.

Bitstamp Incident Report

Privileged and Confidential

February 20, 2015

Table of Contents

I. INTRODUCTION.

This is a confidential report prepared by George Frost, General Counsel of Bitstamp Limited ("Bitstamp" or the "the Company"). This report includes information gleaned from Bitstamp's own records (including contemporaneous emails, forensic evidence and witness interviews), and derived from ongoing investigative reporting provided by the Stroz Friedberg private investigative group,[1] as well as investigators from the Secret Service, FBI and the UK's cyber-crime unit.

This is an active investigation. We believe we have identified at least one of the hackers and are baiting a "honey trap" to lure him into the UK in order to make an arrest. Moreover, we need to be very careful not to educate other criminal hackers about how we safeguard our assets and information. Accordingly, no part of this report may be made public or given to a third party without the prior express written permission of Bitstamp Ltd.

A. Company Background.

Bitstamp Limited is a UK chartered firm. At this time the firm also maintains approximately twenty-five support staff and servers in Slovenia, where the firm was founded. Bitstamp is creating a new operating company in Luxembourg, and is in the process of seeking licensing in Luxembourg as a payments provider. The new company will service only European customers. Similarly, a USA operating entity is also being established, which will serve only US residents.

Bitstamp operates a math-based "crypto-currency" trading platform via the World Wide Web, and has approximately 65,000 verified customers around the world, primarily based in Europe.

[1] Founded in 2000, Stroz Friedberg is an international investigations firm specialising in digital forensics, electronic disclosure, data breach and cybercrime response, as well as business intelligence services and investigations. Stroz Friedberg's management includes former prosecutors and former law enforcement officers with both government and private-sector experience in traditional and cyber-based investigations, digital forensics, data preservation and analysis, infrastructure protection, and electronic discovery.

Bitstamp's primary business is providing a marketplace that facilitates the purchase, trade and exchange of "Bitcoin" between customers by the creation and maintenance of Bitstamp accounts.

B. Fundamentals of Bitcoin.

'Bitcoin' is a digital, decentralized, partially anonymous protocol and currency that is not backed by any government or other legal entity. Bitcoin utilizes peer-to-peer transactions that are verified and recorded in a distributed public ledger called the "blockchain." Consequently, users of bitcoin can make transactions over the Internet directly with other users without needing an intermediary such as a bank. (Bitstamp's customers, however, utilize Bitstamp as an intermediary to maintain their bitcoin for them in a trading account. *See* below.)

Bitcoin utilizes public-key cryptography, which requires two separate cryptographic "keys": one private and one public. These keys have an exclusive mathematical relationship, so that it is possible for the public key to validate whether its corresponding private key has been used in a given cryptographic function. In the case of Bitcoin, the private key is used to create a digital signature for every transaction: the private key thus acts as confirmation of ownership of the bitcoins involved, and it should never be shared. The corresponding public key can then be used to verify the digital signature of the transaction i.e. that the initiator is indeed the owner of the bitcoins for that transaction. Public keys are also used to generate Bitcoin addresses to receive bitcoins from a transaction: only the holder of the corresponding private key can access the bitcoins in the address generated from the public key.

A Bitcoin address is an identifier of 26-35 alphanumeric characters, an example of which is 3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy. Bitcoin addresses are generated by "hashing" the public key. Hashing is a process by which a known algorithm, or mathematical formula, is calculated across a set of data, turning a large amount of data into a fixed-length hash value. The same hash value will always result from the same data. Modifying the data in any way will inevitably change the hash value. The resultant hash value is then converted into a format named Base-58. Base 58 is an encoding system that removes ambiguous characters, such as 0 and O. To complete the Bitcoin address, an identifying number of either 1 or 3 is added to the beginning, indicating that the address is a public Bitcoin network address representing a possible destination for a Bitcoin payment.

A Bitcoin "wallet" is a collection of private keys for a given user. The keys relate to the user's Bitcoin addresses, and provide the ability to conduct transactions to or from those addresses. A wallet is contained within a client, which is the software package providing the user with an interface to the Bitcoin network. A common name for a Bitcoin client wallet file is *wallet.dat*. A growing number of companies offer wallet services to their customers, and safeguard their bitcoin for them.

When a Bitcoin transaction takes place, the information about that transaction is stored within the "blockchain." The blockchain records how many bitcoins were involved in the transaction, the address they came from and the address to which the bitcoins were transferred. The "blockchain" ledger is public, making it is possible (although a bit arduous, until an automated search system is developed) to review historical transactions to determine how many bitcoins are held by each address and from where those bitcoins originated.

C. Bitstamp's transactional process.

Bitstamp's current transaction process works as follows:[2] A customer opens an account with Bitstamp through its website at https://www.bitstamp.net/. During the signup process, Bitstamp requires the customer's name, address, and proof of identity as part of its 'Know Your Customer' (KYC) policies and anti-money laundering (AML) procedures. No banking details or bitcoin deposit addresses are provided to customers until these checks have

[2] Our service providers and certain process features will change once we are operational in Luxembourg, and we will be adding more safeguards to this system, as detailed in our extensive filing with the CSSF.

been completed. Once a customer's account is opened, that customer can deposit cash from a bank account in their name to the Bitstamp client account, which is held with one of several commercial banks.

When funds are received from users into the Bitstamp client account, these are processed and credited into the user's ledger within Bitstamp's system as soon as possible. Bitstamp insists that all deposits into its bank account must come from a bank account in the user's name because the bank provides this information to Bitstamp. This helps prevent fraud, and ensures that Bitstamp will credit the correct user ledger in its system.

Once we have completed our AML procedures in relation to that user, a unique reference number is then automatically generated for that user. Our customers are required to use this as a reference on funds they transfer into Bitstamp's account with our bank (Reiffeisen, although we have other backup banks) to identify the ledger to which the funds should be credited.

The user's ledger with Bitstamp is in two parts – there is a balance in US dollars, and a balance in bitcoins (which will be 0 when the ledger is first opened). Although Bitstamp accepts deposits in almost all currencies, when funds are received they are imported into our system and allocated to a user's ledger converted into US dollars, which is done automatically using the Reiffeisen bank daily exchange rate. The ledger balance in Bitcoins is the user's Bitcoin wallet held within the Bitstamp system. Once the funds received have been credited to the user's Bitcoin ledger, they can trade on the platform and purchase Bitcoins.

The transfer of funds into bitcoins is not automatic, each user decides when and at what price he or she wishes to purchase (and sell) bitcoins. The user is fully in control of the transaction, Bitstamp simply provides the trading platform and credits user ledgers with funds received from Reiffeisen bank. When a user has funds in their account and wishes to use these to buy bitcoins, they will place an order. The dates and times of each order are recorded, although there can be a small delay between the order being placed and the trade taking place. [3]

When the system has matched up an order to sell bitcoins with an order to buy bitcoins, it automatically transfers the bitcoins from one user's bitcoin ledger to the other user's bitcoin ledger. The other type of transaction shown is a bitcoin withdrawal request, where bitcoins are withdrawn to a bitcoin wallet that may be a Bitstamp bitcoin wallet (i.e. a user bitcoin ledger) or a bitcoin wallet held outside the Bitstamp exchange. This is fairly simple and on both types of history provides a record of the date on which the user requested that a certain number of bitcoins were withdrawn from his or her ledger. It is possible to see the bitcoin wallet address to which the bitcoins were withdrawn. The withdrawal process is an automatic process, it is not done manually.

Once bitcoins are removed from the user's unique bitcoin ledger in Bitstamp's system, the transaction is generally irreversible. The whole bitcoin system was set up in this way so

[3] This is shown as "opened instant buy order" or "opened limit buy order". These are technical terms that refer to the two different ways in which a user may wish to buy Bitcoins. An instant order is where the user instructs Bitstamp's system immediately to buy Bitcoins using a certain number of dollars or sell a set number of Bitcoins. This, and all other orders, can be seen in the "order book" which is visible to all users on Bitstamp's website. The order book is a list of all orders that have been placed by Bitstamp's users. On receipt of an instant order, the system will immediately search the order book for the lowest price at which someone is willing to sell or buy Bitcoins and will use the specified funds to purchase or sell Bitcoins as appropriate. In the case of instant sell orders the highest price which is offered for the purchase of Bitcoins is used. In the case of instant buy orders the lowest price which is offered for the selling of Bitcoins is used. If there are an insufficient number of Bitcoins on sale at that lowest asking price to complete the order to the amount of US dollars the user has specified should be used, the system automatically searches again in 1 second intervals and will then purchase Bitcoins at the lowest possible price at that time, using the remaining dollars. The system continues to perform this process until all the funds specified by the user have been converted to Bitcoins, or until all the Bitcoins have been sold. The other type of order listed is a limit order. This is where a user specifies the number of Bitcoins he or she wishes to buy or sell, and the price at which he wants to buy or sell them. The system will then search all orders in the order book to match up the request with another order at the same price and then carry out the trade automatically. This means that the user does not need constantly to search the system for the price he or she wants, or wait until the right price becomes available. He can place the order and the system will perform the transaction when it finds the same price. If the system is only able to find 50% of the desired number of Bitcoins for sale at the price requested, it will purchase those Bitcoins and then wait until it next finds the remaining number of Bitcoins for sale at the price requested. Thus the entire order may take several minutes, or hours, to complete, depending on the availability of the number of Bitcoins for sale or purchase at the right price.

as to provide (partial) confidentiality and certainty for users, and to avoid the risk of charge backs (like those experienced by credit card users) which would bring uncertainty to transactions.

