# Rückblick
# IT-Sicherheit 2018

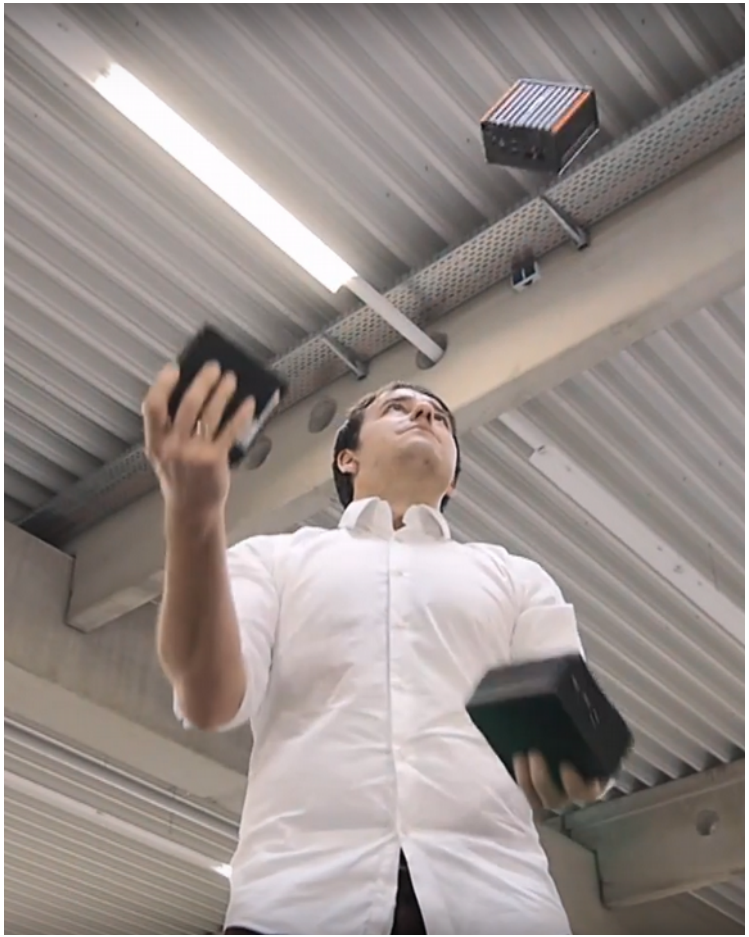
*@cmitasch*
*Christoph Mitasch, Thomas-Krenn.AG*

*Webinar, 23. Jänner 2019*

THOMAS KRENN®

# Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG Niederlassung Österreich
- Diplomstudium Computer- und Mediensicherheit
- Erfahrung in Web Operations, Linux und HA
- Cyber-Security-Practitioner



# Agenda

- CPU-Sicherheitslücken
- Krypto Mining
- Supermicro Spionage Chip
- DNS-Hijacking
- Emotet
- Phishing
- Ausblick 2019

*Quelle: commons.wikimedia.org*

# CPU-Sicherheitslücken

- 1.6.2017: an Intel gemeldet
- 3.1.2018: erste Veröffentlichung Spectre, Meltdown
- 3.5.2018: Spectre NG (8 weitere Varianten)
- 14.8.2018: L1 Terminal Fault / Foreshadow
- SGXPectre, NetSpectre, ret2spec, SpectreRSB, ...

# CPU-Sicherheitslücken

- OS Fixes werden laufend schneller
- verbesserte CPUs erscheinen nur langsam
- Virtuelle Maschinen nicht so gut isoliert wie angenommen
- Lücken sind bisher nur schwer ausnutzbar
- Angriffe allerdings auch nur schwer nachweisbar
- CPU-Sicherheit im Fokus
  → vermutlich kommen noch weitere Lücken

# Was kann man tun?

- laufend Updates einspielen (OS, Microcode, BIOS, Browser, Treiber, Software, ...)
- CPUs erneuern
- Virtualisierungs-Strategie prüfen
- Absicherung automatisiert prüfen, unter Linux mit: https://github.com/speed47/spectre-meltdown-checker
  - --explain (Hinweis, wie es behoben werden kann)
  - --live / --kernel /boot/vmlinuz-4.4.0-141-generic
  - --batch nrpe (Icinga Check)

```
> SUMMARY: CVE-2017-5753:OK CVE-2017-5715:OK CVE-2017-5754:OK CVE-2018-3640:OK CVE-2018-3639:OK CVE-2018-3615:OK CVE-2018-3620:OK CVE-2018-3646:OK
```

