Symantec

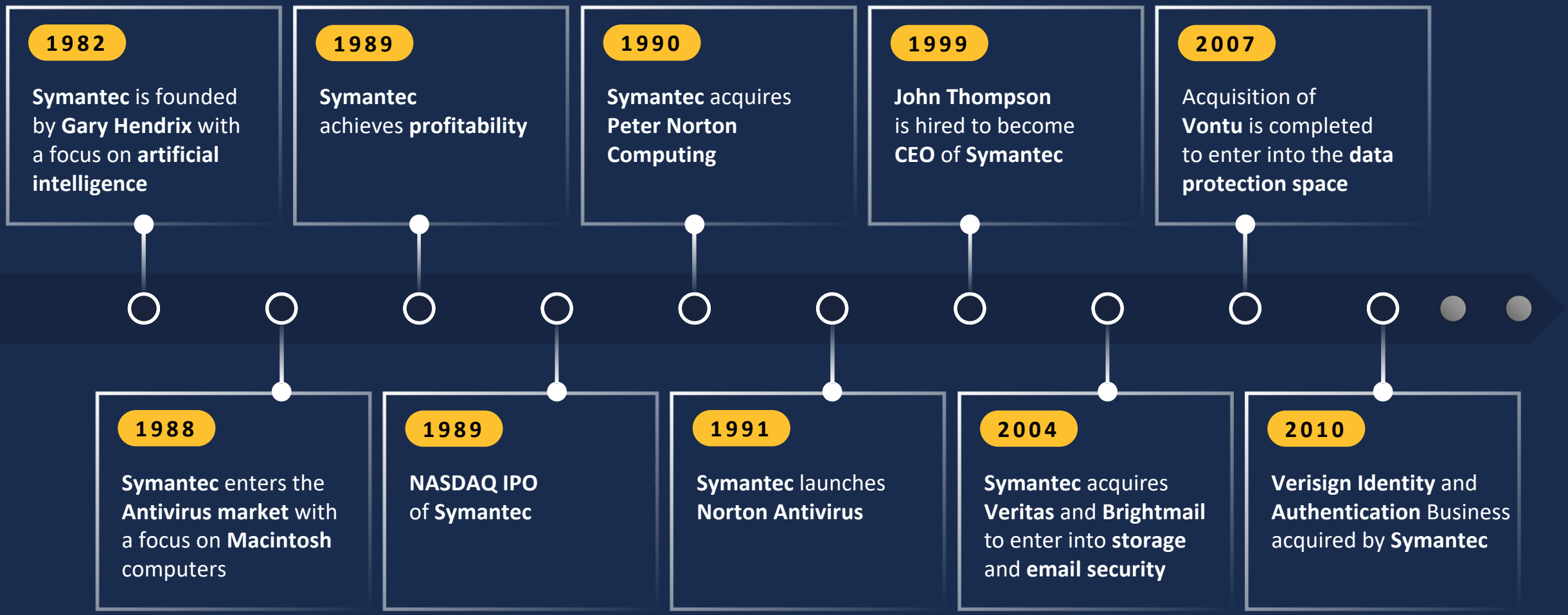
Internet Security Threat Report

Volume

23

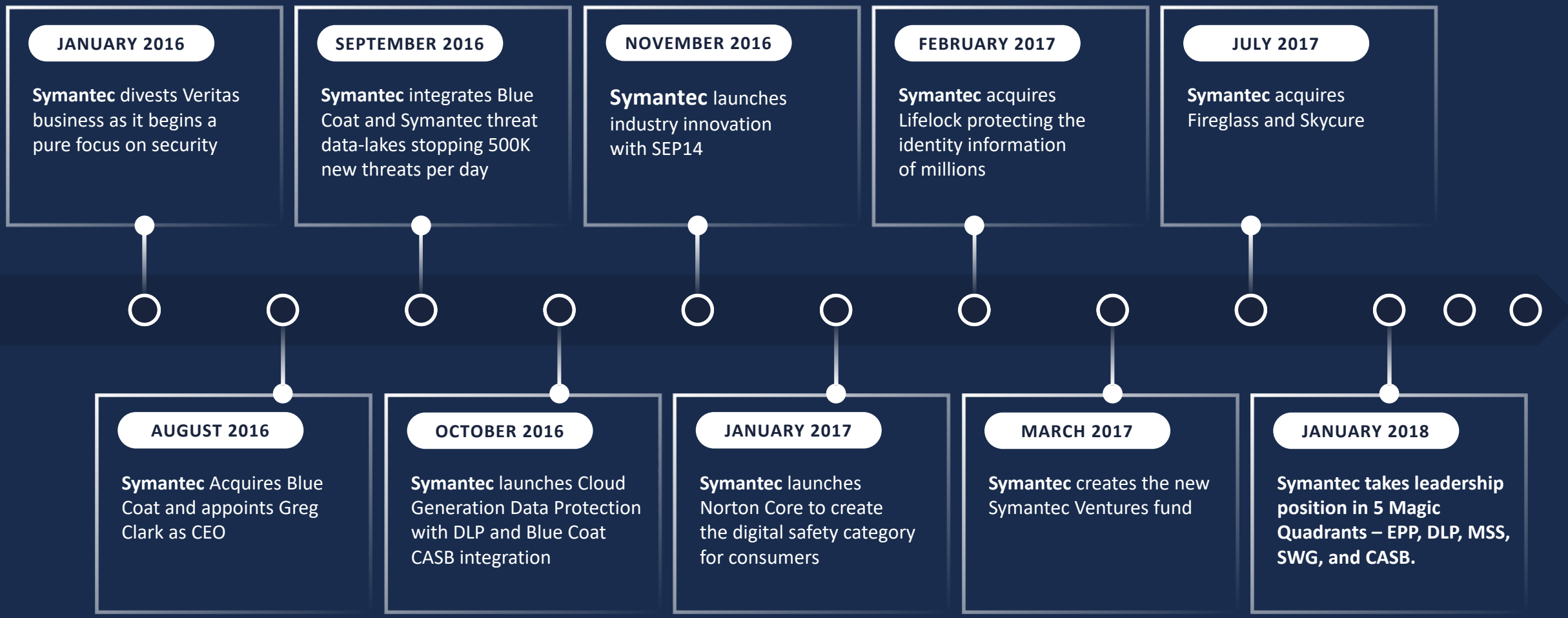
Davor Kodrnja | Regional Sales Manager Adriatics

Symantec:
A History of Industry Leadership



 |

Symantec:
Celebrating The Past Two Years of Advanced Innovation



 |

ISTR23 at a glance

Symantec

10 → **125** → **90**

DATA SOURCES

DeepSight
Email
Endpoint telemetry
ID Analytics **NEW!**
IoT honeypot
Mobile incl. Skycure data **NEW!**
RuleSpace
SRL **NEW!**
Targeted Attack Analytics **NEW!**
Web gateway **NEW!**

METRICS

PAGES OF DATA AND ANALYSIS

The Big Numbers

Symantec.

Web Threats

More than 1 Billion

Web requests analyzed each day

1 in 13

Web requests lead to malware

Email

IoT

600%

Increase in Attacks

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 crimeware detections

Ransomware

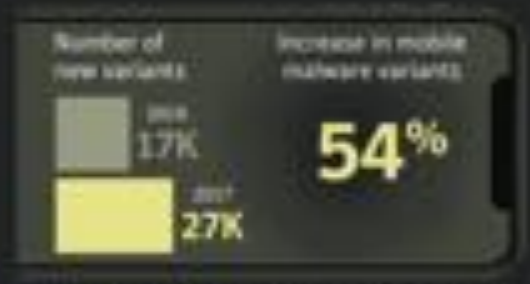
5.4B

WannaCry attacks blocked

46%

Increase in new ransomware variants

Mobile



24,000

Average number of malicious mobile apps blocked each day

29%

Increase in industrial control system (ICS) related vulnerabilities

Key Findings and Messaging

ISTR

Internet Security Threat Report

Volume 23

Symantec

ISTR – Key Messaging

- Cryptojacking Attacks Explode by 8,500 Percent
- Implanted Malware Grows by 200 Percent, Compromising Software Supply Chain
- Mobile Malware Continues to Surge
- Business-Savvy Cyber Criminals Price Ransomware for Profit
- Majority of Targeted Attackers Use Single Method to Infect Victims

