



ZiM

Zentrum für
Informations- und
Mediendienste

EUROPÄISCHER
MONAT
DER CYBER-
SICHERHEIT

UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

Phishers Fritze phisht...

über kuriose Schreibweisen und (Un)sicherheit in der digitalen Welt



Dr. Marius Mertens ■ 20.10.2017, 14:00 Uhr

- **Einleitung: IT-Sicherheit**
- **Aktuelle Angriffe und Sicherheitsvorfälle**
- **Warum ist das alles so unsicher?**
- **Gegenmaßnahmen**



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

■ Einleitung: IT-Sicherheit

- **Anwendbar auf jegliche Art von Information – nicht nur elektronische Daten**
- **Anwendbar auf Speicherung und Transport von Informationen**
- **Eigenschaften gewährleistet → Wir nennen es „sicher“**
- **Eigenschaften gefährdet → Wir nennen es „unsicher“**

Vertraulichkeit
Verfügbarkeit
Integrität

- **Informationen können nur von Berechtigten eingesehen werden**
- **Vertraulichkeit gewährleisten:**
 - Physikalischer Zugriffsschutz
 - Verschlüsselung
- **Auswirkungen nicht gewährleisteter Vertraulichkeit**
 - Persönliche Daten werden bekannt
 - Zugangsdaten können unbefugt verwendet werden
 - Verletzung der Vertraulichkeit ist im Nachhinein praktisch nicht zu korrigieren: Einmal verbreitete Information kann nicht entfernt werden

- **Information ist vorhanden und einsehbar**
- **Verfügbarkeit gewährleisten**
 - Daten mehrfach ablegen und regelmäßig sichern
 - Sicherung überprüfen
 - Ersatzgeräte für den Zugriff bereithalten
 - Transportverfügbarkeit: Redundante Pfade → Internet
- **Auswirkungen nicht gewährleisteter Verfügbarkeit**
 - Temporär: Geschäftsprozesse werden verhindert oder verlangsamt
 - Permanent: Wichtige Informationen sind für immer verloren und können nur mit großem Aufwand oder gar nicht neu erarbeitet werden → Private Fotos, Diplomarbeit

Dieses Risiko lässt sich durch eine ordentliche Datensicherung fast vollständig ausschließen!

- **Information ist unverändert abrufbar wie zuvor abgelegt**
- **Integrität gewährleisten**
 - Mehrfache Speicherung und Vergleich
 - Archive mit Prüfsummen und Wiederherstellungsinformationen
 - Kryptographische Signaturen
- **Auswirkungen nicht gewährleisteter Integrität**
 - Der Information kann beim Abruf nicht vertraut werden
 - Beschädigung kann zu Unlesbarkeit führen
 - Mutwillige Verfälschung kann weitere Auswirkungen haben
 - Information mit nicht gewährleisteter Integrität ist ähnlich wie nicht verfügbare Information



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

- **Aktuelle Angriffe und Sicherheitsvorfälle**

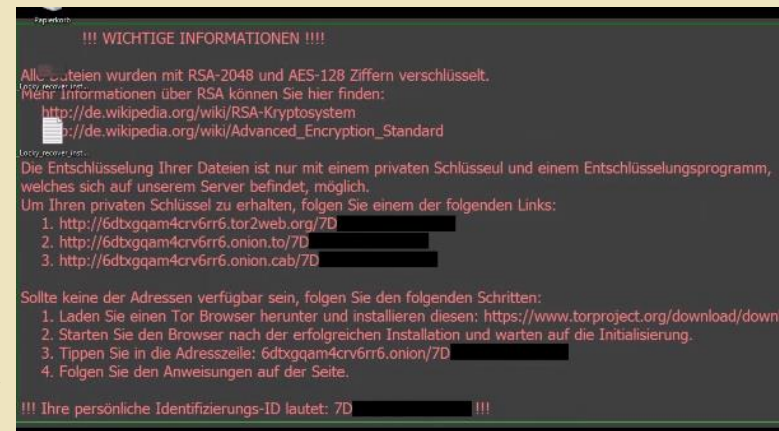
- **Juni 2010**
- **Gezielter und ausgefeilter Angriff auf iranische Zentrifugensteuerungen**
- **Ausnutzung damals unbekannter Sicherheitslücken**
- **Verbreitung per LAN und USB-Stick**
- **Diskretes Vorgehen: Infektionszähler und Löschung des Programms nach einer bestimmten Anzahl Infektionen**
- **Sehr spezifische Schadroutine: Angriff auf Siemens Simatic S7 Anlagensteuerung**
- **Kommunikation mit dem Internet per HTTP-GET**

- April 2014 (veröffentlicht, Fehler bestand schon seit über zwei Jahren)
- Eigene Website: heartbleed.com und Logo:
- Bug in der Implementierung der Heartbeat-Funktion von OpenSSL erlaubt „ausbluten“ von Informationen aus dem Speicher
- Unberechtigter Fernzugriff auf Serverschlüssel, Zugangsdaten, etc. möglich
- Fehlerbehebung durch Serverbetreiber: Einspielen der korrigierten Version 1.0.1g von OpenSSL
- Effekt für den Nutzer: Alle Verbindungen zu betroffenen Servern sind als unverschlüsselt anzusehen → Ändern aller Kennwörter
- ZIM: Infoseiten und Mail-Benachrichtigung
<https://www.uni-due.de/zim/services/sicherheit/heartbleed-bug.php>
<https://www.uni-due.de/zim/services/sicherheit/heartbleed-hinweise.php>

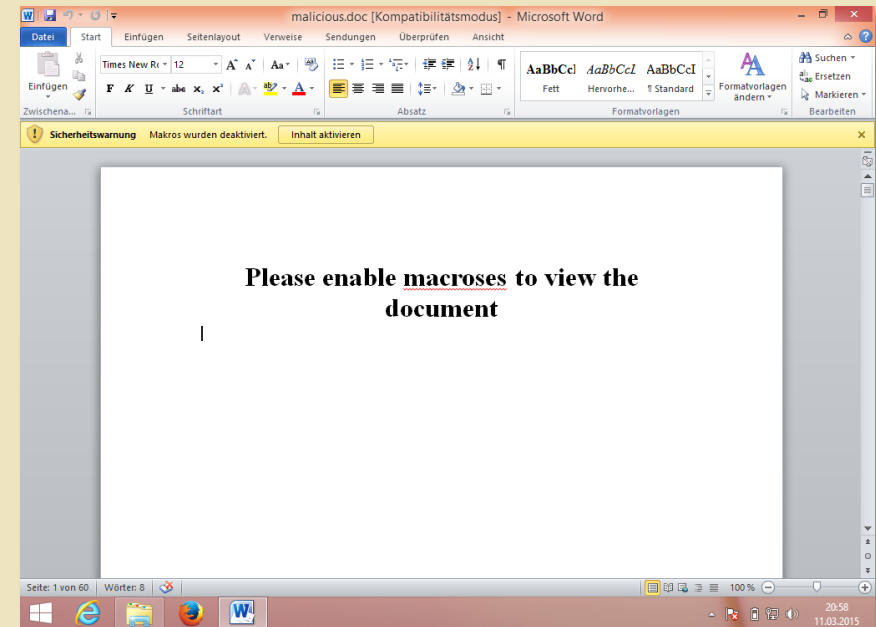
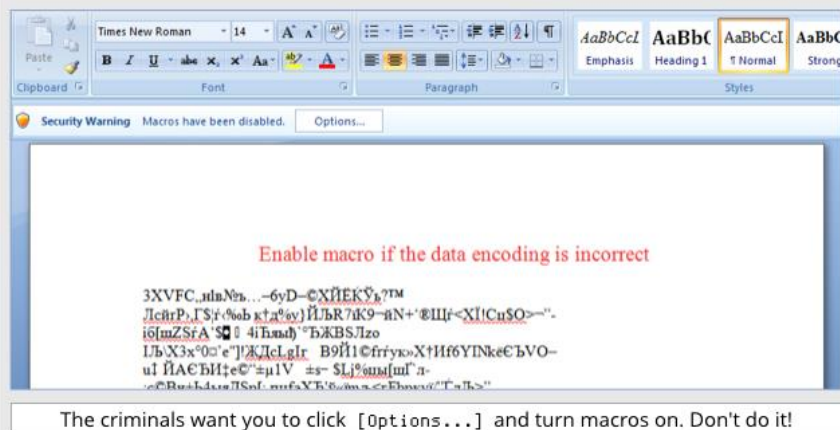


