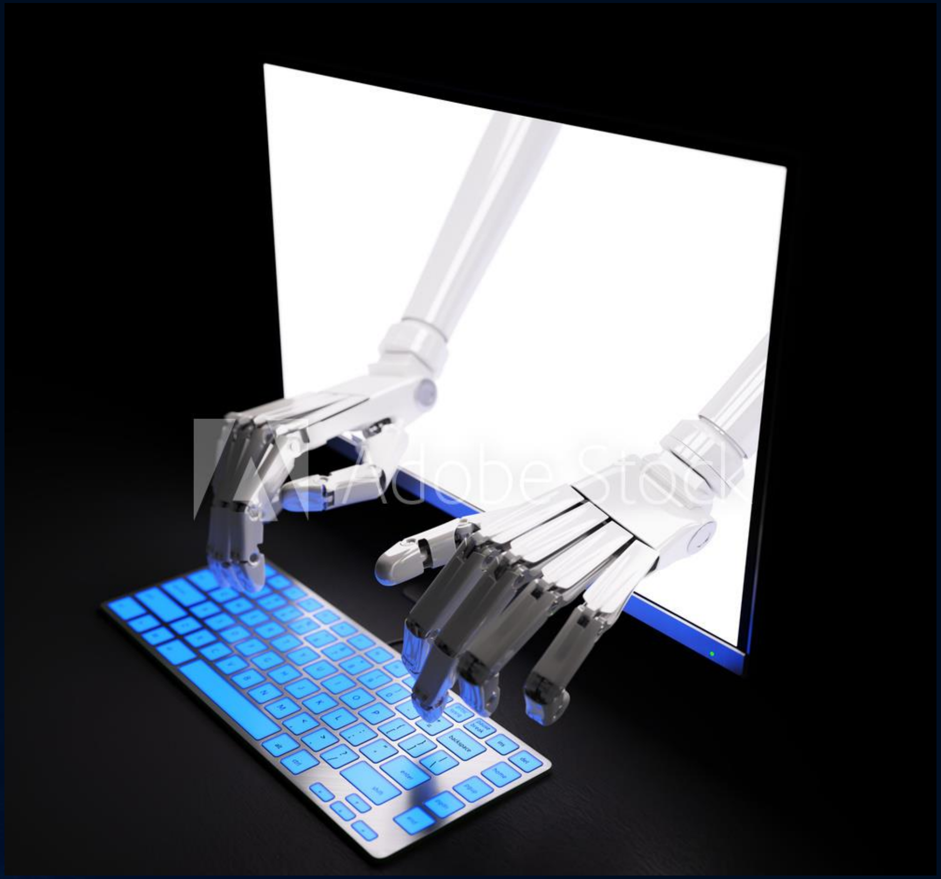
R.A.T s
We’ve Been
HACKED !!

