Data Security & Privacy

CIS 545

Security & Privacy Threats

Birhanu Eshete
birhanu@umich.edu

Lecture Goals

- **Security & privacy threat vectors**: social engineering, malware, exploit kits, ransomware, APTs, …
- **Security & privacy threats in data-driven ecosystems**: online platforms, cloud, IoT, …

S&P Threat Vectors: Conventional

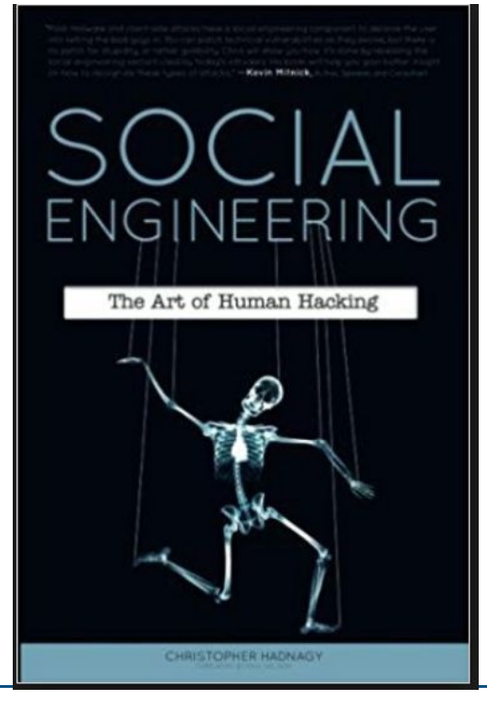
- Social Engineering
- Malware
- Exploit Kits
- Ransomware
- Advanced Persistent Threats

S&P Threats: Data-Driven Ecosystems

- Online Social Networks (e.g., Facebook)
- Online Retailers (e.g., Amazon)
- Search Engines (e.g., Google)
- Cloud (IaaS, SaaS, PaaS, MLaaS, …)
- IoT

Social Engineering

- exploiting the human nature and manipulating people so they give up sensitive information
- Why popular? easier to exploit natural tendency to trust than to discover security weakness in a system
- a broad concept, and includes all kind of ways and methods to exploit humans w.r.t. technology



Flavors of Social Engineering

- Phishing
- Baiting
- Tailgating
- Quid Pro Quo
- Pretexting
- SMishing
- Vishing

Phishing

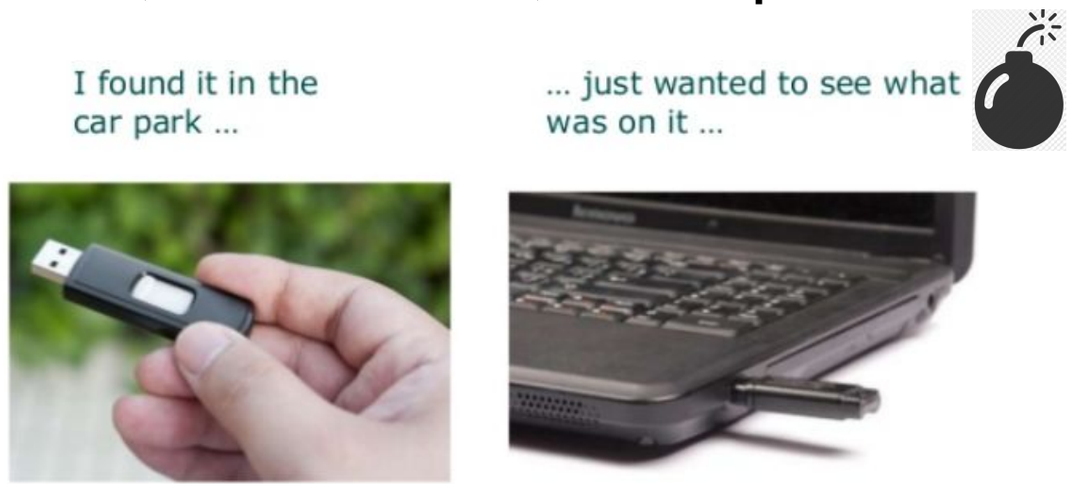
- **Idea**: fraudulent emails, text messages and websites to look like they are from authentic companies (e.g., your bank, your school, your hospital)

- **Goal**: to steal account credentials, PII, and financial information

- highly prevalent because it requires little effort from the bad guys

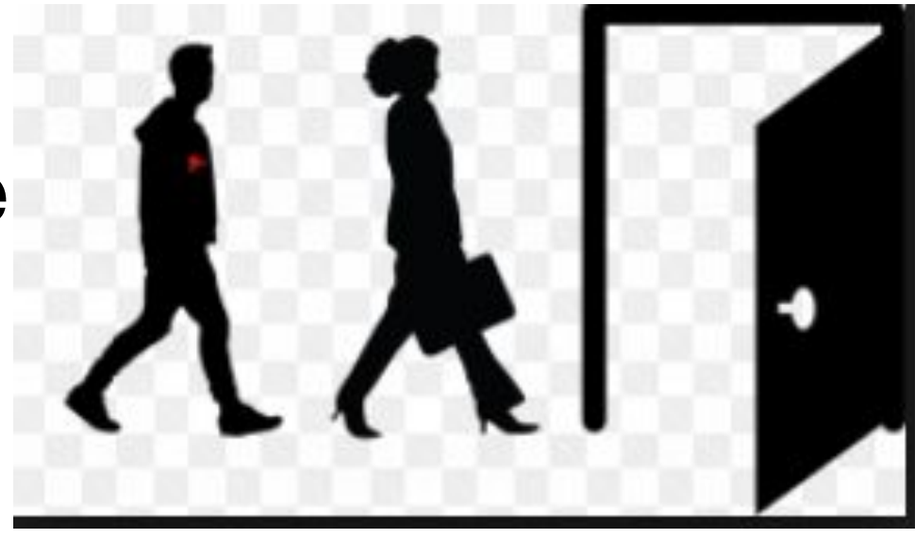
Baiting

- **Idea**: exploit the curiosity or greed of unsuspecting victims
- **Popular strategy**:
  - a hacker plants a USB stick loaded with malware and leaves it somewhere (e.g., lobby, parking lot)
  - an employee picks it up and realizes it has the logo of a rival company
  - the curious employee puts the USB stick in his computer and ….
- **Goal**: infection/compromise, exfiltration, corruption/disruption



