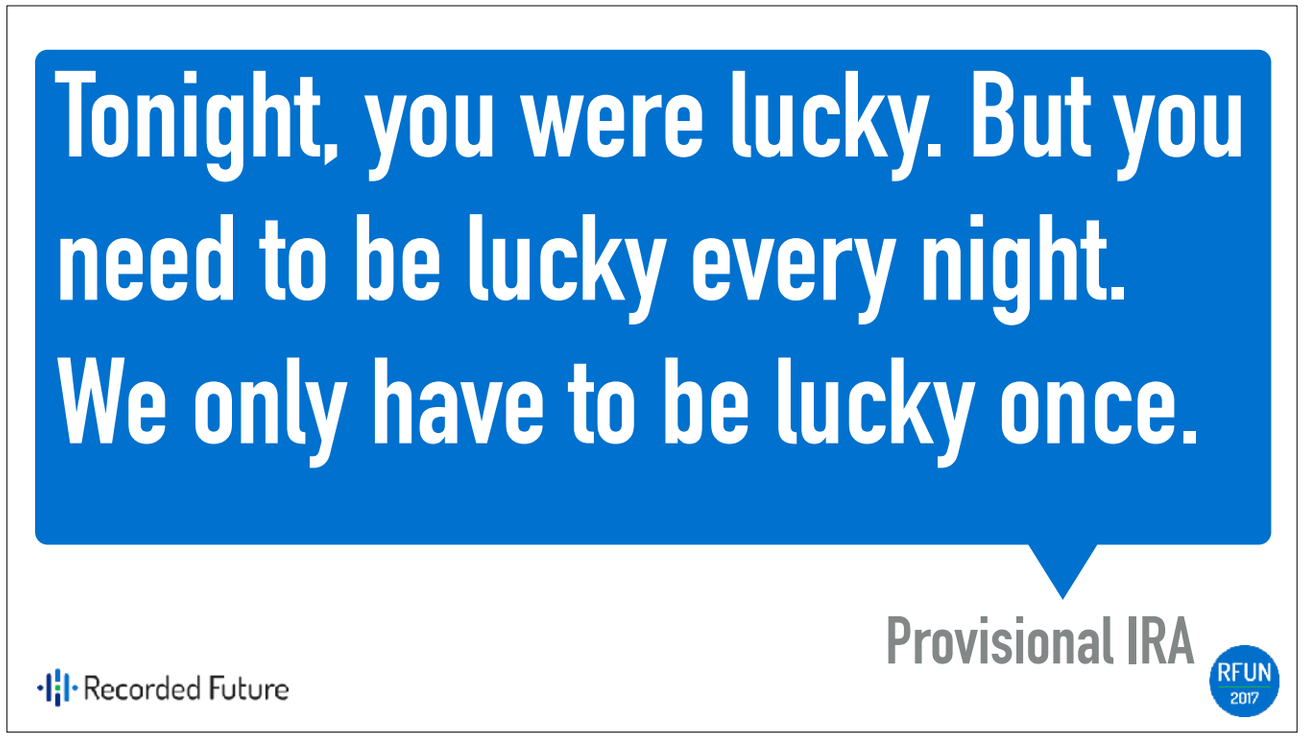
Offence: time is for, then against you

Repeat.

the grugq

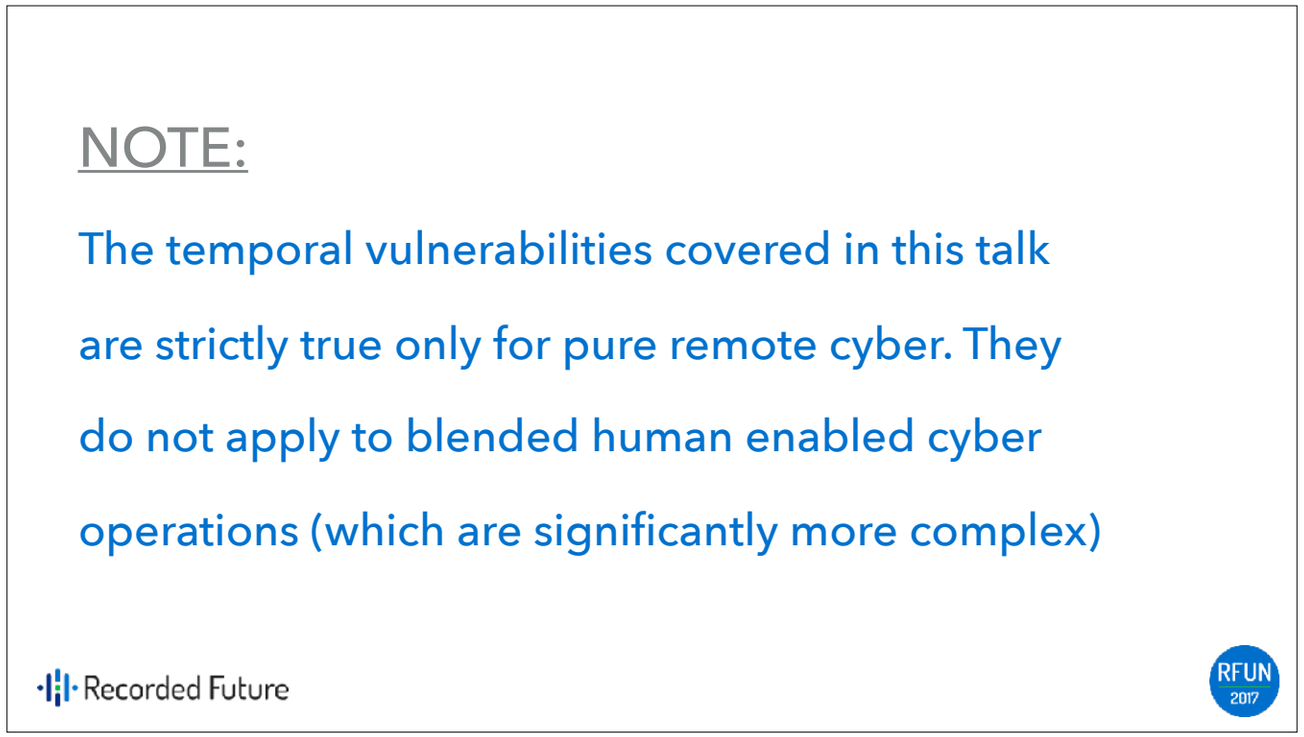
Recorded Future

RFUN 2017



Eternal defence is bound to lose at some point, but eternal offence is also bound to lose.
“in guerrilla war, the guerrilla wins by not losing, the conventional army loses by not winning” - Kissinger

Time has always played a role in conflict.



