Computer Security in 2019

Where we are? What to exp

How to defend our organizati

Anatomy of an attack

Sebastian Łopieński

CERN Deputy Computer Security Officer

(with input from S.Lueders, R.Wartel, L.Valsan, V.Brillault, E.Cruz and other colleagues)

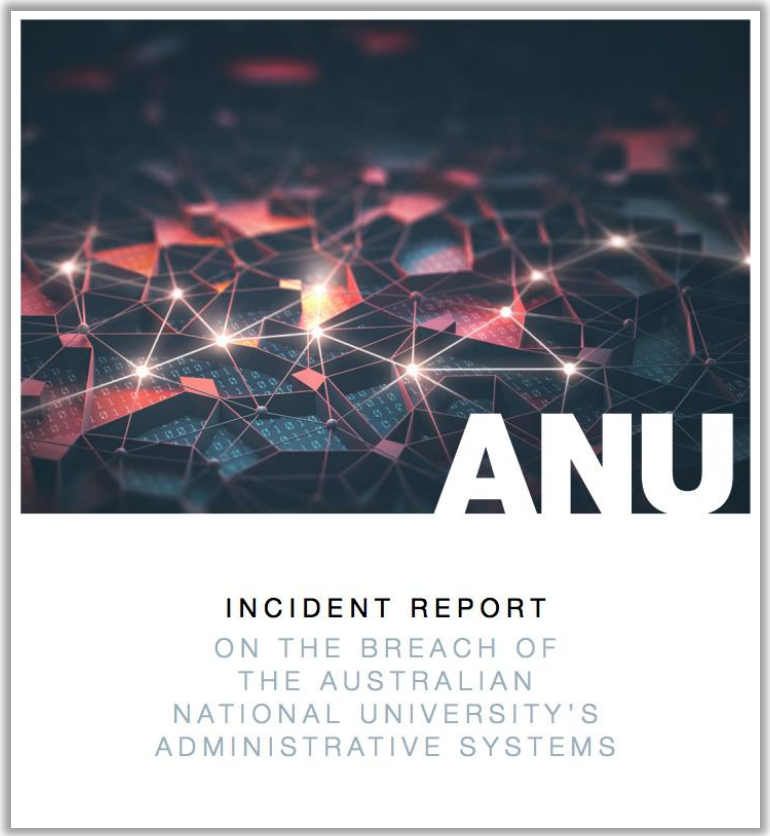
CHEP 2019

24th International Conference on Computing in High Energy & Nuclear Physics

4-8 November 2019, Adelaide, Australia

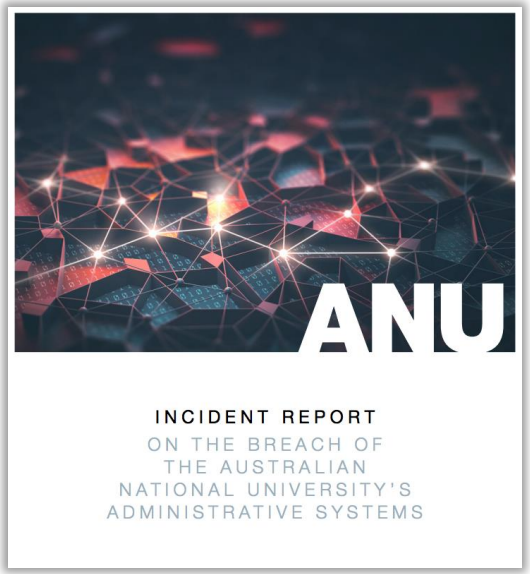
Case study: a recent data breach at ANU

(public detailed report from Oct. 2nd, 2019)



Kudos for being transparent!

Initial attack vector



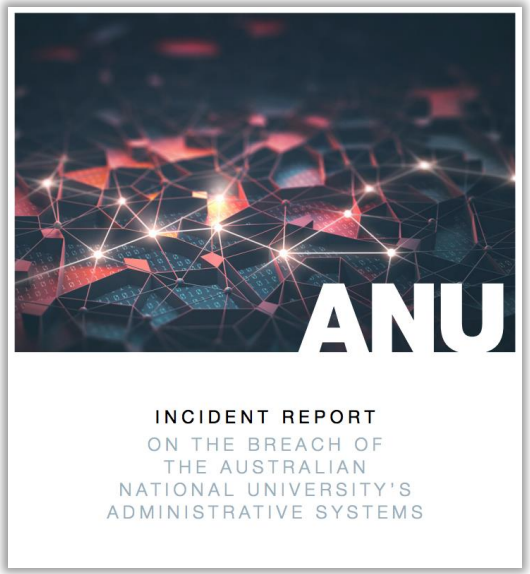
"The initial means of infection was a sophisticated ***spearphishing email*** *(targeting a senior staff member)*

[..]

