RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **SEM-M03D**

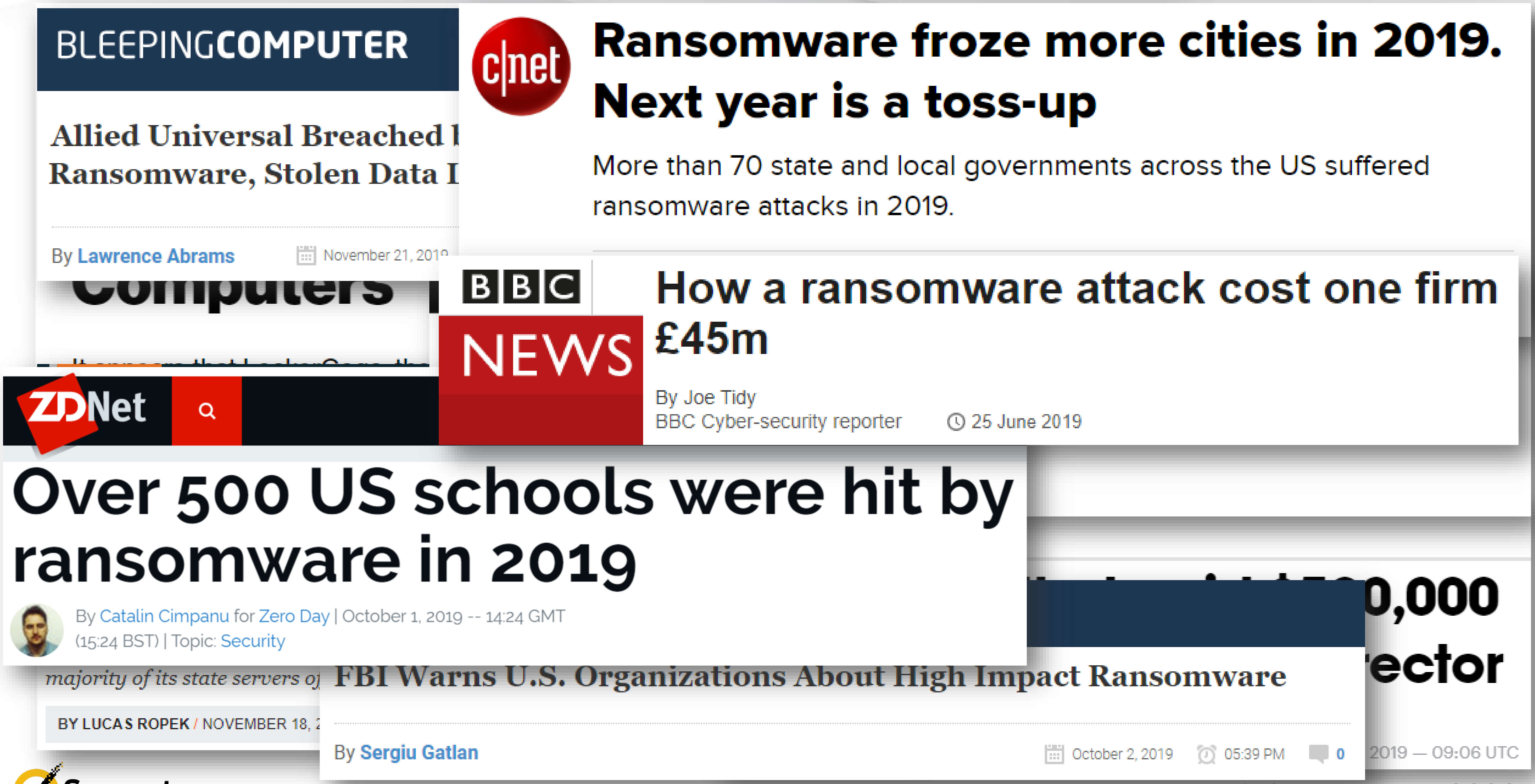
Targeted Ransomware: A Potent Threat Begins to Proliferate

Dick O‘Brien

Principal Editor
Symantec (a Division of Broadcom)
@dickobrien

Jon DiMaggio

Sr. Threat Intelligence Analyst
Symantec (a Division of Broadcom)
@cyber_dimaggio



BLEEPINGCOMPUTER

Allied Universal Breached b
Ransomware, Stolen Data I

By Lawrence Abrams   November 21, 2019

Computers

It appears that LockerGoga the

c|net

Ransomware froze more cities in 2019. Next year is a toss-up

More than 70 state and local governments across the US suffered ransomware attacks in 2019.

