SophosLabs 2020 Threat Report

Walter Narisoni
Sales Engineer Manager

The 2020 Threat Report

- A look at developments in cybersecurity for 2020
- The challenges the world faces for the coming year – securing data, devices and people in an increasingly complex environment
- Produced by the SophosLabs research team and published on 5 November 2019

The Evolving Landscape

- Less skilled cybercriminals are being forced out of business, while the fittest step up their game to survive, leaving a landscape with fewer, but smarter and stronger adversaries

- They use legitimate tools, stealth, multiple attack vectors and hybrid automated-manual (active) attacks to target potential victims

- IT security professionals need to adapt their game plan

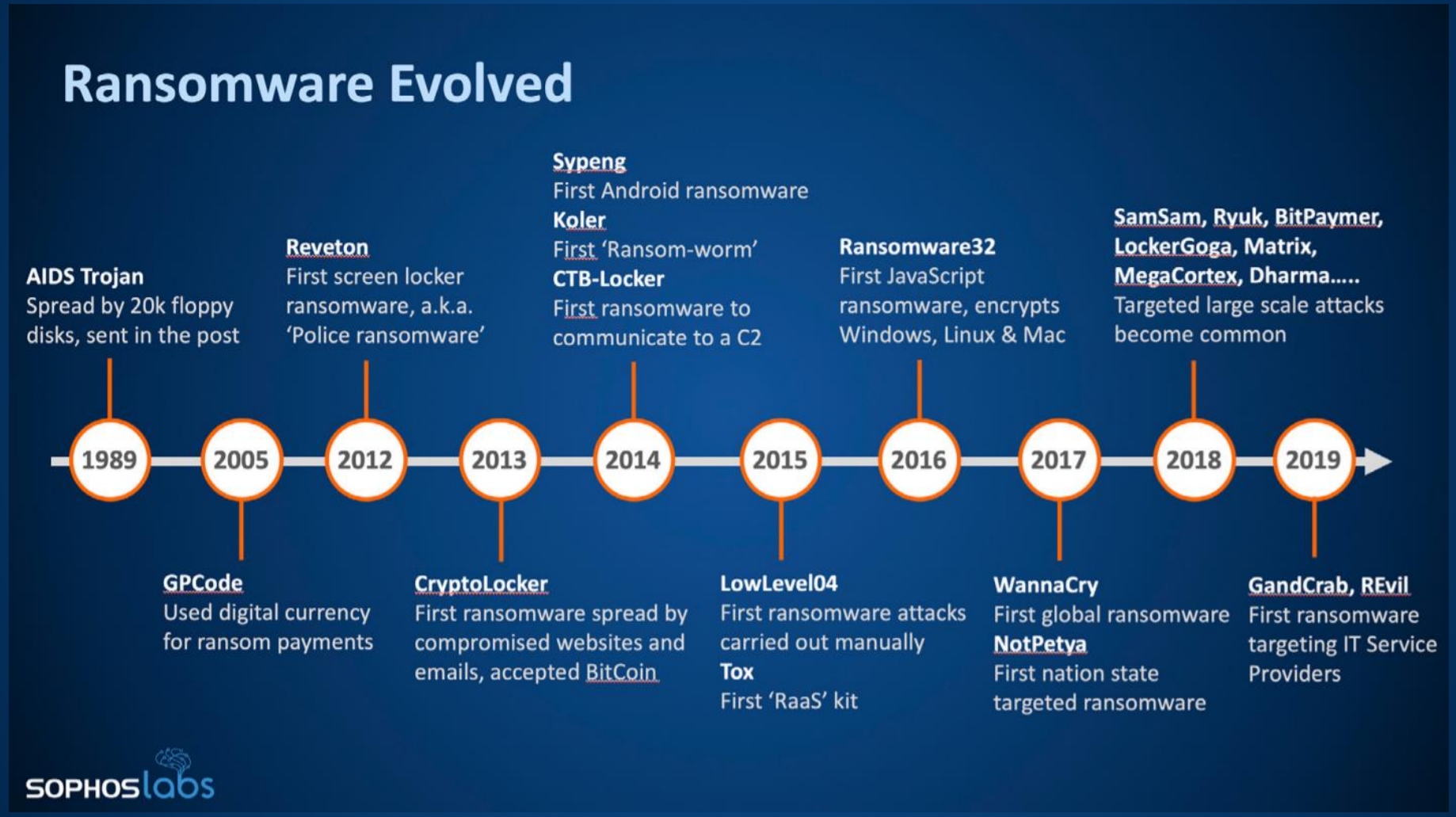
The Threat Report 2020 – Six Key Areas

