

Applying Machine Learning to Cyber Security

CognitiveTank

Aldo Rodenhäuser

Head of Security Consulting

September 18, 2017



swiss made
software



Agenda



Situation Today



Approaches with ML



Putting It All Together



Conclusion





Situation Today

Increasing Trends



sign in become a supporter subscribe search jobs dating more International edition

UK world sport football opinion culture business lifestyle fashion

home > money property savings pensions borrowing careers

Scams

Sim-swap fraud claims another mobile banking victim

Chris Sims' account emptied and loan for £8,000 taken out as fraudsters continue to exploit way banks use customers' mobiles

Source: <https://www.theguardian.com>

Source: <https://securelist.com>

Booking a Taxi for Faketoken

By Victor Chebyshev on August 17, 2017. 9:00 am

MOBILE

GOOGLE ANDROID MALWARE DESCRIPTIONS MOBILE MALWARE TROJAN-BANKERS

The Trojan-Banker.AndroidOS.Fa...
ye contain overlay me...
int...
the malware, while its geographi...
mechanisms for about 2,000 fina...
mechanism for attacking apps fo...
Directorate for Road Traffic Safet...



watching porn in our house | Mariella Frost



Nemanja Matic's Manchester United move may leave Chelsea feeling blue | Daniel Taylor

