



Selbstverteidigung für deine Applikation

Benjamin Brunzel
Rüdiger Heins

Online-Schwarzmarkt: Geklaute Kreditkarten und DDoS-Attacken für 'n Appel und 'n Ei

26.05.2016 11:08 Uhr – Dennis Schirmacher

 vorlesen

(Bild: SecureWorks)

In Untergrund-Marktplätzen gehen Verkäufer neuerdings mit 24/7-Service auf Kundenfang. Oft wird versprochen, dass nur eine erfüllte Dienstleistung bezahlt werden muss, berichten Sicherheitsforscher.

Kryptologen vom Ciso Intel Team waren für SecureWorks in russischen Online-Schwarzmärkten unterwegs und zeigen neben aktuellen Preisen für kriminelle Leistungen auch neue Trends auf. Ihr Report [Underground Hacker Markets](#) erscheint jährlich und wurde in diesem Jahr zum dritten Mal veröffentlicht.

Von Kreditkarten bis zum Trojaner

Um die durchschnittlichen Preise für Diebesgut und illegale Dienstleistungen zu ermitteln, haben die Sicherheitsforscher eigenen Angaben zufolge verschiedene Untergrund-Foren in dem Zeitraum vom dritten Quartal 2015 bis zum ersten Quartal

Dienste

Security Consultant

Netzwerkcheck

Anti-Virus

Emailcheck

Browsercheck

Krypto-Kampagne

Der Einstieg in professionelle Incident Response

Gut Vorbereiten, richtig Reagieren – ein Crash-Kurs für Admins in kleinen und mittleren Unternehmen.



Artikel

PrivateBin: Pastebin-Alternative für Vertrauliches

PrivateBin verschlüsselt Inhalte, ist über das Tor-Netzwerk erreichbar und bietet einen



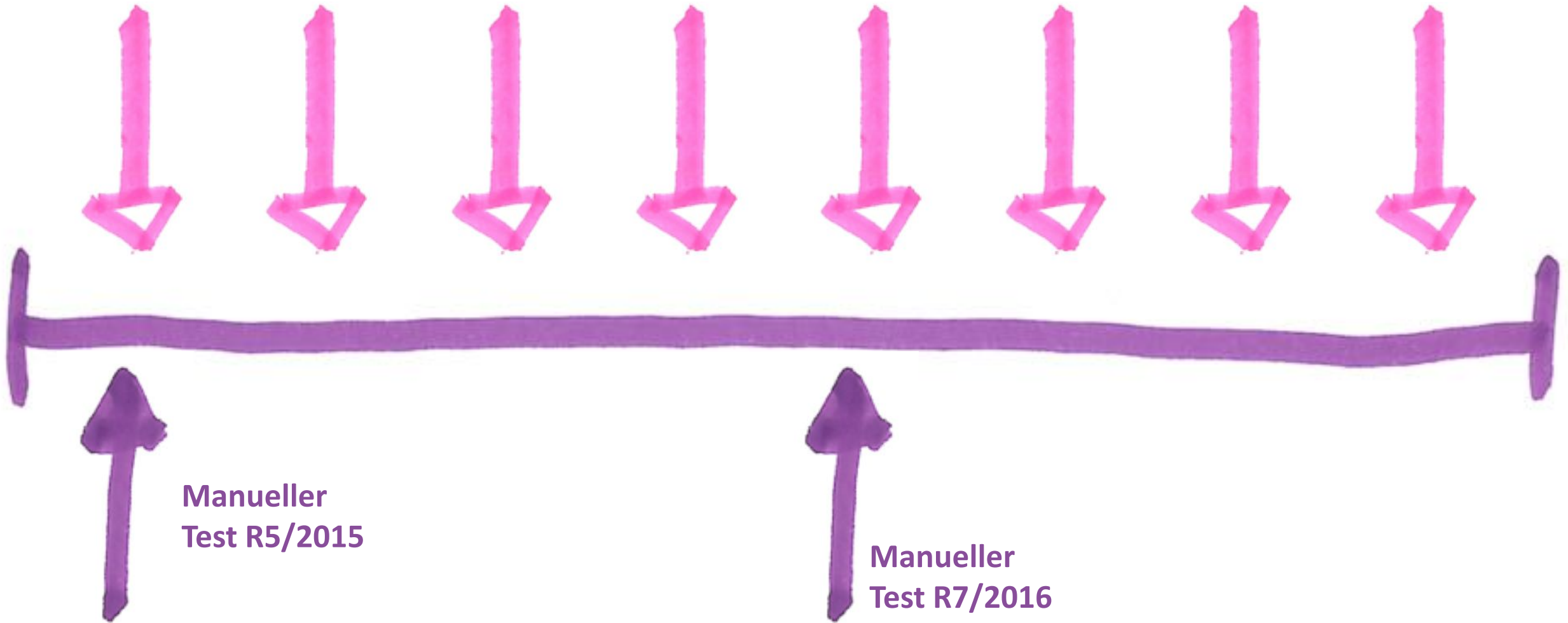
Selbstzerstörungsmodus. Wer möchte, kann das Tool auch selbst auf seinem Server hosten.

