



This is what we Thought would happen in 2021

Gert-Jan Bruggink



Defcon #29 - Blue Team Village 2021
5-8 August 2021
<https://blueteamvillage.org/>

Why am I here?



Source: <https://imgflip.com/i/4ub6s8>

Q1 2021 was like..

...Security Predictions Reports...

...2021 Threat Landscape...

...Cyber security in 2021...

...2021 Threat Report...

...Looking ahead: the 2021 threat landscape...

Who am I?



Gert-Jan Bruggink

Threat Researcher

10+ years in InfoSec.

5+ specialized in cyber threat intelligence (CTI) based risk management.
Consulted at financial services, high tech, manufacturing and governmental.

- Built / led CTI capabilities & delivery of CTI products;
 - Intelligence-led Red- & Purple Teaming;
 - Strategic change through CTI, SOC & Cyber transformation programs;
- Father x 2, Entrepreneurship, Gaming, Painting, Lego, Meme's.

Doesn't like magic tricks.



[@gertjanbruggink](https://twitter.com/gertjanbruggink)



github.com/gertjanbruggink



[/gertjanbruggink](https://www.linkedin.com/company/gertjanbruggink)

What am I going to talk about?

✓ People create all sorts of thoughts and predictions for the upcoming year, **is it any good?**

✓ How are these products created and how do they **influence our thinking about risk?**

✓ There are no surprises in terms of themes and topics, **just in how did publishers emphasize them.**

Objective 1: Change the norm for publishers creating threat predictions

Objective 2: Provide in-house teams guidance how to manage this

Before we dive into the details..



We generally

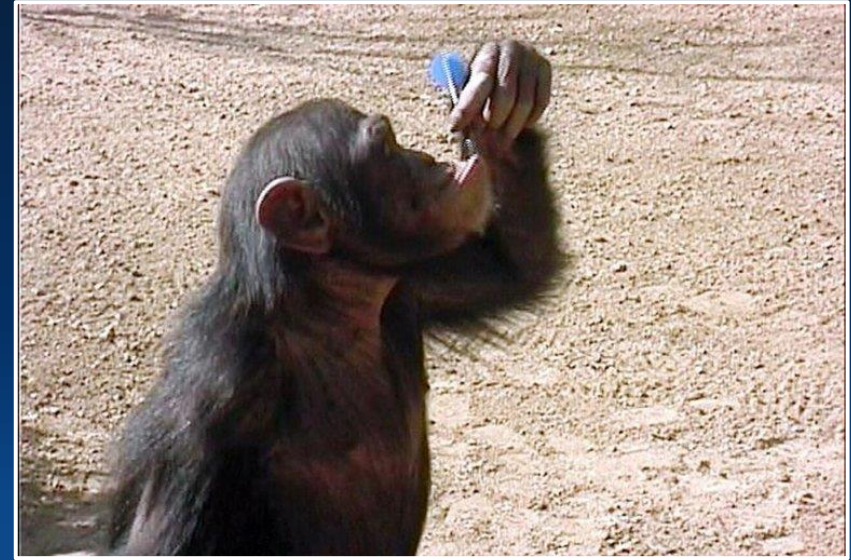
- Are shown the things in front of us
- Have priority for the things in front of us
- Only have budget to solve the biggest risk(s) in front of us
- Have limited understanding of evolving areas of risk around us

Source:
<https://www.freeiconspng.com/img/39531>

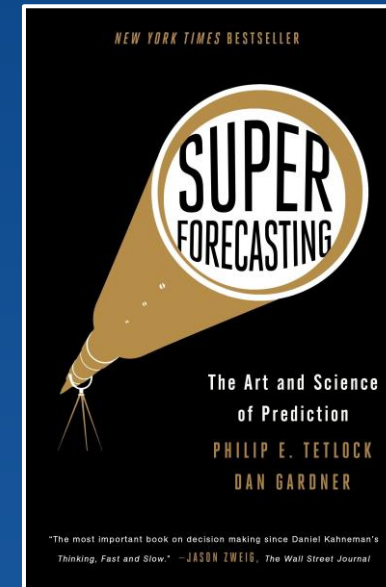
What is forecasting?