REMOTE ACCESS THREATS –

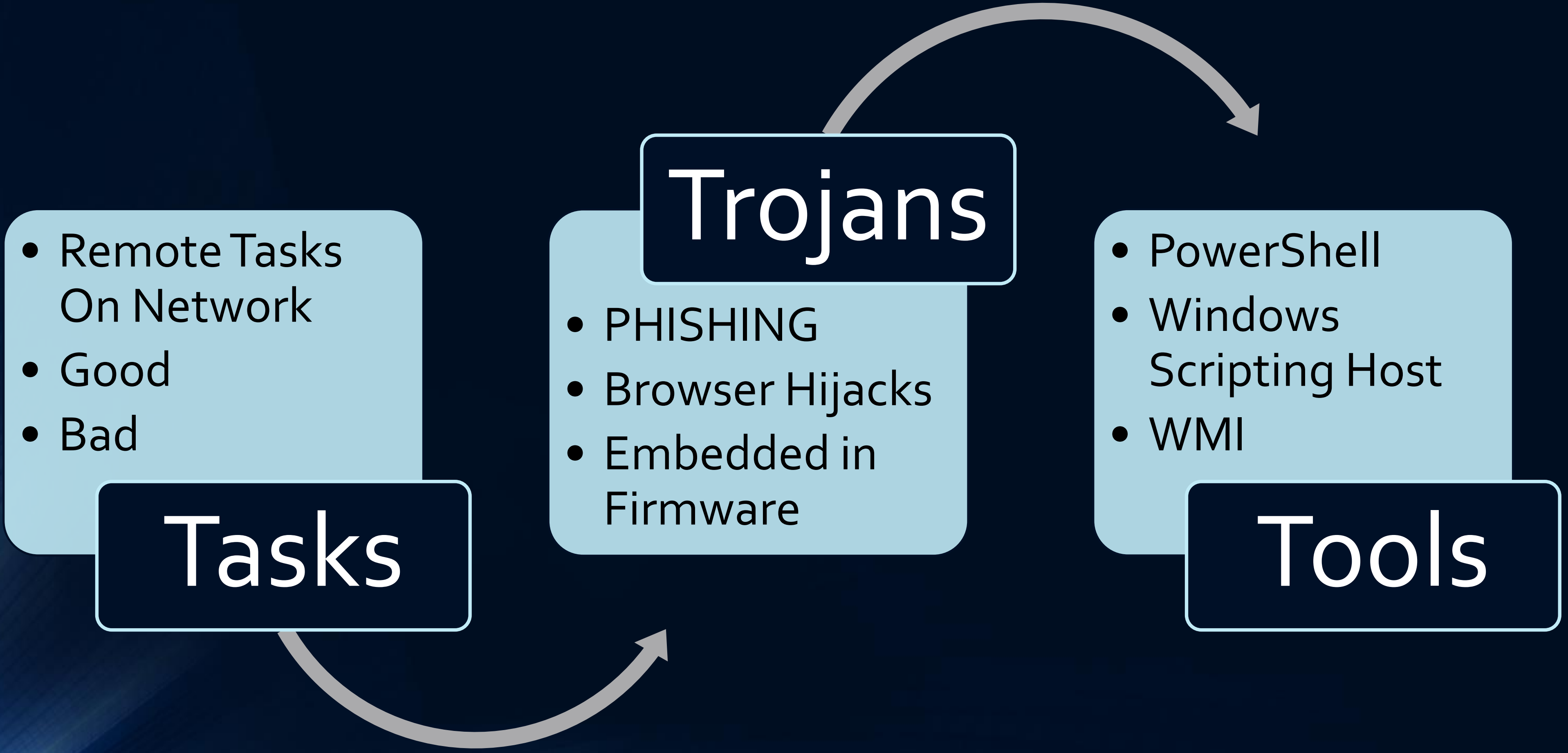
YOU NEED TO BE AWARE

Remote Access Threats (R.A.T s)

- Remote Access Trojans
- Remote Access Tasks
- Remote Access Trojans



Orginally RATs really made networks better and employees more productive



Tasks

- Remote Tasks On Network
- Good
- Bad

Trojans

- PHISHING
- Browser Hijacks
- Embedded in Firmware

Tools

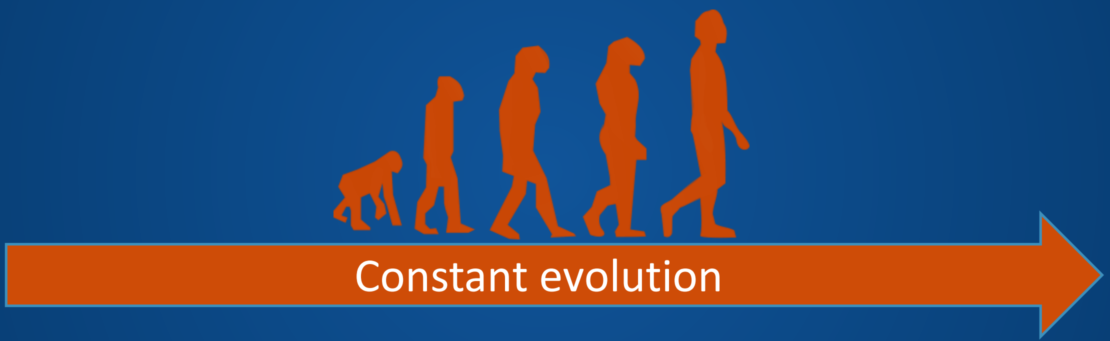
- PowerShell
- Windows Scripting Host
- WMI