- Februar 2016, Ransomware-Angriff „Verschlüsselungstrojaner“
- Verbreitung über Makros in Office-Dokumenten sowie gepackte .js-Skripte
- Effekt für den Nutzer: Verschlüsselung persönlicher Daten bei Infektion, Entschlüsselung nur gegen Lösegeld
- Benötigt (aktuell) zur Ausführung die aktive Mithilfe des Nutzers. Abhilfe: Makros deaktivieren (Standardeinstellung) und nicht manuell aktivieren, bloß weil man dazu aufgefordert wird.
- ZIM: Informationen zu Verschlüsselungstrojanern und Prävention
<https://www.uni-due.de/zim/services/sicherheit/verschluesselungstrojaner.php>

Quelle: <https://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html>



Quelle: <https://nakedsecurity.sophos.com/2016/02/17/locky-ransomware-what-you-need-to-know/>

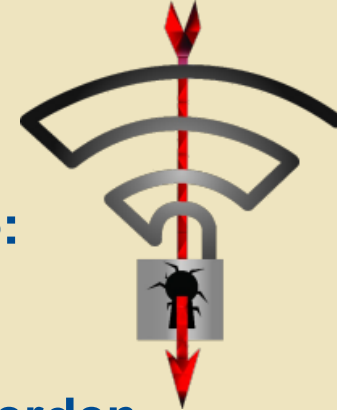


Quelle: <https://www.heise.de/security/artikel/Analysiert-Das-Comeback-der-Makro-Malware-2573181.html>

- Mai 2017 großflächiger Ransomware-Angriff „Verschlüsselungs-Trojaner“
- Strings WANACRY, wnry, Wncry an diversen Stellen verwendet
- Verbreitung als Wurm via EternalBlue Exploit
- EternalBlue wurde zuvor mindestens 5 Jahre lang von der NSA verwendet
- Fehlerbehebung durch Patch MS17-010 für Microsoft CIFS (Seit März 2017 per Windows Update verteilt)
- Effekt für den Nutzer: Verschlüsselung persönlicher Daten bei Infektion, Entschlüsselung nur gegen Lösegeld
- ZIM: Informationen zu Verschlüsselungstrojanern und Prävention
<https://www.uni-due.de/zim/services/sicherheit/verschluesselungstrojaner.php>

**Es gibt zwei Arten von
Daten: Gesicherte Daten
und unwichtige Daten**

- Oktober 2017
- Key Reinstallation AttaCK
- Mit Website www.krackattacks.com und Logo:
- Angriff auf die Implementierung vom WPA2
- Betroffene Clients/APs können gezwungen werden, Sitzungsschlüssel wiederzuverwenden
- Das Verschlüsselungsverfahren selbst ist weiterhin sicher
- Effekt für den Nutzer: Updates einspielen (bis auf Android 6.0 bereits für alle verbreiteten Systeme verfügbar)



Kryptographie-Grundlage: Niemals mehrere Klartexte mit demselben Schlüssel(strom) verschlüsseln

Quelle: <https://www.kb.cert.org/vuls/id/CHEU-AQNMYP>

Microsoft Corporation Information for VU#228519
 Wi-Fi Protected Access II (WPA2) handshake traffic can be manipulated to induce nonce and session key reuse

Date Notified: 28 Aug 2017 Vendor Information Help
 Statement Date: 16 Okt 2017
 Date Updated: 16 Oct 2017

Status
 Affected

Vendor Statement
 Microsoft released a security update on October 10, 2017, and customers who have Windows Update enabled and applied the security updates, are protected automatically.

Vendor Information
 CVE-2017-13080 describes this vulnerability in affected Microsoft products.

Vendor References
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080>

Vendor Information
 We are not aware of further vendor information regarding this vulnerability.

Vendor References
<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080>

Addendum
 There are no additional comments at this time.
 If you have feedback, comments, or additional information about this vulnerability, please send us email.

For the oldstable distribution (jessie), these problems have been fixed in version 2.3-1+deb8u5.

For the stable distribution (stretch), these problems have been fixed in version 2:2.4-1+deb9u1.

For the testing distribution (buster), these problems have been fixed in version 2:2.4-1.1.

For the unstable distribution (sid), these problems have been fixed in version 2:2.4-1.1.

We recommend that you upgrade your wpa packages.

Quelle: <https://www.debian.org/security/2017/dsa-3999>

802.11r Vulnerability (CVE: 2017-13082) FAQ

Overview

On October 16th, 2017, ten new security vulnerabilities (referred as **Key Reinstallation Attack** or **KRACK**) were announced that target the session establishment and management process in WPA(1/2)-PSK and WPA(1/2)-Enterprise. Of the ten vulnerabilities, Meraki access points (AP) are only affected by one (CVE: 2017-13082). Our engineering team has already made the fix available as part of the latest available firmware (i.e. firmware versions MR 24.11 and MR 25.7). For an overview of how Meraki helped its customers, please refer to our [blog](#). For any additional information, please refer to this FAQ page.

Table of contents

1. Overview
2. Impact Assessment
3. Additional Information

This is the first time a security vulnerability has been found with the WPA key installation process since its introduction. The security vulnerability targets the 4-way Handshake, Group rekey Handshake, 802.11r Fast-BSS Transition(FT), and Peer-Key Handshake. Using these vulnerabilities an attacker can force a client or access point (AP) to reinstall the keys used to encrypt wireless data. Depending on targeted frames, either a client or an AP is affected as shown in the table below. The CVEs have been assigned based on the type of frames targeted.

Type of Attack	CVE IDs	Devices Impacted
4-way Handshake	2017-13077	Wi-Fi clients
Group-Key Handshake	2017-13078/2017-13079/2017-13080/2017-13081/2017-13087/2017-13088	Wi-Fi clients
802.11r Fast-BSS Transition(FT)	2017-13082	Access Points
Peer-Key Handshake	2017-13084/2017-13086	Wi-Fi clients

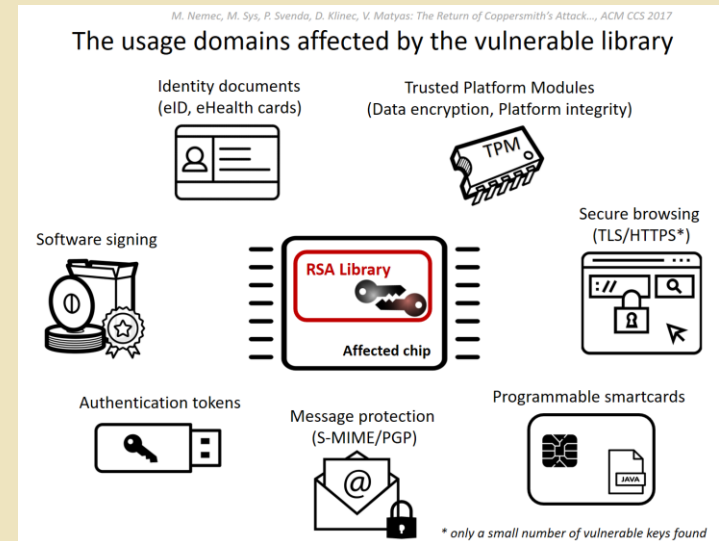
Using these vulnerabilities an attacker can either replay, decrypt or forge packets depending on the data integrity protocol used. The table below gives a summary of the type of attack and the direction of traffic flow that is affected.

