

Tradition of Security

History

Scale that!

Infinity

Ben Gagnon

November 8th, 2017

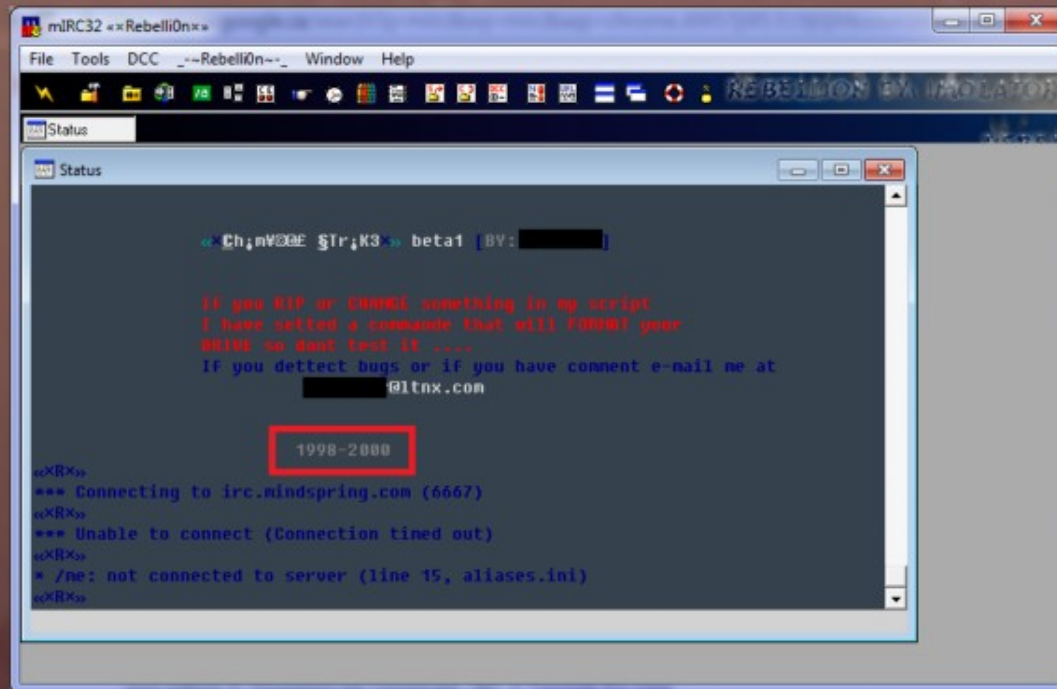
My history



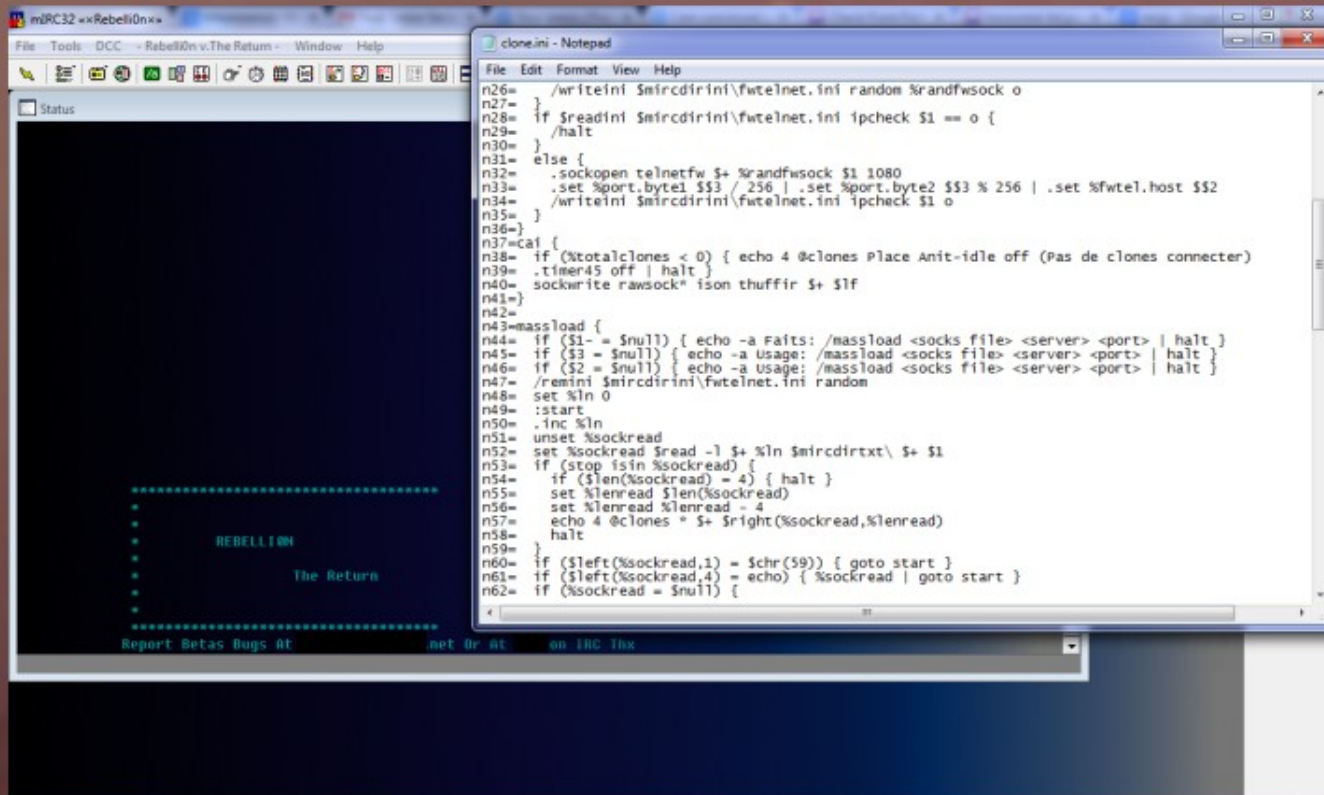
Before everything

Back to the future!

mIRC, 1998



A year later, All out war.



```
mIRC32 «xRebelli0n»
File Tools DCC - Rebelli0n v.The Return - Window Help
Status
*****
*
* REBELLION
*
* The Return
*
*****
Report Betas Bugs At .net Br At on IRC Thx

clone.ini - Notepad
File Edit Format View Help
n26= /writeini $mircdirini\fwtelnet.ini random %randfsock o
n27= }
n28= if $readini $mircdirini\fwtelnet.ini ipcheck $1 == o {
n29= /halt
n30= }
n31= else {
n32= .sockopen telnetfw $+ %randfsock $1 1080
n33= .set %port.byte1 $S3 / 256 | .set %port.byte2 $S3 % 256 | .set %fwtel.host $S2
n34= /writeini $mircdirini\fwtelnet.ini ipcheck $1 o
n35= }
n36= }
n37= cat {
n38= if (%totalclones < 0) { echo 4 @clones Place Anit-idle off (Pas de clones connecter)
n39= .timer45 off | halt }
n40= sockwrite rawsock* ison thuffir $+ $1f
n41= }
n42= }
n43= massload {
n44= if ($1 = $null) { echo -a Faits: /massload <socks file> <server> <port> | halt }
n45= if ($3 = $null) { echo -a Usage: /massload <socks file> <server> <port> | halt }
n46= if ($2 = $null) { echo -a Usage: /massload <socks file> <server> <port> | halt }
n47= /remini $mircdirini\fwtelnet.ini random
n48= set %ln 0
n49= :start
n50= .inc %ln
n51= unset %sockread
n52= set %sockread $read -1 $+ %ln $mircdirtxt\ $+ $1
n53= if (stop isin %sockread) {
n54= if ($len(%sockread) = 4) { halt }
n55= set %lenread $len(%sockread)
n56= set %lenread %lenread - 4
n57= echo 4 @clones * $+ $right(%sockread,%lenread)
n58= halt
n59= }
n60= if ($left(%sockread,1) = $chr(59)) { goto start }
n61= if ($left(%sockread,4) = echo) { %sockread | goto start }
n62= if (%sockread = $null) {
```


Due care, due diligence!