Bitstamp generates its transactional revenue by taking a percentage fee (graduated based on volume) from the dollar value of each trade. Bitstamp does not "monitor" individual trades and transactions as they are being performed. It would be virtually impossible to do so: up to 3,000 users may be accessing the site every second. Bitstamp will outline its security procedures below.

II. **INITIAL DISCOVERY AND RESPONSE TO THE HACKING INCIDENT.**

A. **Discovery of the Breach.**

Bitstamp first learned about the hacking incident on the evening of Jan. 4th. The CTO, Damian Merlak, first noticed the loss of bitcoins from the Bitstamp wallet at *circa* 2300 CET on 4 January 2015. Mr Merlak was in the USA, so he notified David Osojnik and Luka Kodric to investigate locally. After accessing the servers, Bitstamp staff noted a suspicious data transfer on the network logs, dated 29 December 2014, between 1129-1201 CET. The data transfer was approximately 3.5GB and was sent to an unfamiliar German IP address (185.31.209.128).

The data transfer struck an ominous chord because 3.5GB is the approximate size of the *wallet.dat* file containing Bitstamp's Bitcoin wallet [*see Appendix C for the log file relating to this transfer*].

Bitstamp personnel also checked the Bash history and noted file searches that had not been undertaken by our own staff. Mr. Merlak notified the CEO, also enroute to the USA on another flight, and the General Counsel, thus activating the Company's emergency response plan.

B. **Entry point.**

We soon learned from local forensic analysis that the transfer was initiated through a VPN connection from Mr Kodric’s laptop to the server hosting the Bitcoin wallet at Bitstamp’s data centre (LNXSRVBTC). At the time, Mr Kodric’s laptop was in the office and logged in to the network. The VPN connection to the data centre was restricted to three authorised IP addresses: Bitstamp’s office IP, Mr Merlak’s home IP, and Mr Kodric’s home IP. Two-factor authentication was not required to access the data centre from Mr Kodric’s laptop while it was logged in to the office network. Bitstamp therefore suspected that the attacker had remotely initiated the VPN connection in the background whilst Mr Kodric was working.

The theft required access to 2 servers in the data centre: LNXSRVBTC and DORNATA. The *wallet.dat* file was held on LNXSRVBTC. DORNATA held the passphrase to access the bitcoins held in the wallet. Checks by Bitstamp indicated that data was only taken from these two servers. Bitstamp found no evidence of access to other infrastructure. The content of the data transferred was not discernible from the network logs, only the volume of data.

Separately, on 4 January 2015, someone attempted to connect remotely to the Bitstamp office network, again using Mr Kodric’s account. VPN connections from an external IP address to the office network require two-factor authentication (as opposed to VPN connections to the data centre from the three permitted IP addresses, which do not). Between 0932–0955 CET, Mr Kodric received nine notifications on his mobile phone to provide secondary authentication for remote access to the office network from his account. These notifications are only generated once the correct username and password are entered. The remote log-in attempts were from an IP address in Romania (109.163.234.9).

Later on 4 January, the bitcoins started to drain from the Bitstamp wallet. This would not have required access to either the office or data centre VPN, since the attacker(s) already had the *wallet.dat* file and passphrase (from the 29 December transfers). 5000 bitcoins were in the wallet when it was exfiltrated on December 29, but over 18000 bitcoins were stolen in total due to additional deposits made before the theft was noticed. (Deposit volume was unusually high at this time, and a number of large "short" sellers appeared to have been accessing Bitstamp's market at the time.

Following our learning of the theft, Bitstamp employees were asked to keep their laptops turned off, and the servers were kept offline (but powered on). The General Counsel also conducted initial interviews and obtained early forensics, preparing to move forward with briefing the outside investigators from Stroz and various law enforcement authorities.

C. Incident Response Team.

Bitstamp immediately formed an incident response team to assess the loss, protect our customers from further attacks, and to investigate the breach. We set up a response HQ in the company's San Francisco offices, shared with our chief investor, Pantera Capital. The General Counsel notified law enforcement in the US[4] and in London,[5] and retained the Stroz Friedberg firm to assist us in the investigation.

The Stroz Friedberg team arrived at the Bitstamp office in Slovenia at 9 am on 8 January. After interviewing the staff with knowledge of the incident, they identified and catalogued all relevant electronic media from the office and data centre for analysis. The

[4] Our primary USA contact is Jon Rein, Special Agent, US Secret Service, San Francisco Field Office, 415-603-8935; jonathan.rein@usss.dhs.gov.

[5] Our primary UK contact is **Richard Butcher,** Major Investigation Team - Crime Directorate, Mobile: +44 (0) 772 521 9237; Email: Richard.Butcher@cityoflondon.pnn.police.uk

team followed formal "chain of custody" procedures at each step. The team then commenced taking forensic images of the media, including the following items:

- All 22 laptops that were in use on the corporate network.
- Priority virtual machines from physical servers at the data centre, including a logical capture from the local EMC storage.
- Data from both physical servers in the office (containing several internal virtual machines used on the network).

Approximately 13 Terabytes of data was collected in the first sweep, with further imaging ongoing. In addition to these items, there are two lower priority servers acquired for later analysis.

D. <u>Redeploying our Trading Platform.</u>

Pursuant to our incident response plan, we immediately retained a security firm (based in Berlin; which had done prior security work for us) to assist us in preventing further losses, identifying what happened and getting our exchange back on line.

Shortly after discovery of the attack, Bitstamp made an expensive but necessary decision to rebuild our entire trading platform and ancillary systems from the ground up, rather than trying to reboot our old system. We did this from a secure backup that was maintained (according to disaster recovery procedures) in a "clean room" environment. We also decided to deploy our distribution network using Amazon cloud infrastructure servers located in Europe.

By redeploying our system from a secure backup onto entirely new hardware, we were able to protect our customers from further mischief from the hacker, and to preserve all the potential evidence on Bitstamp's hard drives and peripherals for a full forensic investigation of the crime. We also took the opportunity to implement a number of new security measures (including multi-sig technology) and protocols so Bitstamp's customers could resume using Bitstamp with full confidence and trust.

E. Ensuring Transparency.

Also according to our incident response plan, we retained an outside firm to assist in messaging and dealing with customers, who were rightly concerned by the hacking incident and wanted assurances that their bitcoin was safe. We wanted to underscore that Bitstamp is not MtGox, in any respect.

The security of our customers' bitcoin and account information is our top priority, and as part of our stringent security protocol we temporarily suspended our services as of at 9 a.m. UTC on January 5th. Bitstamp was determined to be forthright and transparent in all our communications to customers and the media. We notified all customers by direct email, and posted updates on a temporary Bitstamp website; aided by our crisis team, we employed twitter, media interviews, and all other means available to keep them informed.

One principal message we needed to get out right away: customers should no longer make deposits to any previously issued Bitstamp bitcoin deposit addresses, which might have been compromised by the hacker. Another key message: All bitcoin held with us prior to the temporary suspension of Bitstamp services are completely safe and will be honored in full. Our bottom line: No customer bitcoin was lost, and no customer information was compromised; Bitstamp would be back in business as soon as possible, but only when we are certain we can do so safely.

E. Initial Damages Estimate.

Bitstamp is the sole victim in this incident, as the company used its own capital reserves and bitcoin reserves to cover the loss from its hot wallet. No customer funds or bitcoin were compromised, and we have found no reason whatsoever to believe that any customer account information or personal information was compromised.

The hacker was able to steal 18,866 bitcoins from a "hot wallet" residing on one of Bitstamp's servers. The lost coins had a contemporaneous market value of $5,263,614 based on the Bistamp clearing price of $279 per bitcoin at the time of the theft.

Bitstamp has lost customers, including major clients engaged in providing merchant services in bitcoin, and has suffered significant damage to its reputation, which we are unable to quantify exactly at this point, but which we believe exceeds $2 million. However, it appears that our quick response, transparency, and addition of new safeguards (*see below)* has won the loyalty of the vast majority of our customers.

In addition, we have paid out approximately $250,000 to programmers hired to rebuild and improve our platform; paid approximately $250,000 (and counting) to the Stroz Friedberg team; and at least $150,000 more for various security reviews, and legal and financial advice. These out of pocket costs are continuing to accrue.

In addition, to prevent future capital losses of this kind, we have contracted with a vendor to provide "multi-sig" technology to better protect our hot wallet (this particular transfer could not have happened today) and hired a skilled technology company, Xapo, to assist in managing our cold wallet. (This level of protection is very difficult to penetrate -- Xapo actually *splits apart* the individual cold wallet addresses of our depositors, storing them in secret locations in different parts of the world.) Finally, we are acquiring insurance coverage for *all* bitcoin deposits, thus preserving more of our own capital funds for growth, technological improvements and improved customer service.

III. CHRONOLOGY OF EVENTS FROM STROZ FRIEDBERG INVESTIGATION.

The methodology and technical detail of the investigation conducted by Stroz Friedberg are set out in more detail below. In this section we aim to provide a chronology of the attack as understood following Stroz Friedberg's review. An overview of the attack timeline is provided in Figure 1 below.