	Data Integrity Protocol	Replay	Decrypt	Forge
4-way//Peer-Key Handshake	WPA1 (TKIP)	AP → Client	Client → AP	Client → AP
	WPA2* (CCMP)	AP → Client	Client → AP	N/A
Group Key Handshake	WPA1 (TKIP)	AP → Client	N/A	N/A
	WPA2* (CCMP)	AP → Client	N/A	N/A
802.11r Fast-BSS Transition(FT)	WPA1 (TKIP)	Client → AP	AP → Client	AP → Client
	WPA2* (CCMP)	Client → AP	AP → Client	N/A

*CCMP is the mandatory data integrity protocol in WPA2 but TKIP can be optionally supported.

Quelle: [https://documentation.meraki.com/zGeneral_Administration/Support/802.11r_Vulnerability_\(CVE%3A_2017-13082\)_FAQ](https://documentation.meraki.com/zGeneral_Administration/Support/802.11r_Vulnerability_(CVE%3A_2017-13082)_FAQ)

- Oktober 2017: Erste Veröffentlichung
- Return of Coppersmith's Attack: Faktorisierung von RSA-Schlüsseln mit bekannten Bits
- Angriff auf schlechte Implementierung in Infineon-RSA-Bibliothek
- RSA selbst ist weiterhin nicht gebrochen
- Effekt für Anwender: Yubikey, Bitlocker (per TPM Chip)
- Abhilfe: Neue RSA-Schlüssel auf anderem Weg generieren

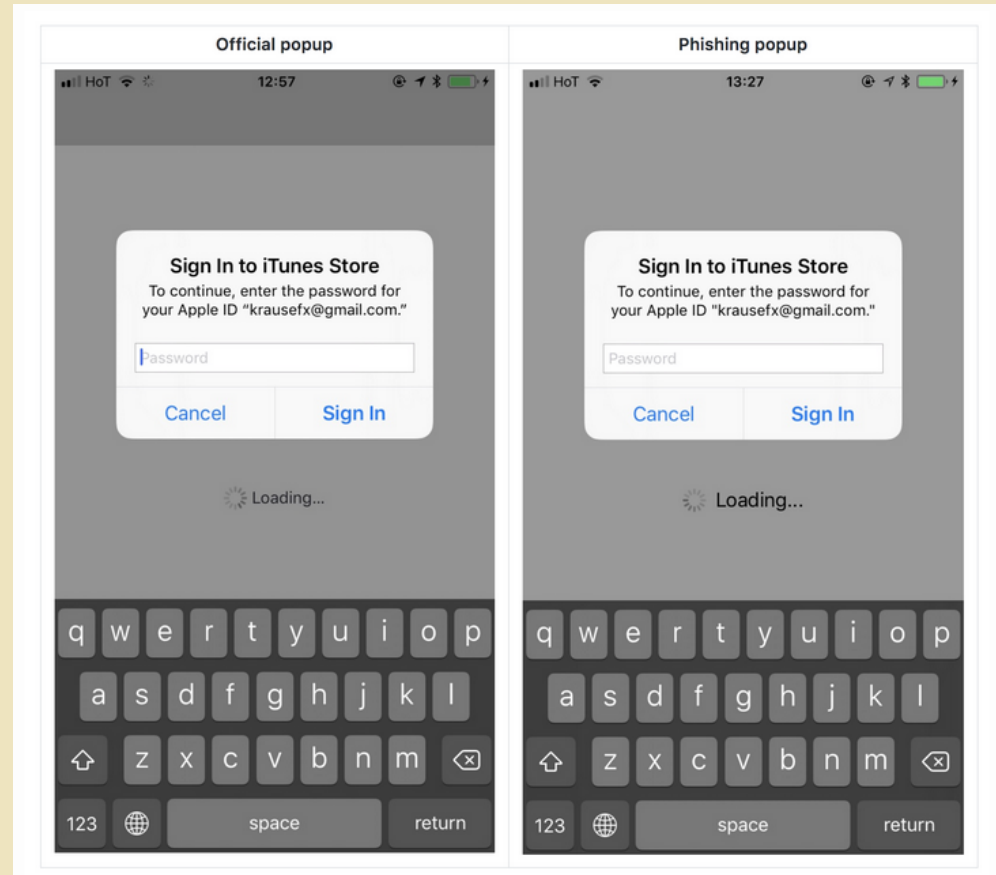


Updates

- 2nd of November 2017 - Presentation of all details at the ACM CCS conference (to come)
- 16th of October 2017 - The initial version of the public disclosure published
- May to October 2017 - Cooperation with the manufacturer and other affected parties to help evaluate and mitigate the vulnerability
- 1st of February - The vulnerability disclosed to Infineon Technologies AG
- End of January - The vulnerability found

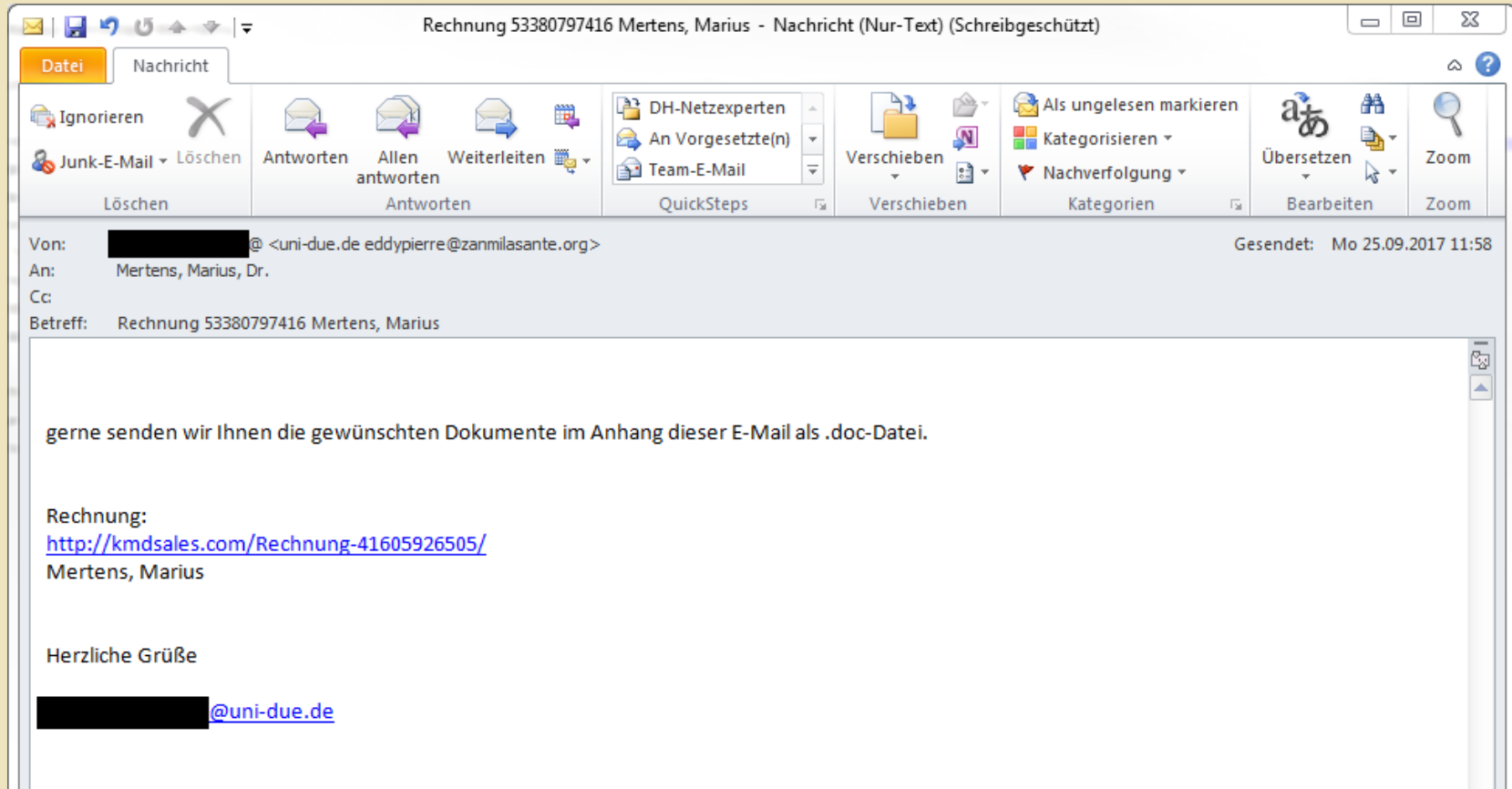
Quelle: https://crocs.fi.muni.cz/public/papers/rsa_ccs17