- What do people think it is?
- Prediction vs forecasting
- Using forecasting to increase buy-in from your organization
- Forecasting vs super forecasting

#infosecdartthrowingchimp



Dart throwing chimp image: <https://www.reuters.com/>



Excellent TLDR:
<https://www.richardhughesjones.com/superforecasting-summary/>

<https://www.amazon.com/Superforecasting-Science-Prediction-Philip-Tetlock/dp/0804136718>

Most used forecasting analysis techniques

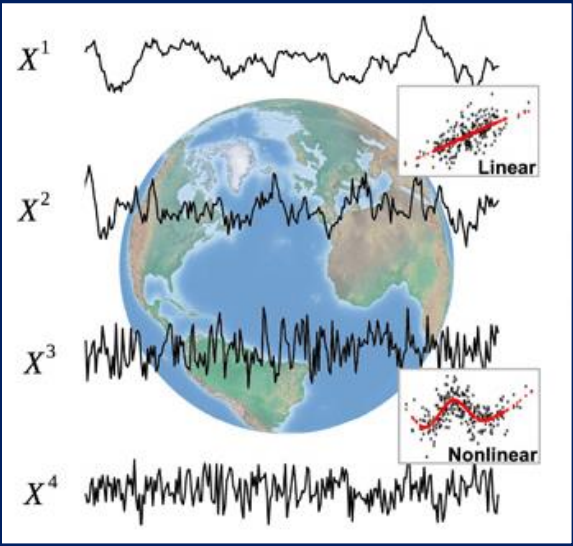
Qualitative



Source:
<https://i.pinimg.com/originals/f8/32/91/f83291a8b909b46c9dac70324ed3c3c8.jpg>

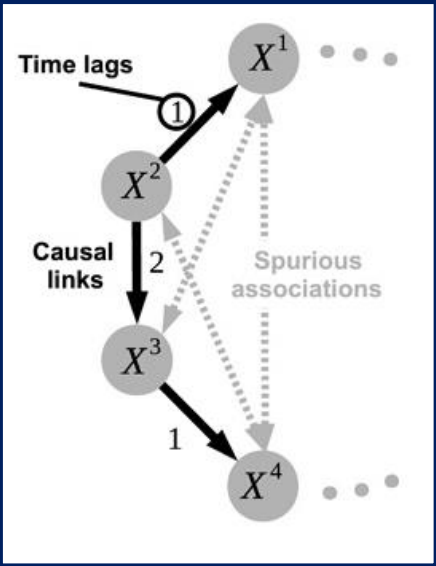
Quantitative

Time series analysis and projection



Source:
<https://advances.sciencemag.org/content/advances/5/11/ea4996/F1.large.jpg>

Causal models



Source:
<https://advances.sciencemag.org/content/advances/5/11/ea4996/F1.large.jpg>

★ Focus of the research

The experiment



Objectives

Timespan

Activities

Constraints

Limitations

TLDR:

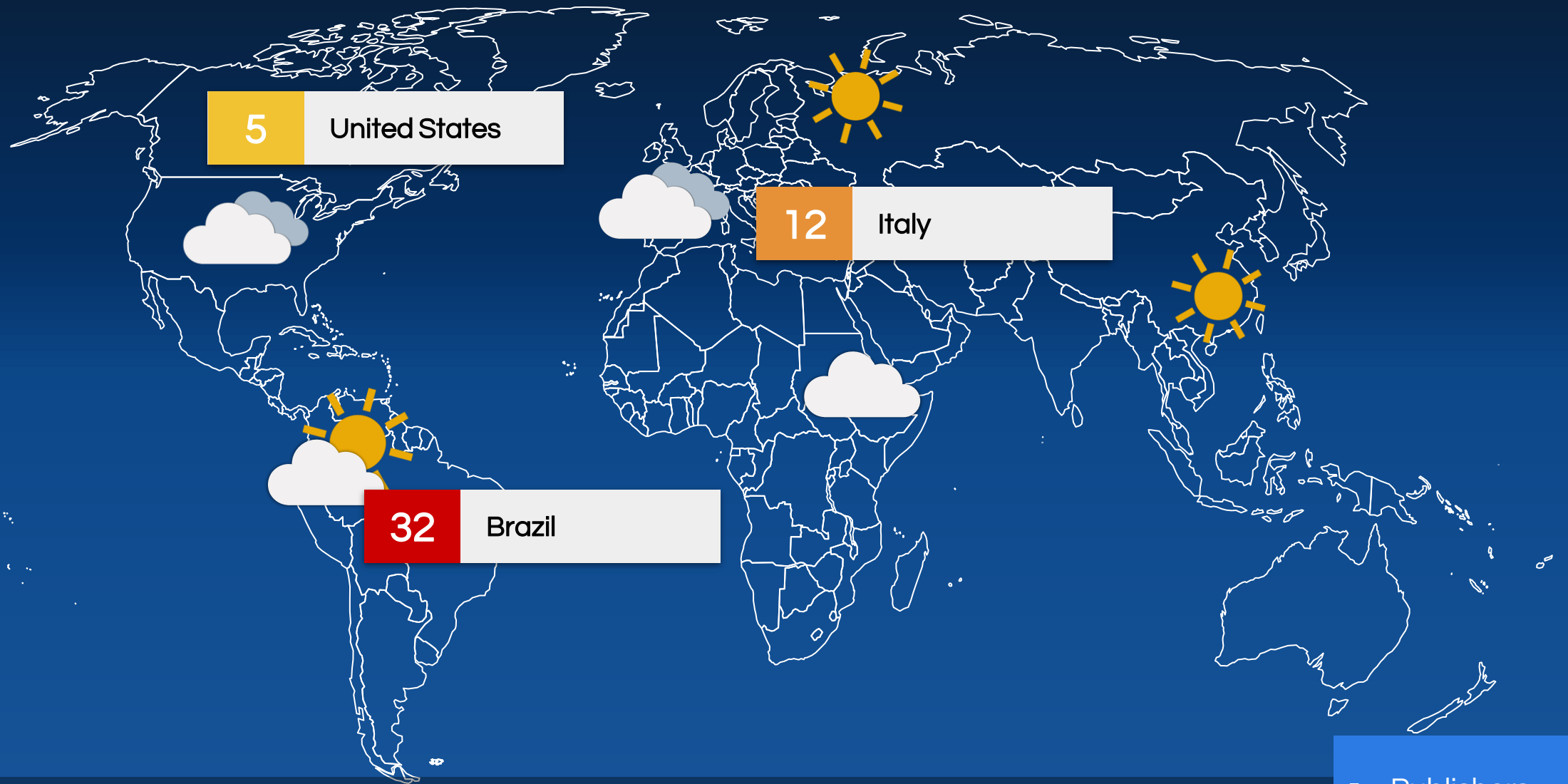
Had time.

Did research.

Present content.

Help people up their game.

Report & article tracking available via Github:
github.com/gertjanbruggink/ThreatReports



Examining content

- Publishers
- Documents
- Themes
- Topics

Comparing publication details



44*

unique 2021
threat
landscapes
reviewed



Overall highest #: Q1 2021 (22)
Highest # publications: January & April (8)

Reports:	27
Online articles:	13

Total # pages: 1100+



pages: 2 (min) to 122 (max)

Average # H1 report pages: ~27,5

- ~10% incorporated MITRE ATT&CK references (Red Canary, Mandiant, VMware, NTT)
- ~20% included explicit forecasting (CERT-EU, CrowdStrike, ISF, law enforcement, public services)
- ~45% applied proprietary telemetry, the remainder applied expert analysis
- ~49% used explicit product marketing in their reporting

*4 reports and articles were released before 2021.
Excluded from future graphs & stats to keep everything consistent.

