Ransomware & Wiper Attacks: An Evolving Threat

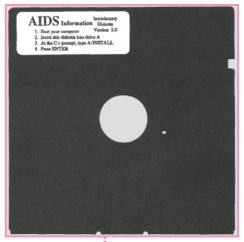
Aaron Ades, AVP Cybersecurity MetLife

MetLife


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

A Brief History of Ransomware

1989
- PC CYBORG Distributed via distributing 20,000 floppy disks to AIDS researchers
- Pay $189 to a PO Box in Panama



2004
- GPCode
- Demanded $120 via wire transfer

2006
- Cryzip began spreading via the Bagle Virus
- Demanded $300 via “e-gold”

2011
- Windows Product Activation
- Tricked user into dialing rogue long distance phone #

February 2016
- Petya
- Infected email attachments
- Later updated to include EternalBlue propagation

March 2016
- WannaCry
- Attributed to North Korea
- EternalBlue propagation
- Kill Switch discovered by Marcus Hutchins

June 2017
- NotPetya
- Targeted Ukraine
- Wiper in disguise
- EternalBlue + Mimikatz + PSExec +EternalRomance
- $10 billion global impact
- Attributed to Russian Military

Feb 2018
- Colorado DOT crippled by Ransomware
- 150 Servers and 2,000 workstations
- Segmented network prevented more damage

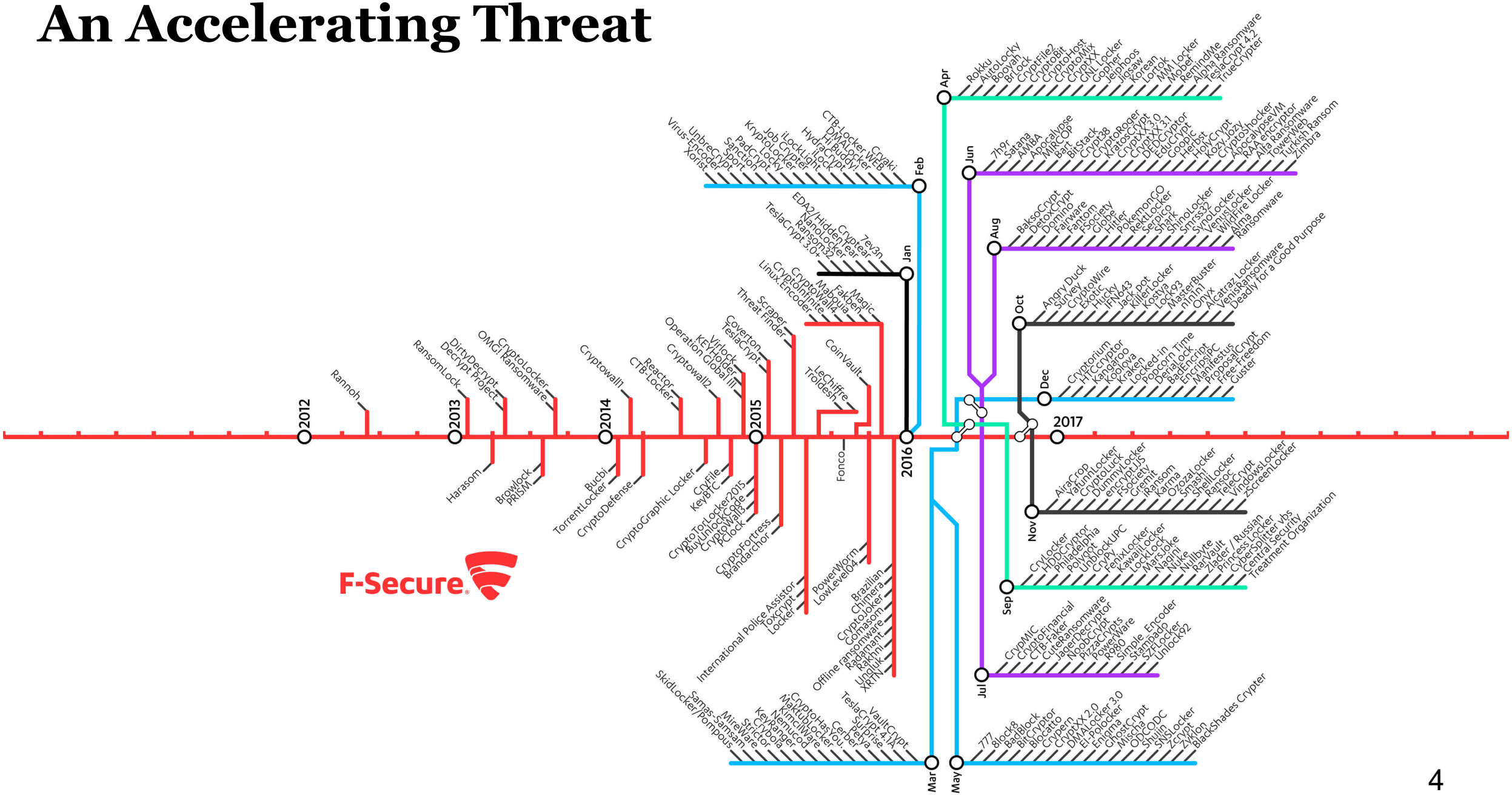
March 2018
- Atlanta crippled by Ransomware
- $17 million in damages
- SamSam
- FBI Indicted 2 Iranian Hackers

