
ALSID

Active Directory Security

Threat Intelligence sharing session – 2019 Q4

Sylvain CORTES– Security Evangelist
December 2019

Agenda

- ✓ Alsid introduction
- ✓ 2019 Q4: Main five tendencies
- ✓ 2019: Cyber Security market statistics
- ✓ 2019 Q4: RYUK ransomware rising
- ✓ 2020: Anticipation

01
INTRODUCTION

ALSID

Break the dynamics of most modern threats to enterprises by preventing attacks to spread internally

Provide field-tested products with a seamless end-to-end user experience

A technical expertise recognized worldwide and awarded by numerous prestigious prizes

AXA INVESTMENT MANAGERS · Lagardère · SANOFI · sodexo · UNIBAIL-RODAMCO-WESTFIELD · VINCI ENERGIES

The Features We Are Proud Of

Cutting-Edge Security Technology

HARDEN, DETECT, RESPOND
All your practices extended to your most vital IT asset: AD

TRUE REAL-TIME
Live exposure visualization, immediate attack alerts

STEP-BY-STEP RECOMMENDATIONS
A follow-the-guide approach for AD admins who are new to security

INTELLIGENCE-DRIVEN, AD-NATIVE
Beyond compliance, detect AD-specific attack patterns

Seamless End-to-End User Experience

NO AGENTS, NO PRIVILEGES
An instant-on application with hardly a footprint on operations

DASHBOARD-ORIENTED UX
To simplify decision-making and prioritization

SIMPLE, NO-NONSENSE ARCHITECTURE
Using standard protocols and proven technologies

NATIVE INTEGRATIONS WITH YOUR OTHER PRACTICES
Turbo-charge your SIEM, SOAR, and IAM solutions

ALSID

A Comprehensive Approach

Anticipate Threats

- Bring vulnerabilities and weaknesses to light
- Prioritize remediations with threat scores and costs estimates
- Harden your directory infrastructure with our step-by-step guides

AD admins
Blue Teams & Auditors

Detect Attacks

- Detect attacks in true real-time with our AD-specific threat intelligence
- Make AD an integral part of your security practice with SIEM & SOAR integrations
- Enable your Threat Hunters with AD-native investigation capabilities

SOC Analysts
Threat Hunters

Respond To Breaches

- Replay attacks and hunt for patients zero
- Remediate at machine-speed through our orchestration playbooks
- Detect persistence mechanisms and kick them out for good

