



ALSID



# Active Directory Security

## Threat Intel Report Q1 2020

---

Sylvain Cortes – Microsoft MVP & Security Evangelist  
March 2020

# Agenda



- ✓ Alsid Introduction
- ✓ Q1 2020: Top 5 Attack Trends
- ✓ 2020: The Rise of Ransomware-as-a-Service
- ✓ Q1 2020: Attack Examples



# 01

## INTRODUCTION



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**



# 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

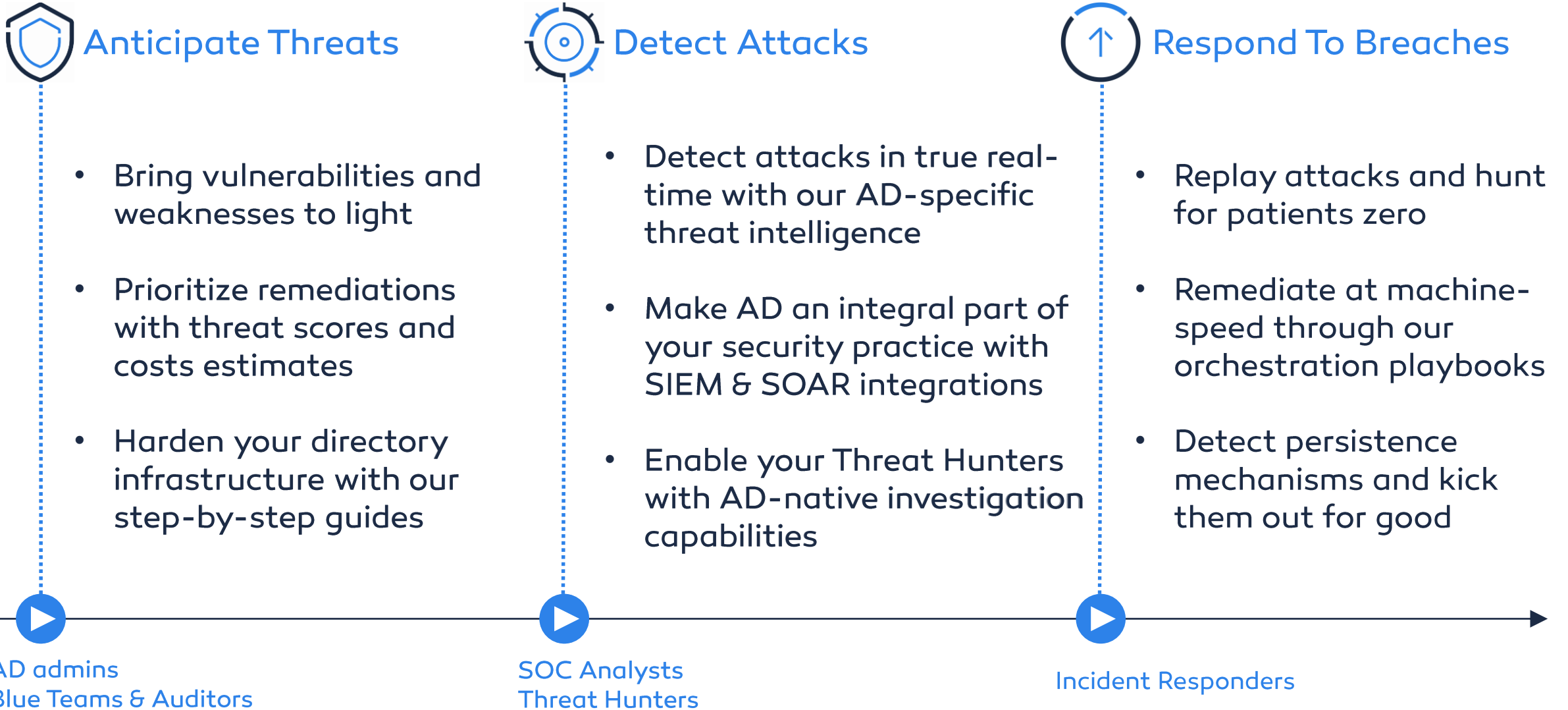
Using standard protocols and proven technologies