1. Ransomware attackers raise the stakes
2. Mobile malware and Potentially Unwanted Apps edging towards malware
3. Cloud computing: misconfiguration is greatest security risk
4. Automated, active attacks to gain access and move laterally through a network
5. "Internet background radiation" affecting a wide range of internet-facing services and devices - RDP is at risk
6. Interest in corruption of machine learning detection models

1. Ransomware Attackers Raise the Stakes

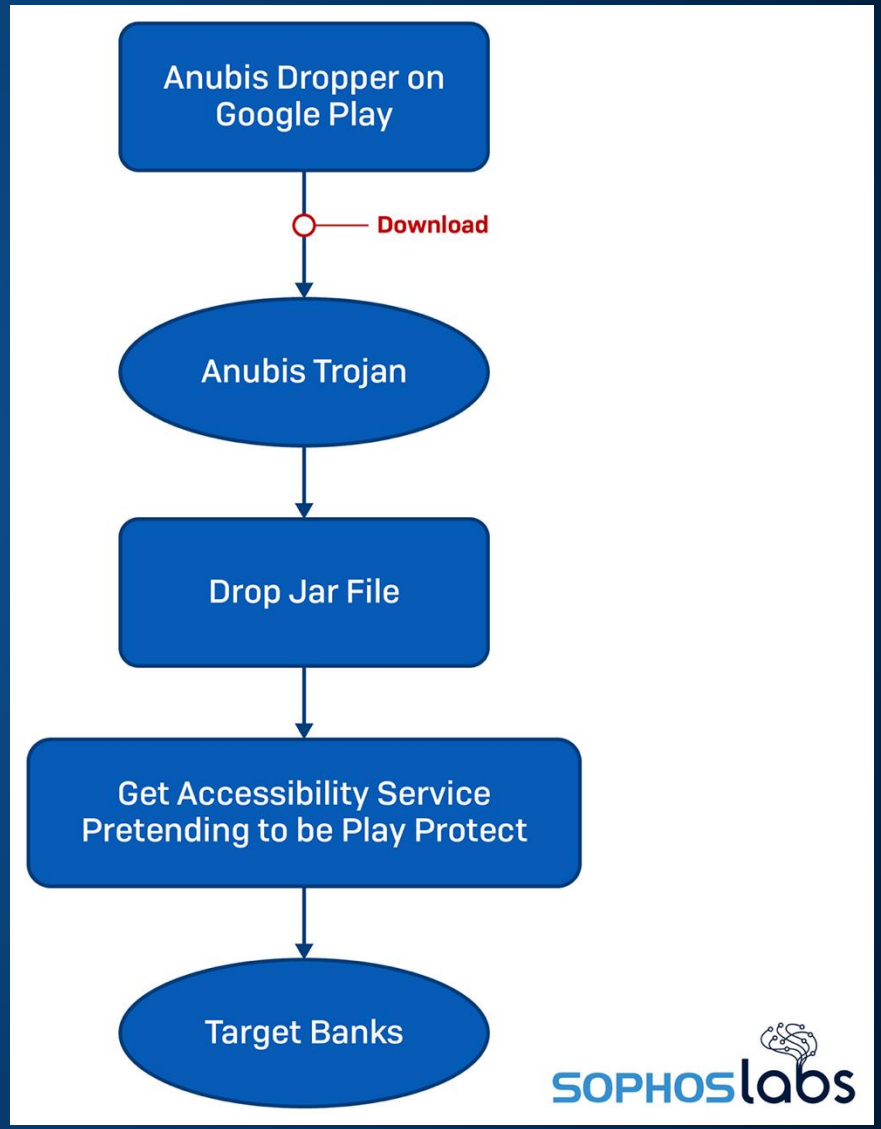
- Use victims’ legitimate management tools against them
- Attacker code appears "trusted" while attacker elevates privileges
- Living off the land, learning to harness or bypass security tools
- Efficiency and prioritization e.g. in terms of files encrypted, concurrent activities etc., give ransomware attackers an edge

