PA197 Secure Network Design
1. Faults, Threats, Attacks

Eva Hladká, Luděk Matyska

Faculty of Informatics

February 22, 2023

Content

Faults and Failures

- All systems susceptible to failures
- Failure resilience mandatory part of the design
  - unfortunately not true for most commercial systems/networks today
  - resilience goes with a cost
  - not possible to build absolute resilience
- Faults: some flaws in the system
  - but sometimes left by design, e.g. just one router for a small network
- Failures: emergent faults
  - Random faults: occurrence unpredictable (probability)
  - Induced (domino): e.g. link disconnection leads to higher service failure
  - Malicious: results of attacks (usually use some (known) flaw)

Internet

- Physical
  - components faults and failures
  - hardware level, but includes immediate software components
    - e.g. active element operating system fault or failure
- Protocols
  - software layer
  - shortcomings (limits) of protocols
  - bugs: incidental and malicious failures
- Applications
  - software layer

Selected failure examples

- Topology failures
- Overload
- Integrity
- Software faults

Topology failures

- Cable failures
  - terrestrial
  - sub-marine
- Sub-marine cable threats
  - fishing and anchoring
  - natural disasters
    - earthquake 27th December 2006 damaged the cables near Taiwan, leading to disruption of Internet and telephone service in Asia Pacific region
    - Hong Kong completely cut off
  - theft
    - March 2007, 11 km section of cable connecting Thailand, Vietnam, and Hong Kong removed
    - Internet speed affected in Vietnam

Topology failures II

- Routing problems
  - link disconnection and/or node failure
- Router failures
  - (D)DoS attacks
  - software bugs
    - example: too long BGP Autonomous Systems paths
- Recovery times:
  - hundreds of milliseconds for intra-domain routing (e.g. OSPF)
  - minutes for inter-domain routing (BGP)
- Pakistan "black hole" in 2008 after banning YouTube
  - propagated through the mis-configuration to the whole world
  - see e.g. `https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-su`

Overload failures

- Result of limited capacity of network equipment
  - congestion (flash/short/long term)
- TCP has congestion control
  - however independent of routing
  - simply slowing down instead of re-routing
    - one of motivations for Software Defined Networks (SDN)
- Flash Crowds versus (D)DoS attacks
  - how to distinguish unusually high but legitimate traffic from malicious traffic?

Software faults

- Bugs in software
  - development phase
  - buffer overflow most prominent example
- Bugs in configuration
  - deployment phase
  - could have wide (global) effect
    - Pakistan/YouTube, Google search, ...

Ad-hoc, mobile and vehicular networks

- In some aspects similar to Internet
  - the mobility introduces additional complexity/source of failures
- Hardware level
  - component faults
    - more fragile "active" elements
    - frequent failure a property
  - disconnection due to distance
    - not possible to distinguish from a failure
- Protocols
  - reliable routing problem
  - link failure a property, not an exceptional event

Sensor networks

- Static nodes, but high probability of failure of any individual node
- Limited life span of a node
  - battery drainage
- Interference
- Routing and transmission protocols
  - redundancy versus energy conservation

Threats—Overview

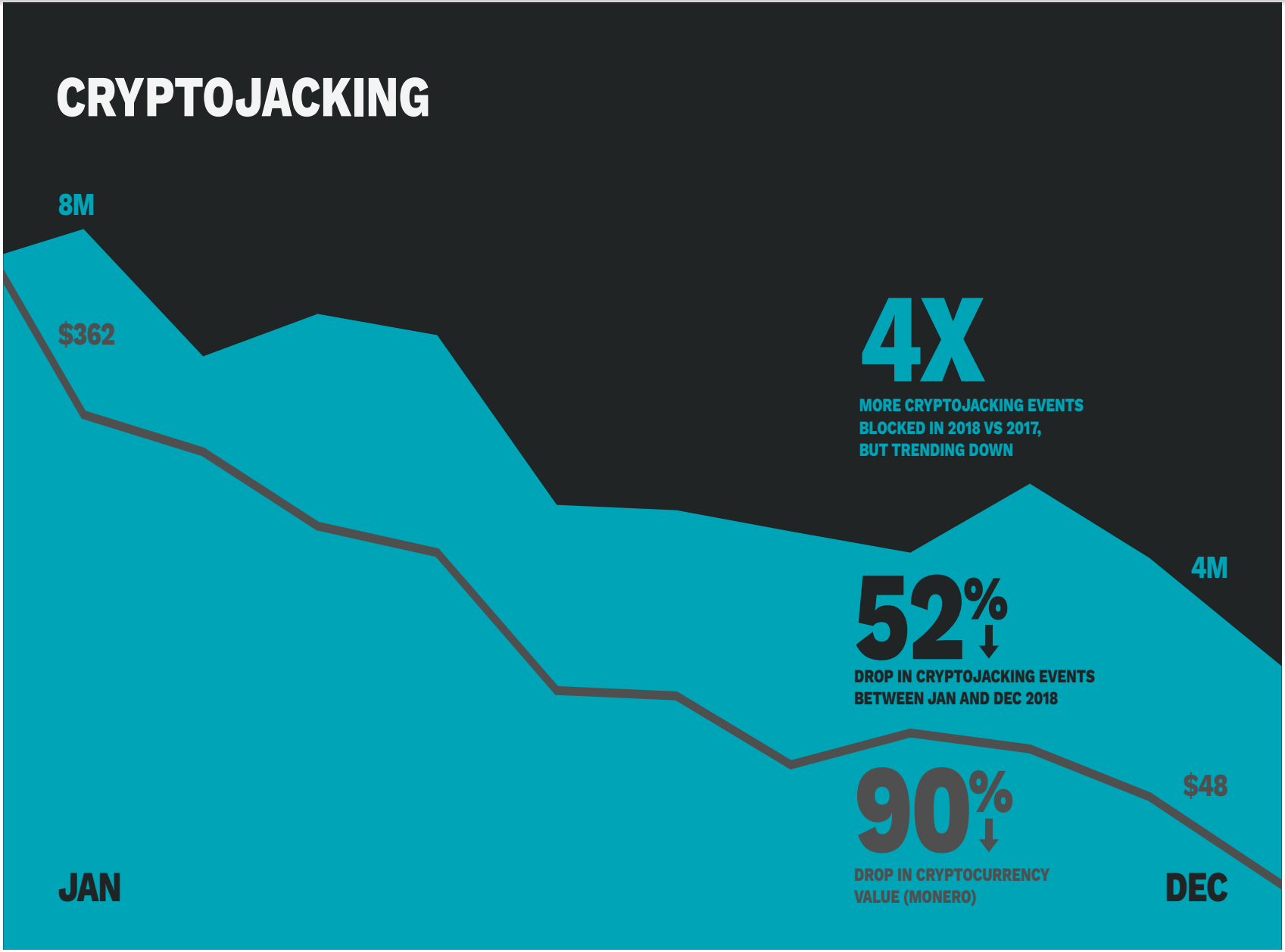
- Physical installation threats
  - hardware threats
    - physical damage to the hardware and/or wires
  - electrical threats
    - electricity fluctuations (brownouts and spikes)
    - electricity loss (blackouts)
  - environments threats
    - external conditions (temperature, electrostatic and magnetic interferences, humidity etc)
    - disasters (flood, fire, . . .)
  - maintenance threats
    - missing, incorrect or damaged spare parts
    - incorrect or missing labeling of components and cables
    - poor handling of components
    - low quality of installation