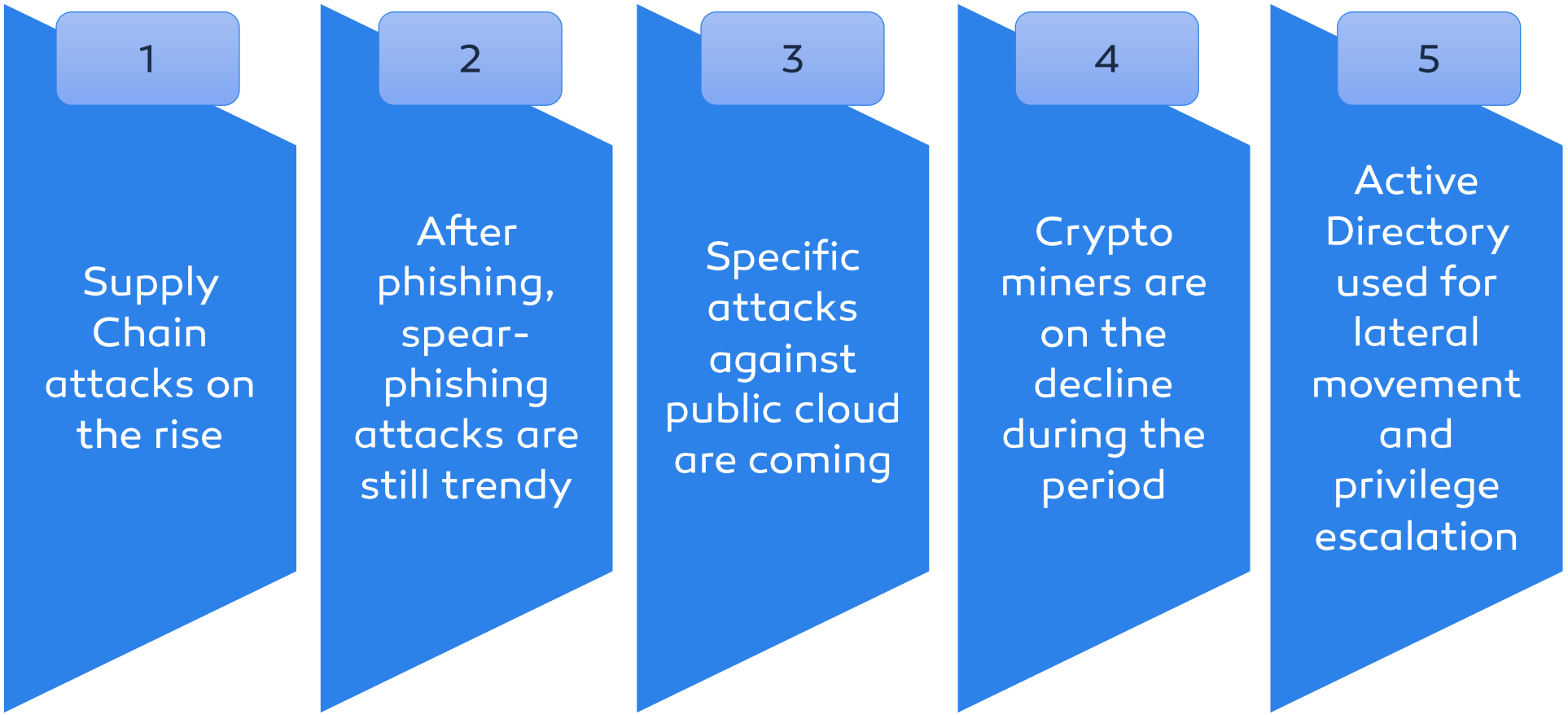
Incident Responders

ALSID

02

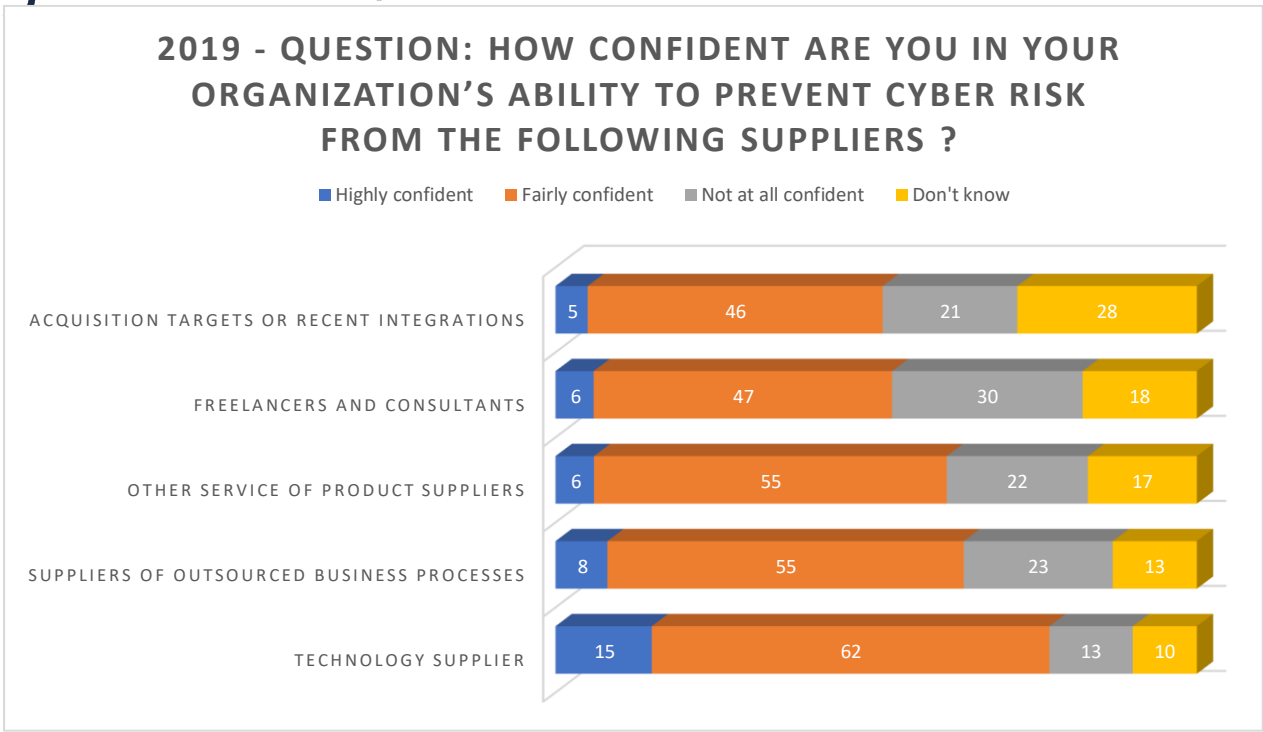
2019 Q4 – MAIN FIVE TENDENCIES

2019 Q4: Main Five Tendencies



2019 Q4: Supply Chain attacks on the rise

- ✓Supply chain attacks doubled in 2019 compared to 2018
- ✓Most of the Software Supply chain attacks are made by installing malicious code into legitimate software
- ✓National Cyber-Agencies created specific content to manage supply-chain vendors: USA, France, etc.
- ✓Supply chain attack examples:
  - ✓ ShadowHammer attack on ASUS
  - ✓ NordVPN attack
  - ✓ PrismWeb e-commerce attack



2019 Q4: After phishing, spear-phishing attacks are still trendy

- ✓Raise of Sextortion scam email: hackers use passwords stolen from major data breaches to abuse users and make them pay Bitcoin ransom
- ✓Spear-phishing are more and more accurate using personal targeting
- ✓Increase of two bands attacks by sending emails from valid business addresses: the first victim is only used to attack the second one with valid email address

2019 Q4: Specific attacks against public cloud are coming

- ✓ Misconfigured cloud environments was one of the main causes of data breaches

- ✓ Examples:
  - ✓ Some unprotected Amazon servers provided Facebook users records exposition
  - ✓ A misconfiguration in the box.com environment revealed several terabytes of sensitive data to the world

2019 Q4: Crypto miners are on the decline during the period

- ✓ We see less attacks to directly install a crypto miner and get some *coins