May 2019
- City of Baltimore
- $18 million in damages
- 4-6 weeks to get to 95% recovery

Who’s Next
?

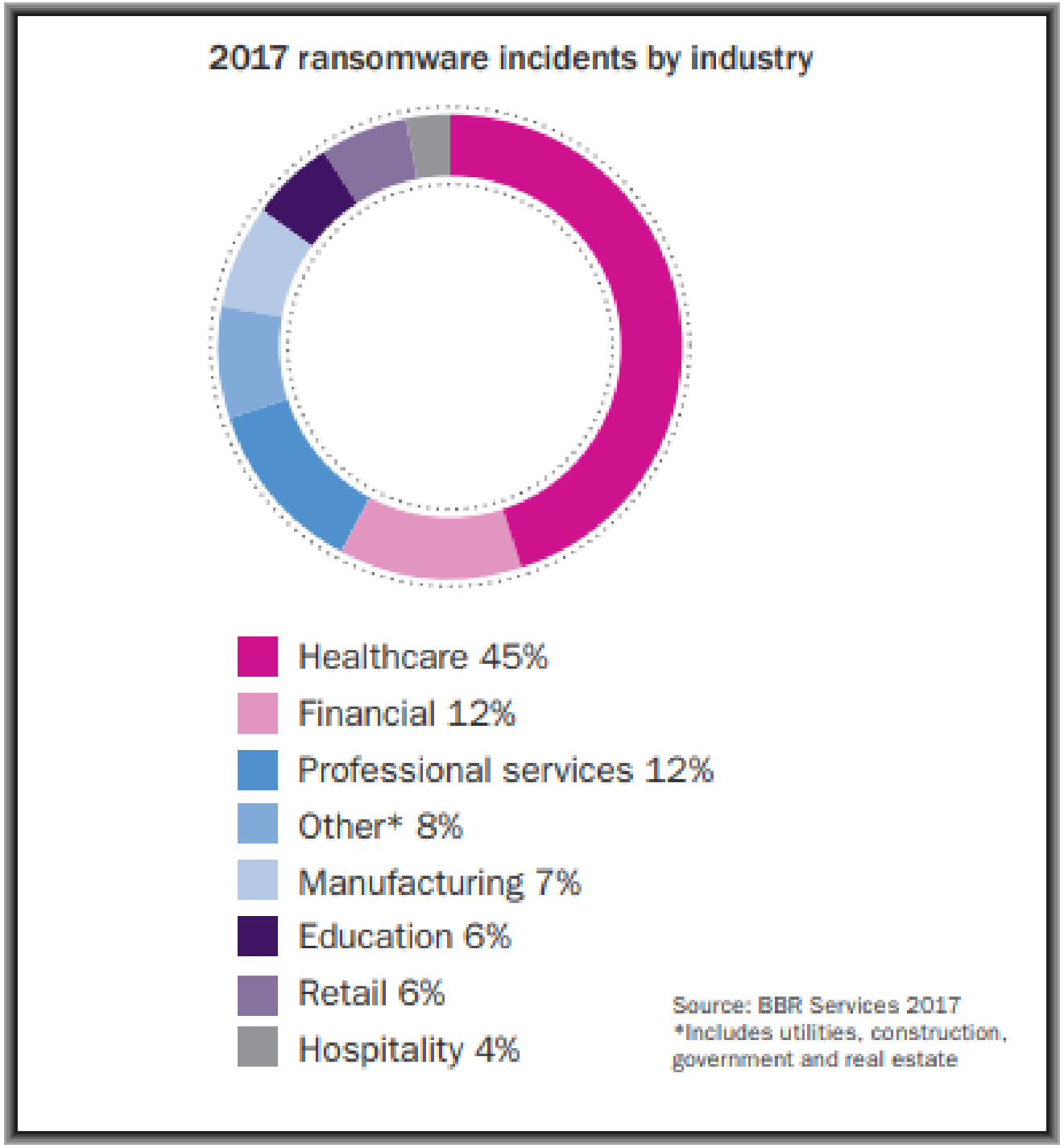
MetLife

An Accelerating Threat



Financial Impact

- Estimated 184 million ransomware infections in 2018
- Losses predicted at 11.5 billion in 2019
- Cyber Risk Management Project believes we may soon see a single attack with a cost of $193 billion
- Productivity costs often outweigh repair costs