Information from victim's calendar was used to conduct additional spearphishing attacks later in the campaign."

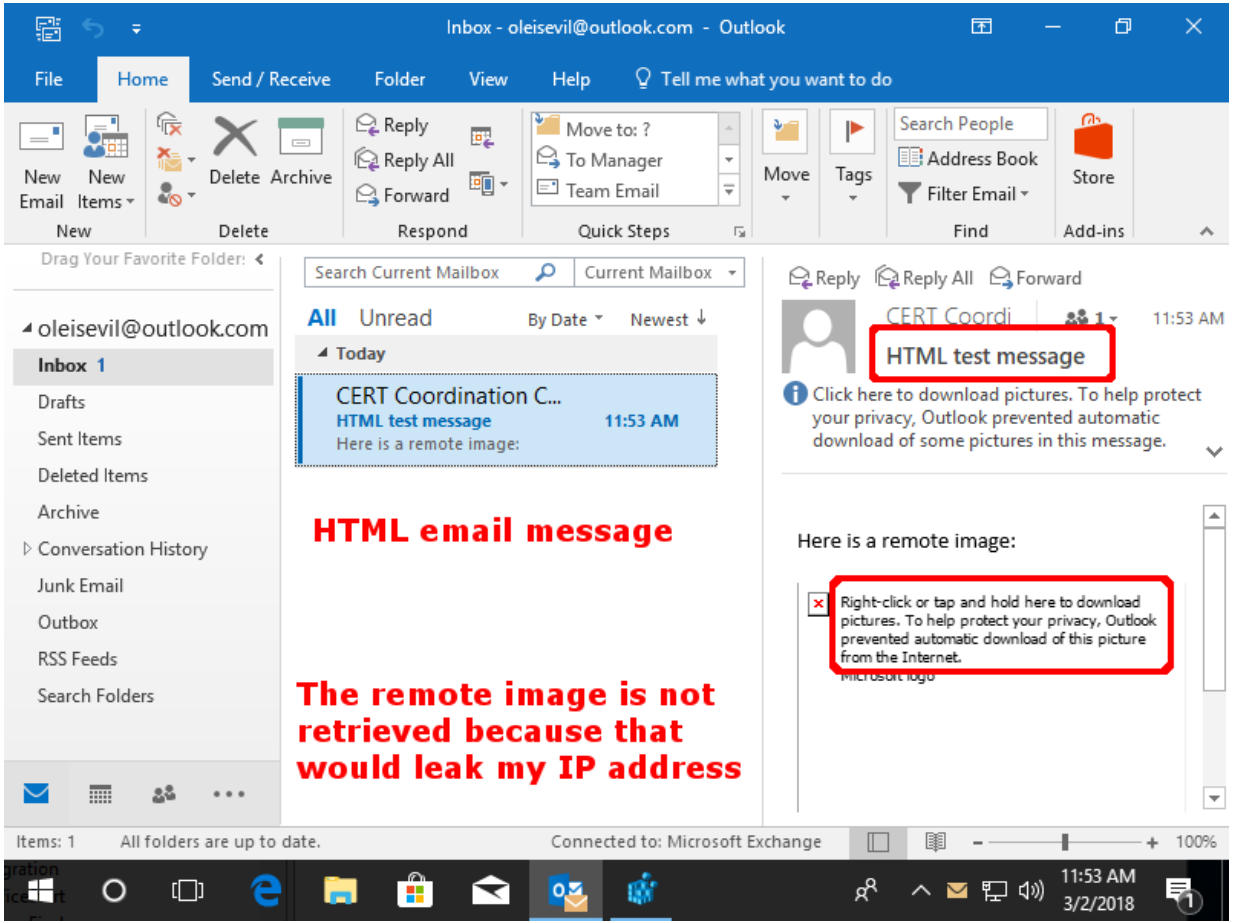
E-mail is the main attack vector

Exploiting a vulnerability



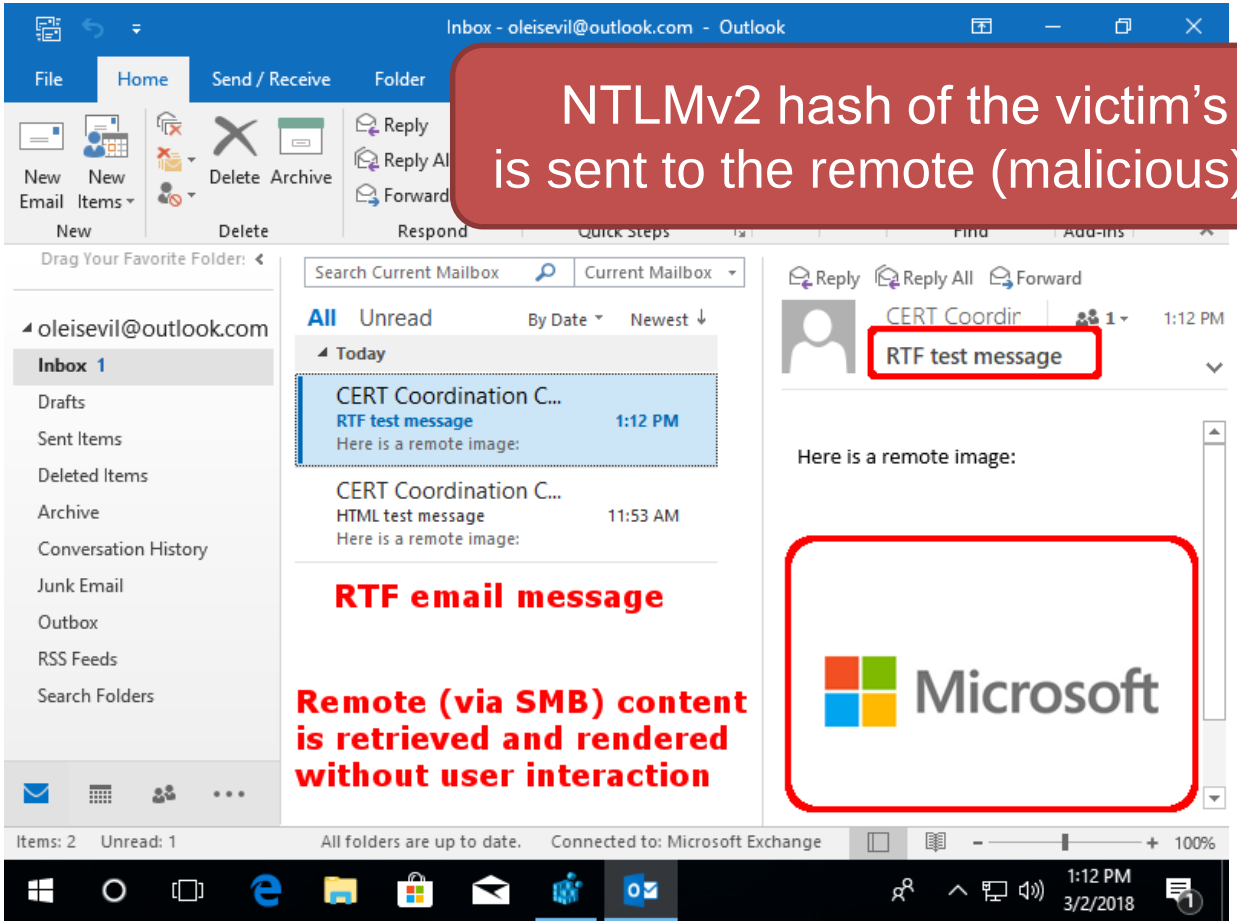
*"The initial means of infection was a sophisticated spearphishing email (targeting a senior staff member) which **did not require user interaction**, ie clicking on a link or downloading an attachment."*

This is how Microsoft Outlook should behave…



https://insights.sei.cmu.edu/cert/2018/04/automatically-stealing-password-hashes-with-microsoft-outlook-and-ole.html

…but for RTF-formatted mails, something else happens



NTLMv2 hash of the victim's password is sent to the remote (malicious) SMB server

https://insights.sei.cmu.edu/cert/2018/04/automatically-s
password-hashes-with-microsoft-outlook-and-ole.html

That was a known vulnerability…

What if you have
more resourceful adversaries?

