

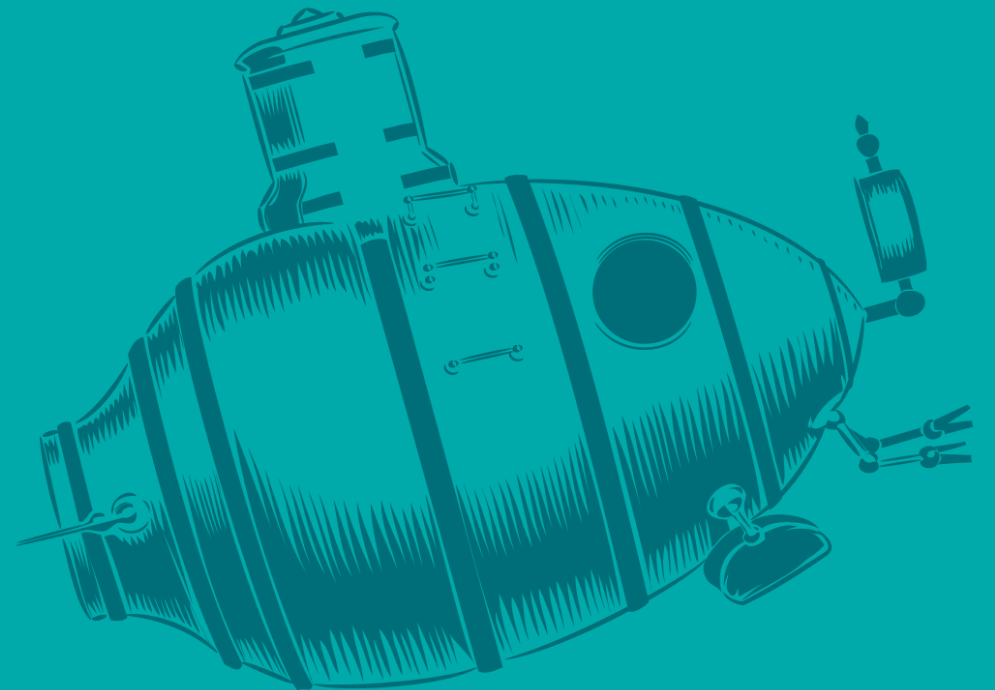


Bezpečnostní hrozby v roce 2019

Jan Kopřiva













































jan.kopriva@alef.com







ALEF CSIRT



TLP: WHITE

Pohled do historie

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware		1. Malware		
2. Web Based Attacks		2. Web Based Attacks		
3. Web Application Attacks		3. Web Application Attacks		
4. Phishing		4. Phishing		
5. Spam		5. Denial of Service		
6. Denial of Service		6. Spam		
7. Ransomware		7. Botnets		
8. Botnets		8. Data Breaches		
9. Insider threat		9. Insider Threat		
10. Physical manipulation/ damage/ theft/loss		10. Physical manipulation/ damage/ theft/loss		
11. Data Breaches		11. Information Leakage		
12. Identity Theft		12. Identity Theft		
13. Information Leakage		13. Cryptojacking		NEW
14. Exploit Kits		14. Ransomware		
15. Cyber Espionage		15. Cyber Espionage		

Legend: Trends:  Declining,  Stable,  Increasing
 Ranking:  Going up,  Same,  Going down

Útoky s využitím dodavatelského řetězce

ars TECHNICA

BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE S

ANDY GREENBERG SECURITY 07.07.17 10:00 AM

THE PETYA PLAGUE EXPOSES THE THREAT OF EVIL SOFTWARE UPDATES

malware in that CCleaner

backdoor signed with its own certificate.

ASUS Live Update Infected with Backdoor in Supply Chain Attack

By [Sergiu Gatlan](#)



March 25, 2019



12:35 PM



1

Socioinženýrské útoky

24% of incidents reported to BBR Services in 2018 were business email compromise



po 21.01.2019 7:21

Anonymous Hacker - Magen <magen_691@j.anonymouswatchers.gq>

Hello,

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Phantom Squad

Your network will be DDoS-ed starting Sept 30st 2017 if you don't pay protection fee - 0.2 Bitcoin @ [removed].