Comparing documents

Average structure

Frontpage

Disclaimers

Quality & Risk
Management
Legal
Company information


Table of contents

Executive summary

Key assessment(s) 
Executive / Management chapter
Results & analysis

Introduction

Introduction
Overall view
Recap

'My product is super-duper-awesome'
Foreword
Timelines 

Themes

Overall categories
Geographical insights

Topics




Trends 
Threat groups
Specific expertise topics


Case studies
Individual stats
Deep dives

Document wrap-up

Conclusion
Recommendations
Scenarios 

Appendices

Methodology 
Predictions 
Data 
Acknowledgements
References
Sources
Contributing organizations

Abbreviations
About: the author, services, stats
More disclaimers
Planning
Recap of previous assessments 

Lessons learned





- We get that it's marketing.
- Be creative. Just make sure to timestamp.
- Explore machine readability.
- Looking forward
(vs looking back & forecasting language).

Pro tip






When detailing your landscape, take your previous reports (and themes discussed) into account. Street cred to those benchmarking their own assessments and content.

Exploring themes

Dominant themes

- Work from home, remote working, remote work tooling & services. Also tying into COVID-19. 
- Pre-compromise behavior & initial access vectors. 
- Post-compromise behavior is generally malware (more specifically ransomware). 
- The evolution of the cyber-crime-as-a-service (CaaS) economy. 

