Live Hacking Demo

KBZ St. Gallen

Donnerstag, 26. Oktober 2017

damian.pfammatter@compass-security.com

Cyber-Attacken

Kriminelle erpressen Schweizer Online-Shops

NZZ AM SONNTAG | von Marco Metzler | 25.3.2016, 18:02 Uhr

Digitec hat noch Cyber-Attacken mittlerweile Lösegeld-Forderungen erhalten. Die Firma ist kein Einzelfall. Die Schweiz ist schlecht geschützt.

Noch nie gab es eine so grosse koordinierte Cyber-Attacke auf Schweizer Firmen wie letzte Woche. Der Web-Shop Digitec/Galaxus hat mehrere Erpresserschreiben mit unklaren Absendern erhalten, wie CEO Florian Teuteberg der «NZZ am Sonntag» bestätigt. «Wir haben umgehend Polizei und Staatsanwaltschaft eingeschaltet.» Mehr sagt er aus ermittlungstaktischen Gründen nicht. Lösegeld will man nicht bezahlen.

In der Nacht vom 18. März auf den 19. März starteten bei Digitec die Angriffe, die zeitweise die interne IT und das Telefonsystem lahmlegten. Bei längeren Ausfällen wird die Schadensumme schnell sechsstellig. Hinzu kommen Imag- und Vertrauensverluste.

LHEBDO

A LA UNE | BLOGS | LE MAGAZINE | FORUM DES 100 | RENCONTRES | CONCOURS

Chères lectrices, chers lecteurs,

Nous vous informons que le dernier numéro de L'Hebdo

En vous remerciant de votre compréhension

04.05.2016 16:16 - POLITIQUE

Ruag a

SVP-Website

Die Gruppe hatte auch die SBB attackiert.

schweizer-
ilie.ch

für

Digitec

Phishing

Post-Kunden

Donnerstag, 9. Juni 2016, 17:10 Uhr; aktualisiert um 22:32 Uhr

Vasilije Mustur

Kunden von Post und Postfinance haben in
eine E-Mail von einem gefälschten Absend
Im Anhang wird zur Abholung eines Pake
Dahinter verbirgt sich ein raffiniertes Vir

Jetzt sind Kun
Cyber-Krimin
zeigen: Kund
haben in de
erhalten. D
Pakets au

Der Anha
versprochene Abholu
beim Öffnen des Anhangs Malware
Virus auf dem Computern der Betroffenen installiert. Der Computer ist alsdann teilweise oder ganz ausser Gefecht

Hacker knacken Zahlungs-Software

Bei Berner Firma verschwanden 1,2 Millionen Franken

BERN - Hacker haben über Nacht 1,2 Millionen Franken von den Konten der Berner Küng Holding abgezweigt. Firma, Banken und Software-Vertreiberin streiten darum, wer schuld ist.

er kapern Telefone
M-Budget-Kunden

ff bei Telefondienst M-Budget: Unbekannten ist es ber die Festnetzanschlüsse von M-Budget-Kunden zu

Very Best Of

Grossangriff auf Schweizer

Mehrere Online-Shops wurden heute Opfer einer Cyber-Attacke. Es könnte ein berüchtigtes Hacker-Kollektiv dahinter stecken.