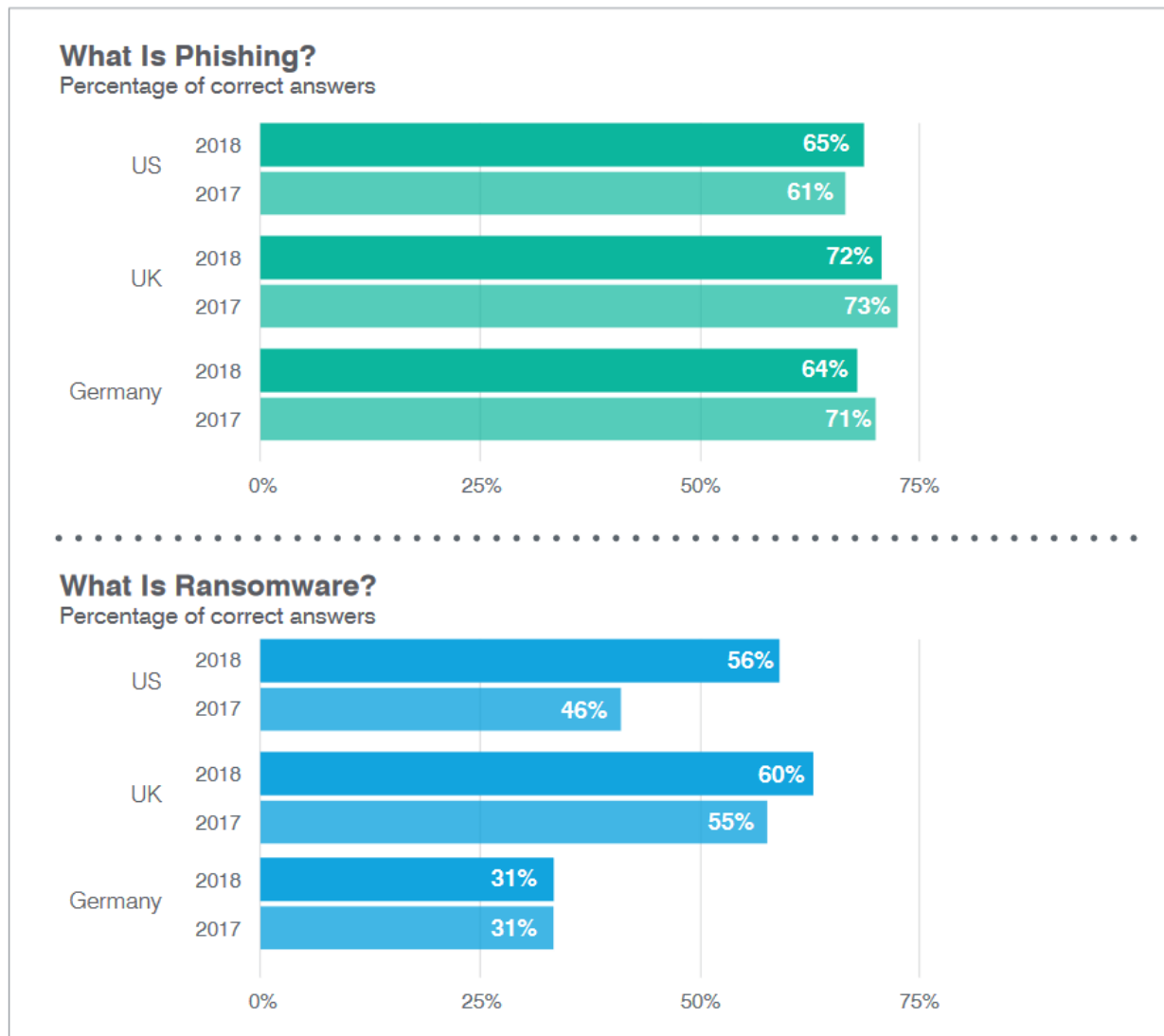
If you don't pay by Sept 30st 2017, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

This is not a joke.

If you want me to delete both files and keep your secret, you must send me Bitcoin payment. I give you the last 72 hours.
If you don't know how to send Bitcoins, visit Google.

