Advanced Malware and Protection - What CISOs Need to Know for the Year 2017

Karel Šimek and Michal Svoboda

12:15 - 12:45h

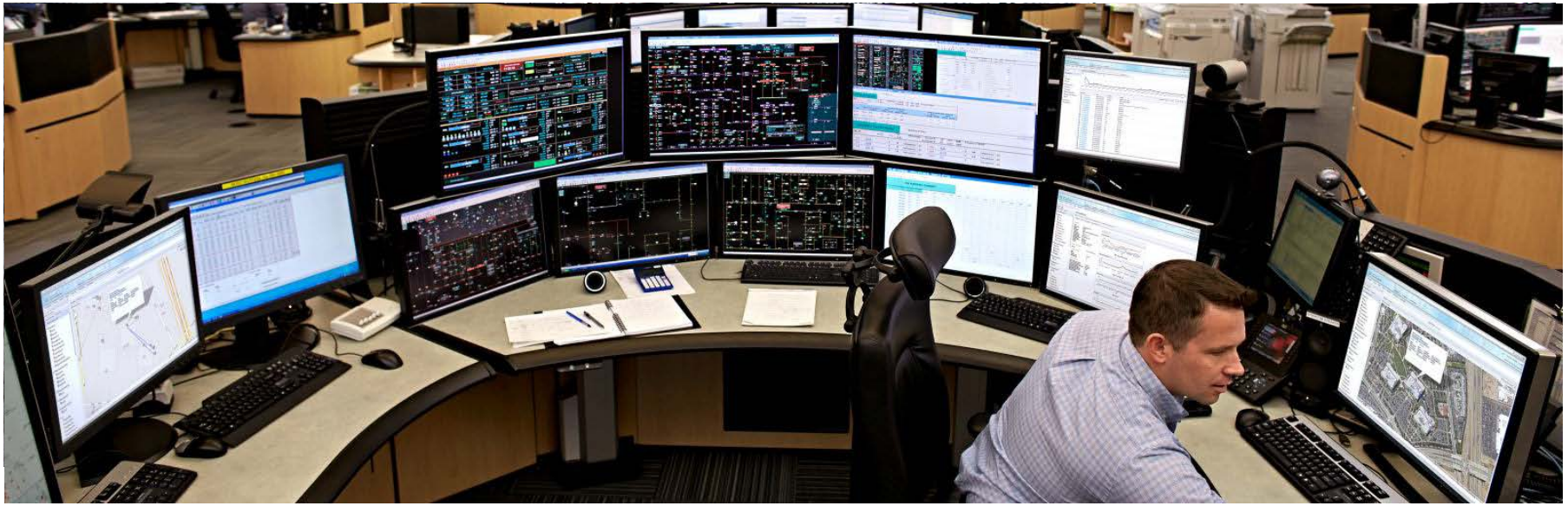
Looking Around Us

2017 continues the trend of widespread breaches in every vertical

- Check haveibeenpwned.com! It's 50:50

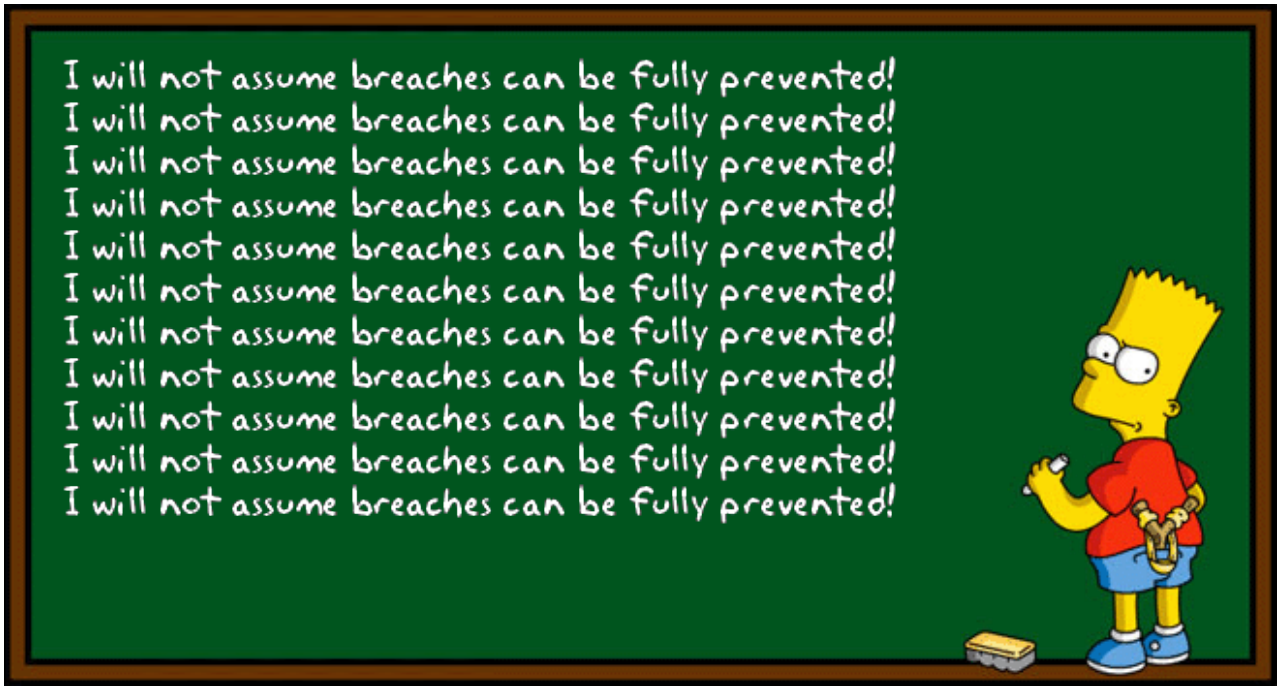
Large changes behind the crime scenes

- Criminals behind Angler and Nuclear EK busted. EK Traffic briefly down by 96%



Part 1: Plan For Breach Detection and Mitigation

Mistake 1: “We are not a target, we only get ransomware from time to time! That is it…”



+

Veil – Framework

↓

FUD

Mistake 2: “We purchased automatic breach prevention technology”

Do not fall for this false marketing

- If malware did not install and execute it was not a breach
- If malware got to install and execute, there is no automatic cleaning

But how do we know the technology is suitable for breach detection and mitigation?

- By examining the process!

Mistake 2: “We purchased automatic breach prevention technology”

If it looks like this:

- Our tool XXX will detect and block the breach trying to infect the organization
- Reporting is reviewed and policies are updated accordingly (monthly)

It is **NOT** breach detection and will not help bridging the gap by finding malware that managed to sneak into your organization

Breach Detection and Mitigation Workflow

- NBA detects C2 channel (or UBA or IoC scan)
- Global sandboxing provides file behavior context and estimate of likely missions
- Endpoint security tool identifies files responsible for C&C activity and spread
- Endpoint security tool quarantines malicious executables and their products
- Identity management tool quarantines the endpoint and identifies the user
- Endpoint security tool s used for root cause analysis before endpoint is re-imaged

Mistake 3: “Our security budget is fixed so we have to distribute the load somehow”