More to the point, while a pure remote cyber operation will at some point in time cease to be a vulnerability for the offence; human enabled cyber ops remain permanent vulnerabilities. Think Snowden’s exfiltration - he will never be safe, he will always be vulnerable to a response from the US.

Overview

- Understanding Operations
- Special Operations Theory
  - Area of vulnerability, Mission Success
- Cyber Operations
  - Temporal Aspects and Operations
- Final Thoughts

Recorded Future

RFUN 2017

Operations have a cycle, a sequence of phases. The split is a bit arbitrary, but it is roughly: Planning, Prep, Execution, Escape & Evasion, Exploitation.

Before, During and After

- Planning
- Preparation
- Execution
- Escape & Evasion
- Exploitation

Recorded Future

RFUN 2017

The sign of the professional is that they work the cycle backwards — figure out how to exploit success, how to get away with it, and then how to execute it. One of the classic sign of amateurism is planning to the execution phase and then sort of trail off. The fantasy takes them to the part where they get revenge (or whatever), and then “lived happily ever after”…

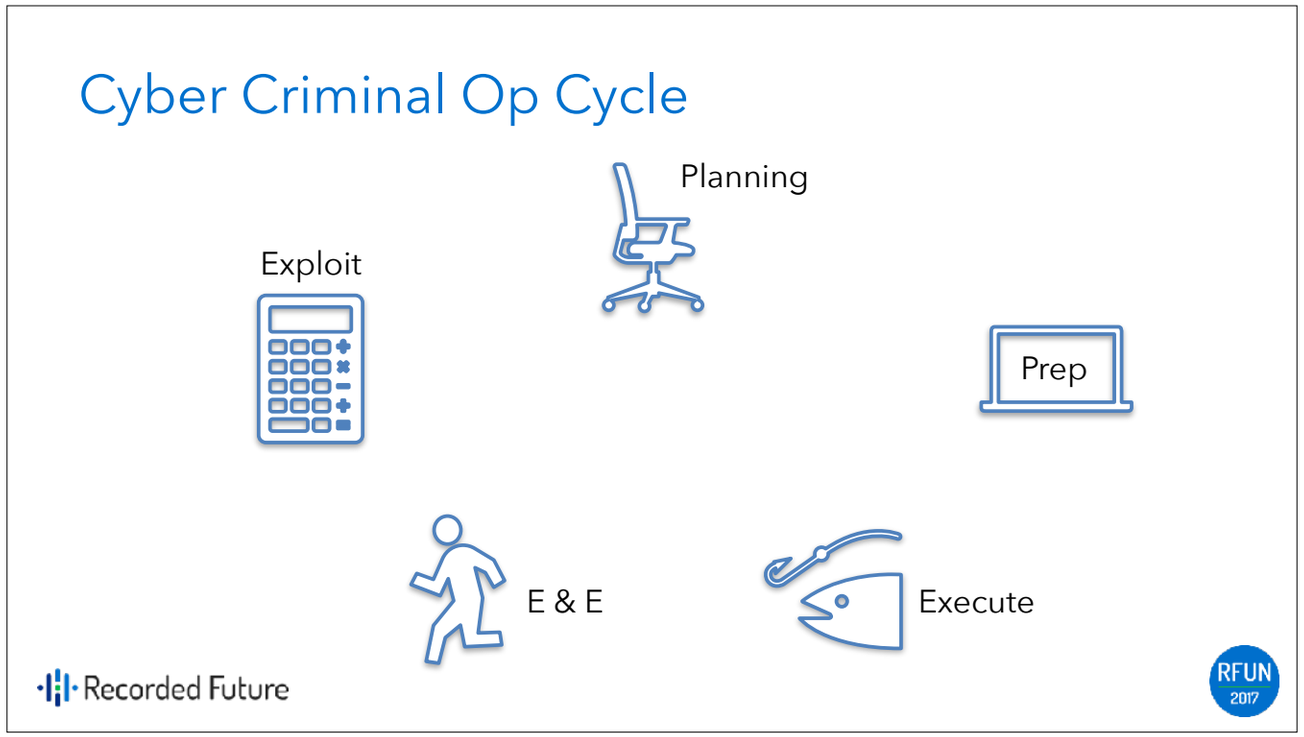
Classic terrorist op cycle

Recorded Future

RFUN 2017

ISIS remote control operations are interesting because the terrorist group isn't invested in the operation, just the exploitation. So what they tell the guys doing the attacks, "give us the material to do the exploitation (i.e. martyrdom video), some way to know the attack was you… then as soon as you get the vaguest idea for a plan, just go for it, do it." They love the cars & cutlery attacks because it is so easy for civilians to do these attacks and the media then helps them with the exploitation.. rather than writing "total loser runs over a family of four out for a stroll <story about family>"… they write "ISIS terrorist strikes fear into the heart of …" It is enabling them and reduces their costs to basically free. Even if they deal with 100 intelligence agents and reporters impersonating volunteers, the cost to ISIS is zero because the real volunteer who caries through the attack is enough. If that wasn't enough, then they'd have to infiltrate actual operatives into Europe, which is much harder for them.