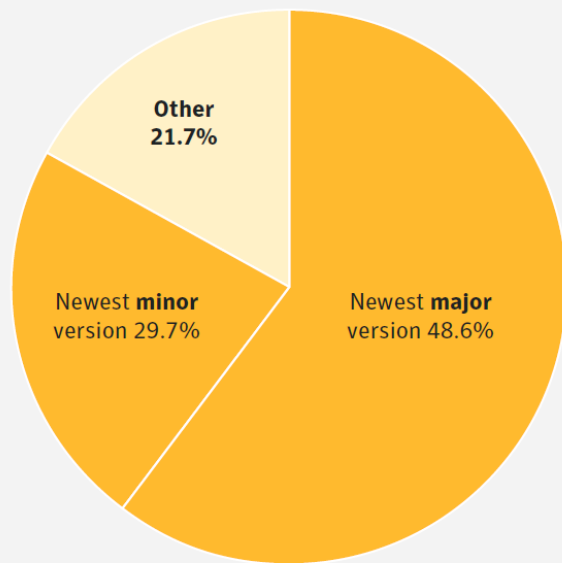
Send 2000 USD to this Bitcoin address immediately:

Uživatelská neznalost



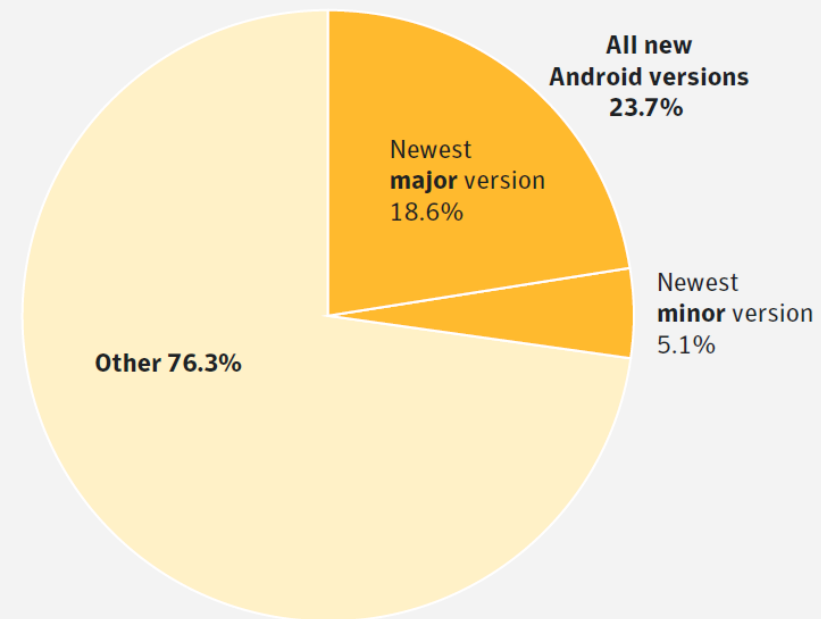
Nedostatečné záplatování

DEVICES RUNNING NEWEST IOS VERSION (YEAR)



All new iOS versions 78.3%

DEVICES RUNNING NEWEST ANDROID VERSION (YEAR)



