BELEID & BEHEER

Tom De Laet

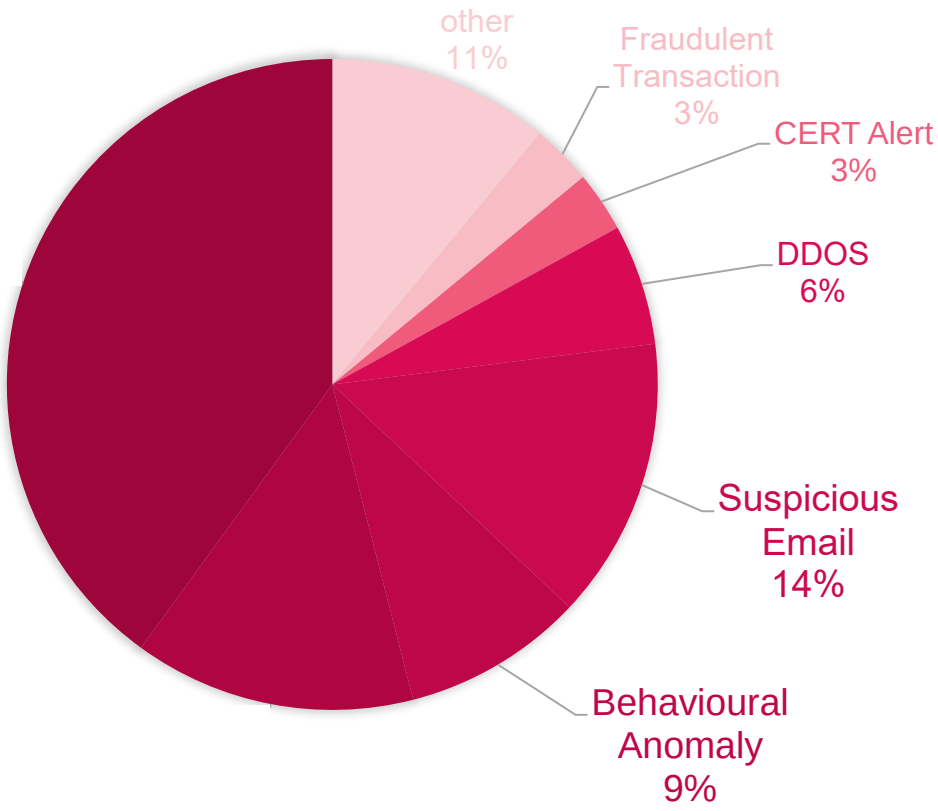
From Firefighting to Fireproofing: Waarom wachten tot het kot in de fik staat?

