Red Teaming: Gaps and Musings

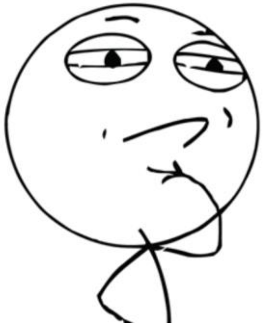
Sam Sayen
keybase.io/keyzer

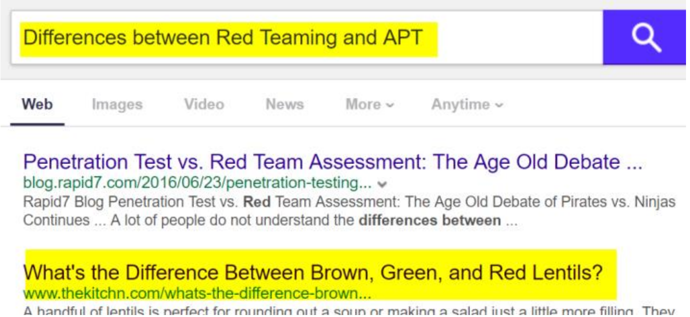
DerbyCon VIII
LOUISVILLE, KY-2018

WTH is this about.

Inspiration for talk

- Wanted to highlight tactics that APT’s are capable of that Red Teamers can’t for various reasons
- Currently phishing and cred harvesting are successful and used 99% + of the time (IMO) on Red Team engagements. What if in 10 years that doesn’t work?
- Phishing and Cred Harvesting are just a few of the avenues of attack for APT’s. How will Red Teams keep up and continue to provide value to customers?





Differences between Red Teaming and APT

Penetration Test vs. Red Team Assessment: The Age Old Debate ...
blog.rapid7.com/2016/06/23/penetration-testing...
Rapid7 Blog Penetration Test vs. **Red** Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues ... A lot of people do not understand the **differences between** ...

What's the Difference Between Brown, Green, and Red Lentils?
www.thekitchn.com/whats-the-difference-brown...
A handful of lentils is perfect for rounding out a soup or making a salad just a little more filling. They

BIO/Background

chAIR Force Intell (1N6)

- Phone tapping (…ourselves)..
- Got to go get Navy l33t network vulnerability hax0r training in 2003. “Ok Seaman, now is when you double click on Back Orifice”.

State Dept. Foreign Service - Security Engineering Officer (SEO)

- Interesting classes : Lock picking, cutting into safes (not for cool reasons), Bug sweeping.
- SOC monkey, Red Team, and Threat Hunting jobs in Virginia
- Regional Cybersecurity Officer based out of US Consulate Frankfurt, Germany

Current Job: Mandiant Proactive Consultant

- Web App testing, Externals, Internals, Red Teaming, Outlook, Outlook, and then some more Outlook
- Exposure to a variety of clients on opposite ends of security spectrum
- Amazing team of consultants to learn from.
  - Top notch open source tools (links on Appendix slide)

Fun(ish) fact - SEO History

- Job was born out of the SNAFU that was the US Embassy construction in the former Soviet Union.

Shockingly, the Soviets filled it with bugs.

Who could of imagined.

¯\_(ツ)_/¯

The Soviets filled the walls of the U.S. embassy in Moscow with diodes to confuse bug detectors.

Definitions (cherry picking definitions from Wikipedia)

APT

- For the sake of this briefing, **APT = an attacker with a high level of skill, intent, and resources**
- **Median Global dwell time for compromises was 101 days in 2017 for Mandiant investigated breaches*. This includes plenty of non “advanced” adversaries of course.**

Red Teaming

- ………..red teams provides "**real-world attack simulations** designed to assess and significantly improve the effectiveness of an entire information security programme“…………
- **Usually 3-5 weeks long** (personal experience), but may be lengthier if using an inhouse Red Team

**2018 FireEye M-Trends Report*

Limiting Factors

Type	APT	Red Team
• **Time**	• Limited by goals, staffing, maybe geopolitical events	• 3-6 Weeks (typically with reporting)
• **Tooling**	• Dedicated support/tooling development team. Actual devops for RAT and modules.	• OpenSource tools, heavy reliance on the excellent Cobalt Strike framework. • Maybe an internal developed RAT frameworks for well funded RT's or ones with allocated dev time.
• **Infrastructure**	• Dedicated support staff to configure/setup infrastructure. Ability to pick/choose already compromised servers for payload delivery or C2.	• Cloud servers if agreement is signed, otherwise limited to your own dedicated infrastructure/IP range.
• **Legal/Scope**	• No restrictions. "Oh no Mr. President, don't put me on your FBI Watch List for following orders from Putin." (note to self: don't start rant)	• Lots of issues if you step out of scope. Plenty of no go areas. Personal email, personal devices, third party web sites, third party contractors, out of scope cloud services, etc.