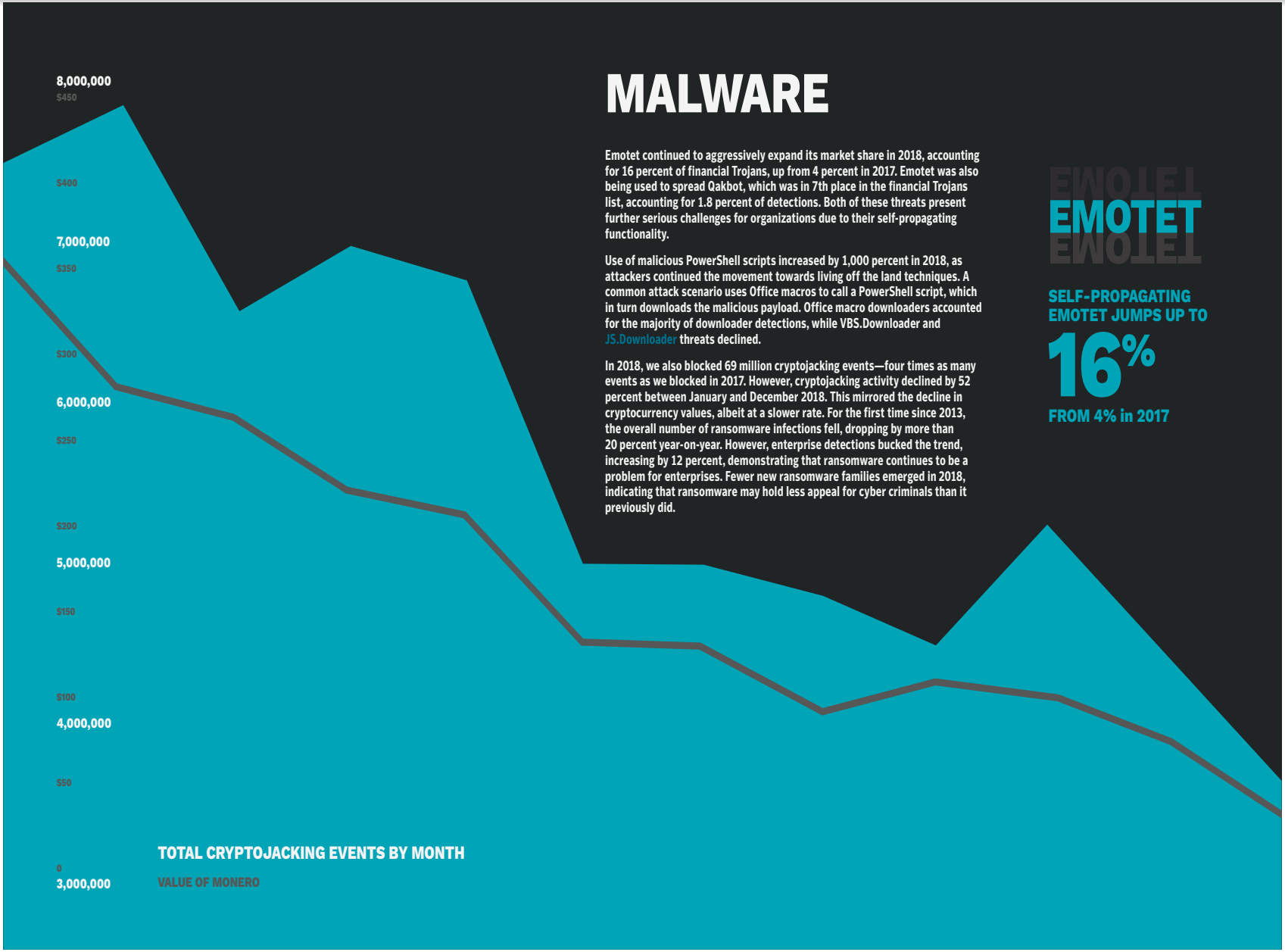
Internet threats

- Phishing
  - search ("fish") for personal details
  - usually using e-mails or social networks
- Viruses and worms
  - malicious software that arrives attached to another (benign) program or data (e.g. e-mail)
  - replicates within the attacked computer
  - worm actively tries to attack new systems over the network
- Spyware and adware
  - spyware collects information about users on Internet
  - adware a special kind of spyware to help targeting advertisements (without user consent)
- Trojans
  - malicious program like virus, but does not replicate itself
- Rogue security software
  - attacks trust relationship

Internet Security Threat Report

- Symantec reports
  - 2019: `https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf`
  - 2017: `https://www.websecurity.symantec.com/security-topics/istr-2017-infographic`
- Main categories
  - mobile devices and Internet of things
  - web threats
  - formjacking and cryptojacking
  - targeted attacks
  - data breaches and privacy
  - ransomware
  - election interference
- Statistics from 2019 report (Symantec bought by Broadcom)


CRYPTOJACKING
8M
$362
4X
MORE CRYPTOJACKING EVENTS BLOCKED IN 2018 VS 2017, BUT TRENDING DOWN
4M
52%
DROP IN CRYPTOJACKING EVENTS BETWEEN JAN AND DEC 2018
$48
90%
DROP IN CRYPTOCURRENCY VALUE (MONERO)
JAN
DEC