### NATIVE INTEGRATIONS WITH YOUR OTHER PRACTICES

Turbo-charge your SIEM, SOAR, and IAM solutions

# A Comprehensive Approach





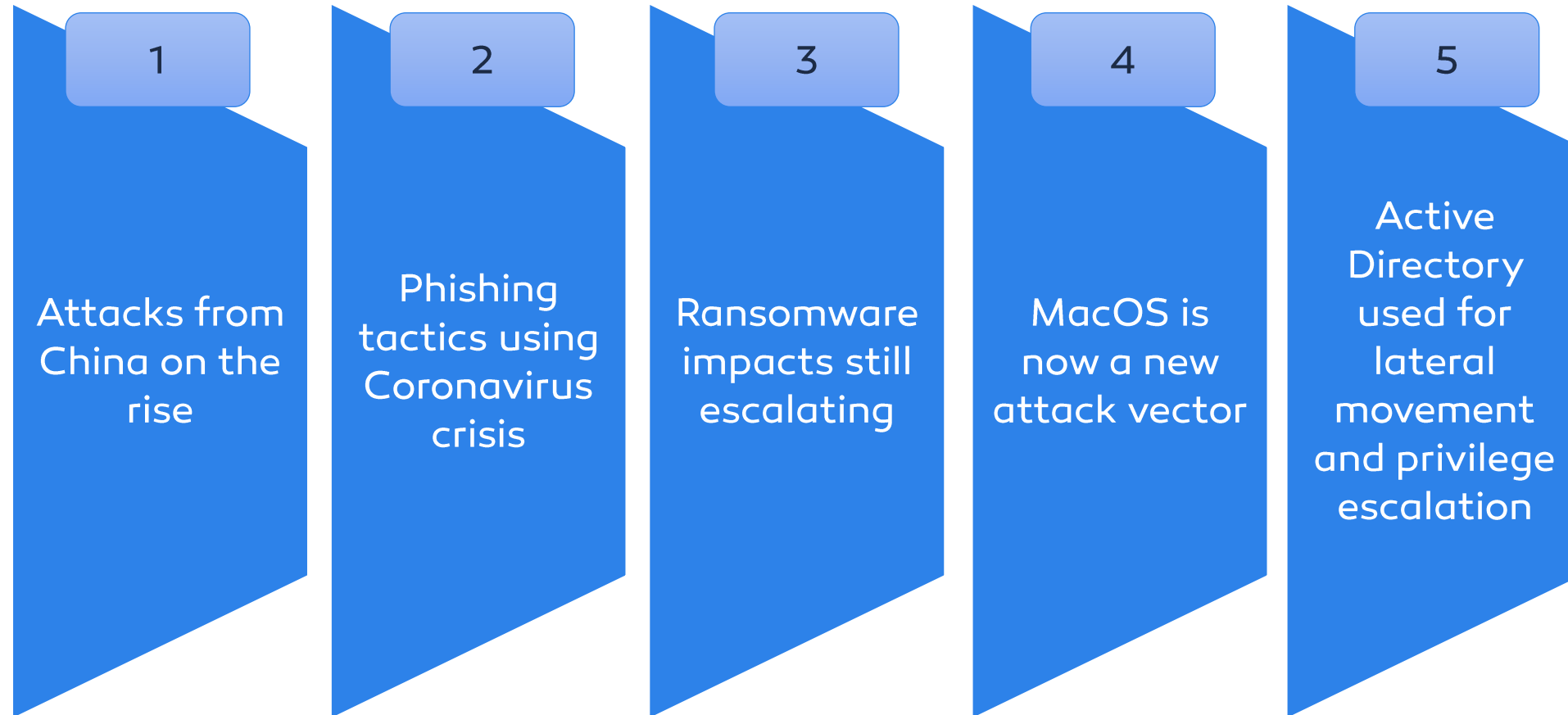
A photograph of a modern architectural interior, likely a large atrium or hallway. The space is characterized by curved glass walls and a white, curved ceiling with recessed lighting. The floor is highly reflective, mirroring the ceiling and walls. The overall color palette is dominated by blue and white, with the blue being a semi-transparent overlay on the image.