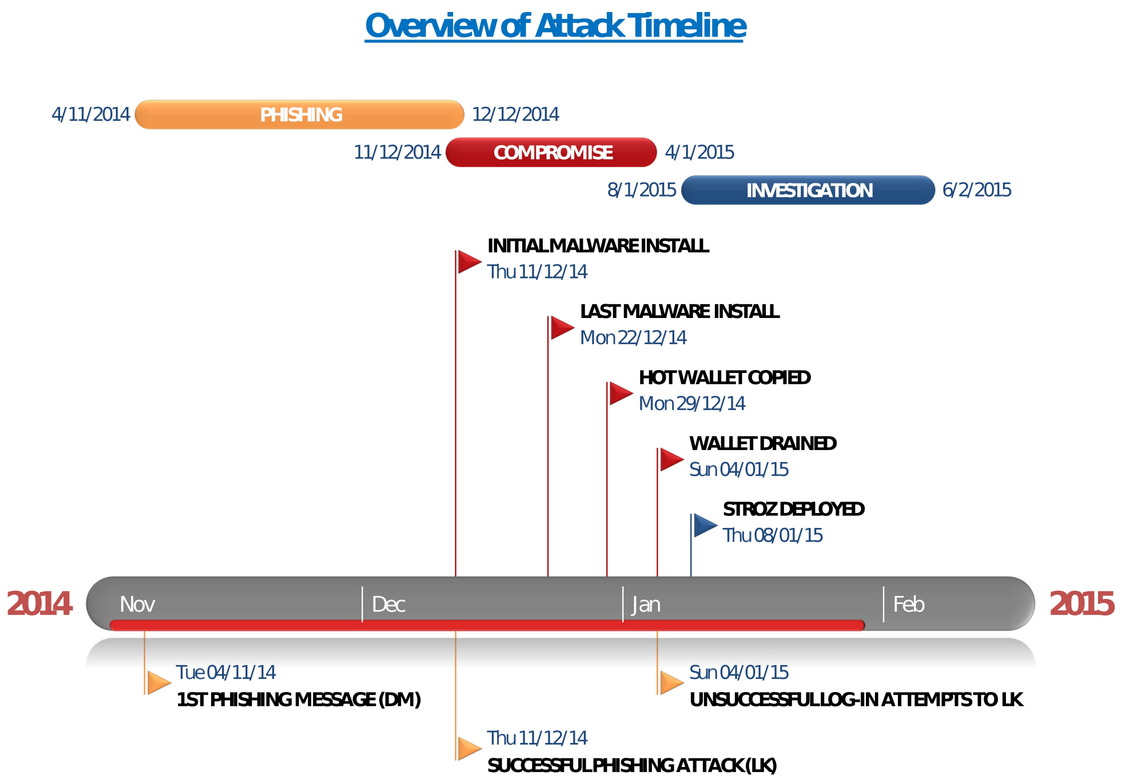


Figure 1: Timeline of Attack

The infection vector for the compromise was a targeted phishing campaign, with six employees known to have been targeted by the attacker in November / December 2014. The CTO, Damian Merlak, was the first employee identified as being targeted by the attacker. On 4 November 2014, Mr Merlak was contacted by Skype account punk.rock.holiday from IP address (94.185.85.171). The gambit for this phishing attack was to offer Mr Merlak free tickets to Punk Rock Holiday 2015. (Merlak is keen on punk rock and has played in a band.)

On 20 November, after a number of exchanges demonstrating persistent effort from the attacker, punk.rock.holiday sent a 'participant form' to Mr Merlak [Punk Rock Holiday 2015 TICKET Form1.doc]. This document contained obfuscated malicious VBA[6] script

[6] Visual Basic for Applications (VBA) is a programming language which enables certain functions to be built into the associated application (Word in this instance) and executed automatically. Such functions would include connections to websites or internet addresses

designed to call out to an external IP address and pull down a file to the victim computer. Although the document was opened on 20 November and 21 November, there is no indication that the script executed, and none of the indicators of compromise identified on other machines as part of the attack were found on DM's laptop. [*See Section III for further technical analysis of this phishing attack.*]

Over a period of approximately five weeks, four more Bitstamp employees received similar highly targeted phishing attacks, each tailored to individual interests. *It is worth noting that, however, that almost all of these targets lacked the Bitstamp security credentials to have allowed access to Bitstamp servers containing bitcoin or account information, much less a successful attack on Bitstamp's hot wallet.*

For example Tomaz Rozman was contacted by Skype account Thomas.wong.dhl from IP address 94.185.85.171. The pretext for this phishing attack was a potential offer of employment. On 5 December 2014, Skype account john.lucas.si (ostensibly a colleague of Thomas.wong.dhl) sent Mr Rozman a message containing candidate_questionnaire.doc, also from IP address 94.185.85.171. This document contained the same obfuscated malicious VBA script described above: if opened, it connected to IP address 185.49.68.164 and downloaded a malicious file named wordlib[1].zip [*see Section III for further technical analysis of this malware*].

Similarly, on 18 November 2014, COO Miha Grcar was contacted by Skype account ivan.foreignpolicy. Mr. Grcar is an avid policy and history buff, particularly with respect to Greece, where he previously worked as a reporter. No IP addresses were recoverable for the communications from this account at the time of our investigation. On this occasion, the suspected attacker was posing as a journalist and engaged Mr Grcar regarding articles he had previously written whilst working for Athens News. On 26 November, as part of this

from within an offline file (such as a Word document).

exchange, ivan.foreignpolicy attempted to send a word document of a recent article, ostensibly seeking comment from Mr Grcar. Mr Grcar declined to accept the document. Despite messages from the attacker persisting until 9 December, there was no sign of compromise on the laptop.

On 24 November 2014, Anzej Simicak was contacted by Skype Account suki_shah. This Skype account uses the same IP address as the other communications linked to the attacker (94.185.85.171). The attacker enquired about RippleWise, a platform for an alternative cryptocurrency (the Ripple). (Mr Simicak is COO for RippleWise as well as working at Bitstamp.) Mr Simicak asked the attacker to utilize his RippleWise account for further communications, and there is no trace of either the malicious word documents, or the associated malware, on Mr Simicak's laptop.

On 9 December 2014, Miha Hrast was contacted by Skype account pixi.jenny.hachmeister from IP address 94.185.85.171. According to his LinkedIn profile, Mr Hrast previously worked at Pixi Labs, so this attack too, was tailored specifically for this target. Two files were transferred successfully from pixi.jenny.hachmeister to Mr Hrast: *Pixi-_Post_Employment_Questionnaire.rar* on 11 December and *Pixi_Post_Employment_Questionnaire.doc* on 12 December. The *.doc* file contained obfuscated malicious VBA script which, when opened, downloaded the malicious file *wordcomp[1].zip* from IP address 185.31.209.145. However, Hrast did not and will not have access to the hot wallet.

On 9 December 2014, Bitstamp's Systems Administrator, Luka Kodric, received a phishing email to his Gmail account. Unlike some of the others targets, Kordic *did* have access to Bitstamp's hot wallet. The email header had been spoofed to appear as if it had been sent from konidas@acm[.]org, although it was actually received from a Tor exit node [the email chain and header details can be seen in full at Appendix A]. ACM is the

Association for Computing Machinery, which describes itself as the world's largest educational and scientific computing society. The sender was offering Mr. Kodric the opportunity to join Upsilon Pi Epsilon (UPE), the International Honour Society for the Computing and Information Disciplines. The UPE site is hosted within the acm.org domain. On 11 December, as part of this offer, the attacker sent a number of attachments. One of these, *UPE_application_form.doc*, contained obfuscated malicious VBA script. When opened, this script ran automatically and pulled down a malicious file from IP address 185.31.209.145, thereby compromising the machine.

On 12 December 2014, the attacker switched to Skype messaging with Mr Kodric, using Skype account upsilon_pi_epsilon from IP address 94.185.85.171. Further malicious executables were then created on Mr Kodric's laptop on 17,18 and 22 December [*see Section III for further technical analysis of this malware*]. On 23 December, Mr Kodric's account logged in to LNXSRVBTC a number of times. Mr Kodric believed these log-ins were probably the attacker, although he could not confirm with absolute certainty that this was not his own legitimate activity.

On 29 December 2014, SSH logs show that Mr Kodric's account logged in to LNXSRVBTC and the DORNATA server at the data centre. On this occasion, Mr Kodric was certain that these log-ins were not made by him, and must therefore have been the attacker. Analysis indicates that the attacker accessed LNXSRVBTC, where the *wallet.dat* file was held, and the DORNATA server, where the passphrase for the Bitcoin wallet was stored, before data was transferred out of both servers to IP address 185.31.209.128, which is part of a range owned by a German hosting provider. We suspect that the attacker copied the Bitcoin wallet file and passphrase at this stage, due to the correlation between the size of these files and the size of the data transfer seen on the logs, although the actual content of the transfers cannot be confirmed from the logs available. Together the wallet and passphrase would have enabled the attacker to steal the bitcoins from the Bitcoin wallet.

On 4 January, the attacker drained the Bitstamp wallet, as evidenced on the blockchain. Although the maximum content of this wallet was 5000 bitcoins at any one time, the attacker was able to steal over 18,000 bitcoins throughout the day as further deposits were made by customers.