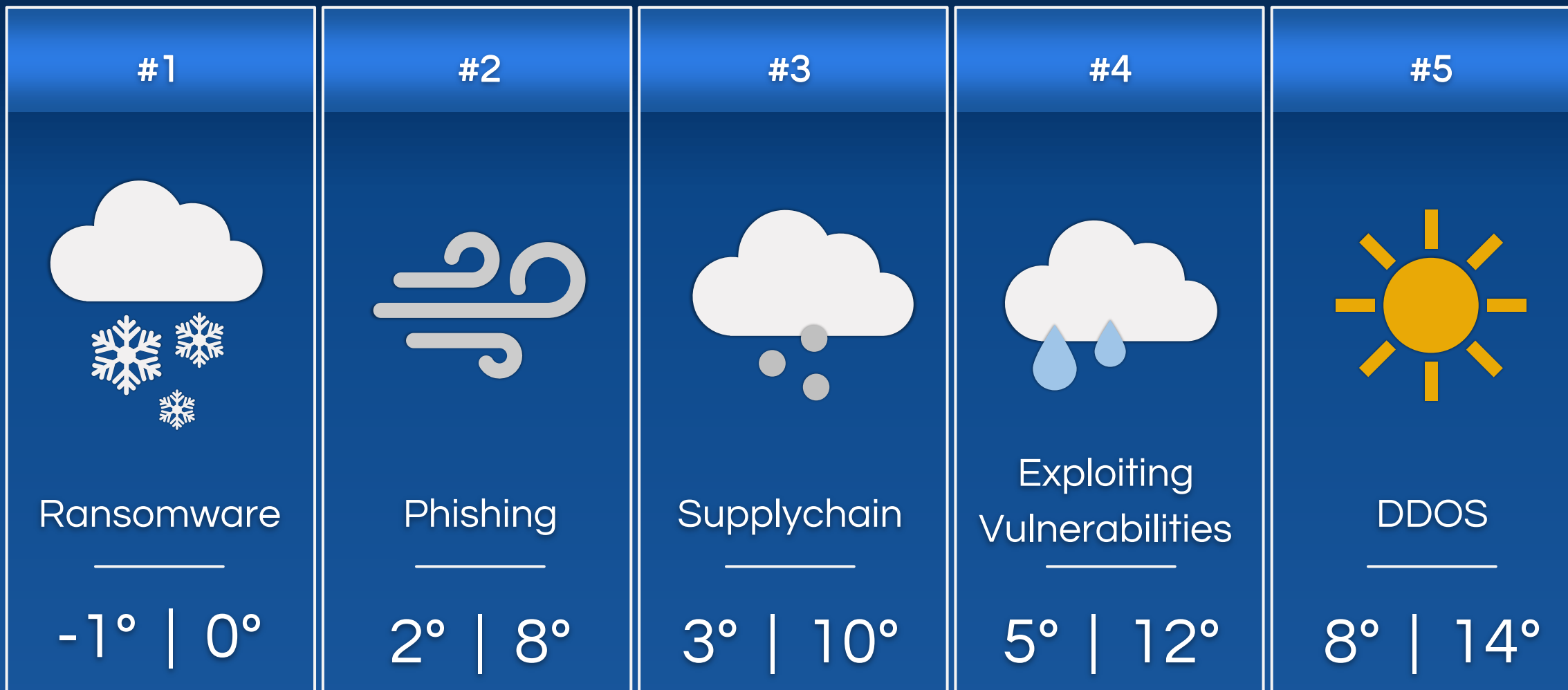
Outlier themes

- IOT, or specifically the targeting of it 
- Where did the hardware/processor themes go? 
- MacOS security 
- The criminal opportunity of 5G 
- AI 

Pro tip

Tracking 'outlier' themes is as important as dominant ones. Your threat management strategy should assess specific risk for both.

5 most referenced topics 📍





Ransomware



MONDAY
(Q1/Q2)

Reporting

- #1 referenced topic in all reporting
- Around since early 90's, bitcoin made it lucrative
- Key driver in the crime-as-a-service economy



WEDNESDAY
(Present)



- Major ransomware incidents across the board
- Ransomware became a topic of geopolitics (finally)
- Collective efforts cracking down anything ransomware



SATURDAY
(Q3/Q4+)

Cyber Weatherman

- Q3 takedown effects; slight drop in Q3, 'storm' in Q4+
- **Victim pressuring** techniques evolves
- **Malware defense evasion** is key, improvements expected in Q4, 'multi-morphic' 🤖

Pro tips 📖

Revisit and **test** your current backup strategy

Perform a Ransomware Readiness Assessment ⁽¹⁾

Add CIS keyboard layouts to your client fleet ⁽²⁾



Phishing (including Business Email Compromise - BEC)



MONDAY
(Q1/Q2)



WEDNESDAY
(Present)



SATURDAY
(Q3/Q4+)

Reporting

Cyber Weatherman

- #2 referenced topic in all reporting
- Most cost-effective initial access vector
- Representing the industries two biggest problems (together with ransomware)

- COVID-19 & cryptocurrency phishing themes
- 'Cat-and-mouse' vendor games
- Microsoft Windows drives trends in attachments (e.g. Macro enabled docs or ZIP files)

- Consistently high volumes expected for H2
- Cross-over scams with other mediums (e.g. WhatsApp)
- BEC tactics becomes more complex thanks to better knowledge

Pro tips 🧠

Enable your users to report suspicious emails. Share reported incidents daily and prioritize threat management, detection and response activities



Supply chain compromise



MONDAY
(Q1/Q2)

Reporting

- Technique as old as Rome, major incidents going public each year
- Big-bang-for-the-buck targets (e.g. service providers)
- SaaS account takeover



WEDNESDAY
(Present)



- Major supply chain incidents hitting service providers
- Exploitation usually is not 'that complex'
- Cloud services have been prime targets



SATURDAY
(Q3/Q4+)

Cyber Weatherman

- We haven't seen the last, big, supply chain incident of 2021
- Geopolitical theater time
- Non-technical 'access' techniques evolve (e.g. malicious insider, bribing)

Pro tips 📖

Yes, I understand your supply chain is big - but do you know how big?