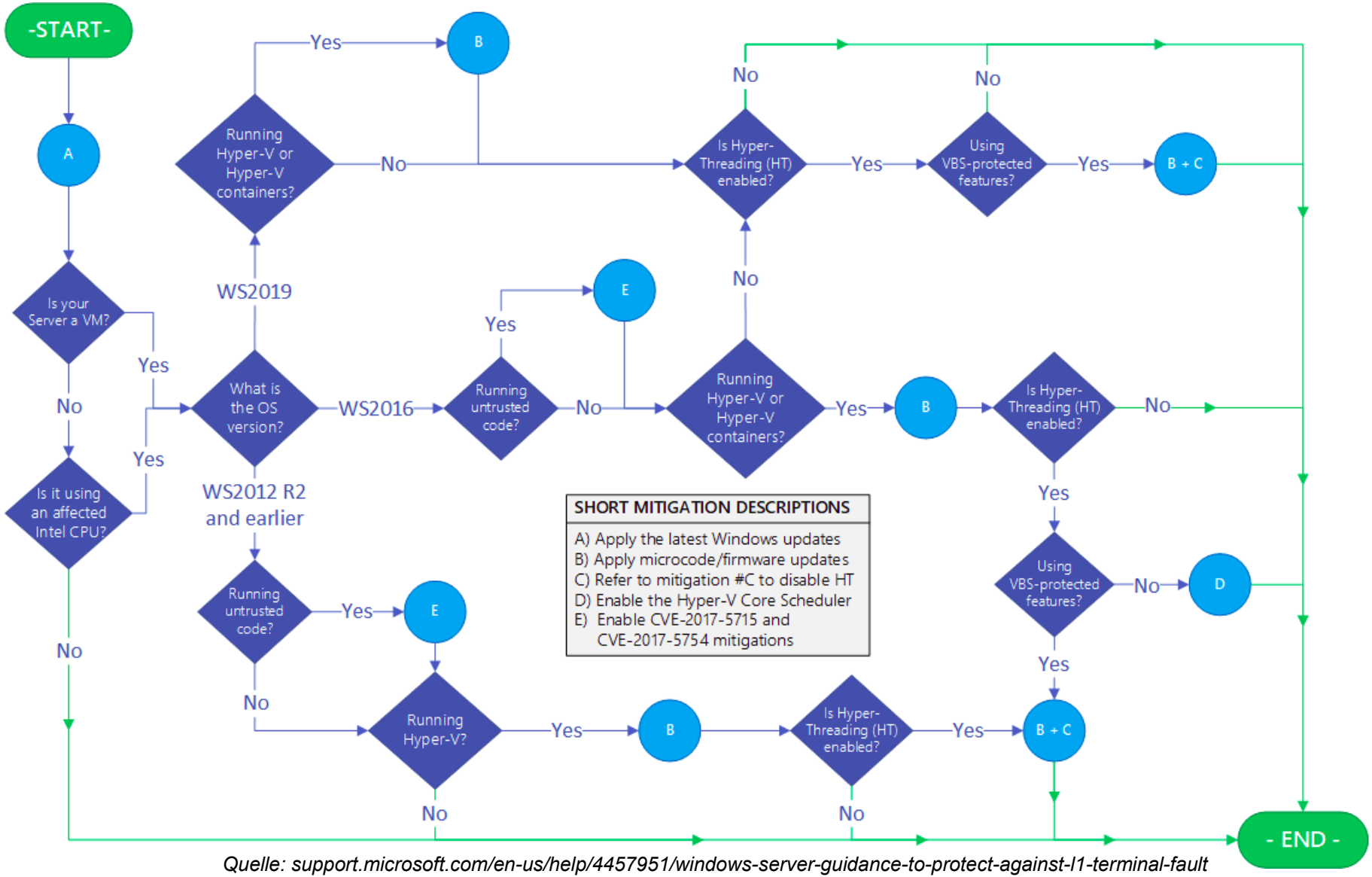
| Spectre and Meltdown on Intel | | | | | | | |
|---|---|---|---|---|---|---|---|
| *AnandTech* | | | SKX-R 3175X | CFL-R | Cascade Lake | Whiskey Lake | Amber Lake |
| **Spectre** | **Variant 1** | **Bounds Check Bypass** | OS/VMM | OS/VMM | OS/VMM | OS/VMM | OS/VMM |
| **Spectre** | **Variant 2** | **Branch Target Injection** | Firmware + OS | Firmware + OS | Hardware + OS | Firmware + OS | Firmware + OS |
| **Meltdown** | **Variant 3** | **Rogue Data Cache Load** | Firmware | **Hardware** | Hardware | Hardware | Firmware |
| **Meltdown** | **Variant 3a** | **Rogue System Register Read** | Firmware | Firmware | Firmware | Firmware | Firmware |
| | **Variant 4** | **Speculative Store Bypass** | Firmware + OS | Firmware + OS | Firmware + OS | Firmware + OS | Firmware + OS |
| | **Variant 5** | **L1 Terminal Fault** | Firmware | **Hardware** | Hardware | Hardware | Firmware |

*Quelle: anandtech.com*

# L1 Terminal Fault

- SGX gibt es nur bei Intel CPUs → AMD nicht betroffen
- L1TF = 1 Name für 3 Lücken
  - CVE-2018-3615 („Foreshadow“) - Intel Software Guard Extensions (Intel SGX)
    - Microcode Update von Intel, OS braucht keine Updates
  - CVE-2018-3620 – Betriebssystem und System Management Mode (SMM)
    - OS Update notwendig
  - CVE-2018-3646 – nur für Virtualisierung relevant
    - Microcode und OS Update notwendig plus weitere Konfiguration
- CVE-2018-3646 unter Linux
  - L1 Data Cache Flushing kann konfiguriert werden
    - default: Cache Flush in speziellen Situationen
    - immer: großer Performance Impact
    - nie
  - CPUS mit Hyper-Threading zusätzlich gefährdet
    - Voller Schutz vor Hyper-Thread basierten Angriff bei VMs
      - Hyperthreading abdrehen ODER
      - VM Gäste auf CPU Core fixieren, welcher nicht mit Host oder Gast geteilt wird

