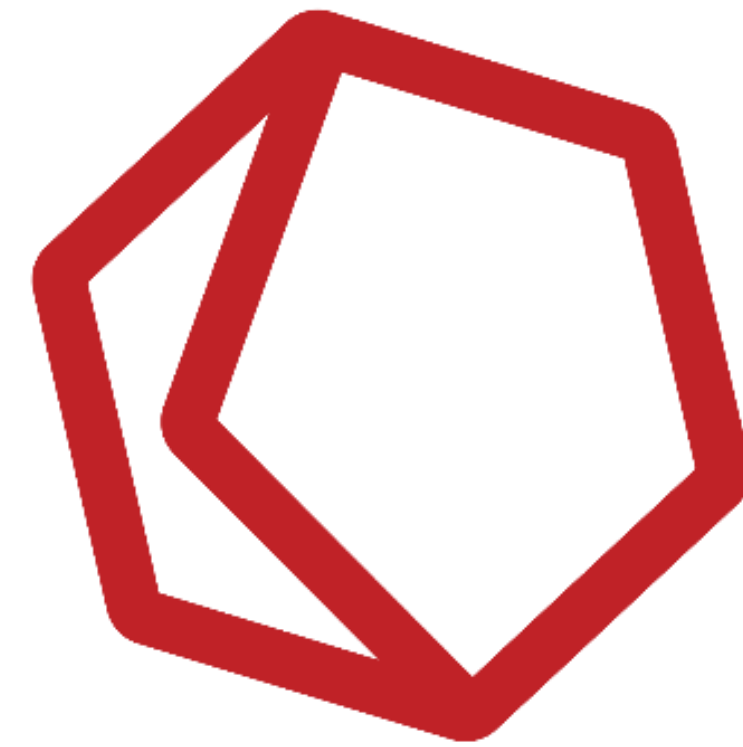


State of Cyber Security in Myanmar

Prepared For

CyberBayKin Conference @ NTP



kernellix

C y b e r D e f e n s e
S o l u t i o n s a n d S e r v i c e s

TLP: WHITE

November 26, 2018



Ye Thura Thet
Principal Analyst

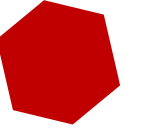


+959 500 9560



ye.tt@kernellix.com

Introduction



an information security practitioner

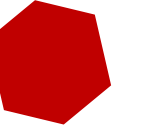
- Penetration Testing, Vulnerability Assessment (aka red team)
- Security Engineering, Monitoring and Response (aka blue team)
- Founder/Principal Analyst of a Cybersecurity Firm

a programmer

- Java, c#, python

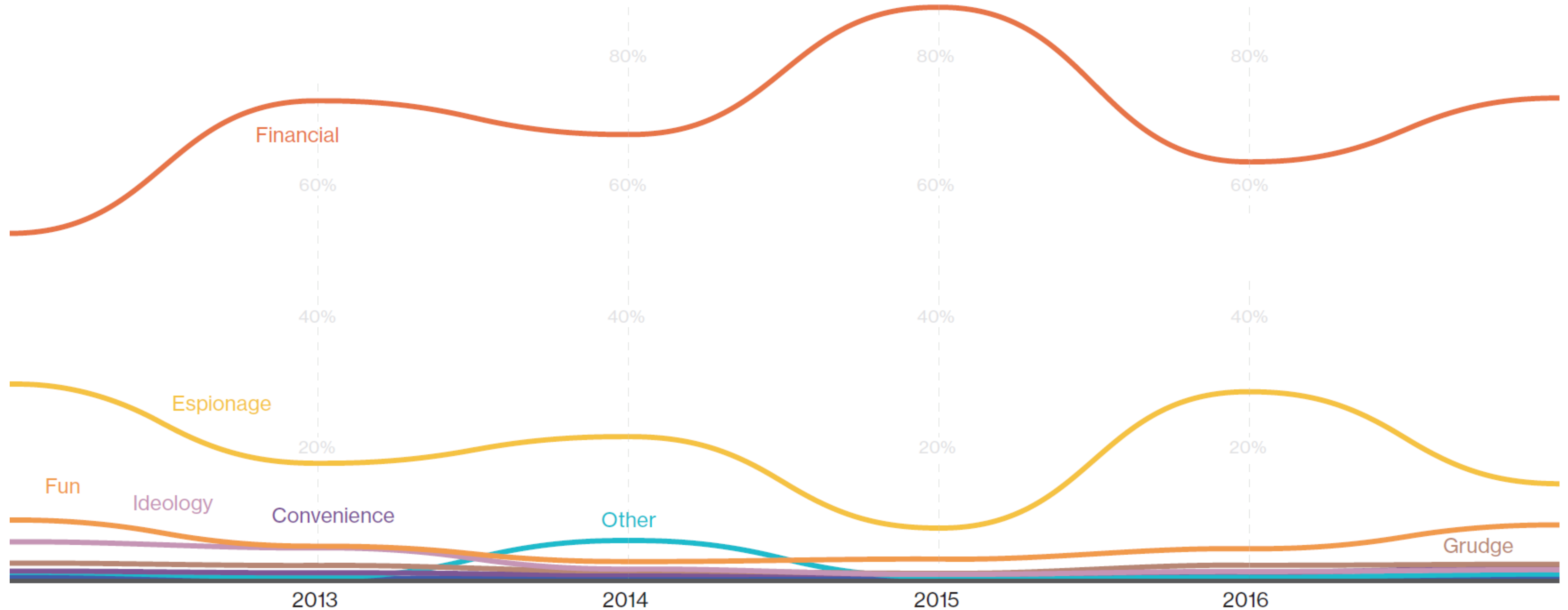
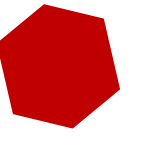
a visiting lecturer/trainer