#swallowthecrappysalespitch



Exploiting vulnerabilities



MONDAY
(Q1/Q2)

Reporting

- Hard- and software will always have vulnerabilities, make sure you manage it
- Zero days will continue to be found
- Remote access solutions should be concerned (e.g. VPN, communication)



WEDNESDAY
(Present)



- Windows vulnerabilities dominate the mainstream media.
- Legacy Windows provides
- Microsoft Windows drives trends in attachments (e.g. Macro enabled docs or ZIP files)



SATURDAY
(Q3/Q4+)

Cyber Weatherman

- No changes expected, 'it's gon rain'
- It's not just Windows. Don't forget Linux or other (custom) OS's
- New Chinese regulation for vulnerability disclosure procedures

Pro tips ¹⁰⁰

Your Windows ops team must have been busy the last few week. Regularly buying them a beer or lunch, gives you human points and an excellent insight into what's threatening the 'domain'.



Distributed Denial of Service (DDoS)



MONDAY
(Q1/Q2)

Reporting

- So.. DDoS.. Is this still a thing?
- Extortion evolution includes DDoS
- Regularly through IOT based botnets



WEDNESDAY
(Present)



- Yes, still a valid technique
- Pandemic lifeline industry remains a target
- DDoS extortion remains very unrefined



SATURDAY
(Q3/Q4+)

Cyber Weatherman

- 2021 will exceed 2020' 10 million (!) DDoS attacks
- DDoS usage will become more refined
- Innovation allows for, increased size, hyper scale and sophisticated targeting

