The Triple A Threat:

Aggressive Autonomous Agents

The Grugq, VP of Threat Intelligence

Agenda

- The Triple A Threat
  - Aggressive Autonomous Agents
- What did we learn - surprise
  - Fundamental security hygiene is surprisingly hard
  - Intranets are connected in a shadow Internet
- What next?
  - Worms everywhere and Map Reduce

Triple A Threat

Aggressive Autonomous Agents

Worms

- Looking back
  - In the beginning there was The Internet Worm
  - Then the Age of Worms: CODE RED, Nimda, Slammer, Sasser
  - Nation state worms: OLYMPIC GAMES (Stuxnet)
- Looking around
  - The big three of 2017: WannaCry, NotPetya, BadRabbit
- Looking forward
  - More nation state worms for attack and espionage

Why Worms?

- There are fundamental benefits to using autonomous agents for computer network operations (CNO)
  - They work
  - No limits: they’re free of fallacies, scope, biological constraints and limitations
  - Cheap and deniable
  - Long tail of persistence

Triple A Threat Best Practices

- Attack across the real network topology
  - Target enumeration based on what the infected system knows about the network
- Propagate using fundamental vulnerabilities
  - Infect via: credential abuse, trust relationships, configuration errors, and exploits
- Avoid discovery, examination, and inoculation
  - Sophisticated counter forensics to avoid detection/analysis
  - Multi infection protection w/ a bypass to avoid a kill switch

Timeless Offensive Strategies

Credential Abuse

- Organisations need their IT infrastructure to function
  - This requires system administrators
    - Who need to perform privileged operations
      - Administration: roles
- **Vulnerability**: some users and systems are more equal than others
- **Exploitation**: password cracking, brute force, reuse, pass the hash…
- Mitigation: multi factor authentication*

Timeless Offensive Strategies

Exploiting Trust Relationships

- Organisations need their IT infrastructure to function
  - This requires system administrators and users
    - Who need to access systems
      - Administration: roles, systems, tools
- **Vulnerability**: users and admins need to use and admin systems
- **Exploitation**: `psexec`, `ssh`, etc.
- Mitigation: Least privilege*

Timeless Offensive Strategies

Configuration Errors

- Organisations need their IT infrastructure to function
  - This requires system administrators
    - Who are human
      - Humans make mistakes, cut corners, forget things
- **Vulnerability**: systems are configured for ease of use and administration
- **Exploitation**: (target specific)
- **Mitigation**: Reduce attack surface, network segmentation

Timeless Offensive Strategies

Memory Corruption/Exploits

- Organisations need their IT infrastructure to function
  - This means many systems and minimal disruption
    - Which means inventory management, patch management
      - Patchy patching
- **Vulnerability**: known vulnerabilities with working exploits remain effective for months (years!) after the patch
- **Exploitation**: `./x2`
- Mitigation: Patch, asset management

The Morris Worm - got it in one

- Innovative and complex, including many modern features
  - Infection: buffer overflow exploit, sendmail bug, trust relationships
  - Counter forensics: Process hopping, `argv[0]` changing, memory resident
  - Target enumeration: searched local files, connection tables
  - Password cracking, and additional target enumeration
  - Kill switch (listen on a local port), but w/ immortal bypass

Anatomy of Triple A Capabilities

- Reuse legitimate credentials (stolen or guessed)
- Exploit existing trust relationships
- Exploit configuration errors
- When all else fails, exploit software vulnerabilities

- Solved: multi factor authentication
- Solved: segmentation, least privilege
- Solved: reduce attack surface
- Solved problem: patch

Mitigating the Triple A Threat

- Basic cybersecurity hygiene limits infection vectors
  - Multi factor authentication
  - Least privilege
  - Reduce attack surface
  - Patch
    - Asset management
- Compartmentation enables impact containment
  - Network segmentation
- Detection
  - Telemetry and deception are critical

The important things are always simple.
The simple things are always hard.
The easy way is always mined.

—Murthy's Laws of War

The Big Three

WannaCry, NotPetya, BadRabbit

WannaCry

Overview

- Manual infection on a limited number of patient 0 orgs
  - Escaped into the wild within hours
- Had some very serious limitations, probably a “beta test” gone wrong
  - Kill switch (pours one out for @MalwareTechBlog)
  - Required:
    - Unpatched Windows 7 with exposed SMB
  - Terrible payment management infrastructure