# CVE-2018-3646 unter Windows




*Quelle: support.microsoft.com/en-us/help/4457951/windows-server-guidance-to-protect-against-l1-terminal-fault*

# L1TF und VMware

- CVE-2018-3620: Updates für Virtual Appliances
- CVE-2018-3646:
  - Sequential-context attack vector: automatisch aktiviert mit Update
  - Concurrent-context attack vector: SCA-Scheduler muss manuell aktiviert werden
- SCA-Scheduler („Side-Channel-Aware“)
  Vmkernel.Boot.hyperthreadingMitigation
- Performanceverluste stark abhängig von CPU-Gesamtlast
  - Bsp:
    Gesamtlast 62 % → 1 % Verluste
    Gesamtlast 90 % → 32 % Verluste
- HTAware Mitigation Tool für Evaluierung
  https://kb.vmware.com/s/article/56931

**Mögliche Performanceverluste durch den SCA-Scheduler laut VMware-Labor**

| Anwendungs-Workload/Gast-OS | Performanceeinbußen nach Aktivieren des SCA-Scheduler |
|---|---|
| Datenbank OLTP/Windows | 32 % |
| Datenbank OLTP/Linux (mit vSAN) | 32 % |
| gemischte Workloads/Linux | 25 % |
| Java/Linux | 22 % |
| VDI/Windows | 30 % |

**Tabelle: Mögliche Performanceverluste durch den SCA-Scheduler laut VMware-Labor**

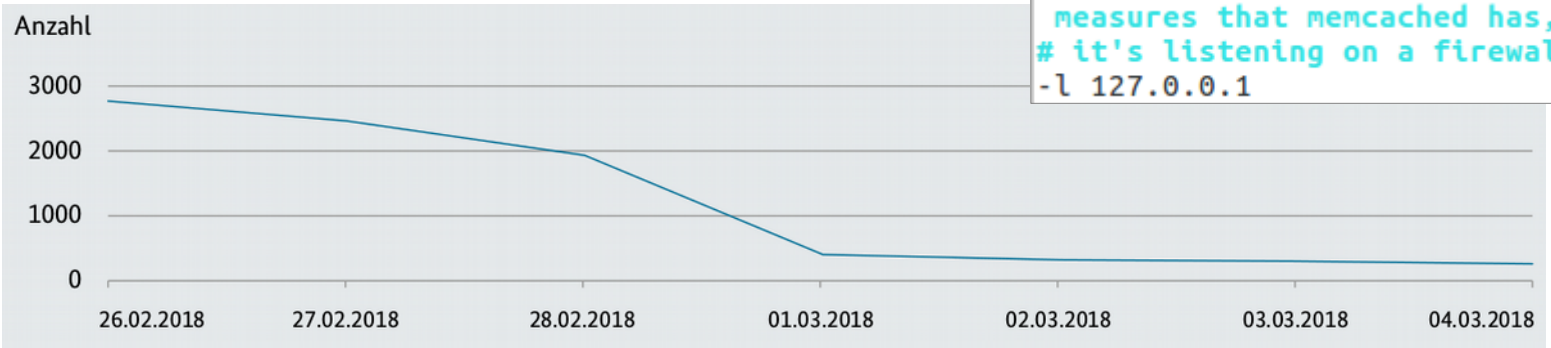
**In voll ausgelasteten Umgebungen kann es nach der Aktivierung des SCA-Scheduler zu erheblichen Leistungseinbußen kommen.**

*Quelle: www.heise.de/select/ix/2018/10/1538797683833455*

# Memcached Amplification

- seit Anfang 2018 Angriffe
- Distributed-Reflected-Denial-of-Service (DRDoS)
- via UDP (Port 11211) offen im Internet
- bis Version 1.5.5 mit Default-Einstellungen
- Verstärkungsfaktor 51.000 (normal ~50)
- neuer Rekord: 1,7TBit/s

