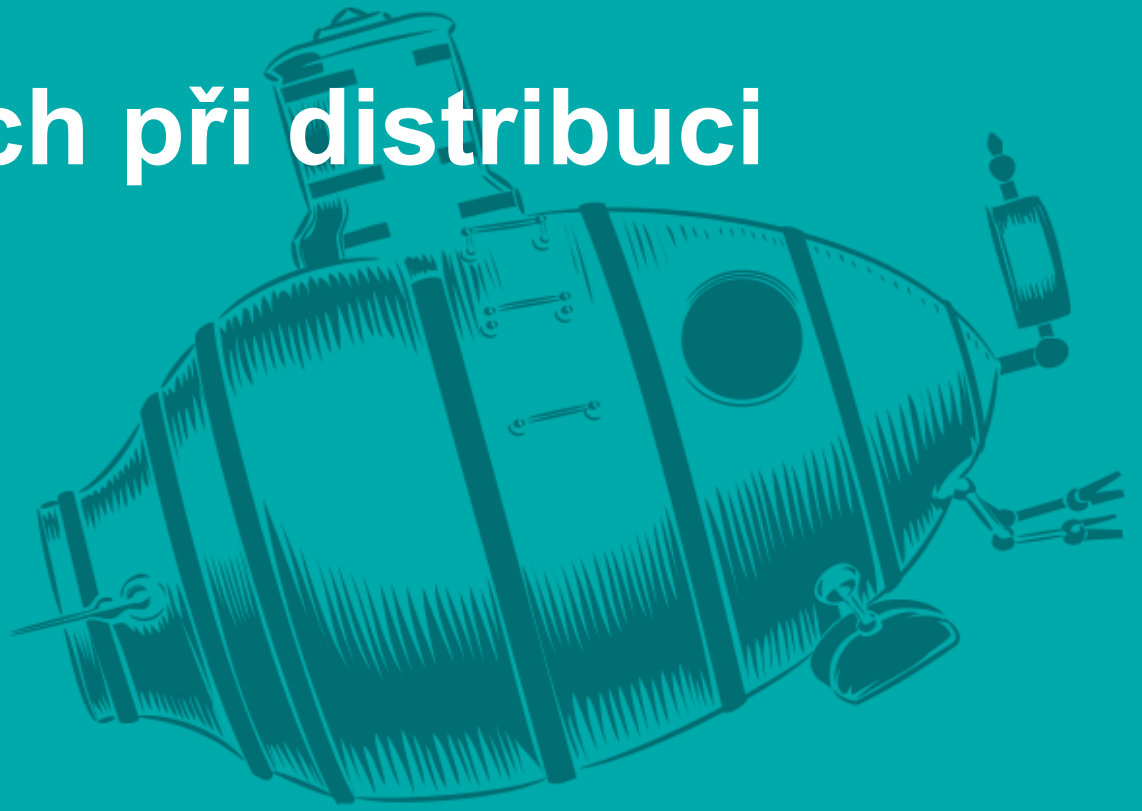
ALEF

Vývoj technik užívaných při distribuci ransomwaru

...a jak na něj efektivně reagovat



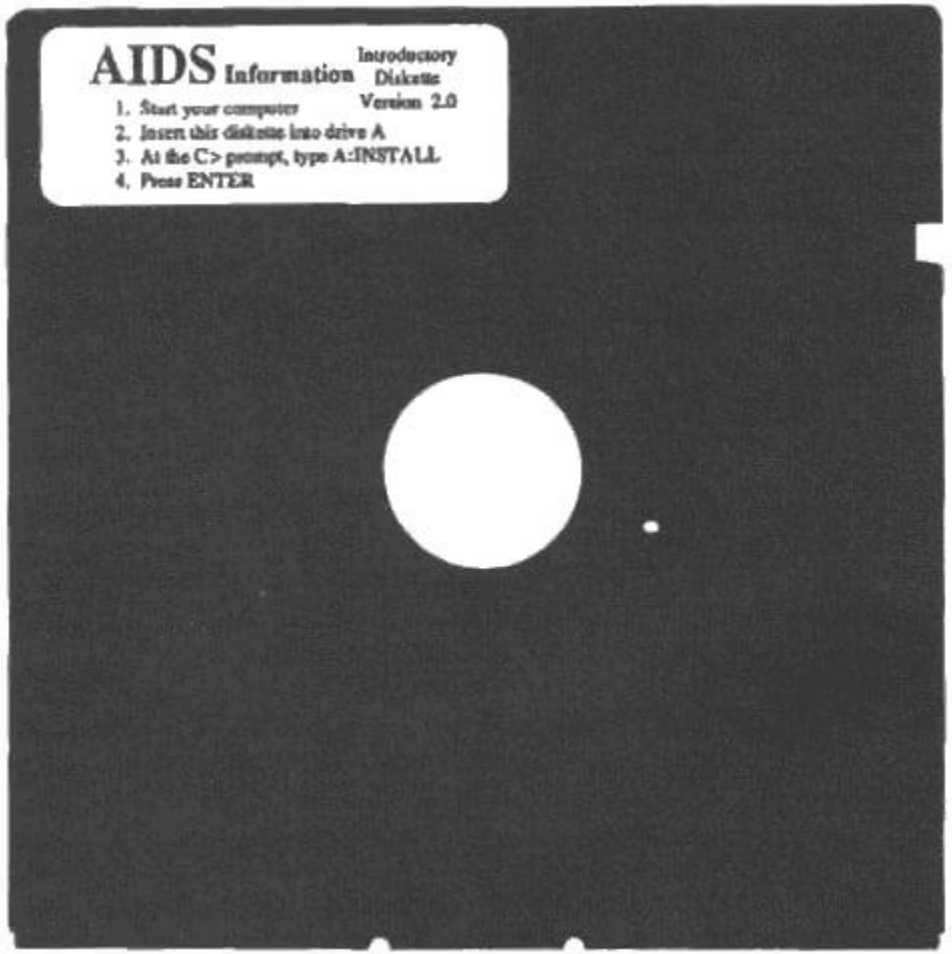
Jan Kopřiva

jan.kopriva@alef.com @jk0pr

ALEF CSIRT

TLP: WHITE

Kde ransomware začal?



ALEF

Kde ransomware začal?

Corporation. These programs are provided for your use as described above on a leased basis to you; they are not sold. You may choose one of the following types of lease (a) a lease for 365 user applications or (b) a lease for the lifetime of your hard disk drive or 60 years, whichever is the lesser. PC Cyborg Corporation may include mechanisms in the programs to limit or inhibit copying and to ensure that you abide by the terms of the license agreement and to the terms of the lease duration. There is a mandatory leasing fee for the use of these programs; they are not provided to you free of charge. The prices for "lease a" and "lease b" mentioned above are US$189 and US$378, respectively (subject to change without notice). If you install