And Then Hackers Weaponized Them

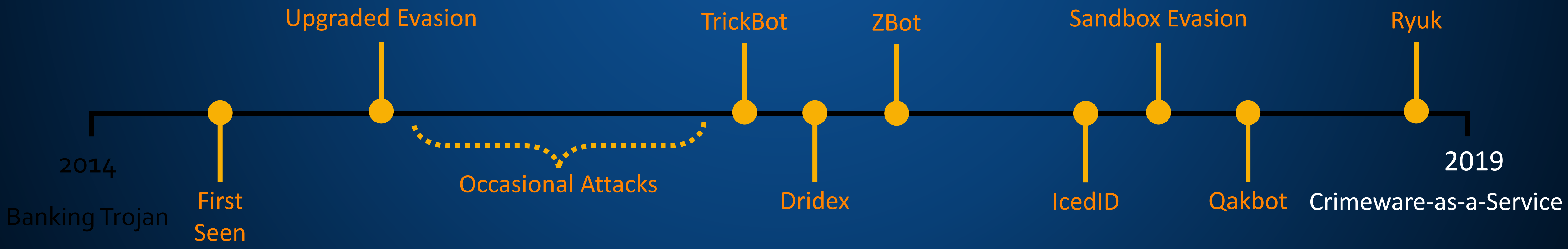
Let's Take A Look At One Of Them

EMOTET

> “Amongst the most costly and destructive threats to U.S. businesses right now”
>
> *U.S. Department for Homeland Security, 2018*