15:30 – 16:15

ANNACON 0X7E8

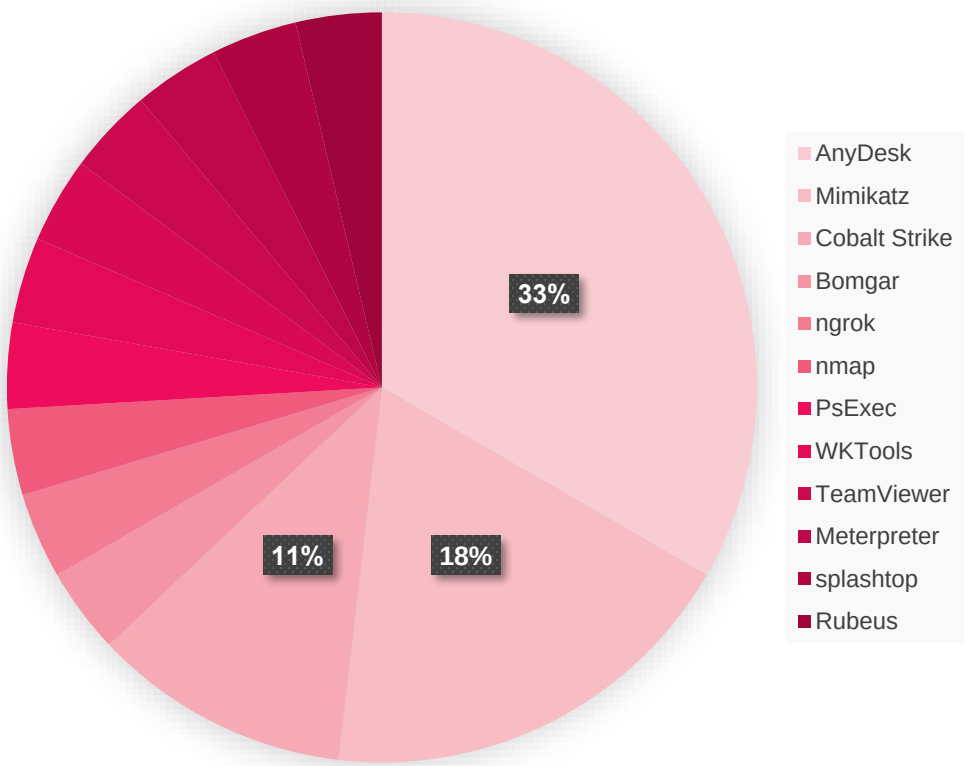

Your network is encrypted by
the Black Basta group.
Instructions in the file
readme.txt
Type here to search
10:17 AM
10/4/2017
ASUS ZenBook

Incident Triggers



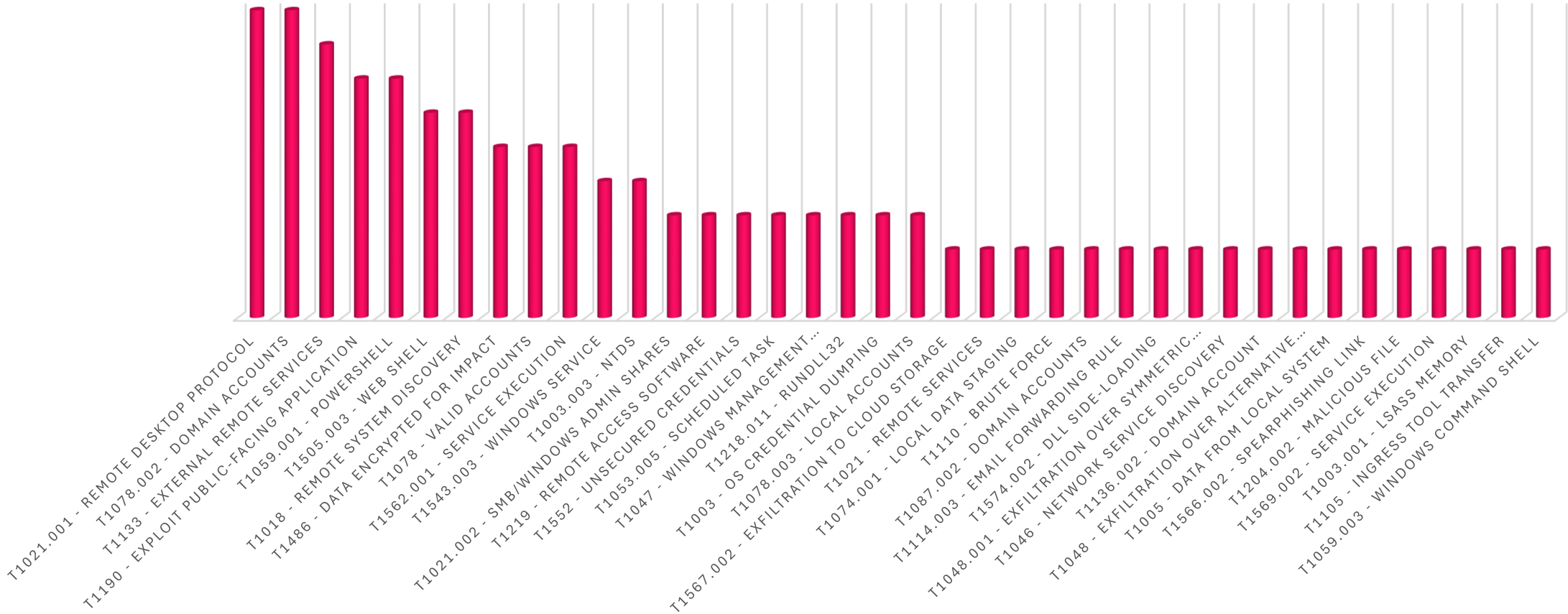
ANNACON
0X7E8

“Attacker Tools”