- IT, Software Development, Cybersecurity



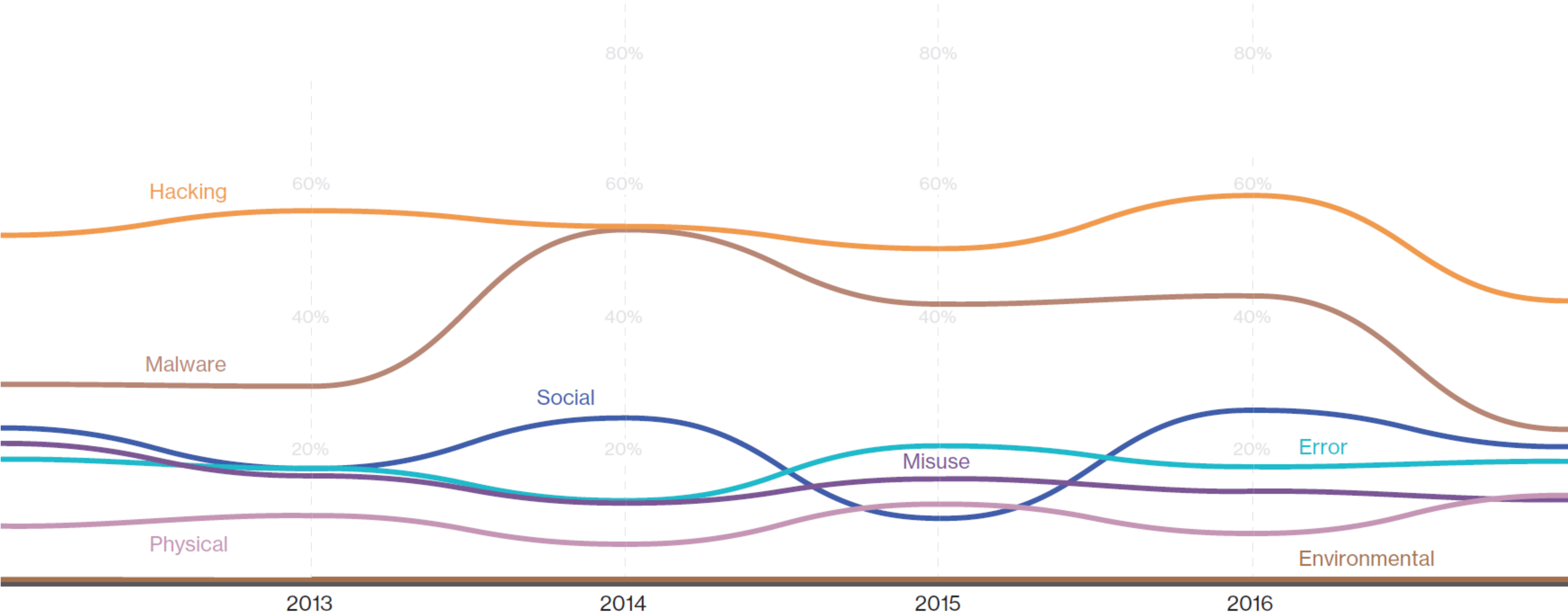
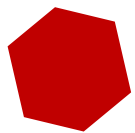
Around the Globe

