

Cyber Threat Intelligence: Where Should You Start?

National Cyber Security Congress

Presented by: [Alyssa Berriche](#)

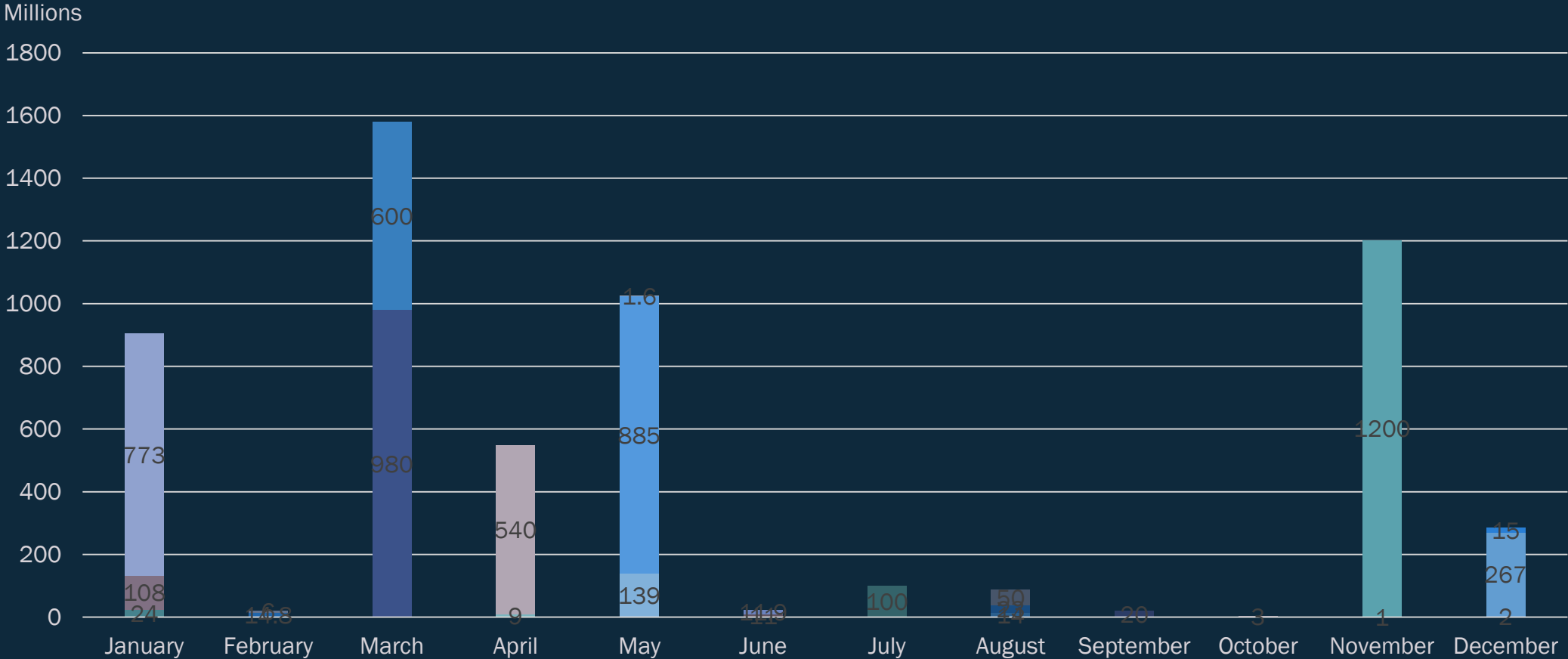
Introduction







Most impacting breaches of 2019



- Wyze
- Unicredit
- Capital One
- AMC Networks
- 500px
- Facebook
- Novaestrat
- Emuparadise
- Bodybuilding
- Coffee meets bagels
- LifeLabs
- Hostinger
- Quest Diagnostics
- Facebook2
- Ascension
- T-Mobile
- Cafepress
- Canva
- Verifications.io
- Betting sites
- LDP
- Poshmark
- First American
- Facebook3
- Collection #1

Modern problems



This year organizations and individuals will pay approximately \$11.5 billion because of ransomware.



24,000 malicious apps are blocked every day.



76% of businesses reported being a victim of a phishing attack in the last year.

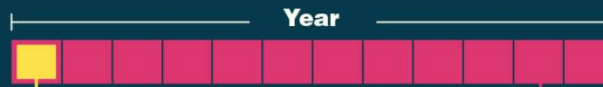
(Wombat Security, 2019)



As much as **38% of malware** is now being disguised as a Word doc.



Cryptojacking



5-8 million attempts per month

Around 96 million attempts per year



Global Cost of Malware



2015 2019 2021



Your home network or business still isn't prepared for a cyberattack.

- The purpose of **threat intelligence** is to provide a deep and accurate analysis of the cyberthreats, to help companies counter them.

WHY?



Keep your friends close but your
enemies closer.

