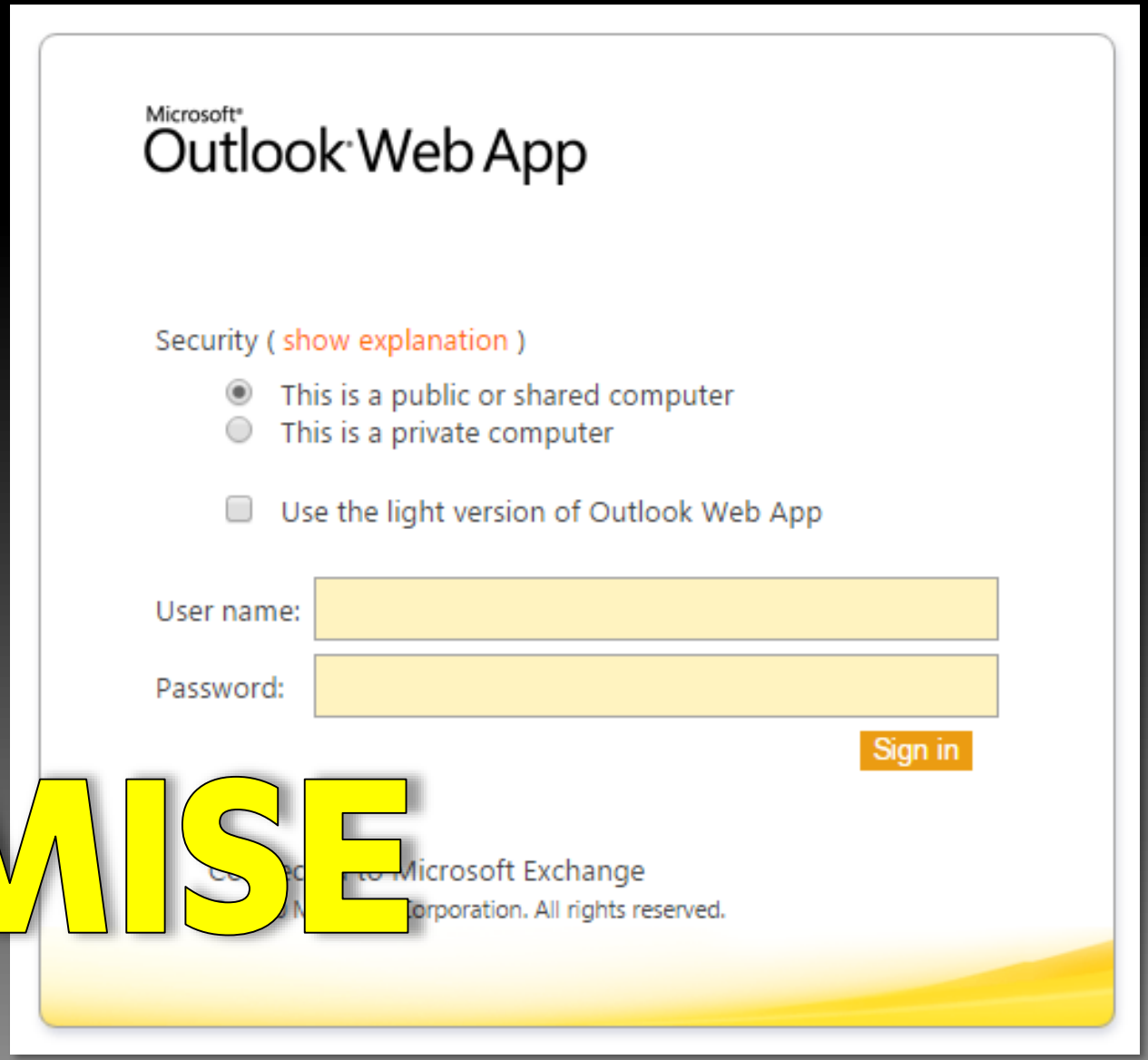

F-Secure
FIGHTING
THE ONLINE BATTLES
Mikko Hypponen
F-Secure
@mikko


F-Secure

300 MILLION

MAERSK

BUSINESS EMAIL COMPROMISE



Daviault, Charles

De: accounts.receivable@clarkbuilders.com <accounts.receivable@clarkbuilders.us>
Envoyé: 27 juin 2017 13:55
À: acctpay@macewan.ca
Objet: Re: Change Of Banking Specifications / Correction
Pièces jointes: ConfirmationOfChangeLetter.pdf

Hiya

Please discard previous email

Please find enclosed and for your records, confirmation of change to our banking details.