DBIR Trends – Motives

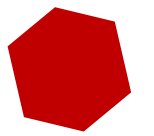


https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

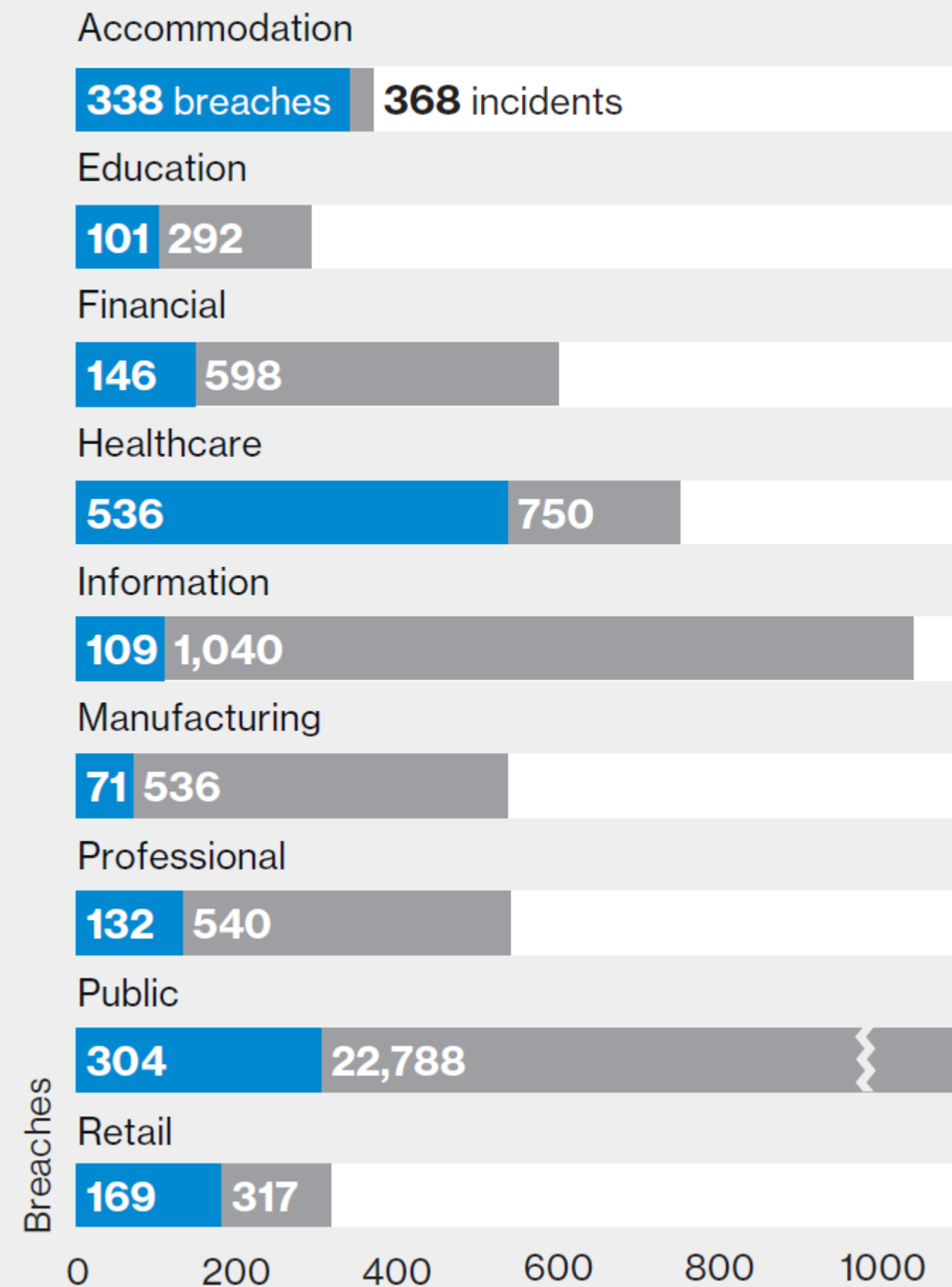
DBIR Trends – Actions



DBIR Trends – Industry



Number of incidents and breaches by sector



Financial

Who 79% external, 19% internal

What 36% personal, 34% payment, 13% bank

How 34% hacking, 34% physical



Retail

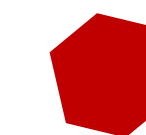
Who 91% external, 10% internal

What 73% payment, 16% personal, 8% credentials

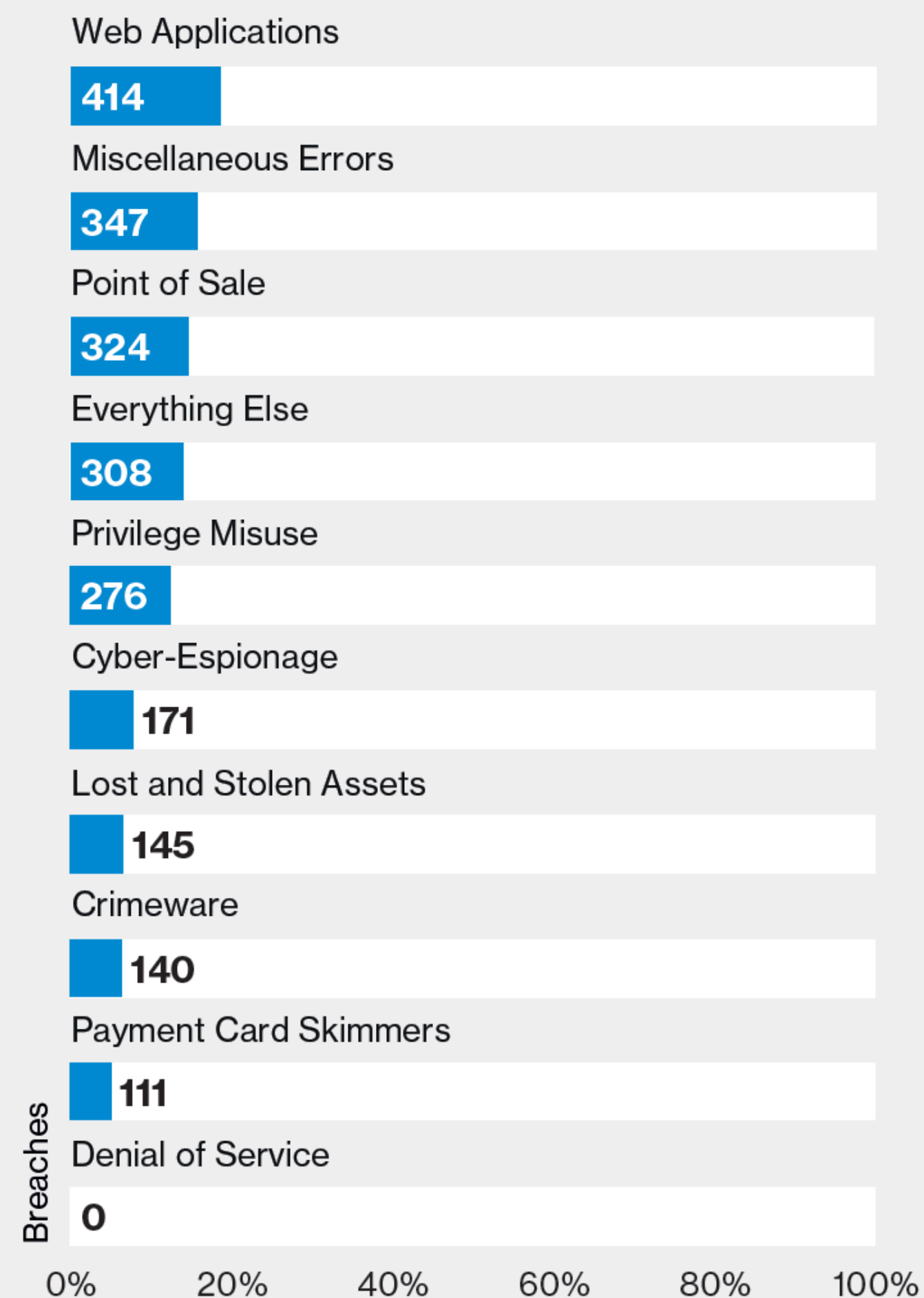
How 46% hacking, 40% physical

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

DBIR Trends – Patterns



Breaches by pattern



Web Application Attacks

Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.

Notable findings

The number of breaches in this pattern are reduced due to the filtering of botnet-related attacks on web applications using credentials stolen from customer-owned devices. Use of stolen credentials is still the top variety of hacking in breaches involving web applications, followed by SQLi.

Payment Card Skimmers

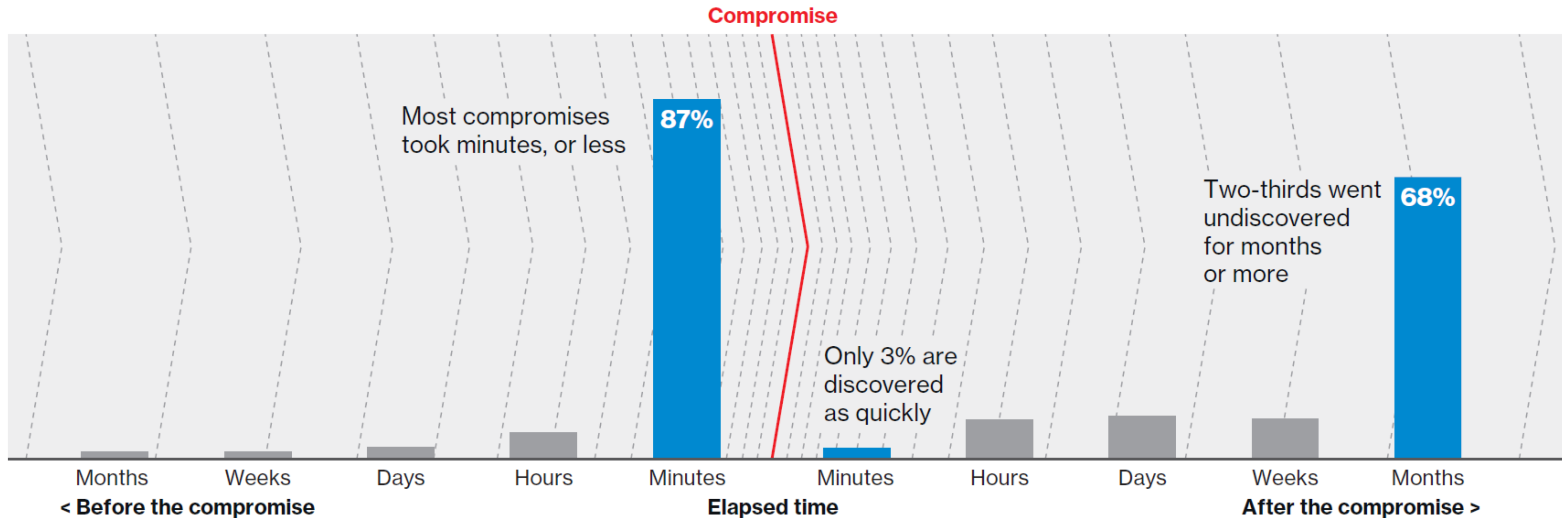
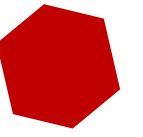
All incidents in which a skimming device was physically implanted (tampering) on an asset that reads magnetic stripe data from a payment card.

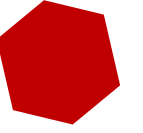
Notable findings

While commonly associated with ATMs, gas pump terminals were just as likely to be targeted in this year's dataset.

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

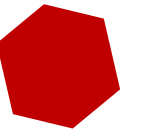
DBIR Trends – Detection





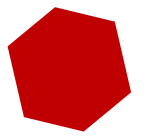
in Myanmar ?

Cyber Crime Trends



The lack of broadband connectivity also affects the amount of cybercrime—one official we interviewed said that once a country **gets broadband connectivity**, usually **without adequate defenses**, **cybercrime spikes** within a few days.

<http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf>



BEC Scam



BEC Scam Losses Top \$12 Billion: FBI

By [Eduard Kovacs](#) on July 16, 2018



Share



Tweet

Recommend 0

RSS

The losses and potential losses reported as a result of business email compromise (BEC) and email account compromise (EAC) scams exceed \$12 billion globally, according to an alert published last week by the FBI.