ZERODIUM Payouts for Desktops/Servers*

Windows
macOS
Linux/BSD
Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME: Virtual Machine Escape

Up to $1,000,000										1.001 Win RCE Zero Click Win
Up to $500,000								3.001 Chrome RCE+LPE Win	2.001 Apache RCE Linux	2.002 MS IIS RCE Win
Up to $250,000							5.001 MS Outlook RCE Win	4.001 MS Exchange RCE Win	2.003 OpenSSL RCE Linux	2.004 PHP RCE Linux
Up to $200,000	6.001 VMware ESXi VME	5.002 Thunderbird RCE Win/Linux			4.002 Sendmail RCE Linux	4.003 Postfix RCE Linux	4.004 Dovecot RCE Linux	4.005 Exim RCE Linux	2.005 nginx RCE Linux	
Up to $100,000		3.002 Safari RCE+LPE Mac	3.003 Edge RCE+LPE Win	3.004 Firefox RCE+LPE Win	5.003 Word/Excel RCE Win	7.001 WordPress RCE Linux	7.002 cPanel/WHM RCE Linux	7.003 Plesk RCE Linux	7.004 Webmin RCE Linux	
Up to $80,000	6.002 VMware WS VME Win/Linux					5.004 Adobe PDF RCE+SBX Win	5.005 WinRAR RCE Win	5.006 7-Zip RCE Win	6.003 Windows LPE/SBX Win	
Up to $50,000	6.004 USB LPE Win/Mac	8.001 Antivirus RCE Win			5.007 WinZip RCE Win	5.008 tar RCE Linux	6.005 macOS LPE/SBX Mac	6.006 Linux LPE Linux	6.007 BSD LPE BSD	
Up to $10,000	9.001 Routers RCE	8.002 Antivirus LPE Win	7.005 phpBB RCE Linux	7.006 vBulletin RCE Linux	7.007 MyBB RCE Linux	7.008 Joomla RCE Linux	7.009 Drupal RCE Linux	7.010 Roundcube RCE Linux	7.011 Horde RCE Linux	

** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

2019/01 © zerodium.com

Example:

CVE-2018-8589: zero-day vulnerability in Edge browser

```
mov     eax, [ebp+var_38.right]
sub     eax, ecx
mov     [ebp+var_14], eax
mov     eax, [ebp+var_38.bottom]
mov     [ebp+var_6C], ecx
mov     ecx, [ebp+var_38.top]
sub     eax, ecx
mov     [ebp+var_8], eax
lea     eax, [ebp+Address]
push    eax             ; Address
push    1               ; UnicodeString
push    83h             ; MbString
push    [ebp+P]         ; P
mov     [ebp+var_64], ecx
call    _xxxSendMessage@16 ; WM_NCCALCSIZE msg
push    dword ptr [ebx+4]
mov     [ebp+var_4], eax
call    _IsStillWindowC@4 ; IsStillWindowC(x)
test    eax, eax
jz      loc_BF88C18A

cmp     [ebp+var_4], 10h
jl      short loc_BF88BEE3
```

Kaspersky: *"In October 2018, our Automatic Exploit Prevention (AEP) systems detected an attempt to exploit a vulnerability in Microsoft's Windows operating system. Further analysis revealed a zero-day vulnerability in win32k.sys. The exploit was executed by the first stage of a malware installer in order to gain the necessary privileges for persistence on the victim's system. So far, we have detected a very limited number of attacks using this vulnerability. The victims are located in the Middle East."*

From https://securelist.com/a-new-exploit-for-zero-day-vulnerability-cve-2018-8589/88845/

… and daily business

Security Bulletins and Advisories

Adobe Acrobat

Brief	Originally posted	Last updated
APSB19-49 Security update available for Adobe Acrobat and Reader	10/15/2019	10/15/2019
APSB19-41 Security update available for Adobe Acrobat and Reader	08/13/2019	08/14/2019
APSB19-18 Security update available for Adobe Acrobat and Reader	05/14/2019	05/14/2019
APSB19-17 Security update available for Adobe Acrobat and Reader	04/09/2019	04/09/2019
APSB19-13 Security Updates available for Adobe Acrobat and Reader	02/21/2019	02/21/2019
APSB19-07 Security Updates available for Adobe Acrobat and Reader	02/12/2019	02/12/2019
APSB19-02 Security Updates Available for Adobe Acrobat and Reader	01/03/2019	01/03/2019
APSB18-41 Security Updates Available for Adobe Acrobat and Reader	12/11/2018	12/11/2018
APSB18-40 Security Updates Available for Adobe Acrobat and Reader	11/13/2018	11/13/2018
APSB18-30 Security updates available for Adobe Acrobat and Reader	10/1/2018	10/1/2018
APSB18-34 Security updates available for Adobe Acrobat and Reader	09/19/2018	09/19/2018

