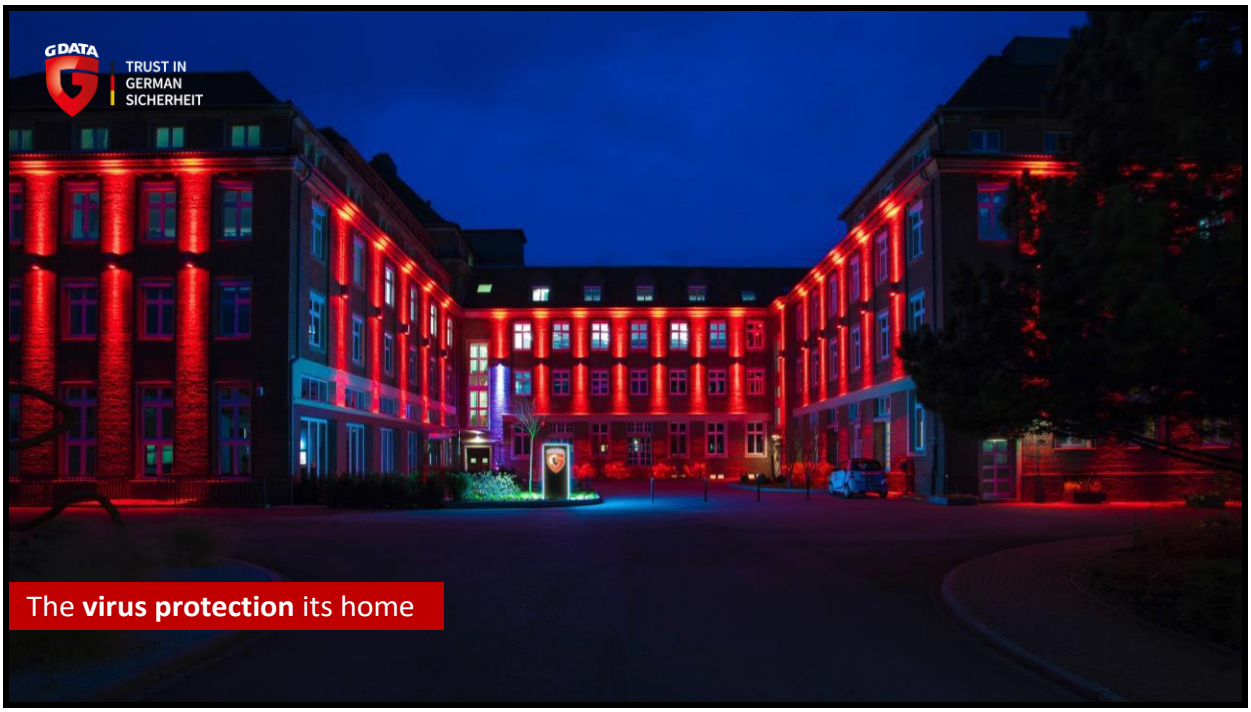
TRUST IN GERMAN SICHERHEIT

Wallet Stealer

In the footsteps of banking Trojans

Ralf Benzmüller, G DATA Software

www.gdata.de/blog
ralf.benzmueller@gdata.de
@rb_gdata



Intro

G DATA Overview

German provider of IT security solutions Founded in Bochum in 1985

Today just under 500 employees

G DATA Software AG

- First virus protection 1987
- Today wide range of products and services for private and business customers
- Products available worldwide

G DATA Advanced Analytics

- Foundation 2015
- High-quality, product-independent services
- Security Consulting, Incident Response,
- Malware Analysis, Software Integration, …