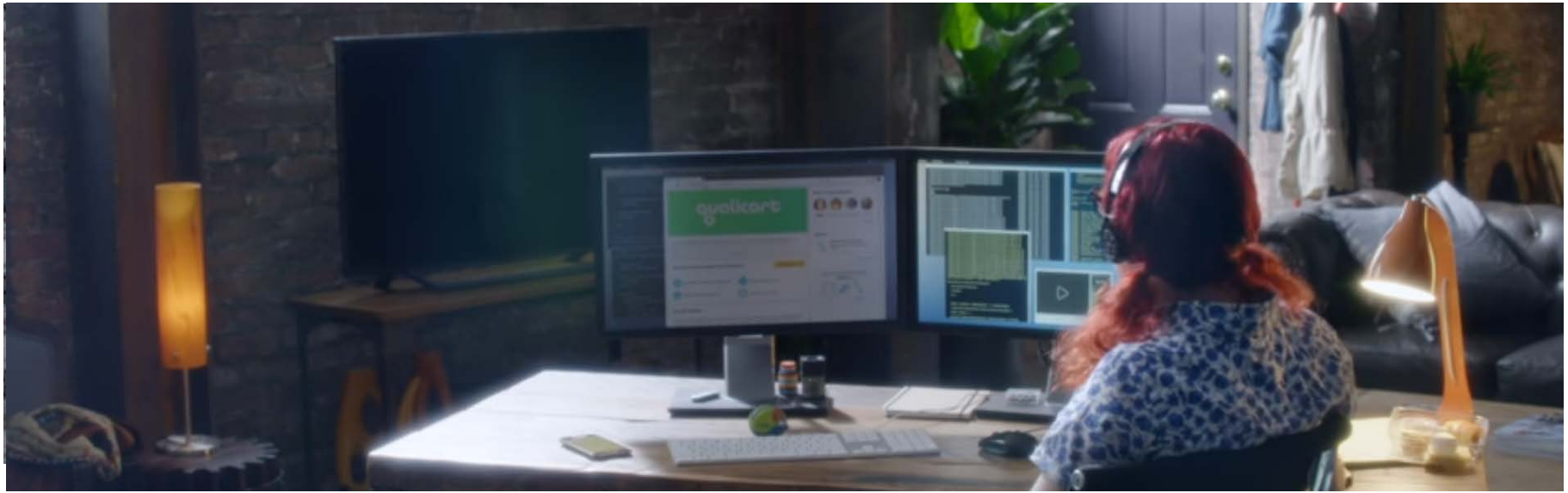
- If you have only 1$ security budget, spend it on visibility
- Expect need for security budget rise or re-allocation
- There will be need for new personnel (and skills)
- Some savings can be made, like SIEM OPEX costs with NBA/UBA
- Resources (books, trainings) are not yet readily available so pick a strong vendor that has experience with the process and can provide advice.

What is Coming in 2017: UBA

- **UBA** = User Behavioral Analytics
- Similar to network Behavioral Analytics but focused on **user modelling** and detection of anomalies within user activity
- **Detects: internal misuse or loss of resources, internal theft and identity impersonation**
- **Brings the needed level of sophistication**, analytics, and machine learning that data loss prevention systems are lacking

Our Advice: UBA vs Date Loss Prevention

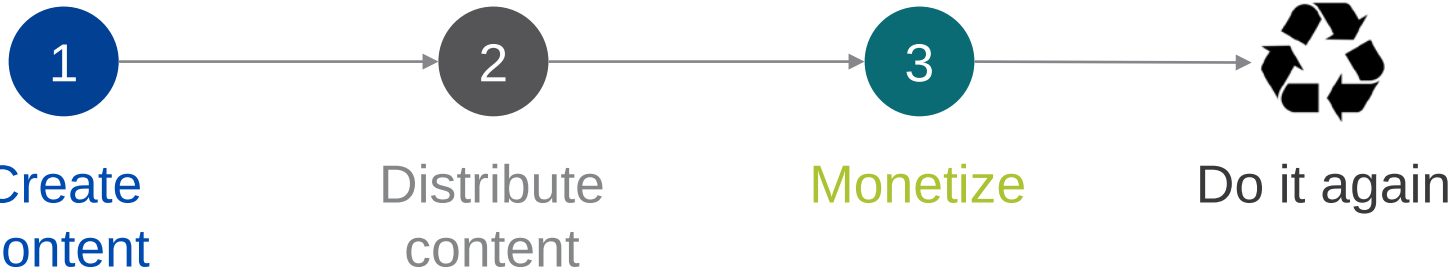
- **Wait** for UBA systems to become readily available before investing into company-wide data leak prevention systems
- **Current systems have significant disadvantages** and require you to costly micro-manage all your digital assets and harass your employees by police-like manners on every corner
- **UBA is far superior** by offering automatic modelling, correlation of activities and misuse of legitimate access. All in near real-time



Part 2: Knowing Your Enemy

Malware campaigns

≈ Marketing campaigns



1 Create content

Bypass AV

Bypass Webrep

Detection ratio: 10 / 56

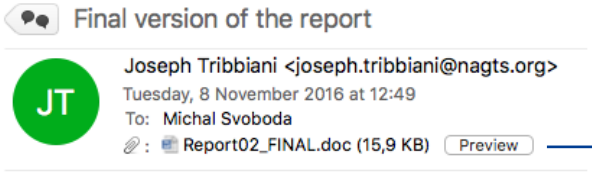
Analysis date: 2015-08-06 06:20:03 UTC (8 months, 3 weeks ago)