Roman Rey

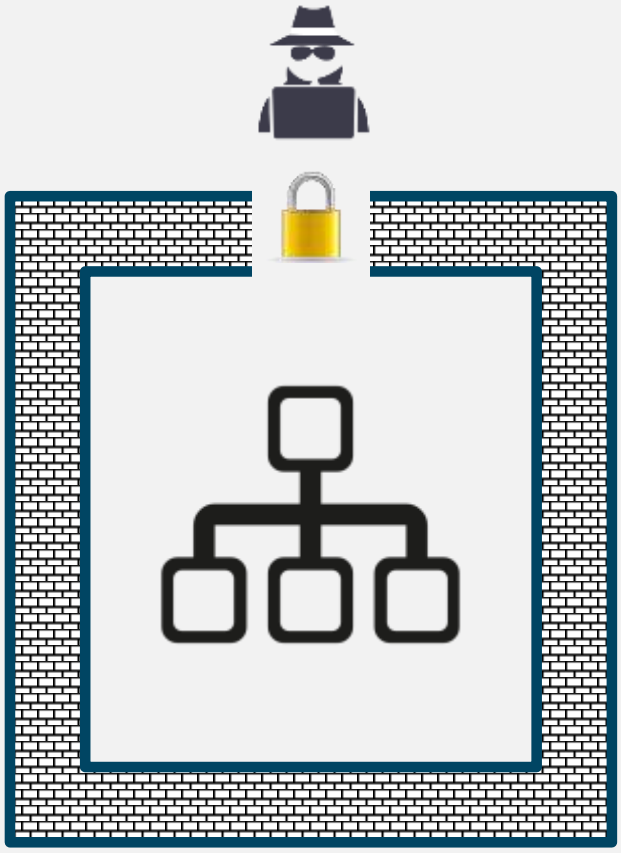
450’000’000’000 $US / Jahr

PROFIT HACKERS

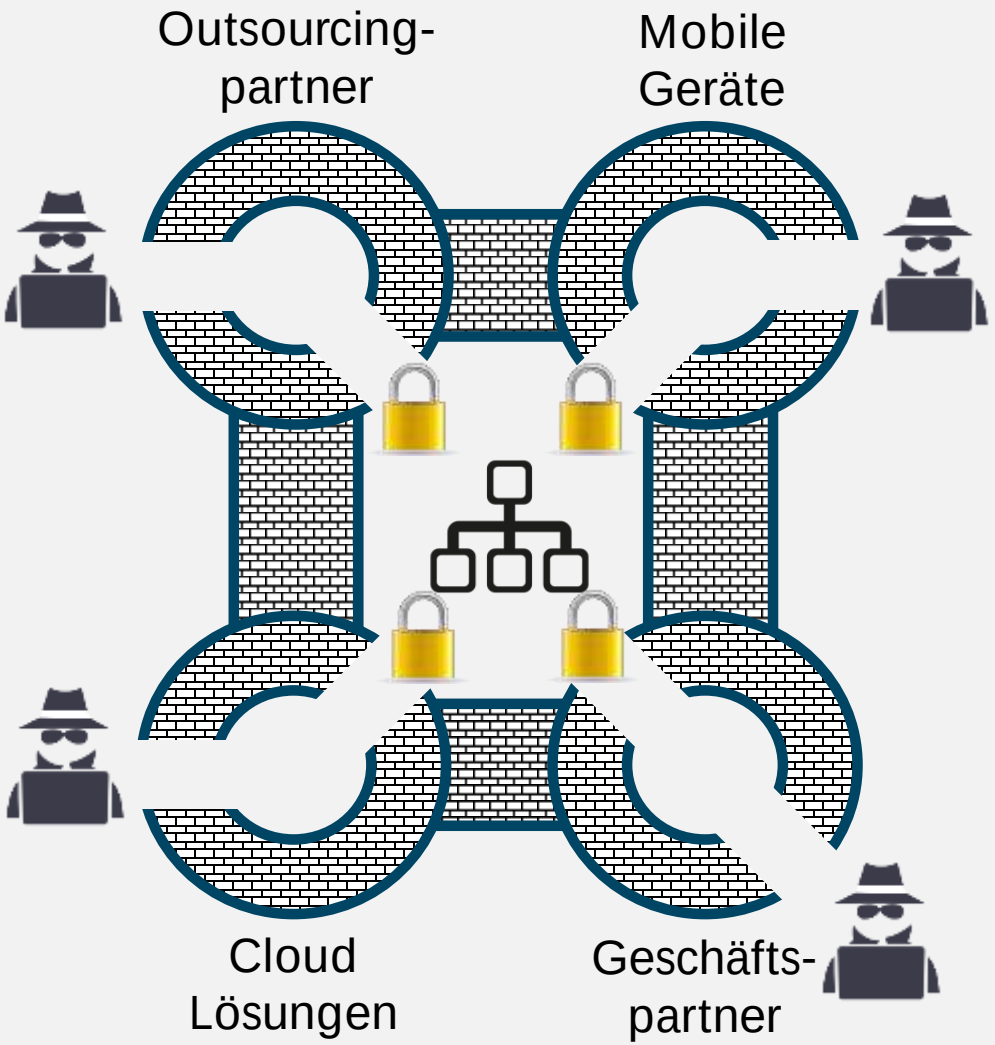
374’000’000 CHF / Jahr

Die Welt verändert sich…

“Alte Welt”



“Neue Welt”




7
6
5
4
Wer sind
diese Hacker?