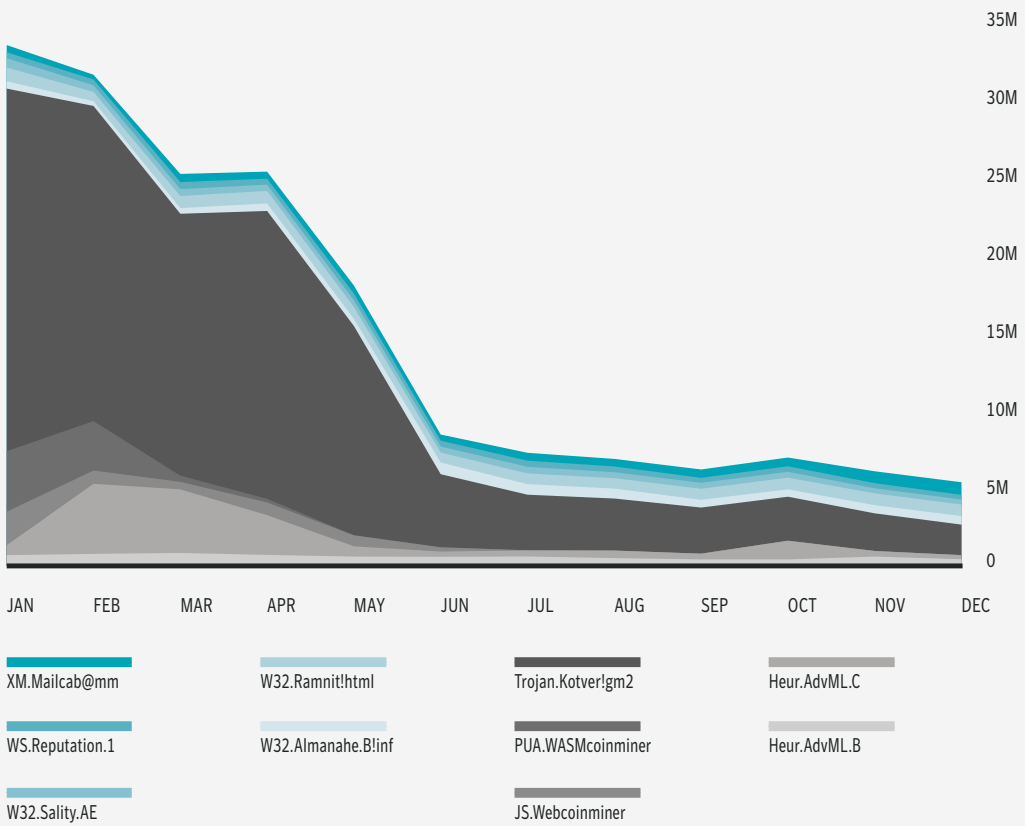

8,000,000
$450
$400
7,000,000
$350
$300
6,000,000
$250
$200
5,000,000
$150
$100
4,000,000
$50
0
3,000,000
TOTAL CRYPTOJACKING EVENTS BY MONTH
VALUE OF MONERO
MALWARE
Emotet continued to aggressively expand its market share in 2018, accounting for 16 percent of financial Trojans, up from 4 percent in 2017. Emotet was also being used to spread Qakbot, which was in 7th place in the financial Trojans list, accounting for 1.8 percent of detections. Both of these threats present further serious challenges for organizations due to their self-propagating functionality.
Use of malicious PowerShell scripts increased by 1,000 percent in 2018, as attackers continued the movement towards living off the land techniques. A common attack scenario uses Office macros to call a PowerShell script, which in turn downloads the malicious payload. Office macro downloaders accounted for the majority of downloader detections, while VBS.Downloader and JS.Downloader threats declined.
In 2018, we also blocked 69 million cryptojacking events—four times as many events as we blocked in 2017. However, cryptojacking activity declined by 52 percent between January and December 2018. This mirrored the decline in cryptocurrency values, albeit at a slower rate. For the first time since 2013, the overall number of ransomware infections fell, dropping by more than 20 percent year-on-year. However, enterprise detections bucked the trend, increasing by 12 percent, demonstrating that ransomware continues to be a problem for enterprises. Fewer new ransomware families emerged in 2018, indicating that ransomware may hold less appeal for cyber criminals than it previously did.
EMOTET
SELF-PROPAGATING EMOTET JUMPS UP TO
16%
FROM 4% in 2017

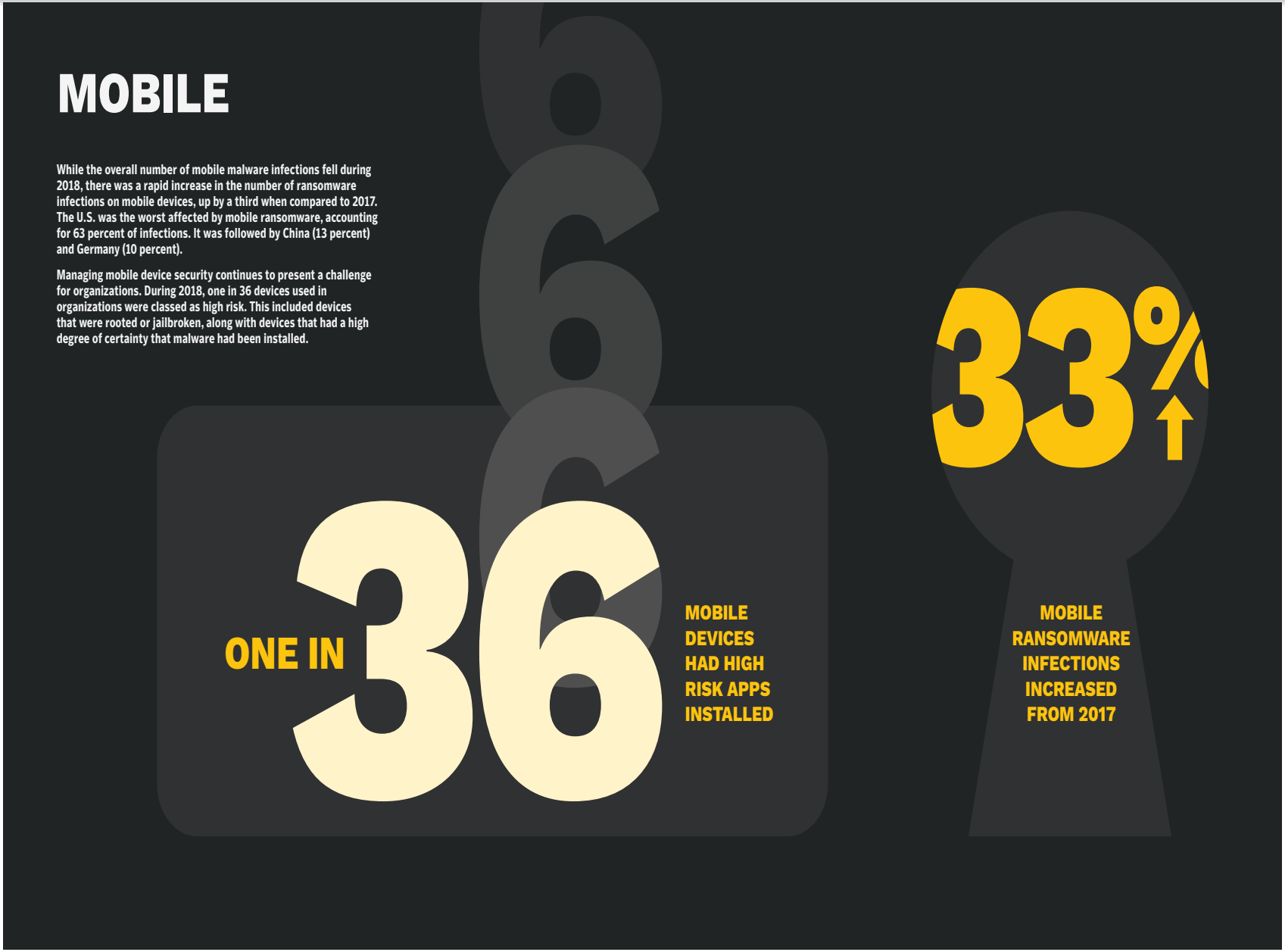
NEW MALWARE VARIANTS (YEAR)