Constant evolution



2014

Banking Trojan

First Seen

Upgraded Evasion

Occasional Attacks

TrickBot

Dridex

ZBot

IcedID

Sandbox Evasion

Qakbot

Ryuk

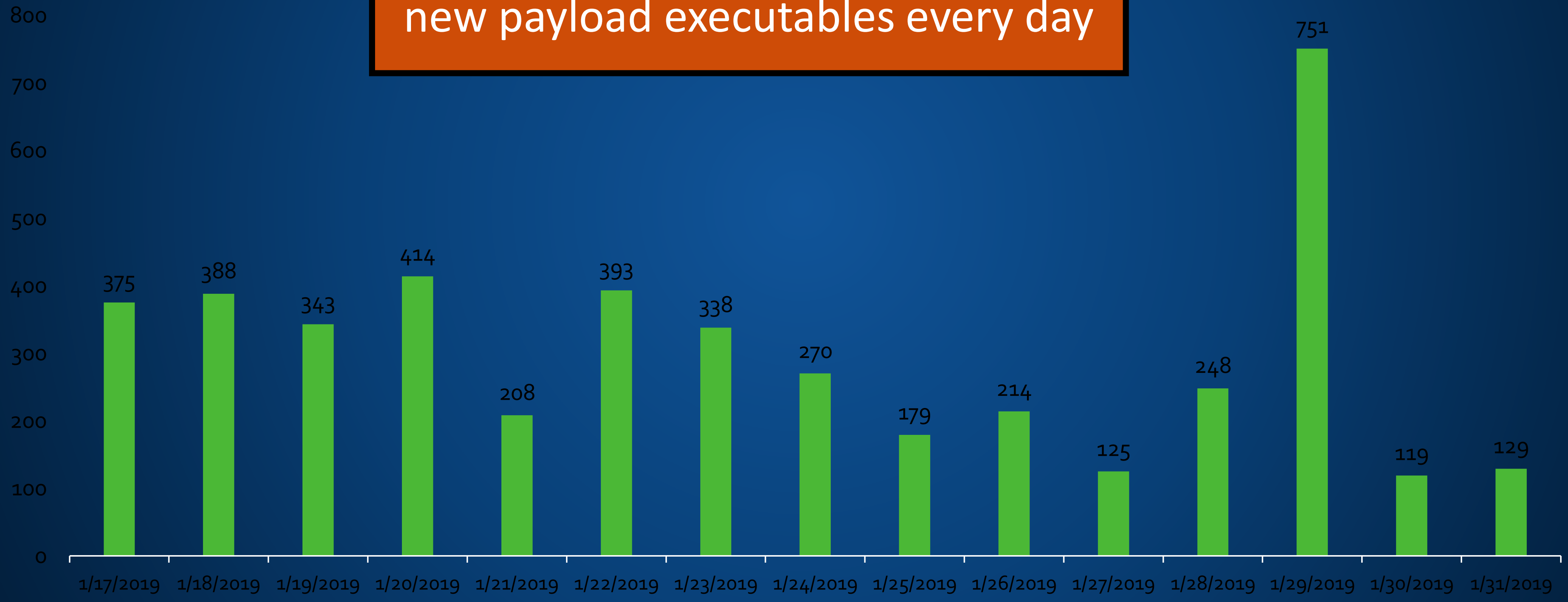
2019

Crimeware-as-a-Service

Emotet payloads change constantly

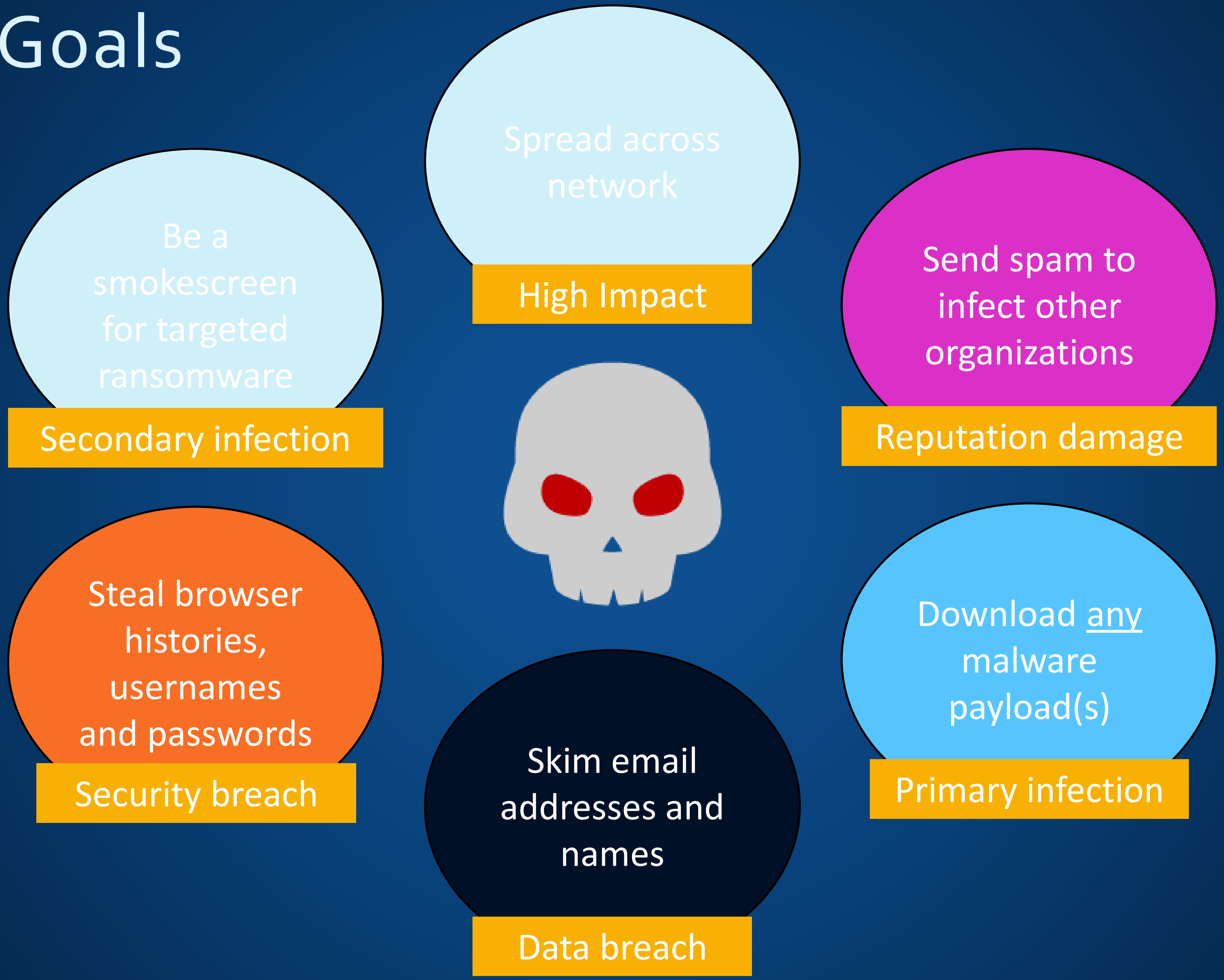
300

new payload executables every day