Tailgating

- **Idea**: an attacker seeking entry to a restricted area, where access is controlled by electronic access control
- **Popular strategy**: simply walk in behind a person who has a legitimate access
- **Goal**: physical access to the target
- **Opportunities with physical access**: stealing information, installing spying tools, or render the equipment dysfunctional



Quid Pro Quo

- **Idea**: promise a benefit in exchange for information

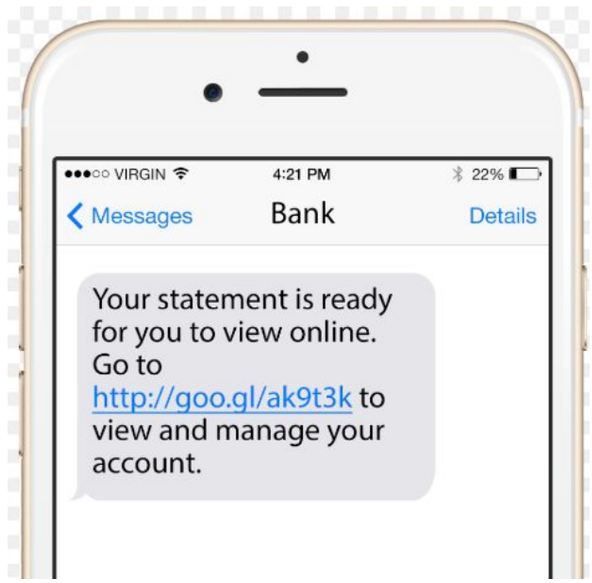
- **Goal**: scamming users for financial gains, identity theft etc.

Pretexting

- **Idea**: attacker creates a fictional backstory that is used to manipulate someone into providing private information
- **Popular strategy**: pretend they need certain information from their target (e.g., to confirm identity)
- **Goal**: after getting victim's info: initiate attack (e.g., stealing the victims' identity, malware infection)

SMishing

- **SMS phishing**: an emerging security threat
- **Strategy**: uses SMS to trick victims into taking an immediate action
- **Goal**: steal sensitive information, confidential data, or compromise a device



Vishing

- **Voice phishing**: phishing done over the phone
- **Strategy**: trick victims into revealing critical financial or personal information
- Works like phishing but does not always occur over the Internet and is carried out using voice
- **Goal**: steal sensitive information, confidential data, identity theft

Malware

- **Malware**: any kind of malicious software or program
- **Goal**: infect your devices by using computer viruses, worms, Trojan horses, spyware, adware, etc
- **Manifestations**: popping up ads, crypto-mining, alter or delete files, steal your data, covertly monitor all your activities, etc

Variants of Malware

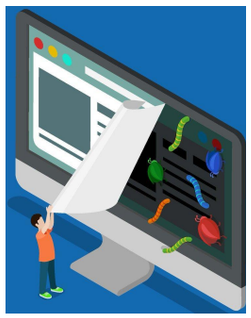
- **Spyware**: monitors your activity covertly
- **Adware**: often come as ‘free’ download and are installed automatically with/without your consent
- **Worm**: computer programs that have the ability to replicate themselves
- **Trojan Horse**: disguises itself as, or embeds itself within, legitimate software