One advisory (patch), multiple vulnerabilities

https://helpx.adobe.com/security/products/acrobat/apsb19-49.html

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Out-of-Bounds Read	Information Disclosure	Important	CVE-2019-8164 CVE-2019-8168 CVE-2019-8172 CVE-2019-8173 CVE-2019-8198 CVE-2019-8201 CVE-2019-8202 CVE-2019-8204 CVE-2019-8207 CVE-2019-8216 CVE-2019-8218 CVE-2019-8222
Out-of-Bounds Write	Arbitrary Code Execution	Critical	CVE-2019-8171 CVE-2019-8186 CVE-2019-8165 CVE-2019-8191 CVE-2019-8199 CVE-2019-8206
Use After Free	Arbitrary Code Execution	Critical	CVE-2019-8175 CVE-2019-8176 CVE-2019-8177 CVE-2019-8178 CVE-2019-8179 CVE-2019-8180 CVE-2019-8211 CVE-2019-8212 CVE-2019-8213 CVE-2019-8214 CVE-2019-8215 CVE-2019-8217 CVE-2019-8219 CVE-2019-8220 CVE-2019-8221 CVE-2019-8223 CVE-2019-8224 CVE-2019-8225
Heap Overflow	Arbitrary Code Execution	Critical	CVE-2019-8170 CVE-2019-8183 CVE-2019-8197
Buffer Overrun	Arbitrary Code Execution	Critical	CVE-2019-8166
Cross-site Scripting	Information Disclosure	Important	CVE-2019-8160
Race Condition	Arbitrary Code Execution	Critical	CVE-2019-8162
Incomplete Implementation of Security Mechanism	Information Disclosure	Important	CVE-2019-8226
Type Confusion	Arbitrary Code Execution	Critical	CVE-2019-8161 CVE-2019-8167 CVE-2019-8169 CVE-2019-8200
Untrusted Pointer Dereference	Arbitrary Code Execution	Critical	CVE-2019-8174 CVE-2019-8195 CVE-2019-8196 CVE-2019-8205

Vulnerability Category	Vulnerability Impact	Severity	CVE Number
Out-of-Bounds Read	Information Disclosure	Important	CVE-2019-8164 CVE-2019-8168

Dealing with “normal” vulnerabilities

(aka *business as usual*)

Mature organisations:

- harden their configurations
- disable unnecessary products/services
- apply patches in a timely manner
- use more secure alternatives
  - e.g. CERN moved to another PDF reader a few years ago
- invest in detection (and response)
  - more: D.Crooks & L.Valsan talk on Tuesday 16:45
    R.Wartel’s plenary talk on Thursday 9:30