# 02

## Q1 2020 – TOP 5 ATTACK TRENDS



# 2019 Q4: Main Five Tendencies





- ✓ Chinese cybercriminal activity exceeds \$15 billion USD. A recent Chinese study provided figures on the Chinese cybercriminal underground: <https://bit.ly/3a1jbSC>
- ✓ Observation shows Chinese non-state cybercriminals transform from small organizations into well-organized criminal groups targeting international organizations
- ✓ Asia is the focus of attack, and advanced ransomware targeting Active Directory for fast movement is the main attack vector



- ✓ 800+ million people have Internet access in China: as this number increases, more criminal groups are engaging in cybercriminal activities to increase revenues
- ✓ The cybercriminal activities from China is growing at an annual rate of 30%
- ✓ An estimated 400,000 people are working for cybercriminal groups in China
- ✓ According to dark web marketplaces, stolen data provided by Chinese actors is growing at a rate of 23% every year



- ✓ Dark web marketplaces are not easily accessible for Chinese cybergroups because the government still blocks access to Tor and anonymous Internet access – so the dark web is only used to sell services (e.g. malware customization) or stolen data
- ✓ Many of the Chinese cybergroups are using “classic” forums (e.g. Weibo or Baidu) and “language codes” to exchange information between groups:

Devices, computers, or servers

= Chicken meat: 鸡肉

Malicious websites

= Fishing boxes: 钓鱼箱

Stolen accounts or passwords

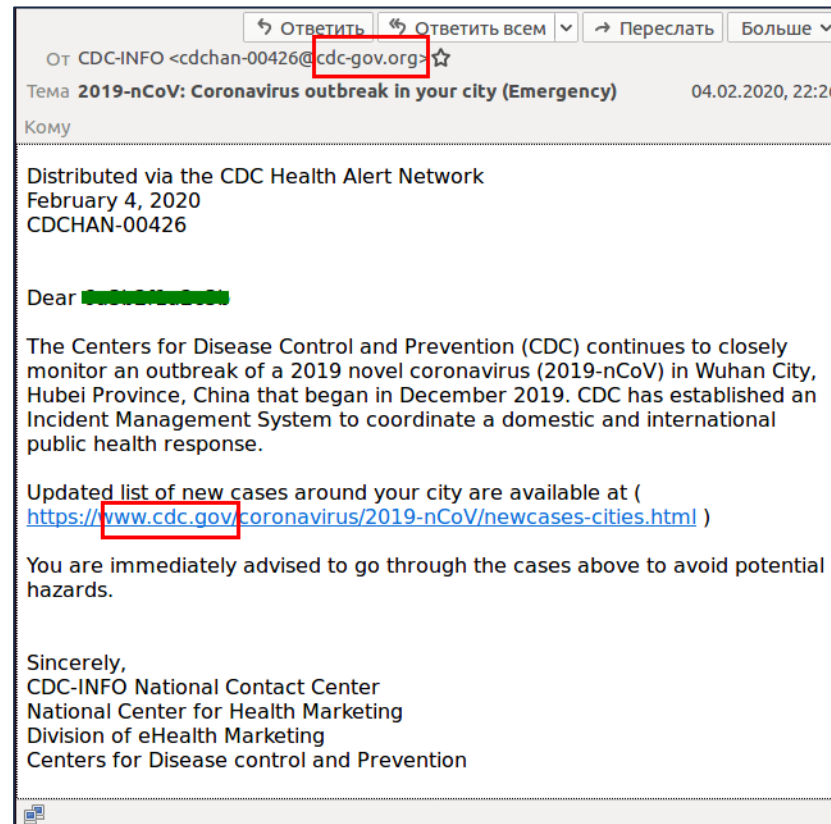
= Letters/envelopes:  
字母      信封

Stolen financial data or credit cards

= Tracking material:  
追踪材料



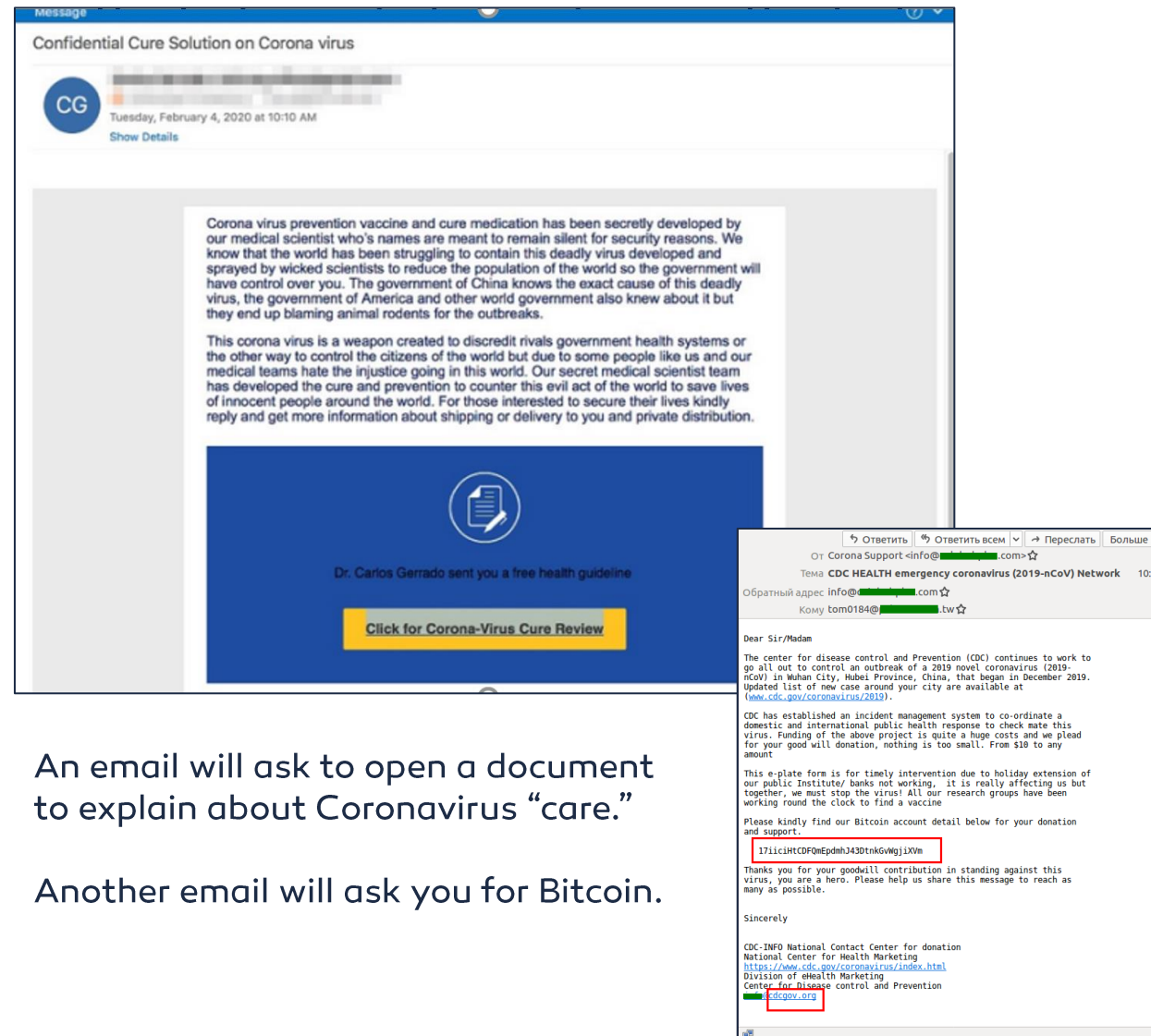
- ✓ New cyberattacks exploit your fears with phishing emails designed to steal money, get personal information, and infect computers



This email is not from the CDC.