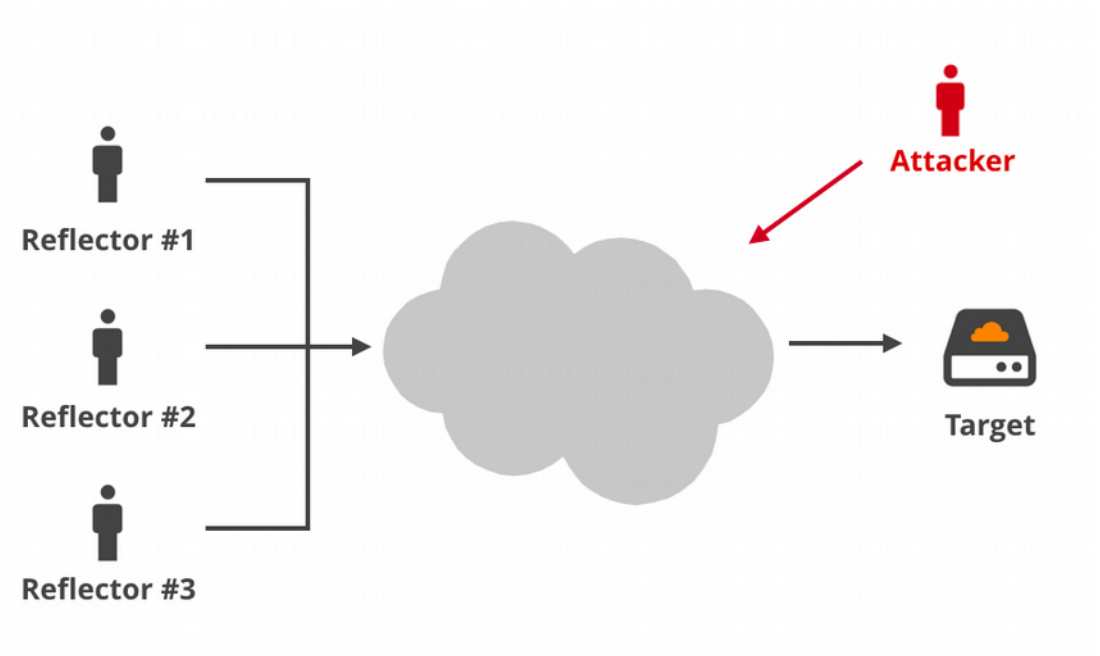
```
# Specify which IP address to listen on. The
 default is to listen on all IP addresses
# This parameter is one of the only security
 measures that memcached has, so make sure
# it's listening on a firewalled interface.
-l 127.0.0.1
```




*Quelle: bsi.de*
*Lagebericht IT-Sicherheit 2018*

# Memcached Amplification

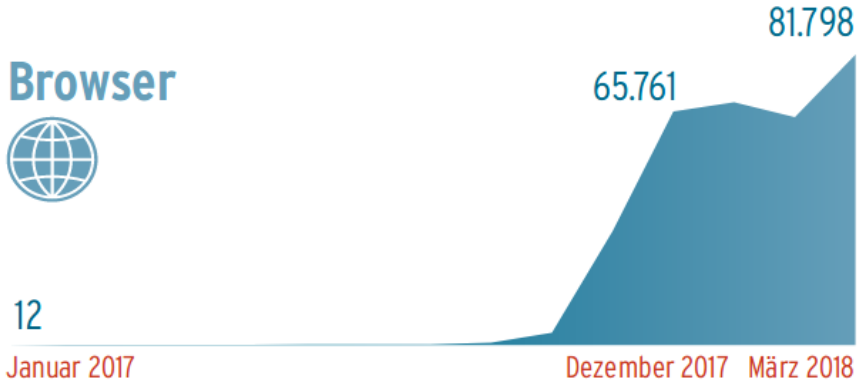
- Firewall hilft ;)
- IP Spoofing notwendig, ist generelles Problem




*Quelle: av-test.org, AV-TEST_Sicherheitsreport_2017-2018*

# Krypto Mining

- Rechenleistung missbraucht (auch IoT und Server)
- Mining via Javascript im Browser oder via Malware (Krypto-Currency-Mining-Malware)
- Popularität durch schlechten Bitcoin-Kurs gebremst
- Alternativ werden Krypto-Wallets gestohlen



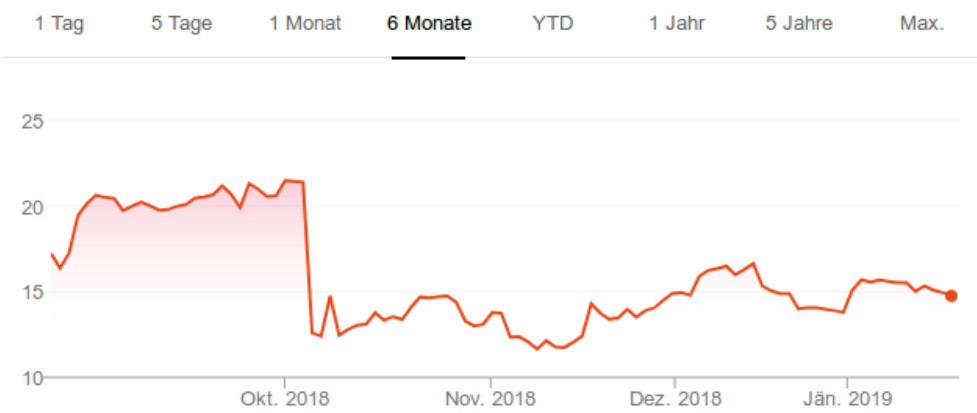

*Quelle: av-test.org, AV-TEST_Sicherheitsreport_2017-2018*

# Supermicro Spionage Chip

- Bloomberg Bericht über manipulierte Supermicro Hardware

**Appleboum said one key sign of the implant is that the manipulated Ethernet connector has metal sides instead of the usual plastic ones. The metal is necessary to diffuse heat from the chip hidden inside, which acts like a mini computer. "The module looks really innocent, high quality and 'original' but it was added as part of a supply chain attack," he said.**

