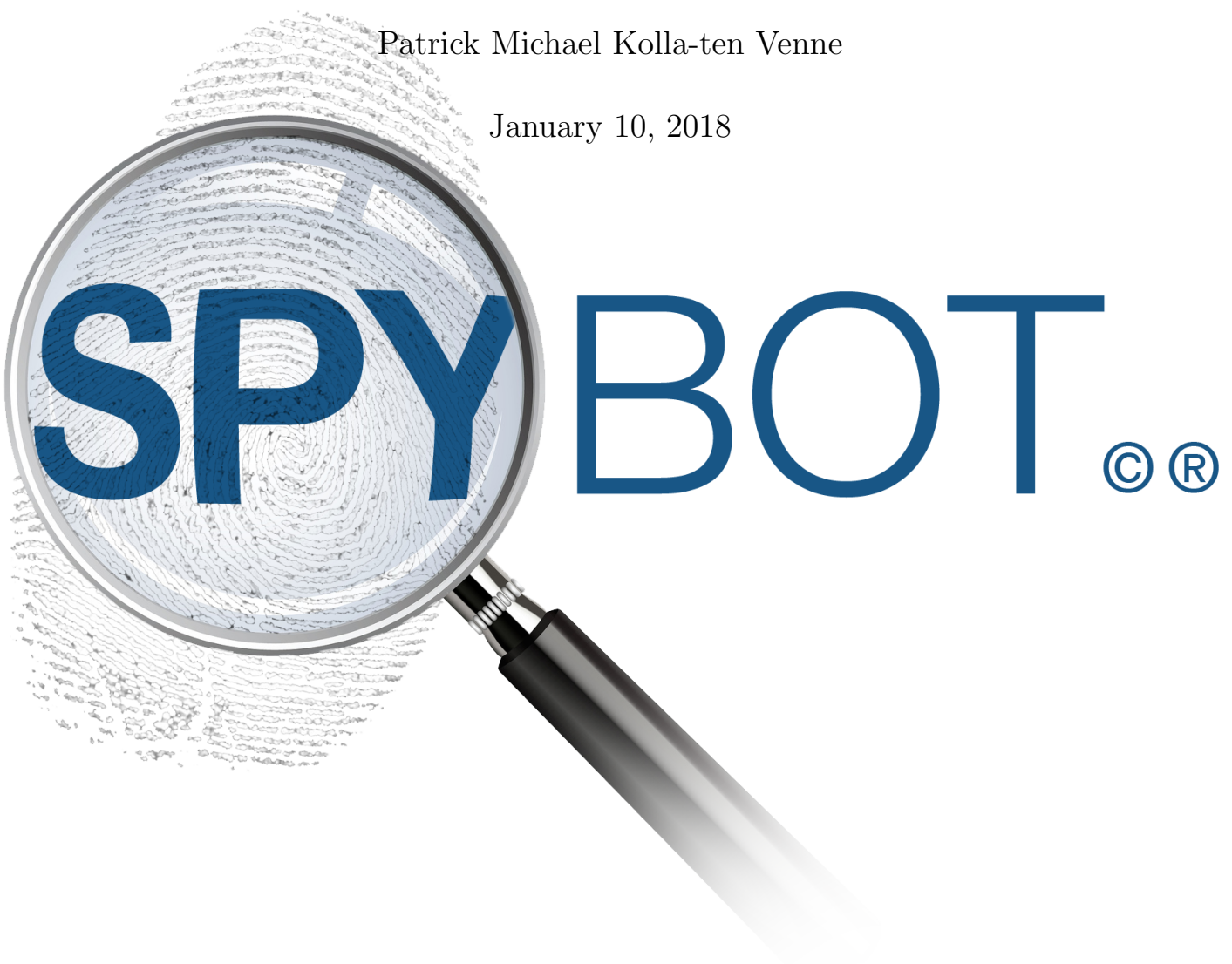


Synergy 2
Version 2.0.1, 2.0.2 & 2.0.4
Security Review

Patrick Michael Kolla-ten Venne

January 10, 2018



Contents

1	Introduction	5
1.1	Abstract	5
1.2	Chronology	6
1.3	Responsible disclosure	7
2	Company	8
2.1	Background	8
2.1.1	Employees	9
2.1.2	Social Media	10
3	Website	12
3.1	Certificate	12
3.2	Imprint	13
3.3	Domain information	14
3.4	Privacy Policy	16
3.5	Shop	17
3.5.1	Invoice	19
3.5.2	Refunds	19
3.5.3	Transactions	20
3.6	Support	22
3.6.1	Personal Information	25
3.6.2	Formal request	26
3.6.3	Request for draft review to Nick Bolton	28
3.6.4	Forum responsible disclosure	29
4	Software	40
4.1	Installer	40
4.2	Installation	42
4.2.1	Files	44
4.2.2	Registry	45
4.2.3	Services	46

4.2.4	Processes	48
4.3	Login	49
4.3.1	Registry	52
4.4	Logs	52
4.4.1	Log server	54
4.4.2	Log contents	56
4.4.3	Log handling	57
4.5	Uninstallation	59
4.6	Open Source	59
5	Communications	69
5.1	Configuration	69
5.1.1	Software update	71
5.1.2	Profile switch	72
5.1.3	Profile update	73
5.1.4	Screen update	73
5.2	Core synchronization	74
5.3	Log sending	74
6	Attack Vectors	76
6.1	userId and -Token	76
6.1.1	Support forum	77
6.1.2	Pastebin	77
6.1.3	One-time physical access, using the registry	77
6.1.4	One-time physical access, using the browser history	78
6.1.5	One-time remote code execution	78
6.1.6	Bookmark and history sharing	78
6.1.7	Network sniffer	78
6.1.8	Tracking software	79
6.2	DNS Spoofing	79
7	Summary	83
	Screenshots	84
	Listings	86
	Requirements	87
	Recommendations	88
	Missing Tests	89

CONTENTS

CONTENTS

URLs **91**

Used Software **92**

Copyright

This document was created by Safer-Networking Ltd. for their own use as well as for informational use by their customers. It is copyrighted by Safer-Networking Ltd., commercial use by third parties is prohibited unless allowed in need written form. An exception to this is the press, as long as the source is clearly specified.

Chapter 1

Introduction

1.1 Abstract



Synergy 2¹ is a software KVM available online. While it's core is open source, there's a commercial version that has recently received a major update from version 1.8 to 2.0. Since it's website is anonymous and neither website nor software have a privacy policy, the author has researched some background about the company, software, and it's handling of personally identifying and identifiable information (PII). Not only is a privacy policy missing, the author also found various careless handling of PII, including communications with a cloud server and published user logs that contain PII. Communication with Symless was difficult, since the company tried to avoid to address the privacy and security issues and instead went to deleting the authors account and data before issues were solved. Symless was offered to comment on these issues, with the spare comment received quoted here.

This document tries to describe the software, company, website and contacts from all perspectives the author looked at during his research to give a complete picture of the software. Critical findings have been commented with *Requirements*², issues where improvements are possible with *Recommendations*³.

¹The logo above is probably copyrighted by Symless Ltd

²See section 7 on page 87 for an overview in list form

³See section 7 on page 88 for an overview in list form

1.2 Chronology

November 21st (T+0 days) Installed Synergy 2, found PII leak, contacted support and requested removal of PII and statement about spyware behavior. Support answered how to process a refund without addressing any of the PII or spyware issues⁴.

November 22nd (T+1 days) Emailed Nick Bolton⁵ a 20 page draft of this document for review and statements.

November 23rd (T+2 days) Nick Bolton, CEO of Symless, answered to ZenDesk thread as if problems would now be solved. PII still online, no comments about spyware behavior. Authors ZenDesk account was suspended⁶ was the only change noticed.

November 24th (T+3 days) Successfully monitored Synergy 2 secure `https` communication with server API⁷. Got a second installation to connect using copied `userId` and `userToken`⁸.

November 26th (T+5 days) Formal PII information request sent⁹.

November 27th (T+6 days) As a reply to the privacy request the day before, Malcolm Lowe informed the author that everything, meaning accounts and logs, has been removed. A quick test showed that these logs, which the complaint was about, are still public. Malcolm Lowe also answered to the draft five days ago, explaining that nearly all issues would be “covered by the new GDPR regulations”, which is questionable.

January 9th (T+49 days) Raised the responsible disclosure issue on the Symless forums. Thread was closed without a direct answer on the topic.

January 10th (T+50 days) Published text description possible man in the middle attack on Symless forums.

⁴See page 16

⁵`nick@synergy-project.org`

⁶See page 22

⁷See section 5.1 on page 69

⁸See section 6.1 on page 76

⁹See section 3.6.2 on page 26

1.3 Responsible disclosure

This article was not published without giving Symless of time to react to the accusations of leaked PII and weak protection of data, following the principles called *responsible disclosure*¹⁰. Since Symless did actively decide to not answer any open issues, the author has deemed two weeks to be enough time.

Responsible disclosure is described at Wikipedia in more detail:

“Responsible disclosure is a computer security term describing a vulnerability disclosure model. It is like full disclosure, with the addition that all stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details. Developers of hardware and software often require time and resources to repair their mistakes. Hackers and computer security scientists have the opinion that it is their social responsibility to make the public aware of vulnerabilities with a high impact. Hiding these problems could cause a feeling of false security. To avoid this, the involved parties join forces and agree on a period of time for repairing the vulnerability and preventing any future damage. Depending on the potential impact of the vulnerability, the expected time needed for an emergency fix or workaround to be developed and applied and other factors, this period may vary between a few days and several months. It is easier to patch software by using the Internet as a distribution channel.”

— Wikipedia, *Responsible disclosure*

¹⁰https://en.wikipedia.org/wiki/Responsible_disclosure

Chapter 2

Company

2.1 Background

There is a number of ways one could usually find out about the company or author behind a software where this one mostly hides successfully:

- A company name on the website (not existing here)
- An imprint on the website (not existing here)
- The https certificate of the website¹ (without ownership here)
- The WhoIs information² of the website domain (anonymous)
- The software signing certificate if it exists³
- Social media pages for the software⁴
- An invoice⁵

It is important to recognize that the existing leads all need either research outside the website, or enough trust to download and start to install the software.

The name used for the software signing certificate leads to a company now based in the UK, registered with company number 08066283. It has been known under the following names:

¹See section 3.1 on page 12

²The WhoIs information is anonymous, see section 3.3 on page 14

³The Authenticode signature is the first existing lead, see section 4.1 on page 40

⁴Social media pages are the second existing lead, see section 2.1.2 on page 10

⁵The invoice is the third existing lead, see section 3.5.1 on page 19

1. Symless Limited (currently)
2. Synergy Seamless Limited (2015 - 2016)
3. Synergy SI Limited (2014 - 2015)
4. Bolton Software Ltd (2012 - 2014)

The company officer is Nicholas John Bolton, who was appointed in 2012 and owns the majority of shares of the company. A second officer, Sarah Taylor, was appointed in 2012 but resigned in 2013. It's address is in Camberley, UK⁶:

Basepoint Business Centre London Road, Unit 014, 377-399
London Road, Camberley, Surrey, England, GU15 3HL

The director, Nick Bolton, describes the software and company in his LinkedIn profile⁷:

*“Symless is the company behind Synergy, keyboard and mouse sharing software.
At Symless, our mission is to combine your devices into one cohesive experience, making the world more seamless. Our keyboard and mouse sharing app, Synergy is used by millions of people worldwide who have multiple computers on their desk. Combining your devices together into one cohesive experience, Synergy shares one mouse, one keyboard and one clipboard between all of your computers.”*

— Nick Bolton, *Mission statement on LinkedIn*

2.1.1 Employees

Employees of Symless seem to be⁸⁹:

Nick Bolton Director¹⁰

⁶Company details can be found at <https://beta.companieshouse.gov.uk/company/08066283>

⁷<https://uk.linkedin.com/in/nbolton/de>

⁸<https://www.linkedin.com/company/2851905/>

⁹<https://symless.com/forums/staff/>

¹⁰<https://symless.com/forums/profile/8-nick-bolton/>

Malcolm Lowe Operations Manager and the person who has answered a support enquiry¹¹¹²

Amy Fox PA to CEO¹³

Dan Sorahan Full Stack Developer since 2016¹⁴¹⁵

Xinyu Hou Software Engineer¹⁶, aka Jerry Hou¹⁷

Julia Katharina Klein Digital Marketing Executive¹⁸, left in October 2017

Polly Jones Software Engineer¹⁹

Karen Williams ²⁰

Andrew Nelles ²¹

Joe Abasolo ²²

Sarah Hebert ²³

2.1.2 Social Media

Various social media accounts exist that are linked to the product or company:

- <https://www.facebook.com/Symless/>
- https://twitter.com/Synergy_App
- <https://www.facebook.com/nbolton4>
- <https://twitter.com/NickBoltonUK>

¹¹<https://www.linkedin.com/in/malcolm-low-75771ab1/>

¹²<https://symless.com/forums/profile/9-malcolm-low/>

¹³<https://www.linkedin.com/in/amy-fox-ba4ab09b/>

¹⁴<https://www.linkedin.com/in/dansorahan/>

¹⁵<https://symless.com/forums/profile/1-dan-sorahan/>

¹⁶<https://www.linkedin.com/in/xinyu-hou-aa310850/>

¹⁷<https://symless.com/forums/profile/7-jerry-hou/>

¹⁸<https://www.linkedin.com/in/julia-katharina-klein-ma-msc-bb70a542/>

¹⁹<https://www.linkedin.com/in/polly-jones-909a73101/>

²⁰<https://symless.com/forums/profile/27559-karen-williams/>

²¹<https://symless.com/forums/profile/27344-andrew-nelles/>

²²<https://symless.com/forums/profile/27614-joe-abasolo/>

²³<https://symless.com/forums/profile/30885-sarah-hebert/>

- <https://www.crunchbase.com/person/nick-bolton-3>

One possibly interesting piece of information is that according to his LinkedIn account, the Director Nick Bolton lives in Camberley, Surrey, United Kingdom, while his Facebook account locates him in Farnborough, Hampshire, and crunchbase lists him as located in San Francisco, California, USA. This might be due to the two years of Synergy Si, Inc.²⁴.

440 N Wolfe Rd, Sunnyvale, CA 94085, United States

Oh, and I have more great news! Our engineering headquarters are now up and running in the beautiful town of Sunnyvale, California (right in the heart of Silicon Valley). I actually split my time between San Francisco and our Sunnyvale office, so if you want to connect with me you can [add me on LinkedIn](#) or just email me.

Thanks,
Nick

p.s. If you want a free Synergy t-shirt, mug or pint glass, please complete our [Swag Request form](#).

Copyright © 2015 Synergy Si, Inc., All rights reserved.
You are receiving this email because you signed up at the Synergy website.

Our mailing address is:
Synergy Si, Inc.
440 N Wolfe Rd
Sunnyvale, CA 94085

Screenshot 2.1: Synergy in California

Various other found accounts of company, product and CEO are not of relevance currently.

²⁴See screenshot 2.1

Chapter 3

Website

The website is using a simple style with information reduced to essential content. It is easy to navigate and information is easy to find, but it is missing company information and a privacy policy.

Clients listed by the website are¹:

- Amazon
- Google
- Intel
- Disney
- Pixar
- Microsoft
- Apple
- Cisco
- Dell EMC

3.1 Certificate

The website <https://symless.com> is using https with a Comodo certificate for cloudflaressl.com that lists symless.com as one of many alternate names².

¹See screenshot [3.2](#) on page [35](#)

²See screenshot [3.4](#) on page [37](#)

It is no EV certificate, and due to being assigned to Cloudflare, it does not allow to verify the identity of the company behind the software as the origin of the website³. Trust is reduced from trusting Comodo, an issuer of certificates, to trusting Cloudflare, which might not have the same stringent authentication mechanisms in place as a root authority.

This becomes more important since there is customer PII available to the public on a symless.com subdomain⁴.

Cloudflare describes this method of operation as *Origin CA*⁵:

“Origin CA uses a Cloudflare-issued SSL certificate instead of one issued by a Certificate Authority. This reduces much of the friction around configuring SSL on your origin server, while still securing traffic from your origin to Cloudflare. Instead of having your certificate signed by a CA, you can generate a signed certificate directly in the Cloudflare dashboard.”

— Cloudflare, *Simple Secure Socket Layer*

Recommendation 1 (Company specific certfite). *Use a company specific certificate with ownership information so that customers can verify they’re really on the website of Symless Limited.*

Recommendation 2 (EV certificate). *Since the website uses a shop to buy, an EV certificate is highly recommended for additional verification.*

Some parts of the website are also not encrypted.

Recommendation 3 (No mixed content). *Make sure all content is delivered through https.*

3.2 Imprint

Continuing on the website, it does not include any imprint at all. There’s no information available about the company the user is about to entrust his data.

Requirement 1 (Imprint). *The user needs to know from whom he buys, and whom he entrusts personally identifying information. Include an imprint page as part of the website. Using the company name in the footer would make this information available right away.*

³See screenshot 3.3 on page 36

⁴See section 4.4.1 on page 54

⁵<https://www.cloudflare.com/en/ssl/>

3.3 Domain information

A WhoIsn query⁶ showed that the domain is registered anonymously.

Listing 3.1: WhoIs record of symless.com

```
Domain Name: SYMLESS.COM
Registry Domain ID: 1997573617_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2017-01-27T17:33:08Z
Creation Date: 2016-01-26T15:29:21Z
Registrar Registration Expiration Date: 2018-01-26T15:29:21Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/
    ↪ epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#
    ↪ clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#
    ↪ clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#
    ↪ clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 14455 N. Hayden Road
Registrant City: Scottsdale
Registrant State/Province: Arizona
Registrant Postal Code: 85260
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: symless.com@domainsbyproxy.com
Registry Admin ID:
```

⁶Check <https://www.whois.com/whois/symless.com> and <http://who.godaddy.com/whoischeck.aspx?domain=symless.com> for up to date information.

```
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 14455 N. Hayden Road
Admin City: Scottsdale
Admin State/Province: Arizona
Admin Postal Code: 85260
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: symless.com@domainsbyproxy.com
Registry Tech ID:
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 14455 N. Hayden Road
Tech City: Scottsdale
Tech State/Province: Arizona
Tech Postal Code: 85260
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: symless.com@domainsbyproxy.com
Name Server: ELINORE.NS.CLOUDFLARE.COM
Name Server: THOMAS.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN WHOISData Problem Reporting System: http://
    ↪ wdprs.internic.net/
>>> Last update of WHOIS database: 2017-11-23T7:00:00Z <<<
```

Since Synergy is a product that uses PII and has access to very important PII, including all account logins and passwords⁷, the user should have the right to know about the vendor of the software. WhoIs records are also helpful to verify a domain has not been highjacked after it has expired and the original owner has not renewed it.

⁷as part of the clipboard synchronized by Synergy

Recommendation 4 (Public WhoIs information). *Symless should be frank and use their company as the visible domain owner.*

3.4 Privacy Policy

No privacy policy can be found at all. A request by email was ignored, with a standard text referring to refunds as the mail body.

Here's an excerpt from the support communication regarding the authors complaints about public PII.

*“The main window offers to ”Send log”, and review information
after it was sent. There is PII available without protection
online, I can open the log from anywhere, it contains my login
name, machine name, information about our local IP addresses
and a bunch of tokens that probably should not be public.*

[...]

*I EXPECT that the two test logs sent from here are immediately
purged from your servers*

[...]

*Neither website nor product does contain any privacy policy,
making it, following the standard definitions, actually spyware
that you're selling.*

[...]”

— Patrick Kolla-ten Venne, *Email to Symless*

“Hi Patrick,

*I'm really sorry Synergy didn't work out for you. Please complete
this refund request form, so we can issue your refund.*

<https://symless.com/account/refund/request>

Thanks, Malcolm”

— Malcolm Lowe, *Answer from Symless*

“Hi Malcolm,

What about my request to remove my PII?

*Are you going to offer a privacy policy, or continue to offer
spyware?*

Patrick”

— Patrick Kolla-ten Venne, *Answer to Symless*

Requirement 2 (Website Privacy Policy). *A privacy policy is mandatory for any website that collects PII.*

No further replies were received, nor did the director, Nick Bolton, answer to an email sent to his specific email address known to the author from previous mails.

3.5 Shop

If the user decides to buy the product, he's asked for his first and last name and email address⁸, all PII, without informing him with whom this information will be shared, and for which purposes.