It's a phishing attack designed to harvest user names and passwords from people who click on the link.

The link looks like it will take you to a CDC.gov website about the coronavirus. It will not.



Another email will ask you for Bitcoin.





- ✓ Malware threat rate and numbers detection is in line with those of Q4 2019
- ✓ Malware automation and industrialization are increasing (estimated to grow 13% over Q4 2019)
- ✓ New Ransomware-as-a-Service platforms are spreading: better service offers and more advanced technical capabilities



- ✓ Adwares infection by OS for 2019 and Q1 2020:
  - ✓ Windows OS: 24 million
  - ✓ MacOS: 30 million
- ✓ Average number of threats by OS for 2019 and Q1 2020:
  - ✓ Windows OS: 6 threats per endpoint
  - ✓ MacOS: 11 threats per endpoint
- ✓ Rise of MacOS threats: increase of 400% in 2019 and Q1 2020 compared to 2018!



- ✓ Threat sophistication increased, with many more attacks using exploits, credential stealing tools, or multi-step attacks
- ✓ Mass infections targeting large organizations increased – AD usage is now a “by design” behavior: embedded Mimikatz increased by 42% during Q1 2020 compared to Q3/Q4 2019
- ✓ Emotet & Trickbot trojans are still increasing: the top 5 infections during Q1 2020 were using Emotet or Trickbot
- ✓ MacOS integrated in Active Directory appears to be a good new attack vector to infect whole organizations

© Alsid copyright 2019

A photograph of a modern architectural interior, likely a large atrium or hallway. The space is characterized by curved glass walls and a white, curved ceiling with recessed lighting. The floor is highly reflective, mirroring the ceiling and walls. The overall color palette is dominated by blue and white, with the blue being a deep, saturated hue and the white being a bright, clean color. The perspective is from a low angle, looking down a long, curved corridor that leads the eye towards the right side of the frame.

