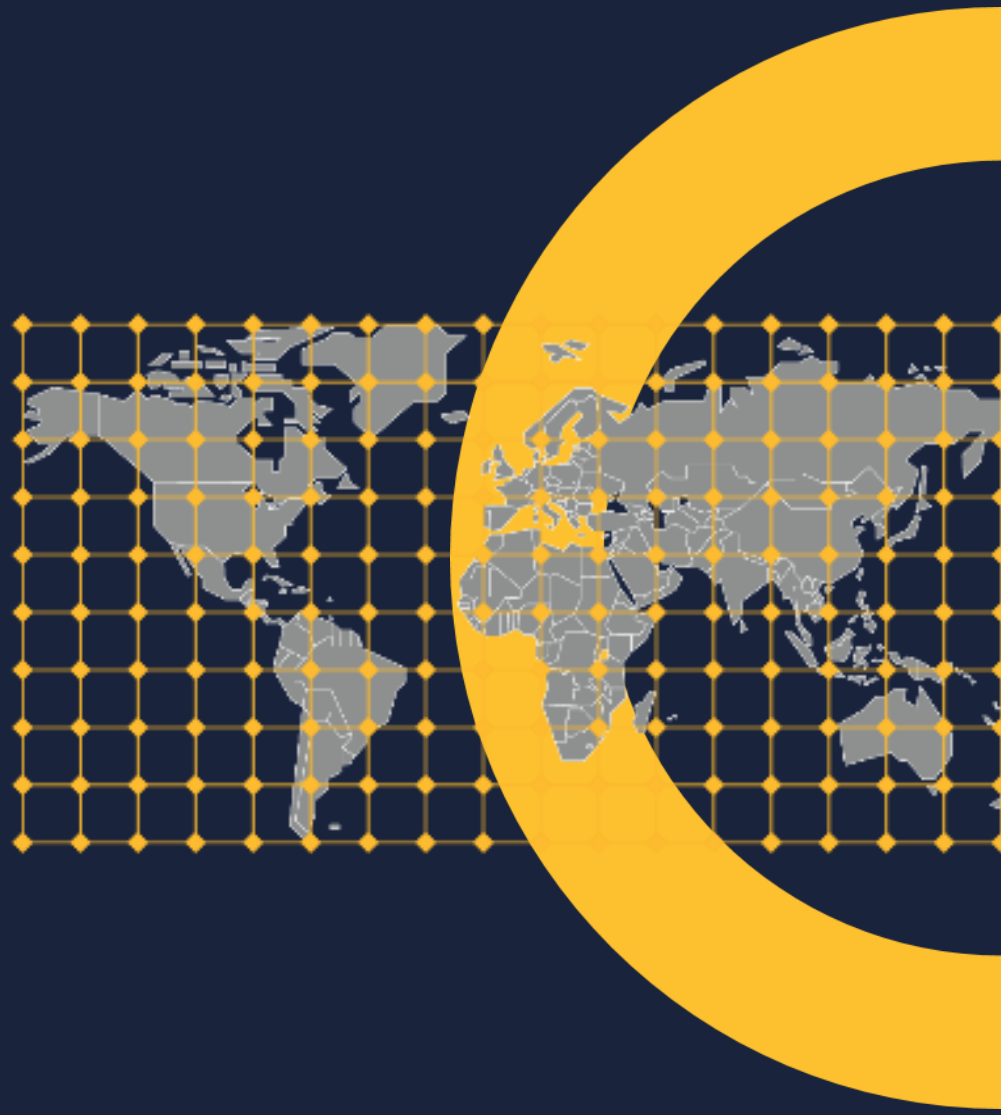
Cyber security trends and horizon scanning 2018 and beyond



Presenter

Goran Gotev

Senior Manager

Government Affairs

Date

09 October 2018

ITU-D

Geneva, Switzerland

Symantec.