⁸See screenshot 3.6 on the next page



Screenshot 3.6: The website shop is asking for PII without informing about receivers or purposes

Requirement 3 (Shop Privacy Policy). *When asking for PII, information about receivers and purpose is mandatory.*

He is then offered the choice to pay with other PayPal or credit card⁹. The PayPal choice leads to the new PayPal subscription payment type that offers to verify only once. The author of this document has issues with this because it contradicts the 2FA security concept for the user. Plus, in the context of Synergy, it does not seem necessary, since the website clearly states:

“One-time payment with lifetime download access”

Recommendation 5 (Non-subscription PayPal payment). *Offer standard PayPal payment without subscription option.*

3.5.1 Invoice

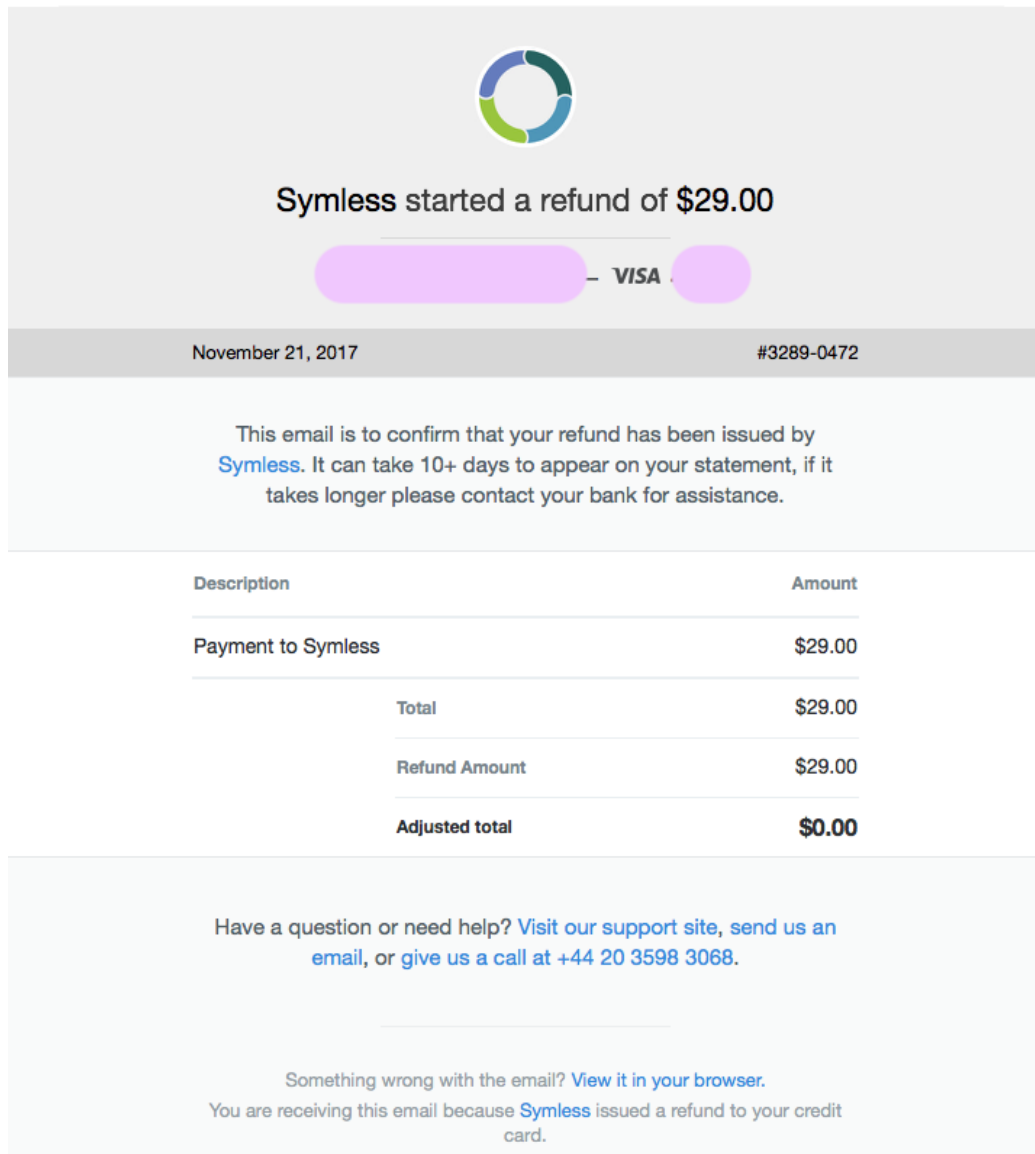
The invoice is one of the few places where the address of Symless can be found.

3.5.2 Refunds

Refunds seem to be simple; the author was sent a link by support¹⁰ and the refund is, according to an email, supposed to be on its way.

⁹See screenshot 3.7 on page 38

¹⁰Refunds should be available at <https://symless.com/account/refund/request>.

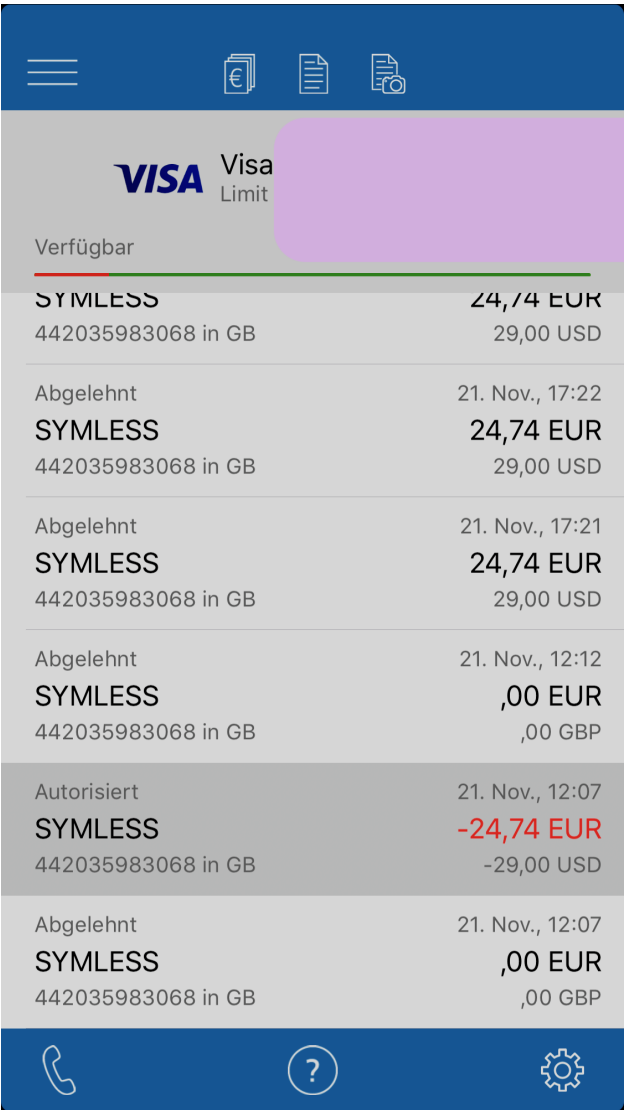


Screenshot 3.9: The refund confirmation received via email

3.5.3 Transactions

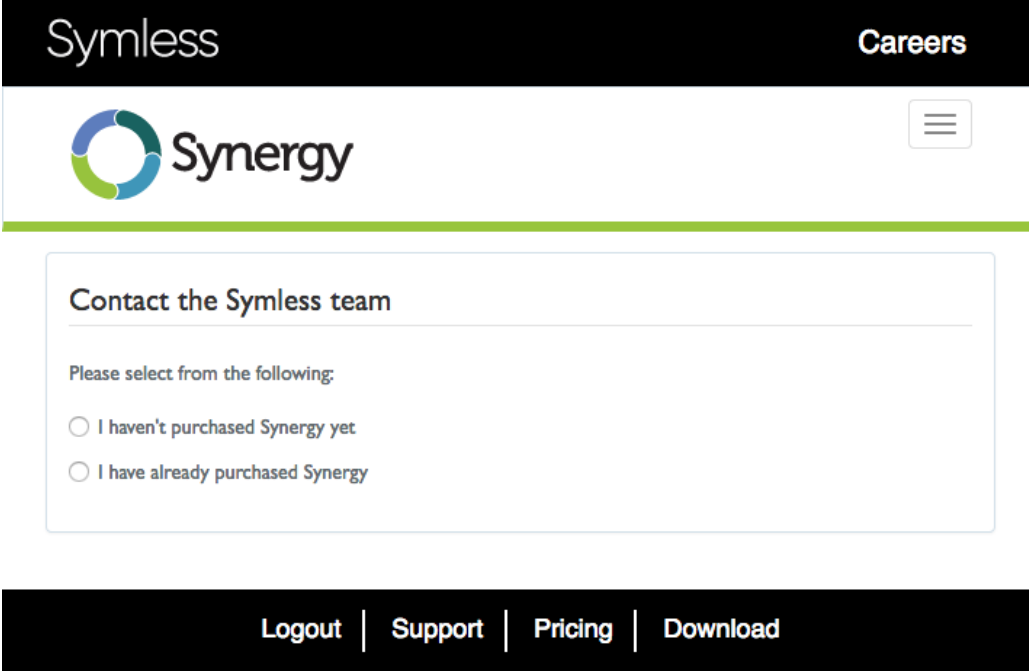
The credit card transactions of the Visa credit card used to purchase the software show a bank account 442035983068 for Symless in GB¹¹.

¹¹Great Britain



Screenshot 3.10: Credit card notifications show company Symless in GB

3.6 Support



Symless Careers

Synergy

Contact the Symless team

Please select from the following:

☐ I haven't purchased Synergy yet

☐ I have already purchased Synergy

Logout | Support | Pricing | Download

Screenshot 3.11: The support page does not inform about the involved third party

Support is offered through a form on the website, found at <https://symless.com/support>¹². In the background, ZenDesk is used, users can access their support cases on <https://symless.zendesk.com/>.

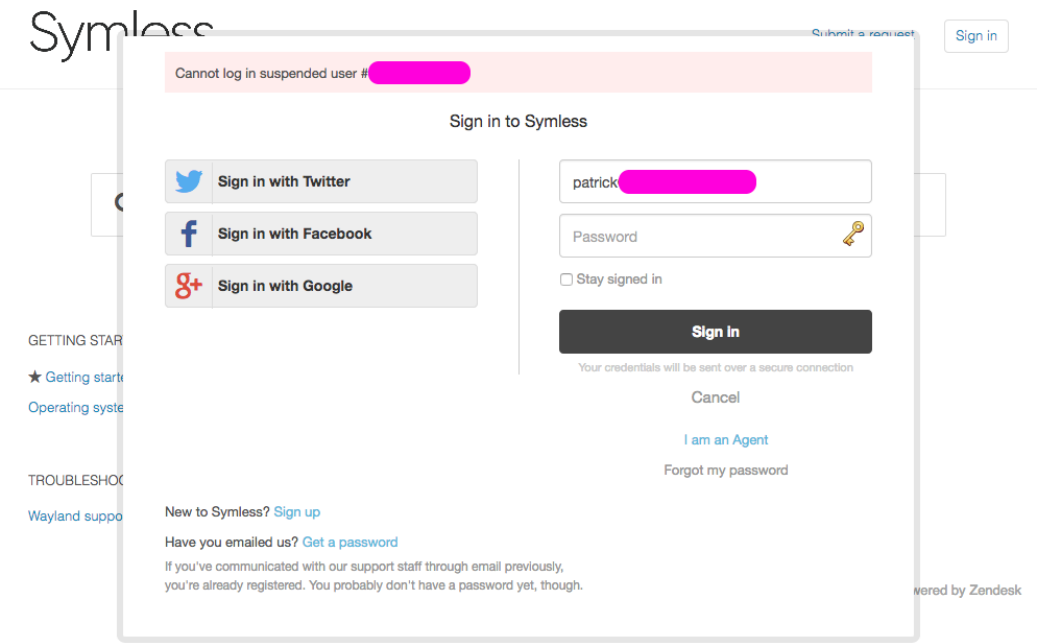
Requirement 4 (Reveal sharing with ZenDesk). *The user needs to be informed, as part of a privacy policy and on the support page, that his personally identifying information is shared with the third party ZenDesk.*

As soon as the authors request to delete his PII was forward from Malcolm Lowe to Nick Bolton, his ZenDesk account was suspended¹³ or even removed¹⁴.

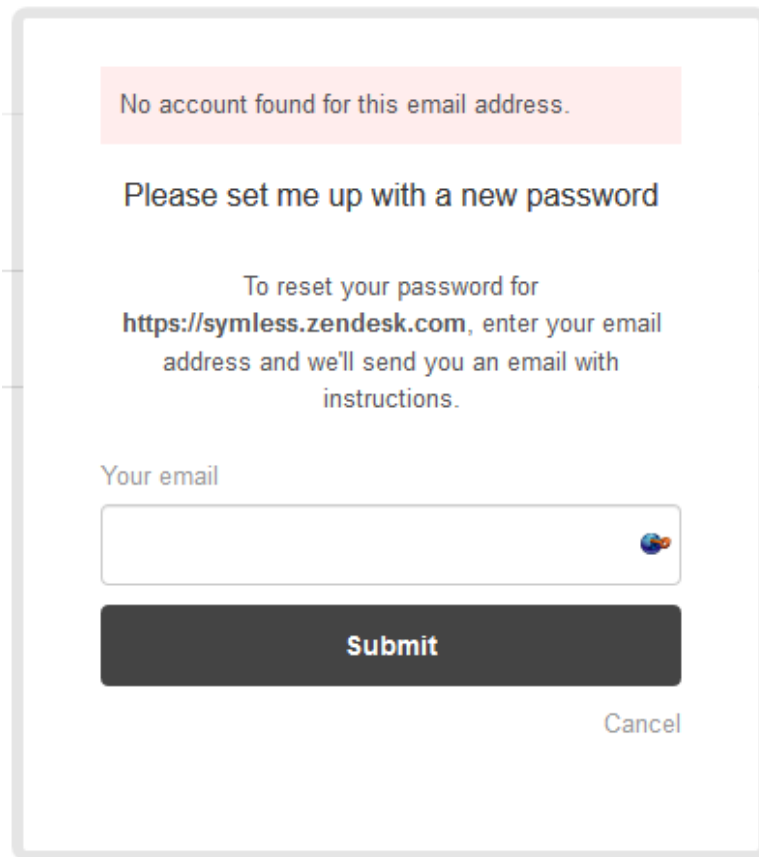
¹²See screenshot 3.11

¹³See screenshot 3.12 on the following page

¹⁴See screenshot 3.13 on page 24



Screenshot 3.12: The support page was suspended for the author



No account found for this email address.

Please set me up with a new password

To reset your password for <https://symless.zendesk.com>, enter your email address and we'll send you an email with instructions.

Your email

Submit

Cancel

Screenshot 3.13: The support desk account of the author was removed

Also suspended was the authors access to the website¹⁵.

¹⁵See screenshot 3.14 on the following page

The screenshot shows the Symless website's login interface. At the top, there is a navigation bar with the Symless logo, a 'Careers' link, and a 'Synergy' logo. Below this, there are links for 'Pricing', 'Support', and a 'Login' button. The main content area features a 'Login' form. A red message box at the top of the form states: 'The email or password that you used was incorrect. If you're having problems, try resetting your password or email login-issues@symless.com.' The form has two input fields: 'E-Mail Address' (containing the text 'patrick') and 'Password'. Below the password field is a 'Remember Me' checkbox. At the bottom of the form are a blue 'Login' button and a link for 'Forgot Your Password?'. The footer of the page contains links for 'Support', 'Pricing', and 'Download'.

Screenshot 3.14: The website login was suspended for the author

3.6.1 Personal Information

A request by a private person to remove personally identifying information from the public servers was ignored¹⁶.

Since there is no EULA¹⁷ nor ToS¹⁸, the applicable law would be defined by REGULATION (EC) No 593/2008 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL¹⁹, so we would need to look at the Privacy and Electronic Communications (EC Directive) Regulations 2003²⁰.

Listed under Confidentiality of communications²¹, we find:

- (1) Subject to paragraph (4), a person shall not use an electronic communications network to store information, or to gain ac-

¹⁶See section 3.4 on page 16

¹⁷End User License Agreement

¹⁸Terms of Service

¹⁹<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008R0593>

²⁰<http://www.legislation.gov.uk/ukxi/2003/2426/contents/made>

²¹<http://www.legislation.gov.uk/ukxi/2003/2426/regulation/6/made>

cess to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.

- (2) The requirements are that the subscriber or user of that terminal equipment—
 - (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
 - (b) is given the opportunity to refuse the storage of or access to that information.

There's an exemption to this:

- (4) Paragraph (1) shall not apply to the technical storage of, or access to, information—
 - (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

It could now be argued if the information transmitted via the log is strictly necessary. In the authors opinion, the PII could easily be at least be pseudonymous without making support impossible.

Requirement 5 (Proper Privacy Request handling). *Appoint a privacy officer that deals with privacy requirements as required by law.*

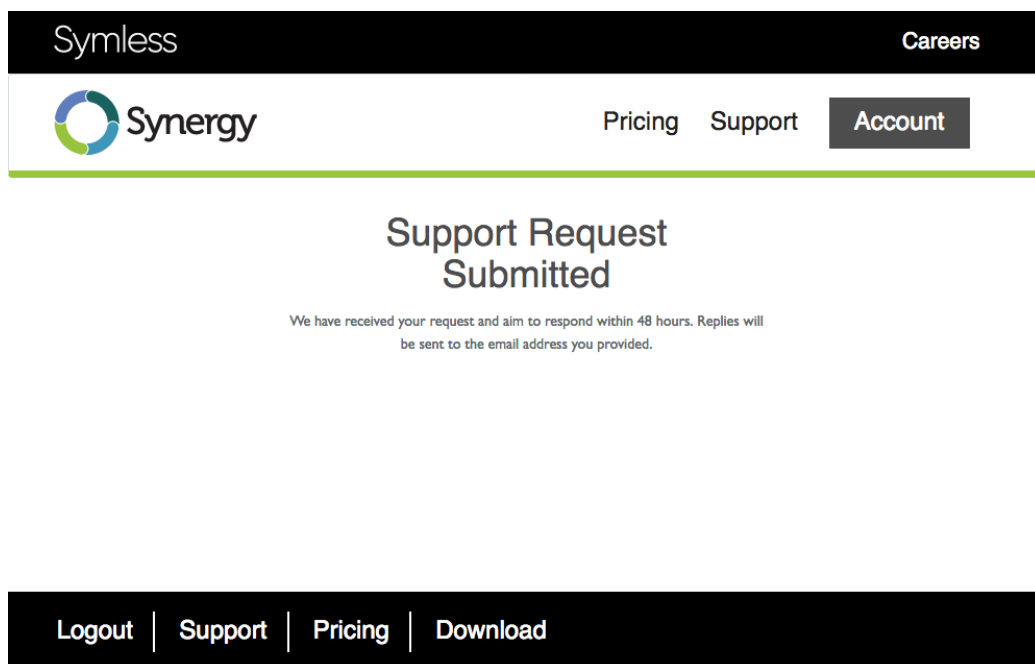
3.6.2 Formal request

On November 26th, the author sent a formal request about data stored about him and it's storage and sharing with third parties. Since there is no dedicated privacy officer mentioned, nor an imprint or whois record listing any email address, this request was sent through the support form, so very likely will go into the same ZenDesk support backend as the initial email thread.

*“Dear Symless,
I hereby write to you to request full information about all
personally identifying and personally identifiable information
you’ve stored about my person, including modes of storage of this
information and third parties with whom this information has
been shared.
Please reply as to what additional information you need to comply
with this request, and when I can expect a complete answer.
The background of this request can be found in both British (The
Privacy and Electronic Communications (EC Directive)
Regulations 2003) and German (Bundesdatenschutzgesetz) laws,
both based on the same European directive.
Best regards and thanks in advance,
Patrick Kolla-ten Venne”*

— Patrick Kolla-ten Venne, *Formal request for PII details*

Receipt of request was confirmed by the website.



Screenshot 3.15: The formal information request was received

An answer to this formal request was avoided by deleting all data on November 27th:

“We have deleted every single bit of information that we held on you, including your Synergy account, any logs you have submitted and your Zendesk account. The only information we hold is any emails you’ve sent to either myself or Nick.

Thanks,

Mal

—

*Malcolm Lowe
Operations Manager
Synergy Team
Symless”*

— Malcolm Lowe, *Reply to formal quest*

Next to trying to avoid having to answer this formal request, the reply is not true either, since logs were still online hours after receiving this email.

3.6.3 Request for draft review to Nick Bolton

A first 20 page draft of this document was sent to Nick Bolton on November, 22nd, to get a statement.

“Hi Nick,

No idea if this old direct email address is still valid, but I’m trying to reach you directly because the support form was answered inadequately.

I’ve written a draft on why Synergy 2 must be labeled as spyware, but would like to offer you a chance to comment before publishing it, since I am (was) a long term Synergy user and fan.

Best regards,

Patrick Kolla-ten Venne”

— Patrick Kolla-ten Venne, *Request for statements on first draft of this document*

On November, 27th, this was answered by Malcolm Lowe:

*“Hey Patrick,
Nick’s forwarded me your email and asked me to get in touch
regarding your draft paper on Synergy 2.
Nearly all of the issues you’ve raised are covered by the new
GDPR regulations, which Symless is currently working on.
Things such as the privacy policy will be on the website within 3
months. Would you like to be kept up to date on the progress of
this?
Thanks,
Mal
—
Malcolm Lowe
Operations Manager
Synergy Team
Symless”*

— Malcolm Lowe, *Reply to request for statements*

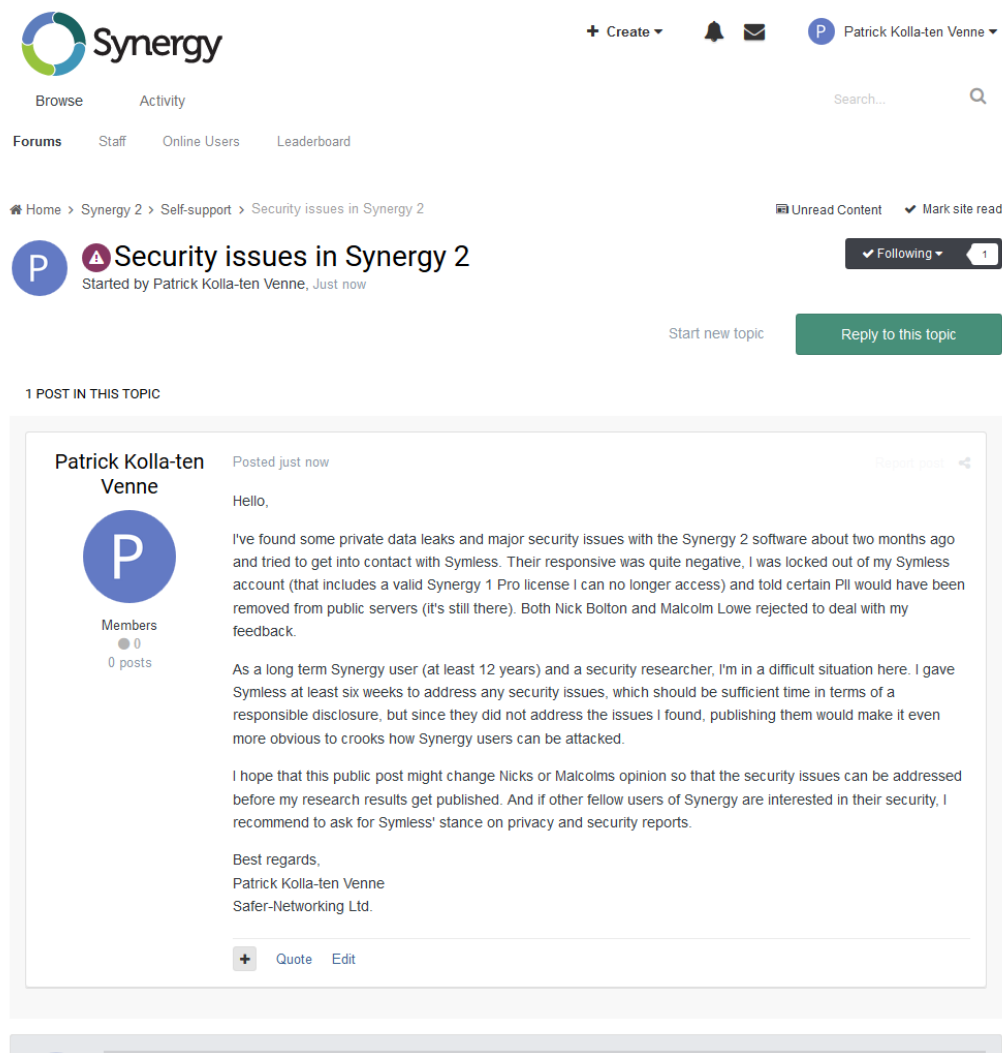
While happy to receive a reply at all, the software security issues cannot be explained with a reference to GDPR, and an approximately three months until operation will properly deal with customers privacy are unacceptable as well.