Script-Kiddies / Verärgerte Mitarbeiter

Alter

- 9 – 18 Jahre

Ziel

- Endbenutzer
- Kleine- und mittelgrosse Unternehmungen

Schaden

- Tief

Motivation / Zweck

- Um cool zu sein und anzugeben
- Seinem Ärger freien Lauf zu lassen
- Medien Aufmerksamkeit erlangen

Black Hat / White Hat

Alter

- 15 – 50 Jahre

Ziel

- Grosse Unternehmungen
- Hardware / Software / Technologie Lieferanten

Schaden

- Mittel

Motivation / Zweck

- Macht demonstrieren
- Medien Aufmerksamkeit Erlangen
- Aus Neugier und uneigennützigem Zweck
- Aus Neugier und eigennützigem Zweck

Organisierte Kriminalität / Staaten

Alter

- 18 – 50 Jahre

Ziel

- Grosse oder strategische Unternehmungen
- Regierungen, Terrorverdächtige, Individuen

Schaden

- Hoch

Motivation / Zweck

- Für Profit
- Spionage / Gegenspionage
- Überwachung, Kontrolle
- Abstürzen von feindlichen Systemen


WHY ME?

Angriffsarten

Nicht-Zielgerichtete Massen-Angriffe

- Zufällige Ziele
- Schwächstes Opfer (z.B. einfaches Passwort)
- Spam, Phishing, etc.
- Unpatched Systeme

Zielgerichtete Angriffe

- Effizient
- Typischerweise kombiniert mit Social Engineering
- Hohe Erfolgsrate

Dazwischenliegende Ziele

- Im Kreuzfeuer zwischen Angreifer und eigentlichem Ziel

Organisierte Cyber-Kriminalität

Cybercrime Versorgungskette

Organisation Leader

Stellt das Team zusammen und definiert die Ziele

Programmierer

Programmieren die Schadprogramme (Malware)