Malware Comes in Many Flavors

Malware

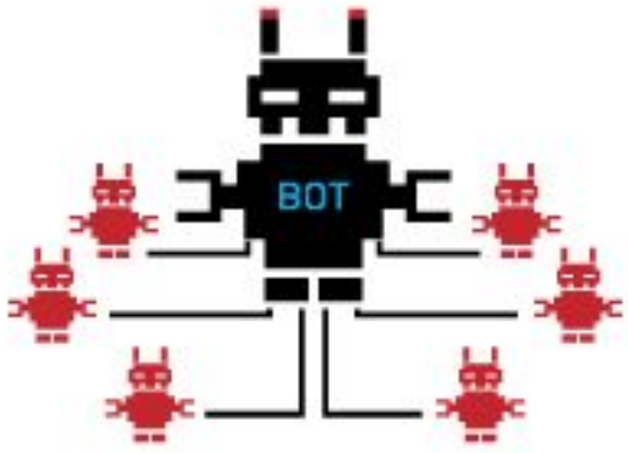
Ransomware

Banking Trojan



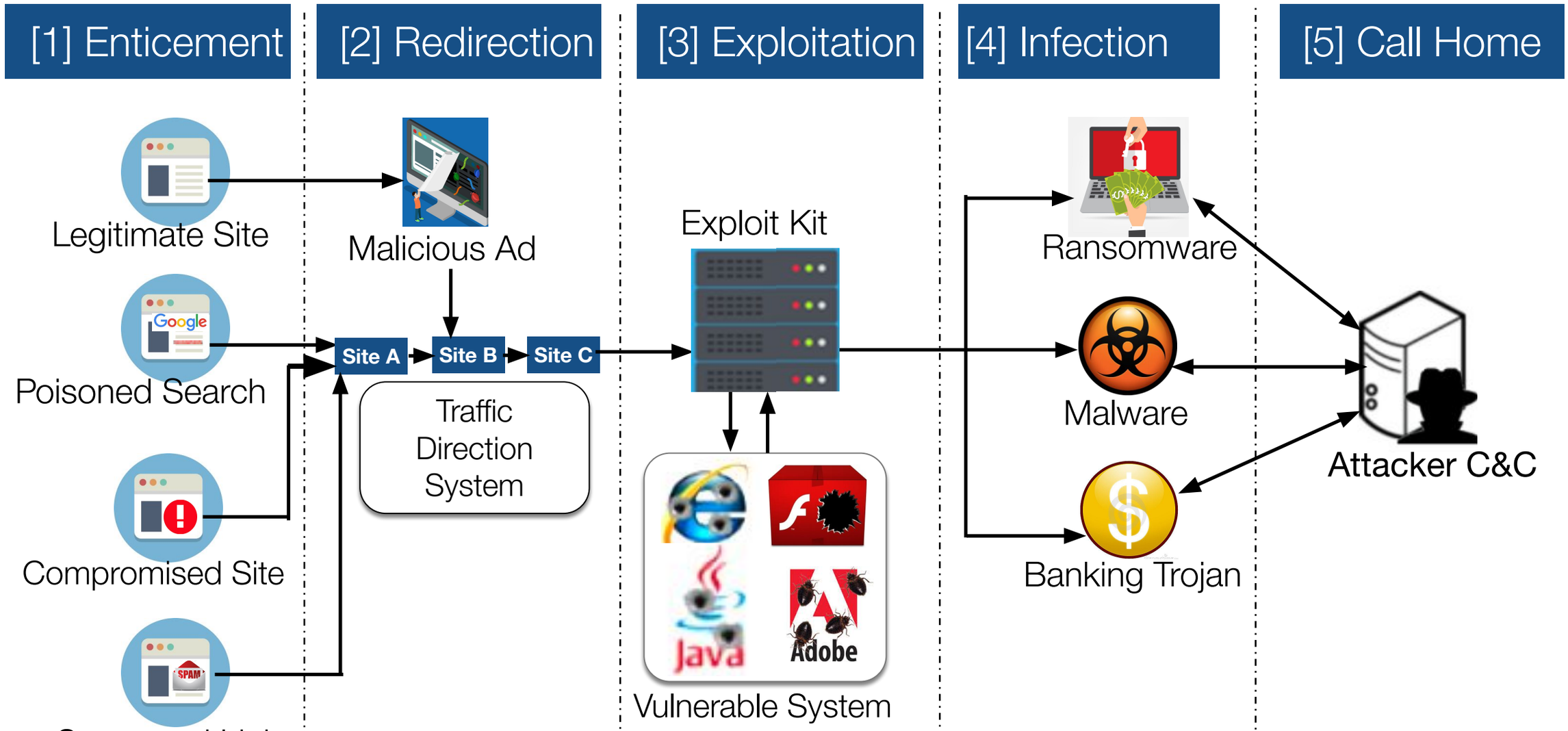
Malicious Ad

Exploit Kit



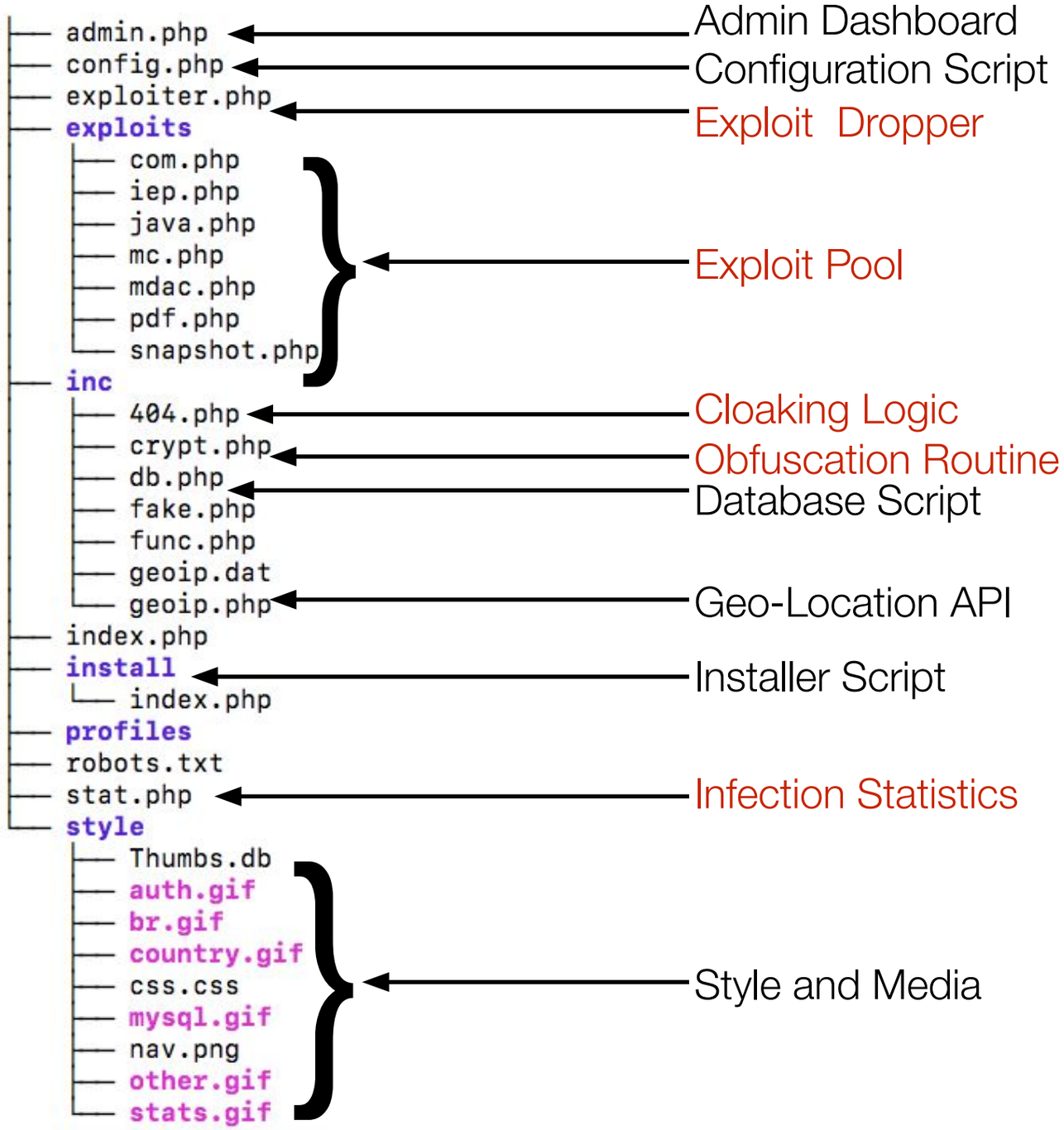
Botnets

Exploit Kit Infection Chain



- Victim lured via drive-by-download / social engineering
