

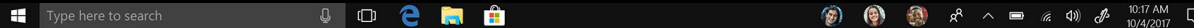


Tom De Laet

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

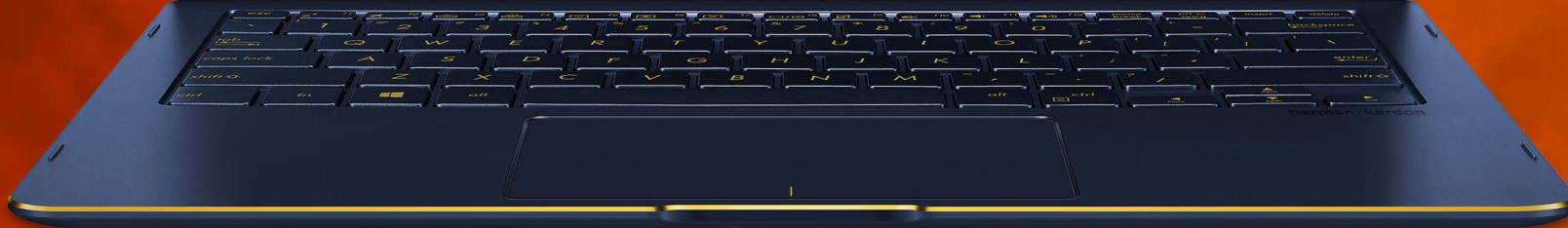
Your network is encrypted by
the Black Basta group.
Instructions in the file
readme.txt