Ransomware – Three Decades of Evolution



2. Mobile Security and Unwanted Apps

- ‘Fleeceware’: Trial version apps that vastly overcharge casual users who don’t follow complicated cancellation rules
- Hidden adware: Android apps that deliver advertising aggressively but hide to avoid uninstall
- Bank-credential stealers, e.g. Anubis, evade Play Store controls by retrieving malicious components after the user installs the app



Hidden Adware

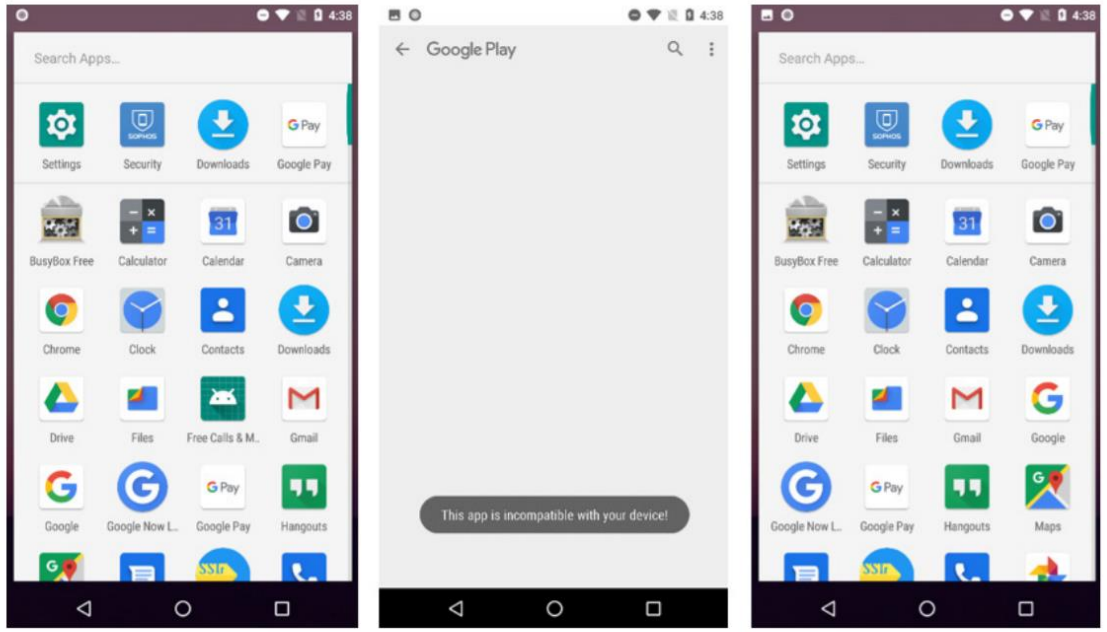


Figure 9: A Hiddad app hides its icon after the first time you launch it

"Hiddad" is a malware family, the primary aim of which is monetization through aggressive advertising. It survives by making itself hard to find on the device. The malware conceals itself in order to circumvent uninstallation attempts. The longer it remains on the device, the more ad revenue it can generate for its author.

3. Cloud Computing Misconfiguration

- The greatest vulnerability for cloud computing is misconfiguration by operators
- Combined with a general lack of visibility, this makes cloud computing environments a ready-made target for cyber attackers

How Cloud Breaches Happen….

