RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: FLE-W08

CYBER-KINETIC ATTACK | EASY AS 1-2-3

Mike Rebultan, *MIT, GrDip-DFCS*
Global Cybersecurity Operation
@Equinix

RSAConference2019
Asia Pacific & Japan

DISCLAIMER |

The knowledge and ideas expressed in this talk does not reflect the view of any of the speaker's employers – past, present, and future.

RSAConference2019
Asia Pacific & Japan

AT A GLANCE

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth

RSAConference2019
Asia Pacific & Japan

AT A GLANCE

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth

RSAConference2019
Asia Pacific & Japan

…71% of cyber criminals say they can breach the perimeter of a target within 10 hours.

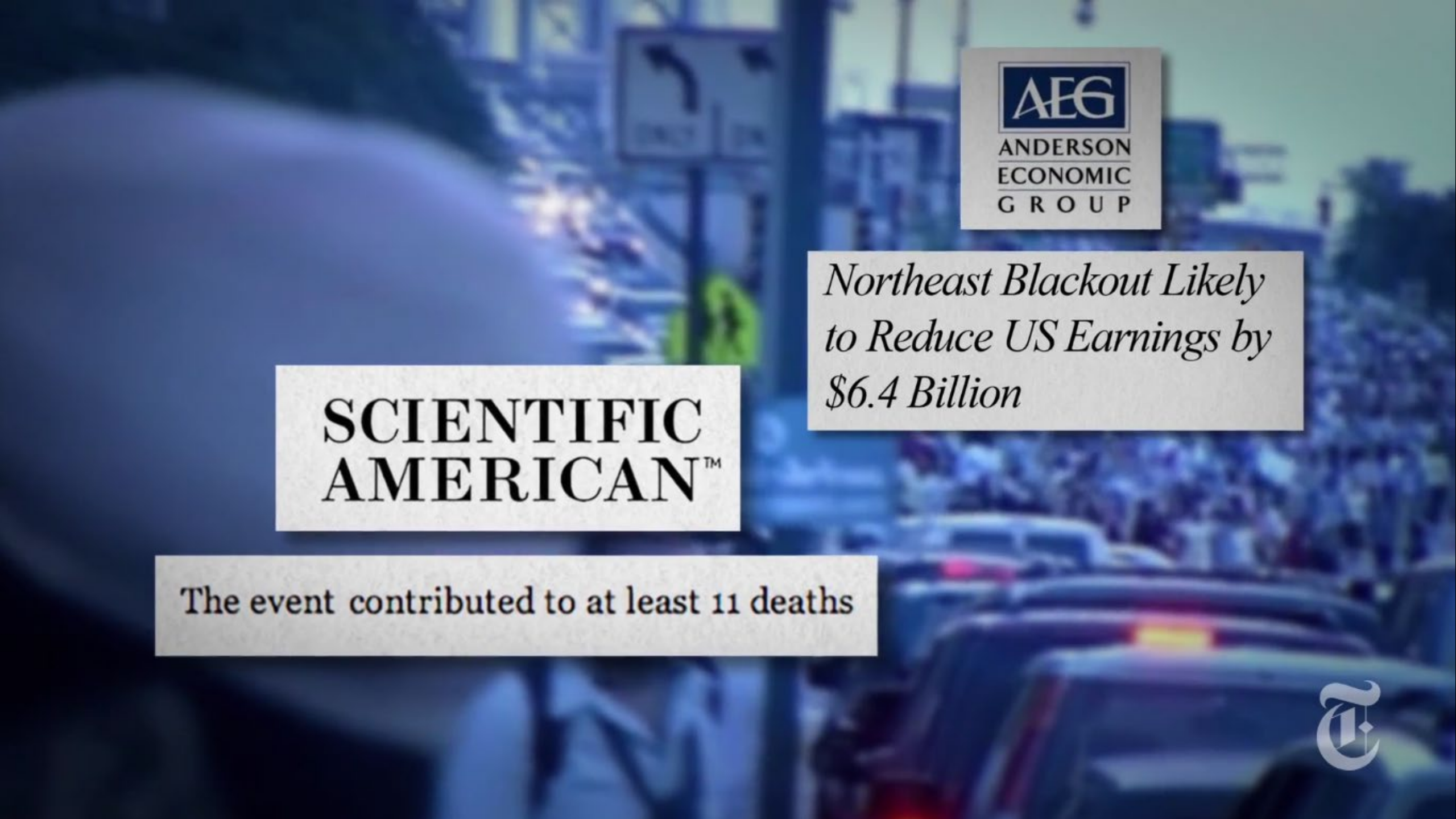
RSAConference2019
Asia Pacific & Japan

FIRESALE

RSAConference2019
Asia Pacific & Japan

AT A GLANCE

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth


AEG
ANDERSON
ECONOMIC
GROUP
Northeast Blackout Likely to Reduce US Earnings by $6.4 Billion
SCIENTIFIC AMERICAN™
The event contributed to at least 11 deaths

The Arleigh Burke-class guided-missile destroyer USS Fitzgerald, damaged by colliding with a Philippine-flagged merchant vessel, at the US naval base in Yokosuka,, Japan, June 18, 2017. Toru

RSAConference2019
Asia Pacific & Japan

PLANE FAILING Boeing 757 controls HACKED remotely while on the runway, officials reveal

The passenger jet failed a security test when a group of experts managed to take over its flight controls

By Margi Murphy
13th November 2017, 10:01 am | Updated: 13th November 2017, 12:21 pm

3 COMMENTS

Emerg

Event Yea

Country:

Industry T

Descriptio

Impact:

A GOVERNMENT official revealed that he and his team of IT experts remotely hacked into a Boeing 757 as it sat on the runway and were able to take control of its flight functions.

Robert Hickey, a US Homeland Security cyber sleuth, managed to take over the passenger at Atlantic City airport in New Jersey.

'I'M NOT IN CONTROL' Horrifying glitch caused packed passenger p towards the ocean TWICE in a sing

After the double nosedives, the cabin was a scene of can screaming, crying and praying

By Lauren McMah and Jon Lockett
18th June 2018, 10:31 am | Updated: 18th June 2018, 11:41 am

RSAConference2019 Asia Pacific & Japan

https://www.forbes.com/sites/leemathews/2019/04/28/ransomware-hits-yet-a

18,341 views | Apr 28, 2019, 12:00pm

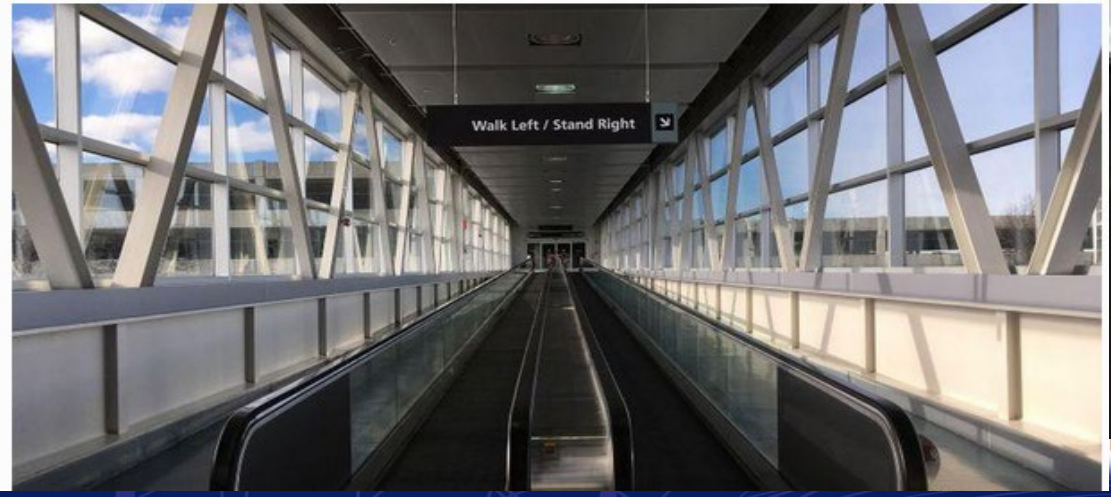
Ransomware Hits Yet Another U.S. Airport

Lee Mathews Contributor

Security

Observing, pondering, and writing about tech. Generally in that order.