Type here to search

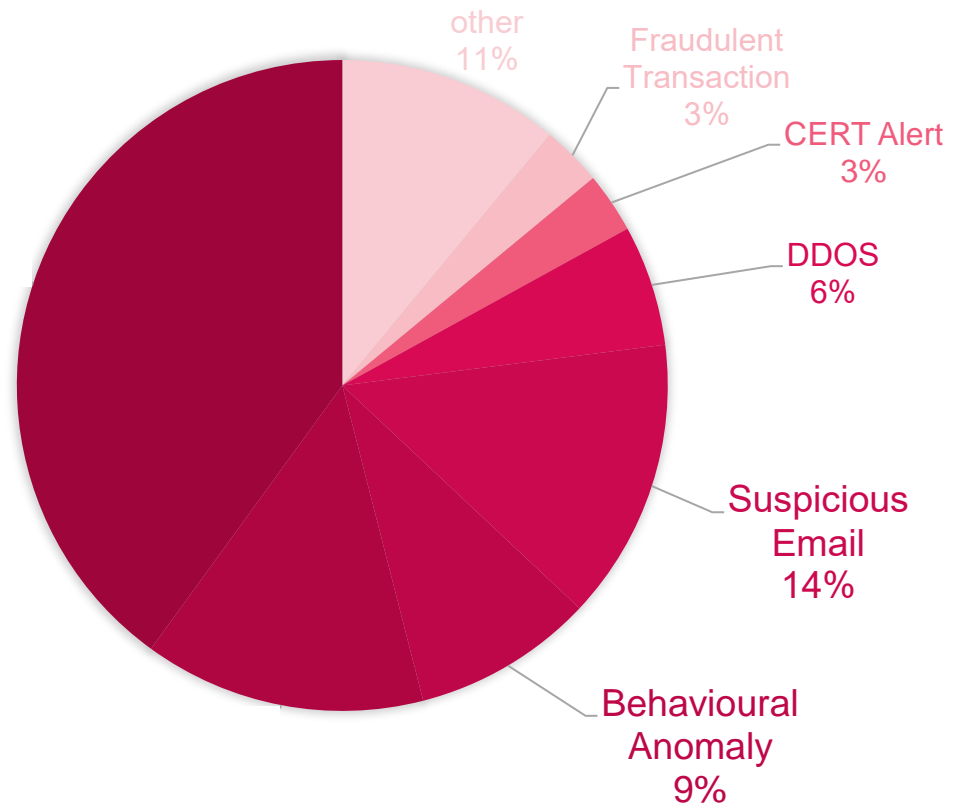


10:17 AM
10/4/2017

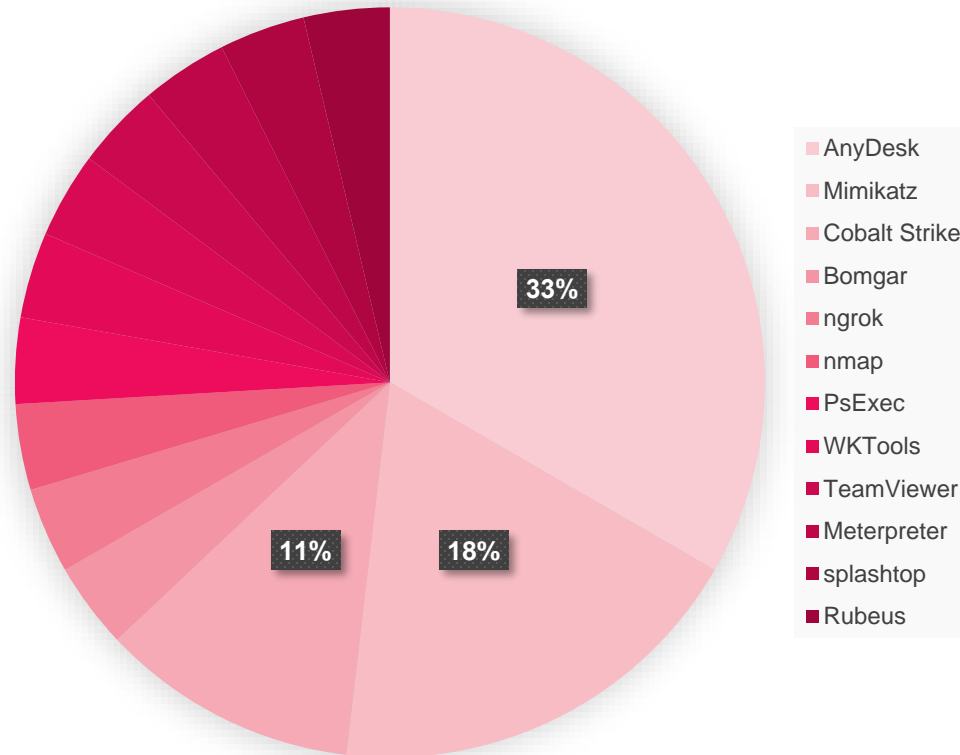
ASUS ZenBook



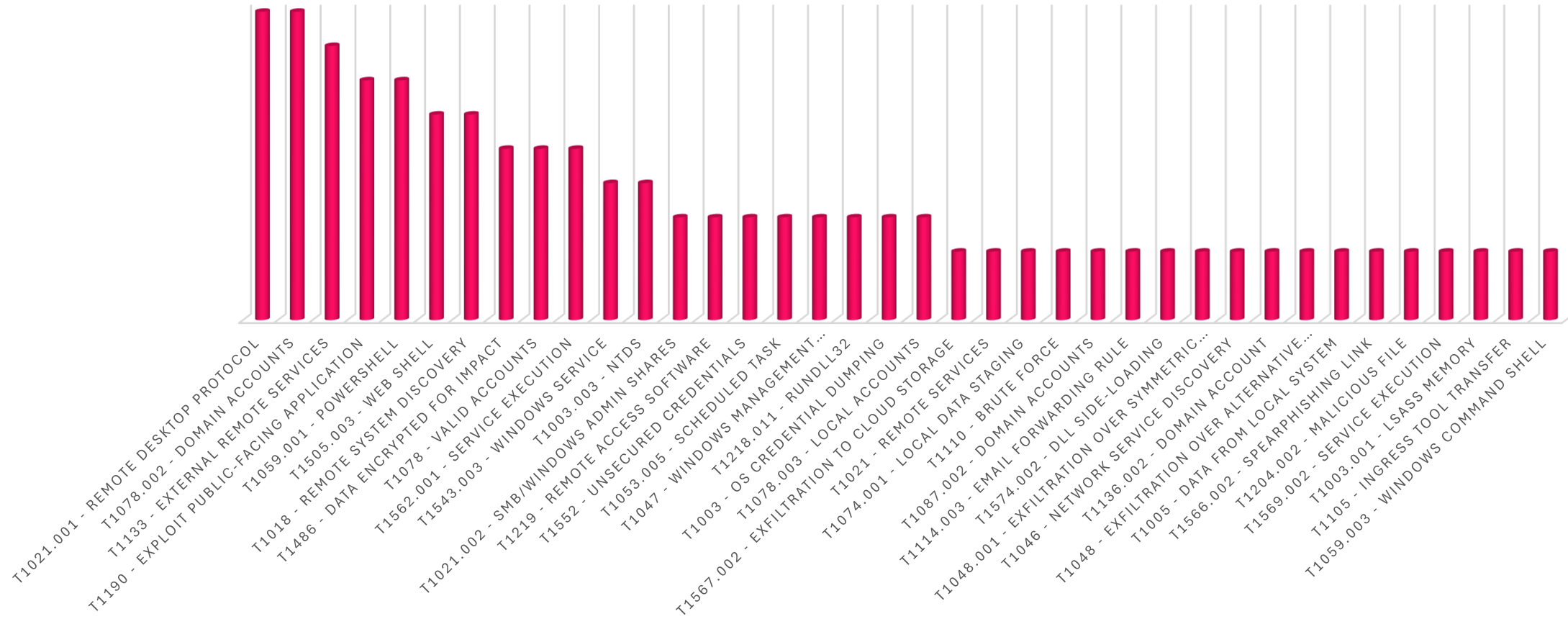
Incident Triggers



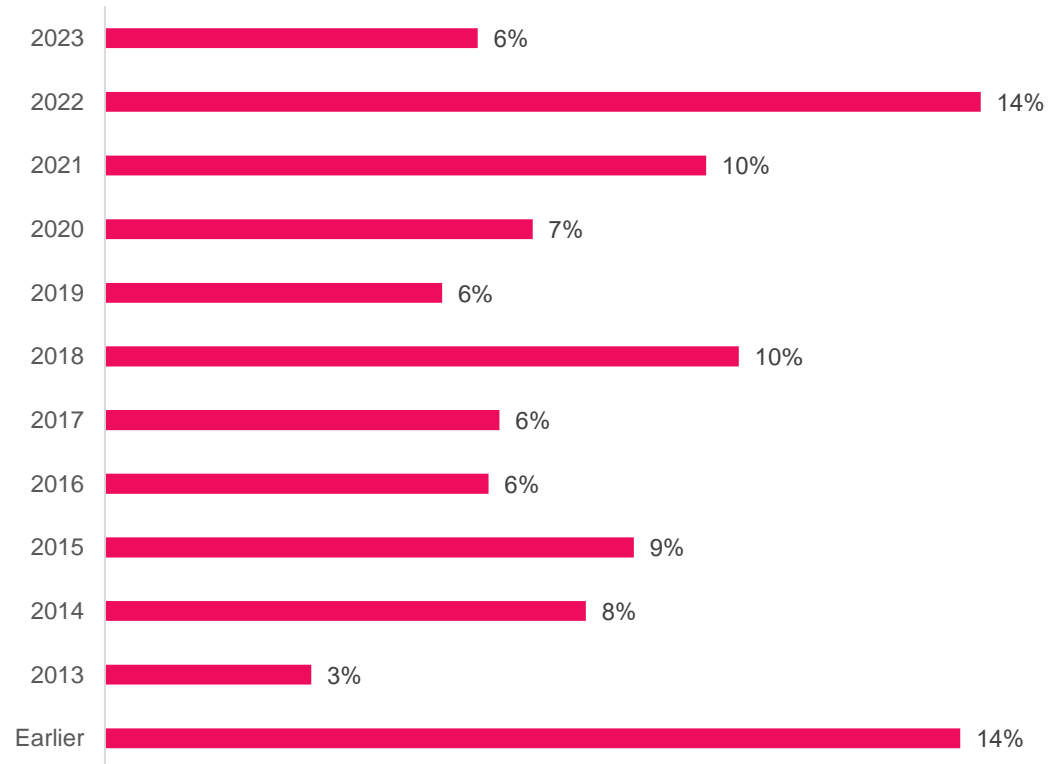
“Attacker Tools”



Observed Mitre ATT&CK Techniques



Exploited CVE's



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...



ANIACON
OX7E8

Once upon a time...



ANIACON
OX7E8

Outerwall Defences...