2018 – The Big Numbers

Web Threats

More than 1 Billion
Web requests analyzed each day
Up 5% from 2016

1 in 13
Web requests lead to malware
Up 3% from 2016

Email

Percentage Spam Rate

2015 **53%**
2016 **53%**
2017 **55%**

IoT

600%
Increase in Attacks

2016 **6K**
2017 **50K**

Vulnerabilities

Overall increase in reported vulnerabilities **13%**

Malware

92% Increase in new downloader variants

80% Increase in new malware on Macs

8,500%
Increase in coinminer detections

Ransomware

5.4B
WannaCry attacks blocked

46%
Increase in new ransomware variants

Mobile

Number of new variants
2016 **17K**
2017 **27K**

Increase in mobile malware variants **54%**

24,000 Average number of malicious mobile apps blocked each day

29%
Increase in industrial control system (ICS) related vulnerabilities

General trends

Simple, but successful

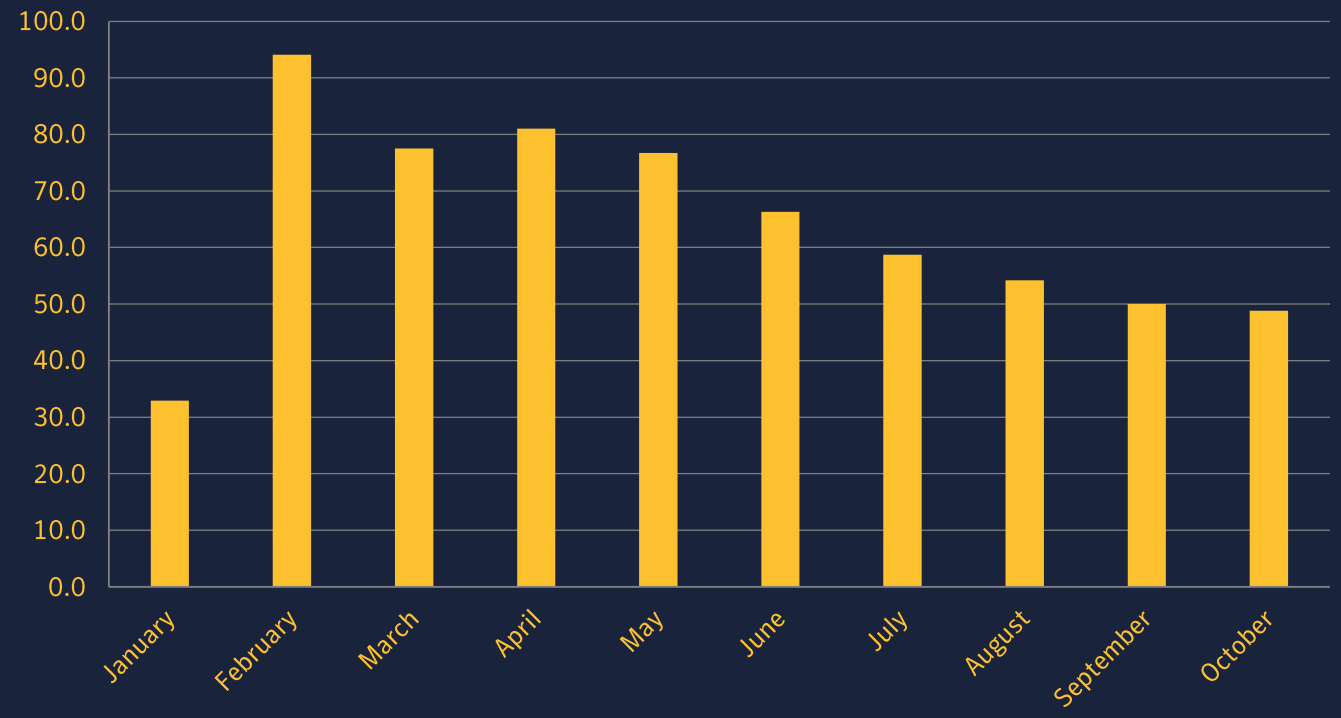
- Low-tech attacks
- Living off the land
- Features replace vulnerabilities