Lidské pochybení

Misconfiguration Exposes 198 Million American Voter Records

by [Varun Badhwar](#) | 06.20.17, 12:26 AM

21 Facebook stored hundreds of millions of user
MAR 19 Passwords in Plain Text for Years

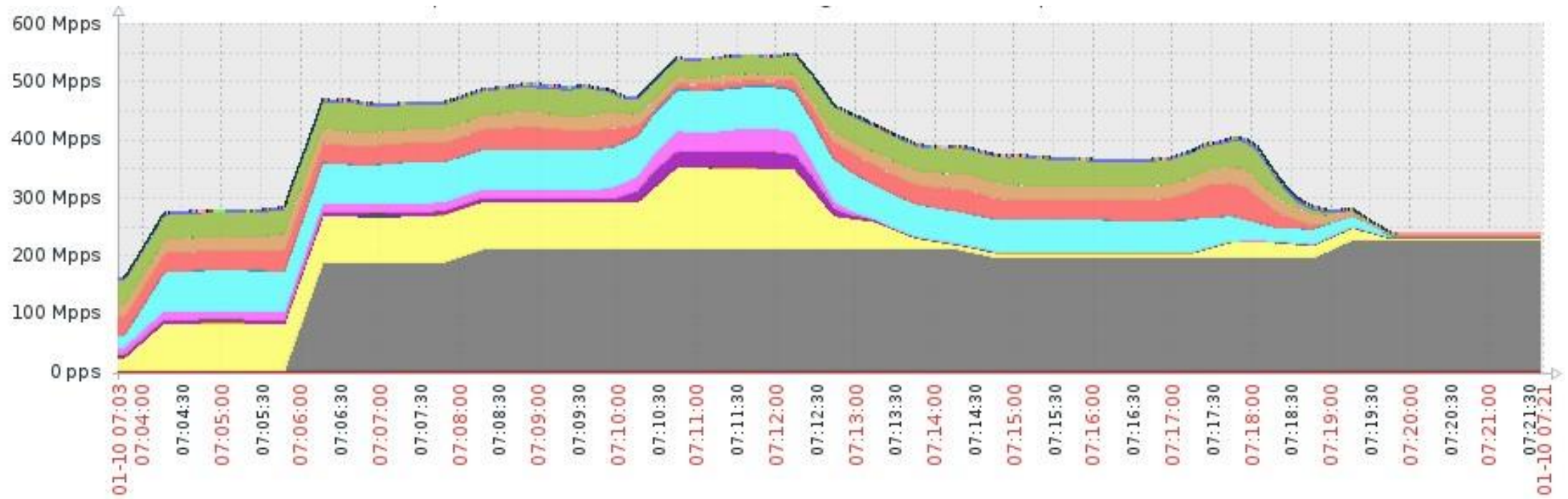
Twitter says bug exposed user plaintext passwords

Change your passwords — immediately.