A few epic hacks to demonstrate the gap

No Time Constraint - Phineas Phisher Hack

Attack path to target - Phishing avoided since target org was small and likely very aware. “Didn’t want to risk alerting them of targeting.”

“So, the hacker explains, three options presented themselves: "look for a zero-day in Joomla, look for a zero-day in postfix, **or look for a zero-day in one of the embedded devices.**"

"A zero-day in an embedded device seemed like the easiest option," the hacker added, **"and after two weeks of work reverse engineering**, I got a remote root exploit."

Red Teamer train of thought:
What if you burned through the engagement hours and at the end there was no working exploit?

Taking large gambles with engagement time and the clients money is not acceptable. Internal Red Teams may be able to attempt something if they have the skills/resources.

```
  _   _            _      ____             _    _ 
 | | | | __ _  ___| | __ | __ )  __ _  ___| | _| |
 | |_| |/ _` |/ __| |/ / |  _ \ / _` |/ __| |/ / |
 |  _  | (_| | (__|   <  | |_) | (_| | (__|   <|_|
 |_| |_|\__,_|\___|_|\_\ |____/ \__,_|\___|_|\_(_)

                    A DIY Guide
```

https://pastebin.com/d19jATvZ
https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/

No Tool/Infrastructure Restraints – “No Easy Breach”

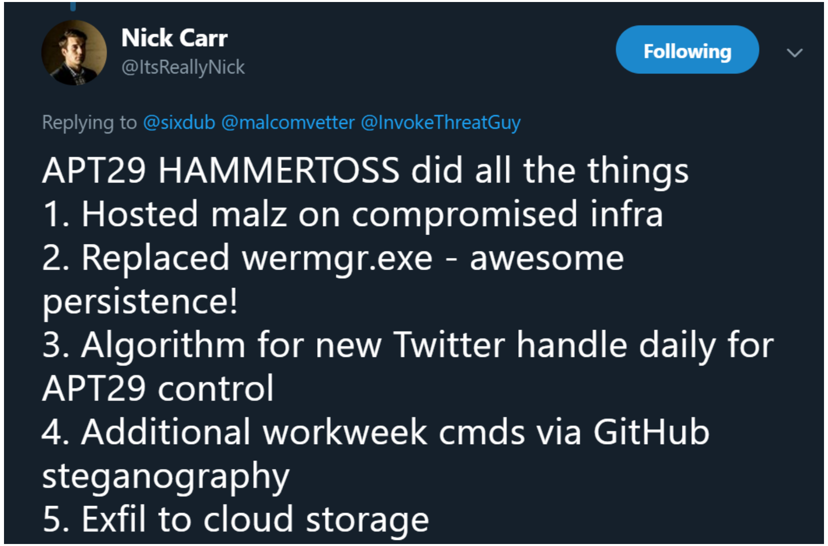
APT actions

Mandiant consultants briefed during DerbyCon 2016.

APT29
1039 compromised systems
1000+ unique malware samples
1000+ unique C2 domains/IPs
7000+ attacker files including scripts & tools
used strong crypto in **C2, used exclusively compromised 3rd party sites and social media**

Pace: Infected ~10 systems/day

For one Breach……………………



Nick Carr
@ItsReallyNick
Following

Replying to @sixdub @malcomvetter @InvokeThreatGuy

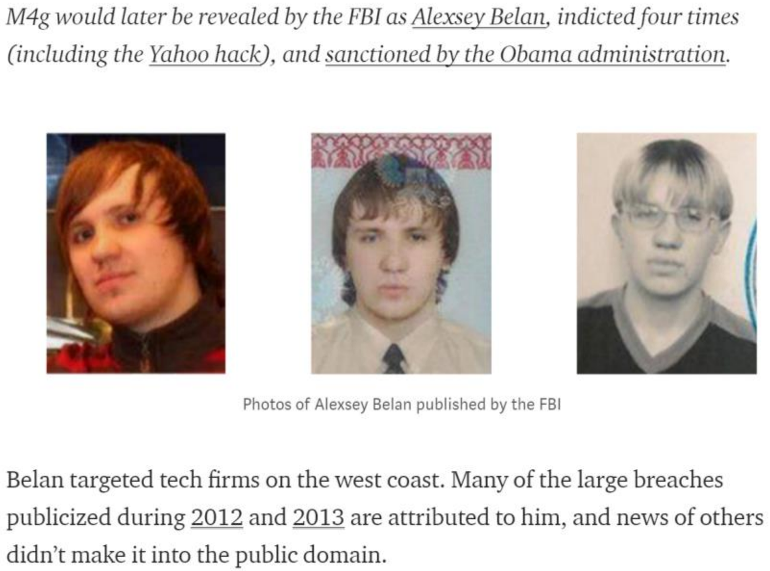
APT29 HAMMERTOSS did all the things
1. Hosted malz on compromised infra
2. Replaced wermgr.exe - awesome persistence!
3. Algorithm for new Twitter handle daily for APT29 control
4. Additional workweek cmds via GitHub steganography
5. Exfil to cloud storage

https://www.slideshare.net/MatthewDunwoody1/no-easy-breach-derby-con-2016
https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf

No Scope Constraint – Yahoo hack

Attack path to target - **located engineers personal website (via Linkedin) - compromised the web server which was hosted in a VM on the engineers personal computer.** He then performed a VM escape to the Host OS via a SSH brute force attack. Then he was able to steal the client VPN certificate and private keys to access target corporate network and development systems.