Firewall

IDS

VPNs

Proxy

And more!

```
199908.log - Notepad
File Edit Format View Help
8:09:08 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=194.229.131.120, sport=1271, dport=80.
8:09:09 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=206.132.137.153, sport=1272, dport=80.
8:09:12 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=194.229.131.120, sport=1271, dport=80.
8:09:12 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=206.132.137.153, sport=1272, dport=80.
8:09:12 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=194.229.131.8, sport=1274, dport=80.
8:09:13 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=206.132.137.153, sport=1269, dport=80.
8:09:32 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.204, sport=1275, dport=400.
8:09:38 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=206.132.137.152, sport=1277, dport=80.
8:10:26 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=206.132.137.157, sport=1279, dport=80.
8:12:13 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.204, sport=1275, dport=400.
8:12:17 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.204, sport=1275, dport=400.
8:12:19 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.204, sport=1282, dport=400.
8:12:21 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=206.132.137.156, sport=1283, dport=80.
Adding rule #71 in checked learning mode, due to outgoing data
8:15:05 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.204, sport=1284, dport=400.
Adding rule #72 in checked learning mode, due to outgoing data
8:18:01 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.246, sport=1285, dport=400.
Adding rule #73 in checked learning mode, due to outgoing data
8:20:38 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.246, sport=1287, dport=400.
Adding rule #74 in checked learning mode, due to outgoing data
8:20:57 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=209.67.4.186, sport=1289, dport=80.
8:21:00 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=208.132.136.161, sport=1296, dport=80.
8:21:01 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=209.85.89.183, sport=1297, dport=80.
8:21:01 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=209.67.4.186, sport=1298, dport=80.
8:21:01 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=209.85.89.183, sport=1299, dport=80.
8:21:02 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=198.164.243.114, dst=208.132.136.161, sport=1300, dport=80.
8:23:30 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.246, sport=1301, dport=400.
Adding rule #75 in checked learning mode, due to outgoing data
8:26:04 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.246, sport=1302, dport=400.
Adding rule #76 in checked learning mode, due to outgoing data
8:28:47 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=198.164.243.114, dst=205.188.252.204, sport=1303, dport=400.
Adding rule #77 in checked learning mode, due to outgoing data
9:25:56 PM: Dial-up Adapter [0000] Ref# 3 Blocking outgoing ICMP: src=207.179.184.133, dst=224.0.0.2, type 10.
9:25:59 PM: Dial-up Adapter [0000] Ref# 3 Blocking outgoing ICMP: src=207.179.184.133, dst=224.0.0.2, type 10.
9:26:02 PM: Dial-up Adapter [0000] Ref# 3 Blocking outgoing ICMP: src=207.179.184.133, dst=224.0.0.2, type 10.
9:26:06 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=209.185.128.146, sport=1306, dport=1863.
9:26:07 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=207.34.179.18, sport=1307, dport=6667.
9:26:07 PM: Dial-up Adapter [0000] Ref# 12 WARNING: incoming traffic: src=207.34.179.18, dst=207.179.184.133, sport=80865, dport=
9:26:31 PM: Dial-up Adapter [0000] Ref# 0 Blocking outgoing UDP: src=207.179.184.133, dst=205.188.252.229, sport=1309, dport=400.
Adding rule #78 in checked learning mode, due to outgoing data
9:30:59 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=216.33.151.7, sport=1312, dport=80.
9:31:03 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=216.33.151.8, sport=1315, dport=80.
9:31:28 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=209.185.243.7, sport=1318, dport=443.
9:31:37 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=209.185.131.251, sport=1321, dport=80.
9:31:41 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=209.185.130.251, sport=1323, dport=80.
9:31:42 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=207.46.188.62, sport=1325, dport=80.
9:31:43 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=207.46.188.45, sport=1327, dport=80.
9:31:45 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=204.71.191.249, sport=1329, dport=80.
9:31:48 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=206.132.79.21, sport=1332, dport=80.
9:32:25 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=216.33.151.7, sport=1333, dport=80.
9:32:27 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=216.33.151.8, sport=1335, dport=80.
9:32:45 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.20, sport=1337, dport=80.
9:32:47 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.31, sport=1339, dport=80.
9:32:48 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.25.89.17, sport=1341, dport=80.
9:32:48 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.20, sport=1340, dport=80.
9:32:49 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.1, sport=1343, dport=80.
9:32:49 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.25.89.18, sport=1344, dport=80.
9:32:50 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.20, sport=1345, dport=80.
9:32:51 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.217, sport=1348, dport=80.
9:32:51 PM: Dial-up Adapter [0000] Ref# 15 Connection Attempt: src=207.179.184.133, dst=195.68.99.20, sport=1349, dport=80.
```

And then.



In hindsight.

Sometimes we have to get really high to see how small we are

Felix Baumgartner, first supersonic skydiver



Lessons learned



Lack of time



Lack of expertise and
resources



Illusion of security



Lack of focus

Lack of time



Lack of expertise and resources

Security Expert with experience required!



I installed this once!



Illusion of security

Deloitte.



TOP SECRET//SI//OC//NOFORN

PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- Twitter
- YouTube
- Skype
- ADL
- Apple

What Will You Receive in Collection (Surveillance and Stored Content)?
It varies by provider. In general:

- Email
- Chat - video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Non-Suspense of target activity - logins, etc.
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page: DA PRISMFA, A

TOP SECRET//SI//OC//NOFORN

EQUIFAX®

140 MILLION PEOPLE

NAMES | DRIVERS LICENSES | SOCIAL SECURITY NUMBERS | BIRTHDATES | ADDRESSES

796



Lack of focus

Optimization is good until it's too much.