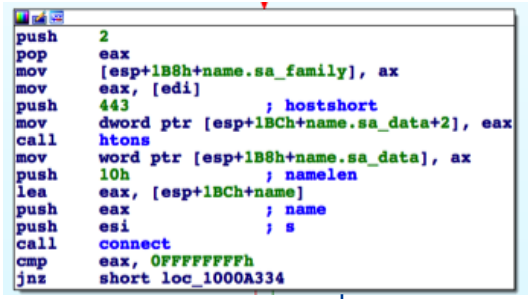
URL	USER AGENT	BYTES UP	BYTES DOWI	HTTP STATUS
http: // 136.243.24.249 / FDPIAFhQ68uGMnNDQR1 / SfKiJ8Iy / rHaDL8RC6r+3QhpTfYSHaH1VTdwsPmEW04M / 60MKWQLnPrF8IDCG…	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; ˜	0	260	200 = OK
http: // 136.243.24.249 / Jw7LAHs50mN8xnmNTh640iCX83MG5 / TLj3h736KMvcX2amo05ZsLMB7vZRN7nDp35RffSuHI7QobTMfbp3M…	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; ˜	0	264	200 = OK
http: // 136.243.24.249 / bu3PAOGchUPxL1dq70cS7L / bT69nFhz12RaUjme9r2x8mkepS2s0m3nl1wxENbJ83U1PO7QnUoViYr6IFUrR3w…	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; ˜	0	260	200 = OK
http: // 136.243.24.249 / wS7TANGnoD3ehgLXeBPTWEoFxXBRscK0yaOkb4ET / z1HJfeDVeEjU7QpqfFFg4rZ1IRMdaZJLYQH9Xur / 5w…	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; ˜	0	264	200 = OK
http: // 136.243.24.249 / 1H7VACAktxXOiWvOm+0hI1fb1Ta3WQDnnKE3y5XbKTonzt21c33LPwij5VqnPI2dYrUIN1EpDKoMJpole6 / OcEy…	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; ˜	0	260	200 = OK
http: // 136.243.24.249 / IhvYAHUm3JCLqs6qpWvC3IPipDEx7H2X7YKeYpW7eEKHPsaHGh+YSP6zWsW1fcZbtR0tfNmC0vsIXCoR3L6v…	Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.1; ˜	0	252	200 = OK

Traffic: **0 B up / 32.6 KiB down**, Blocked: **0.00%**, Requests: **125**, Duration: **1 day 4 hours 11 minutes 50 seconds**, User Agents: **1**, No Referrer: **100%**, HTTP: **200, 404**

2 Distribute content

Email, phishing





Dear Michal,

Alisha Calderon asked me to send you the attached document,which contains the final version of the report.
Please let me know if you have any trouble with the file, and please let Alisha know if you have any questions about the contents of the report.