3.6.4 Forum responsible disclosure

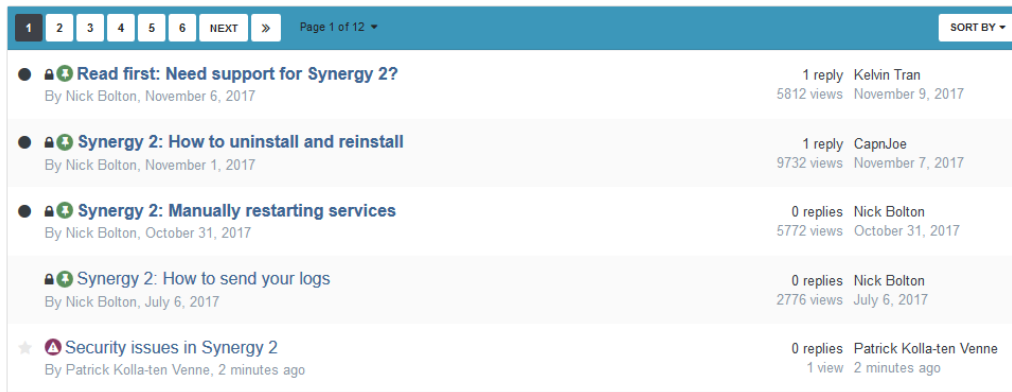
After six weeks without any further response, the author started to evaluate the option of a responsible public disclosure, and started a forum thread²² in the Synergy 2 self support forums²³ as another chance for Symless to react and address any issues. New threads on this forum need to be unlocked by moderators.

²²<https://symless.com/forums/topic/5092-security-issues-in-synergy-2/>

²³<https://symless.com/forums/forum/17-self-support/>



Screenshot 3.16: Request before responsible disclosure, written January 9th, 2018, 10:09 a.m.



Screenshot 3.17: Request listed in thread overview

The Symless account used was not able to answer other public posts, and about an hour later, was unable to login at all. I had to create a new account to be able to post again. The discussion thread was closed with a single comment that the original Symless account was deleted because the software was refunded, without responding to either the deleted Synergy 1 license nor the security question²⁴.



Screenshot 3.18: Closing commit for the disclosure discussion

Without Symless willing to communicate about the issue even there, a description of the possible man in the middle attack was posted to another thread that boasted about a trusted certificate²⁵.

²⁴See screenshot 3.18

²⁵<https://symless.com/forums/topic/5067-auto-config-service-ssl-certificate-broken-also-your?do=findComment&comment=22429>

“I’m glad that you admit that it’s fairly common for malware to install fake root certificates. I guess you would not doubt either that DNS hijacks are even more common (the cheapest one require a simple change to the hosts file).

I’ve verified that Synergy requires a trusted certificate from the API endpoint server, but it’s actually taking any trusted certificate, and even the trusted certificate is extremely weak. This means Synergy can be attacked using fairly common methods. A man-in-the-middle attack can be performed on v1.api.cloud.symless.com using a dns hijack and a locally installed root certificate. The attacker could, to sum it up in simple terms, insert a small 0 or 1 pixel wide screen between the users main screens by manipulating or inserting /profile/update and /screen/update calls, and then track all clipboard content shared between screens, including all those passwords Synergy users might share between desktops.

Usually installing a DNS hijack and a custom root certificate needs elevated admin / root privileges, but there are possible other approaches. DNS hijacks can be (and are) performed using DHCP hijacks (there’s some malware doing exactly that), and since the trusted certificate you use is a common Comodo certificate where symless is just one of dozens of alternate names, hacking any of the other alternate servers (some of which run outdated and vulnerable software) would allow an attacker to use exactly the same original certificate.

This means that to avoid possible attacks, you would not only need to implement certificate pinning, but also use a dedicated trusted certificate instead of that cheap one for the masses. The Synergy machines can be as safe as a machine can be, without those two fixes, they’re vulnerable even without a single piece of malware reaching them.”

— Patrick Kolla-ten Venne, *In reply to Andrew Nelles*

This was followed by information on how to reproduce the issue.

“Don’t believe it? Here are some easy steps to see:

- 1. Install Charles (or Fiddler) on a monitoring machine.*
- 2. Install the Charles (or Fiddler) root certificate on the Synergy machine.*
- 3. Set up Charles (or Fiddler) as http and https proxy on the Synergy machine.*
- 4. Watch how Charles (or Fiddler) decrypts the https traffic on the monitoring machine.*

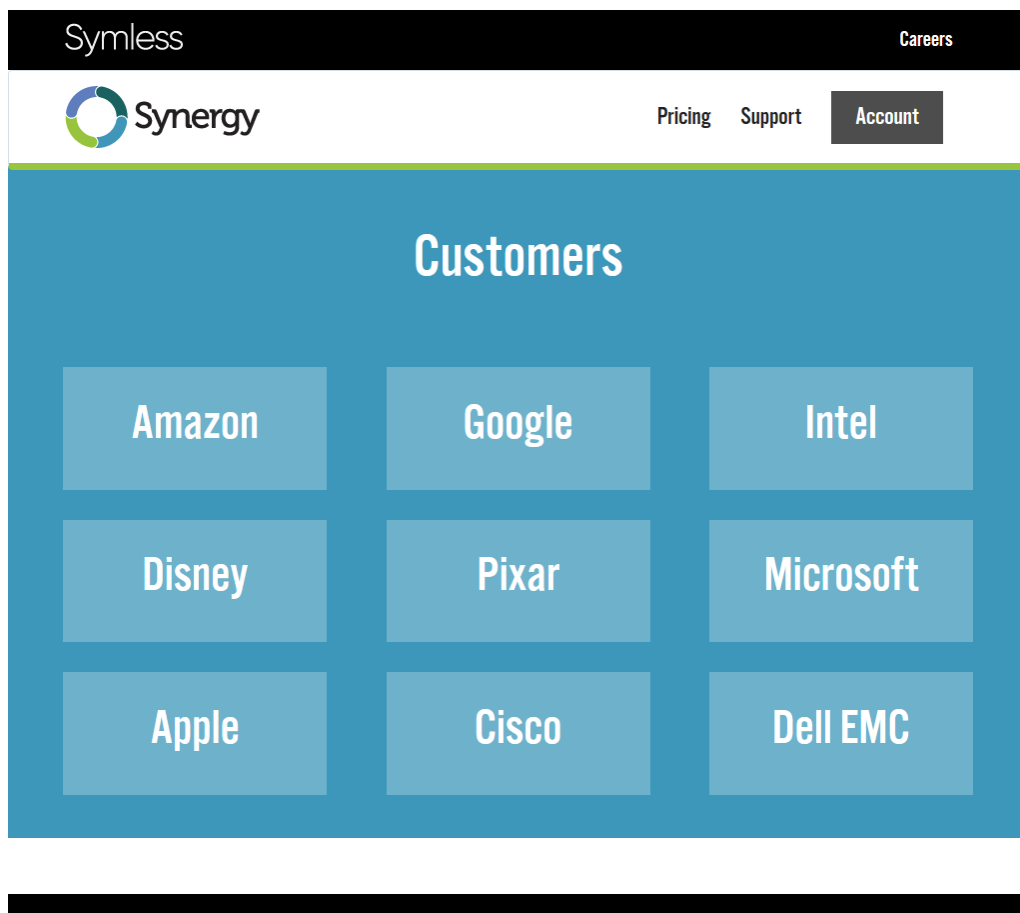
Now imagine that instead of the software above that simply monitors, another software intercepts and manipulates the traffic, either as a proxy, or through a redirection.

As a side note: I informed Symless about this more than six weeks ago to make this a reasonable disclosure. The efforts to fix this would have been a few hundred dollars for a trusted dedicated certificate, an hour for an administration to set this certificate up (including time for coffee and cookies), and a few lines of code for the certificate pinning, maybe a few more lines to make an exception for the software update queries.”

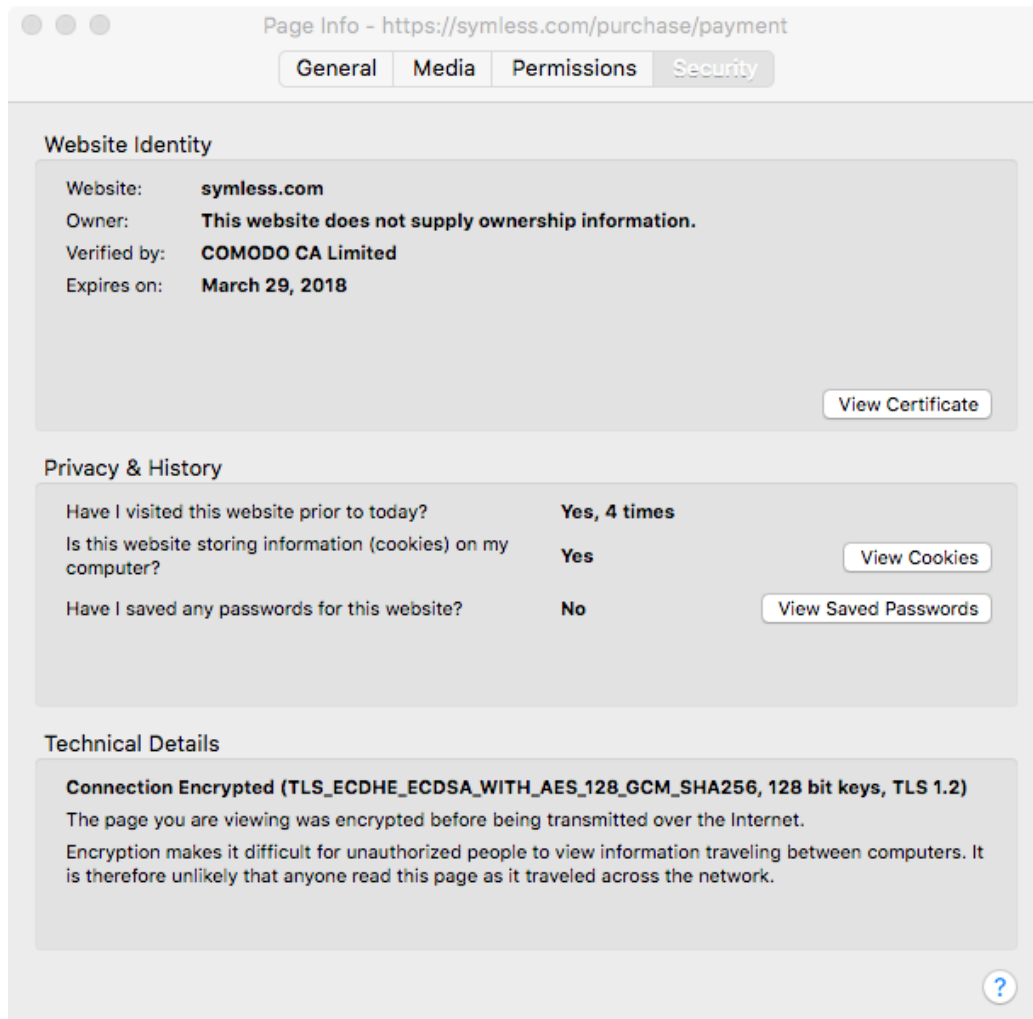
— Patrick Kolla-ten Venne, In the same post as above



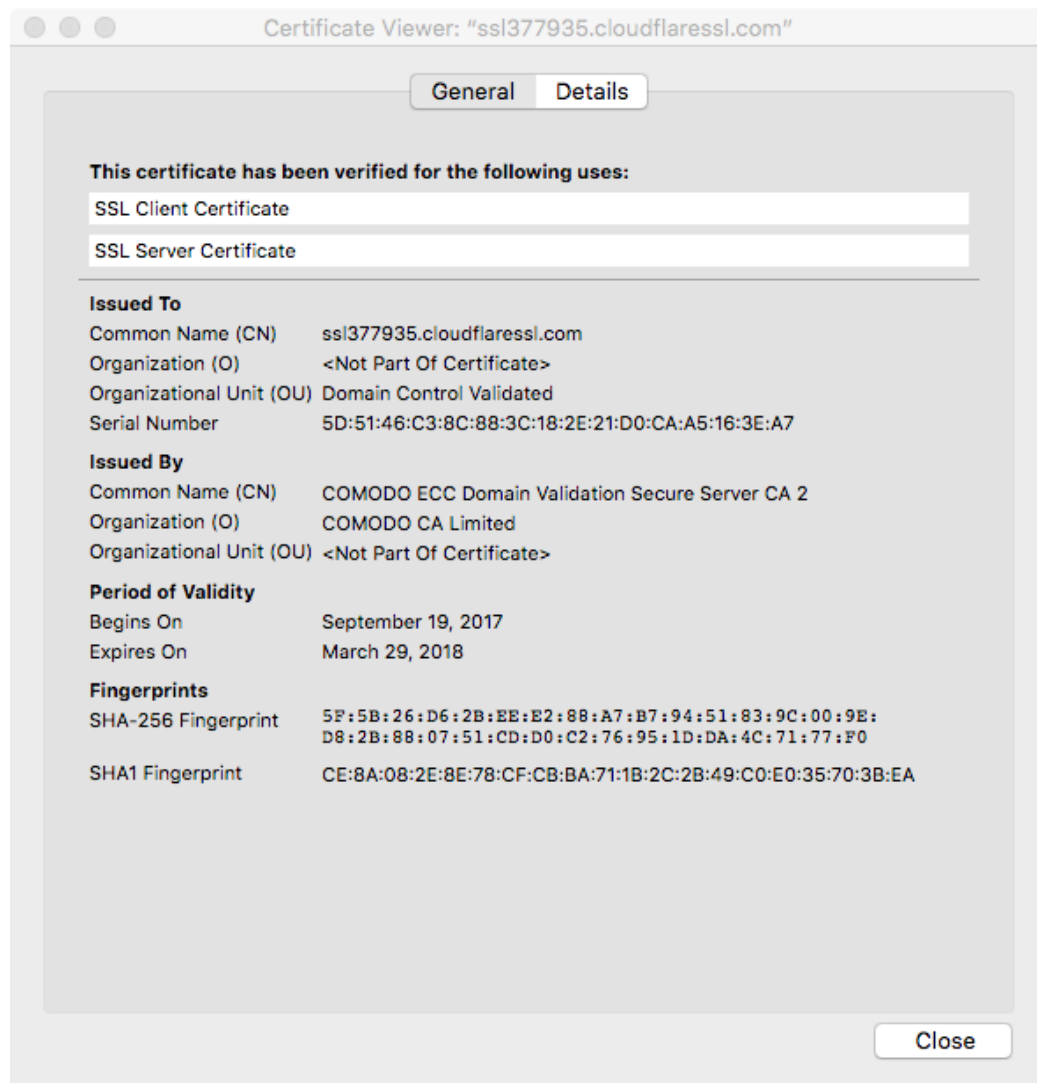
Screenshot 3.1: The website showing off the product



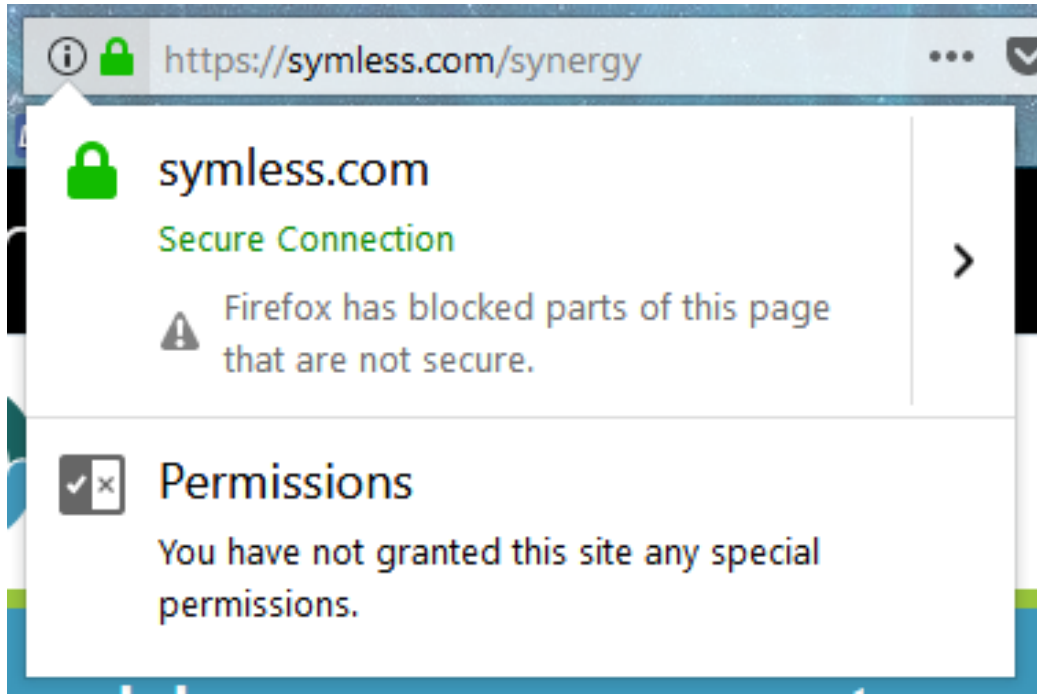
Screenshot 3.2: The website listing well known customers



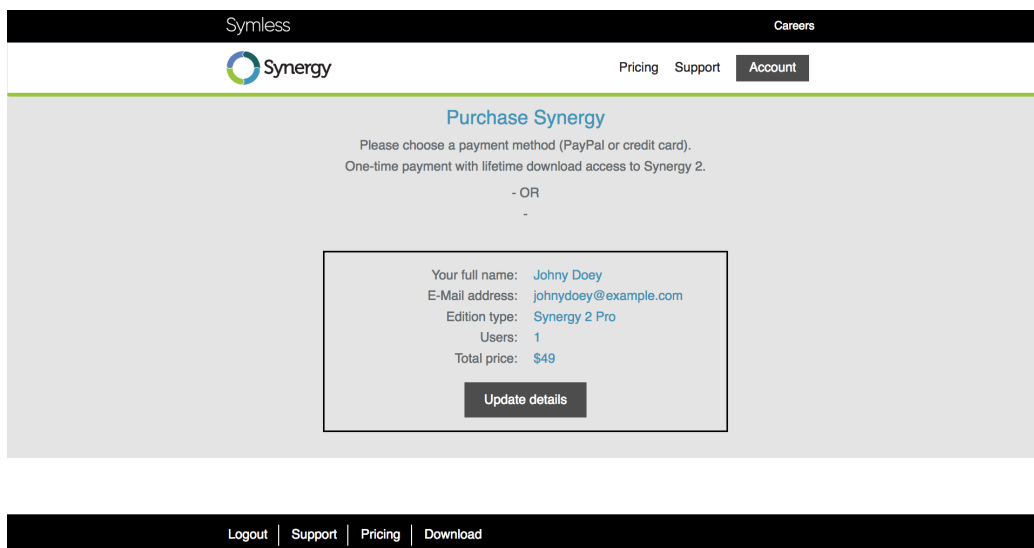
Screenshot 3.3: The website security information from Firefox lists the certificate as having no ownership information



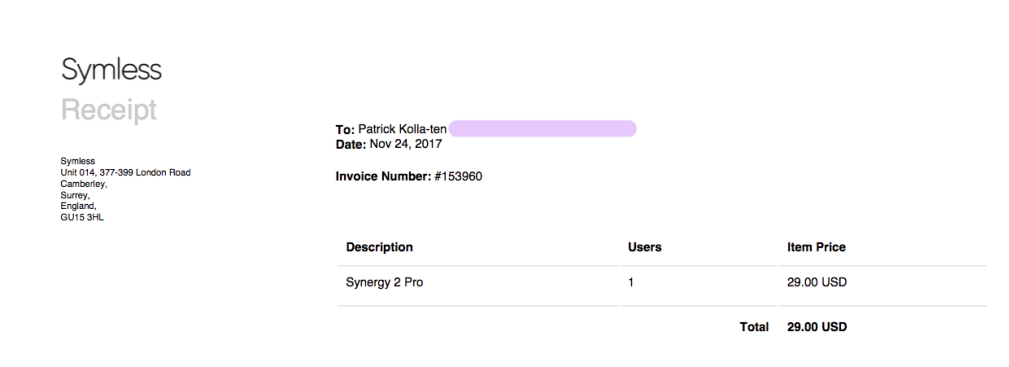
Screenshot 3.4: The certificate information from Firefox does not show the organization



Screenshot 3.5: Firefox warning about unsecure content



Screenshot 3.7: The website shop offering payment methods



Screenshot 3.8: The invoice listing Symless company details

Chapter 4

Software

4.1 Installer

The installers are Windows Installer¹ files. They are signed² by *Symless Ltd*, which is the first place where it is possible to know the name of the company, and verify the source of the files, since the website does not offer ownership information in content nor certificate.

Downloaded for testing was first:

Filename Synergy_v2.0.1-stable_b1240-59dd93a0-x64.msi

Size 33636352 Bytes

MD5 72AFCEB5911A524CC531873BBCC82141

SHA-1 82F754A15E2D8CA8B13791D3DDAA0642E85AE020

SHA-256 AC4190E2785A6E921DFBCBC4C0F264DAE90520B58D0578E5EDF06B9B3AFF6CB3

Codesigning Signer Symless Ltd

Codesigning Timestamp Monday, November 13th, 2017. 10:33

During the tests, a new version was made available:

Filename Synergy_v2.0.2-stable_b1253-665fa610-x64.msi

Size 33628160 Bytes

MD5 0699E66A411617EC9EB2220A9506AFCA

¹https://en.wikipedia.org/wiki/Windows_Installer

²https://en.wikipedia.org/wiki/Code_signing

SHA-1 D17A358FF15406DC2802B0C40409C887025951AB

SHA-256 4B0AE7EB1D3D8CC0EA84E61B2941F50B475F21D3C43245958BF011BE03086980

Codesigning Signer Symless Ltd

Codesigning Timestamp Thursday, November 23th, 2017. 23:38

And later:

Filename Synergy_v2.0.4-stable_b1404-fcb59be4-x64.msi

Size 33665024 Bytes

MD5 15F95BA507F77ABA3532EB7923FF5D70

SHA-1 81352C6C9AA676E44232AFC4B24DF7A88F19C69D

SHA-256 55A84A94E9D0CF69718AC2583575B948CD35E28394633D9556693AC677B80E95

Codesigning Signer Symless Ltd

Codesigning Timestamp Wednesday, December 20th, 2017. 16:36

The digital signature is timestamped³, but signed using only *sha1* as digest algorithm⁴. While this might be needed for Windows Vista, SHA-1⁵ is no longer regarded as state of the art and considered to be broken. Codesigned files should always have signatures using SHA-256⁶.

