Acronis

Acronis Backup

Dokonalý software pro ochranu dat a kybernetickou bezpečnost

Aleš Hok
ales.hok@acronis.cz , +420 776 008 731

Dual headquarters
in Switzerland and Singapore

Ransomware, největší hrozba kyberbezpečnosti

- Použití ransomwaru je jedním z nejsnadnějších způsobů, jak vydělat špinavé peníze prostřednictvím IT.

- Škody způsobené ransomwarem dosáhnou v roce 2021 částky 20 miliard dolarů. To je 57krát více než v roce 2015.

Obvyklé typy ransomwarových útoků

Hromadný, necílený, emailový, ransomwarový útok

- Malá účinnost
- Velký záchyt

Profi penetrace prostřednictvím hackingu a spuštěním kódu uvnitř organizace

- Vyžaduje know how
- Velmi pracné

Spear phishingový útok na konkrétní osobu v konkrétní organizaci

+ Velmi snadné
+ Velmi účinné

Jak funguje ransomware

Jaká bude výše výkupného

Individuální útok = individuální výkupné

Totální kolaps = jistota zaplacení

Výše výkupného = nejvyšší možná částka

Co stačí ke zdařilému útoku

CZ doména

S dobrým názvem
S mail serverem
S anonymní platbou

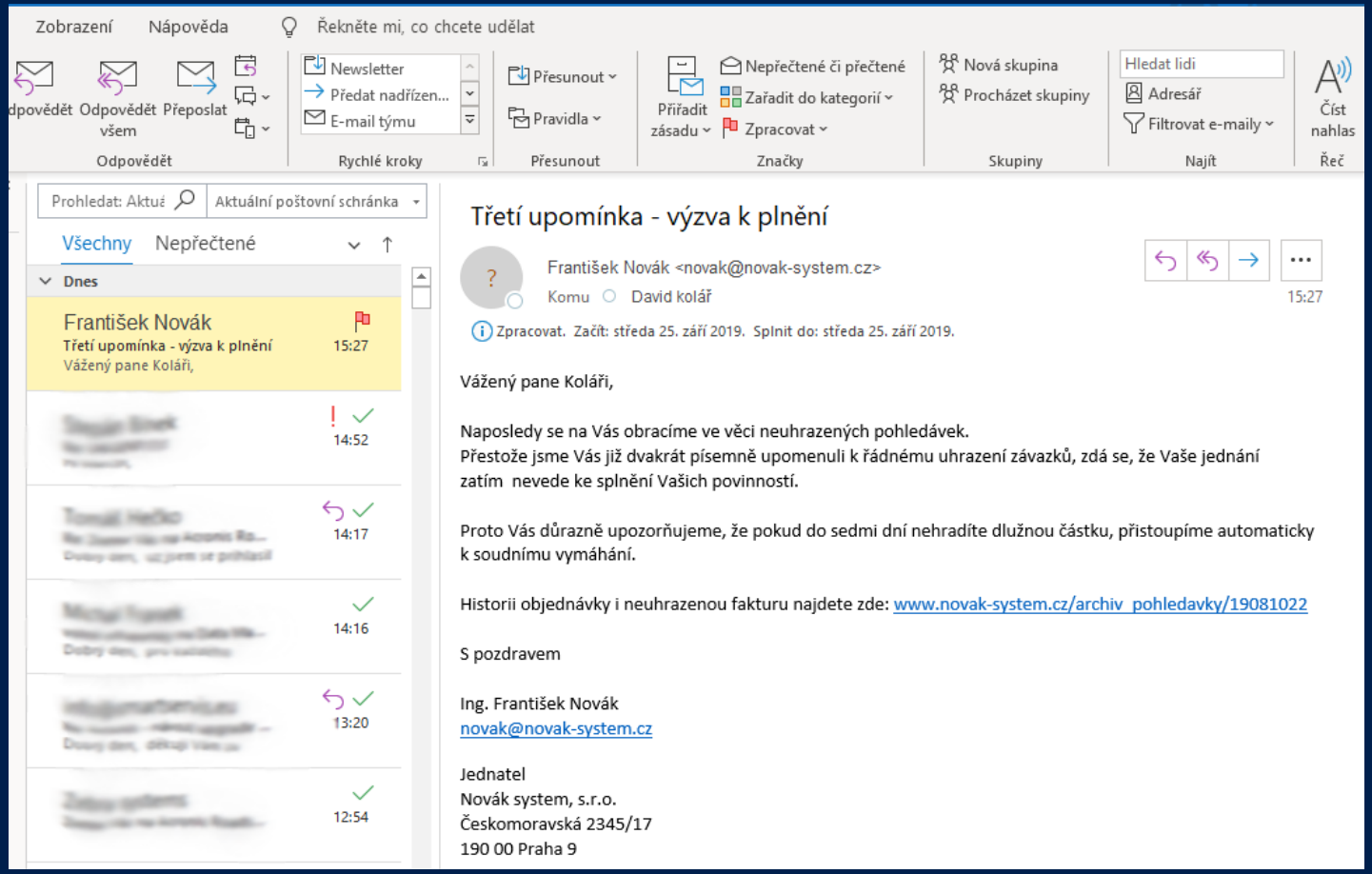
Ransomware

Lze upravit pro
Zero Day útok

Anonymní přístup

Veškeré přístupy jsou realizovány skrze anonymizační služby

Jak to bude vypadat z pohledu uživatele

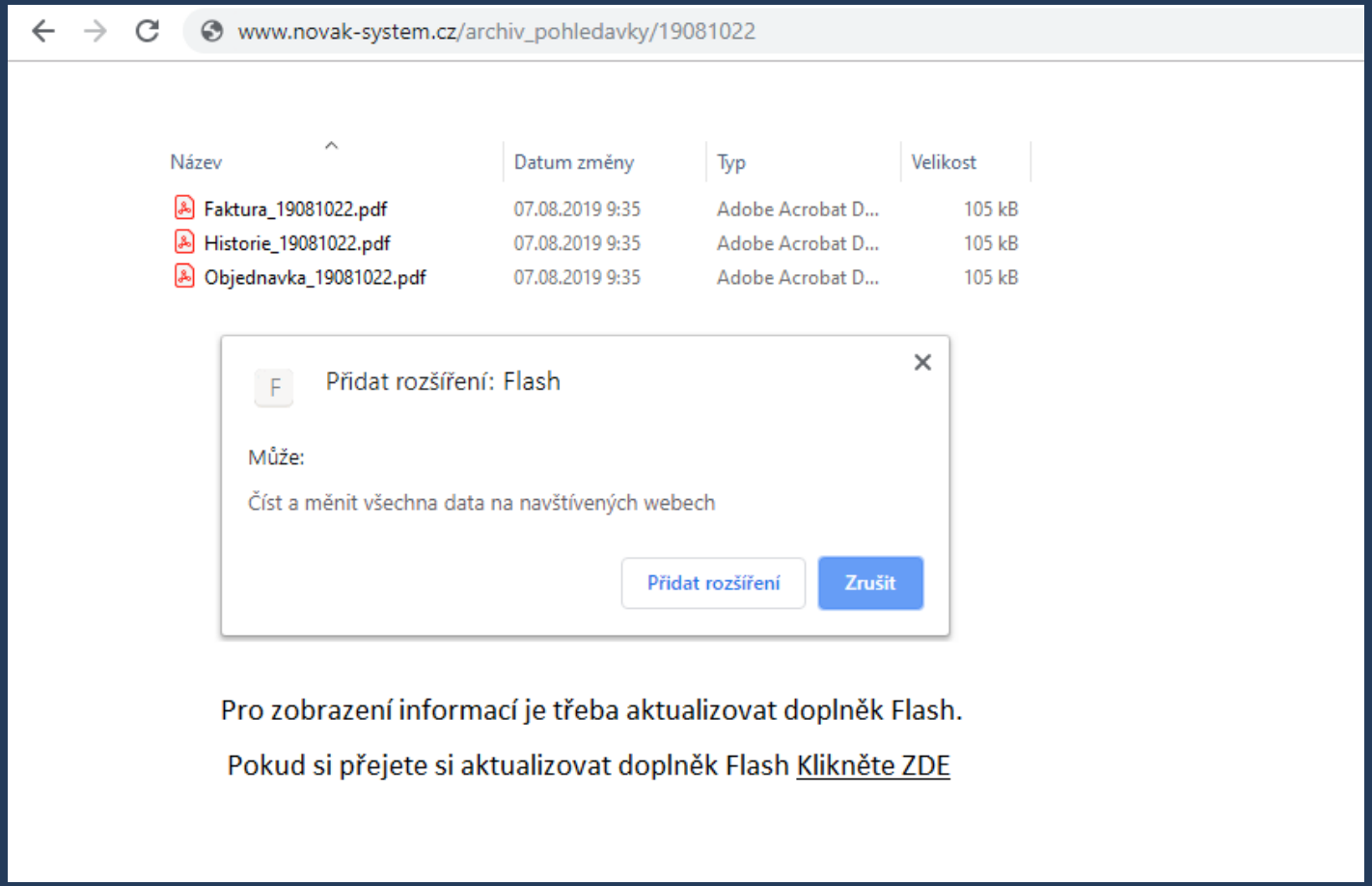

Zobrazení
Nápověda
Řekněte mi, co chcete udělat
Odpovědět
Odpovědět všem
Přeposlat
Odpovědět
Newsletter
Předat nadřízen...
E-mail týmu
Rychlé kroky
Přesunout
Pravidla
Přesunout
Přiřadit zásadu
Nepřečtené či přečtené
Zařadit do kategorií