IV. TECHNICAL ANALYSIS.

A. Materials Relied Upon.

During the course of its investigation, Stroz Friedberg collected the following materials from Bitstamp. All materials were preserved locally in Slovenia, unless specifically stated.

Serial	Type	Make / Model	Name	Location	Date
ES001	Laptop	Lenovo Thinkpad L530	Grcar, Miha	Bitstamp, Slovenia	08/01/2015
ES002	Laptop	Lenovo Thinkpad L540	Bertoncelj, Tomaz	Bitstamp, Slovenia	08/01/2015
ES003	Laptop	Lenovo Thinkpad L530	Rogan, Marko	Bitstamp, Slovenia	08/01/2015
ES004	Laptop	Lenovo Thinkpad L540	Rozman, Tomaz	Bitstamp, Slovenia	08/01/2015
ES005	Laptop	Lenovo Thinkpad L540	ANZEJ, ANZEJ	Bitstamp, Slovenia	08/01/2015
ES006	Laptop	Lenovo Thinkpad T440p	Kodric, Luka	Bitstamp, Slovenia	08/01/2015
ES006_MEM	Memory	Lenovo Thinkpad T440p	Kodric, Luka	Bitstamp, Slovenia	08/01/2015
ES007	Laptop	Lenovo Thinkpad L540	Srecnik, Nejc	Bitstamp, Slovenia	08/01/2015
ES008	Laptop	Lenovo Thinkpad L530	Hrast, Miha (original)	Bitstamp, Slovenia	08/01/2015
ES009	Laptop	Lenovo Thinkpad L540	Skumavc, Janez	Bitstamp, Slovenia	08/01/2015
ES010	Laptop	Lenovo Thinkpad L530	Hrast, Miha (replacement)	Bitstamp, Slovenia	08/01/2015
ES011	Laptop	Lenovo Thinkpad L540	Regouc, Jan	Bitstamp, Slovenia	08/01/2015
ES012	Laptop	Lenovo Thinkpad L540	Bezan, Jure	Bitstamp, Slovenia	08/01/2015
ES013	Laptop	Lenovo Thinkpad L540	Petrevcic, Janez	Bitstamp, Slovenia	08/01/2015
ES014	Laptop	Lenovo Thinkpad L530	Potisek, Benedikt	Bitstamp, Slovenia	08/01/2015
ES015	Laptop	Lenovo Thinkpad L540	Pristov, Rok	Bitstamp, Slovenia	08/01/2015
ES016	Laptop	Lenovo Thinkpad L540	Vezzosi, Luka	Bitstamp, Slovenia	08/01/2015
ES017	Laptop	Lenovo Thinkpad L530	Stucin, Rok	Bitstamp, Slovenia	08/01/2015
ES018	Laptop	Lenovo Thinkpad L540	Grilc, Klemen	Bitstamp, Slovenia	08/01/2015
ES019	Laptop	Lenovo Thinkpad L540	Steblaj, Blaz	Bitstamp, Slovenia	08/01/2015
ES020	Laptop	Lenovo Thinkpad L540	Eri, Marko	Bitstamp, Slovenia	08/01/2015
ES021	Server	HP Proliant ML350p Gen8	WINSRV02 192.168.100.31	Bitstamp, Slovenia	09/01/2015
ES022	Server	HP Proliant ML350p Gen8	WINSRV01 192.168.100.30	Bitstamp, Slovenia	08/01/2015
ES023	Laptop	Lenovo Thinkpad L540	N/K	Bitstamp, Slovenia	08/01/2015
ES024	Laptop	Lenovo Thinkpad L530	Kodric, Luka	Bitstamp, Slovenia	08/01/2015
ES025	Server	HP Proliant DL380p Gen8	LNXSRVDB1	Bitstamp, Slovenia	10/01/2015
ES026_A	Server	HP Proliant DL380p Gen8	BURZUM var/log only	Bitstamp, Slovenia	10/01/2015
ES026_B	Server	LVM Linux Logical Partition	MAYHEM	Bitstamp, Slovenia	10/01/2015
ES026_C	Server	LVM Linux Logical Partition	DORNATA	Bitstamp, Slovenia	10/01/2015
ES027_A	Server	HP Proliant DL380p Gen8	LNXSRVKVM1 var/log only	Bitstamp, Slovenia	10/01/2015
ES027_B	Server	LVM Linux Logical Partition	LNXSRVCACTI	Bitstamp, Slovenia	10/01/2015
ES027_C	Server	LVM Linux Logical Partition	LNXSRVBTC	Bitstamp, Slovenia	10/01/2015
ES028	Server	HP Proliant DL380p Gen8	LNXSRVWWW1	Bitstamp, Slovenia	10/01/2015
ES029	Server	EMC2 VNX Series e3150	EMCStorage01	Bitstamp, Slovenia	10/01/2015
ES030	Server	HP Proliant DL380p Gen8	VADER var/log only	Bitstamp, Slovenia	10/01/2015
ES031	Email	Gmail Account	Kodric, Luka	Stroz Friedberg, London	13/01/2015
ES032	Server	LVM Linux Logical Partition	LNXSRVDB2 var/log only	Stroz Friedberg, London	13/01/2015
ES033	Laptop	Lenovo Thinkpad L540p	Kodric, Nejc	Bitstamp, Slovenia	21/01/2015
ES034	Laptop	Lenovo Thinkpad L540	Ribnikar, Kaja	Bitstamp, Slovenia	21/01/2015
ES035	Laptop	Lenovo Thinkpad T430	Merlak, Damian	Bitstamp, Slovenia	21/01/2015
ES036	Laptop	Apple A1398 MacBook Pro	Merlak, Damian	Bitstamp, Slovenia	21/01/2015
ES037	Server	LVM Linux Logical Partition	LNXSRVDB2	Bitstamp, Slovenia	21/01/2015
ES038	Logs	N/A N/A	CACTI GUI log Output	Bitstamp, Slovenia	21/01/2015
ES039	Laptop	Lenovo Thinkpad L540	Graftieaux, Jean-Baptiste	Stroz Friedberg, London	30/01/2015

Table 1: Materials Collected

Stroz Friedberg analysed all 27 laptops listed in Table 1. Six machines relating to named individuals contained evidence of a targeted phishing attack, with four individuals receiving poisoned attachments, three machines showing signs of additional malware being downloaded and one victim having been fully compromised with a Remote Access Trojan. An overview of key attacker activity leading to the eventual theft of the bitcoins can be seen in Figure 2 below.

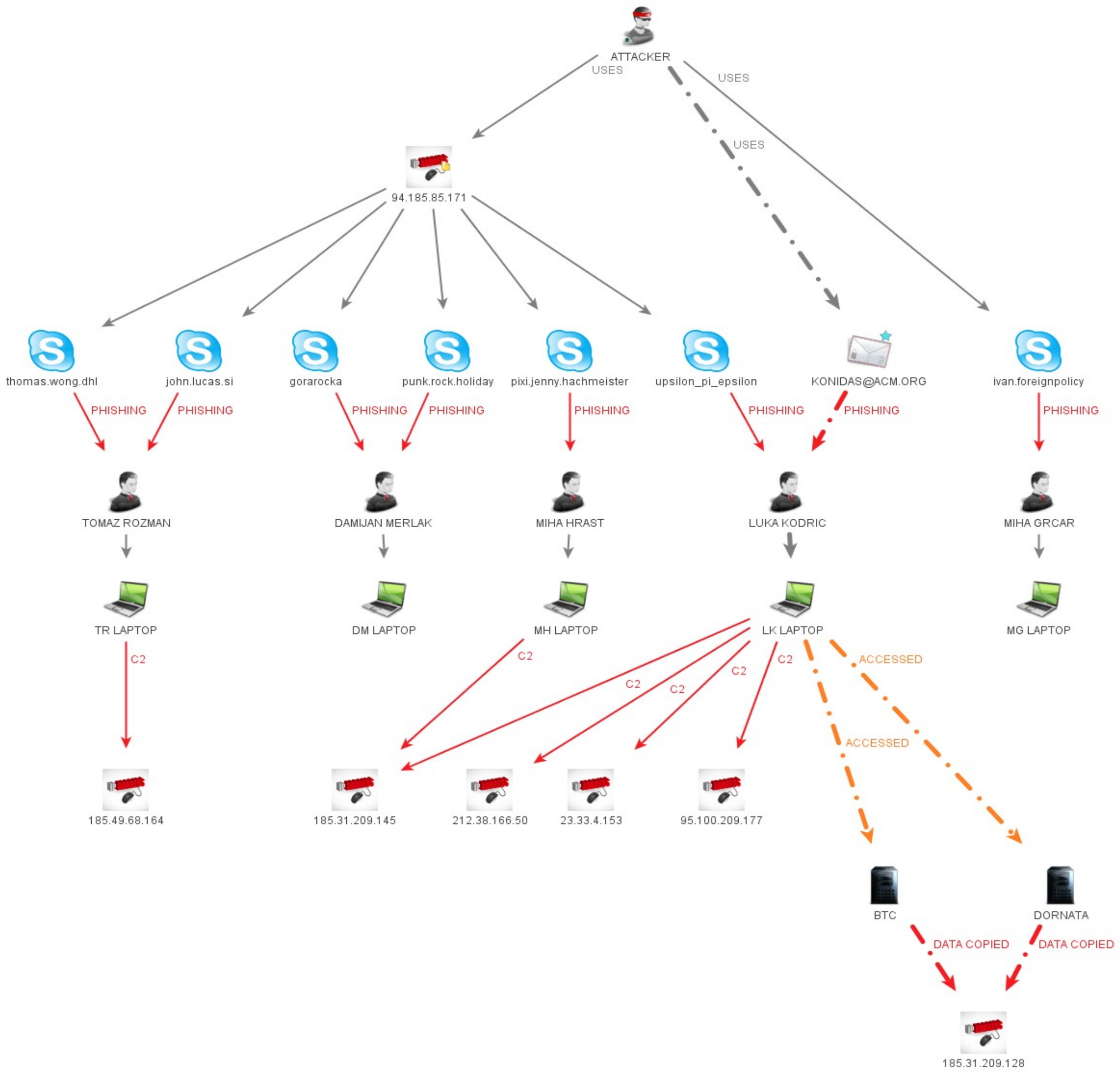


Figure 2: Overview of Attacker Activity

Stroz Friedberg's investigation uncovered evidence that six Bitstamp employees were targeted by phishing emails in total, although only four of these resulted in malicious attachments being received. Miha Grcar refused to accept any attachments and Anzej Simicak, a contractor, was contacted in relation to another company he works for, so continued the conversation outside the Bitstamp network. All of the phishing messages were highly tailored to the victim, and showed a significant degree of background knowledge on the part of the attacker.