It wasn't exactly business as usual at Cleveland Hopkins International Airport last week. Several information systems were disrupted by a ransomware outbreak.



https://www.theregister.co.uk/2019/03/28/f35_software_fail/

A CENTRE | SOFTWARE | SECURITY | DEVOPS | BUSINESS | PERSONAL TECH | SCI

Software

Easy-to-hack combat systems, years-old flaws and a massive bill – yup, that's America's F-35

POGO says no-go on money-pit jet fighter

By Shaun Nichols in San Francisco 28 Mar 2019 at 23:37 84 SHARE

The F-35 aircraft remains woefully unprepared against malware

RSAConference2019
Asia Pacific & Japan

AT A GLANCE |

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth

RSAConference2019
Asia Pacific & Japan

Threat Actors

- OnionDog APT
- Inj3ct0r Team
- IceFog APT
- Operation Ghoul
- Turla Group
- Naikon APT
- Hellsing APT
- APT3
- NewsBeef APT
- Union Spider
- Fancy Bear
- aLLiGaToR
- TeaMp0isoN
- Operation Newscaster
- Silent Chollima
- Transparent Tribe
- Anchor Panda
- APT 5
- Crimson Iron
- The Dukes
- Override Panda
- Magnallium
- Callisto Group
- Shanghai Group
- Cutting Kitten
- Dark Caracal
- SIG25
- Gallmaker
- Gamaredon Group
- Icefog
- Inception Framework
- Ke3chang
- Lazarus Group
- Dragonfish
- Lucky Cat
- Moafee
- Mofang
- MuddyWater
- NetTraveler
- Patchwork
- Pawn Storm
- Mythic Leopard
- Tropic Trooper
- Achilles
- Allanite
- Axiom
- Covellite
- Shadow Crane

RSAConference2019
Asia Pacific & Japan

AT A GLANCE |

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- IT vs OT
- Defense-in-Depth

RSAConference2019
Asia Pacific & Japan

TOOLS

- Inveigh
- Powershell scripts
- PSExec
- SecreetsDump
- THC Hydra
- APT3 Keylogger
- Bemstour
- CookieCutter
- DoublePulsar
- EternalBlue
- HTran
- Hupigon
- Kaba
- LaZagne
- OSInfo
- Pirpi
- PlugX
- Shareip
- SHOTPUT
- TTCalc
- w32times
- 0-days for IE, Firefox and Flash.
- Poison Ivy
- AUMLIB
- DynCalc/DNSCalc
- ETUMBOT
- HIGHTIDE
- IXESHE
- RapidStealer,
- THREEBYTE
- WaterSpout.
- Gh0st RAT
- hcdLoade
- HTTPBrowser
- Pisloader
- Roseam
- StickyFingers
- 0-day exploits for Flash
- C0d0so
- Cobalt Strike
- Empire
- Derusbi
- PlugX
- Mimikatz
- PowerSploit
- Metasploit
- NMAP

RSAConference2019
Asia Pacific & Japan

TECHNIQUES & PROCEDURES

- Watering Hole Attacks
- Trojanized Software
- Remote Access
- Network Penetrations
- Targeting POS
- Phishing Campaign
- Supply Chain Attacks
- Backdoor Installation
- Bruteforce
- Fuzzing / Buffer Over Flow
- Physical Social Engineering Attack

- https://attack.mitre.org/groups/G0035/
- https://attack.mitre.org/groups/G0020/
- https://attack.mitre.org/groups/G0027/
- https://a
- https://a
- https://a
- https://a
- https://attack.mitre.org/groups/G004/
- https://attack.mitre.org/groups/G0011/
- https://attack.mitre.org/groups/G0068/
- https://attack.mitre.org/groups/G0033/

MORE!!!

https://www.securityweek.com/most-ot-organizations-hit-damaging-cyberattacks

https://www.cpomagazine.com/cyber-security/polymorphic-phishing-attacks-now-make-u

CYBER SECURITY NEWS

Polymorphic Phishing Attacks Now Make Up Almost Half of All Phishing Attacks

Scott Ikeda — On **Jun 18, 2019**

An en

An attac
results in dow

Third pa

A cyberattack that causes significant dow me

Leakage of business-confidential inf tion, such as emails

Econo onage (thef nformation)

te attack

somware

breac customer
ee records

d/or lawsu ce with data
prote rement

53%

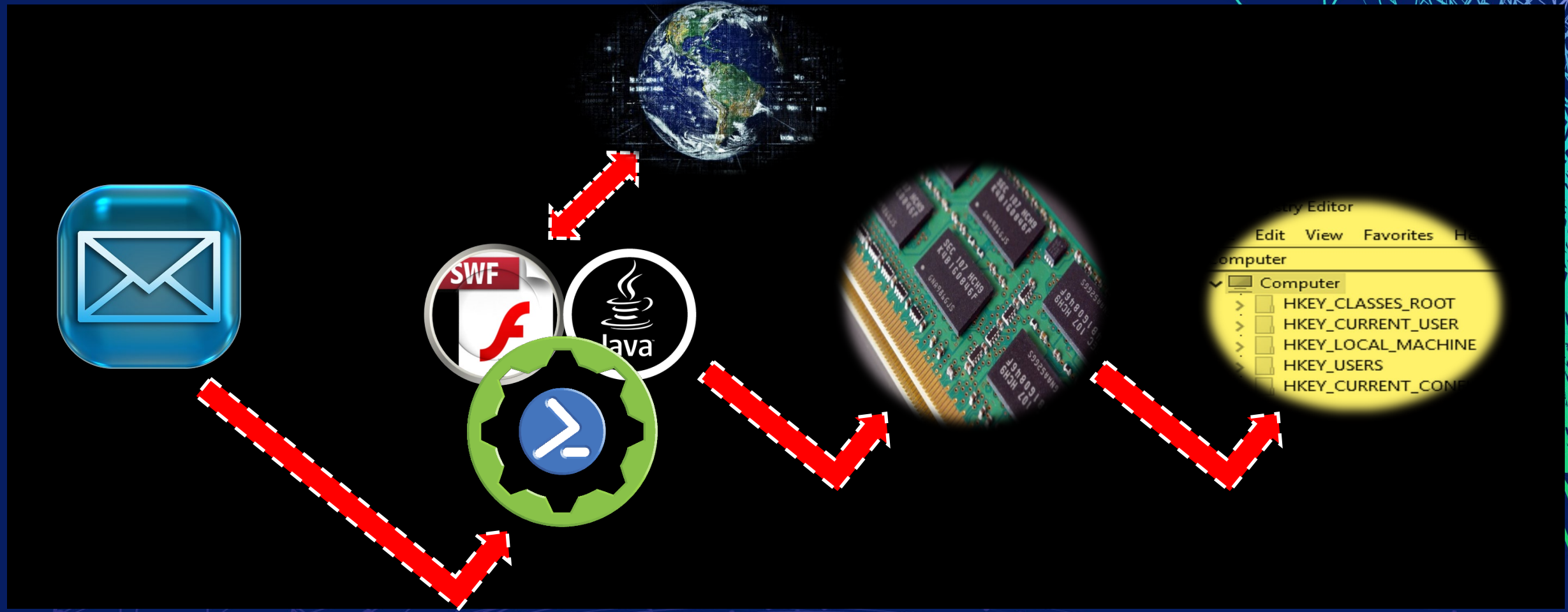
50%

45%

Downtime to OT ster is the number or
respondents citing s a factor. Organiza also assess risk based on the frequency of
unpatched vulnerabilities (45%), theft of i ctu property (41%), loss of employee
productivity (40%), and financial loss (38%)