- Keine weiteren Beweise bekannt geworden
- evtl. war BMC oder RMM gemeint?
- Tim Cook hat von Bloomberg Widerruf gefordert, Amazon ebenfalls dementiert
- Supermicro hat 3rd Party Audit durchführen lassen



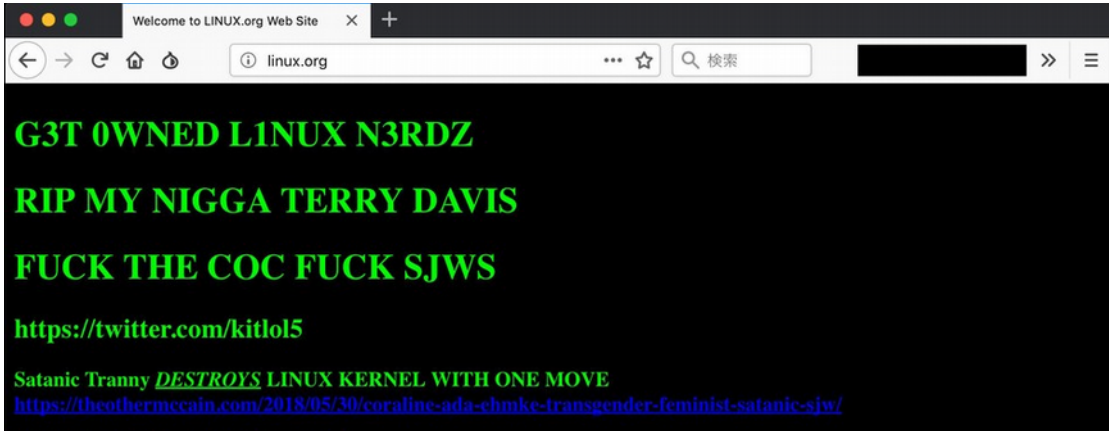

*Quelle: google.at*

# DNS Hijacking / Defacement

- Anfang Dezember wurde www.linux.org übernommen

  **"I think it was a combination of public whois info and no MFA that lead to this," one of the Linux.org admins explained on Reddit.**

- IP wurde im DNS geändert
- → Multifaktor-Auth (MFA) aktivieren für DNS/Domain-Verwaltung




*Quelle: https://motherboard.vice.com/en_us/article/59vkq8/linuxorg-website-defacement-goatse*

# Update: BSI warnt vor Emotet und empfiehlt Schutzmaßnahmen

**Datum** 14.01.2019

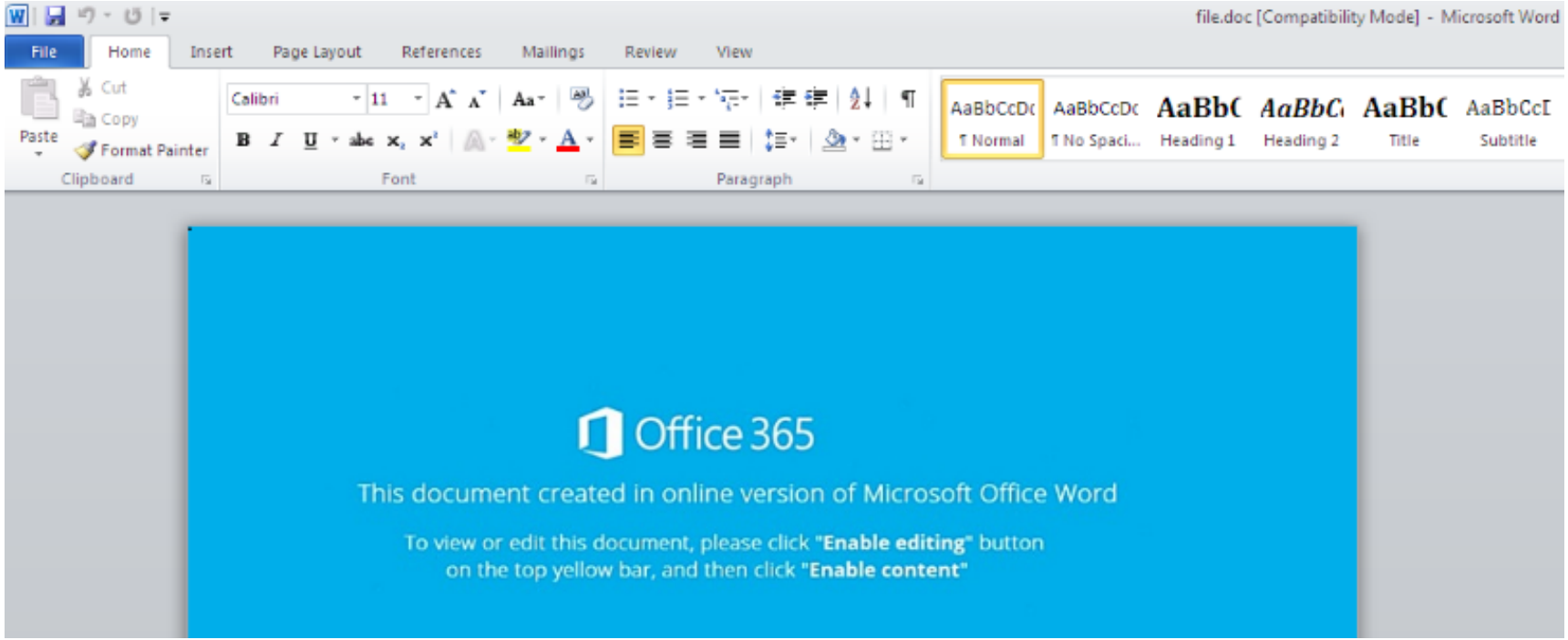
Nach einer Beruhigung während der Weihnachtsfeiertage beobachtet das **BSI** seit dem 14. Januar eine erneute massenhafte Versendung von Spam im Zusammenhang mit der Schadsoftware Emotet. Über Emotet kann unterschiedliche Schadsoftware nachgeladen werden. Häufig sind dies Bankingtrojaner wie Trickbot und in der Folge immer häufiger auch die Ransomware Ryuk.