shadow IT

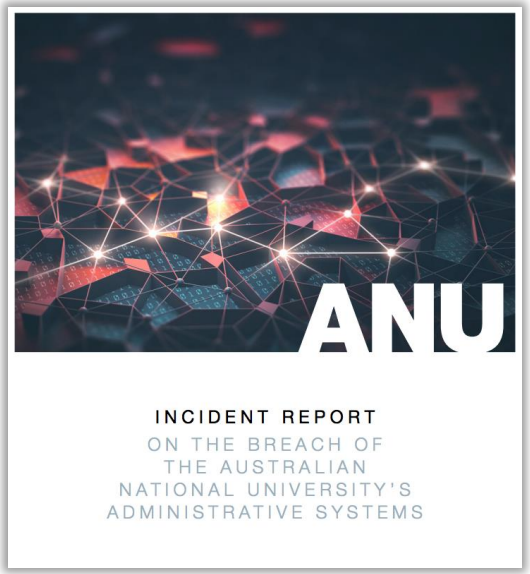
legacy systems

Internet of Things

This applies also to servers / services

- virtualization, clouds, provisioning, orchestration, federated identities…

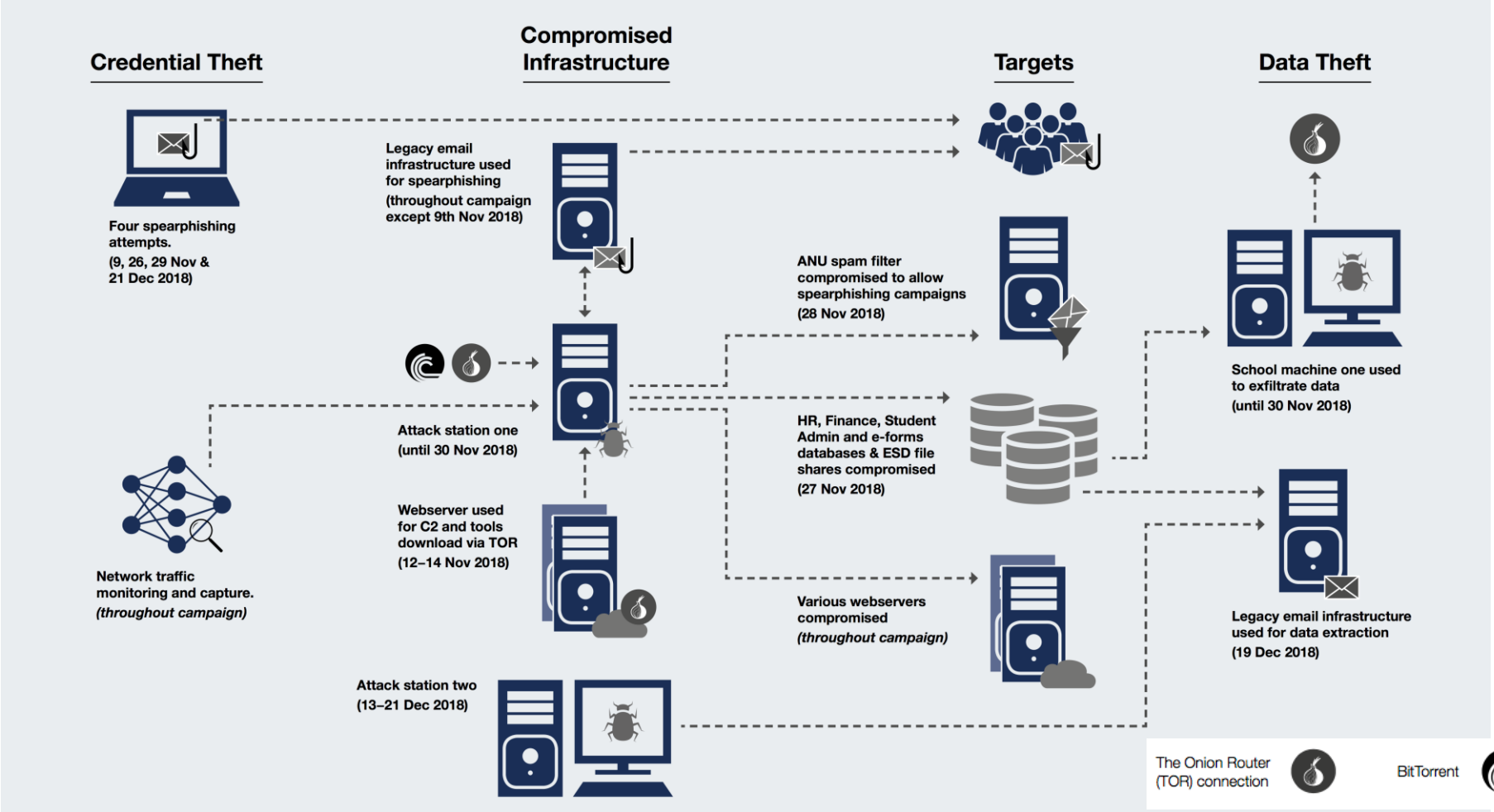
Next steps



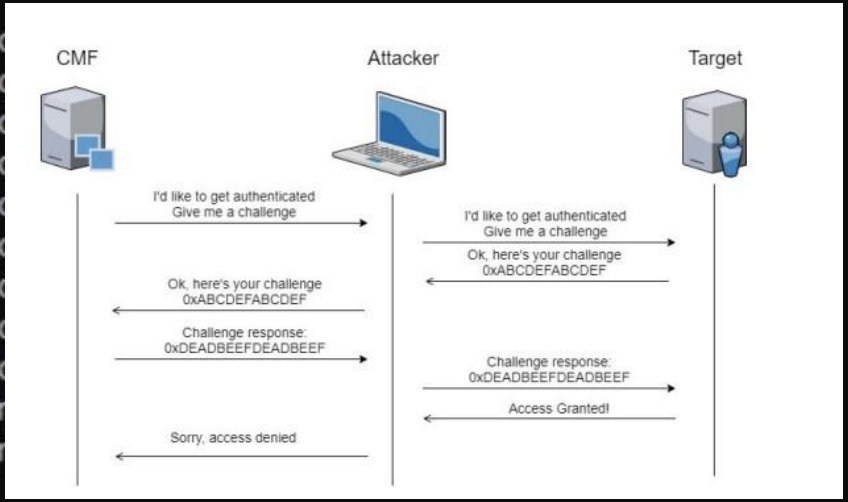
"The credentials taken from this account were used to gain access to other systems.[..]

The actor built ***a shadow ecosystem of compromised ANU machines, tools and network connections to carry out their activities undetected****. Some compromised machines provide a foothold into the network. Others, like the so-called* ***attack stations****, provided the actor with a base of operations to map the network, identify targets of interest, run tools and compromise other machines."*