The installer was created using the WiX Toolset⁷. Possibly outdated installer scripts of Synergy 2.0.0 are available in the Synergy open source repository⁸.

Recommendation 6 (Codesign with SHA-256). *Installer and all PE files should be signed using both SHA-1 and SHA-256.*

This can be done by passing the `/as` (append signature) and `/fd 256` parameters to a second call to `signtool.exe`.

³See screenshot 4.2 on page 62

⁴See 4.1

⁵<https://en.wikipedia.org/wiki/SHA-1>

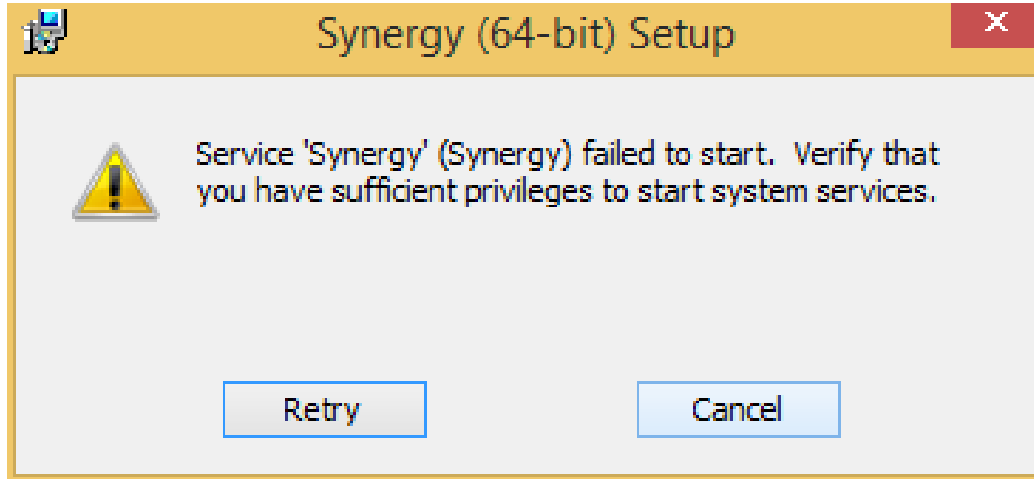
⁶<https://en.wikipedia.org/wiki/SHA-2>

⁷<http://wixtoolset.org/>

⁸<https://github.com/symless/synergy-core/tree/master/dist/wix>

4.2 Installation

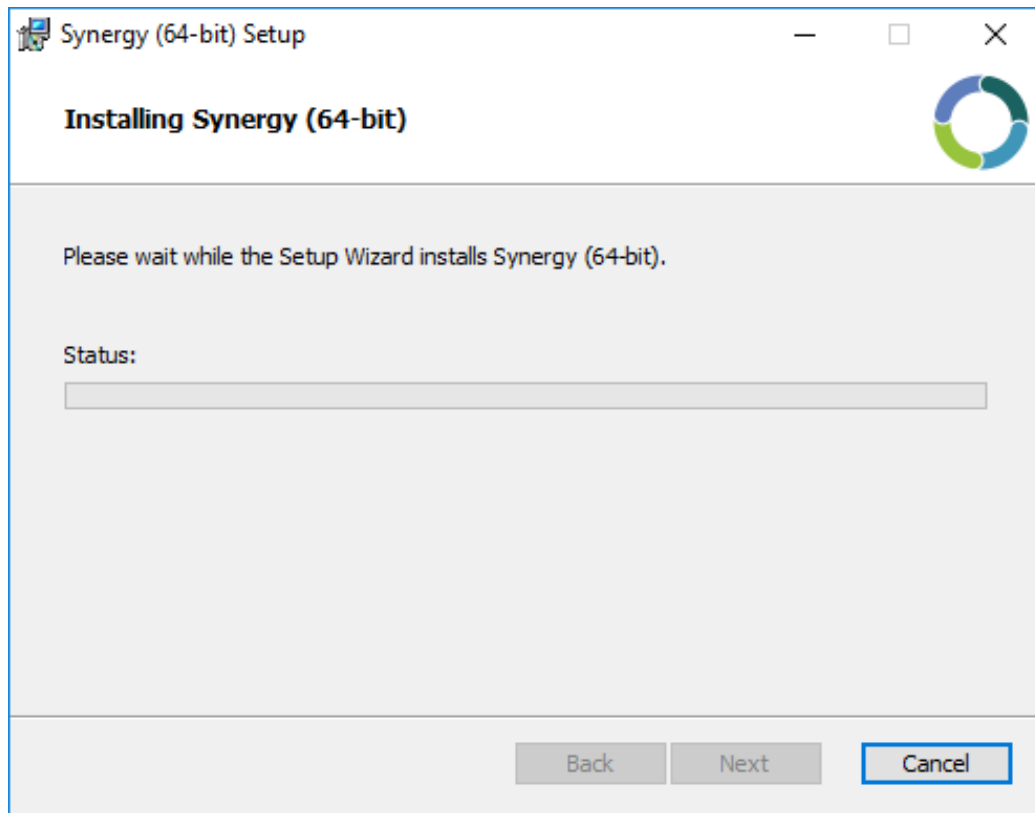
The installation of Synergy 2.0.1 failed on Windows 8 and Windows 8.1⁹.



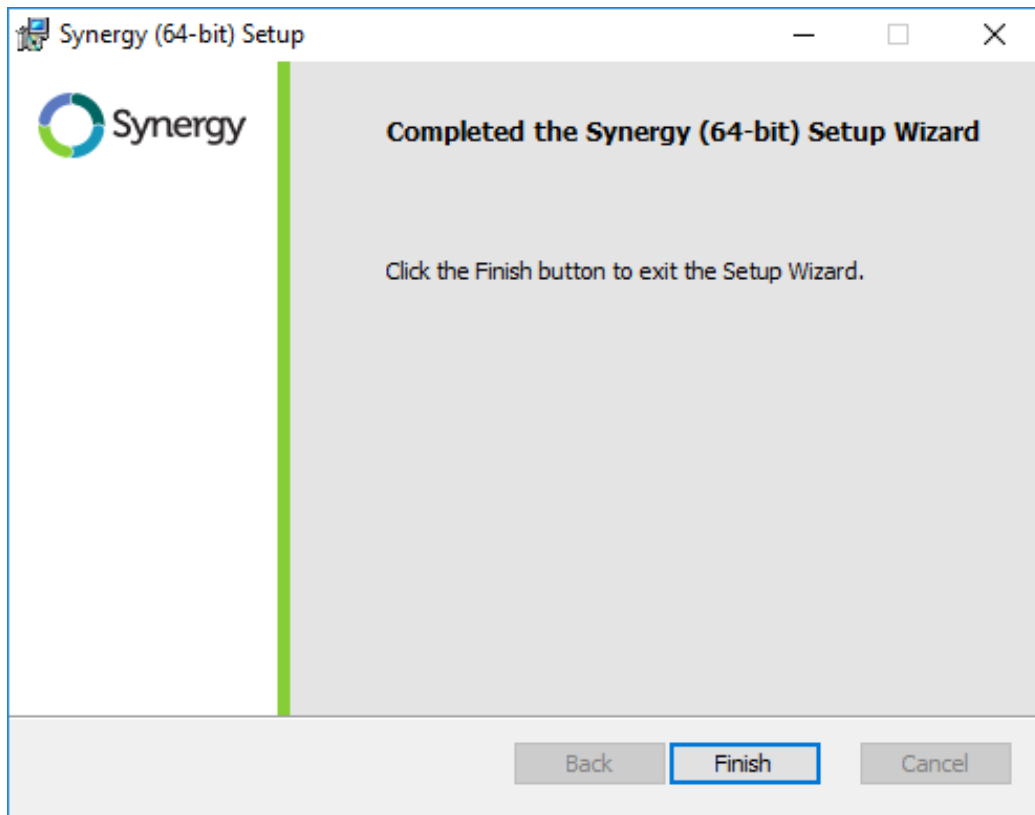
Screenshot 4.4: The installer failing on Windows 8.x

It runs fine on five tests on Windows 10 in various releases.

⁹See screenshot [4.4](#)



Screenshot 4.5: The installer ready to start



Screenshot 4.6: The installer has finished

4.2.1 Files

The installation places the product files on the hard disk without troubles on Windows 10 in our tests.

The installed files include:

- Qt libraries¹⁰
- OpenSSL¹¹ 1.0.2l binaries
- Visual C runtime libraries

Listing 4.1: Installer WiX script component part

```
<Feature Id="ProductFeature" Title="$(var.Name)">
```

¹⁰Qt is a cross-platform application framework, see [https://en.wikipedia.org/wiki/Qt_\(software\)](https://en.wikipedia.org/wiki/Qt_(software))

¹¹<https://www.openssl.org>

```

<ComponentGroupRef Id="ProductComponents"/>
<ComponentGroupRef Id="OpenSSLComponents"/>
<ComponentGroupRef Id="ProductQtPluginComponents"/>
<MergeRef Id="CRT"/>
<?if $(var.Configuration) = "Debug" ?>
<MergeRef Id="DebugCRT"/>
<?endif ?>
<ComponentRef Id="RegistryEntries"/>
</Feature>

```

Files are only installed into the destination location.

Listing 4.2: Installer WiX script files part

```

<Directory Id="TARGETDIR" Name="SourceDir">
  <Directory Id="$(var.ProgramFilesFolder)">
    <Directory Id="INSTALLFOLDER" Name="$(var.Name)">
      <Merge DiskId="1" Id="CRT" Language="0" SourceFile="$(var
        ↪ .CRT)"/>
      <?if $(var.Configuration) = "Debug" ?>
      <Merge DiskId="1" Id="DebugCRT" Language="0" SourceFile="
        ↪ $(var.DebugCRT)"/>
      <?endif ?>
      <Directory Id="OpenSSLDDir" Name="OpenSSL"/>
      <Directory Id="PlatformsDir" Name="Platforms"/>
    </Directory>
  </Directory>
  <Directory Id="ProgramMenuFolder"/>
</Directory>

```

Since encryption is used to protect sensitive PII shared between desktops possibly over the Internet, the OpenSSL libraries play a special role. The used version 1.0.2 is a long term support version, but version 1.0.2l was released in May 2017. Starting November 2nd, version 1.0.2m is available.

Recommendation 7 (Update OpenSSL to 1.0.2m). *Update OpenSSL to 1.0.2m.*

4.2.2 Registry

There are just a few standard registry entries, nothing extraordinary here.

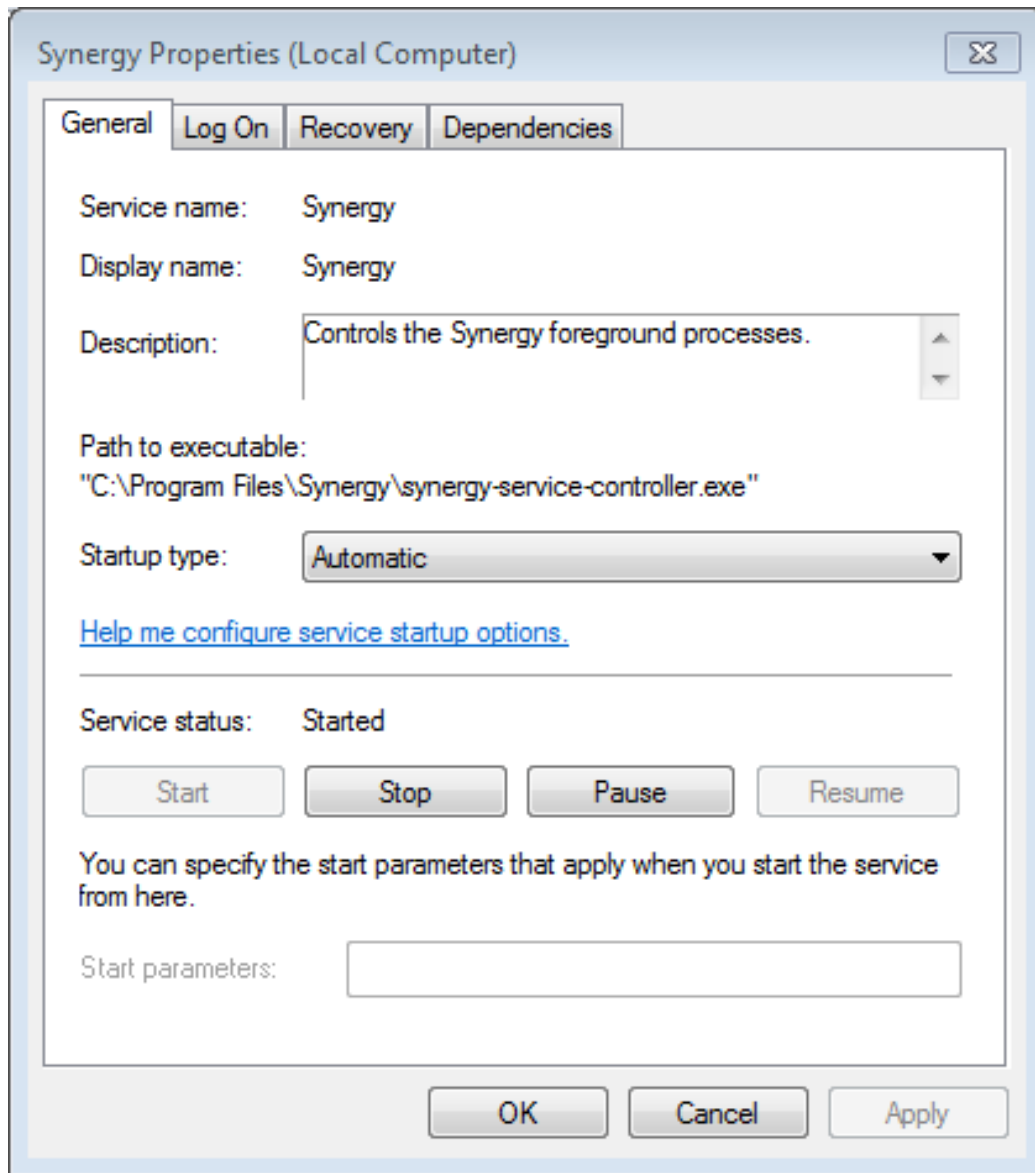
Listing 4.3: Installer WiX script registry part

```
<DirectoryRef Id="TARGETDIR">
  <Component Guid="7CF3564D-1F8E-4D3D-9781-E1EE22D5BD67" Id="
    ↳ RegistryEntries">
    <RegistryKey ForceCreateOnInstall="yes"
      ↳ ForceDeleteOnUninstall="yes" Key="Software\Microsoft\
      ↳ Windows NT\CurrentVersion\AppCompatFlags\Layers" Root
      ↳ ="HKLM">
      <RegistryValue Name="[INSTALLFOLDER]synergys.exe" Type="
        ↳ string" Value="~ HIGHDPIAWARE WIN7RTM"/>
    </RegistryKey>
    <!-- Windows 8 and later only -->
    <Condition><![CDATA[Installed OR (VersionNT >= 602)]]></
      ↳ Condition>
    </Component>
  </DirectoryRef>
```

4.2.3 Services

A background system service called *Synergy*¹² gets installed. This services handles communication between configuration frontend and the background core that supplies the actually KVM functionality. It also acts as a watchdog, restarting killed processes.

¹²See screenshot 4.7 on the next page



Screenshot 4.7: Service Manager showing Synergy service details

When ending this service, it writes user information into the registry. To reset the login, one has to stop this service, close the configuration user interface, and remove the registry content before restarting the user interface and service. The same procedure is necessary when trying to sneak in `userId` and `userToken` from a different installation ¹³.

¹³See section 6.1 on page 76

4.2.4 Processes

synergy-config.exe The user interface that allows to configure screens is shown by this executable. It communicates via TCP/IP with **synergy-service.exe**¹⁴.

synergy-core.exe This executable is responsible for the actual KVM functionality.

synergy-service.exe This executable handles the core module, and communicates with the frontend in **synergy-config.exe** using local TCP/IP connections¹⁵.

synergy-service-controller.exe This is the service executable that belongs to the Windows System Service for Synergy. It starts the actual service that can be found in **synergy-service.exe**. This separation into Windows System Service executable and separate functionality is probably due to the multi-platform approach of Synergy, keeping the platform specific code in this process.

crashpad_handler.exe Is an unsigned executable without version details that is designed to communicate with a background server at **synergy.sp.backtrace.io** on port 6098, probably in case of crashes. This is another sharing of PII (at least the contacting IP address) that would have to be mentioned as part of a *Privacy Policy*.

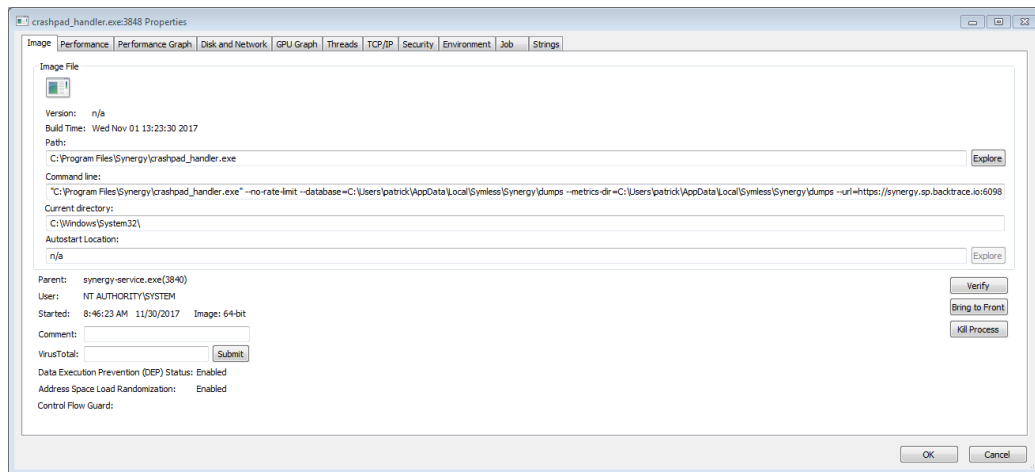
“Crashpad is an open-source library initially developed by Google as a successor to the Google Breakpad library. It is used in popular software such as Google Chrome, and by companies such as Slack and Spotify. For existing users of Crashpad, Backtrace has plug-and-play support. It has a robust architecture designed to allow for a high degree of customizability and stability even in the face of most obscure of software crashes.”

— Backtrace I/O Inc., *Crashpad description*^a

^ahttps://documentation.backtrace.io/product_integration_minidump_crashpad/index.html

¹⁴See screenshot 4.10 on page 65

¹⁵See screenshot 4.12 on page 67



Screenshot 4.8: Process details for crashpad_handler.exe

Requirement 6 (Software Backtrace Privacy Policy). *The user needs to be informed that in case of crashes, PII will be transmitted to a third party, Backtrace I/O Inc.¹⁶, including details on the data and how that third party treats the data.*

To prevent Synergy from sending data to Backtrace I/O Inc., adding the entry `0.0.0.0 synergy.sp.backtrace.io` to the hosts file¹⁷ would work on Windows, macOS and Linux¹⁸.

Inter Process Communication

IPC¹⁹ takes places between `synergy-config.exe`²⁰, which is the configuration user interface, and `synergy-service.exe`²¹, which manages the background.