Malware Tech

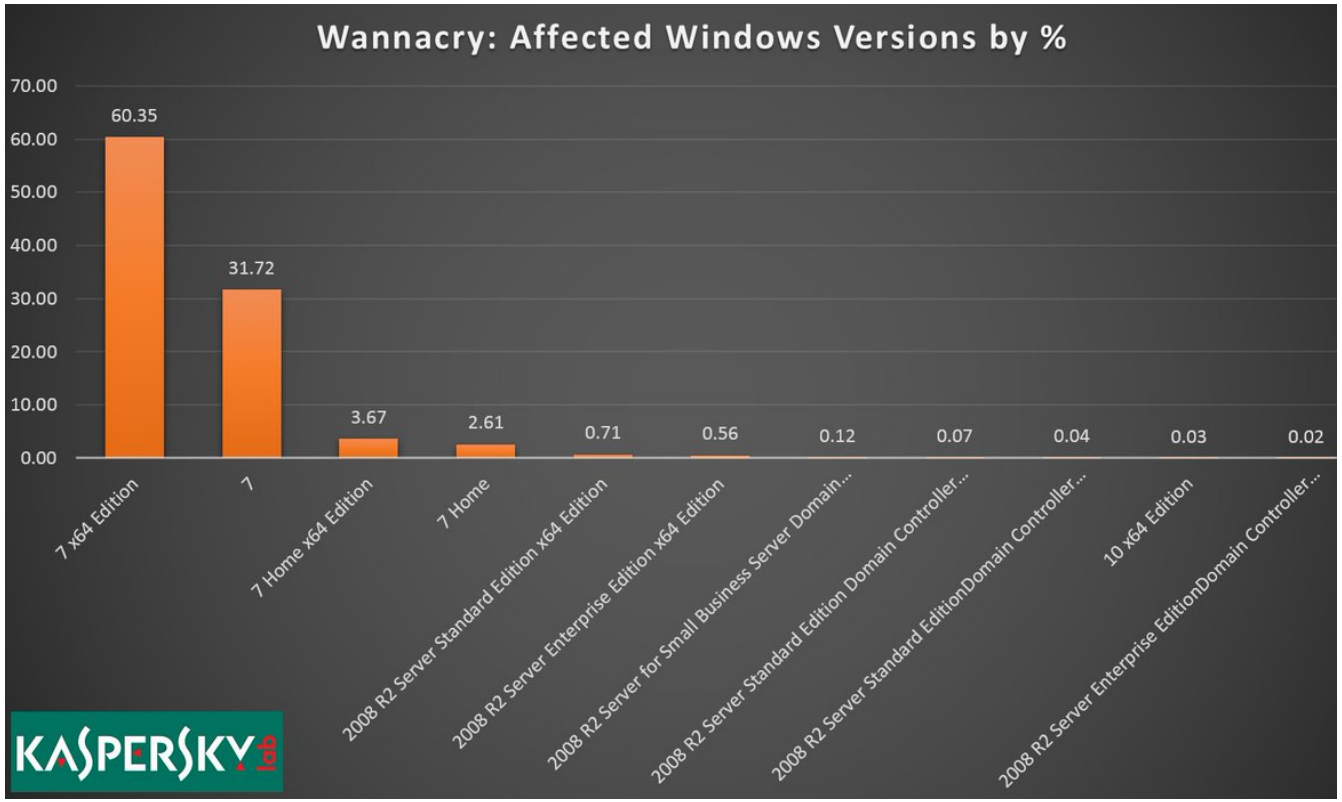
- Initial infection: manual installation
- Propagation
  - Primitive initial versions used, basically, `net exec` on open shares
  - The ETERNALBLUE exploit was critical to the virulence
    - Literally just cut&paste blobs from the `.py` script

Lessons Learned

- Patching is hard
  - MS17-010 released months before WannaCry
- WannaCry spread because of that exploit
  - The lateral traversal was terrible
  - Not very virulent, but very “noisy” (as is most ransomware)
- Long tail persistence is long
  - Comae is still receiving hits on our sinkhole in Dec 2017