A hypothetical cloud security breach incident

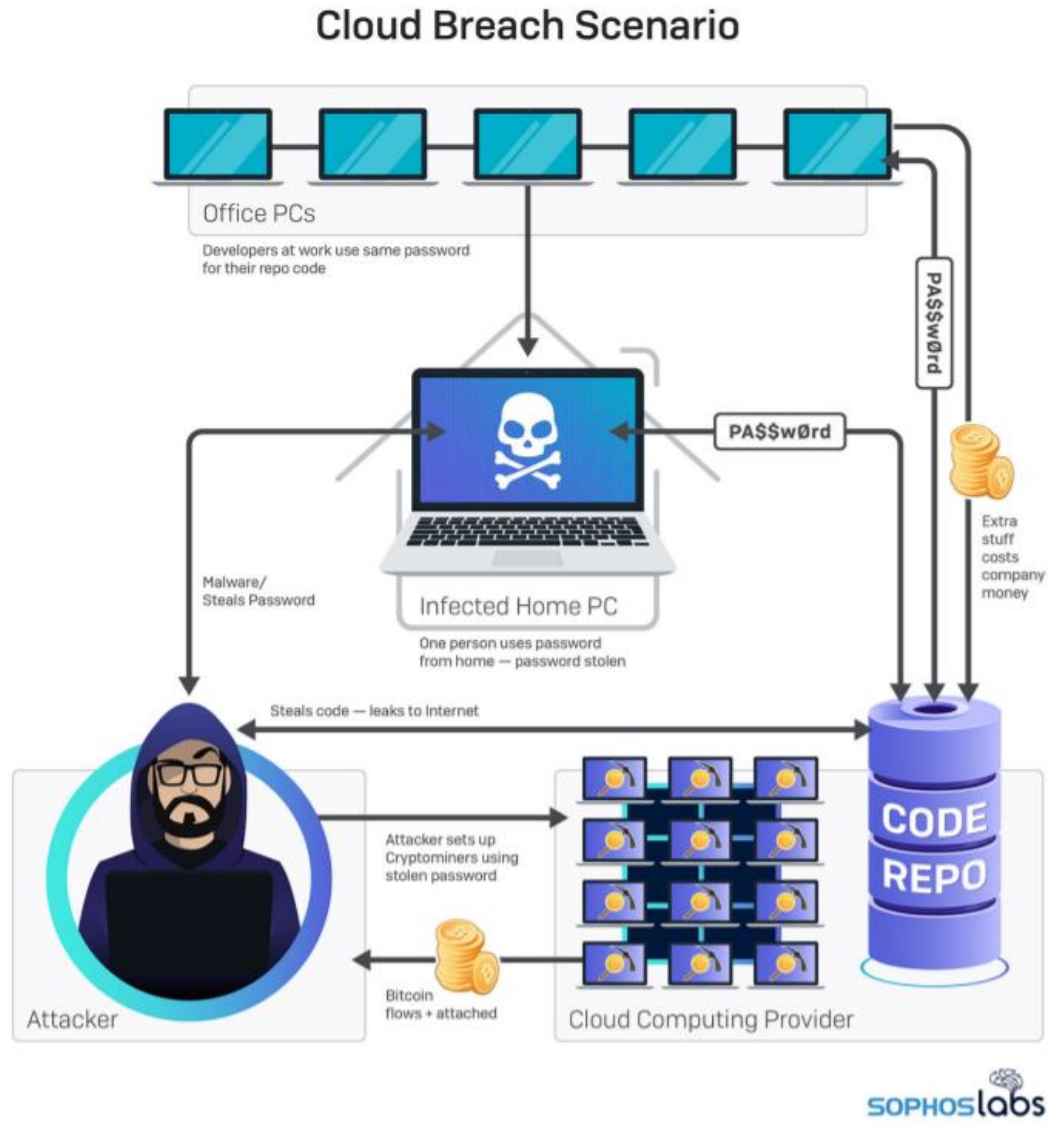


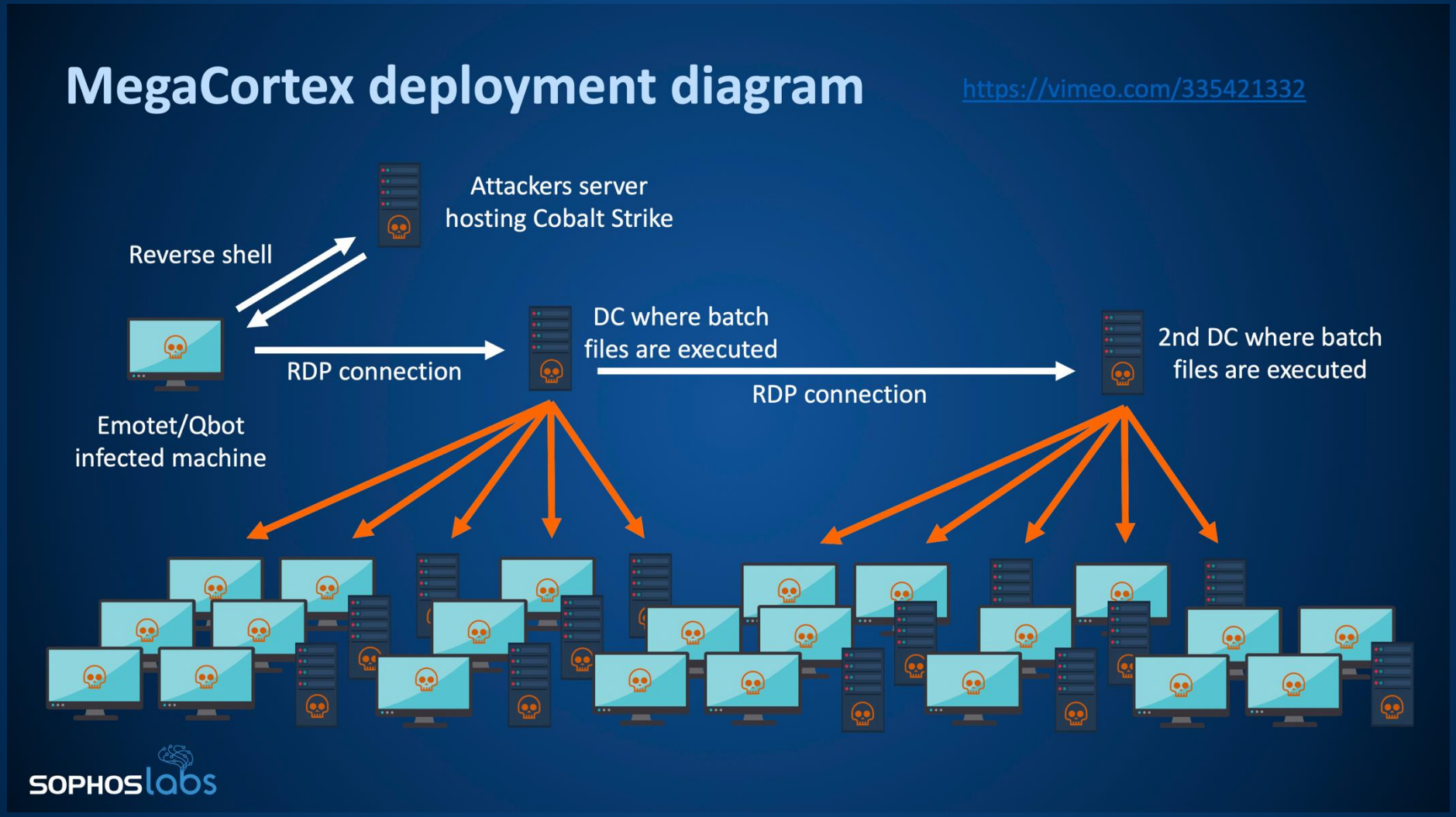
Figure 17: A hypothetical cloud security breach scenario

SOPHOS

4. Automated Active Attacks

- The blending of automated attacks – opportunistic, brute force, credential stuffing etc.
- With active, manual steering and decision making if victim appears interesting to attackers
- Attackers who use this method may be discovered, and stopped, by attentive members of the security team
- Many attackers spend days to weeks poking around in targeted networks laying the groundwork for a larger attack in the future