The Godfather Part II

Who needs Threat Intelligence



Because “Security is everyone’s concern and responsibility”

Benefits of Threat Intelligence

- Useful for companies struggling with skills shortage
 - Because it helps reducing number of alerts, false positives
- Provides context about emerging threats
 - Resilience
 - Improve ability to defend against cyberattacks
- Helps decision makers to prioritize response, or investments in technology and people
- Faster response to threats

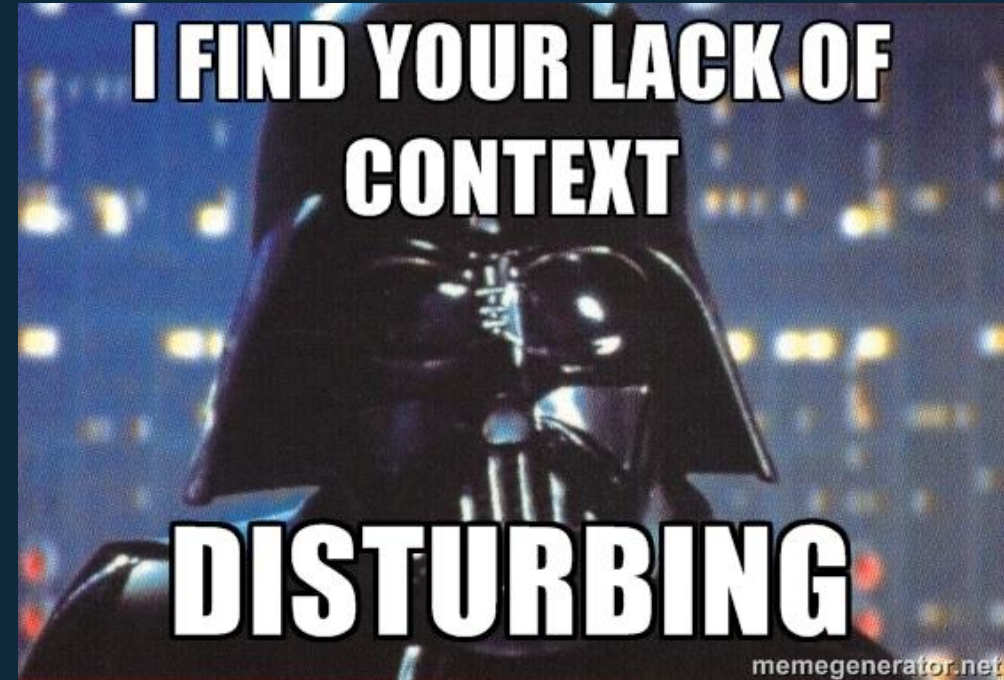
Threat Intelligence for Incident Response

- Reducing false positives
- Enriching alerts with real-time context, like custom risk scores
- Comparing information from internal and external sources

→ Faster identification of threats

Use case 1: reactive hunting

- Based on alerts and detections
- Extract indicators and enrich them with context
- Create your TTPs
- Understand your adversaries
- Hunt for additional IOCs



Use case 2: uncovering hidden attacks

- Search for relevant emerging threats shared by different sources (ISACs, CERTs, vendors, researchers, ...) in your environment



Threat Intelligence for Vulnerability Management

Patch everything, All the time



Patch prioritizing based on risk

Use case: WannaCry

- WannaCry propagated through EternalBlue exploit, developed by US National Security Agency (NSA) and exposed/ released by Shadow Brokers after the MS17-010 patch

Security Patch for MS17-010

- March 14, 2017

Wannacry attack

- 12-15 May 2017

Shadow Brokers released Eternalblue

- April 14, 2017

Threat Intelligence for Fraud Prevention

- Monitoring sources like criminal communities, paste websites and forums for relevant banking information
- Monitoring for compromised data from forums, underground marketplaces, pastes, leaked combos lists,...
- Monitoring for domains and website mimicking official ones to steal credentials, sell counterfeit, promote fake deals, ...

Use case 1: Banking information

BIN: 517065xxxxxxxxxxx	BINS:	530562022081xxxx	Bin : 4895042851xxxxxx
IP: USA us	455255029xxxxxxxx 10/19 312	08/24	IP Paypal - Philippines PH
ZIP: 10004	547046700883xxxx 01/21/532	Ip india	Street 242xx
Works on:	IP: MEXICO	Browser: firefox	Street 9xxx
NAPSTER	4266841425xxxxxx 060/18 238 i	Vpn: express vypr hma	Cavite
TIDAL	KING OF BINS @kingofbin · D	Netflix	State - Cavite
CRUNCHYROLL	BIN ALI EXPRESS	JUST IPHONE	Zip: 1216
NORDVPN	BIN : 411079160716xxxx	BIN SCRIBD VIA PAYPAL	Phone: 39201xxxxx
PRIME VIDEO	DATE : 08/23	BIN : 439129xxxxxxxxxxx	ID: 688xxxx
VIRTUAL SHIELD	CVV : xxx	ip : np ip	BIN DEEZER PREMIUM 3 MONTH
	IP USA	-----	BIN : 5454863242xxxxxx
	ALIEXPRESS BIN (Not tested if wor	Paypal info :	DATE : 11/24
	(GET LIVES FROM FANATICS or CC CHECK	Country : Nepal	
	4852460115xxxxx8 12/23	Street : Street xxxx	
	State : Texas	City : Nepal	
	Zip : 75701	State : Any	
	Country :USA	Phone : 55xxxxxx	
	Phone : 903910xxxx		