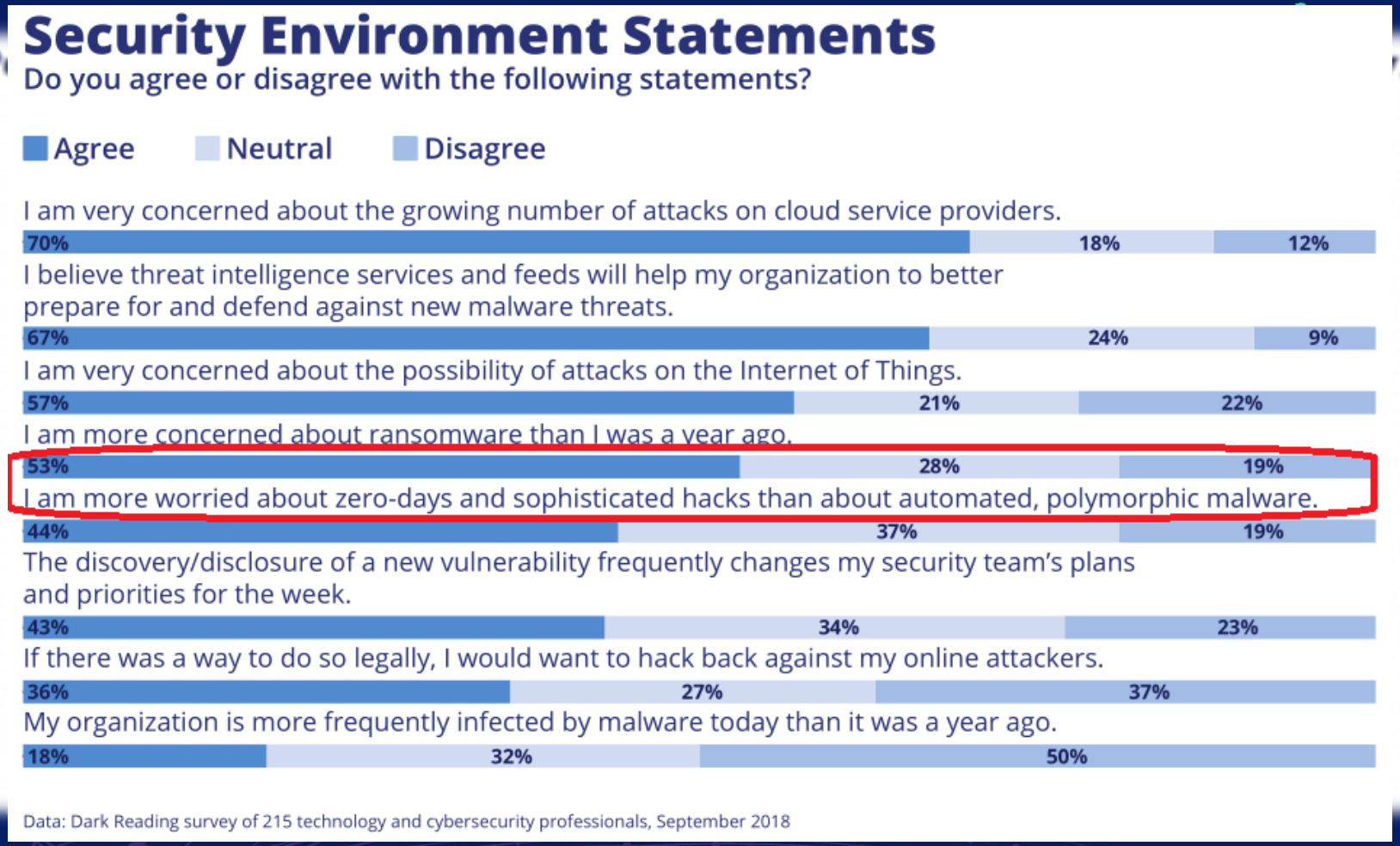
RSAConference2019
Asia Pacific & Japan

FILELESS MALWARE



RSAConference2019
Asia Pacific & Japan

POLYMORPHIC MALWARE

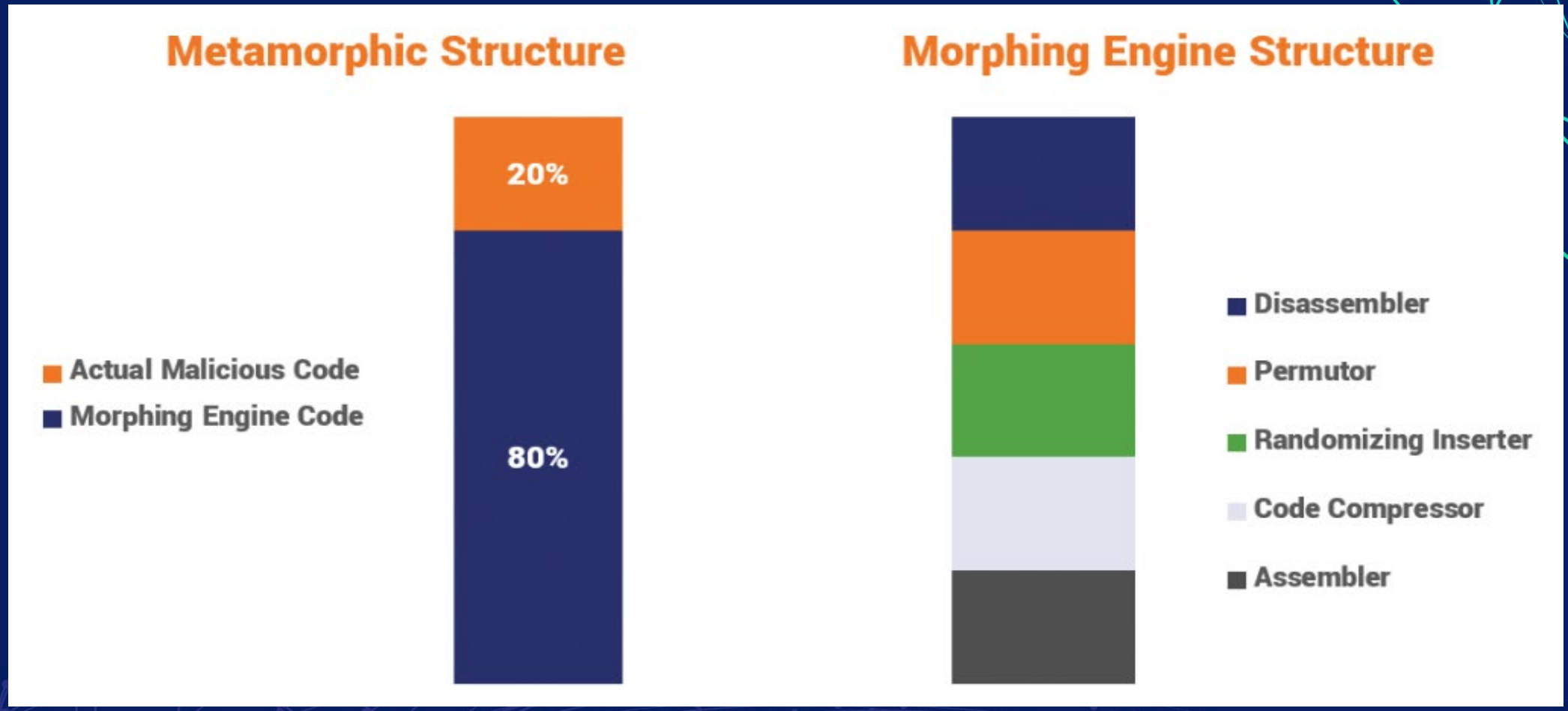


RSAConference2019
Asia Pacific & Japan

METAMORPHIC MALWARE

RSAConference2019
Asia Pacific & Japan

METAMORPHIC MALWARE

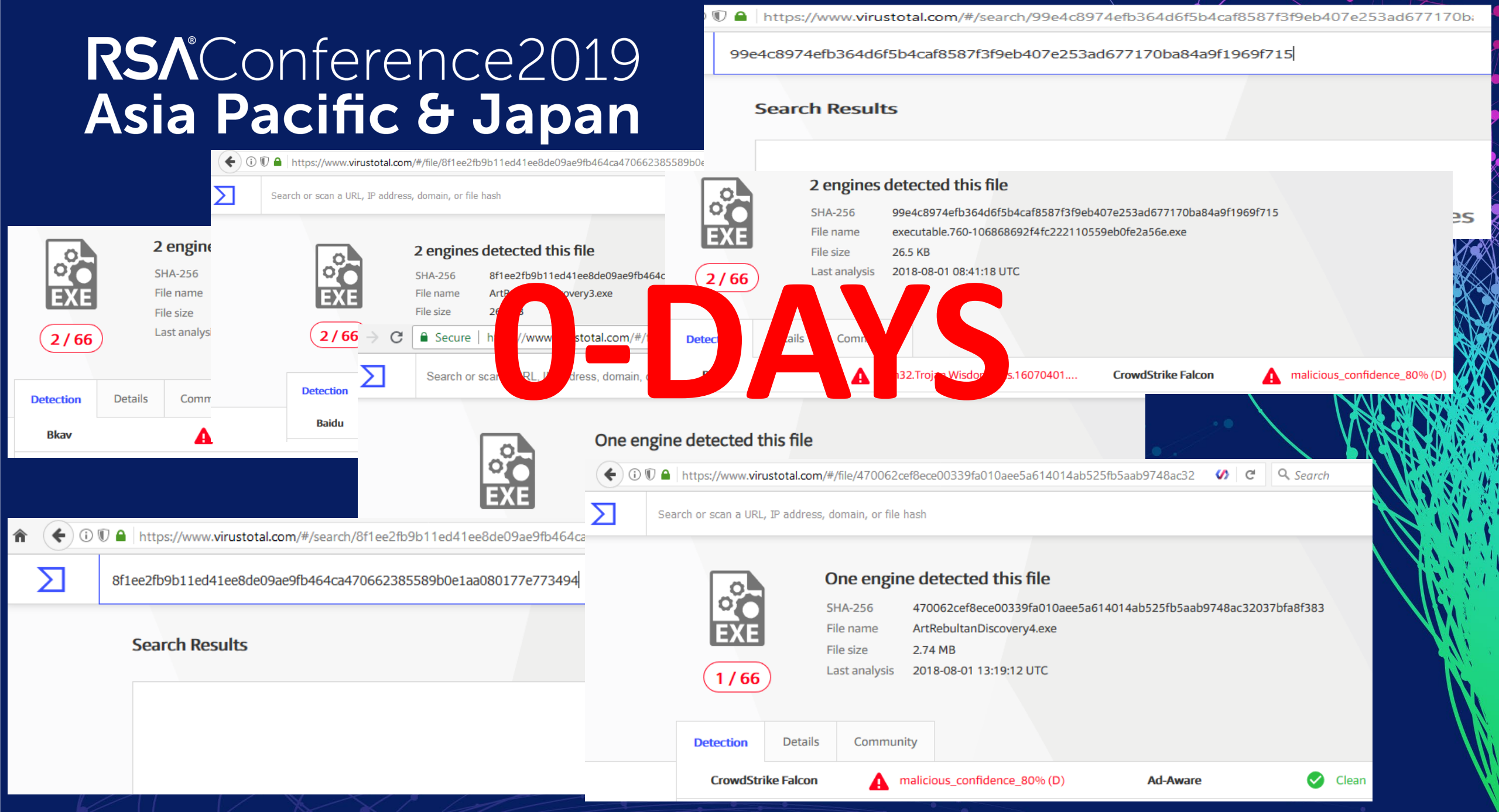


RSAConference2019
Asia Pacific & Japan

AT A GLANCE

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth

RSAConference2019 Asia Pacific & Japan



.vmem = raw memory

.vmsn & .vmss = memory image

.sav = partial memory image

.bin = memory image

.vsv = save state

.MEM = memory image

RSAConference2019
Asia Pacific & Japan

VM SYSTEM & TOOLS

- Win7 x86 w/ Office 2010 SP2, Java 1.8.0_x, Flash 16.x, Acrobat Reader 11.x, IE 11, Chrome 55, Firefox 43
- Win7 x64 w/ Office 2003 SP3, Java 1.8.0_x, Flash 16.x, Acrobat Reader 11.x, IE 11, Chrome 41, Firefox 36
- Win10 x64 (v. 1803) w/ Office 2016 Adobe Reader DC 19, Chrome 70, Firefox 63, Java 8.171, Flash 30.0.0.113
- WinXP x86 SP2 (*least option*)