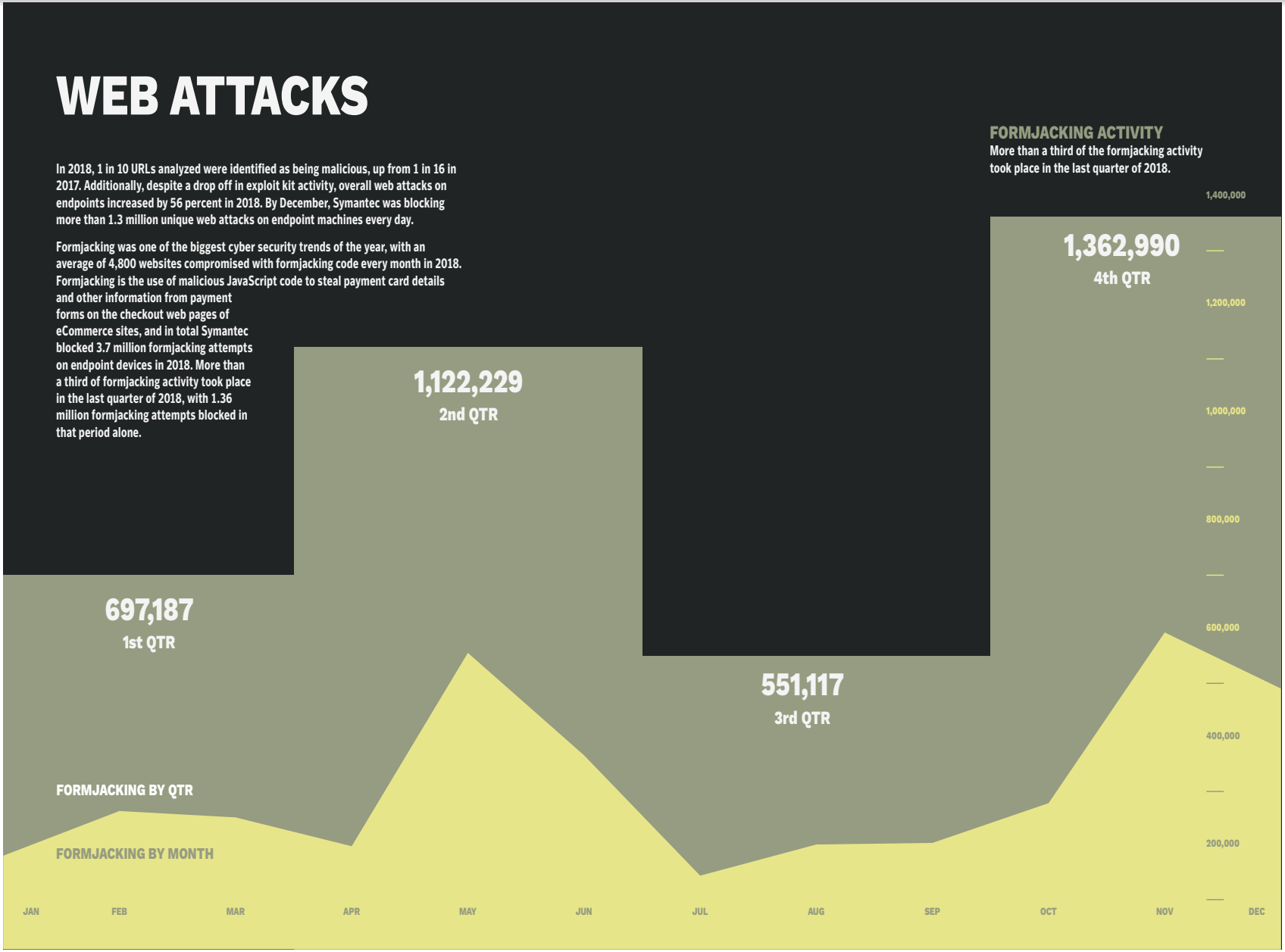
YEAR	NEW VARIANTS	PERCENT CHANGE
2016	357,019,453	0.5
2017	669,947,865	87.7
2018	246,002,762	-63.3

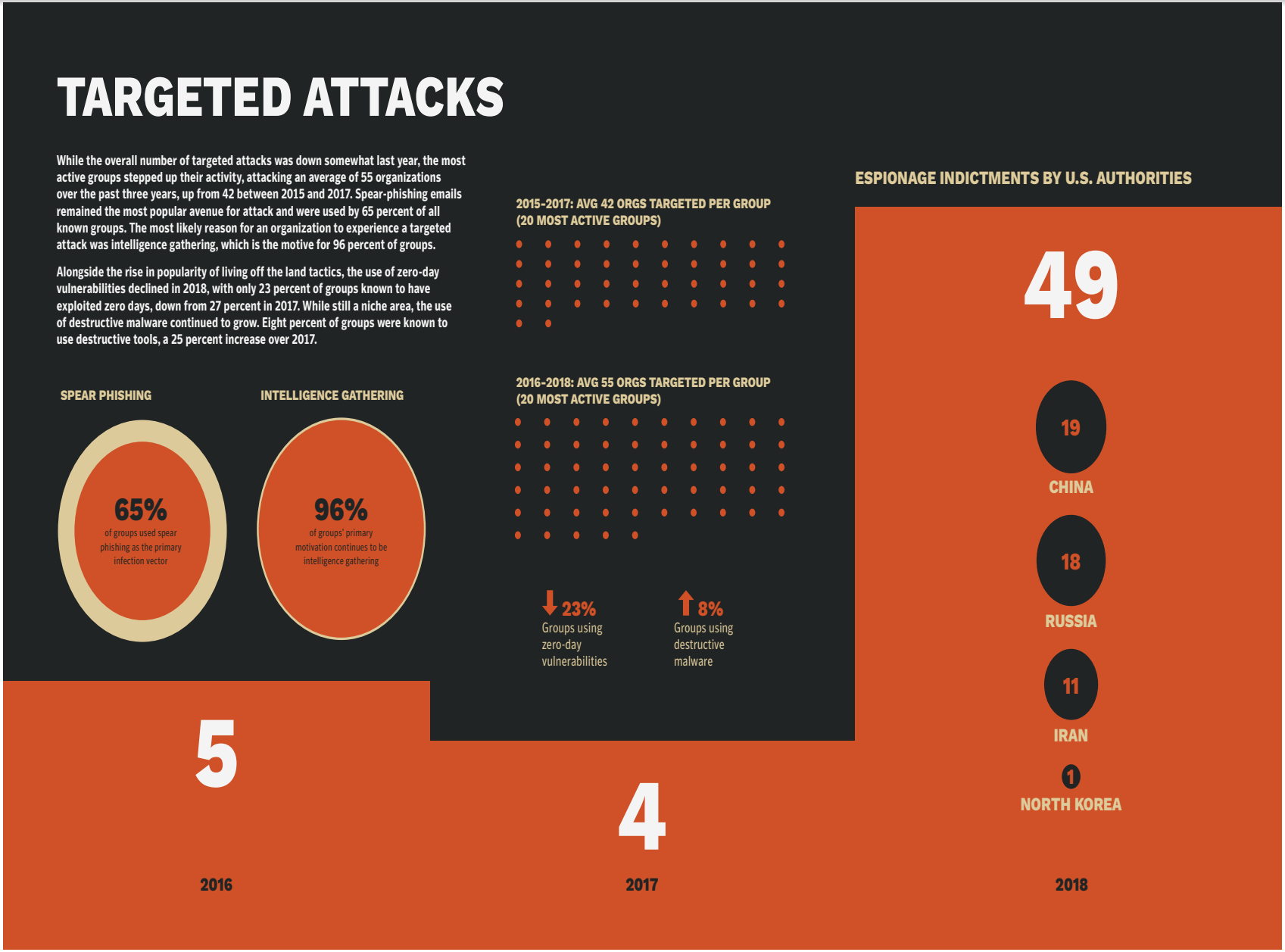
Emotet continued to aggressively expand its market share in 2018, accounting for 16 percent of financial Trojans, up from 4 percent in 2017.