STRATEGIC PLANNING ASSUMPTION

More than 95% of firewall breaches are caused by firewall misconfigurations, not firewall flaws.

Today's challenges



Lack of time:

Long implementations
Change windows
Procedures



Lack of expertise and resources:

Hiring
Efficiency
Projects
Do it all.



Illusion of security:

New technologies
IOT
Shadow IT
New everything
Cloud
Mobility



Lack of focus:

C-Levels!

Where do we focus
what we have to
get the most benefit

Rather than.

Staying proactive and planning months or years in advance.



We know...

Verizon investigation report states:

YoY threats went up 40%

IDC Spending:

YoY growth of 9%

Yet, efficiency of IT Security went down!

The problem is getting worse

50% of reported breaches could not estimate # of records
16% of all breaches reported were of financial access
4% of breaches were encrypted data
40% increase over previous 6 months



Breach statistics in financials NA 2016 (Gemalto)

3.04 million records per day
126 936 records per hour
2116 records per minute!

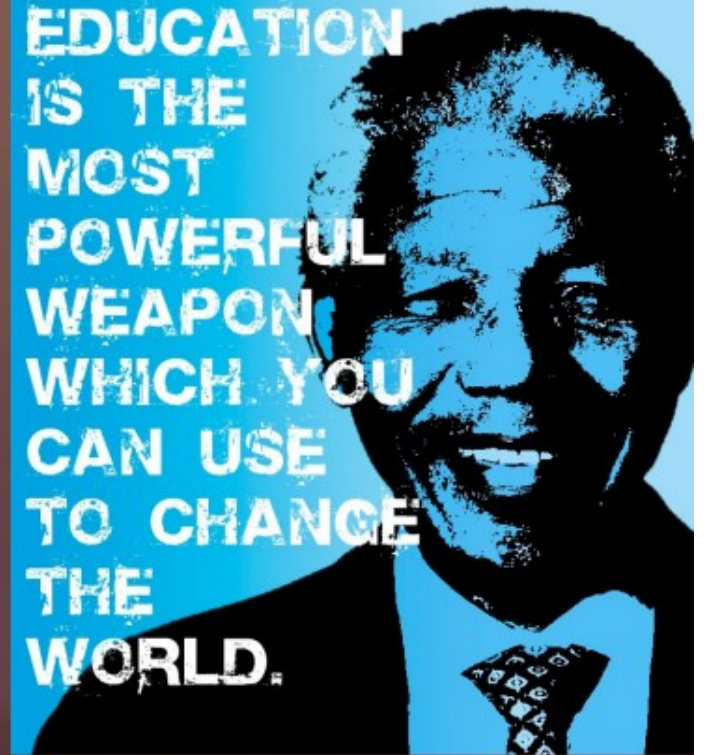


Education is key!

75% of execs think they are invincible
4 out of 5 are confident in their systems
17% would invest in cybersecurity training
28% would invest in mitigating financial losses

(Data from Accenture)

**EDUCATION
IS THE
MOST
POWERFUL
WEAPON
WHICH YOU
CAN USE
TO CHANGE
THE
WORLD.**



What happend?

Where did the 9% go?

Policy enforcement

Care and feeding

Continuity of evidence challenge

Best of breeds!



Tradition of Security

History

Scale that!

Infinity

Ben Gagnon

November 8th, 2017

Scale

Most traditional ways of doing security don't scale:

Logs
Detection (IDS,HIPS)
Policies
etc.

Solutions requiring human intervention inherently cannot scale!



ex machina

Adoption

Consolidation

Cloud Adoption

Public and Private cloud services - IaaS, SaaS, PaaS

Application elements may reside in widely diverse infrastructure elements

Applications are no longer contained within a data center's four walls




What's stopping you?

Physical costs

More maintenance

More rack space and power

Increased application delivery times

A quote by Robert Breault is displayed on a sunset background. The quote is: "It's hard, sometimes, when nothing's stopping you, to know what's stopping you." The text is white and set against a dark, semi-transparent rectangular background. The background of the quote is a sunset over mountains, with the sun low on the horizon, creating a warm, orange glow.

It's hard, sometimes, when
nothing's stopping you, to
know what's stopping you.

Robert Breault

 quadracy

Application and Service delivery

Increased complexity

Changes are prone to conflict

Game changer!