Das **BSI** weist darauf hin, dass Standard-Antivirenprogramme die Schadsoftware häufig nicht erkennen. Unternehmen, Behörden und Institutionen sollten sich daher unbedingt über die Gefahren durch Emotet informieren. Eine umfangreiche Übersicht über Maßnahmen zum Schutz vor Emotet und Empfehlungen zur Reaktion im Falle einer erfolgten Infektion finden Sie auf den Seiten der Allianz für Cyber-Sicherheit.



*Quelle: www.bsi.de*

# Emotet






*Quelle: www.welivesecurity.com/wp-content/uploads/2018/11/Figure5.png*

# Emotet

- APT-Angriffe automatisiert
- Authentische Nachrichten durch „Outlook-Harvesting“
- Kontaktbeziehungen und E-Mail Inhalte ausgelesen
- Schadsoftware kann nachgeladen werden
  → aktuell Banking-Trojaner „Trickbot“ nachgeladen
  → durch Auslesen von Zugangsdaten und SMB-Schwachstellen (Eternal Blue/Romance) Ausbreitung im Netzwerk
- Wegen laufender Anpassungen oft unerkannt von Antivirus Software
- Bereinigung von Systemen meist erfolglos

# Was kann man tun?

- Sensibilisierung der Nutzer für Anhänge und Links
  auch bei bekannten Absendern
  → ggf. beim Absender nachfragen mit anderem Kommunikationskanal
- Backup, auch offline
- Netzwerk-Segmentierung, Benutzerrechte einschränken
- Makros generell deaktivieren, alternativ nur signierte erlauben
- Multifaktor Auth hilft gegen ausgespähte Zugangsdaten
- E-Mail Signatur und Verschlüsselung würde Abhilfe schaffen
- Updates, Updates, Updates…
- Umfassende Infos im FAQ vom BSI:
  https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Micro/E-Mailsicherheit/emotet.html

# Phishing

- wird immer professioneller
- Bsp: gefälschtes BSI-Email inkl. gefälschter Webseite
- Multi-Factor Auth für externe Dienste sinnvoll (VPN, Webmail)

**Kritische Sicherheitslücke - Wichtiges Update**

11. Januar 2018 6:51 nachm.

Von "Bundesamt für Sicherheit i. d. Informationstechnik" <admin@moneycomputing.com>

An [redacted]

Bundesamt für Sicherheit in der Informationstechnik

**Informationen zum Sicherheitsupdate**

Guten Abend,

wir müssen Sie davon in Kenntnis setzen, dass auf Grund der kürzlich bekannten kritischen Sicherheitslücken "Meltdown" und "Spectre" Ihr Endgerät angreifbar ist.

Das Bundesamt für Sicherheit in der Informationstechnik hat in Zusammenarbeit mit den Prozessorenherstellern AMD und Intel ein wichtiges Sicherheitsupdate entwickelt.

Wir sind gem. der geltenden Gesetze dazu verpflichtet, Sie über diesen Umstand zu informieren und Ihnen **dringend zu raten** das bereitgestellte Sicherheitsupdate zu installieren, um weiterhin vor externen Angriffen und Missbrauch geschützt zu sein.

Zum Sicherheitsupdate: **Hier**

Für weiter Informationen rund um das Thema Meltdown/Spectre finden Sie auf unseren Internetseite.

Für weitere Fragen bezügl. Ihrer Sicherheit im Netz nutzen Sie bitte unser Kontaktformular unter www.bsi-fuer-buerger.de.

Diese E-Mail wurde automatisch erstellt und individualisiert. Bitte antworten Sie nicht auf diese.