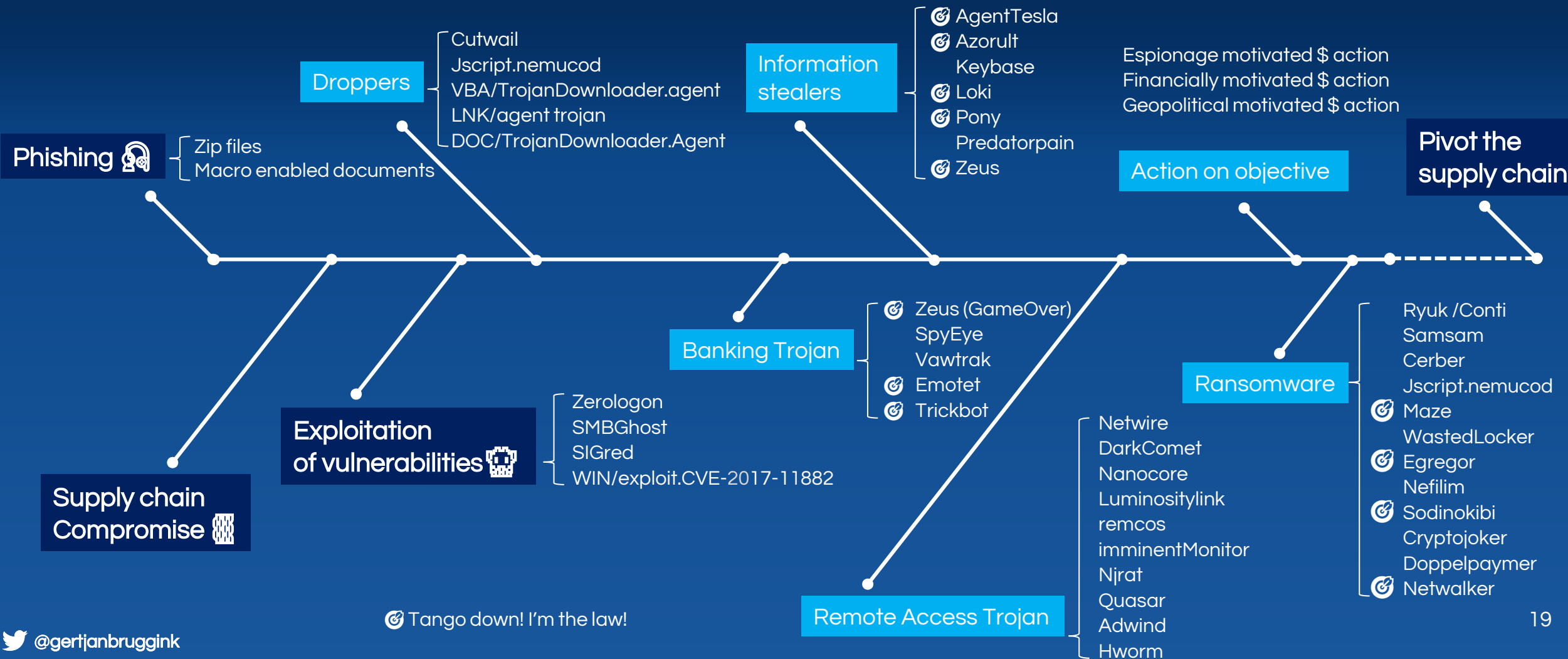
Pro tips

Evaluate the priority of DDoS in your security program, especially for area's (or systems) that are vulnerable to external 'influence'

This is what happened according to everyone

- Mapped different top X's from everyone's reports in one view
- Matched against a chronological flow of how everyone saw incidents

Bonus: Never forget Cobalt Strike



Tango down! I'm the law!

Themes to monitor



Suggestions the overall risk 'is becoming greater'

(especially ransomware & phishing)



Evolution of the crimeware business



Role of 'Western' bias in your threat landscape



MacOS based threats



Microsoft Windows 'high ground'

Pro tip

Tracking 'outlier' themes is as important as dominant ones. Your threat management strategy should assess specific risk for both.

Topics to monitor



Focus on the
old stuff
(especially
Windows)



Extortion
scheme
evolution



DNS
focused
attacks



Evolution of
browser
injection
attacks



Modern
wardriving

Pro tip

Tracking 'outlier' themes is as important as dominant ones.
Your threat management strategy should assess specific risk
for both.

Next steps on our side

This exercise continues EOF 2021

In between:

- Refine experiment's hypotheses and questions.
- Explore analysis to automatic parsing of reports and articles, for example based on n-grams defined on existing keyword set.

It would be awesome if we:

- Build a machine-readable format for threat landscape reporting, based on JSON (e.g. STIX/TAXII enabled) and proper tagging for artifacts.
- Move lessons into scenarios, so people can validate threat/risk within their own environment.

Final thoughts

The average of what everyone thought would happen in 2021 is so far **on point** (hypothesis = ✓)

If you're an in-house team

- ✓ Basic security hygiene vs pre-compromise behavior (e.g. phishing, BEC, exploiting vulnerabilities)
- ✓ Prepare for post-compromise behavior (e.g. malware , ransomware in particular, supply chain compromises)
- ✓ Forecasting vs nowcasting (aka dashboarding)

If you're a vendor

- ✓ Be more creative in messaging
- ✓ Don't be afraid to innovate and fail
- ✓ Make actual forecasts instead of the easy 'topic X will go up'

Looking forward to your upcoming threat landscapes (or predictions, or forecasts..)! 🤖

#infosecdartthrowingchimp



Dart throwing chimp image:
<https://www.reuters.com/>

Let's continue the discussion!

Want to build a weather forecast? #cyberweatherman
Got questions? Want to hang out? Just no magic shows. 😊

Gert-Jan Bruggink

 @gertjanbruggink
 /gertjanbruggink

Threat reports repo:
 github.com/gertjanbruggink/ThreatReports



Happy little clouds

Special thanks to:

Xena Olsen, Christian Bremmers, Peter Higgins, Kyle van de Vooren
Source references made where possible.