Engineering credentials were used to commit backdoors to version control which were self-approved and later deployed into production



M4g would later be revealed by the FBI as Alexsey Belan, indicted four times (including the Yahoo hack), and sanctioned by the Obama administration.

Photos of Alexsey Belan published by the FBI

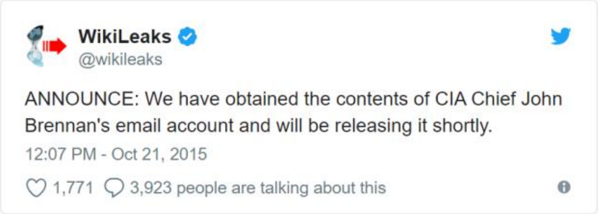
Belan targeted tech firms on the west coast. Many of the large breaches publicized during 2012 and 2013 are attributed to him, and news of others didn't make it into the public domain.

https://medium.com/alphasoc/alexseys-ttps-1204d9050551
https://www.nytimes.com/2017/03/17/technology/yahoo-hack-data-indictments.html

Scope Constraints (continued)

Personal Email Targeting

- **Clear Win for APT over Red Team**
- Many organizations are not doing SSL decryption on webmail, or if they are it is not being parsed and ingested into the SIEM properly.
- Phishing personal emails side steps target organization mail security stack (if applicable). Most orgs don't want users to report suspicious emails to personal accounts even though users are checking those accounts at work.
- If an attacker compromises a personal account and finds work documents/info on there why would the victim report? Talk about conflict of interest. Reporting it incriminates the victim for violating corporate/gov policy..



WikiLeaks
@wikileaks

ANNOUNCE: We have obtained the contents of CIA Chief John Brennan's email account and will be releasing it shortly.

12:07 PM - Oct 21, 2015

♡ 1,771 3,923 people are talking about this

99 problems, but a scope ain’t one (old meme is?)

Plausible APT actions

- **Start a front company**, land a sub contract with the company your target contracts. Gain legit access. If you get detected, “you were the victim of a compromise and were used to pivot to the target network.” ¯_(ツ)_/¯
- **Intercept hardware** being shipped to a company, swap out chips/boards and then let it be delivered. *cough *cough Snowden leaks. How does your company procure IT equipment overseas?
- **Install devices in hotel networks**, make VPN traffic so unbearable that corporate users decide to ride durty. Intercept/Responder all the things. Ala DarkHotel threat group.
- **Internet Café’s, Common Access Computers** – still applicable in much of the developing world. I am guessing using one is probably the most efficient way to get your data directly into a nation states data center?

Come get your Cyber Here →

Rabat, Morocco **2016**

99 problems, but a scope ain’t one (old meme still is?)

Things I would do if I was an APT

- **Develop a browser extension** and get it into Chrome’s store. Push out added functionality as needed. Numerous cases of crime ware groups trying to buy semi popular extensions. APT’s have the time/resources to just create them from the start.
- **Make legit Android Apps** that are overly permissioned and get them in the Google Play Store. How can you sort the good for the bad when people are legitimately siphoning your data for advertising, analytics, and crash debugging anyways? Roll your legit profits back into your APT budget.
- **Data recovery** buy all the enterprise infrastructure you can on Ebay and auction. Scrape for data, then resell. Rinse/Repeat. Locate companies that lease hardware to corporations and try to get used gear after the leases are up.
- **Start a CDN.** The world loves KB’s of minimized/packed JS being delivered on every website from regionally located third party data centers. How could this possibly go wrong?

Trust but ~~verify~~. Awww #@%# it, just trust it.

I DON'T ALWAYS LET THIRD PARTY CODE RUN ON MY SITE
BUT WHEN I DO I MAKE SURE IT IS 80KB OF PACKED JS

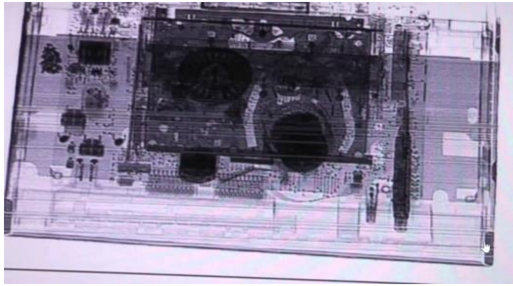
24 Port Elephant in the Room

Core infrastructure

Hard to patch, exposed, and limited endpoint visibility make for a dangerous combo.