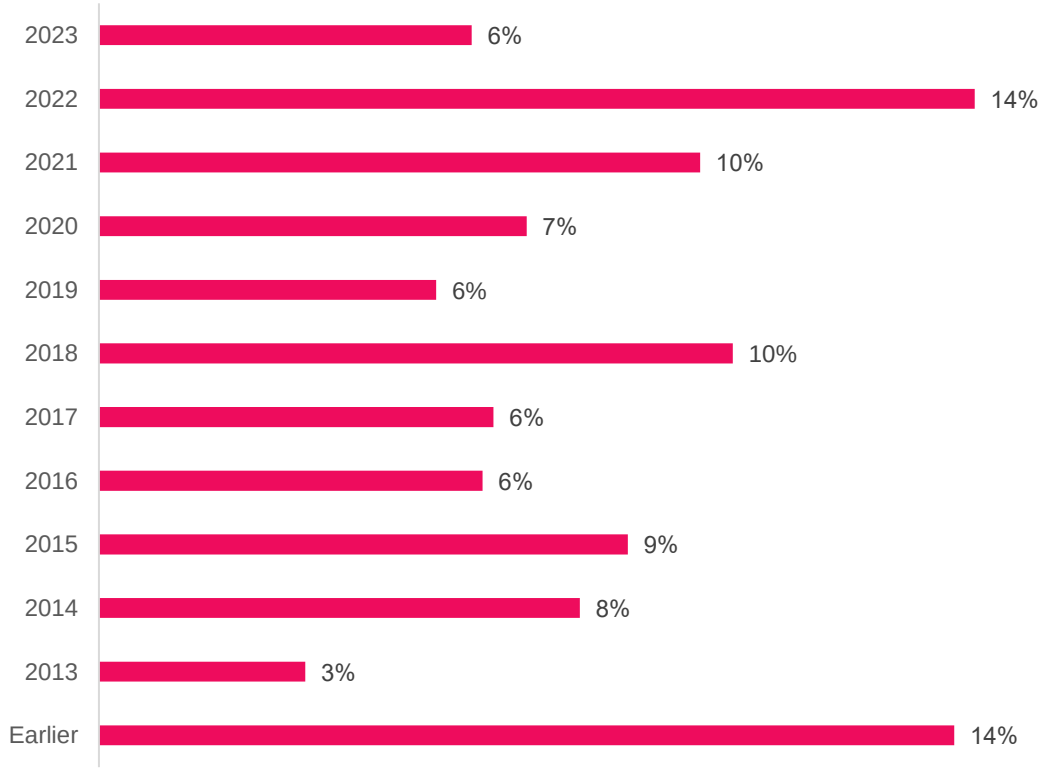
ANNACON
0X7E8

Observed Mitre ATT&CK Techniques



ANNACON
0X7E8

Exploited CVE's



ANNACON
0X7E8

If it ain't broke Don't fix it

Many ransomware attacks are opportunistic!
Threat Actors leverage insecure configurations

Ransomware groups are not (always) stealthy…
In fact, they are often quite loud!

Thwarting ransomware is NOT rocket science!

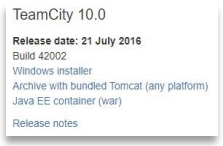
But it's not easy either…

Once upon a time...

ANNACON
0X7E8

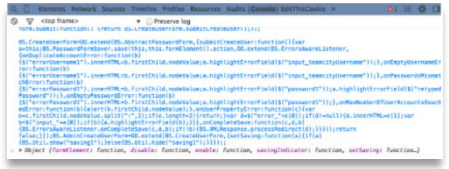
Outerwall Defences…

TeamCity server

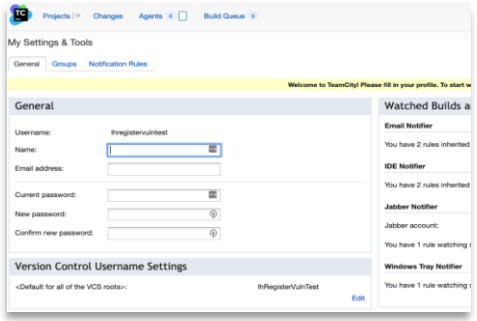


Outdated Software: Since 2016: 30 different vulnerabilities published for this version
TeamCity Server Exposure: Login page exposed (443/HTTPS and 22/SSH)

Javascript Console: <insert code snippet>



TeamCity Nginx Logs: POST /registerUserSubmit.html HTTP/1.1
TeamCity Authentication Logs: New user created: 'service' {id=45}



Next Up… : Lateral Movement…

Timeframe…

4 minutes

Automated & Iterated through a lot of TOR exit nodes

ANNACON
0X7E8

Knowing what is going on in your courtyard

TeamCity server

- Attacker Signed In & Learned Clear Text Password

[redacted]/overview.html
[redacted]/viewLog.html?buildId=6414&buildTypeId=[redacted]_AwsAlertManagerPrd&tab=artifacts
[redacted]/project.html?projectId=[redacted]
[redacted]/diffView.html?id=35631&vcsFileName=configurationgateway2%2fconfiguration[redacted]&personal=false
[redacted]/viewLog.html?buildId=6195&buildTypeId=[redacted]