TOP NEW MALWARE VARIANTS (MONTH)

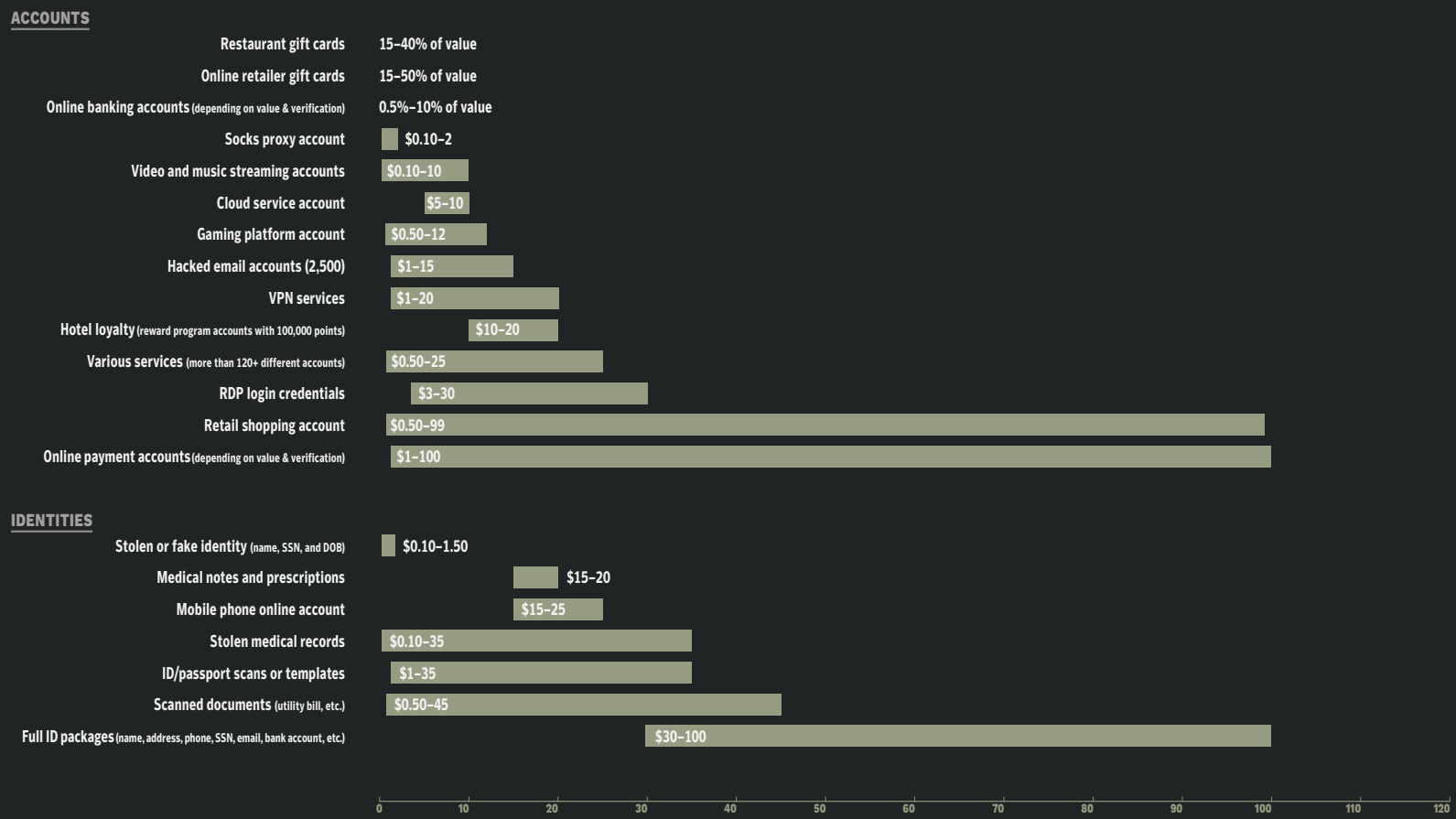



MOBILE
While the overall number of mobile malware infections fell during 2018, there was a rapid increase in the number of ransomware infections on mobile devices, up by a third when compared to 2017. The U.S. was the worst affected by mobile ransomware, accounting for 63 percent of infections. It was followed by China (13 percent) and Germany (10 percent).
Managing mobile device security continues to present a challenge for organizations. During 2018, one in 36 devices used in organizations were classed as high risk. This included devices that were rooted or jailbroken, along with devices that had a high degree of certainty that malware had been installed.
ONE IN 36
MOBILE DEVICES HAD HIGH RISK APPS INSTALLED
33%
MOBILE RANSOMWARE INFECTIONS INCREASED FROM 2017