Please update your systems accordingly, ensuring that any/all future payments should be allocated to this account, everything else
regarding invoice structure will remain the same.

Account Name: Clark Builders
Bank Name: National Bank of Canada
Bank code: 006
Transit No: 01251
Account No: 0371627

Thank you in advance for your attention.

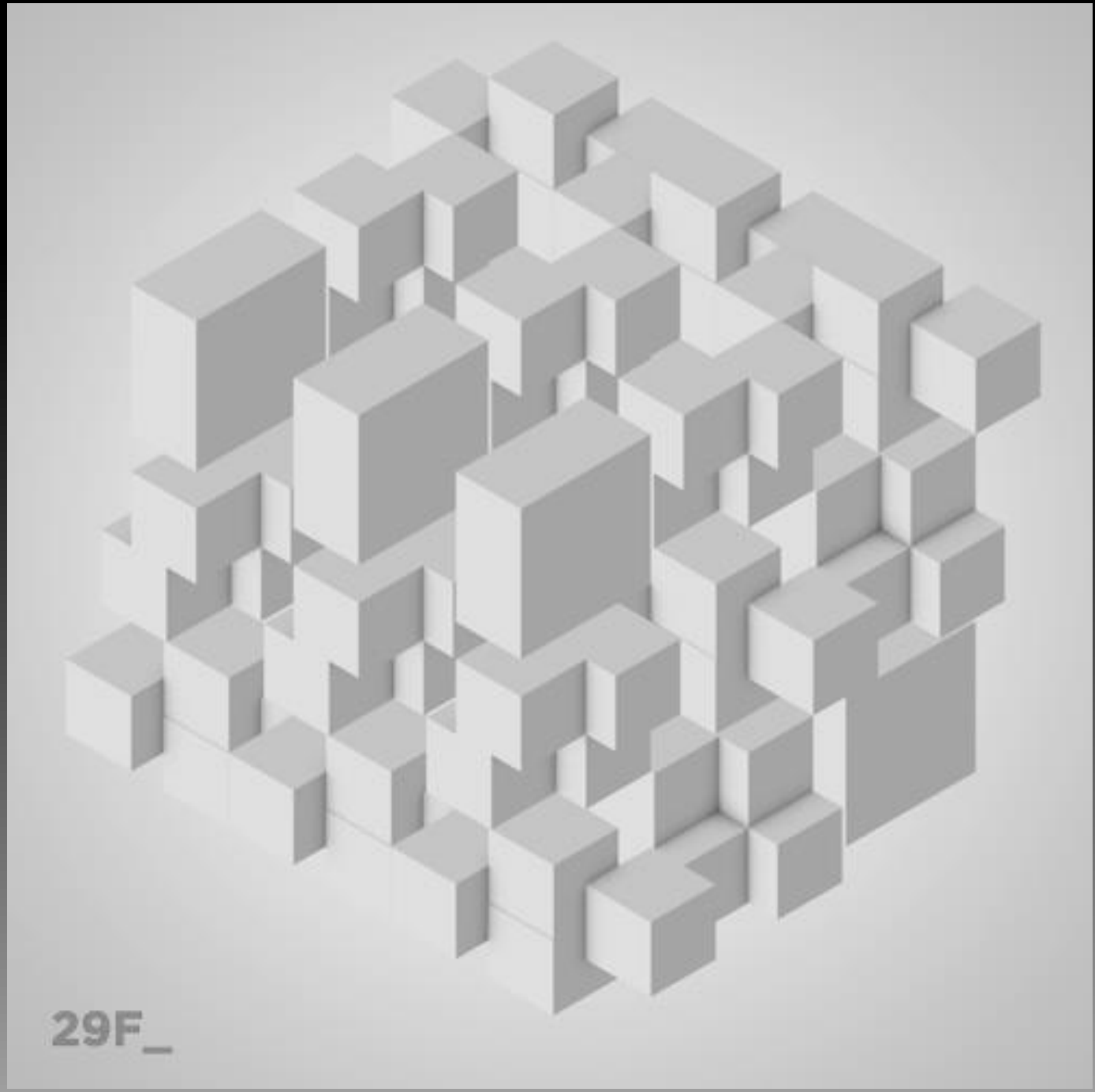
J.Ellis

James Ellis
Accounts Receivable Specialist
Clark Builders

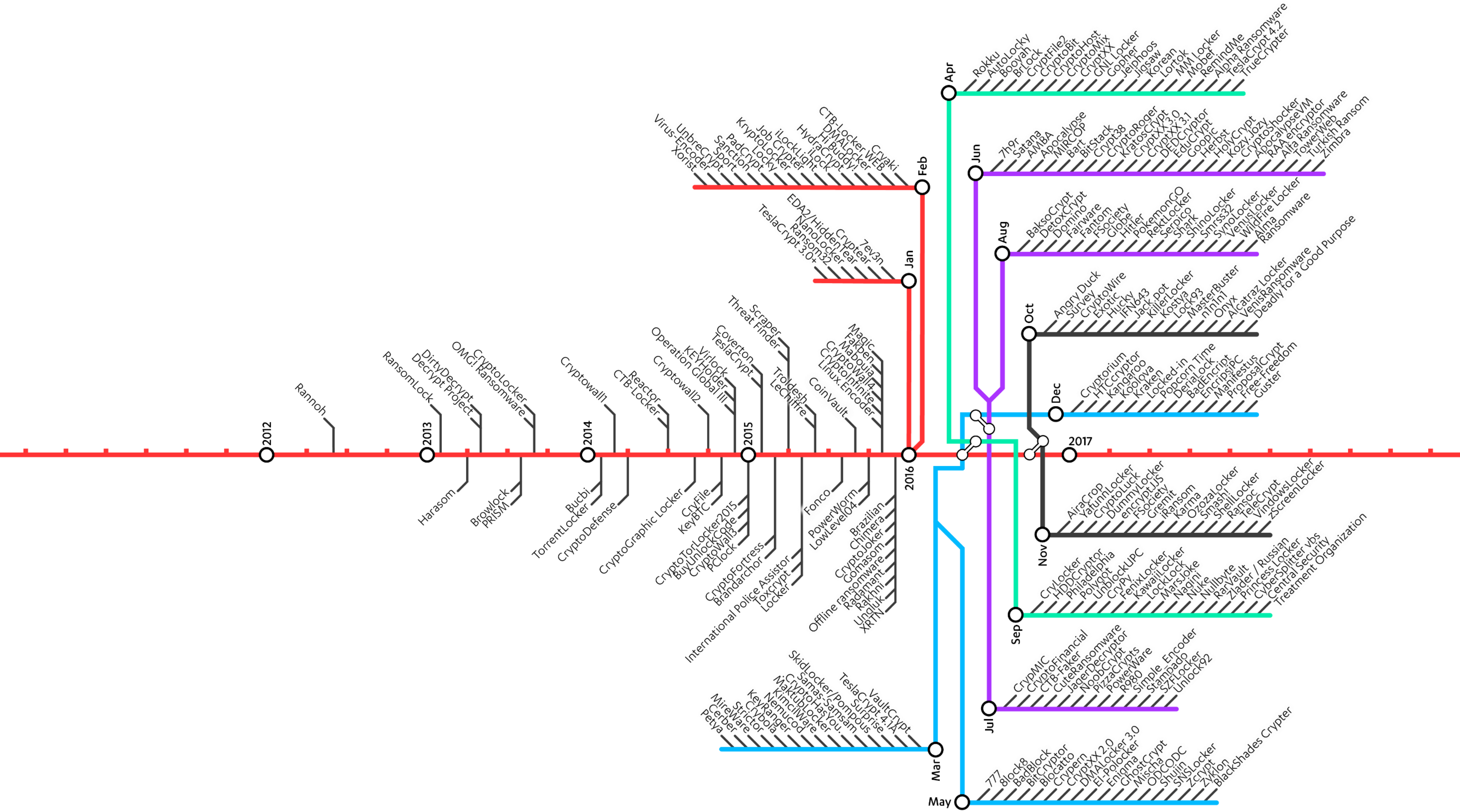
CLARK BUILDERS

4703 - 52 Avenue
Edmonton, AB, Canada
T6B 3R6
Phone: 780-395-3300


MONEY
IS DATA


29F_

2012
Rannoh
2013
RansomLock
DirtyDecrypt
DecrYpt Project
CryptoLocker
OMG! Ransomware
2014
Cryptowall1
Reactor
CTB-Locker
Cryptowall2
Operation Global III
VirLock
KEYHolder
Coverton
TeslaCrypt
Scraper
Threat Finder
2015
Troldesh
LeChiffre
Linux
CoinVa
Xorist
Virus-Encoder
UnbreCrypt
Sport
Sanction
PadCrypt
Locky
KryptoLocker
Job CrypTer
iLockLight
iLock
HydraCrypt
Hi Bu
DM
CTB-
EDA2/Hidden
NanoLocker
Ransom32
TeslaCrypt 3.0+