- TDS auto-redirects victim behind the scene
- EK scans browser & extensions for exploitable vulnerabilities
- EK drops & executes malware payload on victim system
- Malware phones home to exfiltrate info & receive further commands

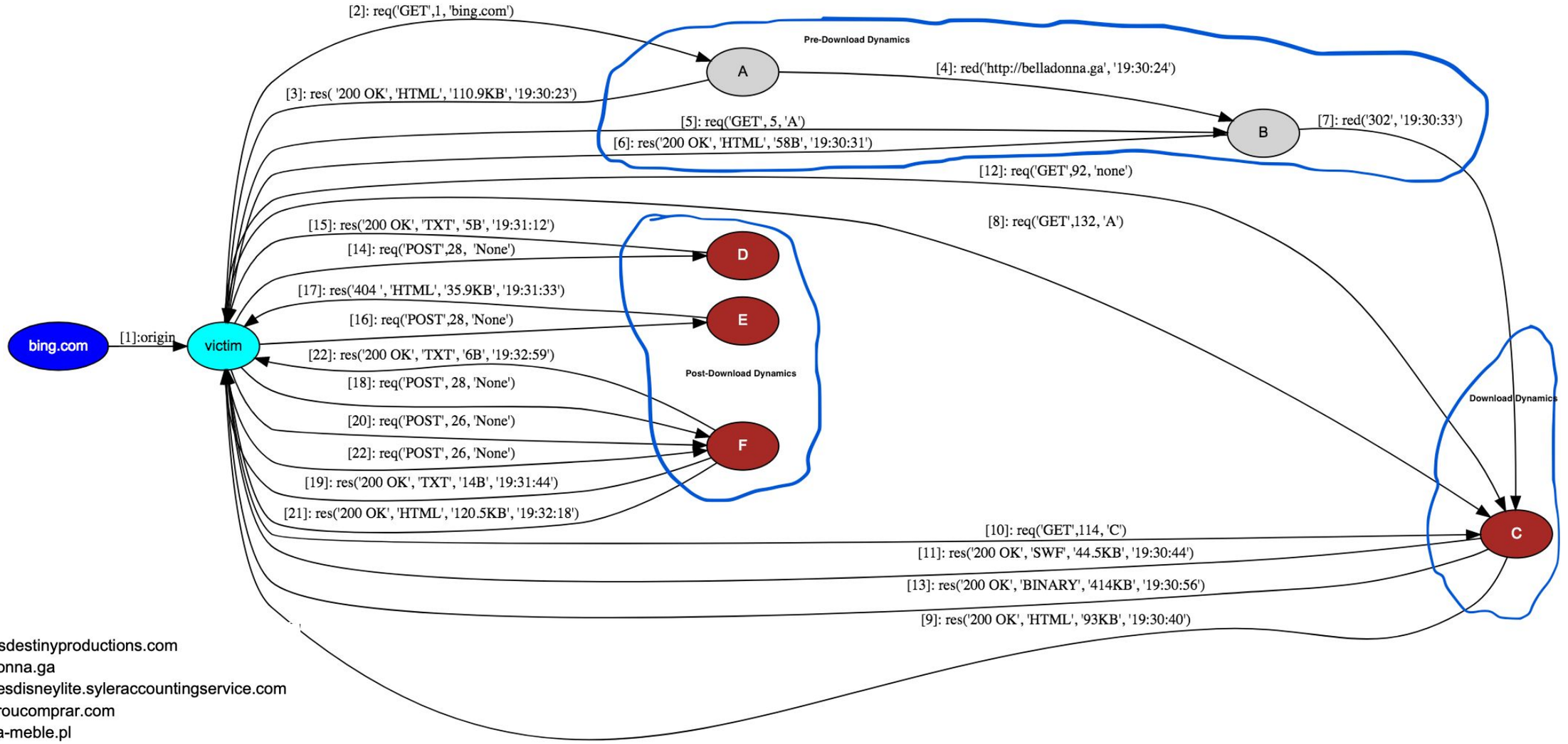
Typical Exploit Kit Structure



Marketed with Colorful ‘Brands’