■ Oktober 2017: Klassisches Password fHISHING



Quelle: <https://krausefx.com/blog/ios-privacy-stealpassword-easily-get-the-users-apple-id-password-just-by-asking>

■ September 2017



Rechnung 53380797416 Mertens, Marius - Nachricht (Nur-Text) (Schreibgeschützt)

Datei Nachricht

Ignorieren, Junk-E-Mail, Löschen, Antworten, Allen antworten, Weiterleiten, DH-Netzexperten, An Vorgesetzte(n), Team-E-Mail, Verschieben, Als ungelesen markieren, Kategorisieren, Nachverfolgung, Übersetzen, Zoom

Von: [REDACTED] <uni-due.de eddypierre@zanmilasante.org> Gesendet: Mo 25.09.2017 11:58
An: Mertens, Marius, Dr.
Cc:
Betreff: Rechnung 53380797416 Mertens, Marius

gerne senden wir Ihnen die gewünschten Dokumente im Anhang dieser E-Mail als .doc-Datei.

Rechnung:
<http://kmdsales.com/Rechnung-41605926505/>
Mertens, Marius

Herzliche Grüße
[REDACTED]@uni-due.de

Nicht vertrauenswürdige Mail



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

■ August 2016

The screenshot shows an Outlook window titled 'Datenergänzung [REDACTED] - Nachricht (Nur-Text)'. The ribbon includes 'Datei', 'Nachricht', and 'QuickSteps'. The email content is as follows:

Sie haben diese Nachricht am 01.08.2016 08:32 weitergeleitet.
Diese Nachricht wurde zum Nur-Text-Format konvertiert.

Von: [REDACTED]
An: Mertens, Marius, Dr.
Cc:
Betreff: Datenergänzung [REDACTED]

Nachricht [REDACTED].jsm (86 KB)

Sehr geehrter Herr [REDACTED]

aufgrund des [REDACTED] melden. Daher bitten wir Sie, das anhängende Erfassungsformular auszufüllen und an uns zurückzusenden.

Bitte befolgen Sie folgende Vorgehensweise (siehe auch Kurzanleitung <[https://\[REDACTED\].pdf](https://[REDACTED].pdf)>):

1. Speichern Sie die anhängende EXCEL-Datei auf Ihrem Computer.
2. Öffnen Sie von dort die Datei; ggf. erhalten Sie die gelb hinterlegte Meldung "Geschützte Ansicht", bitte klicken Sie hier "Bearbeitung aktivieren" an.
3. Sie erhalten die gelb hinterlegte Warnmeldung "Makros wurden deaktiviert."
4. WICHTIG: Klicken Sie "Inhalt aktivieren" an.
5. Füllen Sie die blauen Felder, in dem Sie einen Wert aus der jeweils hinterlegten Auswahlliste wählen.
6. Füllen Sie bitte alle Felder, auch wenn das jeweilige Erhebungsmerkmal nicht auf Sie zutrifft. Wählen Sie in diesem Fall die Antwort "leer" am Ende der Liste aus.
7. Speichern Sie Ihre Änderungen und senden Sie die Datei als Anhang per Email an den Absender dieser Email.

Vielen Dank für Ihre Mithilfe!
[REDACTED]

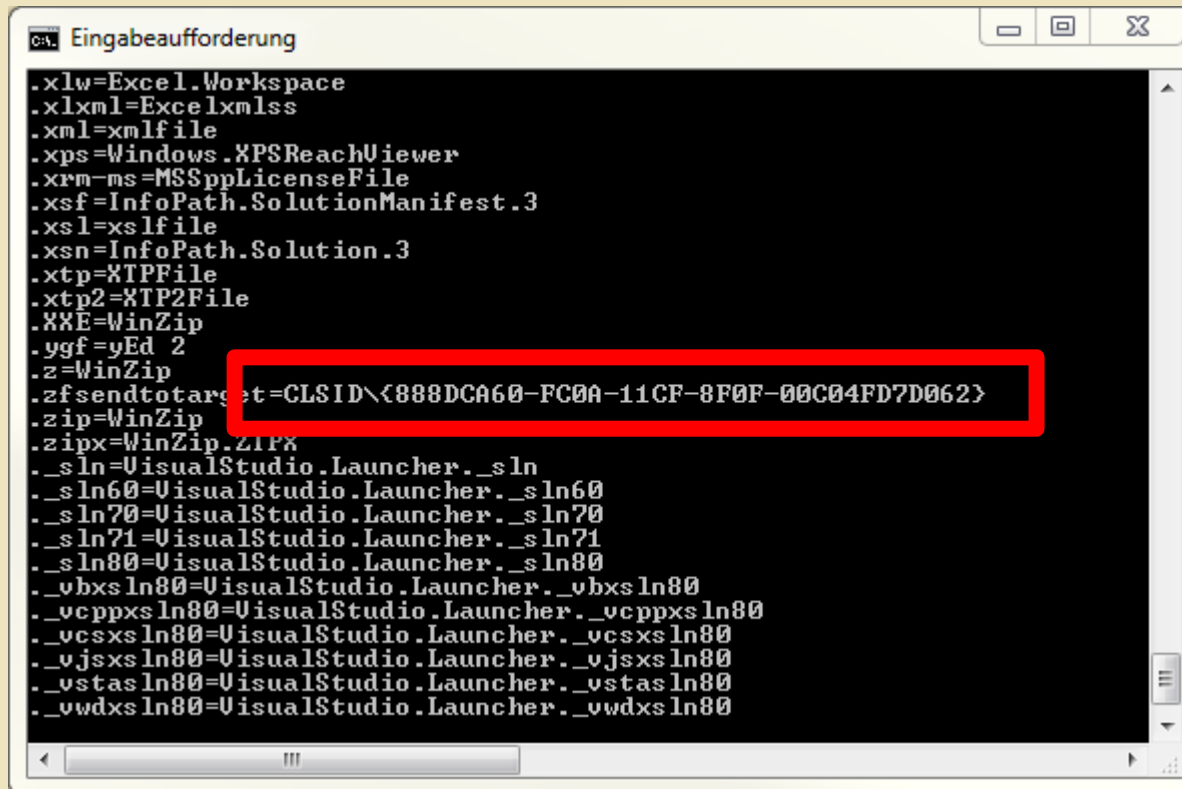
■ Schema:

- Anruf von „Microsoft“-Mitarbeiter
- Der Rechner ist kompromittiert!
- Vertrauensbildende Maßnahmen → z.B. „assoc“
- Installation von Fernwartungssoftware
- Installation von Malware, kostenpflichtige „Bereinigung“, Integration in Botnetz, ...