Moving laterally, staying stealth, exfiltrating data

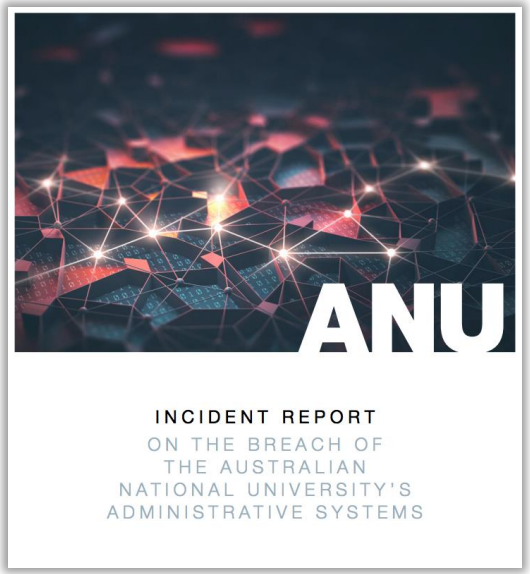


```
[root@cc7-bloodhound examples]# python ntlmrelayx.py -smb2support -t cerndc
Impacket v0.9.18 - Copyright 2018 SecureAuth Corporation

[*] Proto
[*] Proto
[*] Proto
[*] Proto
[*] Proto
[*] Proto
[*] Proto
[*] Proto
[*] Proto
[*] Runni
[*] Setti

[*] Setting up HTTP Server
[*] Servers started, waiting for connections
[*] SMBD: Received connection from 128.141.[redacted], attacking target smb://cerndc
[*] Authenticating against smb://cerndc as C E R N \[redacted] SUCCEED
[*] Target system bootKey: [redacted]
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:[redacted]:::
Guest:501:[redacted]:::
[*] Done dumping SAM hashes for host: cerndc
```



MITM to get domain admin privileges (aka *game over*)