MetLife

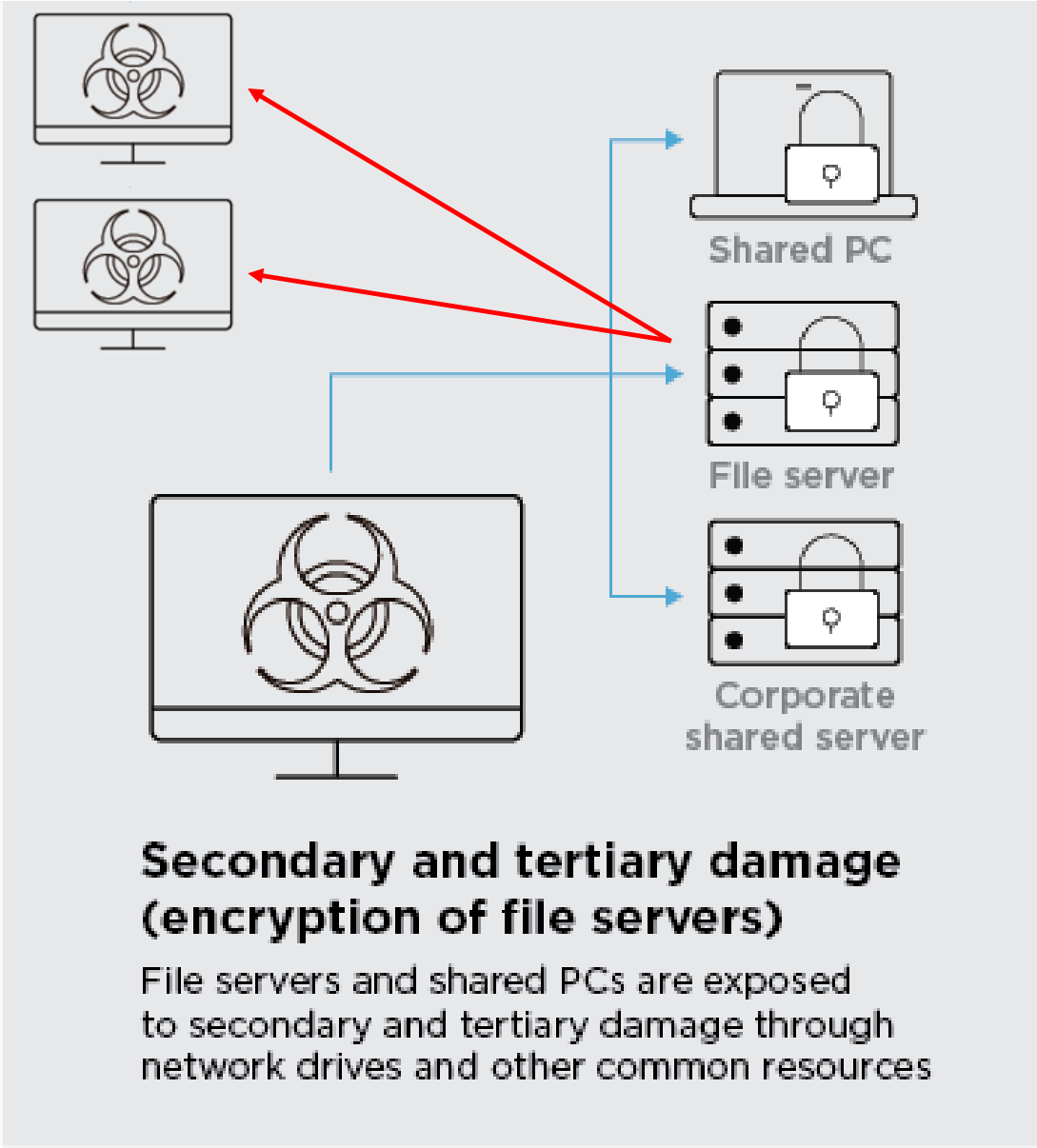
Common Attack Vectors

RDP Brute Force

- Simple and Direct
- Targets internet exposed assets
- High risk for public cloud environments
- 2 control failures:
  - Network access restrictions