B. <u>Damian Merlak's Laptop</u>.

Analysis of the file (Punk_Rock_Holiday_2015_TICKET_Form1.doc) from Mr Merlak's laptop revealed that the malicious VBA script was not password protected as with the other phishing documents, although it is very similar in terms of structure and obfuscation. The author of this document is listed as 'KVBGuhcvk'. A number of online security resources, such as VirusTotal, identify files with this same author listed, using the same type of VBA exploit for various scams or attacks. An initial review indicates that some of these were high volume phishing scams serving up banking malware dating back to October 2014. Documents containing this script and linked to this author would, therefore, have been widely available by the time Mr Merlak was targeted. This author name does not, therefore, necessarily directly link the Bitstamp theft to the previous attackers. The malicious code attempts to pull a file (img_0923.png) from IP address 5.196.140.211. Analysis from VirusTotal links this IP address (which is part of a range allocated to a French hosting service) with the previous distribution of malicious content. From our analysis, it appears that the VBA code was designed to download img_0923.png, rename it to AMFVKZKFCBS.exe, and execute it. We did not see any indication that AMFVKZKFCBS.exe was accessed, downloaded or executed on Mr Merlak's laptop, however. The attacker also used Skype account gorarocka and provided a contact email address of ivan.punk.slov@gmail.com during his exchange with Mr Merlak. On 29 December (18:22:47), Mr Merlak also received a Skype message from tim.lewkow stating that “The Bitstamp hot wallet has a near zero BTC balance.” Stroz Friedberg does not know whether this message was connected to the attack, but it is notable because the wallet was also transferred by the attacker on 29 December.

C. **Tomas Roman’s Laptop**.

Stroz Friedberg identified two separate malware files on Mr Roman’s laptop as a result of this attack. The first of these, *wordlib[1].zip*, was pulled down from IP address 185.49.68.164 on 5 December after Mr Rozman opened Candidate_questionnaire.zip. This file contained the same obfuscated malicious VBA script as seen on Mr Merlak’s computer, although this time it was password protected. This file is the earliest file we have observed that resulted in the successful download of one of the attacker’s malicious payloads. However, our analysis indicates that this malware failed to execute properly.

On 11 December, the second malware file, wordcomp[1].zip, was downloaded from IP address 185.31.209.145 after Mr Rozman opened Int_GmbH_dhl_mutual_non-disclosure_agreement.doc. Once again, the malware failed to execute properly.

D. **Miha Grcar’s Laptop.**

There were no recoverable log files relating to the IP address for Mr Grcar’s Skype contact with ivan.foreignpolicy. However, the unsolicited nature of the contact, the attempt to inveigle Mr Grcar in to opening an attachment, and the complete lack of verifiable background data on the pseudonym used are all consistent with the confirmed attacker communications.

E. **Miha Hrast’s Laptop**.

A review of the application event logs from Mr Hrast’s laptop show a recorded warning with the following details, explaining why the malware executable was not run:

Access to C:\Users\MIHA~1.HRA\AppData\Local\Temp\AMFVKZKFCBS.exe has been restricted by your Administrator by the default software restriction policy level. There are also references to the wordcomp.zip and also the AMFVKZKFCBS.exe file within a file generated by Microsoft Security Essentials named 'MpWppTracing-12122014-082330-00000003-ffffffff.bin' suggesting that these two files were flagged by the Microsoft Security Essentials program installed on the laptop.

F. Luka Kodric's Laptop.

Mr Kodric was the first employee whom we identified as being initially targeted through email, rather then Skype. The attacker ostensibly emailed Mr Kodric from address konidas@acm.org, but analysis of the header information reveals that all of the emails originated from mail servers hosted by a Greek ISP (otenet.gr) which is not designated as a permitted sender for the acm.org domain[7]. The attacker connected to the mail servers through various Tor exit nodes, thereby disguising his own IP address. His mail client registered as being set to UTC +0400 for all communications[8].

The malicious VBA script contained within the 2_UPE_application_form.doc emailed to Mr Kodric pulled down a large programme, wordcomp[1].zip. This is identical to the file of the same name found on Mr Rozman's laptop, and was downloaded from the same IP address. Despite the file extension, the file is actually an executable. Upon execution, the file installs itself to the registry location 'Software\Microsoft\Windows\CurrentVersion\Run' to achieve persistence on the machine. The executable was UPX-packed (meaning the UPX programme had been used to compress the file size and thereby disguise the signature of the original executable).

[7] Based on Sender Policy Framework. Further details can be found in Appendix A and at www.openspf.org/.

[8] The UTC time zone covers, *inter alia*, western Russia, Georgia and Armenia, as well as UAE and parts of eastern Africa. This does not, however, mean that the attacker is physically located in this zone.

The wordcomp[1].zip is file a highly sophisticated programme with diverse functionality. It could provide an attacker with: access to the host machine's registry; access to its clipboard; emulation of mouse movements; possible keyboard logging capability (these functions may be used or may be the result of importing whole libraries). At the time of analysis, it was not detected when submitted to major AV providers.

Our analysis of wordcomp[1].zip indicates that it is designed to call IP address 217.12.202.34, and possibly to hxxp://advermarket.net and hxxp://advermarketnonfree.net[9]. The wordcomp[1].zip file also contains thousands of domain names, such as homeftp.org, kimino.gifu.jp, and Cambridge.museum. The exact purpose of these is unclear, although it is consistent with click-fraud malware where legitimate referring URLs are coded into the malware. It is therefore possible that this is a multi-functional malware, with only part of its capability being used for this attack.

In addition to wordcomp[1].zip, we also found malware files named wf.exe, mso2010.exe and office.exe. We could not determine the provenance of these files from the log data available at the time of the investigation, and comprehensive reverse engineering of the malware files has not been conducted. Analysis of wf.exe identified that it drops a driver, winntdrv.sys, which could possibly be a rootkit (software designed to hide the existence of certain processes or programs and enable continued privileged access to a computer) onto the host machine. This file contains the string ssdthook: an SSDT hook is a type of rootkit. The file calls out to IP address 212.38.166.40. wf.exe and mso2010.exe are the "same" program in terms of functionality. However, they are merely unpackers for the majority of the binary data.

G.Server Analysis.

[9] 'http' has been replaced with 'hxxp' as a precaution to prevent readers accidentally linking to the malicious URL.

Our investigation strongly indicated that the attacker accessed two servers directly, LNXSRVBTC and DORNATA, and had access to information held on the EMC server through DORNATA. We did not find any sign of intrusion into, or exfiltration of data from, any other servers from the data available at the time of our investigation.

During our review of the servers, we discovered a gzip file on DORNATA, which was created a few minutes before the attacker sent data to the German server (29 December 2014, 1129-1201CET). While we cannot confirm whether the file itself was exfiltrated, it was clearly accessed by the attacker shortly before the attacker exfiltrated data. This folder is a zip of the /srv folder contained on DORNATA. The /srv folder contains the bitstamp.net.key file, as well as what appears to be a small amount of source code. One of the subfolders of /srv is "uploads" (/srv/bitstamp/uploads). That uploads folder is a link to //emcshare00. The zip file contains a substantial amount of information from the "account_history" sub-folder relating to customer account interactions. Our review has not identified any personally identifiable information or financial data in the account_history folder. It does, however, demonstrate that the attacker had access to the EMC server through DORNATA.

H. Other Media.

Our investigators conducted analysis of all the machines listed in Table 1. We did not find any known indicators of compromise for this attack on machines other than those specifically referenced above.

V. CONCLUSION.

Based on our investigation, we believe that this was a highly targeted attack undertaken by a determined attacker, who showed a very degree of operational security and technical sophistication. The phishing attacks were highly tailored and appeared, at least initially, credible to the recipients. The attacker only ever targeted a small number of victims simultaneously, and persevered in the face of apparent disinterest on the part of his interlocutors. As an example, Mr Merlak required 11 prompts to respond on one occasion.