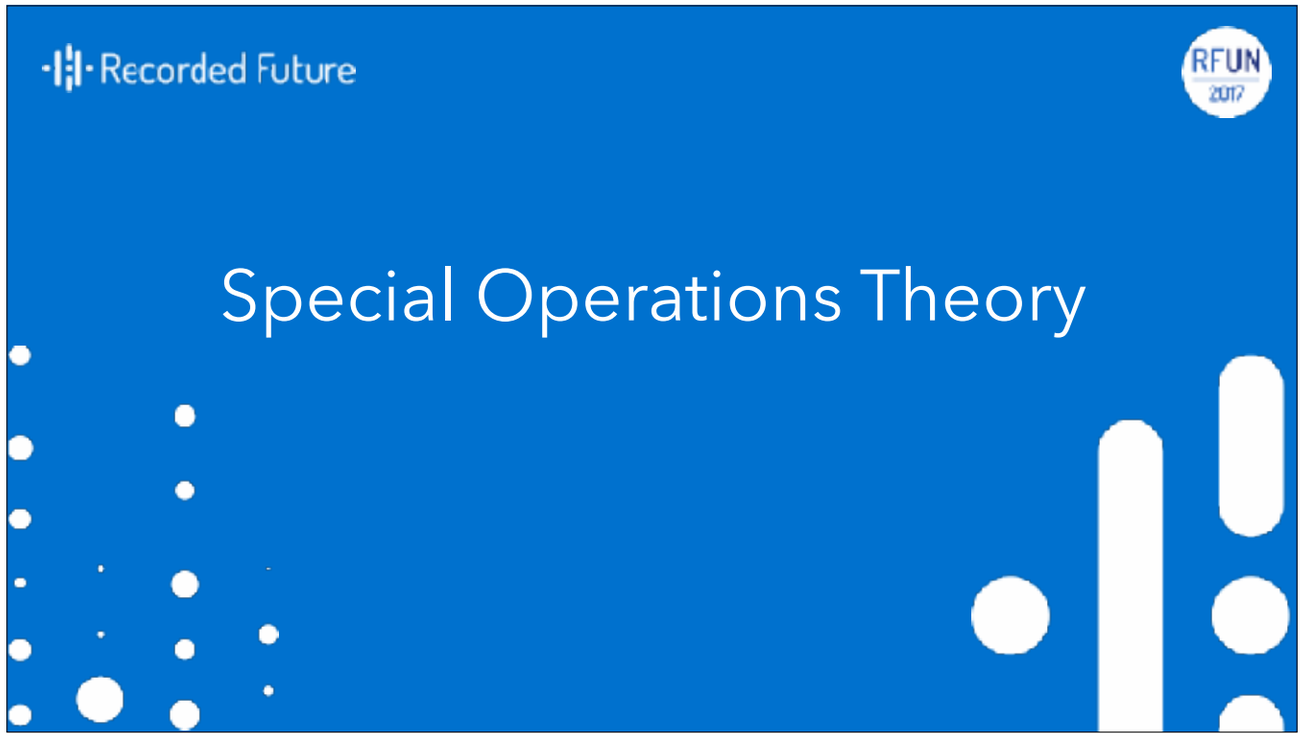
The media, ISIS, CT experts, and intel agencies all benefit from hyping the threat here and it is so amazingly counterproductive… there is, I suspect, a Werther Effect with remote control terrorist ops. The fact that experts discount it completely, and yet we see clusters of attacks and tactical diffusion based on media reports (vehicles, kitchen knives, fake suicide vests) provides some pretty strong empirical evidence otherwise. There is no one but civilians who benefit from downplaying the these attacks, so naturally we're stuck with everyone pushing fear and idiots running over little kids. Tragedy.