  - Account lockout policy

Email-borne with Propagation via Fileservers

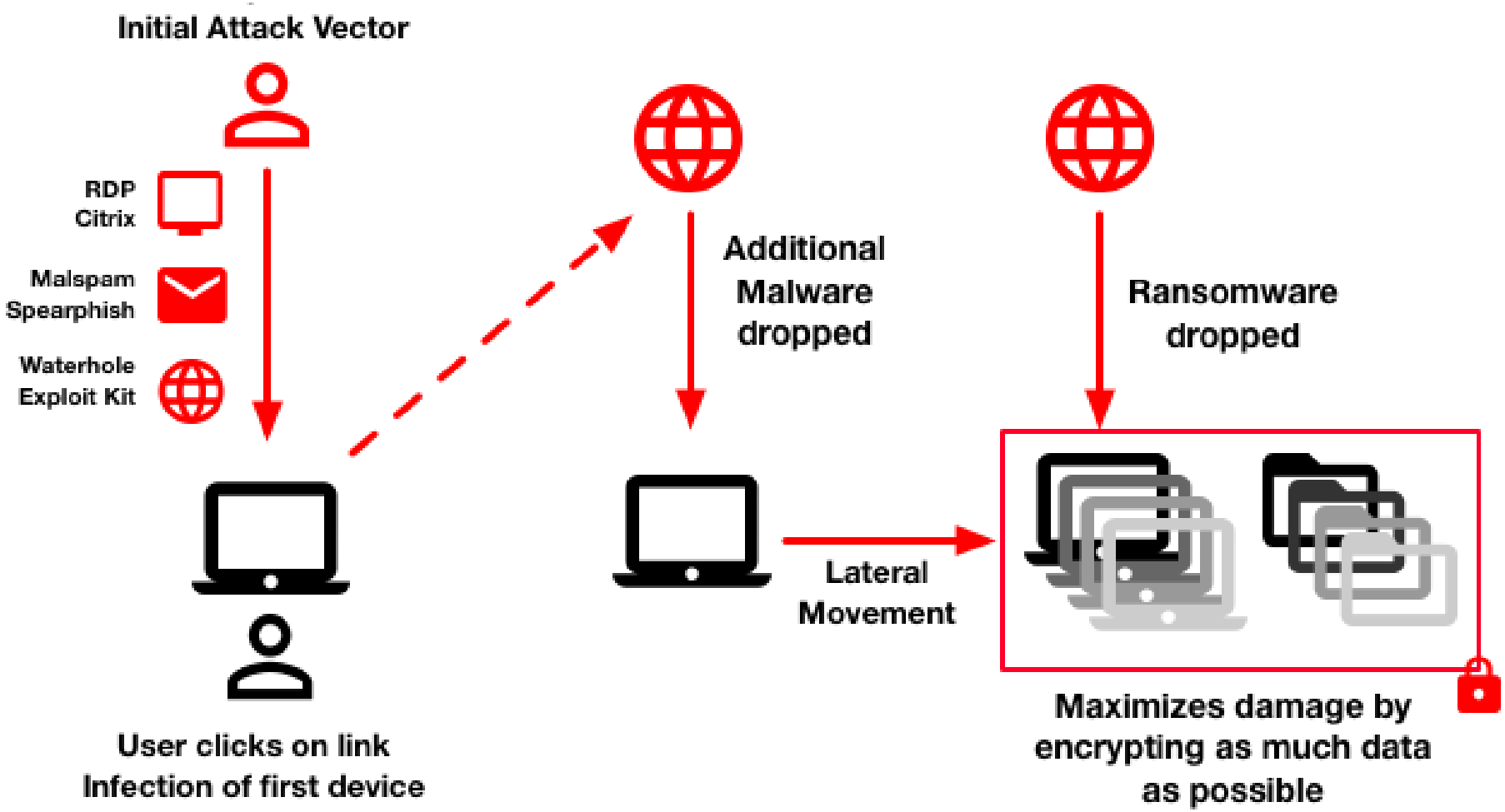
- Initial infection via malicious email or website
- Local data and file share are both encrypted and infected
- Other users impacted via file shares