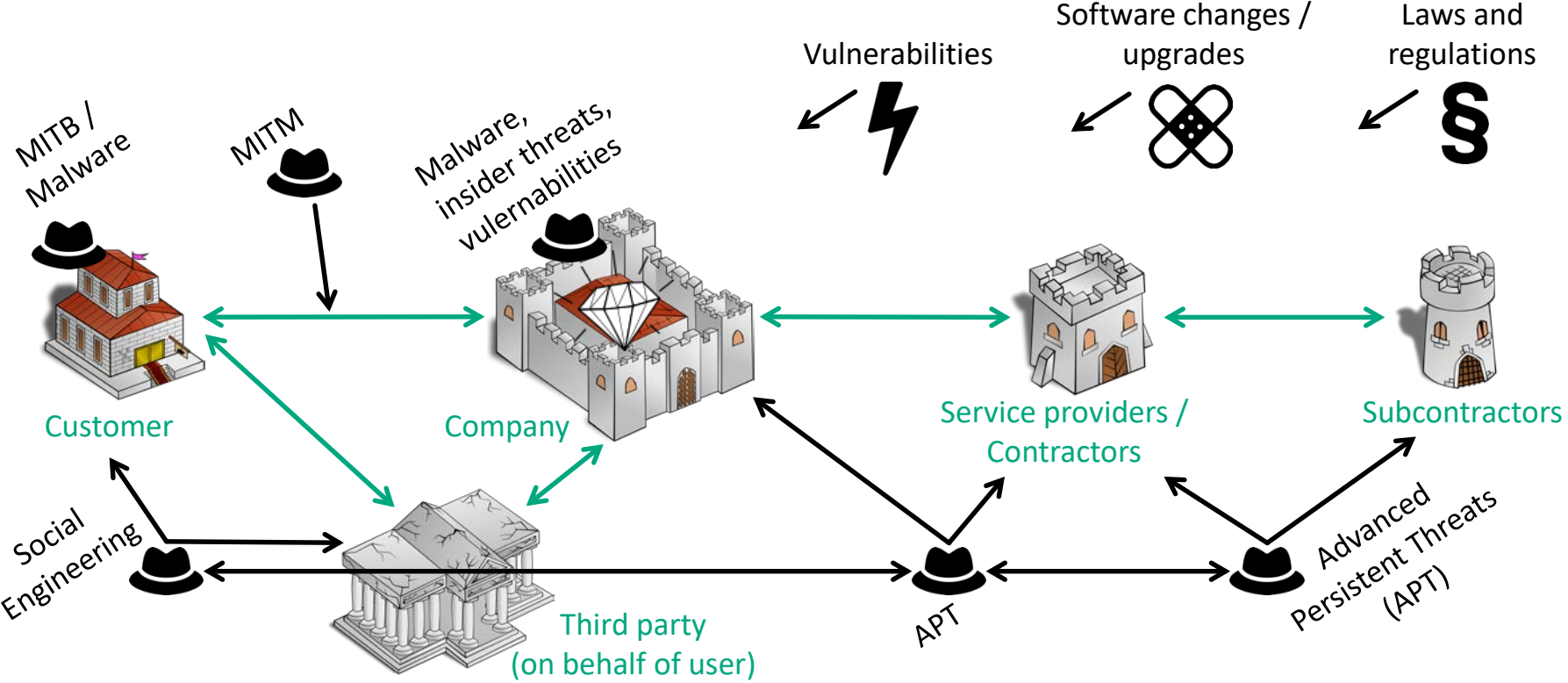
CRITICAL INFRASTRUCTURE BEING SOLD ON THE DARK WEB

POSTED BY: DEEPPDOTWEB AUGUST 14, 2017 IN FEATURED, NEWS UPDATES 2 COMMENTS

Cyber criminals on a darknet marketplace have taken hacking to another dimension this time around by bypassing the private computer networks of several government systems, gaining access to critical infrastructure targets such as hospitals, power plants, financial firms and airlines,

Source: <https://www.deepdotweb.com>

Enterprise Landscape



Challenges Today



- Cost of IT security (infrastructure, staff with a lot of manual tasks)
- Too many false positives of security events
- Too long incident and response time as well as resolution time
 - The more time required – the bigger the risks
- Getting the right security people
- Keeping up knowledge on new threats and vulnerabilities

→ Today's security measures cannot cope with today's business requirements



Approaches with ML

Categories of Available Data



Device and network information

- All information that is only influenced by the device of the user. In case of a web application, this might be e.g. the used OS or browser version.



Context information

- Through the physical context defined data, such as geolocation, time or noise.



Biometric information

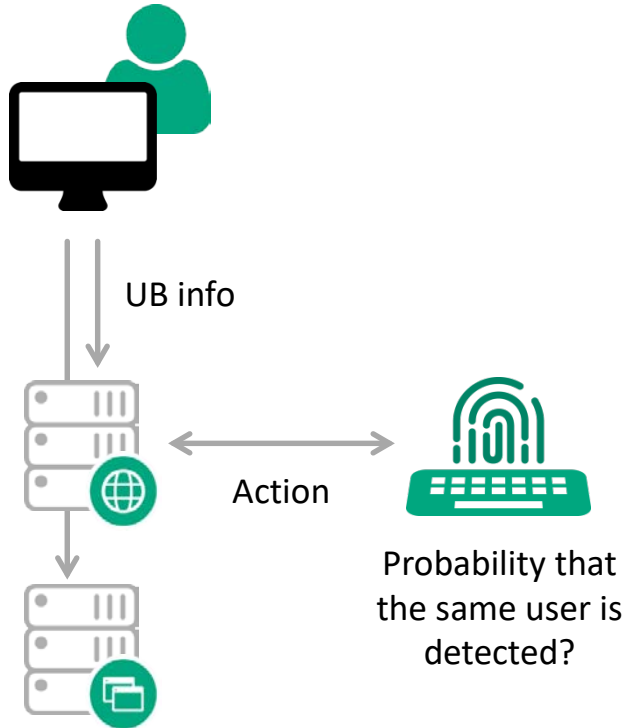
- Information that is defined by the user or its behavior itself, such as how the user looks or sounds and how he uses his keyboard or touchpad.