The attacker communications, whether Skype or email, were all channelled through an anonymous proxy in order to protect the identity of the sender. The infrastructure used to support the attack, such as the servers used to deliver the malware files or the destination server for the bitcoin wallet theft, are part of hosted infrastructure across multiple jurisdictions, leaving limited opportunity for further investigation. Based on the data available at the time of the investigation, the attacker's activity within the network also appeared to be focused and left minimal footprint. The malicious VBA script used in the initial compromise shows signs of being a multi-purpose crime tool. However, both had been significantly modified so as to evade major AV software. This tailoring and obfuscation enabling it to evade AV products indicates that the attackers had a high degree of sophistication and experience in this field, as it reduces the ability for attribution.

This was a significant loss for Bitstamp, and it cast further doubt on the safety and integrity of the bitcoin ecosystem. However, it could have been much worse, and we are determined to use this as a learning tool, and as a basis for making improvements in our technology, security protocols, incident response planning and so forth.

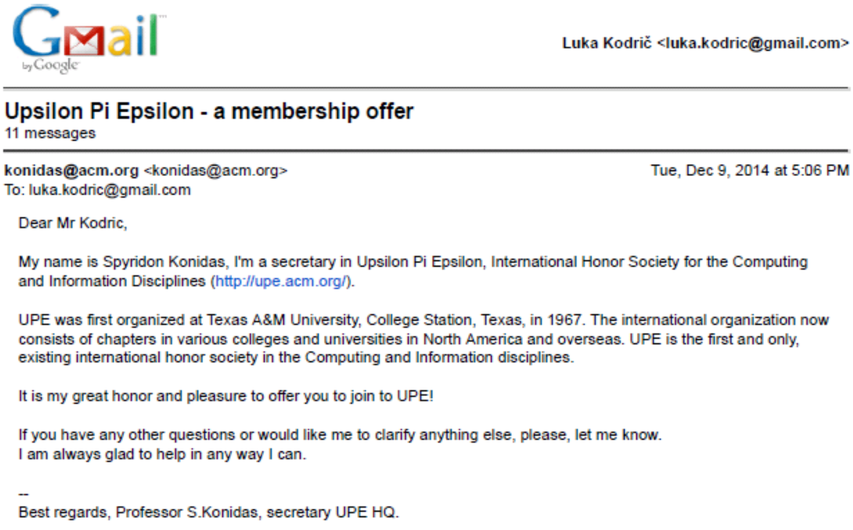
Bitstamp was the first exchange to implement the hot and cold wallet system, and it worked as designed. We lost only a small portion of the bitcoin placed with us, and we covered all losses from our own reserves. No customer funds or data were lost. And because of our nimble disaster recovery efforts, we were able to get up and operating within days after the hack — standing up a completely new and "clean" instance of our trading platform, while preserving all the prior servers and laptops for evidentiary purposes.

Following this criminal attack, Bitstamp has instituted additional industry-leading protections — we are first to be using multi-sig to protect our hot and cold wallets, and are obtaining insurance coverage for all funds. We are undergoing a top to bottom security review by a third party, and will make whatever changes are indicated. (A few of these are obvious – we have implemented FireEye email and internet screening software; we will require multi-sig approvals for any and all access to the hot wallet; and we will ensure that any manager's laptop with access to bitcoin deposits or sensitive customer information is highly restricted, and "single purpose," i.e., it does not also have capabilities to receive email, engage in skype calls, or cruise the internet.

Finally, Bitstamp is working closely with the Secret Service, FBI and UK cybercrime investigators to apprehend and prosecute the hacker, and we are very close to doing so. We intend to be industry leaders in developing technology and practices to fully safeguard our customers' assets and sensitive information, and we will share what we have learned to assist others in the Bitcoin ecosystem, including regulators and law enforcement.

Any questions or comments may be directed to George Frost, General Counsel, at geofrost@comcast.net.

APPENDIX A – Luka Kodric Phishing Email & Headers



Luka Kodrič <luka.kodric@gmail.com>

Upsilon Pi Epsilon - a membership offer
11 messages

konidas@acm.org <konidas@acm.org> Tue, Dec 9, 2014 at 5:06 PM
To: luka.kodric@gmail.com

Dear Mr Kodric,

My name is Spyridon Konidas, I'm a secretary in Upsilon Pi Epsilon, International Honor Society for the Computing and Information Disciplines (http://upe.acm.org/).

UPE was first organized at Texas A&M University, College Station, Texas, in 1967. The international organization now consists of chapters in various colleges and universities in North America and overseas. UPE is the first and only, existing international honor society in the Computing and Information disciplines.

It is my great honor and pleasure to offer you to join to UPE!

If you have any other questions or would like me to clarify anything else, please, let me know.
I am always glad to help in any way I can.

--
Best regards, Professor S.Konidas, secretary UPE HQ.

```
Delivered-To: luka.kodric@gmail.com

Return-Path: <konidas@acm.org>

Received: from echidna.otenet.gr (smtp-out33.otenet.gr. [83.235.69.33])

      by mx.google.com with ESMTP id vf7si2735363wjc.81.2014.12.09.08.06.43

      for <luka.kodric@gmail.com>;  Tue, 09 Dec 2014 08:06:44 -0800 (PST)

Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not

designate 83.235.69.33 as permitted sender) client-ip=83.235.69.33;

Received: from [0.0.0.0] (tor-exit3-readme.dfri.se [171.25.193.235])

         by echidna.otenet.gr (ESMTP) with ESMTPSA

         for <luka.kodric@gmail.com>; Tue,  9 Dec 2014 18:06:36 +0200 (EET)

Message-ID: <54871E0A.6070100@acm.org>

Date: Tue, 09 Dec 2014 20:06:34 +0400

From: "konidas@acm.org" <konidas@acm.org>

To: luka.kodric@gmail.com

Subject: Upsilon Pi Epsilon - a membership offer
```

```
--------------------------------------------------------------------------
Delivered-To: luka.kodric@gmail.com
Return-Path: <konidas@acm.org>
Received: from sphinx.otenet.gr (smtp-out34.otenet.gr. [83.235.69.34])
      by mx.google.com with ESMTP id dh10si16780784wib.80.2014.12.09.12.57.23
      for <luka.kodric@gmail.com>;     Tue, 09 Dec 2014 12:57:23 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not
designate 83.235.69.34 as permitted sender) client-ip=83.235.69.34;
Received: from [0.0.0.0] (195-154-215-83.rev.poneytelecom.eu [195.154.215.83])
         by sphinx.otenet.gr (ESMTP) with ESMTPSA
         for <luka.kodric@gmail.com>; Tue,  9 Dec 2014 22:57:20 +0200 (EET)
Message-ID: <5487622A.7010002@acm.org>
Date: Wed, 10 Dec 2014 00:57:14 +0400
From: "konidas@acm.org" <konidas@acm.org>
To: Luka Kodric <luka.kodric@gmail.com>
Subject: Re: Upsilon Pi Epsilon - a membership offer
--------------------------------------------------------------------------
Delivered-To: luka.kodric@gmail.com
Return-Path: <konidas@acm.org>
Received: from medusa.otenet.gr (smtp-out31.otenet.gr. [83.235.69.31])
      by mx.google.com with ESMTP id wx8si6324074wjb.75.2014.12.10.00.43.23
      for <luka.kodric@gmail.com>;       Wed, 10 Dec 2014 00:43:24 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not
designate 83.235.69.31 as permitted sender) client-ip=83.235.69.31;
Received: from [0.0.0.0] (cs-tor.bu.edu [204.8.156.142])
```