■ Gefahr:

- Medienbruch „Telefon“ erweckt Vertrauen
- Zeitdruck, man kann sich nicht unabhängig informieren

■ Ausgabe von assoc



```
C:\> assoc

.xlw=Excel.Workspace
.xmlxml=Excel.xmlss
.xml=xmlfile
.xps=Windows.XPSReachViewer
.xrm-ms=MSAppLicenseFile
.xsf=InfoPath.SolutionManifest.3
.xsl=xslfile
.xsn=InfoPath.Solution.3
.xtp=XTPFile
.xtp2=XTP2File
.XXE=WinZip
.ygf=yEd 2
.z=WinZip
.zfsendtarget={CLSID\<888DCA60-FC0A-11CF-8F0F-00C04FD7D062>}
.zip=WinZip
.zipx=WinZip.ZIPX
._sln=VisualStudio.Launcher._sln
._sln60=VisualStudio.Launcher._sln60
._sln70=VisualStudio.Launcher._sln70
._sln71=VisualStudio.Launcher._sln71
._sln80=VisualStudio.Launcher._sln80
._vbxsln80=VisualStudio.Launcher._vbxsln80
._vcppxsln80=VisualStudio.Launcher._vcppxsln80
._vcsxsln80=VisualStudio.Launcher._vcsxsln80
._vjsxsln80=VisualStudio.Launcher._vjsxsln80
._vstasln80=VisualStudio.Launcher._vstasln80
._vwdxsln80=VisualStudio.Launcher._vwdxsln80
```

- Der „global eindeutige Identifikator“ ist auf allen Windows-Systemen identisch



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

■ **Warum ist das alles so unsicher?**

- **Spezielle Software kann auch Malware sein...**

Fritzbox: UPnP aktivieren - so geht's

29.03.2016 16:26 | von **Tim Aschermann**

Aktivieren Sie UPnP in Ihrer FritzBox, kann spezielle Software auf Ihrem PC beliebige Ports in der FritzBox freigeben. So ersparen Sie es sich, die Ports selbst einzurichten.

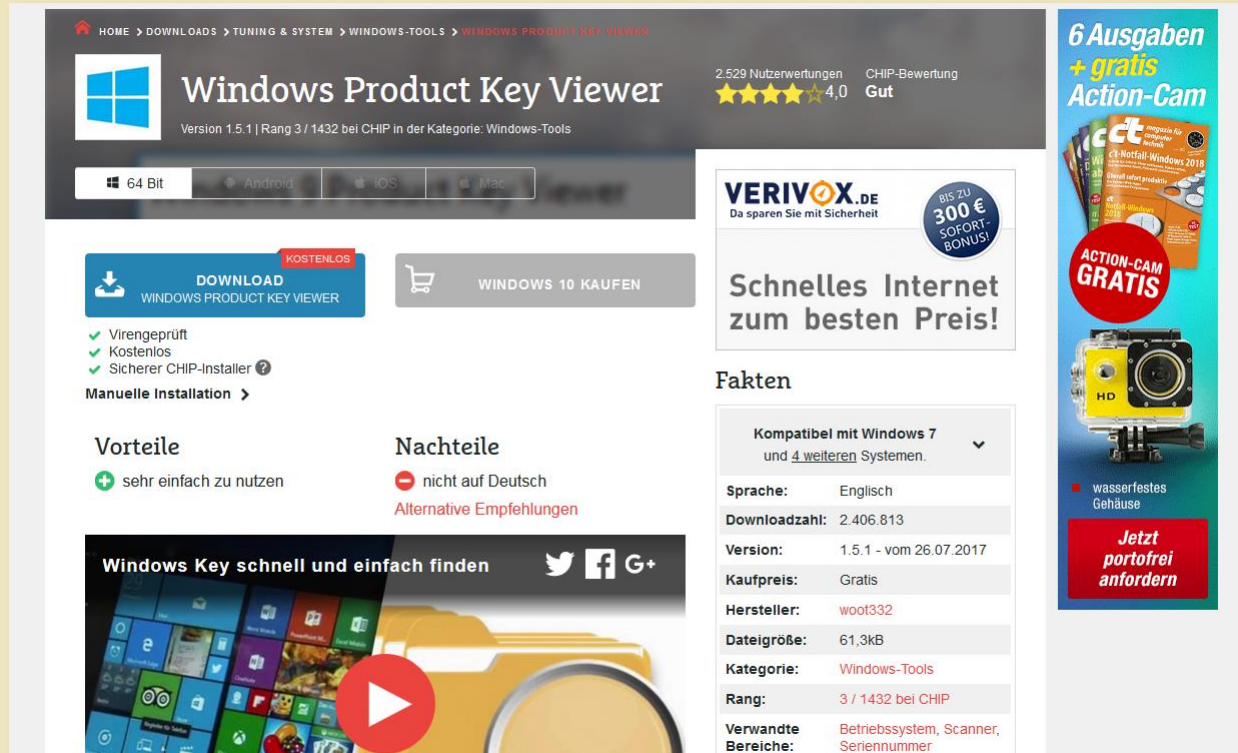
ANZEIGE

Quelle: http://praxistipps.chip.de/fritzbox-upnp-aktivieren-so-gehts_36344

- **Der Verteidiger müsste alle Lücken absichern, an die der Angreifer jemals gedacht hat und denken wird**



Quelle: Sebastian Stein



HOME > DOWNLOADS > TUNING & SYSTEM > WINDOWS-TOOLS > WINDOWS PRODUCT KEY VIEWER

Windows Product Key Viewer

2.529 Nutzerwertungen ★★★★☆ 4,0 CHIP-Bewertung **Gut**

Version 1.5.1 | Rang 3 / 1432 bei CHIP in der Kategorie: Windows-Tools

64 Bit | Android | iOS | Mac

DOWNLOAD KOSTENLOS
WINDOWS PRODUCT KEY VIEWER

WINDOWS 10 KAUFEN

- ✓ Virengeprüft
- ✓ Kostenlos
- ✓ Sicherer CHIP-Installer

Manuelle Installation >

Vorteile

- + sehr einfach zu nutzen

Nachteile

- nicht auf Deutsch

[Alternative Empfehlungen](#)

Windows Key schnell und einfach finden

Fakten

Kompatibel mit Windows 7 und 4 weiteren Systemen.

Sprache:	Englisch
Downloadzahl:	2.406.813
Version:	1.5.1 - vom 26.07.2017
Kaufpreis:	Gratis
Hersteller:	woot332
Dateigröße:	61,3kB
Kategorie:	Windows-Tools
Rang:	3 / 1432 bei CHIP
Verwandte Bereiche:	Betriebssystem, Scanner, Seriennummer

6 Ausgaben + gratis Action-Cam

ACTION-CAM GRATIS

wasserfestes Gehäuse

Jetzt portofrei anfordern

Screenshot: www.chip.de

Ihr Download startet nun automatisch.