Hacker

Suchen und nutzen Schwachstellen in Anwenderprogrammen und Netzwerken aus

Geldüberbringer

Führen elektronische Bankkontoüberweisungen durch

Verteiler

Kaufen und verkaufen gestohlene Daten

Betrüger

Umwerben potenzielle Opfer mit “sozialen Manipulationen” wie Phishing und Spam

Geldwäscher

Waschen illegale Einnahmen mittels Überweisung an digitalen Finanzdienstleister

Tech. Experten

Pflegen und unterhalten die Infrastruktur der kriminellen Unternehmen

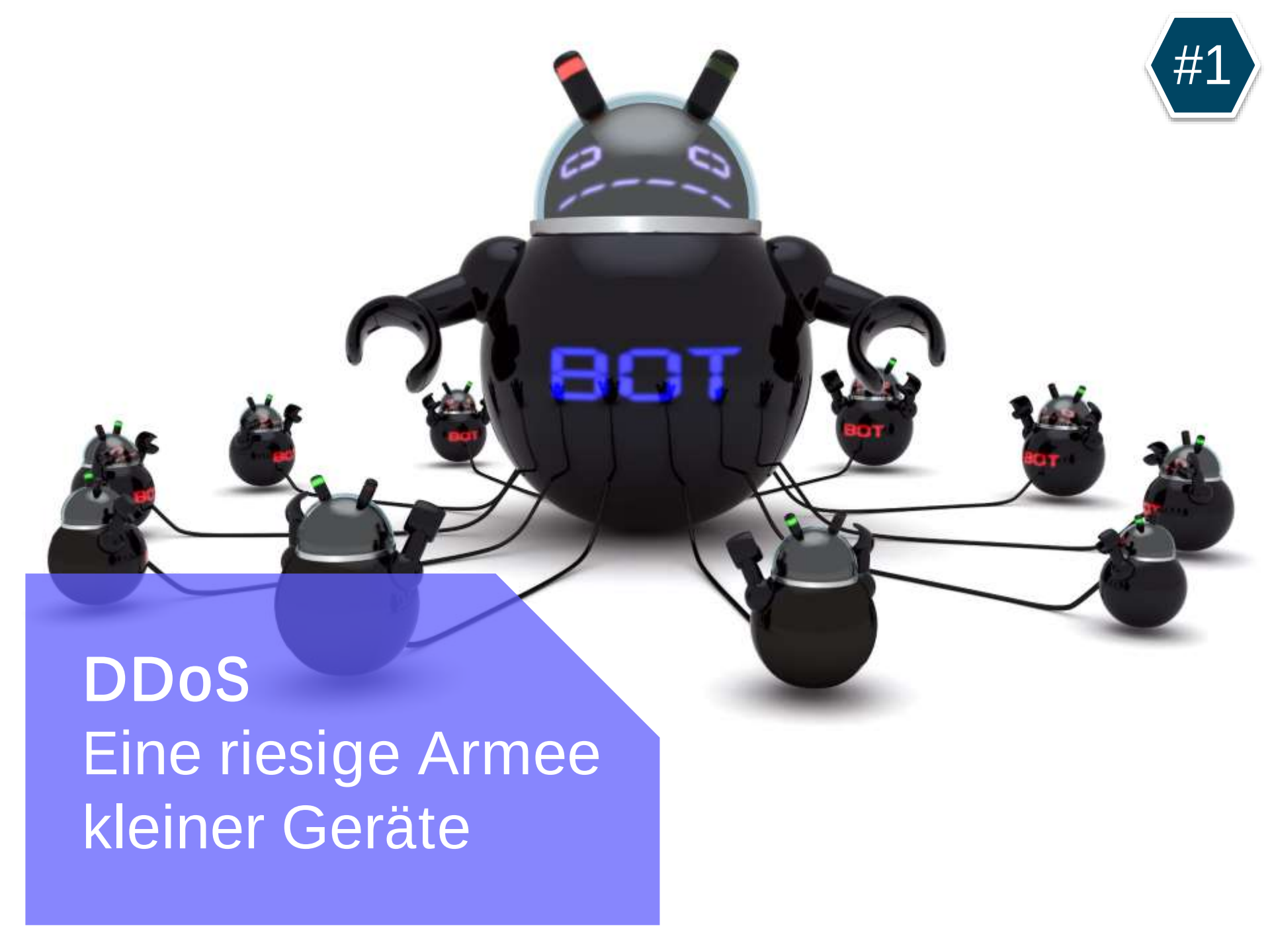
Kassier

Überwachen geknackte Konten und liefern gegen Gebühr Kontenangaben an andere Kriminelle