4.3 Login

After finishing installation, a login with the Symless website login is mandatory²². While the website lists a *Cloud Bridge* as ‘coming soon’, this is

¹⁶110 Fifth Avenue, Floor 5, New York, NY 10011, United States of America

¹⁷[https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file))

¹⁸For macOS and Linux, make sure `nsswitch.conf` gives files priority over dns

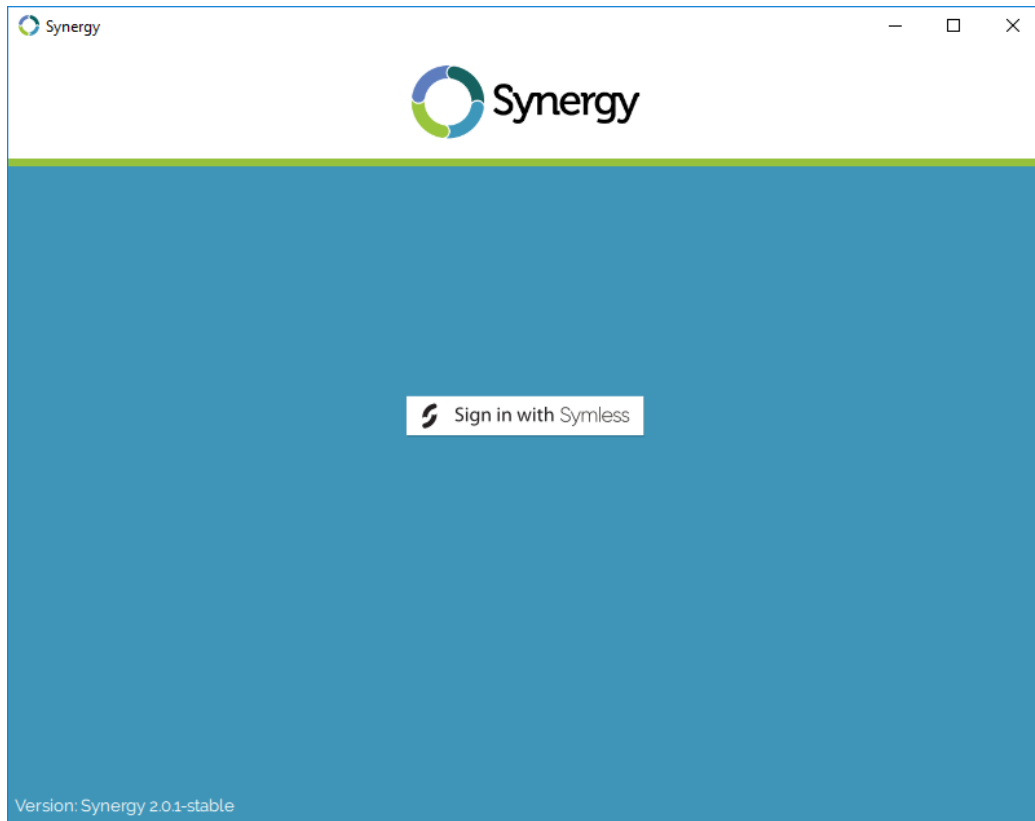
¹⁹IPC stands for Inter Process Communication

²⁰See screenshot 4.10 on page 65

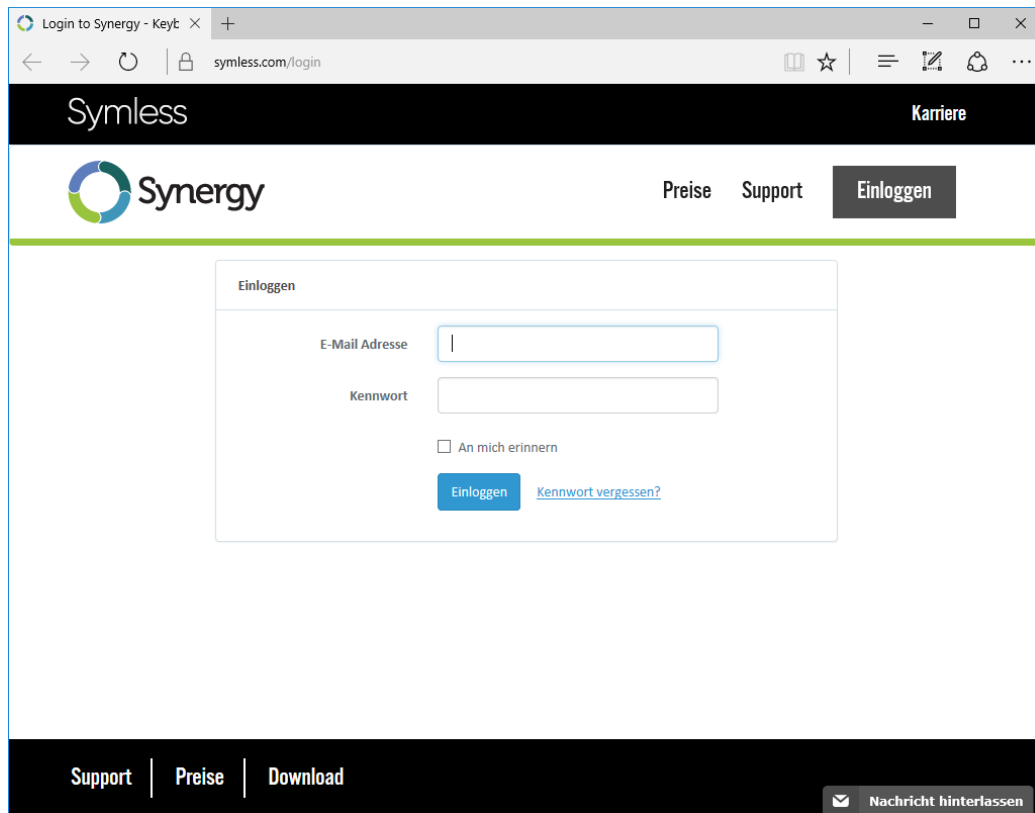
²¹See screenshot 4.12 on page 67

²²See screenshot 4.14 on the next page

unexpected behaviour since previous versions were running in a local context only.



Screenshot 4.14: The login prompt shown by the software



Screenshot 4.15: The login shown in the systems standard browser

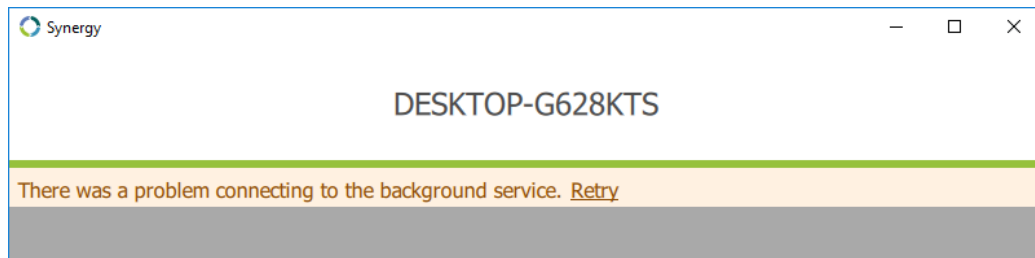
Recommendation 8 (Inform on new behaviour). *Inform the user before downloading or buying that this product will behave differently than previous versions in that it connects to the Internet before establishing sessions.*

The login opens a browser for login²³ and seems to perform an OAuth authentication. Once returned to the software, the user is prompted with an error message encountered in all three test runs²⁴:

“There was a problem connecting to the background service.
Retry.”

²³See screenshot 4.15

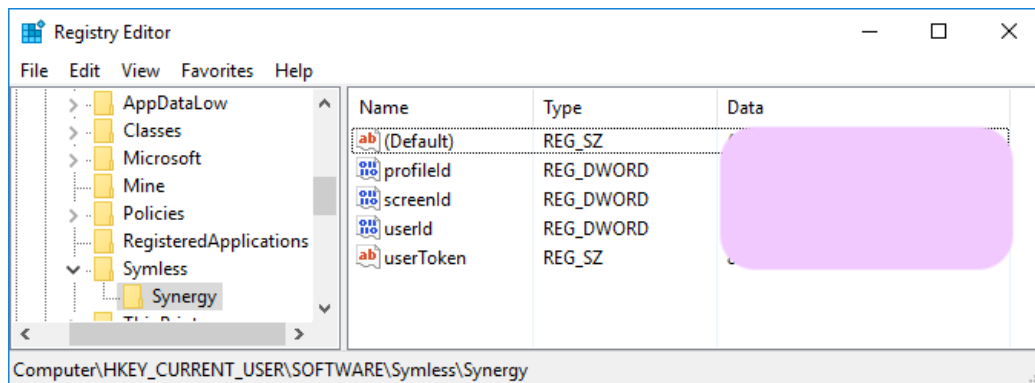
²⁴See screenshot 4.16 on the next page



Screenshot 4.16: Software failure after login

4.3.1 Registry

The login will also fill in certain pieces of information inside the registry.



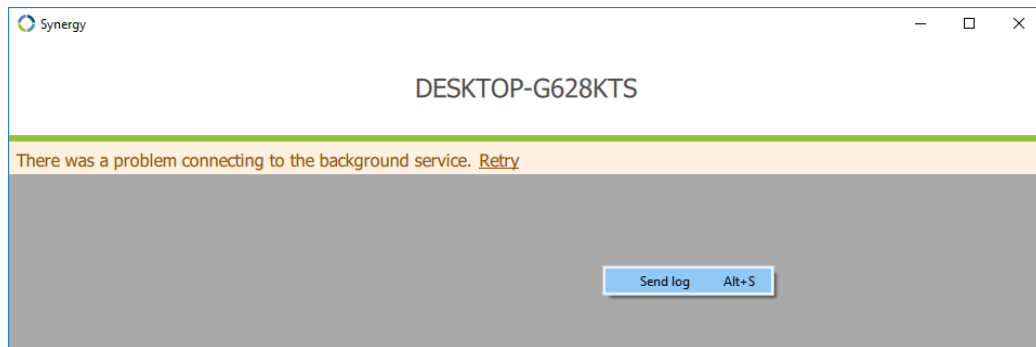
Screenshot 4.17: Registry entries used by Synergy

The entries named *userId* and *userToken* are of importance here, since they are part of the logs transmitted, as part of the path and contents.

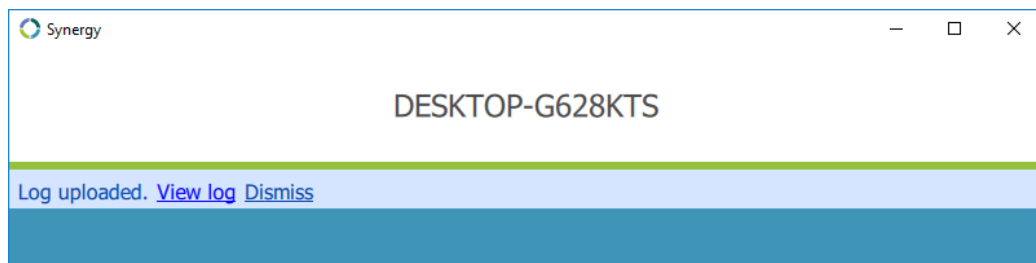
Recommendation 9 (Improve data storage). *Do not store important information like the OAuth token in plain text.*

4.4 Logs

When right-clicking the user interface, it offers a choice names *Send log*. Synergy uploads a log to Synergy servers right away, and only afterwards allows the user to view the log content. This is done through a URL that would allow others to view this log by just knowing or guessing the URL, without further protection.



Screenshot 4.18: Context menu offers upload of log



Screenshot 4.19: Log available via URL after upload only

Requirement 7 (Software Privacy Policy). *Before transmitting PII, the user needs to be informed about the exact PII, the purpose of the transmission, any third parties with whom the data will be shared, and the terms of storage.*

On Windows, the end ellipsis here could indicate to the user that he will be shown a dialog with options before the action described in the menu item is executed. This is documented for example in the Punctuation Guidelines²⁵:

“Ellipsis: Use at the end of a menu item or button label for a command that opens a dialog box rather than immediately performing an action. The ellipsis is a visual cue that the user has to supply additional information to complete the command, not simply that a message, dialog box, or window opens (hence, Properties does not use an ellipsis). Always use an ellipsis on Browse buttons. Also, ellipses are used in progress indicator labels to indicate a continuing action.”

— Microsoft, *Punctuation Guidelines*

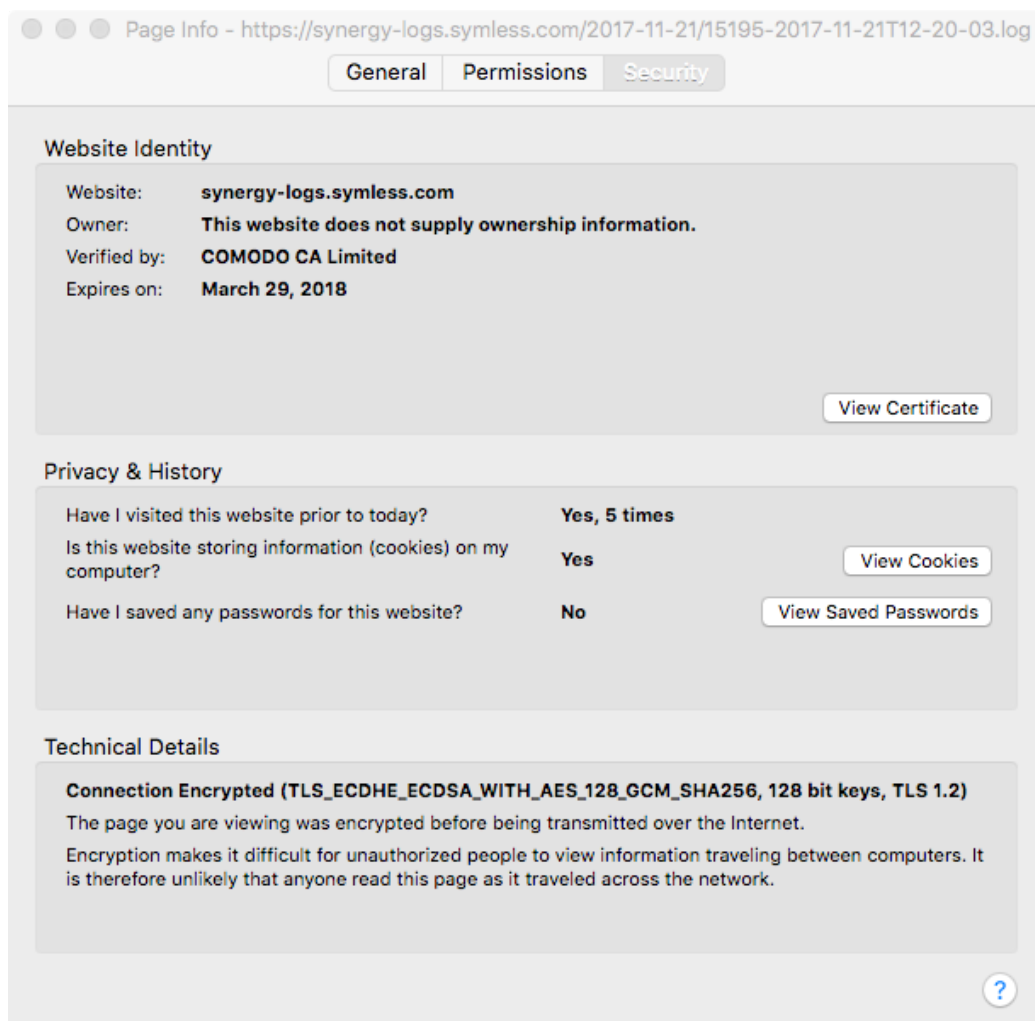
²⁵[https://msdn.microsoft.com/en-us/library/windows/desktop/bb226801\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/bb226801(v=vs.85).aspx)

4.4.1 Log server

Logs are stored on <https://synergy-logs.symless.com> with a path constructed of date, time, and the *userId* known from section 4.3.1 on page 52, and are accessible without login from anywhere.

`https://synergy-logs.symless.com/<year>-<month>-<date>/<userId>-<year>-<month>-<date>T<hour>-<minute>-<second>.log`

This subdomain is also hosted by CloudFlare and the certificate has no ownership information ²⁶.



Screenshot 4.20: Log subdomain certificate not showing the organization either

²⁶See screenshot 4.20

Let's take a look at the ASC²⁷'s definition of spyware²⁸. While the ASC is no longer active, these definitions are the last definitions agreed upon by the whole industry. Emphasis was placed by author and is not part of the quote.

Underlying Technology Tracking Software

Description of Underlying Technology Used to monitor user behavior or gather information about the user, sometimes including personally identifiable or other sensitive information.

- May be used for legitimate monitoring: e.g. by parents or companies
- May be a necessary component of adware that is linked to wanted software
- May allow customization

Why the Underlying Technology May Be Wanted .

- *Done covertly, tracking is spying*
- May collect personal information that can be shared widely or stolen, resulting in fraud or ID theft
- Can be used in the commission of other crimes, including domestic violence and stalking
- Can slow machine down
- May be associated with security risks and/or loss of data

Why the Underlying Technology May Be Unwanted .

- *Spyware (narrow)**
- Snoopware
- Unauthorized Keylogger
- Unauthorized Screen Scraper

Common Terms for Well- Known Unwanted Varieties

²⁷Anti-Spyware Coalition

²⁸<http://web.archive.org/web/20121025143706/http://antispywarecoalition.org/documents/2007definitions.htm>

4.4.2 Log contents

The log file includes personally identifiable and personally identifying information like user names, computer names, local and public IP addresses as well as authentication tokens used by the software.

Listing 4.4: A few PII containing lines from the logs

```
[ Core ] [2017-11-21T12:13:32] INFO: switch from "machine1" to  
    ↪ "machine2" at 1049,933  
[ Core ] [2017-11-21T12:13:18] DEBUG: opening configuration "C  
    ↪ :\Users\JohnnyDoey\AppData\Local\Symless\Synergy\synergy.  
    ↪ conf"  
[ Router ] [2017-11-21T12:13:37] debug: Connecting to  
    ↪ 1.2.3.4:24802 (attempt 7/10)  
[ Router ] [2017-11-21T12:13:37] debug: Connecting to  
    ↪ 5.6.7.8:24802 (attempt 7/10)  
[ Service ] [2017-11-21T12:20:01] debug: got user auth token:  
    ↪ XXXXX
```

User name and computer name can often help to identify a user by full name (e.g. *Johnny Doey's Notebook* as computer name or full name as user name). Using a geo lookup on the public IP would then likely result in a clear identification of an individual.

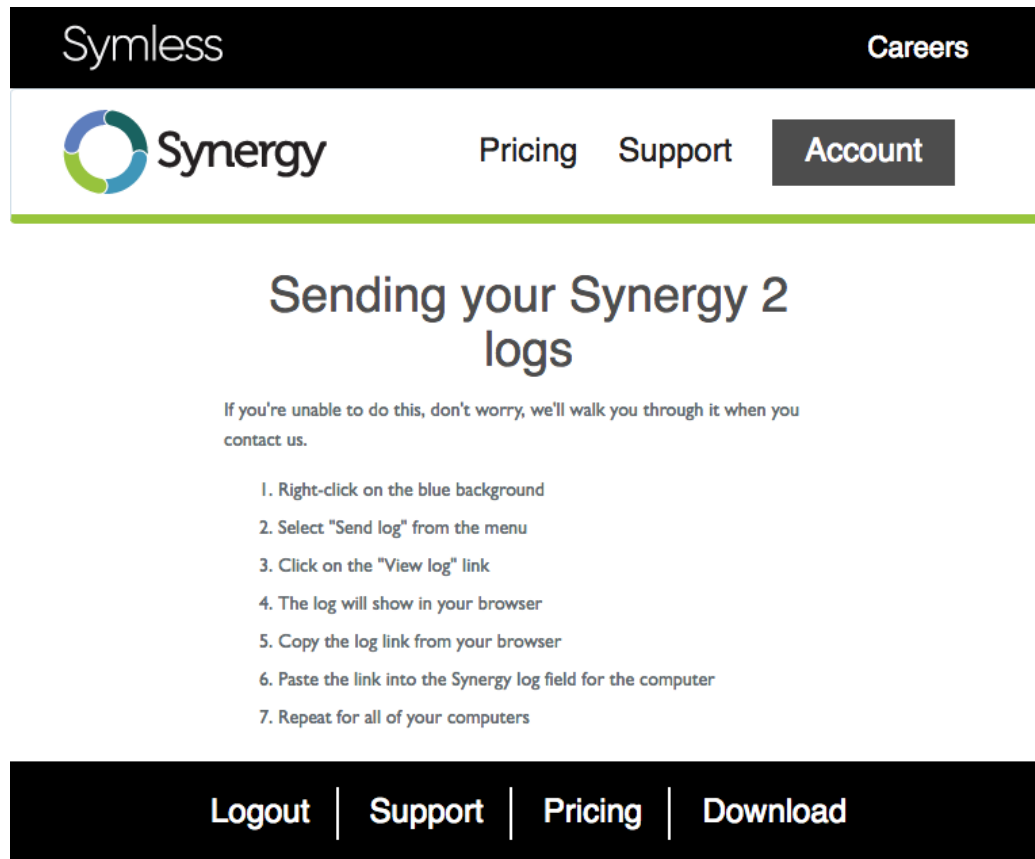
Requirement 8 (No public PII). *PII must not be stored in public locations like it is currently done.*

The user auth token, which is also stored in the registry and static, allows authentication to the service. Since Synergy is open source, the protocol is available and hackers with access to log URLs could probably use this token to hook into systems. Due to the clipboard sharing features, they would get access to sensitive information like logins and passwords.

Requirement 9 (No unnecessary data in logs). *Do not transmit authentication information like the user token at all. Should it be required for support operation to validate the correct token, transmit only a few characters of it.*

4.4.3 Log handling

Website support page

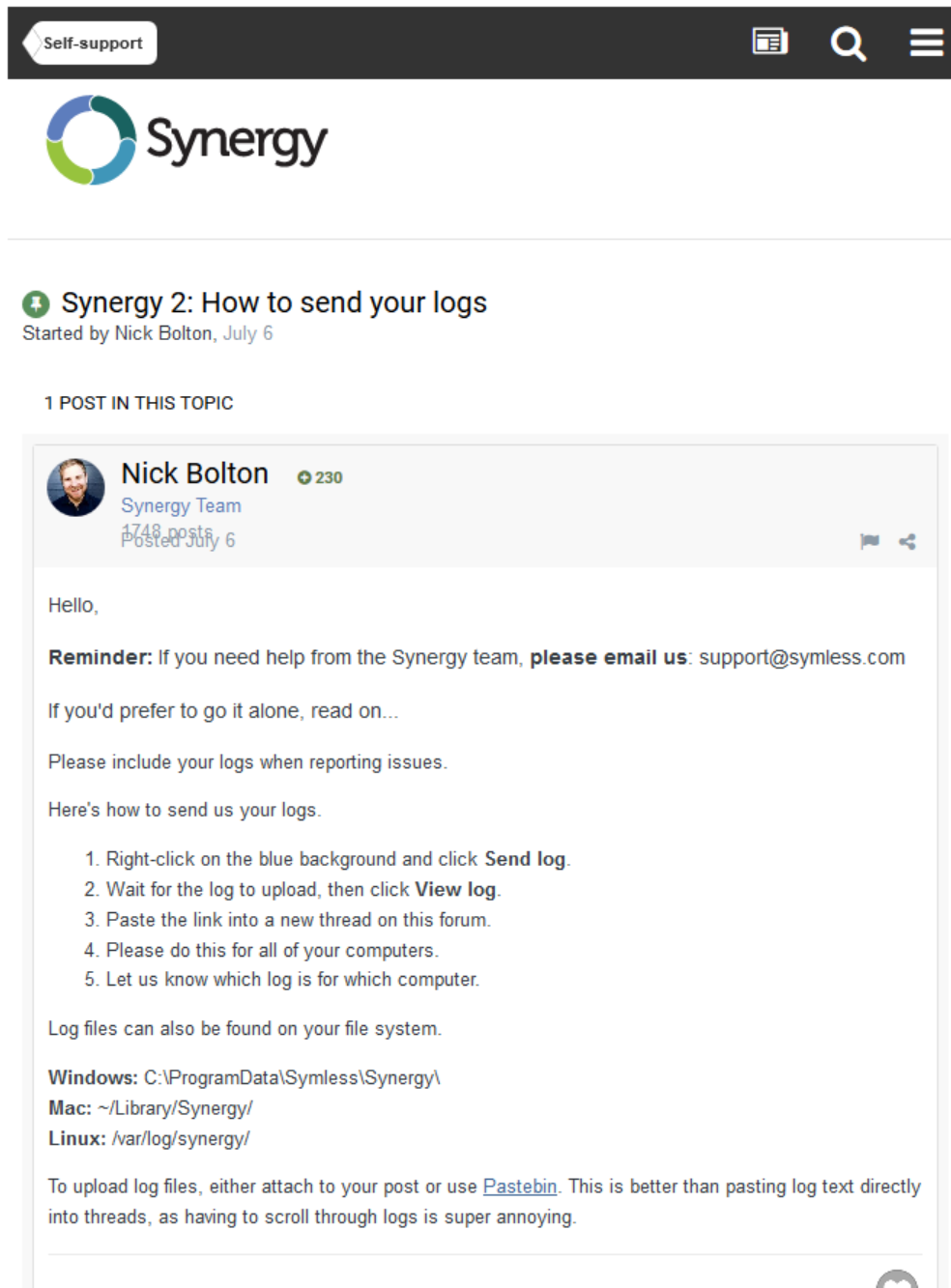


Screenshot 4.21: Support website asking to spread logs

The support website informs the user on how to submit logs, not informing him that these will be stored in the public.