ISTR – Key Messaging

With a low barrier of entry – only requiring a couple lines of code to operate – cyber criminals are harnessing stolen processing power and cloud CPU usage from consumers and enterprises to mine crypto currency.
(p.17)

Coinminers can slow devices, overheat batteries, and in some cases, render devices unusable. For organizations, coin miners can put corporate networks at risk of shutdown and inflate cloud CPU usage, adding cost.
(p.17)

Cryptojacking Attacks Explode by 8,500 Percent

IoT devices continue to be ripe targets for exploitation: Symantec found a 600 percent increase in overall IoT attacks in 2017, Which means that cyber criminals could exploit the connected nature of these devices to mine en masse.
(p.76)

Macs are not immune: we saw an 80 percent increase in coin mining attacks against Mac OS. By leveraging browser-based attacks, criminals do not need to download malware to a victim's Mac or PC.
(p.5)

ISTR – Key Messaging

Symantec identified a 200 percent increase in attackers injecting malware implants into the supply chain in 2017.

(p.39)

The Petya/NotPetya outbreak was the most notable example: after using Ukrainian accounting software as the point of entry, Petya/NotPetya used a variety of methods to spread laterally across corporate networks to deploy their malicious payload.

(p.39)

Implanted Malware Grows by 200 Percent, Compromising Software Supply Chain

One attack every month as compared to four attacks the previous year.

(p.39)

Hijacking software updates provides attackers with an entry point for compromising well-guarded networks.

(p.4)

ISTR – Key Messaging

In 2017, the number of new mobile malware variants increase by 54 percent year over year. (p.46)

Symantec also blocked 24,000 malicious mobile applications each day last year. (p.46)

Mobile Malware Continues to Surge

As older operating systems continue to be in use, this problem is exacerbated. For example, on Android, only 20 percent of devices are running the newest version and only 2.3 percent are on the latest minor release. (p.48)

Mobile users also face privacy risks from grayware, apps that aren't completely malicious but can be troublesome. Symantec found that 63 percent of grayware apps leak the device's phone number. With grayware increasing by 20 percent in 2017, this isn't a problem that's going away. (p.48)

ISTR – Key Messaging

In 2016, the profitability of ransomware led to a crowded market. In 2017, the market made a correction, lowering the average ransom cost (average demand $522) and signaling that ransomware had become a commodity.

(p.58)

Many cyber criminals may have shifted their focus to coin mining as an alternative to cash in while cryptocurrency where values are high.

(p.4)

Business-Savvy Cyber Criminals Price Ransomware for Profit

While the number of ransomware families decreased, the number of ransomware variants increased by 46 percent, indicating that criminal groups are innovating less but still very productive.

(p.14)

Excluding WannaCry and Petya/NotPetya ransomware detections went flat in 2017.

(p.13)

ISTR – Key Messaging

The number of targeted attack groups is on the rise with Symantec now tracking 140 organized groups. (p.21)

Last year, 71 percent of all targeted attacks started with spear phishing – the oldest trick in the book – to infect their victims. (p.24)

Majority of Targeted Attackers Use Single Method to Infect Victims

As targeted attack groups continue to leverage tried and true tactics to infiltrate organizations, the use of zero days is falling out of favor. Only 27 percent of targeted attack groups have been known to use zero-day vulnerabilities at any point in the past. (p.25)

The security industry has long discussed what type of destruction might be possible with cyber attacks. This conversation has now moved beyond the theoretical, with more than 10 percent of all attacks designed to destroy. (p.22)

Questions?

Symantec

"Ne mogu vjerovati da je sve to napravio klinac od 19 godina. I to naš dečko, iz Zaprešića! Mislim da je pred njim svijetla budućnost, nakon što odsluži kaznu, za njegove usluge mogli bi biti zainteresirani svjetski internetski maheri", nadovezao se

IZVELI ČETIRI MILIJUNA NAPADA, IMALI 239 TISUĆA KORISNIKA, A CIJELA OPERACIJA VODILA SE IZ - ZAPREŠIĆA!