Falls der Download nicht startet, klicken Sie bitte [hier](#).

So führen Sie den Download durch:

1. Wenn das Dialogfeld "Öffnen von Windows Product Key Viewer" angezeigt wird, klicken Sie auf "Datei speichern".



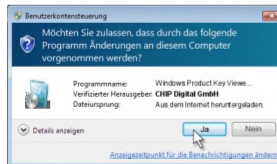
2. Klicken Sie in der "Downloadliste" doppelt auf die Datei.



3. Wenn das Dialogfeld "Datei öffnen - Sicherheitswarnung" angezeigt wird, klicken Sie auf "Ausführen".



4. Wenn das Fenster "Benutzerkontensteuerung" angezeigt wird, klicken Sie auf "Ja".



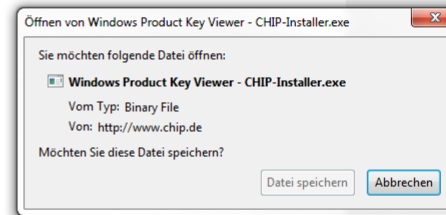
5. Falls der Dialog aus dem vorherigen Schritt nicht erscheint und die Installation nicht beginnt, müssen Sie zunächst auf das blinkende Symbol in der Taskleiste klicken.



Satire-Magazin veröffentlicht Foto-Montage von Sebastian Kurz - jetzt ermittelt der Verfassungsschutz

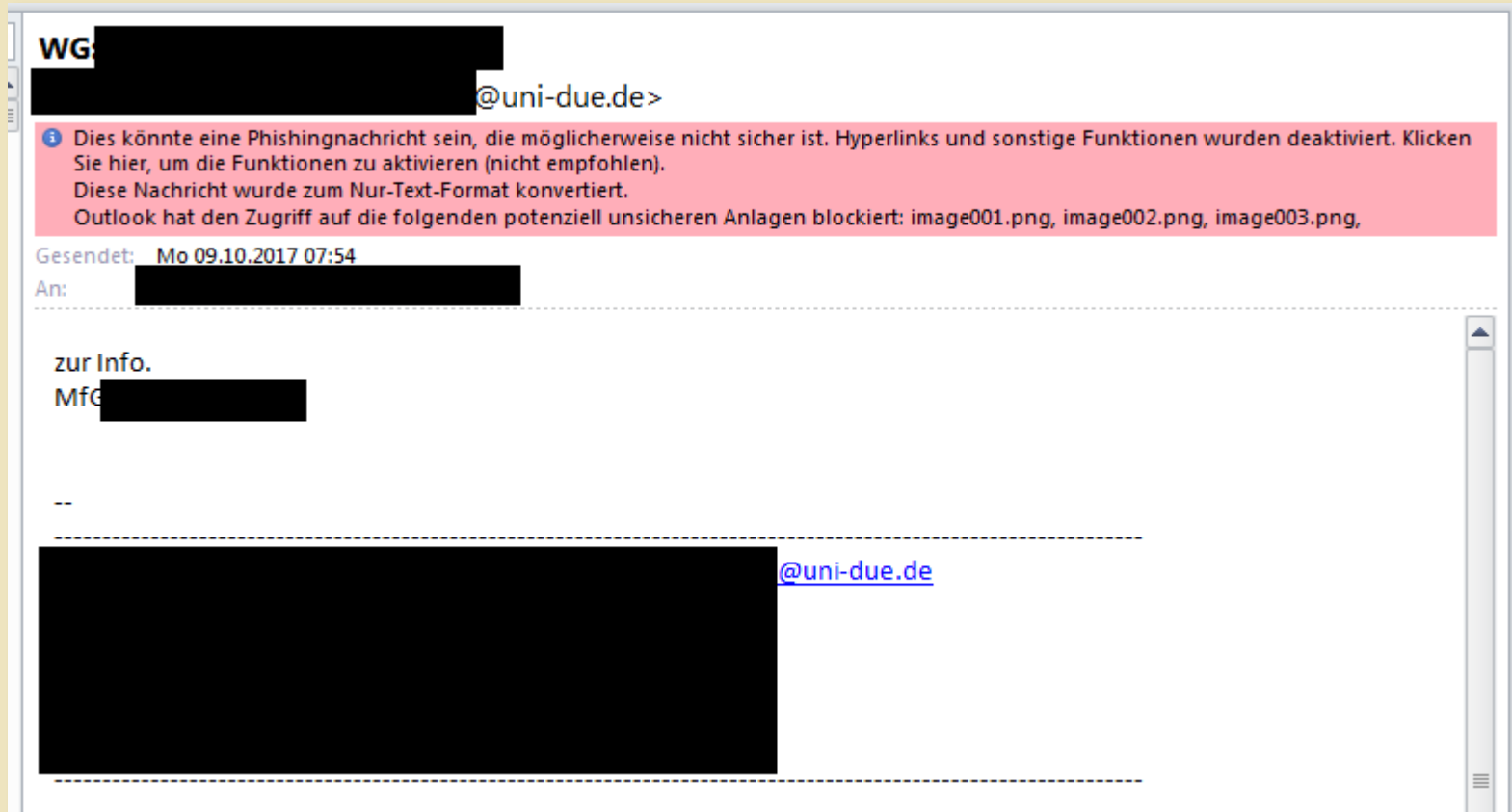
HUFFPOST DEUTSCHLAND

empfohlen von Outbrain



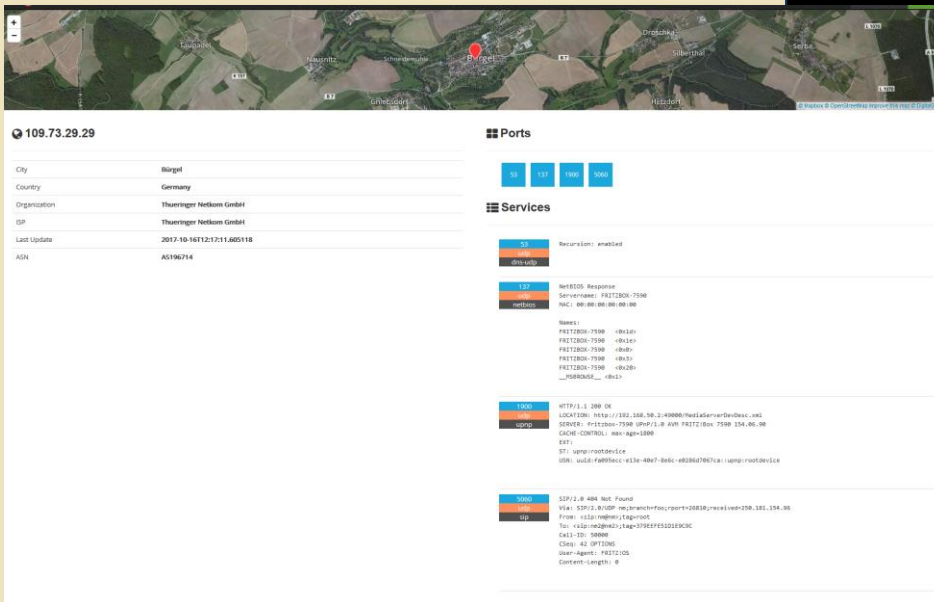
Screenshot: www.chip.de

■ Falsche Klassifizierung als Phishingnachricht



- **Viele Technologien und Vorgehensweisen aus der Zeit vor dem Internet → Offline ließ sich alles rückgängig machen**
- **Viele Technologien und Vorgehensweisen aus der Anfangszeit der Internet → Sehr kleine Benutzergruppe, es gab wenig bis keine Motivation für Angriffe**
- **Anfangs sehr stark getrennt von der realen Welt, heute sehr stark verknüpft → Höhere Motivation für Angriffe**
- **Finanzielle Beweggründe: Adressdaten verkaufen, Botnetz-Kapazität vermieten, ...**
- **Riesige Anzahl angreifbarer Systeme im Internet**