Ransom: 12 Million $

- Sample of Password Showed in Logging

[2018-10-14 17:19:13,537] INFO - tbrains.buildServer.ACTIVITIES - ""builder (1) (2) (1) (1) (1) (1)" {internal id=43, id=[redacted]11, description: "https://[redacted]Username[redacted]:[redacted]Password[redacted]@bitbucket.org/[redacted].git#refs/heads/[redacted]"}" VCS root settings were edited ("version before: 1, version after: 2") by "[redacted]=1}" with comment ""builder (1) (2) (1) (1) (1) (1)' VCS root was updated"

Data Exfiltration

Interesting!

let's use this

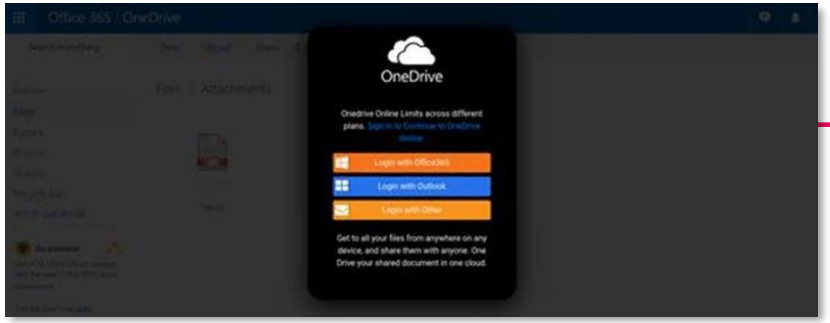
after ~25 minutes

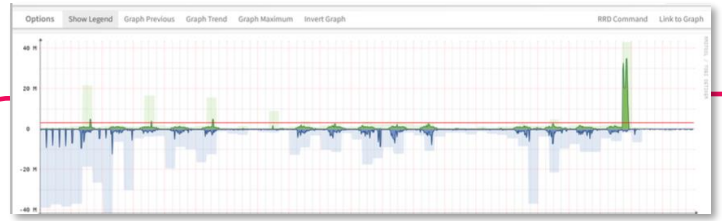
ANNACON
0X7E8

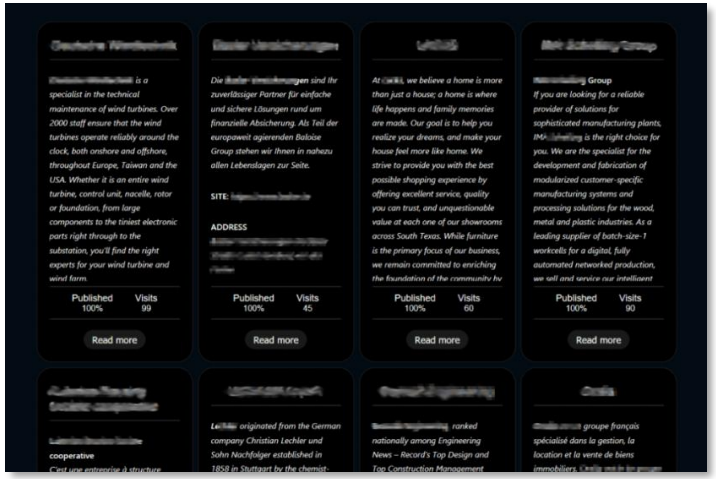
Another one…

ANNACON
0X7E8

Everyone in the castle was sleeping…







ANNACON
0X7E8

Lessons?

Attack Surface?

Asset Management

Patching & Vuln mgmt

No additional email security solution

User != Administrators

Principle of least privilege

Application allow listing-/ ”Baselining”

FW policy

Backups

Identity Access mgmt

Logging AND Monitoring & Alerting

Resouce hogged (people)

IR Plan & Playbooks ?

Knowledge (specialists)

…

and A LOT more!