Zpracovat
Značky
Nová skupina
Procházet skupiny
Skupiny
Hledat lidi
Adresář
Filtrovat e-maily
Najít
Číst nahlas
Řeč
Prohledat: Aktuá
Aktuální poštovní schránka
Všechny
Nepřečtené
Dnes
František Novák
Třetí upomínka - výzva k plnění
Vážený pane Koláři,
15:27
14:52
14:17
14:16
13:20
12:54
Třetí upomínka - výzva k plnění
František Novák <novak@novak-system.cz>
Komu
David kolář
15:27
Zpracovat. Začít: středa 25. září 2019. Splnit do: středa 25. září 2019.
Vážený pane Koláři,
Naposledy se na Vás obracíme ve věci neuhrazených pohledávek.
Přestože jsme Vás již dvakrát písemně upomenuli k řádnému uhrazení závazků, zdá se, že Vaše jednání zatím nevede ke splnění Vašich povinností.
Proto Vás důrazně upozorňujeme, že pokud do sedmi dní nehradíte dlužnou částku, přistoupíme automaticky k soudnímu vymáhání.
Historii objednávky i neuhrazenou fakturu najdete zde: www.novak-system.cz/archiv_pohledavky/19081022
S pozdravem
Ing. František Novák
novak@novak-system.cz
Jednatel
Novák system, s.r.o.
Českomoravská 2345/17
190 00 Praha 9

www.novak-system.cz/archiv_pohledavky/19081022

Název	Datum změny	Typ	Velikost
Faktura_19081022.pdf	07.08.2019 9:35	Adobe Acrobat D...	105 kB
Historie_19081022.pdf	07.08.2019 9:35	Adobe Acrobat D...	105 kB
Objednavka_19081022.pdf	07.08.2019 9:35	Adobe Acrobat D...	105 kB

Pro zobrazení informací je třeba aktualizovat doplněk Flash.

Pokud si přejete si aktualizovat doplněk Flash Klikněte ZDE


www.novak-system.cz/archiv_pohledavky/19081022
Název
Datum změny
Typ