RSAConference2019
Asia Pacific & Japan

MEMORY FORENSICS

- **Rogue Processes**
  - pslist, psscan, pstree
- **Process DLLs and Handles**
  - dlllist, getsids, handles, filescan, svcscan
- **Network Artifacts**
  - connections, connscan, sockets, netscan
- **Code Injection**
  - malfind, ldrmodules, malfinddeep, hollowfind, malprocfind
- **Rootkit Signs**
  - psxview, driverscan, apihooks, driverirp, idt
- **Dump Suspicious Processes and Drivers**
  - dlldump, moddump, procdump, memdump

```
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/remnux/ parasabayan.vmem
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
```

```
Offset(P)  Local Address               Remote Addr
---------- ------------------------ ------------
0x010732d8 172.16.176.143:1086       65
0x010735e0 172.16.176.143:1098       65
0x01073778 172.16.176.143:1077       65
0x01073d00 172.16.176.143:1096       65
0x0107ae70 172.16.176.143:1063       20
0x0107e6d8 172.16.176.143:1073       65
0x0107ed58 172.16.176.143:1088       65                1:80    1884
0x010c5e70 172.16.176.143:1074       65                :80     1884
0x010f1d00 172.16.176.143:1079       20                242:80  1884
0x010fb4b8 172.16.176.143:1089       65                :80     1884
0x0111d900 172.16.176.143:1070       72                :80     1884
0x01134e70 172.16.176.143:1068       65                :80     1884
0x0113b638 172.16.176.143:1076       65                :80     1884
0x02214988 172.16.176.143:1052       65                :80     1884
0x02db12e8 172.16.176.143:1091       65                :80     1884
0x02db1480 172.16.176.143:1080       65                :80     1884
0x0485dd58 172.16.176.143:1061       65                80      1884
0x04862b60 172.16.176.143:1069       96                80      1884
0x04863810 172.16.176.143:1078       65                :80     1884
0x05ce6e70 172.16.176.143:1059       65                :80     1884
0x05e354b8 172.16.176.143:1090       65                :80     1884
0x05e3cb48 172.16.176.143:1062       4.                80      1884
0x06015ab0 172.16.176.143:1056       69                80      1884
0x06232e70 172.16.176.143:1064       64                80      1884
0x06384e70 172.16.176.143:1055       20                21:80   1884
```

```
Process: IEXPLORE.EXE Pid: 1884 Address: 0x10020000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 22, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x10020000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x10020010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x10020020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x10020030  00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00   ................
```

Shodan | Developers | Monitor | View A

SHODAN port:502 country:"SG"

Exploits | Maps | Share Search

naystak Search About Go Premium

Search

satellite jammer

Search

Found 420 results.

Advertise here - contact us via the form

GPS Jammers blocker Satellite TV signal reception

http://43f74pccymmgu3sf.onion/tv-satellite.html

GPS Jammers blocker Satellite TV signal reception [] Welcome to the Jammer-Shop,You can choose retail Phone Jammer []$219.87 Buy Very High Power Broadband Jammers [] $216.36 [] [] Satellite TV signal signal jammer.

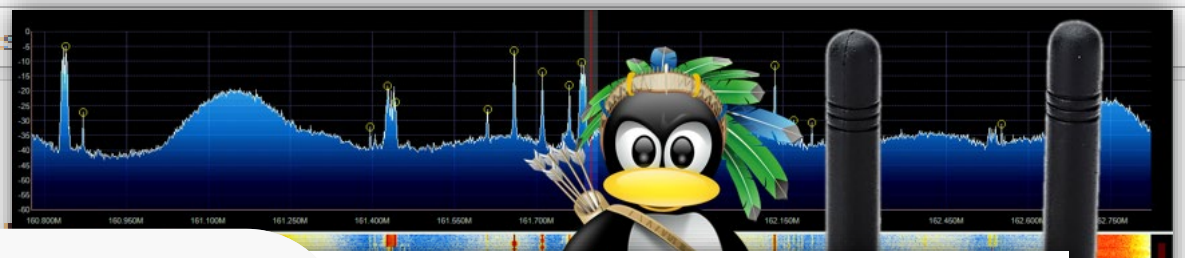
Satellite radio jammer interference signal radiation is bigger, can affect the health of the residents Through the above information we know that the satellite signal jammer to accept to be reckoned with GPS Jammers blocker Satellite TV signal reception

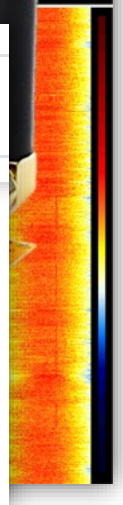
Cached version - Historical versions - Datapoints (e.g. bitcoin addresses) - Report for removal

GPS Jammers blocker Satellite TV signal reception

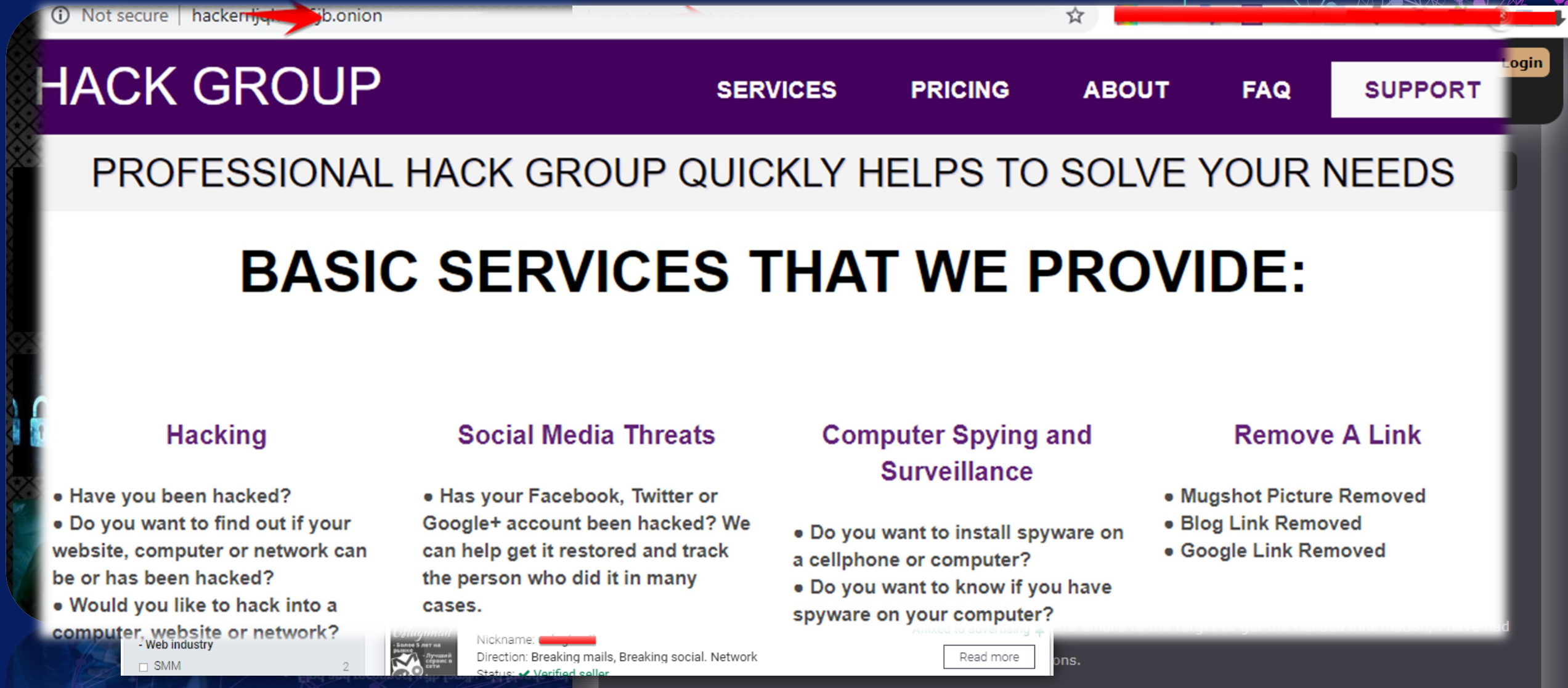
http://2tnhglajammerekg.onion/tv-satellite.html

GPS Jammers blocker Satellite TV signal reception [] Welcome to the Jammer-Shop,You can choose retail Phone Jammer []$219.87 Buy Very High Power Broadband Jammers [] $216.36 [] [] Satellite TV signal signal jammer.