ANNACON
0X7E8

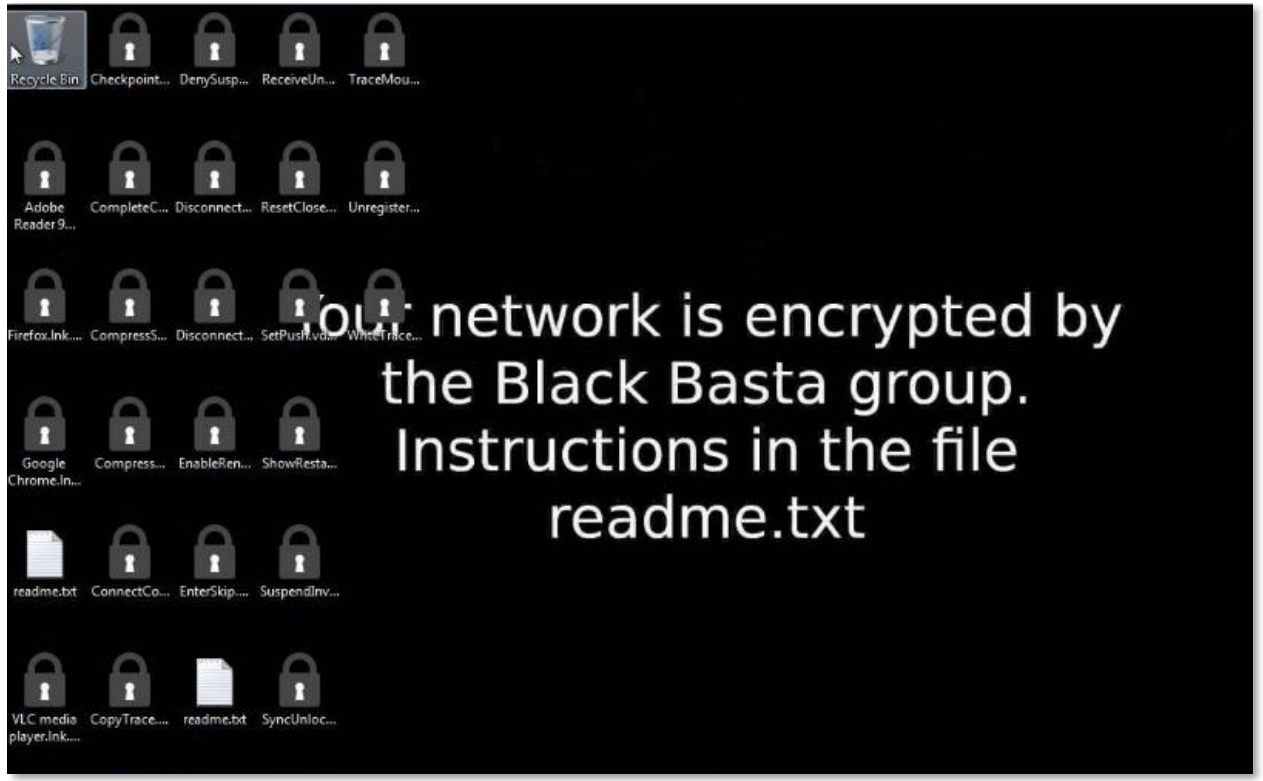
Lessons Implemented…?
Learned…?
Identified…?

We'll see…

Before Ransomware Note

A Threat Actor has:

- Initial Recon
- Exploited an initial vector
- Gained access
- Installed software
- Dumped credentials
- Internal Recon
- Moved laterally
- Installed some more software
- Collected data
- Exfiltrated data
- Deployed ransomware…



ANNACON
0X7E8

This leads us to…

“ If you can't do the little things right, you will never be able to do the big things right. ”

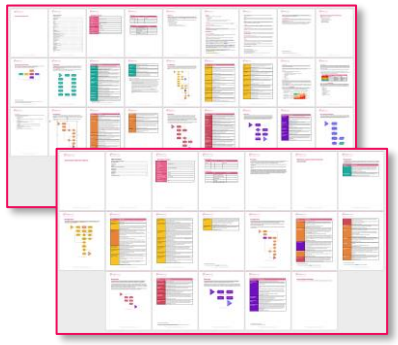
Admiral William H. McRaven

“ Failing To Prepare Is Preparing To Fail ”

Benjamin Franklin

Adopt a proactive mindset

Your variables for success



IR Plan

Attack Surface

Framework

Threat & Risk Prioritisation

Continuous Monitoring & Alerting

ANNACON
0X7E8

What’s your game plan?

sudo DON'T wait Until Your House is on Fire

ANNACON
0X7E8

Deze partners hebben een ❤️ voor ANNACON 0x7E8.

ANNACON
0X7E8

easi
NEUVIK
astrea
UPRIGHT
INFOSENTRY
TSF
pwc
Business
exabeam
REFRACTED
JARVISS
FOX IT
SentinelOne
sweepatic
Beltug
ISACA
Belgium Chapter
SAI