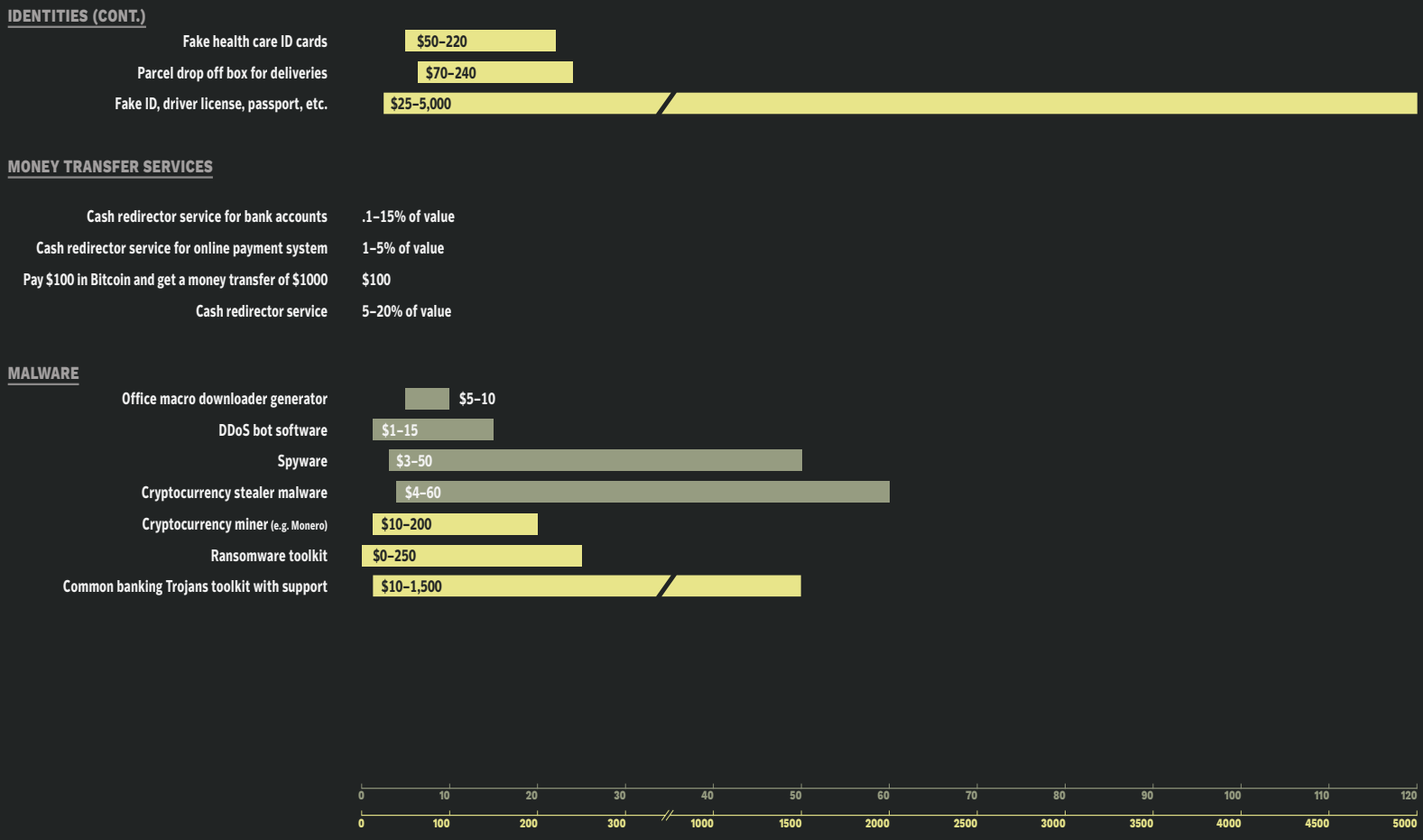

WEB ATTACKS
In 2018, 1 in 10 URLs analyzed were identified as being malicious, up from 1 in 16 in 2017. Additionally, despite a drop off in exploit kit activity, overall web attacks on endpoints increased by 56 percent in 2018. By December, Symantec was blocking more than 1.3 million unique web attacks on endpoint machines every day.
Formjacking was one of the biggest cyber security trends of the year, with an average of 4,800 websites compromised with formjacking code every month in 2018. Formjacking is the use of malicious JavaScript code to steal payment card details and other information from payment forms on the checkout web pages of eCommerce sites, and in total Symantec blocked 3.7 million formjacking attempts on endpoint devices in 2018. More than a third of formjacking activity took place in the last quarter of 2018, with 1.36 million formjacking attempts blocked in that period alone.
FORMJACKING ACTIVITY
More than a third of the formjacking activity took place in the last quarter of 2018.
697,187
1st QTR
1,122,229
2nd QTR
551,117
3rd QTR
1,362,990
4th QTR
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
FORMJACKING BY QTR
FORMJACKING BY MONTH
JAN
FEB
MAR
APR
MAY
JUN
JUL
AUG
SEP
OCT
NOV
DEC


TARGETED ATTACKS
While the overall number of targeted attacks was down somewhat last year, the most active groups stepped up their activity, attacking an average of 55 organizations over the past three years, up from 42 between 2015 and 2017. Spear-phishing emails remained the most popular avenue for attack and were used by 65 percent of all known groups. The most likely reason for an organization to experience a targeted attack was intelligence gathering, which is the motive for 96 percent of groups.
Alongside the rise in popularity of living off the land tactics, the use of zero-day vulnerabilities declined in 2018, with only 23 percent of groups known to have exploited zero days, down from 27 percent in 2017. While still a niche area, the use of destructive malware continued to grow. Eight percent of groups were known to use destructive tools, a 25 percent increase over 2017.
SPEAR PHISHING
65%
of groups used spear phishing as the primary infection vector
INTELLIGENCE GATHERING
96%
of groups' primary motivation continues to be intelligence gathering
2015-2017: AVG 42 ORGS TARGETED PER GROUP (20 MOST ACTIVE GROUPS)
2016-2018: AVG 55 ORGS TARGETED PER GROUP (20 MOST ACTIVE GROUPS)
23%
Groups using zero-day vulnerabilities
8%
Groups using destructive malware
ESPIONAGE INDICTMENTS BY U.S. AUTHORITIES
5
2016
4
2017
49
2018
19
CHINA
18
RUSSIA
11
IRAN
1
NORTH KOREA

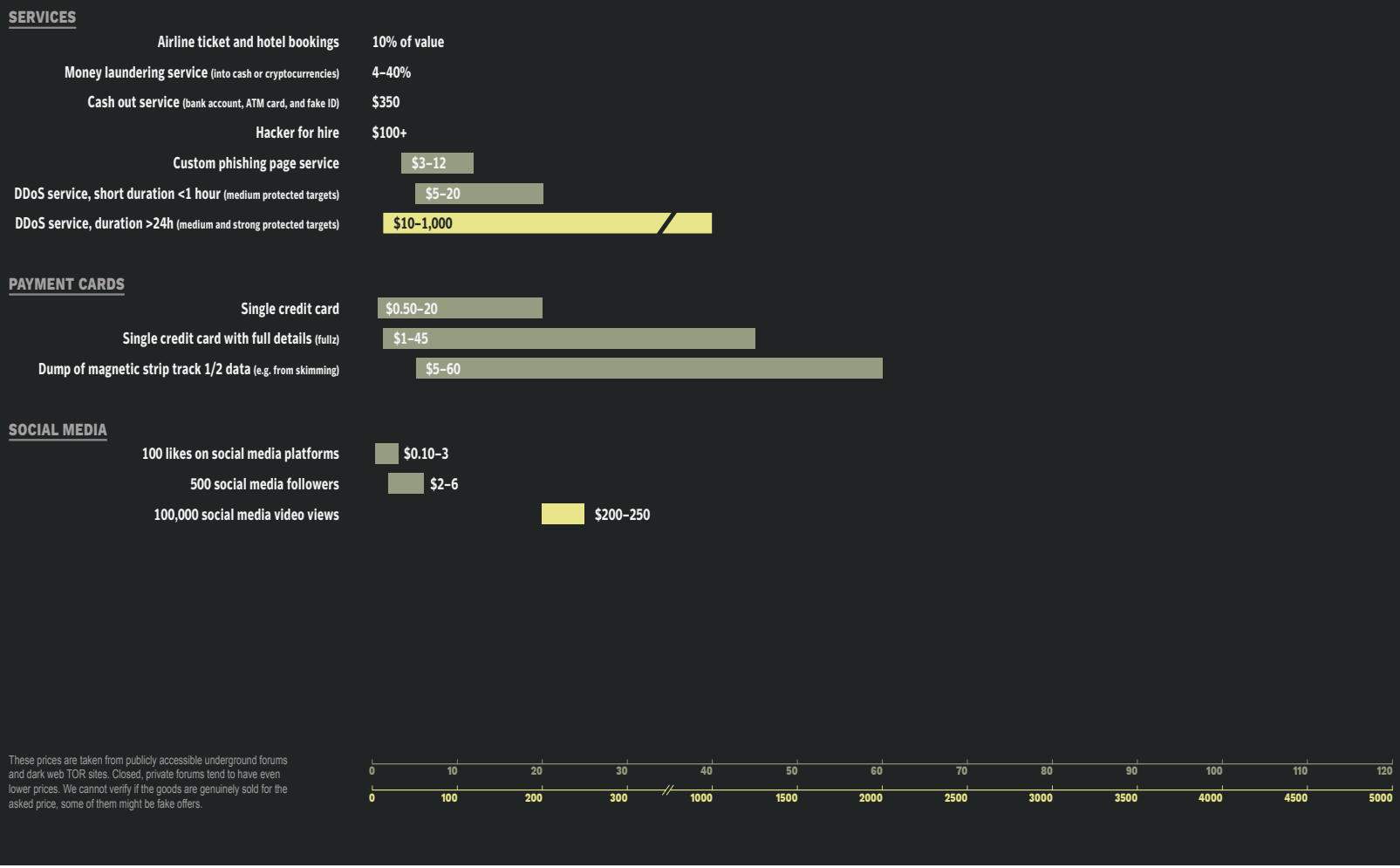
UNDERGROUND ECONOMY



UNDERGROUND ECONOMY



UNDERGROUND ECONOMY



Sensor networks

- Major threats:
  - physical
  - software
- Physical threats:
  - interference
  - battery drainage
  - overtake of a node
- Security
  - routing mis-information
  - data loss
  - data injection

Ad-hoc, mobile and vehicular networks

- Ad hoc network
  - a network build for a specific purpose
  - no central base stations or access points
  - each node sender/receiver
  - peer to peer and multi=hop architecture
- Mobile ad hoc network (MANET)
  - adds mobility to individual nodes
- Vehicular ad hoc network (VANET)
  - specific version of MANET
  - (semi)organized (i.e. not completely random) movement of nodes
  - Roadside Units (RSU)
    - immobile units
    - two side communication with cars
    - specific user interaction modes (drivers disturbance)