these programs on a microcomputer (by the install program or by the share program option or by any other means), then under the terms of this license you thereby agree to pay PC Cyborg Corporation in full for the cost of leasing these programs. In the case of your breach of this license agreement, PC Cyborg Corporation reserves the right to take any legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use of the programs. These program mechanisms will adversely affect other program applications on microcomputers. You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement: your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally. Warning: Do not use these programs unless you are prepared to pay for them. You are strictly prohibited from sharing

Source: https://omgcybersecurity.co.uk/

Kde ransomware začal?

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed INVOICE, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

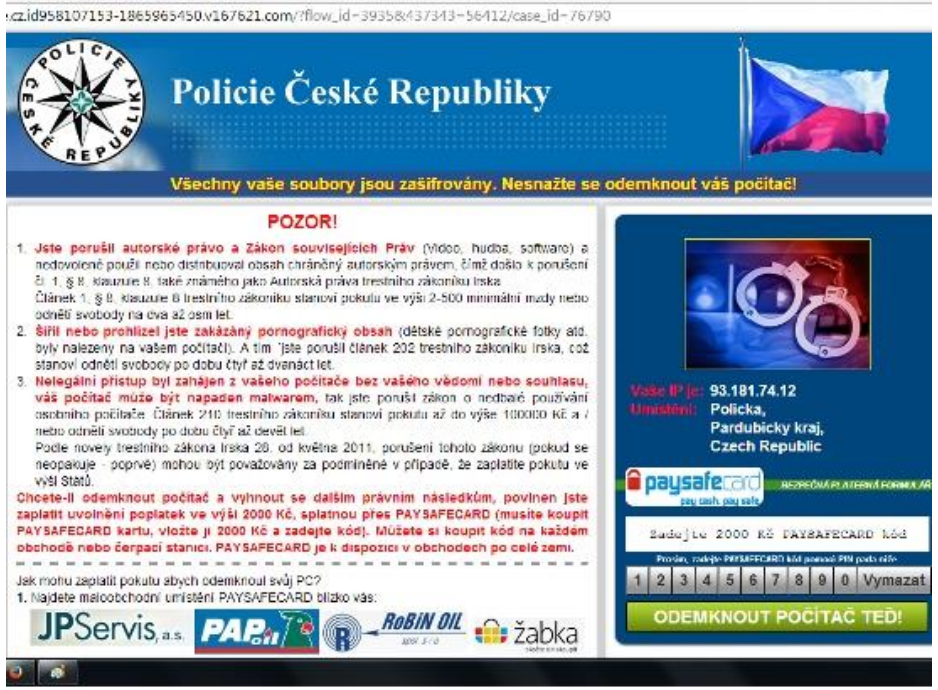
Important reference numbers: A5599796-2695577-