BBC NEWS

How a ransomware attack cost one firm £45m

By Joe Tidy
BBC Cyber-security reporter   25 June 2019

ZDNet

Over 500 US schools were hit by ransomware in 2019

By Catalin Campanu for Zero Day | October 1, 2019 -- 14:24 GMT (15:24 BST) | Topic: Security

majority of its state servers of

BY LUCAS ROPEK / NOVEMBER 18, 2

0,000
ector

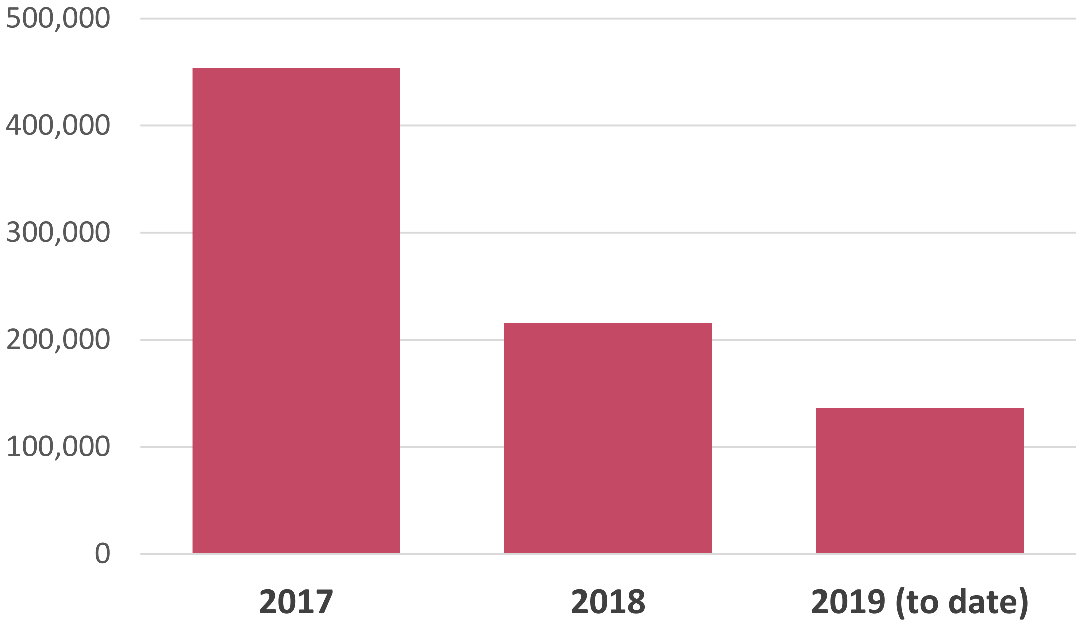
2019 — 09:06 UTC

FBI Warns U.S. Organizations About High Impact Ransomware

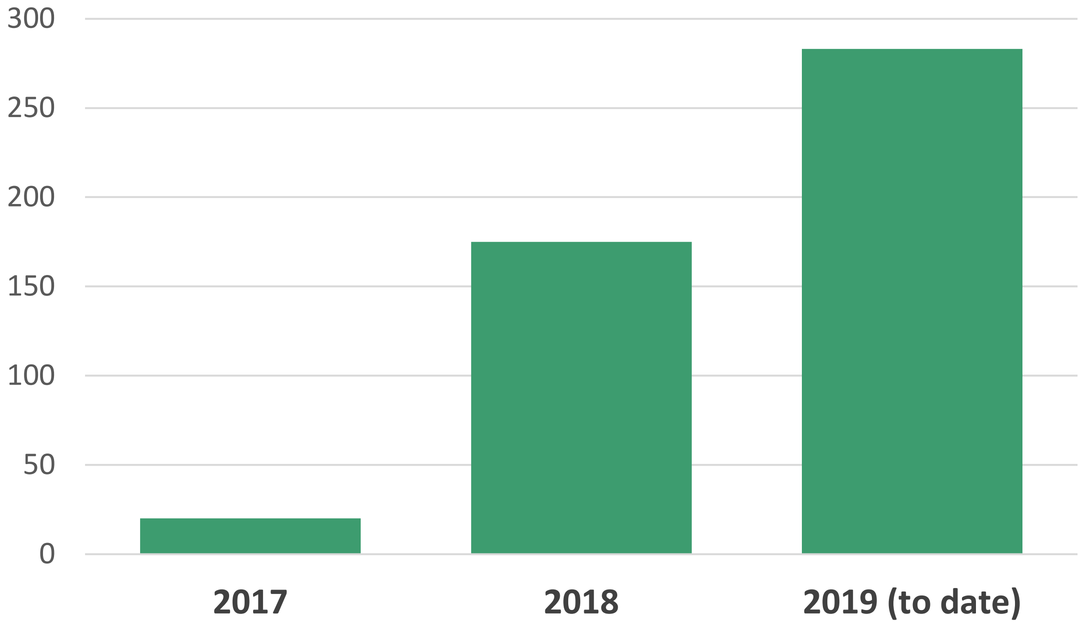
By Sergiu Gatlan   October 2, 2019   05:39 PM   0