MANET Properties

- Each node can communicate
  - power constraints for nodes
- Communication is possible only between nodes “in range”
  - the set of neighbours changes in time
  - bandwidth usually limited
- Each node can retransmit a message
  - router capability
  - multi-hop delivery
- General performance a function of cooperation between nodes

Security problems

- Open media
  - easy to eavesdrop or interfere with
- Open routing protocol
  - no security mechanism
- Continuously changing topology
  - easy hiding for an attacker
- Relies on cooperation between devices
  - malicious node can “divert” others
- Hijacked nodes

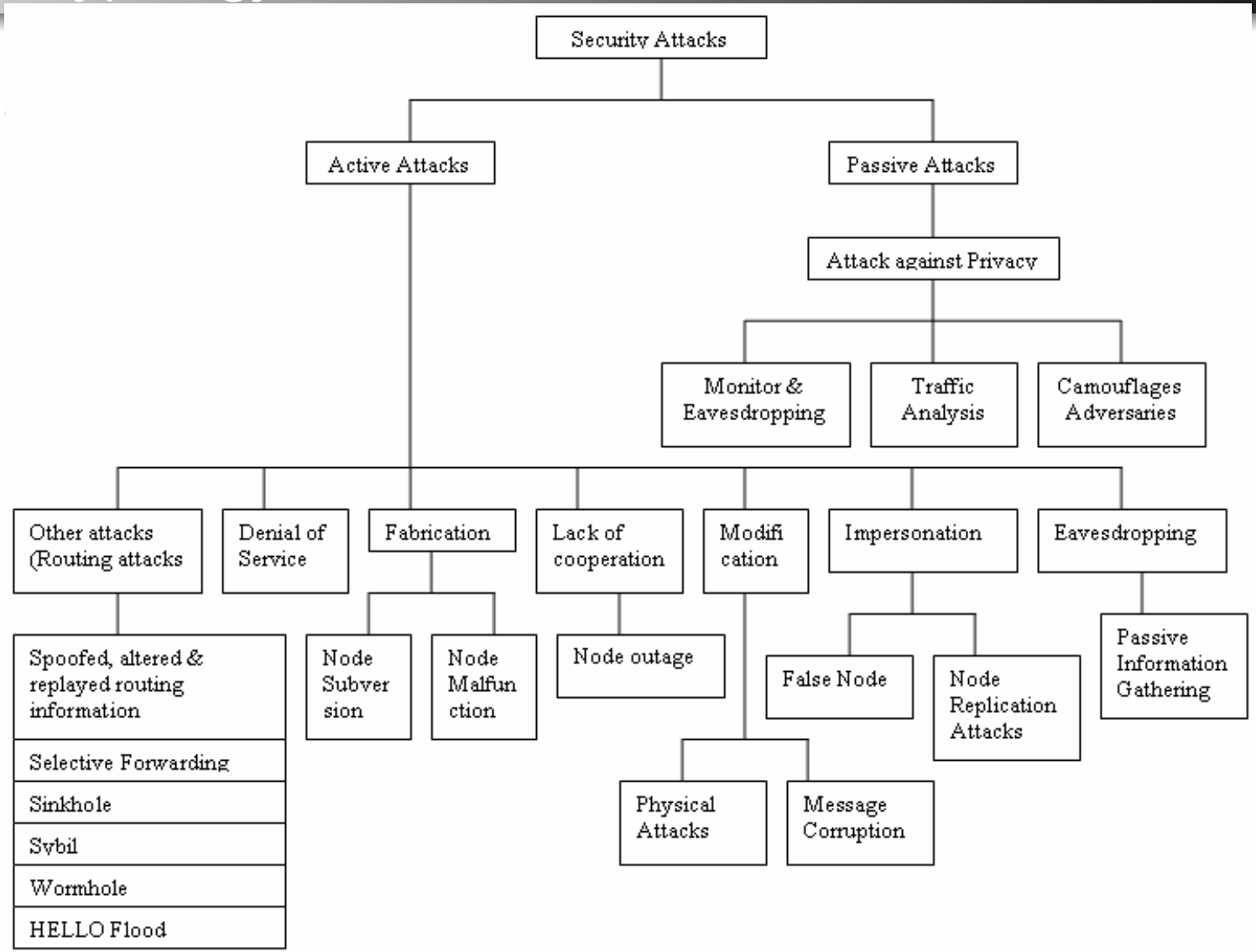
VANET specific problems

- Privacy
  - drivers identity
  - unit identification (where are they moving)
- Clear benefit for a malicious user
  - divert traffic
  - clear its own path

Basic attack modes

- Passive attacks
  - not directly influencing the target systems
  - monitoring the (unencrypted) traffic
    - authentication information (passwords)
    - other sensitive information
  - result is access to information
- Active attacks
  - break into a target system
  - bypass a security perimeter or break through it
  - manipulate messages
    - reply, modify, create, delete
  - impersonation (identity theft), Man-in-the-middle attack
  - result is access to data, modification of data, DoS

Attack typology



Sybil Attack

- Attacker assumes several identities
  - defeat trust of a reputation system
- Used to hide the malicious node (e.g. car in VANET)

Internet

- Physical attacks
  - targets the physical infrastructure
  - immediately indistinguishable form hardware faults
- Internet service attacks
  - Domain Name Service (DNS)
  - e-mail
  - protocol vulnerabilities (e.g. TCP SYN attack)
- Man-in-the-middle attack
- DoS and DDoS attacks

Other types of attack

- Insider attack
  - majority of attacks initiated from within the security perimeter
- Close-in attack
  - social engineering
  - physical access/proximity to the network
- Phishing attack
- Hijack attack
  - takes over the network session
- Exploit attacks
  - uses known security hole
- Protocol attacks
  - spoof attack
  - buffer overflow
- Password attack
  - cracking passwords: brute force and dictionary attack
  - uses access to the file/database with passwords

TCP SYN Flood Attack

- Exploits "trust" in the the TCP 3-way handshake protocol
  1. client initiates connection with SYN packet
  2. server acknowledges (SYN/ACK) and allocates resources
  3. client sends the final acknowledgment (ACK)
- What if client does not respond with ACK?
  - victim allocates resources (memory)
  - resources eventually freed through time out
  - but in the meantime victim not able to serve legitimate requests

  Simple Denial of Service attack
- Attacker does not use its own IP address
  - why?