Velikost
Faktura_19081022.pdf
07.08.2019 9:35
Adobe Acrobat D...
105 kB
Historie_19081022.pdf
07.08.2019 9:35
Adobe Acrobat D...
105 kB
Objednavka_19081022.pdf
07.08.2019 9:35
Adobe Acrobat D...
105 kB
Přidat rozšíření: Flash
Může:
Číst a měnit všechna data na navštívených webech
Přidat rozšíření
Zrušit
Pro zobrazení informací je třeba aktualizovat doplněk Flash.
Pokud si přejete si aktualizovat doplněk Flash Klikněte ZDE

Novák system, s.r.o.
Českomoravská 2345/17
190 00 Praha 9

IČ : 25557035
DIČ : CZ25557035

Naše falešná společnost

FAKTURA - daňový doklad č. 19081022

Symboly
Konstantní: 0308
Variabilní 19081022
Specifický

Bankovní účet pro platbu faktury

212235282/0600

Datum
Vystavení: 10.8.2019
Splatnosti: 10.9.2019
Zd. plnění: 10.8.2019

Armakov plus s.r.o.

Nádražní 25
266 01 Beroun
Česká republika

IČ : 28157035
DIČ: CZ28157035

Nejedná se o společnost napadeného subjektu, takže je to omyl

Označení dodávky	Kód	Počet MJ	Cena za MJ	Sazba	Základ	Celkem s DPH
Obalový materiál A560XR1		2 500	99,00	21%	247 500,00	299 475,00

Vaše organizace se stala obětí ransomwarového útoku.

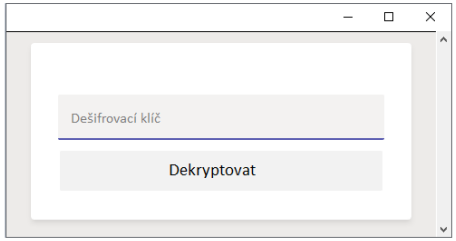
Zašifrovali jsme všechna vaše data.

Zaplaťte nejpozději do 48 hodin 5 Bitcoinů na tento Bitcoinový účet:

1PeVtJcgz9iJjyfVHrkjnog1qn2Si2uqhQ

Po zaplacení se objeví dešifrovací klíč na této webové adrese:

www.novak-system.cz/archiv_pohledavky/19081022/key



Po zadání dešifrovacího klíče do vyskakovacího okna se data dešifrují zpět a vše bude fungovat jako dříve.