Evolution of Ransomware

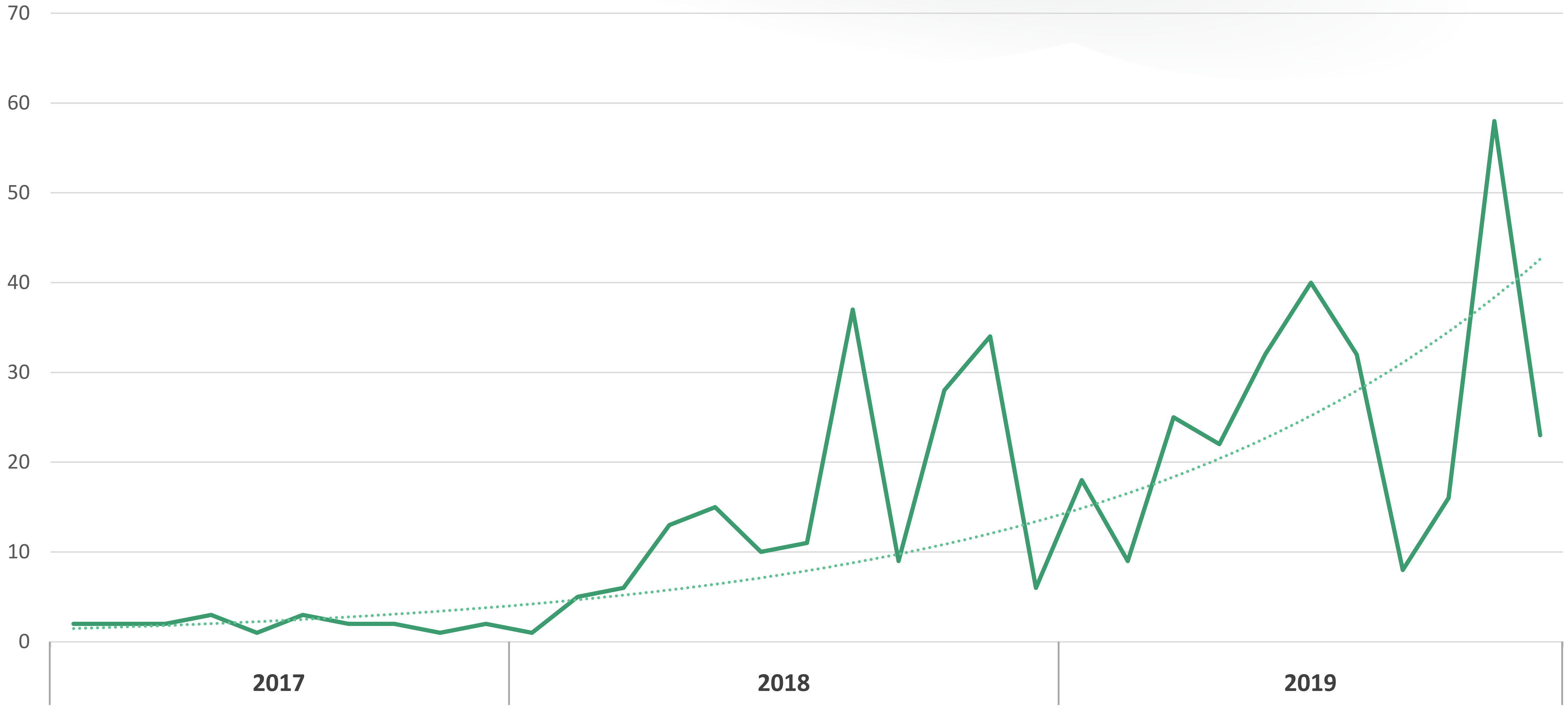
37% drop
on ransomware attacks: 2019



62% increase