Kako je pao jedan od najtraženijih hakera

Razum je sada zatvorenu internetsku stranicu webstresser.org administrirao sa stanovitim **Jovanom Mirkovićem**, također 19-godišnjakom iz Prokuplja, koji je web vodio pod nadimkom m1rk, a također je koristio i alias Mirkovik Babs kada bi bio na Facebooku. Nije čak ni skrivao čime se bavi, otvoreno je o tome raspravljao na najvećoj društvenoj mreži i nudio svoje usluge. Na njegovu se profilu mogu pronaći nadimci i drugih administratora, poput Kris, dakle Kristijana Razuma.

TEHNOLOGIJA

Mega haker iz Zaprešića iza rešetaka, policija slaže mozaik, a sugrađani čekaju rasplet

Curi sve više detalja o 19-godišnjaku iz Zaprešića koji je uhićen kao vođa najveće hakerske mreže u svijetu. Njegovi sugrađani podijeljenih su emocija. Za jedne je kriminalac, za druge heroj.

Hakeru iz Zaprešića mjesec dana pritvora. Kristijan i Jovan otkriveni i zbog tetovaže

Deep Dive

ISTR

Internet Security Threat Report

Volume 23

Symantec

Cryptocurrency malware

Coin mining malware:

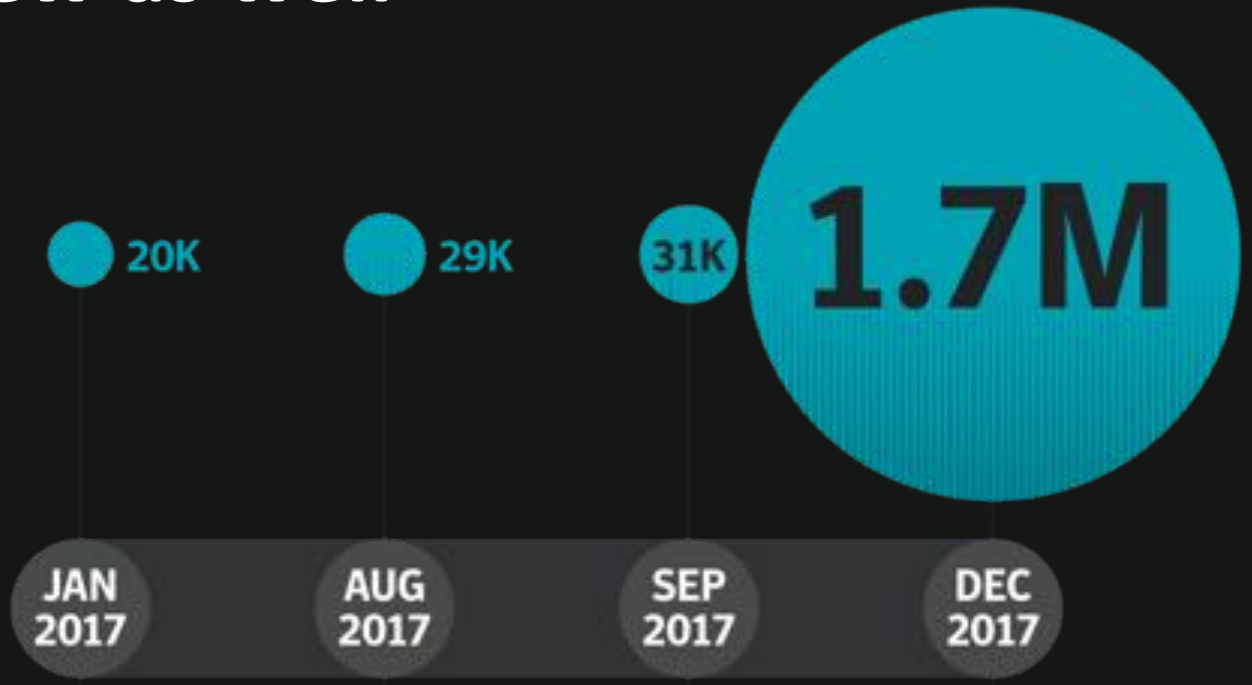
- Misuse local resources to mine cryptocurrencies with CPUs and GPUs
- Number of blocked samples increased by 8,500% in 2017
- Focus is not on Bitcoin
  - Preference for coins that can still be mined with a CPU e.g. Monero
  - Monero is also more anonymous then Bitcoin