Hosted System Provider

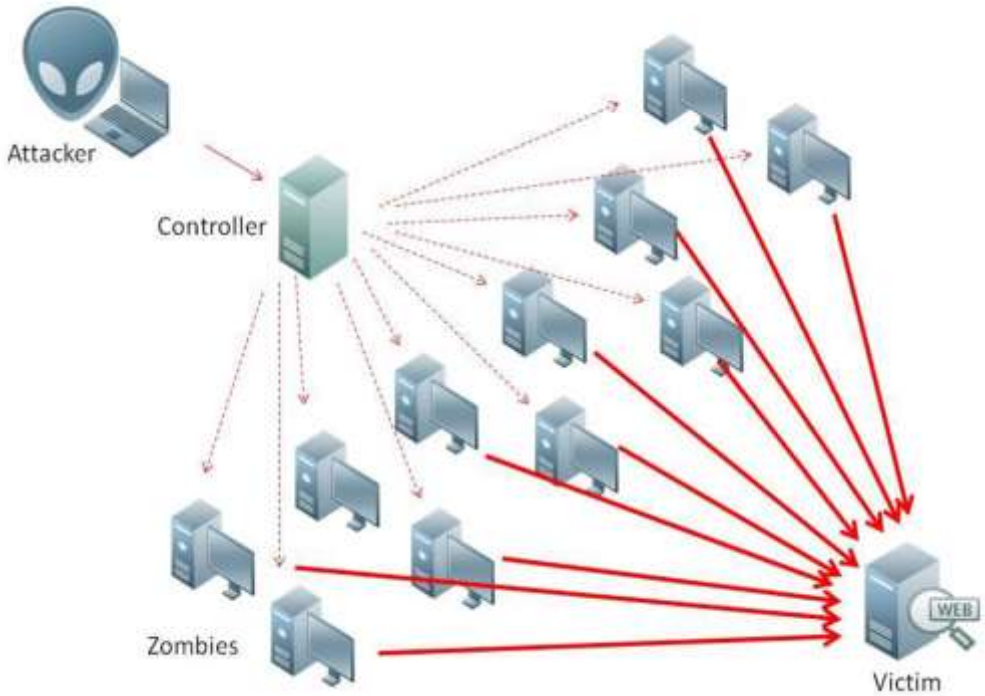
Bieten illegale Server an

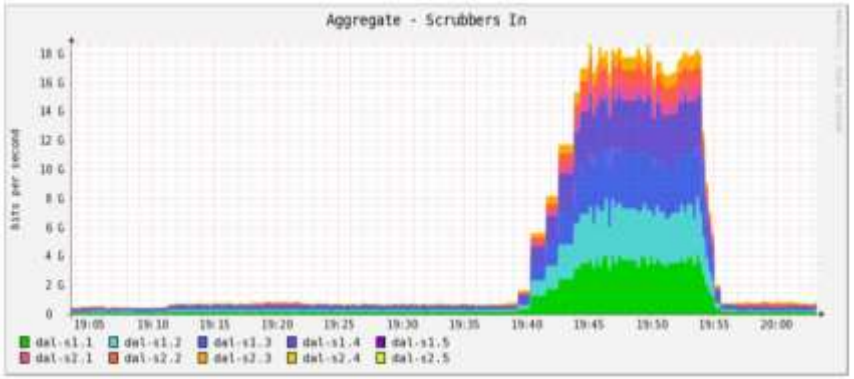

Live Hacking Demos


#1
BOT
DDoS
Eine riesige Armee
kleiner Geräte

Distributed Denial of Service (DDoS)