in targeted ransomware attacks



Surge in targeted attacks



Why the shift?

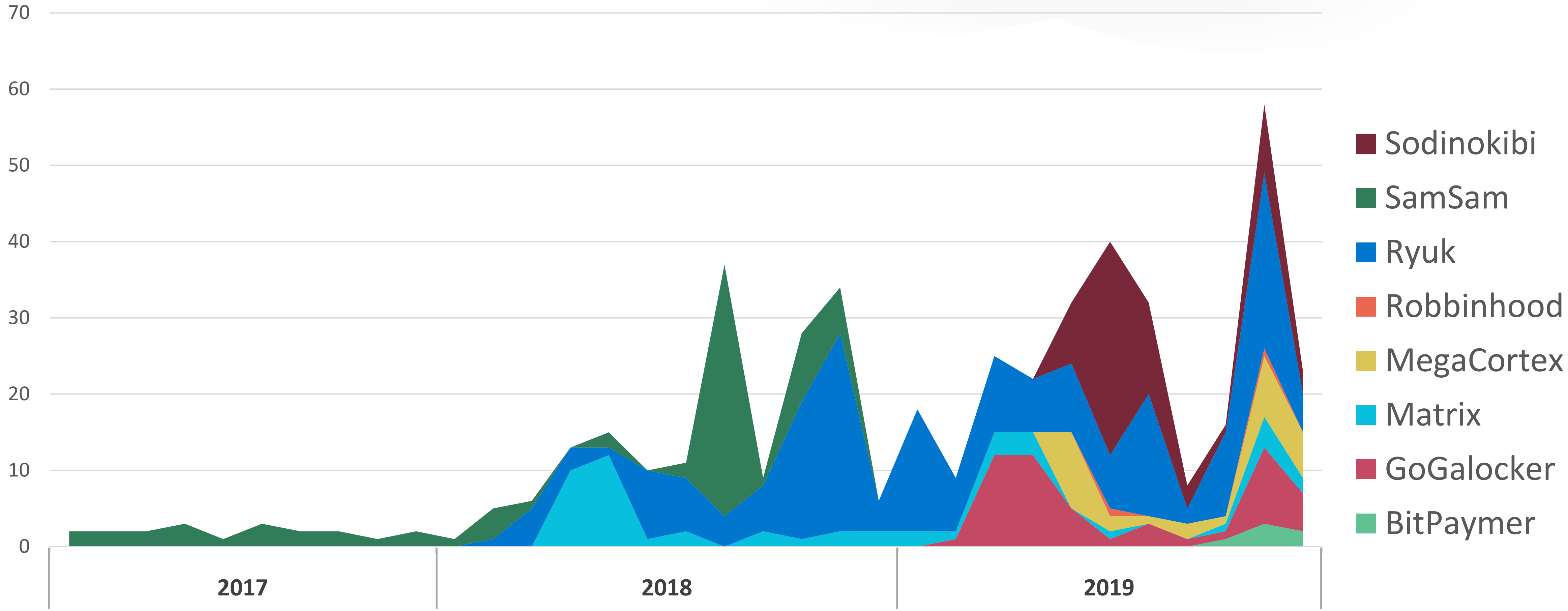
Consumers:

- Less PCs, more mobile devices
- Critical data backed up in the cloud
- Less email, more chat

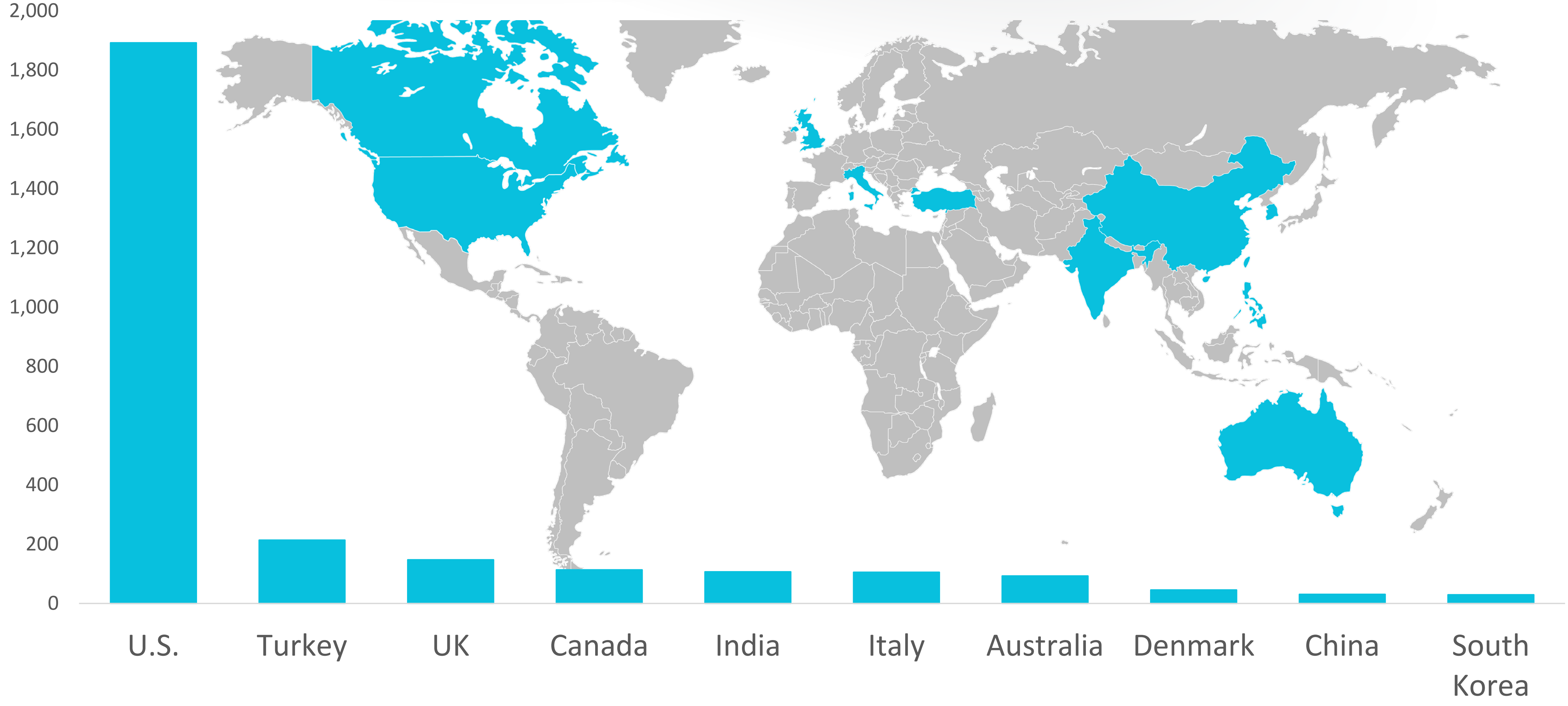
Enterprise:

- Higher payouts on offer
- Paying can be a business decision
- Cyber insurance might cover losses

Breakdown of attacks



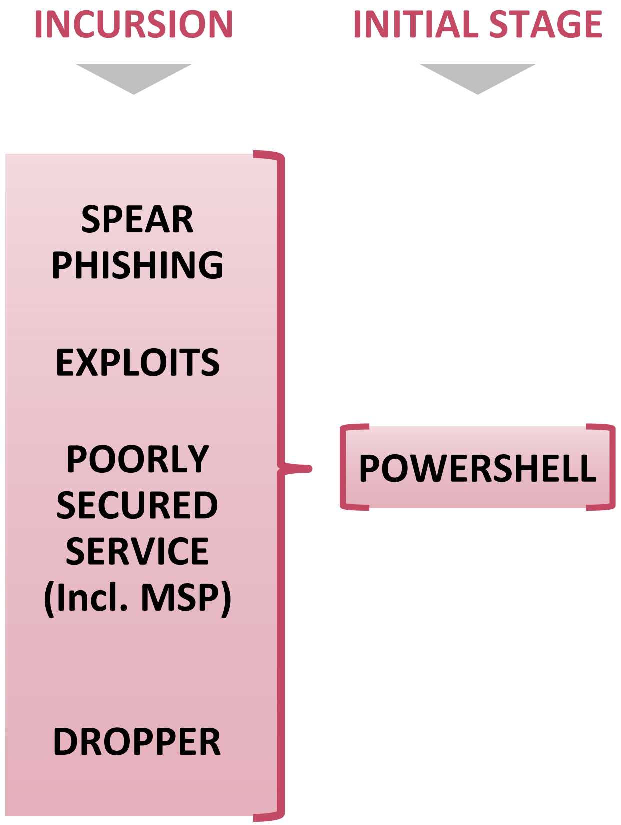
Where are the victims?



RSAConference2020

GogaLocker:
New bred of threat

GogaLocker a Targeted Ransomware Case Study



INCURSION

INITIAL STAGE

SPEAR PHISHING

EXPLOITS

POORLY SECURED SERVICE (Incl. MSP)