Criminals adapt known scam schemes for the age of cryptocurrencies

- Attacks against crypto exchanges
- Wallet theft
- Phishing
- Tech support scams
- Fake mobile apps

As the price of cryptocurrencies increased, the attacker's interest in it grew as well

Detection count for coinminers on the endpoint



Monero price (average)

 |

Three main impacts of crypto currency mining

DEVICE PERFORMANCE

- Slower device
- CPU usage at 100%

ENERGY CONSUMPTION

- High energy consumption
- Fast battery drain
- Hard on mobile devices

SECURITY POSTURE

- Reflects badly on security posture

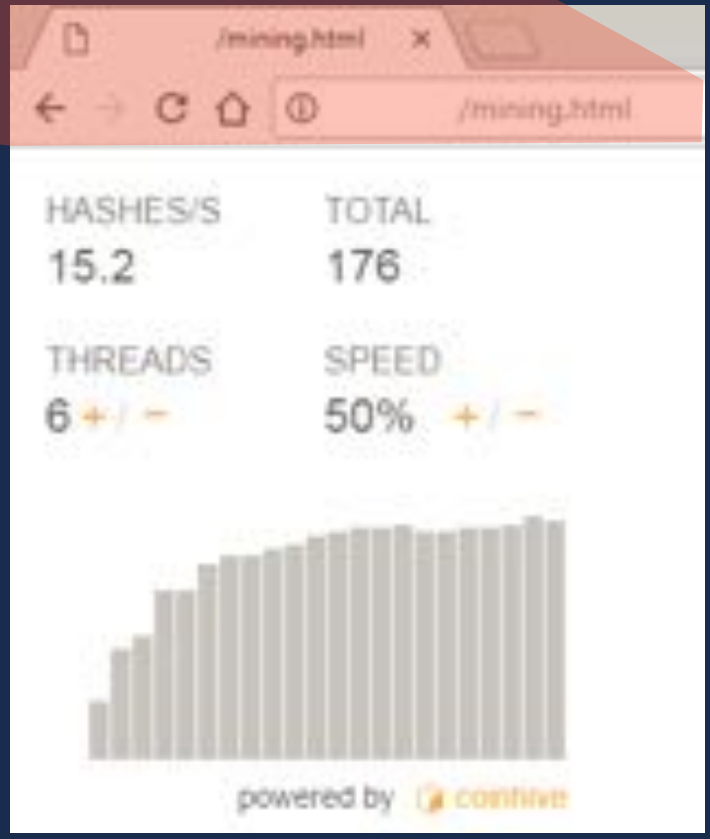
2 out of **3** victims are consumers
but targeting of organizations is increasing

Launching Excel with and without mining

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

Scripts that mine cryptocurrencies in your browser while you browse a site

```
<script src="https://some-website.tld/mining-script.js"></script>
```



- Very simple for the attacker, add one script line to website
- No exploits needed, client is not “hacked”
- Seen in 2011, but boosted by Coinhive script in Sept 2017
- Some instances are non-malicious e.g. ad replacements
- Try to hide as long as possible, e.g. with pop-under windows

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

Predictions for Cryptojacking

BOTNETS

Distributed mining, either through conventional botnets of malware-infected computers and IoT devices or browser-based coinminers, hosted on websites.

TARGETING ORGANIZATIONS

Targeting of corporate or organizational networks in order to harness the power of servers or supercomputers.

CLOUD HIJACKING

Cloud services offer the possibility of high-powered mining. This has a possible financial impact on cloud customers where they pay based on CPU usage.