- ✓ Nevertheless we know that > 70% of cryptocurrency transactions are done for illegal activity
- ✓ The hackers will focus on attacks to get *coins from a ransom – not trying to mine directly on the target network: doing this they increase the return of investment because the target network is not structured to mine

2019 Q4: Active Directory used for lateral movement and privilege escalation

- ✓ > 80% of the attacks are using Active Directory to perform lateral movement and privilege escalation
- ✓ > 60% of the new malwares include specific codes to target AD misconfiguration (mimikatz, Rubeus, etc.)
- ✓ Cheaper tools and kits to target AD: Cybercrime tools and kits can be purchased for as little as $1 on the Dark Web and online marketplaces
- ✓ Main feedback from 2019: no need to be expert anymore to create a cybercrime tool to target AD – just invest between 0,00013 and 0,00015 Bitcoins to buy a kit

03

2019: CYBER SECURITY MARKET STATISTICS

2019: Cyber Security Market Statistics: Economy

2019 figures:

- ✓ $1.5 trillion cybercrime economy The cybercrime economy has grown to enjoy at least $1.5 trillion in profits each year
- ✓ 300 billion cybersecurity Market The value of the cyber security market is anticipated to reach $300 billion by 2024, according to a 2019 press release by Global Market Insights, Inc.
- ✓ $15 billion in cyber security funding
- ✓ 9% increase in cyber security spending
- ✓ Small businesses invest <$500 per year in cyber security products

2019: Cyber Security Market Statistics: Attacks cost

2019 figures:

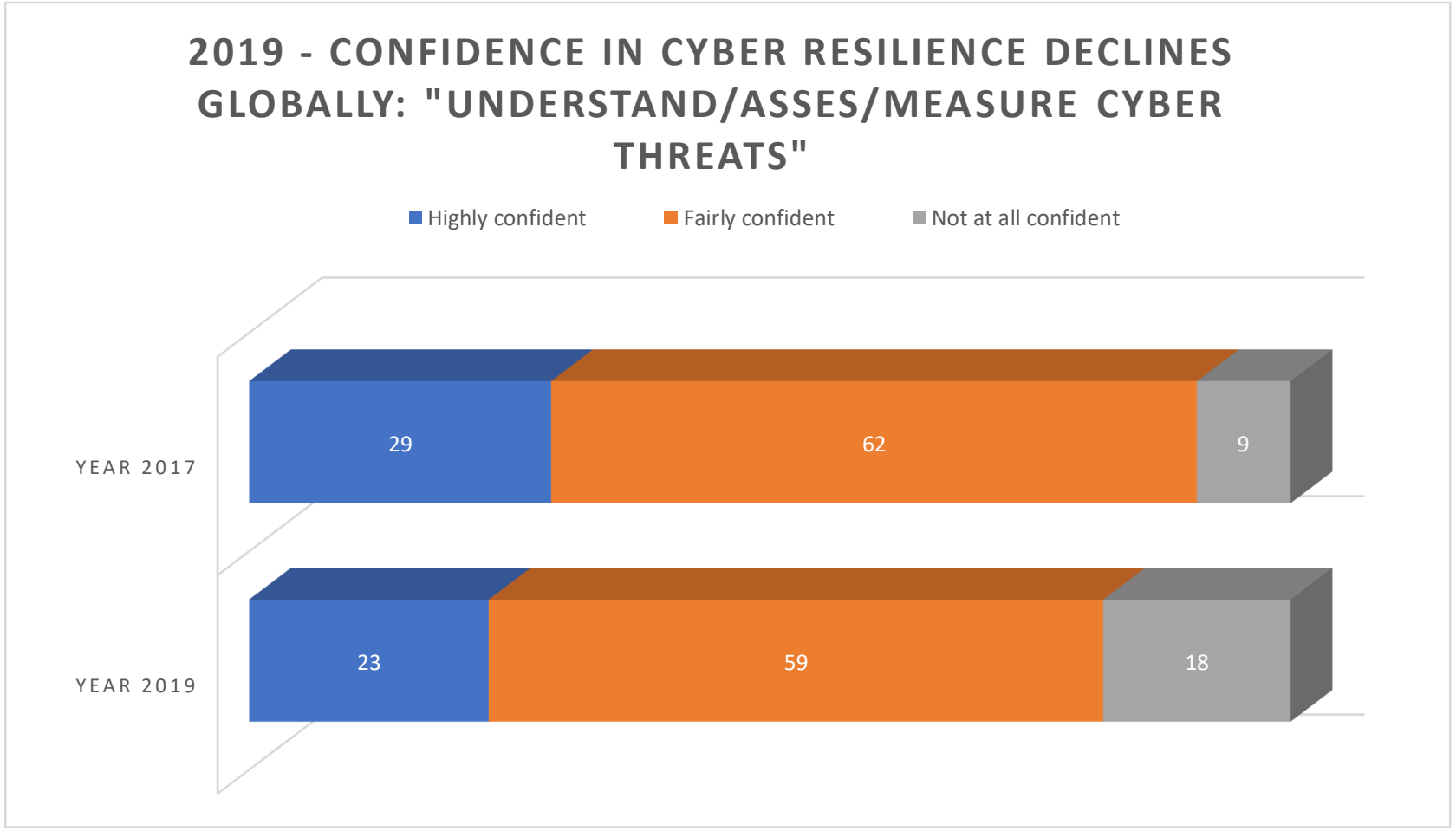
- ✓ Cybercrime damages cost $6 trillion during 2019
- ✓ Ransomware damage estimated to $20 billion during 2019
- ✓ In average, worldwide, global cybercrime costs organizations $13 million during 2019

2019: Cyber Security Market Statistics: Feed back from the field

2019 figures:

- ✓ 49.6 days between breach discovery and reporting dates
- ✓ >70% of cryptocurrency transactions are done for illegal activity
- ✓ Security breaches up >11%
- ✓ SMBs are targeted 43% of the time
- ✓ Ransomware attacks occur every 14 seconds