© Bundesamt für Sicherheit in der Informationstechnik

LEICHTE SPRACHE GEBÄRDENSPR

Bundesamt für Sicherheit in der Informationstechnik

Risiken Empfehlungen

Service

## Kritisches Sicherheitsupdate: Spectre und Meltdown

Prozessoren verschiedener Hersteller weisen gravierende und schwer zu behebende Sicherheitslücken auf, wie Sicherheitsforsche von Google Project Zero und der Technischen Universität Graz aufgezeigt haben. Die gefundenen Schwachstellen, die als "Spectre" und "Meltdown" bezeichnet werden, ermöglichen das Auslesen von sensiblen Speicherinhalten des Computers. Das Bundesamt für Sicherheit in der Informationstechnik rat zwingend dazu das Sicherheitsupdate umgehend zu installieren.

### Wie können Systeme kurzfristig geschützt werden?

Das Bundesamt für Sicherheit in der Informationstechnik bietet in Zusammenarbeit mit den Chipherstellern Intel und AMD eine schnelle Softwarelösung an, um die Lücken vor externen Missbrauch zu schützen. Für die meisten Einsatzszenarien auf einem PC oder Smartphone schließt das Sicherheitsupdate alle kritischen Lücken. Es ist zwingend notwendig, dieses Update zu installieren, um weiterhin Ihr Endgerät vor externen Angriffen zu schützen.

#### Updates zum Schließen der Lücken:

Das Sicherheitsupdate sollte umgehend auf allen normalen PCs installiert werden. Alle gängigen Windows Betriebssysteme werden unterstützt.

Microsoft Windows:

Bitte laden Sie sofort das Sicherheitsupdate herunter und installieren Sie dieses:

Link zum Herunterladen: **Hier**

**Die Installation findet im Hintergrund statt und schließt umgehend alle beschriebenen Lücken**

**Unter Umständen kann es vorkommen, dass verschiedenen Antivirenprogramme fälschlicherweise ausschlagen, dies resultiert dadurch, dass das Sicherheitsupdate Lücken innerhalb der Prozessoren Architektur schließt. Wir raten dazu Ihr Antivirenprogramm für das Update kurzzeitig zu pausieren!**

From Facebook <yardgen@gmail.com>

Reply | Forward | Junk | Delete | More

Subject **Did you log into Facebook from somewhere new?** 9/6/14, 7:34 AM

To tty198410@gmail.com

## Did you log into Facebook from somewhere new?

Dear [redacted],

Your Facebook account was recently logged into from a computer, mobile device or other location you've never used before. For your protection, we've temporarily locked your account until you can review this activity and make sure no one is using your account without your permission.

Did you log into Facebook from a new device or an unusual location?

If this was not you, please log into Facebook from your computer and follow the instructions provided to help you control your account information.

If this was you, there's no need to worry. Simply log into Facebook again to get back into your account.

**Log In**

Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

http://www.fancug.com/link/facebook_en.html Today Pane

Google Drive

https://googledrive.com/host/0B9w_QaGzABUaUHpv

Google

One account. All of Google.

Sign in to continue to Google Drive

Email

Password

Sign in

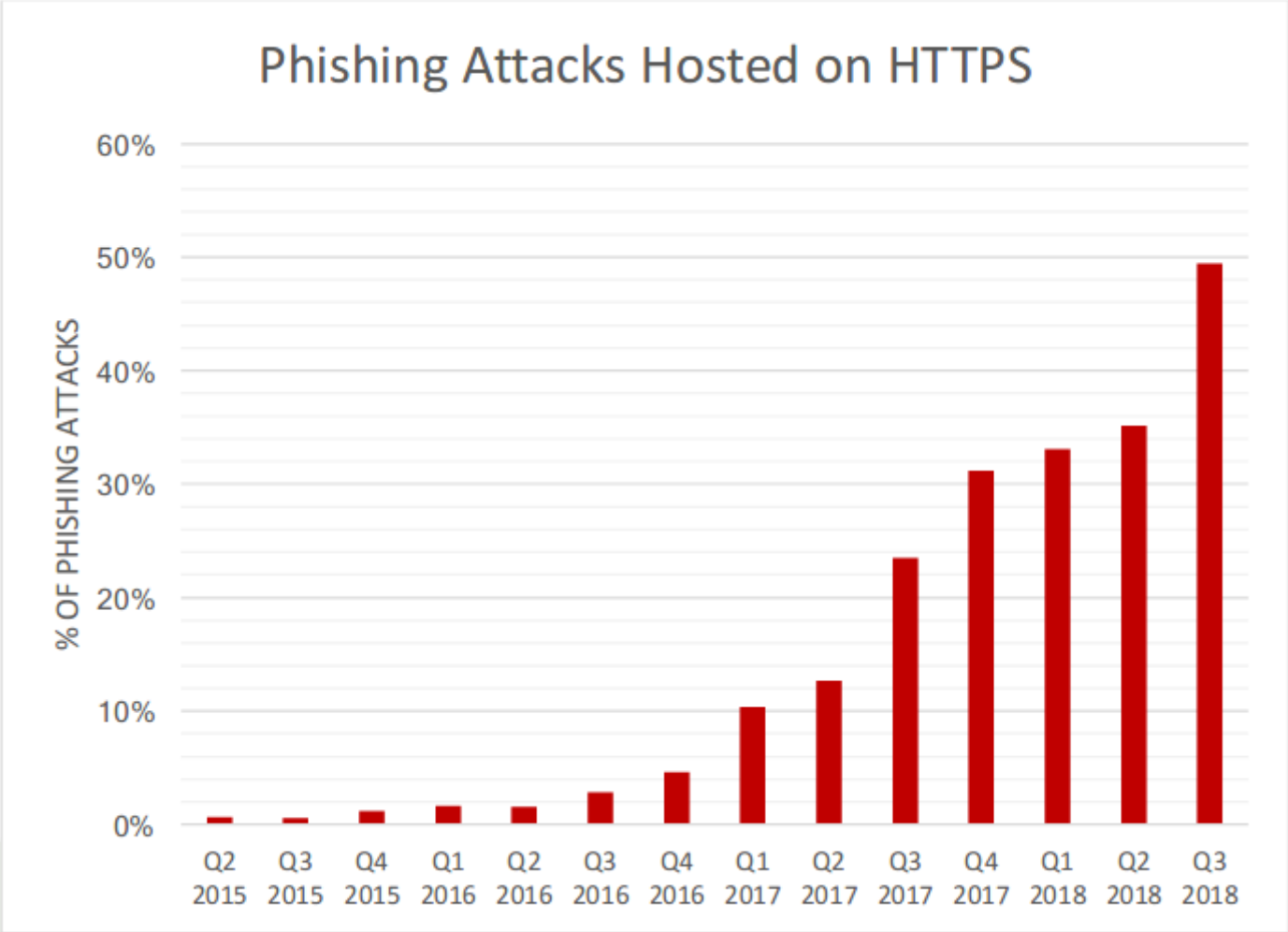
Stay signed in Need help?