Screenshot: shodan.io



109.73.29.29

City: Wargel
Country: Germany
Organization: Thueninger Netkom GmbH
ISP: Thueninger Netkom GmbH
Last Update: 2017-10-16T12:21:11.605118
ASN: AS196274

Ports: 58, 135, 199, 2000

Services:

- 25 recursion: enabled
- 137 NetBIOS: Response
ServerName: FRITZBOX-7598
NIC: 00-00-00-00-00-00
- 80 HTTP/1.1 200 OK
LOCATION: /192.168.16.2:49990/mediaviewerService.svc
SERVER: FRITZBOX-7598 WHPF1.0 AVM FRITZ!Box 7598 154.06.08
CACHE-CONTROL: max-age=3000
EAT:
ST: ump:rootdevice
URL: uid:f405ecc-e13e-40e7-86dc-0b2867067ca:ump:rootdevice
- 500 SIP/2.0 404 Not Found
Via: SIP/2.0/UDP me:branch-fax/report:20010:received=200.101.134.05
From: <512.166666>@gigaset
To: <512.166666>@gigaset:50050505050505050505
Call-ID: 50000
CSeq: 42 500505
User-Agent: FRITZ!OS
Content-Length: 0

```
[zim096@noc10 ~]$ nslookup
> server 109.73.29.29
Default server: 109.73.29.29
Address: 109.73.29.29#53
> www.google.de
Server:          109.73.29.29
Address:         109.73.29.29#53

Non-authoritative answer:
Name:   www.google.de
Address: 172.217.22.3
> █
```

Offene Überwachungskameras



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

SHODAN port:554 has_screenshot:true

TOTAL RESULTS: 1,216

TOP COUNTRIES

Germany	198
Russian Federation	139
United States	118
Poland	113
Czech Republic	67

TOP ORGANIZATIONS

Deutsche Telekom AG	121
Rostelecom	48
Orange Polska	31
Telekom Austria	25
Vodafone DSL	10

TOP OPERATING SYSTEMS

Linux 2.6.x	22
Linux 3.x	1

87.177.230.160
pFTB1B5AQ-dip0-kipponnet.de
Deutsche Telekom AG
Added on 2017-10-16 14:36:25 GMT
Germany
Details

190.56.166.114
110-100-00-100-static-mexnet.net.gt
Claro Guatemala Static IP
Added on 2017-10-16 13:24:42 GMT
Guatemala, Guatemala City
Details

206.51.217.6
206-51-17-6-static-rio.envents.net
Envents Telecom
Added on 2017-10-16 13:18:20 GMT
United States, Menasha
Details

RTSP/1.0 200 OK
CSeq: 1
Server: Hipcarn RealServer/V1.0
Public: OPTIONS, DESCRIBE, SETUP, TEARDOWN, PLAY, SET_PARAMETER, GET_PARAMETER

RTSP/1.0 200 OK
CSeq: 1
Server: UBNT Streaming Server v1.2
Public: DESCRIBE, SETUP, TEARDOWN, PLAY

RTSP/1.0 200 OK
CSeq: 1
Server: UBNT Streaming Server v1.2
Public: DESCRIBE, SETUP, TEARDOWN, PLAY

Screenshot: *shodan.io*



UNIVERSITÄT
DUISBURG
ESSEN

Offen im Denken

■ Gegenmaßnahmen

- Mobilgeräte → Vortrag Andreas Bischoff
- Betriebssystem → Vortrag Andreas Michels
- E-Mail → Vortrag Rainer Pollak
- Browser
- Malware/Adware/*ware
- Netzwerkdienste (Dateifreigabe, Webserver, PHP, etc.)
- Netzwerkinfrastruktur (WLAN, offene LAN-Ports, etc.)

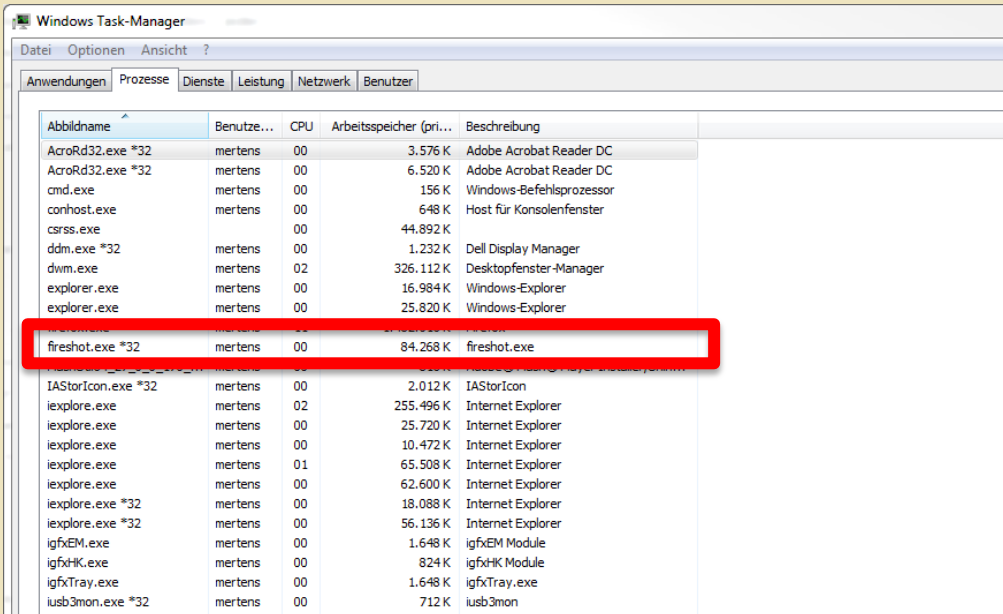
▪ **Nutze ich aktuell:**

- uBlock Origin
- Cookie AutoDelete
- (Privacy Badger)

▪ **Nutze ich nicht mehr (primär wg. FF57+-Kompatibilität):**

- NoScript
 - Adblock Plus
 - Ghostery
 - Self-Destructing Cookies → Cookie AutoDelete
 - Better Privacy → Bisher kein wirklich guter Ersatz
- } uBlock Origin + Privacy Badger

- Installation und Ausführung zusätzlicher Binärdateien direkt aus Firefox-Addon möglich
- Keine unnötigen Addons installieren, nur vertrauenswürdige Quellen verwenden