2019: Confidence in cyber resilience declines globally

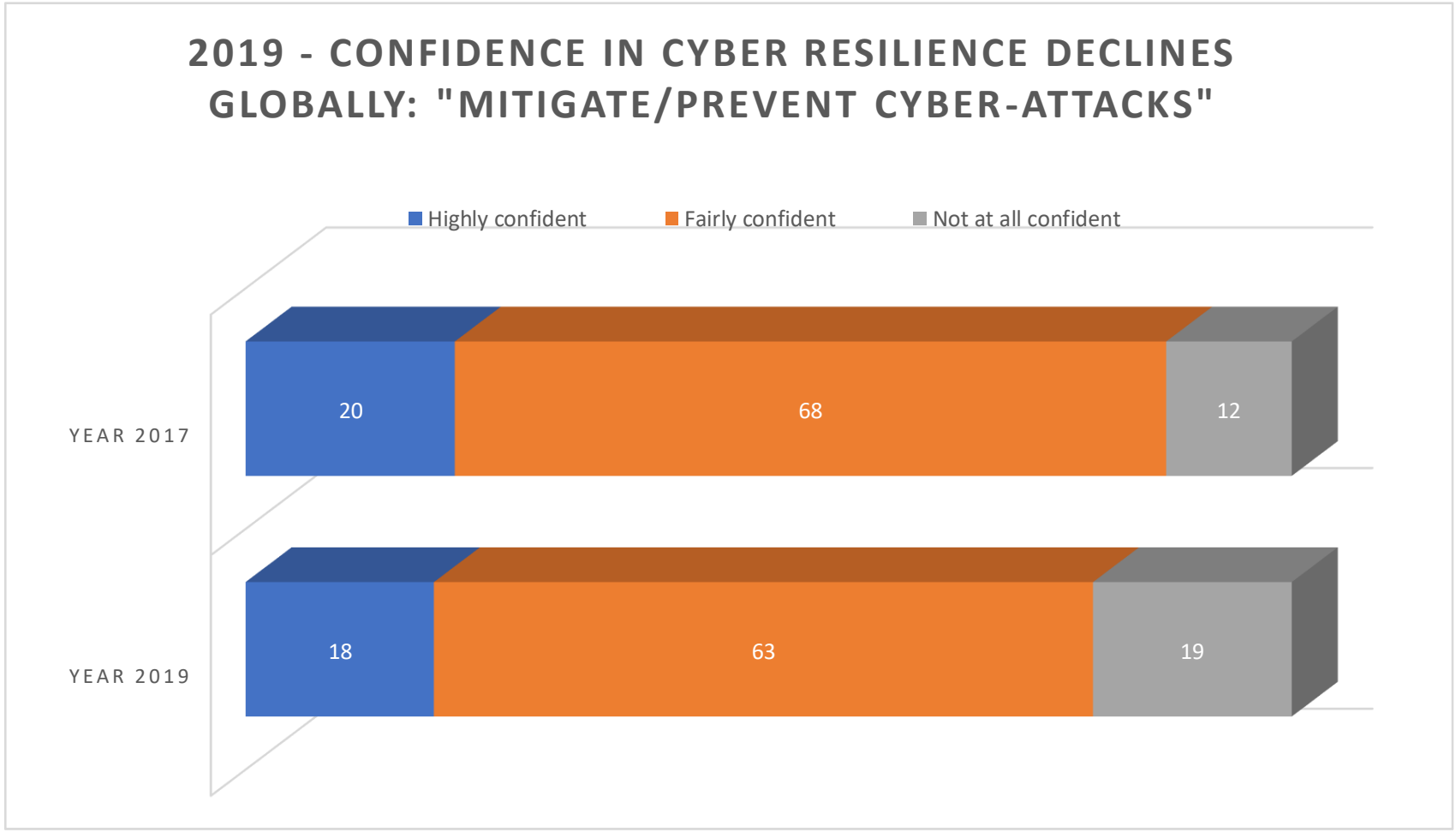


Along 2019, as Alsid, we meet some prospects who invested a lot of money and effort in Anti-Virus or EDR solutions in year 2018.

But they were hacked.

We certainly feel discouragement from certain contacts.