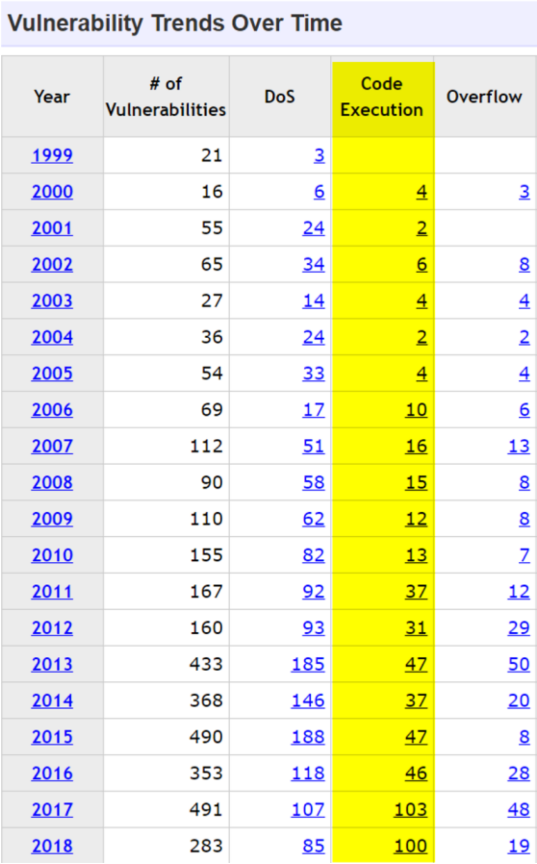
Snowden leaks shed a lot of light on this, but seems to be shrugged off for the most part.

How do you procure devices? Overseas offices? Secure procurement from the US, or shipped? 24/7 manned office by your company staff at your overseas offices?



https://www.wired.com/2013/09/nsa-router-hacking/

Interesting CISCO trend…



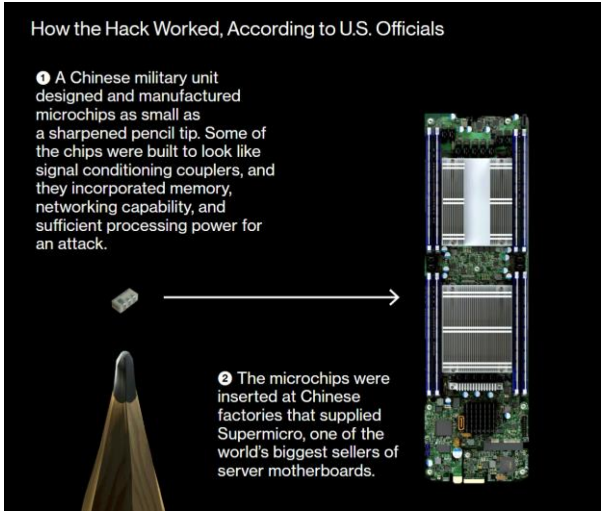
Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow
1999	21	3		
2000	16	6	4	3
2001	55	24	2	
2002	65	34	6	8
2003	27	14	4	4
2004	36	24	2	2
2005	54	33	4	4
2006	69	17	10	6
2007	112	51	16	13
2008	90	58	15	8
2009	110	62	12	8
2010	155	82	13	7
2011	167	92	37	12
2012	160	93	31	29
2013	433	185	47	50
2014	368	146	37	20
2015	490	188	47	8
2016	353	118	46	28
2017	491	107	103	48
2018	283	85	100	19

Holy crap…. Oct 4th headline

Hardware compromise

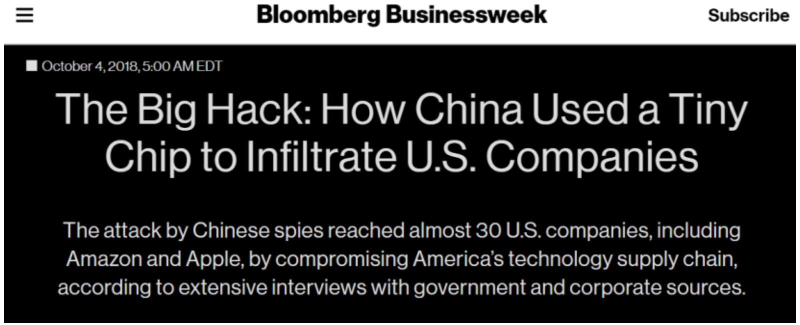
- "Multiple people familiar with the matter say investigators found that the chips had been inserted at factories run by manufacturing subcontractors in China."



How the Hack Worked, According to U.S. Officials

❶ A Chinese military unit designed and manufactured microchips as small as a sharpened pencil tip. Some of the chips were built to look like signal conditioning couplers, and they incorporated memory, networking capability, and sufficient processing power for an attack.

❷ The microchips were inserted at Chinese factories that supplied Supermicro, one of the world's biggest sellers of server motherboards.



