SWITCHcert Security Report

July 2016

SWITCH

I. DAO-ism on the ethereal plane – hacker bags cryptocurrency worth USD 50 million

It was recently announced that a hacker had used a recursive calling vulnerability that had apparently been known about for some time to siphon 3.6 million «ether» tokens from a virtual investment fund calling itself the Decentralized Autonomous Organization (DAO). At the time of the theft, these were worth over USD 50 million – more than 35% of the fund's assets.

To understand why this could lead to a cryptocurrency crisis with further-reaching consequences than the attack that forced Mt. Gox, the best-known Bitcoin exchange, to file for bankruptcy, we need to take a closer look at the individual elements: the DAO, the Ethereum blockchain, the recursive vulnerability and the options after the hack.

The DAO was developed as an alternative to classic venture capital funds. The idea was to replace the investment firm managed by individuals whose interests are often at odds with those of the firm with a decentralised network of self-executing, digital «smart contracts». People are only involved in the capacity of co-owners of the DAO. They buy digital tokens in the form of a cryptocurrency known as «ether», which is traded via the Ethereum blockchain, a decentralised peer-to-peer network. The quantity of ether you buy determines your voting

rights in the e-vote to decide where and how the money is invested. Another difference between the DAO and a traditional investment firm is that is has no physical address and is therefore – at least in theory – beyond the reach of outsiders, including governments, financial regulators and tax authorities. The Ethereum blockchain structure has two advantages for the DAO. Unlike the Bitcoin blockchain, it can be used for more complex exchanges such as programs or indeed smart contracts. At the same time, because Ethereum must ensure that information can be found on the network at any time (as is the case with any blockchain), the address and letter codes it employs are ideal for use as anonymous numbered accounts.

The DAO now has some explaining to do on a number of fronts, since the hack was performed with a «simple» recursive calling vulnerability. While the transfer is technically transparent, meaning that the account into which the ether was transferred is known, no one knows who the account belongs to, even though an anonymous claim of responsibility was posted on pastebin.com. In it, the purported thief insists he or she did nothing wrong and was merely exploiting the scope offered by the DAO's code.

We may well ask whether exploiting a bug in the code qualifies as a hack or a crime if that same code serves as the binding element of a contract. This calls the whole concept of smart contracts into question, especially since the DAO's developers have since used the same methodology to protect the remaining capital against any further unauthorised withdrawals. On top of this, the attack has made it abundantly clear that the DAO could not back up its claim of being secure and untouchable, while all the options put forward for recovering the tokens (and thus the money) would undermine the DAO's credibility and its members' trust. It turns out, therefore, that the supposed advantage of having no physical address and thus placing yourself outside the jurisdiction of any law enforcement authority quickly turns into a disadvantage when the help of those very authorities is exactly what you need.

It remains to be seen how the case will pan out going forward and how it will affect a motion submitted to the Swiss National Council on16 June 2016 to relax security requirements for startups that want to handle financial transactions via blockchains.

Read more here:

http://www.zeit.de/digital/internet/2016-06/the-dao-blockchain-ether-hack/komplettansicht
http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human
http://www.zeit.de/digital/internet/2016-05/blockchain-dao-crowdfunding-rekord-ethereum
https://de.wikipedia.org/wiki/Ethereum
http://www.btc-echo.de/dao-hack-falsche-entscheidung-ethereum-zerstoeren
http://www.zeit.de/digital/internet/2016-05/blockchain-dao-crowdfunding-rekord-ethereum
http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs
http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit
http://pastebin.com/CcGUBgDG
http://www.heise.de/newsticker/meldung/Nach-dem-DAO-Hack-Verbliebenes-Kryptogeld-mit-freundlichem-Hack-gesichert-3246539.html
http://www.computerworld.ch/news/it-branche/artikel/politiker-wollen-tiefere-huerden-fuer-blockchain-gruender-70394
http://www.digitale-nachhaltigkeit.ch/2016/06/blockchain-motion

II. Ransomware – smart, greedy and unkillable

The demise of TeslaCrypt proves that even virtual blackmailers can eventually tire and give up. According to a report by BleepingComputer on 18 May, its developers had been pulling out gradually for weeks. Surprisingly, they even complied with a security expert's request to make the master key available online so that victims could decrypt all their data for free instead of paying a ransom. The BleepingComputer link below has detailed instructions for using the decoder.

Meanwhile, anyone whose hopes were raised by the three-week break taken by the Locky Trojan in June has been brought back down to earth with a bump. Locky is back and appears to be going all-out to live up to the dubious distinction of «most dominant ransomware distributed in spam e-mail» given to it by cybersecurity provider FireEye. The Trojan is now as active as before. Its developers seem to have used their break to come up with an insidious new version that is not only smarter, but also much greedier than Locky. Going by the name Bart, it also prompts Windows users to open an e-mail attachment. When they do so, it uses RockLoader and HTTPS to load their computers with malware that encrypts their data in the form of password-protected ZIP files, even if a firewall blocks any connection between the malware and the command-and-control server. Whereas the «industry standard» ransom for freeing kidnapped

data is half a Bitcoin (about CHF 300), Bart demands three Bitcoins (more than CHF 1,800)!

There is also bad news from the cyber hellhound Cerber. The encryption and blackmail Trojan now goes beyond taking data hostage and misuses targeted computers as bots to launch DDoS attacks on other targets. The people who discovered this published their findings under the heading «Two Attacks for the Price of One». It looks as though the pressure to make savings and improve efficiency has reached the virtual underworld.