DROPPER

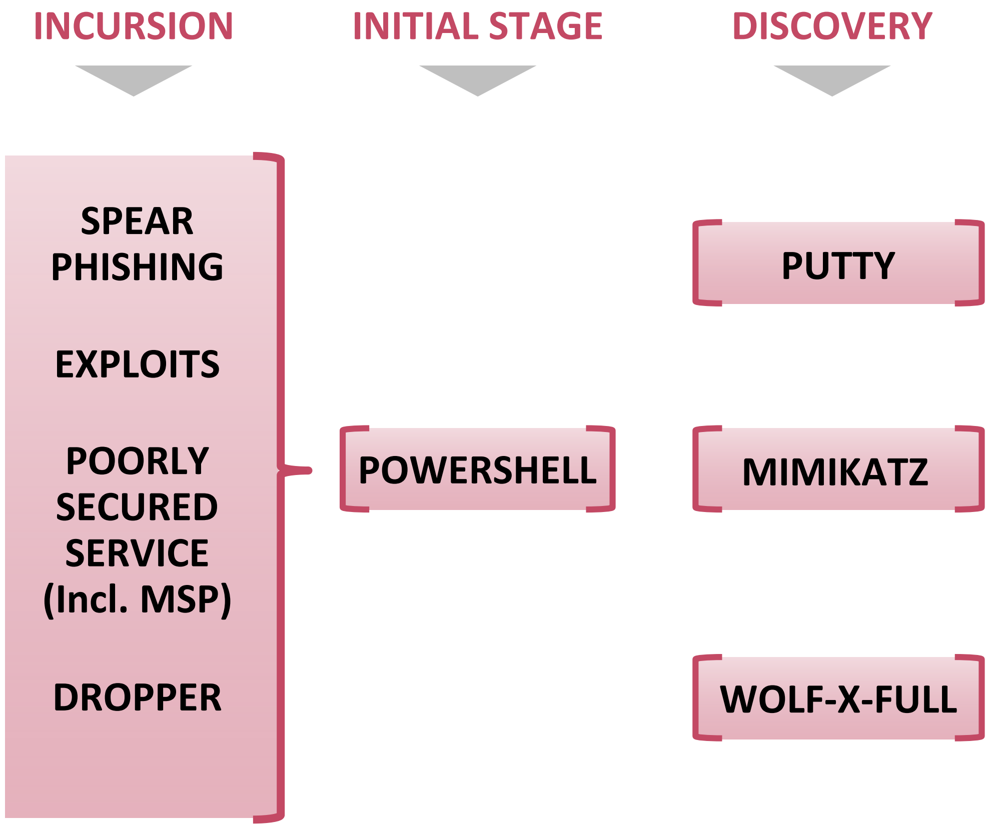
POWERSHELL

Simple PowerShell commands used:

- powershell -nop -w hidden -encodedcommand JABzAD#####
- CompileAssemblyFromSource → fileless payload in memory
- Using Cobalt Strike Beacon's Reflective Loader backdoor

→ Using known tools for fileless payload

GogaLocker Ransomware – Step Two



INCURSION

INITIAL STAGE

DISCOVERY

SPEAR PHISHING

EXPLOITS

POORLY SECURED SERVICE (Incl. MSP)

DROPPER

POWERSHELL

PUTTY

MIMIKATZ

WOLF-X-FULL

Get credentials/passwords

- Mimikatz in all variations
- others use password guessing → account lockouts
- or alternatives like Int-Monologue or Kerberoasting
- Bloodhound Active Directory enumeration

The goal is AD/DA password
→ distribute malware & disable security for all devices