MetLife

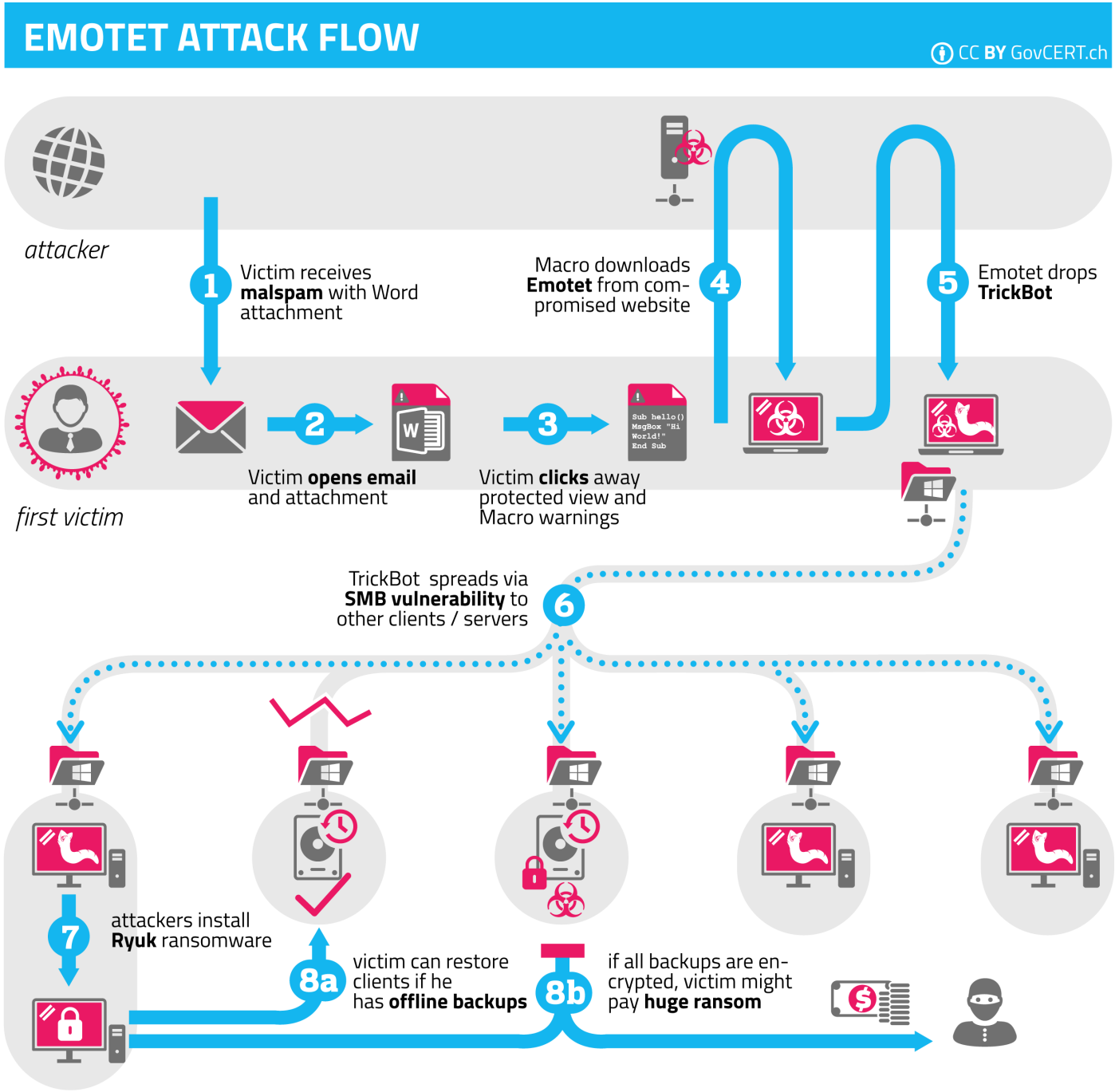
Land and Expand

Pivoting after initial entry



Layers on Layers

- Victim opens “malspam” email
- Word macro installs Emotet as a dropper
- Emotet drops TrickBot
- TrickBot spread internally via various modules
  - Eternal Blue (SMB)
  - Internal Email
- TrickBot installs Ryuk Ransomware