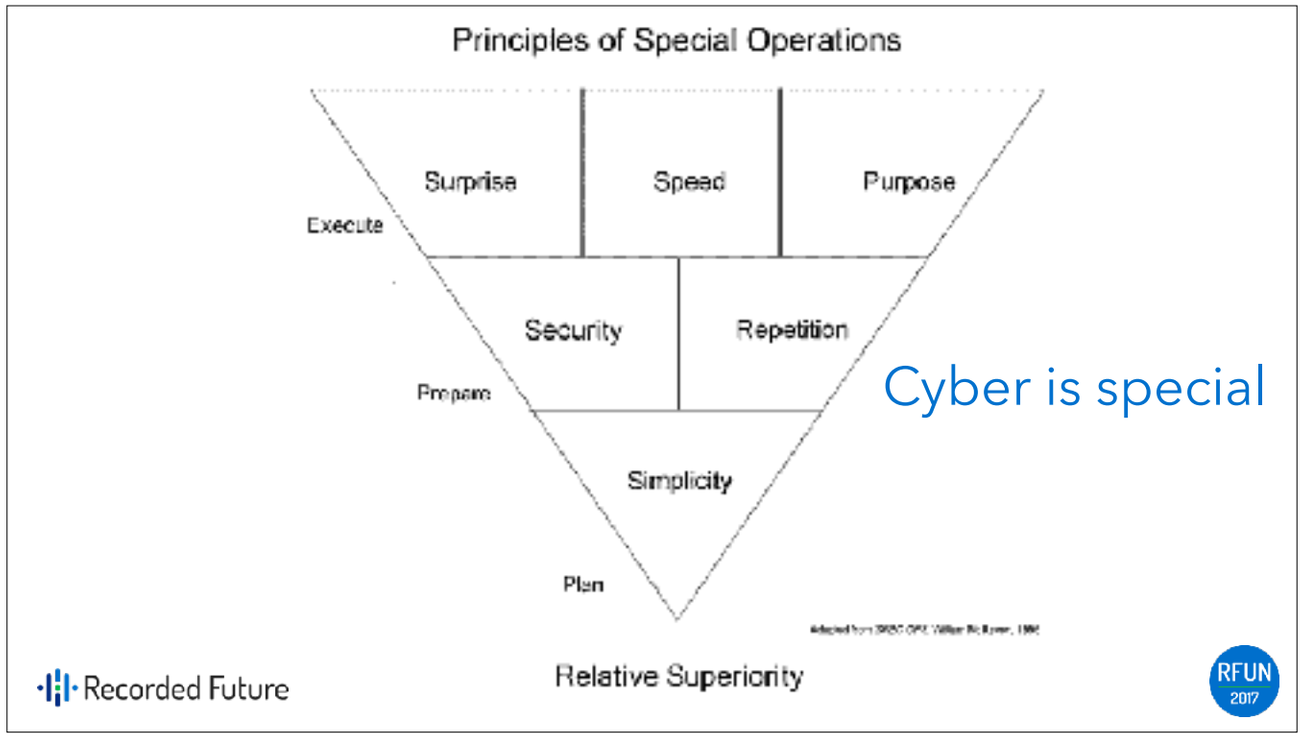


The objective of a cyber criminal is to make money. All the hacking and so on is just a precursor to get some cash. This leaves them extremely vulnerable to certain types of deception operation, since they're unlikely to pass up the opportunity to make a quick buck.

E&E actually has to be integrated into the prep and execution (just like with guerrilla war) because otherwise it is too late…

This is the same for pretty much all cyber ops, the method of exploitation is the thing that changes most.


Recorded Future
RFUN
2017
Special Operations Theory



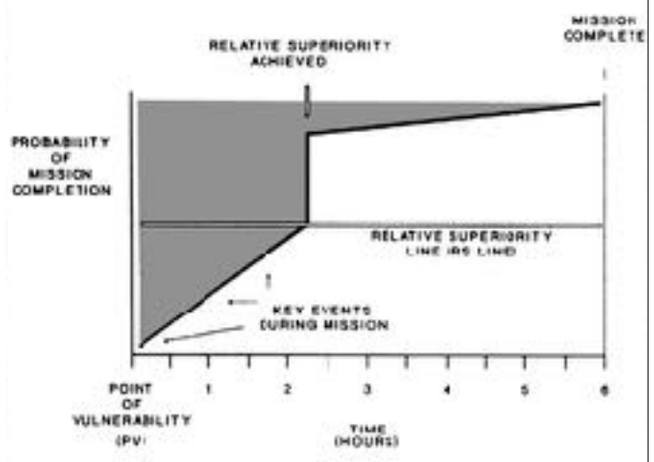
Cyber is special

A simple plan, carefully concealed, repeatedly and realistically rehearsed, and executed with surprise, speed and purpose.

Cyber operations usually don’t involve significant coordination between lots of moving parts (ignoring blended ops). Defenders don’t know when, or where, the attack will come. Attackers use automated tools and perform the same types of operation on a daily basis - hacking is routine, rote skills. Attacks are fast, compromise is usually seconds, a breach might take hours or days.

Visualisation of Ops and Mission Success

- Vulnerability for attackers starts as soon as they compromise a box
- Relative Superiority is when they achieve dominance over the defenders, e.g. install an implant
- Mission success, operations, and operational success are different
  - Short term objectives met
  - Long term persistence/access
  - Covert? Stay out of jail? Sabotage?



Recorded Future

RFUN 2017


Recorded Future
RFUN
2017
Cyber Operations

In cyber, time is corrosive

Recorded Future

RFUN 2017

And on the pedestal these words appear:

'My name is Ozymandias, king of kings:

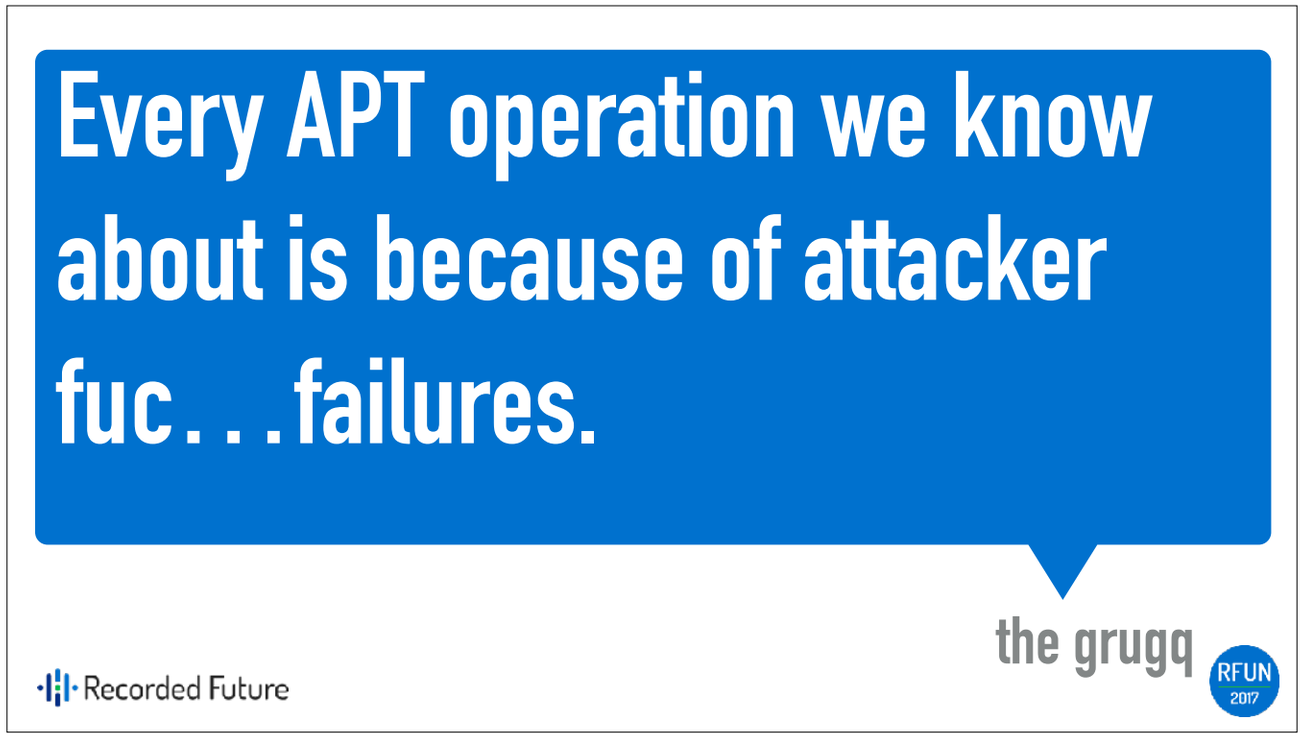
Look on my works, ye Mighty, and despair!'