TRUST IN GERMAN SICHERHEIT

SecurITy made in Germany

Machine Learning @ G DATA

Agenda

01

Intro Crypto Currencies

TRUST IN GERMAN SICHERHEIT

Cryptocurrencies

Overview

CoinMarketCap

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$97.406.368.579	$5.603,59	$4.119.796.590	17.382.850 BTC	0,92%	
2	XRP	$20.260.753.773	$0,503101	$881.312.880	40.271.748.947 XRP *	2,26%	
3	Ethereum	$18.154.162.100	$175,77	$1.794.223.830	103.283.903 ETH	0,95%	
4	Bitcoin Cash	$6.722.759.280	$384,92	$282.028.716	17.465.225 BCH	-1,20%	
5	Stellar	$4.769.573.084	$0,247585	$101.937.778	19.264.393.114 XLM *	1,08%	
6	EOS	$4.137.873.952	$4,57	$752.370.260	906.245.118 EOS *	-0,09%	
7	Litecoin	$2.500.222.553	$42,22	$344.556.144	59.216.663 LTC	0,80%	
8	Tether	$1.739.793.703	$0,990533	$3.013.326.992	1.756.421.736 USDT *	0,29%	
9	Cardano	$1.598.737.612	$0,061663	$16.880.051	25.927.070.538 ADA *	1,52%	

TRUST IN GERMAN SICHERHEIT

https://coinmarketcap.com/ data as of 19.11.2018

CoinLore BETA Home Rank Exchanges Tools Login/Register USD English Search Coins

Cryptocurrencies:1973 Markets:10030 Market Cap:€161,334,064,148 24h Vol:€10,997,667,295 BTC Dominance:53.1%

	#	Name	Market Cap	Price	Volume(24h)	Supply	Change(24h)	Change(7d)
☆	1	Bitcoin	€85,625,779,736	€4,954.43	€3,283,915,785	17,282,687	↑1.17%	
☆	2	Ripple	€17,852,540,950	€0.448454	€1,010,698,812	39,809,069,106	↑4.13%	
☆	3	Ethereum	€15,811,172,774	€154.82	€1,449,845,970	102,125,453	↑1.41%	
☆	4	Bitcoin Cash	€5,614,561,460	€323.36	€208,198,810	17,363,063	↑3.20%	
☆	5	Stellar	€4,129,919,177	€0.219847	€74,793,383	18,785,416,663	↑1.61%	
☆	6	EOS	€3,661,090,978	€4.04	€628,118,814	906,245,118	↓-0.07%	
☆	7	Litecoin	€2,187,063,729	€37.44	€283,601,848	58,410,256	↑1.20%	
☆	8	Cardano	€1,403,637,852	€0.054138	€13,645,237	25,927,070,538	↑0.71%	
☆	9	Monero	€1,279,621,253	€77.89	€131,097,577	16,428,971	↓-0.12%	
☆	10	TRON	€1,092,083,980	€0.016610	€52,608,402	65,748,111,645	↓-0.22%	

TRUST IN GERMAN SICHERHEIT

Cryptocurrencies

Key data

CoinMarketCap

Cryptocurrencies	2081
Markets	15.891
Market capitalization	185,058,868,984 USD
24h Volume	13.350.841.689
BTC share	52,6%

TRUST IN GERMAN SICHERHEIT

https://coinmarketcap.com/ data as of 19.11.2018

Cryptocurrencies

Exchanges

CoinMarketCap

#	Name	Adj. Vol (24h)*	Volume (24h)	Volume (7d)	Volume (30d)	No. Markets	Change (24h)	Vol Graph (7d)	Launched
1	Binance	$639.574.452	$639.574.452	$4.557.482.048	$19.090.558.432	384	-1.21%		Jul 2017
2	OKEx	$583.511.820	$583.511.820	$4.735.942.336	$16.813.341.984	509	4.29%		Jan 2014
3	Huobi	$546.438.708	$546.438.708	$3.422.032.736	$12.007.789.120	284	10.48%		Sep 2013
4	DigiFinex	$311.595.865	$311.595.865	$2.508.768.416	$9.260.001.200	88	12.68%		Apr 2018
5	BitForex	$307.121.227	$307.121.227	$1.949.045.968	$9.394.867.248	102	59.33%		Jun 2018
6	Bibox	$300.016.029	$300.016.029	$1.511.001.392	$6.941.377.200	208	0.86%		Nov 2017
7	LBank	$297.877.198	$297.877.198	$1.771.165.392	$6.385.306.248	92	-0.12%		Oct 2017
8	CoinBene	$294.249.428	$294.249.428	$1.620.091.456	$6.611.877.972	163	1.14%		Sep 2017
9	HitBTC	$288.514.429	$288.514.710	$1.511.903.792	$7.105.715.920	808	5.17%		Feb 2014