Focused and selective

- Ransomware hits businesses
- Selective spreading of malware
- Supply chain attacks

Malware statistics

- ~ **2 Million** new malware variants per day
- Script malware leads to many variants

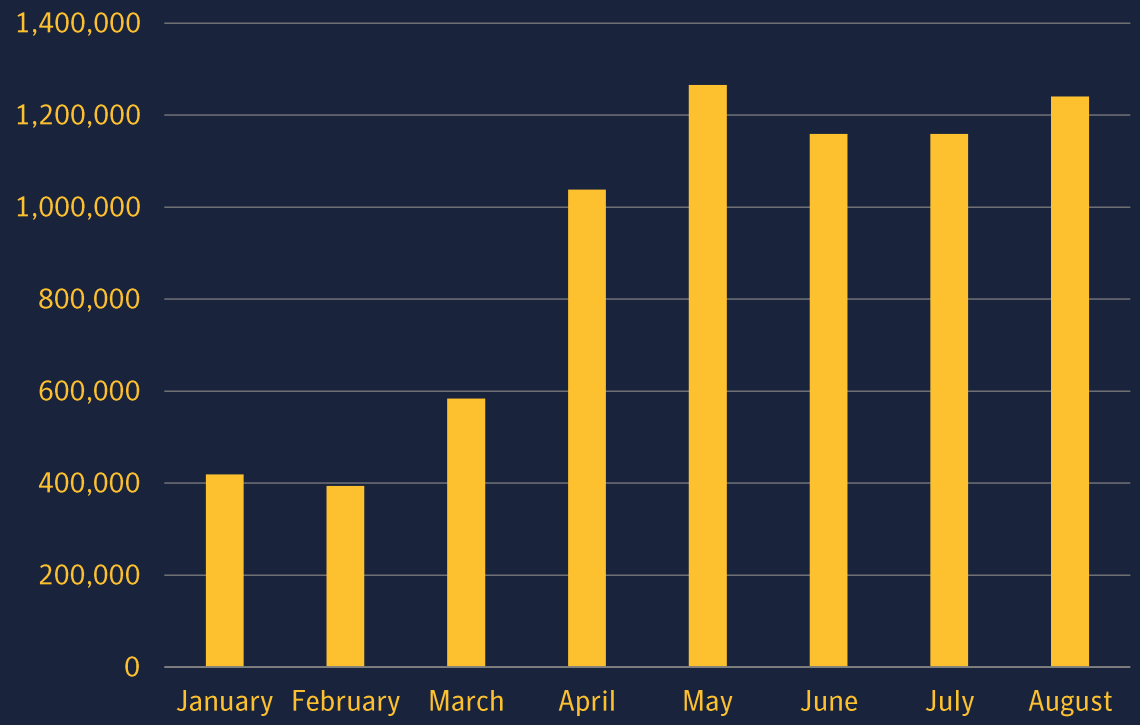


New malware variants per month in millions

Region	% of global
USA	26%
Japan	7%
China	6%
India	5%
Germany	4%
Brazil	4%
United Kingdom	4%
Canada	3%
Russia	3%
France	2%
Australia	2%
Italy	2%
Mexico	2%
Turkey	1%
South Korea	1%

Web attacks still elevated

- Zero-days exploits very rare
- RIG toolkit is most active
- Link spread through email or advertisement
- Sometimes infections are restricted to specific IP addresses