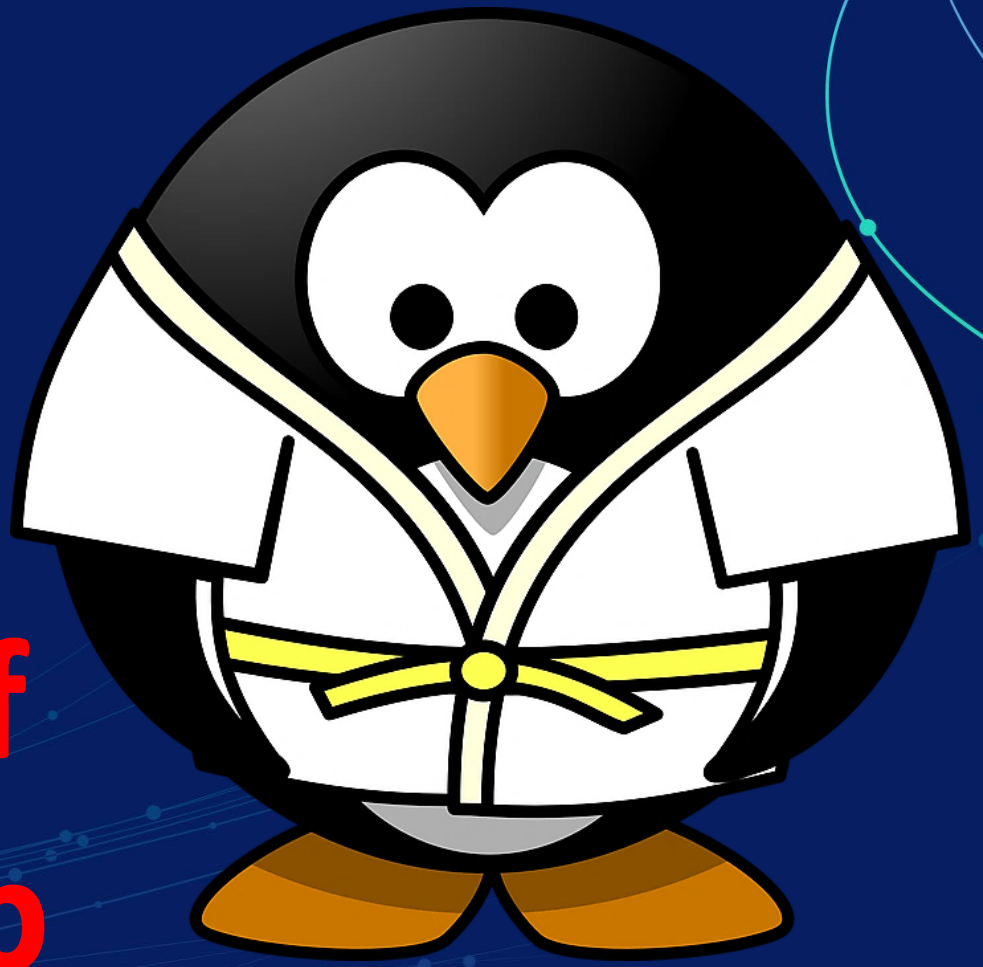


	Disclosure Date	Initial MSF Release Date
dataserver_listall.rb	Mar. 24, 2011	May 16, 2011
dataserver_rename.rb	Mar. 24, 2011	Jun. 9, 2011
c.rb	Mar. 24, 2011	May 30, 2011
17.rb	Mar. 21, 2011	Mar. 22, 2011
y_bof.rb	Sep. 13, 2011	Sep. 17, 2011
veb_server.rb	Dec. 2, 2011	Dec 13, 2011
csv.rb	Sep. 16, 2010	Nov. 11, 2010
pro.rb	Aug. 11, 2011	Aug. 11, 2011
cat.rb	Sep. 13, 2011	Oct. 10, 2011
	Jan. 19, 2012	Jan. 19, 2012
bd.rb	Jan. 19, 2012	Jan. 19, 2012
nbroker.rb	Mar. 21, 2011	Jul. 17, 2011
ebhmi_setactivexguid.rb	May 5, 2011	May 11, 2011
cmdexe.rb	Sep. 16, 2011	Sep. 16, 2011
ntool.rb	Oct. 20, 2010	Nov. 6, 2010
	Sep. 26, 2008	Sep. 30, 2008
pc_initialize.rb	Oct. 15, 2010	Oct. 18, 2010
pc_initialize_rf.rb	Oct. 15, 2010	Oct. 18, 2010
pc_txtevent.rb	Nov. 18, 2010	Nov. 24, 2010
fc_binfile_a.rb	Mar. 21, 2011	Jun. 19, 2011
fcs_login.rb	Mar. 21, 2011	Jun. 22, 2011
ore_server.rb	Sep. 8, 2011	Sep. 12, 2011
hone_zip.rb	Sep. 12, 2011	Sep. 13, 2011
da_odbc.rb	Jun. 11, 2008	Nov. 8, 2010
ntime.rb	Jan. 13, 2011	Jun. 21, 2011
nk_cssservice.rb	Mar. 25, 2011	Jun. 24, 2011
orylink_vrn_09.rb	Mar. 21, 2011	Jun. 21, 2011
Unitronics | OPC Server | n/a | exploit/exploits/windows/browser/teechart_pro.rb	Aug. 11, 2011	Aug. 11, 2011


Not secure
b.onion
HACK GROUP
SERVICES
PRICING
ABOUT
FAQ
SUPPORT
Login
PROFESSIONAL HACK GROUP QUICKLY HELPS TO SOLVE YOUR NEEDS
BASIC SERVICES THAT WE PROVIDE:
Hacking
• Have you been hacked?
• Do you want to find out if your website, computer or network can be or has been hacked?
• Would you like to hack into a computer, website or network?
Social Media Threats
• Has your Facebook, Twitter or Google+ account been hacked? We can help get it restored and track the person who did it in many cases.
Computer Spying and Surveillance
• Do you want to install spyware on a cellphone or computer?
• Do you want to know if you have spyware on your computer?
Remove A Link
• Mugshot Picture Removed
• Blog Link Removed
• Google Link Removed
- Web industry
SMM
Nickname:
Direction: Breaking mails, Breaking social. Network
Read more

RSAConference2019
Asia Pacific & Japan

"TORless" Journey to the Center of the Dark Web



```
msf5 > search scada

Matching Modules
================
```

```
msf5 > search modbus

Matching Modules
================
```

```
msf5 > search plc

Matching Modules
```

```
msf5 > search radio

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  auxiliary/scanner/gprs/gtp_echo                                normal  Yes    GTP Echo Scanner
   1  exploit/windows/browser/aol_ampx_convertfile  2009-05-19       normal  No     AOL Radio AmpX ActiveX Control ConvertFile() Buffer Overflow
   2  exploit/windows/fileformat/xradio_xrl_sehbof  2011-02-08       normal  No     xRadio 0.95b Buffer Overflow
   3  post/hardware/rftransceiver/transmitter                        normal  No     RF Transceiver Transmitter
```

```
   8   auxiliary/scanner/scada/modbusclient                          normal  No     Modbus Client Utility
   9   auxiliary/scanner/scada/modbusdetect          2011-11-01      normal  Yes    Modbus Version Scanner
   10  auxiliary/scanner/scada/pcomclient                            normal  No     Unitronics PCOM Client
```

```
flow
   68  exploit/windows/scada/yokogawa_bkhodeq_bof                    2014-03-10      average    Yes    Yokogawa CENTUM CS 3000 BKHOdeq.exe Buffer
Overflow
```