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashier's check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

Jaké bylo pokračování?

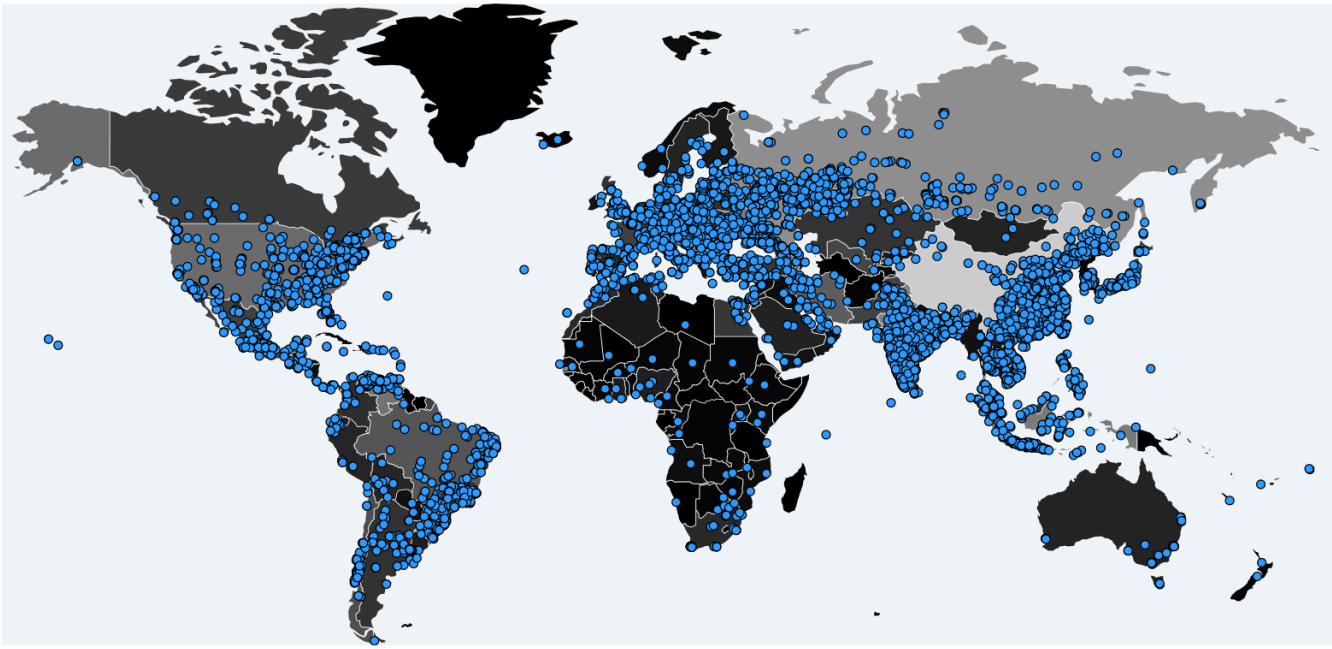
- Od roku 2005 souborový krypto-ransomware
  - E-mail, distribuce na „boty“
- Od 2010 „lockery“
  - Exploit kity
- Od 2013 „moderní“ necílený ransomware
  - Exploit kity, e-mail



ALEF

Jaké bylo pokračování?

- Od 2014 mobilní a „chytrá“ zařízení
  - Škodlivé/trojanizované aplikace, drive-by downloady
- 2017
  - Červy
- 2020 – netradiční IoT
  - API



Source: Malwaretech

Kam jsme dospěli?

- U necíleného ransomware se techniky distribuce od let 2013/2017 příliš nezměnily
- Totéž často platí i o mentalitě obránců
  - Postihne nás „necílený“ ransomware
  - AV/“anti-ransomware“ aplikace nás ochrání

    ...ale je to opravdu tak?