So has the realisation that «smart» opens up a whole new world of possibilities. FLocker, for example, has been wreaking havoc on Android smartphones since April 2015, and a new version is targeting smart TVs. Security researchers at Trend Micro say that this TV-FLocker does not encrypt data but instead locks the screen and extracts data from the device, unless it is located in Armenia, Azerbaijan, Bulgaria, Georgia, Kazakhstan, Ukraine, Hungary or Russia. It is unclear at this stage whether this could be a clue to where the attack originated.

Read more here:

https://www.switch.ch/news/ransomware-day
http://www.20min.ch/digital/news/story/27616624
http://www.economiesuisse.ch/de/artikel/das-bewusstsein-erhöhen-für-internet-gefahren
http://www.bleepingcomputer.com/news/security/teslacrypt-shuts-down-and-releases-master-decryption-key
http://www.heise.de/security/meldung/I-f-Sorry-Bitte-benutzen-Sie-dieses-kostenlose-Entschluesselungs-Tool-3217315.html
https://www.fireeye.com/blog/threat-research/2016/06/locky-is-back-and-asking-for-unpaid-debts.html
http://www.heise.de/security/meldung/Locky-Sproessling-Erpressungs-Trojaner-Bart-verschluesselt-anders-und-verlangt-hohes-Loesegeld-3250058.html
http://www.heise.de/security/meldung/Neben-Erpressung-nun-auch-DDoS-Verschluesselungs-Trojaner-Cerber-lernt-dazu-3217254.html
https://www.invincea.com/2016/05/two-attacks-for-the-price-of-one-weaponized-document-delivers-ransomware-and-potential-ddos-attack
http://www.zdnet.de/88272059/ransomware-flocker-legt-android-basierte-smart-tvs-lahm/

III. CANVAS ready to launch – bridging cybersecurity and ethics

The growing complexity of the digital ecosystem and increasing global risks entail the danger that enforcing cybersecurity may bypass other fundamental values like freedom, equality, fairness and privacy. To counter this threat, a consortium called Constructing an Alliance for Value-driven Cybersecurity (CANVAS) will start work in September 2016. Scientists, engineers and data

protection experts from 11 institutions in seven European countries will create a network of IT developers and specialists in ethics, law and social sciences to conduct research in three main areas: the healthcare system, finance and law enforcement/national security. The aim is to start by taking stock of the current situation and then develop suitable briefing materials for politicians as well as a reference curriculum for ethics training for IT experts and a massive open online course (MOOC) for value-driven cybersecurity.

This topic is also a focus for the US Open Technology Fund, which finances the work of Ben Zevenbergen at the Oxford Internet Institute, part of the University of Oxford. Zevenbergen, a legal expert researching the ethics of networked systems, gave an impressive keynote speech at Troopers 16 in Heidelberg back in March. Based on his research findings, he put forward the interesting theory that IT developers primarily follow the utilitarian principle «the end justifies the means» and are thus diametrically opposed to the thinking of scholars in the fields of social science, philosophy and law, who believe that generally applicable ethical rules must be followed at all levels of a development process. He believes that, in an age when all areas of life are going digital, a symbiosis of both mindsets is needed. His conclusion: «To make the world a safer place, we don't just need the skills of engineers, we also need a moral framework.»

Read more here:

http://www.ethik.uzh.ch/de/ufsp/forschungsprojekte/nemos/forschungsprojekte/CANVAS.html
http://www.regensburg-digital.de/eine-bruecke-zwischen-cybersicherheit-und-ethik-das-canvas-konsortium/20052016
http://www.heise.de/security/meldung/Forschungsprojekt-Wie-gehen-Ethik-und-Cybersecurity-zusammen-3239827.html
https://www.researchgate.net/publication/289489876_Philosophy_Meets_Internet_Engineering_Ethics_in_Networked_Systems_Research
https://www.youtube.com/watch?v=9xEaokeP0mg

IV. US border guards want to be your Facebook friend – and other news on anti-terror measures

US Customs and Border Protection has proposed a change to the form for non-US citizens entering the country allowing them to enter their social media accounts and profile names – on a voluntary basis, at least to start with. The reason the

authority gives is to make it easier to contact travellers, but it is clear that it also hopes to facilitate investigations in connection with attacks or links to terror groups when needed. There are concerns that anyone who does not want their online communications spied on by the Americans will in future have to be much more careful with them before travelling to the US than certain presidential candidates have been.

The German government, too, has new ideas for shedding light on what it sees as a digital darkness spreading due to increased encryption by providers, WhatsApp messages and iPhone locking codes being two examples. If it has its way, a new security authority called Zitis will be created with 400 staff. It will develop decryption technology for the police, constitutional protection and criminal prosecution services that will allow them to intercept suspects' online communications despite provider-side encryption. Minister of the Interior Thomas de Maizière claims that the German law requiring police and intelligence staff to be separate will not be violated because Zitis itself will not collect data, it will only develop or procure the technology required to do so. Former Federal Commissioner for Data Protection and Freedom of Information Peter Schaar responded to the announcement of this new authority by pointing out that ever greater efforts are being made to bolster intelligence services, but not to improve data protection. It would appear that CANVAS (see III above) has not come a moment too soon.

Read more here:

http://www.theverge.com/2016/6/24/12026364/us-customs-border-patrol-online-account-twitter-facebook-instagram
https://www.wired.de/collection/life/bei-der-usa-einreise-koennten-bald-eure-social-media-profile-abgefragt-werden
http://www.computerworld.ch/news/it-branche/artikel/us-einreisebehoerden-wollen-zugriff-auf-social-media-accounts-70420
http://www.heise.de/security/meldung/Datenschuetzer-Peter-Schaar-kritisiert-Plaene-fuer-neue-Sicherheitsbehoerde-3249124.html

The SWITCHcert Security Report was written by Dieter Brecheis and Frank Herberg.