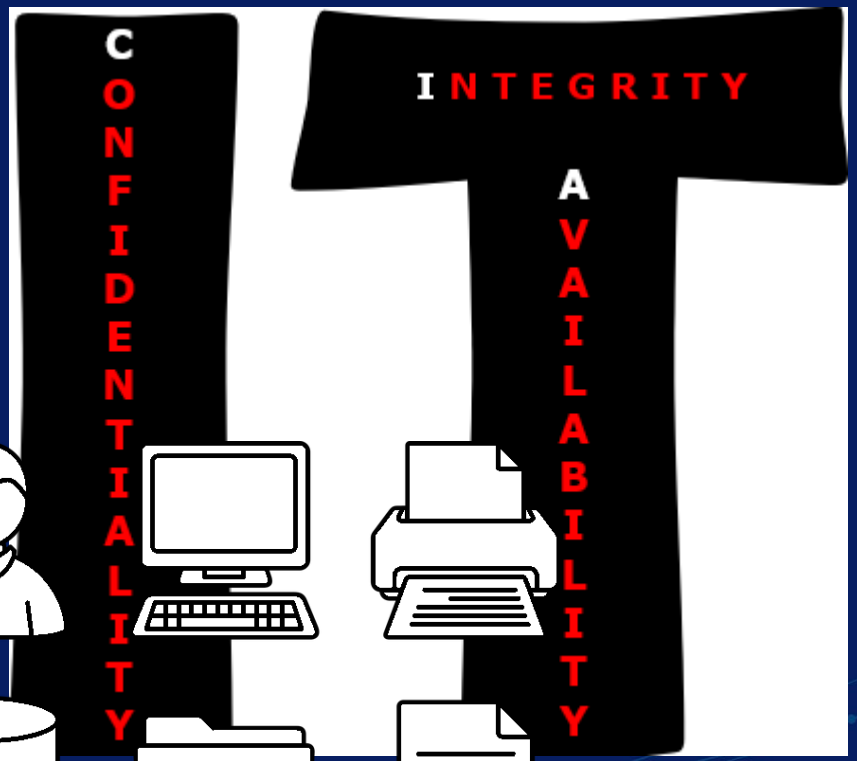
RSAConference2019
Asia Pacific & Japan

RSAConference2019
Asia Pacific & Japan

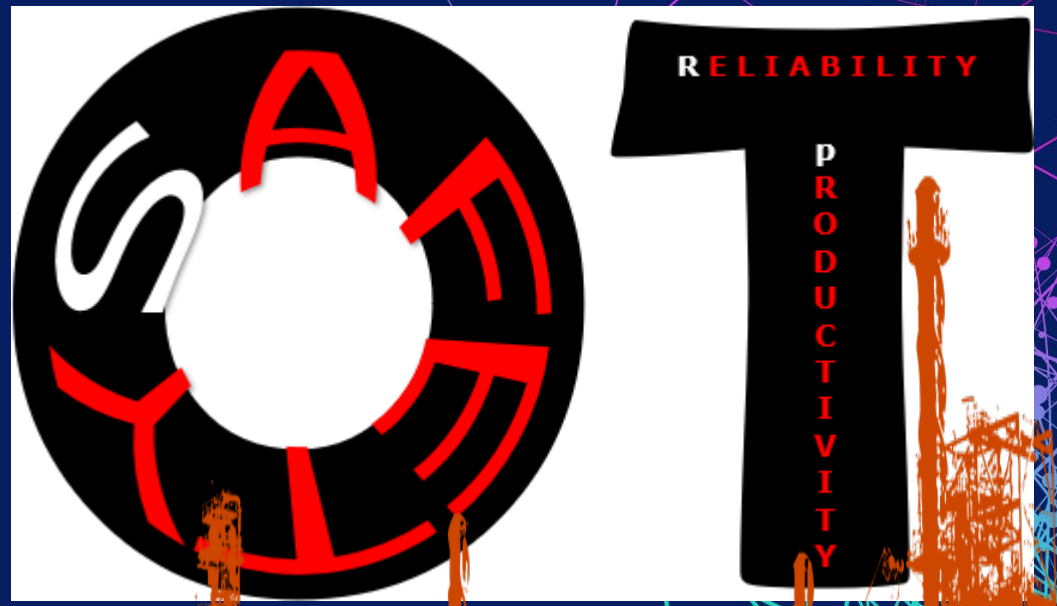
AT A GLANCE

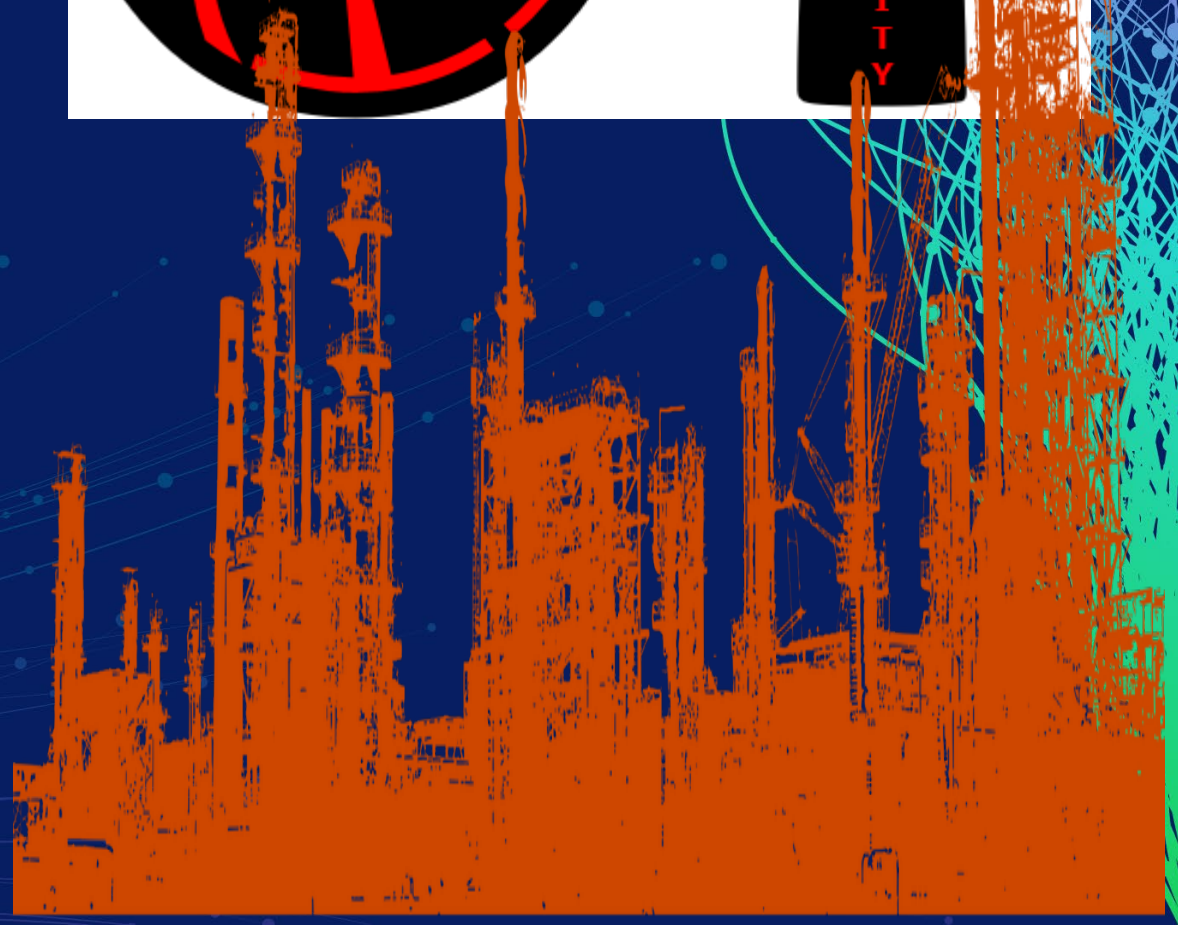
- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth

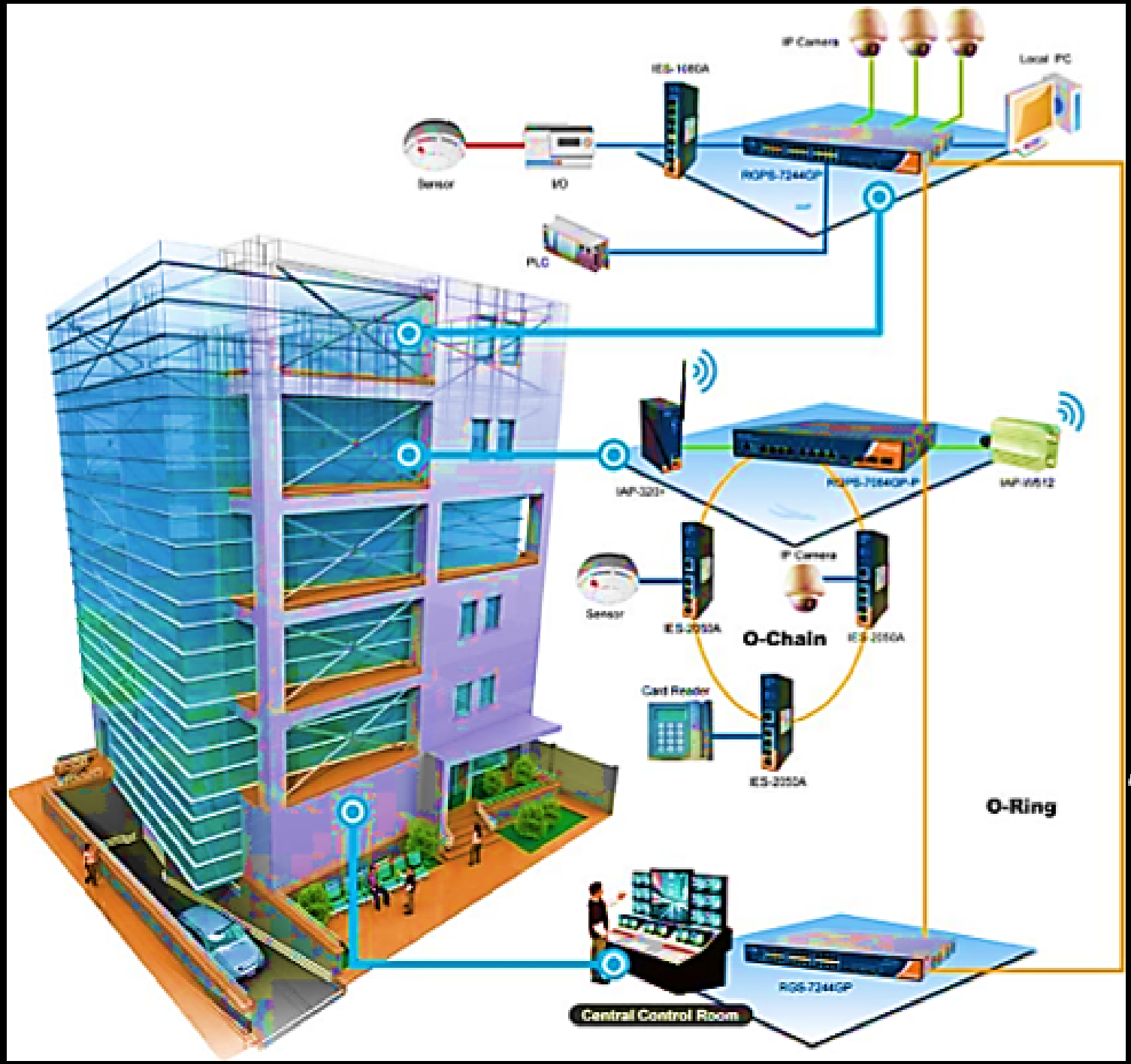
RSAConference2019
Asia Pacific & Japan



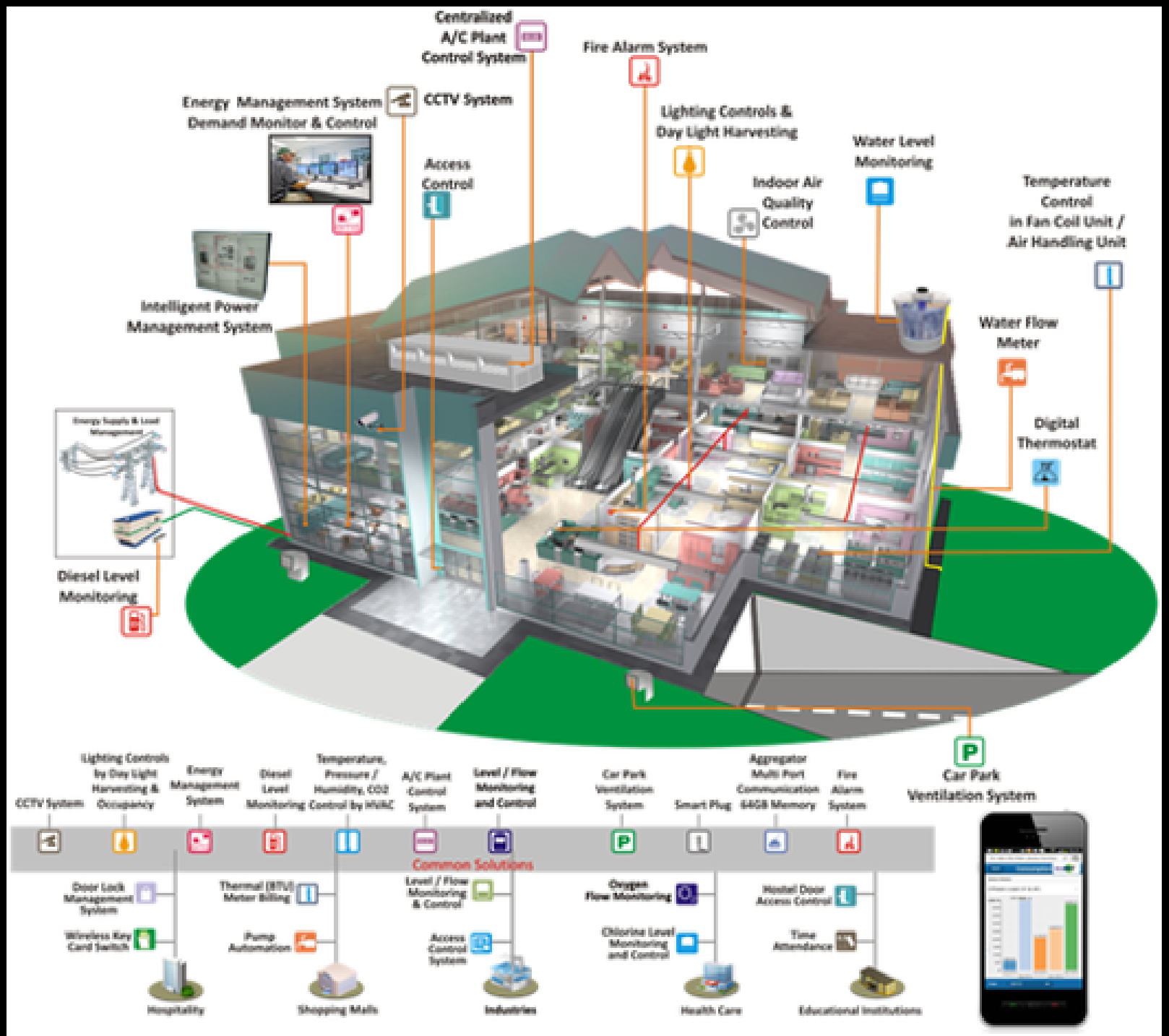
≠





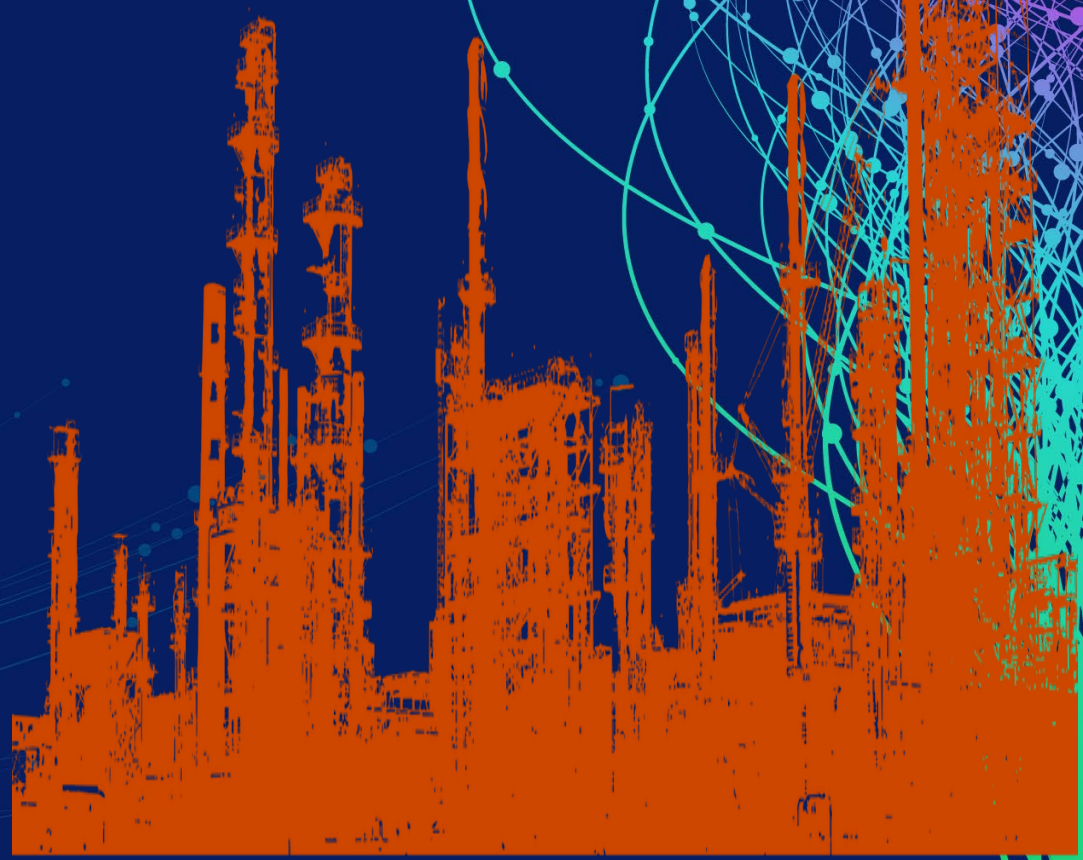


Building
Management
System
– to monitor and control the mechanical devices (ex: *power, light, fire, heating systems and security systems* etc.)



Energy Management System – monitors, controls and optimizes performance of the electrical buildings.