Use case 2: Compromised data

```
----- [ 1 ] -----  
  
Email : rashidab[REDACTED]@gmail.com  
Pass : sc[REDACTED]  
Combo : rashidab[REDACTED]@gmail.com:sc[REDACTED]  
Expires in (Days) : 50 Days  
Expires in (Date) : 2020-02-14  
NordVPN Checker | by xRisky  
  
----- [ 2 ] -----  
  
Email : lain[REDACTED]@yahoo.com  
Pass : Mama[REDACTED]  
Combo : lain[REDACTED]@yahoo.com:Mama[REDACTED]  
Expires in (Days) : 6 Days  
Expires in (Date) : 2020-01-01  
NordVPN Checker | by xRisky
```


```
=====AVAST-ANTIVIRUS=====  
COMBO: p.[REDACTED]hotmail.com:[REDACTED]  
CORREO: p.[REDACTED]hotmail.com  
CONTRASEÑA: luke[REDACTED]  
SUBSCRIPTION: ACTIVADA  
SERIAL: B89[REDACTED]-7S[REDACTED]-44[REDACTED]
```

```
pr[REDACTED]do@gmail.com:pi[REDACTED]  
ki[REDACTED]12@gmail.com:Ye[REDACTED]  
al[REDACTED]ay@gmail.com:hc[REDACTED]  
[REDACTED]!k@yahoo.com:kej[REDACTED]  
mc[REDACTED]x@gmail.com:sr[REDACTED]  
de[REDACTED]0@gmail.com:dai[REDACTED]  
be[REDACTED]ls@gmail.com:B[REDACTED]  
c[REDACTED]321@gmail.com:La[REDACTED]3  
t[REDACTED]n@yahoo.com:Sl[REDACTED]1  
ce[REDACTED]1@hotmail.com:nc[REDACTED]1  
den[REDACTED]3@outlook.com:sv[REDACTED]99  
m[REDACTED]ill@hotmail.fr:k[REDACTED]a  
gu[REDACTED]an@yahoo.com:me[REDACTED]  
ca[REDACTED]s@gmail.com:C[REDACTED]  
tir[REDACTED]@web.de:ki[REDACTED]4  
jac[REDACTED]l@hotmail.com:pe[REDACTED]  
lyr[REDACTED]ar@yahoo.com:Un[REDACTED]  
n[REDACTED]08@yahoo.com:ise[REDACTED]
```

```
Steph[REDACTED]3@yahoo.com:Lin[REDACTED] | Subscription =  
anime|drama|manga  
yule[REDACTED]@gmail.com:Ba[REDACTED] | Subscription =  
anime|drama|manga  
cra[REDACTED]hotmail.com:Wir[REDACTED] | Subscription =  
anime|drama|manga  
sta[REDACTED]@gmail.com:Hiç[REDACTED] | Subscription =  
anime|drama|manga  
logar[REDACTED]n@icloud.com:Fir[REDACTED] | Subscription =  
anime|drama|manga  
zkn[REDACTED]@yahoo.com:Zk[REDACTED] | Subscription =  
anime|drama|manga  
k[REDACTED]@gmail.com:Rur[REDACTED] | Subscription =  
anime|drama|manga  
luisd[REDACTED]l@gmail.com:Ld[REDACTED] | Subscription =  
anime|drama|manga  
just[REDACTED]@gmail.com:Gho[REDACTED] | Subscription =  
anime|drama|manga
```

































Use case 3: typosquatting

Details

 domains from various malware, phishing or counterfeiting black lists that may interfere with **PayPal, Inc.** brand or trademarks

active domains

inactive domains

URL	Server	Location / Server IP	Domain Registry	Created
 https://ftp.service-invest...		 91.216.107.198	LIGNE WEB SERVICES - LWS	06.01.2020
 https://shulovmarket.xyz...	 	 72.9.152.26	XYZ.COM LLC	06.01.2020
 https://paypallimited.ser...	 	 67.207.91.187	TLDS L.L.C. d/b/a SRSPlus	05.01.2020
 https://paypallimited.serveirc.com/signin/login.php	 	 177.52.181.15	Churrascaria Mein Haus Ltda - ...	05.01.2020
 https://saradesh24live.c...	 	 198.54.116.167	NameCheap, Inc.	05.01.2020
 https://ytmp3converts.c...	 	 199.188.206.58	GoDaddy.com, LLC	04.01.2020
 https://paypal.re		 52.58.78.16	TLD Registrar Solutions Ltd	04.01.2020
 http://paypal-198390927...		 81.88.52.22	Register SPA	04.01.2020
 http://vire0002.000web...		 145.14.144.90	Hostinger, UAB	03.01.2020

Threat Intelligence for Leadership and Decision Makers

- Helps identifying and understanding the nature of the risk including emerging threats
 - Which attacks are becoming more/less frequent
 - Which kind of threat actors are expected
 - Which assets are most targeted
- Optimized investments to enhance defensive measures

My Course on « Cybrary.it »





THANK YOU