October 4, 2018, 5:00 AM EDT

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

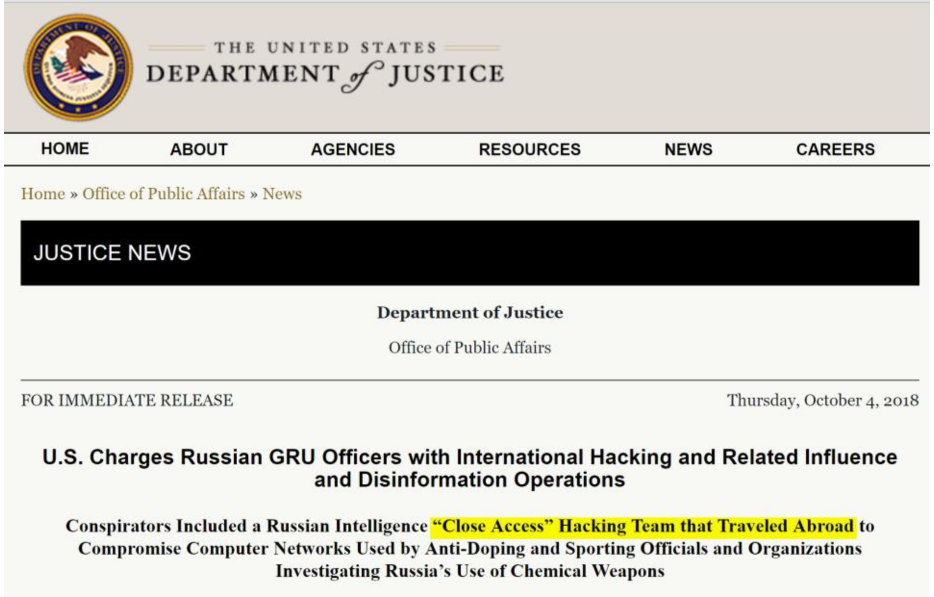
The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

- **"In emailed statements, Amazon, Apple, and Supermicro disputed summaries of Bloomberg Businessweek's reporting."**
- **"The companies' denials are countered by six current and former senior national security officials, who—in conversations that began during the Obama administration and continued under the Trump administration—detailed the discovery of the chips and the government's investigation. "**
- That's a school bus size discrepancy in reporting…..

https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
https://www.bloomberg.com/news/articles/2018-10-04/the-big-hack-amazon-apple-supermicro-and-beijing-respond

Holy crap…. Another Oct 4th headline

Russian GRU “Close Access” Hacking Team - FancyBear



THE UNITED STATES DEPARTMENT of JUSTICE
HOME
ABOUT
AGENCIES
RESOURCES
NEWS
CAREERS
Home » Office of Public Affairs » News
JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Thursday, October 4, 2018

U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations

Conspirators Included a Russian Intelligence “Close Access” Hacking Team that Traveled Abroad to Compromise Computer Networks Used by Anti-Doping and Sporting Officials and Organizations Investigating Russia’s Use of Chemical Weapons

- “We want the hundreds of victims of these Russian hackers to know that we will do everything we can to hold these criminals accountable for their crimes,” said U.S. Attorney Brady.
- Man oh man, we are REALLY keeping Russia in line… (sarcasm)
- “Using **specialized equipment**, and with the remote support of conspirators in Russia, ………….**these close access teams hacked computer networks used by victim organizations or their personnel through Wi-Fi connections, including hotel Wi-Fi networks.”**
- Maybe Responder on the hotel network isn’t just for the DPRK (DarkHotel)? Shocker.

https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and
https://securelist.com/the-darkhotel-apt/66779/

Legal/Scope Constraints

APT actions	Typical Red Team adaptation
• Watering hole attack. Infect dozens of government sites with fake analytics scripts that profiles end users and delivers second stage script if victim falls within IP ranges of target organization.	• None. No legal way to emulate.
• Target organizations users by going after their personal email accounts. Many times organizations are not properly doing SSL decryption on webmail, and sending a mal link to personal email side steps the organizations mail security stack. Most orgs don't want users to report suspicious emails to personal accounts even though users are checking those accounts at work. (countless breaches)	• None. No legal way to emulate.
• Low and slow password spraying of companies public facing Outlook Web Access (OWA) portals/Citrix/Cisco VPN gateways over the course of days/weeks/months. (countless breaches)	• Password spray the OWA portal across the user base using "Summer2018" as the password or similar. Make sure not to lock anyone out or affect operations. If you have no hits, move on.
• Target organizations admin/developer home computers to get access to VPN keys for corporate network. (Yahoo Breach) • Target lower security network of subcontractor to gain access (Target Breach)	• None. All out of scope.