Application-specific information

- Transaction data and usage patterns

Biometric Information – User Behavior Analytics

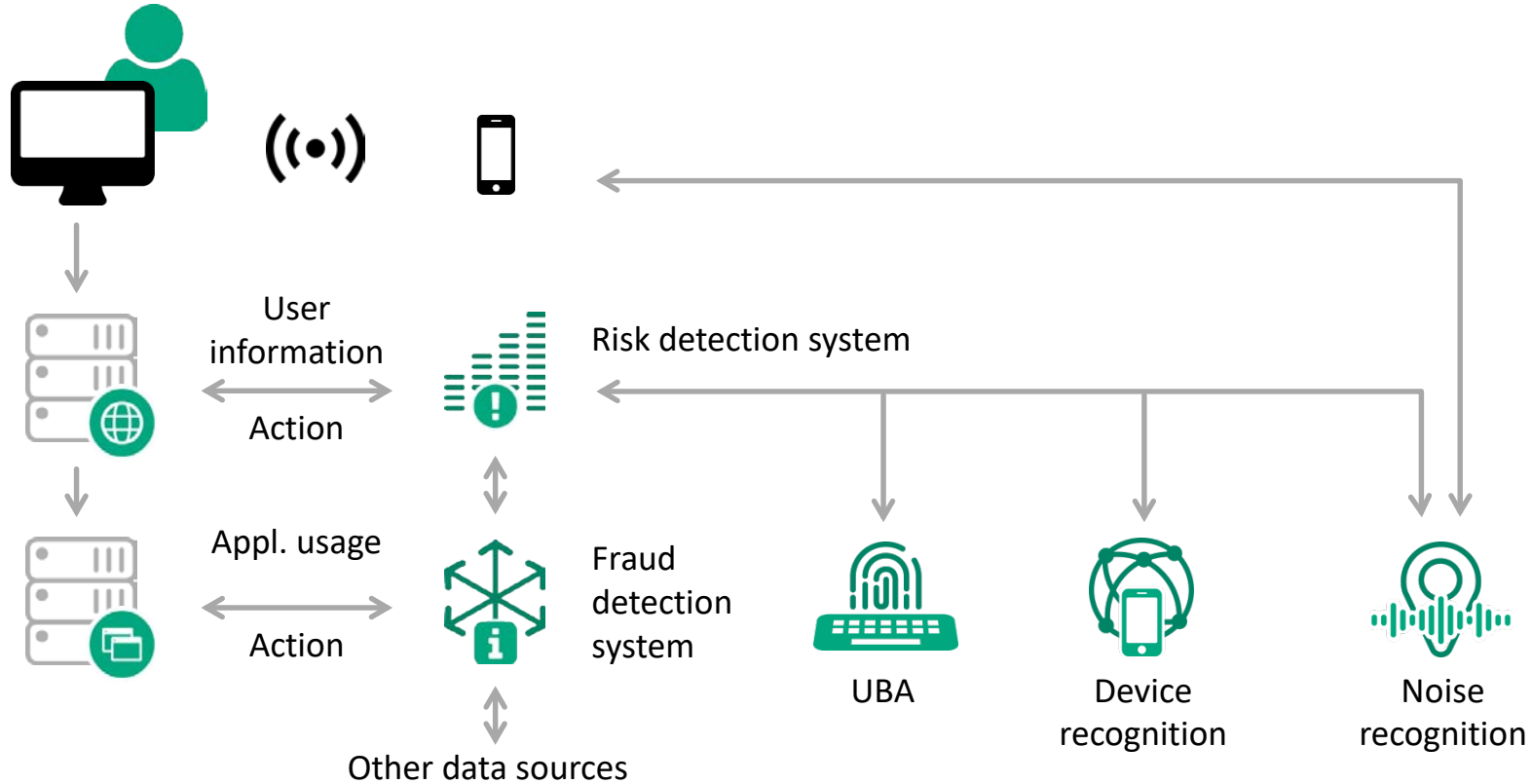


- User behavior analytics (UBA)
 - Keyboard interaction, device position, etc.
- User needs to train the system
- Profile required for each user and device
- Once the system is trained, the method is without user interaction
- Continuous authentication possible



Putting It All Together

Central Risk Detection System





Conclusion

What Did We Gain?



Threat	Measures today	Limitation with today's measures	Status Today	Status with ML
Customer / Employee impersonification	Two-factor authentication	Only at the start of a session; not compatible with "always logged on" mentality Stolen credentials can only be detected by the user	●	●
MITM (Network)	Transport Layer Security		●	●
Malware, MITB	AV, awareness trainings	Difficult to detect client-side malware Detecting 0-days is very difficult	●	●
Vulnerabilities (OWASP Top 10)	Secure coding; Web application firewall; keep up with patches	Almost impossible to get all things right	●	●
Social Engineering	Awareness trainings	Even after training – impossible to be aware of all forms of social engineering attacks	●	● ↑
Rogue employee	Monitoring, DLP		●	● ↑
Advanced Persistent Threats	Mix of above measures DLP tools (rule-based)	With current tools almost impossible to detect	●	● ↑

Aldo Rodenhäuser, Head of Security Consulting

aldo.rodenhaeuser@adnovum.ch

www.adnovum.ch



IT Consulting



Software Solutions



NEVIS



IT Security



Application Management