TRUST IN GERMAN SICHERHEIT

https://coinmarketcap.com/ data as of 19.11.2018

CoinLore BETA Home Rank Exchanges Tools Login/Register USD English Search Coins

#	Name	Founded	Location	Volume	Fiat	USDT
1	Bithumb	2013	South Korea	$742,906,303	Yes	No
2	CoinsBank			$654,516,696	Yes	No
3	OKEX	2014	Hong Kong	$567,982,198	No	No
4	Huobi	2013	Singapore	$552,550,851	No	No
5	Binance	2014	Japan	$546,034,131	No	Yes
6	DigiFinex			$298,978,170	No	Yes
7	Lbank	2017	HK	$292,262,865	No	Yes
8	HitBTC	2013	Hong Kong	$277,610,969	No	No
9	Bibox	2017	China	$275,784,034	No	Yes
10	IDAX			$243,358,367	No	No
11	Bit-z	2016	Hong Kong, Beijing, Singapore	$190,756,818	No	No
12	BCex	2017	Vancouver	$188,078,307	No	No
13	Upbit			$165,913,905	Yes	No
14	IDCM			$162,457,005	No	Yes
15	Bitfinex	2012	Hong Kong	$158,883,729	No	Yes

G DATA TRUST IN GERMAN SICHERHEIT

Agenda

02

Wallets

G DATA TRUST IN GERMAN SICHERHEIT

Wallets

There are very many wallets

TRUST IN GERMAN SICHERHEIT

Wallets

Overview

Function:	Necessary to use crypto currencies. Manages private and public keys of cryptocurrencies Interacts with the blockchain to transfer money, view account balance, etc.
Types:	Desktop Online Mobile Hardware Paper
Application	Hot Storage - frequent transactions Cold Storage - for long-term installations

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

Azorult

Distribution	Email campaigns (application), exploit kits on websites
Since	2016
Context	InfoStealer, Downloader, Banking Trojan, Ransomware
Camouflage	Conditions (e.g. cookies) for download of target file Attachment of mails password encrypted. Password in mail
Configuration	*wallet*.txt,*seed*.txt,*btc*.txt,,*key*.txt,*2fa*.txt,*2fa*.png,*2fa*.jpg,*auth*.jpg,*auth*.png,*crypto*.txt,*coin*.txt,*poloniex*,*kraken*,*okex*,*binance*,*bitfinex*,*gdax*,*private*.txt,*upbit,**bcex*,*bithimb*,*hitbtc*,*bitflyer*,*kucoin*,*huobi*,*wallet.json*
CnC communication	XOR encrypted. Hardcoded 3-byte key
Wallets affected	Exodus, Jaxx, Mist, Ethereum, Electrum, Electrum-LTC, among others.

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

ComboJack - Clipboard Monitor

Distribution	Email with PDF opens RTF with embedded HTA that uses DirectX vulnerability. If this succeeds, PowerShell scripts reload an SFX that contains a reloads further password-protected SFX with ComboJack
Since	Feb 2018
Procedure	Replaces wallet addresses in the clipboard with your own
Wallets affected	Bitcoin, Litecoin, Ethereum, Monero, Qiwi, Yandex Money, WebMoney

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

ComboJack - Clipboard Monitor

Wallet	Criteria	
Ethereum	Length: 42;	starts with "0
Monero	Length: 106;	starts with "4
Bitcoin	Length: 34;	starts with "1
Litecoin	Length: 34;	starts with "L
Qiwi	Length: 11;	starts with "8
WebMoney Ruble	Length: 13;	starts with "R
WebMoney USD	Length: 13;	starts with "Z
Yandex Money	Length: 15;	starts with "4100