Jak provést platbu na Bitconový účet se můžee dočíst na adrese https://cs.wikipedia.org/wiki/Bitcoin

V případě potřeby nás můžete kontaktovat na emailu juraj.janosik501@gmail.com

Jako důkaz o tom, že máme v moci vaše data Vám můžeme poslat ukázky vašich souborů.

S úctou
Juraj Jánošík
(bohatým bral a chudým mával)

Jak to bude vypadat z pohledu správce IT

Jak útok prožívá správce IT

Nejhorší možná varianta

Bez funkční aktivní ochrany

Bez spolehlivých záloh

Uživatelé začínají hlásit poruchy

Přestávají fungovat kritické systémy

Zjišťujete rozsah škod, vypínáte systémy

Není z čeho nebo jak obnovovat

Nakonec nezbývá než zaplatit a doufat

Pro vaši organizaci to může být likvidační

Pro správce nastává konec světa

Jak útok prožívá správce IT

Stejně špatná varianta

Bez funkční aktivní ochrany

Nechráněné, zálohy, chybějící offsite zálohy

Ransomware zašifruje vše - včetně záloh

Není z čeho obnovovat

Nakonec nezbývá než zaplatit a doufat

Pro vaši organizaci to může být likvidační

Pro správce nastává konec světa

Jak útok prožívá správce IT

Lepší varianta

Bez funkční aktivní ochrany

Chráněné nebo nedobytně ukryté zálohy případně kopie záloh offsite

Postupně obnovujete všechny stroje

Ideálně asi celé stroje včetně systémů

Ransom. se může na strojích dále skrývat

Začínáte od nejdůležitějších strojů

Dle rozsahu obnovujete hodiny až dny

Pro organizaci je výpadek obrovskou ztrátou

Pro správce je to velmi špatný den

Jak útok prožívá správce IT

Absolutně nejlepší varianta

Funkční aktivní ochrana

Chráněné nebo nedobytně ukryté zálohy případně kopie záloh offsite

Na email vám píše Acronis Backup

Stroj XY spustil neoprávněné kryptování

Kryptování zastaveno, proces zablokován

Automaticky bylo dekryptováno 5 souborů

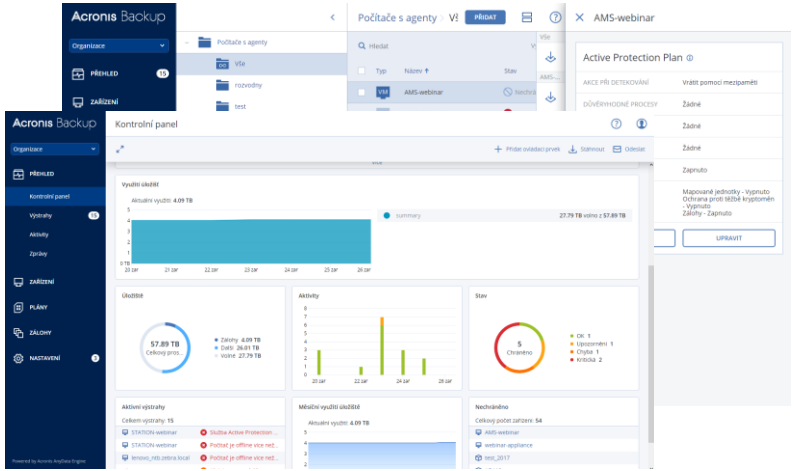
Nic zlého se nestalo, hezký den

Organizace nemá žádnou újmu

Pro správce je to skvělý den, právě ospravedlnil investici do ochrany dat

Zálohovací řešení Acronis

- Aktivně blokuje šifrování a šíření ransomwaru
- Brání vypínání procesů a služeb (znemožní vypínat ochranu)
- Automaticky obnovuje zašifrované soubory z mezipaměti
- Chrání vlastní zálohy proti ransomwaru
- Brání neautorizované těžbě kryptoměn
- Informuje správce o pokusech o útok



Závěrem

- Účinný spear phishingový útok dokáže spáchat 15 letý středoškolák
- Útokům tohoto typu se nedá zabránit
- Používejte zálohování s aktivní ochranou a chraňte zálohy
- Pravidelně žádejte navýšení budgetu na ochranu systémů a dat

TIP

Proveďte falešný útok ve vaší organizaci nebo u vašich zákazníků

Nechte si poslat zprávu o tom, že uživatel XY spustil „jakoby kryptování“

Použijte tento důkaz jako podklad k jednání o navýšení budgetu

Acronis

Děkuji za pozornost

Aleš Hok
ales.hok@acronis.cz , +420 776 008 731

Dual headquarters
in Switzerland and Singapore