Requirement 10 (Support website privacy information). *The support website that tells the user to use the Send log function needs to emphasize that PII of the user will be stored in a public location.*

Support forums



Screenshot 4.22: Forum asking to spread logs

The official support forum has a thread called *How to send your logs*²⁹ that suggests how logs should be treated, including:

- Paste link to log on forum
- Upload log to Pastebin website³⁰

While one could argue that with public log URLs, the PII is already out there in the public, asking users to post it on a forum or the Pastebin website is grossly negligent.

Requirement 11 (Forum log handling). *Inform user that by following your instructions, he will share PII with the public.*

4.5 Uninstallation

Uninstall complains about files in use, but was able to remove all files from the test system.

Recommendation 10 (Improve uninstall). *Proper termination and uninstallation without error interruptions will help the user to feel assured the software has really been removed and will no longer transmit PII.*

4.6 Open Source

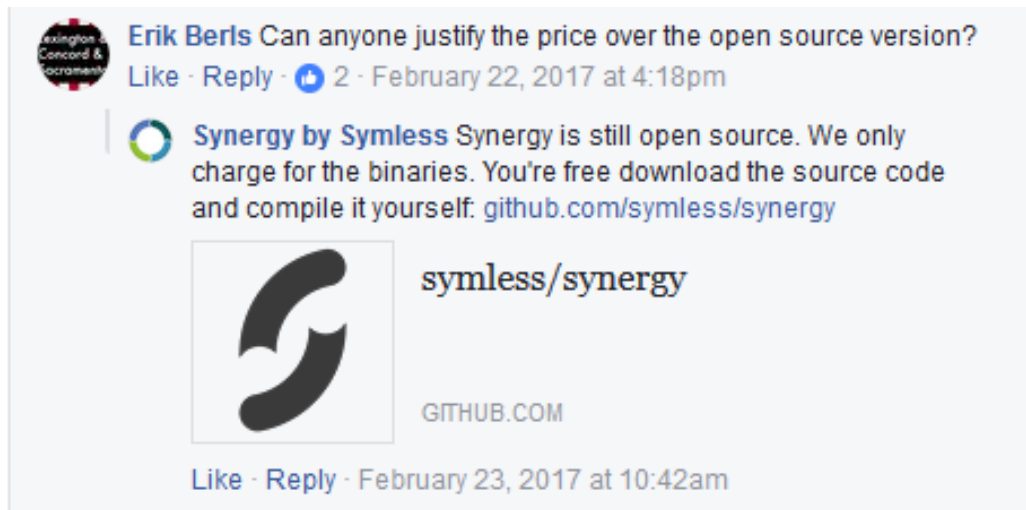
According to a Facebook post from February 23rd³¹, Synergy should be open source. The repository cannot be found on GitHub though³².

²⁹<https://symless.com/forums/topic/3207-synergy-2-how-to-send-your-logs/>

³⁰<https://pastebin.com/>

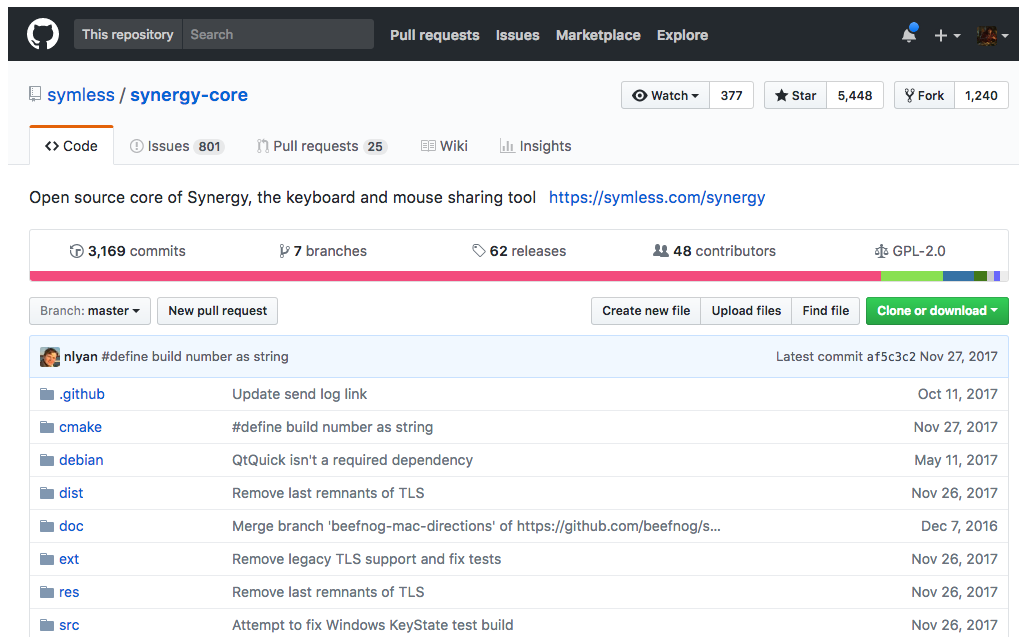
³¹See screenshot 4.23 on the following page

³²<https://github.com/symless/synergy>



Screenshot 4.23: Facebook post mentioning open source

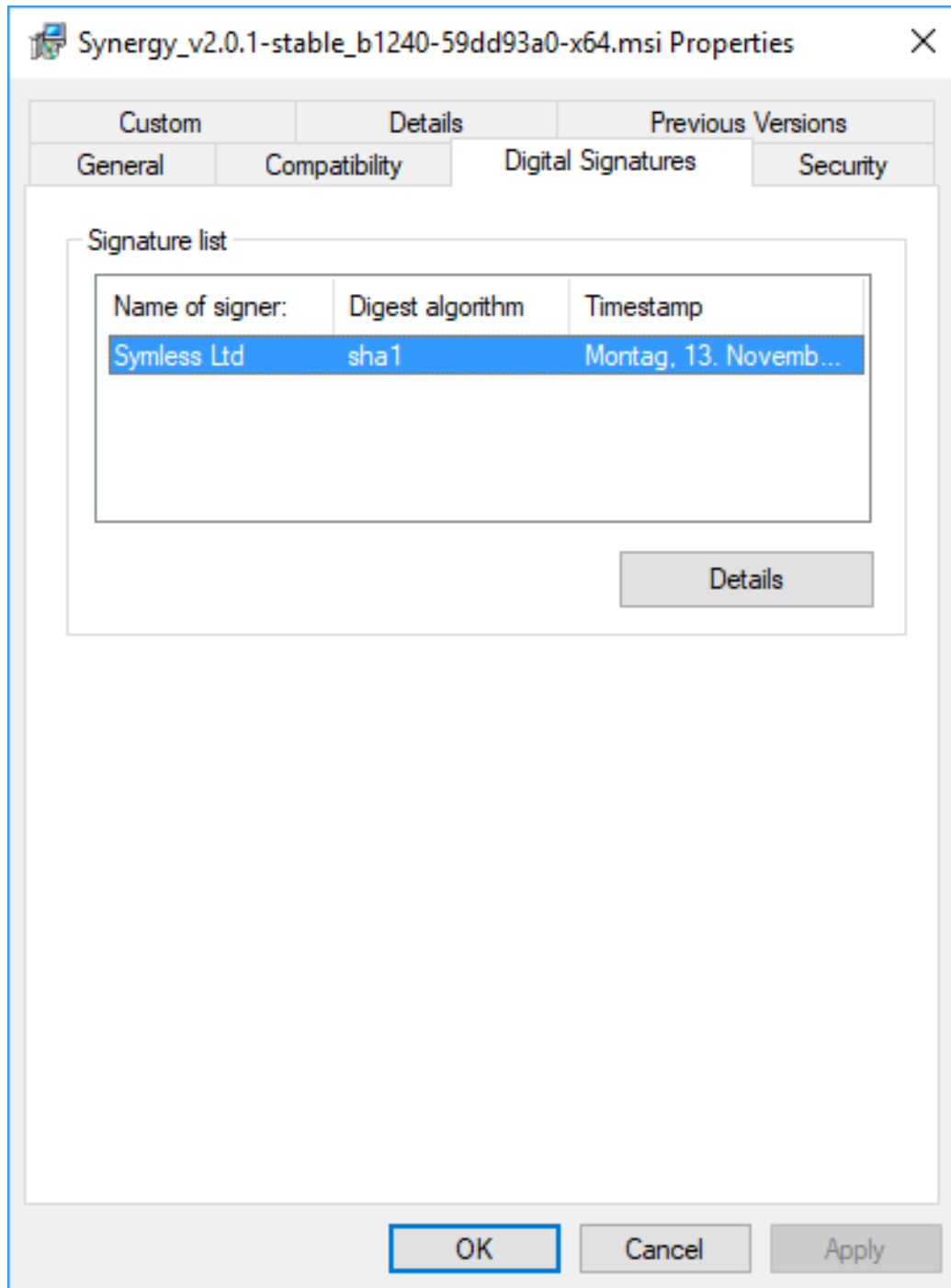
The core components only are open source and as such, available online³³.



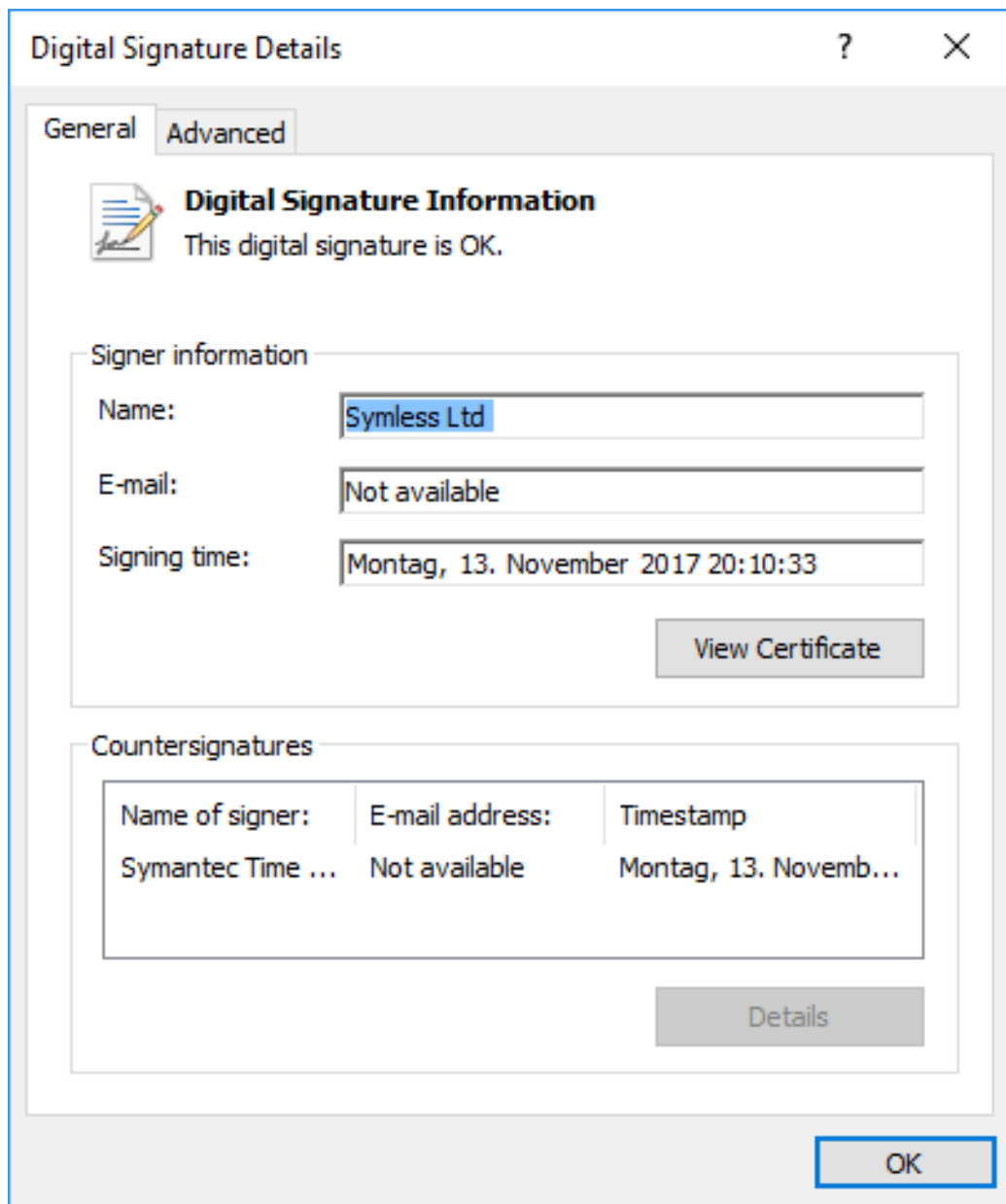
Screenshot 4.24: GitHub start page for Synergy core project

The issues here mostly arise out of the user interface and cloud features that are not open source.

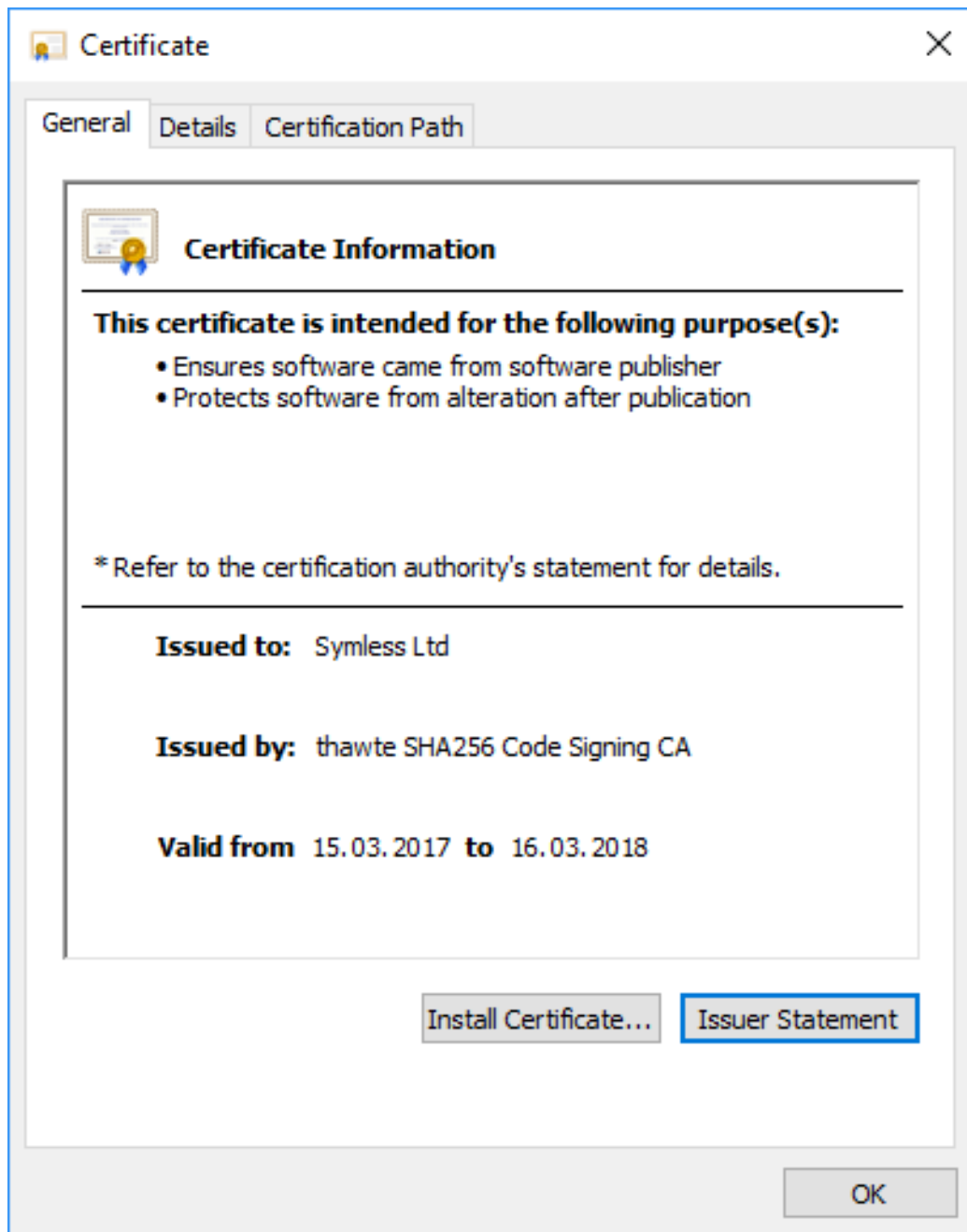
³³<https://github.com/symless/synergy-core>



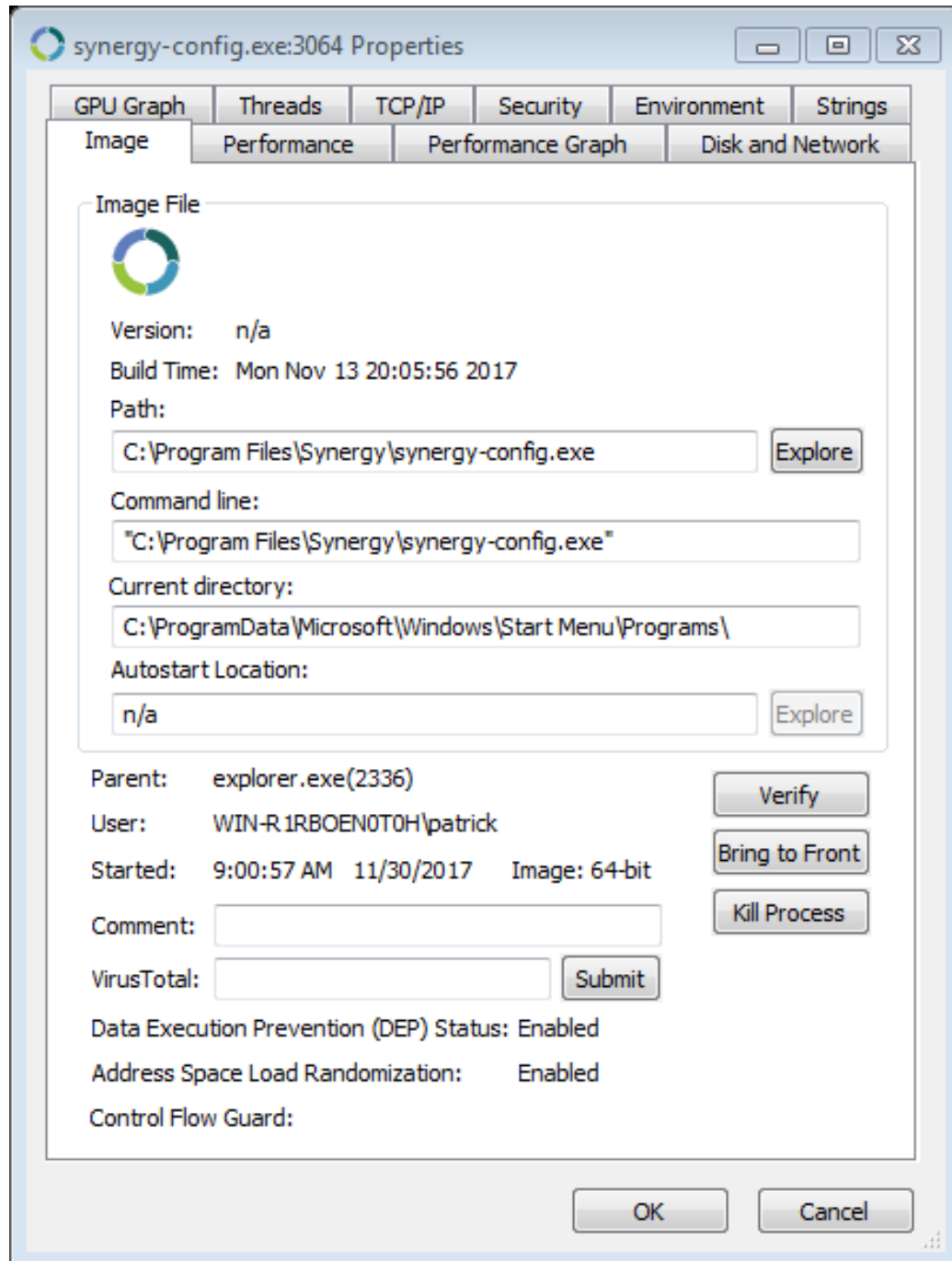
Screenshot 4.1: Digital signatures of installer



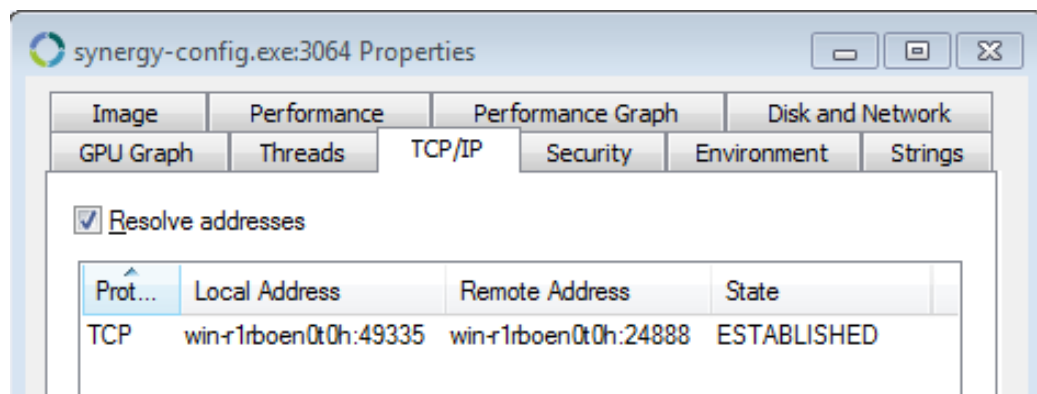
Screenshot 4.2: Digital signature details of installer