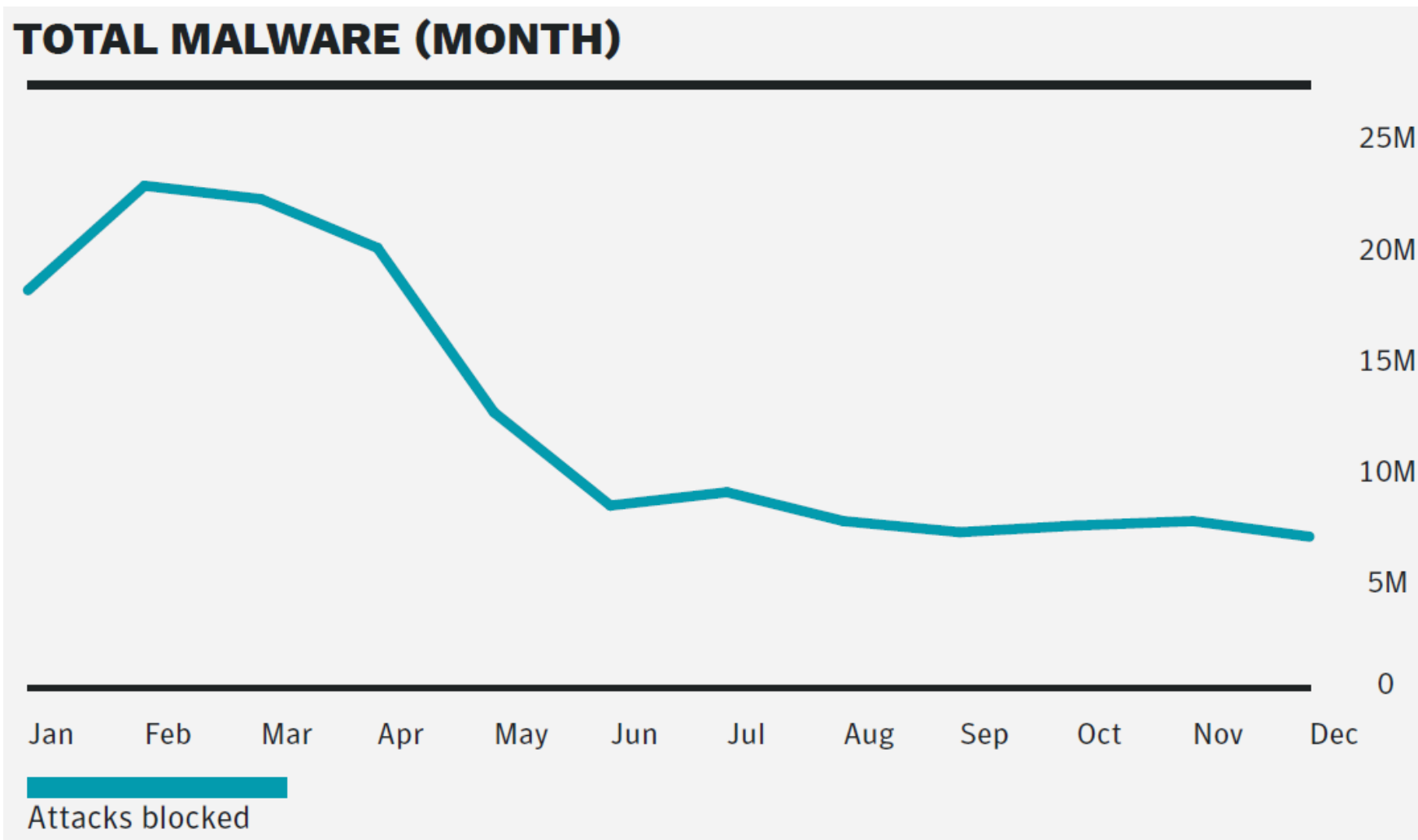


By [Zack Whittaker](#) for [Zero Day](#) | May 3, 2018 -- 20:23 GMT (21:23 BST) | Topic: [Security](#)