Web attacks blocked per day

Email

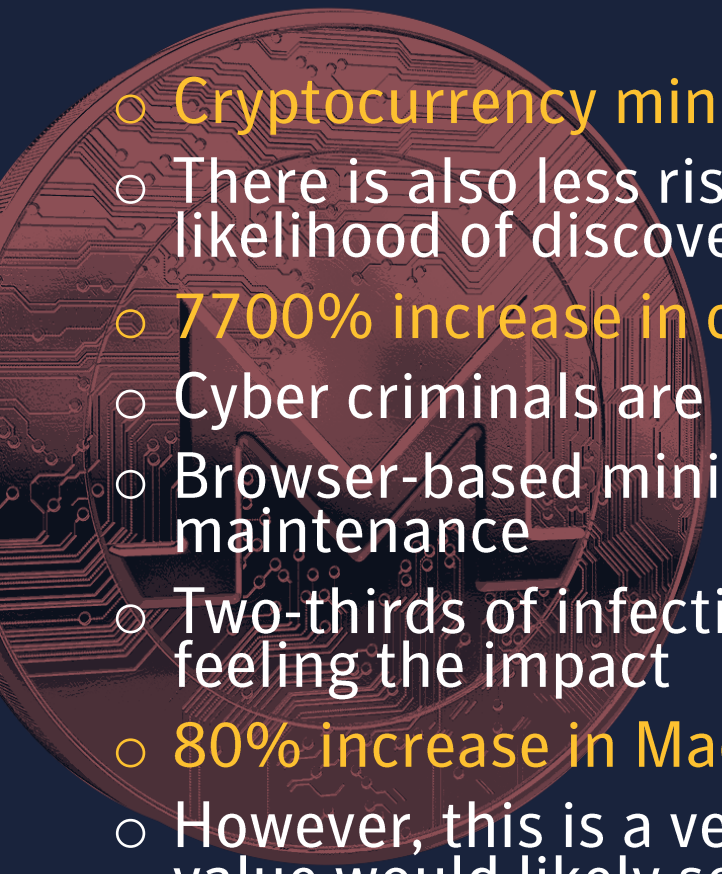
- The email malware rate is 1 in 412, down from 1 in 131 in 2016
- Rate drop is a result of a cessation of activity from the Necurs spam botnet from January to March 2017
- Email is still the primary vector for ransomware, however we're seeing evidence of a shift towards the distribution of financial malware
- Spear-phishing taken to the next level
  - Convince the employee to perform a payment transaction
  - Scams often use typo-squatted domains
  - Some attacks change the IBAN in invoices
  - 8,000 businesses targeted monthly

Living off the land

When attackers turn what you have against you

- Fewer new files on disk
  - more difficult to detect attack, no IoC to share
- Use off-the-shelf tools & cloud services
  - difficult to determine intent & source
- These tools are ubiquitous
  - hiding in plain sight
- Finding exploitable zero-day vulnerabilities is getting more difficult
  - use simple and proven methods such as email & social engineering