The report is based on data collected by the FBI's Internet Crime Complaint Center (IC3), international law enforcement and financial institutions between October 2013 and May 2018. The amounts represent both money that was actually lost by victims and money they could have lost had they taken the bait.

BEC scams, which involve sending requests for fund transfers and personally identifiable information from hijacked business email accounts, have been observed in 50 U.S. states and 150 countries, with money being sent to 115 countries.

The top destinations for money generated by BEC scams are Asian banks in China and Hong Kong, but a significant number of schemes involve financial organizations in the U.K., Mexico and Turkey.

According to the FBI, more than 78,000 complaints have been made globally between October 2013 and May 2018, with over 41,000 victims reported in the United States. Targeted individuals and businesses lost or could have lost \$12.5 billion, nearly \$3 billion of which in the U.S. Losses increased by 136% between December 2016 and May 2018.

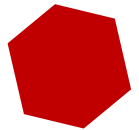
DEFINITION

Business E-mail Compromise (BEC)/E-mail Account Compromise (EAC) is a sophisticated scam targeting both businesses and individuals performing wire transfer payments.

The scam is frequently carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

The scam may not always be associated with a request for transfer of funds. A variation of the scam involves compromising legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees.¹

<https://www.ic3.gov/media/2018/180712.aspx>



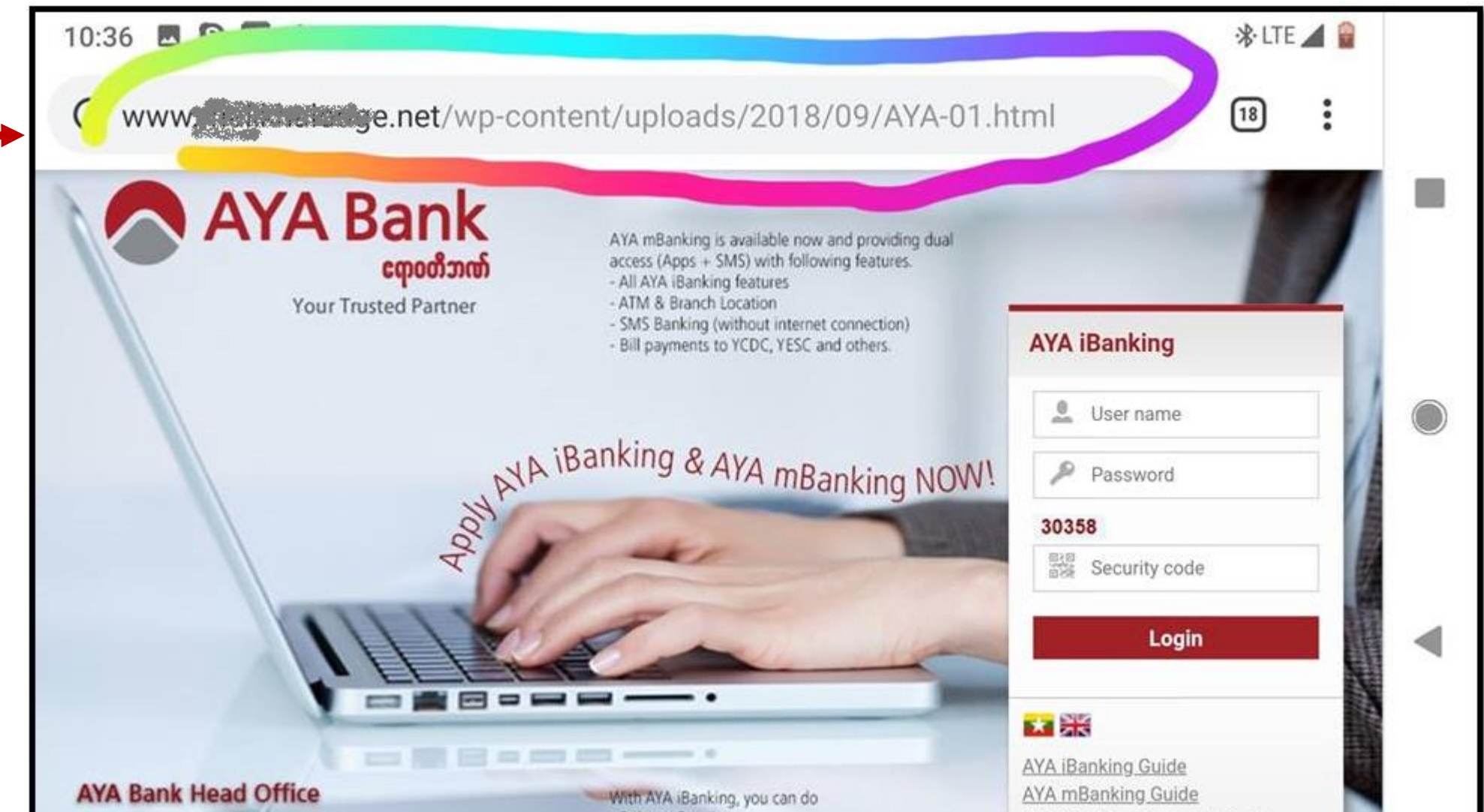
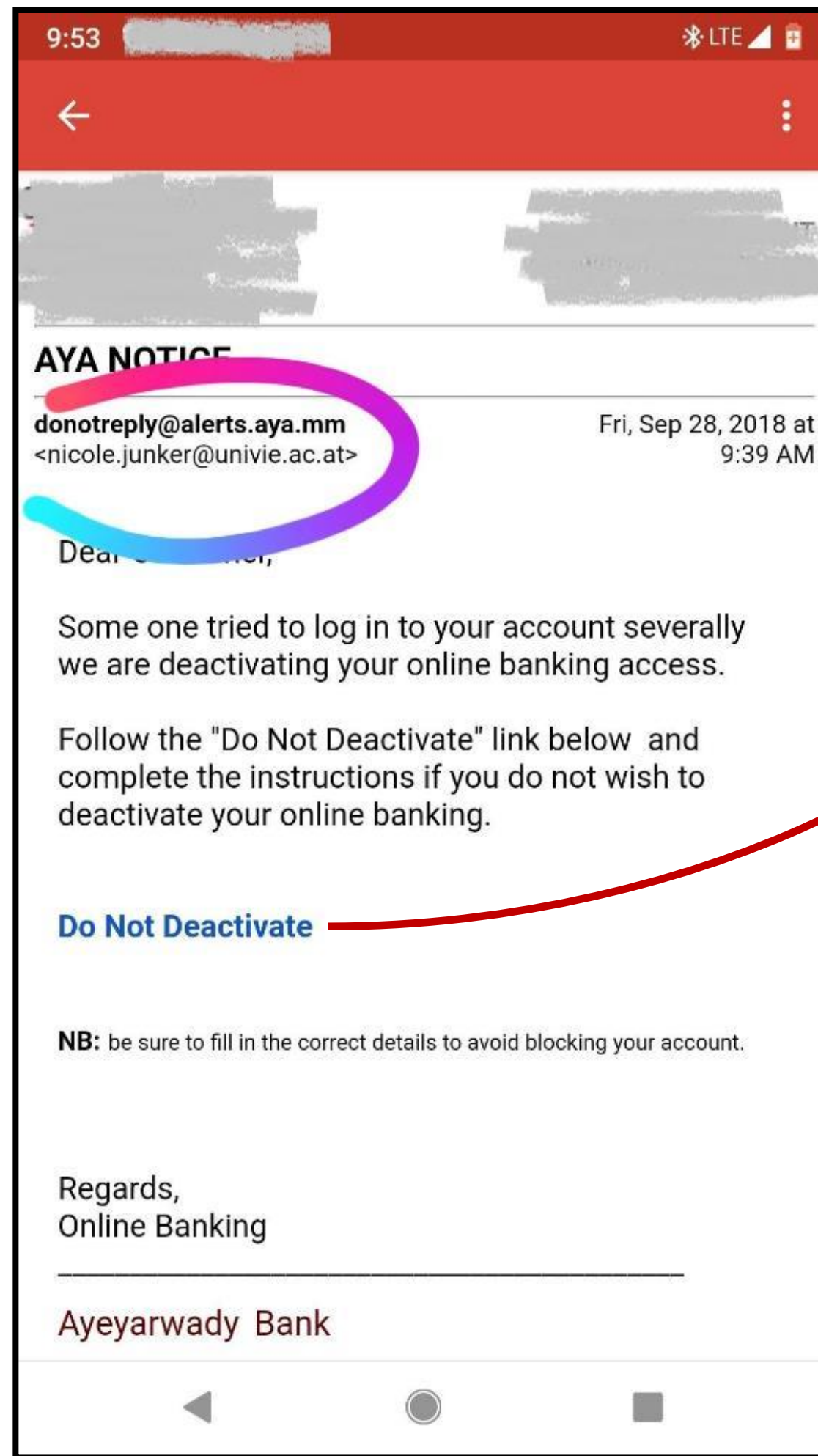
BEC Scam