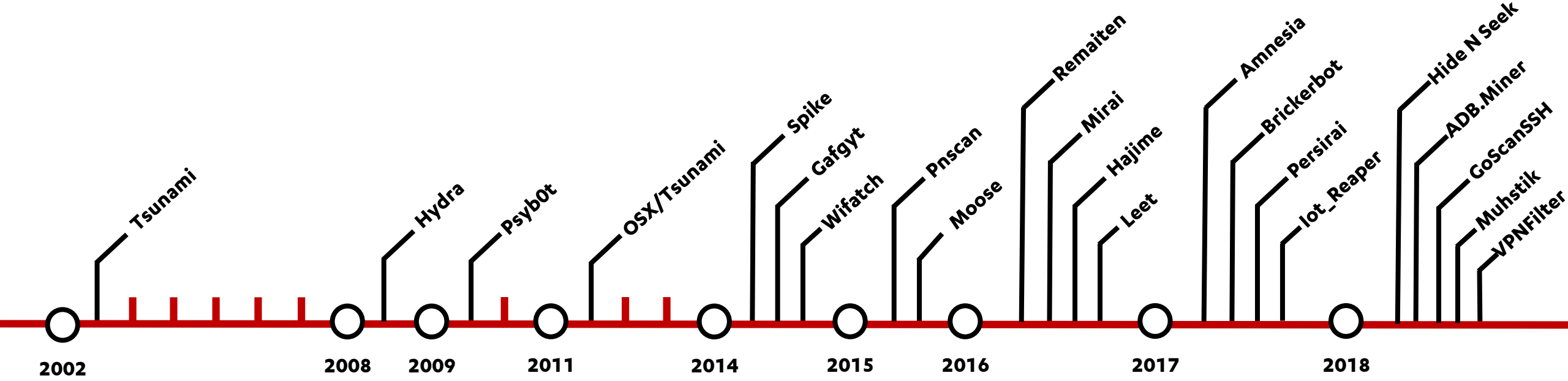


2012
Rannoh
2013
RansomLock
Harasom
DirtyDecrypt
Decrypt Project
OMG! Ransomware
CryptoLocker
Browlock
PRISM
2014
Cryptowall1
Bucbi
TorrentLocker
CryptoDefense
Reactor
CTB-Locker
Cryptowall2
CryptoGraphic Locker
Operation Global III
KEYHolder
Virlock
CryFile
KeyBTC
Coverton
TeslaCrypt
2015
CryptoTorLocker2015
BuyUnlockCode
CryptoWall3
PClock
Threat Finder
Scraper
CryptoFortress
Brandarchor
Troldesh
LeChiffre
International Police Assistor
Toxcrypt
Locker
CoinVault
Fonco
PowerWorm
LowLevel04
Magic
Fakben
Mabouia
CryptoWall4
CryptoInfinite
Linux.Encoder
Brazilian
Chimera
CryptoJoker
Gomasom
Offline ransomware
Radamant
Rakhni
Ungluk
XRTN
2016
Jan
7ev3n
Cryptear
EDA2/HiddenTear
NanoLocker
Ransom32
TeslaCrypt 3.0+
Feb
Cryaki
CTB-Locker WEB
DMALocker
Hi Buddy!
HydraCrypt
iLock
iLockLight
Job Crypter
KryptoLocker
Locky
PadCrypt
Sanction
Sport
UnbreCrypt
Virus-Encoder
Xorist
Mar
VaultCrypt
TeslaCrypt 4.1A
Surprise
SkidLocker/Pompous
Samas-Samsam
CryptoHasYou.
MaktubLocker
KimcilWare
Nemucod
KeyRanger
Crybola
Strictor
MireWare
Cerber
Petya
Apr
Rokku
AutoLocky
Booyah
BrLock
CryptFile2
CryptoBit
CryptoHost
CryptoMix
CryptXXX
GNL Locker
Gopher
Jeiphoos
Jigsaw
Korean
Lortok
MM Locker
Mobef
RemindMe
Alpha Ransomware
TeslaCrypt 4.2
TrueCrypter
May
777
8lock8
BadBlock
BitCryptor
Blocatto
Crypern
CryptXXX 2.0
DMALocker 3.0
El-Polocker
Enigma
GhostCrypt
Mischa
ODCODC
Shujin
SNSLocker
Zcrypt
Zyklon
BlackShades Crypter
Jun
7h9r
Satana
AMBA
Apocalypse
MIRCOP
Bart
BitStack
Crypt38
CryptoRoger
KratosCrypt
CryptXXX 3.0
CryptXXX 3.1
DEDCryptor
EduCrypt
Goopic
Herbst
HolyCrypt
Kozy.Jozy
CryptoShocker
ApocalypseVM
RAA encryptor
Alfa Ransomware
TowerWeb
Turkish Ransom
Zimbra
Jul
CrypMIC
CryptoFinancial
CTB-Faker
CuteRansomware
JagerDecryptor
NoobCrypt
PizzaCrypts
PowerWare
R980
Simple_Encoder
Stampado
SZFLocker
Unlock92
Aug
BaksoCrypt
DetoxCrypt
Domino
Fairware
Fantom
FSociety
Globe
Hitler
PokemonGO
RektLocker
Serpico
Shark
ShinoLocker
Smrss32
SynoLocker