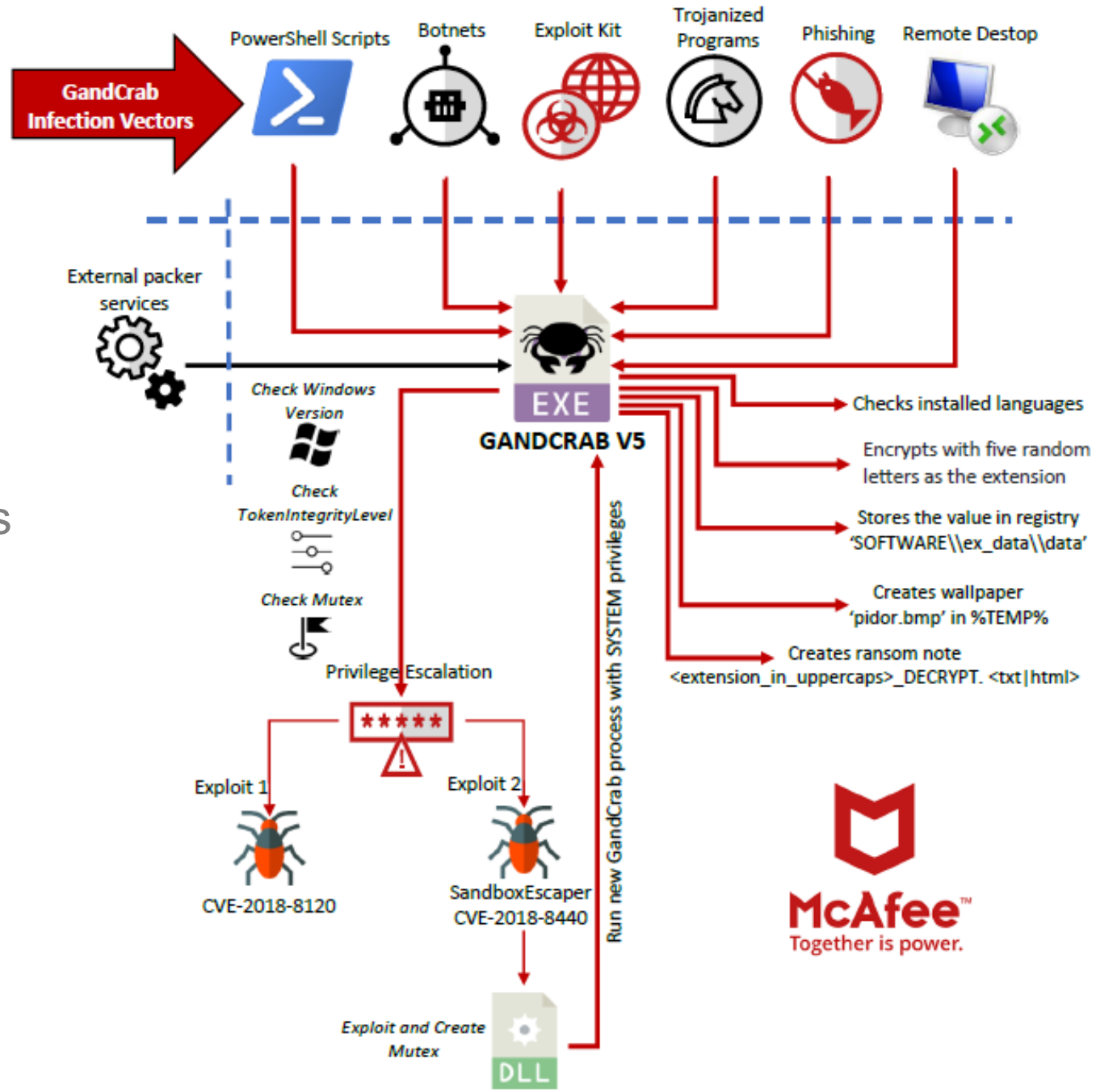


MetLife

GandCrab

"Ransomware-as-a-Service"

