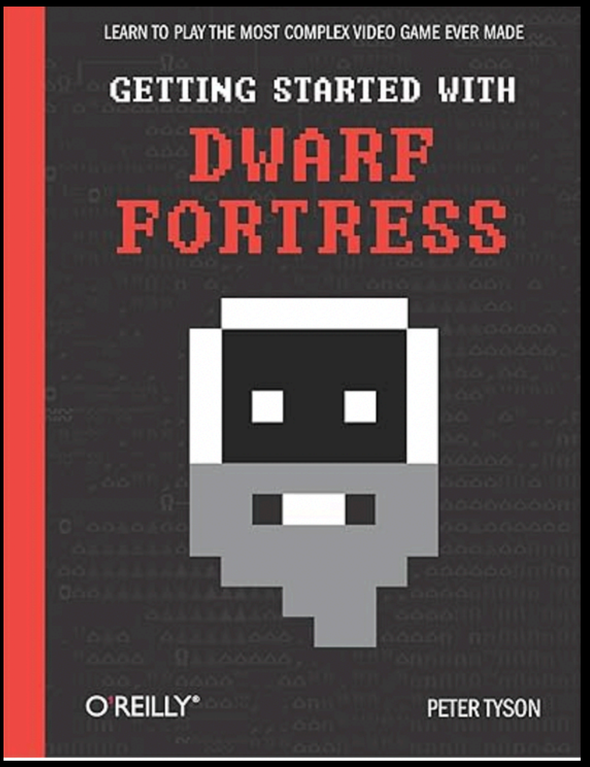
Expect the unexpected!

Or always be ready!
Or whatever, sometimes we can’t predict stuff.

Alex Breger



r/dwarffortress - Just started playing, is it normal for cats to adopt dwarves?

reddit.com

Dwarf Fortress

- Most unexpected chain reaction you know?
- Dwarf Fortress has a complicated intertwined system.
- It has cats.
- It has dwarves.
- What dwarves like to drink the most?

Let’s look at some other drunk cats

- AWS S3 2017 incident.
- Stuxnet in the wild.
- NotPetya going abroad.

Goal

The “problem” with:

- Anticipation and assumptions of how something will/should work.
- Intertwined systems.
- Reliance on 3rd party services, wether we know it or not.

AWS S3 outage

- February 2017.
- Routine maintenance.
- S3 - Simple Storage Service - in US-EAST-1.
- Fix billing process lag.
- Hours of S3 down time.

Cause

https://aws.amazon.com/message/41926/

- At 9:37AM PST, an authorized S3 team member using an established playbook executed a command which was intended to remove a small number of servers for one of the S3 subsystems that is used by the S3 billing process. Unfortunately, one of the inputs to the command was entered incorrectly and a larger set of servers was removed than intended. The servers that were inadvertently removed supported two other S3 subsystems.
- Index subsystem - manages metadata and S3 objects in the region. Serves requests to S3.
- Placement subsystem - manages allocation of new storage and requires the index subsystem to work.
- Removing a significant portion of the capacity caused each of these systems to require a full restart.

Assumptions

- We build our systems with the assumption that things will occasionally fail.
- While this is an operation that we have relied on to maintain our systems since the launch of S3, we have not completely restarted the index subsystem or the placement subsystem in our larger regions for many years. S3 has experienced massive growth over the last several years and the process of restarting these services and running the necessary safety checks to validate the integrity of the metadata took longer than expected.

← **Post** Reply

Amazon Web Services ✓
@awscloud

The dashboard not changing color is related to S3 issue. See the banner at the top of the dashboard for updates.

9:17 PM · Feb 28, 2017

Steve Buck @stevebuckfl · Feb 28, 2017
Have you tried blowing on the back of the cartridge?

1

@karptonite@mstdn.social @karptonite · Feb 28, 2017
.@awscloud Making your status page dependent on the service whose status the page is reporting--not the best idea in retrospect, I bet.

4 98 286

Marin Bek @marinbek · Feb 28, 2017
maybe you should host your status dashboard on some reliable provider?

1

Jake Wilson @Jakobud · Feb 28, 2017
So the reliability of your status dashboard is dependent on the very systems it is monitoring??? I think that needs some rethought

4 27

Matt Russell ✓ @mattdrussell · Feb 28, 2017
maybe you should host it with Azure?

3 9

Effect

- Adobe’s services, Amazon’s Twitch, Atlassian’s Bitbucket and HipChat, Autodesk Live and Cloud Rendering, Buffer, Business Insider, Carto, Chef, Citrix, Clarifai, Codecademy, Coindesk, Convo, Coursera, Cracked, Docker, Docker's Registry Hub, Elastic, Expedia, Expensify, FanDuel, FiftyThree, Flipboard, Flippa, Giphy, GitHub, GitLab, Google-owned Fabric, Greenhouse, Heroku, Home Chef, iFixit, IFTTT, Imgur, Ionic, isitdownrightnow.com, Jamf, JSTOR, Kickstarter, Lonely Planet, Mailchimp, Mapbox, Medium, Microsoft’s HockeyApp, the MIT Technology Review, MuckRock, New Relic, News Corp, OrderAhead, PagerDuty, Pantheon, Quora, Razer, Signal, Slack, Sprout Social, Square, StatusPage (which Atlassian recently acquired), Talkdesk, Travis CI, Trello, Twilio, Unbounce, the U.S. Securities and Exchange Commission (SEC), The Verge, Vermont Public Radio, VSCO, Wix, Xero, Yahoo! Mail, Zendesk, and numerous publications that stored images and other media in S3.