Nothing beside remains. Round the decay

Of that colossal wreck, boundless and bare

The lone and level sands stretch far away

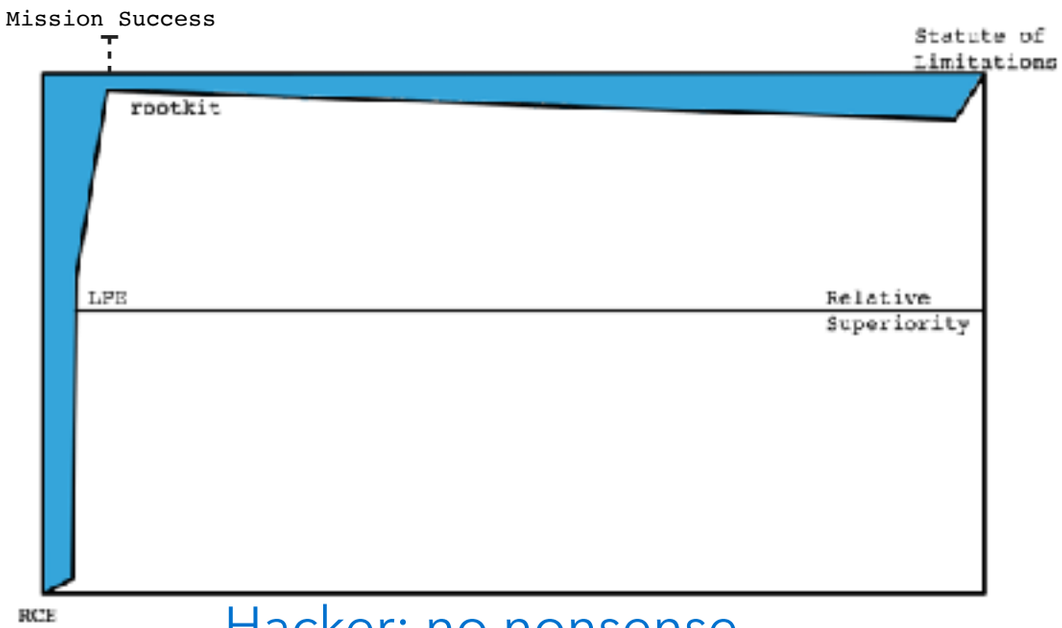

Recorded Future
RFUN
2017
Temporal Aspects of Cyber Ops



Our data set on APT campaigns and activities is inherently limited. Firstly, the classified stuff from HUMINT assets and SIGINT is a known unknown; then there is the limit to what gets released publicly by the TI companies (known known); finally, what we know about is all the ops that got blown - so the great success campaigns are unknown.


Recorded Future
RFUN
2017
A Study of Failures

The following diagrams have been simplified significantly to clarify the content. Real world operations typically involve multiple computers, and "`exfil`" is actually almost any activity on the compromised system / network.



Hacker: no nonsense

Recorded Future

RFUN 2017

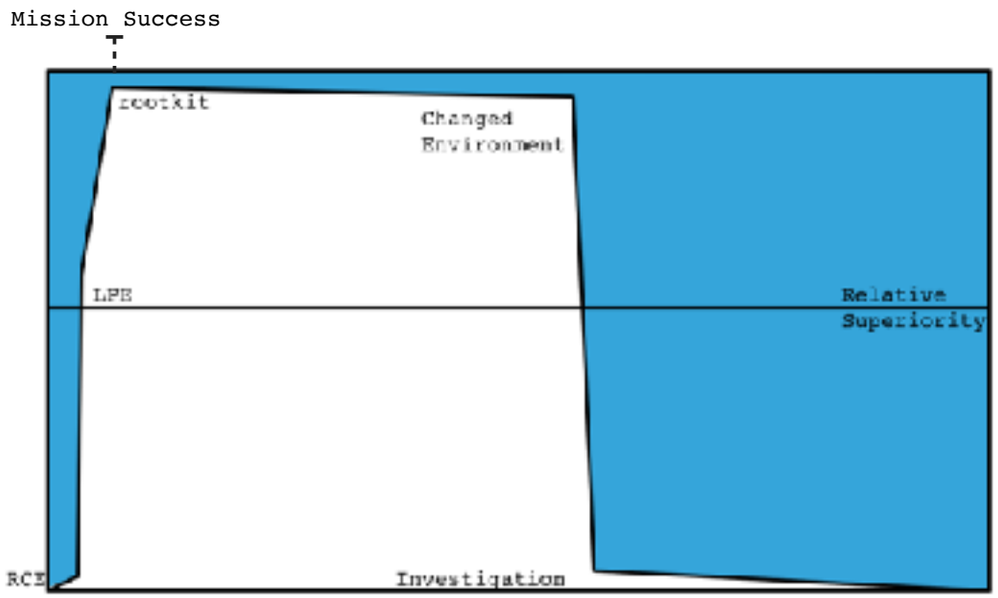
The Saga of Ryan and kernel.org

- Linux's kernel.org system was hacked on[1]: 2011-08-12 [2]
  - Phalanx rootkit was installed for 17 days: 2011-08-29
- OOPSEC
  - [redacted]
- Donald Ryan Austin is arrested for the hack: 2016-08-28 [3]
  - CFAA statute of limitations is 5 years