Create an account

One Google Account for everything Google

Google Privacy & Terms Help ?English (United States)?

Quelle: www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays

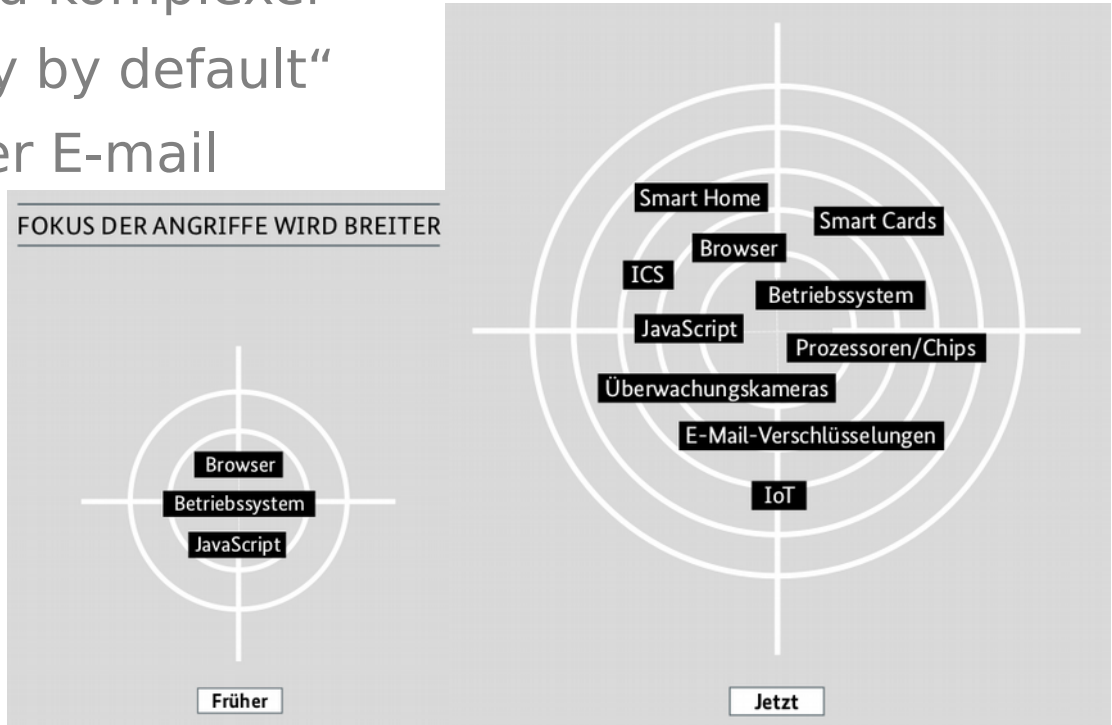





*Quelle: docs.apwg.org/reports/apwg_trends_report_q3_2018.pdf*

# Ausblick 2019

- „Problem liegt in der Kombination von wachsender Gefährdung mit zunehmender Abhängigkeit von IT“
- Angriffe werden vielfältiger und komplexer
- „security by design“ - „security by default“
- Phishing zukünftig nicht nur per E-mail
- Wachstum IoT / Smart Home
- Cloud Sicherheit
- Tipp: Kostenlos Mitglied bei der Allianz für Cyber-Sicherheit vom BSI werden
  https://www.allianz-fuer-cybersicherheit.de




*Quelle: bsi.de*
*Lagebericht IT-Sicherheit 2018*

# Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®