- **License**: annual, single-domain, multi-domain, SaaS
- **Tech support**: as in legitimate software

Real Exploit Kit Infection Flow

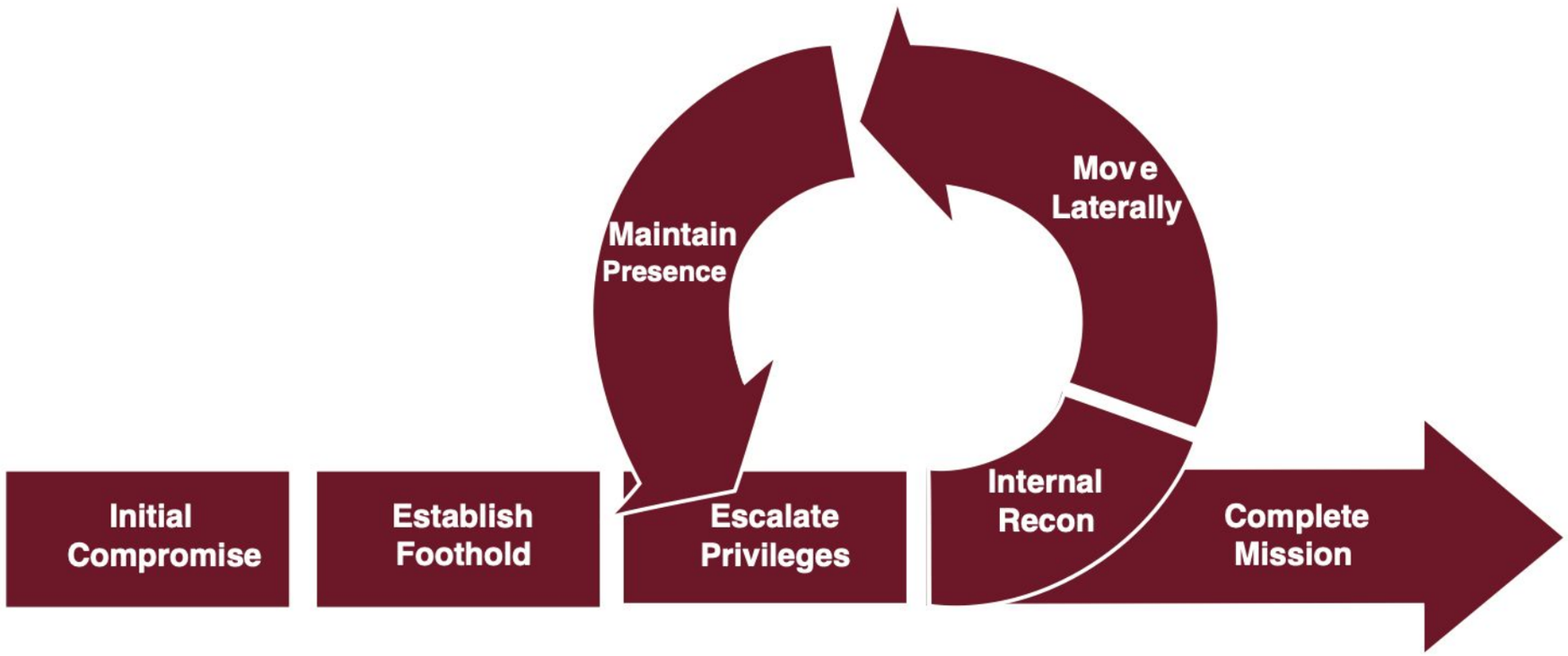


A: http://reneesdestinyproductions.com
B: http://beladonna.ga
C: http://sviteresdisneylite.syleraccountingservice.com
D: http://baixaroucomprar.com
E: http://acadia-meble.pl
F: http://balustradydrewniane.pl

Angler Exploit Kit serving CryptoWall ransomware on 12/21/2015

Paper: Birhanu Eshete, V.N. Venkatakrishnan. "**DynaMiner: Leveraging Offline Infection Analytics for On-the-Wire Malware Detection**". 47th IEEE/IFIP International Conference on Dependable Systems and Networks, 2017.

Advanced and Persistent Threats (APTs)



- advanced threat groups (usually nation backed agencies, or skilled hacker groups with lots of resources
- **Goal**: cyber espionage, and other targeted high-level (harmful) objectives such as information warfare

Real APT Infection Flow

Scenario-2: Trojan. This attack scenario (Fig. 19) begins with a user downloading a malicious file. The user then executes the file. The execution results in a C&C communication channel with the attacker's machine. The attacker then launches a shell and executes some information gathering commands such as *hostname*, *whoami*, *ifconfig*, *netstat*, and *uname*. Finally, the attacker exfiltrates some secret files.