2019: Confidence in cyber resilience declines globally

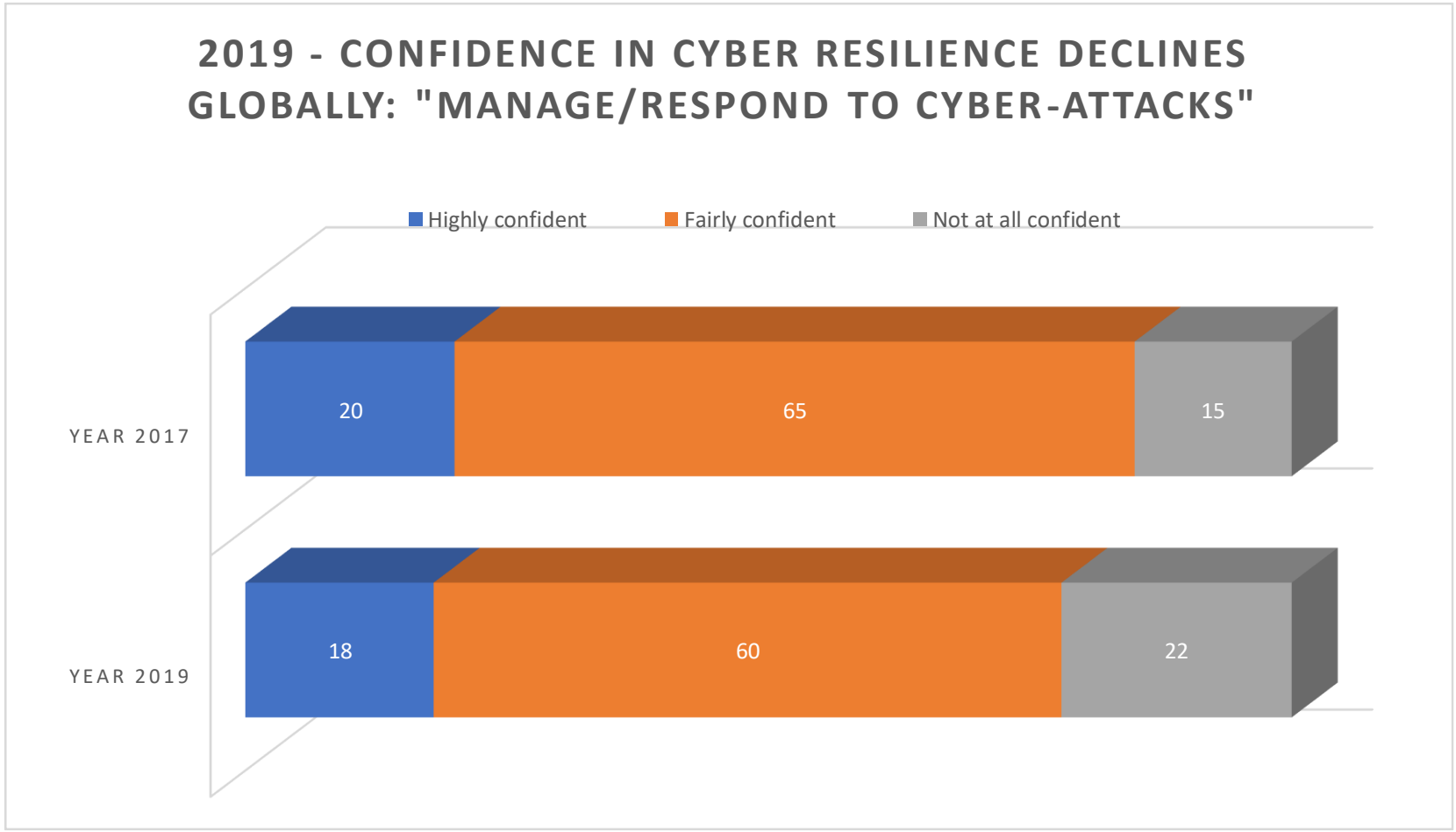


Along 2019, as Alsid, we meet some prospects who invested a lot of money and effort in Anti-Virus or EDR solutions in year 2018.

But they were hacked.

We certainly feel discouragement from certain contacts.

2019: Confidence in cyber resilience declines globally



Along 2019, as Alsid, we meet some prospects who invested a lot of money and effort in Anti-Virus or EDR solutions in year 2018.