Cryptocurrency mining



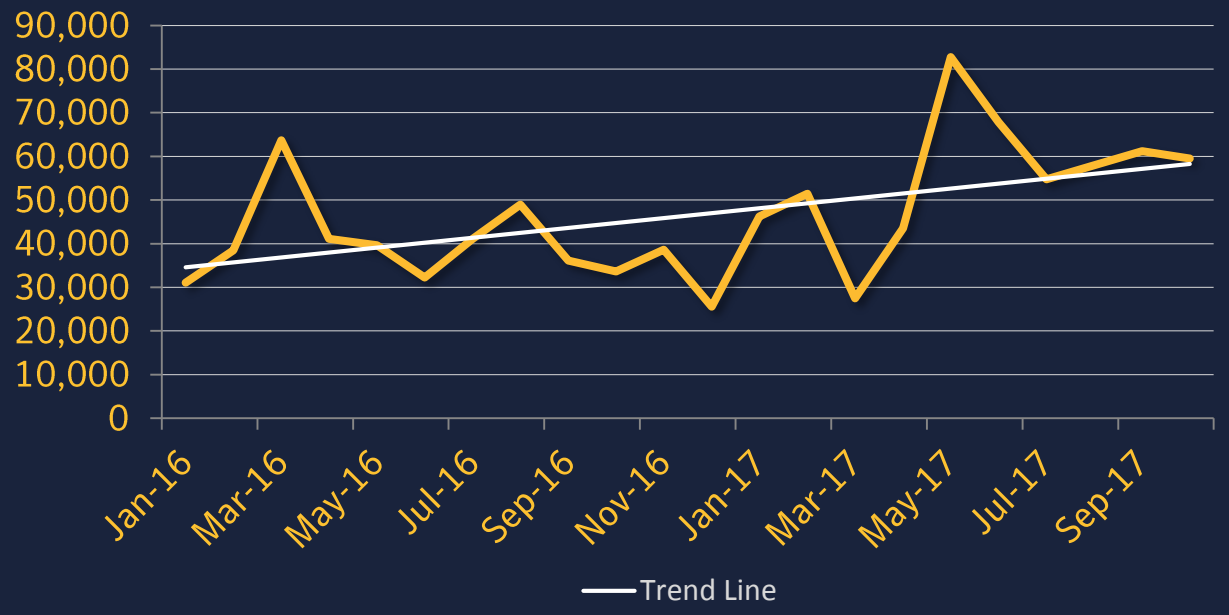
- Cryptocurrency mining has become more lucrative than ransomware for attackers
- There is also less risk involved – it's not considered a crime and there is less likelihood of discovery
- 7700% increase in cryptominer detections from September to December 2017
- Cyber criminals are motivated by the increased value of digital currencies
- Browser-based mining is the most popular as it requires little skill and is low maintenance
- Two-thirds of infections are on consumer machines, but organisations are also feeling the impact
- 80% increase in Mac malware, driven primarily by crypto miners
- However, this is a very volatile revenue generator; a decrease in cryptocurrency value would likely see this threat disappear

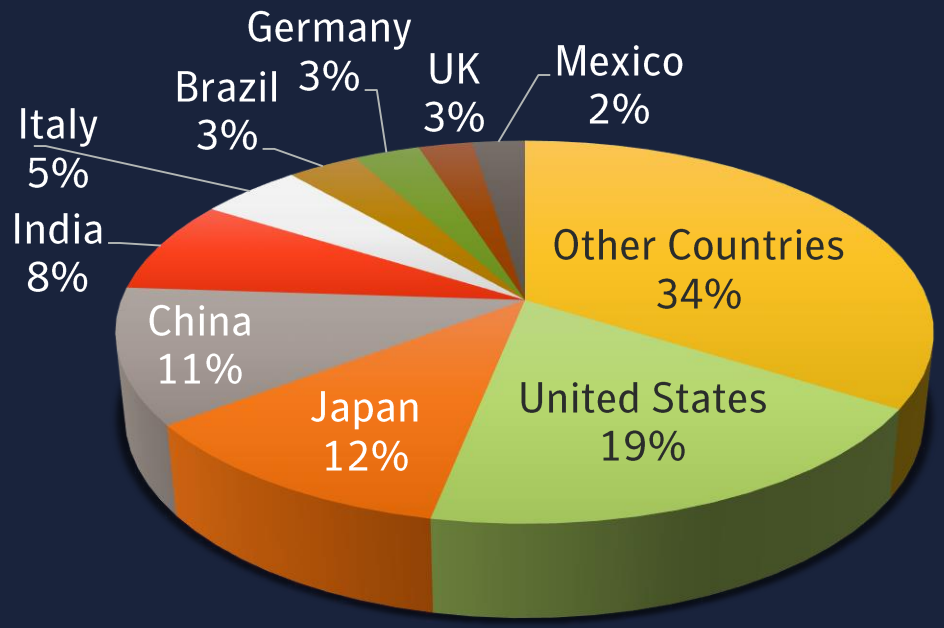
In-browser coin mining a.k.a. Cryptojacking

- In-browser mining **increased by 34,000%** in 2017 (24% of all web attacks in December 2017)
- 8 Million blocked in December 2017
- Not just Windows — threats exist on OS X, Linux, mobile, and IoT
  - Mobile apps incorporating cryptocurrency mining code increased by 34 percent in 2017
  - Mirai IoT bot variant with cryptocurrency mining capabilities (April 2017)
  - Works in Office documents, other script languages, browser extensions and widgets