VenusLocker
WildFire Locker
Alma Ransomware
Sep
CryLocker
HDDCryptor
Philadelphia
Polyglot
UnblockUPC
CryPy
FenixLocker
KawaiiLocker
LockLock
MarsJoke
Nagini
Nuke
Nullbyte
RarVault
Zlader / Russian
Princess Locker
CyberSplitter vbs
Central Security Treatment Organization
Oct
Angry Duck
Survey
CryptoWire
Exotic
Hucky
IFN643
Jack.Pot
KillerLocker
Kostya
Lock93
MasterBuster
n1n1n1
Onyx
Alcatraz Locker
VenisRansomware
Deadly for a Good Purpose
Nov
AiraCrop
YafunnLocker
CryptoLuck
DummyLocker
encryptJJS
FSociety
Gremit
iRansom
Karma
OzozaLocker
Smash!
ShellLocker
Ransoc
TeleCrypt
WindowsLocker
ZScreenLocker
Dec
Cryptorium
HTCcryptor
Kangaroo
Koolova
Kraken
Locked-in
Popcorn Time
DeriaLock
BadEncript
EncripsiPC
Manifestus
ProposalCrypt
Free-Freedom
Guster
2017

HYPPONEN's LAW

Whenever an appliance is described as "smart", it's vulnerable.

Malware targeting connected devices



F-Secure.


GOVERNMENTAL
ATTACKS


f you see this text, then your files are no longer accessible, because they
ave been encrypted. Perhaps you are busy looking for a way to recover your
iles, but don't waste your time. Nobody can recover your files without our
ecryption service.
e guarantee that you can recover all your files safely and
eed to do is submit the payment and purchase the decryption key.
lease follow the instructions:
. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
. Send your Bitcoin wallet ID and personal installation key to e-mail
wousmith123456@posteo.net. Your personal installation key:
sVC7Ff-MmKBo5-Df1kXY-QHqet5-LCsHWn-G1F8bf-t9dgTM-eXsTVN-
f you already purchased your key, please enter
ey:
PEHOME

M.E.Doc

medoc.ua/uk

Технічна підтримка +380 44 206 72 10
Відділ продажів +380 44 206 72 15

me doc
МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

ПРО НАС ПАРТНЕРСЬКА МЕРЕЖА НОВИНИ КОНТАКТИ

Дистрибутив 10.01.194

Оновлення 10.01.196

Завантажити інструкцію

Гарячі питання

Отримати код доступу

Вийшло оновлення 10.01.196

Детальніше

Russian Cyber Operatives

F-Secure.