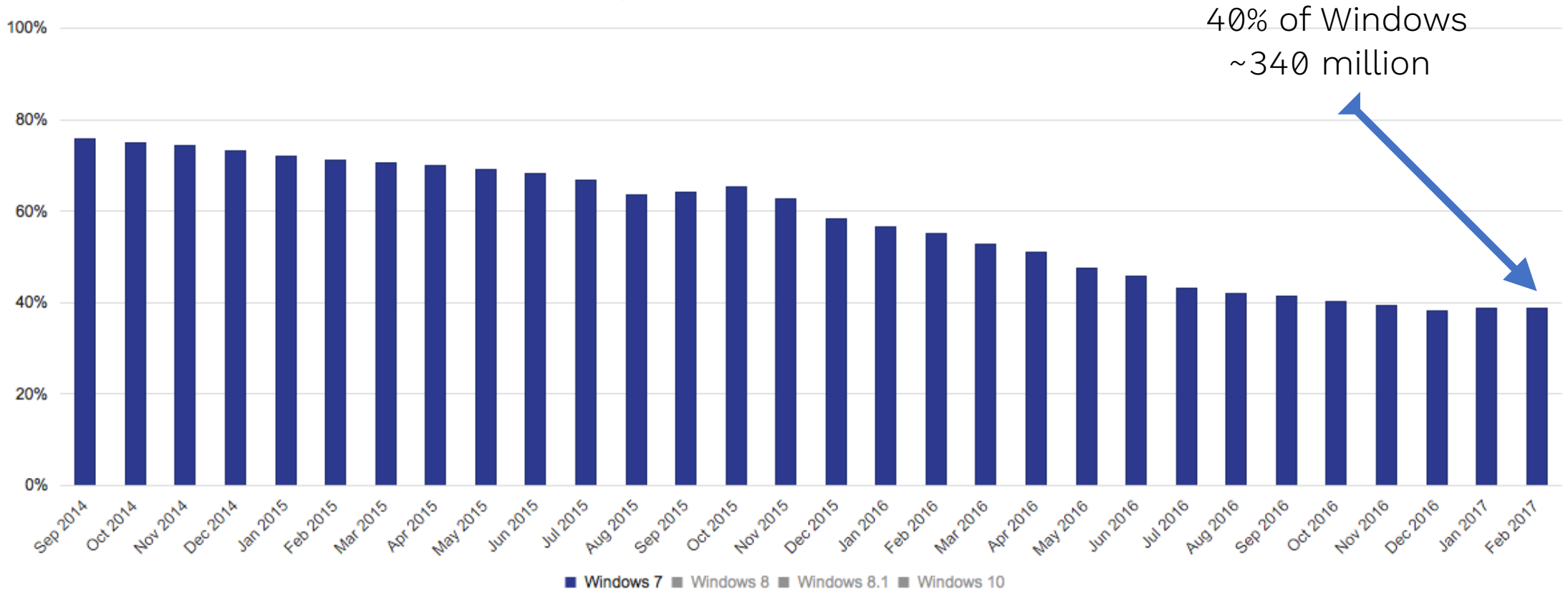
Lessons Learned

- Poor virulence isn't really a problem for propagation



Lessons Learned

- Windows 7 is a big thing



Lessons Learned

- A development version of a program that has only one badly implemented exploit that only works on unpatched Windows 7 with exposed SMB ports can go from a Spanish telco to the NHS in hours
- Real world networks are not castles
  - There is moat
  - There is no outer wall
  - There are no guards screening visitors
  - The perimeter as security boundary is a myth

NotPetya

Overview

- Probably a nation state attack against Ukraine
  - Released day before Ukraine's Constitution day
  - Targeted MeDoc users
  - Phishing attacks directly targeted politicians
- Very tightly targeted w/ a blast radius of "does business in Ukraine"
- Many indicators of a rushed development process
  - Buggy code—not just the "discard the decryption key" bug
- Not maximally infectious
  - Required Local Admin to do damage

Malware Tech

- Frankensteinware
  - Binary patched ransomware kernel REUSED
  - ETERNALBLUE exploit REUSED
  - `mimikatz` REUSED
  - Windows admin tools REUSED

Malware Tech

- ~~Frankensteinware~~ Reuseware
  - Binary patched ransomware kernel REUSED
  - ETERNALBLUE exploit REUSED
  - `mimikatz` REUSED
  - Windows admin tools REUSED

Pandemic

- Targeting* meant global businesses were most exposed
  - Maersk (shipping): $300m + 3 months to cleanup
  - TNT (FedEx): $300m + 3 months to cleanup
  - Merck (pharmaceuticals): $310m
  - WPP (ad group): weeks to cleanup (diversity provided resilience)
  - Reckitt Benckiser (Durex condoms): factories + invoicing problems caused a portion of $100m loss

* (“companies that operate in Ukraine”)

BadRabbit

Overview

- Probably a trial run of a cleaned NotPetya propagation engine
- Initial infection vector: drive by websites with fake update installer, or manual infection
  - Russia, Ukraine, Bulgaria, Turkey, Japan
    - WTF??
- Minor pandemic with a few infections reaching the US

Malware Tech

- A cleaned up NotPetya propagation mechanism
  - Significant improvements indicative of a sr. developer
- A repurposed open source disk encryption tool
  - Popular with the kids these days apparently
- Major improvements over NotPetya
  - Better propagation module
  - Better disk encryption module
- So why the limited release?