Mitigation

- Can you think of mitigations? How this could be prevented?

Possible mitigations

- It may be worth questioning whether the operator should be able to enter a command that took out more capacity than should have been allowed.
- Simulate the problem occasionally. Especially with growing systems.
- Redundancy, multi-region failover.

Stuxnet

https://spectrum.ieee.org/the-real-story-of-stuxnet, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

- 500 kb worm (Ben, what is the difference between virus and worm? Note to self, if he answers correctly, say that it is incorrect. Remember to delete note in production.)
- Used 4 interconnected zero-days.
- Infected 14 industrial sites in Iran.
- First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself.
- Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges.
- Finally, it compromised the programmable logic controllers.

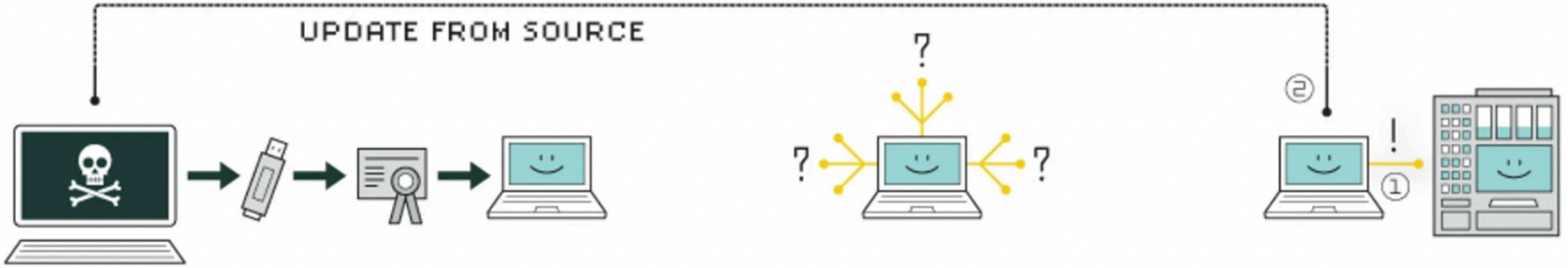
Cause

- The worm is deployed via USB.
- It used a stolen digital signature to install the rootkit.
- It stays in the network for quite a while. When (probably) the needed effect was not achieved, the worm was updated to become more “powerful” and less stealthy.
  (Stuxnet had self-update capabilities by using P2P communications and online connection.)
- For some reason, either because of the code modification, or bad security practice on part of the Iranians, the worm gets out.

Assumptions

- Stuxnet is in an air-gaped system/network (no outside internet access) and should stay there.
- Had a control system, a counter that limited the spread to just three PCs, which was supposed to limit its spread.
- 21-day propagation window; in other words, the worm would migrate to other machines in a network only for three weeks before calling it quits.

HOW STUXNET WORKED



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Effect

- Spreads in Iran and makes PCs to malfunction (BSoD, Reboots), even on freshly installed OSs.
- Spread to thousands of PCs outside Iran, in countries as far flung as China and Germany, Kazakhstan and Indonesia. But didn’t harm them as it couldn’t be armed without the exact system it was designed for.
- From the attackers point: everything gets patched, so now we need new zero-days and new malware.

Mitigation

- Can you think of mitigations? How this could be prevented?

Possible Mitigations

- Maintain strict removable media policies to prevent dodgy USBs being connected to your devices.
- Closely monitor your network for unusual activity.