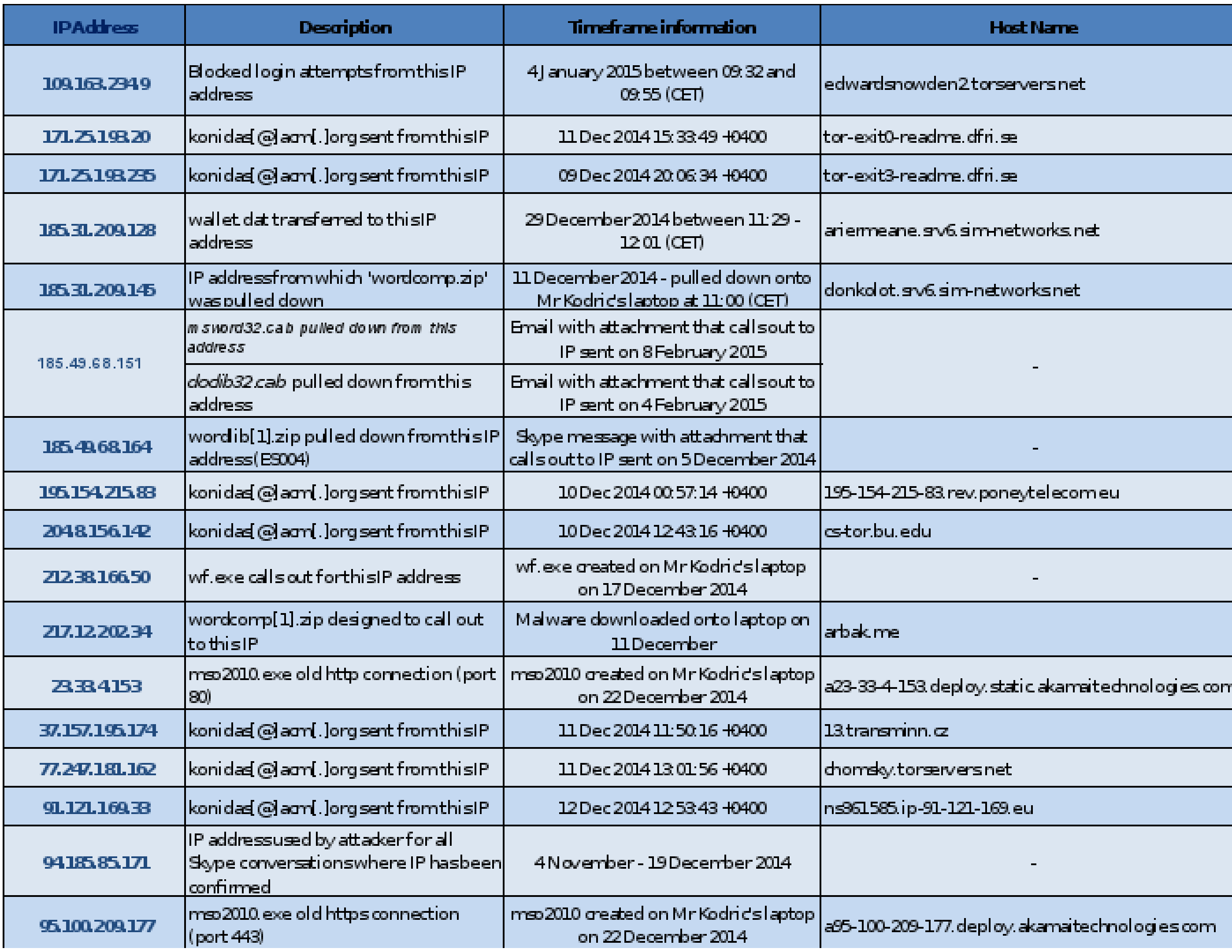
```
          by medusa.otenet.gr (ESMTP) with ESMTPSA
          for <luka.kodric@gmail.com>; Wed, 10 Dec 2014 10:43:20 +0200 (EET)
Date: Wed, 10 Dec 2014 12:43:16 +0400
From: "konidas@acm.org" <konidas@acm.org>
To: Luka Kodric <luka.kodric@gmail.com>
Subject: Re: Upsilon Pi Epsilon - a membership offer
---------------------------------------------------------------------------
Return-Path: <konidas@acm.org>
Received: from sphinx.otenet.gr (smtp-out34.otenet.gr. [83.235.69.34])
      by mx.google.com with ESMTP id r5si642001wjy.74.2014.12.10.23.50.26
      for <luka.kodric@gmail.com>;      Wed, 10 Dec 2014 23:50:28 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not
designate 83.235.69.34 as permitted sender) client-ip=83.235.69.34;
Received: from [0.0.0.0] (13.transminn.cz [37.157.195.174])
          by sphinx.otenet.gr (ESMTP) with ESMTPSA
          for <luka.kodric@gmail.com>; Thu, 11 Dec 2014 09:50:21 +0200 (EET)
Date: Thu, 11 Dec 2014 11:50:16 +0400
From: "konidas@acm.org" <konidas@acm.org>
To: Luka Kodric <luka.kodric@gmail.com>
Subject: Re: Upsilon Pi Epsilon - a membership offer
---------------------------------------------------------------------------
Delivered-To: luka.kodric@gmail.com
Return-Path: <konidas@acm.org>
Received: from sphinx.otenet.gr (smtp-out34.otenet.gr. [83.235.69.34])
      by mx.google.com with ESMTP id ev3si2703692wic.87.2014.12.11.01.02.07
```

```
    for <luka.kodric@gmail.com>;     Thu, 11 Dec 2014 01:02:08 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not
designate 83.235.69.34 as permitted sender) client-ip=83.235.69.34;
Received: from [0.0.0.0] (chomsky.torservers.net [77.247.181.162])
      by sphinx.otenet.gr (ESMTP) with ESMTPSA
      for <luka.kodric@gmail.com>; Thu, 11 Dec 2014 11:01:59 +0200 (EET)
Date: Thu, 11 Dec 2014 13:01:56 +0400
From: "konidas@acm.org" <konidas@acm.org>
To: Luka Kodric <luka.kodric@gmail.com>
Subject: Re: Upsilon Pi Epsilon - a membership offer
--------------------------------------------------------------------------
Delivered-To: luka.kodric@gmail.com
Return-Path: <konidas@acm.org>
Received: from chimaera.otenet.gr (smtp-out32.otenet.gr. [83.235.69.32])
    by mx.google.com with ESMTP id lc9si1744680wjc.9.2014.12.11.03.33.55
    for <luka.kodric@gmail.com>;     Thu, 11 Dec 2014 03:33:55 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not
designate 83.235.69.32 as permitted sender) client-ip=83.235.69.32;
Received: from [0.0.0.0] (tor-exit0-readme.dfri.se [171.25.193.20])
      by chimaera.otenet.gr (ESMTP) with ESMTPSA
      for <luka.kodric@gmail.com>; Thu, 11 Dec 2014 13:33:52 +0200 (EET)
Date: Thu, 11 Dec 2014 15:33:49 +0400
From: "konidas@acm.org" <konidas@acm.org>
To: Luka Kodric <luka.kodric@gmail.com>
Subject: Re: Upsilon Pi Epsilon - a membership offer
```

```
--------------------------------------------------------------------------------

Delivered-To: luka.kodric@gmail.com
Return-Path: <konidas@acm.org>
Received: from medusa.otenet.gr (smtp-out31.otenet.gr. [83.235.69.31])
        by mx.google.com with ESMTP id o2si1172889wjy.79.2014.12.12.00.53.49
        for <luka.kodric@gmail.com>;        Fri, 12 Dec 2014 00:53:49 -0800 (PST)
Received-SPF: softfail (google.com: domain of transitioning konidas@acm.org does not
designate 83.235.69.31 as permitted sender) client-ip=83.235.69.31;
Received: from [0.0.0.0] (ns361585.ip-91-121-169.eu [91.121.169.33])
            by medusa.otenet.gr (ESMTP) with ESMTPSA
            for <luka.kodric@gmail.com>; Fri, 12 Dec 2014 10:53:47 +0200 (EET)
Date: Fri, 12 Dec 2014 12:53:43 +0400
From: "konidas@acm.org" <konidas@acm.org>
To: Luka Kodric <luka.kodric@gmail.com>
Subject: Re: Upsilon Pi Epsilon - a membership offer
```

APPENDIX B – INDICATORS OF COMPROMISE



IP Address	Description	Timeframe information	Host Name
109.163.234.9	Blocked login attempts from this IP address	4 January 2015 between 09:32 and 09:55 (CET)	edwardsnowden2.torservers.net
171.25.193.20	konidas[@]acm[.]org sent from this IP	11 Dec 2014 15:33:49 +0400	tor-exit0-readme.dfri.se
171.25.193.235	konidas[@]acm[.]org sent from this IP	09 Dec 2014 20:06:34 +0400	tor-exit3-readme.dfri.se
185.31.209.128	wallet.dat transferred to this IP address	29 December 2014 between 11:29 - 12:01 (CET)	ariermeane.srv6.sim-networks.net
185.31.209.145	IP address from which 'wordcomp.zip' was pulled down	11 December 2014 - pulled down onto Mr Kodric's laptop at 11:00 (CET)	donkolot.srv6.sim-networks.net
185.49.68.151	*msword32.cab pulled down from this address*	Email with attachment that calls out to IP sent on 8 February 2015	-
	dodlib32.cab pulled down from this address	Email with attachment that calls out to IP sent on 4 February 2015	
185.49.68.164	wordlib[1].zip pulled down from this IP address (ES004)	Skype message with attachment that calls out to IP sent on 5 December 2014	-
195.154.215.83	konidas[@]acm[.]org sent from this IP	10 Dec 2014 00:57:14 +0400	195-154-215-83.rev.poneytelecom.eu
204.8.156.142	konidas[@]acm[.]org sent from this IP	10 Dec 2014 12:43:16 +0400	cs-tor.bu.edu
212.38.166.50	wf.exe calls out for this IP address	wf.exe created on Mr Kodric's laptop on 17 December 2014	-
217.12.202.34	wordcomp[1].zip designed to call out to this IP	Malware downloaded onto laptop on 11 December	arbak.me
23.33.4.153	mso2010.exe old http connection (port 80)	mso2010 created on Mr Kodric's laptop on 22 December 2014	a23-33-4-153.deploy.static.akamaitechnologies.com
37.157.195.174	konidas[@]acm[.]org sent from this IP	11 Dec 2014 11:50:16 +0400	13.transminn.cz
77.247.181.162	konidas[@]acm[.]org sent from this IP	11 Dec 2014 13:01:56 +0400	chomsky.torservers.net
91.121.169.33	konidas[@]acm[.]org sent from this IP	12 Dec 2014 12:53:43 +0400	ns361585.ip-91-121-169.eu
94.185.85.171	IP address used by attacker for all Skype conversations where IP has been confirmed	4 November - 19 December 2014	-
95.100.209.177	mso2010.exe old https connection (port 443)	mso2010 created on Mr Kodric's laptop on 22 December 2014	a95-100-209-177.deploy.akamaitechnologies.com