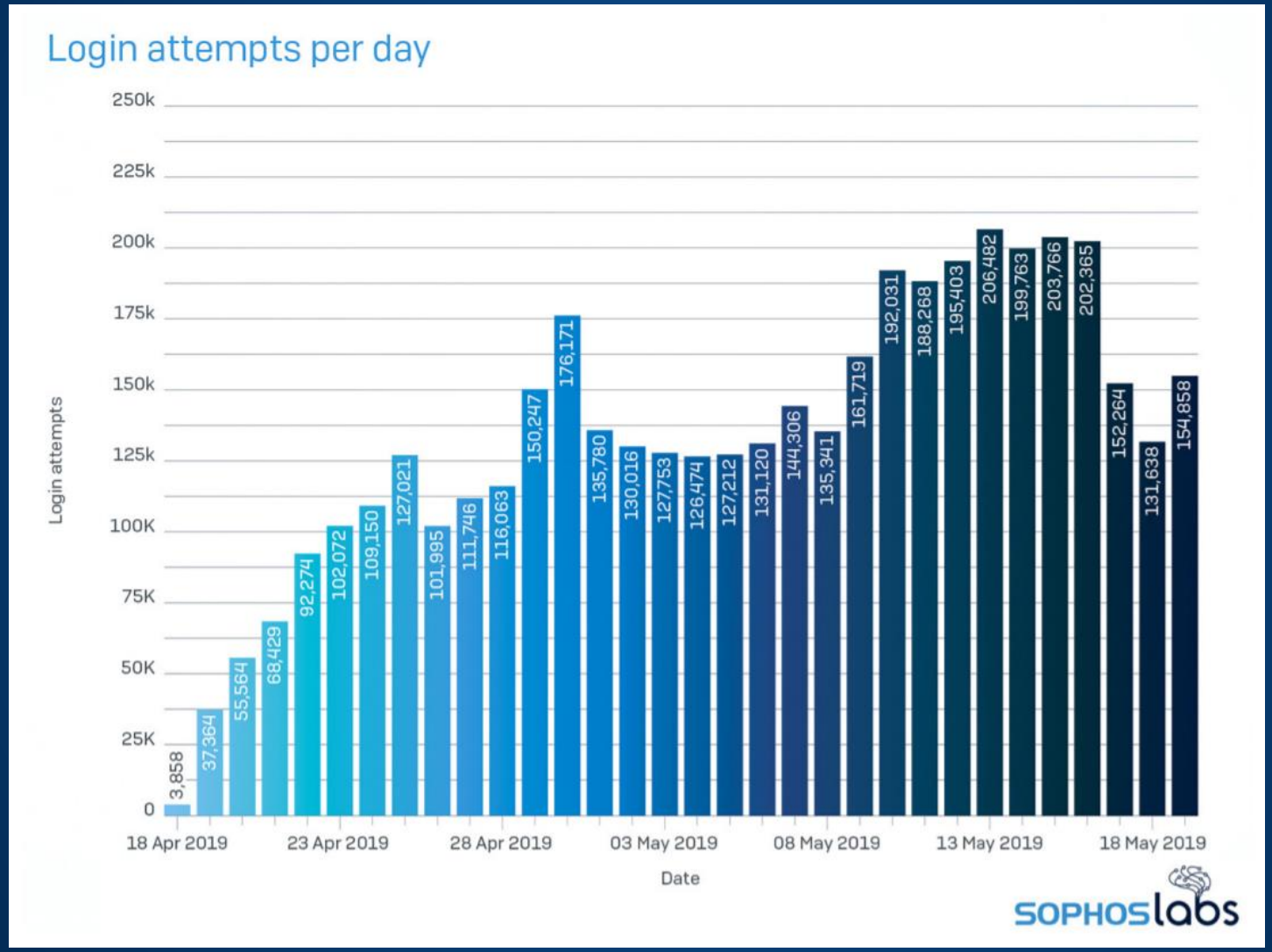
Automated Active Attacks - Ransomware



5. The Risk of Ignoring “Internet Background Radiation”

- Attacker scans for services and devices exposed to the public internet accounts for a growing number of breaches and compromises affecting a wide range of internet-facing services and devices
- Public-facing services are targeted by increasingly sophisticated automation
- RDP poses a “low hanging fruit” risk
- Attackers have been building automation targeting many different services, including various remote access tools and SQL database servers