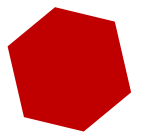
Most of the BEC scams in Myanmar are not reported.

Lost ranging from USD 10,000 to USD 500,000 per scam

<https://www.ic3.gov/media/2018/180712.aspx>

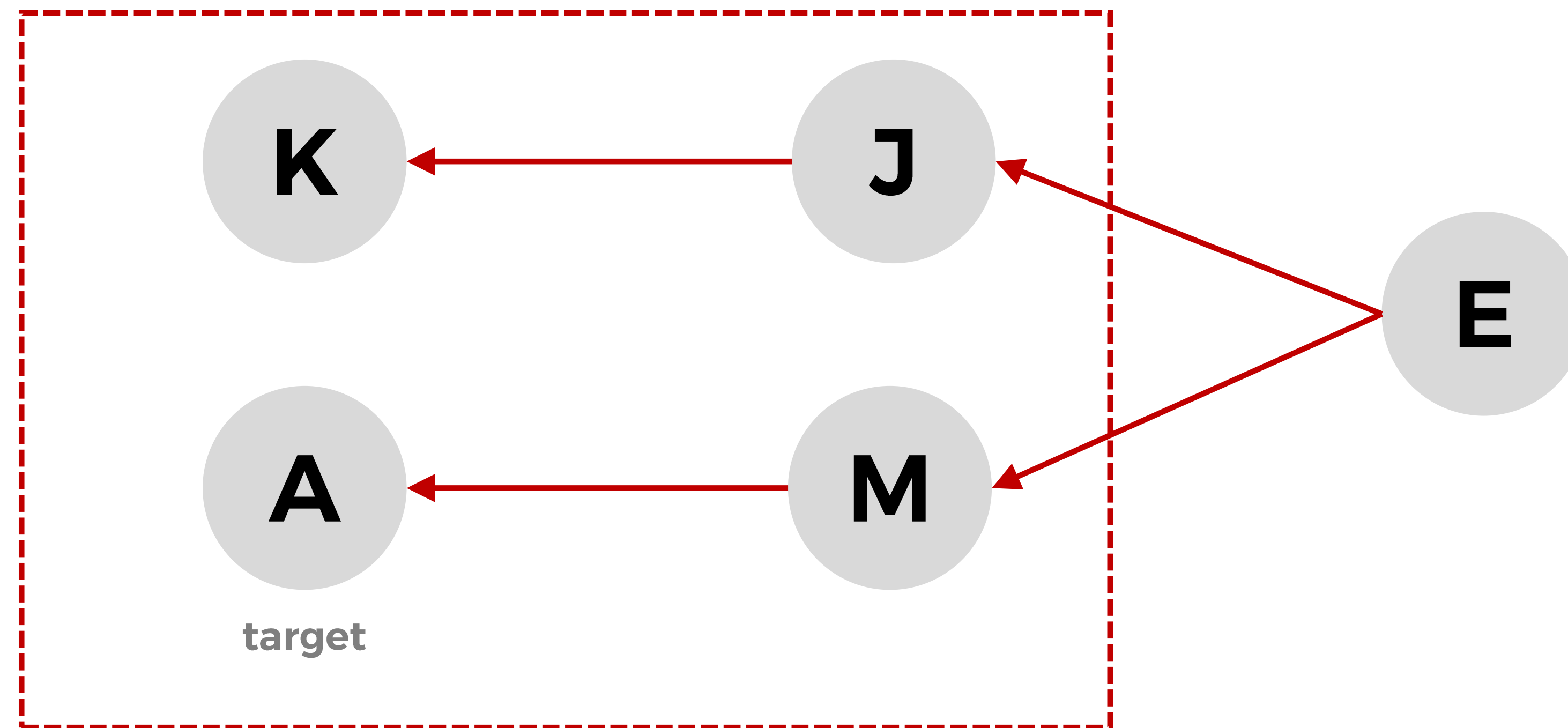
Phishing



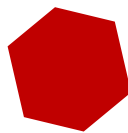


Phishing

Domestic /Foreign threat actors are targeting now Myanmar business



Myanmar Cyberspace



Fraud / Hack

Four foreigners hit with heavy prison terms over ATM fraud

Defendants arrive at Botahtaung Township court on Friday morning. (Teza Hlaing | Frontier)



By SU MYAT MON | FRONTIER

YANGON – Four foreigners have received heavy prison sentences after being convicted of using fraudulent pre-paid cards to withdraw millions of kyats from ATMs in Yangon.

British national Mr Niranjan Rasalingham received a 17-year prison term after being found guilty of a range of offences under the Penal Code, the 1947 Immigration Act and the Electronic Transactions Act.

His three Indian co-defendants were found guilty under the Penal Code and Immigration Act, and received sentences ranging from seven to nine years.

In announcing her verdict, the Botahtaung Township Court judge said the fraudulent ATM cards used to withdraw the money had been examined by the Singapore office of global payments company Visa. It had deemed them fake,

Two Nigerians withdraw money by hacking KBZ account of an economic adviser

Two Nigerian citizens hacked the KBZ Bank account of an economic adviser of a businessman and withdrew money on July 17, police confirmed on July 22.