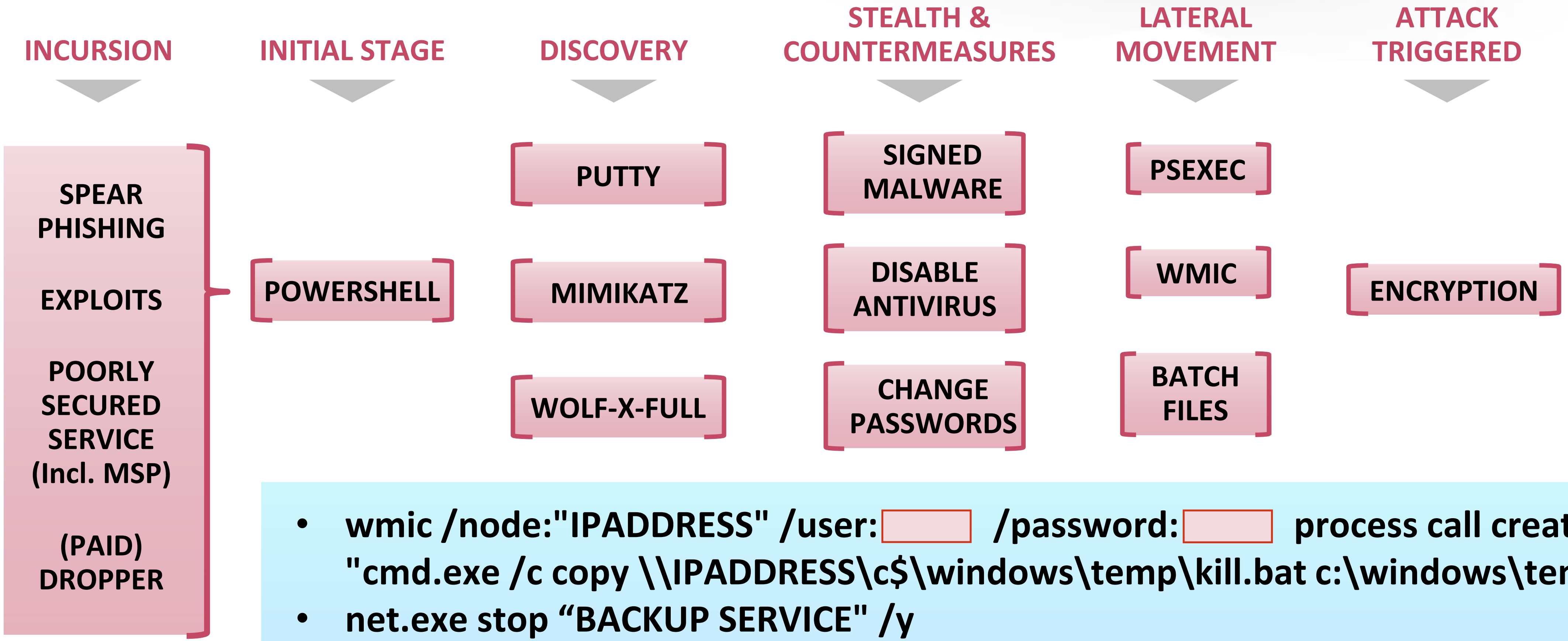
The Human Element

The attackers learn about your environment…

… and then adapt to it on the fly.

They know how to disrupt your organization the most!

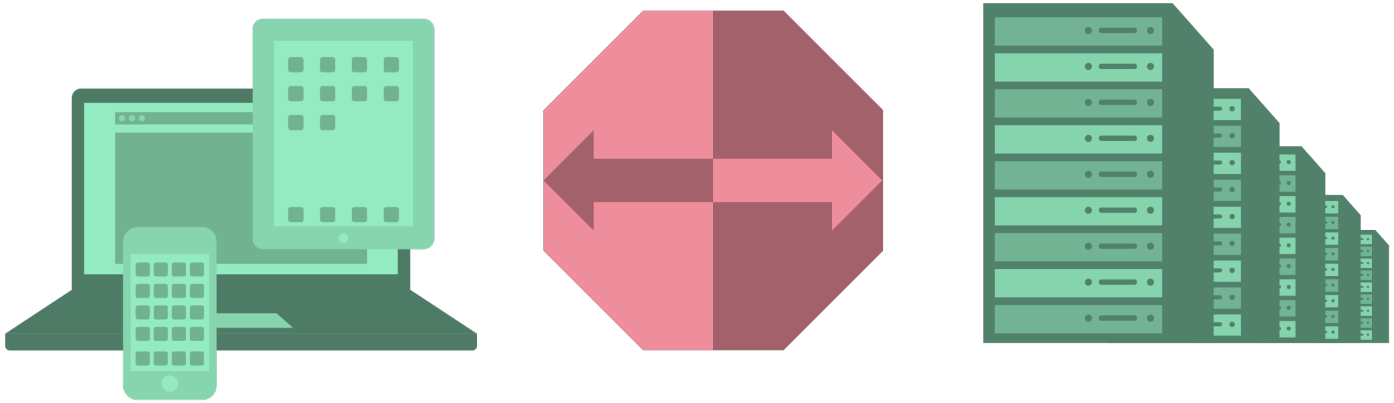
GogaLocker Ransomware – Final Step



```
• wmic /node:"IPADDRESS" /user:[redacted] /password:[redacted] process call create
  "cmd.exe /c copy \\IPADDRESS\c$\windows\temp\kill.bat c:\windows\temp\“
• net.exe stop “BACKUP SERVICE" /y
• net.exe user [redacted]
• logoff.exe <num>
```

Conclusion

- Targeted ransomware against organizations is increasing
- Weak authentication practices foster lateral movement
- Attackers might steal data and delete all your backups



Be prepared

You should already:

- Back up your data (and check your restore capability)
- Keep your operating system and software up to date

In the near future you should:

- Be prepared for ransomware – conduct a drill
- Check your email protection
- Follow best practices & monitor dual-use tools

RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **SEM-M03D**

Thank you for your attention !

Dick O‘Brien

Principal Editor
Symantec (a Division of Broadcom)
@dickobrien

Jon DiMaggio

Sr. Threat Intelligence Analyst
Symantec (a Division of Broadcom)
@Cyber_DiMaggio

#RSAC