Low Rate TCP DoS

- A paper of Kuzmanovic&Knightly: *Low-Rate TCP-Targeted Denial of Service Attacks*. SIG COMM 2003.
- Exploits TCP congestion control mechanism
- Retransmission time-out
- Exponentially reduce available bandwidth

Low Rate TCP DoS II

- Pinciples
  - mis-uses the congestion avoidance mechanism of TCP
  - if severe congestion risk is recognized, TCP reduces congestion window to one packet and waits for a period of Retransmission Time Out (RTO) after which the packets is resent
  - further loss doubles RTO period
  - short outages (on adversary flow) at around RTT force TCP to timeout; all flows *simultaneously* enter the same state
  - when TCP attempts to exit timeout and enter slow-start
  - adversary creates another outage to force the flows synchronously back to timeout state
- Difficult to detect
  - recognizable: high-rate bursts on short time-scales
- And mitigate
  - randomized minRTO

Distributed DoS

- Single source DoS attack (rather) easily defended
  - does not mean we know who is the attacker
  - but we can stop her (usually)
- Distributed DoS
  - many sources of attack
  - each harmless by its own
  - their quantity is the problem
- Uses a (huge) set of attacking machines
  - under control of attacker: bots, zombies, ...
  - innocent (secondary victims)

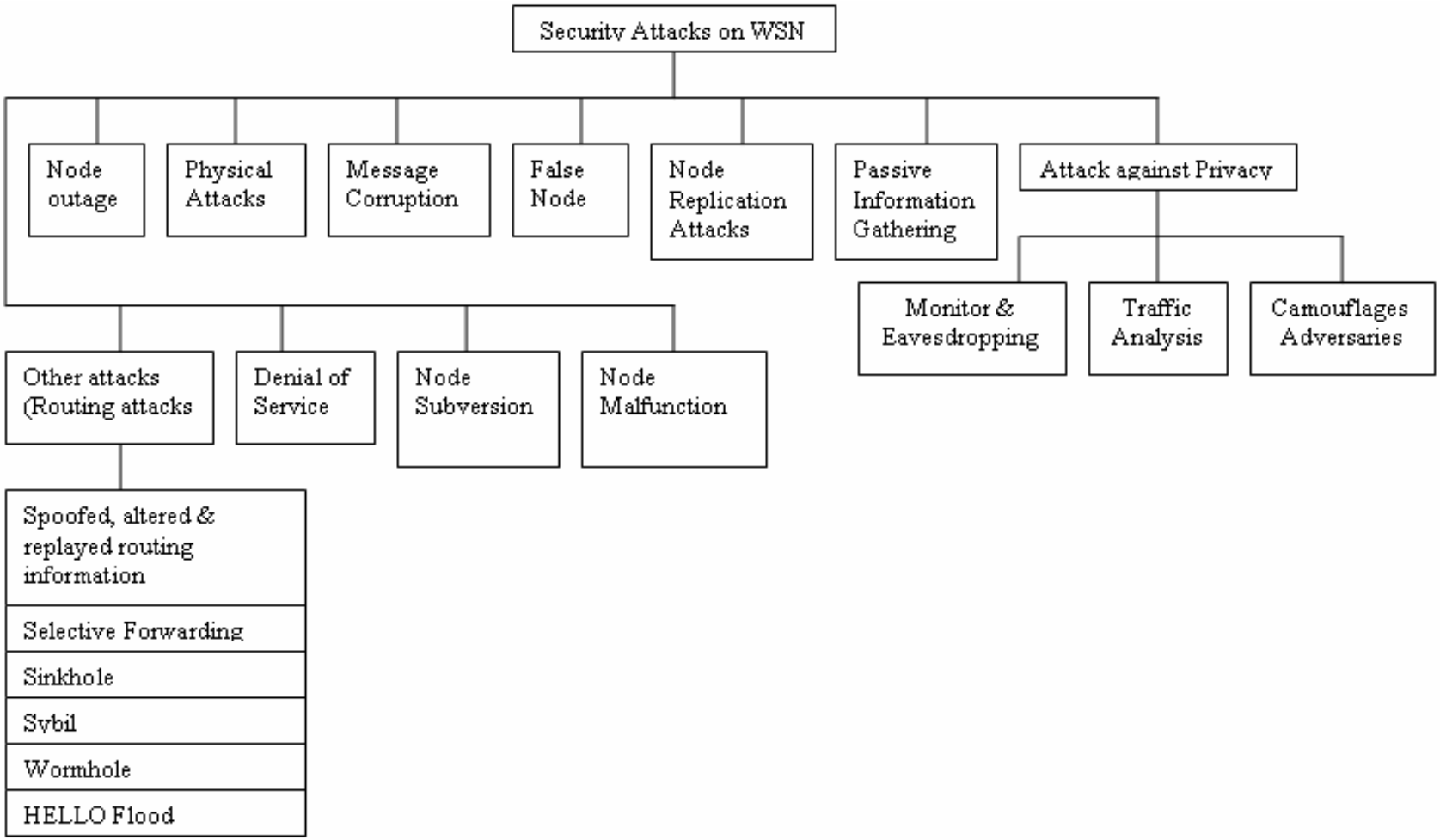
Multiple Source DDoS Attack

- Attacker controls an army of slave machines
  - result of previous successful attacks
    - legitimate owners without knowledge
  - available "on demand"
- Synchronized overload of the victim
  - sending legitimate requests from many sources
  - victim unable to differentiate the requests
    - crash of many media servers on September 11th 2001 not by attack but too extensive interest
- Usually hierarchical to hide the attacker
  - attacker directly controls only first layer of machines, these used to control the second layer, not sending the data directly to the victim

DDoS Reflector Attack

- A smaller set of machines directly controlled by attackers
- Exploits "reflector" vulnerabilities of some network protocols
  - TCP SYN Flood
  - ICMP
- Attacker send requests with forged victim's address
  - requests go to "secondary victims"—innocent machines not under attacker's control
- All responses from these secondary victims go to the primary victim $\longrightarrow$overload

Sensor networks–attack typology



Sleep Deprivation

- Also called resource consumption attack
- Overload the victim node by requests
  - route discovery
  - packets forwarding
- Exhausts internal resources
  - battery drainage
- and puts the node off-line

Ad-hoc, mobile and vehicular networks

- Passive and active attack as in other network categories
- External attacks
  - nodes that do not belong to the network
- Internal attacks
  - hijacked nodes
- Basic attack scenarios:
  - black hole, wormhole, Byzantine, sleep deprivation

Basic attacks

- Black hole attack
  - node reports route availability to targets
    - announces the shortest route
    - attracts traffic to the target node through itself
  - inspects all the packets
  - modifies, drops, delays them
- Wormhole attack
  - two cooperating malicious nodes
  - a packet collected by one are sent directly to the other ("wormhole")
  - disrupts routing when also routing control messages are tunneled
    - could prevent a discovery of any other routes

Location disclosure

- Collects information about the topology and/or structure of the network
  - route maps
- Useful for future attacks
  - important in more regular ad hoc networks like the vehicular one
  - identities of communicating parties
- Dangerous in security sensitive scenarios
  - military MANETs

Specific VANET attacks

- Sybil attacks
- Bogus information
- Denial of Service
- Impersonation (masquerading)
- Alteration attack
- Reply attack
- Illusion attack

Illusion attack

- Adversary deceives sensors in his own car to produce wrong sensor readings
  - car broadcasts false traffic warning messages
- Creates an illusion for other cars about the traffic event
- Drivers behaviour is modified
  - ultimate goal of the adversary
- Difficult to mitigate with traditional methods like trust schemes, message authentication, message integrity checks

Summary

- Provided basic classification for
  - failures and faults
  - threats
  - attacks

  for different kinds of network
  - Internet
  - sensor networks
  - ad hoc, mobile and vehicular networks
- Similarities and differences between specific networks discussed
  - random failures versus targeted use of faults
  - capacity limits
- Threats come from nature as well as from attackers
  - one issue is to properly distinguish these
  - to properly mitigate their impact
- Next lecture: Security architecture

Figure sources

- Figs.1&2 on slides 29 and 38 are taken from
  - Pamavathi et al: *A Survey of Attacks, Security Mechanisms and Challenges in WSN*. IJCIS, vol.4(1,2), 2009
    `http://arxiv.org/pdf/0909.0576.pdf`