Ransomware stats

- Ransomware is still profitable and common
- Multiple self-propagating variants appeared





Targeted attacks

- Intelligence-gathering is the primary motive for 90% of targeted attacks
  - Other motivations are financial and disruption
- Average number of organizations targeted per group is 42
- The number of organizations hit by targeted attacks has increased by 10% from 2016 to 2017
- Spear-phishing is the primary infection vector for targeted attacks, used in over 70% of attacks
  - Other infection vectors are watering holes, SQL injections and supply chain attacks
- Zero-day vulnerabilities are used by 27% of attack groups

Supply chain attacks

- Number of highly-publicized supply chain attacks in 2017
  - Petya and MeDoc
  - CCleaner
- 6% of targeted attacks use the supply chain as a vector but it's coming more popular
- At least one large supply chain attack per month was observed in 2017
- This trend is an extension of the Living off the Land trend we noted in last year's report
  - Attackers avoiding the use of vulnerabilities and malware and instead using what's commonly available to them

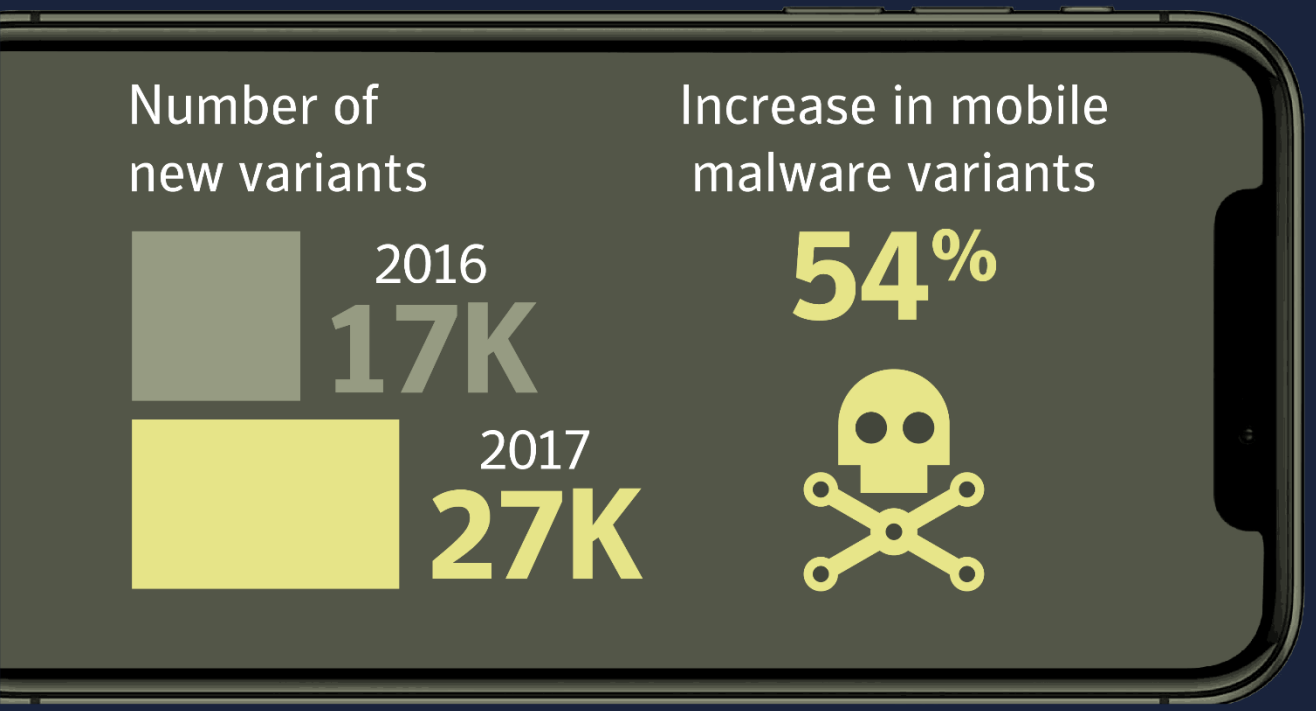
Vulnerabilities

- There has been an overall increase of 13% in the number of vulnerabilities discovered in 2017
- Increased numbers are likely driven by bug bounty programs
- Zero day vulnerabilities have increased by 7%
- ICS vulnerabilities have increased by 29%
- Android vulnerabilities are up by 146%
- iOS vulnerabilities are down by 5%
- Browser vulnerabilities are down overall, only Safari saw an increase
- Despite vulnerabilities numbers being up, cyber criminals still favour email as an infection vector