Cyber crime is changing …

ISTR

Internet Security Threat Report

Volume

23

Symantec

Trends in cyber crime

Cybercriminals try to find new ways to generate revenue

Ransomware

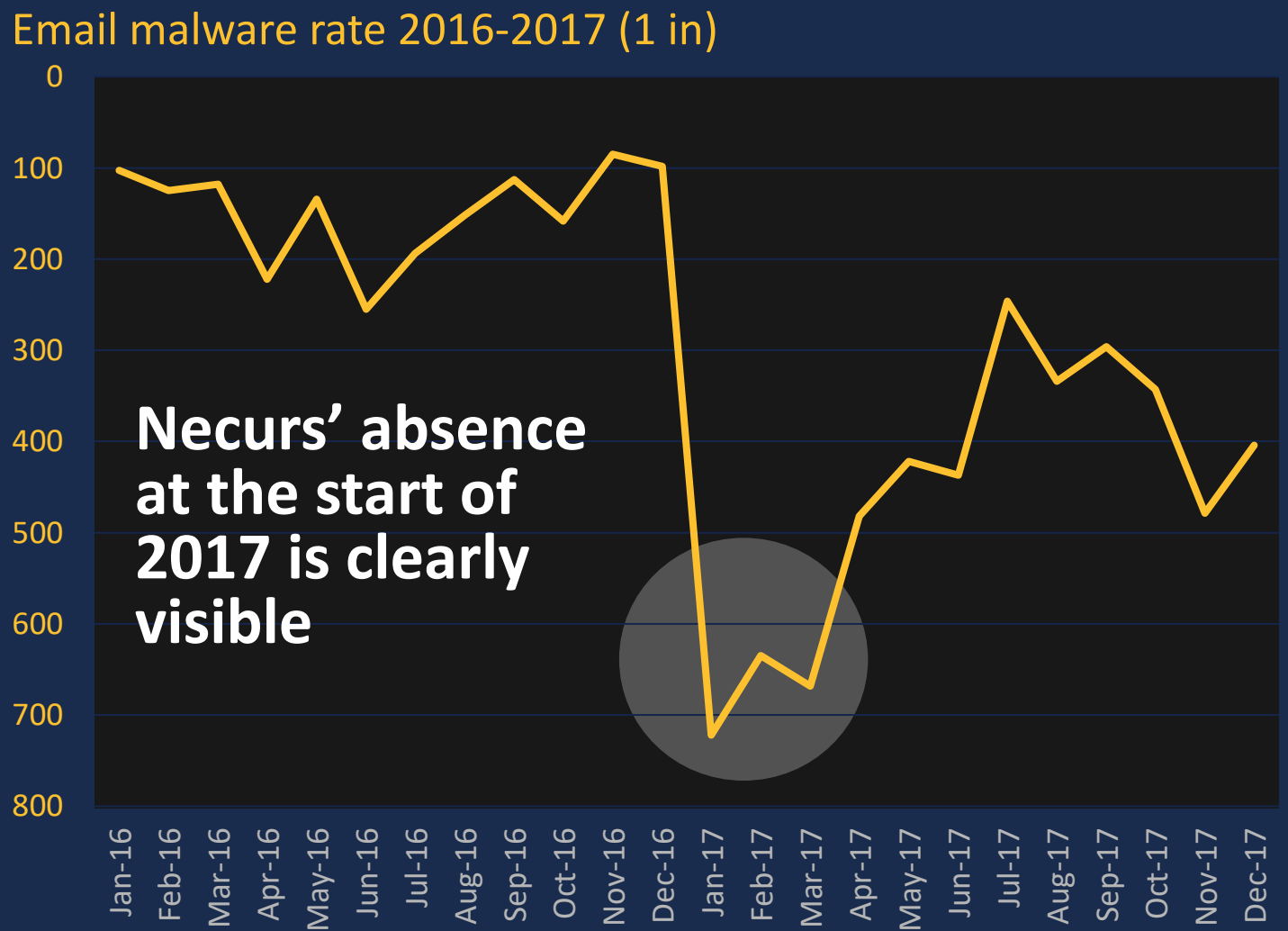
- Detections stable at 1,242 per day in 2017 (-2%)
- Downloader detections increased by 92%
- 46% increase in new ransomware variants
- Average ransom down to $522 from $1,070

Shift to other attacks

- To coin mining e.g. VenusLocker shifted from ransomware to crypto mining
- To financial Trojans e.g. Emotet activity increased by 2,000% in Q4

Necurs botnet reappeared

- **Very active spam botnet:**
  - 67,000 malicious emails per day
  - Maximum of 392,000 spam emails per day in October
- **Pivoted from ransomware (Locky) to financial Trojans**
- **Tried crypto coin pump & dump spams in 2017**
- **Currently expermenting with coin mining**



Supply Chain Attacks

ISTR

Internet Security Threat Report

Volume 23

Symantec

Attacking the software supply chain ...