‘Honeypot’ Research Into RDP Targeting

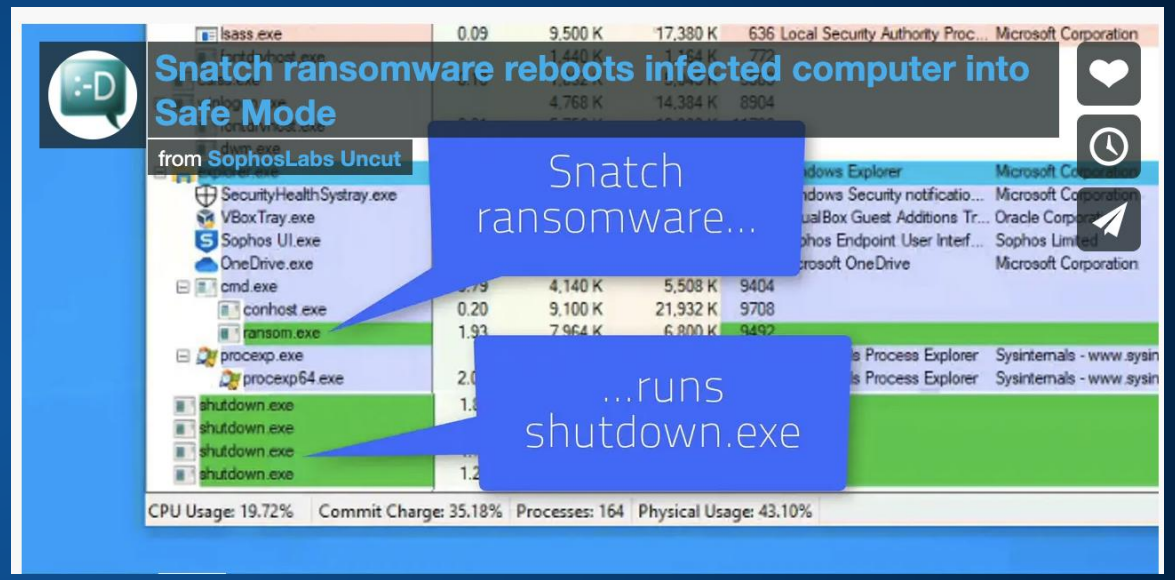


6. Machine Learning Draws Attacker Interest

- Machine learning is bringing huge benefits to detection of previously-unknown malware
- But that success has made machine learning a target
- Attackers are beginning to look at how they can corrupt machine learning detection models
- Research showed how machine learning detection models could possibly be tricked
- And how machine learning could be applied to offensive activity to generate highly convincing fake content for social engineering

The Cyberthreat Landscape Continues to Evolve…

- **Dec. 10 – Snatch ransomware reboots PCs into Safe Mode to bypass protection**
- Uncovered by Sophos MTR team and SophosLabs researchers
- An automated active attack
- Targets vulnerable remote services (like RDP)
- Exfiltrates data before launching ransomware
- Reboots in Safe Mode where anti-ransomware behavioural detection technologies don’t work



https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/

Advice for Defenders

- Prevention and protection
- Threat hunting – managed and professional
- Multi-layered, synchronized security
- Access and authentication
- Patching
- Employee education and awareness
- The four practices to adopt right now!

Where to find the Threat Report 2020

- https://www.Sophos.com/threatreport2020
- https://nakedsecurity.sophos.com/2019/11/19/sophos-2020-threat-report/
- https://news.sophos.com/en-us/2019/11/05/sophoslabs-surveys-the-threat-landscape-for-2020-trends/

Sophos History

Evolution to complete security

1985
Founded in Abingdon (Oxford), UK


Peter Lammer c1985


Jan Hruska c1985

1988
First checksum-based antivirus software

1989
First signature-based antivirus software

1996
Voted best small/medium sized company in UK

US presence established in Boston

2007
Acquired ENDFORCE

2008
Acquired Utimaco Safeware AG

2011
Acquired Astaro

2012
Acquired DIALOGS

2013
Divested non-core Cyber business

2014
Acquired Cyberoam

Acquired Mojave Networks

2015
Acquired Reflexion

Launched Synchronized Security

IPO London Stock Exchange

Acquired Surfright

2016
Acquired PhishThreat

Acquired Barricade

2017
Acquired Invincea

2019
Acquired Rook Security

Acquired Avid Secure

Acquired DarkBytes

Sophos Synchronized Security

Security Heartbeat™

Next-Gen Firewall

Wireless

Web

Email

PhishThreat

Next-Gen Endpoint

Mobile

Server

Encryption

Sophos Central

Cloud Optix