IoT

- There has been a 600% increase in IoT attacks
- An old DDoS worm called Linux.Lightaidra accounts for 40% of attacks
- China accounts for 21.6% of attacks, slightly down from 22.4% in 2016
- US accounts for 10.9% of attacks, down from 18.7% in 2016
- Root and admin are still the top 2 usernames for attempted logins
- However 6 of the top 10 usernames in 2017 are new

Mobile Malware Continues to Surge

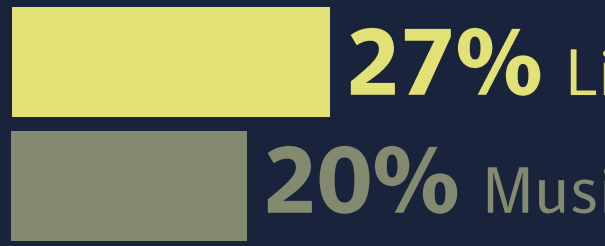


24,000 malicious mobile applications blocked each day

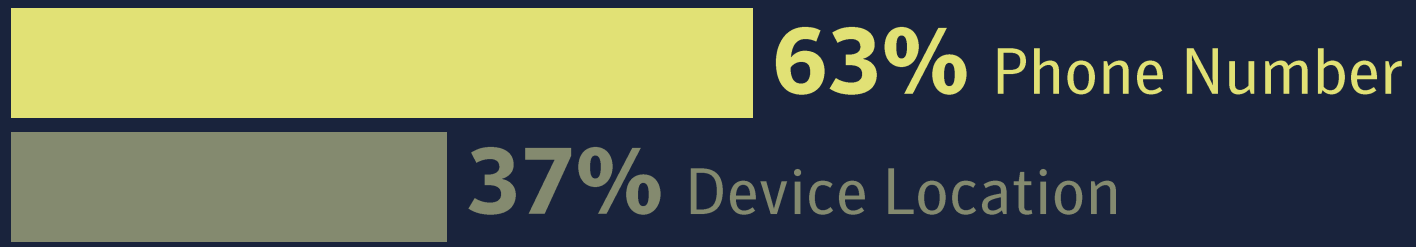
99.9% of malware discovered on third-party app stores

Privacy on mobile phones

App categories that have the most malicious mobile apps are:



Leaky Apps – what sensitive information do they most often leak?



20% Percent increase in grayware in 2017

2018 and beyond

CURRENT TRENDS SHOW NO SIGN OF ABATING

Living off the lands techniques will persist and evolve	• Attackers will continue to identify and exploit OS and application features similar to macros, powershell and DDE • Detecting these attacks will require greater use of attack analytics • Zero days will remain rare, but will be high impact if discovered
Cyber crime will diversify	• Attackers need to adopt new revenue-generating activities • Ransomware, while still prevalent, is starting to stagnate • Crypto currency mining will increase in popularity
Targeted attacks	• Motives for targeted attacks are broadening and leading to the emergence of new types of attack groups • Supply chain attacks are increasing in popularity and will be more widely adopted

17

Any Questions? Thank you!

Goran_Gotev@Symantec.com