Definition: *Implanting a piece of malware into an otherwise legitimate software package at its usual distribution location; This can occur during production at the software vendor, at a third-party storage location, or through redirection.*

... Is an extension of the "Living off the Land" attack trend

Fewer exploitable zero day vulnerabilities available

Only **27%** of targeted attack groups ever used zero days

Trojanized updates are difficult to identify

Trusted domain, digitally signed, and trusted update process

 |

One attack per month in...

2015

- APR — EvLog update compromised with malware
- MAY — Japanese Word Processor tool used to install malware
- JUN — XcodeGhost: Malware found in Apple dev environment
- DEC — Backdoor found in Juniper Networks firewall

2016

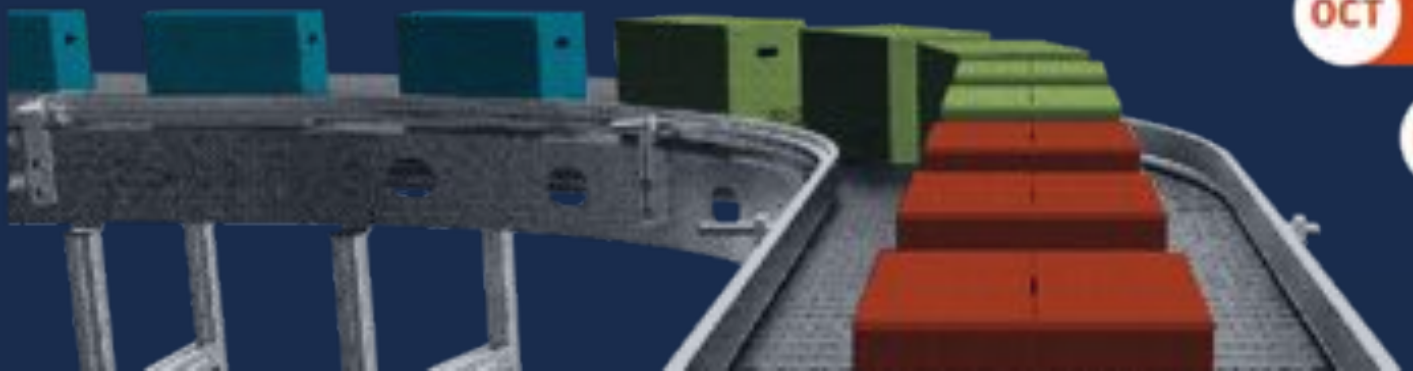
- SEP — S. Korean security software used to install malware
- OCT — Attackers hijack Brazilian Bank's entire DNS
- NOV — Ask Network Toolbar used to install malware
- DEC — Ask Partner Network updater used to install malware

2017

- FEB — • Trojanized version of Yeecall Pro for Android used to RAT • Kingslayer campaign hijacks sysadmin software updates
- MAR — Adobe reader installer bundled with malware
- MAY — • Handbrake video tool used to install malware • Operation WiySupply compromises editing tool updates
- JUN — M.E.Doc updater used to distribute Petya/NotPetya
- JUL — ePrica pharmacy software installs backdoor Trojan
- AUG — • CCleaner tool injected with malware • Backdoor found in NetSarang server mgmt. software
- SEP — • Modified Python modules found on official repository • "ExpensiveWall" malware found in Android SDK
- OCT — Elmedia Player for OSX bundled with malware
- NOV — Bitcoin Gold wallet replaced with malware
- DEC — Wordpress Plugins used to install Backdoors

NotPetya
M.E.Docs, 96% of initial infections in Ukraine

CCleaner
Multi staged, selecting interesting targets for follow-up



Why?

Trust

Infiltration of well-protected organizations by leveraging a trusted channel

Fast

number of infections can grow quickly as users update automatically

Focus

Targeting of specific regions or sectors

Reach

Infiltration of isolated targets, such as those in industrial environments

Hidden

Difficult for victims to identify attacks as trusted processes are hijacked

Privileges

May provide attacker with elevated privileges during installation

Three different methods to achieve their goal

Compromising the software supplier directly

Hijacking DNS, domains, IP routing or network traffic

Hijacking third-party hosting services

Questions?

Symantec