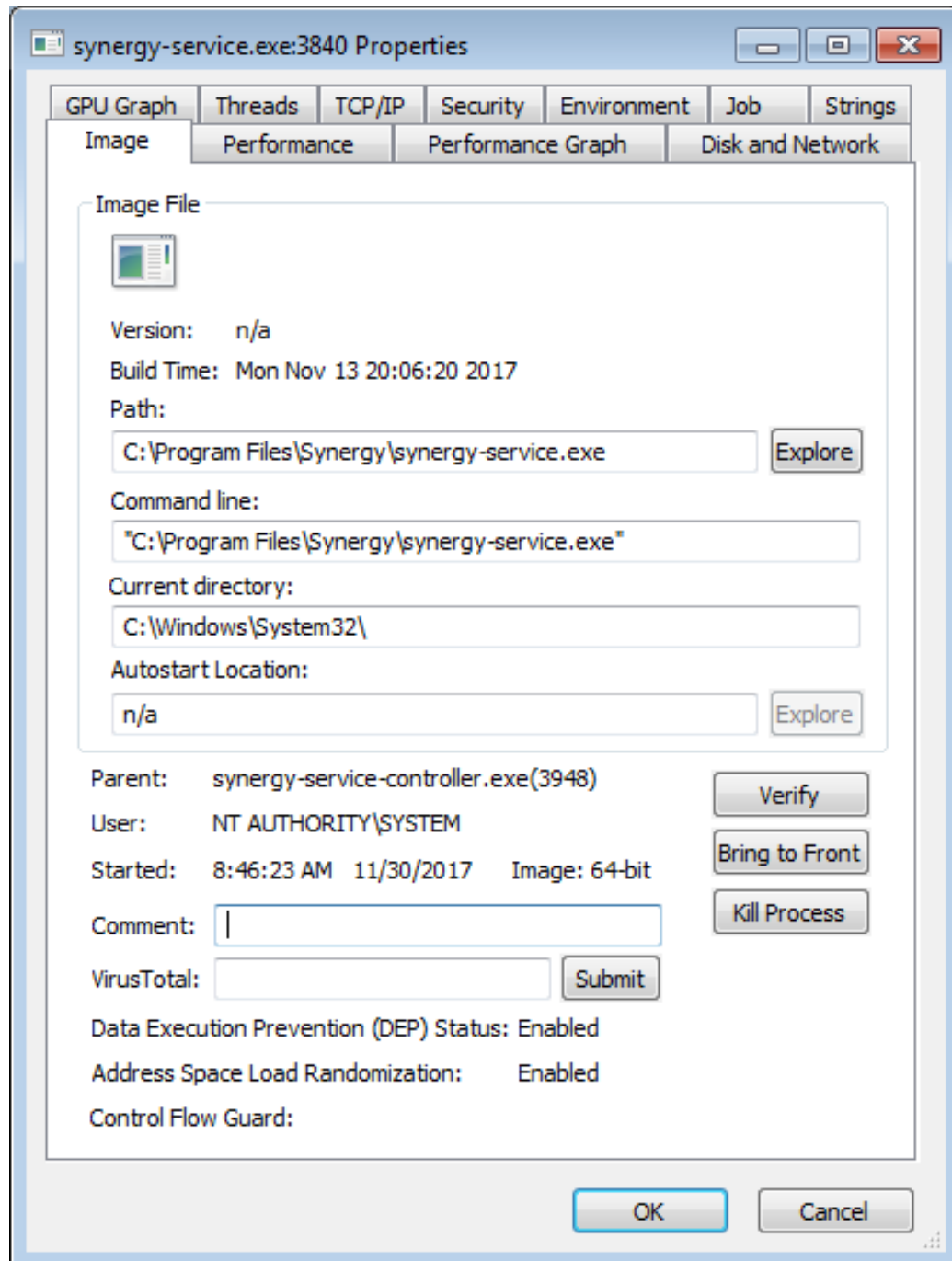
Screenshot 4.3: Installer certificate properties



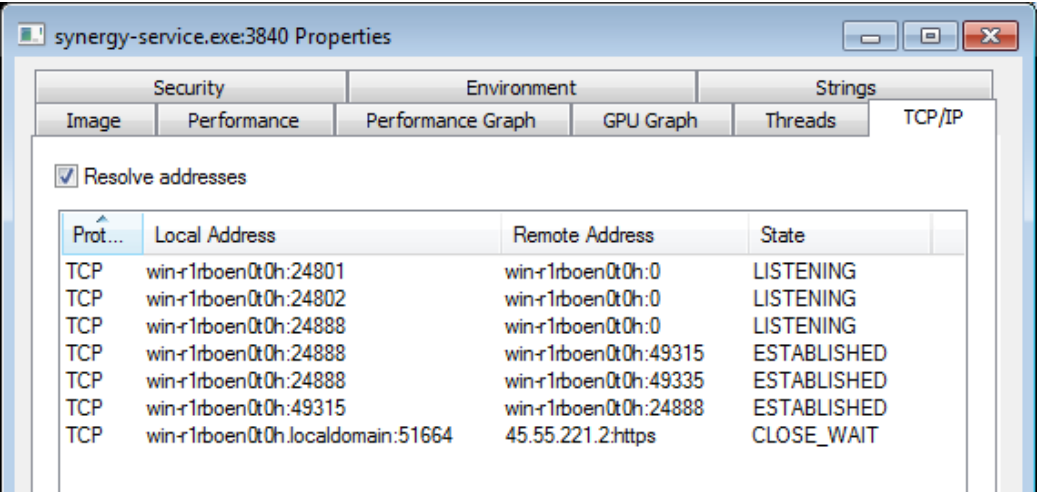
Screenshot 4.9: Process details for synergy-config.exe



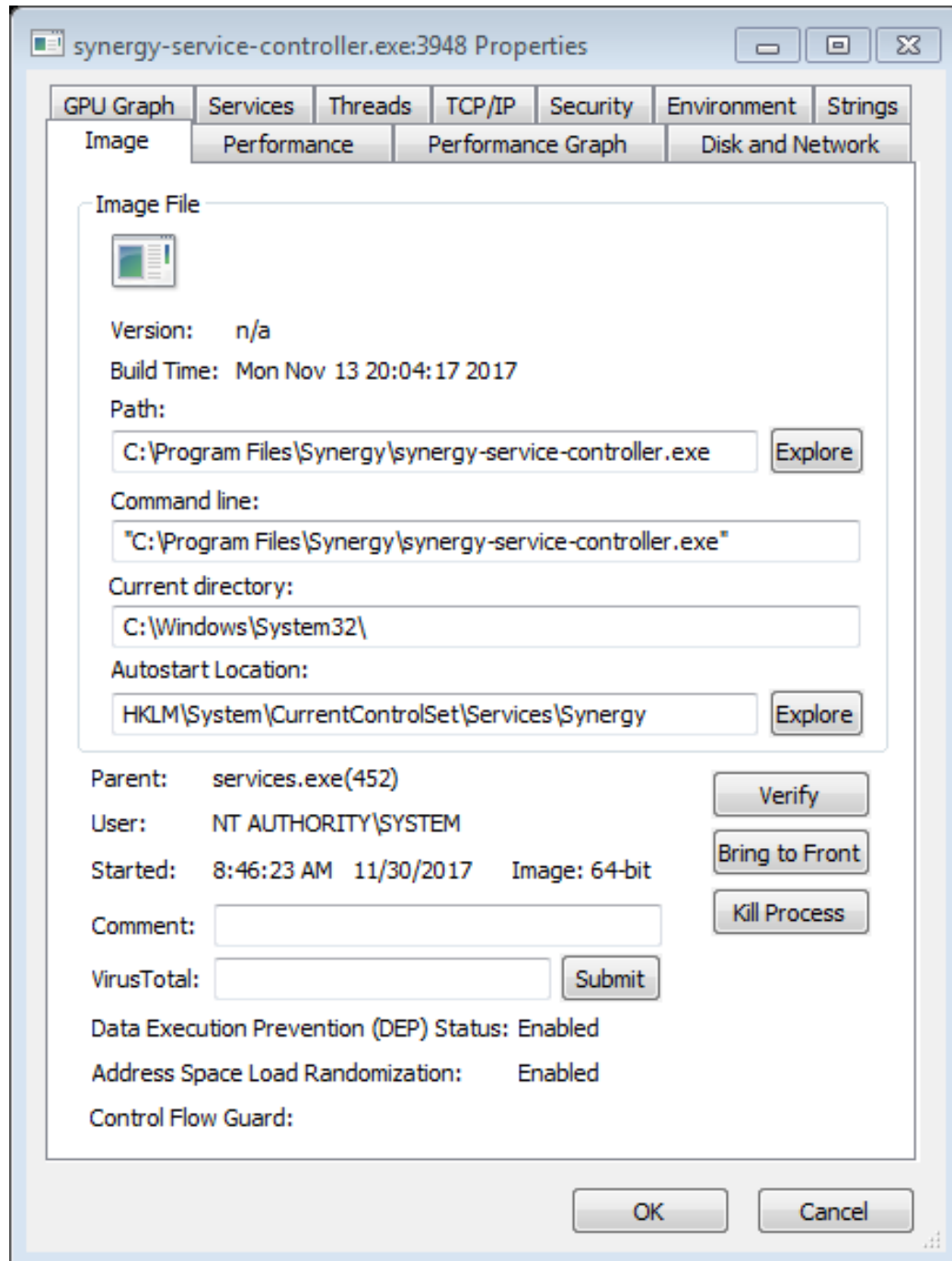
Screenshot 4.10: TCP/IP details for synergy-config.exe



Screenshot 4.11: Process details for synergy-service.exe



Screenshot 4.12: TCP/IP details for synergy-service.exe



Screenshot 4.13: Process details for synergy-service-controller.exe

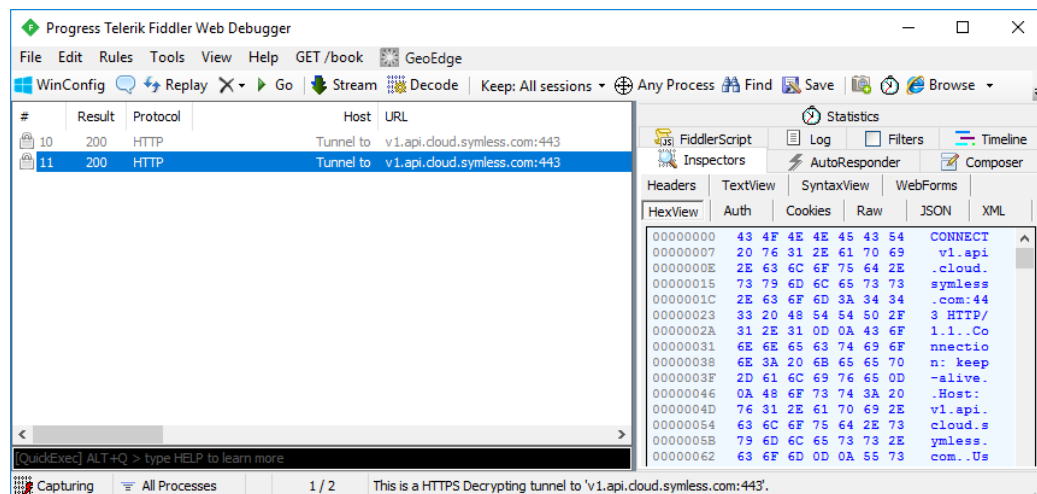
Chapter 5

Communications

There are multiple levels of communication that should be looked at.

5.1 Configuration

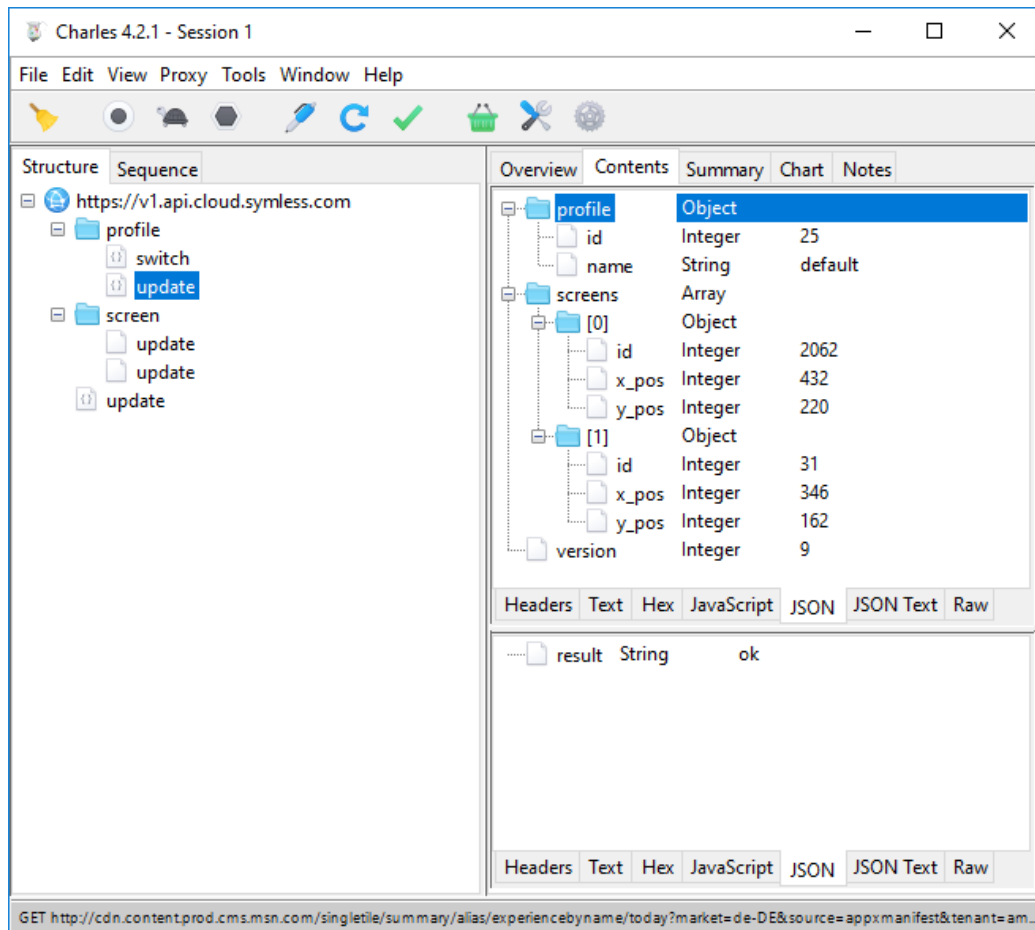
Traffic monitoring of the configuration part does not seem to be a problem - Synergy seems to communicate through a https decoding proxy like Fiddler¹ or Charles² without complaining.



Screenshot 5.1: Fiddler showing Synergy connections

¹<https://www.telerik.com/fiddler>

²<https://www.charlesproxy.com/>



Screenshot 5.2: Charles showing Synergy connection details

Requirement 12 (Configuration Certificate Pinning). *Certificate pinning should ensure that Synergy is only talking to Symless servers when speaking to `v1.api.cloud.symless.com`.*

The author has drafted a test suite on GitLab³.

A simple workaround is possible on Linux and macOS by adding the real IP address of `v1.api.cloud.symless.com` to the hosts file⁴, and changing the priorities for `hosts` in `nsswitch.conf`⁵ as an alternative to certificate pinning, since IP hijacking would be way more complicated than DNS hijacking.

³<https://gitlab.com/ccrdude/symless-cloud-tests>

⁴[https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file))

⁵https://en.wikipedia.org/wiki/Name_Service_Switch

5.1.1 Software update

Queries to `/update` submit the current software version and get in return the latest version, and whether the update is optional or mandatory.

Listing 5.1: API call `/update`

```

1 {
2   "currentVersion": "2.0.1-stable"
3 }
```

Returns

Listing 5.2: API answer `/update`

```

1 {
2   "latestVersion": "2.0.2-stable",
3   "update": "optional"
4 }
```

This can be reviewed in test case method procedure `TestQueryUpdate`⁶:

Listing 5.3: Simple call to `/update`

```

procedure TTestCaseSynergyCloudV1.TestQueryUpdate;
var
  h: THTTPSend;
  sl: TStringList;
  b: boolean;
begin
  h := THTTPSend.Create;
  sl := TStringList.Create;
  sl.Add('{ "currentVersion": "2.0.1-stable" }');
  try
    h.Document.Seek(0, soFromBeginning);
    h.Document.SetSize(0);
    sl.SaveToStream(h.Document);
    Status('https://v1.api.cloud.symless.com/update');
    Status(sl.Text);
    b := h.HTTPMethod('POST', 'https://v1.api.cloud.symless.
      ↪ com/update');
    CheckTrue(b, 'POST https://v1.api.cloud.symless.com/
      ↪ update');
```

⁶<https://gitlab.com/ccrdude/symless-cloud-tests/blob/master/source/SymlessCloudV1Tests.pas>


```
        if b then begin
            sl.Clear;
            h.Document.Seek(0, soFromBeginning);
            sl.LoadFromStream(h.Document);
            Status(sl.Text);
        end;
        CheckEquals(200, h.ResultCode);
    finally
        h.Free;
        sl.Free;
    end;
end;
```

5.1.2 Profile switch

Listing 5.4: API call /profile/switch

```
1 {
2   "profile":
3   {
4     "name": "default"
5   },
6   "screen":
7   {
8     "ipList": "192.168.60.129",
9     "name": "DESKTOP-G628KTS",
10    "status": "Disconnected"
11  }
12 }
```

Returns

Listing 5.5: API answer /profile/switch

```
1 {
2   "profile_id": 25,
3   "screen_id": 2062
4 }
```

5.1.3 Profile update

`/profile/update` is called whenever the layout is changed in the user interface.

Listing 5.6: API call `/profile/update`

```
1 {
2   "profile":
3   {
4     "id": 25,
5     "name": "default"
6   },
7   "screens":
8   [
9     {
10      "id": 2062,
11      "x_pos": 260,
12      "y_pos": 161
13    },
14    {
15      "id": 31,
16      "x_pos": 346,
17      "y_pos": 162
18    }
19  ],
20   "version": 15
21 }
```

Returns

Listing 5.7: API answer `/profile/update`

```
1 {
2   "result": "ok"
3 }
```

5.1.4 Screen update

A query to `/screen/update` informs the cloud about the status of a screen.

Listing 5.8: API call `/screen/update`

```
1 {
2   "id": 2062,
```

```

3   "name": "DESKTOP-G628KTS",
4   "status": "Connecting"
5 }

```

5.2 Core synchronization

5.3 Log sending

The log is sent via POST to <https://symless.com/api/client/log>, as multipart mime. It returns a JSON object with a public URL where the log can be queried.

Listing 5.9: Begin of POST content to /api/client/log

```

--boundary_.oOo._OTQ2NQ==ODU2NzE5MA==
Content-Disposition: form-data; name="logId"

25-2017-11-27T19-45-36
--boundary_.oOo._OTQ2NQ==ODU2NzE5MA==
Content-Disposition: form-data; name="log"; filename="
  ↳ 25-2017-11-27T19-45-36.log"

[ Core ] [2017-11-24T10:33:14] DEBUG: event queue is ready
[ Core ] [2017-11-24T10:33:14] DEBUG: unregistered hotkey id=1
[ Router ] [2017-11-24T13:20:09] error: Read error on
  ↳ connection 7: The network connection was aborted by the
  ↳ local system (code 1236)
[...]

```

Returns

Listing 5.10: API answer /api/client/log

```

1 {
2   "success": true,
3   "message": "Upload path: https:\\\\synergy-logs.symless.com
4     ↳ \2017-11-27\25-2017-11-27T19-45-36.log"
5 }

```

Missing certificate pinning allows to intercept `https` traffic with a fake certificate here.

Requirement 13 (Send Log Certificate Pinning). *Certificate pinning should ensure that Synergy is submitting logs only to Symless servers when speaking to `symless.com/api/client/log`.*

Chapter 6

Attack Vectors

6.1 Using `userId` and `userToken`

Both *userId* and *userToken* are not that difficult to get. Once an attacker has them, he can set up another Synergy desktop using these, and monitor the clipboard.

1. Get *userId* and *userToken*.
2. Install Synergy 2 on attacking machine.
3. Close Synergy UI.
4. Stop Synergy system service.
5. Run `regedit.exe`.
6. Navigate to `HKEY\CURRENT\USER\SOFTWARE\Symless\Synergy`.
7. Set `userId`.
8. Set `userToken`.
9. Set `profileId` to retrieved `userId`.
10. Set `screenId` to random value.
11. Start Synergy system service.
12. Open Synergy UI.
13. On attacked machine, copy something into the clipboard, move to screen border.

14. On attacking machine, paste from clipboard.

This obviously is a quick first draft that can be refined. Instead of manually retrieving the clipboard, code that monitors and logs clipboard contents would be helpful. Instead of using the Synergy 2 software, a minimal client based on the open source¹ or traffic monitoring would simplify access.

This minimal client should define a screen width or height of one pixel and place itself between existing monitors to make sure it gets notified of clipboard changes whenever the user switches between desktops.

Missing Test 1 (Proof of Concept). *A Proof of Concept based on the code could demonstrate this further.*

Since Synergy communicates without certificate pinning, traffic monitoring would not be a problem².

The following ways to retrieve *userId* and *userToken* are possible; with probably more existing.

6.1.1 Support forum

Since the support forum recommends to post logs there³, monitoring it for new posts and extracting information there is a simple approach to get *userToken* and possible *userId*.

6.1.2 Pastebin

Since the support forum recommends to upload logs to Pastebin⁴, monitoring Pastebin for new Synergy 2 logs might be a simple approach, depending on how easy it is to parse Pastebin.