Scope Constraints (continued)

Improper threat modeling

- If the client doesn't know the network or core business functions your RT goals and are usually an after thought along with the usual, "Get Domain Admin".
- RT'ers usually try to pop Domain Admin and then gain access to the objectives. "Trickle down pwnomics".
- In a company with a decent SOC, segmentation, and log analysis capabilities that may cause a wire to be tripped prematurely.
- End result: You get evicted, and the client thinks that they have a mature security posture, despite the reality which is that the scope dictated pace forced you to escalate actions beyond what a real attacker might want/have to do.
- You pushed for Domain Admin to meet a timeline rather than staying quiet in the network for months and learning where things are by using shares/sharepoint/wiki's/jira/confluence like a real world attacker might have the patience to do.

A few ideas to mix things up

Overcome Imaginary Scope Restraints

BenHeise liked

@fouroctets · 1h

Point - Counterpoint

- **CLIENT:** You can’t target XYZ because they are too important.
- **RT:** If they are that important, then someone else is already targeting them without your permission.
- **CLIENT:** You can’t pretend to be from our security team, that undermines user trust.
- **RT:** Employees should know how to reach the security team to verify identities out of band. Pick up a phone.
- **CLIENT:** You can’t phish after 2pm each day because we need to know of any compromises before COB.
- **RT:** Are you thinly staffed at night or on the weekend/holidays? Maybe TIER 2 is M-F, 9-5? Do your job postings for senior analysts say shift work or are they 9-5?

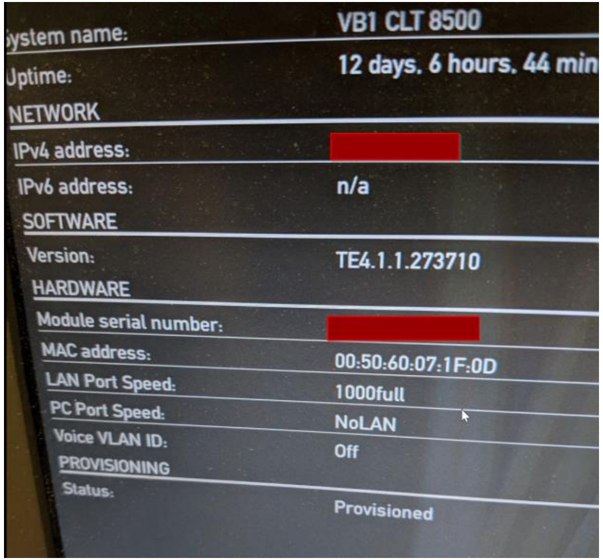
  Is your entire TIER 3 one guy named “Bob” that is tearing up Twitter with Derbycon selfies?

  Staffing/manpower issues aren’t lost on adversaries... Just a thought.

Loosely Replicate Hardware Compromises

For Hard Targets

- Typically we think of Internal Red Teaming as Insider Threat scenarios, but it is also the closest example of an actual hardware compromise.
    - Bypasses any sort of NAC or 802.1x on the network if they exist since the device is there legitimately
- Put a tap on a core device
    - grep your pcaps. Anything sensitive? Answer: yes
- Responder.py yourself from different choke points.
    - Is LLMNR and NBT-NS actually disabled?
- Use a VOIP Phone MAC/IP to RDP to servers or connect to the internet even if you don't have to.
    - Anything tripped??
    - "Don't worry, we put the phones in a VLAN."
    - "……..yeah, and it still has access to the servers and internet"

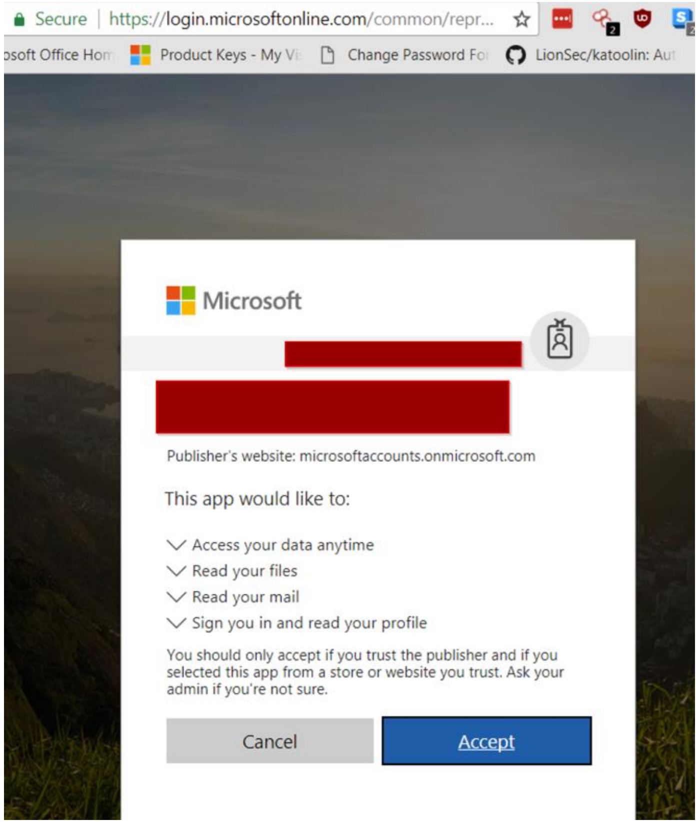


```
ystem name:            VB1 CLT 8500
Uptime:                12 days. 6 hours. 44 min
NETWORK
IPv4 address:          [redacted]
IPv6 address:          n/a
SOFTWARE
Version:               TE4.1.1.273710
HARDWARE
Module serial number:  [redacted]
MAC address:           00:50:60:07:1F:0D
LAN Port Speed:        1000full
PC Port Speed:         NoLAN
Voice VLAN ID:         Off
PROVISIONING
Status:                Provisioned
```