TeamCity server

TeamCity 10.0
 Release date: 21 July 2016
 Build 42002
 Windows installer
 Archive with bundled Tomcat (any platform)
 Java EE container (war)
 Release notes

Outdated Software: Since 2016: 30 different vulnerabilities published for this version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



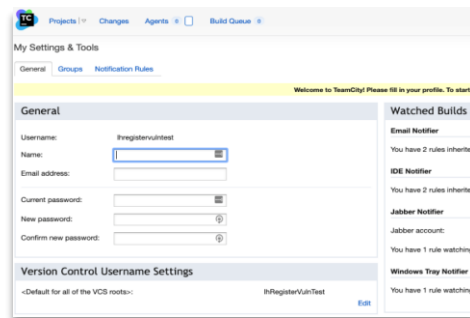
Javascript Console: <insert code snippet>

```

// Example javascript snippet
function() {
    console.log("Exploiting XSS");
    document.write("<img alt='Exploit' src='http://example.com/exploit.png' />");
}
    
```



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



ANIACON
OX7E8

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]ManualProjectBranch&tab=buildChangesDiv  
[REDACTED] /viewLog.html?top=build&name=[REDACTED]&buildTypeId=[REDACTED]&buildId=2972
```

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: Password@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"
```

Interesting!
Data Exfiltration
after 25 minutes
let's use it

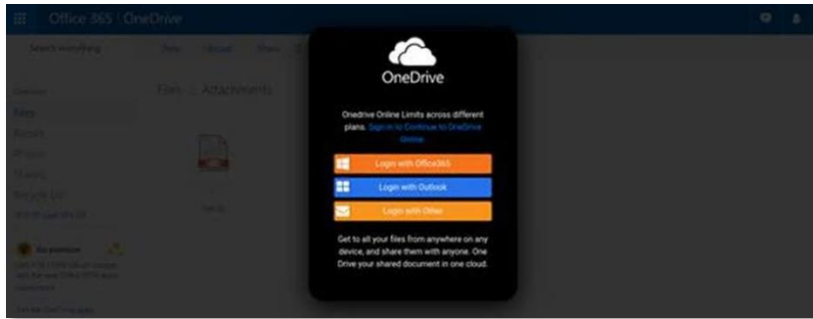


Another one...



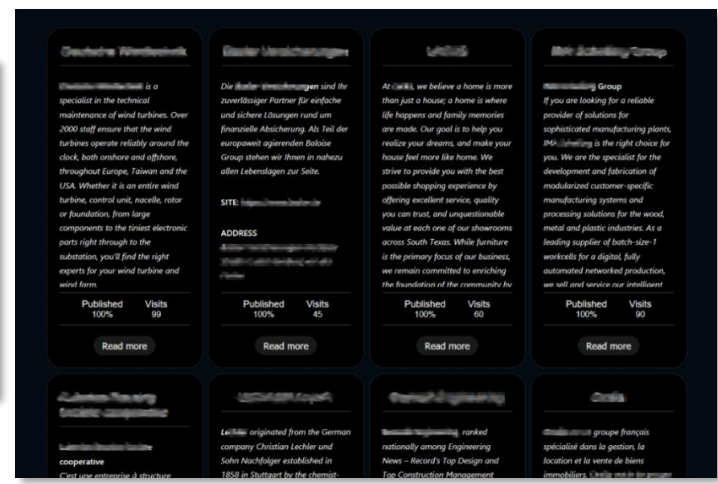
ANIACON
OX7E8

Everyone in the castle was sleeping...



```

Set-MpPreference -DisableArchiveScanning 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableBehaviorMonitoring 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableIntrusionPreventionSystem 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableIOAVProtection 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableRemovableDriveScanning 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableLockatFirstSeen 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableScanningNetworkShares 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableScriptScanning 1 -ErrorAction SilentlyContinue
Set-MpPreference -DisableRealTimeMonitoring 1 -ErrorAction SilentlyContinue
Get-EventLog -List | foreach {Clear-EventLog -LogName $_.log}
Get-EventLog -List | foreach {Clear-EventLog -LogName $_.log}
Get-EventLog -List | foreach {Clear-EventLog -LogName $_.log}
    
```



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!



ANIACON
OX7E8

**Lessons Implemented...?
Learned...?
Identified...?**

We'll see...