# of unique Emotet payload executables seen by SophosLabs

Emotet’s Goals



Spread across network

High Impact

Be a smokescreen for targeted ransomware

Secondary infection

Send spam to infect other organizations

Reputation damage

Steal browser histories, usernames and passwords

Security breach

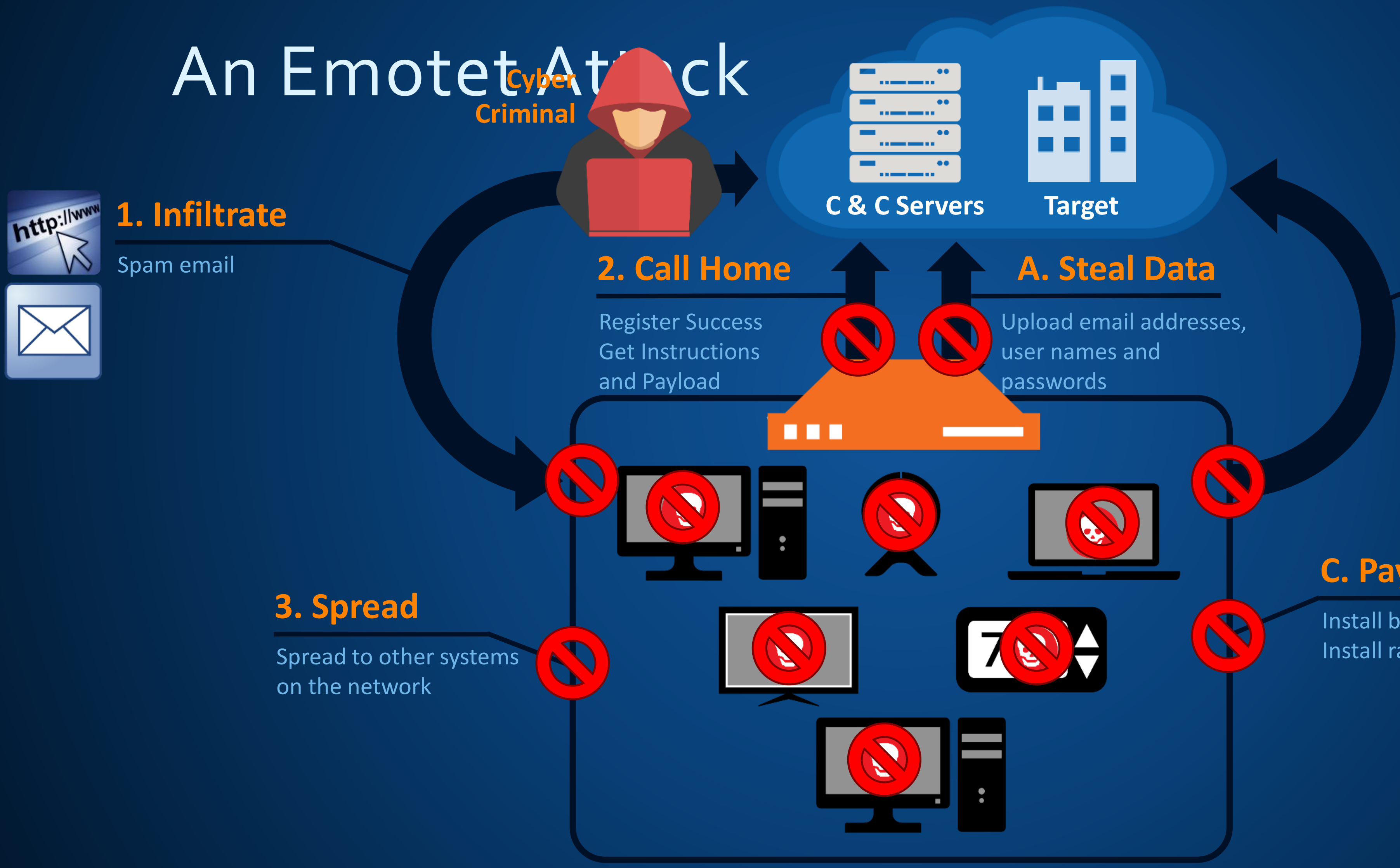
Download <u>any</u> malware payload(s)