Lessons Learned

Conclusions

0days Not Included

- Initial infection vector only matters once
  - Manual breach - WannaCry
  - Supply chain - NotPetya
  - Drive by - BadRabbit
- Global presence means bigger attack surface
  - And more exposure to local conflicts
- Worms traverse true network topologies
  - They don’t care about scope

The future is behind us

- The future of CNO is the Morris Worm from 1988
  - Triple A threat to build a cooperative, communicative, heterogenous sensor network
  - Task a result
  - Collect the take
    - Map Reduce the “deep web”
- NotPetya’s propagation engine was cleaned up and tested
  - Why invest the resources unless it’s for use?

- Core offensive methodologies exploit human factors
  - Decades of success prove they aren't going away
- The problems are solved, but the implementation…
- Defenders have an overwhelming advantage
  - Basic cyber security hygiene, telemetry, detection, deception, compartmentation
- Cyber:

  The problem domain is technical

  The solution domain is political

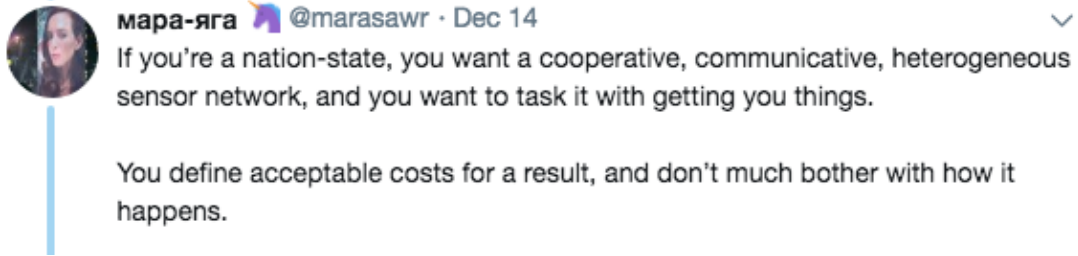
Your perimeter is not the boundary of your network
it’s the boundary of your telemetry

Your perimeter is not the boundary of your network

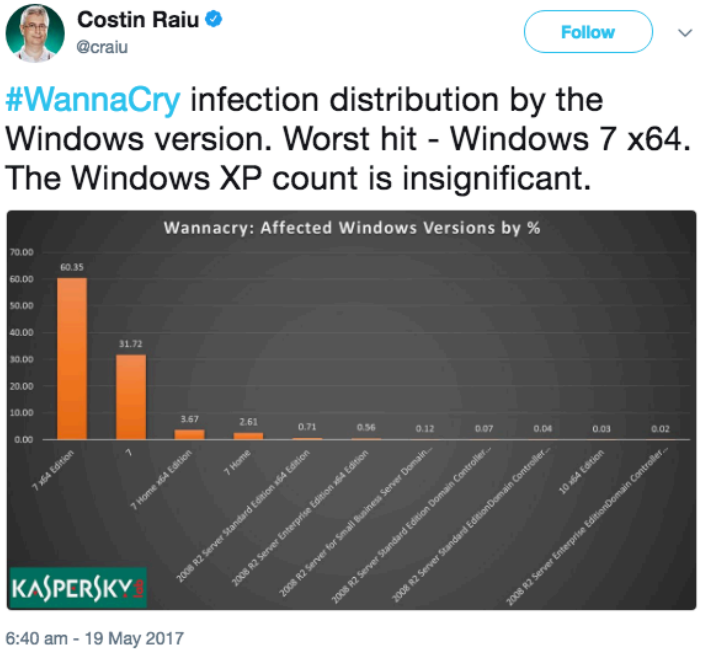
it's the boundary of your telemetry

g@comae.io

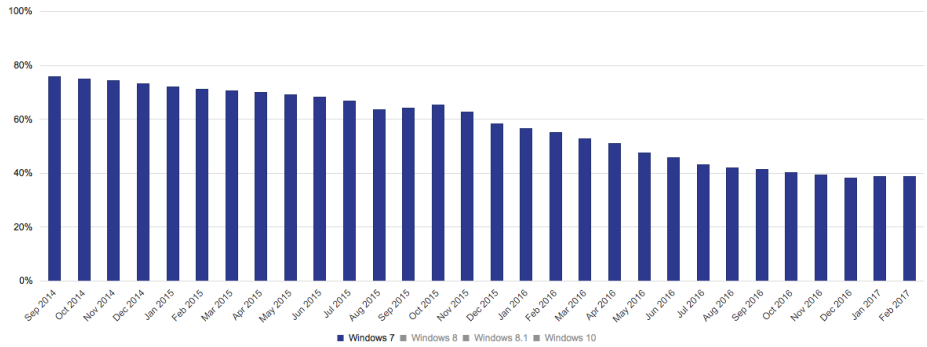
Citations



https://twitter.com/marasawr/status/941011516911996928



https://twitter.com/craiu/status/865562842149392384



https://developer.microsoft.com/en-us/store/windows-app-data-trends