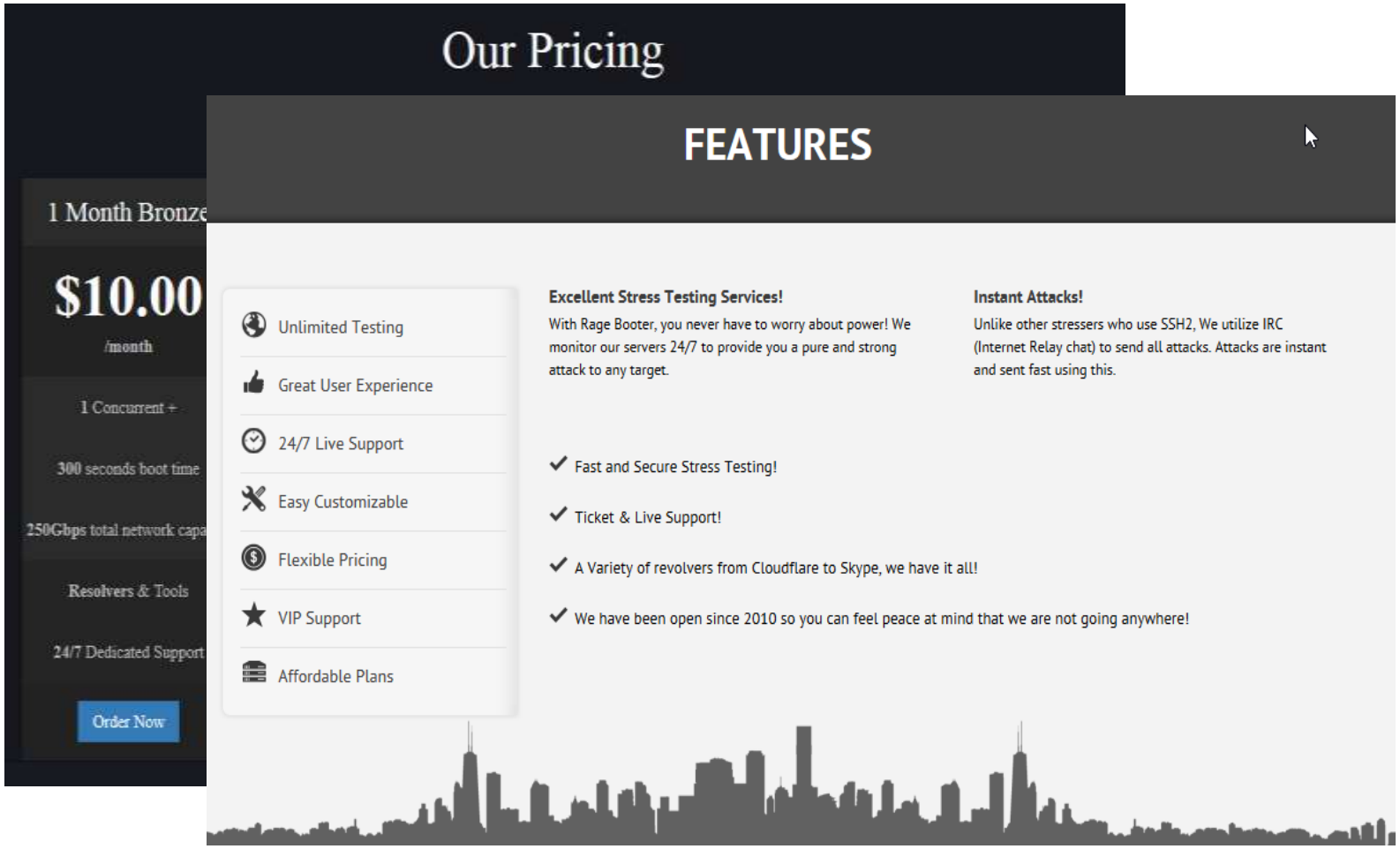
#1



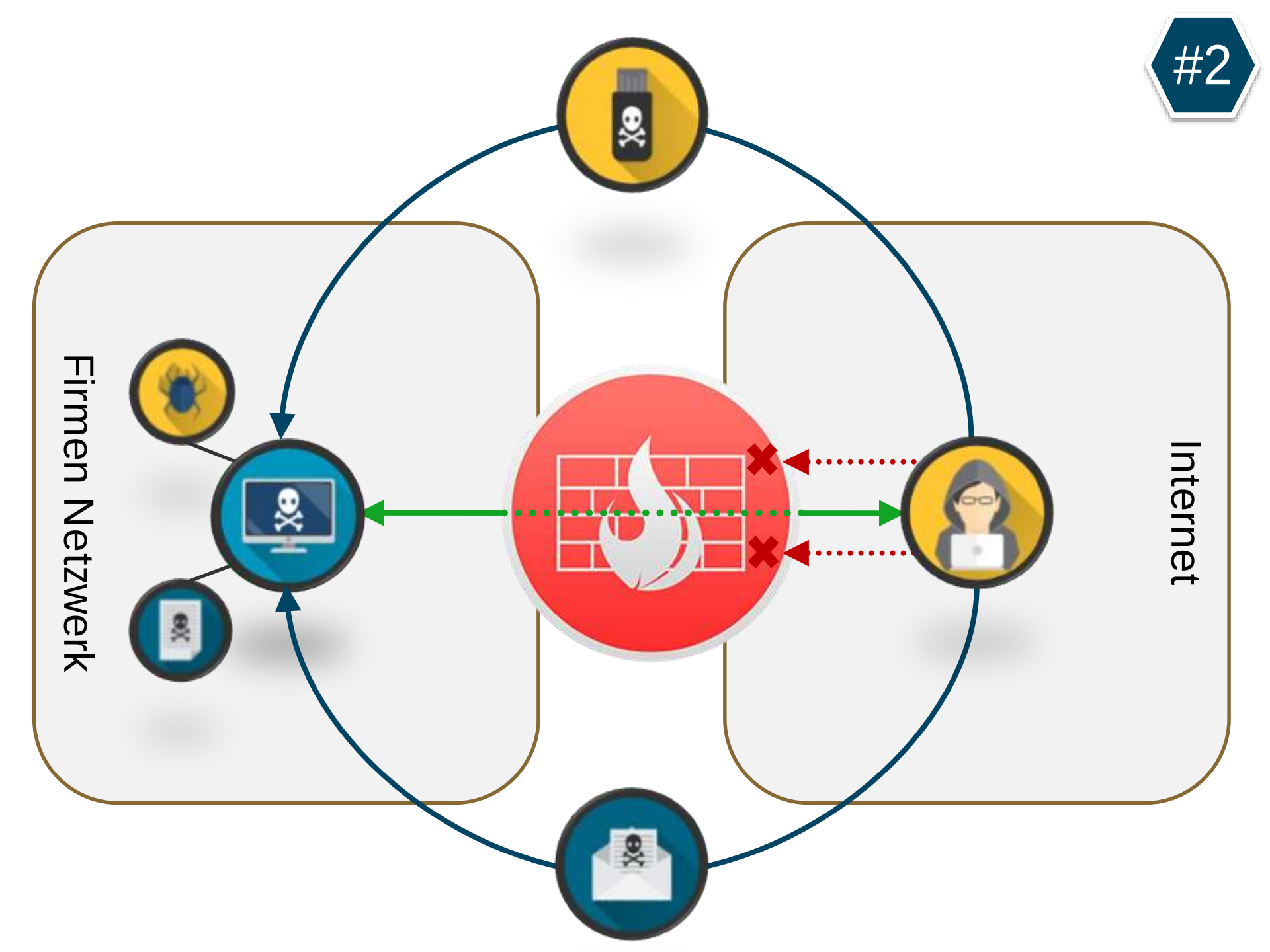


"Network Stressers"

#1

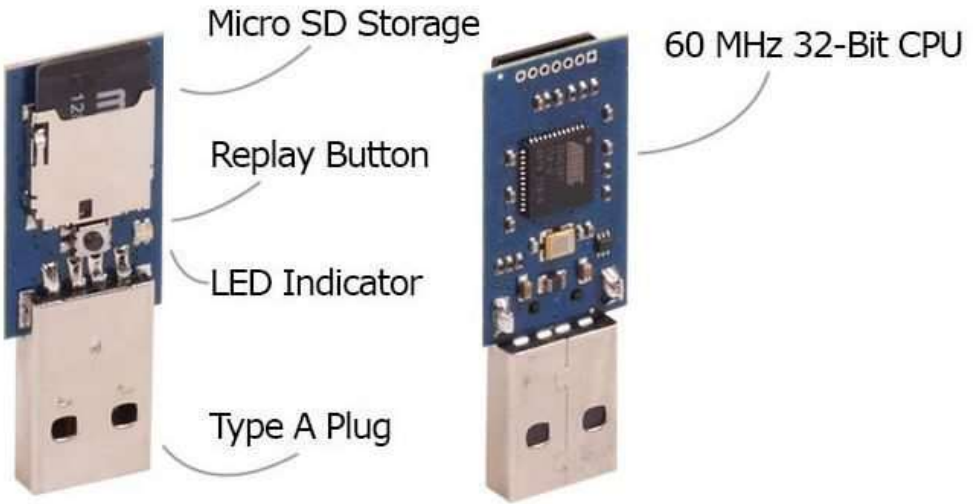



#2
“Verlorener”
USB Stick


#2
Firmen Netzwerk
Internet

“Wenn es wie eine Tastatur quakt…
…muss es eine Tastatur sein.”

#2



#3

SMShing & Vishing

Gegenmassnahmen

Schutzmassnahmen für Unternehmungen

- Bewusstsein zu Sicherheitsproblemen und Bedrohungen erhöhen
- Mitarbeitende in Ausbildungsprogrammen schulen
- Klare Richtlinien für soziale Medien etablieren
- Sensible Daten verschlüsseln
- Schutzsysteme für Hard- und Software aktuell halten
- Gute Passwort-Richtlinien durchsetzen

Schutzmassnahmen für Privatpersonen

- Verschiedene Passwörter für unterschiedliche Online-Dienste
- Passwort-Manager gebrauchen
- Software regelmässig aktualisieren (OS, Browser, Java, Flash, …)
- Aktuelles Anti-Virus Programm verwenden
- Eingehende Email kritisch hinterfragen (Phishing)
- Absender von Emails, SMS, etc. nicht blind vertrauen


CONCLUSIONS
A.
B.
C.


Cyberkriminalität ist hoch organisiert
und
Profit orientiert

Einfache und profitable Ziele werden attackiert

Sei nicht die “Low-Hanging Fruit”!

Danke für die Aufmerksamkeit

Damian Pfammatter
IT Security Analyst
damian.pfammatter@compass-security.com

Compass Security Schweiz AG
Werkstrasse 20, Postfach 2038, CH-8645 Jona
T +41 55 214 41 75, F +41 55 214 41 61