RSAConference2019
Asia Pacific & Japan



RSAConference2019
Asia Pacific & Japan

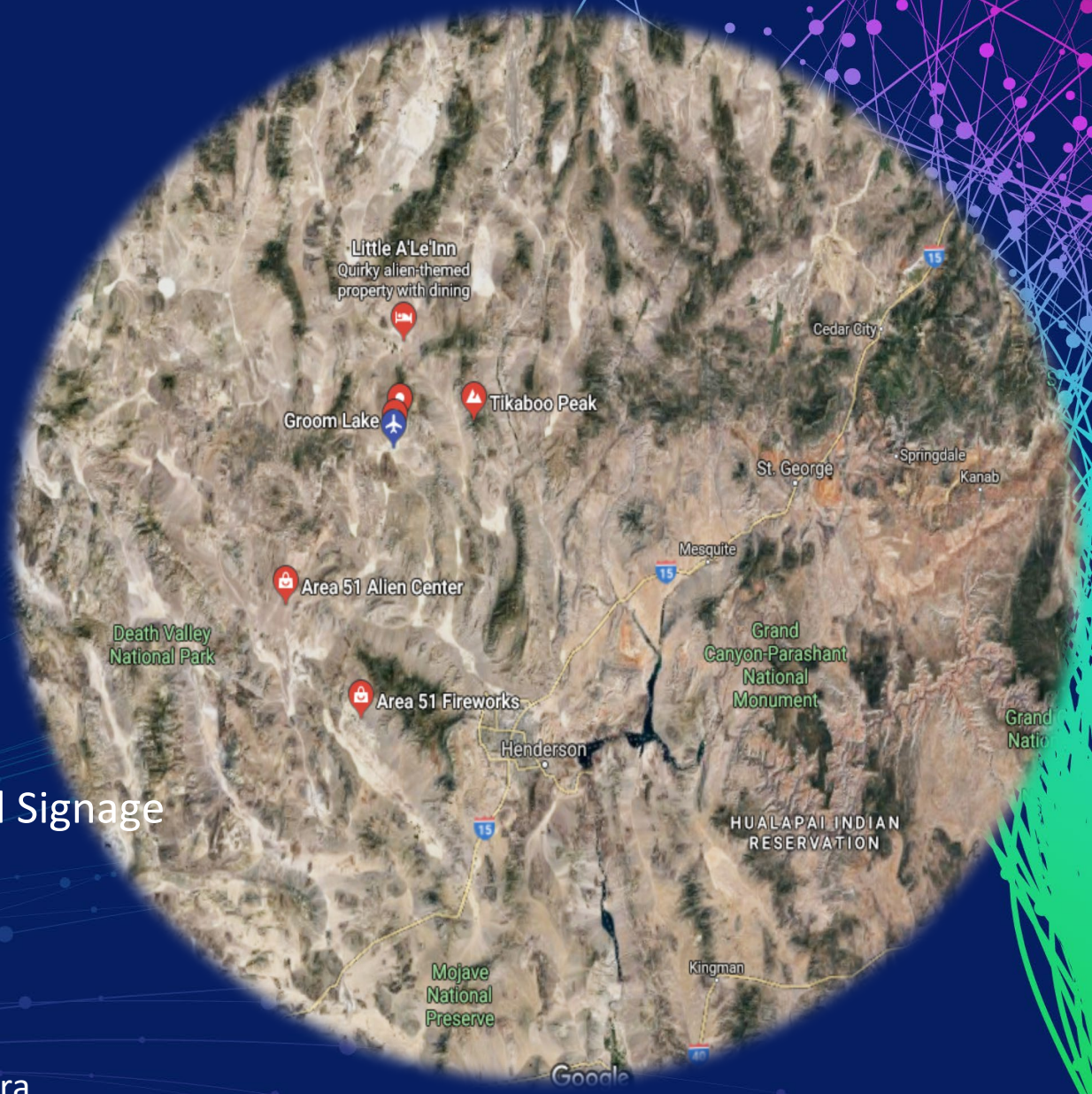
AT A GLANCE |

- Threat Landscape
- Notable Incidents
- Threat Actors
- TTP's
- 0DAY Threat Hunting
- IT vs OT
- Defense-in-Depth

RSAConference2019
Asia Pacific & Japan

PHYSICAL SECURITY |

- **Perimeter Defense**
  - Fence, CCTV, Guarded and Limited Entry/Access Points
- **Clear Zone & Parking Lot**
  - CCTV/Surveillance Camera, Intrusion Detection Sensor
- **Reception Area**
  - Card Reader, Security Key System, Door Operator, CCTV
- **Hallway Area**
  - Security Personnel, CCTV, Access Control, Computerized Signage
- **Server Room**
  - Biometric Reader, Card Reader, CCTV / Surveillance Camera
- **Server Rack / Cabinet**
  - Designated Access Control / Escorted Security Personnel, Dome Camera,



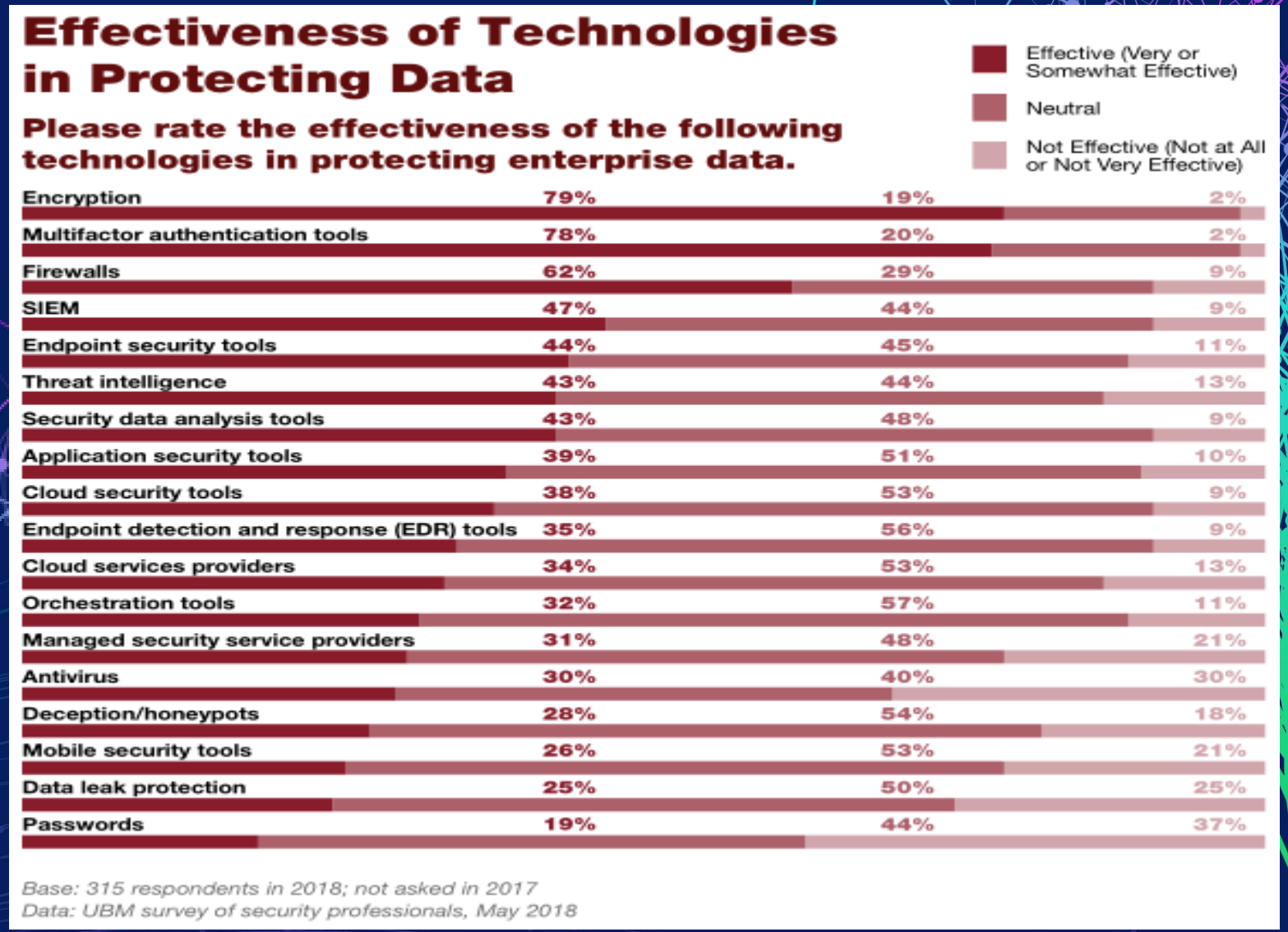
RSAConference2019
Asia Pacific & Japan

OPERATIONS TECHNOLOGY

- **Policies & Procedures**
  - NIST, NERC, USNRC, NIE, IIC, CMMI, ISO, etc.
- **Network Segmentation**
  - ISA-99 or IEC 62243
- **MFA**
- **Application Whitelisting**
- **Network Sensors**
  - Ingress and Egress Point
- **IDS/IPS, DMZ, FW**
  - Deny All
- **Real-Time Monitoring**
  - NMS and Log Management System
- **Visibility & Control**
  - Asset Management & EPP
- **Patch Management**
- **OS Lockdown**
  - CIS, OPC Host Hardening
- **OS Auditing**
- **Vulnerability Management**
  - Regular Basis, Iteration
- **Penetration Testing and/or Red Teaming**
  - Attack Simulation (IT Prod / OT Backup)
- **Continuous Cyber Security Awareness**
  - IT/OT Personnel

RSAConference2019
Asia Pacific & Japan

INFORMATION TECHNOLOGY



RSAConference2019
Asia Pacific & Japan

OPERATIONS TECHNOLOGY

- **Policies & Procedures**
  - NIST, NERC, USNRC, NIE, IIC, CMMI, ISO, etc.
- **Network Segmentation**
  - ISA-99 or IEC 62243
- **MFA**
- **Application Whitelisting**
- **Network Sensors**
  - Ingress and Egress Point
- **IDS/IPS, DMZ, FW**
  - Deny All
- **Real-Time Monitoring**
  - NMS and Log Management System
- **Visibility & Control**
  - Asset Management & EPP
- **Patch Management**
- **OS Lockdown**
  - CIS, OPC Host Hardening
- **OS Auditing**
- **Vulnerability Management**
  - Regular Basis, Iteration
- **Penetration Testing and/or Red Teaming**
  - Attack Simulation (IT Prod / OT Backup)
- **Continuous Cyber Security Awareness**
  - IT/OT Personnel

RSAConference2019
Asia Pacific & Japan

Links |

- **The 2016 UK Rail Cyber Security Guidance**
  - https://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf
- **Critical Aspects in the Maritime Sector, European Network and Information Security Agency**
  - https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1
- **Cyber Kinetic Attack Timeline**
  - https://www.ultra-3eti.com/timeline-of-key-cyber-kinetic-attacks-incidents-and-research/
- **Past Recorded Incident Database**
  - https://www.risidata.com/

RSAConference2019
Asia Pacific & Japan

THANK YOU !!!

- **LinkedIn**
  - https://www.linkedin.com/in/ArtRebultan
- **CyberSec-Blogs**
  - https://www.cybrary.it/members/Strainer/
  - https://www.peerlyst.com/users/Mike-Art-Rebultan
- **FB Page**
  - InfoSec-Tarlac

RSAConference2019
Asia Pacific & Japan

SPEAKER BIO

- **Mike Rebultan**, aka "**Art**" has more than 16 years of experience as an IT professional with a background in PCI-DSS audit management, Unix/Linux server lockdown and systems administration, R&D, VAPT, and currently a DFIR/SecOps in an ICS/OT company.

- Holding a master degree in IT with concentration in E-Commerce security. He has also a professional graduate diploma in Digital Forensics and Cyber Security as continuing education.

- Specializing in Computer Forensics, Network Intrusion, Data Breach, Cybercrime Investigation, Malware Analysis and Reverse Engineering.