Abbildname	Benutze...	CPU	Arbeitsspeicher (pri...	Beschreibung
AcroRd32.exe *32	mertens	00	3.576 K	Adobe Acrobat Reader DC
AcroRd32.exe *32	mertens	00	6.520 K	Adobe Acrobat Reader DC
cmd.exe	mertens	00	156 K	Windows-Befehlsprozessor
conhost.exe	mertens	00	648 K	Host für Konsolenfenster
csrss.exe		00	44.892 K	
ddm.exe *32	mertens	00	1.232 K	Dell Display Manager
dwm.exe	mertens	02	326.112 K	Desktopfenster-Manager
explorer.exe	mertens	00	16.984 K	Windows-Explorer
explorer.exe	mertens	00	25.820 K	Windows-Explorer
freshot.exe *32	mertens	00	84.268 K	freshot.exe
IASStorIcon.exe *32	mertens	00	2.012 K	IASStorIcon
ieexplorer.exe	mertens	02	255.496 K	Internet Explorer
ieexplore.exe	mertens	00	25.720 K	Internet Explorer
ieexplore.exe	mertens	00	10.472 K	Internet Explorer
ieexplore.exe	mertens	01	65.508 K	Internet Explorer
ieexplore.exe	mertens	00	62.600 K	Internet Explorer
ieexplore.exe *32	mertens	00	18.088 K	Internet Explorer
ieexplore.exe *32	mertens	00	56.136 K	Internet Explorer
igfxEM.exe	mertens	00	1.648 K	igfxEM Module
igfxHK.exe	mertens	00	824 K	igfxHK Module
igfxTray.exe	mertens	00	1.648 K	igfxTray.exe
iusb3mon.exe *32	mertens	00	712 K	iusb3mon



■ Netzzugang UDE:

- Portfilter gegen unbeabsichtigte Bereitstellung von Diensten zum Internet
- Freigabe per Formular: <https://www.uni-due.de/zim/services/online/portfreischaltung.php>
- Innerhalb des Campusnetzes in der Regel ungefiltert → Firewall des Betriebssystems aktivieren/aktiviert lassen

■ Netzzugang Heimnetz

- In der Regel über Router des Providers mit NAT
- Funktion ähnlich zum Portfilter der UDE
- Innerhalb des Campusnetzes in der Regel ungefiltert → Firewall des Betriebssystems aktivieren/aktiviert lassen

■ WLAN UDE

- Abgesichert durch WPA2-Enterprise
- Zugang per Unikennung
- Separates WLAN-Kennwort nutzen! Einrichten unter <https://benutzerverwaltung.uni-duisburg-essen.de/portal/> und dort „WLAN-Passwort setzen“

■ WLAN Heimnetz

- Selbst absichern per WPA2-PSK
- Zugang mit (sicherem!) Kennwort

- Grundsätzlich sinnvoll, sich nicht nur auf eine Schutzebene zu verlassen: **https + WPA2**, ggf. VPN
- Bildschirm sperren: **Windows+L**
- Eigene Kennwörter niemals auf fremden Geräten eingeben
- Prävention: Vermeiden, dass ein die Sicherheit gefährdendes Ereignis eintritt
- Mitigation: Nach Eintritt des die Sicherheit gefährdenden Ereignisses möglichst schnelle Rückkehr zum Normalzustand
- Information: **Stets am Ball bleiben, Sicherheit ist kein statischer Zustand**

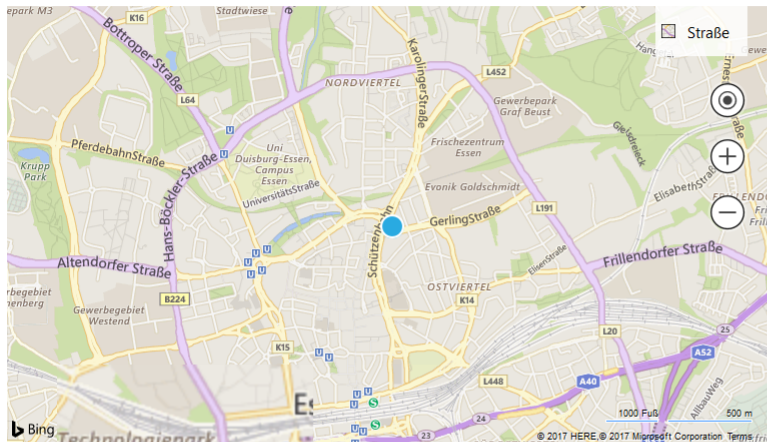
Broschüre zum Herunterladen:

http://www.bundesregierung.de/Content/Infomaterial/BPA/Bestellservice/Sicher_unterwegs_im_Netz.pdf?__blob=publicationFile&v=4



■ Bei Verlust von Mobilgeräten: Ortung und Killswitch

Status Geräteinformationen & Support Mein Handy finden



Karte aktualisieren

Zuletzt angezeigt um 19.10.2017, 11:12:49 in Stadtkern, Nordrhein-Westfalen, Deutschland

83 % verbleibende Akkukapazität

Klingeln

Auch wenn Ihr Telefon stumm geschaltet ist, hören Sie einen Klingelton, sodass Sie es finden können.

Sperren

Sperren Sie für andere Benutzer den Zugriff auf Ihr Handy und zeigen Sie eine benutzerdefinierte Meldung auf dem Bildschirm an.

Löschen

Wenn Sie vermuten, dass Ihr Handy gestohlen wurde, sollten Sie die persönlichen Daten darauf löschen lassen.

Gebühren für SMS und Datenverbindungen können anfallen.

Hilfe zum Microsoft-Konto

[Suchen eines verlorenen Handys](#)

[Schützen Ihres Handys](#)

[Bevor Sie ein Gerät verkaufen oder verschenken](#)

[Einrichten des ersten Kontos auf einem Windows-Telefon](#)

[Weitere Hilfe zu Ihrem Microsoft-Konto](#)

- **Robocopy**
- **Sehr nützlich, sehr schnell**
- **Auf jedem Windows-System bereits vorhanden**

```
robocopy <Quelle> <Ziel> /E /Z /COPY:DAT /DCOPY:T /XJ  
/X /V /NP /ETA /R:0 /W:5 /TEE /LOG+:<Logdatei>
```

- **Backups sind immer sinnvoll!**

- **Die Gefahrenpotentiale beim Umgang mit vernetzten IT-Systemen sind unendlich – Man kann sich nicht auf alle Eventualitäten vorbereiten**
- **Prävention: Gesunde Vorsicht, Ungewöhnliches stets hinterfragen und niemals annehmen „das wird so schon richtig sein“**
- **Mitigation: Immer darauf vorbereitet sein, dass ein Angreifer trotz aller Vorsicht Erfolg hat. Aktuelles, getestetes Backup und Ersatzgerät bereithalten.**

- Die Gefahrenpotentiale beim Umgang mit vernetzten IT-Systemen sind unendlich – Man kann sich nicht auf alle Eventualitäten vorbereiten

Vielen Dank für Ihre Aufmerksamkeit!

- **Mitigation:** Immer darauf vorbereitet sein, dass ein Angreifer trotz aller Vorsicht Erfolg hat. Aktuelles, getestetes Backup und Ersatzgerät bereithalten.

- Die Gefahrenpotentiale beim Umgang mit vernetzten IT-Systemen sind unendlich – Man kann sich nicht auf alle Eventualitäten vorbereiten

Vielen Dank für Ihre Aufmerksamkeit!

- **Mitigation:** Immer darauf vorbereitet sein, dass ein Angreifer trotz aller Vorsicht Erfolg hat. Aktuelles, getestetes Backup und Ersatzgerät bereithalten.

- 10.10.2017 - Andreas Michels
Mit Sicherheit am Windows-Rechner - aber wie?
- 13.10.2017 – Rainer Pollak
Security-Check „E-Mail“
- 17.10.2017 – Dr. Andreas Bischoff
**Der Kulturbeutel für das mobile Internet –
sicher unterwegs mit Smartphone und Tablet**
- 20.10.2017 – Dr. Marius Mertens
Phishers Fritze phisht...