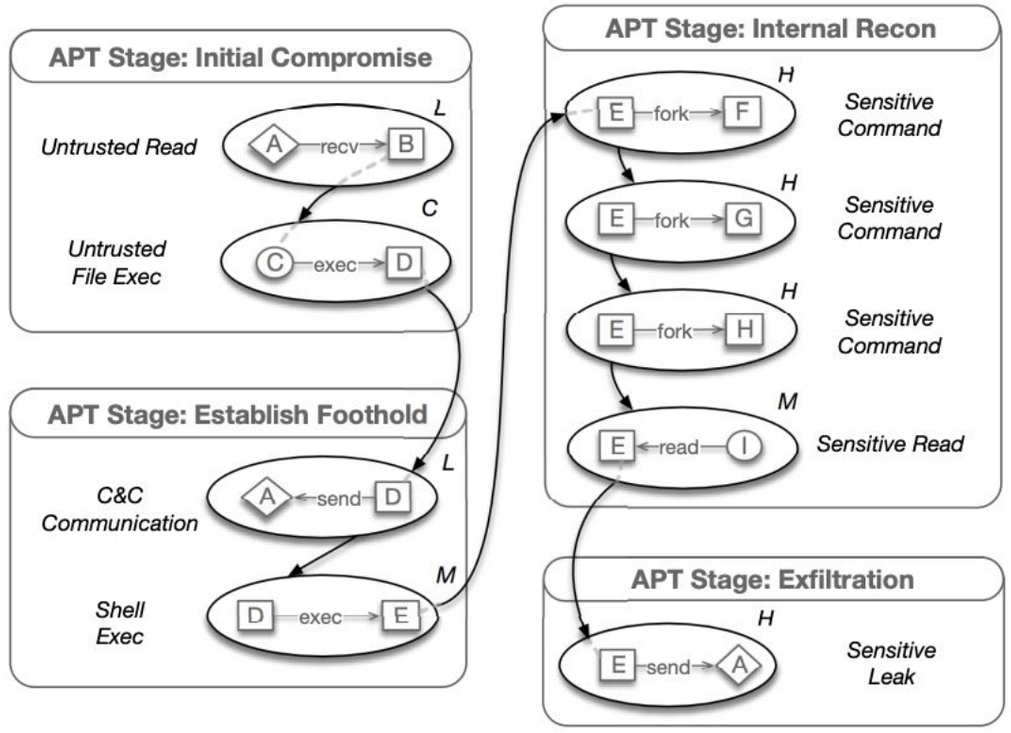


Fig. 19. HSG of Scenario-2. Notations: A= Untrusted External Address; B= Firefox; C= Trojan File (diff); D= Executed Trojan Process; E= /bin/dash; F= ifconfig; G= hostname; H= netstat; I= password.txt;

Paper: Sadegh M. Milajerdi, Rigel Gjomemo, Birhanu Eshete, R. Sekar, V.N. Venkatakrishnan. "**HOLMES: Real-time APT Detection through Correlation of Suspicious Information Flows**". 40th IEEE Symposium on Security & Privacy, 2019.

OSN Security & Privacy Threats

- **On OSN users**:
  - isolated, targeting a small population (random or specific)
- **On the OSN**:
  - aimed at the service provider itself, by threatening its core business

Attacks on OSN Users (1/3)

- **From other users**:
  - interaction with strangers (mere acquaintances)
  - interaction with trusted but compromised friend(s)
- **Note**: some of these users may not even be humans (e.g., social robots, crowdsourcing workers)

Attacks on OSN Users (2/3)

- **From social apps**:
  - potential disclosure of more than what applications need
  - exploit users' browsers, XSS attacks, form a botnet to launch attacks such as DoS, propagate malware, send spam, …
  - access private user data, store, and send to advertising and Internet tracking companies (violation of privacy)
  - unfortunately, any data harvested by third-party apps are beyond the control of the OSN site
  - platforms (e.g., Facebook) give coarse-grained access-control for 3rd-party apps (fine-grained is advisable)

Attacks on OSN Users (3/3)

- **From the OSN**:
  - abuse of full control over user's information in exchange for the services provided by the OSN
- **De-anonymization and inference attacks**:
  - OSN services: publish anonymized social data for others (e.g., researchers, advertisers) to analyze
  - Attacker: de-anonymize social data and infer attributes that the user did not even mention in the OSN (e.g., sexual or political orientation inferred from association with others)

Attacks on the OSN (1/3)

- **Sybil Attacks**:
  - fake identities used to out-vote honest users (e.g., influence online ratings, manipulate search results)
  - compromise existing accounts or generate fake (Sybil) accounts
  - compromised: can exploit established trust among friends

Attacks on the OSN (2/3)

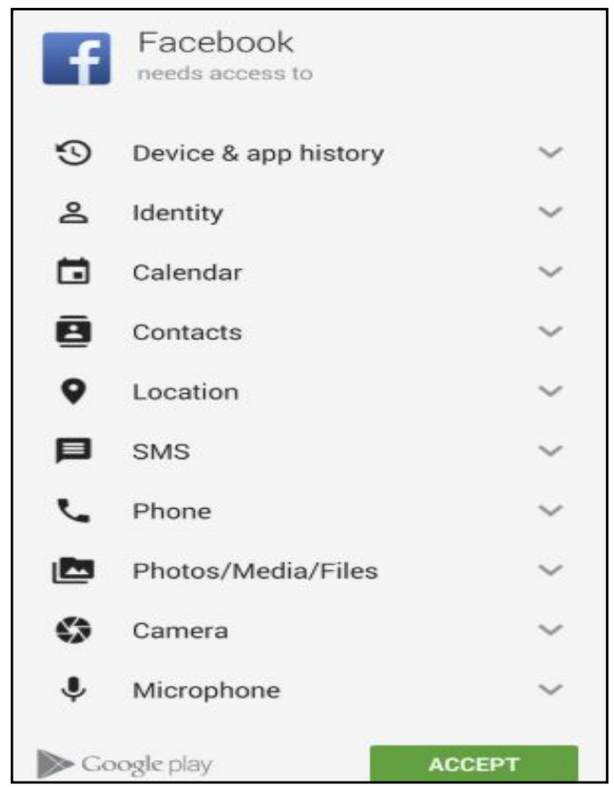
- **Crawling Attacks**:
  - Large-scale distributed data crawlers from data aggregators exploit the OSN-provided APIs or scrape publicly viewable profile pages to build databases from user profiles and social links
  - Professional data aggregators sale such databases to insurance companies, background-check agencies, credit-ratings agencies, etc
  - Crawling users' data from multiple sites and multiple domains increases profiling accuracy
  - Profiling might lead to "public surveillance", where an overly curious agency (e.g., government) could monitor individuals