# 03

## 2020: THE RISE OF RANSOMWARE-AS-A-SERVICE



- ✓ Definition: “Ransomware-as-a-Service is abbreviated as RaaS. This is a form of Software-as-a-Service (SaaS) used by underground vendors to threaten actors by providing them a ransomware platform tool.”
- ✓ Ransomware-as-a-Service (RaaS) borrows from the Software-as-a-Service (SaaS) model. This subscription-based model enables even the novice cybercriminal to launch ransomware attacks without much difficulty. You can find various RaaS packages on the market that reduce the need to have much technical knowledge of how to create ransomware. This malicious model allows anyone to become an “affiliate” of an established RaaS package or service.





## ✓ RaaS example: Sodinokibi

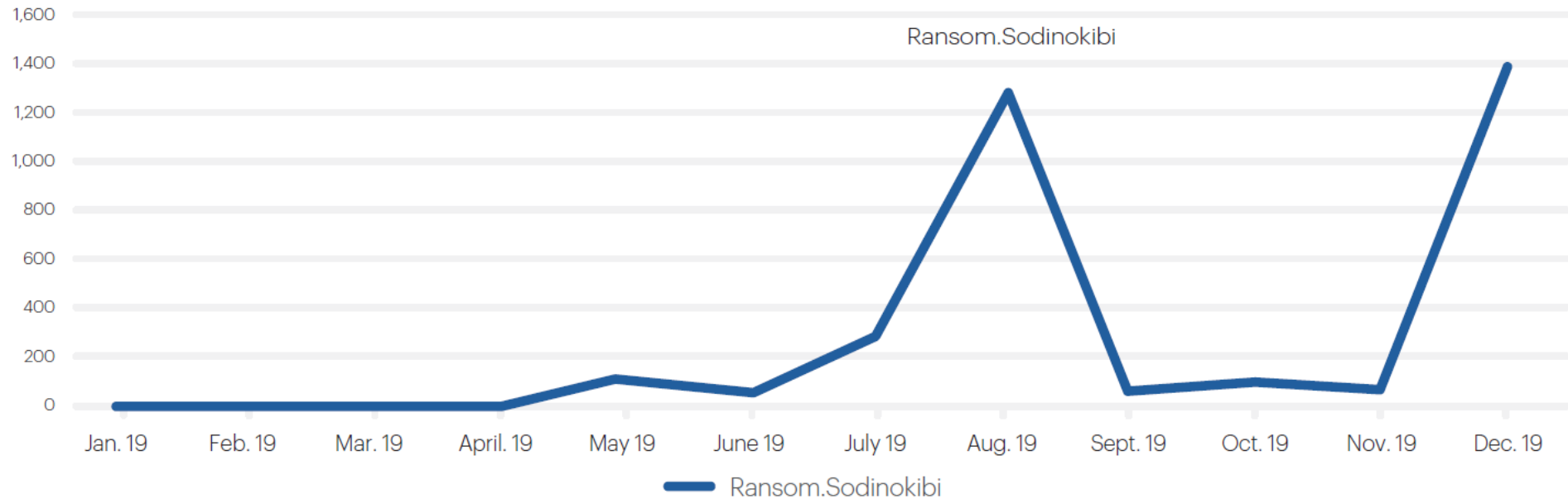
Sodinokibi attack methods include:

- › Active exploitation of a vulnerability in Oracle WebLogic, officially named CVE-2019-2725
- › Malicious spam or phishing campaigns with links or attachments
- › Malvertising campaigns that lead to the RIG exploit kit, an avenue that GandCrab has used before
- › Compromised or infiltrated managed service providers (MSPs) to push the ransomware en masse. This is done by accessing networks via a remote desktop protocol (RDP) and then using the MSP console to deploy the ransomware.
- › Evading detection through the “Heaven’s Gate” technique used to execute 64-bit code on a 32-bit process, which allows malware to run

*Source:  
Malwarebytes*



## Sodinokibi ransomware business detections 2019



Source:  
Malwarebytes

# 2020: The Rise of Ransomware-as-a-Service



## ✓ Other examples: Philadelphia & Stampado

Get Philadelphia at a Special Price!	
\$389	Unlimited License
Unlimited Builds	
Unlimited Campaigns	
No monthly fees or % rate	
Constant Updates	
Bitcoin Payment Autodetect	
Plain-English help file	
No dependencies (.net or whatever)	
Get In Touch!	