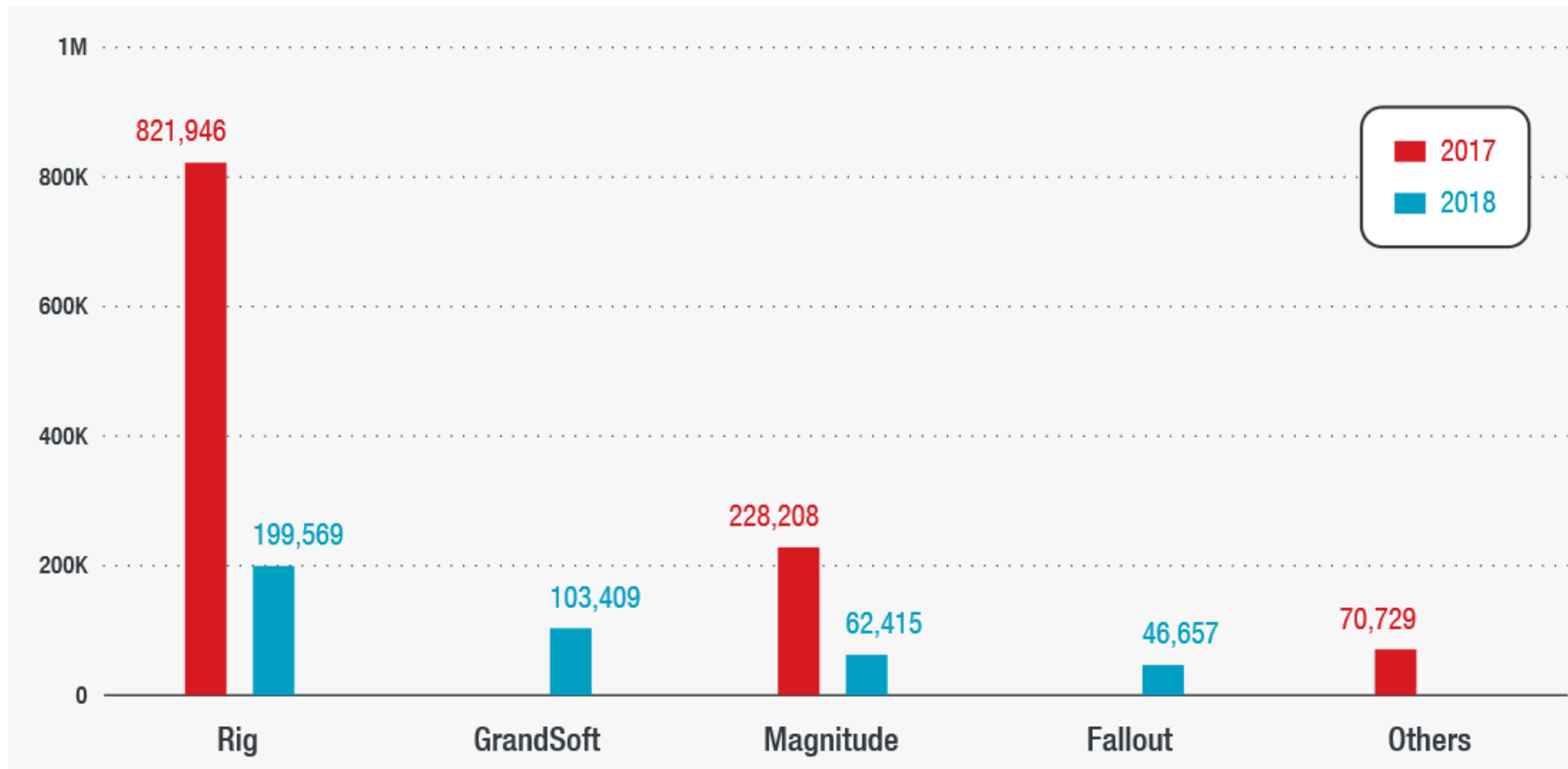
DDoS



Malware

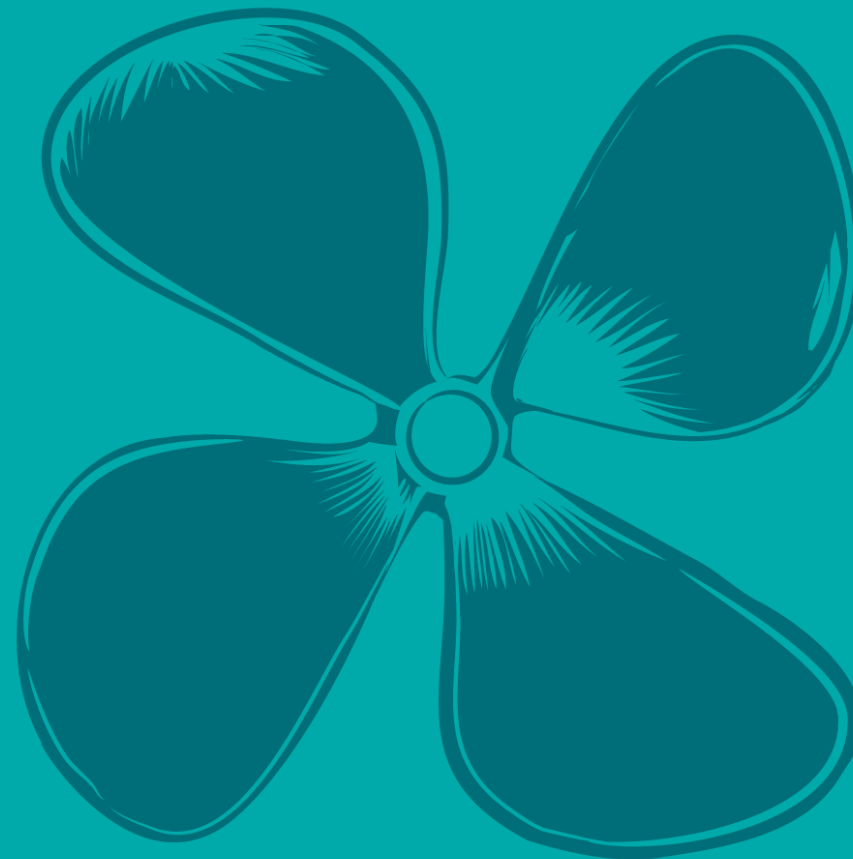


Co nás bude (snad) trápit méně?



ALEF

**Děkuji Vám za
pozornost**



TLP: WHITE