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

Jigsaw Bitcoin Stealer

Distribution	File download
Since	April 2018
Context	Jigsaw Ransomware
Origin	Japan
Procedure	Changes bitcoin address in clipboard Replace with own bitcoin address Applies only to individual addresses USP: Selection of a target address with similar beginning and end from 10,000 Uses mixer service to disguise transactions
Targets concerned	Bitcoin /^1|3[1-9A-HJ-NP-Za-km-z]{26,34}$/

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

Evrial - Wallet Stealer and Clipboard Monitor

Distribution	Email campaigns (application), exploit kits on websites
Since	Jan. 2018
Context	InfoStealer, Wallet Stealer (BTC), Document Stealer, Password Stealer
Procedure	Changing certain contents in the clipboard Detection of Bitcoin addresses and replace with own (CnC query).
Wallets affected	Bitcoin, Litecoin, Monero, WebMoney, Qiwi and Steam

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

njRAT Lime Edition - Wallet Stealer and Ransomware

Distribution	njRAT aka Bladabindi
Since	2013
Context	Keylogger, Password Stealer, Screenlocker, DDoS, USB worm
Procedure	Searches for process names and titles of windows Detection of bitcoin addresses Transaction manipulation
Wallets affected	BitcoinCore, Bitcoin.com Wallet, Electrum
CnC communication	Proprietary TCP protocol over DNS
Technical data	Based on .NET Framework
Camouflage	VM Detection, Anti-AV

TRUST IN GERMAN SICHERHEIT

Alternative attacks

Syscoin - Github Hack

Credentials to Syscoin github stolen from one of the developers June 2018: Replaces Windows client with version using Arkei Stealer Client allows mining of Syscoins and management of Syscoins Costs $80

	Arkei Stealer
Distribution	File download from Syscoin
Context	InfoStealer (passwords, cookies, files, SystemInfo), Form Grabber, Downloader
Procedure	Copying the wallet files
Wallets affected	Bitcoin Core, Ethereum, ElectrumLTC, Monero, Electrum, Dash, Litecoin, ElectronCahs, ZCash, MultiDoge, AnonCoin, BBQCoin, DigitalCoin, FlorinCoin, Franko, FreiCoin, GoldCoin, InfiniteCoin, IOCoin, IxCoin, MegaCoin, MinCoin, NameCoin, PrimeCoin, TerraCoin, YACoin

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

All targets

AnonCoin
BBQCoin
Bitcoin
Bitcoin Cash
Bitcoin Core
Bitcoin.com Wallet
BlackCoin
Bytecoin
Cardano
Dash
DevCoin
DigitalCoin
Dogecoin
ElectronCash
Electroneum
Electrum
ElectrumLTC
EmerCoin
Ethereum
Exodus
FlorinCoin
Franko
FreeCoin
GoldCoin
Graft
InfiniteCoin
IOCoin
IxCoin
Lisk
Litecoin
MegaCoin
MinCoin
Miota
Monero
Monero Core
MultiBitHD
MultiDoge
Namecoin
Neo
PrimeCoin
Qiwi
Qtum
ReddCoin
Ripple
Stellar
Stratis
Targets
TerraCoin
ViaCoin
Waves
WebMoney
WME, WMR
WMU, WMX
WMZ
YACoin
YaMoney
Yandex Money
ZCash
Zicash

TRUST IN GERMAN SICHERHEIT

Wallet Stealer

Frequency distribution October 2018

Total: 945

TRUST IN GERMAN SICHERHEIT

Agenda

04

Conclusion

TRUST IN GERMAN SICHERHEIT

Conclusion

CyberCrime goes where the money is

The billion-dollar crypto-money market has also arrived in the cybercrime economy

Following the run on ransomware and crypto-jacking, wallets are popular targets

Professional attacks are multi-layered

This danger should not be underestimated

TRUST IN GERMAN SICHERHEIT

Web: www.gdata.de
Mail: ralf.benzmueller@gdata.de
Twitter: @rb_gdata