Cílený ransomware = APT hrozba pro každého

Zapojení více specializovaných jednotlivců/skupin

1. Sběr dat
2. Průnik do cílového prostředí (RDP, VPN, USB disky, insider, zranitelnosti perimetru,...)
3. Rozšíření na zájmové systémy v rámci sítě
4. Exfiltrace dat
5. Šifrování vybraných dat

Co s tím můžeme dělat?

- Komplexní přístup přes
  - Technologie
    - AV/EPP/“Anti-ransomware“, EDR, komplexní logování sítě i endpointů
  - Procesy
    - Bezpečnostní monitoring, threat intelligence, připravené reakce na incidenty, zálohování a testování záloh i reakce
  - Personál
    - Kontinuální zajištění dohledu i reakce na incidenty

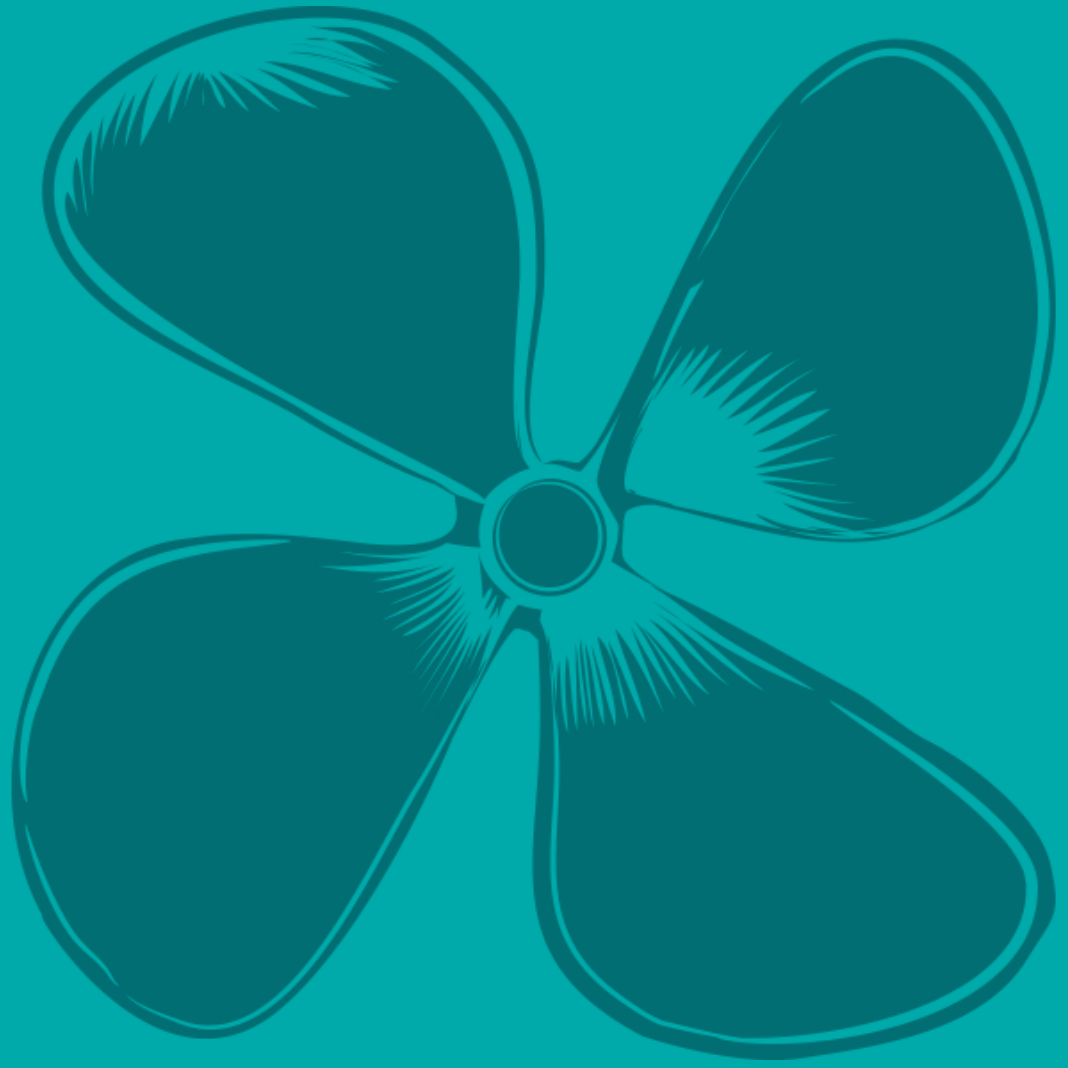
Je námi připravená reakce efektivní?