Recorded Future

RFUN 2017

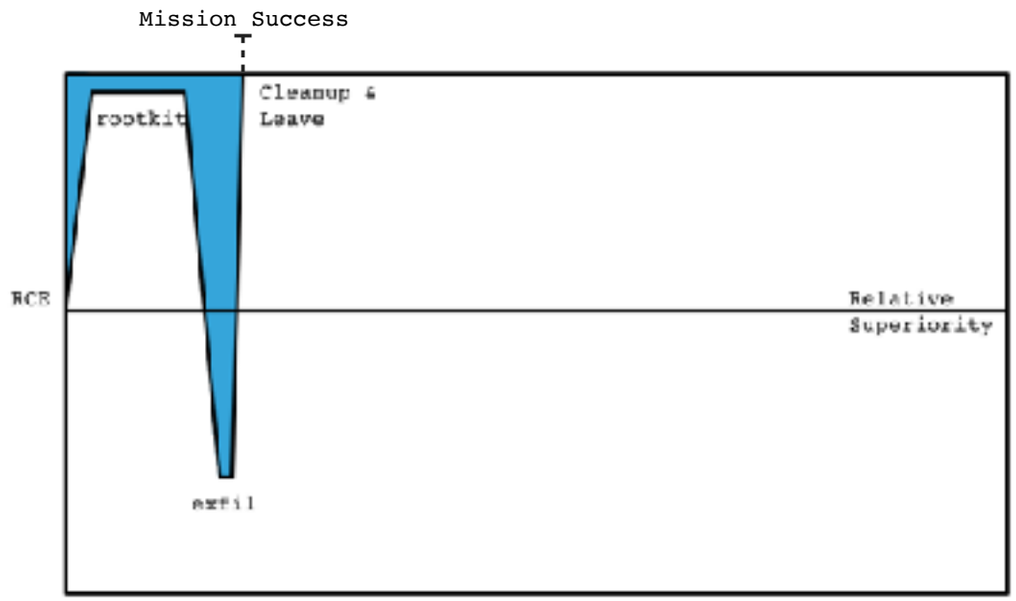
[1] kernel.org has been hacked many many more times than the one compromise here
[2] story here: https://www.theregister.co.uk/2011/08/31/linux_kernel_security_breach/
[3] story here: https://www.theregister.co.uk/2016/09/02/alleged_linux_hacker_arrested/