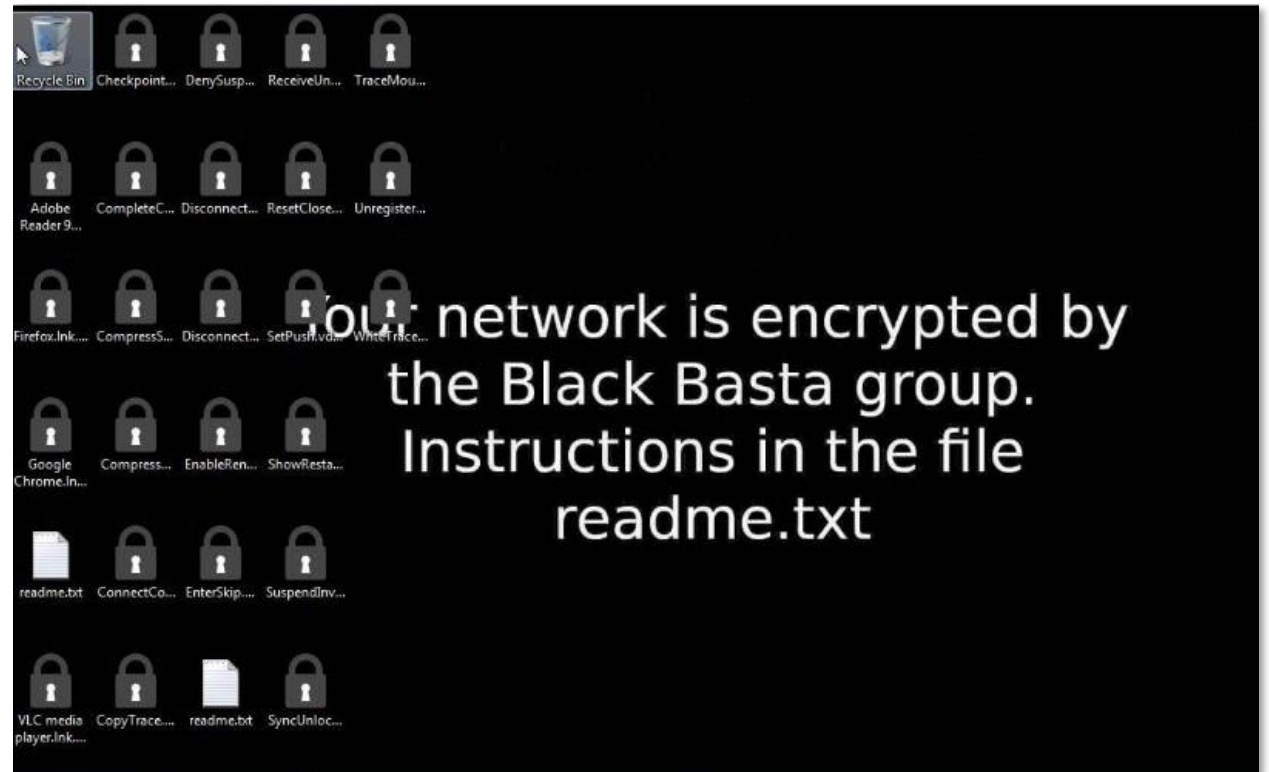


ANIACON
OX7E8

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...



This leads us to...

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

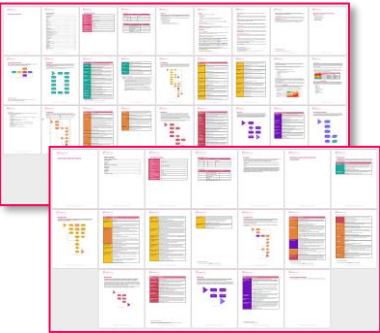
Admiral William H. McRaven

“ Failing To Prepare Is Preparing To Fail ”

Benjamin Franklin

Adopt a proactive mindset

Your variables for success



IR Plan



Attack Surface

A grid of 18 numbered security framework items, each with a title and a progress indicator. The items are: 01 Inventory and Control of Enterprise Assets, 02 Inventory and Control of Software Assets, 03 Data Protection, 04 Secure Configuration of Enterprise Assets and Software, 05 Account Management, 06 Access Control Management, 07 Continuous Vulnerability Management, 08 Audit Log Management, 09 Email and Web Browser Protections, 10 Malware Defenses, 11 Data Recovery, 12 Network Infrastructure Management, 13 Network Monitoring and Defense, 14 Security Awareness and Skills Training, 15 Service Provider Management, 16 Applications Software Security, 17 Incident Response Management, and 18 Penetration Testing.

Framework



Threat & Risk
Prioritisation



Continuous
Monitoring & Alerting





What's your game plan?

sudo **DON'T**
wait Until Your
House is on
Fire



Deze partners hebben een ❤️ voor ANNACON 0x7E8.



ANNACON
0x7E8