- Jsme schopní detekovat a zastavit útočníky dříve než dojde k zašifrování dat?
- Máme funkční DR (tedy nejen „na papíře“)?
- Můžeme obnovit business procesy a současně poskytnout podklady pro vyšetření incidentu?

Nestačí spoléhat na obecná doporučení – ta jsou výchozím bodem, ale reakci je vždy třeba uzpůsobit specifickému prostředí konkrétní organizace.

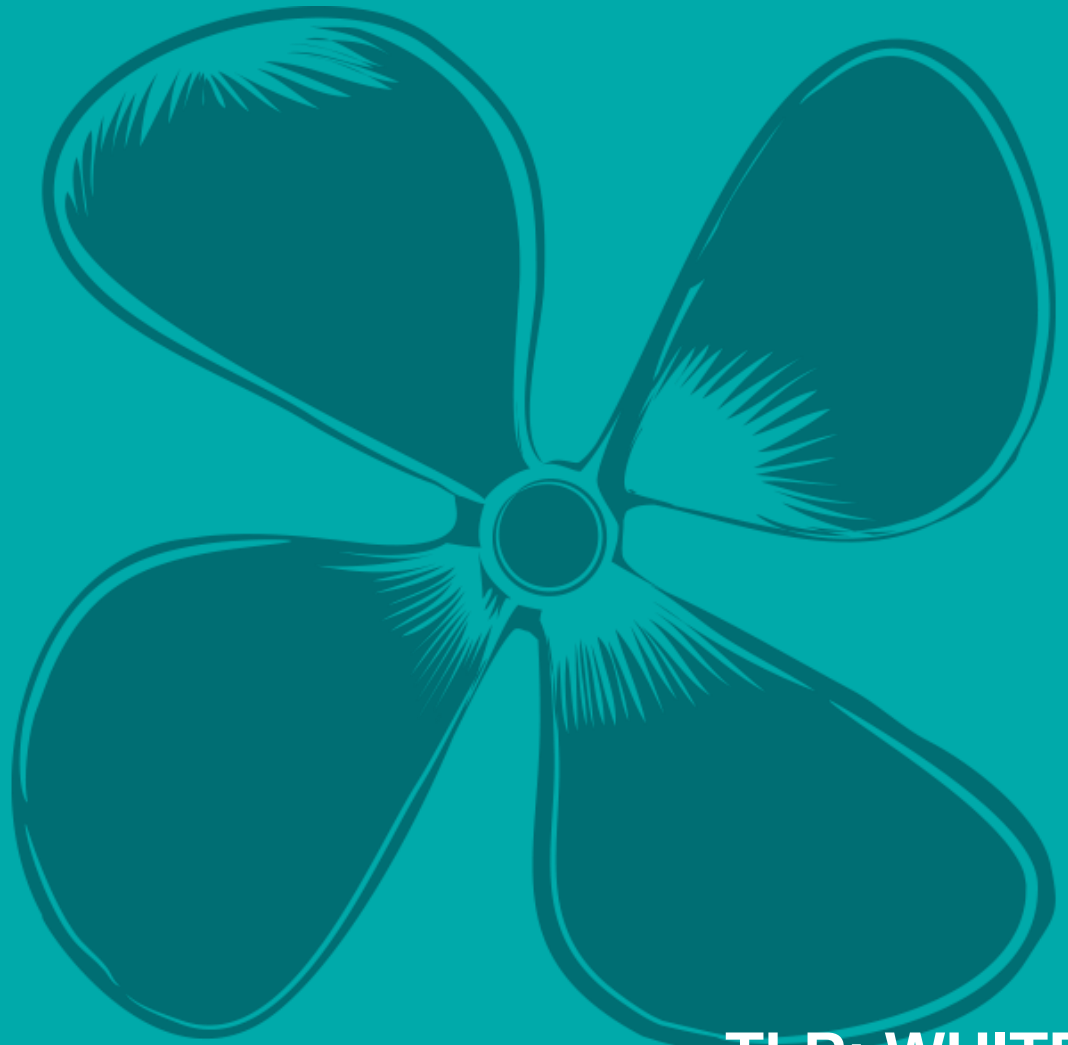
ALEF

Q&A



ALEF

Děkuji Vám za pozornost



TLP: WHITE