Recorded Future

Hacker: bad luck

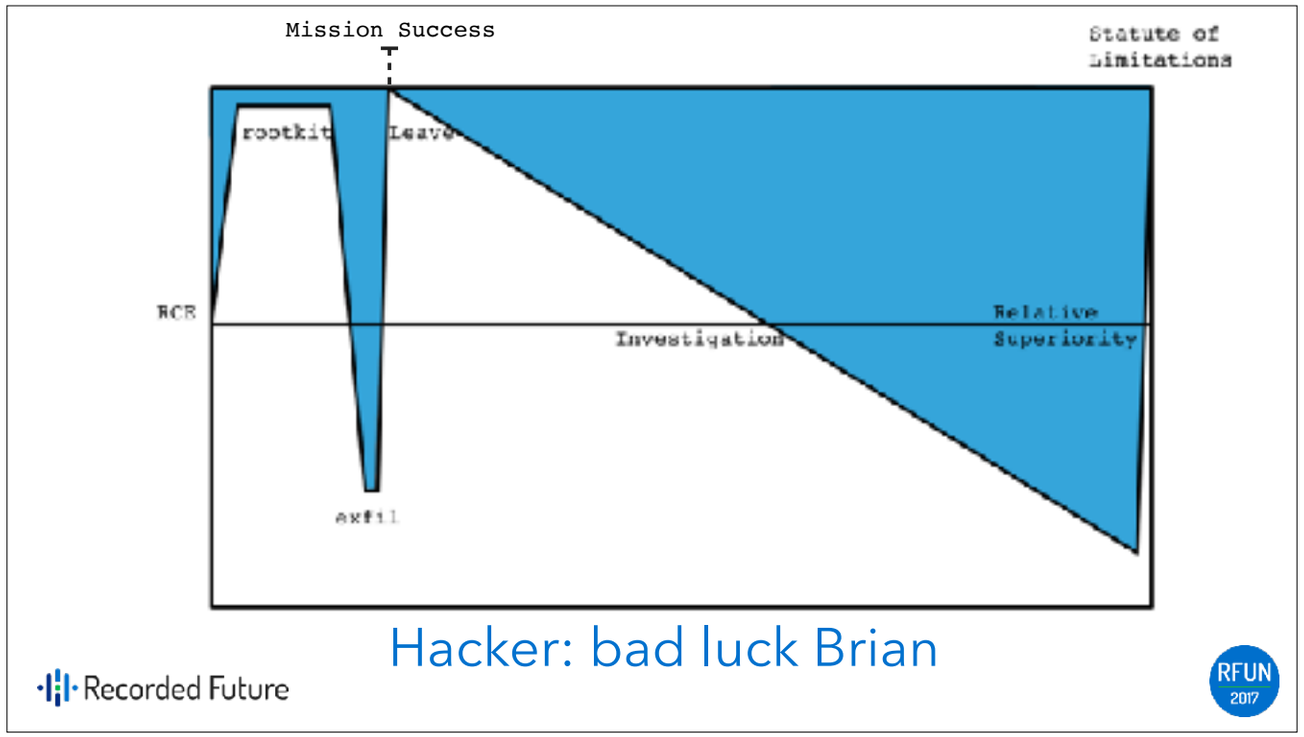
RFUN 2017



Recorded Future

Hacker: Platonic ideal

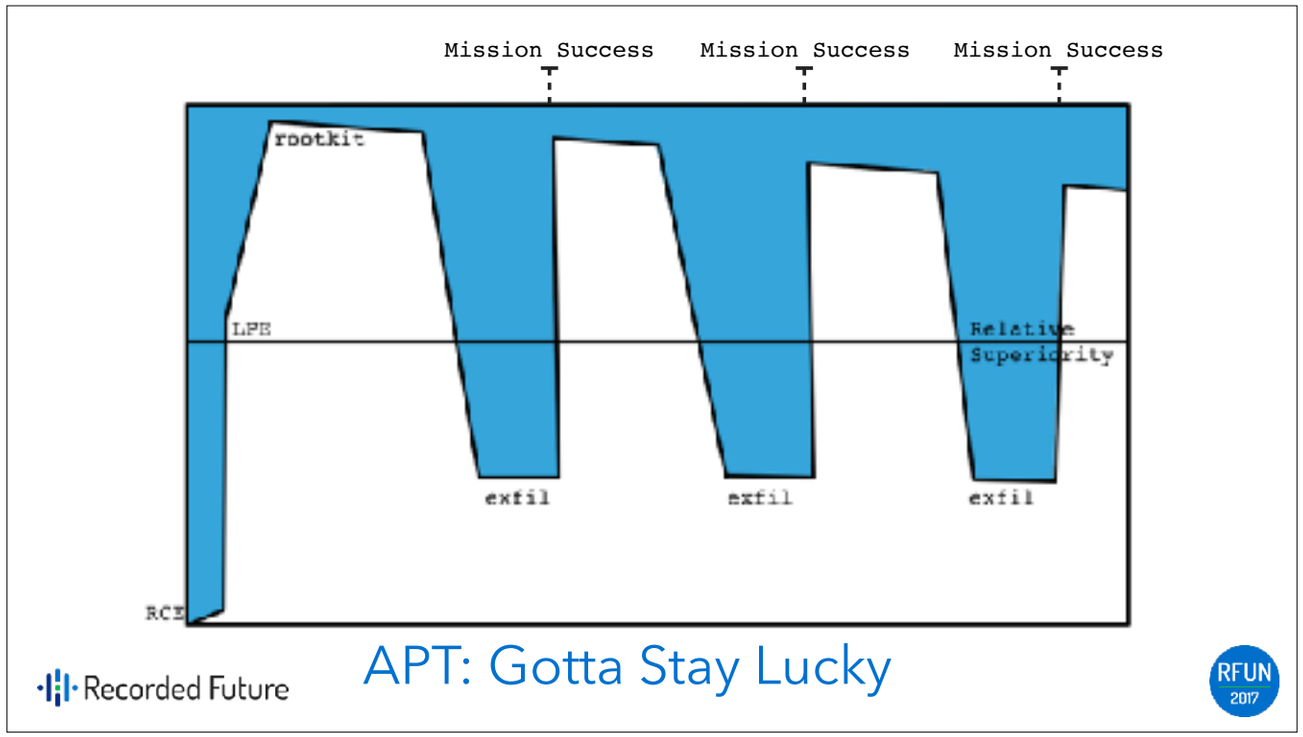
RFUN 2017



Hacker: bad luck Brian

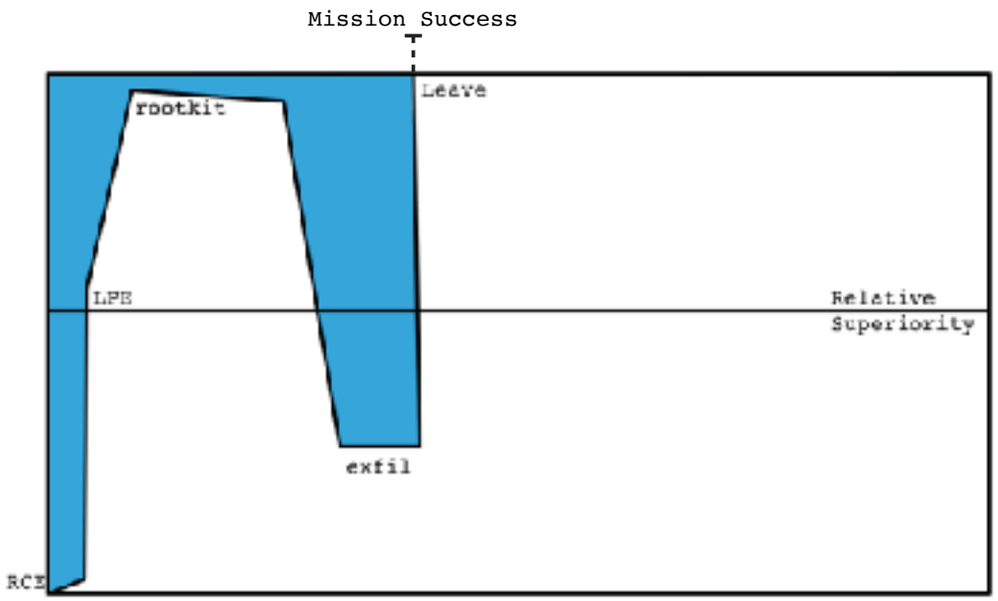
Recorded Future

RFUN 2017



The odds are stack against APT operations. Remaining hidden forever is a pretty hard task. Not many crews are capable of it. I suspect the self deleting timeouts in US malware is not just about legal requirements (“the warrant for this surveillance has expired”) but because they are aware that time is not on their side, so they want to ensure that automatic anti-forensics (counterintelligence) kicks in and removes malware traces.