Attacks on the OSN (3/3)

- **Social Spam**:
  - contents or profiles that an OSN's "legitimate" users don't wish to receive (e.g., phishing attacks, unwanted commercial messages)
  - spreads rapidly due to the embedded trust relationships among online friends
- Distributed Denial-of-Service Attacks:
  - a large amount of seemingly inoffensive service requests that overload the service and deny access to legitimate OSN users
- Malware Attacks:
  - malware propagation is rapid due to the trust relationships in OSNs

Social Apps vs. Permissions

- Rich set of permissions granted by innocent users
- Users unaware of personal details they are giving away
- Harvesting private information to sell to cyber-criminals
- Apps packaged with malware that steals your critical banks
- On mobile phone: erase your data or impersonate you



Online Retailers

- **Every time you go shopping online:**
  - you share intimate details about your consumption patterns with retailers
- **They use them to figure out:**
  - what you like, what you need, coupons most likely to make you happy

What Amazon Knows About You

- name, address, phone numbers, credit card information
- "people to whom purchases have been shipped, including addresses and phone number”
- "people (with addresses and phone numbers) listed in 1-Click settings”
- "e-mail addresses of your friends and other people”
- "content of reviews and e-mails to us”
- "personal description and photograph in Your Profile”
- "financial information, including Social Security and driver's license numbers”

What Amazon Knows About You…

- "IP address used to connect your computer to the Internet”
- login, your email address, your Amazon password
- "browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform”
- "purchase history”, "full URL clickstream to, through, and from our Web site, including date and time”, "products you viewed or searched for”

What Amazon Knows About You…

- “the phone number you used to call our 800 number”
- "session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page”
- "information about your location and your mobile device, including a unique identifier for your device”

And So Much More …

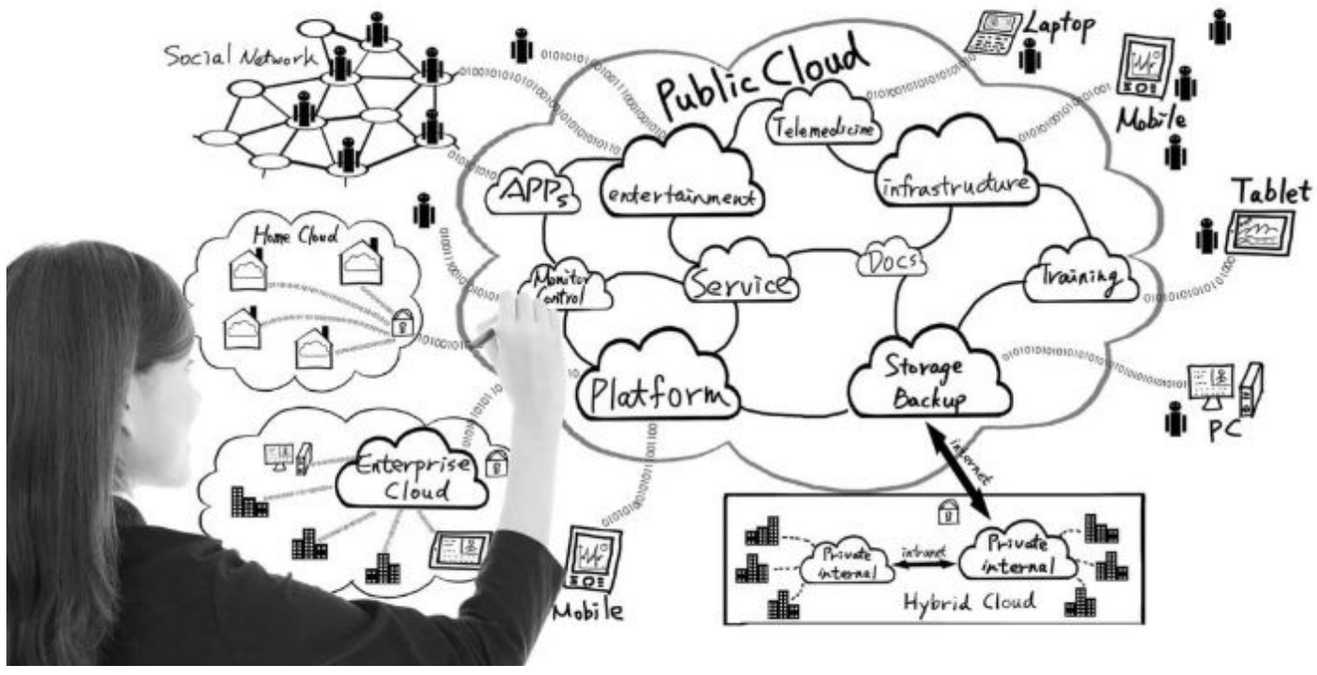
- Via Alexa: transcripts of voice interactions
- The goal: "improve the accuracy of the results provided to you and to improve our services."
- But, not clear what "improve our services" means
- Amazon swears: it is "not in the business of selling [Information about our customers] to others"
- Does that sound familiar?
- Oh! yes, Facebook "didn't sell any personal data to Cambridge Analytica", either
- Amazon shares your data with: Starbucks, OfficeMax, Verizon Wireless, Sprint, T-Mobile, AT&T, J&R Electronics, …

Staring deep into your digital soul!