The police however did not release details. According to initial reports, the adviser opened a case under section 66 (c) of the Telecommunications Law on July 19, one of the two hackers was arrested in Kamayut Township, Yangon, on July 21.

“It is true that money was withdrawn after the bank account had been hacked” the head of Mingalar Taungnyunt Township Police Force told the Daily Eleven.



Honorable Mentions

Fake News

- Lucky draw pages
- Like and Share

Cyber Bullying

- Few isolated cases leading physical and psychology harm

Online spread of hate speech

- Racial, Religious, Politics

Breach of Privacy

- Celebrities accounts, Sextortion

Myanmar Cyberspace: Exposures



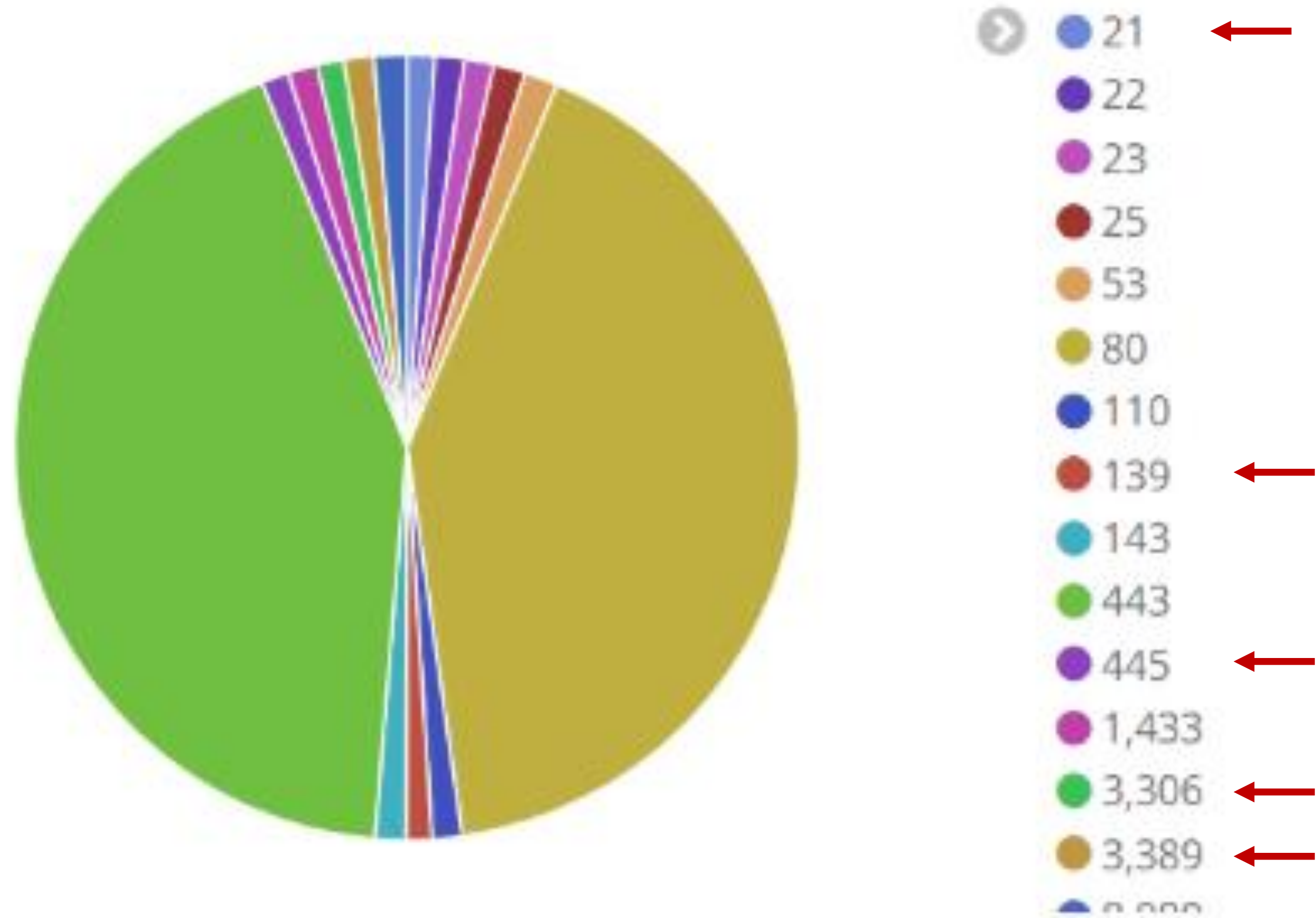
53,268

ip addresses

127,031

Internet
accessible
common
services

Myanmar Cyberspace: Exposures



Myanmar Cyberspace: Exposures

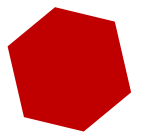
Filter: Hiding CSS and image content

#	Host	Method	URL	P
1	http://www[REDACTED].com	GET	/	
3	http://[REDACTED].anmar.com	GET	/wp-content/plugins/slidedeck2/js/jquery.easing...	
6	http://[REDACTED].anmar.com	GET	/wp-includes/js/jquery/jquery.js?ver=1.11.1	
9	http://[REDACTED].anmar.com	GET	/wp-includes/js/jquery/jquery-migrate.min.js?ve...	
11	http://[REDACTED].anmar.com	GET	/wp-content/plugins/daves-wordpress-live-sear...	
12	http://[REDACTED].anmar.com	GET	/wp-content/plugins/daves-wordpress-live-sear...	
13	http://[REDACTED].anmar.com	GET	/wp-content/plugins/ckeditor-for-wordpress/ck...	
14	http://[REDACTED].anmar.com	GET	/wp-content/plugins/daves-wordpress-live-sear...	
15	http://[REDACTED].anmar.com	GET	/wp-content/plugins/ckeditor-for-wordpress/in...	
16	http://[REDACTED].anmar.com	GET	/wp-content/plugins/ckeditor-for-wordpress/in...	
17	http://[REDACTED].anmar.com	GET	/wp-content/plugins/slidedeck2/js/jquery-mous...	
18	http://[REDACTED].anmar.com	GET	/wp-content/plugins/slidedeck2/js/slidedeck.jqu...	
19	http://[REDACTED].anmar.com	GET	/wp-content/plugins/slidedeck2/js/slidedeck-pu...	
24	http://[REDACTED].anmar.com	GET	/library/styles/images.css	

```
vulnresearch — bash — 127x35
[+] We could not determine a version so all vulnerabilities are printed out

[!] Title: W3 Total Cache 0.9.2.4 - Username and Hash Extract ←
Reference: https://wpvulndb.com/vulnerabilities/6621
Reference: http://seclists.org/fulldisclosure/2012/Dec/242
Reference: https://github.com/FireFart/W3TotalCacheExploit
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6079
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-6078
Reference: http://osvdb.org/92742
Reference: http://osvdb.org/92741
Reference: http://www.rapid7.com/db/modules/auxiliary/gather/wp_w3_total_cache_hash_extract
[i] Fixed in: 0.9.2.5

[!] Title: W3 Total Cache - Remote Code Execution ←
Reference: https://wpvulndb.com/vulnerabilities/6622
Reference: http://www.acunetix.com/blog/web-security-zone/wp-plugins-remote-code-execution/
Reference: http://wordpress.org/support/topic/pwn3d
Reference: http://blog.sucuri.net/2013/04/update-wp-super-cache-and-w3tc-immediately-remote-co
sclosed.html
Reference: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2010
Reference: https://secunia.com/advisories/53052
```