Philadelphia

As Featured on: [Forbes](#), [Softpedia](#), [The Wall Street Journal](#) and [MSN.com](#)

Stampado is a Quick-Deploy Ransomware with a dreamly price that allows you to start your First Campaign in Seconds! You do not need servers, and the Payment options will be as many as you know: Bitcoin, Paypal, Bank Transfer or whatever else.

## Your First campaign in 30 seconds

Just Run Stampado and you'll be presented with a panel where you will find everything you need: Generate Builds, create and track campaigns, decrypting individual files (for victims who want a proof that you will do so once they pay) and generate Decryption Key.



Stampado

# 2020: The Rise of Ransomware-as-a-Service



## ✓ Other examples: FileFrozzr

Online builder

You must have [license](#) to use builder.

Receiver address

Payment page

Encryption method

Default decrypter

UAC bypass

Locker message

Receiver address should be put in with protocol and without slash on end. Example: <http://onionsite.onion/p.php>

Payment page should be written in the same way.


In locker message word {IDENTY} would be replaced with User ID so that you can construct links to the payment page. Example <http://ytrfjyeddvasd.onion/payment.php?ID=>  
>>> <http://ytrfjyeddvasd.onion/payment.php?ID=AAAA-AAAA-AAAA>

Create build Download panel

Panel setup short guide

Buy license

The purchase is considered completed after first confirmation.  
Current price of FROZR is 0.14 BTC ~150\$  
To buy license send exactly 0.14 BTC to  
[18Tbd2SCSY5oPwXwpyeHdB3gp8edLYq9uf8](https://blockchain.info/address/18Tbd2SCSY5oPwXwpyeHdB3gp8edLYq9uf8)  
or pay using QR code



Support

If you need support in the installation of the panel, configuration of FILE FROZR or any other help, feel free to communicate us by following contacts:  
Tox Id: C216445DDE28F475A725941F75D3FBA52F83D8C7EA774F03161C90ABA3F16768D4B4ADE77817  
E-mail support: [filefrozzr@protonmail.com](mailto:filefrozzr@protonmail.com)  
Jabbder (OTR+PGP) [frozzr@thesecure.biz](mailto:frozzr@thesecure.biz)

To install the panel, you will need a host or a server with MySQL database

1. Setup MySQL database, and using MySQL shell or PhpMyAdmin and ex
2. Upload panel files except bd.sql to your host.
3. Edit config.php
4. Check is your setup working by accessing log.php?LOGIN=passfromconfig

If you are not satisfied by the current panel, send your ideas to our support contacts (better e-mail), or wait until the ASP.NET panel is released. Due to your responses, we may change both PHP and ASP.NET panels.

# 2020: The Rise of Ransomware-as-a-Service



## ✓ RaaS business model



1 RaaS factory:  
Creation of a  
RaaS offer  
and  
publication  
on dark web



3 The RaaS factory  
will  
automatically  
create a  
ransomware code  
with an affiliate  
number + step-  
by-step  
information for  
how to launch a  
ransomware  
campaign, a  
platform which  
displays the  
status of the  
attack using a  
real-time  
dashboard, etc.



5 Once the  
organization  
pays the ransom,  
50% of the  
money goes to  
the Beginner,  
50% of the  
money goes to  
the RaaS factory



2 Beginner will go  
to the RaaS  
platform and  
ask for a  
Ransomware Kit



4 Beginner will use  
the RaaS to  
deploy, infect  
organizations, and  
demand ransom



# 04

## Q1 2020: ATTACK EXAMPLES





- ✓ **Travelex: Ransomware & Data breach – source [EN]:**  
<https://www.nytimes.com/2020/01/09/business/travelex-hack-ransomware.html>
- ✓ **Enloe Medical Center: Ransomware – source [EN]:**  
<https://www.chicoer.com/2020/01/04/cyber-attack-hits-enloe-patient-records-safe-officials-say/>
- ✓ **Tampa Bay Times: Ryuk Ransomware – source [EN]:**  
<https://www.tampabay.com/news/business/2020/01/23/tampa-bay-times-hit-by-ransomware-attack/>
- ✓ **ISS World: Emotet + Ryuk Ransomware – source [EN]:**  
<https://www.computerweekly.com/news/252478890/Facilities-firm-ISS-World-crippled-by-ransomware-attack>