What Google Knows About You

- Pretty much your digital footprint:
  - things you search for, websites you visit, videos you watch, ads you click on or tap, your location, device info., IP @ & cookie data, emails on Gmail, contacts you add, calendar events, photos and videos you upload, docs, spreadsheets, and slides on Drive, name, email address and password, birthday, gender, phone number, country
- Also likely knows:
  - most places you've physically been since you started using its services, what you search for day in and day out, and your entire digital network (among plenty of other personally revealing tidbits)

Security & Privacy Issues in the Cloud (1/2)



- IaaS
- SaaS
- PaaS
- MLaaS

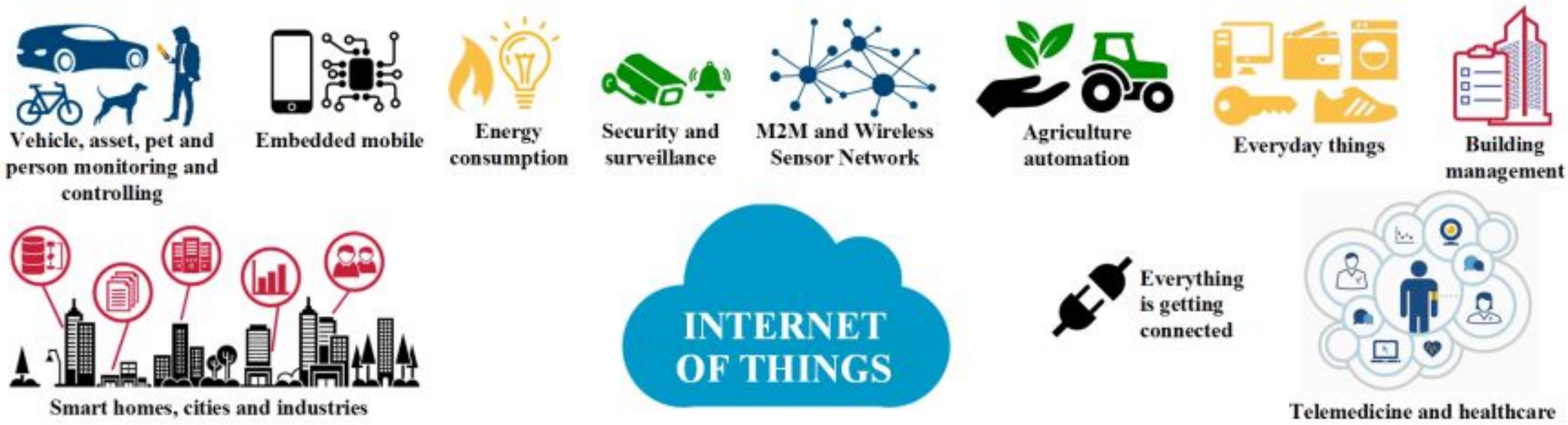
- **Data breaches**: due to the massive data stored in the cloud
- **Network security**: security data is migrated to SaaS providers
- **Data locality**: data storage and processing on the premises of the cloud provider

Security & Privacy Issues in the Cloud (2/2)

- **DoS attacks**: to overpower resources of the cloud service
- **System vulnerabilities**: flaws in the cloud infrastructure and protocols (e.g., authentication, encryption)

- **Compromised credentials**: stolen/hijacked accounts leveraged by cyber-criminals
- **Malicious insiders**: previous employee, contractor, or accomplice

Security Risks in IoT



- **Security vulnerabilities**: devices ship with vulnerabilities
- **Insecure communications**: unauthenticated, unencrypted, lack of network isolation
- **Data leaks**: from the cloud, from and between devices
- **Exposure**: to malware infection and other forms of abuse
- Potential for service **disruption**
- Lack of frequent software **update**

Privacy Risks in IoT

- **Identity disclosure:**
  - device may transmit PII
  - device transmissions may be recognizable
- **Location disclosure:**
  - device may transmit its explicit location
  - device may be traceable through its communications
- **Data confidentiality:**
  - cloud services may contain records full of PII

Privacy Risk Mitigation

- **Identity disclosure:**
  - pseudonym
  - connection anonymization
- **Location disclosure:**
  - pseudonym
- **Data confidentiality:**
  - no direct access to PII from devices
  - secure data center / cloud resources

Examples: IoT Security & Privacy Pitfalls

- **2017**: 120K IP cameras at risk of attack (zero-days to access and UPnP to connect to device)

- **2016**: over 900K routers compromised in Germany (Mirai botnet leveraged default credentials to change router's firmware)

Allestoerungen.de and OpenMaps

- **2015**: Jeep Cherokee hacked remotely (zero-day allowed remote control)

Lecture Summary

- Social engineering, malware, exploit kits, ransomware, APTs, … evolve as we speak
- OSNs pose a lot of S&P risks
- Online retailers such as Amazon know a great deal about us
- Google knows almost all of our digital footprint
- New paradigms such as cloud and IoT have a several S&P blind spots (old and new)

References & Further Reading

- A Survey on Privacy and Security in Online Social Networks: https://arxiv.org/pdf/1504.03342.pdf
- The Red-Book: http://www.red-book.eu/m/documents/syssec_red_book.pdf
- Security and Privacy Issues in the Cloud Computing Environment: https://www.omicsonline.org/open-access/security-and-privacy-issues-in-cloud-computing-environment-2165-7866-1000216-96442.html
- The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved: https://arxiv.org/pdf/1802.03110.pdf
- Malware Variations: https://blog.mailfence.com/viruses-spywares-malware-botnets-protect/
- Various Threats: http://www.ict4u.net/security/threats.php