MARRIOTT


NL
PF-934-R

Connected to:

-Smartphone (4G)

-WiFi panel antenna

Computer

WiFi panel antenna (covered)

Bag with battery

Transformer

Aleksei MORENETS

Naam: Aleksei Sergeyvich MORENETS
Geboortedatum: 31-07-1977
Geboorteplaats: Moermanskaya Oblast
Paspoortnr: 100135556

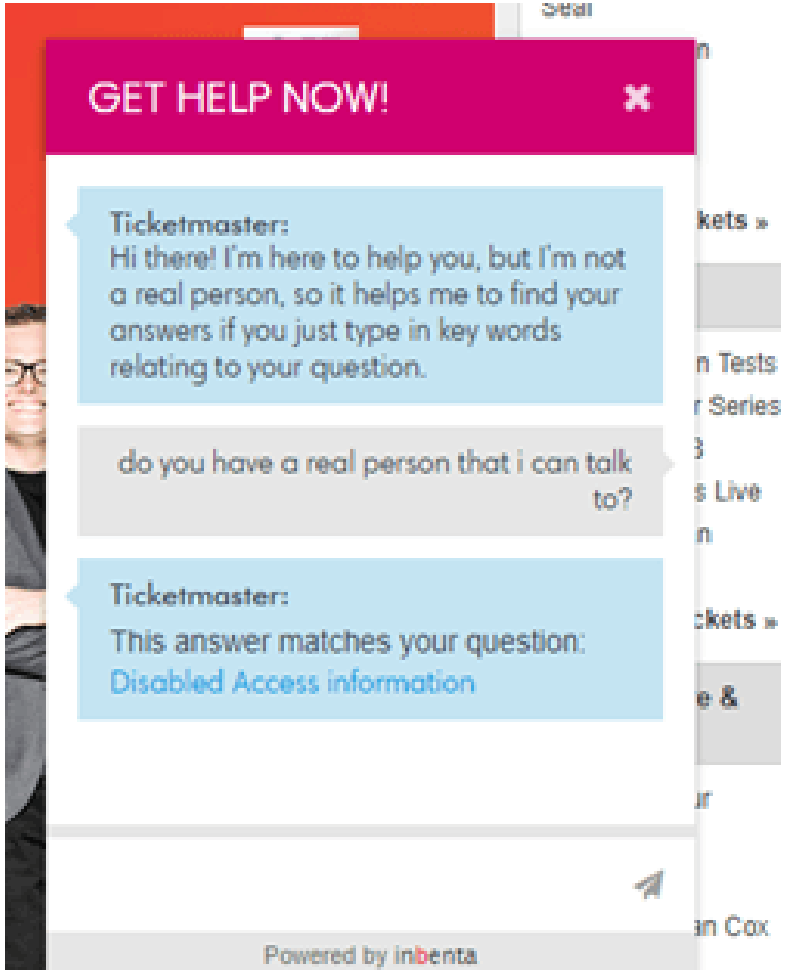
Rol: Cyber operator


f you see this text, then your files are no longer accessible, because they
ave been encrypted. Perhaps you are busy looking for a way to recover your
iles, but don't waste your time. Nobody can recover your files without our
ecryption service.
e guarantee that you can recover all your files safely and
eed to do is submit the payment and purchase the decryption key.
lease follow the instructions:
. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
. Send your Bitcoin wallet ID and personal installation key to e-mail
wousmith123456@posteo.net. Your personal installation key:
sVC7Ff-MmKBo5-Df1kXY-QHqet5-LCsHWn-G1F8bf-t9dgTM-eXsTVN-
f you already purchased your key, please enter
ey:
PEHOME

Important Notice: unauthorized access to payment card data in U.S. stores

F-Secure

ticketmaster®




F-Secure

gecko
@gco__

@pizzahut One large pepperoni pizza for delivery at 1109 virginia ave 94061-2049 . my card number is 4217-1688-7534-2619 exp. 04/21 cvv 173

15/06/2018, 13.30

Lan Ron @mcl166 · 12/07/2018
Replying to @gco__ and @pizzahut
You shouldn't post that here XD

1

gecko @gco__ · 12/07/2018
why


F-Secure
FIGHTING
THE ONLINE BATTLES
Mikko Hypponen
F-Secure
@mikko