Computer Security in 2019: Where we are? What to expect? How to defend our organizations?

Sebastian Łopieński
CERN Deputy Computer Security Officer

(with input from S.Lueders, R.Wartel, L.Valsan, V.Brillault, E.Cruz and other colleagues)
Case study: a recent data breach at ANU
(public detailed report from Oct. 2nd, 2019)
Initial attack vector

“The initial means of infection was a sophisticated \textit{spearphishing email} (targeting a senior staff member)

[...

\textit{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...

HTML email message

The remote image is not retrieved because that would leak my IP address

...but for RTF-formatted mails, something else happens.

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

Remote (via SMB) content is retrieved and rendered without user interaction.
That was a known vulnerability...

What if you have more resourceful adversaries?
# ZERODIUM Payouts for Desktops/Servers*

<table>
<thead>
<tr>
<th>Payout</th>
<th>Software</th>
<th>OS</th>
<th>RCE Type</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to $1,000,000</td>
<td>Win, MacOS</td>
<td>Windows</td>
<td>RCE: Remote Code Execution</td>
<td>Win RCE Zero Click</td>
</tr>
<tr>
<td>Up to $500,000</td>
<td>Linux/BSD</td>
<td>Windows</td>
<td>LPE: Local Privilege Escalation</td>
<td>Apache RCE</td>
</tr>
<tr>
<td>Up to $250,000</td>
<td>VME</td>
<td>Win/Linux</td>
<td>SBX: Sandbox Escape or Bypass</td>
<td>OpenSSL RCE</td>
</tr>
<tr>
<td>Up to $200,000</td>
<td>VMware ESXi</td>
<td>Win/Linux</td>
<td>VME: Virtual Machine Escape</td>
<td>PHP RCE</td>
</tr>
<tr>
<td>Up to $100,000</td>
<td>Thunderbird</td>
<td>Win/Linux</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $80,000</td>
<td>Safari</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $50,000</td>
<td>Edge</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $30,000</td>
<td>Firefox</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $20,000</td>
<td>Word/Excel</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $10,000</td>
<td>Adobe PDF</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $5,000</td>
<td>WinRAR</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $3,000</td>
<td>tar</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $2,000</td>
<td>macOS LPE/DBX</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $1,000</td>
<td>Roundcube</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $500</td>
<td>phpBB</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $250</td>
<td>vBulletin</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $100</td>
<td>MyBB</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $50</td>
<td>Joomla</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $25</td>
<td>Drupal</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up to $10</td>
<td>Roundcube</td>
<td>MacOS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

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

2019/01 © zerodium.com
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.”

... and daily business
### Security Bulletins and Advisories

#### Adobe Acrobat

<table>
<thead>
<tr>
<th>Brief</th>
<th>Originally posted</th>
<th>Last updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>APSB19-41 Security update available for Adobe Acrobat and Reader</td>
<td>08/13/2019</td>
<td>08/14/2019</td>
</tr>
<tr>
<td>APSB19-18 Security update available for Adobe Acrobat and Reader</td>
<td>05/14/2019</td>
<td>05/14/2019</td>
</tr>
<tr>
<td>APSB19-13 Security Updates available for Adobe Acrobat and Reader</td>
<td>02/21/2019</td>
<td>02/21/2019</td>
</tr>
<tr>
<td>APSB19-07 Security Updates available for Adobe Acrobat and Reader</td>
<td>02/12/2019</td>
<td>02/12/2019</td>
</tr>
<tr>
<td>APSB19-02 Security Updates Available for Adobe Acrobat and Reader</td>
<td>01/03/2019</td>
<td>01/03/2019</td>
</tr>
<tr>
<td>APSB18-30 Security updates available for Adobe Acrobat and Reader</td>
<td>10/1/2018</td>
<td>10/1/2018</td>
</tr>
<tr>
<td>APSB18-34 Security updates available for Adobe Acrobat and Reader</td>
<td>09/19/2018</td>
<td>09/19/2018</td>
</tr>
</tbody>
</table>
One advisory (patch), multiple vulnerabilities


<table>
<thead>
<tr>
<th>Vulnerability Category</th>
<th>Vulnerability Impact</th>
<th>Severity</th>
<th>CVE Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Bounds Read</td>
<td>Information Disclosure</td>
<td>Important</td>
<td>CVE-2019-8164</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8168</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8172</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8173</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8198</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8201</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8202</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8204</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8207</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8216</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8218</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8222</td>
</tr>
<tr>
<td>Out-of-Bounds Write</td>
<td></td>
<td></td>
<td>CVE-2019-8171</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8186</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8165</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8191</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8199</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2019-8206</td>
</tr>
</tbody>
</table>

- Use After Free
- Arbitrary Code Execution
- Critical

Heap Overflow
- Arbitrary Code Execution
- Critical

Buffer Overrun
- Arbitrary Code Execution

Cross-site Scripting
- Information Disclosure
- Important

Race Condition
- Arbitrary Code Execution
- Critical

Incomplete Implementation of Security Mechanism
- Information Disclosure
- Important

Type Confusion
- Arbitrary Code Execution
- Critical

Untrusted Pointer Dereference
- Arbitrary Code Execution
- Critical
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

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

Credential Theft

- Four spearphishing attempts. (8, 26, 29 Nov & 21 Dec 2018)

Compromised Infrastructure

- Legacy email infrastructure used for spearphishing (throughout campaign except 9th Nov 2018)
- Attack station one (until 30 Nov 2018)
- Webserver used for C2 and tools download via TOR (12–14 Nov 2018)
- Attack station two (13–21 Dec 2018)

Targets

- ANU spam filter compromised to allow spearphishing campaigns (28 Nov 2018)
- HR, Finance, Student Admin and e-forms databases & ESD file shares compromised (27 Nov 2018)
- Various webservers compromised (throughout campaign)

Data Theft

- School machine one used to exfiltrate data (until 30 Nov 2018)
- Legacy email infrastructure used for data extraction (19 Dec 2018)

Network traffic monitoring and capture. (throughout campaign)
MITM to get domain admin privileges
(aka game over)
“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.”
Ongoing attacks

- **Initial attack**
  - Spearphishing against senior officer
  - Compromise of legacy server
  - Creation of virtual machines on attack station one
  - Webserver compromised & C2 via TOR

- **2nd spearphishing campaign**
  - Creation of attack station one
  - Exfiltration of network data
  - Access gained to Enterprise Services Domain

- **3rd spearphishing campaign**
  - 2nd spearphishing campaign
  - 3rd spearphishing campaign
  - Clean-up operations and loss of attack station one

- **4th spearphishing campaign**
  - 4th spearphishing campaign and loss of attack station two
  - C2 intrusion and second intrusion attempt in Feb 2019
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