Myanmar Cyberspace: Exposures

```
$>nc 23

CCCC
*****
                                NOTICE TO USERS

This system is the private property of ██████████ Bank ,Ltd
It is for authorized use only. Users (authorized or unauthorized) have no explicit
or implicit expectation of privacy.

Any or all uses of this system and all files on this system may be intercepted,
monitored, recorded, copied, audited, inspected, and disclosed to your employer,
to authorized site, government, and law enforcement personnel, as well as authorized
officials of government agencies, both domestic and foreign.

By using this system, the user consents to such interception, monitoring, recording,
copying, auditing, inspection, and disclosure at the discretion of such personnel or
officials. Unauthorized or improper use of this system may result in civil and criminal
penalties and administrative or disciplinary action, as appropriate.

By continuing to use this system you indicate your awareness of and consent to these
terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions
stated in this warning.

*****

User Access Verification

Username:
$>
```

MM-WRK2014-0505	10.95.6.143
MM-WRK2013-0501	10.95.6.90
16-ph-g	10.95.6.114
IT-WRK2013-0100	10.95.6.103
android-4b819a90dfd2dddc	10.95.6.124
IT-WRK2014-0040	10.95.6.121
MM-WRK2014-1001	10.95.6.118
IT-WRK2014-0038	10.95.6.100
android-e047575ebcb9985d	10.95.6.102
android-997fd07c0d601572	10.95.6.87
IT-WRK2014-0030	10.95.6.142
MM-WRK2013-0503	10.95.6.159
MM-WRK2014-0039	10.95.6.246
MM-WRK2014-0509	10.95.6.242
IT-WRK2013-0046	10.95.6.244
IT-WRK2013-0096	10.95.6.248
IT-WRK2013-0102	10.95.6.245
MM-WRK2014-1002	10.95.6.249
MM-WRK2013-0510	10.95.6.241
MM-WRK2014-0506	10.95.6.247
IT-WRK2012-0191	10.95.6.97
switch4a88ba	10.95.6.101
switch43a799	10.95.6.164