Hardware-Fuzzing: Hintertüren und Fehler in CPUs aufspüren

Ein Prozessor-Fuzzer analysiert Hardware, der man normalerweise blind vertrauen muss. In ersten Testläufen



Angreifer



Manueller
Test R5/2015

Manueller
Test R7/2016

Verteidiger



```
buildscript {  
    repositories {  
        mavenCentral()  
    }  
    dependencies {  
        classpath("org.springframework.boot:spring-boot-  
gradle-plugin:1.5.15.RELEASE")  
        classpath("org.owasp:dependency-check-gradle:3.3.1")  
    }  
}  
  
apply plugin: 'org.owasp.dependencycheck'
```

Was sollte ich ab morgen tun?

Bugs & Vulnerabilities

4 ^C

Bugs

0 ^A

Vulnerabilities

Leak Period: since previous version
started vor 4 Monaten

0

New Bugs

0

New Vulnerabilities

Code Smells

2d ^A

Debt

started vor 4 Monaten

38

Code Smells

0

New Debt

0

New Code Smells

Coverage



81.7%

Coverage

313

Unit Tests

—

Coverage on New Code

Duplications



6.2%

Duplications

19

Duplicated Blocks

0.0%

Duplications on
1 New Lines

out-of-the-box

Cloud Ready

Plug 'n Play

µServices

hochskalierbar

Continuous Secure Delivery

Spider
(ZAP)

Scanner
(BURP)

nmap

Reporting
(Kibana)

Spider
(iteratec)

Scanner
(ZAP)

...

Job Steuerung (Camunda)

Build

Int.
Tests

Last
Tests

**Security
Tests**

Release

Continuous Delivery

Werkzeuge der Angreifer nutzen





Low hanging fruits finden



... bevor es jemand anderes tut!



secure code**box**



<https://github.com/secureCodeBox/secureCodeBox>

Perception!



logstash

Demo Time ;)

Metriken

Womit starte ich?

› Login

- › Anzahl der erfolgreichen Logins
- › Anzahl der fehlgeschlagenen Logins
 - › Differenz zwischen den Beiden.
- › Anzahl der Logouts (ggf. Fehlschläge)
- › Anzahl der Logins pro User-Konto
 - › Top 10 Accounts (Datenschutz beachten)

› Sessions

- › Anzahl der aktiven Sessions / bekannte Token
- › Anzahl der Requests mit abgelaufener Session / Token
- › Anzahl der Requests mit ungültiger Session / Token
- › Anzahl der Refreshes
- › Durchschnittliche Sessionlänge
 - › Top 10 Accounts (Datenschutz beachten)

Metriken

Womit starte ich?

- › Allgemein / Fachlich
 - › Aufruftrate der einzelnen Unterseite / Funktion
 - › Fachliche Metriken:
 - › Anzahl der Buchungen / Bestellungen
 - › Anmeldung Newsletter
 - › Anzahl Timeouts
 - › Anzahl der Requests HTTP-1 vs HTTP-2
 - › Validation Fehler

Interessante Request-Details

Metadaten

- › Aufgerufene URL / Funktion
- › Referer
- › Accept-Header
- › Accept-Encoding-Header
- › Accept-Language-Header
- › User-Agent-Header
- › IP-Adresse-Header
- › Beliebige Custom X-Header