Abuse the Cloud

OAUTH bypasses MFA

- Overall the cloud is probably a more secure move for most companies
- But, there are some abusable avenues
- PWNAuth by Doug Bienstock
- Amazing tool (https://github.com/fireeye/PwnAuth)
- Yet…… seemingly underutilized which is odd considering the number of targets this is perfect for.
- Note: He's giving a talk on MFA bypasses here as well with Austin Baker.



[redacted]

[redacted]

Publisher's website: microsoftaccounts.onmicrosoft.com

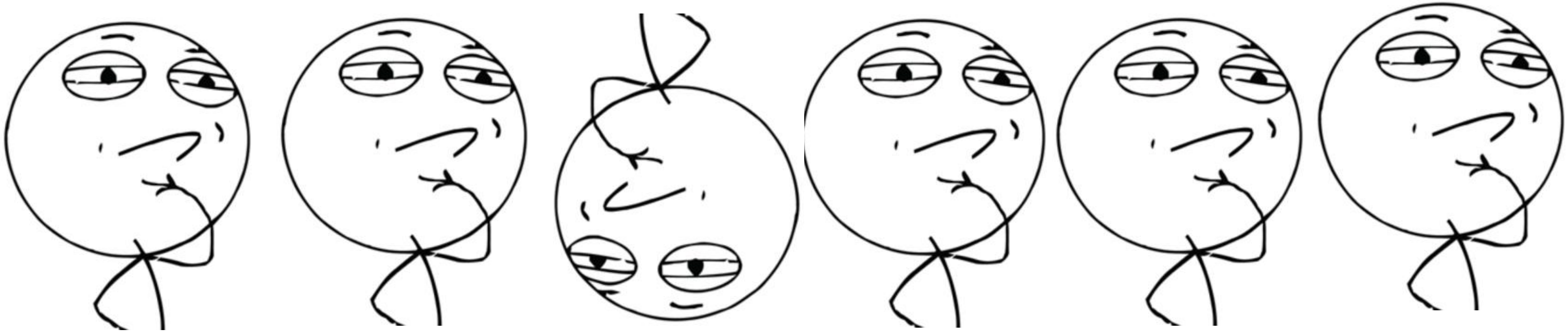
This app would like to:

- Access your data anytime
- Read your files
- Read your mail
- Sign you in and read your profile

You should only accept if you trust the publisher and if you selected this app from a store or website you trust. Ask your admin if you're not sure.

This got me thinking.

Is the status quo for Red Teaming from the outside **really** the closest thing to advanced adversary simulation???



My take on current status quo for RT’ing

Red Team

- Red Team spends valuable ($$$$) time
    - Setting up infrastructure,
    - Creating payloads,
    - Obfuscating payloads
    - Creating phishing scenarios
        - Getting those client approved
    - Creating target lists
        - Getting those client approved
    - Phishing
    - Getting a foothold
    - Maybe losing a foothold
    - Burning infrastructure
    - Rinse/Repeat if needed
- **Finally… you are in and the actual assessment with actionable items for the client to fix begins!!!!**

Client reaction to the Red Team

- They already invest in “Phishing Testing” subscriptions
    - Users still click. They, aren’t going to get fired. What did we learn here today Bob? Shrug.
    - **No real gains.**
- You phished them from a legit domain and your C2 is domain fronted and a top 10 tech company.
    - They can’t feasibly block a CDN and proxy services are a joke to bypass.. Shrug.
    - **No real gains**
- They already invest in AV and probably EDR
    - You got around it.
    - They get angry at EDR/AV vendor. The vendor gets a signature for the payloads you sent. Maybe they do a Hash match or maybe a signature based on a 4 byte string. LOLZ!!!!!
    - **No real gains**
- **Red Teamer gets in and the the actual assessment begins!!!**