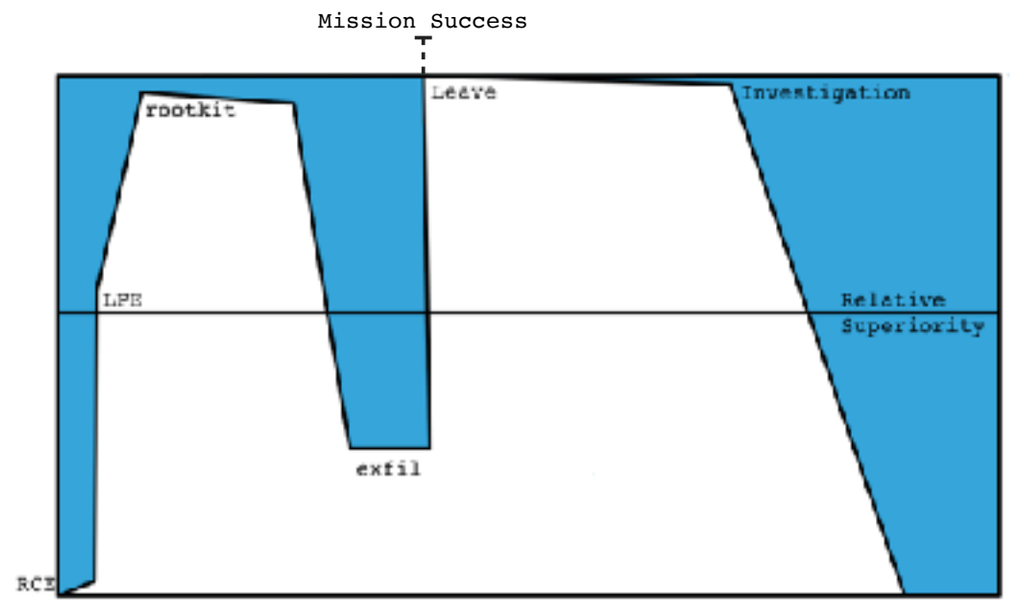
Their network access too is built on really cool ephemeral multi hop bouncers.



APT: lucky lucky

Recorded Future

RFUN 2017



APT: lucky til it ain't

Recorded Future

RFUN 2017

Recorded Future

RFUN 2017

For most threat actors it really doesn’t matter… nation states just go back and do it again. Few criminals get caught because they operate out of protected territory. Most experienced hackers are too good to be detected.

Anything you do can get you killed, including doing nothing.

Murphy's Laws of War

Recorded Future

RFUN 2017

Cyber operations are cyclical. Even after the attacker “loses” and is evicted from the network, they (or another attacker) will begin seeking access again.

One option might be to leave contingency implants which provide a fail safe last resort method of gaining access after the primary implants have been removed.

Another option is that persistence is overrated… maybe it is easier to just re-compromise machines when you need them. This is certainly safer in that the long tail exposure is reduced as there isn’t anything to be accidentally discovered.

CI for CNO

- Is persistence worth it? Security in not leaving implants around for chance discovery.
- National characteristics of APT style play a part here, persistence by default vs “in 10 yrs will we even care?”
- Attacker counterintelligence is important: monitoring administrator activity to detect changes (e.g. discovery of a breach)

Recorded Future

RFUN 2017

Attackers have to worry about a lot of things when they break into a network. Weigh trade offs between discovery, which might retroactively impact operational success vs. “perfect forward subversion of trust” -> Iran can have a nuclear program …but will it be their nuclear program?

There are tricks and techniques for alerting on discovery, so you know when you’ve been rumbled. Additionally, an attacker may want to place contingency implants in “safe” areas, so that if they lose access to their primary network, they have a mechanism to regain entry without having to hack things all over again.

How these trade offs are applied Is in some way a reflection of the national characteristics of the APT group, where some very strictly “build a better washing machine” operators (china!) don’t know what sort of washing machine they’ll care about in a decade, so they don’t as much about persistence. They want to have more data more faster. Russia is by nature very wedded to secrecy and being covert. Once they’re in, they like to stay in, if for no other reason than they don’t want to be exposed.


Recorded Future
RFUN
2017
Final Thoughts

Lifespan of Tooling

- Vulnerabilities and exploits are, by nature, ephemeral
- Implants age, support infrastructure grows old
  - Defenders make discoveries, knowledge accrues and spreads
- Targeted systems have a life cycle too
  - Systems get upgraded, rebuilt, or decommissioned
  - New systems are introduced

Recorded Future

RFUN 2017

“Once you have trained a surveillance team to perfection, it is time to start replacing them, for they’re old and blown… // side effect of time working for defenders is that attackers tools “wear out.” What this means in cyber is kinda fascinating.

One of the problems for attackers is that each time they’re discovered and ejected, their tools techniques and procedures are compromised. If defenders have adequate knowledge sharing then eventually the attacker has to replace their TTP chain entirely. This is expensive (for big groups which need to standardise because training + support). Costly for small groups too (relatively speaking), but some APTs (e.g. Iran) are so chaotic and diverse in their tooling that losing one TTP chain doesn’t matter too much.

Lifespan of Tooling, cont.

- Operational requirements change
  - Adapt to new defensive technology
- Size matters: operators
  - Large teams require more standardisation (training)
  - Collaboration and sharing (geo location,)
- Size matters: victims
  - Managing 10 implants is different from 10k

Recorded Future

RFUN 2017

Tooling is a major commitment by an APT. It has to be designed and developed and there is the secrecy aspect which adds overhead and friction, and basically, as a group you don't want to change TTP more than you need to. This is why elite TTP that are used for elite targets, once they start getting blown and compromised, rather than discarding the tools and replacing them, APTs will instead move that TTP chain down a layer to less important targets.

So while in a hard target would get an advanced elite implant set with 0days and so on… as that kit becomes more "weathered" and well known, the group will switch to new TTP suites for hard targets, but they will take the "TTP v1.0" and use it against less interesting targets. This "democratization of the implant" is a funny effect. The tools used by advanced actors gradually become relevant for less and less critical targets… so the TTP is basically dispersed, diffused out, not by economic actors or dark web secret societies — but because the attackers keep getting caught and have to extract maximum value from their toolchains before retiring them.

Changes in diffusion of tooling are because discoveries democratises who the elite tools can be used against.

Eternal defence is bound to lose at some point, but eternal offence is also bound to lose.
“in guerrilla war, the guerrilla wins by not losing, the conventional army loses by not winning” - Kissinger


Recorded Future
RFUN
2017
Questions?


Recorded Future
RFUN
2017
Thank you.