But they were hacked.

We certainly feel discouragement from certain contacts.

04

2019 Q4: RYUK RANSOMWARE RISING

Ryuk in a nutshell

- ✓ Huge increase of Ryuk ransomware attacks during the second part of 2019 Q4
- ✓ Ryuk is associated to WIZARD SPIDER – a Russian-based criminal organization, targeting large organizations for a high-ransom return. This methodology, known as “big game hunting”
- ✓ Ryuk includes some specific tools in order to use AD to perform Escalation or Lateral movement
- ✓ Remarkable abilities:
  - ✓ Bypasses anti-virus products
  - ✓ Maintains persistence on the targeted machine
  - ✓ Runs as legitimate process by injecting to Windows process
  - ✓ Terminates processes
  - ✓ Stops services

Ryuk behavior

- ✓ Initial compromise is performed through TrickBot (not always, but often) or through Emotet which includes a download function to get Ryuk on the system
- ✓ Pwgrab, a TrickBot module, can perform the first credentials hack
- ✓ At the end the Ryuk binary is downloaded and start his actions following these different steps:
  - ✓ An obfuscated PowerShell script is executed and connects to a remote IP address.
  - ✓ A reverse shell is downloaded and executed on the compromised host.
  - ✓ PowerShell anti-logging scripts are executed on the host.
  - ✓ Reconnaissance of the network is conducted using standard Windows command line tools .
  - ✓ Lateral movement throughout the network is enabled using Remote Desktop Protocol (RDP).
  - ✓ Service User Accounts are created.
  - ✓ PowerShell Empire is downloaded and installed as a service.
  - ✓ Lateral movement is continued until privileges are recovered to obtain access to a domain controller.
  - ✓ PSEXEC is used to push out the Ryuk binary to individual hosts.
  - ✓ Batch scripts are executed to terminate processes/services and remove backups, followed by the Ryuk binary.

Ryuk behavior

Malicious documents files (droppers) distributed as attachments through phishing attacks

User is invited to open the attachment, then malicious code is run to download additional code: Trickbot or Emotet

Dropper downloads Trickbot or Emotet to be used for:

- Stealing credentials
- Downloading the ransomware

Performs lateral movement using Active Directory:

- MS17-010 vulnerability (SMB exploit)
- Networks shares (compromised accounts)
- PsExec

Upon execution, it will perform its encryption routine

Local and shared files becomes encrypted and ransom notes are activated

Ryuk ransom

Ryuk ransom notes:

~~RyukReadMe.txt~~

```
Your network has been penetrated.

All files on each host in the network have been encrypted with a strong algorithm.

Backups were either encrypted or deleted or backup disks were formatted.
Shadow copies also removed, so F8 or any other methods may damage encrypted data but
not recover.

We exclusively have decryption software for your situation
No decryption software is available in the public.

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.
This may lead to the impossibility of recovery of the certain files.

To get info (decrypt your files) contact us at
KurtSchweickardt@protonmail.com
or
KurtSchweickardt@tutanota.com

BTC wallet:
14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk

Ryuk
No system is safe
```

- ✓ Various ransom notes have been observed
- ✓ The body of the template is static with the exception of the email address and the Bitcoin (BTC) wallet address, which may change
- ✓ Email address is using prontonmail.com
- ✓ The ransom demand varies significantly – we think WIZARD SPIDER calculates the ransom amount based on the size and value of the victim organization
- ✓ To date, the lowest observed ransom was for 1.7 BTC and the highest was for 99 BTC
- ✓ WIZARD SPIDER has made 705.80 BTC, which has a current value of $3.7 million (USD)

05

2020: ANTICIPATION

Our anticipation for 2020

- ✓ Ransomware damages will increase
- ✓ The malware kits are cheaper and cheaper: we will see a global movement from unknown criminal groups – in the coming months, a kid without any specific technical expertise, from his bedroom, could be a new criminal
- ✓ Active Directory will be the preferred target, because the attacker knows in advance it resides in your organization
- ✓ MacOS vulnerabilities are increasing, we will see more ransomwares dedicated to MacOS – In the large organizations, the MacOS are integrated in AD, this will be a new challenge for AD security people