user00012@security.iteratec.de:QXFyT2l0WNLQztXND1TanhyWnA=
user00013@security.iteratec.de:QFo5P0xcMUM+UVtd02w8Y1ZLMM=
user00014@security.iteratec.de:bkkyVz48ZUA5T0FoUHI3ZEBYck8=
user00015@security.iteratec.de:Z1w4dnplWsnLLVmRJVL5ZQwVcT0g=
user00016@security.iteratec.de:XF9iVTNLRk01Vkr5Pno/MTVONlwm=
user00017@security.iteratec.de:STVwMfhjPnA5c3ZwbHA8TWDXOFQ=
user00018@security.iteratec.de:c1NxDNEEyN2txVT1ncmQ7N29FPjI=
user00019@security.iteratec.de:dLjvUnJIUF1oXzh5X3R0VvthPHo=
user00020@security.iteratec.de:XGJuPU9oZubcnHlIZHlBYTtWNU=
user00021@security.iteratec.de:UzhMeESPc0BE004wXlo5cVt6MnY=
user00022@security.iteratec.de:QXFUJjpc0mxIam5Q0GY6PzLJ0D0=
user00023@security.iteratec.de:VDNLQ2l1cktteXZnQ8FVPUFRYHQ=
user00024@security.iteratec.de:ZDAzaTxgdUQ9VH060TNMbEQwXFI=
user00025@security.iteratec.de:PlVeVYrZMkRwPj81dZVGPUSbVUg=
user00026@security.iteratec.de:Ql1KZltWnlSP0V1PjoxcFtnC00=
user00027@security.iteratec.de:Yk9Q0EpoVU1GajlBPkh0TLw2SDw=
user00028@security.iteratec.de:cGJwMnExaF09UVZ2dw1jMnlZelc=
user00029@security.iteratec.de:Y1lHukRVc05MdjtSc1lQdHBw00Y=
user00030@security.iteratec.de:TVx2ejphRVlCdWlA0lFjVHp6a3I=
user00031@security.iteratec.de:aUs0RnN5ck0Hnj5kNnhgdTw7VEk=
user00032@security.iteratec.de:czkxPH8cU0dzXT4zN0dlVWdc03o=
user00033@security.iteratec.de:MTxETGVXcd0lkaFZPw1s6bEVXbmI=
user00034@security.iteratec.de:N0dnaT1D0kg2X3A0cV1KVjZTaks=
user00035@security.iteratec.de:ZUt0Mj0Rn5ieTVG0Xc5PTNPVUo=
user00036@security.iteratec.de:dVdvUHBTazR2Rl9Han8SYz1UVFk=
user00037@security.iteratec.de:RVPMZPM4Xn85QGI1anZ0Yj8l0lw=
user00038@security.iteratec.de:MEpCVGp4Xw8LW1JJJeTl80WlAYnA=
user00039@security.iteratec.de:aGRsXEZ5bE4wMnRcdFA8dUpVdTg=
user00040@security.iteratec.de:MFG9R0oyV3vVYj5RP3hiZUdJ0Vg=
user00041@security.iteratec.de:bjthMldUZkAzRzZJTzNPU1thMYLI=
user00042@security.iteratec.de:TlVDbXVQeE8XVUI+aE1NUU1WZFU=
user00043@security.iteratec.de:RDgwaXoTVzhP0XZaRT5e5080akM=

Angriffe abwehren

Java-Script-Challenges

Your account may be compromised!

Based on your visited websites, we believe you may have visited a phishing site. We can not rule out that your account has been stolen.

Please change your password.

Ok, got it!

User informieren



Stefán Jökull Sigurðarson - CCP G...

@stebets

Folgen

WIP: Helping our @EveOnline players to be aware if their passwords are on a list of known compromised passwords. Thanks @havebeenpwned ! CC: @troyhunt #tweetfleet #security #workingprogress

What?

Your current password is a known, commonly-used password. It is known to have been used at least 46980 times in public security breaches.

What should I do?

To keep your account secure we highly recommend that you go to the [account management website](#) and change your password.

How do you know this?

We utilize a free security service



Honeypot

Summary

Was mache ich ab Morgen?

- › Dependency-Scanner in die Build einbauen
- › Eintrittsaktionen loggen und monitoren
- › Fachliche Bedrohungen mit Bedrohungsanalysen identifizieren
- › Gegenmaßnahmen ermitteln und umsetzen
- › Checkout **GitHub**: <https://github.com/iteratec/security-karate>
- › <https://github.com/iteratec/secureCodeBox>



Kontakt

Benjamin Brunzel | Rüdiger Heins
@asciijungle @therockinbear

Benjamin.Brunzel@iteratec.de | Rüdiger.Heins@iteratec.de

Am Sandtorkai 75
20457 Hamburg

Weiterführende Links & Quellen

- › [https://www.owasp.org/index.php/Logging Cheat Sheet](https://www.owasp.org/index.php/Logging_Cheat_Sheet)
- › [https://www.owasp.org/index.php/OWASP Security Logging Project](https://www.owasp.org/index.php/OWASP_Security_Logging_Project)
- › [https://www.owasp.org/images/b/b2/Security Metics- What can we measure-Zed Abbadi.pdf](https://www.owasp.org/images/b/b2/Security_Metics-What_can_we_measure-Zed_Abbadi.pdf)
- › <https://www.digitalocean.com/community/tutorials/an-introduction-to-metrics-monitoring-and-alerting>
- › [https://www.owasp.org/index.php/OWASP Proactive Controls#8: Implement Logging and Intrusion Detection](https://www.owasp.org/index.php/OWASP_Proactive_Controls#8:_Implement_Logging_and_Intrusion_Detection)
- › Photos by [sebastian stam](#), [Tobias Mrzyk](#), [Eric Ward](#), [Patrick Fore](#), [Markus Spiske](#) on [Unsplash](#)