Primary infection

Skim email addresses and names

Data breach

An Emotet Attack



1. Infiltrate

Spam email

2. Call Home

Register Success
Get Instructions
and Payload

3. Spread

Spread to other systems
on the network

A. Steal Data

Upload email addresses,
user names and
passwords

B. Bot Attack

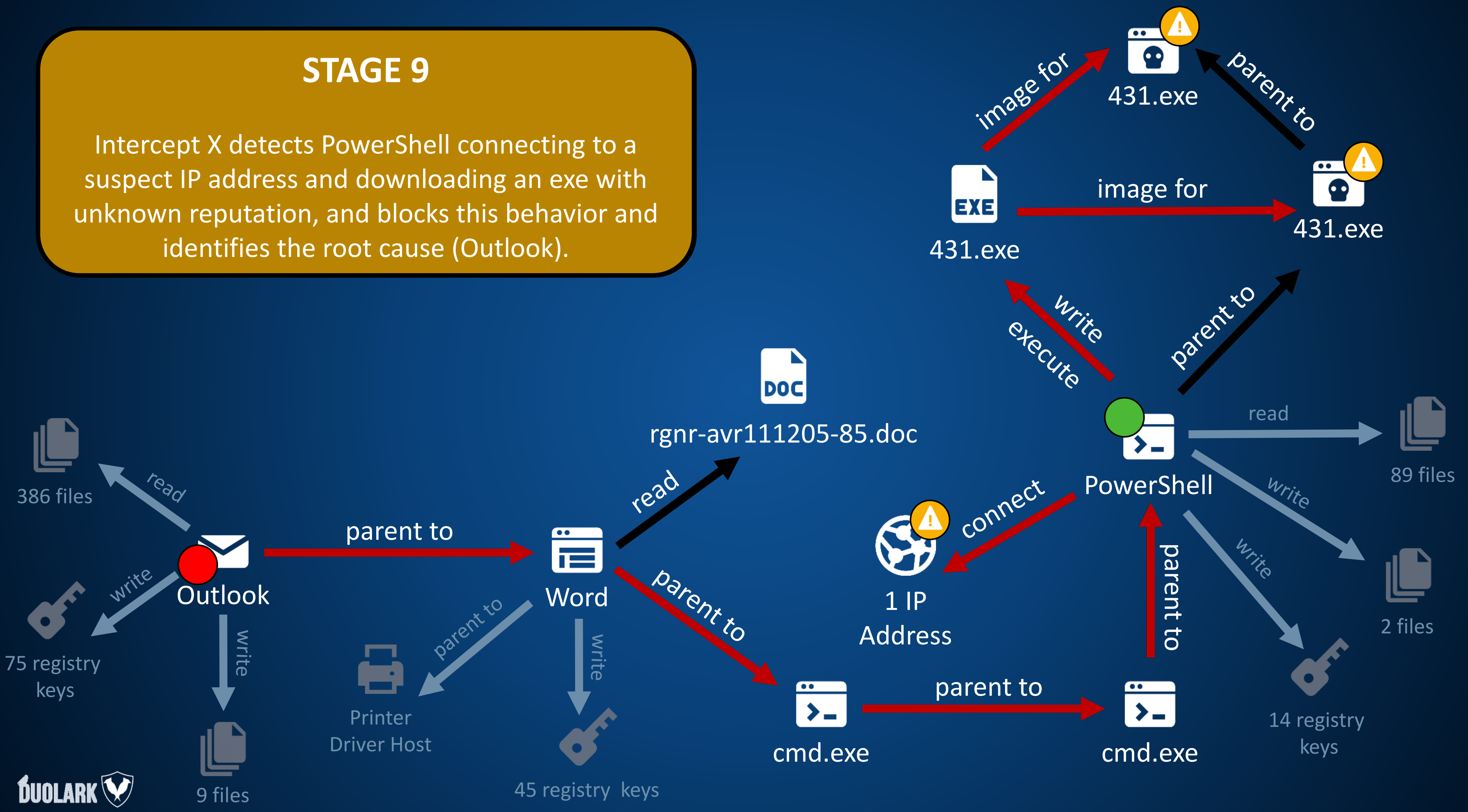
Send spam
to infect other orgs

C. Payload

Install banking Trojan
Install ransomware

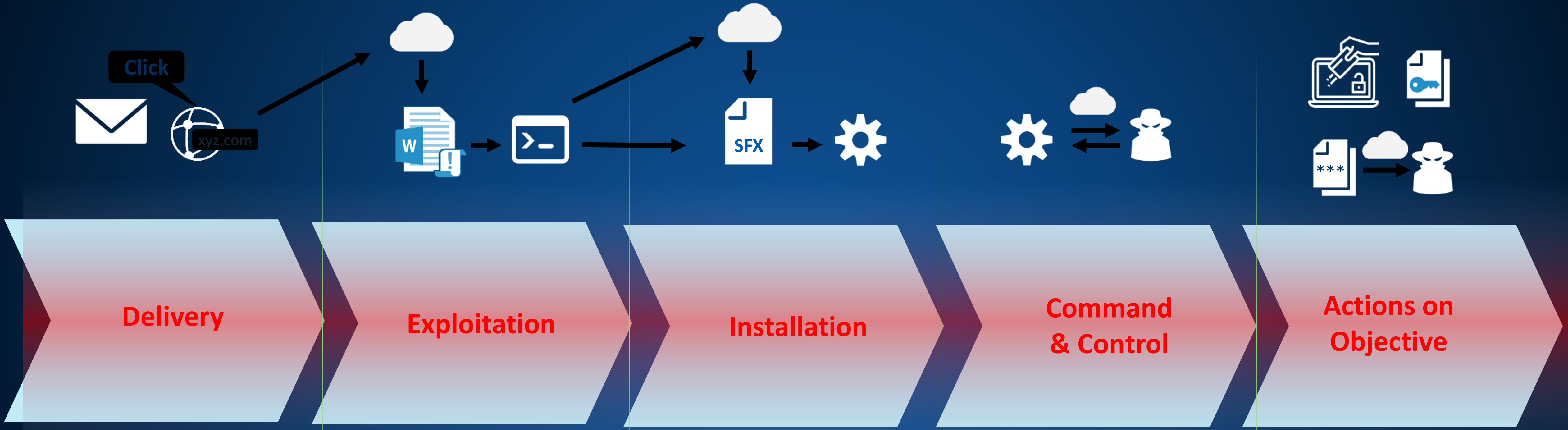
STAGE 9

Intercept X detects PowerShell connecting to a suspect IP address and downloading an exe with unknown reputation, and blocks this behavior and identifies the root cause (Outlook).



DUOLARK

Emotet Attack Chain



WEB PROTECTION

ANTI –EXPLOIT (CODE/MEMORY/APC) MITIGATIONS

APPLICATION LOCKDOWN

LOCAL PRIVILEGE MITIGATION

APPLICATION CONTROL

DEEP LEARNING

HIPS

MALICIOUS TRAFFIC DETECTION

ANTI-RANSOMWARE

CREDENTIAL THEFT PROTECTION

RUNTIME HIPS

THREAT CASE (RCA) & EDR

DUOLARK

3 Best Practices for Everyone to Follow

Secure ALL of your machines

Patch early.

Patch often.

Block PowerShell by default

What Is The HACKER ACTOR AFTER

Valuable Data Targets

- Personally Identifiable Information (PII)
- Personal Health Information (PHI)
- Trade Secrets
- Business Contacts
- Credit Card Information
- Social Security Numbers
- Bank Account Information
- Medical History – for ransom, bribes, etc

YOU CAN CHANGE ACCOUNT NUMBERS

YOU CANNOT CHANGE YOUR MEDICAL HISTORY

We All Need To Become…

HUMAN FIREWALLS

SIMPLE Things We Can Do To Ensure Security

The Business Network

#1 - Keep Patches Updated

#2 - Users Should Never Have ADMIN Rights

#3 – Disable PowerShell, WMS, and Windows Scripting

#4 – Introduce Long Password Phrases

#5 – Reduce complex passwords

EACH INDIVIDUAL

#1 – Use Two Factor Authentication

#2 – Mouse Over First, Click Last

#3 – Participate In Security Awareness Training

#4 – Use Common Sense

#5 – Report Suspicious Activity

LEADERSHIP

#1 – Employ Depth Of Defense Strategy

#2 – Business Continuity Plan

#3 – Ensure Business Associates Use Two Factor Authentication

#4 – Employ the Boy Scout Motto:

BE PREPARED

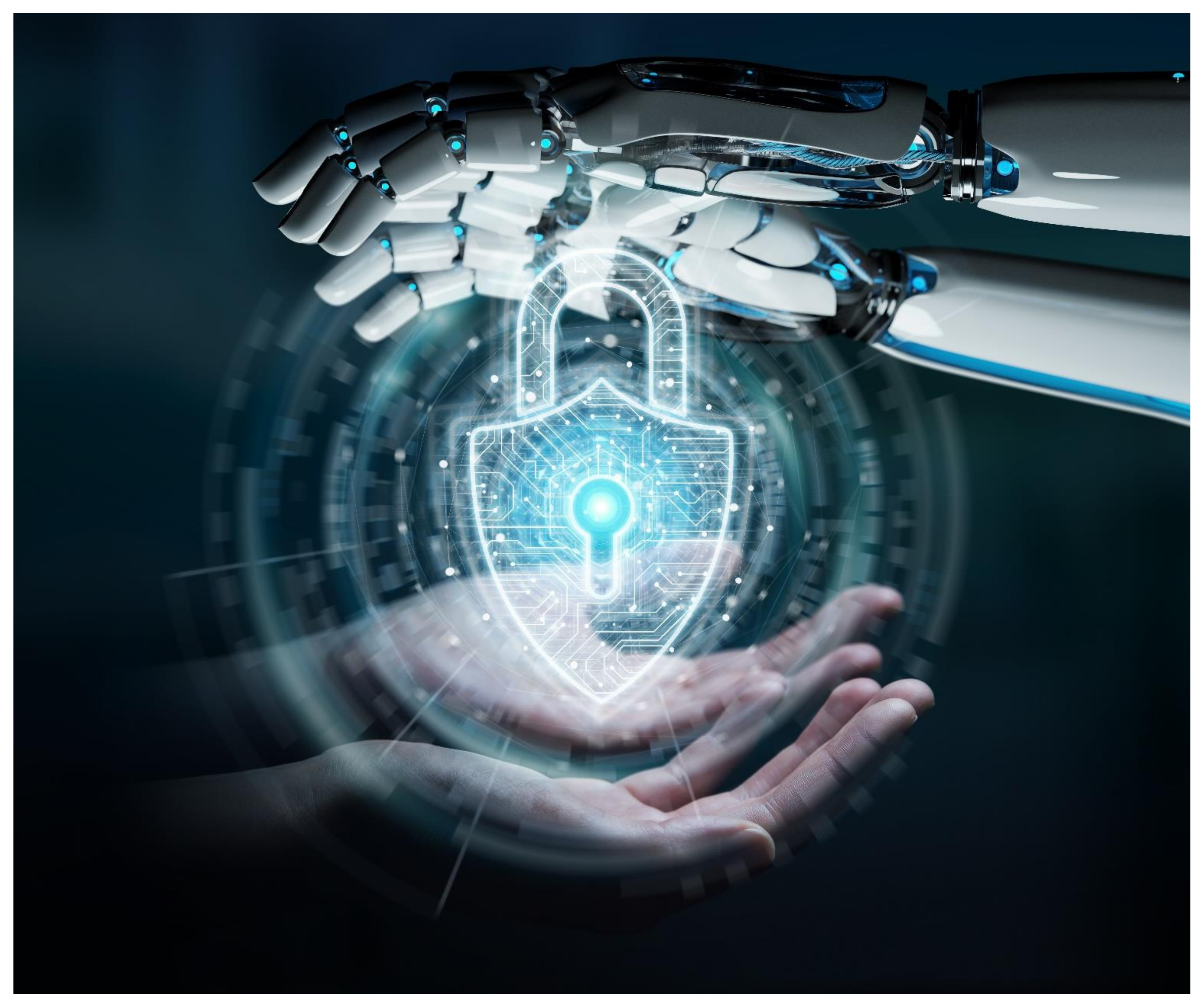
DUOLARK

Simple Steps Turn RATS into SECURE USERS

DUOLARK

Contact us for more on our Technology Advocate Program

- HIPAA | HITECH | FIPA
- Watch The Watcher
- Remote Access Threat Check
- (954) 324-3478



DUOLARK