Detection only failures

Creates tremendous human overhead

Slows the delivery of services due to disconnected nature

Technologies are not portable and do not integrate well in a SaaS, IaaS environments



A leaking example!



Kevin the
roof is
leaking!



Focus on remediation?



Patch with point solutions?



Focus on incident response?

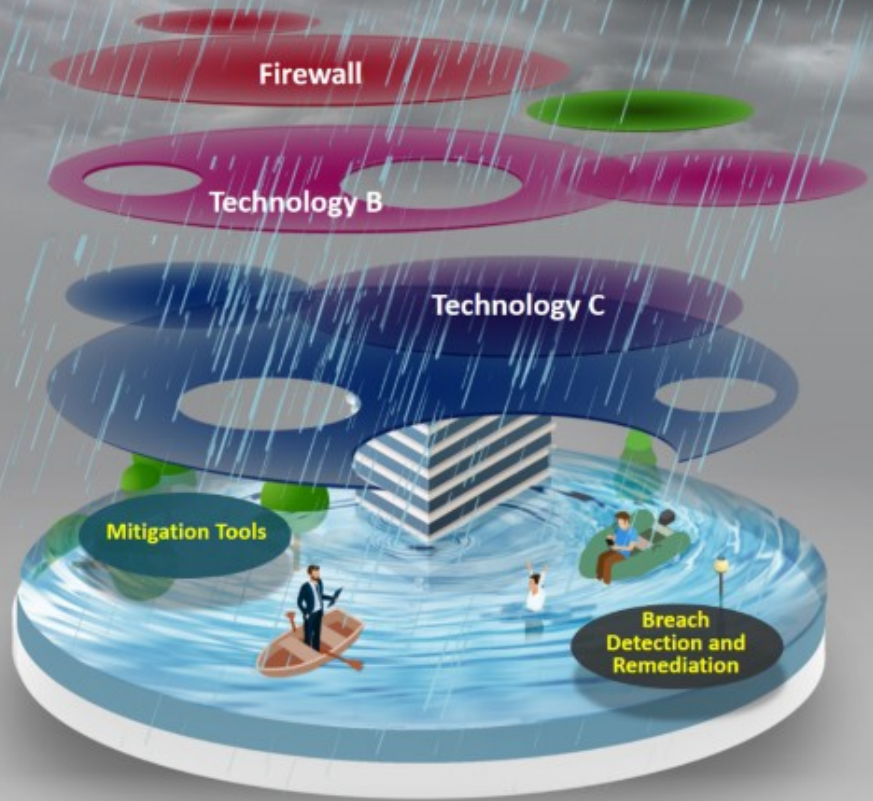


Pretend it isn't happening?

We All
Need Protection

ARCHITECTURE A

MULTI-VENDOR, ATTACK DETECTION
AND MITIGATION



ARCHITECTURE B

FOCUS ON PREVENTION SINGLE VENDOR,
UNIFIED ARCHITECTURE



ARCHITECTURE A

We All
Need Protection

ARCHITECTURE B

MULTI-VENDOR, ATTACK DETECTION
AND MITIGATION

FOCUS ON PREVENTION SINGLE VENDOR,
UNIFIED ARCHITECTURE

Firewall

Next Generation Firewall

Technology B

Threat Prevention (AV, IPS)

Advanced Threat Prevention

Average **40** days to
identify the attack

Average **2** days to
identify the attack

Cost of remediation:
\$667,500

Cost of remediation:
\$6,800

Tradition of Security

History

Scale that!

Infinity

Ben Gagnon

November 8th, 2017

STRATEGY



CHECK POINT
INFINITY

Infinity

Thanks!



CHECK POINT
INFINITY



CONSOLIDATED
SYSTEM

#1 - R80 Platform

Dynamic delivery of services and applications

Security policy changes and adapts to application owner based on tags

Scoped policy ensures application owners can only affect changes within defined rules



CHECK POINT
INFINITY



THREAT
PREVENTION

#2 - Sandblast & Threat Extraction

Pass known good
Proactively sanitize threats using unique approach
Provide unified policy management across entire architecture



CHECK POINT
INFINITY



MOBILE

#3 - Mobility

Address proactively threats that may exist in the mobile space
Fill security gaps left by traditional MDM solutions



CHECK POINT
INFINITY



CLOUD

#4 - vSEC

Private cloud security

Public cloud security

Dynamic and adaptive security across platforms and architectures



nuagenetworks
From Nokia



Google Cloud Platform



Benoit Gagnon, MBA, CISSP, CISA

bgagnon@checkpoint.com

Tradition of Security

History

Scale that!

Infinity

Ben Gagnon

November 8th, 2017