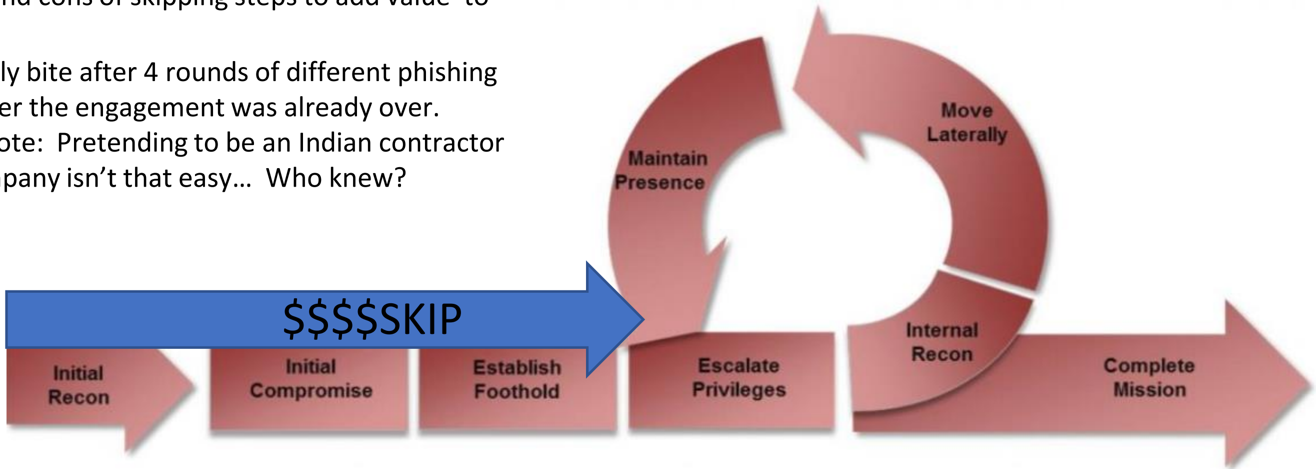
Internal “Red Teaming”

For Hard Targets*

- For clients on the mature side there may be more benefit from skipping the Recon/Compromise/Foothold steps of the ATTACK cycle. (Probably not a popular thing to say)
- Spear Phishing hard targets takes a bit of luck, and time. Particularly for tech savy targets. AKA Phineas Phisher hack on the Hacking Team. Weigh the pros and cons of skipping steps to add value to the engagement.
- I had one customer finally bite after 4 rounds of different phishing scenarios…. A week after the engagement was already over. Everybody loses. Side note: Pretending to be an Indian contractor to a Middle Eastern company isn’t that easy… Who knew?

For Time Restricted Targets

- Two weeks to do light recon, setup infrastructure, get targets, get scenarios approved, conduct status updates…….. And then perform all the stages of the ATTACK lifecycle is not realistic.



* For softer targets, starting inside the network or outside won’t change the results

Internal RT’ing. New take on an old idea.

Flexible

- Can be onsite
- Can be remote
  - Target whitelist’s a payload and executes it
  - Or use hardware like Pwnie devices

Red Team has a heavy reliance on Phishing/Cred Harvesting

- Not a problem now, but what if in 10+ years:
  - Companies are finally using properly configured VDI/dumb clients?
  - MFA is consistent and can’t easily be bypassed.
  - Application Whitelisting doesn’t have dozens of bypasses
  - Scripts/droppers from the internet are defang’d or blocked by browsers…….. By default.
    - SRSLY. Why in the hell can you still download and execute an .hta by double clicking?

Future Proof???

- APT’s have a massive advantage to get a foothold in the future if phishing/cred harvesting is no longer easy/viable.
  - Possible Zero days (cough cough Eternal Blue)
  - Third party access (Target hack with HVAC co.)
  - Data center access
  - Hardware interdiction
  - Supply chain
  - Exfill via 4G/LTE, or even sneakernet
  - Evil Maid
  - Personnel targeting (Dark Hotel threat actors)
  - On and on and on.
- **However, once an APT is inside the perimeter the playing field levels out with a good Red Team**

Thank You, and enjoy the con

Appendix: Mandiant Tools/Scripts (offensive)

Tool	Purpose
• https://github.com/danielbohannon/**Invoke-Obfuscation** • https://github.com/danielbohannon/**Invoke-DOSfuscation**	• Obfuscate Powershell/cmdline – Inspired by FIN threat actors. (Author: Daniel Bohannon @danielhbohannon)
• https://github.com/Raikia/**FiercePhish**	• Phishing framework – (Author: Chris King @raikiasec)
• https://github.com/fireeye/**PwnAuth**	• OAUTH phishing/abuse framework (Author: Doug Bienstock @doughsec)
• https://github.com/GreatSCT/**GreatSCT**	• Application whitelisting bypass payload generator (Author: Chris Spehn @ConsciousHacker)
• https://github.com/fireeye/**ReelPhish**	• MFA Phishing framework (Author: Pan Chan, Trevor Haskell)
• https://github.com/harleyQu1nn/**AggressorScripts**	• Cobalt Strike Aggressor Scripts (Author: Harley Lebeau @r3dQu1nn)
• https://github.com/keyzerrezyek/**JQueryingU**	• APT 29 inspired profiling script packed inside legit jQuery (Author: Sam Sayen @penetrate_io mod of Christian Ludwig open source script)