https://my.policy



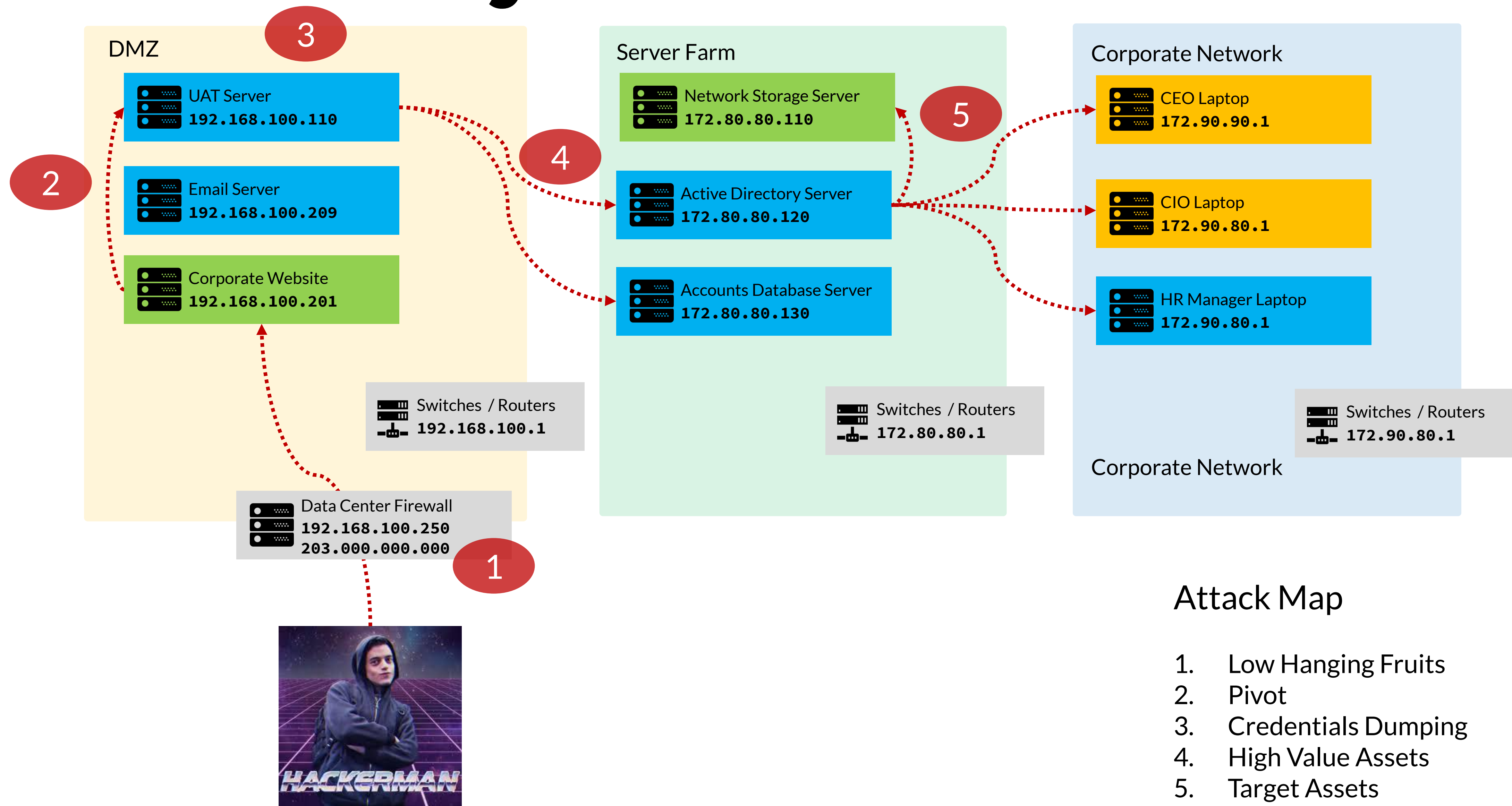
Secure Logon
for F5 Networks

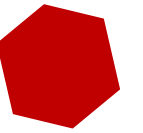
Username

Password

Logon

Cyber Intrusion





Cyber Security

to

protect

detect

respond

via

people

process

technology

preserve

confidentiality

integrity

availability



People : Workforce

Not sizable industry

- Shortage of job opportunities

Shortage of skilled professionals

- At least for the local skilled professionals

People : Consumers

Low level awareness

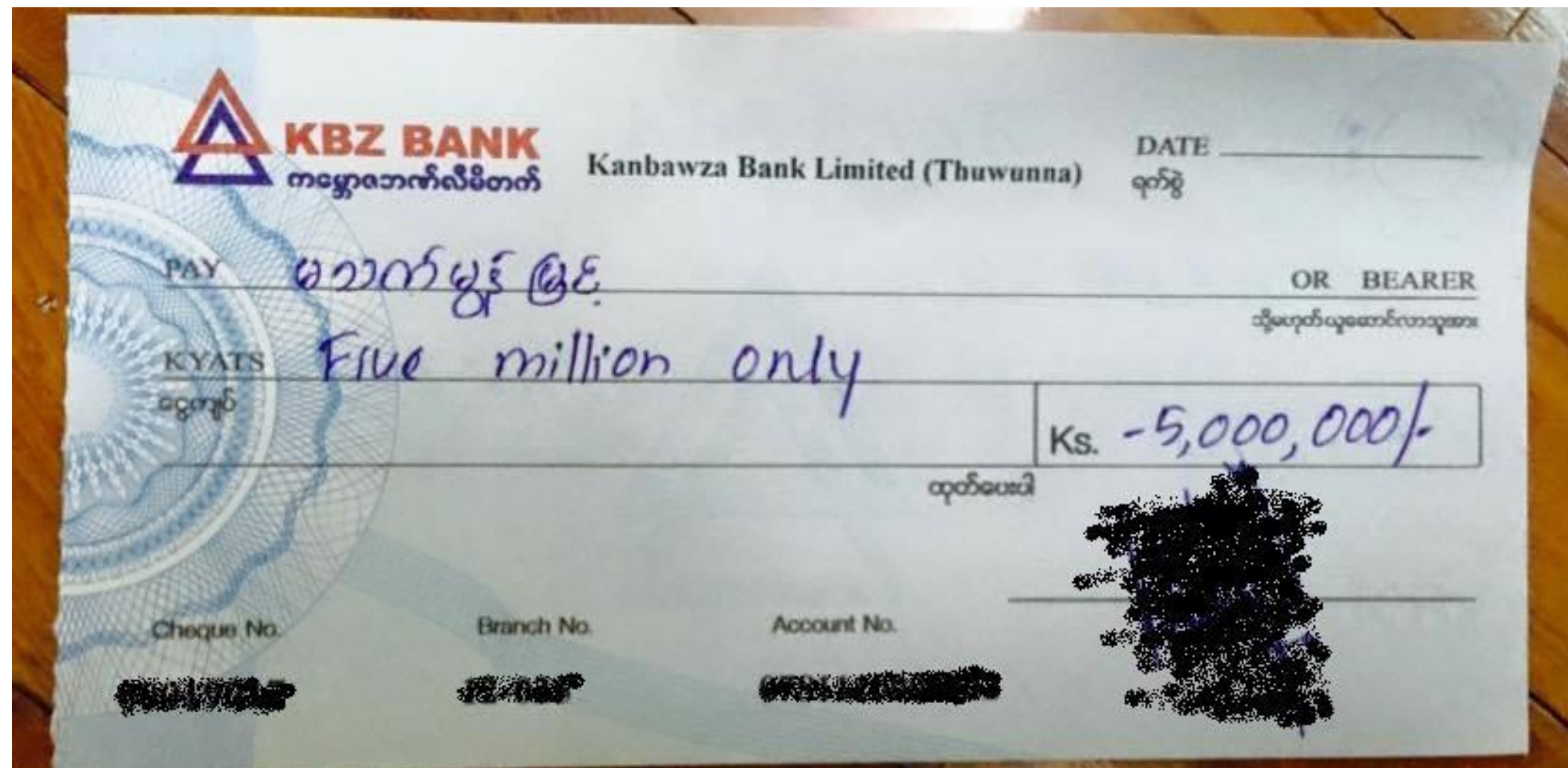
- Oblivious to common online safety measures
- Vulnerable to social engineering attacks



People : Consumers

Culture?

- Respect for own or other privacy



People



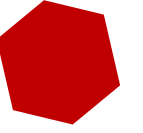
Cyber security conferences



Skilled based cyber security training programs



Awareness Campaigns



Process

No industry regulation on cyber security (yet)

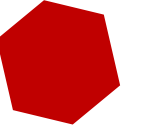
- Banking
- Telecommunication
- Internet Service Providers
- Online services



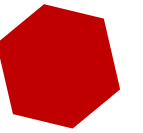
Process : Example Regulation

- Board of Director and Senior Management accountability for Risk Management
- IT Security Awareness
- Technology Risk management Framework
- IT Service Management
- Reliability, Availability and Recoverability
 - BCP
- Security Monitoring
 - Real-time monitoring capacity (24/7)
- Security Testing
 - Annual Penetration Testing

Process : Example Regulation



- Must implement process and framework to identify critical system
- Maximum of
 - unscheduled downtime 4 hours per annum
- Upon system failure
 - Recovery Time Objective (RTO) less than 4 hours
- For each incidents
 - Notification to authority in 60 minutes
 - Root cause and business impact analysis in 14 days



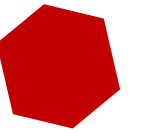
Process : ISO

- To guide organizations of all size and industry to build Information Security Management System (ISMS) or information security program
- Formerly British Standard 7799 (BS7799)
- Contains series of documents (guides) for organizations to follow to implement ISMS
- ISO 27001: General Requirement
 - The most common of ISO 27000 series
- Per typical ISO implementation
 - Implementation (Usually Consulting, Third Party Assisted)
 - Third Party Auditing and Certification
- ISO 27015: Financial Sector



Process : NIST CSF

- The newest and the most recent framework
 - 2018
- Originally to improve critical infrastructure cybersecurity
 - 16 sectors per US DHS
 - Financial services, telecommunication, electricity generation, water supply and etc.
- Vendor neutral
 - No compliance, No Certification
 - Ideal Self assessment tools
 - **Free**
- Consists of Three Parts:
 - Framework Core
 - Framework Profile
 - Framework Implementation Tiers



Process : CIS

Critical Security Controls

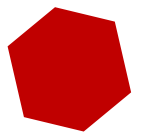
- Informed by **real world** attacks
- Developed by **global communities**
 - ASD 35 Mitigation Strategies is the Australian counter part
- Align with top compliance frameworks

Objectives

- Block initial compromise
- Address detection
- Disruption attackers objectives

Effectiveness

- First 5 controls (claims to) deter 85% of cyber attacks



Technology

Prevention Oriented

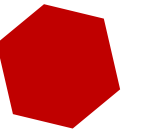
- Aka traditional defense

Preventive
Firewall – NGFW
Minimize Administrative Privilege
Antivirus
Patching
Network segmentation

Detective
Intrusion Detection
Account Monitoring
Incident Response
Regular log review
Lateral Movement Detection

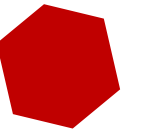
Prevention and detection controls are not mutually exclusive

Technology : Trend



Legend

EPP : Endpoint Protection
NGFW: Next Generation Firewall
SIEM: Security Information Event Management
EDR: Endpoint Detection and Response



Conclusion

Risk

- Threat actors both domestic and foreign are targeting Myanmar business

Challenges

- Lack of resources, regulations and guidelines

Opportunities

- Learn and adopt suitable tools

Thank you!



+959 500 9560



ye.tt@kernellix.com