- Dark web/Criminal "affiliate enterprise"
- Affiliates help spread infections and share profits
- $2 billion in shared profits in 18 months
- $150 million netted by GandCrab crew
- Creators "retired" May 31st 2019
- Evidence is that they regrouped into a smaller, more advanced and exclusive group

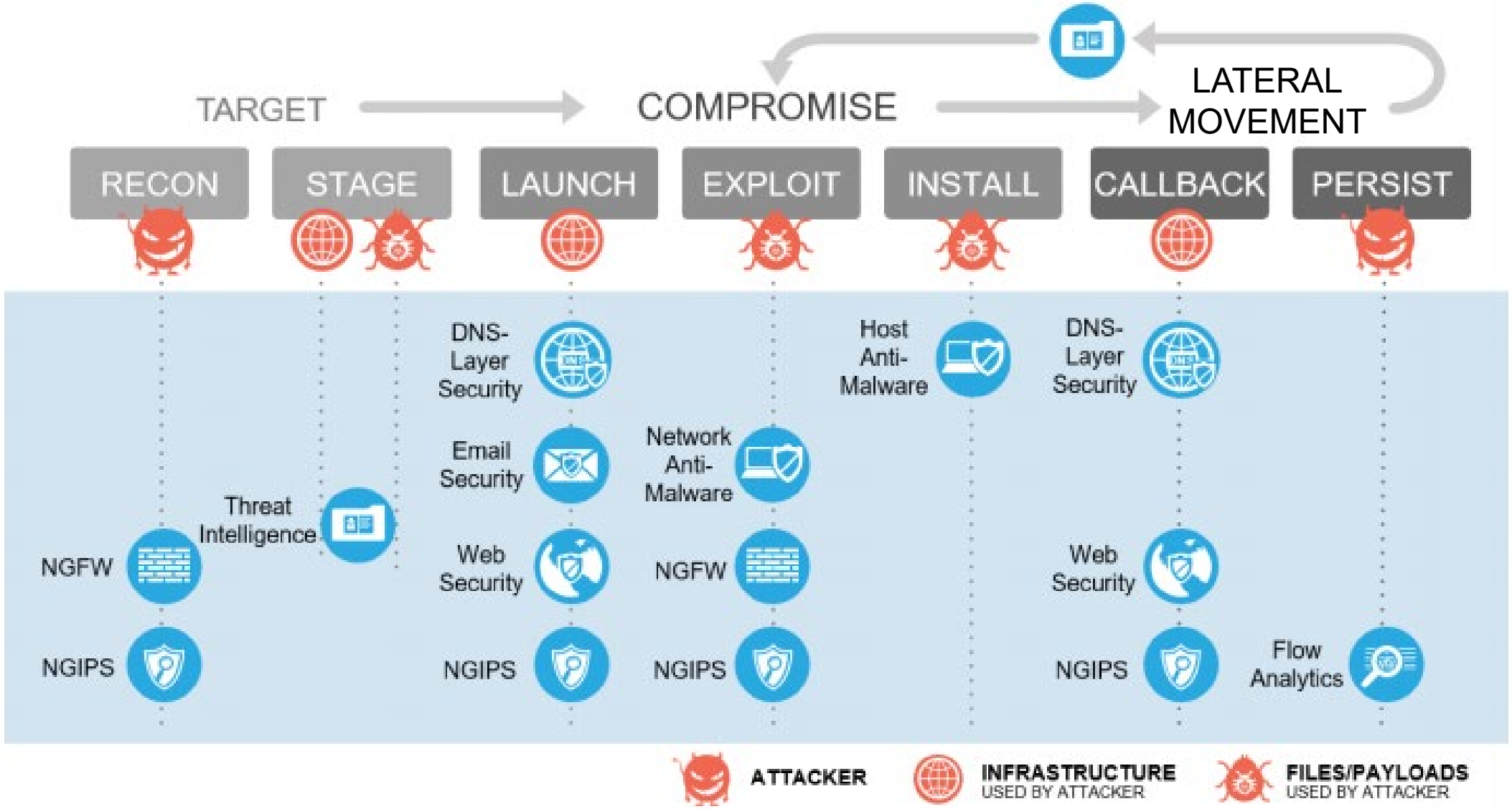


MetLife

Protecting Against Ransomware

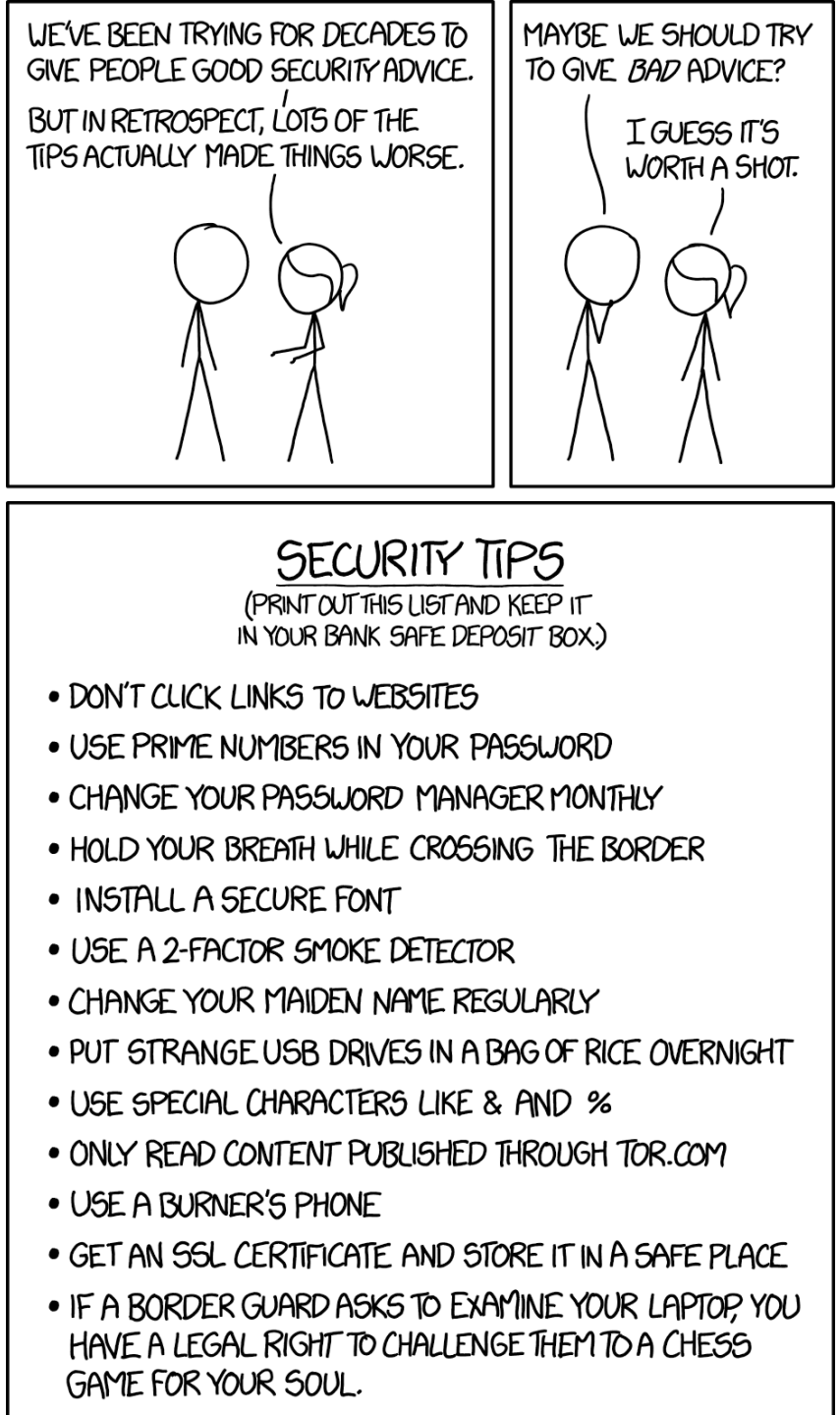
MetLife

Harden Endpoints and Networks



Harden The Humans

- Stay patched
- Always think twice before clicking on links or opening attachments
- Backup personal data on a regular basis to a protected location
- Remove infected endpoints ASAP
- If it's suspicious, report it!



MetLife

DRP, BCP and Data Protection

- Offline backups
- Laptop and workstation reimaging
- SAN/NAS Data Protection

Recovering From Ransomware Discussion

MetLife