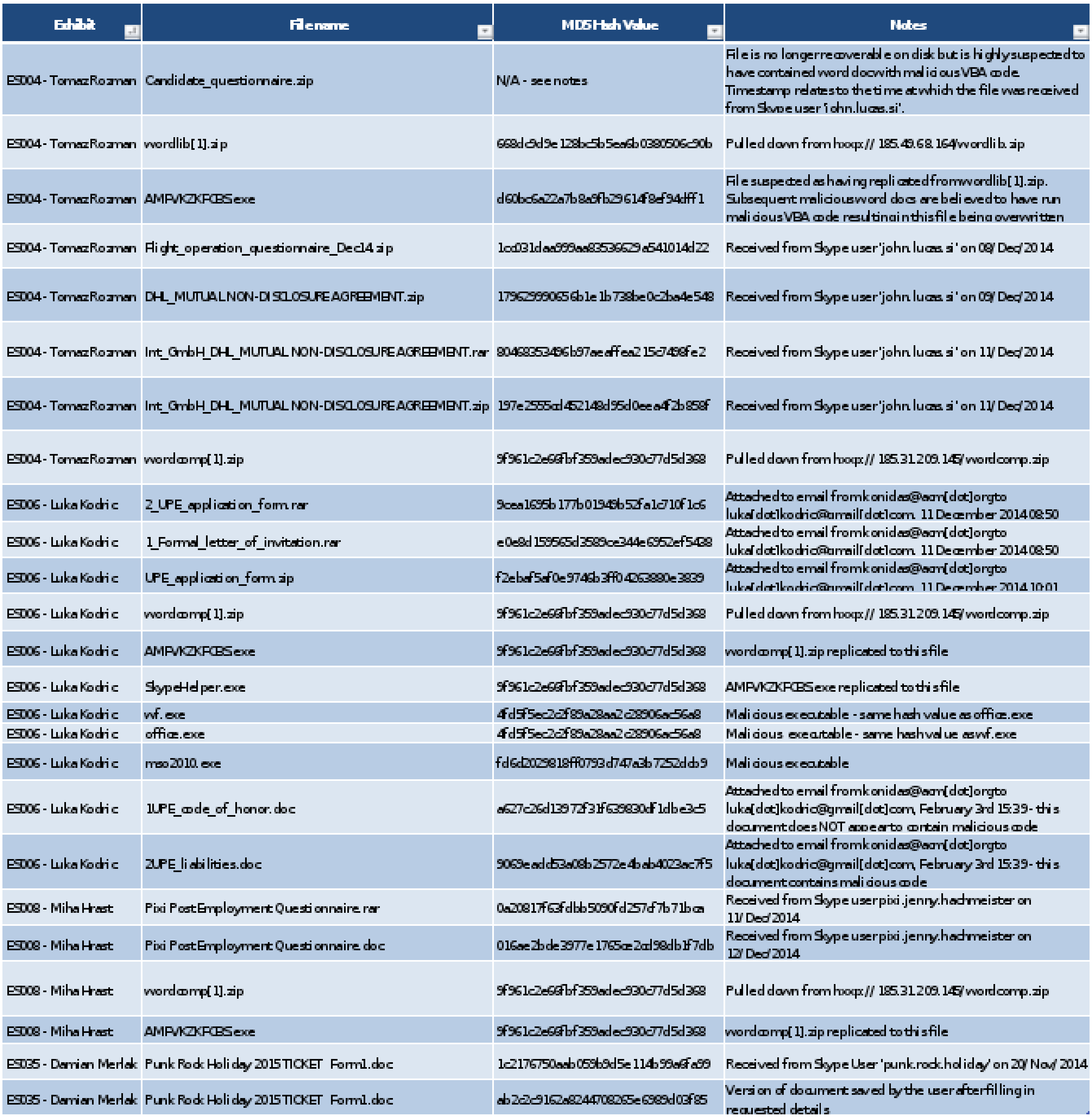


Exhibit	Filename	MD5 Hash Value	Notes
ES004 - Tomaz Rozman	Candidate_questionnaire.zip	N/A - see notes	File is no longer recoverable on disk but is highly suspected to have contained word doc with malicious VBA code. Timestamp relates to the time at which the file was received from Skype user 'john.lucas.si'.
ES004 - Tomaz Rozman	wordlib[1].zip	668dc9d9e128bc5b5ea6b0380506c90b	Pulled down from hxxp:// 185.49.68.164/wordlib.zip
ES004 - Tomaz Rozman	AMPVKZKFCBS.exe	d60bc6a22a7b8a9fb29614f8ef94dff1	File suspected as having replicated from wordlib[1].zip. Subsequent malicious word docs are believed to have run malicious VBA code resulting in this file being overwritten
ES004 - Tomaz Rozman	Flight_operation_questionnaire_Dec14.zip	1cd031daa999aa83536629a541014d22	Received from Skype user 'john.lucas.si' on 08/ Dec/ 2014
ES004 - Tomaz Rozman	DHL_MUTUAL NON-DISCLOSURE AGREEMENT.zip	179629990656b1e1b738be0c2ba4e548	Received from Skype user 'john.lucas.si' on 09/ Dec/ 2014
ES004 - Tomaz Rozman	Int_GmbH_DHL_MUTUAL NON-DISCLOSURE AGREEMENT.rar	80468353496b97aeaffea215c7498fe2	Received from Skype user 'john.lucas.si' on 11/ Dec/ 2014
ES004 - Tomaz Rozman	Int_GmbH_DHL_MUTUAL NON-DISCLOSURE AGREEMENT.zip	197e2555cd452148d95d0eea4f2b858f	Received from Skype user 'john.lucas.si' on 11/ Dec/ 2014
ES004 - Tomaz Rozman	wordcomp[1].zip	9f961c2e69fbf359adec930c77d5d368	Pulled down from hxxp:// 185.31.209.145/wordcomp.zip
ES006 - Luka Kodric	2_UPE_application_form.rar	9cea1695b177b01949b52fa1c710f1c6	Attached to email from konidas@acm[dot]org to luka[dot]kodric@gmail[dot]com. 11 December 2014 08:50
ES006 - Luka Kodric	1_Formal_letter_of_invitation.rar	e0e8d159565d3589ce344e6952ef5438	Attached to email from konidas@acm[dot]org to luka[dot]kodric@gmail[dot]com. 11 December 2014 08:50
ES006 - Luka Kodric	UPE_application_form.zip	f2ebaf5af0e9746b3ff04263880e3839	Attached to email from konidas@acm[dot]org to luka[dot]kodric@gmail[dot]com. 11 December 2014 10:01
ES006 - Luka Kodric	wordcomp[1].zip	9f961c2e69fbf359adec930c77d5d368	Pulled down from hxxp:// 185.31.209.145/wordcomp.zip
ES006 - Luka Kodric	AMPVKZKFCBS.exe	9f961c2e69fbf359adec930c77d5d368	wordcomp[1].zip replicated to this file
ES006 - Luka Kodric	SkypeHelper.exe	9f961c2e69fbf359adec930c77d5d368	AMPVKZKFCBS.exe replicated to this file
ES006 - Luka Kodric	wf.exe	4fd5f5ec2c2f89a28aa2c28906ac56a8	Malicious executable - same hash value as office.exe
ES006 - Luka Kodric	office.exe	4fd5f5ec2c2f89a28aa2c28906ac56a8	Malicious executable - same hash value as wf.exe
ES006 - Luka Kodric	mso2010.exe	fd6d2029818ff0793d747a3b7252ddb9	Malicious executable
ES006 - Luka Kodric	1UPE_code_of_honor.doc	a627c26d13972f31f639830df1dbe3c5	Attached to email from konidas@acm[dot]org to luka[dot]kodric@gmail[dot]com, February 3rd 15:39 - this document does NOT appear to contain malicious code
ES006 - Luka Kodric	2UPE_liabilities.doc	9069eadd53a08b2572e4bab4023ac7f5	Attached to email from konidas@acm[dot]org to luka[dot]kodric@gmail[dot]com, February 3rd 15:39 - this document contains malicious code
ES008 - Miha Hrast	Pixi Post Employment Questionnaire.rar	0a20817f63fdbb5090fd257d7b71bca	Received from Skype user pixi.jenny.hachmeister on 11/ Dec/ 2014
ES008 - Miha Hrast	Pixi Post Employment Questionnaire.doc	016ae2bde3977e1765ce2cd98db1f7db	Received from Skype user pixi.jenny.hachmeister on 12/ Dec/ 2014
ES008 - Miha Hrast	wordcomp[1].zip	9f961c2e69fbf359adec930c77d5d368	Pulled down from hxxp:// 185.31.209.145/wordcomp.zip
ES008 - Miha Hrast	AMPVKZKFCBS.exe	9f961c2e69fbf359adec930c77d5d368	wordcomp[1].zip replicated to this file
ES035 - Damian Merlak	Punk Rock Holiday 2015 TICKET Form1.doc	1c2176750aab059b9d5e114b99a6fa99	Received from Skype User 'punk.rock.holiday' on 20/ Nov/ 2014
ES035 - Damian Merlak	Punk Rock Holiday 2015 TICKET Form1.doc	ab2c2c9162a8244708265e6989d03f85	Version of document saved by the user after filling in requested details

APPENDIX C – CACTI LOG FILE OUTPUT FOR LNXSRVBTC