6.1.3 One-time physical access, using the registry

With one-time physical access to the machine that is logged on to as either the user or an administrator, both values can be retrieved from the registry by accessing *userId* and *userToken* in this registry key:

HKEY_CURRENT_USER\SOFTWARE\Symless\Synergy

¹<https://github.com/symless/synergy-core/tree/master/src>

²section 5 on page 69

³See section 4.4.3 on page 58

⁴See section 4.4.3 on page 58

Steps would be simple:

1. Run `regedit.exe` using the *Start* menu
2. If the account logged in is not the Synergy user, use *File – Load hive...* to load the registry hive file of that user.
3. Navigate to `HKEY_CURRENT_USER\SOFTWARE\Symless\Synergy`
4. Copy value of `userId`
5. Copy value of `userToken`

6.1.4 One-time physical access, using the browser history

If another person has access to your browser, it can look up the log address in your browser history. With access to URLs, the `userId` can be retrieved from the filename part of the URL, and the `userToken` from its contents.

6.1.5 One-time remote code execution

The same values can be retrieved (and then transmitted) by code executed either in the context of the user account that uses Synergy, or any administrator, by accessing the registry key mentioned above.

6.1.6 Bookmark and history sharing

There are various methods of sharing browser history across machines, so due to the log being available without protection by URL, the physical access could be to any owned machine. With access to URLs, the `userId` can be retrieved from the filename part of the URL, and the `userToken` from its contents.

6.1.7 Network sniffer

Since the log server uses `https`, the file location is encrypted and not easily available to a network sniffer on the same network. A proxy supporting `https` injection would allow it though. This would either require access to install the injectors root certificate, or social engineering to get the user to do it. With access to URLs, the `userId` can be retrieved from the filename part of the URL, and the `userToken` from its contents.

6.1.8 Tracking software

There are tons of toolbars and other browser plugins that are adware and/or tracking software and do track all browser URLs. With access to such information, the `userId` can be retrieved from the filename part of the URL, and the `userToken` from its contents.

Here are some adwares from the first page of Google search results querying `adware tracking urls`⁵:

Adware.2Search Adware.2Search monitors URLs visited by Internet Explorer and displays similar URLs to the user.⁶

Adware.Adpopup Adware.Adpopup is an adware component that records URLs visited during Web browsing, and then generates pop-up advertisements.⁷

Adware.Tbon Adware.Tbon is an adware program from The Best Offer Networks online advertising company. It tracks URLs visited through a variety of Web browsers and displays advertisements based on these URLs.⁸

The authors of such adwares would have immediate access to the data in question. The adwares might transmit the data using plain http, making it easier to intercept. And the adware servers might not store this data as safe as should be expected.

6.2 DNS Spoofing

Using DNS Spoofing⁹, an attacker could proxy `v1.api.cloud.symless.com` and inject it's own listener between screens. This would be possible due to no certificate pinning for the `https` traffic being in place¹⁰.

There is a lot of malware that uses DNS changing methods. A few examples widely spread enough to have made it into Wikipedia follow.

⁵The author does not recommend the use of Symantec, these links are present simply because they're the first results found on said query.

⁶https://www.symantec.com/security_response/writeup.jsp?docid=2005-080302-3232-99

⁷https://www.symantec.com/security_response/writeup.jsp?docid=2003-102117-2037-99

⁸https://www.symantec.com/security_response/writeup.jsp?docid=2006-010515-2519-99

⁹https://en.wikipedia.org/wiki/DNS_spoofing

¹⁰See screenshot 5.2 on page 70

DNSChanger From Wikipedia¹¹: “DNSChanger is a DNS hijacking Trojan. The work of an Estonian company known as Rove Digital, the malware infected computers by modifying a computer’s DNS entries to point toward its own rogue name servers, [...]”

Alureon aka TDSS From Wikipedia¹²: “Alureon (also known as TDSS or TDL-4) is a trojan and bootkit created to steal data by intercepting a system’s network traffic [...]”

Trojan.Win32.DNSChanger From Wikipedia¹³: “DNS changer Trojans are dropped onto systems by other malware such as TDSS or Koobface. The DNS-Changer-Trojan is a malicious .exe file, but is unable to spread of its own accord. It may therefore perform several actions of an attacker’s choice on an compromised computer, such as changing the Domain Name Server (DNS) settings in order to divert traffic to unsolicited, and potentially illegal and/or malicious domains. The Win32.DNSChanger is used by organized crime syndicates to maintain Click-Fraud.”

Koobface ¹⁴ “mong the components downloaded by Koobface are a DNS filter program that blocks access to well known security websites and a proxy tool that enables the attackers to abuse the infected PC.”

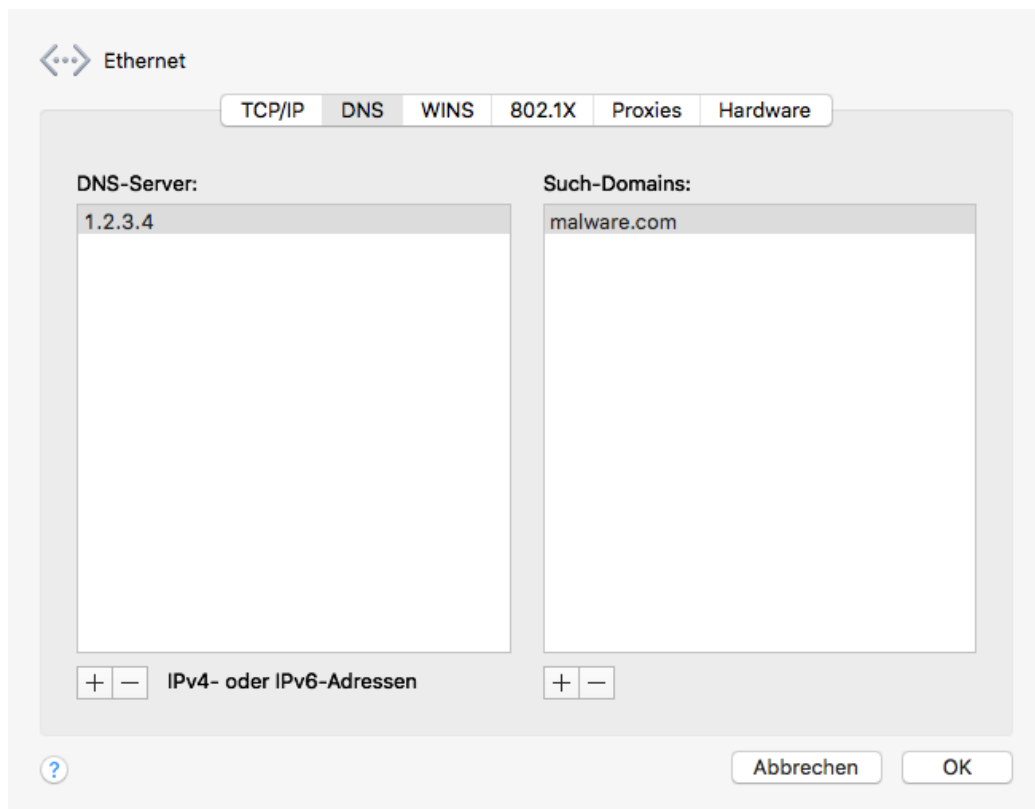
The danger about DNS spoofing is that protecting your own machines might not be sufficient. If the weakest machine within a network is infected, it can set up a fake DHCP and start redirecting others from there, without having actual code or data on the redirected machines.

¹¹<https://en.wikipedia.org/wiki/DNSChanger>

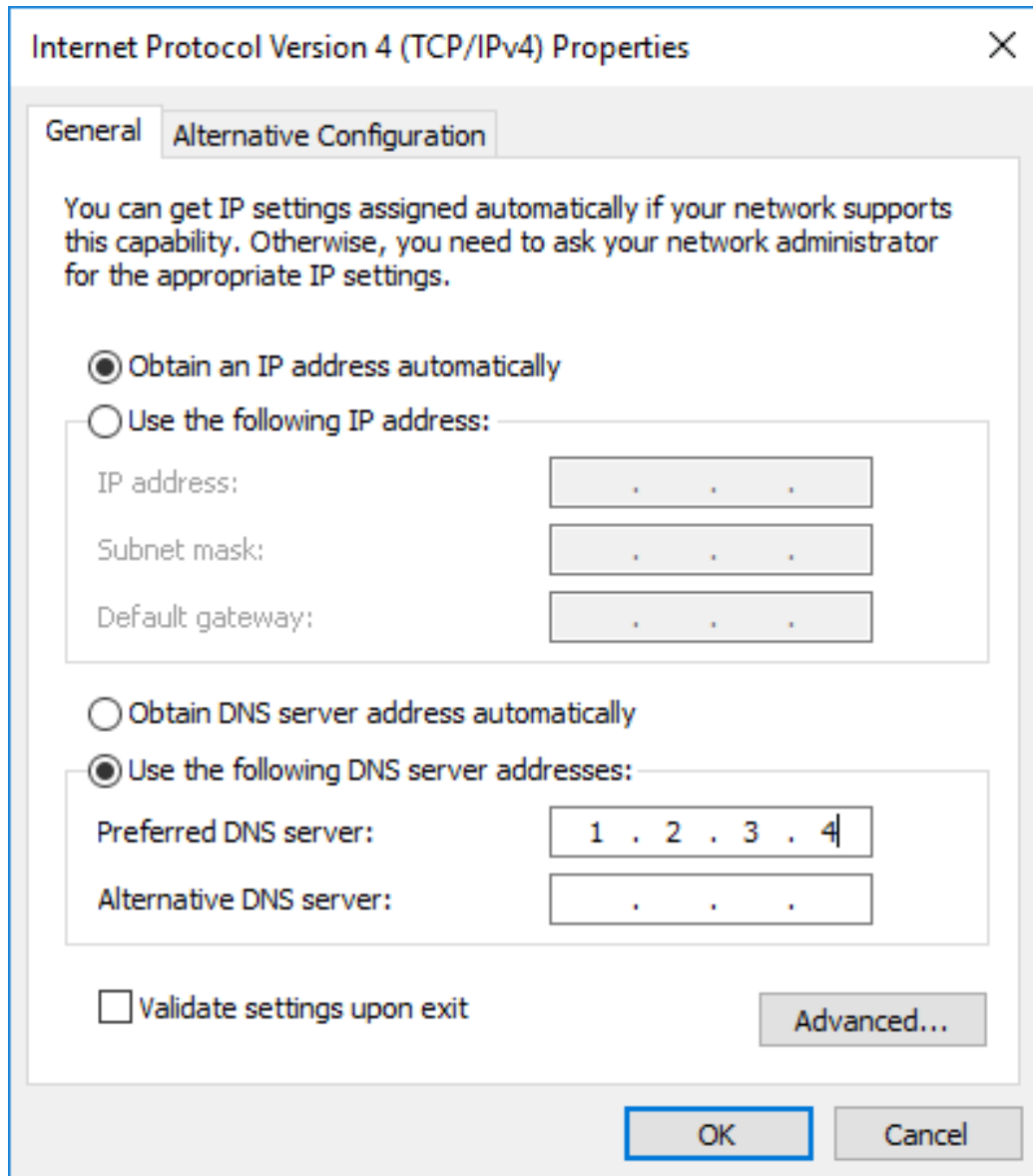
¹²<https://en.wikipedia.org/wiki/Alureon>

¹³<https://en.wikipedia.org/wiki/Trojan.Win32.DNSChanger>

¹⁴<https://en.wikipedia.org/wiki/Koobface>



Screenshot 6.1: Custom DNS settings on macOS High Sierra



Screenshot 6.2: Custom DNS settings on Windows 10

Chapter 7

Summary

The big amount of attempts to appear anonymous (whois information, certificate, missing company name and imprint) makes it impossible to put trust into the vendor. With a software that has access to very sensitive data¹, this is an absolute no-go.

Website and software come without any privacy policy. The software transmits personally identifiable and personally identifying information without user consent nor the mandatory information about purposes of use and storage.

PII is even stored on a public server without access control. This includes the OAuth access token that could probably be used for attacks that would allow e.g. listening to clipboard contents.

The product can clearly be labeled as spyware, which could be reduced to tracking software if the vendor adds required information to website and product and improves the log sending workflow.

Communications are done through `https`, but not pinned to a Symless certificate, so that man-in-the-middle attacks are possible.

¹All clipboard content, possibly including account logins and passwords

Appendix

List of Screenshots

2.1	Synergy in California	11
3.6	The website shop is asking for PII without informing about receivers or purposes	18
3.9	The refund confirmation received via email	20
3.10	Credit card notifications show company Symless in GB	21
3.11	The support page does not inform about the involved third party	22
3.12	The support page was suspended for the author	23
3.13	The support desk account of the author was removed	24
3.14	The website login was suspended for the author	25
3.15	The formal information request was received	27
3.16	Request before responsible disclosure, written January 9th, 2018, 10:09 a.m.	30
3.17	Request listed in thread overview	31
3.18	Closing commit for the disclosure discussion	31
3.1	The website showing off the product	34
3.2	The website listing well known customers	35
3.3	The website security information from Firefox lists the certifi- cate as having no ownership information	36
3.4	The certificate information from Firefox does not show the organization	37
3.5	Firefox warning about unsecure content	38
3.7	The website shop offering payment methods	38
3.8	The invoice listing Symless company details	39
4.4	The installer failing on Windows 8.x	42
4.5	The installer ready to start	43
4.6	The installer has finished	44
4.7	Service Manager showing Synergy service details	47
4.8	Process details for crashpad_handler.exe	49

4.14	The login prompt shown by the software	50
4.15	The login shown in the systems standard browser	51
4.16	Software failure after login	52
4.17	Registry entries used by Synergy	52
4.18	Context menu offers upload of log	53
4.19	Log available via URL after upload only	53
4.20	Log subdomain certificate not showing the organization either	54
4.21	Support website asking to spread logs	57
4.22	Forum asking to spread logs	58
4.23	Facebook post mentioning open source	60
4.24	GitHub start page for Synergy core project	60
4.1	Digital signatures of installer	61
4.2	Digital signature details of installer	62
4.3	Installer certificate properties	63
4.9	Process details for synergy-config.exe	64
4.10	TCP/IP details for synergy-config.exe	65
4.11	Process details for synergy-service.exe	66
4.12	TCP/IP details for synergy-service.exe	67
4.13	Process details for synergy-service-controller.exe	68
5.1	Fiddler showing Synergy connections	69
5.2	Charles showing Synergy connection details	70
6.1	Custom DNS settings on macOS High Sierra	81
6.2	Custom DNS settings on Windows 10	82

Listings

3.1	WhoIs record of symless.com	14
4.1	Installer WiX script component part	44
4.2	Installer WiX script files part	45
4.3	Installer WiX script registry part	45
4.4	A few PII containing lines from the logs	56
5.1	API call /update	71
5.2	API answer /update	71
5.3	Simple call to /update	71
5.4	API call /profile/switch	72
5.5	API answer /profile/switch	72
5.6	API call /profile/update	73
5.7	API answer /profile/update	73
5.8	API call /screen/update	73
5.9	Begin of POST content to /api/client/log	74
5.10	API answer /api/client/log	74

List of Requirements

1	Requirement (Imprint)	13
2	Requirement (Website Privacy Policy)	17
3	Requirement (Shop Privacy Policy)	19
4	Requirement (Reveal sharing with ZenDesk)	22
5	Requirement (Proper Privacy Request handling)	26
6	Requirement (Software Backtrace Privacy Policy)	49
7	Requirement (Software Privacy Policy)	53
8	Requirement (No public PII)	56
9	Requirement (No unnecessary data in logs)	56
10	Requirement (Support website privacy information)	57
11	Requirement (Forum log handling)	59
12	Requirement (Configuration Certificate Pinning)	69
13	Requirement (Send Log Certificate Pinning)	75

List of Recommendations

1	Recommendation (Company specific certifite)	13
2	Recommendation (EV certificate)	13
3	Recommendation (No mixed content)	13
4	Recommendation (Public WhoIs information)	15
5	Recommendation (Non-subscription PayPal payment)	19
6	Recommendation (Codesign with SHA-256)	41
7	Recommendation (Update OpenSSL to 1.0.2m)	45
8	Recommendation (Inform on new behaviour)	51
9	Recommendation (Improve data storage)	52
10	Recommendation (Improve uninstall)	59

List of Missing Tests

1	Missing Test (Proof of Concept)	77
---	---	----

List of URLs

http://pages.uoregon.edu/koch/texshop/	p. 93
http://web.archive.org/web/20121025143706/http://antispwarecoalition.org/documents/2007definitions.htm	p. 55
http://who.godaddy.com/whoischeck.aspx?domain=symless.com	p. 14
http://wixtoolset.org/	p. 41
http://www.legislation.gov.uk/ukxi/2003/2426/regulation/6/made	p. 25
http://www.tug.org/texworks/	p. 93
https://beta.companieshouse.gov.uk/company/08066283	p. 9
https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer	p. 93
https://documentation.backtrace.io/product_integration_minidump_crashpad/index.html	p. 48
https://en.wikipedia.org/wiki/Alureon	p. 80
https://en.wikipedia.org/wiki/Code_signing	p. 40
https://en.wikipedia.org/wiki/DNSChanger	p. 80
https://en.wikipedia.org/wiki/DNS_spoofing	p. 79
https://en.wikipedia.org/wiki/Hosts_(file)	pp. 49, 70
https://en.wikipedia.org/wiki/Koobface	p. 80
https://en.wikipedia.org/wiki/Name_Service_Switch	p. 70
https://en.wikipedia.org/wiki/Qt_(software)	p. 44
https://en.wikipedia.org/wiki/Responsible_disclosure	p. 7
https://en.wikipedia.org/wiki/SHA-1	p. 41
https://en.wikipedia.org/wiki/SHA-2	p. 41
https://en.wikipedia.org/wiki/Trojan.Win32.DNSChanger	p. 80
https://en.wikipedia.org/wiki/Windows_Installer	p. 40
https://github.com/symless/synergy	p. 59
https://github.com/symless/synergy-core	p. 60
https://github.com/symless/synergy-core/tree/master/dist/wix	p. 41
https://github.com/symless/synergy-core/tree/master/src	p. 77
https://gitlab.com/ccrdude/symless-cloud-tests	p. 70
https://gitlab.com/ccrdude/symless-cloud-tests/blob/master/source/SymlessCloudV1Tests.pas	p. 71
https://miktex.org	p. 93
https://msdn.microsoft.com/en-us/library/windows/desktop/bb226801(v=vs.85).aspx	p. 53

https://pastebin.com/	p. 59
https://symless.com	p. 12
https://symless.com/account/refund/request	p. 19
https://symless.com/api/client/log	p. 74
https://symless.com/forums/forum/17-self-support/	p. 29
https://symless.com/forums/profile/1-dan-sorahan/	p. 10
https://symless.com/forums/profile/27344-andrew-nelless/	p. 10
https://symless.com/forums/profile/27559-karen-williams/	p. 10
https://symless.com/forums/profile/27614-joe-abasolo/ .	p. 10
https://symless.com/forums/profile/30885-sarah-hebert/ .	p. 10
https://symless.com/forums/profile/7-jerry-hou/	p. 10
https://symless.com/forums/profile/8-nick-bolton/	p. 9
https://symless.com/forums/profile/9-malcolm-lowel/	p. 10
https://symless.com/forums/staff/	p. 9
https://symless.com/forums/topic/3207-synergy-2-how-to-send-your-logs/	p. 59
https://symless.com/forums/topic/5067-auto-config-service-ssl-certificate-broken-also-your-customer-support-for-do=findComment&comment=22429	p. 31
https://symless.com/forums/topic/5092-security-issues-in-synergy-2/	p. 29
https://symless.com/support	p. 22
https://symless.zendesk.com/	p. 22
https://synergy-logs.symless.com	p. 54
https://twitter.com/NickBoltonUK	p. 10
https://twitter.com/Synergy_App	p. 10
https://uk.linkedin.com/in/nbolton/de	p. 9
https://www.charlesproxy.com/	pp. 69, 93
https://www.cloudflare.com/en/ssl/	p. 13
https://www.crunchbase.com/person/nick-bolton-3	p. 11
https://www.facebook.com/Symless/	p. 10
https://www.facebook.com/nbolton4	p. 10
https://www.freepascal.org/	p. 94
https://www.lazarus-ide.org/	p. 94
https://www.linkedin.com/company/2851905/	p. 9
https://www.linkedin.com/in/amy-fox-ba4ab09b/	p. 10
https://www.linkedin.com/in/dansorahan/	p. 10
https://www.linkedin.com/in/julia-katharina-klein-ma-msc-bb70a542/	p. 10
https://www.linkedin.com/in/malcolm-lowel-75771ab1/	p. 10
https://www.linkedin.com/in/polly-jones-909a73101/	p. 10

https://www.linkedin.com/in/xinyu-hou-aa310850/	p. 10
https://www.openssl.org	p. 44
https://www.safer-networking.org/products/filealyzer/	p. 93
https://www.symantec.com/security_response/writeup.jsp?docid=2003-102117-2037-99	p. 79
https://www.symantec.com/security_response/writeup.jsp?docid=2005-080302-3232-99	p. 79
https://www.symantec.com/security_response/writeup.jsp?docid=2006-010515-2519-99	p. 79
https://www.symless.com/download	p. 93
https://www.telerik.com/fiddler	pp. 69, 93
https://www.tug.org/mactex/	p. 93
https://www.whois.com/whois/symless.com	p. 14
https://www.wireshark.org	p. 93

Used Software

Synergy 2.0.1 The software that's analyzed here,

<https://www.symless.com/download>

Synergy 2.0.2 The software that's analyzed here,

<https://www.symless.com/download>

Synergy 2.0.4 The software that's analyzed here,

<https://www.symless.com/download>

Charles 4.2.1 A proxy that allows to monitor **https** traffic,

<https://www.charlesproxy.com/>

Fiddler 4.6.20173.38786 A proxy that allows to monitor **https** traffic,

<https://www.telerik.com/fiddler>

FileAlyzer 2.0.5.57 A file content analysis tool,

<https://www.safer-networking.org/products/filealyzer/>

WireShark A monitor for all network traffic,

<https://www.wireshark.org>

Process Explorer 16.21 Advanced process explorer,

<https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer>

TeXShop 3.92 A LaTeX environment for macOS,

<http://pages.uoregon.edu/koch/texshop/>

TeXworks 0.6.2 A LaTeX environment for Windows,

<http://www.tug.org/texworks/>

MacTeX-2017 A TeX distribution for macOS,

<https://www.tug.org/mactex/>

MiKTeX A TeX distribution for Windows,

<https://miktex.org>

Lazarus 1.8 An IDE and component library for FreePascal used for test code,

<https://www.lazarus-ide.org/>

FreePascal 3.0.4 A Pascal compiler used for test code,

<https://www.freepascal.org/>