NotPetya

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

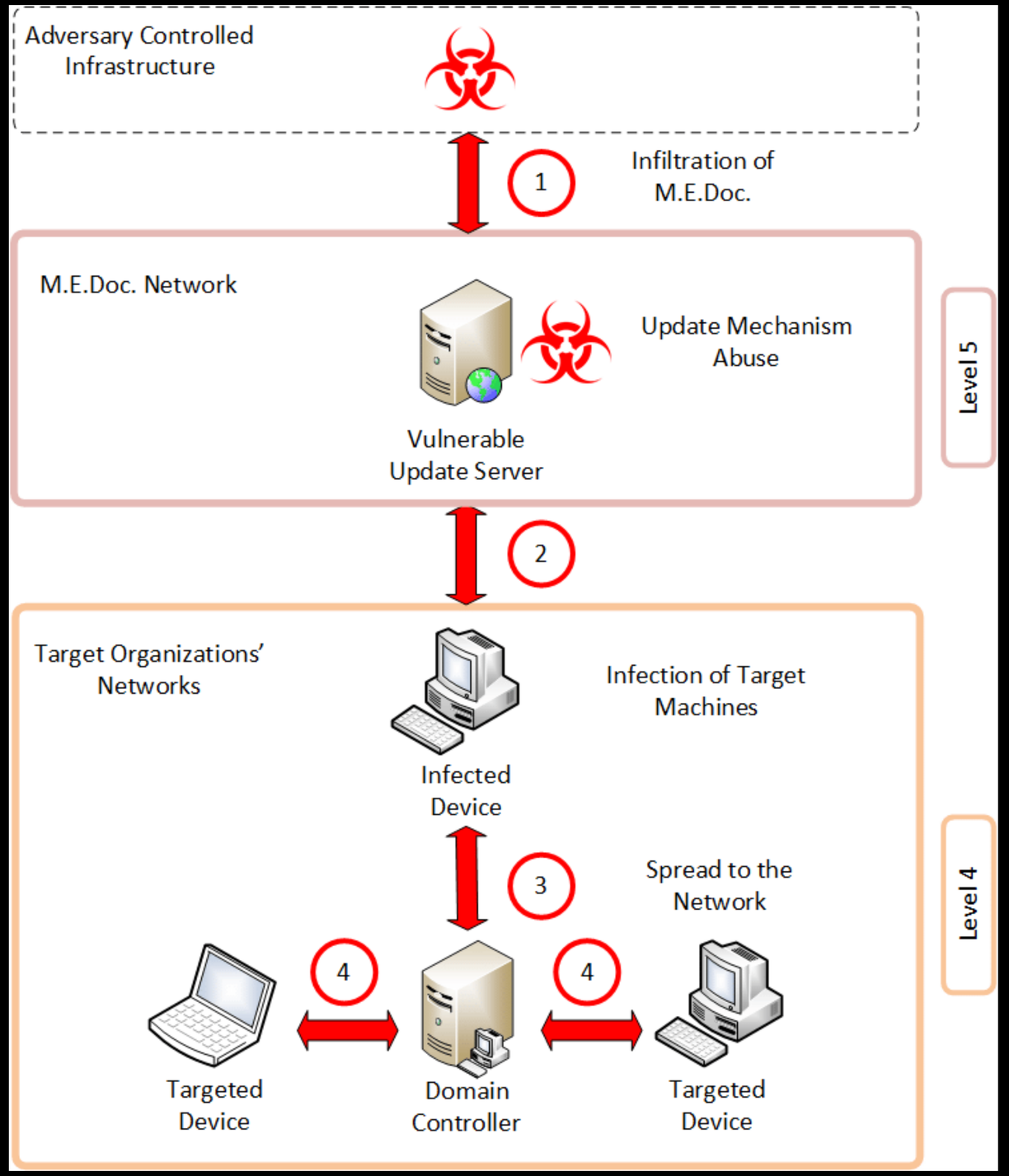
- 10 billion $ in damages globally.
- Targeted Ukraine.
- M.E.Doc, which is more or less Ukraine’s equivalent of TurboTax or Quicken. It’s used by nearly anyone who files taxes or does business in the country.
- Two exploits working in tandem: One was a penetration tool known as EternalBlue (created by the US National Security Agency and leaked a month prior) and Mimikatz (POC of Benjamin Delpy, created in 2011).
- “oops, your important files are encrypted” and demanded a payment of $300 worth of bitcoin to decrypt them. Which was futile because it was purely destructive. It irreversibly encrypted computers’ master boot records, the deep-seated part of a machine that tells it where to find its own operating system

Cause

- Linkos Group, Ukrainian software business, who's job is to push out routine updates—bug fixes, security patches, new features—to a piece of accounting software called M.E.Doc.
- Russian military hackers hijacked the company's update servers to allow them a hidden back door into the thousands of PCs around the country. The saboteurs used that back door to release the piece of malware.
- The code that the hackers pushed out was honed to spread automatically, rapidly, and indiscriminately.
- Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, through the circulatory system of the global economy.

Assumptions

- Attacking a server for a software that was used only in Ukraine.
- It will affect only the companies that use the software.
- Or were they mere assumptions?


Adversary Controlled Infrastructure
1
Infiltration of M.E.Doc.
M.E.Doc. Network
Update Mechanism Abuse
Vulnerable Update Server
Level 5
2
Target Organizations' Networks
Infection of Target Machines
Infected Device
3
Spread to the Network
4
4
Targeted Device
Domain Controller
Targeted Device
Level 4

Effect

- Mondelez International (Oreo, Triscuits, etc) filed insurance claim for damages, but was answered that the insurer doesn’t cover damages caused by war.
- Maersk responsible for 76 ports on all sides of the earth and nearly 800 seafaring vessels, including container ships carrying tens of millions of tons of cargo, representing close to a fifth of the entire world’s shipping capacity, was dead in the water.
- It irreversibly encrypted computers’ master boot records, the deep-seated part of a machine that tells it where to find its own operating system.
- In each case of big companies, it inflicted nine-figure costs. It even spread back to Russia, striking the state oil company Rosneft.

Mitigations

- Can you think of mitigations? How this could be prevented?

Possible Mitigations

- Patch your systems.
- Use backups.
- Encapsulate your systems.