Kind regards,

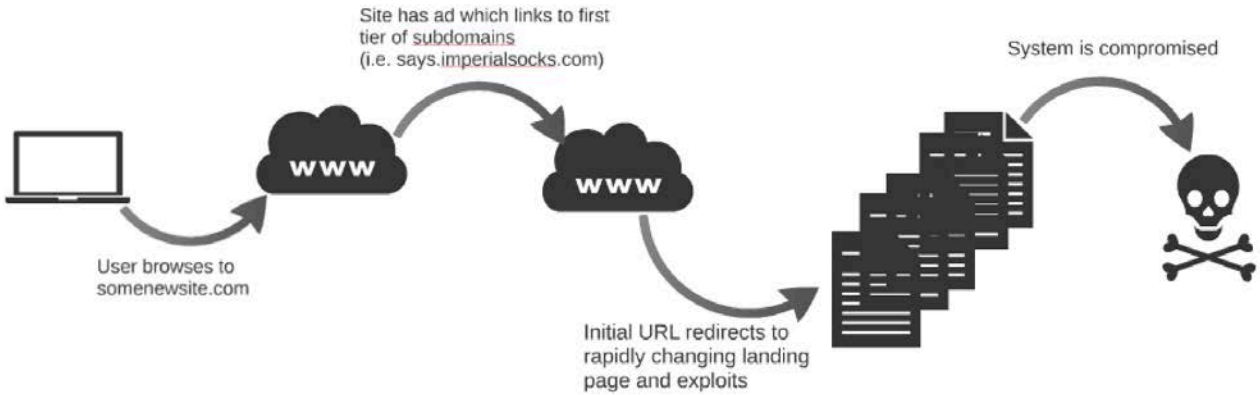
Joseph Gibson
Program Mgr, Operations

2 Distribute content

Web – exploit kits

Malvertising

Watering holes



3 Monetize

Ransomware

Targeted ransomware

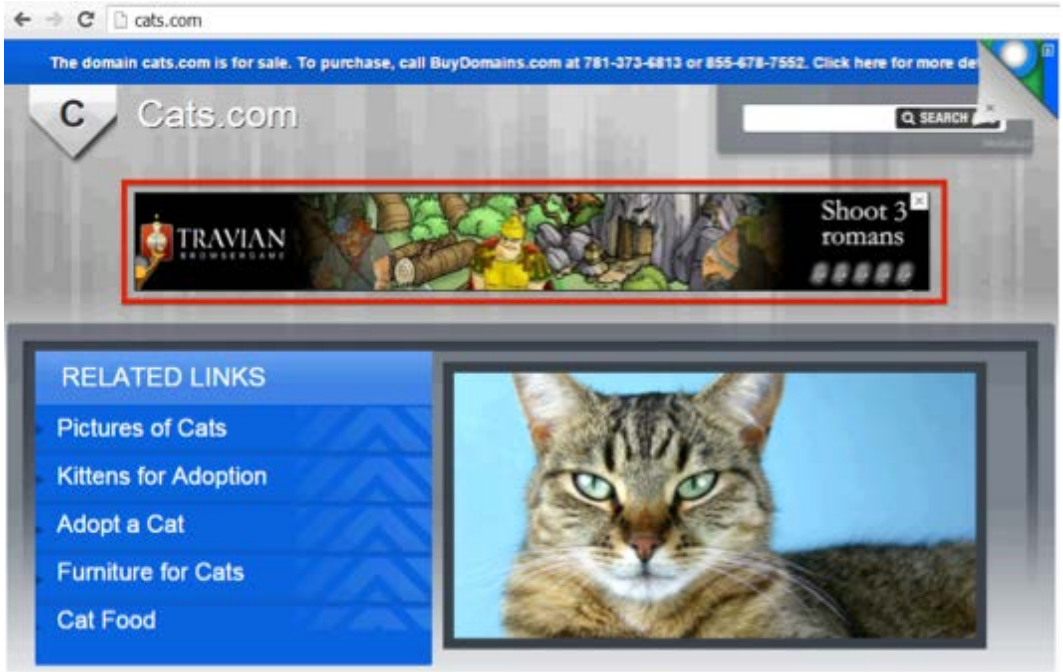
ВНИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
Подробности вы можете прочитать в файлах README.txt, которые можно найти на любом из дисков.

ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any of your disks.

3 Monetize

Ads

Click-fraud



3 Monetize

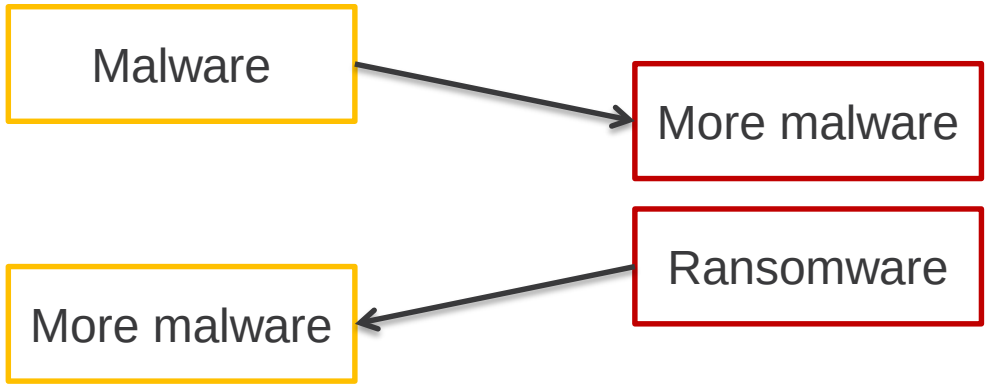
Steal data

Resell assets

Escalation

Reuse of distribution vectors

Reuse of infected assets




Thank You…
…and see you around
for more questions
JUDGMENT
DAY 11