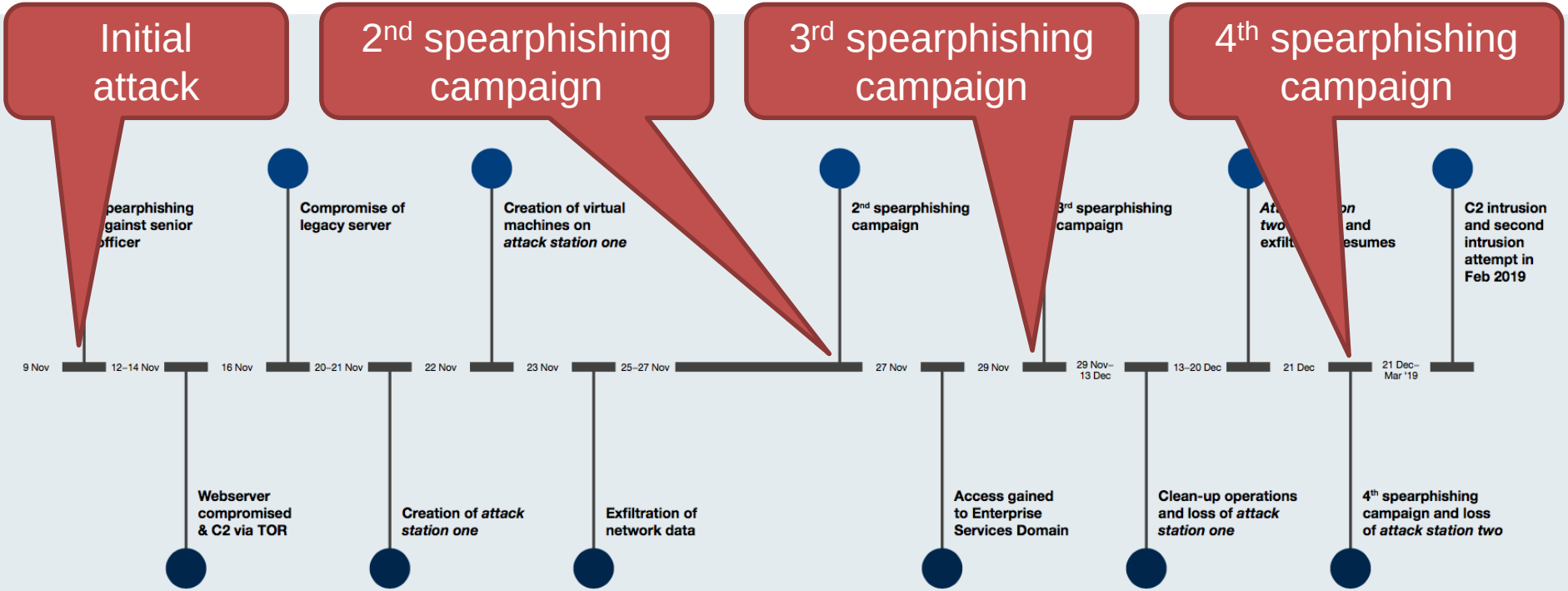
Target system



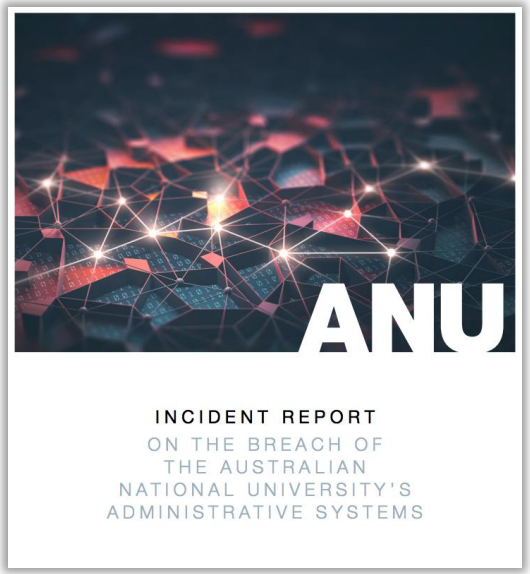
"This attack resulted in the breach of [..] the Enterprise Systems Domain (ESD), which houses our ***human resources, financial management, student administration and enterprise e-forms systems.****"*

All organizations have sensitive data and valuable assets

Ongoing attacks



Detection



*"In early **November 2018**, a sophisticated actor gained unauthorized access [..]*

*Indications of an intrusion were first detected in **April 2019** during a baseline threat hunting exercise. [..]*

*The incident response team uncovered the data breach on **May 17**."*

Detected 6 months later…
… while looking for something else!

Conclusions

Instead of conclusions

Whatever you do:

- develop web applications
- manage the domain controller
- maintain some code
- do system administration
- run a computing service
- have access to sensitive data or systems
- just use computers (email, web browsing)

… you have an impact on the security of your organization!

Thank you for your attention!

See also other security talks at CHEP 2019:

- Harnessing the power of threat intelligence for WLCG cybersecurity
  by David Crooks (STFC) and Liviu Valsan (CERN) **T3, Tue 16:45**
- Tackling modern cyberthreats together is the only way forward
  by Romain Wartel (CERN) **Plenary, Thu 09:30**
- Email-based threats - addressing the human factor
  by Sebastian Lopienski (CERN) **T8, Thu 11:45**